LA ENCICLOPEDIA DE LOS SERVICIOS DE CERTIFICACIÓN PARA LAS ADMINISTRACIONES LOCALES

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

RED
RED DE ENTIDADES LOCALES POR LA TRANSPARENCIA Y PARTICIPACIÓN CIUDADANA

PRESENTACIÓN

El despliegue de la administración electrónica como facilitadora de la transparencia en la gestión pública, es una realidad indiscutible pero condicionada por una normativa que prevé todo un conjunto de derechos y obligaciones para las administraciones y la ciudadanía que condicionan su despliegue integral.

Desde hace ya unos años, el principal freno a toda esta actividad se centra en la forma de identificarse y acceder a los datos, en definitiva en los certificados electrónicos. La ciudadanía e incluso los empleados públicos renuncian al uso de estas plataformas digitales para evitar su identificación sin otro motivo aparente que el desconocimiento o la inseguridad.

Pues bien, el objetivo de esta nueva publicación de la RED es ayudar a los ayuntamientos, especialmente a los de menor población, a definir su propia hoja de ruta en los distintos procesos de gestión que requiere la identificación en el acceso a los datos dentro del proceso global de transformación digital de las entidades locales.

La UE propone incrementar la transparencia de las plataformas digitales y al mismo tiempo hace un llamamiento para asegurar la identidad digital en los accesos. Más transparencia, más seguridad, porque la facilidad y seguridad para acceder al dato es lo que permite que una institución sea realmente transparente.

Quiero, por último, agradecer el trabajo de los miembros del Grupo de Trabajo de Identidad Digital, funcionarios locales, expertos de la Administración general del Estado y del mundo universitario, para que el objetivo marcado hace unos meses sea hoy una realidad.

Muchas gracias.

Carlos González Serna
Alcalde de Elche
Presidente de la Red de Entidades Locales
por la Transparencia y la Participación Ciudadana de la FEMP

Dentro de la Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias, que tengo el honor de presidir, durante el año 2018 hemos configurado un grupo de trabajo cuyo objetivo fue la creación de una serie de pautas para ayudar a las Administraciones Locales a interpretar de forma práctica y homogénea toda la materia relacionada con Identidad Digital.

Pues bien, tras el trabajo realizado en los últimos meses, por fin ve la luz el presente documento, en forma de Enciclopedia sobre Identidad Digital, donde se pueden encontrar todas las claves que una Entidad Local debe conocer.

Confío en la buena acogida de esta publicación y espero que su utilidad se refleje en el buen hacer del personal que trabaja para prestar un mejor servicio al ciudadano.

Me gustaría manifestar mi agradecimiento, a todas las personas y entidades que han colaborado en este proyecto de manera absolutamente desinteresada:

¡Muchas gracias a todos por este magnífico trabajo!

Ramón Fernández-Pacheco Monterreal
Alcalde de Almería
Presidente de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

Índice

TOMO I

Servicios de Certificación para las AALL

TECNOLÓGICO Y JURÍDICO.
PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS

1 Introducción

La revolución de la tecnología de información, conjuntamente con el desarrollo de la infraestructura de comunicaciones, está haciendo cambiar significativamente las relaciones entre personas y organizaciones, tanto en España como en todo el mundo. Estas nuevas formas de comunicación abren un gran abanico de posibilidades tanto para la ciudadanía como para las empresas.

En España, las distintas Administraciones están apostando decididamente por el Internet de las personas como vía de comunicación, creando portales con información, documentos y servicios de interés público a disposición de la ciudadanía.

Sin embargo es cierto que, desde hace más de diez años, el principal freno a todo esto está en la forma de identificarse y acceder, en definitiva en los certificados electrónicos. La ciudadanía e incluso el personal al servicio de las administraciones públicas renuncian al uso de estas plataformas digitales para evitar su identificación sin otro motivo aparente que el desconocimiento.

El despliegue de la administración electrónica es una realidad y su despliegue es indiscutible pero se ve condicionado por un conjunto muy amplio y disperso de normativas que prevén todo un conjunto de derechos y obligaciones para administraciones y ciudadanía que condicionan su despliegue integral. El derecho de la transformación digital se ha convertido en un revulsivo y un freno para la administración electrónica, aunque no podemos olvidar que su desarrollo es el resultado de un complejo proceso impulsado y al mismo tiempo contenido por otros elementos como la tecnología, el liderazgo y el cambio organizativo.

2 Objetivo y alcance

Por una parte, se considera enciclopedia a un conjunto de conocimientos los cuales pueden ayudar a facilitar el aprendizaje sobre los mismos, y a la vez cooperar con la culturalización de las personas.

El objetivo es mejorar la e-Administración y adoptar soluciones digitales para una prestación eficiente de los servicios públicos.

Una de las razones que nos llevan a redactar este documento, es **conseguir aprender todo lo relacionado con los certificados electrónicos,** de forma que podamos inculcar ese conocimiento ausente en la utilización de técnicas y sistemas criptográficos de clave pública, y se pueda garantizar los principios de Autenticación, Integridad, Confidencialidad y No repudio en las comunicaciones a través de redes abiertas.

Los certificados electrónicos emitidos por cualquier autoridad certificadora a la ciudadanía empresas y administraciones, permiten la realización de trámites telemáticos a través de Internet con plenas garantías de seguridad, evitando así desplazamientos, esperas y errores de cumplimentación de formularios, gracias a la administración electrónica, abierta 24x7.

En este documento se facilitarán los conocimientos necesarios para profundizar en diferentes aplicaciones de los medios electrónicos en las relaciones entre las administraciones públicas y la ciudadanía desde la perspectiva del usuario final, lo que nos permitirá analizar aspectos que no fueron objeto de análisis en el día a día de la gestión administrativa automatizada.

3 A quién va dirigido

A todas aquellas personas tecnólogas y no tecnólogas inmersas en el proceso de Transformación digital de las Administraciones públicas, que necesitan **hacer uso de un certificado digital** de distinta tipología para acceder y gestionar a través de distintas plataformas tecnológicas los expedientes y documentos electrónicos con distintas responsabilidades.

4 Marco Legal y regulatorio

4.1. Marco histórico esencial

Sin que sea necesario remontarnos a otros antecedentes exclusivamente nacionales o sectoriales[1], el origen regulatorio de la firma electrónica podemos situarlo en la **Directiva 1999/93/CE del Parlamento Europeo y del Consejo, por la que se establece un marco comunitario para la firma electrónica**, norma europea de la que trajo causa nuestra **Ley 59/2003, de 19 de diciembre, de Firma Electrónica**, todavía vigente al tiempo de redactar estas líneas. Esta última norma, posteriormente concretada en diferentes regulaciones de carácter sectorial, autonómico o local, ha venido constituyendo el basamento de nuestro ordenamiento en materia de identificación y firma electrónicas, utilizándose como referencia en multitud de normas de Derecho Público posteriores. Por citar las más significativas: La Ley 11/2007, de 22 de junio, de Acceso Electrónico de la ciudadanía a los Servicios Públicos y los Reales Decretos 3/2010 y 4/2010, ambos de 8 de enero de 2010, por los que se regulan el Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad (ENI), respectivamente.

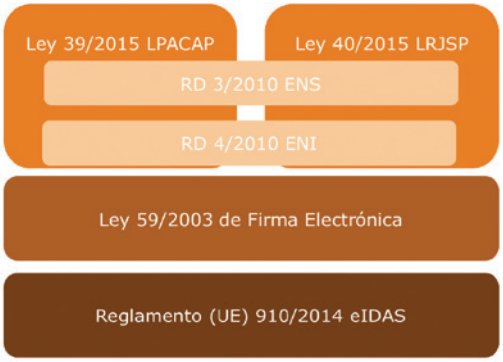
Pese a la existencia de tal normativa, el desenvolvimiento de la firma electrónica en el ambiente del Derecho Público (y, también, en el Derecho Privado) no ha estado exento de obstáculos. La escasa armonización europea en materia de definición, generación y expedición de certificados electrónicos, la presencia de herramientas de firma poco "amigables", la exageración de cierta normativa que ha requerido la utilización de las variantes más exigentes de firma electrónica (firma electrónica reconocida o cualificada) y la ausencia de alternativas sustentadas en un adecuado análisis de riesgos previo que permitan obtener unas garantías alineadas con el procedimiento de que se trate, a un coste de implantación y uso razonables, han contribuido a limitar el uso de los medios electrónicos en la identificación y la firma electrónica y, como consecuencia de ello, la pretendida relación transfronteriza europea.

Así las cosas, las instituciones europeas, conscientes de la necesidad de incrementar la relación electrónica entre los Estados, sus organizaciones, empresas, profesionales y ciudadanos, decidieron trabajar en una nueva norma europea, de obligado cumplimiento, que unificara criterios y garantizara la necesaria interoperabilidad transnacional. De esta pretensión nació el vigente **Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE**, comúnmente conocido como **Reglamento eIDAS**.

La entrada en vigor de la **Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas** (LPACAP, en adelante) y la **Ley 40/2015, de Régimen Jurídico del Sector Público** (LRJSP, en adelante), ambas de 1 de octubre, consagrando el uso de los medios electrónicos en las relaciones externas e internas de las Administraciones Públicas, otorgan a la identificación y a la firma electrónica una importancia capital en el desenvolvimiento de las actividades públicas, precisando su uso y eficacia jurídica.

[1] Entre los que destaca, el Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

La figura siguiente esquematiza el marco jurídico básico[2].



4.2. La Identificación y la firma electrónica en las leyes administrativas

4.2.1. Dos conceptos distintos: identificación y firma

A diferencia de regulaciones previas, las recientes LPACAP y LRJSP han querido diferenciar normativamente dos conceptos tradicionalmente tratados de forma conjunta, aunque claramente distintos: la identificación (electrónica) y la firma (electrónica). La definición de ambos conceptos se reparte en las citadas normas, de la forma que se muestra en la figura siguiente.

La Identificación y la firma en las Leyes 39/2015 y 40/2015

Examinemos ambos conceptos, separadamente.

[2] Fuente: GALÁN, Carlos. "Identificación de la Administración y los interesados", en *La Reforma Legal del Régimen Administrativo. Universidad Carlos III de* Madrid*, 2016.*

4.2.2. Sistemas de identificación de los interesados

El art. 9.1 de la LPACAP es muy claro cuando afirma que las AA.PP. están (irrenunciablemente) **obligadas a verificar la identidad de los interesados** en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

Cuando tal identificación hubiere de realizarse por medios electrónicos, prevé el art. 9.2 que los interesados podrán identificarse electrónicamente ante las AA.PP. a través de cualquier sistema que cuente con un **registro previo** como usuario que permita garantizar su identidad, señalándose entre ellos:

a) Sistemas basados en **certificados electrónicos reconocidos o cualificados de firma electrónica** expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

b) Sistemas basados en **certificados electrónicos reconocidos o cualificados de sello electrónico** expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Sistemas de **clave concertada y cualquier otro sistema** que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

La figura siguiente muestra un esquema de estas posibilidades.

Sistemas de identificación electrónica de los interesados

Independientemente de que cada Administración Pública pueda determinar si sólo admite alguno de estos sistemas para realizar determinados trámites o procedimientos, como se deduce de la figura, la admisión de alguno de los sistemas de identificación previstos en la letra c) anterior conllevará la admisión de todos los previstos en las letras a) y b) para tal trámite o procedimiento. En todo caso, **la aceptación de cualquiera de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas**, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.

4.2.3. Sistemas de firma de los interesados

El art. 10.1 de la LPACAP señala que los interesados podrán firmar (manual o electrónicamente) a través de cualquier medio que permita acreditar el cumplimiento de dos requisitos:

1. La **autenticidad de la expresión de su voluntad y consentimiento**, y
2. La **integridad** e inalterabilidad del documento.

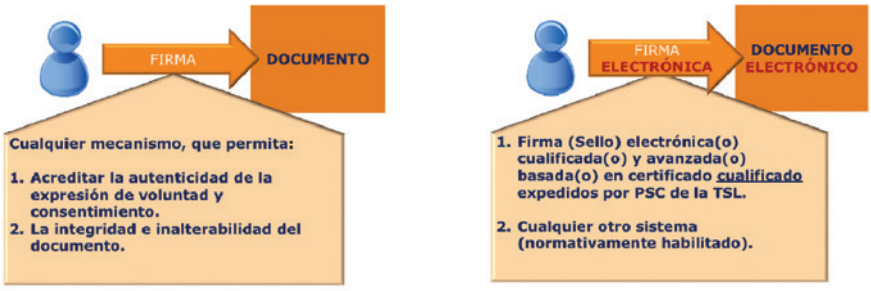
Cuando se trate de una relación electrónica -sigue el art. 10.2-, se considerarán válidos a efectos de firma:

a) Sistemas de **firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados** de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación».

b) Sistemas de **sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados** de sello electrónico incluidos en la «Lista de confianza de prestadores de servicios de certificación».

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

La figura siguiente muestra un esquema de lo dicho.

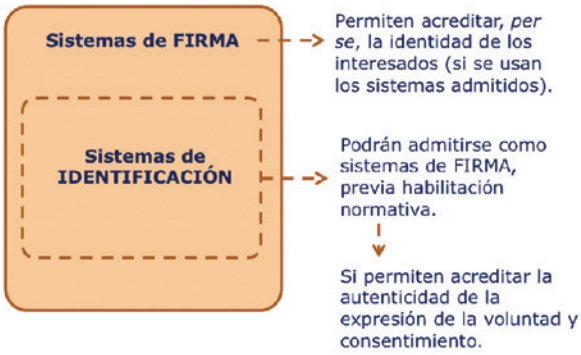


Firma y Firma Electrónica de los interesados

Cada Administración Pública, Organismo o Entidad podrá determinar si sólo admite algunos de estos sistemas para realizar determinados trámites o procedimientos de su ámbito de competencia.

Finalmente, el apartado 3 del art. 10 prevé que **las AA.PP. podrán admitir los sistemas de identificación contemplados en la LPACAP como sistema de firma** cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados -olvidando el legislador la exigencia de integridad señalada de forma general-, cuando así lo disponga expresamente la normativa reguladora aplicable.

Mejores tratos reciben los mecanismos de firma en el apartado 4 del citado precepto, que señala que cuando los interesados utilicen un sistema de firma de los recogidos en el artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.



Admisibilidad cruzada de los mecanismos de identificación y firma

4.2.4. Uso de los medios de identificación y firma de los interesados en el procedimiento administrativo

La exigencia de identificación de los interesados en el desenvolvimiento del procedimiento administrativo, con carácter general, se recoge de nuevo en el art. 11.1 de la LPACAP, admitiéndose a tal propósito cualquier medio de identificación de los señalados anteriormente.

En lo tocante a la firma, el art. 11.2 limita la exigencia de firma a los siguientes supuestos:

a) Formular solicitudes.

b) Presentar declaraciones responsables o comunicaciones.

c) Interponer recursos.

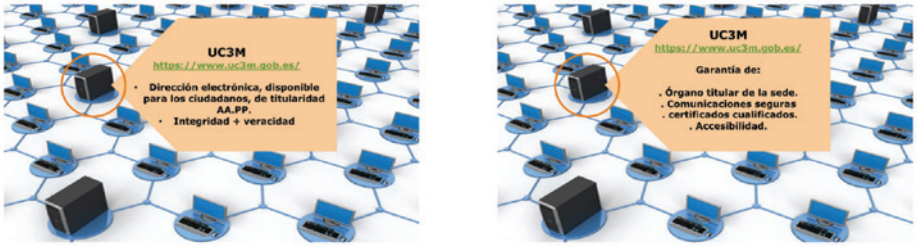
d) Desistir de acciones.

e) Renunciar a derechos.

4.2.5. La identificación electrónica de los sites públicos: la sede electrónica

Según dispone el art. 38.1 de la LRJSP, la sede electrónica es aquella **dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.**

Como es lógico suponer -art. 38.2-, el establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.



La sede electrónica como dirección pública

Sigue el apartado 3 del art. 11 señalando que cada Administración Pública determinará las **condiciones e instrumentos de creación de las sedes electrónicas**, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la **identificación del órgano titular de la sede**, así como los medios disponibles para la formulación de sugerencias y quejas.

La seguridad de la información (expresada a través de las dimensiones recogidas en el RD 3/2010, Esquema Nacional de Seguridad[3]: disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) se pone de manifiesto en el apartado 4 del antedicho precepto, al exigir que las sedes electrónicas dispongan de **sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.**

En todo caso, la publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará en todo caso los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos (art. 11.5).

Finalmente, y siendo más significativo para el propósito de este trabajo, señala el apartado 6 del precepto antedicho, que las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, **certificados reconocidos o cualificados de autenticación de sitio web**, añadiendo "o medio equivalente", expresión poco afortunada con la que el legislador parece guardarse las espaldas en previsión de un eventual uso futuro de otras tecnologías.

[3] Véase "Guía estratégica en seguridad para Entidades Locales. ESQUEMA NACIONAL DE SEGURIDAD (ENS)". FEMP, (2018)

4.2.6. Sistemas de identificación de las AA.PP.

Independientemente del uso de certificados de autenticación de sitios web para la identificación de sus páginas web, la LRJSP señala -art. 40- . que las AA.PP. podrán identificarse mediante el uso de un **sello electrónico basado en un certificado electrónico reconocido o cualificado** que reúna los requisitos exigidos por la legislación de firma electrónica[4], adoptando las medidas adecuadas para facilitar la verificación de tales sellos.

Exige el precepto que los antedichos certificados electrónicos deberán incluir el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

Finalmente, y por la parte que ahora interesa, termina el precepto señalando que la **relación de sellos electrónicos** utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos.

4.2.7. Actuación Administrativa Automatizada

Parece lógico pensar que, entrado el Siglo XXI y contando con el desarrollo tecnológico actual, el desenvolvimiento electrónico de la actuación administrativa no debiera exigir, en todos los casos, la presencia física de una persona que otorgue validez al acto de que se trate.

Consciente de esta realidad, la LRJSP (art. 41.1) consagra el concepto de **actuación administrativa automatizada**, definiéndolo como **cualquier acto o actuación realizada íntegramente a través de medios electrónicos en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público**.

Se trata, por tanto, de actuaciones totalmente automáticas y, por otro lado, extraordinariamente frecuentes en el desarrollo electrónico del procedimiento -como, por ejemplo, en el momento de expedir el preceptivo recibo electrónico tras una solicitud presentada ante un registro electrónico-, que exige, no obstante, el mantenimiento de un vínculo (material y jurídico) entre el mecanismo automático y la responsabilidad exigible al órgano.

Por tal motivo, el apartado 2 del citado precepto señala que deberá establecerse previamente el órgano u órganos competentes, según los casos, para:

- La definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad,
- La auditoría del sistema de información y de su código fuente, en su caso, y
- La indicación del órgano que debe ser considerado responsable a efectos de impugnación.

Como es lógico suponer, la actuación administrativa automatizada exige la presencia de elementos de firma electrónica, como veremos seguidamente.

[4] Que habrá que entender referida, en primera instancia, al Reglamento eIDAS, que desplaza a la todavía vigente Ley 59/2003.

4.2.8. Sistemas de firma electrónica para la actuación administrativa automatizada

El art. 42 de la LRJSP confiere a cada Administración Pública la **potestad para determinar los supuestos de utilización de la firma electrónica** en el desenvolvimiento de su actuación.

Este precepto prevé los siguientes sistemas de firma electrónica:

a) **Sello electrónico** de Administración Pública, órgano, organismo público o entidad de derecho público: que deberá estar basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) **Código seguro de verificación** vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público: siempre en los términos y condiciones previamente establecidos normativamente. Como es conocido, este procedimiento permite la verificación de la integridad del documento (no alteración) mediante el acceso a la sede electrónica de la entidad firmante.

Se muestra un ejemplo tomado de la actuación administrativa de la Agencia Estatal de Administración Tributaria.

Estimado ciudadano:

Como respuesta a su **solicitud de alta en el sistema Cl@ve** le enviamos el Código Seguro de Verificación (CSV) **LMWLSZ5THNHJKWRF**, con el que podrá registrarse en este sistema accediendo a la Sede Electrónica de la Agencia Tributaria, ruta: *Procedimientos, Servicios y Trámites (Información y Registro) - Otros Servicios - Registro y obtención de Cl@ve PIN, Trámites, Registro en Cl@ve con código seguro de verificación* o bien directamente desde los **Trámites Destacados** de la citada Sede.

Ejemplo de Código Seguro de Verificación usado por la AEAT

4.2.9. Firma electrónica del personal al servicio de las AA.PP.

Determinados actos administrativos exigen la firma del titular del órgano competente, en cuanto personificación de tal órgano.

Por tal motivo, y sin perjuicio de lo que hemos visto en relación con la identificación de la sede electrónica y los procedimientos de firma electrónica para la actuación administrativa automatizada, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante **firma electrónica del titular del órgano o empleado público**.

Se trata, por tanto, de una firma "personalizada", en la que la persona física investida de la capacidad y competencia precisas, firma (manifestación de voluntad respecto del documento firmado) y, en su consecuencia, asume la responsabilidad de lo firmado.

El art. 43 de la LRJSP señala que es competencia de cada Administración Pública determinar los sistemas de firma electrónica que debe utilizar su personal, que podrán identificar de forma conjunta al **titular del puesto de trabajo o cargo** y a la **Administración u órgano** en la que presta sus servicios.

Añade el precepto que, por razones de seguridad pública, los sistemas de firma electrónica podrán referirse sólo el **número de identificación profesional** del empleado público. Tal es el caso, por ejemplo, de lo dispuesto en el Real Decreto 668/2015, en relación con la expedición de certificados de empleado público con seudónimo[5].

4.2.10. Interoperabilidad de la firma electrónica

A la vista de lo anterior y de la diversidad de los tipos de firma que pueden utilizarse en ambiente administrativo, el art. 45 de la LRJSP señala la potestad de las Administraciones Públicas para **determinar los trámites e informes** que necesariamente deban incluir firma electrónica cualificada y avanzada basada en certificados electrónicos cualificados de firma electrónica.

Finalmente, y con el propósito de favorecer la interoperabilidad y posibilitar la verificación automática de la firma electrónica de los documentos electrónicos, cuando una Administración utilice sistemas de firma electrónica distintos de aquellos basados en certificado electrónico reconocido o cualificado, para remitir o poner a disposición de otros órganos, organismos públicos, entidades de Derecho Público o Administraciones la documentación firmada electrónicamente, podrá superponer un sello electrónico basado en un certificado electrónico reconocido o cualificado.

4.3. La Identificación y las firmas electrónicas en el Derecho de la Unión Europea

4.3.1. La necesaria armonización transfronteriza

El contenido de la Directiva 1999/93/CE y su heterogénea transposición al ordenamiento de los Estados miembro provocaron que el originario deseo de una relación transfronteriza fluida y garantista entre personas y organizaciones no se materializara adecuadamente.

Efectivamente, la relación entre estados requiere en la mayoría de las ocasiones unos mecanismos fiables y homogéneos en materia de identificación y firma electrónicas. Por ejemplo, no es posible un desarrollo coherente de la contratación pública electrónica si las partes implicadas (poderes adjudicadores y licitadores, de cualquier estado de la UE) no disponen de medios de identificación y firma reconocidos asimismo por todos ellos.

Consciente de esta realidad, las instituciones de la Unión Europea han venido trabajando durante los últimos años en una regulación que, con carácter obligatorio para sus destinatarios europeos, señale de manera armonizada los mecanismos de identificación y firma que deberán ser aceptados por todos en sus relaciones transfronterizas.

[5] Sin que ello sea óbice, como se señala en la norma, para que «Los órganos judiciales y otros órganos y personas legitimadas podrán solicitar que se les revele la identidad de los firmantes con certificado electrónico de empleado público con seudónimo, en los casos previstos en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En ese caso, el prestador de servicios de certificación actuará de conformidad con lo previsto en la Ley 59/2003, de 19 de diciembre.»

Resultado de ello ha sido, como hemos señalado más arriba, el Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, conocido como **Reglamento eIDAS.**

El Reglamento eIDAS persigue, por tanto, asegurar la interoperabilidad en la UE:

- De la **Identificación Electrónica** (de personas y entidades)
- De los **Servicios de Confianza** (entre ellos, la generación y expedición de certificados electrónicos y otros servicios de confianza).

Su condición jurídica (Reglamento Europeo) confiere al Reglamento eIDAS la potestad de ser **directamente aplicable** en los Estados miembro (desplazando, por ejemplo, a la Ley 59/2003, de firma electrónica).

El gráfico siguiente muestra un esquema de los servicios regulados por el Reglamento eIDAS.

Esquema de servicios regulados por el Reglamento eIDAS

Una nueva ley nacional de Servicios de Confianza, que al tiempo de redactar estás líneas permanece en borrador, regulará aquellos aspectos que el Reglamento eIDAS deja a la libre regulación de los Estados miembro.

4.3.2. La Identificación Electrónica en el Derecho de la UE

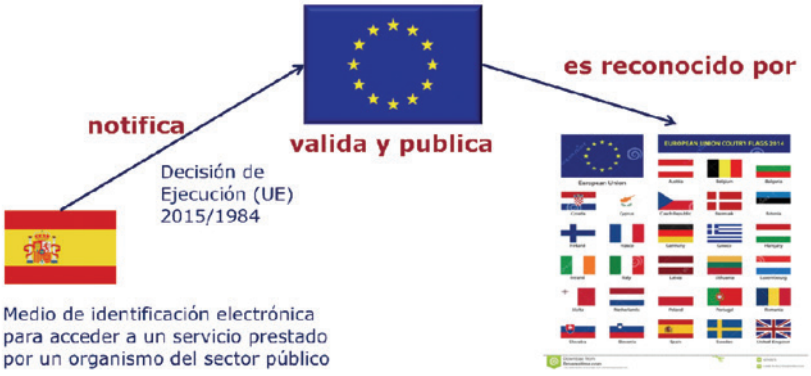
Como hemos señalado, una de las razones que impulsaron a las instituciones europeas la publicación del Reglamento eIDAS fue el deseo de mantener los **principios del mercado interior**, evitando imponer restricciones a la prestación de servicios de confianza en el territorio de un Estado miembro por un prestador de servicios de confianza establecido en otro Estado miembro por razones que entraran en los ámbitos cubiertos por tal norma, permitiendo la libre circulación en el mercado interior de los productos y servicios de confianza que se ajusten al citado Reglamento.

Estos principios relativos al mercado interior posibilitan y obligan al **reconocimiento mutuo de los medios de identificación electrónica** expedidos y **notificados** por los diferentes Estados miembros cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, siempre que tal medio de identificación haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9 del Reglamento eIDAS; el nivel de seguridad de este medio de identificación electrónica corresponda a un **nivel de seguridad** igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto; y el organismo público en cuestión utilice un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea.

Como se muestra en el cuadro siguiente, el Reglamento eIDAS contempla tres **niveles de seguridad**: **Bajo, Sustancial y Alto,** atendiendo al grado de confianza de un medio de identificación en la identidad pretendida o declarada de una persona, niveles de seguridad regulados en el Reglamento de Ejecución (UE) 2015/1502.

Nivel de Seguridad	Descripción
Bajo	Se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un **grado limitado de confianza** en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad;
Sustancial	Se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un **grado sustancial de confianza** en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad;
Alto	Se referirá a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un **grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial**, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos, cuyo objetivo es evitar el uso indebido o alteración de la identidad.

El reconocimiento mutuo de los medios de identificación electrónica será obligatorio a partir del 29 de septiembre de 2018, debiendo los Estados fomentar el uso de los medios de identificación electrónica también en el sector privado.



Esquema del reconocimiento mutuo de los medios de identificación electrónica en la UE

4.3.3. Los Servicios de Confianza

El aseguramiento transfronterizo de la firma electrónica exige que la UE establezca mecanismos a través de los cuales sus usuarios (firmantes emisores, por un lado, y receptores de documentos firmados, por otro) alcancen las debidas garantías respecto del procedimiento de firma usado, la identidad de los firmantes y la adecuada generación y expedición de los certificados digitales por los prestadores de tales servicios.

Esta necesidad ha obligado al Reglamento eIDAS a contemplar dos clases de servicios, el **Servicio de Confianza**, definido como: "El servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.", y el **Servicio de Confianza Cualificado**, más exigente que el anterior y para el que la UE contempla un especial control por parte de las entidades supervisoras de cada Estado miembro y de la propia UE[6].

Sea como fuere, el art. 19 del Reglamento eIDAS exige que los prestadores cualificados y no cualificados de servicios de confianza deberán adoptar las **medidas técnicas y organizativas** adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan, que eviten o reduzcan al mínimo el impacto de los incidentes de seguridad, informando al organismo de supervisión en un plazo no superior a 24 horas tras tener conocimiento y, en caso pertinente, a

[6] En el caso de España, el organismo supervisor es la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) del Ministerio de Energía, Turismo y Agenda Digital.

otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, la autoridad de protección de datos o, incluso, a los propios usuarios, de cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

La figura siguiente muestra este esquema de supervisión de los Prestadores de Servicios de Confianza.

Esquema de Supervisión de los Prestadores de Servicios de Confianza

Como hemos señalado, los **Prestadores de Servicios de Confianza Cualificados** sufren de un régimen de supervisión especial que implica que deberán ser auditados, al menos cada 24 meses, por un organismo de evaluación de la conformidad[7], confirmando que tanto los prestadores cualificados de servicios de confianza como los servicios de confianza cualificados que prestan cumplen los requisitos establecidos en el Reglamento eIDAS.

A efectos de publicidad, cada Estado miembro establecerá, mantendrá y publicará **Listas de Confianza** con información relativa a los prestadores cualificados de servicios de confianza con respecto a los cuales sea responsable, junto con la información relacionada con los servicios de confianza cualificados prestados por cada uno de ellos[8].

Finalmente, aquellos Prestadores Cualificados de Servicios de Confianza que, habiendo superado el procedimiento de verificación de la conformidad señalado, hubieren sido incluidos en la correspondiente Lista de Confianza, podrán usar la **Etiqueta de Confianza «UE»** para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan.

En este sentido, la UE publicó el Reglamento de Ejecución (UE) 2015/806 2015/806 de la Comisión, de 22 de mayo de 2015, por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados.

[7] En España, estos organismos o Entidades de Evaluación de la Conformidad han de ser previa y preceptivamente acreditados por la Entidad Nacional de Acreditación (ENAC) conforme al esquema de acreditación correspondiente.

[8] En España, esta Lista de Prestadores de Servicios de Confianza (TSL) se encuentra permanentemente actualizada y accesible en https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf

Etiqueta de confianza «UE» para servicios de confianza cualificados (en color)

En el ejercicio de sus competencias, y observándose un incumplimiento de alguno de los requisitos del Reglamento eIDAS, el organismo de supervisión (SESIAD, en España) podrá requerir a un prestador cualificado de servicios de confianza que corrija tales incumplimientos. Si este prestador no actúa en consecuencia en el plazo fijado, el organismo de supervisión, teniendo en cuenta el alcance, la duración y las consecuencias del incumplimiento, podrá retirar la cualificación al prestador o al servicio que éste presta, procediendo a actualizar la correspondiente Lista de Confianza.

En la actualidad, los **servicios de confianza cualificados** regulados en el Reglamento eIDAS son los siguientes:

1. Servicio de expedición de certificados electrónicos cualificados de firma electrónica;
2. Servicio de expedición de certificados electrónicos cualificados de sello electrónico;
3. Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web;
4. Servicio de expedición de sellos electrónicos cualificados de tiempo;
5. Servicio cualificado de entrega electrónica certificada;
6. Servicio cualificado de validación de firmas electrónicas cualificadas;
7. Servicio cualificado de validación de sellos electrónicos cualificados;
8. Servicio cualificado de conservación de firmas electrónicas cualificadas;
9. Servicio cualificado de conservación de sellos electrónicos cualificados.

Servicios de confianza cualificados

4.3.4. Los certificados electrónicos derivados del Reglamento eIDAS

Atendiendo a lo dispuesto en el Reglamento eIDAS, los **tipos de certificados** regulados son los que se muestran en el cuadro siguiente (véase capítulo 5, donde se unifican y codifican estas tipologías):

- Certificado de firma electrónica.
- Certificado cualificado de firma electrónica (Anexo I).

- Dispositivo de creación de firma electrónica.
- Dispositivo cualificado de creación de firma electrónica (Anexo II).

- Certificado de sello electrónico.
- Certificado cualificado de sello electrónico (Anexo III).

- Dispositivo de creación de sello electrónico.
- Dispositivo cualificado de creación de sello electrónico (Anexo II).

- Certificado de autenticación de sitio web.
- Certificado cualificado de autenticación de sitio web (Anexo IV).

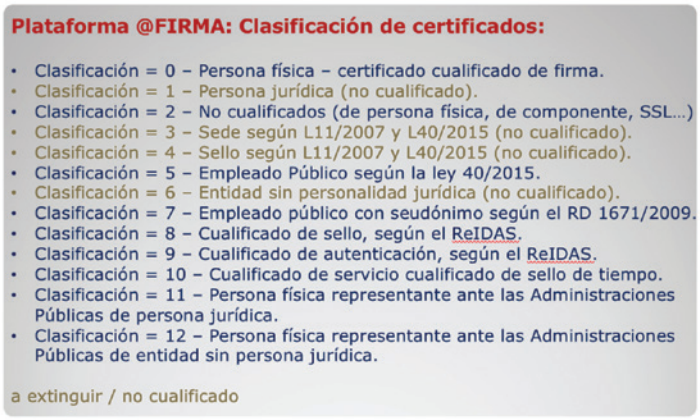
Tipos de certificados previstos en el Reglamento eIDAS

Obsérvese que los certificados que gozan del carácter de "cualificados" se encuentran especialmente definidos y regulados en los Anexos del Reglamento eIDAS que se mencionan.

Así pues, el Reglamento eIDAS ha venido a alterar el anterior régimen en materia de expedición y uso de certificados. La figura siguiente muestra esta evolución normativa.

La evolución normativa de los certificados a raíz del Reglamento eIDAS

En la actualidad, **@FIRMA**, en su calidad de plataforma de validación y firma electrónica multi-PKI, que se pone a disposición de las Administraciones Públicas, proporcionando servicios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva, clasifica los certificados de la forma mostrada en el cuadro siguiente:



Clasificación de certificados tratados por @FIRMA

A título de ejemplo, reproducimos seguidamente la tipología de certificados electrónicos expedidos por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT-RCM), al tiempo de redactar estas líneas.

Persona Física eIDAS	El Certificado FNMT de Persona Física, que se emite sin coste a cualquier persona que esté en posesión de su DNI o NIE, es la certificación electrónica expedida por la FNMT-RCM que vincula a su Suscriptor con unos Datos de verificación de Firma y confirma su identidad personal. Este certificado le permitirá identificarse de forma telemática y firmar o cifrar documentos electrónicos.
Certificado de Representante eIDAS	**Representante para Administradores únicos y solidarios:** Certificado de Representante para administradores únicos y solidarios es la certificación electrónica expedida por la FNMT-RCM que vincula un Firmante con unos Datos de verificación de firma y confirma su identidad. El Firmante actúa en representación de una Prsona jurídica en calidad de representante legal con su cargo de administrador único o solidario inscrito en el Registro Mercantil. **Representante de Persona Jurídica:** Certificado de Representante de Persona jurídica es la certificación electrónica expedida por la FNMT-RCM que vincula un Firmante a unos Datos de verificación de firma y confirma su identidad. Este certificado sustituye al tradicionalmente utilizado por las Administraciones Públicas para el ámbito tributario y que, posteriormente, se extendió para otros usos. Por tanto, este certificado se expide a las Personas Jurídicas para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas. **Representante de Entidad sin Personalidad Jurídica:** Certificado de Representante de Entidad sin personalidad jurídica es la certificación electrónica expedida por la FNMT-RCM a una Entidad sin personalidad jurídica que vincula un Firmante a unos Datos de verificación de firma y confirma su identidad en los trámites tributarios y otros ámbitos admitidos por la legislación vigente.
Administración Pública eIDAS	La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regula los sistemas de identificación de las Administraciones Públicas, así como los sistemas de firma electrónica del personal al servicio de las Administraciones Públicas y de sello electrónico para la actuación administrativa automatizada. Si desea utilizar alguno de los sistemas previstos en la citada Ley 40/2015, y por tanto está interesado en que su Administración cuente con el correspondiente acuerdo con la FNMT-RCM para la provisión de los mismos, puede dirigir su consulta al Área Comercial CERES.
Certificados de Componente eIDAS	La FNMT-RCM también emite certificados electrónicos para la identificación de servidores o aplicaciones informáticas heredando la confianza de la FNMT-RCM como Autoridad de Certificación. Dentro de esta categoría ponemos a su disposición certificados de servidor SSL, certificados wildcard, certificados de firma de código y certificados de sello de entidad.

Tipología de certificados expedidos por la FNMT-RCM

4.3.5. La firma electrónica, el sello electrónico y el sello de tiempo electrónico derivados del Reglamento eIDAS y su eficacia jurídica

Como hemos señalado, el Reglamento eIDAS ha venido a alterar la regulación en materia de firma electrónica, desplazando a la -todavía vigente al tiempo de redactar estas líneas- Ley 59/2003, de Firma Electrónica.

La nueva regulación europea define la **firma electrónica** de la siguiente manera:

firma electrónica	Datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar (art. 3.10).
firma electrónica avanzada	La firma electrónica que cumple los siguientes requisitos (art. 3.11): a) Estar vinculada al firmante de manera única; b) Permitir la identificación del firmante; c) Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y d) Estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
firma electrónica cualificada	Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica (art. 3.12).

Desaparecido el concepto de "firma electrónica de las personas Jurídicas", de controvertida andadura en nuestra doctrina, el Reglamento eIDAS introduce -en su sustitución, podría decirse, y de forma similar a la firma- el **sello electrónico**, que define como se muestra seguidamente:

sello electrónico	Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos (art. 3.25).
sello electrónico avanzado	Un sello electrónico que cumple los siguientes requisitos (art. 3.26): a) Estar vinculado al creador del sello de manera única; b) Permitir la identificación del creador del sello; c) Haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo, y d) Estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.
sello electrónico cualificado	Un sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico (art. 3.27).

Concluimos este repaso a los conceptos fundamentales y su acomodo en el Reglamento eIDAS con los mecanismos para la estampación de evidencias en materia de tiempo. Nos encontramos así con el tradicional concepto de **sello de tiempo**, que esta norma europea define del siguiente modo:

sello de tiempo electrónico	Datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante;
sello cualificado de tiempo electrónico	Un sello de tiempo electrónico que cumple los siguientes requisitos (art. 3.34): a) Vincular la fecha y hora con los datos de forma que se elimine razonablemente la posibilidad de modificar los datos sin que se detecte; b) Basarse en una fuente de información temporal vinculada al Tiempo Universal Coordinado, y c) Haber sido firmada mediante el uso de una firma electrónica avanzada o sellada con un sello electrónico avanzado del prestador cualificado de servicios de confianza o por cualquier método equivalente.

Este nuevo marco jurídico derivado del Reglamento eIDAS contiene, entre otras, tres precisiones en torno a los **efectos jurídicos de las firmas electrónicas**, a saber:

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada.

   En todo caso, corresponde a las legislaciones nacionales determinar los efectos jurídicos de las firmas electrónicas en los Estados miembros, salvo para los requisitos establecidos en el Reglamento eIDAS.
2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.
3. Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.

Por lo que respecta al **uso de firmas electrónicas/sellos electrónicos en los servicios públicos**, el Reglamento eIDAS hace las siguientes precisiones (arts. 27 y 37, respectivamente):

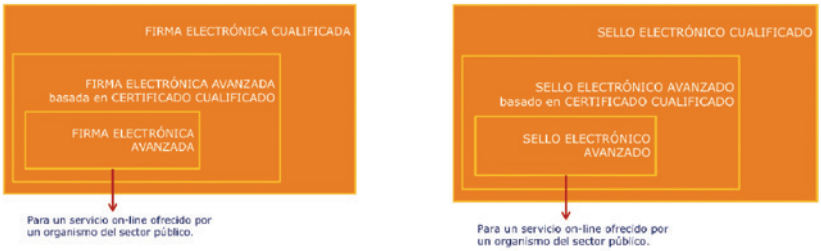
1. Si un Estado miembro requiere [una firma electrónica avanzada/un sello electrónico avanzado] con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá [las firmas electrónicas avanzadas/los sellos electrónicos avanzados], [las firmas electrónicas avanzadas basadas/los sellos electrónicos avanzados basados] en un certificado cualificado de [firma electrónica/sello electrónico] y [las firmas electrónicas cualificadas/los sellos electrónicos cualificados] por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en la norma[9].

[9] Los actos de ejecución a los que se refiere el Reglamento eIDAS se concretan en la Decisión de Ejecución (UE) 2015/1506.

2. Si un Estado miembro requiere [una firma electrónica avanzada basada/un sello electrónico avanzado basado] en un certificado cualificado con el fin de utilizar un servicio en línea ofrecido por un organismo del sector público, o en nombre del mismo, dicho Estado miembro reconocerá [las firmas electrónicas avanzadas basadas/los sellos electrónicos avanzados basados] en un certificado cualificado y [las firmas electrónicas cualificadas/los sellos electrónicos cualificados] por lo menos en los formatos o con los métodos definidos en los actos de ejecución contemplados en la norma.

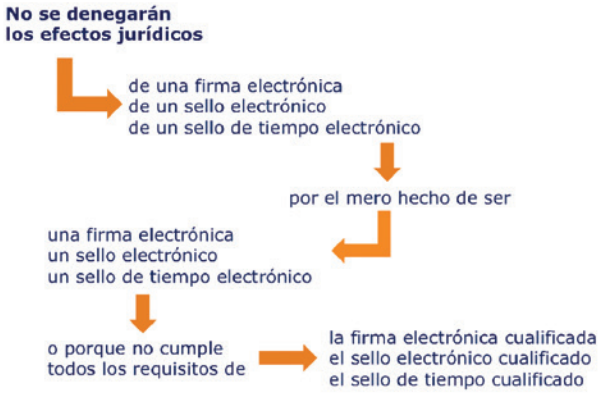
3. Los Estados miembros no exigirán para la utilización transfronteriza de un servicio en línea ofrecido por un organismo del sector público [una firma electrónica/un sello electrónico] cuyo nivel de garantía de la seguridad sea superior al de [una firma electrónica cualificada/un sello electrónico cualificado].

Lo que puede representarse mediante el gráfico mostrado seguidamente.



Utilización de firmas/sellos electrónicos en los servicios públicos

La no denegación de los efectos jurídicos a las firmas electrónicas no cualificadas es igualmente predicable de los sellos electrónicos y a los sellos de tiempo electrónicos, como se muestra en el gráfico siguiente.



Eficacia jurídica de las firmas/sellos/sellos de tiempo electrónicos/as

5 Certificados. Tipos de Certificados

5.1. Clasificación y relación de nomenclaturas

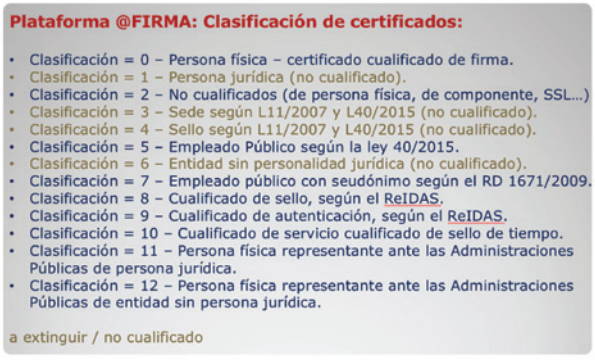
Con la entrada en vigor de la ley de firma electrónica 59/2003, la ley 11/2007 y las leyes 39/2015 y 40/2015 van apareciendo sucesivamente diferentes definiciones de tipos de certificados que, unido a la diferente nomenclatura existente en los prestadores de servicios de certificación, ha causado cierta confusión.

Con la aparición del Reglamento eIDAS que tiene aplicación desde el 1 de enero de 2016, se han debido reclasificar todos los tipos de certificados y unificar los mismos.

Sin embargo, los certificados emitidos hasta ahora se han de respetar, por lo que, según la forma de expedición, podemos encontrar 2 tipos de certificados electrónicos:

- Certificados electrónicos que se han emitido cumpliendo los requisitos establecidos por la Ley 59/2003, de firma electrónica y el Reglamento eIDAS, y que no se consideran cualificados por este último.
- Certificados electrónicos cualificados, que son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Dependiendo de la finalidad para la que se expiden existen gran cantidad de tipos de certificados diferentes. Tal y como se ha indicado anteriormente, la clasificación actual de los certificados por parte de la plataforma @FIRMA es la siguiente:



Clasificación de certificados tratados por @FIRMA

El objetivo del Reglamento eIDAS es que finalmente las tipologías de certificados queden en los siguientes

Clasificación de certificados eIDAS			
Cód	**Nombre**	**Descripción**	**Valores en los campos TSL**
UE00	Certificado de firma	Orientado a la identificación y firma de personas físicas (firmantes). La firma implica la garantía de origen e integridad de los datos firmados, así como la conformidad/consentimiento con dichos datos y obligación legal respecto al contenido. Es equivalente al certificado de firma de persona física de la ley 59/2003.	certQualified = YES certClassification = ESIG
UE01	Certificado de sello	Orientado al sello de personas jurídicas (creadoras de sello). Es parcialmente similar al certificado de persona jurídica de la Ley 59/2003, con las diferencias: No llevan una persona custodio/responsable del certificado. Se orienta al sello (garantía de origen e integridad de los datos). Además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores (considerando 65 del eIDAS) Cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica. (considerando 58 del eIDAS). No a la inversa.	certQualified = YES certClassification = ESEAL
UE02	Certificado de autenticación web	Orientado a vincular el sitio web (dominio de Internet) con la persona física o jurídica titular del certificado.	certQualified = YES certClassification = WSA
UE03	Certificado de firma no cualificado	No se garantiza que vayan a poder ser validados. Este tipo de certificados no se contempla su uso en España puesto que no está recogidos en la legislación vigente (ley 39/2015)	certQualified = NO / UNKNOWN certClassification = ESIG
UE04	Certificado de sello no cualificado	"	certQualified = NO / UNKNOWN certClassification = ESEAL
UE05	Certificado de autenticación web no cualificado	"	certQualified = NO / UNKNOWN certClassification = WSA

A partir de la aplicación del reglamento eIDAS se ha realizado una adaptación en la plataforma @firma, y se ha procedido a una reclasificación que tiene en cuenta las tipologías existentes actualmente pero que se centra en realizar correspondencias con el modelo europeo.

La tabla de equivalencias es la siguiente:

Clasificación de certificados en España				
Cód	**Nombre**	**Equiv.**	**Descripción**	**Otros nombres**
ES00	Persona física	UE00	Orientado a la identificación y firma de personas físicas (firmantes). La firma implica la garantía de origen e integridad de los datos firmados, así como la conformidad/consentimiento con dichos datos y obligación legal respecto al contenido. Es equivalente al certificado de firma de persona física de eIDAS. Certificado cualificado de firma	Certificado reconocido de persona física. Certificado cualificado de persona física
ES01	Persona jurídica (a extinguir)	UE01	Se consideran desde el 1 de Julio de 2016 como NO CUALIFICADOS. Se mantiene el tipo para que en @firma se pueda validar y el impacto sea el menor posible en las aplicaciones.	Certificado reconocido de persona jurídica
ES02	No reconocidos	UE04/ UE05	Pueden incluir certificados de persona física, de componente, SSL... No se garantiza que vayan a poder ser validados. No se validarán aquellos que no figuren en sus listas publicadas por la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información relativa a la firma electrónica.	Certificado no cualificado
ES03	Sede	UE05	Sede electrónica (según ley 11/2007). No reconocido desde julio de 2016.	Certificado SSL Certificado de sitio seguro Certificado web
ES04	Sello	UE05	Sello electrónico (según ley 11/2007). No reconocido desde julio de 2016.	
ES05	Empleado Público	UE00	Empleado público (según ley 11/2007). Estos certificados se siguen aceptando por parte de la SETSI. En caso de eliminarse dicha clasificación pasarían a ser no reconocidos y a catalogarse en ES00.	
ES06	Entidad sin personalidad jurídica	UE04	No reconocido y a extinguir. Pasan a ser certificados no reconocidos (no cualificados).	
ES07	Empleado Público con seudónimo	UE00	Recogido en el RD 1671/2009. Son un subconjunto de certificados cualificados de persona física (ES00), que, además, son de empleado público con seudónimo. Se siguen aceptando por parte de la SETSI. En caso de eliminarse dicha clasificación pasarían a ser ES00, pero no tendrá los campos Nombre, Apellidos y DNI, y contendrá en cambio un campo "seudónimo".	

ES08	Cualificado de sello	UE01	Orientado al sello de personas jurídicas (creadoras de sello). Es parcialmente similar al certificado de persona jurídica de la Ley 59/2003, con las diferencias: No llevan una persona custodio/responsable del certificado. Se orienta al sello (garantía de origen e integridad de los datos). Además de autenticar el documento expedido por la persona jurídica, los sellos electrónicos pueden utilizarse para autenticar cualquier activo digital de la persona jurídica, por ejemplo, programas informáticos o servidores (considerando 65 del eIDAS) Cuando una transacción exija un sello electrónico cualificado de una persona jurídica, debe ser igualmente aceptable una firma electrónica cualificada del representante autorizado de la persona jurídica. (considerando 58 del eIDAS). No a la inversa. Incluye certificado de aplicación, al ser firmado por entes o personalidades jurídicas.	
ES09	Cualificado de autenticación de sitio web	UE02	Orientado a vincular el sitio web (dominio de Internet) con la persona física o jurídica titular del certificado.	Certificado SSL Certificado de sitio seguro Certificado web Certificado de sede
ES10	Cualificado de sello de tiempo	UE01	Si el servicio de sellado de tiempo figura en la TSL y el certificado cumple con las Normas Técnicas para ser considerado sello de tiempo.	Timestamp Sellado de tiempo Estampado de tiempo
ES11	Persona física Representante ante las Administraciones Públicas de persona jurídica	UE00	Se siguen aceptando por parte de la SETSI. En caso de eliminarse dicha clasificación pasarían a ser ES00.	Certificado de representante
ES12	Persona física Representante ante las Administraciones Públicas de entidad sin persona jurídica	UE00	Se siguen aceptando por parte de la SETSI. En caso de eliminarse dicha clasificación pasarían a ser ES00.	Certificado de representante

5.2. Para los Ayuntamientos

5.2.1. Tipos de certificados

Con carácter general, en las Entidades Locales se utilizan los siguientes tipos de certificados digitales:

a. Certificado de persona física (ES00).

Este tipo de certificado permite acreditar la identidad y voluntad de una persona en nombre propio, sin incluir otras consideraciones, que deberán acreditarse por otros medios. El ejemplo más típico es el DNIe, habilitado para su utilización en cualquier situación.

b. Certificado de Empleado Público (ES05, ES07)

El certificado de empleado público se expide a funcionarios, personal laboral, estatutario y personal autorizado, al servicio de la Administración Pública, y para el ejercicio de sus funciones en dicha Administración Pública.

Se utilizan típicamente en procesos de firma electrónica, o para acceder a servicios electrónicos de otras administraciones en el ejercicio de sus funciones y para los cuales hayan obtenido el correspondiente permiso de acceso (identificación).

Es posible que el certificado, en vez de llevar el nombre y apellidos de la persona, incorpore un seudónimo, es decir, un número profesional que permite su identificación en el ámbito concreto del ejercicio de sus funciones. Un ejemplo típico de este seudónimo sería un número de agente de Policía.

c. Certificado de Representante de la Entidad Local (ES11)

Son certificados que identifican a una persona física como representante de una persona jurídica. El representante debe ser una persona física con la capacidad legal de actuar completamente en nombre de la Entidad.

Se pueden utilizar, entre otros, para la firma electrónica, el cifrado de documentos o para relacionarse telemáticamente con las diferentes Administraciones (Sede electrónica de la Agencia Tributaria, Sede electrónica de la Seguridad Social, Sede electrónica del Catastro, etc.).

d. Certificado de Sede Electrónica (ES03, ES09)

Un certificado de Sede Electrónica es un certificado reconocido o cualificado de autenticación de sitio web. Básicamente, es similar al de servidor web SSL pero incluye la identificación del Órgano titular de la Sede Electrónica. Sirve para dos propósitos:

- Identificar que un determinado portal web actúa como Sede Electrónica de la Administración Pública titular del certificado
- Establecer comunicaciones seguras (vía https) con las personas que navegan por sus páginas, de tal forma que se garantiza la privacidad e integridad de la información que se ofrece.

e. Certificados de Sello Electrónico (E04, ES08)

Un certificado de sello electrónico vincula unos datos de verificación de firma a los datos identificativos y de autenticación de una determinada Administración Pública, órgano o entidad de derecho público que realiza una actuación administrativa automatizada y la persona física responsable de la actuación administrativa.

De acuerdo con lo establecido en el artículo 42 de la Ley 40/2015, se utilizan para firmar actos administrativos por medio de sistemas informáticos sin intervención directa de una persona física. Es decir, se utilizan en procesos automatizados, como firma de acuses de recibo en el registro telemático, digitalización certificada, emisión de volantes de empadronamiento de forma automática, etc.

Estos actos automatizados siguen siendo responsabilidad del Órgano administrativo que los realizaba en papel, y que es el que consta como titular del certificado, de ahí que también se les denomine Sellos de Órgano.

Por tanto, el certificado de sello electrónico está vinculado a un órgano administrativo, no a un equipo o servidor informático, debiéndose distinguir entre la "persona solicitante" del certificado y la "persona responsable" del mismo y de los trámites en los cuales se va a realizar la firma electrónica con el certificado. Según lo establecido en el Artículo 40 de la Ley 40/2015, el certificado de Sello Electrónico debe incorporar la identidad de la persona titular del Órgano administrativo

Una administración pública puede tener tantos Sellos Electrónicos como considere conveniente, para utilizar en procedimientos automatizados concretos y con responsables definidos.

f. Certificados de Componente (ES02, ES09)

Son certificados utilizados en distintos entornos, para acciones concretas, como por ejemplo:

- Firma del código de aplicaciones, garantizando su autoría e integridad. Aunque está pensado principalmente para empresas, pueden ser utilizados por los departamentos de desarrollo de TI de las AAPP.
- Establecer canales seguros de comunicación bajo protocolo SSL. Normalmente se instalan en servidores que ofrecen servicios sobre HTTPS, FTPS, etc. Además de para la creación de redes privadas virtuales a través de internet (VPN), un ejemplo típico es el uso de aplicaciones de comercio electrónico para pago de impuestos, sanciones, etc.
- Creación de sellos de tiempo

5.2.2. Procesos de obtención

Las administraciones públicas deben adquirir los certificados digitales a través de un Proveedor de Servicios de Confianza (PSC). Esta denominación, que es la utilizada por el Reglamento (UE) Nº 910/2014 (conocido como eIDAS) sustituye lo que anteriormente se llamaba Prestador de Servicios de Certificación, o Autoridad de Certificación. Dependiendo del proveedor, y el tipo de certificado a obtener, los certificados tienen un coste diferente.

Pueden obtenerse certificados en “software”, es decir, que se guardan en archivos pkcs#12 (extensión .p12 o .pfx) o se descargan directamente en la cryptoapi de Windows, y pueden obtenerse en “hardware”, es decir, grabados en dispositivos físicos seguros (tarjetas criptográficas, token USB,…).

Es posible hacer copias de un certificado software con su clave privada, y llevarlo de un sitio a otro con un Pendrive, o tener el mismo certificado “instalado” en más de un PC. Sin embargo, no es posible exportar un certificado con su clave privada, de un dispositivo hardware, por lo que se considera este último mucho más seguro.

Cada Prestador de Servicios de Confianza tiene su propia operatoria a la hora de solicitar los distintos tipos de certificados, que está claramente detallada en su página web.

Si la administración pública tiene un convenio/acuerdo con un PSC, el empleado público acreditará su identidad en la Oficina que actúe como Autoridad de Registro del PSC, donde se generará el certificado y se le enviará de forma telemática (permitiendo una descarga del archivo .p12, o enviándolo por email) o se le entregará en un dispositivo criptográfico.

5.2.3. Responsabilidades

Es responsabilidad de la Entidad Pública la custodia y el correcto uso de los certificados que se utilizan en su nombre: Certificados de Sede Electrónica, o de Sello Electrónico, y de su renovación en tiempo y forma.

En la Sede Electrónica hay que indicar los certificados de Sello y los procesos automatizados que los utilizan, en nombre de los Órganos Administrativos de la Entidad.

Según el artículo 40 de la Ley 40/2015, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos. Por ello, el Ministerio de Política Territorial y Función Pública ofrece de forma gratuita la plataforma VALIDe (https://valide.redsara.es), donde la ciudadanía podrá comprobar la validez de los certificados utilizados, y de las firmas realizadas por las Administraciones Públicas

Es responsabilidad individual de cada persona la custodia y el correcto uso de los certificados personales (de Persona Física, empleado público o representante de Entidad). Para ello, es conveniente que cada titular de un certificado lo proteja del uso no autorizado con un PIN que solo conozca el titular.

En el caso de certificados software que se instalan en la cryptoapi de Windows, es recomendable que en el proceso de instalación del certificado se especifique el PIN que deberá incluirse cada vez que se vaya a utilizar el certificado. De esta forma, otras personas no podrán firmar con ese certificado conociendo únicamente el usuario y contraseña de acceso al equipo.

En caso de pérdida del dispositivo criptográfico donde se encuentre almacenado, o ante la sospecha de que está teniendo un uso fraudulento por parte de terceros, es preciso comunicarlo a la Autoridad de Certificación para que revoque el certificado lo antes posible.

6 Firma y plataformas de firma

6.1. FIRMA

6.1.1. Plataforma de Firma

Es una herramienta tecnológica en la que se basa la implementación de una solución de validación y firma electrónica y que hacen efectiva la firma de archivos mediante los certificados digitales.

Su uso permite la firma de facturas, de contratos, documentos, informes, transacciones,...

Existen distintas plataformas, disponibles en modo tradicional "in house", donde puede instalarse en servidores propios de la Institución tipo web o en cliente/servidor en los puestos de trabajo finales. Además, existen plataformas que compaginando lo anterior también permiten la modalidad como servicio en la nube (SaaS).

Se suele desarrollar arquitecturas y plataformas de desarrollo de mercado, como Java, .NET, PHP. Incluyen funciones de autenticación y firma digital utilizando los servicios implementados, independizando la lógica empresarial del propio proceso de firma y validación.

Un ejemplo es la plataforma @Firma del MINHAFP que está basada en software libre y estándares abiertos.

https://administracionelectronica.gob.es/ctt/afirma

El servicio de validación de certificados y firmas electrónicas de @firma10 es una plataforma de validación multi-PSC desarrollada inicialmente por la Junta de Andalucía, y cedida al Ministerio de Administraciones Públicas (hoy Ministerio de Política Territorial y Función Pública) con el objeto de fomentar y extender el desarrollo de la Administración Electrónica y la Sociedad de la Información.

[10] Confirma que el certificado del firmante o sus certificados principales existen en la lista de identidades de confianza del validador y si el certificado de firma es válido.
[La] verificación de integridad de documento confirma si el contenido firmado ha cambiado después de su firma y la verificación de integridad de documento.

6.1.2. Soporte a la firma Biométrica y en movilidad

Es un rasgo biométrico que cuenta con una alta aceptación social por parte de la ciudadanía y autoridades, habiendo sido utilizada durante siglos como medio de autenticación de documentos legales y de transacciones y contratos civiles.

La firma biométrica es también conocida como firma electrónica avanzada, consiste en una tecnología que permite capturar datos biométricos durante el proceso de firma manuscrita sobre dispositivos electrónicos. La biometría es el estudio automático para el reconocimiento único de humanos, basado en uno o más rasgos conductuales o características intrínsecas. Los datos biométricos capturados durante el proceso de firma son la presión del lápiz, la velocidad de escritura y la aceleración.

Los dispositivos electrónicos que permiten la captura de datos biométricos, entre los que se encuentran fabricantes como Wacom o Topaz, detectan hasta 1024 niveles de presión distintos, lo que permite obtener una identificación única e inequívoca del firmante.

En el reconocimiento de la firma existen dos tratamientos o punto de vista:

- Tratamiento Estático: Se lleva a cabo cuando la firma ya está realizada solo se dispone de una imagen estática, plana en dos dimensiones.
- Tratamiento Dinámico: Se adquieren funciones temporales, de presión, velocidad, de espacio... durante la realización de la firma.

La firma biométrica basa su seguridad en dos aspectos bien diferenciados:

- Por una parte, la imposibilidad de replicar un trazo de firma por otra persona distinta al firmante.
- Por otra la correspondencia unívoca de una huella digital a un único documento.

Al combinar estas dos características, tenemos un activo (la firma biométrica) que asocia entonces al firmante con el documento firmado.

Para asociar el trazo biométrico con el documento firmado:

- La captura de la información biométrica.
- El enlace entre la información biométrica y el documento firmado.
- Protección adicional del PDF.
  - » Una firma electrónica PadES.
  - » Un sello de tiempo para todo el PDF.

Es importante recalcar que la firma biométrica ofrece una seguridad (técnica y jurídica) "suficiente", con independencia de su consideración como firma electrónica simple o avanzada (ley 59/2003 o reglamento europeo 910/2014), debiendo, como se ha recordado anteriormente, aplicar un principio de proporcionalidad (de igual manera que no se firma ante notaría una factura, pero sí al constituir una hipoteca).

Existe un desarrollo software, "BioSign-HandWritten", https://github.com/clawgrip/biosign-handwritten desarrollado inicialmente por la AEAT y publicado como software libre (EUPLv1.1) en GitHub.

Actualmente la firma biométrica en el mercado nos ofrece una amplia gama de tabletas y móviles que pueden realizar dicha firma biométrica, un ejemplo de APP es ***SIGNply*** **tanto para IOS como Android.**

6.1.3. Soportes Criptográficos y HSM.

Un HSM **H**ardware **S**ecurity **M**odule" (Módulo de Seguridad Física) es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas. Otorgan protección a las transacciones, identidades y aplicaciones mediante la protección de claves criptográficas y la prestación de servicios de cifrado, descifrado, autenticación y firma digital para las diversas de aplicaciones de las organismos o compañías. Estos dispositivos pueden tener conectividad SCSI / IP u otras y aportar funcionalidad criptográfica de clave pública (PKI) de alto rendimiento que se efectúa dentro del propio hardware.

Los HSM permiten integrar seguridad hardware en aplicaciones críticas tales como infraestructuras de clave pública (PKI), bases de datos, servidores web y servidores de aplicaciones. El "National Institute of Standards and Technology" (NIST), desarrolló un estándar que permite establecer el nivel de seguridad ofrecido por este tipo de dispositivos. Dicho estándar se denomina "Federal Information Processing Standard" (FIPS), actualmente en su versión FIPS-2. Este es el estándar de facto en estos casos, y surge como una guía de requisitos deseables para el uso de dispositivos criptográficos para organismos gubernamentales o sujetos a normativas muy estrictas.

El estándar establece cuatro niveles distintos, los cuales gradúan el nivel de seguridad del dispositivo evaluado. Se detallan a grandes rasgos los requisitos para cada uno de los niveles establecidos:

Nivel 1: Este es el nivel que podría tener cualquier ordenador personal con una tarjeta criptográfica genérica. En este nivel únicamente se requiere el uso de un algoritmo criptográfico y una función de seguridad reconocidos; no existen requisitos de seguridad física.

Nivel 2: De forma adicional a los requisitos establecidos por el nivel anterior, en este caso, se requerirán mecanismos de seguridad física que permitan identificar si se han realizado manipulaciones del módulo que hayan podido permitir un acceso no autorizado a las claves gestionadas en el módulo. Estos mecanismos deben ser desde sellos que se rompan cuando se accede al dispositivo que almacena las claves en claro o a los parámetros de seguridad críticos del dispositivo (parámetros que se almacenan en claro sobre los registros del criptoprocesador y que se emplean para generar las claves).

Nivel 3: Sumado a los requisitos incluidos en el nivel 2, se requiere que el dispositivo no sólo permita detectar accesos no autorizados, sino que responda a dichos accesos, uso no autorizado o modificación del módulo. Por ejemplo, un nivel de seguridad 3 sería un dispositivo que detectara su apertura y de forma automática borrara por ejemplo los parámetros de seguridad críticos, inutilizándolo y asegurando la confidencialidad de las claves almacenadas.

Nivel 4: Del mismo modo que en los casos anteriores, en el nivel 4 se mantienen los requisitos de los niveles anteriores y se añaden nuevos. En este caso, aparte de requerir más capacidad de detectar intrusiones físicas, el módulo deberá detectar condiciones inadecuadas de hume-

dad, temperatura o tensión que pudieran afectar a su funcionamiento. De este modo, se puede asegurar que se gestionarán estas contingencias y la confidencialidad de la información custodiada en el módulo.

Cualquier HSM para implementar una PKI deberá al menos tener un certificado FIPS-2, obteniendo un nivel 3. Más información respecto a este estándar puede obtenerse de http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

La rápida evolución del software y el empuje de las soluciones de código abierto han hecho que existan soluciones aceleradoras software que superan en rendimiento a los aceleradores hardware.

La principal ventaja del HSM por Hardware frente al de Software consiste en que, mientras el primero funciona como una "Caja Negra" con poco mantenimiento y configuración, el segundo requiere un mayor esfuerzo en estos dos aspectos.

Varios ejemplos de este Software HSM Open Source:

https://github.com/OpenSC/OpenSC

https://github.com/gozdal/accessl

https://github.com/PirataNervo/HSM

6.1.4. Validación de certificados y documentos firmados.

La validación de una firma electrónica es el proceso por el que se comprueba:

- La identidad del firmante
- La integridad del documento firmado
- La validez temporal del certificado utilizado

Sabemos que, en el proceso de firma, el firmante utiliza su certificado electrónico, en concreto su clave privada, para obtener la firma electrónica.

Las dos primeras verificaciones se pueden realizar desde una aplicación sin conexión a Internet simplemente utilizando el certificado incluido en la misma firma.

El proceso de validación de la firma no puede separarse del proceso de validación del certificado usado para la firma. Y por eso, la validación de la firma implica también la validación del certificado. El certificado electrónico solamente se puede validar mientras esté activo, ya que una vez

caducado desaparece de las listas de revocación de la Autoridad de Certificación y ya no se puede comprobar cuál era el estado en el momento de la firma. Si el certificado no es válido, o está caducado o revocado, la firma no puede ser validada correctamente puesto que no podemos saber cuál era el estado del certificado en el momento de la firma.

Por tanto, las tres validaciones dependen de la capacidad de validar el certificado, para lo cual es necesaria una conexión a Internet que permita acceder a una plataforma de validación de certificados.

La **Autoridad de Validación**[11] es el componente que suministra información sobre la vigencia de los certificados electrónicos que han sido registrados por una **Autoridad de Registro**[12] y certificados por la **Autoridad de Certificación**[13]. En general, la Autoridad de Certificación es también Autoridad de Validación, aunque ambas figuras pueden estar representadas por entidades diferentes.

La información sobre los Certificados electrónicos revocados (no vigentes) se almacena en las denominadas **L**istas de **R**evocación de **C**ertificados (CRL) mantenidos por las Autoridades de Validación. La validación o verificación del estado de un certificado se puede realizar a través de Internet accediendo al servicio que proporciona la Autoridad de Validación o de Certificación que ha emitido el certificado.

https://valide.redsara.es/valide/

Plataforma de validación de documentos:

Las plataformas de validación son sistemas que permiten validar los certificados electrónicos y los documentos que deberán de llevar **C**ódigo de **V**erificación **E**lectrónica (CVE) o **Có**digo **S**eguro de **V**erificación (CSV) que consiste en un conjunto de dígitos que identifican de forma única los documentos electrónicos emitidos por las aplicaciones, así como la URL donde verificar dicho

[11] La Autoridad de Validación (VA) como tercero de confianza, proporciona información del estado de Certificados y de Firmas Electrónicas, verifica si el certificado electrónico presentado se encuentra un uno de los siguientes estados: válido, revocado, incierto o caducado y proporciona certeza sobre el estado de una firma electrónica en cualquiera de los formatos soportados, pudiendo ser ésta calificada como válida o inválida.

[12] Una Autoridad de Registro (AR, en inglés RA) es una entidad que identifica de forma inequívoca al solicitante de un certificado. La Autoridad de Registro suministra a la Autoridad de Certificación los datos verificados del solicitante a fin de que la Autoridad de Certificación emita el correspondiente certificado.

[13] La Autoridad de certificación, o certificadora, o certificante, o las siglas AC o CA (por la denominación en idioma inglés Certification Authority), señalan a una entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública. Desde la entrada en vigor del reglamento eIDAS se denominan PSC, Proveedor de Servicios de Confianza-

documento o sede electrónica de la entidad emisora del documento. Por lo tanto, los documentos que disponen de CSV asociado y verificable en sede electrónica, son considerados copias electrónicas auténticas.

Un ejemplo de validación de documentos es el de la Carpeta Ciudadana del Gobierno de España.

https://sede.administracion.gob.es/carpeta/utilidades/consultaCSV.htm

La relación de entidades públicas que usan esta Carpeta y que se pueden validar sus documentos además de la Agencia Tributaria puede identificarse en el siguiente enlace:

https://sede.administracion.gob.es/PAG_Sede/ayuda/ayudaCSV.html

Visor de Firmas Electrónicas:

El visor es una herramienta que permite generar un informe de la firma y ver información de la propia firma electrónica y del documento firmado.

El documento que se genera no tiene el mismo valor legal que la firma. De hecho, puede ser válido en los términos que se determine para su uso. En general, en este caso, el documento impreso deberá contener un CSV o Código Seguro de Verificación que permite contrastar la copia impresa con la original electrónica. El uso del visor de firmas se suele utilizar en documentos XML firmados (XadES).

https://valide.redsara.es/valide/validarFirma/ejecutar.html

Cómo configurar Adobe para que valide los certificados en los documentos PDFs (PadES).

https://www.boe.es/diario_boe/preguntas_frecuentes/documentos/manual_firma_boe.pdf

6.1.5. Factura Electrónica.

En España.

Es una factura que se expide y se recibe en formato electrónico y se regula en el Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre y se define en el artículo 9 de este Reglamento y la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

face
Punto General de Entrada de Facturas Electrónicas

https://face.gob.es/es

La factura electrónica se realiza en dos fases:

- Se crea la factura (al igual que se hace con la factura en papel) y se almacena en un fichero de datos, el formato es un fichero XML.
- Una vez creada la factura, se procede a firmarla electrónicamente mediante el certificado digital propiedad del emisor de la factura y mediante firma XadES.

El formato de factura electrónica Facturae se crea mediante la Orden PRE/2971/2007, de 5 de octubre, sobre la expedición de facturas por medios electrónicos cuando el destinatario de las mismas sea la Administración General del Estado u organismos públicos vinculados o dependientes de aquélla y sobre la presentación ante la Administración General del Estado o sus organismos públicos vinculados o dependientes de facturas expedidas entre particulares.

Las sucesivas versiones de este formato y otras informaciones útiles sobre el mismo se publican en el portal

FACTURA·e

www.facturae.gob.es

A partir del 15-1-15, conforme a la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público, las facturas que se remitan a las Administraciones Públicas serán electrónicas y se ajustarán al formato estructurado de factura electrónica Facturae versión 3.2.x con firma electrónica XAdES.

El día 25 de febrero de 2018 entro en vigor la Resolución del 24 de agosto de 2017, de la Subsecretaría, por la que se publica la Resolución de 25 de julio de 2017, de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital y de las Secretarías de Estado de Hacienda y de Presupuestos y Gastos, por la que se publica una nueva versión, 3.2.2, del formato de factura electrónica «facturae».

BOE https://www.boe.es/boe/dias/2017/08/25/pdfs/BOE-A-2017-9982.pdf

La versión actual es la 3.2.2 de Facturae que incorpora nuevos campos respecto a su predecesora, la versión 3.2.1.

Los campos incorporados son:

- Para la documentación acreditativa de cesiones: FactoringAssignmentDocument, DocumentCharacter, RepresentationIdentity, DocumentType, Repository, RepositoryName, URL y Reference
- Para identificación de la factura rectificada: InvoiceIssueDate
- Para la descripción general de la factura: InvoiceDescription
- Para las nuevas etiquetas a nivel de factura: ReceiverTransactionReference, FileReference y ReceiverContractReference
- Para el pago en especie: PaymentInKind, PaymentInKindReason y PaymentInKindAmount

También se ha añadido el Kilovatio por hora (KWh) a la lista de unidades de medida y el formato HTML a la lista de formatos admitidos.

En Europa, red PEPPOL, CEF eInvoicing (La Norma Europea y su contenido).

Los Estados miembros de la Unión Europea deberán implantar la factura electrónica europea entre *el Sector Público y sus proveedores antes del 27 de noviembre de 2018*. La Directiva 2014/55/UE (http://www.boe.es/diario_boe/txt.php?id=DOUE-L-2014-80922) es una norma que pretende facilitar las relaciones comerciales transfronterizas con la creación de un estándar común que sea interoperable. Una vez que la factura electrónica se haya masificado en toda la Unión Europea, se espera un ahorro económico que podría alcanzar 2.3 billones de euros.

> Todos estos intercambios de facturas se realizarán dentro de la red PEPPOL, que se está encargando del desarrollo de acuerdos y estándares y del alineamiento con las legislaciones de cada país.

PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

https://peppol.eu/

edicom
connecting business

https://www.edicomgroup.com/es_ES/home.html#

El Reglamento (UE) Nº 1316/2013 crea el Mecanismo CEF (Connecting Europe Facility) "Conectar Europa", concretado posteriormente con el Reglamento (UE) Nº 283/2014, relativo a las redes transeuropeas en el sector de las infraestructuras de telecomunicaciones (CEF-Telecom). Mediante ambos reglamentos, se precisan los objetivos, presupuesto, condiciones de financiación y de participación para proyectos que financien el desarrollo de bloques de construcción y servicios digitales de infraestructura (DSI) que permitan el desarrollo de servicios públicos y privados transfronterizos tales como la interoperabilidad de la identidad electrónica (eID), la factura electrónica, la contratación electrónica, etc.

La norma EN 16931 mantiene como uno de sus objetivos prioritarios el favorecer y facilitar la implantación de un ecosistema de facturación electrónica en el cual la interoperabilidad se presente como su principal valor añadido.

También es importante recordar que el evento tuvo lugar con posterioridad a que la norma fuera publicada el 17 de octubre de 2017 en el Diario Oficial de la UE. Esto significa que se mantiene el calendario establecido por la directiva 2014/55, por lo que para el 18 de abril de 2019 será obligatorio para Administracion General del Estado y un año más tarde para que todos los niveles y entidades públicas de la UE estén preparados para aceptar facturas electrónicas remitidas por los proveedores, siempre que éstas cumplan con los requisitos de sintaxis UBL y CII definidos en CEN en las especificaciones TS 16931.

En *España* el proyecto cofinanciado por Europa *"FACe - The core platform of the Spanish public authorities to process the European standard on electronic invoice"*. Se centra en la integración de la norma europea eInvoice en el sistema español FACe de acuerdo con la Directiva 2014/55/Eu y desarrollándose los mapeos apropiados y necesarios para con las distintas sintaxis y semántica, a fin de facilitar el uso de dicha norma por todas las entidades públicas.

Proyecto publicado en http://euroface.unizar.es/

El proceso inverso, poder enviar empresas españolas a otros países europeos, se recoge en el proyecto denominado SMeTOOLS y se puede encontrar información aquí:

http://www.cambrabcn.org/es/que-te-ofrecemos/proyectos-europeos/smetools

https://www.b2brouter.net/es/blog/b2b-router-proyecto-smetools-nuevo-estandar-factura-electronica-europeo/

6.1.6. Publicación Certificada

La publicación sustituye a la notificación surtiendo sus mismos efectos en los siguientes casos:

- Cuando el acto tenga por destinatario a una pluralidad indeterminada de personas o cuando la Administración estime que la notificación efectuada a un solo interesado es insuficiente para garantizar la notificación a todos, siendo, en este último caso, adicional a la notificación efectuada.
- Cuando se trata de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo. En este caso, la convocatoria del procedimiento deberá indicar el tablón de anuncios o medios de comunicación donde se efectuarán las sucesivas publicaciones, careciendo de validez las que se lleven a cabo en lugares distintos.
- Cuando así lo establezcan las normas reguladoras de cada procedimiento.
- Cuando lo aconsejen razones de interés público apreciadas por el órgano competente
- La publicación de un acto deberá contener el mismo contenido que el señalado para las notificaciones.

La ley 39/2015 en su Artículo 45. Publicación.

1. Los actos administrativos serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente. En todo caso, los actos administrativos serán objeto de publicación, surtiendo ésta los efectos de la notificación, teniendo en cuenta:
    - Origen de la publicación, entidad pública y/o departamento...
    - Objeto, descripción o resumen de la publicación y deberá contener el texto íntegro de la resolución.
    - Acreditar fehacientemente que el anuncio se ha ubicado en la Web en un momento preciso en el tiempo.
    - Inalterabilidad de contenidos, que dicho anuncio no ha sido modificado en un transcurso de tiempo.

- Garantía de accesibilidad, que 24 horas y 7 días a la semana está disponible on line el mencionado anuncio.
- Custodia de las pruebas. Que se custodie el archivo (normalmente un PDF) y el certificado de sellado de tiempo, para que sea recuperable su contenido y su fehaciencia para ser utilizado por un tercero que pueda efectuar reclamación.
- Vigencia y la garantía de disponibilidad de la publicación en plazos.
- Que se cumple con la normativa de dicha publicación si existiese dicha norma. Ejemplo Perfil Contratante, Foro electrónico de Accionistas...

Ejemplos de publicación certificada:

El **perfil del contratante de las entidades públicas**.

PLATAFORMA DE CONTRATACIÓN DEL SECTOR PÚBLICO

https://contrataciondelestado.es/wps/portal/plataforma

Agencia Estatal Boletín Oficial del Estado

BOE

http://boe.es/diario_boe/

SITE Tablón Edictal Único TEU

TEU

http://boe.es/tablon_edictal_unico/

DGT Dirección General de Tráfico

TESTRA

https://sede.dgt.gob.es/es/tramites-y-multas/alguna-multa/consulta-tablon-edictal-testra/consultar-testra.shtml

6.1.7. Notificación Electrónica.

La notificación es el trámite procedimental mediante el cual el órgano administrativo competente practica una comunicación oficial y fehaciente al interesado o interesados en una Resolución o acuerdo administrativo. El término deriva de nota, esto es, de un escrito con la debida información acerca de un tópico específico; en latín, el término madre es "noscere", es decir, aprender; la nota es aquel medio por el cual se le da a conocer algo a alguien. En el pasado, las notas tenían que ver especialmente con el uso de un soporte específico, el papel,

Las notificaciones que se realizan en papel (con entrega bajo firma) que incluía la prueba de entrega física y dos intentos de entrega a domicilio, según requerimiento legal tienen un tiempo medio de una notificación superior a varios días y un coste que no baja de los 4 euros, entre preparación, envío y recepción de los acuses y un coste estimado entre papel, impresión, empresa notificadora, etc.

¿Qué es la notificación electrónica?

Se puede definir como aquella efectuada por medios electrónicos y que pone fin a un procedimiento electrónico, bien porque el interesado está obligado a ello, bien porque así lo haya manifestado expresamente un interesado que no esté obligado por Ley o Reglamento a comunicarse con la Administración por medios electrónicos.

El correo electrónico y el SMS no son en consecuencia medios válidos de notificación a partir de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, pero encajan claramente en el concepto de aviso complementario (a la notificación electrónica). El aviso debe hacerse, pero el art. 41.6 ("La falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida") tiene sentido porque debemos recordar que el aviso es un complemente de la notificación, no la notificación. Sería contrario a la lógica y al principio de seguridad jurídica considerar que no se ha practicado la notificación porque no se ha practicado el aviso, ya que este tiene un carácter más práctico y funcional que jurídico. La falta de la práctica de este aviso no impedirá que la notificación sea considerada plenamente válida (art. 41.7 de la referenciada ley).

¿Quién está obligado a recibir las notificaciones electrónicas?

Para ello nos dirigimos al art. 14 de la ley 39/2015, donde se indica:

1. Las personas físicas podrán optar a la tramitación electrónica. No obstante, la Ley prevé que se establezca reglamentariamente la obligación de utilizar medios electrónicos en determinados procedimientos y colectivos de personas que, con motivo de su capacidad económica, técnica, profesional u otros, se presuma acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.
2. Las personas jurídicas, entidades sin personalidad jurídica, los profesionales colegiados en el ejercicio de su actividad profesional, los Notarios y Registradores de la propiedad y mercantiles están obligadas a relacionarse con la Administración por medios electrónicos.
3. Cada representante de los interesados estará obligado cuando lo estén sus representados. La representación se realizará por medio de APODERA, explicado más adelante.
4. Los empleados de las Administraciones Públicas en las actuaciones que realicen con ellas por motivo de su condición de empleado público.

Sin embargo, continúa el precepto estableciendo dos excepciones:

a) Cuando la notificación se realice con ocasión de la comparecencia espontánea del interesado o su representante en las oficinas de asistencia en materia de registro y solicite la comunicación o notificación personal en ese momento. (Posición integrada ciudadana. Plataforma de atención multicanal)

b) Cuando para asegurar la eficacia de la actuación administrativa resulte necesario practicar la notificación por entrega directa de un empleado público de la Administración notificante.

El artículo 14, obliga a enviar **TODAS las notificaciones a nuestro portal de notificaciones**, unos por obligación y otros porque tenemos que poner a su disposición la notificación electrónica, aunque tengamos que notificarle en papel. Además, por el acuerdo de 21 de junio de 2017 de la CSAE, ese punto independientemente que tengamos uno propio debería de ser el **P**unto **Ú**nico de **N**otificación (PUN).

La **D**irección **E**lectrónica **H**abilitada (DEH): cualquier persona física o jurídica dispondrá de una dirección electrónica para la recepción de las notificaciones administrativas que por vía telemática pueda practicar las distintas Administraciones Públicas. Asociado a la Dirección Electrónica Habilitada, su titular dispondrá de un buzón electrónico en el que recibirá las notificaciones electrónicas correspondientes a aquellos procedimientos a los que voluntariamente decida suscribirse. En el caso de que de la práctica de la notificación sea obligatoria se podrá asignar de oficio una dirección electrónica habilitada. Este servicio cumple con las máximas garantías de confidencialidad, autenticidad y privacidad con el fin de asegurar la identidad de los participantes y de las comunicaciones.

https://notificaciones.060.es/PCPublic_publicInfo.action

La notificación por medios electrónicos, regulada en el art.43 LPACP, se entiende realizada por la comparecencia del interesado o su representante al contenido de la notificación disponible en la sede electrónica de la Administración u organismo actuante, por medio de la dirección habilitada única (DEH) o a través de ambos canales, dependiendo de lo que cada Administración haya dispuesto en materia de notificaciones. (Gestor de notificaciones y avisos electrónicos). En cuanto a los efectos propios de la notificación se entenderá producida en el momento en que el interesado o su representante acceda al contenido. En los casos en que el interesado esté obligado al uso de estos medios o lo haya elegido expresamente, se entenderá rechazada cuando hayan transcurrido 10 días naturales desde la puesta a disposición sin haber accedido a su contenido. (art. 43.2 LPACP).

El Registro Electrónico de Apoderamientos (APODERA) creado por el artículo 15 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la ley 11/2007 de 22 de junio, de Acceso Electrónico de la ciudadanía a tos Servicios Públicos, permite hacer constar las representaciones que los ciudadanos otorguen a terceros para actuar en su nombre de forma electrónica ante la Administración General del Estado y sus organismos públicos vinculados o dependientes.

¿Qué puede hacer un ciudadano como poderdante por Internet?

- Crear un apoderamiento para uno o varios trámites
- Consultar sus apoderamientos
- Ampliar la vigencia de sus apoderamientos
- Revocar apoderamientos

¿Qué puede hacer un apoderado por Internet?

- Consultar sus apoderamientos
- Renunciar a apoderamientos
- Confirmar apoderamientos (si los trámites asociados así lo requieren)

¿A quién se puede otorgar un apoderamiento?

A cualquier persona física o empresa, aportando en este último caso la razón social y el NIF de la misma y de su representante legal.

¿Qué puedo apoderar?

Todos Los trámites y actuaciones por medios electrónicos que con carácter previo hayan comunicado al Registro los departamentos ministeriales y organismos públicos competentes para su tramitación. Los trámites que se pueden apoderar dependen de las diferentes Administraciones Públicas.

Más información sobre APODERA

https://sede.administracion.gob.es/PAG_Sede/ServiciosElectronicos/RegistroElectronicoDeApoderamientos.html#2

Sobre las notificaciones podemos destacar los siguientes artículos:

- Artículo 41. Condiciones generales para la práctica de las notificaciones.
  - » Art. 41.1 Las notificaciones preferentemente electrónico, y en todo, cuando el interesado resulte obligado a recibirlas por esta vía.
- Artículo 42. Práctica de las notificaciones en papel.
  - » 42.1. Todas las notificaciones que se practiquen en papel deberán ser puestas a disposición del interesado en la sede electrónica de la Administración u Organismo actuante para que pueda acceder al contenido de las mismas de forma voluntaria.

- Artículo 43. Práctica de las notificaciones a través de medios electrónicos.
  - » 43.1. Las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica de la Administración u Organismo actuante, a través de la dirección electrónica habilitada única o mediante ambos sistemas, según disponga cada Administración u Organismo. A los efectos previstos en este artículo, se entiende por comparecencia en la sede electrónica, el acceso por el interesado o su representante debidamente identificado al contenido de la notificación.
  - » 43.2. Las notificaciones por medios electrónicos se entenderán practicadas en el momento en que se produzca el acceso a su contenido. Cuando la notificación por medios electrónicos sea de carácter obligatorio, o haya sido expresamente elegida por el interesado, se entenderá rechazada cuando hayan transcurrido diez días naturales desde la puesta a disposición de la notificación sin que se acceda a su contenido.
- Artículo 44. Notificación infructuosa.
- Cuando los interesados en un procedimiento sean desconocidos, se ignore el lugar de la notificación o bien, intentada ésta, no se hubiese podido practicar, la notificación se hará por medio de un anuncio publicado en el «Boletín Oficial del Estado», para lo que existe la siguiente plataforma:

El Tablón Edictal Único (TEU).

https://www.boe.es/tablon_edictal_unico/

Asimismo, previamente y con carácter facultativo, las Administraciones podrán publicar un anuncio en el boletín oficial de la Comunidad Autónoma o de la Provincia, en el tablón de edictos del Ayuntamiento del último domicilio del interesado o del Consulado o Sección Consular de la Embajada correspondiente. Las Administraciones Públicas podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión, que no excluirán la obligación de publicar el correspondiente anuncio en el «Boletín Oficial del Estado».

El 21 de junio de 2017, la *Comisión Sectorial de Administración electrónica (CSAE)*, que es el órgano técnico que contemplado en la ley 40/2015, para la cooperación en materia de administración electrónica entre la Administración General del Estado, las administraciones de las comunidades Autónomas y las administraciones que integran la Administración Local, aprobaron los siguientes acuerdos con respecto a Notificaciones y Comunicaciones Electrónicas:

- Crear un **Punto Único de Notificaciones** para todas las Administraciones Públicas de forma similar al Punto General de Entrada de Facturas electrónicas (FACe). Dicho punto será proporcionado por el actual Ministerio de Política Territorial y Función Pública. Cada Comunidad Autónoma y Entidad Local asume la obligación de disponer de un punto único propio que concentre todas las notificaciones que se produzcan dentro de su sector público, de cara a facilitar el intercambio de información con el Punto Único de Notificaciones. El objetivo de esta medida es concentrar el acceso a las notificaciones en un solo punto, cumpliendo así con el Art. 43.4 de la ley 39/2015 "Los interesados podrán acceder a las notificaciones desde el Punto de Acceso General electrónico de la Administración, que funcionará como un portal de acceso". Este punto es la carpeta ciudadana del Gobierno de España.

carpeta Ciudadana
administracion.gob.es

COMISIÓN SECTORIAL
:)@dministración electrónica

https://sede.administracion.gob.es/carpeta/clave.htm

- Disponer de un **punto centralizado de datos de contacto de ciudadanía y empresas** para garantizar la correcta realización del envío del aviso de la puesta a disposición de una notificación electrónica al dispositivo electrónico y/o a la dirección de correo electrónico del interesado. Este punto centralizado debiera estar disponible de forma federada para que el ciudadano pueda revisar los datos de contacto que obran en poder de las Administraciones Públicas y para que pueda asegurarse de la eficacia de las notificaciones que realicen las Administraciones Públicas.
- Para consultar las **notificaciones pendientes** y comparecer a las mismas por parte **de una Administración Pública** no debe ser necesario utilizar un certificado de persona física representante de persona jurídica. Para posibilitar la automatización, debería admitirse **el sello electrónico reconocido o cualificado**.

6.1.8. Custodia de Claves

La Directiva 95/46/CE del Parlamento Europeo y el Consejo establece la obligatoriedad de proteger la confidencialidad de los datos de carácter personal.

La técnica criptográfica de claves bajo custodia, o también de depósito de claves, (en inglés key escrow) consiste en que las claves que se necesitan para descifrar los datos cifrados son depositadas y almacenado en un dispositivo seguro (HSM)

La gestión de claves centralizada permite a una organización gestionar de una manera centralizada todos los certificados emitidos a su personal.

- Mejora la seguridad en la custodia de las claves privadas de los certificados.
- Facilita la movilidad de los usuarios entre diferentes equipos de la organización manteniendo los certificados accesibles.
- Trazabilidad en el uso de los certificados digitales de la organización.
- Ahorro importante de costes.

El establecer una separación clara entre las funciones de gestión de claves, que deberán ejecutarse de forma centralizada, y las distintas aplicaciones en las que las claves sean utilizadas, el cual todas las claves simétricas se gestionan de forma centralizada, se le denomina *Enterprise Key Management* (EKM).

Solo bajo ciertas circunstancias, una tercera parte autorizada pueda tener acceso a ellas para poder descifrar los datos. Esta tercera parte podría ser por ejemplo empresas que quieren acceder a las comunicaciones de sus empleados, o gobiernos, que quieren ver el contenido de las comunicaciones.

7 Procesos de firma y Política de Firma e identidad digital

7.1. Proceso de Firma

Para entender el proceso de firma de forma sencilla vamos a introducir unos conceptos básicos: función hash, criptografía asimétrica (clave pública/privada), informe de firmas.

Función Hash

Uno de los elementos más importantes del proceso de firma es la función hash utilizada. Una función hash recoge un documento y genera una representación condensada de éste de un tamaño fijo (SHA-1 utilizado en formato CADES reduce el documento a 160 bits, SHA-256 en 256bits y SHA512 en 512 bits, siendo más seguros cuanto mayor sea el tamaño de la representación) que permite determinar la integridad del documento original. Cualquier cambio mínimo en el documento original, generará una representación completamente diferente. La función hash SHA-1 es obsoleta, debido a que el algoritmo desarrollado en los años 90 presentaba debilidades que han sido superadas, por lo que se recomienda su cambio urgente en todos los procesos de firma donde se emplee.

Criptografía Asimétrica

La criptografía permite cifrar una información/documento con una clave de forma que podrá ser descifrado usando la misma clave (criptografía simétrica) u otra clave (criptografía asimétrica). Esta última está basada en dos claves, conocidas como clave pública y clave privada. Para el proceso de firma digital, el documento se cifra con la clave privada y con la clave pública se puede verificar la firma. Esta verificación implica que el emisor es quien dice ser (Autenticidad), que el documento no ha sido modificado (Integridad) y que el emisor no puede negar haber sido el quien firmó el documento (No repudio).

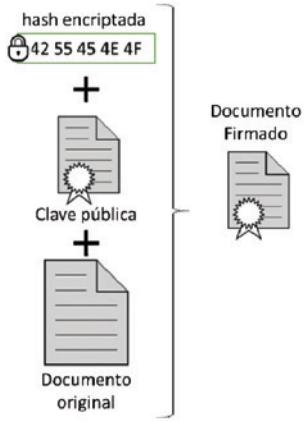
Proceso de Firma del Documento

En este apartado se verán los pasos para generar el documento firmado.

1. Calcular la función hash del documento a firmar. Suele ser un documento pdf, aunque también puede ser una imagen.

2. Encriptar hash con la clave privada

3. Generar el documento firmado electrónicamente.



Verificación de la firma

Cuando una aplicación recibe un documento firmado realiza las siguientes comprobaciones para ver que el documento no ha sido manipulado.

1. Usando la clave pública, desencriptarla para obtener el hash original

2. Generar de nuevo el hash a partir del documento recibido

3. Si el valor hash desencriptado en el paso 1 coincide con el hash generado en el paso 2. Se ha comprobado las tres propiedades de autenticidad, integridad y no repudio.

Formatos de firma

El formato de firma es la **forma como se genera el documento de firma** y como se guarda o estructura la información de firma en el documento generado. En una firma electrónica se puede almacenar información sobre el documento original, el firmante, la fecha de la firma, algoritmos utilizados y posible caducidad de la firma.

La existencia de múltiples formatos de firma se debe a razones históricas, a cómo se ha ido introduciendo la firma en formatos de documentos ya existentes y a cómo se han ido añadiendo funcionalidades a lo largo del tiempo.

Los formatos de los documentos electrónicos con firma avanzada deben ajustarse a las especificaciones de los estándares europeos. Un formato de firma viene determinado por estos aspectos:

a) Estructura interna de la firma

Cómo se estructura esta información (el orden de esa información dentro del fichero, las etiquetas que indican cuando empieza un campo y cuando termina, la opcionalidad de esos campos, etc.) viene determinado por distintos formatos:

- **CAdES** (CMS Avanzado)

  Es la evolución del primer formato de firma estandarizado. Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información. Tras firmar, no podrás ver la información firmada, porque la información se guarda de forma binaria.

- **XAdES** (XML Avanzado)

  El resultado es un fichero de texto XML, un formato de texto muy similar al HTML que utiliza etiquetas. Los documentos obtenidos suelen ser más grandes que en el caso de CAdES, por eso no es adecuado cuando el fichero original es muy grande.

- **PAdES** (PDF Avanzado)

  Este es el formato más adecuado cuando el documento original es un pdf. El destinatario de la firma puede comprobar **fácilmente la firma** y el **documento firmado.** Con los formatos anteriores esto no es posible si no se utilizan herramientas externas.

Algunas aplicaciones de firma permiten elegir el formato a utilizar. Otras imponen siempre el mismo formato y otras deciden automáticamente el formato en función del formato original del documento a firmar

b) ¿Dónde se guarda el documento original?

Según cómo se referencie o dónde se guarde el documento original en el fichero de firma, podemos tener dos casos:

El documento original se incluye en el **fichero de firma.**

Ventaja: No es necesario guardar siempre el documento original y el documento de firma porque aquél ya está incluido en éste. Es, por tanto, un formato cómodo de almacenar.

Desventaja: Si el tamaño del fichero es elevado, se consume más espacio de almacenamiento, porque al final se acaba teniendo por un lado el documento original, que siempre habrá que guardarlo, y por otro, la firma.

En el caso de CAdES estas firmas se llaman **firmas implícitas.**

En el caso de firmas **XAdES XML**, lo habitual es que el documento esté incluido en el fichero de firma. Hablamos de firmas **envolventes (enveloping) y envueltas (enveloped)** según en qué sitio del propio fichero de firma se guarde el documento original.

En el caso de PAdES, el archivo PDF contiene las firmas, con lo que no es necesario guardar el documento original

El documento **no se incluye en la firma.**

En este caso, el documento no se incluye en el resultado de firma o solamente se **incluye una referencia al lugar** en el que se encuentra para que el documento pueda ser localizado. Por tanto, se obtienen **ficheros de tamaño más reducido**, pero, por el contrario, el **documento original siempre hay que guardarlo junto a la firma.**

En el caso de CAdES estas firmas se llaman **firmas explícitas**.

En el caso de firmas XAdES XML, se denominan **firmas despegadas (detached)**

a) Firmas con múltiples usuarios.

En el mundo del papel y de la firma manuscrita, un documento puede contener la firma de varias personas:

- En un caso, las firmas pueden tener el **mismo peso o valor legal**, por lo que da igual el orden en el que se estampen las firmas en el documento.
- Otro caso, es el que unas firmas sirven para **refrendar o certificar otras firmas anteriores,** por lo que el orden en el que se estampan las firmas es importante.

El equivalente a esas firmas en el mundo electrónico son las **firmas múltiples.** Atendiendo al criterio del número de firmantes podemos tener:

- **Firmas simples.** Son las firmas básicas que contienen la firma de un solo firmante.
- **Co-firma o firma en línea.** Es la firma múltiple en la que todos los firmantes están al mismo nivel y en la que no importa el orden en el que se firma. La co-firma se utiliza en la firma de documentos que son resultados de reuniones, conferencias o comités.
- **Contra-firma o firma en cascada.** Firma múltiple en la que el orden en el que se firma es importante, ya que cada firma **debe refrendar o certificar la firma del firmante anterior.** La contra-firma se utiliza especialmente en aplicaciones como los Porta Firmas, en los que un documento debe seguir una línea específica a través de varios firmantes hasta que todo el proceso es aprobado.

Las aplicaciones de firma **@Firma y eCoFirma** permiten ambas los tres tipos de firma. En ellas, el usuario puede elegir el tipo de firma múltiple que desea realizar.

b) Longevidad de la firma y sello de tiempo

Para verificar una firma es necesario:

- Comprobar la **integridad de los datos firmados** asegurando que éstos no hayan sufrido ninguna modificación.
- Comprobar que el **estado del certificado con el que se firmó era el correcto**, es decir, era vigente en el momento de la operación.

En el caso de la firma electrónica básica, si el certificado está caducado automáticamente se da la firma como no válida.

Entonces, ¿cómo sabemos que el certificado estaba vigente o no en la fecha en la que se firmó? Y ¿qué debe hacerse para que cuando **se quiera validar o verificar una firma en el futuro la validación sea posible aunque esté caducado el certificado?**

Para dar respuesta a estas preguntas, los formatos AdES (forma genérica de llamar a los formatos CAdES, XAdES y PAdES) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional que **garantiza la validez de una firma a largo plazo**, una vez vencido el periodo de validez del certificado.

Estos formatos añaden a la firma evidencias de terceros (de **autoridades de certificación/PSC**) y **certificaciones de tiempo**, que realmente certifican cuál era el estado del certificado en el momento de la firma.

Concretamente, existen distintos formatos de firma que van incrementando la calidad de la misma hasta conseguir una firma que pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas:

- **Firma Básica (AdES - BES),** es el formato básico para satisfacer los requisitos de la firma electrónica avanzada.
- **AdES T**, se añade un sellado de tiempo (T de TimeStamp) con el fin de situar en el tiempo el instante en que se firma un documento
- **AdES C**, añade un conjunto de referencias a los certificados de la cadena de certificación y su estado, como base para una verificación longeva (C de Cadena)
- **AdES X**, añade sellos de tiempo a las referencias creadas en el paso anterior (X de eXtendida)
- **AdES XL**, añade los certificados y la información de revocación de los mismos, para su validación a largo plazo (XL de eXtendido Largo plazo)
- **AdES A**, permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones (A de Archivo)

En caso de PAdES, una firma XL se denomina LTV (Long Term Validation)

El Sello de Tiempo es una firma de una Autoridad de Sellado de Tiempo **(TSA),** que actúa como **tercera parte de confianza** testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

El sellado de tiempo proporciona un valor añadido a la utilización de firma digital, ya que la firma por sí sola no proporciona ninguna información acerca del momento de creación de la firma, y en el caso de que el firmante la incluyese, ésta habría sido proporcionada por una de las partes, cuando lo recomendable es que la marca de tiempo sea proporcionada por **una tercera parte de confianza**.

Puesto que el Sello de Tiempo es una firma realizada con el certificado electrónico de la Autoridad de Sellado, cuando ese certificado caduca, el sello y, por tanto la firma, dejan de ser válidas. Por eso, antes de que el certificado de la TSA caduque es necesario **resellar** o aplicar un nuevo Sello Temporal para mantener la validez temporal de la firma.

Código Seguro de Verificación (CSV)

En el artículo 18.1.b de la ley 11/2007 de acceso electrónico de la ciudadanía a los Servicios Públicos se dice que:

Para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar... b) Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Ese CSV es un código que se genera automáticamente y se incluye en el informe de firmas que se genera al firmar un documento cuando este va a imprimirse en papel. Las administraciones deben tener una web de validación de documentos impresos, en la que podrá escribirse el CSV y acceder al documento original asociado a su copia en papel.

7.2. Política de Firma e identidad digital

Una política de firma electrónica son las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica. En el artículo 18 del Real Decreto 4/2010 se indica que la Administración General del Estado deberá definir una política que será el marco de referencia dentro de su ámbito de actuación permitiendo que esta pueda ser utilizada como referencia por otras Administración Públicas para definir sus políticas de certificados y firmas en los ámbitos en los que tengan competencia.

Esa podría ser la opción más sencilla por parte de otras administraciones de cumplir con la obligación que se indica en el mismo artículo de definir sus propias políticas, es decir, adecuarse a la política de la AGE[14].

[14] La última versión está disponible en: http://administracionelectronica.gob.es/ctt/politicafirma

En una política se definen todos los elementos a tener en cuenta relacionados con la firma electrónica en una Administración entre los que destacan:

- Alcance de la Política de Firma
- Actores Involucrados en la Firma Electrónica
- Gestión de la Política de Firma
- Archivado y custodia
- Formatos admitidos de firma
- Creación de la Firma Electrónica
- Verificación de la Firma Electrónica

En los siguientes apartados se verán con más detalle los elementos anteriores.

Alcance de la Política de Firma

En el alcance hay que indicar el marco de aplicación de la política que se esté definiendo, la convivencia con otras políticas y la forma de identificación única de la misma. Dicha identificación tiene que estar en un formato que pueda ser interpretado y procesado automáticamente por los sistemas de creación y validación de firma (por ejemplo, estándar ETSI TR 102 038).

Actores Involucrados en la Firma Electrónica

En este apartado hay que indicar todos los actores relacionados con los procesos de creación y validación de firma. En la política de la AGE se definen cuatro actores: Firmante, verificador, prestador de servicios de firma electrónica y emisor de la política de firma.

Gestión de la Política de Firma

Se indica en este punto como se mantiene y actualizan los documentos de política de firma, quién es el órgano competente y la necesidad de que las diferentes versiones de la política tienen que tener un identificador único.

Archivado y custodia

Para que se garantice la fiabilidad de la firma debe mantenerse en el tiempo junto con la información sobre el estado del certificado en el momento en que se realizó incorporando un sello de tiempo. Es decir, que la firma debe poder validarse incluso si el certificado con el que se firmó ha caducado en el momento de la verificación. Para que esto funcione debe existir un servicio que mantenga las evidencias de la validez de la firma. En este apartado hay que definir como se realizará este servicio que deberá realizar resellados de forma periódica para asegurar la validez a lo largo del tiempo.

Formatos admitidos de firma

Los formatos de los documentos electrónicos con firma avanzada deben ajustarse a las especificaciones de los estándares europeos. En la versión 1.9 de la política de la AGE se admiten los formatos: XAdES, CAdES y PAdES. Los formatos admitidos deberán actualizarse para permitir la interoperabilidad conforme vayan evolucionando las normas europeas.

Creación de la Firma Electrónica

La política debe indicar en este punto, directamente o referenciando a algún anexo las características que debe tener los objetos firmados. El servicio de firma debe ejecutar una serie de verificaciones relacionadas con la política de firma correspondiente que indique como realizar la validación y la comprobación de validez de los certificados. El resultado será crear un fichero con una extensión .xsig para XAdES, .csig para CAdES y se incluirá dentro del mismo documento .pdf para las firmas con PAdES.

Verificación de la Firma Electrónica

Es muy importante que los documentos firmados puedan ser verificados y la validación de firma debe dar: Garantía de validez de la firma, validez de los certificados en el momento en que se firmó y verificar los sellos de tiempo en el caso en que así lo requiera la plataforma o el servicio concreto.

8 Servicios electrónicos de confianza: el papel del Ministerio de Economía y Empresa

8.1. Introducción

La «Estrategia para el Mercado Único Digital» desarrolla la «Agenda Digital[15] para Europa» basándose en tres pilares relacionados con la economía digital: mejorar el acceso de consumidores y empresas a los bienes y servicios digitales, crear las condiciones adecuadas para su éxito y aprovechar al máximo su potencial de crecimiento.

En consecuencia, en junio de 2012 la Comisión Europea presentó una ambiciosa propuesta para el desarrollo de un nuevo Reglamento europeo que sustituyese a la ya obsoleta Directiva 1999/93/CE, de firma electrónica. En lugar de una revisión de la Directiva, la elección de un Reglamento como instrumento legislativo, de inmediata aplicación en los Estados miembros, vino motivada por la necesidad de reforzar la seguridad jurídica en el seno de la UE, acabando con la dispersión normativa provocada por las transposiciones de la Directiva en los ordenamientos jurídicos internos a través de leyes de firma nacionales (en España, la Ley 59/2003, de 19 de diciembre, de firma electrónica), que había provocado una importante fragmentación e imposibilidad de prestación de servicios transfronterizos en el mercado interior, agravada por las diferencias en los sistemas de supervisión aplicados en cada Estado. Por otro lado, se pretendía legislar en un mismo vehículo normativo dos importantes realidades: la identificación y los servicios de confianza electrónicos en sentido amplio, añadiendo los sellos de tiempo, los sellos electrónicos, los servicios de entrega electrónica y los de autenticación web a la firma electrónica, e instaurando el reconocimiento transfronterizo de identidades y servicios de confianza, armonizando y potenciando así las transacciones electrónicas seguras en el mercado interior, y aumentando la eficacia de los servicios en línea tanto del sector público como del privado y el comercio electrónico en la UE.

Tras dos años de negociaciones, el 28 de agosto de 2014 se publicó en el DOUE el *Reglamento*[16] *(UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE* (Reglamento eIDAS). El Reglamento entró en vigor el 17 de septiembre de 2014, aunque su fecha de aplicación efectiva fue el 1 de julio de 2016, provocando el desplazamiento jurídico de la Ley de firma electrónica.

[15] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Asi0016
[16] https://boe.es/doue/2014/257/L00073-00114.pdf

8.2. Prestación de servicios electrónicos de confianza

El Reglamento eIDAS como ya comentamos anteriormente sustituye el término «prestador de servicios de certificación» por el de «prestador de servicios de confianza», que define en el artículo 3(19) como *una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado (QTSP) o como prestador no cualificado de servicios de confianza.*

Estos prestadores pueden tener naturaleza pública o privada y estar dirigidos al público en general o bien centrarse en una organización concreta o un colectivo de personas (ej. administraciones, empresas o colegios profesionales).

Asimismo, el artículo 3(16) define servicio de confianza como el «*servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:*

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios».

Por otra parte, el Reglamento eIDAS establece una lista *numerus clausus* de servicios de confianza cualificados que se enmarcan en su ámbito y que se encuentran sometidos a su régimen de obligaciones y responsabilidades específicas, en concreto el sello electrónico de persona jurídica, el servicio de validación de firmas y sellos cualificados, el servicio de preservación de firmas y sellos cualificados, el servicio de sellado de tiempo, el servicio de entrega electrónica certificada y el servicio de expedición de certificados autenticación web (para acceso a páginas mediante el protocolo seguro HTTPS), que pueden ser combinados entre sí para la prestación de servicios complejos e innovadores, reforzándose así la seguridad jurídica de las transacciones electrónicas entre empresas y particulares, y entre éstos y las Administraciones públicas.

8.3. Régimen de supervisión y control

El establecimiento de un régimen armonizado de supervisión de los prestadores de servicios electrónicos de confianza tiene como objetivo garantizar las mismas condiciones en el conjunto de la Unión en relación con su seguridad y la responsabilidad.

El Ministerio de Economía y Empresa, a través de la Secretaría de Estado para el Avance Digital, ostenta la competencia de supervisión de los prestadores de servicios de confianza, con un régimen de supervisión ligera, reactiva y posterior respecto de los prestadores no cualificados, y una supervisión completa e integral de los prestadores cualificados. En concreto, las funciones principales del órgano de supervisión son las siguientes:

- Supervisar a los prestadores cualificados (QTSP), a fin de garantizar, mediante actividades de supervisión previas y posteriores, que dichos prestadores cualificados de servicios de confianza, y los servicios de confianza cualificados prestados por ellos, cumplen los requisitos establecidos en el Reglamento;

- Adoptar medidas, en caso necesario, en relación con los prestadores no cualificados de servicios de confianza, mediante actividades de supervisión posteriores, cuando reciba la información de que dichos prestadores no cualificados de servicios de confianza, o los servicios de confianza prestados por ellos, supuestamente no cumplen los requisitos establecidos en el Reglamento;
- Cooperar con otros organismos de supervisión de otros Estados miembros;
- Analizar los informes de evaluación de la conformidad remitidos por los QTSP;
- Informar a otros organismos de supervisión y al público de violaciones de seguridad o la pérdida de integridad;
- Informar a la Comisión Europea de sus actividades principales;
- Realizar auditorías o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la conformidad de prestadores cualificados de servicios de confianza;
- Cooperar con las autoridades de protección de datos;
- Conceder y retirar la cualificación a los prestadores;
- Verificar la existencia y la correcta aplicación de las disposiciones relativas a los planes de cese;
- Requerir que los prestadores de servicios de confianza corrijan cualquier incumplimiento.

A su vez, los QTSP tienen como principales obligaciones:

1. Ser auditados, al menos cada 24 meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad acreditado.
2. Cuando el supervisor requiera a un QTSP que corrija un incumplimiento y éste no actúe, el supervisor podrá retirar la cualificación al prestador o al servicio en cuestión.

8.4. Entidades de evaluación de la conformidad

El Reglamento eIDAS define a las entidades de evaluación de la conformidad (ConformityAssessmentBodies, o CAB) como aquéllas cuya competencia para realizar una evaluación de conformidad de un prestador cualificado y de los servicios de confianza cualificados que presta esté acreditada en virtud de lo previsto en el Reglamento (CE) nº 765/2008, es decir, ante el organismo nacional de acreditación (NationalAccreditationBody, o NAB). De esta manera, los informes de evaluación de la conformidad (ConformityAssessmentReport, o CAR) son remitidos al supervisor como certificación del cumplimiento por parte del prestador cualificado de los requisitos exigidos en el Reglamento.

A fecha de 15 de junio de 2018, en España están acreditados por parte de ENAC (Entidad Nacional de Acreditación) los CAB siguientes:

- AENOR INTERNACIONAL
- EPOCHE AND ESPRI, S.L.
- CERTICAR, S.L.
- TRUST CONFORMITY ASSESSMENT BODY, S.L.

No obstante, de acuerdo con los principios del mercado interior, cualquiera de los CAB acreditados en cualquier Estado miembro podría emitir un CAR sobre un prestador establecido en España.

8.5. Lista de Servicios de Confianza (TSL)

De acuerdo con la Decisión 2009/767/CE, y en virtud de la Decisión de Ejecución (UE) 2015/1505/CE de la Comisión, el Ministerio de Economía y Empresa elabora desde junio de 2010 una Lista de confianza de prestadores de servicios de certificación (TSL) correspondiente a los prestadores que expiden certificados reconocidos y que están establecidos y supervisados en España. Con la irrupción del Reglamento (UE) nº 910/2014, la Lista de Confianza pasó a formar parte del articulado del propio Reglamento.

La TSL contiene información sobre todos los prestadores cualificados de servicios de confianza (firma electrónica, sello electrónico, conservación y validación de firmas y sellos, sello de tiempo, entrega electrónica y autenticación web). Las secuencias de las listas se van publicando a medida que surgen nuevos prestadores o servicios cualificados, y están oportunamente firmadas con certificados electrónicos específicos para este uso, que son comunicados a la Comisión Europea, de forma que se pueda comprobar su autenticidad e integridad. Se puede encontrar en las siguientes direcciones en sus formas HR (legible por humanos) y MP (procesable por máquinas):

- HR: (PDF/A PAdES): https://sede.minetur.gob.es/prestadores/tsl/tsl.pdf
- MP: (XML XAdES): https://sede.minetur.gob.es/Prestadores/TSL/TSL.xml

Por su parte, la Comisión Europea mantiene una relación de listas de los diferentes Estados miembros, agregando los enlaces a cada una de ellas en la "List of TrustedLists" (LoTL)[17].

8.6. Inicio de la prestación de un servicio cualificado

Cuando un prestador sin cualificación desee iniciar la prestación de un servicio de confianza cualificado, presentará al Ministerio de Economía y Empresa una notificación de su intención junto con un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad acreditado. Por su parte, el supervisor verifica si el prestador cumple los requisitos establecidos en el Reglamento y la legislación nacional aplicable. Si concluye que así es, concede

[17] https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers

la cualificación al prestador y a los servicios de confianza que éste presta, y actualiza la Lista de Confianza (TSL) en consecuencia.

Se trata por tanto de una autorización y no de una comunicación de inicio de actividad. Una vez el servicio cualificado haya sido incorporado a la TSL, el prestador podrá hacer uso de la «Etiqueta de confianza UE», de acuerdo con el Reglamento de Ejecución (UE) 2015/806 de la Comisión, de 22 de mayo de 2015.

Figura. Etiqueta de confianza UE

8.7. Aspectos adicionales en la futura Ley de Servicios de Confianza

Conforme a lo indicado *ut supra*, desde el 1 de julio de 2016, la Ley de firma electrónica se encuentra jurídicamente desplazada por el Reglamento eIDAS en todo aquello regulado por él, por lo que los preceptos que se opongan al mismo son inaplicables.

Esta situación se normalizará cuando sea promulgada, a instancias del Ministerio de Economía y Empresa, la nueva *Ley reguladora de determinados aspectos de los servicios electrónicos de Confianza*, cuyo objetivo es complementar el Reglamento eIDAS, cuya tramitación normativa prosigue su curso, habiéndose recibido en primera instancia de Consejo de Ministros[18] el 6 de abril de 2018.

Con la promulgación de la futura ley se pretende eliminar el riesgo de situaciones de inseguridad jurídica en las relaciones telemáticas de ciudadanos, empresas y Administraciones Públicas, derivadas de la transición al nuevo marco legislativo comunitario como consecuencia de diferencias en la interpretación de las normas aplicables, así como evitar vacíos normativos en la aplicación de la Ley firma electrónica a los servicios de confianza distintos de la firma electrónica regulados por el Reglamento.

Asimismo, se pretenden regular aquellos aspectos que el Reglamento eIDAS deja al criterio de los Estados miembros, como es el caso, entre otros, del régimen sancionador, los efectos legales de algunos servicios cualificados, el régimen de responsabilidad y de previsión de riesgo de los prestadores de servicios, la comprobación de la identidad y atributos de quien lo solicita de un certificado cualificado, la inclusión de requisitos adicionales a nivel nacional para certificados cualificados tales como identificadores nacionales, el tiempo máximo de vigencia de los certificados cualificados, o el régimen de suspensión de certificados.

[18] http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/060418_servicioselect.aspx

9 Plataformas comunes relacionadas con la identificación y firma electrónica

La identificación y firma electrónica es la base de cualquier trámite digital. Históricamente, estas funcionalidades se realizaban a través de infraestructuras de clave pública, pero el nuevo reglamento europeo innova en la posibilidad de expandir la identificación y firma electrónica no sólo basándose en certificados digitales, si no también importantes mejoras sobre éstos, por ejemplo, la posibilidad de que estén en la nube.

Relacionado con esta problemática también hay determinadas cuestiones, como los Códigos Seguros de Verificación, o los "hashes" de los documentos, que forman parte del ecosistema general de identificación y firma por medios digitales como se ha expuesto en capítulos anteriores.

Desde la Secretaría General de Administración Digital, se provee de determinados servicios comunes y sistemas de información para facilitar que las administraciones públicas puedan realizar de manera efectiva las cuestiones relacionadas con la identificación y firma electrónica. Asimismo, potencia que se plantean soluciones interoperables, y criterios comunes, en un ámbito donde la dispersión puede hacer complicado el funcionamiento automatizado de los sistemas de información. A continuación, se desarrollan algunas de estas iniciativas

9.1. Sistema Cl@ve

El Servicio Común fundamental para la identificación y firma electrónica, tanto criptográfica como no criptográfica, provisto por la Secretaría General de Administración Digital, es el servicio cl@ve.

Este servicio facilita la identificación de la ciudadanía, bien sea a través de los certificados electrónicos clásicos, bien sean los sistemas relacionados con claves concertadas

En relación con los certificados criptográficos, permite el funcionamiento de cualquier proveedor de certificación admitido por el regulador, sean en tarjeta o en software, gracias a la conexión del proyecto cl@ve con el proyecto @firma. En lo que se refiere a los sistemas relacionados con claves concertadas, se puede trabajar en las dos versiones que existen en la actualidad, el sistema cl@ve pin, y el sistema cl@ve permanente.

Se puede encontrar información del sistema cl@ve, tanto para la difusión como para facilitar su uso o incluir esta información para el ciudadano en http://clave.gob.es

Para encontrar información técnica, formas de uso e integración con aplicaciones, la información de identificación está en https://administracionelectronica.gob.es/ctt/clave

9.2. Identificación de la ciudadanía

El Servicio Común fundamental para la identificación y firma electrónica, tanto criptográfica como no criptográfica, provisto por la Secretaría General de Administración Digital, es el servicio cl@ve.

Este servicio facilita la identificación de la ciudadanía, bien sea a través de los certificados electrónicos clásicos, bien sean los sistemas relacionados con claves concertadas.

En relación con los certificados criptográficos, permite el funcionamiento de cualquier proveedor de certificación admitido por el regulador, sean en tarjeta o en software, gracias a la conexión del proyecto cl@ve con el proyecto @firma. En lo que se refiere a los sistemas relacionados con claves concertadas, se puede trabajar en las dos versiones que existen en la actualidad, el sistema cl@ve pin, y el sistema cl@ve permanente

Se puede encontrar información del sistema cl@ve, tanto para la difusión como para facilitar su uso o incluir esta información para el ciudadano en http://clave.gob.es

Para encontrar información técnica, formas de uso e integración con aplicaciones, la información de identificación está en https://administracionelectronica.gob.es/ctt/clave

9.3. Firmas de la ciudadanía

En relación con la firma no criptográfica, la Secretaría General de Administración digital publicó una resolución en el cual se indican los criterios que debieran seguir todas las administraciones públicas para que estas firmas electrónicas tengan unos niveles equivalentes de seguridad y de funcionamiento en todo el territorio.

Por lo que refiere a la firma criptográfica, el sistema cl@ve incorpora la posibilidad novedosa que permite el reglamento europeo de identificación y firma electrónica de realizar firmas electrónicas del máximo nivel de seguridad, y por medios completamente criptológicos, a través del sistema de cl@ve firma.

En este caso, el certificado digital en lugar de estar ubicado en una tarjeta, o en una pieza de software, se encuentra ubicado en unos dispositivos especiales, dotados de altas medidas de seguridad, siendo estos certificados emitidos por la Dirección General de la Policía, al igual que el DNI electrónico tradicional. Estos sistemas de información, que en cuanto a su proceso están ubicados tanto en la policía como en la gerencia informática de la seguridad social, para mayor seguridad y redundancia, permiten realizar las firmas electrónicas criptográficas con dichos certificados en los documentos obteniendo un resultado equivalente al que hasta ahora se conseguía con los certifi-cados en tarjeta o en software, y realizando la firma electrónica en cliente

Estas firmas criptográficas son de utilidad para favorecer la interoperabilidad y comprobación auto-matizada de firmante, o el no repudio de la información sin requerir ningún otro tipo de sistema o de pista de auditoría. De igual forma, mantiene la sencillez y facilidad de uso para el ciudadano que los sistemas basados en claves compartidas, porque no se tienen que preocupar de llevar una tarjeta en la que esté incluido el certificado criptográfico, ni es necesario que tengan a su disposición el ordenador o sistema de firma software con el que se estuvieran trabajando.

Información ampliada de este sistema que permite la firma electrónica en la nube se puede encontrar en https://administracionelectronica.gob.es/ctt/clavefirma

9.4. Suite de soluciones de firma electrónica @firma

Además de la plataforma mencionada de cl@ve firma, la SGAD proporciona un conjunto de soluciones orientadas a la realización y validación de firmas electrónicas criptográficas, entre las que destacan:

9.4.1. @Firma - Plataforma de validación de certificados y firmas

Existen muchos servicios públicos electrónicos que requieren firma electrónica y métodos avanzados de identificación o autenticación basados en certificados digitales. Debido a los múltiples certificados que pueden utilizarse y la multitud de estándares, implantar sistemas que soporten todas las funcionalidades resulta complejo y costoso.

La plataforma @firma, es un servicio multi-PKI de validación de certificados y firmas electrónicas, no intrusivo, integrable en cualquier servicio de administración electrónica de cualquier Administración Pública. Cumple los requisitos establecidos en los artículos 18, 19 y 20 del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010).

Los servicios son aplicables a todos los certificados electrónicos generados por cualquier proveedor de servicio de certificación supervisado por el Ministerio de Economía y Empresa, incluidos los del DNIe.

9.4.2. FIRe - Solución Integral de Firma electrónica

FIRe es una solución integral de firma electrónica que permite simplificar todos los requisitos de creación de firmas basadas tanto en certificados locales como en certificados en la nube.

Gracias a FIRe las aplicaciones ya no tienen que gestionar los componentes de realización de firmas como el Miniapplet, Autofirma o Clave Firma y pueden centrarse en su negocio ya que todas las cuestiones relativas a la firma se delegan en FIRe.

La solución FIRe está compuesta por dos componentes:

- El API FIRe son librerías que se integran en las aplicaciones que necesitan servicios de realización de firmas. Estas librerías permiten conectarse al servidor FIRe y se ofrecen en los lenguajes JAVA, PHP y .Net.
- El Servidor FIRe es el componente central de la solución y contiene la inteligencia que permite al usuario la selección del método de firma y la propia realización de las firmas, usando tanto certificados en local como certificados en la nube. Para la firma en local, el Servidor FIRe incluye el Miniapplet de @firma y la adaptación a Autofirma. Para la firma en la nube, FIRe se conecta al servicio de Cl@ve Firma proporcionado por la GISS y la DGP.

9.4.3. TS@ - Plataforma de sellado de tiempo

La Plataforma de Sellado de Tiempo (TS@) proporciona servicios de sellado de tiempo sincronizados con la hora oficial del Estado. Deja constancia, mediante la emisión de un sello de tiempo, de la fecha y la hora de cualquier operación o transacción en un momento dado y de que ninguno de los datos de la operación ha sido modificado desde entonces.

TS@ está reconocida por el Ministerio de Economía y Empresa como autoridad de sellado de tiempo y funciona como tercera parte de confianza.

El sellado de tiempo se puede aplicar a la firma electrónica para acreditar el momento de creación de la firma. Así, permite la protección de información y firma y garantiza su uso como evidencia electrónica en el futuro, ayudando al cumplimento de las medidas de seguridad del Esquema Nacional de Seguridad (Real Decreto 3/2010).

Ofrece también la validación de sellos de tiempo emitidos previamente y dispone de una interfaz de resellado.

9.4.4. VALIDe - Validación de firmas y certificados electrónicos

VALIDe es un portal de servicios online para la validación de Firmas y Certificados electrónicos.

El objetivo de este servicio es comprobar que el certificado utilizado es válido y no ha sido revocado, así como la validez de una firma electrónica realizada mediante certificado digital emitido por un prestador de servicios de certificación reconocido. También permite realizar firmas con un certificado digital del que se disponga de la clave privada.

Los servicios en línea que se ofrecen, abiertos a cualquier colectivo (ciudadanía, empresa, personal adscrito a la función pública), son:

- Validar el estado de un certificado digital emitido por cualquier entidad de servicio de certificación reconocida.
- Validar el estado de un certificado de Sede electrónica.
- Validar la firma electrónica de un documento con múltiples formatos y tipos de certificados, como facturas electrónicas, contratos, etc.
- Firmar electrónicamente un documento con cualquier certificado reconocido, con las máximas garantías de integridad y autenticidad.
- Visualizar una firma, descargando un justificante en formato PDF que incluya el documento original y los datos de los firmantes.

9.4.5. Port@firmas - Firma electrónica de empleado público

Port@firmas permite incorporar la firma electrónica en los flujos de trabajo de una organización. Usa el Cliente @firma para la firma cliente de usuario y se integra con la plataforma @firma para la validación de las firmas que se generan. Estas son algunas de las funcionalidades que incorpora:

- Firmas en paralelo o en cascada y usuarios que otorguen el visto bueno.
- Definir y utilizar flujos desde aplicaciones externas mediante servicios web.
- Organización de las peticiones en bandejas (enviados, entrantes, terminados y pendientes).
- Creación de grupos de firmantes.
- Consulta por CSV de documentos firmados.

El Port@firmas dispone de los siguientes interfaces de acceso:

- Interfaz web a través de navegador, para petición o realización de firmas.
- Clientes o aplicaciones móviles que permiten firmar desde smartphones y otros dispositivos móviles.
- Interfaz de servicios web para peticiones de firma y recepción de documentos firmados.

9.5. Códigos Seguros de Verificación

Pero hay otra forma de expresar las firmas electrónicas en los documentos, y ésta se utiliza de manera habitual en las administraciones públicas: a través de los códigos seguros de verificación, que son los que se suelen utilizar cuando se hacen firmas electrónicas no criptográficas.

La Secretaría General de Administración digital también ofrece determinados servicios, dentro de sus infraestructuras y sistemas para el documento electrónico, proyecto INSIDE, con el que facilitar el funcionamiento relacionado con este tipo de documentos. Por un lado, permite la generación de firmas basadas en Código Seguro de Verificación (CSV), o la creación de dichos códigos, lo que permite la realización de cambios de formato, de manera que documentos firmados con firma criptográfica, en algunas ocasiones no visible de manera fácil por los ciudadanos, o que no se pueden imprimir, tengan un documento que sea copia equivalente, en este caso con código seguro de verificación, que permite cotejo e impresión sencilla.

Aparte de tener cubierta la opción de la generación de este tipo de firmas, también a través de un módulo de la infraestructura y sistemas para el documento electrónico la Secretaría General de Administración Digital ofrece la parte del consumo, visualización o cotejo de los documentos que tienen CSV. Esto es importante para la ciudadanía, ya que gracias a este proyecto pueden consultar en un único punto, en la carpeta ciudadana, o en el punto de acceso general, los documentos relacionados a los códigos seguros de verificación enviados por distintas administraciones públicas, lo que les evita tener la complejidad de dirigirse a distintas sedes electrónicas, buscar el cotejo de documentos, incorporar el CSV en un campo de formulario distinto en cada caso, y a partir de ahí obtener el documento original para realizar dicho cotejo. Puede usarse este servicio en https://sede.administracion.gob.es/pagSedeFront/servicios/consultaCSV.htm?hc=&tam=2

Pero más importante que para la ciudadanía es para las Administraciones Públicas este proyecto, ya que cada vez es más habitual que los documentos no se adjunten, sino que se referencian, o es habitual presentar documentos con código seguro de verificación. Este proyecto (llamado CSV Broker) permite a las distintas administraciones públicas que, dado un código seguro de verificación, consulte en el nodo central, el cual se encarga de la interoperabilidad con la administración pública que tenga el documento, y se lo facilita por medios electrónicos y automáticos a la administración que necesite dicho documento para su expediente. La información de este proyecto está en el punto de acceso general, https://administracionelectronica.gob.es/ctt/inside/descargas

Es muy importante que todas las administraciones públicas que emiten documentos con códigos seguros de verificación se incorporen al proyecto para permitir no solamente a la ciudadanía la facilidad de consultar el documento en un punto único, sino, sobre todo, permitir la tramitación automatizada de los documentos que tienen código seguro de verificación, incorporación a los distintos expedientes administrativos.

9.6. Normalización de los resúmenes ("hash") de los archivos

Por último, hay que destacar, que en muchos casos no procede la firma como tal, pero sí que hay que relacionar de manera muy inequívoca y clara el documento a un determinado registro, expediente electrónico, o sistema información. Para ello, lo que se utiliza es los resúmenes criptográficos, o funciones hash en relación con los documentos.

Desde la Secretaría General de Administración Digital también se está promoviendo que, por un lado, todas las administraciones utilicen algoritmos criptográficos seguros para la creación de es-tos resúmenes de documentos, y por otro lado, que la información sobre este tipo de resúmenes en los distintos resguardos de registro, índices de expedientes, notificaciones etcétera, sea común e interoperable, para poder permitir de manera automática la comprobación de que un documento dado se relaciona de forma clara y unívoca con un determinado ticket de registro, por poner un ejemplo, algo que cada vez empieza a ser más necesario en general

En el punto de acceso general, al igual que ya existe un sistema validador de expedientes ENI, https://sede.administracion.gob.es/pagSedeFront/servicios/validarENI.htm, existirá en breve la posibilidad de dado un ticket (de registro, de índice electrónico, una notificación...) que tenga un hash, se pueda comprobar que coincide con un documento en cuestión.

10 Plan de Difusión

Este Plan de Difusión tiene como finalidad dar a conocer al conjunto de Entidades Locales Españolas el documento "Enciclopedia" sobre los "Servicios de Certificación para las Administraciones Locales".

Esta publicación surge de la necesidad detectada por la *Comisión de Sociedad de la Información y Tecnologías* de la *Federación Española de Municipios y Provincias* (FEMP), de ayudar a los Entes Locales, especialmente a aquellos que carecen de los conocimientos necesarios y facilitadores para el uso de los variados tipos de certificados digitales.

Cobra por tanto especial relevancia, el diseño y ejecución de un Plan de Difusión que permita llegar con acierto a los lugares donde la demanda es más evidente, contando para ello con otros interlocutores, buenos conocedores de la realidad en cada uno de los territorios.

Por otra parte, la FEMP dispone de mecanismos de comunicación a través de los cuales será posible dar la información y publicidad necesaria que el documento se merece.

Pero el Plan quedaría incompleto si no fuéramos capaces de realizar convocatorias presenciales, en las que exponer el alcance de la guía, resolver las dudas que puedan surgir, y realizar ejercicios prácticos que consoliden el conocimiento de los Servicios de Certificación, y que faciliten la elección del más apropiado cuando la situación así lo requiera.

De esta manera, nuestro Plan de Difusión se apoyará sobre tres pilares:

10.1. Diputaciones Provinciales/Federaciones Territoriales

Como socios prioritarios de esta Federación, y como conocedores de su realidad Territorial, solicitaremos su colaboración para realizar acciones de difusión que en su mayor parte tengan como destinatarios últimos a los municipios de menor población.

En especial, buscaremos la implicación de Diputaciones, Cabildos y Consejos Insulares, que tiene el mandato normativo de facilitar el desarrollo de la Administración Electrónica en municipios de su competencia menores de 20.000 habitantes, para que se involucren activamente en dar a conocer los servicios de Certificación, facilitando su uso en cada momento específico.

10.2. Difusión a través de las herramientas de Comunicación FEMP

10.2.1. Correo electrónico

Se realizará el envío de la información al conjunto de Entidades Locales españolas, intentando personalizarla en el responsable del desarrollo de la e-Administración.

10.2.2. Carta Local

Se publicará una noticia relacionada con los servicios de certificación y el trabajo desarrollado con la "Enciclopedia", en la Revista de la FEMP de edición mensual "Carta Local"

10.2.3. Página Web de la FEMP

Se pondrán a disposición los contenidos desarrollados, en la Página Web de la FEMP, en el apartado del Área de Sociedad de la información, para consulta y descarga, en su caso, por parte de los interesados.

10.2.4. Edición Impresa

Se buscaran alternativas y esponsorización para poder contar con una mínima edición impresa del documento, que facilite su visibilidad en determinados entornos.

10.3. Formación/Jornadas

10.3.1. Jornada de Presentación en la FEMP

Con cabida para técnicos de Entidades locales, pero a la que se invitará prioritariamente a los Cargos Electos, que deben liderar y propiciar el cambio en las Administraciones.

10.3.2. Formación Continua

Se propondrá, dentro del Plan de Formación Continua de la FEMP 2019, el desarrollo de una Acción Formativa, que gire en torno a los servicios de certificación y la Enciclopedia elaborada, con casos prácticos e intentando resolver las preguntas más frecuentes.

Una segunda edición de dicha Acción formativa, será propuesta, a los responsables del Plan de Formación Continua de la FEMP 2020.

10.3.3. Jornadas en Diputaciones/Federaciones Territoriales

Se facilitará un modelo de jornada al conjunto de Federaciones Territoriales, así como a las Diputaciones Provinciales, Cabildos y Consejos Insulares, para que puedan replicar acciones de formación en sus territorios, colaborando y coordinando las mismas en la medida de las necesidades y/o la demanda.

10.3.4. Otras Jornadas/Conferencias

Se buscará oportunidades para divulgar el trabajo en jornadas y conferencias desarrolladas por terceros, tales como: NovaGob, CNIS, etc.

Las actuaciones que deben implementarse se desarrollarán a partir del **último trimestre de** 2018, y se extenderán durante 2019. Siguiendo la siguiente Cronología:

Actividad	Fecha
Mesa redonda en JOMCAL 2018	octubre 2018
Presentación en NovaGob	octubre 2018
Correo divulgativo, artículo en carta Local y Publicación en Web FEMP	noviembre/diciembre 2018
Edición Impresa	noviembre/diciembre 2018
Jornada de Presentación en la FEMP	diciembre 2018
Acción Formativa FEMP	durante 2019 y 2020
Jornadas Diputaciones/Federaciones Territoriales	durante 2019 y 2020
Otras Jornadas/Conferencias	durante 2019 y 2020

11 Plan de Concienciación

La Identidad Digital mediante el uso de certificados electrónicos es una de las necesidades básicas que se debe de cubrir en una institución si se quiere hacer un despliegue integral de la administración electrónica y dar cumplimiento a la normativa vigente.

Sin embargo, cada vez se complica más. En este momento tenemos que tener en cuenta el uso de distintos dispositivos y plataformas, móvil y física y tomar conciencia corporativa de todas ellas.

El correcto y fácil uso de los certificados electrónicos, es una de las asignaturas pendientes, siendo uno de los aspectos fundamentales que debe tener en cuenta toda institución. Concienciar tanto al personal como a los agentes potenciales de las herramientas de gestión y servicios públicos que se desarrollen, es una tarea fundamental.

Desde las administraciones, hay que concienciar y establecer una **cultura corporativa en política de identidad digital** tanto teórica como práctica, para cada persona, específica según sus conocimientos, y adaptada a las tareas que lleva a cabo diariamente en su puesto de trabajo.

11.1. Formación vs Concienciación

Hay que diferenciar entre concienciar y formar.

Concienciar: crear cultura digital. Es necesario concienciar a todos los miembros de la institución en el uso de medios digitales, la seguridad y las implicaciones y riesgos de no asumirla.

Formar: la formación es continua y no acaba nunca. Se debe involucrar a toda la organización, pero a diferencia de la concienciación, los cursos deben ser dirigidos.

Es por ello que en este documento se trabajan dos apartados, por un lado el **Plan de Concienciación** y por otro el **Plan de Formación**.

11.2. Concienciación

En este apartado se incluyen algunas recomendaciones con las que se pretende concienciar a todos de que contar una **Política de Identidad digital debe constituir una parte central de la estrategia en la administración electrónica** que vayamos a desplegar.

La administración tiene que tener una estrategia que tenga por objetivo una concienciación en los ámbitos políticos y técnicos para que respondan de forma ágil a las necesidades de una competencia cada vez más compleja en la materia de Identidad digital.

Cualquier proceso interno supone un **cambio cultural** importante en la organización, por tanto será fundamental plantear un plan de concienciación interno que culturice al conjunto de la organización de la importancia y beneficios que implican el uso de certificados digitales y su implicación en los procesos electrónicos.

Cada organización tiene su propia estructura interna de funcionamiento. No obstante, es recomendable definir y pensar acciones de concienciación adecuadas a la **heterogeneidad de las personas que forman parte de nuestra organización** y al rol que puedan tener en materia de identidad digital.

11.3. Propuesta Plan de Concienciación corporativo

El plan se desarrollará de forma **transversal** durante todo el ciclo de vida del proceso. Las acciones de concienciación **deberán ser presenciales** y como mejora, se aconseja complementar con acciones on-line.

Sesión para responsables de la información y servicios

Número de sesiones: a determinar según las características de la organización.

Duración: deseable 3 horas

Objetivo: Conocer las Funciones y Obligaciones derivadas de la Política de Identidad Digital.

Será deseable siempre que las sesiones presenciales se complementen mediante sesiones alternativas on-line, como mejora y refuerzo de concienciación.

Sesión específica funciones y obligaciones (Parametrización y uso de distintos certificados digitales)

Número de Sesiones: a determinar según las características de la organización.

Duración: 2-3 horas

Objetivo: Difundir en la organización el modelo de identidad y uso de certificados y la asignación de responsabilidades

Destinatarios: Responsables de la información y servicios

Acciones de concienciación general para toda la organización

Con el objetivo de mejorar el grado de cultura de identidad digital se desarrollaran una serie de acciones para toda la organización, agrupando por tipología. Los grupos se definirán durante una fase previa de formación, conteniendo al menos los siguientes grupos:

- Jornada para grupos políticos
- Jornada para responsables de áreas
- Jornada para personal IT
- Jornada para personal adscrito a la función pública

Jornada para directivos (Equipo de gobierno)

¿Por qué una jornada para "directivos" (equipo de gobierno)?

Cada vez más organismos y/o empresas abordan planes para sensibilizar a su personal en medios electrónicos y uso de distintas plataformas y dispositivos digitales, conscientes del riesgo que entraña la falta de concienciación y el desconocimiento de las normas básicas.

Número de Sesiones: 1

Duración: 2 horas

Objetivo: Desarrollar los principales conceptos vinculados con la seguridad de la información, evitando los principales riesgos derivados del uso de nuevas tecnologías

Destinatarios: Equipo de Gobierno / personal directivo

Jornada para responsables de áreas y/o departamentos

Número de Sesiones: 1

Duración: 2 horas

Objetivo: Conocer los principales riesgos que resultan de aplicación en función del rol que desempeñan en la organización, así como las funciones y obligaciones.

Destinatarios: Responsables de la información por áreas

Jornada para personal IT

Número de Sesiones: a determinar según las características de la organización.

Duración: 8 horas

Objetivo: Conocimiento sobre los distintos medios de certificación, como aplica cada uno de ellos, requisitos técnicos, tipología de certificados y alcance, medidas de seguridad conforme a la norma UNE-ISO/IEC 27001 (SGSI) e integración con el Esquema Nacional de Seguridad (ENS)

Destinatarios: Personal IT del área de nuevas tecnologías/departamento de informática

Jornada general para el personal de la organización

Número de Sesiones: a determinar según las características de la organización. **Duración:** 1-2 horas

Objetivo: Desarrollar las pautas en política de identidad digital, necesarias para hacer un buen uso de la información y de los sistemas que la tratan, con el objetivo de que puedan ser conocidas y aplicadas por todo el personal y reducir la probabilidad de fallos y daños causados por problemas de seguridad y autentificación.

Destinatarios: Todo el personal de la organización

Es necesario volver a recordar que **no existen actuaciones milagrosas**. Como decíamos, ésta es una actividad que se valorará por la **perseverancia y continuidad**. Se trata de realizar, con cierta metodología, reuniones, acciones de concienciación tradicionales o innovadoras con los colectivos definidos, de forma constante y no sólo al inicio del proceso de cambio.

Cada administración deberá escoger las acciones que mejor se adapten a sus características, y, siempre que sea posible, implicar en nuestra estrategia y diseño del Plan de Concienciación a los departamentos de prensa y de comunicación de la organización.

12 Plan de Formación Interno (cargos políticos y personal adscrito a la función pública)

El uso del certificado electrónico y la firma de documentos electrónicos forma parte ya de nuestro día a día en nuestras instituciones y es importante conocer los pasos que debemos seguir para potenciar el uso de la administración electrónica.

Parece oportuno después de todos los conceptos analizados en este documento crear un test de valoración de los conocimientos adquiridos para así asegurar la aplicación y el uso de los certificados y la firma en nuestras administraciones públicas. Ya se hace la siguiente propuesta:

- **Destinatarios**: Personal al Servicio de las Administraciones Públicas.
- **Duración:** 10 horas

IDENTIDAD DIGITAL Y FIRMA ELECTRÓNICA ADMINISTRACIONES PÚBLICAS.

A. MARCO LEGAL.

1. LEY ORGÁNICA 4/2015, DE 30 DE MARZO DE PROTECCIÓN DE LA SEGURIDAD CIUDADANA.
2. LEY 59/2003, DE 19 DE DICIEMBRE DE FIRMA ELECTRÓNICA.
3. REAL DECRETO 1553/2005, DE 23 DE DICIEMBRE, POR EL QUE SE REGULA LA EXPEDICIÓN DEL DOCUMENTO NACIONAL DE IDENTIDAD Y SUS CERTIFICADOS DE FIRMA ELECTRÓNICA.
4. LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS.
5. LEY 40/2015, DE 1 DE OCTUBRE, DE RÉGIMEN JURÍDICO DEL SECTOR PÚBLICO.

B. REGLAMENTO (UE) N.º 910/2014 SOBRE IDENTIFICACIÓN ELECTRÓNICA Y SERVICIOS DE CONFIANZA (EIDAS).

1. IDENTIFICACIÓN ELECTRÓNICA.
2. SERVICIOS DE CONFIANZA.
3. RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS.
4. FIRMA ELECTRÓNICA REMOTA.
5. SELLO ELECTRÓNICO.
6. AUTENTICACIÓN DE SITIOS WEB.
7. TERCEROS DE CONFIANZA.

C. CARACTERISTICAS Y CLASES DE FIRMA ELECTRÓNICA

D. CERTIFICADO ELECTRÓNICO.

E. PRESTADORES DE SERVICIOS DE CONFIANZA.

F. FIRMA BIOMETRICA.

G. IDENTIDAD Y FIRMA DE CIUDADANO EN EL SECTOR PÚBLICO.

1. SISTEMAS ADMITIDOS POR LA ADMINISTRACIÓN GENERAL DEL ESTADO Y SU IMPOSICIÓN AL RESTO DE ADMINISTRACIONES.
2. NIVELES DE SEGURIDAD DE LA FIRMA ELECTRÓNICA. RELACIÓN ENTRE FIRMA Y ESQUEMA NACIONAL DE SEGURIDAD.
3. USOS OBLIGATORIOS DE LA FIRMA.
4. TIPOS DE FIRMA ELECTRÓNICA.
   - » PIM.
   - » Clave/Contraseña.
   - » Firma digitalizada.
   - » Firma digital.
5. FIRMA E IDENTIFICACIÓN EN LA NUBE; SISTEMA CL@VE.
   - » Ámbito de aplicación.
   - » Registro de usuarios.
   - » Modalidades de identificación.
   - » Firma de documentos electrónicos.
   - » Punto de acceso al sistema CL@ve.
   - » Adhesión al sistema CL@ve.
   - » Costes de CL@ve.
   - » Nivel de seguridad requerido.

H. IDENTIDAD Y FIRMA DE LA PROPIA ADMINISTRACIÓN.

- » Sello electrónico.
- » Código seguro de verificación.

I. FIRMA DE PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PUBLICAS.

J. POLÍTICA DE FIRMA

TOMO II

Servicios de Certificación para las AALL

CIUDADANÍA Y EMPRESAS

1 Introducción

La revolución de la tecnología de información, conjuntamente con el desarrollo de la infraestructura de comunicaciones, está haciendo cambiar significativamente las relaciones entre personas y organizaciones, tanto en España como en todo el mundo. Estas nuevas formas de comunicación abren un gran abanico de posibilidades tanto para las personas, como para empresas.

El tomo II de la Enciclopedia, se desarrolla para complementar el Tomo I y ver todos los conceptos relacionados con la identificación e identidad en la administración electrónica desde la perspectiva de la ciudadanía, empresas y emprendedores/as que son realmente los que completan el ciclo de la administración electrónica con el acceso y gestión de la información y los documentos, haciendo uso de los servicios.

2 A quién va dirigido

A las personas y empresas que deseen relacionarse con la administración pública por medios electrónicos, con mayor o menor conocimiento tecnológico y que tras la lectura de este tomo les permita:

a. Servir de lectura inicial para tener nociones claras del lenguaje empleado, comprendiendo sus términos y significados de la materia, dotando al lector de los conocimientos adecuados que le permitan profundizar en otros textos de mayor especialización
b. Conocer y saber identificar herramientas que se emplean y están a disposición
c. Desenvolverse con soltura en las relaciones electrónicas con las administraciones públicas
d. Generar confianza en el empleo de los medios tecnológicos en su relación cotidiana con las administraciones.

3 ¿Qué son los certificados electrónicos?

Si bien en el tomo I de la Enciclopedia se ha explicado que son los certificados electrónicos y tipología existente habiéndose tratado con profundidad en los aspectos jurídicos y tecnológicos, si su lectura comenzó por este tomo, le facilitamos un breve resumen; remitiéndole al Tomo I para mayor detalle.

Un certificado electrónico es la certificación electrónica expedida por un prestador de servicios de certificación de forma que se vincula a su suscriptor con unos datos de verificación de Firma confirmando que la persona/empresa es quien dice ser con las garantías necesarias. Digamos que los certificados permiten y conforman la Identidad Digital de una persona o empresa en el terreno digital.

Existen distintos tipos de certificados para múltiples propósitos de forma que las actuaciones digitales se puedan realizar con las mismas garantías jurídicas y técnicas que hasta ahora se realizaban en la operativa diaria hasta la existencia de este mundo "electrónico".

El Certificado digital de Persona Física es la certificación electrónica expedida por un prestador de servicios que vincula a su suscriptor con unos datos de verificación de Firma y confirma su identidad.

Este certificado, también conocido como Certificado de Ciudadano o de Usuario, es un documento digital que contiene sus datos identificativos. Le permitirá identificarse en Internet e intercambiar información con otras personas y organismos con la garantía de que sólo Ud. y su interlocutor pueden acceder a ella.

Por lo general, los PSC disponen de una red de Oficinas de Registro y acreditación que cuentan con los medios informáticos precisos para conectarse telemáticamente. En ellas, la acreditación e identificación de los solicitantes de los certificados se exige la comprobación de su identidad y de su voluntad de que sea expedido un certificado electrónico y, en su caso, de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente, y se verifica de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

Los Certificados de persona física expedidos por los PSC tienen validez durante un periodo máximo años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que el Titular desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.

Son expedidos por los distintos prestadores como Prestador Cualificado de Servicios de Confianza cumpliendo con los criterios legales y distintas normativas técnicas. El tamaño de las claves relativas al certificado raíz de la Autoridad de certificación que emite los certificados electrónicos puede diferir en función del prestador, del mismo modo que las claves relativas a los certificados electrónicos cualificados para identificar a las personas físicas o los algoritmos de cifrado de los certificados emitidos.

3.1. Generación de claves

En el procedimiento de obtención de certificados, cada prestador desarrolla los elementos necesarios para activar, en el puesto del solicitante, el software que genera a través de su navegador web, un par de claves, pública y privada, que le permitirá firmar e identificarse, así como proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado.

Las claves privadas serán utilizadas bajo el control del software de navegación web del que disponga la propia persona, enviando todas las claves públicas al prestador con el fin de integrarlas en un certificado.

Las claves privadas de firma, permanecerán siempre bajo el control exclusivo de su titular, y guardadas en el soporte correspondiente, no guardándose copia de ellas por los prestadores.

Los prestadores garantizarán que la persona, Titular del certificado, puede tener el control exclusivo de las claves privadas correspondientes a las claves públicas que se consignan en el certificado, mediante la obtención de las pruebas de posesión oportunas, a través de la adjudicación del número de identificación único.

3.1.1. Archivo de las claves públicas

Las claves públicas de los usuarios permanecerán archivadas, por si fuera necesario su recuperación, en archivos seguros, tanto física como lógicamente, durante un periodo no menor de 15 años.

3.1.2. Exclusividad de las claves

Las claves privadas son exclusivas para los Titulares de los certificados y son de uso personal e intransferible.

Las claves públicas son exclusivas para los Titulares de los certificados, independientemente del soporte físico donde estén almacenadas y protegidas.

3.1.3. Renovación de claves

Cada prestador identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar distintos certificados para una misma clave. Es por esto que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

3.2. Registro de usuarios

El registro de usuarios es el procedimiento a través del cual se identifica al solicitante de un certificado electrónico, se comprueba su personalidad y se constata su efectiva voluntad de que le sea emitido el "Certificado Básico" o "Título de Usuario" por cada prestador.

Este registro podrá ser realizado por el propio prestador o cualquier otra Administración pública y, en su caso, por las demás personas, entidades o corporaciones habilitadas a tal efecto por las normas que resulten de aplicación. En todo caso el registro se llevará a cabo según lo dispuesto por cada prestador, al objeto de que este registro se realice de acuerdo con lo establecido por la normativa específica aplicable y homogénea en todos los casos. De igual manera será cada prestador, quien defina y aporte los medios necesarios para la realización de este registro.

En el caso de que el registro lo realizara una Administración Pública, distinta del prestador, la persona que se encargue de la actividad de registro ha de ser personal al servicio de la Administración Pública. En estos casos, el prestador dará soporte a la implantación de las distintas oficinas de registro, que se establezcan cuando fuere necesario, en los siguientes términos:

a) Aportación de la aplicación informática de registro

b) Aportación de la documentación relativa a la instalación y manejo de la aplicación, así como toda aquella referente a los procedimientos y normas sobre el registro.

c) Registro y formación de los encargados del registro, lo que supone la expedición de un certificado emitido por el prestador para cada encargado del registro, que permita garantizar la seguridad de las comunicaciones con el prestador, incluyendo la firma electrónica de las solicitudes de registro.

3.2.1. Identificación de los solicitantes de los certificados, comprobación de su personalidad y constatación de su voluntad.

La identificación de los solicitantes de los certificados en las oficinas de registro y la comprobación de su personalidad se hará mediante la exhibición del Documento Nacional de Identidad, Pasaporte u otros medios admitidos en derecho.

En el acto de registro, el personal encargado de las oficinas de acreditación constatará que el solicitante tiene la voluntad de solicitar que le sea emitido un certificado electrónico por el prestador y que éste reúne los requisitos exigidos por el ordenamiento jurídico.

3.2.2. Necesidad de presentarse en persona

El procedimiento de registro requiere presencia física del interesado para formalizar el procedimiento de registro en la oficina de acreditación. No obstante, serán válidas y se dará el curso correspondiente a las solicitudes de emisión de certificados electrónicos cumplimentadas siempre que la firma del interesado haya sido legitimada notarialmente en los términos señalados en el referido modelo.

3.2.3. Incorporación de la dirección de correo electrónico del titular al certificado

No es preceptiva la incorporación de la dirección de correo electrónico del titular al certificado si bien se hará constar en él en el caso en que el titular aporte dicha dirección en el momento del registro.

Esta incorporación se realizará a los efectos de que el certificado pueda soportar el protocolo S/MIME en el caso de que la aplicación utilizada por el usuario así lo requiera.

3.2.4. Obtención del "Certificado Básico" o "Título de usuario"

Para la obtención de este certificado, así como para su revocación o suspensión, el solicitante deberá observar las normas y procedimientos desarrollados a tal fin por el prestador de conformidad con la normativa vigente aplicable.

3.3. Emisión de los certificados

La emisión de certificados supone la generación de documentos electrónicos que acreditan la identidad u otras propiedades del usuario y su correspondencia con la clave pública asociada; del mismo modo, la emisión de los certificados implica su posterior envío al directorio de manera que se pueda hacer uso de él cuando resulte necesario.

Las emisiones de certificados por parte de los prestadores sólo pueden realizarlos ellos mismos, no existiendo ninguna otra entidad u organismo con capacidad de emisión de estos certificados.

El prestador, por medio de su firma electrónica, garantizará los certificados, así como la verificación de la identidad y cualesquiera otras circunstancias personales de sus titulares. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los certificados, el prestador utilizará mecanismos criptográficos para asegurar la autenticidad e integridad de dicho certificado.

4 TIPOS DE CERTIFICADOS

4.1. Para la ciudadanía

La ciudadanía puede utilizar, en sus relaciones con la Administración, certificados de persona física reconocidos o cualificados, es decir, expedidos por Autoridades de Certificación incluidas en la lista de confianza de prestadores de servicios de certificación del Ministerio de Energía, Turismo y Agenda Digital, y que puede consultarse en la Sede Electrónica de este Ministerio: https://sede.minetur.gob.es/Prestadores/Paginas/Inicio.aspx

Los certificados de Persona Física solamente proveen seguridad respecto de la identidad de su titular. Además del nombre y email, incorporan datos que, antes de expedir el certificado, el prestador de servicios de certificación debe verificar, como por ejemplo, el número del Documento Nacional de Identidad. La mayoría de la ciudadanía utiliza certificados de este tipo para relacionarse electrónicamente con la Administración. El ejemplo más típico es el DNIe y el certificado de persona física de la FNMT.

4.1.1. ¿Cómo lo hago?

En el caso del DNIe, cuando se produce la renovación del Documento Nacional de Identidad, se ofrece la posibilidad de activar los certificados que incluye en su interior. También pueden activarse y renovarse en los cajeros automáticos colocados en las Comisarías. Poseen lectores de huella dactilar, para las personas que no conocen o han olvidado su PIN.

Para obtener certificados de otras Autoridades de Certificación, debemos hacer una solicitud electrónica a través de la página web del Prestador de Servicios de Certificación, personarnos en una Oficina de Registro del Prestador con la documentación acreditativa de nuestra identidad, y descargar el certificado electrónico en nuestro equipo o almacenarlo en un dispositivo criptográfico.

En algunos casos, por ejemplo, en el proceso de renovación de un certificado, se permite no realizar el trámite presencial, si se utiliza en la solicitud telemática un certificado electrónico reconocido para acreditar la identidad de la persona que solicita. Es decir, el certificado próximo a caducar, me sirve para obtener el nuevo, sin hacer acto de presencia en las oficinas.

4.1.2. ¿Para qué lo necesito?

El DNIe incorpora 2 certificados en el chip con funciones separadas. Uno sirve para la autenticación de su titular en procesos electrónicos, como por ejemplo, al acceder a su Carpeta Ciudadana, y otro para utilizar en procesos de firma electrónica de trámites y documentos. Este certificado, al generarse directamente en un dispositivo seguro de creación de firma (el chip del DNIe) permite legalmente sustituir a la firma manuscrita.

Los certificados de otros Prestadores de Servicios de Certificación no tienen esta separación, pudiendo utilizar el mismo certificado, tanto para autenticar a la persona como para firmar electrónicamente. En cualquier caso, el titular del certificado actúa en nombre propio, sin que en los datos del certificado se acrediten posibles poderes de representación, ni pertenencia a Entidad alguna, por lo que, en caso de firmar documentos ejerciendo dichas funciones, deberán acreditarse mediante otros documentos.

Estos certificados permiten a un ciudadano acceder a Carpetas Ciudadanas, firmar envíos de documentos al Registro Telemático, acceder de forma fehaciente a un buzón de notificaciones, etc.

4.1.3. Responsabilidades

Es responsabilidad de cada persona la custodia y el correcto uso de los certificados personales emitidos a su nombre. Para ello, es conveniente que cada titular de un certificado lo proteja del uso no autorizado con un PIN que solo conozca el titular. Además, es recomendable que lo almacene en un dispositivo criptográfico que tenga permanentemente bajo su control. El DNIe cumple todas estas medidas, pero puede utilizarse cualquier otro Certificado de persona Física para la misma finalidad.

4.2. Para las empresas

Además de los certificados personales que puedan utilizar los empleados o dueños de las empresas, éstas pueden utilizar, en sus relaciones con la Administración, certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por Prestadores de Servicios de Confianza de los siguientes tipos:

4.2.1. Tipos de certificados

a. Certificados de Representante de Persona jurídica

   Este certificado sustituye al de Persona Jurídica, tradicionalmente utilizado por las empresas para el ámbito tributario y que, posteriormente, se extendió para otros usos. Desde el 1 de Julio de 2016 ya no se expiden certificados de Persona Jurídica para su uso en trámites de la AEAT.

   La diferencia radica en el titular del certificado. En los de Persona Jurídica, el titular del certificado era la empresa, e incorporaba internamente datos de su representante. En el certificado de Representante, el titular es la persona física con poderes de representación, y se incorporan, como datos adicionales, los de la Persona Jurídica a quien representa.

   Pueden solicitar este tipo de certificado las sociedades que tengan como administrador único a otra sociedad, y aquellas cuyo NIF tenga como letra inicial, la siguiente:

- A y B: Las sociedades anónimas y limitadas, si la representación de la sociedad es mancomunada, por apoderamiento, por sociedad unipersonal, presidencial, por un miembro del consejo, por un miembro del consejo de manera delegada solidaria, persona administradora conjunta, persona liquidadora, etc...
- C: Sociedades colectivas.
- D: Sociedades comanditarias.
- F: Sociedades cooperativas.
- G: Asociaciones L.O. 1/2002, fundaciones, partido político, sindicato, asociación de personas consumidoras y usuarias, organización empresarial, federación deportiva, otras asociaciones distintas de las anteriores con personalidad jurídica. Otras asociaciones.
- J: Sociedades civiles.
- N: Entidades extranjeras con personalidad jurídica, sociedades anónimas europeas, sociedades cooperativas europeas, corporación, asociación o ente con personalidad jurídica con presencia en España, embajadas, consulados u oficina comercial de país extranjero. en España, etc.

- Q: Organismos públicos.
- R: Congregaciones e instituciones religiosas.
- S: Gobiernos de las CC.AA.
- P: Ayuntamientos o diputaciones.
- V: Sociedad agraria en transformación, agrupación de interés económico, agrupación europea de interés económico, etc.

b. Certificados de Representante para Administradores únicos y solidarios

Los certificados de Representante para administradores únicos o solidarios se emiten, para la relación de las Personas Jurídicas a través de sus Representantes legales en sus relaciones con las administraciones públicas o en la contratación de bienes o servicios propios o concernientes a su giro o tráfico ordinario.

Este certificado puede ser obtenido por las sociedades anónimas (Letra de NIF A) y limitadas (Letra de NIF B) si el representante de la sociedad es administrador único o solidario inscrito correctamente en el Registro Mercantil.

c. Certificados de Entidad sin personalidad jurídica

Este certificado se expide a las personas físicas como representantes de las entidades sin personalidad Jurídicas para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas.

Según la letra inicial del NIF de su entidad, pueden solicitar este tipo de certificado:

- E: Las comunidades de bienes, herencias yacentes, titularidad compartida de explotaciones agrarias.
- H: Comunidades de personas propietarias.
- N: Corporación o ente independiente pero sin personalidad jurídica con presencia en España, conjunto unitario de bienes perteneciente a 2 o más personas en común sin personalidad jurídica con presencia en España, y otras entidades sin personalidad jurídica distintas de las reflejadas en el apartado de representante de persona jurídica.
- P: Juntas vecinales, departamento u órgano dependiente de la Administración sin personalidad jurídica.
- S: Órganos de la administración central y autonómica, excepto los Gobiernos de las CC.AA.
- U: Unión temporal de empresas.
- V: Otros tipos sin personalidad jurídica como son: fondos de inversiones, de capital-riesgo, de pensiones, de regulación de mercado hipotecario, u otras entidades sin personalidad jurídica.
- W: Entidades no residentes con establecimiento permanente en España.

d. Certificados de Sello electrónico

   Al igual que las Administraciones Públicas, las empresas pueden realizar firmas automatizadas con Sellos electrónicos. Un ejemplo sería el proceso de emisión de facturas electrónicas.

e. Certificados SSL con validación de dominio

   La Autoridad de Certificación comprueba el derecho del solicitante a usar un nombre de dominio específico. No se inspecciona la identidad de la empresa y únicamente se muestra la información encriptada al hacer clic sobre el Sello de Página Segura. Sirve para establecer una comunicación segura mediante el protocolo Secure Sockets Layer entre las páginas de ese servidor y equipo cliente. Típicamente se utiliza para que los datos de una página web, que pueden ser confidenciales, viajen encriptados a través de https, y se evite el robo de esos datos por parte de terceros. Los sitios web que tienen páginas que solicitan contraseñas, datos bancarios, o muestran información personal utilizan este tipo de certificados.

f. Certificados SSL con validación de organización o empresa.

   Son similares a los anteriores, pero en éstos, la Autoridad de Certificación comprueba el derecho del solicitante a usar un nombre de dominio específico y somete a la organización a una inspección. La información corporativa inspeccionada se muestra al cliente final con un simple clic de ratón sobre el Sello de Página Segura. Este método aumenta la visibilidad de la empresa responsable del sitio web y mejora la fiabilidad.

4.2.2. ¿Para qué lo necesito?

El Artículo 14 de la Ley 39/2015, en su apartado 2 regula la obligación de las empresas a relacionarse con la Administración por medios electrónicos, de la siguiente forma:

2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

a) Las personas jurídicas.

b) Las entidades sin personalidad jurídica.

c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.

d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.

Es decir, que las empresas y/o sus representantes legales, así como los colectivos profesionales que deben estar colegiados para el ejercicio de su actividad, están obligados a relacionarse por medios electrónicos con las Administraciones Públicas con las que trabajen. Por lo tanto, utilizarán certificados digitales en aquellos trámites en los que deban firmar documentos, y en aquellos trámites en los que deban acreditar su identidad como empresa, o como representante de la misma con poder suficiente.

Es obligatorio el uso de la firma electrónica para

a) Formular solicitudes.

b) Presentar declaraciones responsables o comunicaciones.

c) Interponer recursos.

d) Desistir de acciones.

e) Renunciar a derechos.

Como regla general se deberán utilizar certificados electrónicos reconocidos o cualificados para firmar electrónicamente en todas las actuaciones descritas, aunque es posible que se puedan utilizar, en aquellos casos concretos que las Administraciones Públicas consideren válido, otros sistemas de firma.

Otros ejemplos en los que es necesario un certificado digital para firmar electrónicamente:

- Envío de facturas electrónicas a FACe en formato Facturae
- Firma de contratos para la prestación de servicios

Por otro lado, será preciso el uso de certificados digitales para acreditar la identidad al realizar trámites telemáticos, como por ejemplo:

- Consultar el estado de tramitación de los expedientes
- Recibir notificaciones electrónicas
- Realizar consultas de información en las diferentes Carpetas Ciudadanas de las diferentes Administraciones Públicas

4.2.3. Responsabilidades

En general, las mismas que las personas físicas en cuanto a la custodia y vigilancia del certificado para impedir un uso indebido del mismo. Para ello, es conveniente que cada titular de un certificado lo proteja del uso no autorizado con un PIN que solo conozca el titular.

En el caso de certificados software que se instalan en la cryptoapi de Windows, es recomendable que en el proceso de instalación del certificado se especifique el PIN que deberá incluirse cada vez que se vaya a utilizar el certificado. De esta forma, otras personas no podrán firmar con ese certificado conociendo únicamente el usuario y contraseña de acceso al equipo.

En caso de pérdida del dispositivo criptográfico donde se encuentre almacenado, o ante la sospecha de que está teniendo un uso fraudulento por parte de terceros, es preciso comunicarlo a la Autoridad de Certificación para que revoque el certificado lo antes posible.

4.3. Prestadores de Servicios de Confianza

En el tomo I de la Enciclopedia se ha explicado que son los certificados electrónicos y tipología existente habiéndose tratado con detalle los aspectos jurídicos y tecnológicos, en el tomo II se ha facilitado los aspectos más generales, y a continuación se facilita una muestra representativa de Prestadores de Servicios de Confianza que han accedido a colaborar en esta enciclopedia en materia de identidad digital tanto para la Ciudadanía como para Empresas y Administración Pública. mostrando información, características y funcionalidades que ofrecen en sus servicios:

- ✓ AGÈNCIA CATALANA DE CERTIFICACIÓ (CATCERT)
- ✓ AUTORITAT DE CERTIFICACIÓ DE LA COMUNITAT VALENCIANA (ACCV)
- ✓ CAMERFIRMA
- ✓ FÁBRICA NACIONAL DE MONEDA Y TIMBRE (FNMT-CERES)
- ✓ FIRMA PROFESIONAL
- ✓ IVNOSYS
- ✓ UANATACA

4.3.1. AGÈNCIA CATALANA DE CERTIFICACIÓ (CATCERT)

AUTORIDAD CERTIFICADORA: CONSORCI ADMINISTRACIÓ OBERTA DE CATALUNYA (CATCERT)

Consorci Administració Oberta de Catalunya

1. Información General

Consorci Administració Oberta de Catalunya.

Creada en 2002.

Proveedor Cualificado de Servicios de Confianza eIDAS.

Sedes en Barcelona.

2. Modelo de Prestación de Servicios

Proveedor de Servicios de Certificación y de Confianza Electrónica (QTSP), autorizados por el regulador español (Ministerio de Energía, Turismo y Agenda Digital) de acuerdo al Reglamento Europeo eIDAS. El Consorci Administració Oberta de Catalunya, en adelante Consorci AOC, presta esta este tipo de servicios al conjunto de las Administraciones Públicas Catalanas.

La emisión de certificados y sellos cualificados, así como los certificados cualificados de sitios web, requieren de una identificación personal que el Consorci AOC lleva a cabo a través de su red de entidades de registro.

3. Características del Modelo

El modelo de prestación de servicios de certificación del Consorci AOC se basa en una jerarquía que consiste en un certificado raíz (EC-ACC) y dos raíces intermedias (EC-SectorPublic y EC-Ciutadania) que se usan para emitir los siguientes tipos de certificados:

- EC-ACC: Se usa para emitir certificados de infraestructura.
- EC-SectorPúblic: Emite certificados utilizados en el ámbito de las Administraciones Públicas Catalanas (trabajador público, sellos electrónicos, certificados de sede electrónica, etc.)
- EC-Ciutadania: Emite certificados de persona física para ciudadanos (certificados idCAT).

Las administraciones públicas que lo solicitan pueden establecerse como entidades de registro tanto de EC-SectorPúblic como de EC-Ciutadania.

El Servicio se caracteriza por un SLA definido y un tarifado en función de la tipología de certificado y su soporte.

4. Solución Tecnológica

En la actualidad la gestión del servició está externalizada, siendo la empresa adjudicataria FirmaProfesional.

Solución basada en software de Autoridad de Registro propio, con interfaz gráfico web.

5. Tipos de Certificados

Todos los certificados que se listan a continuación están cualificados de acuerdo con el Reglamento eIdAS.

Personas físicas:

- Certificado cualificado de identificación y firma electrónica avanzada idCAT (ES00 / UE00)

Administración Pública:

- Certificados TCAT de trabajador público en tarjeta. (ES05 / UE00)
- Certificados TCAT-P de trabajador público de firma avanzada (ES05 / UE00)
- Certificados de trabajador público con pseudónimo (ES07 / UE00)
- Sellos electrónicos (ES08 / UE01)
- Certificados de Sede Electrónica (ES09 / UE02)
- Certificados de Representante (ES11-ES12 /UE00)

Técnicos:

- SSL cualificado eIDAS (ES09 / UE02)
- Certificados de Dispositivo Aplicación (CDA) (ES08 / UE01)

6. Servicios/Productos para AALL

El Consorci AOC ofrece los siguientes servicios:

- Servicio de Entidad de Registro (RA):
  - » Servicio de Entidad de registro IdCAT (EC-Ciutadania), que permite a las entidades la emisión de certificados cualificados de firma avanzada para ciudadano.
  - » Servicio de Entidad de registro TCAT (EC-SectorPublic), que permite la emisión de certificados en el ámbito de la Administración Pública.

  Por su parte, el Consorci AOC actúa también como entidad de registro para aquellas administraciones que, por cuestiones volumétricas, no sea factible establecer una entidad de registro propia.
- Servicio de Custodia y Firma:
  - » Servicio de custodia de expedientes electrónicos (iArxiu)
  - » Servicio de custodia de sellos electrónicos de nivel medio (Signador Centralitzat).
  - » Servicio de Portafirmas.
  - » Plataforma de validación de certificados y documentos electrónicos (Validador)
- Servicio de Identidad Digital Móvil:
  - » Servicio VALid de integración de mecanismos de identificación y firma electrónica.
  - » Servicio idCAT Mòbil de identificación de ciudadanos basado en el envio de claves de un solo uso al móvil.
- Certificados Digitales:
  - » Sede Electrónica
  - » Sello de Órgano
  - » Representante Legal de la Administración
  - » Empleado Público
  - » Certificados cualificados de firma avanzada para ciudadanos
  - » SSL cualificado eIDAS
  - » Certificados de Dispositivo Aplicación (CDA)

7. Garantías y Servicios de Soporte

Servicio de soporte de incidencias:

- Portal de soporte:

https://www.aoc.cat/portal-suport/t-cat/idservei/tcat

- Formas de trasladar al equipo de soporte del Consorci AOC:
  - » Por teléfono: 900 90 50 90 o bien 93 272 25 01
  - » Por E-Mail: suport@aoc.cat

» Por formulario Web:

https://www.aoc.cat/portal-suport/necessiteu-mes-ajuda-t-cat/idservei/tcat

- Horario de atención: de lunes a viernes de 8.00 a 19.00 horas, excepto festivos.

  Todas las incidencias se gestionan por un sistema de ticketing y existe un SLA establecido con los clientes.

8. Interoperabilidad con otras Instituciones/Organismos

Soluciones basadas en estándares que facilitan la interoperabilidad.

Prestador de Servicios de Confianza cualificado, presente en la Lista de Servicios de Confianza española, y las grandes plataformas validadoras como @firma, PSIS, o la G.I.S.S.

9. Clientes de Referencia

Son usuarias de los servicios del Consorci AOC todas las administraciones públicas de Catalunya. En particular:

- Generalitat de Catalunya
- Ayuntamientos
- Diputaciones y Consejos Comarcales
- Universidades Públicas

10. Acreditaciones / Certificaciones

Servicios cualificados:

- emisión de certificados de firma
- emisión de certificados de sello
- emisión de certificados de autenticación de sitio web

HSM y software de CA CC EAL 4+

11. Prácticas y Políticas de Certificación

La documentación jurídica del servicio de certificación del Consorci AOC está disponible en https://www.aoc.cat/regulacio. En concreto:

- Política general de Certificación
- Declaración de Prácticas de Certificación de:
  - » EC-ACC
  - » EC-SectorPublic
  - » EC-Ciutadania
- Perfiles de certificados
- Textos de divulgación

4.3.2. AUTORITAT DE CERTIFICACIÓ DE LA COMUNITAT VALENCIANA (ACCV)

AUTORIDAD CERTIFICADORA: AGENCIA DE TECNOLOGÍA Y CERTIFICACIÓN ELECTRÓNICA - ACCV

1. **Información General**

   La Agencia de Tecnología y Certificación Electrónica es un Prestador de Servicios de Confianza cuya andadura se inicia en el año 2000, ante la necesidad de proporcionar herramientas de identificación telemática y de firma electrónica a los participantes en diferentes proyectos de desarrollo de la Sociedad de la Información.

   En 2007 se constituye como entidad pública dependiente de la Generalitat Valenciana y, más tarde en 2014, se integra en el Instituto Valenciano de Finanzas.

   Contacto:

   www.accv.es

   gestioncerts@accv.es

   Tel. 961 971 720 / 902 482 481

2. **Modelo de Prestación de Servicios**

   La Agencia de Tecnología y Certificación Electrónica presta servicios de confianza sin limitación territorial y sin restricciones a entidades privadas o públicas. No obstante, dado de la mayor parte de las entidades usuarias de sus servicios tienen carácter público (ayuntamientos, diputaciones, mancomunidades, etc.) hay una alta especialización en la prestación de servicios a este tipo de entidades y a empleados públicos.

3. **Características del Modelo**

   La principal característica del modelo de prestación de servicios es el intento de simplificar los procesos de emisión de certificados y de la posterior gestión del ciclo de vida de éstos.

   Con esta premisa, se ha logrado disponer de procesos de identificación y emisión de certificados que requieren un número mínimo de personaciones de los usuarios en los Puntos de Registro de Usuario y que tratan de aprovechar identificaciones seguras ya realizadas para evitar nuevos desplazamientos, siempre dentro de los márgenes establecidos por la legislación aplicable.

   Otra característica reseñable es el esfuerzo que se realiza para la creación de Puntos de Registro de Usuario en los que identificar a los usuarios y en los que emitir los certificados. Para fomentar la creación de los Puntos de Registro de Usuario se proporciona un servicio de asistencia/soporte y se ofrece la instalación de manera gratuita cuando existe el compromiso de ofrecer los servicios a la ciudadanía por parte de la entidad en la que se crea el Punto de Registro de Usuario.

4. Solución Tecnológica

Las soluciones tecnológicas utilizadas han sido seleccionadas bajo la premisa de la utilización de desarrollos de código abierto y con la condicionante de disponer de altos niveles de seguridad certificados bajo esquemas de acreditación comúnmente aceptados.

En caso de no existir soluciones para la prestación de determinados servicios, se llevan a cabo desarrollos propios.

5. Tipos de Certificados

Los certificados emitidos tratan de cubrir todas las posibilidades y necesidades de los usuarios. En concreto se emiten los siguientes tipos de certificados, que clasificamos en personales y no personales:

Personales:

- Certificado de persona física en soporte software (ES00 / UE00)
- Certificado de persona física en tarjeta criptográfica (ES00 / UE00)
- Certificado de empleado público en soporte software (ES05 / UE00)
- Certificado de empleado público en tarjeta criptográfica (ES05 / UE00)
- Certificado de empleado público con seudónimo en tarjeta criptográfica (ES07 / UE00)
- Certificado de pertenencia a empresa en tarjeta criptográfica (ES11-ES12 /UE00)
- Certificado de representante de entidad en soporte software (ES11-ES12 /UE00)
- Certificado de representante de entidad en tarjeta criptográfica (ES11-ES12 /UE00)

No personales:

- Certificado de Sede Electrónica (ES09 / UE02)
- Certificado de Sello de Órgano (ES08 / UE01)
- Certificado de Sello de Entidad (ES08 / UE01)
- Certificado de servidor web SSL (ES09 / UE02)
- Certificado de servidor de VPN (ES09 / UE02)
- Certificado de firma de código (ES08 / UE01)
- Certificado de Aplicación (ES08 / UE01)

6. Servicios/Productos para AALL

Los servicios principales que presta la ACCV son los siguientes:

1. Emisión y gestión de certificados digitales, tanto personales como no personales.
2. Validación de certificados propios y de otros Prestadores de Servicios de Certificación españoles (todos los que emiten certificados reconocidos y están integrados en @firma).
3. Autoridad de Sellado de Tiempo.

4. Servicio de Custodia documental.
5. Acceso a Plataforma de Intermediación de Datos de la Administración General del Estado
6. Servicio de Certificación de Publicaciones en web
7. Registro de Representantes, para flexibilizar el registro y consulta de representaciones entre personas físicas y jurídicas, o entre profesionales colegiados y sus representados. Se incluye la figura de "Funcionario Habilitado". Desde abril de 2011 está en producción.
8. Servicio de compleción de firmas electrónicas para obtener formatos de firma avanzada, para poder realizar archivo de documentación electrónica y recuperación a lo largo del tiempo.
9. Emisión y gestión de certificados de firma centralizada.

Puede encontrarse información detallada y actualizada de esos servicios y de otros que se vayan añadiendo en nuestra página web https://www.accv.es

7. Garantías y Servicios de Soporte

La Agencia de Tecnología y Certificación Electrónica dispone de un servicio de soporte de varios niveles, pudiendo acceder a dicho servicio por:

- Teléfono (24x7)

- Correo electrónico

- Formulario web

Puede encontrar información detallada y actualizada al respecto en https://www.accv.es/contacto

8. Servicios de Valor Añadido

Adicionalmente a los servicios de confianza, la Agencia de Tecnología y Certificación Electrónica presta los siguientes servicios de valor añadido:

a. Servicios de análisis de seguridad de las entidades que alberguen PRUs para garantizar la seguridad de los sistemas y el entorno.
b. Servicios de generación y verificación de Códigos Seguros de Verificación (CSV)
c. Provisión de dispositivos relacionados con la certificación digital y la firma electrónica.
d. Servicio de información técnica, de procedimientos, de normativa, noticias, eventos, servicios, etc.
e. Provisión de librerías criptográficas para el desarrollo de aplicaciones –Arangí–.
f. Servicios del nodo federado ACCV de @firma.
g. Servicios de formación a agentes de call center.

Puede encontrarse información detallada y actualizada de esos servicios y de otros que se vayan añadiendo en nuestra página web https://www.accv.es

9. Interoperabilidad con otras Instituciones/Organismos

La Agencia de Tecnología y Certificación Electrónica es un Prestador de Servicios de Confianza cualificado y como tal se encuentra incluido en los sistemas de validación proporcionados por las distintas AAPP a nivel europeo.

Más concretamente, a nivel nacional, los distintos perfiles de certificados se encuentran incluidos en la plataforma @firma, servicio que se ha constituido en método de facto para validar y completar certificados y firmas para las AAPP, permitiendo interoperar con la totalidad de las instituciones/organismos conectados a este servicio (AGE, CCAA, y AALL).

Destacar que la Agencia de Tecnología y Certificación Electrónica es nodo federado de @firma para la Comunidad Valenciana, permitiendo llevar la interoperabilidad entre organismos un paso más allá siendo actor activo en el proceso.

10. Clientes de Referencia

La Agencia de Tecnología Y Certificación Electrónica presta servicios a AAPP y empresas principalmente en todo el territorio nacional, entre sus usuarios de AAPP se encuentran CCAA, Diputaciones, Ayuntamientos, Universidades. Por citar algunas de ellas:

- Generalitat Valenciana	- Ayuntamiento de Burgos
- Universidad de Murcia	- Ayuntamiento de Fuenlabrada
- Universitat Politècnica de València	- Ayuntamiento de Murcia
- Universitat de Valencià	- Ayuntamiento de Cartagena
- Universidad Miguel Hernández	- Ayuntamiento de Benidorm
- Universitat Jaume I	- Ayuntamiento de Castellón
- Universidad Católica San Antonio de Murcia	- Ayuntamiento de Altea
- Universidad Politécnica de Cartagena	- Ayuntamiento de Torrent
- Diputación de León	- Ayuntamiento de Sagunt
- Diputación de Valladolid	- Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT) del Ministerio de Economía y Competitividad
- Diputación de Palencia	- Instituto de Salud Carlos III de Madrid (ISCIII)
- Diputación de Alicante	- Federación de Empresarios del Metal de la Prov de Alicante -FEMPA-
- Ayuntamiento de Valencia	- Agencia Española de Meteorología (AEMET)
- Ayuntamiento de Alicante	

Además de los que por tamaño se han citado, entre nuestros clientes se encuentran alrededor de 600 AALL distribuidas por todo el territorio nacional.

11. Acreditaciones / Certificaciones

Además de las auditorías preceptivas de cumplimiento de la legislación de protección de los, la ACCV supera anualmente tres importantes auditorías

ISO 27001 del Sistema de Gestión de la Seguridad de la Información

- Webtrust para CA
- Auditoría de cumplimiento del Reglamento 910/2014 (eIDAS)

WebTrust para Autoridades de Certificación es un sello de confianza, calidad y seguridad que se concede a las entidades prestadoras de servicios de confianza tras obtener un informe favorable de auditoría independiente, el cual constata el cumplimiento de los Principios y Criterios Webtrust definidos por el Instituto Americano de Auditores Públicos de Cuentas (AICPA) y el Instituto Canadiense de Auditores de Cuentas (CICA).

WebTrust para Autoridades de Certificación - SSL Baseline Requirements es un sello complementario que se entrega a aquellos prestadores de servicios de confianza que superan una auditoría independiente de cumplimiento con las directrices que marca el CA/Browser Forum respecto al ciclo de vida de los certificados de SSL, obteniendo un informe favorable.

Ambos sellos están mundialmente reconocidos y aceptados por la comunidad internacional (Microsoft Inc., Mozilla Foundation, Google, etc.), convirtiéndose en el método más efectivo de transmitir confianza para los usuarios de Internet.

La ACCV obtuvo y mantiene el Sello Webtrust para CA en 2006 y lo mantiene desde entonces, tras auditorías anuales.

Por otra parte, la norma ISO 27001 proporciona los objetivos y controles que se deben incluir en el Sistema de Gestión de Seguridad de la Información para medir y validar el éxito de una organización a la hora de implementar y cumplir las buenas prácticas de seguridad. Por tanto, esta certificación garantiza una revisión continua de los riesgos y controles estipulados y con ellos la seguridad de la información y de los servicios prestados.

Con este tipo de certificación, las entidades y compañías ratifican ante sus clientes y accionistas la integridad y seguridad de sus operaciones.

Asimismo, el certificado ISO 27001 es un sello mundialmente reconocido que garantiza a los usuarios de los servicios de la Agencia de Tecnología y Certificación Electrónica la conformidad de sus modelos y prácticas de gestión en materia de seguridad en los servicios TIC.

La Agencia de Tecnología y Certificación Electrónica fue la primera entidad de la Generalitat de La Comunitat Valenciana en obtener y mantener esta certificación desde hace 6 años que refleja su compromiso con la seguridad en sus procesos y con la mejora continua, a fin de mantener la confianza de los usuarios de sus certificados y resto de servicios.

Además, tras la entrada en vigor del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, la ACCV ostenta la acreditación para utilizar la etiqueta confianza "UE" para servicios de confianza cualificados.

Al menos cada dos años, la ACCV debe someterse a una auditoría de cumplimiento del Reglamento 910/2014 para poder mantener su condición de prestador de servicios de confianza cualificado y poder mantener así la más alta garantía de calidad y seguridad entre las entidades europeas. Actualmente se está realizando esta auditoría.

Finalmente, es necesario llevar a cabo una auditoría de cumplimiento del Esquema Nacional de Seguridad, tras la entrada en vigor del Real Decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del Esquema.

Esta auditoría de cumplimiento del ENS deberá realizarse, al menos, cada dos años.

12. Prácticas y Políticas de Certificación

Las prácticas y políticas de certificación asociadas a cada uno de los perfiles de certificados mencionados pueden encontrarse actualizadas en el enlace:

https://www.accv.es/quienes-somos/practicas-y-politicas-de-certificacion/

4.3.3. CAMERFIRMA

AUTORIDAD CERTIFICADORA: CAMERFIRMA

1. Información General

AC Camerfirma es un Prestador de Servicios de Certificación reconocido para la emisión de certificados digitales basados en el **RD 1671/2009**, los cuales han sido desarrollados en base a los perfiles propuestos por el grupo de Autenticación y Firma del Consejo Superior de Administración Electrónica y el Esquema Nacional de Seguridad.

2. Modelo de Prestación de Servicios

AC Camerfirma dispone de un servicio de atención y coordinación (SAC) propio. La organización del servicio es la siguiente:

- Servicio primer nivel a los titulares de los certificados.
- Servicio segundo nivel a red de RA.
- Responsables del servicio dentro de la Entidad.

El personal del departamento está altamente especializado en consultas sobre el uso y gestión de los certificados ya que mantiene una formación continua y una movilidad mínima.

El servicio para la atención de incidencias de operadores de Autoridad de Registro consta de dos especialistas de segundo nivel y una Coordinación del servicio.

El horario de prestación del servicio de soporte de titulares de certificados es de 8:00 a 20:00 de lunes a viernes.

El horario de prestación del servicio de soporte de atención a Operadores de RA es de 8:00 a 19:00 de lunes a viernes y sábados de 11:00 a 14:00.

La gestión de las incidencias se realizará de las siguientes maneras:

- Por teléfono: La llamada se atenderá a través de los siguientes números de teléfono:
  - » Primer Nivel: 902 361 207
  - » Segundo Nivel: 902 550 332
- Por la aplicación de soporte https://secure.camerfirma.com/incidencias/

Los operadores de registro también dispondrán de un acceso web para realizar sus solicitudes. Las solicitudes vía web son gestionadas por el módulo de incidencias de la plataforma STATUS.

La plataforma STATUS permite la adaptación de las pantallas de soporte por proyecto de forma que tanto los usuarios finales como los operadores de Autoridad de Registro trabajen en un entorno personalizado.

3. Características del Modelo

AC Camerfirma como Autoridad de Certificación reconocida tiene entre sus objetivos satisfacer las demandas especializadas en firma electrónica de **empresas**, **administraciones**, **colectivos**, **colegios profesionales** e **instituciones**.

Camerfirma ha participado y participa, en la implantación de diferentes proyectos dentro del marco de la firma digital en Organismos Públicos con certificado de empleado público, sello electrónico, sede electrónica, de ciudadano, de sellado de tiempo, de firma de código, de servidor seguro, etc.

4. Solución Tecnológica

Tecnología Propia AC Camerfirma: desde el comienzo de su actividad, ha considerado que para implantarse en el mercado es determinante el desarrollo de una tecnología propia.

AC Camerfirma cuenta con **"STATUS",** una plataforma de emisión y gestión de certificados desarrollada internamente siguiendo las especificaciones técnicas del mercado y el estado del arte en materia de la certificación digital. La plataforma incorpora adicionalmente el seguimiento de los procesos operativos y administrativos necesarios para completar el ciclo de vida de un certificado digital. Obviamente todos los certificados emitidos cumplen con las diferentes normativas españolas e Internacionales, así lo avalan las diferentes auditorías realizadas sobre todos los procedimientos: *Webtrust for CA*, *Webtrust for EV*.

Todos los componentes que dan soporte a esta plataforma están duplicados y albergados en un CPD que cumple las exigencias de seguridad impuestas a las labores de gestión de certificados digitales, tal como se puede comprobar en las certificaciones ISO27001 e ISO20000, para acreditar la calidad del sistema, aportadas por **AC Camerfirma**.

AC Camerfirma ha dispuesto un diseño técnico de centros de datos que integra seguridad, escalabilidad y optimización de costes. El esquema se basa en la ubicación externa de los servicios de cliente (certificados, sello de tiempos, OCSP, etc.) y la gestión en un centro propio de los servicios críticos como la gestión de claves raíz y ceremonias de claves criptográficas, a la vez que mantiene en el centro interno, los sistemas de control de nivel de servicio.

5. Tipos de Certificados

AC Camerfirma debido al proceso de adaptación de sus certificados y servicios para el cumplimiento del reglamento **eIDAS**, figura actualmente en la TSL como Prestador Cualificado de Servicios de Confianza y tiene cualificados a fecha 1 de julio de 2017 todos sus certificados de persona física de "natural person" y "legal person" (p.e. certificados cualificados de empleados públicos, ciudadanos, representante de persona jurídica, sello electrónico, etc.) conforme al Reglamento eIDAS. Entre otros, los certificados acreditados son aquellos perfiles de certificados para AAPP que determinó la Administración General del Estado para sustituir a los actuales.

Certificados cualificados de ciudadano (ES00 / UE00)

El certificado digital de ciudadano garantiza la identidad de la persona física titular del certificado.

Característica	Característica ofertada
Formato	Hardware y Software
AC Raíz	Global Chambersign Root
Autoridad de Certificación	RACER
Longitud de clave	Mínimo 2.048 bits
Algoritmo de firma	RSA/SHA2-256 o RSA/SHA2-512
Periodo de Vigencia	4 años
Características técnicas del servicio de validación	CRL, OCSP y HTTP
Compatibilidad de tarjetas criptográficas	FNMT, BIT4ID, Gemalto, Oberthur,....
Reconocimiento de la CA por el MINETAD	SI
Reconocimiento de la CA	Android, Windows mobile, iOS, Safari, Internet Explorer, Firefox, Chrome y Java

Certificados cualificados de representación ante las AAPP (ES11-ES12 /UE00)

El certificado digital de representante para las Administraciones Públicas es un certificado que se emite a favor de una persona física apoderada por una Entidad (CON o SIN personalidad Jurídica) para llevar a cabo trámites ante las Administraciones públicas, tales como presentación de declaraciones de impuestos, solicitudes de subvenciones, etc.

Característica	Característica ofertada
Formato	Hardware, Software y Centralizado
AC Raíz	Chambers of Commerce Root
Autoridad de Certificación	AC Camerfirma AAPP
Longitud de clave	Mínimo 2.048 bits
Algoritmo de firma	RSA/SHA2-256 o RSA/SHA2-512
Periodo de Vigencia	2 años
Características técnicas del servicio de validación	CRL, OCSP y HTTP
Compatibilidad de tarjetas criptográficas	FNMT, BIT4ID, Gemalto, Oberthur,....
Reconocimiento de la CA por el MINETAD	SI
Reconocimiento de la CA	Android, iOS, Safari, Internet Explorer, Firefox, Chrome y Java

Certificados cualificados de empleado público (ES05 / UE00)

El certificado digital de empleado público garantiza la identidad de la persona física titular del certificado, así como su vinculación a una determinada entidad pública en virtud del cargo que ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.

Característica	Característica ofertada
Formato	Hardware, Software y Centralizado
AC Raíz	Chambers of Commerce Root
Autoridad de Certificación	AC Camerfirma AAPP
Longitud de clave	Mínimo 2.048 bits
Algoritmo de firma	RSA/SHA2-256 o RSA/SHA2-512
Periodo de Vigencia	3 años
Características técnicas del servicio de validación	CRL, OCSP y HTTP
Compatibilidad de tarjetas criptográficas	FNMT, BIT4ID, Gemalto, Oberthur,....
Reconocimiento de la CA por el MINETAD	SI
Reconocimiento de la CA	Android, iOS, Safari, Internet Explorer, Firefox, Chrome y Java

Certificados cualificados de empleado público con pseudónimo (ES07 / UE00)

El certificado digital de empleado público garantiza la identidad de la persona física titular del certificado, así como su vinculación a una determinada entidad pública en virtud del cargo que ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.

Característica	Característica ofertada
Formato	Hardware, Software y Centralizado
AC Raíz	Chambers of Commerce Root
Autoridad de Certificación	AC Camerfirma AAPP
Longitud de clave	Mínimo 2.048 bits
Algoritmo de firma	RSA/SHA2-256 o RSA/SHA2-512
Periodo de Vigencia	3 años
Características técnicas del servicio de validación	CRL, OCSP y HTTP
Compatibilidad de tarjetas criptográficas	FNMT, BIT4ID, Gemalto, Oberthur,....
Reconocimiento de la CA por el MINETAD	SI
Reconocimiento de la CA	Android, iOS, Safari, Internet Explorer, Firefox, Chrome y Java

El art. 22.4 del RD 1671/2009 justifica la existencia de estos certificados con pseudónimo y nombra estos perfiles como "(…) certificados que se utilicen en aquellas actuaciones que realizadas por medios electrónicos afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización".

Debemos de tener en cuenta los casos establecidos por la norma, no especifica los cargos que podrán poseerlo, sino las actuaciones en que se podrá utilizar, es decir, no se marca el "quién", sino el "cuándo".

El uso de este certificado está restringido únicamente a su titular, quedando la cesión de este bajo su exclusiva responsabilidad.

6. Servicios/Productos para AALL

AC Camerfirma ofrece a distintas Administraciones, Instituciones y Organismos Públicos, soluciones de certificación digital y sellado de tiempo que permiten dar solución a los distintos requerimientos definidos por el Real Decreto 1671/2009, de 6 de noviembre que desarrolla la Ley 11/2007 de acceso electrónico de la ciudadanía a los Servicios Públicos, y que implican autenticación, firma electrónica, cifrado y evidencias temporales. Los certificados de AC Camerfirma cumplen con el perfil del Consejo Superior de Administración electrónica para la Ley 11/2007 y son válidos por la plataforma @firma.

7. Garantías y Servicios de Soporte

AC Camerfirma dispone de un departamento de atención al cliente para dar soporte a la red de operadores de registro como a los empleados públicos. Todos los niveles de atención están formados por personal propio, lo que permite un servicio de alto valor al contar con una gran experiencia en el uso de los certificados digitales y los procesos de su gestión.

Disponibilidad de los servicios. La actual configuración en alta disponibilidad de los equipos soporte al servicio en el centro principal (Madrid) garantizan su funcionamiento ininterrumpido en caso de incidencia en alguno de sus nodos. AC Camerfirma dispone de un documento de nivel de servicio con garantía de disponibilidad del 99,9%.

La plataforma STATUS gestiona las consultas e incidencias tanto de los clientes como de los operadores de registro. El acceso a la información de la incidencia puede ser seguida por el ciudadano o el operador de registro vía interface web.

AC Camerfirma ofrece su servicio de consulta online del estado de sus certificados (OCSP) en base a los estándares y requisitos de servicio requeridos, firmando las respuestas con un certificado emitido por la CA que emitió el certificado a consultar.

AC Camerfirma garantiza los más altos niveles de seguridad, calidad y disponibilidad de los servicios, tal como atestiguan sus certificaciones ISO27001 / ISO20000 / ISO 14001

8. Servicios de Valor Añadido

- El servicio de **Time Stamping** está basado en la tecnología PKI. Esta tecnología se fundamenta en la existencia de dos claves únicas (pública y privada) y un Certificado Digital, en este caso, emitido por Camerfirma. Camerfirma como autoridad de certificación reconocida internacional-

mente (Chambers of Commerce Root) firma el token de tiempo con las garantías de Cámaras de Comercio, entidad reconocida a nivel mundial. Este es un archivo informático que vincula la información a una fecha y una hora. Esta vinculación se produce a través de un sistema seguro de tiempo sincronizado con la Escala de Tiempo Universal (UTC). Además, Camerfirma cuenta con la sincronización del ROA, Real Observatorio de la Armada en San Fernando, autoridad que regula el tiempo y que Camerfirma cuenta con sus sistemas instalados allí.

- El sistema de **almacenamiento centralizado** de claves (CKC) permitirá la implantación y uso de la firma electrónica en las organizaciones de una forma segura, auditada y transparente.

  Mediante la emisión o importación de los certificados electrónicos en el sistema centralizado no se requerirá ningún tipo de hardware en los puestos de trabajo de los usuarios para firmar electrónicamente cualquier documento, tanto desde las aplicaciones del Prestador como desde cualquier otra aplicación o página web habilitada (incluyendo las de las administraciones públicas).

- Los certificados emitidos por CAMERFIRMA son reconocidos en los navegadores web (internet explorer, chrome, firefox...) y en los applets de Java, siendo un valor diferencial a la hora de adquirir un certificado para la Sede Electrónica o el uso con aplicaciones Java, evitando así el típico aviso de seguridad que se obtiene con otros certificados.

9. Interoperabilidad con otras Instituciones/Organismos

AC Camerfirma ofrece a distintas Administraciones, Instituciones y Organismos Públicos, soluciones de certificación digital y sellado de tiempo que permiten dar solución a los distintos requerimientos definidos por el Real Decreto 1671/2009, de 6 de noviembre que desarrolla la Ley 11/2007 de acceso electrónico de la ciudadanía a los Servicios Públicos, y que implican autenticación, firma electrónica, cifrado y evidencias temporales. Los certificados de AC Camerfirma cumplen con el perfil del Consejo Superior de Administración electrónica para la Ley 11/2007 y son válidos por la plataforma @firma.

10. Clientes de Referencia

Actualmente Camerfirma está llevando la gestión de 7 Comunidades Autónomas con todos sus ayuntamientos (22 Diputaciones y unos 520 Ayuntamientos), aparte de casi todas las Autoridades Portuarias y multitud de empresas dependientes de las Administraciones Públicas.

11. Acreditaciones / Certificaciones

AC Camerfirma SA se encuentra debidamente acreditado como Prestador Cualificado de Servicios de Confianza conforme al Reglamento eIDAS y tiene cualificados la mayoría de sus servicios tal como consta en la TSL publicada por el MINETAD. Respecto de los servicios en trámite de cualificación (TSU, autenticación web, sede electrónica) pasarán a ser parte de la TSL de servicios Cualificados, y los certificados, actualmente clasificados como no cualificados, serán reemplazados por AC Camerfirma a partir del día en que dichos perfiles tengan la consideración de Cualificados, para lo cual se podrán sustituir TODOS aquellos certificados no cualificados y se procederá a su revocación.

Los objetivos de **AC Camerfirma** respecto a la seguridad y la calidad han sido fundamentalmente la obtención de la certificación **UNE-ISO/IEC 27001:2014, UNE-ISO/IEC 20000-1:2011 y UNE-EN ISO 14001:2015** y la realización de Auditorías internas al Sistema de certificación

Camerfirma, y en concreto a las Autoridades de registro, para garantizar el cumplimiento de los procedimientos internos.

AC Camerfirma es una entidad prestadora de servicios de certificación y servicios asociados (sello de tiempo, facturación electrónica, etc.) debidamente homologada por parte del Ministerio de Industria, Turismo y Comercio, Órgano controlador de los prestadores de servicios de certificación conforme la **Ley 59/2003**, de 19 de diciembre, de firma electrónica y hoy en día figura en la TSL del MINETAD como Prestador Cualificado de Servicios de Confianza conforme al Reglamento eIDAS.

AC Camerfirma ha obtenido la Certificación internacional ***Web Trust for CA*** y ***Web Trust for EV*** **y *cumplimiento de los Baseline Requirements de CABFORUM*** específica de los prestadores de servicios de certificación digitales.

Los dispositivos hardware **USB** de los certificados de Camerfirma cumplen los requisitos de **"dispositivo seguro de creación de firma",** conforme los criterios establecidos en la Ley 59/2003, de 19 de diciembre, de firma electrónica, para la realización con todas las garantías de la firma electrónica reconocida. Estos dispositivos están acreditados bajo la norma europea **EN 14169 (EAL 4+)**.

Los dispositivos hardware **USB** de los certificados de Camerfirma soportan SHA256y disponen de controladores para Microsoft Windows, Linux y OS X.

12. Prácticas y Políticas de Certificación

Declaración de Prácticas de Certificación (CPS/DPC):

Es el conjunto de prácticas adoptadas por un prestador de servicios de certificación para la emisión de certificados. Contiene información detallada sobre el sistema de seguridad, soporte, administración y emisión de los certificados… y en general, una descripción de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc. AC Camerfirma publica la última versión disponible, pero dispone de un registro de versiones anteriores que pueden solicitarse a través de la cuenta de correo juridico@camerfirma.com.

La DPC da respuesta a las diferentes Políticas de Certificación descritas en el propio documento. Tal como se indica en el apartado (1.2) en caso de contradicción entre políticas y DPC, prevalecerá siempre lo dispuesto en la DPC.

Puede consultarse de forma íntegra en el siguiente enlace: http://docs.camerfirma.com/publico/DocumentosWeb/politicas/CPS_eidas_v_1_2_2.pdf

4.3.4. FÁBRICA NACIONAL DE MONEDA Y TIMBRE (FNMT-CERES)

AUTORIDAD CERTIFICADORA:

FÁBRICA NACIONAL DE MONEDA Y TIMBRE – REAL CASA DE LA MONEDA

1. Información General

La actividad de FNMT – RCM como Prestador de Servicios de Certificación nace con el objetivo de proveer:

1. Mecanismos de identificación, autenticación y firma electrónica (certificados) a los empleados públicos y entidades de la administración.
2. Servicios de certificación necesarios para garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación.

El alcance de los servicios de certificación y productos de FNMT - RCM está diseñado para abarcar todas aquellas relaciones entre las distintas administraciones (Central, Autonómica y Local) y los ciudadanos, que necesiten ser securizadas en términos de garantías de identidad, confidencialidad e integridad.

Así pues, FNMT – RCM se constituye como tercero de confianza en la prestación de servicios de certificación a ciudadanos, empresas privadas y entidades de la administración. Entre los servicios de certificación que se prestan están los referentes a la gestión de certificados, información sobre el estado de los certificados, sellado de tiempo, etc.

Desde su inicio hasta la fecha actual, la evolución de la actividad de FNMT – RCM y de los servicios de firma electrónica se han caracterizado por:

- La consolidación de FNMT – RCM como Prestador de Servicio de Certificación de referencia en España, con más de 1 millón de validaciones diarias, cerca de 3,5 millones de ciudadanos usando los servicios y más de 5.000 oficinas de registro distribuidas por toda España.
- La evolución de la firma electrónica en España, que ha venido de la mano de la iniciativa pública y legislación sectorial en la materia (Ley 59/2003 de firma electrónica y Ley 11/2007 de acceso electrónico de la ciudadanía a los servicios públicos).

A modo de resumen, FNMT – RCM presta en la actualidad servicios en ámbitos muy diferentes, habiéndose constituido en Autoridad de Certificación en dos contextos bien diferenciados.

- Prestación de servicios de certificación a ciudadanos, empresas y administración que se quieran relacionar con garantías de confidencialidad, integridad y no repudio.
- Prestación de servicios de certificación en el marco de la Ley 39/2015 y Ley 40/2015.

Adicionalmente, FNMT – RCM presta servicios de sellado de tiempo y ofrece servicios de información sobre el estado de certificados emitidos por otras autoridades (por ejemplo, DNIe).

2. Modelo de Prestación de Servicios

Diagrama general de servicios

El marco general en el que son ofrecidos estos servicios puede verse en la siguiente ilustración:

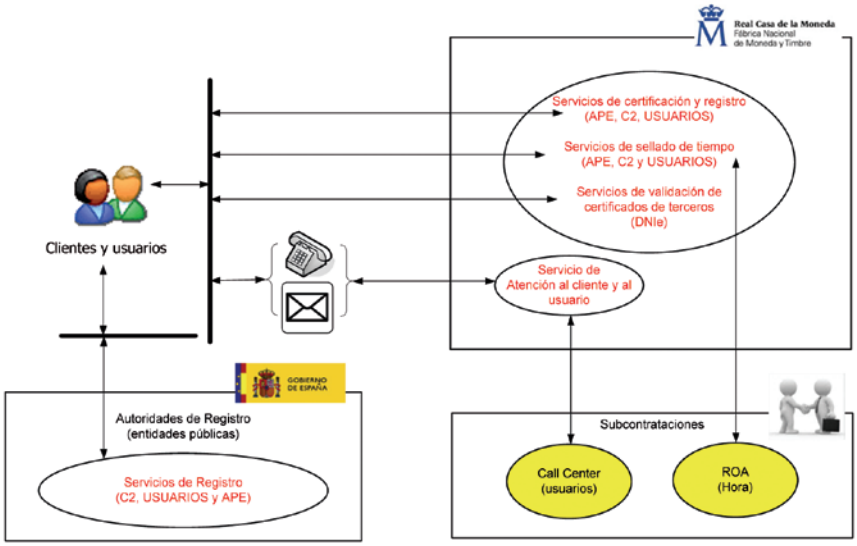


Ilustración 1 – Diagrama de servicios FNMT – RCM – CERES

En líneas generales, los servicios de certificación que la FNMT-RCM presta a clientes y usuarios son desarrollados por la propia FNMT en sus instalaciones. La excepción lo constituyen tres servicios con diferentes niveles de externalización. Éstos son:

- Servicio de Atención a Usuarios o Contact Center
- Servicio de Sincronismo de Tiempo con el Real Observatorio de la Armada
- Servicios de Registro de Usuarios (presencial)

3. Características del Modelo

El modelo de prestación de servicios se sustenta en el cumplimiento de la legislación, la adaptación dinámica y de forma puntual de todas las variables del entorno, políticas de seguridad, cumplimiento normativo y técnico, establecimiento y medición de los controles de seguridad para garantizar un modelo de servicio donde la seguridad se articula como una máxima en la prestación de los servicios FNMT-CERES.

Cumplimiento de las políticas y normas de seguridad: CERES establece la normativa de cumplimiento y desarrollo de las políticas y normas de seguridad corporativas sobre la que se prestan los servicios. Esto precisa el cumplimiento de los procedimientos operativos de seguridad y de la implementación de los correspondientes controles en cada una de las áreas CERES y sus servicios mediante la revisión continua del cumplimiento, analizando desviaciones, proponiendo acciones de mejora y comunicando las actuaciones en un ciclo de mejora continua.

Cumplimiento técnico: CERES chequea periódicamente los sistemas de información para verificar el cumplimiento con los estándares de implantación de seguridad con el uso de herramientas de auditoría técnica de sistemas. El resultado de estas revisiones técnicas se almacena para su posterior consulta y análisis.

Controles de auditoría de los sistemas de información: FNMT-RCM CERES dispone de un plan de auditorías y controles periódicos y planificados de los sistemas de información que prestan sus servicios.

INFRAESTRUCTURA DE SEGURIDAD

Los servicios ofrecidos se sustentan sobre una infraestructura de seguridad dinámica y robusta sustentándose en los pilares de seguridad jurídica, física y lógica.

Seguridad jurídica

El diseño, el funcionamiento, el uso y la gestión de los sistemas de información están sujetos a requisitos legales, reglamentarios y contractuales de seguridad tal y como se recoge en la Declaración de Prácticas de Certificación que puede consultarse en la sede electrónica de la FNMT > Normativa > Declaración de Practicas de Certificación. (https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion)

Cumplimiento de la legislación aplicable

FNMT – RCM cuenta con un marco de actuación para la vigilancia del cumplimiento legal y normativo que le es de aplicación, garantizando así la adecuación de su actividad como Prestador de Servicios de Certificación a la normativa que, a título de ejemplo, se menciona a continuación:

Servicios de certificación y firma electrónica:

- REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 59/2003 de firma electrónica. Texto consolidado de julio 2015.
- Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

- Real Decreto 1317/2001, de 30 de noviembre, por el que se desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, en materia de prestación de servicios de seguridad, por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en las comunicaciones a través de medios electrónicos, informáticos y telemáticos con las Administraciones Públicas.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de la ciudadanía a los Servicios Públicos
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de la ciudadanía a los servicios públicos (sedes electrónicas)
- Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

Protección de datos de carácter personal

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- ORDEN EHA/2357/2008, de 30 de julio, por la que se regulan los ficheros de datos de carácter personal de la Fábrica Nacional de La Moneda y Timbre-Real Casa de la Moneda
- Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Otros

- Real Decreto 1114/1999 de 25 de junio, por el que se adapta la Fábrica Nacional de La Moneda y Timbre a la Ley 6/1997 de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se aprueba su Estatuto y se acuerda su denominación como Fábrica Nacional de La Moneda y Timbre-Real Casa de la Moneda, modificado por el Real Decreto 199/2009 de 23 de Febrero

- Estatutos de la Fábrica Nacional de La Moneda y Timbre de 1999.
- Texto Refundido de la Ley de Contratos del Sector Público de 2011.
- UNE-EN ISO 9001: Sistemas de gestión de la calidad

Derechos de propiedad intelectual

En CERES se encuentran implantados los procedimientos necesarios para el más estricto cumplimiento legal en materia de Ley de Propiedad Intelectual y además existen auditorias periódicas programadas en la que se contempla su cumplimiento. En cualquier caso, toda la información adquirida por la FNMT-RCM está regulada por los contratos de licencia que acompañan a cada una de ellas.

Los casos en los que la FNMT-RCM es el proveedor de información a terceros y siempre que se encuentre protegida por los derechos de propiedad intelectual, se establecen los contratos necesarios para regular su explotación.

La FNMT-RCM es titular en exclusiva de todos los derechos, incluidos los derechos de explotación, sobre el Directorio seguro de Certificados, Listas de Revocación, servicios de información sobre el estado de los Certificados y servicios de Sellado de Tiempo en los términos señalados en el Texto Refundido de la Ley de Propiedad Intelectual aprobado mediante Real Decreto Legislativo 1/1996, de 12 de abril (Ley de Propiedad Intelectual), incluido el derecho sui generis reconocido en el artículo 133 de la citada Ley. En consecuencia, el acceso a los Directorios seguros de Certificados queda permitido a los miembros de la Comunidad Electrónica legitimados para ello, quedando prohibida cualquier reproducción, comunicación pública, distribución, transformación o reordenación salvo cuando esté expresamente autorizada por la FNMT-RCM o por la Ley. Queda asimismo prohibida la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido, ya sea considerada como tal desde una perspectiva cuantitativa o cualitativa, así como su realización de forma repetida o sistemática.

Los OID utilizados tanto en los certificados como para el almacenamiento de ciertos objetos en el Directorio, son propiedad de la FNMT-RCM y han sido registrados en el IANA (Internet Assigned Number Authority) bajo la rama iso.org.dod.internet.private.enterprise (1.3.6.1.4.1 - IANA-Registered Private Enterprises), habiéndose asignado el número 1.3.6.1.4.1.5734 (FABRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA). Esto puede ser consultado y comprobado en: http://www.iana.org/assignments/enterprise-numbers

Protección de los documentos de la organización.

Uno de los activos críticos de la FNMT-RCM son los propios registros y datos que almacena para el cumplimiento legal al que se encuentra sometido. Estos registros se encuentran clasificados en registros contables, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, y para salvaguardar su *Confidencialidad*, *Integridad* y *Disponibilidad*, la Dirección ha aprobado los procedimientos necesarios para su mantenimiento, desde su generación hasta su destrucción.

Protección de datos y privacidad de la información personal.

Otra de las Leyes con las que la FNMT-RCM debe cumplir es la actual Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Desde la Dirección se tiene conciencia de los derechos fundamentales de las personas, entre los que se encuentra el derecho a la intimidad de sus datos personales, por lo que la FNMT-RCM tiene implantados todos los controles exigidos por la ley y el Reglamento de Medidas de Seguridad según Real Decreto 1720/2007.

Prevención del uso indebido de los recursos de procesado de la información.

Desde CERES se impide que los usuarios utilicen los recursos de procesado de la información para fines no autorizados.

Para ello, existen políticas y procedimientos publicados y distribuidos a todos los empleados y usuarios de la información de la FNMT-RCM que regulan el uso de dicha información, y que incluyen las consecuencias y responsabilidad por tratamiento no autorizado.

Regulación de los controles criptográficos. Real Decreto 4/2010.

Con la aprobación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, se han desarrollado políticas de firma electrónica para su uso en las entidades de la Administración.

La FNMT-RCM-RCM velará por el cumplimiento de dichas políticas en el ámbito de su actuación.

Por otra parte, el Centro Criptológico Nacional (CCN) es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

El CCN es el encargado de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones de la Administración.

En este sentido, la FNMT-RCM considerará las normas CCN-STIC como normas de referencia, en especial en lo que se refiere a controles criptográficos y empleo de algoritmias.

Seguridad física

Las instalaciones de la FNMT – RCM, como Proveedor de Servicios de Certificación, están situadas en: Calle Jorge Juan, 106. 28009 Madrid

La FNMT-RCM en su marco de operación cumple y dispone de las medidas establecidas en el proceso de Sistemas de Gestión de Seguridad de la Información, estando plenamente certificada en el modelo cumpliendo con las medidas que aplican a:

Instalaciones y medios técnicos.

Medidas de control de acceso a las instalaciones físicas

Ubicación de las instalaciones

Situación del Centro de Proceso de Datos

Acceso Físico

- Perímetro de seguridad física
- Controles físicos de entrada
- El trabajo en áreas seguras
- Áreas aisladas de carga y descarga

Electricidad y Aire Acondicionado

Seguridad del cableado

Exposición al agua

Prevención y Protección contra incendios

Almacenamiento de Soportes

Recuperación de la información

Eliminación de Residuos

Copias de Seguridad fuera de las instalaciones

Plan de contingencias.

Sistema de registro y archivo de todo el proceso de emisión y custodia de certificados

Sistema de gestión de la seguridad de la información

La FNMT-RCM tiene establecido un Sistema de Gestión de la Seguridad de la Información (SGSI) para su Departamento CERES con el objetivo final de mantener y garantizar la seguridad de la información de los clientes y la suya propia, de forma que el servicio prestado por la FNMT-RCM tenga los niveles suficientes de fiabilidad y seguridad que exige el Mercado.

El SGSI de la FNMT-RCM es aplicable a los activos de información definidos en el Análisis de Riesgos realizado utilizando las normas de referencia:

- UNE ISO 71501-1,2,3 IN: Guía para la Gestión de la Seguridad de TI
- UNE ISO 71502:2002 IN Especificaciones para los Sistemas de Gestión de la Seguridad de la Información
- UNE-ISO/IEC 17799 Código de Buenas Prácticas para la Gestión de la Seguridad de la Información
- ETSI EN 319 401 - General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 - Trust Service Providers issuing certificates
- ETSI EN 319 411-2 - Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421 - Trust Service Providers issuing Time-Stamps
- Seguimiento de la metodología MAGERIT versión 1.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas).

4. Solución Tecnológica y Tipos de Certificados

Se enumeran y explican los certificados expedidos por la FNMT-RCM:

- Certificados cualificados eIDAS de persona física emitidos por la AC FNMT Usuarios (ES00 / UE00)
- Certificados cualificados eIDAS de Representante de persona jurídica emitidos por la AC Representación (ES11-ES12 / UE01)
- Certificados cualificados eIDAS de empleado público y empleado público con seudónimo emitidos por la AC Administración Pública. (ES05-ES07 / UE00)
- Certificados cualificados eIDAS de Sello electrónico para la actuación automatizada de la Administración Público emitidos por la AC Administración Pública. (ES08 / UE01)
- Certificados reconocidos de Sede electrónica emitidos por la AC Administración Pública (ES09 / UE02)
- Certificados de componente emitidos por la AC Componentes: (ES08 /UE01)
  - » Certificado SSL/TLS estándar
  - » Certificado wildcard
  - » Certificado SAN multidominio
  - » Certificado de firma de código
  - » Certificado cualificado eIDAS de sello de entidad

4.1 Certificados cualificados eIDAS de persona física emitidos por la AC FNMT Usuarios

El Certificado digital FNMT de Persona Física es la certificación electrónica expedida por la FNMT-RCM que vincula a su suscriptor con unos Datos de verificación de Firma y confirma su identidad.

Este certificado, también conocido como Certificado de Ciudadano o de Usuario, es un documento digital que contiene sus datos identificativos. Le permitirá identificarse en Internet e intercambiar información con otras personas y organismos con la garantía de que sólo Ud. y su interlocutor pueden acceder a ella.

Se dispone de una red de Oficinas de Registro y acreditación que cuentan con los medios informáticos precisos para conectarse telemáticamente con la FNMT-RCM. En ellas, la acreditación e identificación de los solicitantes de los certificados se exige la comprobación de su identidad y de su voluntad de que sea expedido un certificado electrónico y, en su caso, de las facultades de representación, competencia e idoneidad para la obtención del certificado correspondiente, y se verifica de conformidad y con pleno respeto a lo dispuesto en la normativa aplicable.

Los Certificados de persona física expedidos por la FNMT-RCM tienen validez durante un periodo máximo de cuatro (4) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que el Titular desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.

Son expedidos por la FNMT-RCM como Prestador Cualificado de Servicios de Confianza cumpliendo con los criterios establecidos en la Ley 59/2003, de 19 de diciembre, citada y en la normativa técnica EESSI, concretamente de conformidad con el estándar europeo ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y "ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

Los certificados de persona física son cualificados conforme al Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl

El tamaño de las claves RSA relativas al certificado raíz de la Autoridad de certificación que emite los certificados electrónicos es actualmente de 4.096 bits.

El tamaño de las claves RSA relativas a los certificados electrónicos cualificados para identificar a las personas físicas es actualmente de 2.048 bits.

El algoritmo de cifrado de todos los certificados emitidos es de SHA-265.

4.1.1. Generación de claves

En el procedimiento de obtención de certificados, la FNMT-RCM desarrolla los elementos necesarios para activar, en el puesto del solicitante, el software que genera a través de su navegador web, un par de claves, pública y privada, que le permitirá firmar e identificarse, así como proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado.

Las claves privadas serán utilizadas bajo el control del software de navegación web del que disponga el propio usuario, enviando todas las claves públicas a la FNMT-RCM con el fin de integrarlas en un certificado.

Las claves privadas de firma permanecerán siempre bajo el control exclusivo de su titular, y guardadas en el soporte correspondiente, no guardándose copia de ellas por la FNMT-RCM.

La FNMT-RCM garantizará que el usuario, Titular del certificado, puede tener el control exclusivo de las claves privadas correspondientes a las claves públicas que se consignan en el certificado, mediante la obtención de las pruebas de posesión oportunas, a través de la adjudicación del número de identificación único.

Archivo de las claves públicas

Las claves públicas de los usuarios permanecerán archivadas, por si fuera necesario su recuperación, en archivos seguros, tanto física como lógicamente, durante un periodo no menor de 15 años.

Exclusividad de las claves

Las claves privadas son exclusivas para los Titulares de los certificados y son de uso personal e intransferible.

Las claves públicas son exclusivas para los Titulares de los certificados, independientemente del soporte físico donde estén almacenadas y protegidas.

Renovación de claves

La FNMT-RCM identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar distintos certificados para una misma clave. Es por esto por lo que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

4.1.2. Registro de usuarios

El registro de usuarios es el procedimiento a través del cual se identifica al solicitante de un certificado electrónico, se comprueba su personalidad y se constata su efectiva voluntad de que le sea emitido el "Certificado Básico" o "Título de Usuario" por la FNMT-RCM.

Este registro podrá ser realizado por la propia FNMT-RCM o cualquier otra Administración pública y, en su caso, por las demás personas, entidades o corporaciones habilitadas a tal efecto por las normas que resulten de aplicación. En todo caso el registro se llevará a cabo según lo dispuesto por la FNMT-RCM, al objeto de que este registro se realice de acuerdo con lo establecido por la normativa específica aplicable y homogénea en todos los casos. De igual manera será la FNMT-RCM, quien defina y aporte los medios necesarios para la realización de este registro.

En el caso de que el registro lo realizara una Administración Pública, distinta de la FNMT-RCM, la persona que se encargue de la actividad de registro ha de ser personal al servicio de la Administración Pública. En estos casos, la FNMT-RCM dará soporte a la implantación de las distintas oficinas de registro, que se establezcan cuando fuere necesario, en los siguientes términos:

a) Aportación de la aplicación informática de registro

b) Aportación de la documentación relativa a la instalación y manejo de la aplicación, así como toda aquella referente a los procedimientos y normas sobre el registro.

c) Registro y formación de los encargados del registro, lo que supone la expedición de un certificado emitido por la FNMT-RCM para cada encargado del registro, que permita garantizar la seguridad de las comunicaciones con la FNMT-RCM, incluyendo la firma electrónica de las solicitudes de registro.

Identificación de los solicitantes de los certificados, comprobación de su personalidad y constatación de su voluntad.

La identificación de los solicitantes de los certificados en las oficinas de registro y la comprobación de su personalidad se hará mediante la exhibición del Documento Nacional de Identidad, Pasaporte u otros medios admitidos en derecho.

En el acto de registro, el personal encargado de las oficinas de acreditación constatará que el solicitante tiene la voluntad de solicitar que le sea emitido un certificado electrónico por la FNMT-RCM y que éste reúne los requisitos exigidos por el ordenamiento jurídico.

Necesidad de presentarse en persona

El procedimiento de registro requiere presencia física del interesado para formalizar el procedimiento de registro en la oficina de acreditación. No obstante, serán válidas y se dará el curso correspondiente a las solicitudes de emisión de certificados electrónicos cumplimentadas siempre que la firma del interesado haya sido legitimada notarialmente en los términos señalados en el referido modelo.

Incorporación de la dirección de correo electrónico del titular al certificado

No es preceptiva la incorporación de la dirección de correo electrónico del titular al certificado si bien se hará constar en él en el caso en que el titular aporte dicha dirección en el momento del registro.

Esta incorporación se realizará a los efectos de que el certificado pueda soportar el protocolo S/MIME en el caso de que la aplicación utilizada por el usuario así lo requiera.

Obtención del "Certificado Básico" o "Título de usuario"

Para la obtención de este certificado, así como para su revocación o suspensión, el solicitante deberá observar las normas y procedimientos desarrollados a tal fin por la FNMT-RCM de conformidad con la normativa vigente aplicable.

4.1.3. Emisión, Revocación y archivo de certificados de clave pública

EMISIÓN DE LOS CERTIFICADOS

La emisión de certificados supone la generación de documentos electrónicos que acreditan la identidad u otras propiedades del usuario y su correspondencia con la clave pública asociada; del mismo modo, la emisión de los certificados implica su posterior envío al directorio de manera que se pueda hacer uso de él cuando resulte necesario.

La emisión de certificados por parte de la FNMT-RCM sólo puede realizarla ella misma, no existiendo ninguna otra entidad u organismo con capacidad de emisión de estos certificados.

La FNMT–RCM, por medio de su firma electrónica, garantizará los certificados, así como la verificación de la identidad y cualesquiera otras circunstancias personales de sus titulares. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los certificados, la FNMT-RCM utilizará mecanismos criptográficos para asegurar la autenticidad e integridad de dicho certificado.

La FNMT - RCM, una vez emitido el certificado, lo publicará y mantendrá una relación de certificados emitidos durante todo el periodo de vida de este en un servicio de acceso telemático, universal, en línea y siempre disponible.

La FNMT-RCM garantiza para un certificado emitido:

a) Que el usuario dispone de la clave privada, correspondiente a la clave pública del certificado en el momento de su emisión.

b) Que la información incluida en el certificado se basa en la información proporcionada por el usuario.

c) Que no omite hechos conocidos que puedan afectar a la fiabilidad del certificado

ACEPTACIÓN DE CERTIFICADOS

- Para que un certificado sea publicado por la FNMT-RCM, ésta comprobará previamente:

  a) Que el signatario es la persona identificada en el certificado

  b) Que el signatario tiene un identificativo único

  c) Que el signatario dispone de la clave privada

- El organismo garantizará que, al solicitar un certificado electrónico, su titular acepta que:

  a) La clave privada con la que se genera la firma electrónica corresponde a la clave pública del certificado.

  b) Únicamente el titular del certificado tiene acceso a su clave privada.

  c) Toda la información entregada durante el registro por parte del titular es exacta.

  d) El certificado será usado exclusivamente para fines legales y autorizados y de acuerdo con lo establecido por la FNMT-RCM.

  e) El usuario final del certificado no es un Prestador de Servicios de Certificación y no utilizará su clave privada asociada a la clave pública que aparece en el certificado para firmar otros certificados (u otros formatos de certificados de clave pública), o listados de certificados, como un Prestador de Servicios de Certificación o de otra manera.

- El organismo garantizará que, al solicitar un certificado electrónico, su titular asume las siguientes obligaciones sobre su clave privada:

  a) A conservar su control.

  b) A tomar las precauciones suficientes para prevenir su pérdida, revelación, modificación o uso no autorizado.

  Al solicitar el certificado, el titular deberá prestar su conformidad con los términos y condiciones de su régimen y utilización.

REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS ELECTRÓNICOS

La Fábrica Nacional de La Moneda y Timbre – Real Casa de la Moneda dejará sin efecto los certificados electrónicos otorgados a los usuarios, cuando concurra alguna de las siguientes circunstancias:

a) Solicitud de revocación de este por la persona física o jurídica representada por éste o por un tercero autorizado.

b) Resolución judicial o administrativa que lo ordene.

c) Fallecimiento o extinción de la personalidad del usuario o incapacidad sobrevenida.

d) Finalización del plazo de vigencia del certificado.

e) Pérdida o inutilización por daños en el soporte del certificado.

f) Utilización indebida por un tercero.

g) Inexactitudes graves en los datos aportados por el usuario para la obtención del certificado.

h) Cualquier otra prevista en la normativa vigente.

La extinción de la eficacia de un certificado producirá efectos desde la fecha en que la Fábrica Nacional de La Moneda y Timbre – Real Casa de la Moneda tuviera conocimiento cierto de cualquiera de los hechos determinantes de la extinción previstos en el apartado anterior y así lo haga constar en su Registro de certificados. En el supuesto de expiración del período de validez del certificado, la extinción surtirá efectos desde que termine el plazo de validez.

La Fábrica Nacional de La Moneda y Timbre – Real Casa de la Moneda podrá suspender temporalmente la eficacia de los certificados, si así lo solicita el usuario o lo ordena una autoridad judicial o administrativa, o cuando existan dudas razonables, por parte de cualquier usuario público, sobre la vigencia de los datos declarados y su verificación requiera la presencia física del interesado. En este caso, la FNMT-RCM podrá requerir, de forma motivada, su comparecencia ante la oficina de acreditación donde se realizó la actividad de identificación previa a la obtención del certificado o, excepcionalmente, ante otra oficina de acreditación al efecto de la práctica de las comprobaciones que procedan. El incumplimiento de este requerimiento por un periodo de 10 días podrá dar lugar a la revocación del certificado.

La suspensión de los certificados surtirá efectos en la forma prevista para la extinción de su vigencia.

Comunicación y publicación en el Registro de Certificados de circunstancias determinantes de la suspensión y extinción de la vigencia de un certificado ya expedido.

La FNMT-RCM suministrará al organismo los mecanismos de la transmisión segura para el establecimiento de un servicio continuo e ininterrumpido de comunicación entre ambas a fin de que, por medios telemáticos o a través de un centro de atención telefónica a usuarios, traslade inmediatamente a la FNMT-RCM cualquier circunstancia de la que tenga conocimiento y que sea determinante para la suspensión, revocación o extinción de la vigencia de los certificados ya expedidos, a fin de que se pueda dar publicidad de este hecho, de manera inmediata, en el directorio actualizado de certificados a que se refiere el artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

La FNMT-RCM pondrá a disposición de los titulares de los certificados un centro de atención de usuarios que permitirá resolver cualquier duda o incidencia relativa a la validez o utilización de los certificados.

4.2. Certificados cualificados eIDAS de Representante de persona jurídica emitidos por la AC Representación

El Certificado de Representante de Persona jurídica es un certificado electrónico destinado a personas jurídicas en sus relaciones con las Administraciones Públicas, Entidades y Organismos Públicos vinculados o dependientes de las mismas.

Estos certificados electrónicos son cualificados en cumplimiento con los requisitos del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y por la que se deroga la directiva 1999/93/CE.

Las funcionalidades y propósitos del Certificado de Representante de Persona jurídica permiten garantizar la autenticidad, integridad y confidencialidad de las comunicaciones en las que participe su Titular. La expedición y firma del Certificado se realizará por la "AC FNMT Representación" subordinada de la "AC Raíz" de la FNMT-RCM.

Los Certificados de Representante de Persona jurídica expedidos por la FNMT-RCM tienen validez durante un periodo máximo de dos (2) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que el Titular desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.

El Certificado de Representante de Persona jurídica no podrá ser utilizado cuando expire su periodo de validez, cuando sea solicitada su revocación por el Titular del Certificado o se cumpla alguna de las otras causas de extinción de su vigencia, establecidas en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica y en las Políticas y Prácticas Particulares de los Certificados de Representante.

La longitud de la clave utilizada en la "AC FNMT Representación" es de 2048 bits y en la "AC Raíz" es de 4096 bits.

La validación del estado de vigencia de este tipo de certificados se puede comprobar a través del servicio de información y consulta del estado de los Certificados que provee la FNMT – RCM mediante el protocolo OCSP, disponible en la ubicación especificada en el propio certificado.

La FNMT – RCM, como Prestador de Servicios de Confianza, expide estos certificados de conformidad con los estándares europeos ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons".

Los certificados de representante de persona jurídica se expiden como cualificados conforme al Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

4.3. Certificados cualificados eIDAS de empleado público y empleado público con seudónimo emitidos por la AC Administración Pública.

Estos certificados se emiten por la FNMT-RCM por cuenta de la Administración Pública correspondiente a la que la FNMT-RCM presta los servicios técnicos, administrativos y de seguridad necesarios como Prestador Cualificado de Servicios de Confianza.

Los certificados para personal al servicio de la Administración Pública son desarrollados por la FNMT-RCM mediante una infraestructura PKI específica y ad hoc, basada en actuaciones de identificación y registro realizadas por la red de Oficinas de Registro designadas por el órgano, organismo o entidad Suscriptora del certificado. Los "Procedimientos de Emisión" podrán establecer, en el ámbito de actuación de las Administraciones Públicas, Oficinas de Registro comunes para este ámbito de actuación con efectos uniformes para cualesquiera Administraciones, organismos y/o entidades públicas.

Son expedidos por la FNMT-RCM como Prestador Cualificado de Servicios de Confianza cumpliendo con los criterios establecidos en la Ley 59/2003, de 19 de diciembre, citada y en la normativa técnica EESSI, concretamente de conformidad con el estándar europeo

ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates" y "ETSI EN 319 412-2 "Certificate profile for certificates issued to natural persons". Estos certificados electrónicos son emitidos exclusivamente al personal al servicio de la Administración, y por tanto no se emiten al público general.

Los certificados de firma electrónica del personal al servicio de la Administración Pública son cualificados conforme al Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl

El tamaño de las claves RSA relativas al certificado raíz de la Autoridad de certificación que emite los certificados electrónicos es actualmente de 4.096 bits.

El tamaño de las claves RSA relativas a los certificados electrónicos cualificados para identificar a los empleados públicos es actualmente de 2.048 bits.

El algoritmo de cifrado de todos los certificados emitidos es de SHA-265.

La FNMT – RCM garantiza que el tiempo máximo en la emisión de un certificado electrónico de empleado público es de 5 minutos, desde el momento de la acreditación de la identidad y demás circunstancias asociadas que forman parte de los citados certificados.

4.3.1. Generación y gestión de claves

La FNMT-RCM, bajo ningún concepto, genera ni almacena las Claves Privadas de los Firmantes, que son generadas bajo su exclusivo control y con la intervención de la Oficina de Registro correspondiente y cuya custodia está bajo responsabilidad del personal al servicio de la Administración Pública.

4.3.2. Registro de usuarios

La acreditación de la identidad de los empleados públicos se realizará en una Oficina de Registro designada a tal efecto por el órgano, organismo o entidad pública Suscriptora de la que depende el personal a su servicio. Dicha Oficina de Registro es creada por la Administración suscriptora, que notifica a la FNMT-RCM la relación de personas habilitadas para realizar estas actividades de Registro, de acuerdo con los procedimientos establecidos a tal efecto, así como cualquier variación en la estructura de dicha Oficina.

A estos efectos FNMT-RCM tendrá en cuenta las funcionalidades previstas en la legislación aplicable en relación con el DNIe, así como los sistemas de identificación y comprobación del cargo, función o empleo aplicables en las Administraciones Públicas, por lo que la acreditación de la identidad mediante la personación física podrá ser sustituido por otros procedimientos que permitan la identificación, siempre que estén amparados por la intervención de la Oficina de Registro. En estos supuestos de procedimientos especiales de identificación propios del ámbito público, no será necesaria la personación cuando por el órgano competente de la Administración se proceda a certificar los requisitos de identidad, vigencia del cargo y demás condiciones a comunicar a la Oficina de Registro, de acuerdo con lo previsto en el artículo 13.1 in fine de la Ley 59/2003 de Firma electrónica.

En los certificados de empleado público con seudónimo el organismo deberá vincular la identidad del usuario con su seudónimo, siendo este último único por cada organismo.

La FNMT-RCM, una vez realizadas las comprobaciones pertinentes por la Oficina de Registro, comprobará mediante la Clave Pública del peticionario la validez de la información de la presolicitud firmada, comprobando la posesión y correspondencia de la pareja de Claves criptográficas por parte del peticionario y el tamaño de las claves generadas.

4.3.2.1. Precarga de datos de un conjunto de certificados electrónicos de empleado público

Adicionalmente se ofrece la posibilidad de emplear la aplicación de precarga de datos que permite realizar cargas por lotes de ficheros XML con información referente a solicitudes de gestión de certificados digitales de empleado público.

Dispone de dos interfaces para el usuario final:

(1) Una aplicación Web para interacción de los usuarios del Sistema y

(2) Otro interfaz basado en "Web Services" que permite la integración con otros sistemas de clientes externos.

Sistema de Precarga de Datos tiene la misión de habilitar la posibilidad de precargar datos correspondientes a personas que van a realizar solicitudes de certificado. La finalidad de precargar datos es agilizar el proceso de registro de solicitudes de certificados, así como minimizar la posibilidad de comisión de errores humanos.

Las principales funcionalidades del Sistema son las siguientes:

- El sistema permite la recepción de lotes de información estructurada (actualmente ficheros XML) correspondiente a la precarga de datos que se utilizarán en las solicitudes de gestión de certificados.
- Dispone de un interfaz Web para interactuar con los usuarios del Sistema. A través de interfaz, un usuario autorizado podrá "subir" al sistema un lote de registros (fichero XML) para que sea procesado.
- El sistema dispone de un interfaz de usuario basado en Web Services que permite la integración con los sistemas informáticos de nuestros clientes externos. Este interfaz permite intercambiar registros de datos uno a uno o mediante un lote de registros.
- Interfaz de administración que permite la gestión de autorizaciones de acceso al servicio. Para autenticar el acceso al mismo también se emplean certificados electrónicos.
- El sistema comprueba que los datos provienen de un actor autorizado. La autenticación se realiza mediante el uso de certificados electrónicos.
- Validación de la información asegurando que es sintácticamente correcta antes de realizar la inserción en el repositorio de datos.
- Registro de la actividad e información enviada por parte de los actores.
- Información de retorno informando del resultado de la operación de carga de datos (registros individuales o lotes).

4.3.3. Emisión, Revocación y archivo de certificados de clave pública

Emisión de certificados de los certificados de empleado público

Una vez recibidos en la FNMT-RCM los datos personales del personal Solicitante, la información que describe su relación con la Administración Pública, así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del Certificado.

La emisión de Certificados supone la generación de documentos electrónicos que confirman la identidad del personal/seudónimo, su relación, cargo o empleo con la Administración Pública, así como su correspondencia con la Clave Pública asociada. La emisión de Certificados de la FNMT-RCM sólo puede realizarla ella misma, en su calidad de Prestador Cualificado de Servicios de Confianza, no existiendo ninguna otra entidad u organismo con capacidad de emisión de estos. La Autoridad de Certificación de la FNMT-RCM solo acepta solicitudes de generación de Certificados provenientes de fuentes autorizadas. Todos los datos contenidos en cada solicitud están protegidos contra alteraciones a través de mecanismos de firma electrónica realizada mediante el uso de certificados emitidos a dichas fuentes autorizadas.

La FNMT-RCM, por medio de su Firma electrónica, autentica los Certificados y confirma la identidad del Firmante/seudónimo, así como la vigencia del cargo o empleo de su personal, de conformidad con la información recibida por la Oficina de Registro. Por otro lado, y con el fin de evitar la manipulación de la información contenida en los Certificados, la FNMT-RCM utilizará mecanismos criptográficos que doten de autenticidad e integridad al Certificado.

Revocación de los certificados de empleado público

La revocación de un Certificado para el personal al servicio de la Administración podrá ser solicitada por el organismo a través de la Oficina de Registro habilitada para tal efecto o por el Firmante, bien a través de dicha Oficina de Registro, bien a través del teléfono habilitado para tal fin (previa identificación del Solicitante) cuyo número se hace público en la web de la FNMT – RCM y que estará operativo en horario 24x7. En este último caso se pide al Solicitante de la revocación, entre otros datos, el código único de solicitud que recibió en el proceso de presolicitud del certificado, al objeto de verificar su identidad.

Una vez que la FNMT-RCM ha procedido a la revocación del Certificado, se publicará en el Directorio seguro la correspondiente Lista de Certificados Revocados conteniendo el número de serie del Certificado revocado, la fecha y hora de revocación y la causa de revocación. Una vez que un Certificado ha sido revocado, su vigencia queda definitivamente extinguida, sin posibilidad de revertir su estado.

Este servicio está operativo en horario 24x7. El periodo máximo entre la recepción en la FNMT-RCM de la solicitud de revocación y la publicación del cambio de estado de revocación del Certificado a efectos del Servicio de información y consulta del estado de los certificados, es de 24 horas.

El estado del Certificado del personal al servicio de la Administración se podrá comprobar bien a través del acceso a las Listas de Revocación, bien a través del Servicio de información y consulta del estado de los Certificados a través de OCSP. Estos servicios estarán disponibles las veinticuatro (24) horas del día, todos los días del año, salvo por circunstancias ajenas a la FNMT-RCM u operaciones de mantenimiento.

4.3.3.1. Servicio de revocación y suspensión automatizada de un conjunto de certificados electrónicos de empleado público

El proceso tradicional de gestión de un certificado usualmente involucra al custodio de las claves y a un registrador. Este proceso, en algunas circunstancias como en las revocaciones masivas, puede llegar a ser tedioso y poco efectivo. Por ello, se proporciona un procedimiento que permite realizar el procesado de estos y otros tipos de solicitud en un proceso batch.

La solución más sencilla y funcional es remitir dichas solicitudes a un servicio web (Web Services) desarrollado para tal propósito.

Los datos se intercambian de forma segura entre la Oficina de Registro y la FNMT mediante ficheros XML. Esta información es interpretada y procesada por un proceso residente en las instalaciones de la FNMT-RCM.

En el proceso se garantiza la integridad, autenticidad y no repudio del "lote".

4.4. Certificados cualificados eIDAS de Sello electrónico para la actuación automatizada de la Administración Público emitidos por la AC Administración Pública.

Certificado cualificado de Sello electrónico para Administración Pública, órgano, organismo público o entidad de derecho público, como sistema de identificación y para la actuación administrativa automatizada y para la actuación judicial automatizada, que permite autenticar documentos expedidos por dicha Administración o cualquier activo digital.

Se expiden de conformidad con el estándar europeo ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", y ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons".

Los certificados de sello electrónico son cualificados conforme al Reglamento (UE) No 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl.

La duración de estos se establece en 3 años y la longitud de clave RSA en 2.048 bits. Cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados

4.5. Certificados reconocidos de Sede electrónica emitidos por la AC Administración Pública

Certificados para la identificación de sedes electrónicas de la administración pública, organismos y entidades públicas vinculadas o dependientes emitidos por la FNMT – RCM bajo la denominación de certificados administración.

Estos certificados se expiden conforme al Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, de conformidad con los estándares europeos ETSI EN 319 411-1 "Policy and Security Requirements for Trust Services Providers issuing certificates- General Requirements.

Emitidos en conformidad con los "Requisitos base para la emisión y gestión de certificados de confianza", requisitos establecidos por la entidad CA/Browser fórum.

La duración de estos se establece en 2 años y la longitud de clave RSA en 2.048 bits. Cuentan con servicio validación mediante OCSP, de libre acceso por parte de cualquier interesado, operativo las 24 horas del día, todos los días del año, y cuya URL, accesible desde internet, se refleja en los propios certificados.

4.6. Certificados de componente emitidos por la AC Componentes

Los Certificados de Componentes son expedidos y firmados por la FNMT-RCM para ser instalados y utilizados por Componentes informáticos, con el objeto de que se herede la confianza que representa la FNMT-RCM como Prestador de Servicios de Confianza.

Los certificados de componente que actualmente emite la FNMT-RCM y que componen parte de la solución propuesta son:

- **Certificado SSL/TLS estándar**: es aquel que permite establecer comunicaciones seguras con sus clientes utilizando el protocolo SSL/TLS. Este tipo de certificados garantiza la identidad del dominio donde se encuentra su servicio Web
- **Certificado wildcard**: Identifica todos los subdominios asociados a un dominio determinado, sin necesidad de adquirir y gestionar múltiples certificados electrónicos. Por ejemplo, el certificado wildcard emitido a "*.ejemplo.es" garantiza la identidad de dominios como compras.ejemplo.es, ventas.ejemplo.es o altas.ejemplo.es.
- **Certificado SAN multidominio**: El certificado de tipo SAN, también conocido como certificado multidominio, UC o Unified Communications Certificates, le permite securizar con un solo certificado hasta doce dominios diferentes.
- **Certificado de firma de código** este Certificado permite firmar programas y componentes informáticos acreditando la identidad del autor y realizar de este modo distribuciones seguras a través de Internet.
- **Certificado cualificado eIDAS de sello de entidad** es aquel que se utiliza habitualmente para establecer conexiones seguras entre componentes informáticos genéricos. Su flexible configuración permite dotarle de diferentes usos: Autenticación de componentes informáticos de una Entidad en su acceso a servicios informáticos, o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente, e intercambio de mensajes o datos cifrados con garantías de confidencialidad, autenticación e integridad. Se expiden conforme al Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior con el estándar europeo ETSI EN 319 411-2 "Requirements for trust service providers issuing EU qualified certificates", y ETSI EN 319 412-3 "Certificate profile for certificates issued to legal persons". Puede comprobarse su inclusión en la lista de confianza de prestadores de servicios de confianza (TSL, por sus siglas en inglés) de España, a través del enlace https://sede.minetur.gob.es/es-ES/datosabiertos/catalogo/lista-prestadores-tsl

El tamaño de las claves RSA relativas al certificado raíz de la Autoridad de certificación AC Componentes que emite los certificados electrónicos es actualmente de 4.096 bits.

El tamaño de las claves RSA relativas a los certificados electrónicos de componente es actualmente de 2.048 bits.

El algoritmo de cifrado de todos los certificados emitidos es de SHA-265.

La entrega del Certificado se realiza, previa notificación, poniéndolo a disposición del Solicitante en la aplicación de descarga de Certificados una vez sean cumplidos el resto de los requisitos para su expedición.

Revocación de los certificados de componente

El Suscriptor enviará el formulario de solicitud de revocación, cumplimentado y firmado electrónicamente a la FNMT-RCM, con los mismos Certificados que son admitidos para la solicitud y por los canales electrónicos habilitados por esta Entidad.

Adicionalmente, existe un servicio de atención telefónica, en horario 24 x 7, en los teléfonos 902200616 / 917406848 / 913878337, al que se pueden dirigir las solicitudes de revocación. La comunicación quedará grabada y registrada, sirviendo de soporte y garantía de la aceptación de la solicitud de revocación solicitada.

Para solicitar una revocación telefónica de un Certificado, el Solicitante de esta debe ser el Suscriptor o su representante en el caso de personas jurídicas u organismos públicos, y debe aparecer como tal en el certificado a revocar. En el caso del representante, este debe ser la misma persona que actuó como tal en la solicitud de expedición del certificado objeto de la revocación.

5. Servicios/Productos para AALL

La FNMT-RCM pone al servicio de las AALL la expedición de todos los tipos de certificados mencionados en el apartado anterior con las características indicadas, además de los siguientes servicios:

Publicación de certificados y servicio de consulta de vigencia

El servicio de información sobre el estado de revocación de los certificados permite, tanto a los suscriptores como a los verificadores de estos, validar la vigencia de dichos certificados electrónicos. Dicho servicio se constata como de obligado cumplimiento por parte de CERES hacia las entidades a las que presta servicios de certificación para que el certificado FNMT sea admitido por dichas entidades, en virtud de la normativa vigente en materia de firma electrónica. Por ser la piedra angular de cualquier operación relacionada con los certificados electrónicos (verificación de firma electrónica y autenticación de usuarios), es fundamental la prestación de este servicio en alta disponibilidad dentro de la Infraestructura de Clave Pública de CERES.

Por tanto, debido a su criticidad, este servicio está disponible las 24 horas del día y todos los días del año, con una disponibilidad mínima de un 99%, tanto a través de Internet como a través de la red SARA.

El centro de respaldo de la FNMT – RCM garantiza estos niveles de disponibilidad.

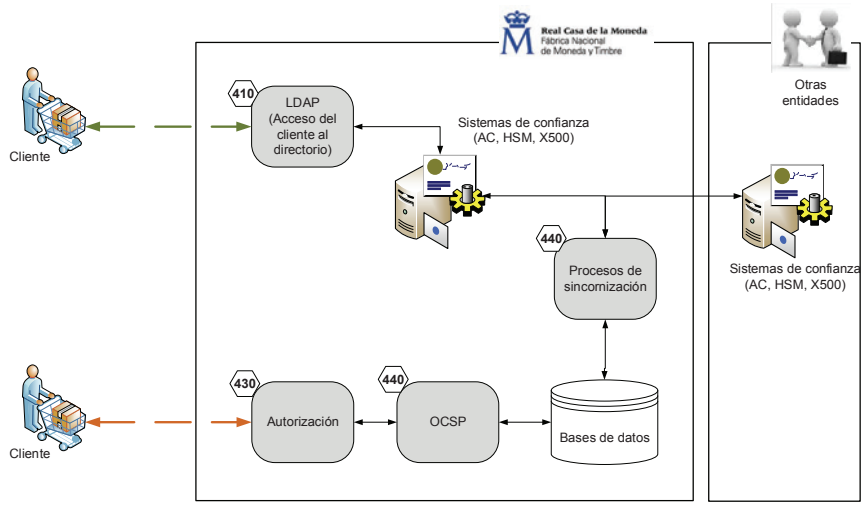
La FNMT – RCM pondrá a disposición de los organismos un servicio de verificación de firma electrónica para comprobar la integridad de los datos firmados, asegurando así que no han sufrido ninguna modificación y además confirmar que el estado del certificado con el que se realizó la firma era vigente en el momento de la operación.

El servicio de información sobre el estado de los certificados se presta en diferentes modalidades y según la CA de que se trate. En líneas generales existe la posibilidad de:

- Consultar directamente las ramas del directorio X500 de la FNMT correspondientes a las CRL's o listas de certificados revocados, que son firmadas por la FNMT – RCM.
- Obtener la información del estado del certificado por medio de consultas OCSP.

El servicio de verificación del estado de revocación de los certificados de la FNMT-RCM se presta sin restricción alguna de acceso. Dicho servicio de verificación del estado de revocación es de carácter universal, anónimo, gratuito y sin ningún tipo de autenticación, de forma que cualquier administración puede acceder a dicho servicio sin la necesidad de acuerdo alguno con la FNMT – RCM.

Los procesos de alto nivel intervinientes en el servicio se pueden observar en la siguiente figura:



Descripción del Servicio de Consulta del Estado del Certificado vía OCSP

Uno de los usos de los certificados electrónicos por parte de terceras personas es la verificación de firmas electrónicas efectuadas por el usuario del certificado. Sin embargo, la firma electrónica de un determinado documento ha de ser verificada en el momento de su utilización, ya que puede que el usuario haya invalidado ese certificado con anterioridad a la realización de esa firma (revocación/suspensión del certificado) o se haya producido la caducidad del certificado por las causas legales correspondientes. Por tanto, es necesario que siempre que se utilice un certificado para generar una firma electrónica se compruebe, en tiempo real, la validez (vigencia) del certificado del firmante.

DESCRIPCIÓN DEL SERVICIO

El servicio de consulta y validación de certificados vía OCSP se basa en una arquitectura cliente-servidor. El usuario solicitante de la verificación de un certificado vía OCSP será el que haga uso de la aplicación cliente y la autoridad de validación OCSP hará las labores de servidor.

Servidor OCSP Responder

El servidor de OCSP (OCSP responder) informa del estado en el que se encuentran los certificados en ese momento.

OCSP Cliente

Herramienta cliente para hacer peticiones de OCSP. Se pueden utilizar los productos del mercado. La FNMT-RCM no suministrará un OCSP cliente, pues se pueden encontrar con facilidad en el mercado de forma estándar.

Los intercambios de información entre las partes cliente y servidor OCSP se ajustarán a las estructuras definidas por el estándar RFC 6960, correspondiente a la norma de OCSP (Online Cetificate Status Protocol) de IETF-PKIX.

Una petición de OCSP contiene los siguientes datos:

- Versión del protocolo.
- Identificador/es del/los certificado/s a verificar.
- Extensiones.

Cuando se recibe la petición, el servidor de OCSP determina si el mensaje está correctamente formado y contiene la información necesaria para poder componer una respuesta satisfactoria.

Todas las respuestas proporcionadas por el servidor de OCSP deben ser firmadas digitalmente, y además deben componer los siguientes campos:

- Versión de la respuesta.
- Nombre del OCSP Responder.
- Respuestas para cada uno de los certificados.
- Extensiones opcionales.
- OID del algoritmo de firma.
- Firma.

La respuesta para cada uno de los certificados consiste en:

- Identificador del certificado.
- Estado del certificado.
- Intervalo de validez de la respuesta.
- Extensiones opcionales.

El estado de un certificado puede ser:

- Good.
- Revoked.
- Unknown.

La URL de acceso al servicio OCSP se incluye, en cada certificado emitido, en el campo "Acceso a información de Autoridad (AIA)".

1. AC FNMT Usuarios, http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder

2. AC Representación: http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder

3. AC Componentes: http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder

4. AC Administración Pública: http://ocspap.cert.fnmt.es/ocspap/OcspResponder

5. AC RAIZ FNMT RCM: http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder

Publicación de certificados de clave pública y registro de certificados

Validación del estado del certificado mediante consulta de CRLs (Publicación directa por parte de la FNMT-RCM)

Las listas de certificados revocados, o CRLs, contienen los nº de serie de aquellos certificados que han sido revocados por algún motivo antes de su fecha de caducidad. El formato de CRLs viene establecida en la RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

La FNMT-RCM ofrece un servicio de publicación de las listas de revocación de certificados, con el objetivo de que los organismos puedan comprobar si un certificado está revocado.

Para los certificados de todas las CAs se utilizan CRLs fraccionadas; por cada 750 certificados se genera una nueva CRL. Por ejemplo, al emitir el certificado 1 se genera la CRL1. En ella se reserva espacio para incluir la información de revocación de los 750 primeros certificados. Al emitir el certificado 751 se crea la CRL2 donde se almacenará el estado de revocación de los siguientes 750 certificados.

Este acceso está restringido a sólo lectura y búsqueda, pudiendo utilizar como clave de búsqueda cualquier información contenida en una entrada de un usuario.

URL de acceso:

- AC Usuarios
  - » Host, ldapusu.cert.fnmt.es
  - » Puerto, 389
  - » Base DN, cn=ac usuarios, ou=ceres, o=fnmt-rcm, c=es
  - » Versión, 3

- Fnmt Clase2 CA:
  - » Host, ldap.cert.fnmt.es
  - » Puerto, 389
  - » Base DN, ou=FNMT Clase 2 CA, o=FNMT, c=es
  - » Versión, 3
- AC Representación:
  - » Host, ldaprep.cert.fnmt.es
  - » Puerto, 389
  - » Base DN= OU=AC Representacion, OU=CERES,O=FNMT-RCM,C=ES
  - » Versión, 3
- AC Componentes:
  - » Host, ldapcomp.cert.fnmt.es
  - » Puerto, 389
  - » Base DN, cn=AC Componentes Informaticos, o=fnmt-rcm, c=es
  - » Versión, 3
- AC Administración Pública (AP)
  - » Host, ldapape.cert.fnmt.es
  - » Puerto, 389
  - » Base DN, cn=ac administración pública, ou=ceres, o=fnmt-rcm, c=es
  - » Versión, 3

Servicio cualificado de sellado de tiempo

El sellado de tiempo es un método para probar que un conjunto de datos (datum) existió antes de un momento dado y además que ningún bit de estos datos ha sido modificado desde entonces.

Además, el sellado de tiempo proporciona un valor añadido a la utilización de firma digital ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma. Los certificados digitales utilizados por el algoritmo de la firma digital tienen un periodo de validez y, por lo tanto, la firma sin el fechado digital, pasada la validez del certificado, siempre puede ser repudiada.

Para asociar los datos con un específico momento de tiempo es necesario utilizar una Autoridad de Sellado (TSA - Time Stamp Authority) como tercera parte de confianza.

Tipo de sello de tiempo electrónico y uso

El servicio cualificado de Sellado de Tiempo es ofrecido por la Autoridad de Sellado de Tiempo de la FNMT-RCM como Prestador de Servicios de Confianza y de conformidad con el Reglamento (UE) No 910/2014 del Parlamento Europeo y la norma técnica de aplicación ETSI EN 319 421 y RFC 3161.

- Son sellados con los Datos de Creación de Sello de la FNMT-RCM y los algoritmos utilizados son SHA-256 y RSA 3072
- El tiempo de vigencia de los Datos de Creación de Sello que la FNMT-RCM utiliza para ofrecer el servicio cualificado de sellado de tiempo es hasta el 3/3/2022.

El cliente de Sellado que el usuario debe montar se atendrá a la especificación recogida en la ETSI EN 319 422.

Límites de uso

La precisión declarada para la sincronización de la TSU con UTC es de 50 milisegundos, cumpliendo así sobradamente con los requisitos del estándar europeo [ETSI EN 319 421]. Por tanto, el Servicio cualificado de Sellado de Tiempo de la FNMT-RCM no expedirá ningún Sello cualificado de tiempo electrónico durante el periodo de tiempo en el que existiera un desfase mayor de 50 milisegundos entre los relojes de la TSU y la fuente de tiempo UTC del Real Observatorio de la Armada (ROA).

La FNMT – RCM registra y mantiene archivados aquellos eventos significativos necesarios para verificar la actividad de este servicio de confianza durante un periodo nunca inferior a 15 años, conforme a la legislación aplicable.

Protocolo

La TSA centraliza la emisión de certificados temporales. El papel que jugará esta entidad será producir, almacenar, verificar y renovar los certificados temporales. La TSA será una tercera parte de confianza (TTP), siendo su firma sobre el certificado temporal suficiente para probar la validez de éste.

Este protocolo permite el sellado de tiempo de cualquier tipo de información digital, y protege la confidencialidad de los datos fechados.

El usuario del servicio de sellado de tiempo debe ser poseedor de un certificado emitido por la Autoridad de Certificación de esta FNMT y que deberá ser solicitado por el usuario o parte autorizada.

La TSA hace uso de un certificado exclusivamente emitido para labores de sellado de tiempo, es decir, en su certificado está presente críticamente la extensión “extendedKeyUsage”, cuyo valor es id-kp-timestamping.

Solicitud de sellado de tiempo

Una vez que el usuario dispone de un certificado X.509 y su correspondiente clave privada podrá realizar peticiones de sellado de tiempo. El proceso para realizar una petición de sellado es el siguiente:

1. El usuario selecciona el fichero electrónico del cual se solicitará el sellado a la TSA.
2. La aplicación cliente compone un resumen (hash) del contenido de ese fichero.
3. El usuario selecciona la política de servicio que desea, el número de referencia, la versión...
4. La aplicación cliente compone una petición de fechado digital y la envía vía HTTPS.

Respuesta de sellado de tiempo

Una vez que la TSA haya recibido la solicitud de sellado y la haya aceptado, procederá a devolver a la aplicación cliente la respuesta de sellado o Response vía HTTPS. Este Response es un objeto que contiene un campo obligatorio que es el estado de la operación y en caso de que se haya realizado satisfactoriamente contiene además un objeto CMS SignedData, que es la firma del objeto que contiene toda la información del certificado de tiempo. El cliente podrá optar por almacenar directamente ese Response, validándolo previamente o también podrá optar por realizar la verificación de este, en caso de que no haya habido errores. Para ello:

1. La aplicación cliente recompone el objeto Response, extrayendo el estado de la operación, y si éste es GRANTED se puede extraer también el objeto CMS SignedData.
2. La aplicación cliente recompone el objeto CMS SignedData, extrayendo los datos firmados y verificando que la firma es correcta, haciendo uso del certificado de la TSA incluido en el objeto CMS.
3. Se obtienen los certificados incluidos en el objeto CMS y se hace “path validation”.
4. La aplicación cliente obtendrá los datos de sellado del token.

Estándares aplicables

La definición del servicio de Sellado de Tiempo está basada en las especificaciones del estándar IETF-PKIX RFC-3161 – “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)” y la correspondiente norma ISO 18014-2, en la cual la FNMT-RCM ha participado como elaboradores de esta.

A continuación, se describen brevemente algunos de los puntos del mencionado estándar que tienen mayor impacto en la definición de la solución final del servicio.

El estándar RFC3161 define entre otros, el formato de la solicitud de un sellado de tiempo y de la respuesta generada por la TSA. También establece los diferentes requerimientos de seguridad que debería cumplir una TSA.

Uno de estos requerimientos, es que todos los sellados de tiempo generados por la TSA deben estar firmados digitalmente por ella con la clave privada de un certificado digital válido emitido especialmente para este propósito.

Por otro lado, el mencionado estándar especifica que los sellados de tiempo (tokens) generados por la TSA no pueden incluir ninguna identificación del cliente que ha solicitado la operación. Como consecuencia, no es necesario que los mensajes de solicitud de sellado de tiempo que recibe la TSA contengan algún tipo de autenticación del cliente.

El estándar enumera diferentes mecanismos de transporte para mensajes de TSA. Ninguno de estos métodos es obligatorio; todos ellos son opcionales e incluso se contempla la posibilidad de soportar en un futuro nuevos mecanismos. Los mecanismos que especifican el documento RFC3161 son:

- Protocolo utilizando correo electrónico
- Protocolo basado en la utilización de FTP
- Protocolo basado en sockets utilizando el puerto IP 318
- Protocolo vía http/ssl.

También hay que recalcar que el estándar solamente define la operación de solicitud de sellado de tiempo y de la respuesta correspondiente, dejando otros tipos de operaciones, como por ejemplo la validación del sellado, sin ninguna especificación, aunque se deba realizar la implementación de este tipo de operaciones.

Servicio de firma electrónica centralizada para empleados públicos (firma en la nube)

La AC Administración Pública expide certificados de firma electrónica centralizada para funcionarios, personal laboral, estatutario a su servicio y personal autorizado, al servicio de la Administración Pública, órgano, organismo público o entidad de derecho público.

Estos Certificados son válidos como sistemas de firma electrónica de conformidad con la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y de conformidad con la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

El certificado de firma electrónica centralizada para empleados públicos es un certificado cualificado para la creación de firmas electrónicas avanzadas generadas en un dispositivo de creación de firma remoto, en un entorno seguro y confiable. Esto es, la generación de las Claves pública y privada no se realiza directamente en el navegador de Internet del Firmante o en otro dispositivo en su poder, sino que se generan y se almacenan en un entorno seguro perteneciente a la FNMT-RCM. Para proveer este servicio, se ha integrado en la infraestructura de la FNMT-RCM, el módulo TrustedX eIDAS de Safelayer.

El Certificado de firma electrónica centralizada para empleado público, confirma de forma conjunta, la identidad del personal al servicio de las Administraciones Públicas, y al suscriptor del certificado, que es el órgano, organismo o entidad de la Administración Pública, donde dicho personal ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

Asimismo, la firma electrónica se realiza de forma centralizada, garantizándose en todo momento el control exclusivo del proceso de firma por parte del Personal al servicio de la Administración al que se le ha expedido el Certificado. El acceso a las claves privadas del firmante se llevará a cabo garantizando siempre un Nivel de Aseguramiento ALTO (usuario+password + 2º factor de autenticación OTP).

Las funcionalidades y propósitos del Certificado de firma electrónica centralizada para empleado público permiten garantizar la autenticidad, integridad y confidencialidad de las comunicaciones. La expedición y firma del Certificado se realizará por la "AC Administración Pública" subordinada de la "AC Raíz" de la FNMT-RCM.

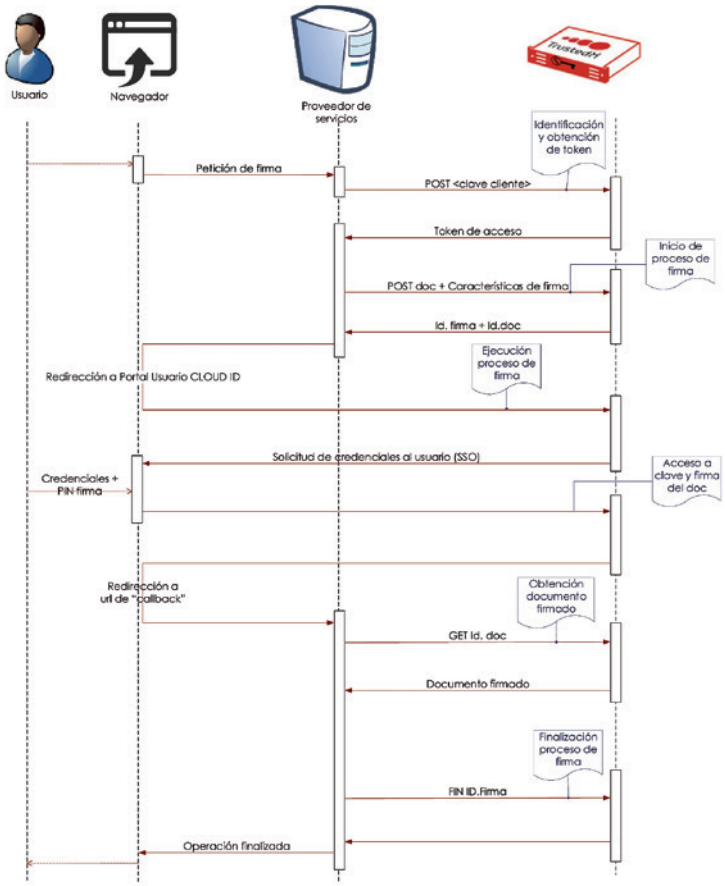
Los Certificados de firma electrónica centralizada para empleado público expedidos por la FNMT-RCM tendrán validez durante un periodo máximo de tres (3) años contados a partir del momento de la expedición del Certificado, siempre y cuando no se extinga su vigencia. Transcurrido este periodo y si el Certificado sigue activo, caducará, siendo necesaria la expedición de uno nuevo en caso de que se desee seguir utilizando los servicios del Proveedor de Servicios de Confianza.

La longitud de la clave utilizada en la "AC Administración Pública" es de 2048 bits y en la "AC Raíz" es de 4096 bits.

La validación del estado de vigencia de este tipo de certificados se puede comprobar a través del servicio de información y consulta del estado de los Certificados que provee la FNMT – RCM mediante el protocolo OCSP, disponible en la ubicación especificada en el propio certificado.

La plataforma de firma centralizada está actualmente siendo auditada conforme con los requisitos del Reglamento (UE) Nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, y por la que se deroga la directiva 1999/93/CE, para adquirir así la condición de servicio de firma cualificada.

A continuación, se presenta un esquema con el flujo de firma centralizada del servicio:



6. Garantías y Servicios de Soporte

La FNMT – RCM pone a disposición de los organismos un servicio de soporte técnico con personal altamente cualificado y experiencia en la resolución de incidencias y consultas sobre la operativa y funcionamiento de los servicios ofertados.

La atención telefónica por dicho personal se prestará en horario de 9 a 18:00 horas, los días laborales de lunes a viernes. El servicio de atención a las oficinas de registro los sábados de 11:00 a 14:00 horas se llevará a cabo a través del CAU 917 406 982.

Además, se posibilita la recepción de incidencias a través de un formulario en el portal web de Ceres y a través de una dirección específica de correo electrónico.

Este servicio hace uso de los sistemas de gestión que se describen en los siguientes apartados.

6.1 Sistema de información para el seguimiento del servicio de soporte técnico.

FNMT – RCM ha desarrollado un sistema de información para el seguimiento del servicio de Soporte Técnico. Si bien se utiliza una herramienta del mercado (Footprints), su configuración y parametrización es llevada a cabo por el personal del Área de Normalización, por lo que es posible implementar un proyecto específico.

Con este fin, se propone utilizar este sistema dirigido al personal de los organismos.

Los asuntos que llegan al Área de Soporte pueden ser de varios tipos (consultas, peticiones, incidencias, reclamaciones, sugerencias, etc.) y es este Área quien identifica el tratamiento específico para cada uno de ellos. La dirección de correo de contacto para los organismos es soporte_tecnico_ceres@fnmt.es.

No obstante, estos correos se redirigen a una dirección interna de forma que el flujo incorpora automáticamente como asuntos todos los correos recibidos en dicho buzón.

La apertura de un asunto en la herramienta Footprints se realiza por dos vías y, siempre que el contacto esté dado de alta en la libreta de contactos, se asocia éste al asunto.

- Entrada manual realizada por el Área de Soporte ante un asunto comunicado por el organismo a través del teléfono. En este caso la asociación del asunto al contacto del organismo es manual.
- Entrada automática ante la llegada de un correo a la cuenta de buzón interno. En este caso la asociación del asunto a un contacto del organismo es automática utilizando para identificarlo la dirección del remitente del correo. Si el asunto estaba cerrado, y se recibe un correo de respuesta a una de las notificaciones anteriores, el asunto vuelve a abrirse.

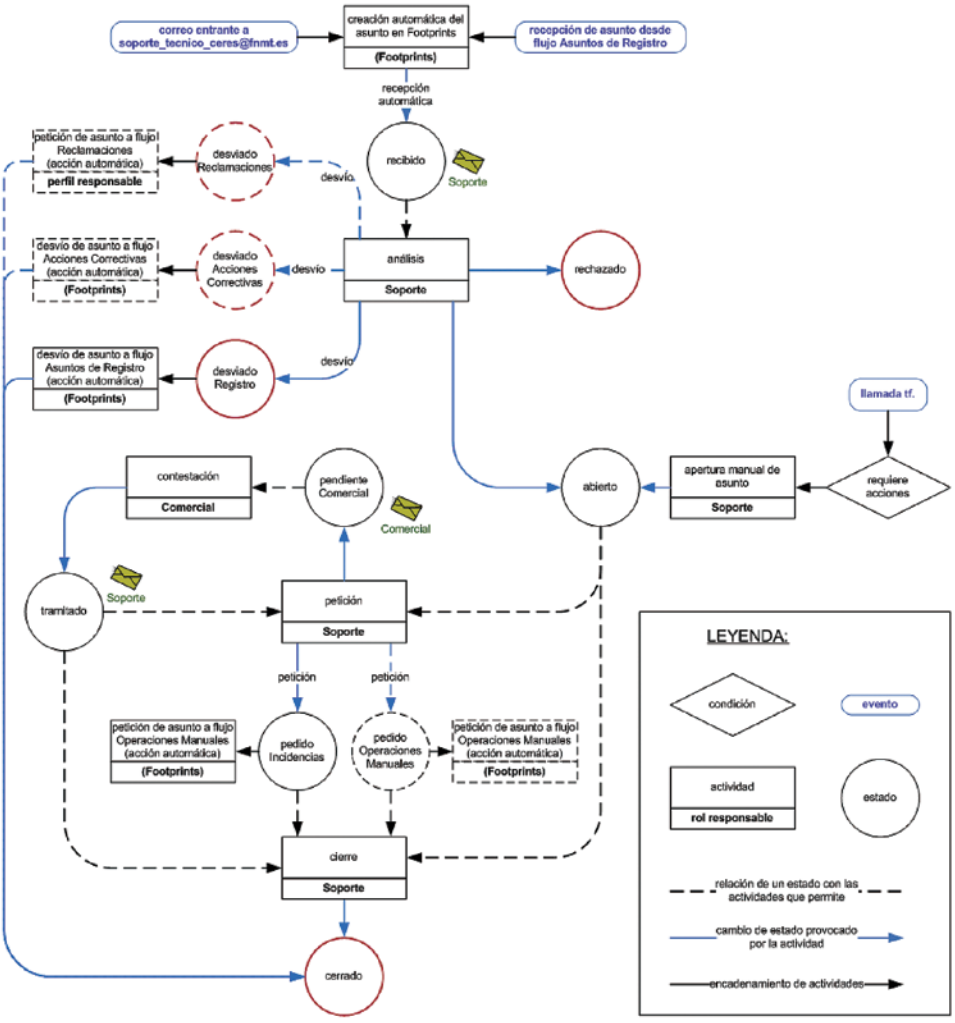
Tanto para la entrada manual como la automática el remitente recibe un mensaje automático de confirmación de que se ha abierto su asunto. A partir de ese momento, todos los correos que envíe el contacto en respuesta a cualquiera de las notificaciones se procesan no creando un nuevo asunto, sino adjuntando el cuerpo del mensaje como una nueva descripción del asunto existente.

Los miembros del Área de Soporte son siempre los únicos que pueden cerrar los asuntos y, en el momento de hacerlo, Footprints automáticamente envía al correo electrónico del creador del asunto la última descripción de este.

En resumen, las notificaciones automáticas a los contactos del organismo se producen únicamente cuando se modifica (o crea) un asunto y el estado final es abierto o cerrado.

Ya dentro del flujo automatizado, el encadenamiento de las tareas para el tratamiento de los asuntos se muestra en el siguiente diagrama:

FLUJO DE TRABAJO DE LA GESTIÓN DE ASUNTOS DEL AREA DE SOPORTE DE CERES



6.2 Sistema de gestión de incidencias

El protocolo definido en este apartado es de aplicación en la gestión de incidencias que se producen en procesos y sistemas horizontales, entendiendo como tales a los procesos y sistemas en los que participan o son utilizados por varias áreas de CERES.

La gestión de incidencias en el seno de cada una de las áreas es realizada según dictamina el responsable del área en cuestión.

Para la gestión de las incidencias se emplea una base de datos de Lotus Notes que básicamente maneja el flujo de operaciones asociado a la creación, gestión, control y resolución de las incidencias. El medio para informar acerca de nuevas incidencias son mensajes de correo.

El ciclo de vida genérico de cualquier tipo de incidencia es el que se muestra a continuación.

6.2.1 Ciclo de vida de las incidencias

Fase I: Detección y Apertura (alta)

El solicitante, si puede hacerlo o la persona a la que le ha llegado la información de la detección de la incidencia, debe rellenar el formulario de la Base de Datos de Control de Incidencias, aportando la siguiente información:

- **Título**: Título de la incidencia. Siempre que se ajuste se seleccionará una de las opciones de la lista desplegable. Solo si la incidencia no coincide con ninguna de las tipificaciones mostradas se completará manualmente.
- **Prioridad**: Urgencia o gravedad de la incidencia
- **Tipo**: Sistema afectado por la incidencia
- **Descripción**: Explicación detallada de la incidencia detectada aportando el máximo detalle posible (mensajes de error, capturas de pantalla, etc.).
- **Área que debe resolverla**: El área que va a recibir la incidencia para su resolución.

Una vez documentada la incidencia se envía pulsando sobre el botón "Enviar Incidencia" (aparece un desplegable con las áreas permitidas). Automáticamente la herramienta envía un mensaje al área seleccionada.

En caso de tratarse de una incidencia urgente, sería conveniente una llamada telefónica para agilizar la resolución (además de tramitarse por el procedimiento normal).

Cualquier persona de la organización puede abrir una incidencia de modo que es responsabilidad de todos y cada uno de los miembros de CERES realizar una apertura de incidencia ante cualquier debilidad (sospechada o detectada) de seguridad de la información, productos o servicios.

Si la incidencia está relacionada con la seguridad de la información, el solicitante notificará al responsable de seguridad para que la incidencia sea debatida en las reuniones del comité de seguridad y se proponga una respuesta rápida y eficaz como solución a ésta. Los registros y documentación asociados a este tipo de incidencias quedarán almacenados en el sistema de gestión habitual. En caso de que esta incidencia de seguridad tenga su origen en algún miembro de la organización será de aplicación el procedimiento disciplinario vigente.

Fase II: Recepción

Esta fase, el área receptora de la incidencia recibe un correo del sistema (reciben este correo una serie de personas del área previamente acordadas como receptoras de incidencias por parte del jefe de área correspondiente).

Fase III: Asignación personal

Cuando las personas del área receptora reciben la notificación de la incidencia, la consultan y una de ellas se la asigna personalmente mediante el botón "Asignar Incidencia". A partir de este momento es la persona encargada de resolver esta incidencia o de escalarla a otra área. El cómo se realiza el reparto de las incidencias entre las personas del área es algo que dependerá de la política organizativa de cada área.

Si la solución de la incidencia es desconocida por el área, ésta se reenviará al área que corresponda. La aplicación dispone de un botón para reasignar la incidencia.

Fase IV: Resolución de incidencia

En el caso de ser una incidencia que puede ser resuelta por el área, la persona que tiene asignada la incidencia llevará a cabo las acciones oportunas para solucionarla, acciones de las que se dejará constancia en el campo "Acciones" del formulario. El formato de este campo será:

Fecha: DD/MM/YYYY

Persona: Nombre de la persona que actualiza la incidencia

Descripción de las acciones: Descripción de las acciones llevadas a cabo.

En ocasiones puede ocurrir que una incidencia no avance sencillamente porque la persona que la tiene asignada está ausente. En ese caso, la aplicación prevé la posibilidad de recuperar la incidencia que tenga una persona para asignársela a otra.

Una vez resuelta la incidencia, se incluirá un texto descriptivo de la situación alcanzada para posteriormente pulsar el botón "Cerrar incidencia", esta pasará al estado "Cerrada". El sistema enviará automáticamente un correo electrónico al Solicitante notificando el cierre de la incidencia.

6.2.2 Obligaciones y responsabilidades

- Todo el personal del Departamento CERES está obligado a abrir una incidencia en el caso de que detecte cualquier anomalía en algún sistema, servicio, producto o proceso relacionado con la actividad de CERES.
- Es responsabilidad de la persona que tenga asignada una incidencia documentarla adecuadamente de forma que quede traza de las acciones llevadas a cabo para su resolución. A tal efecto, los registro incluidos en el campo "Descripción de las acciones" tendrán el formato descrito anteriormente (Fecha, Persona, Descripción de las acciones)
- Es responsabilidad de la persona que cierra la incidencia, comunicar esta situación al solicitante de esta.

6.3 Sistema de gestión de acciones correctivas, preventivas y de mejora

FNMT – RCM – Ceres utiliza un sistema para la gestión y análisis de no conformidades (reales o potenciales), así como la apertura, tratamiento y cierre de acciones correctivas, preventivas y de mejora, con el fin de eliminar las causas de las no conformidades y prevenir su reaparición en el caso de las acciones correctivas. Para el caso de las acciones preventivas, el objetivo es eliminar las causas potenciales y prevenir su aparición.

Son de aplicación las siguientes definiciones:

Acción Correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.

NOTA 1 - Puede haber más de una causa para una no conformidad.

NOTA 2 - La acción correctiva se toma para prevenir que algo vuelva a producirse, mientras que a acción preventiva se toma para prevenir que algo suceda.

NOTA 3 - Existe diferencia entre corrección y acción correctiva.

Acción Preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente indeseable.

NOTA 1 - Puede haber más de una causa para una no conformidad potencial

NOTA 2 - La acción preventiva se toma para prevenir que algo suceda, mientras que la acción correctiva se toma para prevenir que vuelva a producirse

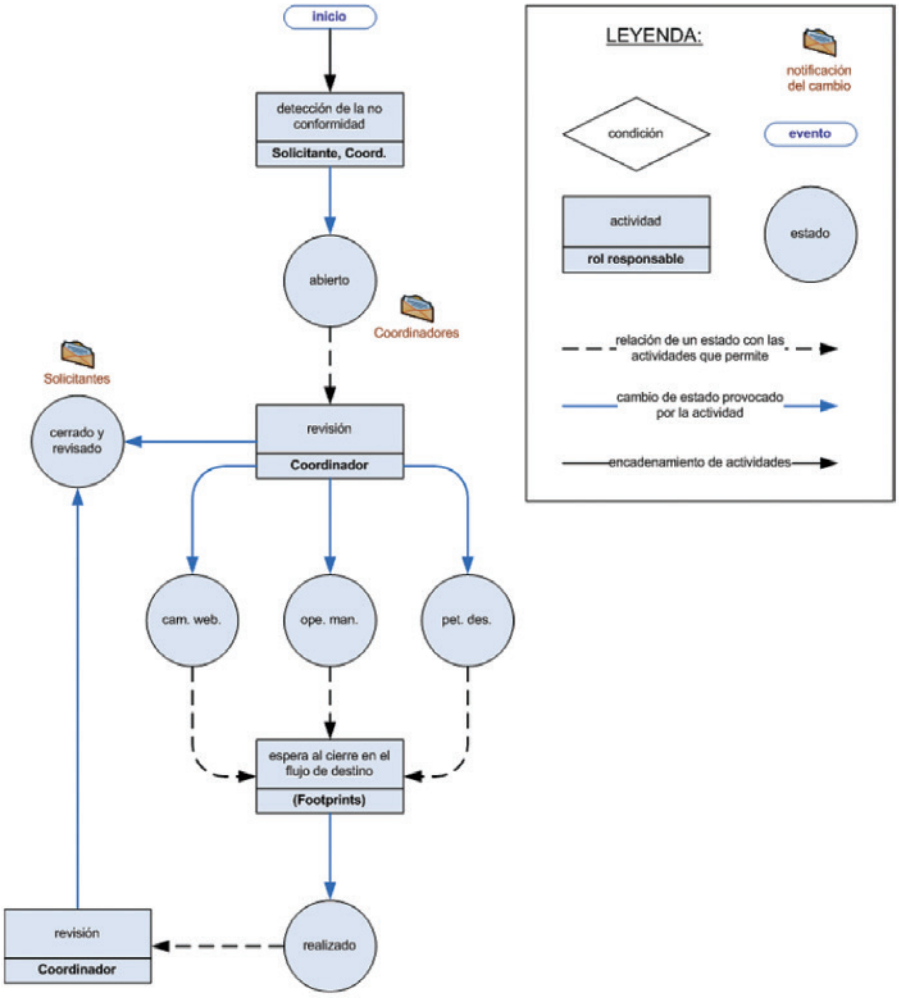
Acciones de mejora: En todos los casos, consideraremos a las acciones correctoras y preventivas como acciones de mejora. También serán acciones de mejora aquellas que se realizan con motivo de la búsqueda de la eficacia y eficiencia en el desempeño de los procesos y actividades, independientemente de que están vinculadas con la aparición potencial de no conformidades.

Conformidad: Cumplimiento de un requisito. El requisito puede ser de especificaciones, contractual, normativo, etc.

No conformidad: Incumplimiento de un requisito.

Sin entrar en detalles de responsabilidades internas, el flujo de trabajo del sistema se describe según la siguiente figura:

FLUJO DE TRABAJO DE LA GESTIÓN DE ACCIONES CORRECTIVAS, PREVENTIVAS Y DE MEJORA



6.4 Aplicación de gestión de certificados para consulta y seguimiento online de los certificados emitidos

La FNMT-RCM cuenta con una potente solución de gestión de la información que permite obtener de forma ágil y sencilla una visión completa y agregada de los datos asociados a cada Organismo dentro de nuestros sistemas de información.

Esta solución permite la generación de Informes, Cuadros de Mando y estadísticas para obtener en cada momento la información requerida por cada usuario manteniendo unos estrictos niveles de seguridad.

La FNMT-RCM pone a disposición de los organismos un servicio de consulta on-line que permitirá realizar consultas relativas a la propia estructura organizativa del organismo (registradores, oficinas, puestos, ROR, etc.) así como de los certificados emitidos. Todos los datos son exportables a formatos de propósito general (pdf, texto, csv, excel, word, etc.) para facilitar su uso por otros usuarios o en diferentes entornos.

Se contempla el acceso a la información correspondiente al Organismo, así como de los certificados emitidos por la FNMT – RCM bajo la denominación de Certificados para la Administración Pública (Certificados AP) y certificados de componente.

Desde un punto de vista funcional cada informe o cuadro de mando permitirá el uso de un conjunto de criterios de filtrado de datos para que el usuario pueda sacar en cada momento la información relevante para su tarea. Una vez seleccionado el filtro la plataforma generará los informes con la información demandada en el formato elegido por el usuario (HTML, pdf, texto, csv, excel, word, etc.).

La aplicación cuenta con los mecanismos de seguridad necesarios para que de forma dinámica cada usuario tenga acceso solo a la información sobre la que tiene visibilidad permitiendo que un mismo informe sea útil para usuarios de diferente naturaleza.

6.5 Servicio de información y "call center" a usuarios finales

La FNMT – RCM pone a disposición de todos los usuarios de los certificados, así como de los registradores, un completo servicio de asistencia técnica para la resolución de cualquier problema o consulta que necesiten resolver. La plataforma de asistencia técnica cuenta con los siguientes recursos disponibles:

- Apartado de **Respuestas a Preguntas Frecuentes** (FAQ's) actualizado permanentemente según las últimas necesidades detectadas de nuestros usuarios y **Formulario de contacto vía Web** disponible a través de nuestra página en la url:

  https://www.sede.fnmt.gob.es/soporte-tecnico/atencion-a-usuarios

- **Servicio de Call Center** a través de los teléfonos **902181696 / 917406982 / 917040191** y de la dirección de correo electrónico ceres@fnmt.es, en todos los idiomas oficiales en las diferentes CCAA (Gallego, Euskera, Catalán y Castellano), en el siguiente horario:

De 8h a 19h de lunes a viernes. Laborables de ámbito nacional.

Excepto:

Del 2 de mayo al 30 de junio que será de 9h a 21h de lunes a viernes y de 9h a 14h los sábados.

Del 28 de Julio al 29 de agosto que será de 9h a 15h de lunes a viernes.

6.6 Prestación del servicio desde un centro de respaldo

Con objeto de garantizar un nivel de servicio en alta disponibilidad, la FNMT – RCM cuenta con un centro alternativo de respaldo alojado en ciudad distinta de la de Madrid, dónde se encuentra el CPD principal.

Dicho centro de respaldo está configurado en modo activo/pasivo con replicación síncrona de datos.

La solución de respaldo comprende, además de la infraestructura Hardware y Software necesaria, un servicio de comunicaciones redundante entre el CPD y el centro de respaldo.

Por tanto, en caso de incidencia técnica del CPD principal, la FNMT – RCM proporcionará al organismo los servicios de certificación y firma electrónica desde el CPD de respaldo.

7. Servicios de Valor Añadido

La Fábrica Nacional de La Moneda y Timbre – Real Casa de la Moneda es una entidad pública empresarial dependiente de la Administración General del Estado y se encuentra adscrita al Ministerio de Hacienda y Administraciones Públicas (ahora Ministerio de Política Territorial y Función Pública), a través de la Subsecretaría de este departamento, que ejerce la dirección estratégica y el control de eficacia de la Entidad.

Por su parte, el apartado 7 del artículo 2 y el apartado 2 del artículo 3 de su Estatuto, según redacción dada por el artículo único del Real Decreto 336/2014, de 25 de junio, configura a la FNMT-RCM como medio propio y servicio técnico de la Administración General del Estado, así como de los organismos, entes y entidades del sector público estatal, sean de naturaleza jurídica pública o privada, en los términos del citado Real Decreto Legislativo 3/2011, de 14 de noviembre, TRLCSP y de su Estatuto.

Controles de auditoría de los sistemas de información

Para asegurar las propiedades de seguridad de la información, la FNMT-RCM-CERES ha establecido un plan de auditorías y controles.

Las auditorías de sistemas serán planificadas de modo que se reduzca el riesgo de interrupciones en el proceso de negocio. Además, se limita formalmente el alcance de la auditoría y su acceso únicamente a leer información, identificando los sistemas utilizados para realizar dicha auditoria y registrando todos sus rastros, que posteriormente serán revisados para comprobar el cumplimiento de lo acordado. En el caso de procesos especiales o adicionales se identifican sus requisitos.

Se establecen cláusulas de responsabilidad en el caso de desastres producidos por la auditoría, planificando previamente la restauración de los servicios que se vean afectados por la elaboración de la auditoría.

El auditor es independiente de las actividades auditadas.

8. Interoperabilidad con otras Instituciones/Organismos

Declaración de aplicabilidad del ENS a los sistemas de información

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica da cumplimiento a lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de la ciudadanía a los Servicios Públicos. Su objeto es establecer la política de seguridad en la utilización que realizan las entidades de la Administración de medios electrónicos. Está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Por tanto, la finalidad del Esquema Nacional de Seguridad, en adelante ENS, es la creación de las condiciones necesarias para generar confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El artículo 2 de la Ley 11/2007 establece el ámbito de aplicación del ENS e incluye, entre otros, a las entidades de derecho público vinculadas a Administración General del Estado; siendo por tanto una norma de obligado cumplimiento para la FNMT-RCM.

En el presente documento se define en qué medida el ENS afecta a la FNMT-RCM, determinado aquellos servicios y actividades concretas de la organización que deberán cumplir lo dispuesto en dicho esquema.

Alcance del ENS

El ámbito de aplicación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS), es coincidente, según dispone su artículo 3, con el ámbito de aplicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de la ciudadanía a los servicios públicos (LAECSP).

Por otro lado, el artículo 2 de la LAECSP señala que esta Ley será de aplicación a las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas (siempre que actúen en régimen de derecho público) y a las relaciones entre distintas administraciones (o entre organismos de la misma administración) .

En lo relativo a los servicios o sistemas de la organización que pudieran resultar del ámbito de aplicación del ENS, es necesario recordar que el concepto “ciudadano” mencionado en la LAECSP (y, en su consecuencia, en el ENS) debe entenderse en sentido amplio, es decir: ciudadanos, empresas, profesionales y también los propios funcionarios o empleados públicos cuando resulten ser destinatarios de los servicios prestados por organismos públicos entre cuyas competencias o potestades estatutarias se encuentren precisamente la prestación de tales servicios.

Además, dentro del concepto “servicio” no sólo deberán incluirse aquellos que preste un organismo concreto, de manera independiente o autónoma, sino también aquellos otros servicios para los que es necesario el concurso de la actividad de varios organismos o, incluso, varias administraciones públicas o la colaboración (o concierto) con terceras entidades (públicas o privadas).

Por todo ello, y por lo dispuesto en el articulado de las antedichas normas, los sistemas de información en los que el ENS resulta de directa aplicación son:

- Sedes electrónicas.
- Registros electrónicos.
- Sistemas de Información accesibles electrónicamente por los ciudadanos, profesionales y empresas.
- Sistemas de Información para el ejercicio de derechos (por parte de ciudadanos, profesionales y empresas).
- Sistemas de Información para el cumplimiento de deberes (de la ciudadanía, profesionales y empresas; y de los organismos públicos, en su relación con los ciudadanos).
- Sistemas de Información para recabar información y estado del procedimiento administrativo.
- Sistemas de Información para el desarrollo del procedimiento administrativo.

Sistemas de Información para el cumplimiento de las misiones comprendidas en las competencias o potestades estatutarias de derecho público del organismo en cuestión (es decir todas aquellas que aparezcan en la norma de creación del organismo en cuestión y/o en sus estatutos, y todos ellos, sea cual fuere la forma de prestación o ejecución de los servicios (propia, subcontratada, externa, concertada, modalidad Cloud Computing, en colaboración, etc.).

9. Clientes de Referencia

Entre nuestros clientes se encuentra la AGE, numerosas CCAA y EELL, así como empresas privadas.

Se puede consultar donde hacer uso de los certificados emitidos por la FNMT-RCM en nuestra sede electrónica: https://www.cert.fnmt.es/certificados/donde-usar-certificado

10. Acreditaciones / Certificaciones

Todas las certificaciones obtenidas están publicadas en nuestra web, donde se pueden consultar los diferentes sellos de los que dispone: https://www.cert.fnmt.es/que-es-ceres/calidad

11. Prácticas y Políticas de Certificación

Pueden consultar las Declaraciones, Políticas y Prácticas de Certificación de la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda en: https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

4.3.5. FIRMA PROFESIONAL

AUTORIDAD CERTIFICADORA:

FIRMAPROFESIONAL S.A.

1. Información General

Firmaprofesional, S.A.

Creada en 2001.

Proveedor Cualificado de Servicios de Confianza eIDAS.

Sedes en Madrid y Sant Cugat de Vallés (Barcelona).

2. Modelo de Prestación de Servicios

Proveedor de Servicios de Certificación y de Confianza Electrónica (QTSP), autorizados por el regulador español (Ministerio de Energía, Turismo y Agenda Digital) de acuerdo con el Reglamento Europeo eIDAS.

Dichos servicios son prestados de forma directa o mediante canal de distribución, según la solución/servicio y el mercado.

La prestación de algunos servicios de confianza permite ser realizada en modalidad SaaS y también en modalidad "In-house", según decisión del usuario o conveniencia por condiciones de eficiencia. Un claro ejemplo es la emisión de sellos cualificados de tiempo.

La emisión de certificados y sellos cualificados, así como los certificados cualificados de sitios web requieren de una identificación personal que de momento se realiza de forma presencial hasta que en el Estado Español se regule la telepersonación con garantías legales para estos fines. Este es el único requerimiento que actualmente limita la prestación completamente en línea de los servicios de un QTSP en España.

3. Características del Modelo

El modelo de Firmaprofesional se basa en una plataforma de emisión de certificados, sellos y certificados de sitios web constituida como Autoridad de Registro (RA).

Los clientes de Firmaprofesional, SA se constituyen en RA y emiten certificados personales en software o soporte criptográfico, instalados en dispositivos móviles o en servidores remotos homologados de alta seguridad, para producir firmas y sellos avanzados y/o cualificados.

Dicha emisión y otros servicios del porfolio permiten la gestión completa del ciclo de vida de los documentos electrónicos, con plena validez legal. Para garantizar dicha validez legal, Firmaprofesional actúa como tercero de confianza en las transacciones electrónicas de sus clientes.

Cada servicio se caracteriza por un SLA definido y un tarifado en función de volumen de unidades o transacciones, siempre decreciente en función del volumen.

4. Solución Tecnológica

Solución basada en software de Autoridad de Registro propio, con GUI web y accesible también vía webservice.

Firma centralizada cualificada también accesible vía webservices.

Infraestructuras propias en alta disponibilidad y virtualización, HSM en red y software de CA líder de mercado cumpliendo los máximos estándares de seguridad.

5. Tipos de Certificados

Empresas y Organizaciones: (todos cualificados eIDAS)

- Representante Legal en todas sus variantes (representante único o voluntario, de entidades con y sin personalidad jurídica) (ES09-ES11-ES12 / UE01-UE00)
- Corporativo de persona física (ES00 / UE00)
- Autónomo (ES11 / UE00)
- Colegiado (ES11 / UE00)
- Sello de Empresa (ES08 / UE01)

Administración Pública:

- Sede Electrónica (ES09 / UE02)
- Sello de Órgano (ES08 /UE01)
- Empleado Público (ES05 /UE00)
- Ciudadano (ES00 / UE00)

Técnicos:

- SSL cualificado eIDAS (ES09 / UE02)
- Certificados No Cualificados, de larga duración y de un solo uso (ES02 / UE04-UE05)

6. Servicios/Productos para AALL

- Servicio de Entidad de Registro (RA):
  - Servicio de Emisión de certificados digitales cualificados de forma autónoma por parte de la Administración.
  - Emisión en todos los soportes criptográficos.
  - Emisión centralizada para la firma remota avanzada.
  - Emisión centralizada para la firma remota cualificada según eIDAS.

- Servicio de Custodia y Firma Remota:
  - » Servicio de custodia remota centralizada de certificados digitales cualificados.
  - » Servicio de Firma Remota avanzada y cualificada eIDAS.
- Servicio de Identidad Digital Móvil:
  - » Servicio de identidad digital móvil, mediante App, con certificado para firma simple, avanzada, o cualificada. Para ciudadanos y trabajadores públicos.
- Certificados Digitales:
  - » Sede Electrónica
  - » Sello de Órgano
  - » Representante Legal de la Administración
  - » Empleado Público
  - » Ciudadano
  - » SSL cualificado eIDAS
  - » Certificados No Cualificados
- Servicio Cualificado de Sellado de Tiempo (TSA/TSU):
  - » Servicio cualificado de sellado de tiempo.
  - » Instalación Inhouse de TSU cualificada.

7. Garantías y Servicios de Soporte

Servicio de soporte de incidencias:

- Formas de trasladar al equipo de soporte de Firmaprofesional:
  - » Por teléfono: 915762181; 934774245
  - » Por E-Mail: soporte@firmaprofesional.com
  - » Por formulario Web: https://otrs.firmaprofesional.com/otrs/customer.pl
- Horario de atención: de lunes a jueves de 8.00 a 19.00 horas y el viernes de 8:00 a 15:00 horas. Extensible en casos concretos previa contratación.

Todas las incidencias se gestionan por un sistema de ticketing y existe un SLA establecido con los clientes.

8. Interoperabilidad con otras Instituciones/Organismos

Soluciones basadas en estándares que facilitan la interoperabilidad.

Prestador de Servicios de Confianza cualificado, presente en la Lista de Servicios de Confianza española, y las grandes plataformas validadoras como @firma, PSIS, o la G.I.S.S.

9. Clientes de Referencia

- Consorci AOC
- Congreso de los Diputados
- Senado de España
- Ayuntamiento de Barcelona
- SACYL

10. Acreditaciones / Certificaciones

- ISO 9001
- ISO 27001
- Servicios cualificados:
  - » emisión de certificados de firma
  - » emisión de certificados de sello
  - » emisión de certificados de autenticación de sitio web
  - » sellado de tiempo
- HSM y software de CA CC EAL 4+

11. Prácticas y Políticas de Certificación

Disponibles en: www.firmaprofesional.com/cps

- Corporativo de Colegiado
- Corporativo de Persona Física
- Servidor Web SSL y EV
- Servicio Seguro TSA
- Corporativo de Persona Jurídica
- Corporativo de Sello Empresarial
- Corporativo de Representante Legal
- Sede Electrónica
- Sello de Órgano
- Empleado Público
- Certificado Personal
- En los siguientes dispositivos:
- DCCF portable (Nivel Alto)
- DCCF centralizado (Nivel Alto)
- Otros dispositivos (Nivel Medio - software)

4.3.6. IVNOSYS

AUTORIDAD CERTIFICADORA:

IVNOSYS SOLUCIONES

1. Información General

Ivnosys Soluciones es un Prestador de Servicios de Confianza especializado en la centralización de claves y la firma electrónica a distancia, a través de su plataforma IvSign.

Alrededor de la firma electrónica, Ivnosys ofrece otros servicios que permiten mejorar la productividad de los procesos corporativos mediante la automatización de procesos y la transformación digital, como son la gestión automática de notificaciones (IvNeos) o la interoperabilidad entre Administraciones Públicas (Agente SC).

2. Modelo de Prestación de Servicios

Los servicios de firma electrónica y centralización de certificados prestados por Ivnosys Soluciones pueden ofrecerse en 3 modalidades, de acuerdo con las necesidades y requerimientos del cliente:

- Software as a Service, en la nube.
- Cloud privado, con servicios virtuales dedicados para el cliente.
- On-Premise, implantando los servicios en las instalaciones del cliente.

3. Características del Modelo

El sistema de almacenamiento centralizado de claves permite la implantación y uso de la firma electrónica en las organizaciones de una forma segura y confiable. Mediante la emisión o importación de los certificados electrónicos en un sistema centralizado no se requerirá ningún tipo de hardware en los puestos de trabajo de los usuarios (smartcards y tarjeteros). El usuario podrá utilizar el certificado digital para firmar electrónicamente cualquier documento desde cualquier aplicación o página web de la misma forma que lo venía haciendo con los certificados tradicionales en software o tarjeta.

IvSign facilita la movilidad de los usuarios dentro de la organización manteniendo sus certificados accesibles.

Además, los certificados de persona jurídica o representación y los sellos electrónicos estarán sujetos a un control absoluto de su uso, de forma centralizada y sin necesidad de replicarlos en diferentes servidores y aplicaciones a lo largo de la organización.

4. Solución Tecnológica

La plataforma IvSign está compuesta por los siguientes módulos independientes, que ofrecen una solución integrada y global adaptada a las necesidades del cliente:

- **IvCKC**: Módulo base para la custodia segura y gestión centralizada de los certificados digitales, accesibles desde entornos Windows, sin adaptaciones mediante Key Controller. Basado en un módulo seguro de creación de firma (HSM), para la generación y uso de los certificados, garantizando el uso exclusivo de las claves por parte del firmante.
- **IvSign Mobile**: Aplicación móvil (compatible con sistemas iOS y Android) usable e intuitiva, que permite firmar con certificados centralizados en IvSign, así como acceder al registro de auditoría del uso de los certificados.
- **Portafirmas IvSign**: Plataforma web que permite la definición y ejecución de flujos de firma electrónica de documentos en base a usuarios, cargos y departamentos de la organización.
- **IvSignature**: Avanzado motor corporativo de firma electrónica basado en arquitectura REST/SOA para firma de documentos con certificados digitales X.509 (centralizados o locales) en todos los formados estándar como PAdES, XAdES, CAdES, Office, … con capacidades de sellado de tiempo y formatos de firma de larga duración entre otras características.
- **IvBioSignature**: Motor de firma biométrica integrable, que permitirá la captura y almacenamiento de los rasgos biométricos (presión, velocidad, tiempo del puntero en el aire, geolocalización) de la firma manuscrita en tabletas, dispositivos de escritorio, etc. Ideal para la digitalización total de las oficinas de registro de las Administraciones Públicas.
- Integración instantánea con aplicación PKI del PSC AC Camerfirma, para la emisión, custodia y control del ciclo de vida de los certificados digitales, con posibilidad de contratar una de Autoridad de Registro (RA) para la gestión delegada de emisión de certificados, evitando desplazamientos a puntos de registro para verificar la identidad de los titulares y aportar documentación.

5. Tipos de Certificados

Los Servicios de Centralización compatible con cualquier tipo de certificado para la realización de firmas avanzadas, tanto de persona física (ES00-ES11-ES12 / UE00) (corporativos o de representación) como de persona jurídica (ES08 / UE01) (Sellos electrónicos).

Ivnosys Soluciones cuenta con una alianza con AC Camerfirma para la emisión de certificados digitales centralizados a través de una Autoridad de Certificación Subordinada denominada IvSign CA, la cual estará disponible en el segundo semestre de 2018.

6. Servicios/Productos para AALL

Servicios dirigidos a la Administración Local:

- **IvSign**: centralización de certificados digitales y plataforma de firma electrónica.
- **IvNeos**: gestión de notificaciones electrónicas recibidas, para la monitorización automática de la existencia de notificaciones en las sedes electrónicas de diferentes organismos, incluyendo la Dirección Electrónica Habilitada y el Punto de Acceso General.

- **Agente SC**: consulta de servicios de intermediación de la plataforma Datos. Las AALL podrán ofrecer servicios a los ciudadanos libres de papeles y requisitos con consultas de servicios como el IRPF, Familia Numerosa, estar al corriente de pago o certificados del Registro Civil.
- **PLACSP**: complemento de gestión de contratos electrónicos integrado con la Plataforma de Contratación del Estado. Completo registro de contratos que permite cumplir con las obligaciones de información y transparencia de la Ley de Contratos del Sector Público.

7. Garantías y Servicios de Soporte

El mantenimiento del suministro ofrecido se ofrece durante todo el periodo de contratación. La política de mantenimiento de Ivnosys Soluciones es actualizar los sistemas SaaS de manera continua con nuevas funcionalidades del software, así como cualquier mantenimiento correctivo, perfectivo u otras mejoras que pudieran desarrollarse para el sistema con el fin de mantener la seguridad, estabilidad y rendimiento de los sistemas.

El soporte técnico de IVNOSYS comprende los siguientes servicios en el ámbito de los proyectos relacionados a continuación:

- Mantenimiento correctivo de la plataforma y productos que la componen.
- Soporte a los módulos de integración y clientes de firma.
- Servicio de atención a incidencias y consultas de segundo nivel de la solución.

Ivnosys ofrece un soporte estándar por correo electrónico mediante sistema de seguimiento de tickets en horario laboral nacional de lunes a viernes, exceptuando solamente las fiestas a nivel nacional.

Para ofrecer este servicio, Ivnosys cuenta con un centro de atención al usuario propio formado por un equipo de más de 15 personas.

8. Servicios de Valor Añadido

Ivnosys Soluciones tiene una amplia experiencia en consultoría y asesoría para la integración de sus soluciones con aplicaciones de terceros, pudiendo beneficiarse sus clientes de este Know-How.

Además, Ivnosys ha realizado proyectos relacionados con herramientas públicas como son @ firma, ACCEDA, Cl@ve, Inside, Port@firmas o ARCHIVE

9. Interoperabilidad con otras Instituciones/Organismos

Además de los productos Agente SC e IvNeos, que interactúan con servicios de la plataforma de intermediación Datos y con sedes de notificación electrónica como la DEH, Ivnosys se ha integrado con diferentes tipos de organismos y servicios públicos en sus proyectos y productos, como, por ejemplo, FACe, la Plataforma de Contratación del Sector Público o Entidades bancarias.

10. Clientes de Referencia

Durante el 2017, Ivnosys ha prestado sus servicios de forma directa en un total de 53 Ayuntamientos, 3 Diputaciones provinciales (Alicante, Almería y Castellón), en una Universidad Pública y en la Sociedad Española de Correos y Telégrafos. Por otro lado, Ivnosys posee un canal de partners /distribuidores de sus soluciones a través de los cuales se ha trabajado con otras muchas AALL.

Estos partners son:

Las AALL con las que hemos trabajo a lo largo del 2017 son:

Ajuntament D´Esplugues de Llobregat	Ayuntamiento de Castellón de la Plana
Ajuntament d´Ontinyent	Ayuntamiento de Chiva
Ajuntament d'Almassora	Ayuntamiento de Crevillent
Ajuntament de Benaguasil	Ayuntamiento de Cuenca
Ajuntament de Benetússer	Ayuntamiento de Deleitosa
Ajuntament de Carcaixent	Ayuntamiento de Denia
Ajuntament de Catarroja	Ayuntamiento de Guadalajara
Ajuntament de Cullera	Ayuntamiento de Logroño
Ajuntament de Gandía	Ayuntamiento de Lorca
Ajuntament de Godella	Ayuntamiento de Massanassa
Ajuntament de L´Eliana	Ayuntamiento de Meliana
Ajuntament de la Pobla de Vallbona	Ayuntamiento de Moncofa
Ajuntament de Manises	Ayuntamiento de Parla
Ajuntament de Paiporta	Ayuntamiento de Puçol
Ajuntament de Paterna	Ayuntamiento de Ribarroja del Túria
Ajuntament de Picanya	Ayuntamiento de Sagunto
Ajuntament de Sedaví	Ayuntamiento de Saucedilla
Ajuntament de Silla	Ayuntamiento de Sueca
Ajuntament de Tavernes de la Valldigna	Ayuntamiento de Torre Pacheco
Ajuntament de Teulada	Ayuntamiento de Tres Cantos
Ajuntament de Torrent	Ayuntamiento de Utiel
Ajuntament de Xàtiva	Ayuntamiento Molina del Segura
Ajuntament de Xeraco	Ayuntamiento Oropesa del Mar
Ajuntament Mollet del Vallés	Diputación Provincial de Alicante
Asociación Nuclear Ascó-Vandellós II, AIE	Diputación Provincial de Almería
Autoridad Portuaria de Valencia	Diputación Provincial de Castellón
Ayuntamiento de Alboraya	S.E CORREOS Y TELÉGRAFOS, S.A., S.M.E
Ayuntamiento de Alfafar	Sdad Estatal Loterías y Apuestas Estado,SME,S.A
Ayuntamiento de Almussafes	Sociedad Estatal de Correos y Telégrafos,S.A.
Ayuntamiento de Boadilla del Monte	Universidad Autónoma de Madrid

11. Acreditaciones / Certificaciones

Contamos con informe de auditoría de emisión de certificados, firma en servidor y registro remoto de identidad. Los informes han sido emitidos en formato eIDAS – Conformity Assesment Report (CAR) por Trust Conformity Assessment Body, S.L – (TCAB) durante su visita de acompañamiento para la acreditación y utilizados en el trámite de notificación al MINETAD para inclusión en las listas TSL.

Ivnosys Soluciones dispone de las siguientes acreditaciones:

- Norma UNE-ISO/IEC 27001:2014 de Sistema de Gestión de Seguridad de la Información certificado por AENOR Internacional S.A.U. con el siguiente alcance: "Los sistemas de información que soportan los procesos de instalación y operación de los siguientes servicios de confianza en modalidad cloud:

  i. La recepción de notificaciones electrónicas de forma automática.

  ii. Las comunicaciones electrónicas entre organizaciones con evidencias electrónicas de las diferentes transacciones.

  iii. La interoperabilidad entre administraciones públicas.

  iv. La conexión con entidades financieras para descargar de forma automática la información bancaria de múltiples cuentas y permitir la gestión contable de los movimientos integrado con la aplicación de contabilidad.

  v. La gestión centralizada de claves criptográficas (certificados digitales) y servicios web para comunicaciones y evidencias electrónicas, y emisión y gestión de sellos de tiempo.

  vi. Gestión del ciclo de vida de los certificados digitales (emisión, validación, mantenimiento y revocación).

  De acuerdo con la declaración de aplicabilidad vigente."

- Norma UNE-EN-ISO9001:2015 de Sistema de Gestión de la Calidad por Certificación y Confianza Cámara, S.L.U., con el siguiente alcance: "Actividades de Diseño, desarrollo e implementación de software; Soporte al usuario y mantenimiento correctivo, perfectivo y evolutivo de software"

12. Prácticas y Políticas de Certificación

Se podrán consultar en la dirección https://policy.ivsign.net.

Más información en https://www.ivnosys.com.

4.3.7. UANATACA

AUTORIDAD CERTIFICADORA:

UANATACA, S.A.

1. **Información General**

   Uanataca es un Prestador de Servicios de Confianza perteneciente al grupo **Bit4id** nacido con la vocación de generar confianza en las transacciones electrónicas mediante la creación de Identidades Digitales y servicios asociados para el uso sencillo e interoperable de la firma digital, la autenticación y el cifrado de las comunicaciones.

2. **Modelo de Prestación de Servicios**

   Uanataca ofrece en la actualidad los siguientes Servicios:

   - Servicio de expedición de certificados electrónicos cualificados de firma electrónica.
   - Servicio de expedición de certificados electrónicos cualificados de sello electrónico.
   - Servicio de expedición de sellos electrónicos cualificados de tiempo.
   - Servicio de Autoridad de Registro para la emisión autónoma de certificados electrónicos.
   - Servicio de Custodia centralizada de claves de certificados para su uso desde dispositivos móviles, PC's y aplicaciones web.
   - Servicio de Firma Masiva.
   - Servicio de Firma Longeva.
   - Servicio de validación.
   - Servicio de Consultoría y gestión de proceso de acreditación para la creación de PKI propia.

3. **Características del Modelo**

   La innovación tecnológica que ha supuesto internet trae consigo enormes beneficios, pero también riesgos de seguridad, como ataques cibernéticos, malware, etc., que facilitan la suplantación de la identidad, exponiéndose a grandes riesgos y por ende dificultando el progreso y beneficios que proporcionan las tecnologías. Estas vulnerabilidades crean desconfianza en los ciudadanos, empresas e instituciones cuando tienen que realizar transacciones online.

Uanataca ha sido creada sobre la premisa de generar confianza, dotando de certificados digitales a personas y transacciones, con el fin de garantizar la identidad digital para la firma digital, la autenticación y el cifrado de las comunicaciones, asegurando el activo más valioso; la información, y para combatir las amenazas de ataques y malware que constantemente causan estragos a nivel mundial en diferentes realidades.

Para la erogación de servicios de emisión, custodia y uso de certificados digitales, la Autoridad de Certificación Uanataca dispone de una suite completa de funcionalidades que permiten la implantación inmediata de infraestructuras de clave pública sin una inversión inicial, escalable y bajo consumo.

4. Solución Tecnológica

La infraestructura del sistema está almacenada en un Centro de Procesamiento de Datos (CPD) de última tecnología ubicado en Europa.

Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.
- Disponibilidad del 99,99%.

Uanataca dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos

5. Tipos de Certificados

A continuación, se detallan los tipos de certificados emitidos por UANATACA, la descripción detallada de los perfiles de estos se encuentra en el apartado 12 y en la declaración de las prácticas de certificación:

Certificados cualificados de PERSONA FÍSICA. (UE00)

Los certificados cualificados de Persona Física se diferencian en 3 variantes:

1. Persona física ciudadano.(ES00 / UE00)
2. Persona física perteneciente a empresa. (ES11-ES12 / UE00)
3. Persona física colegiado. (ES11 / UE00)

Certificados cualificados de REPRESENTANTE. (UE00)

Los certificados cualificados de Representante disponen de los siguientes perfiles:

1. Persona física representante. (ES11 / UE00)
2. Persona física representante de persona jurídica. (ES11 / UE00)
3. Persona física representante de entidad sin personalidad jurídica. (ES12 / UE00)

Certificados cualificados de EMPLEADO PÚBLICO. (ES05 / UE00)

Certificado cualificado de Empleado Público de Nivel Medio

Certificado electrónico de autenticación Empleado Público Nivel Alto

Certificado cualificado de firma de Empleado Público de Nivel Alto

Certificados cualificados de SELLO. (ES08 / UE01)

Los certificados cualificados de SELLO incluyen los siguientes perfiles:

1. Sello de órgano, para administraciones públicas.
2. Sello de empresa, para todo tipo de empresas, entidades u organizaciones.

Certificados de SELLO DE TIEMPO. (ES10 / UE01)

Certificado de sello cualificado de tiempo electrónico

6. Servicios/Productos para AALL

- Servicio de PKI.
- Servicio de Autoridad de Registro para la emisión autónoma de certificados electrónicos.
- Servicio de Custodia centralizada de claves de certificados para su uso desde dispositivos móviles, PC's y aplicaciones web.
- Servicio de Firma electrónica masiva.
- Servicio de Firma electrónica longeva masiva o atendida.
- Servicio de emisión de sellos de tiempo.
- Servicio de verificación y validación de forma masiva de documentos firmados electrónicamente.

7. Garantías y Servicios de Soporte

A continuación, se indican las características y niveles del servicio en función del impacto:

- Crítico: Inhabilitación total del servicio para poder desarrollar las funciones objeto de la oferta.
  - » Tiempo de respuesta: 3 hora laborables.
  - » Tiempo de restauración: 9 horas laborables.
  - » Tiempo de solución definitiva: 1 semana laborable.

- Mayor: Funcionamiento deficiente del servicio objeto de la oferta, que genere problemas o inconvenientes para la prestación de uno o más servicios del cliente.
  - » Tiempo de respuesta: 6 horas laborables.
  - » Tiempo de restauración: 16 horas laborables.
  - » Tiempo de solución definitiva: 2 semanas laborables.

El soporte se realiza mediante comunicaciones por email, teléfono y otros medios de comunicación acordados.

Este SLA garantiza la continuidad de todos aquellos servicios dentro del alcance con un nivel de disponibilidad mayor de **99,9 %.**

8. Servicios de Valor Añadido

- Poner a disposición los servicios de Uanataca S.A. para su distribución a través de distribuidores en diferentes países.
- Uanataca, S.A. Prestador de Servicios de Confianza pertenece al grupo Bit4id, con más de 15 años de experiencia desarrollando y fabricando tecnología PKI.
- APP móvil Uanataca para el uso de certificados tanto para firma como para autenticación en las sedes electrónicas de las AAPP con las siguientes características funcionales:
  - » Compatible con certificados digitales almacenados en Uanataca SignCloud, DigitalDNA Key y miniLector BLUE. Blue.
  - » Navegación libre por internet
  - » Autenticación fuerte (client SSL) en aplicaciones web
  - » Firma electrónica PAdES, CAdES, XAdES:
    - – Archivos en local
    - – Autofirma @firma
    - – 4identity
  - » Validación de firmas electrónicas PAdES, CAdES, XAdES
  - » Informes de validación de firmas electrónicas
  - » Disponible en App Store y Play Store
  - » Accesos directos personalizables
  - » Gestión del ciclo de vida del certificado digital (suspensión, revocación, reactivación)
  - » Renovación del certificado digital

9. Interoperabilidad con otras Instituciones/Organismos

Los certificados electrónicos de UANATACA permiten su utilización en las sedes electrónicas de diferentes Instituciones u organismos de la Administración Central y Autonómica, a destacar por ejemplo las siguientes:

PLATAFORMAS / SEDES ELECTRÓNICAS		
ADMINISTRACIÓN / ORGANISMO	TIPO	SEDE ELECTRÓNICA
@firma - Plataforma de validación de firma electrónica	Central	https://administracionelectronica.gob.es/ctt/afirma#.WfxHUGjWyHt
Administració Oberta de Catalunya (AOC)	CCAA	https://www.aoc.cat/
Adminsitración.gob.es - Punto de acceso general	Central	https://sede.administracion.gob.es/PAG_Sede/HomeSede.html
Agencia Española de Protección de Datos (AEPD)	Central	https://www.agpd.es/
Agencia Tributaria	Central	http://www.agenciatributaria.es/
Agencia Tributaria de Catalunya	CCAA	http://atc.gencat.cat/ca/inici/
Boletín Oficial del Estado (BOE)	Central	http://www.boe.es/
CatSalut. Servei Català de la Salut	CCAA	https://lamevasalut.gencat.cat/web/guest/pre-login-cps
Centro para el Desarrollo Tecnológico Industrial (CDTI)	Central	https://www.cdti.es/
Comisión Nacional de los Mercados y la Competencia (CNMC)	Central	https://sede.cnmc.gob.es/
Dirección general de tráfico (DGT)	Central	http://www.dgt.es/es/
Dirección general del Catastro	Central	http://www.catastro.meh.es/
Dirección General del Tesoro y Política Financiera	Central	https://www.tesoropublico.gob.es/carga_contenido.aspx?sec=10&tipo_sec=1
Fondo Español de Garantía Agraria (FEGA)	Central	https://www.sede.fega.gob.es/
Generalitat de Catalunya	CCAA	http://web.gencat.cat/ca/inici/
Gobierno de Navarra	CCAA	http://www.navarra.es/
ICEX España Exportación e Inversiones	Central	https://www.icex.es/icex/es/index.html
Instituto de Contabilidad y Auditoría de Cuentas (ICAC)	Central	http://www.icac.meh.es/
Ministerio de Agricultura, Alimentación y Medio Ambiente	Central	https://sede.mapama.gob.es/portal/site/se
Ministerio de Asuntos Exteriores y de Cooperación	Central	http://www.exteriores.gob.es/
Ministerio de defensa	Central	https://sede.defensa.gob.es/acceda/
Ministerio de Economía, Industria y Competitividad	Central	https://sede.mineco.gob.es/

Ministerio de Educación, Cultura y Deporte	Central	https://sede.educacion.gob.es/portada.html
Ministerio de Empleo y Seguridad Social	Central	http://www.empleo.gob.es/
Ministerio de Energía, Turismo y Agenda Digital (MINETAD)	Central	https://sede.minetur.gob.es/es-es/Paginas/Index.aspx
Ministerio de Fomento	Central	https://sede.fomento.gob.es/sede_electronica/lang_castellano/
Ministerio de Hacienda - Sede central y múltiples sedes.	Central	https://sedeminhap.gob.es/es-ES/Paginas/default.aspx
Ministerio de Hacienda y Administraciones Públicas	Central	http://www.minhafp.gob.es/es-ES/Paginas/Home.aspx
Ministerio de Justicia	Central	http://www.mjusticia.gob.es/
Ministerio de la Presidencia	Central	https://sedempr.gob.es/es
Ministerio de Sanidad, Servicios Sociales e Igualdad	Central	https://sede.msssi.gob.es/
Ministerio del Interior	Central	https://sede.mir.gob.es/index2.html
Red.es	Central	http://www.red.es/redes/
Servei Català de Trànsit	CCAA	http://transit.gencat.cat/ca/inici/
Servicio de Notificaciones Electrónicas - Notificaciones.060.es	Central	http://notificaciones.060.es/
Servicio Público de Empleo Estatal (SEPE)	Central	https://sede.sepe.gob.es/portalSede/

Asimismo, Uanataca está presente en multitud de Instituciones u organismos pertenecientes a la administración local, como por ejemplo ayuntamientos, diputaciones y otros órganos que dan soporte a éstas.

10. Clientes de Referencia

Algunos de nuestros clientes:

- Gestores Administrativos de Catalunya.
- Consejo General de Colegios de Médicos de España
- Animsa, Ayuntamiento de Navarra.
- Bit4id, S.A.C.

11. Acreditaciones / Certificaciones

Certificado de Prestadores de Servicio de Confianza. Reglamento UE 910/2014 eIDAS.

12. Prácticas y Políticas de Certificación

Las Prácticas y Políticas de Certificación de UANATACA, S.A., se encuentran disponibles en www.uanataca.com.

- Políticas: https://www.uanataca.com/es/politicas.html
- Declaración de Prácticas de Certificación: http://www.uanataca.com/public/pki/dpc-es/

PERFILES DE CERTIFICADOS

PERSONA FÍSICA (ES00 / UE00)

- Certificado cualificado de Persona Física en software.
- Certificado cualificado de firma de Persona Física en QSCD.
- Certificado cualificado de Persona Física en QSCD.
- Certificado cualificado de Persona Física en HSM centralizado.
- Certificado cualificado de Persona Física Representante en software. (ES11 / UE00)
- Certificado cualificado de Persona Física de firma Representante en QSCD. (ES11 / UE00)
- Certificado cualificado de Persona Física Representante de Persona Jurídica ante las administraciones en software. (ES11 / UE00)
- Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en QSCD. (ES11 / UE00)
- Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en HSM centralizado. (ES11 / UE00)
- Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en software. (ES12 / UE00)
- Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en QSCD. (ES12 / UE00)
- Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en HSM centralizado. (ES12 / UE00)

SELLO DE ÓRGANO (AAPP) (ES08 / UE01)

- Certificado cualificado de Sello Electrónico de Nivel Medio APE.
- Certificado cualificado de Sello Electrónico de Nivel Alto APE.

EMPLEADO PÚBLICO (ES05 / UE00)

- Certificado cualificado de Empleado Público de Nivel Medio.
- Certificado cualificado de autenticación de Empleado Público de Nivel Alto.
- Certificado cualificado de firma de Empleado Público de Nivel Alto.

SELLO DE EMPRESA (ES08 / UE01)

- Certificado cualificado de Sello Electrónico en software.
- Certificado cualificado de Sello Electrónico en QSCD.
- Certificado cualificado de Sello Electrónico en HSM centralizado.

SELLO DE TIEMPO (ES10 / UE01)

Certificado de sello cualificado de tiempo electrónico.

5 Plan de concienciación

La Identidad Digital mediante el uso de certificados electrónicos es una de las necesidades básicas que se debe de cubrir en una sociedad si se quiere hacer un despliegue integral de la administración electrónica y dar cumplimiento a la normativa vigente y que la ciudadanía apueste por ello.

Sin embargo, cada vez se complica más. En este momento tenemos que tener en cuenta el uso de distintos dispositivos y plataformas, móvil y física y tomar conciencia de todas ellas.

El correcto y fácil uso de los certificados electrónicos, es una de las asignaturas pendientes, siendo uno de los aspectos fundamentales que debe tener en cuenta todas las personas para tramitar de forma electrónica. Concienciar a la ciudadanía y a las empresas, es una tarea fundamental.

Desde las administraciones, hay que concienciar y establecer una **cultura digital** práctica, y adaptada a las gestiones que se llevan a cabo diariamente con las personas que utilizan los servicios públicos.

Formación vs Concienciación

Hay que diferenciar entre concienciar y formar.

Concienciar: crear cultura digital. Es necesario concienciar a toda la ciudadanía en el uso de medios digitales, la seguridad y las implicaciones y riesgos de no asumirla.

Formar: la formación es continua y no acaba nunca. Se debe involucrar a todos/as, pero a diferencia de la concienciación, los cursos deben ser dirigidos.

Es por ello que en este documento se trabajan dos apartados, por un lado el **Plan de Concienciación** y por otro el **Plan de Formación**.

6 Plan de formación externo (ciudadanía, empresas y emprendedores/as)

El uso del certificado electrónico y la firma de documentos electrónicos forma parte ya de nuestro día a día en nuestras gestiones con las administraciones públicas y es importante conocer los pasos que debemos seguir para potenciar el uso de la administración electrónica.

Parece oportuno después de todos los conceptos analizados en este documento crear un test de valoración de los conocimientos adquiridos para así asegurar la aplicación y el uso de los certificados y la firma en nuestros trámites electrónicos. Y se hace la siguiente propuesta:

- **Destinatarios: Ciudadanía y empresas.**
- **Duración:**
  - » **Ciudanía: 5 horas.**
  - » **Empresas: 10 horas.**

Identificación y firma digital

TEMARIO

A. Criptografía.

1. ¿Qué es la criptografía?
2. Historia de la criptografía.
3. Criptografía simétrica.
4. Criptografía asimétrica.

B. Certificados digitales.

1. ¿Qué es un certificado digital?
2. ¿Cómo consigo mi certificado digital de usuario?
3. ¿El DNI electrónico?
4. Tipo de certificados.
   - 4.1. Certificado de persona física.
   - 4.2. Certificado de sello electrónico.
   - 4.3. Certificado de representante de persona jurídica.
   - 4.4. Certificado de autenticación de sitio web.
   - 4.5. Certificado de servidor seguro.

5. Soporte de los certificados digitales.
   5.1. Hardware.
   5.2. Software.
   5.3. Nube.
6. ¿Dónde se instalan los certificados digitales?
7. ¿Caduca mi certificado digital?
8. Verificar certificados.
9. Validación de un certificado.
10. Ciclo de vida de un certificado.
11. ¿Para qué sirve un certificado digital?
    11.1. Autenticar
    11.2. Firmar electrónicamente.
    11.3. Cifrar datos.

C. prestadores de servicios electrónicos de confianza.

1. Prestadores de servicios electrónicos de confianza.
   1.1. Principales componentes de un prestador de servicios electrónicos de confianza.
   1.2. Funcionamiento básico de los prestadores de servicios electrónicos de confianza.
   1.3. Prestadores de servicios electrónicos de confianza “Generalistas”.
   1.4. Prestadores de servicios electrónicos de confianza “nacionales”.

D. Firma electrónica.

1. ¿Qué es la firma electrónica?
2. ¿Qué validez tiene la firma electrónica?
3. Tipos de firma.
   3.1. Firma electrónica.
   3.2. Firma electrónica avanzada.
   3.3. Firma electrónica cualificada.
4. Dispositivos cualificados de creación de firma.
5. Los códigos HASH
6. ¿Cómo funciona un sistema de firma electrónica?
7. Validación de firmas electrónicas.

8. Formatos de firma electrónica.
    8.1. CAdES
    8.2. XAdES
    8.3. PAdES
    8.4. OOXML, ODF, otros
9. Firmas longevas.
10. Marca de tiempo/sello de tiempo.

E. Firma biométrica.

F. IDENTIDAD E IDENTFICACIÓN.

1. La identidad digital
2. La identificación electrónica
3. Sistema Cl@ve
4. Identificación de la ciudadanía
    4.1. El DNI Electrónico
    4.2. Certificados electrónicos
    4.3. Sistemas de claves concertadas
5. Identificación de las administraciones públicas
    5.1. Identificación de las sedes
    5.2. Identificación mediante sello electrónico.
    5.3. Código Seguro de Verificación o CSV

G. Diferencia entre indentificación y firma

H. Aplicación práctica.

1. Ejercicio práctico con alguna herramienta de firma.
    1.1. Ejemplo: https://www.xolido.com/lang/xolidosign/xolidosigndesktop/
    1.2. Ejemplo: https://sedeaplicaciones.minetur.gob.es/ecofirma/
    1.3. Ejemplo: https://valide.redsara.es/valide/?

TOMO III

Servicios de Certificación para las AALL

GUÍA DIDÁCTICA

El uso del certificado electrónico y la firma de documentos electrónicos forma parte ya de nuestro día a día en nuestras instituciones y es importante conocer los pasos que debemos seguir para potenciar el uso de la administración electrónica.

Parece oportuno después de todos los conceptos analizados en este documento crear una propuesta de temas en forma de test de valoración de los conocimientos adquiridos para así asegurar la aplicación y el uso de los certificados y la firma en nuestras administraciones públicas.

Al mismo tiempo resultará útil tener una relación de preguntas frecuentes que nos puedan resolver cualquier duda que surja en cualquier proceso de gestión o necesidad para relacionarse de forma electrónica con cualquier organismo o institución que lo requiera.

1 Propuesta temas para ejercicios de refuerzo de conocimientos según destinatarios

Se hace la siguiente propuesta según perfil de los destinatarios:

1.1. PERSONAL ADSCRITO A LA FUNCION PÚBLICA

- **Destinatarios**: Personal de las Administraciones Públicas.
- **Duración:** 10 horas

IDENTIDAD DIGITAL Y FIRMA ELECTRÓNICA ADMINISTRACIONES PÚBLICAS.

A. Marco legal.

1. Ley Orgánica 4/2015, de 30 de marzo de Protección de la Seguridad Ciudadana.
2. Ley 59/2003, de 19 de diciembre de Firma Electrónica.
3. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la Expedición del Documento Nacional de Identidad y sus Certificados de Firma Electrónica.
4. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
5. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

B. Reglamento (UE) N.º 910/2014 sobre identificación electrónica y servicios de confianza (EIDAS).

1. Identificación electrónica.
2. Servicios de confianza.
3. Responsabilidad de los prestadores de servicios.
4. Firma electrónica remota.
5. Sello electrónico.
6. Autenticación de sitios web.
7. Terceros de confianza.

C. Caracteristicas y clases de firma electrónica.

D. Certificado electrónico.

E. Prestadores de servicios de confianza.

F. Firma biométrica.

G. Identidad y firma de ciudadano en el sector público.

1. Sistemas admitidos por la Administración General del Estado y su imposición al resto de administraciones.
2. Niveles de seguridad de la firma electrónica. Relación entre firma y Esquema Nacional de Seguridad.
3. Usos obligatorios de la firma.
4. Tipos de firma electrónica.
    - PIM.
    - Clave/Contraseña.
    - Firma digitalizada.
    - Firma digital.
5. Firma e Identificación en la nube; sistema CL@VE.
    - Ámbito de aplicación.
    - Registro de usuarios.
    - Modalidades de identificación.
    - Firma de documentos electrónicos.
    - Punto de acceso al sistema CL@ve.
    - Adhesión al sistema CL@ve.
    - Costes de CL@ve.
    - Nivel de seguridad requerido.

H. Identidad y firma de la propia administración.

- Sello electrónico.
- Código seguro de verificación.

I. Firma de empleados públicos.

J. Política de firma

1.2. CIUDADANÍA Y EMPRESAS

- Destinatarios: Ciudadanía y empresas.
- Duración:
  - » **Ciudadanía:** 5 horas.
  - » **Empresas:** 10 horas.

IDENTIFICACIÓN Y FIRMA DIGITAL

TEMARIO

I. Criptografía.

1. ¿Qué es la criptografía?
2. Historia de la criptografía.
3. Criptografía simétrica.
4. Criptografía asimétrica.

J. Certificados digitales.

1. ¿Qué es un certificado digital?
2. ¿Cómo consigo mi certificado digital de usuario?
3. ¿El DNI electrónico?
4. Tipo de certificados.
   - 4.1. Certificado de persona física.
   - 4.2. Certificado de sello electrónico.
   - 4.3. Certificado de representante de persona jurídica.
   - 4.4. Certificado de autenticación de sitio web.
   - 4.5. Certificado de servidor seguro.
5. Soporte de los certificados digitales.
   - 5.1. Hardware.
   - 5.2. Software.
   - 5.3. Nube.
6. ¿Dónde se instalan los certificados digitales?
7. ¿Caduca mi certificado digital?

8. Verificar certificados.
9. Validación de un certificado.
10. Ciclo de vida de un certificado.
11. ¿Para qué sirve un certificado digital?
    11.1. Autenticar
    11.2. Firmar electrónicamente.
    11.3. Cifrar datos.

K. prestadores de servicios electrónicos de confianza.

2. Prestadores de servicios electrónicos de confianza.
    2.5. Principales componentes de un prestador de servicios electrónicos de confianza.
    2.6. Funcionamiento básico de los prestadores de servicios electrónicos de confianza.
    2.7. Prestadores de servicios electrónicos de confianza “Generalistas”.
    2.8. Prestadores de servicios electrónicos de confianza “nacionales”.

L. Firma electrónica.

1. ¿Qué es la firma electrónica?
2. ¿Qué validez tiene la firma electrónica?
3. Tipos de firma.
    3.1. Firma electrónica.
    3.2. Firma electrónica avanzada.
    3.3. Firma electrónica cualificada.
4. Dispositivos cualificados de creación de firma.
5. Los códigos HASH
6. ¿Cómo funciona un sistema de firma electrónica?
7. Validación de firmas electrónicas.
8. Formatos de firma electrónica.
    8.1. CAdES
    8.2. XAdES
    8.3. PAdES
    8.4. OOXML, ODF, otros
9. Firmas longevas.
10. Marca de tiempo/sello de tiempo.

M. Firma biométrica.

N. Identidad e identificación.

1. La identidad digital
2. La identificación electrónica
3. Sistema Cl@ve
4. Identificación de la ciudadanía
   - 4.1. El DNI Electrónico
   - 4.2. Certificados electrónicos
   - 4.3. Sistemas de claves concertadas
5. Identificación de las administraciones públicas
   - 5.1. Identificación de las sedes
   - 5.2. Identificación mediante sello electrónico.
   - 5.3. Código Seguro de Verificación o CSV

O. Diferencia entre indentificación y firma.

P. Aplicación práctica.

1. Ejercicio práctico con alguna herramienta de firma.
   - 1.4. Ejemplo: https://www.xolido.com/lang/xolidosign/xolidosigndesktop/
   - 1.5. Ejemplo: https://sedeaplicaciones.minetur.gob.es/ecofirma/
   - 1.6. Ejemplo: https://valide.redsara.es/valide/?

2 Preguntas Frecuentes

A continuación presentamos un conjunto de respuestas a problemas y dudas más habituales en el ámbito del uso de los sistemas de identidad digital, estructurada en varios apartados agrupados por temática y tratando de recoger la más amplía casuística del sector:

PREGUNTAS GENERALES

► ¿Qué es la Firma Digital?

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

La firma digital no implica que el mensaje está cifrado, esto es, un mensaje firmado será legible en función de que está o no cifrado.

El firmante generará mediante una función, un 'resumen' o huella digital del mensaje. Este resumen o huella digital la cifrará con su clave privada y el resultado es lo que se denomina firma digital, que enviará adjunta al mensaje original.

Cualquier receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación porque podrá generar el mismo resumen o misma huella digital aplicando la misma función al mensaje. Además podrá comprobar su autoría, descifrando la firma digital con la clave pública del firmante, lo que dará como resultado de nuevo el resumen o huella digital del mensaje.

► ¿Existe un portal en el que pueda encontrar información básica acerca de la firma electrónica?

http://firmaelectronica.gob.es/

► ¿Qué tipos de firma electrónica existen?

- Firma electrónica: Permite identificar a un firmante, por ejemplo, mediante usuario y contraseña. Es la más básica y la que menos seguridad proporciona al usuario
- Firma electrónica avanzada: Identifica al firmante y detecta cualquier cambio ulterior de los datos firmados.
- Firma electrónica reconocida: Es la única que puede ser considerada como equivalente legal a la firma manuscrita. Solamente puede ser emitida por una Autoridad de Certificación que comprueba fehacientemente la identidad del certificado y se genera en un dispositivo seguro de creación de firma.

El Reglamento (UE) 910/2014 define tres tipos de firma electrónica:

- «firma electrónica», los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- «firma electrónica avanzada», la firma electrónica que cumple los siguientes requisitos:
  - » estar vinculada al firmante de manera única.
  - » permitir la identificación del firmante.
  - » haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
  - » estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
- «firma electrónica cualificada», una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

Además existen otro tipo de firmas electrónicas como las firmas mediante Código de Verificación Seguro (CSV) y las firmas biométricas.

► ¿Cuáles son los principales tipos de firmas electrónicas cualificadas, mediante certificado, según el tipo de documento o información que firmemos?

Formatos de documentos con firma nativa:

- Documentos PDF – Firma PADES
- Documentos OOXML de MicrosoftOffice – Firma OOXML
- Documentos ODF de LibreOffice u OpenOffice – Firma ODF
- Facturas electrónicas – FacturaE
- Documento XML – XADES

Además, se podrá firmar cualquier tipo de documento con los siguientes formatos de firma:

- XADES
- CADES

► ¿Cómo puedo verificar un documento firmado electrónicamente mediante certificado cualificado?

Podemos comprobar la validez de la firma de un documento y sus firmantes en VALIDe [https://valide.redsara.es].

Si es un documento firmado con CSV, debes acudir a la URL de verificación impresa y seguir las instrucciones. En todo caso, deberás poder descargarte el documento original y la firma electrónica que respaldan al documento CSV para poder verificar la firma en VALIDe.

Ver pregunta frecuente ¿Cómo se valida un documento con firma CSV?

¿Qué significa Integridad?

La integridad es un servicio de seguridad que permite comprobar que no se ha producido manipulación alguna en el mensaje original. La integridad de un mensaje se obtiene adjuntando al mismo, otro conjunto de datos de comprobación de la integridad.

Una función hash que genere una huella digital asociada a un mensaje es un mecanismo que aporta esta característica.

¿Qué significa No Repudio o irrenunciabilidad?

El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Existirán por tanto dos posibilidades:

- No repudio en origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío.
- No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

La posesión de un documento y su firma digital asociada será prueba efectiva del contenido y del autor del documento.

¿Qué significa Autenticación?

La autenticación es un servicio de seguridad que permite verificar la identidad.

Una firma digital es un mecanismo que asegura la identidad del firmante del mensaje y por tanto su autenticidad.

¿Qué significa Confidencialidad?

La confidencialidad es un servicio de seguridad que permite asegurar que un mensaje no es entendible por alguien a quien no va destinado.

El cifrado es un mecanismo que aporta esta característica a un mensaje.

¿Qué es la Criptografía?

La criptografía (kryptos = oculto + graphe = escritura) es el arte de escribir en clave o de forma enigmática. En principio se puede expresar como el conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido. En la actualidad estas técnicas permiten además, asegurar que el mensaje no se ha modificado, reconocer al emisor del mensaje, probar la emisión y recepción del mensaje, etc.

¿Qué es la Criptografía de Clave Pública?

La criptografía de clave pública o asimétrica está basada en el uso de un par de claves que cumplen, entre otros requisitos, que lo que somos capaces de cifrar con una de ellas, somos capaces de descifrarlo con la otra y sólo con ella.

Una de las claves solo está en poder de la persona propietaria, que debe conservarla de forma segura, y se denomina clave privada.

La otra clave es publicada para que la conozcan todas las personas que quieran comunicarse de modo seguro con la persona propietaria mencionado, a esta última se la denomina clave pública.

¿Qué es la Encriptación o Cifrado?

La encriptación o cifrado es un mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario. De modo inverso, la desencriptación o descifrado permitirá hacer legible un mensaje que estaba cifrado.

Usando criptografía de clave pública el emisor del mensaje cifrará el mensaje aplicando la clave pública del destinatario. Será por tanto el destinatario, el único que podrá descifrar el mensaje aplicando su clave privada.

¿Qué es una Huella Digital?

Una huella digital es un conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado.

La huella digital o resumen de un mensaje se obtiene aplicando una función, denominada hash, a ese mensaje, esto da como resultado un conjunto de datos singular de longitud fija.

Una función hash tiene entre otras las siguientes propiedades:

Dos mensajes iguales producen huellas digitales iguales.

Dos mensajes parecidos producen huellas digitales completamente diferentes.

Dos huellas digitales idénticas pueden ser el resultado de dos mensajes iguales o de dos mensajes completamente diferentes.

Una función hash es irreversible, no se puede deshacer, por tanto su comprobación se realizará aplicando de nuevo la misma función hash al mensaje.

¿Qué es un Certificado?

Un certificado es un documento emitido y firmado por la Autoridad de Certificación que identifica una clave pública con la persona propietaria. Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

Diferencias entre .pfx .p12 .cer y .crt.

Básicamente:

- .pfx y .p12: copia de seguridad o exportación con clave privada de un certificado. Al importarlos pueden ser utilizados para firmar.
- .cer y .crt: copia de seguridad o exportación de clave pública de certificados. No contienen la clave privada por lo que si los importamos no pueden ser utilizados para firmar.

¿Qué es y para qué sirve un Certificado Raíz?

Un certificado raíz es un certificado emitido por la Autoridad de Certificación (AC) para sí misma. En este certificado consta la clave pública de la Autoridad de Certificación. Es el certificado origen de la cadena de confianza.

¿Qué es una Autoridad de Certificación?

Una Autoridad de Certificación (AC, en inglés CA) es una entidad de confianza del emisor y del receptor del mensaje. Esta confianza de ambos en una 'tercera parte confiable' permite que cualquiera de los dos confíe a su vez en los documentos firmados por la Autoridad de Certificación, en particular, en los documentos que identifican cada clave pública con la persona propietaria correspondiente y se denominan certificados.

¿Qué es una Autoridad de Registro?

Una Autoridad de Registro (AR, en inglés RA) es una entidad que identifica de forma inequívoca al solicitante de un certificado. La Autoridad de Registro suministra a la Autoridad de Certificación los datos verificados del solicitante a fin de que la Autoridad de Certificación emita el correspondiente certificado.

¿Qué es la Declaración de Prácticas de Certificación?

La Declaración de Prácticas de Certificación es un documento elaborado por una Autoridad de Certificación que recoge o regula la prestación de los servicios de certificación por parte de dicha Autoridad de Certificación en su condición de Prestador de Servicios de Certificación.

Se regula, entre otras cosas, la gestión de los Datos de creación y verificación de Firma y de los Certificados, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los Certificados.

¿Por qué los Certificados Electrónicos tienen fecha de caducidad?

Los procesos criptográficos de firma electrónica basan su robustez en el tamaño de los módulos de las claves asimétricas. A medida que la capacidad de computación de los ordenadores va aumentando es necesario incrementar el tamaño de las claves para evitar que éstas puedan ser comprometidas.

Al establecer un periodo de validez de los certificados se facilita el procedimiento de migración de claves con una determinada longitud a otras de mayor tamaño.

La Ley 59/2003 de firma electrónica establece que dicho periodo de validez para los certificados reconocidos no podrá ser superior a cuatro años.

¿Qué significa revocar un Certificado?

Revocar un certificado es anular su validez antes de la fecha de caducidad que consta en el mismo. La revocación puede ser solicitada en cualquier momento, y en especial, cuando el titular crea que sus claves privadas son conocidas por otros.

La revocación tiene efectos a partir de la fecha efectiva de revocación que consta junto al número de serie del certificado revocado en un documento firmado y publicado por la Autoridad de Certificación.

Cualquier firma digital realizada con la clave privada asociada a ese certificado con posterioridad a la fecha efectiva de revocación no tendrá validez.

¿Qué pasos he de seguir para revocar un certificado?

Debe ponerse en contacto con la Autoridad de Certificación que ha emitido el certificado que se desea revocar. Debe ponerse en contacto lo antes posible si ha extraviado el certificado o sospecha que ha podido ser accedido por terceros sin autorización.

Cada Autoridad de Certificación define su propio procedimiento para la revocación de un certificado, por lo que debe consultarlo desde su página web o a través del soporte telefónico.

Por ejemplo, para solicitar la revocación del Certificado de Persona Física expedido por la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda se procederá de la siguiente manera:

- Si el titular del certificado está en posesión del mismo, la revocación se efectuará a través de Internet.
- Si el titular del certificado no dispone del mismo por extravío, pérdida o robo, deberá personarse en una Oficina de Acreditación.
- En cualquier caso, podrá utilizar el Servicio de revocación telefónica.

¿Se puede modificar la dirección de correo electrónico asociada al certificado?

No, la dirección de correo electrónico que aparece en el certificado no puede ser modificada. Si es preciso modificarla se tendrá que solicitar un certificado nuevo.

¿Se puede reactivar un certificado revocado?

No, un certificado que ha sido revocado por cualquier motivo no puede ser activado de nuevo. Hay que solicitar un certificado nuevo.

¿Qué son los OIDs de los certificados?

El OID o identificador de política es una referencia que se incluye en el Certificado al objeto de determinar un conjunto de reglas que indican la aplicabilidad de un determinado tipo de Certificado a la Comunidad Electrónica y/o clase de aplicación con requisitos de seguridad comunes. Siempre se incluye en el certificado pero no siempre está visible dependiendo del tipo del certificado.

Ejemplos:

AC FNMT Usuarios

- Persona Física (OID = 1.3.6.1.4.1.5734.3.10.1)

AC Representación

- Certificado de representante para administradores únicos y solidarios (OID 1.3.6.1.4.1.5734.3.11.1)
- Certificado de representante de persona jurídica (OID 1.3.6.1.4.1.5734.3.11.2)
- Certificado de representante de entidad sin personalidad jurídica (OID 1.3.6.1.4.1.5734.3.11.3)

¿Cómo puedo saber el número de serie de un certificado?

Si su certificado está instalado en Internet Explorer o en tarjeta pero lo abre con Internet Explorer siga las siguientes instrucciones:

- Abra Internet Explorer.
- Pulse en Herramientas - Opciones de Internet.
- Acceda a la pestaña Contenido y pulse el botón “Certificados”.
- Haga doble clic sobre el certificado del que desea saber el número de serie.
- Pulse en la pestaña Detalles del mismo.
- En la lista de campos podrá ver uno donde se indica el número de serie del certificado.

NOTA: El número de serie aparece en formato hexadecimal.

Si su certificado está instalado en Firefox o en tarjeta pero lo visualiza con Firefox siga las siguientes instrucciones:

Abra Firefox.

- Pulse en Herramientas - Opciones.
- Pulse el icono Avanzado, la pestaña Cifrado y el botón “Ver certificados”.
- Haga doble clic sobre el certificado del que desea saber el número de serie.
- En la pestaña General puede ver el número de serie del certificado.

NOTA: El número de serie aparece en formato hexadecimal.

¿Se puede tener más de un certificado por titular emitido por una Autoridad de Certificación?

Por regla general, las personas físicas titulares de un certificado solamente podrán tener un certificado en vigor emitido a su nombre. Si ya se dispone de un certificado digital de persona física y se solicita otro con el mismo nombre, apellidos y NIF provocará que se revoque de forma automática el certificado anterior y será vigente el nuevo solicitado.

Las empresas podrán tener emitidos y en vigor, tantos certificados de representación de persona jurídica como representantes legales tengan.

Consulte con la Autoridad de Certificación con la que desea emitir un certificado estos extremos según sus políticas.

¿Qué período de validez tiene un certificado?

La validez de un certificado puede variar según la Autoridad Certificadora y del tipo de certificado (persona física, empleado público, representante, sello electrónico, sede electrónica, servidor seguro,...) que se traten.

Típicamente, los certificados de persona física tienen una validez de 3 a 4 años, los de empleado público 3 años, los de sede electrónica y sello electrónico 3 años, los de representante de 2 a 5 años, los de servidor seguro 1 año, etc.

En todo caso, las Autoridades de Certificación tienen publicadas en sus páginas web las políticas de certificación para cada tipo de certificado, documentos en los que se especifica la vigencia de los certificados entre otras condiciones.

REGLAMENTO UE 910/2014 (EIDAS)

¿Cuáles son las novedades del Reglamento Eidas?

eiDAS crea un marco jurídico común y borra las barreras entre países. Esto supone nuevas oportunidades porque legisla más allá de lo que abarcaba la directiva del 99 (por lo que recoge aquellos aspectos en los que países se habían sobrepasado) y elimina las incertidumbres que se habían creado al respecto.

Ahora, todos los estados miembros de la UE deben emitir los mismos tipos certificados y regirse por criterios únicos.

Son objeto de nueva regulación los siguientes servicios y certificados: Certificado de autenticación web, Servicio de sellado de tiempo, Servicio de validación de las firmas y de los certificados, Servicio de conservación de las firmas electrónicas y Notificación electrónica.

¿Qué certificados validará @firma/VALIDE a partir de la entrada en vigor del eIDAS?

Se validarán todos los certificados europeos, además de los españoles.

Tengo más dudas sobre el Reglamento eIDAS ¿A quién puedo dirigirme?

Puede enviar una consulta sobre información general, no individualizada, en relación con el Reglamento (UE) Nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, así como la Ley 59/2003, de 19 de diciembre, de firma electrónica, a través de mlfe@minetad.es.

¿Cuáles son los certificados no reconocidos o a extinguir?

- Clasificación = 1 (a extinguir) – Persona jurídica (no reconocido).
- Clasificación = 3 – Sede según la ley 11/2007 (no reconocido).
- Clasificación = 4 – Sello según la ley 11/2007 (no reconocido).
- Clasificación = 6 (a extinguir) – Entidad sin personalidad jurídica (no reconocido).

A partir de la aplicación en su totalidad del Reglamento Eidas ¿Cuáles son los certificados válidos o reconocidos en la plataforma @firma?

A partir de la aplicación en su totalidad del Reglamento eIDAS, @firma debe adaptarse a la nueva normativa. Devolverá los tipos de certificados indicados en el eIDAS, y adicionalmente aquellos que clasifique Ministerio de Industria, Energía y Turismo.

Para los certificados ESPAÑOLES: Todos los nuevos certificados que se den de alta tendrán en cuenta la clasificación eIDAS. Los tipos de certificados existentes a partir del 1 de julio del 2016 serán:

- Clasificación = 0 – Persona física - Certificado cualificado de firma.
- Clasificación = 1 **(a extinguir)** – Persona jurídica **(no reconocido).**
- Clasificación = 2 – **No reconocidos**. Pueden incluir certificados de persona física, de componente, SSL….
- Clasificación = 3 – Sede según la ley 11/2007 **(no reconocido).**
- Clasificación = 4 – Sello según la ley 11/2007 **(no reconocido).**
- Clasificación = 5 – Empleado Público según la ley 11/2007 (Si se mantiene la clasificación por la SETSI. En caso contrario se actualizará la clasificación a "0 - Persona física - Certificado cualificado de firma" y se informará de ello a través de las listas de correo de @firma)
- Clasificación = 6 **(a extinguir)** – Entidad sin personalidad jurídica **(no reconocido).**
- Clasificación = 7 – Empleado Público con seudónimo según el RD 1671/2009. Son un subconjunto de certificados cualificados de persona física (0), que además, son de empleado público con seudónimo. (Si se mantiene la clasificación por la SETSI. En caso contrario se indicará en la clasificación a "0 - Persona física – Certificado cualificado de firma", pero no tendrá los campos Nombre, Apellidos y DNI, y contendrá en cambio en campo 'seudónimo')
- Clasificación = 8 -Certificado cualificado de sello, según el reglamento UE 910/2014.
- Clasificación = 9 - Certificado cualificado de autenticación de sitio web, según el reglamento UE 910/2014.
- Clasificación = 10 - Certificado cualificado de sello de tiempo. Si el servicio de sellado de tiempo figura en la TSL y el certificado cumple las normas técnicas para ser considerado de sello de tiempo.

- Clasificación = 11 – Certificado de persona física Representante ante las Administraciones Públicas de persona jurídica. Si se mantiene la clasificación por la SETSI o se cumple el perfil indicado para ello.
- Clasificación = 12 – Certificado de persona física Representante ante las Administraciones Públicas de entidad sin persona jurídica. Si se mantiene la clasificación por la SETSI o se cumple el perfil indicado para ello.

¿Cuál es la correspondencia entre la clasificación de @firma con los certificados CERES FNMT-RCM?

La clasificación en tipos 0...5 establecida por @firma se corresponden con los siguientes certificados CERES FNMT-RCM:

- Clasificación = 0 – Persona física, según el reglamento UE 910/2014. Persona física clase 2 CA (hasta caducidad de los mismos) según la ley 59/2003
- Clasificación = 1 – Persona jurídica clase 2 CA **(hasta caducidad de los mismos)** según la ley 59/2003
- Clasificación = 2 – Componente/SSL/no reconocido/sello de empresa
- Clasificación = 3 – Sede electrónica según la ley 40/2015
- Clasificación = 4 – Sello de órgano según la ley 40/2015
- Clasificación = 5 – Empleado Público según la ley 40/2015
- Clasificación = 6 – Entidad sin personalidad jurídica clase 2 CA **(hasta caducidad de los mismos)** según la ley 59/2003
- Clasificación = 7 - Empleado público con seudónimo según el RD 1671/2009
- Clasificación = 8 - Cualificado de sello de entidad, según el reglamento UE 910/2014
- Clasificación = 9 - Cualificado de autenticación de sitio web, según el reglamento UE 910/2014
- Clasificación = 10 - Servicio cualificado de sello de tiempo
- Clasificación = 11 – Representación Persona Jurídica / Administrador Único y Solidario, según el reglamento UE 910/2014
- Clasificación = 12 – Representación Entidad sin Personalidad Jurídica, según el reglamento UE 910/2014

¿Dónde puedo consultar el listado de Prestadores de Servicios Electrónicos de Confianza Cualificados?

MINETUR: PRESTADORES DE SERVICIOS ELECTRÓNICOS DE CONFIANZA CUALIFICADOS [https://sedeaplicaciones.minetur.gob.es/Prestadores]

PROVEEDORES DE SERVICIOS DE CERTIFICACIÓN – PLATAFORMA @FIRMA: [https://forja-ctt.administracionelectronica.gob.es/webdav/site/ctt-map/users/soporte_afirma/public/@FirmaV5p0_ANEXO_PSC.pdf]

Referencia:

- https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Racionaliza_y_Comparte/elementos_comunes/Servicios_Comunes_Firma_Electronica/FAQ-AFIRMA.html
- https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html

¿Dónde se encuentra publicada la lista de confianza de proveedores de servicios de certificación conforme al Reglamento (UE) nº 910/2014?

MINETUR: PRESTADORES DE SERVICIOS ELECTRÓNICOS DE CONFIANZA CUALIFICADOS [https://sedeaplicaciones.minetur.gob.es/Prestadores]

¿Qué legislación es aplicable en materia de Prestadores de Servicios Electrónicos de Confianza Cualificados?

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

¿Podrá seguir utilizándose el certificado de persona jurídica a partir de 1 de julio de 2016?

Los certificados de persona jurídica y de entidad sin personalidad jurídica emitidos antes del 1 de julio de 2016, fecha de aplicación completa del Reglamento (UE) 910/2014, podrán seguir utilizándose hasta su caducidad o revocación, pero no podrán renovarse después de esa fecha.

Definición de Sellado de Tiempo

El sellado de tiempo o timestamping es un mecanismo que permite demostrar la existencia de una serie de datos y que éstos no han sido alterados desde un instante específico en el tiempo.

Una Autoridad de Sellado de Tiempo (Time Stamp Authority) actúa como tercera parte de confianza certificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

¿Qué es son OCSP y las listas de revocación?

OCSP (Online Certificate Status Protocol o Protocolo Online del Estado de un Certificado) es un protocolo mediante el cual se puede comprobar el estado de validez de un certificado.

OCSP es un método más avanzado simple que descargar las Listas de Revocación de Certificados (CRL) y procesarlas.

FIRMA MEDIANTE CÓDIGO SEGURO DE VERIFICACIÓN (CSV)

► ¿Qué se entiende por un documento con firma CSV?

Se entiende por Código Seguro de Verificación (en adelante CSV) el sistema de firma electrónica y de verificación de los actos y documentos administrativos vinculado a una administración pública, órgano o entidad y, en su caso, a las personas firmantes del documento, que permite comprobar la autenticidad e integridad del mismo mediante el acceso a la Sede Electrónica correspondiente.

Dicho código se imprime en el pie de página del documento firmado, indicando al menos:

1. El Código Seguro de Verificación, que es un código alfanumérico.
2. La URL o dirección en internet para la comprobación del CSV.

El sistema de código seguro de verificación deberá garantizar, en todo caso:

a) El origen e integridad de los documentos mediante el acceso a la sede electrónica correspondiente.

b) El carácter único del código generado para cada documento.

c) Su vinculación con el documento generado y con el firmante. Cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente.

d) La posibilidad de verificar el documento en la sede electrónica como mínimo por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.

e) Un acceso al documento restringido a quien disponga del código seguro de verificación.

El Código Seguro de Verificación debe ser tratado con la debida cautela por el destinatario del documento; su comunicación a terceras personas les permitiría acceder al contenido del documento.

► ¿Cómo se valida un documento con firma CSV?

El proceso de validación de un documento firmado con CSV es el siguiente:

1. Accedemos a la URL o dirección de verificación del CSV
2. Introducimos el CSV para validarlo
3. Descargamos el documento CSV que devuelve el sistema de verificación
4. Comprobamos que el documento descargado coincide con el documento CSV que queremos validar.

► ¿Se debe superponer una firma de sello electrónico a un documento con firma electrónica CSV?

Sí, para asegurar la Interoperabilidad.

En las comunicaciones de documentos electrónicos a otros órganos, organismos o entidades y cuando así lo determinen las partes implicadas, la interoperabilidad se garantizará mediante la superposición al código seguro de verificación de un sello electrónico de los previstos en el artículo 42 de la Ley 40/2015, de 1 de octubre, como mecanismo de verificación automática del origen e integridad de los documentos electrónicos.

VALIDE/@FIRMA

¿Qué es VALIDE?

VALIDe es un servicio on-line ofrecido por la Administración General del Estado para la validación de Firmas y Certificados electrónicos. Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

El objetivo de este servicio es permitir a un usuario comprobar que el certificado utilizado es un certificado válido y que no ha sido revocado. También permite comprobar la validez de una firma electrónica realizada mediante certificado digital emitido por un prestador de servicios de certificación reconocido, y realizar firmas mediante certificado digital del que se disponga de la clave privada correspondiente.

La aplicación está disponible en https://valide.redsara.es y ofrece las siguientes secciones:

- Validar Certificado
- Validar Certificado de Sede Electrónica
- Validar Firma
- Realizar Firma
- Visualizar firma

¿Qué es @firma?

@firma es una plataforma de validación y firma electrónica, que se pone a disposición de las Administraciones Públicas, proporcionando servicios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva.

Es una solución de referencia para cumplir con las medidas de Identificación y autentificación descritas en la Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas.

El objetivo es comprobar que el certificado utilizado por el ciudadano es un certificado válido y que no ha sido revocado y que por tanto sigue teniendo plena validez para identificar a la persona propietaria. Los servicios de la plataforma son aplicables a todos los certificados electrónicos cualificados publicados por cualquier proveedor de servicio de certificación cualificado.

Para facilitar la integración con el servicio se proporcionan unas librerías de integración 'Integr@', que también permiten firma en servidor.

¿Cuáles son los formatos de firma soportados en la versión actual de VALIDE/@firma?

Formato	Descripción
CAdES B-Level	Firma CAdES (CMS Advanced Electronic Signature)
CAdES T-Level	Firma CAdES con sellado de tiempo
XAdES B-Level	Firma XAdES (XML Advanced Electronic Signature)
XAdES T-Level	Firma XAdES con sellado de tiempo
XAdES LT-Level	Firma XAdES con sellado de tiempo y validación a largo plazo (firmas longevas)
XAdES LTA-Level	Firma XAdES con posibilidad de sellado de tiempo periódico de sobre XAdES LT archivados
PAdES B-Level	Firma PAdES (PDF Advanced Electronic Signature)
PAdES T-Level / LT-Level / LTA-Level	Firma PAdES con sellado de tiempo, validación a largo plazo (firmas longevas)y resellado de firmas archivadas

¿Cuál es el tamaño máximo del archivo de firma que podemos validar?

VALIDE tiene un límite del tamaño de 8MB a la hora de validar firmas.

En caso de que introduzcamos un documento de firma de tamaño superior, aparecerá el siguiente mensaje:

- "El tamaño de la firma (...) supera el tamaño máximo permitido (8.388.608bytes)."

¿Cuál es el tamaño máximo del archivo de firma que podemos validar mediante Servicios Web?

El tamaño máximo de firma admitido es de 8MB, al igual que para la validación a través de https://valide.redsara.es

¿Cómo validar documentos PADES con un tamaño superior a 8MB?

Se puede seguir la siguiente estrategia combinando AUTOFIRMA y VALIDE:

1. Validar estructura de la firma mediante AUTOFIRMA
2. Validar los certificados de firma en VALIDE
3. Validar los certificados de sellado de tiempo en VALIDE, en su caso.

También se puede utilizar el programa Acrobat Reader, en el que debemos importar primero los certificados de las Autoridades Certificadoras que han emitido los certificados con los que se ha firmado el documento y con los que se ha realizado el sellado de tiempo, en su caso.

¿Desde qué versión de @firma se puede aplicar un sellado de tiempo a un fichero firmado PADES?

Desde @firma 6

¿Cuáles son los servicios disponibles en @firma? ¿Cuáles son los requisitos técnicos para integrarse con los servicios de @firma?

Los servicios de @firma disponibles son los siguientes:

- Firma de servidor simple, cofirma y contrafirma
- Verificación de firmas
- Sellado de tiempo de una firma (upgrade)
- Validación de certificados

Para poder hacer uso de @firma es necesario cumplir los siguientes requisitos:

1. Ser una administración pública.
2. Disponer de conexión a la Red SARA
3. Formular solicitud de alta a través del soporte CAID.
4. Disponer de un certificado cualificado de sello de entidad (sello electrónico) para la integración.
5. Aplicación que se integre con los servicios web de @firma o hacer uso de librerías de integración Integr@.

¿Hasta qué fecha estarán disponibles los servicios de sello de tiempo TS@?

Desde el equipo de soporte de @firma se ha avisado que se van a discontinuar los servicios de validación de sello de tiempo y de resellado de la TS@, ya que son de uso minoritario y se proveen de manera más eficiente a través de @firma.

Si se hace uso de estos servicios, se aconseja su migración a los servicios de @firma, ya que a partir del **4 de noviembre de 2019** los servicios de validación de sello de tiempo y de resellado podrán no estar disponibles.

CERTIFICADOS ENTIDADES LOCALES / ADMINISTRACIONES PÚBLICAS

¿Cuáles son los certificados cualificados de mayor interés para una entidad o administración pública?

- Certificado cualificado de Empleado público: de los empleados en el ejercicio de sus funciones.
- Certificado cualificado de Empleado público con pseudónimo: de los empleados en el ejercicio de sus funciones y que por motivos de seguridad no deban ser identificados directamente (en actuaciones que afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones en las que esté legalmente justificado el anonimato para su realización).
- Certificado cualificado de Representante: en su relación con otras administraciones públicas.
- Certificado cualificado de sello de entidad / sello electrónico: para la firma de documentos en actuaciones automatizadas y a la hora de integrarse con aplicaciones de otras administraciones mediante servicios web.
- Certificado cualificado de autenticación de sitio web / sede electrónica: para la identificación de la Sede Electrónica y de otros sitios web de la entidad.

¿Cuáles son los aspectos más relevantes a la hora de solicitar un certificado de Empleado Público?

- Certificado cualificado de Autoridad de Certificación cualificada (es validado en VALIDE).
- Admisión por parte de las Administraciones y aplicaciones con las que nos vamos a relacionar (*).
- Soporte (hardware/software).
- Vigencia.
- Precio.

(*) Es posible que alguna Administración Pública no está admitiendo todos los certificados cualificados de todas las Autoridades de Certificación cualificadas, a pesar de su obligatoriedad, por lo que es recomendable comprobar tal extremo previamente a la adquisición del certificado.

¿Cuáles son los aspectos más relevantes a la hora de solicitar un certificado de Sello Electrónico?

- Certificado cualificado de Autoridad de Certificación cualificada (es validado en VALIDE).
- Admisión por parte de las Administraciones y aplicaciones con las que nos vamos a relacionar (*).
- Soporte (hardware/software).
- Vigencia.
- Precio.

(*) Es posible que alguna Administración Pública no está admitiendo todos los certificados cualificados de todas las Autoridades de Certificación cualificadas, a pesar de su obligatoriedad, por lo que es recomendable comprobar tal extremo previamente a la adquisición del certificado.

- **¿Qué tipo de certificado de empleado público debemos utilizar en nuestra entidad? ¿Hardware o software?**

Dependerá de si la política de seguridad de tu entidad lo define y, en todo caso, dependerá de la categoría ENS del Sistema de Información al que accedas: si es de categoría alta, se requerirá token criptográfico (tarjeta empleado público) y para categoría media será suficiente con certificado software. La política de seguridad puede elevar estos requisitos de seguridad. Por ejemplo, para un sistema de categoría media la política puede requerir proteger por contraseña el uso de los certificados software o requerir el uso de tarjetas de empleado público.

En todo caso, es más seguro el uso de certificados de empleado público en tarjeta criptográfica, ya que se protegen las claves del certificado desde el mismo instante de su generación y la tarjeta se custodia físicamente y en todo momento por parte del titular del certificado, y tiene la ventaja de poder ser utilizado en cualquier equipo con lector de tarjeta sin necesidad de instalar el certificado en el equipo.

- **¿Puedo utilizar mi certificado de empleado público para realizar trámites personales?**

Sólo podrán usarse en el desempeño de las funciones propias del puesto que ocupen los empleados o para relacionarse con las Administraciones públicas cuando éstas lo admitan

Artículo 22. RD 1671/2009

- **¿Es obligatorio que mi certificado de empleado público contenga información de mi NIF? ¿Es suficiente con que contenga mi código de identificación NRP o NIP? Contiene información incorrecta, dadas las novedades en cuanto a pseudónimo introducidas en la propuesta de RD**

Sí, el certificado de empleado público debe incluir obligatoriamente el número de DNI/NIE, junto con la letra de control, de acuerdo con lo indicado en el DNI/NIE, a excepción de los certificados de empleado público con pseudónimo.

“Perfiles de certificados electrónicos Aprobado por el Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012” [política de firma AGE 1.9]

En determinadas situaciones especiales se podrá solicitar la emisión de Certificado de Empleado Público con pseudónimo según el RD 1671/2009. Son un subconjunto de certificados cualificados de persona física (0), que además, son de empleado público con seudónimo (no tendrá los campos Nombre, Apellidos y DNI, y contendrá en cambio en campo ‘seudónimo’)

Art 43.2 de la Ley 40/2015 “Por razones de seguridad pública los sistemas de firma electrónica podrán referirse solo el número de identificación profesional del empleado público” previsiblemente para los cuerpos de seguridad del estado y para los colectivos que tiene previsto el RD 1671/2009: “afecten a información clasificada, a la seguridad pública o a la defensa nacional o a otras actuaciones, en las que esté legalmente justificado el anonimato para su realización”, que incluirán únicamente el número de identificación profesional del empleado.

► **En la localidad de la entidad donde trabajo no hay oficina en la que pueda presentarme para identificarme para la solicitud de emisión de un certificado digital ¿Puedo constituir en mi entidad una oficina de registro para la emisión de certificados? ¿Qué tipo de certificados se podrían emitir?**

Sí, se puede constituir una oficina de registro para la emisión de certificados. Para ello se debe formalizar convenio o contrato con una Autoridad de Certificación reconocida que ofrezca este servicio, disponer de personal responsable adecuadamente formado e informado de la política de emisión de certificados y disponer de un PC con los recursos necesarios (típicamente conexión a internet, lector o lectores de tarjetas, tarjetas con chip e impresora de tarjetas).

El personal operador asume una serie de obligaciones que tiene que cumplir en materia de seguridad y protección de datos y debe seguir estrictamente los protocolos definidos por la Autoridad de Certificación (identificación, documentación a solicitar, documentación a conservar,...) según el tipo de certificado que se vaya a emitir.

Los certificados que se pueden emitir habitualmente desde una oficina de registro para la emisión de certificados son los siguientes: empleado público (software/tarjeta), representante (software/tarjeta) y ciudadano (software/tarjeta). Es decisión de la entidad definir el ámbito de emisión de certificados y establecer el acuerdo con la Autoridad de Certificación.

► **Una aplicación de mi entidad necesita integrarse con servicios web ofrecidos por otra administración pública y se requiere que utilice en el servidor de la aplicación un certificado electrónico para la identificación, establecimiento y aseguramiento de la conexión ¿Qué tipo de certificado debo solicitar? ¿Cómo genero las claves? ¿Cómo lo custodio?**

Se debe contactar con la administración pública que ofrece el servicio con el que queremos integrarnos. Típicamente se nos requerirá de un certificado de Sello Electrónico cualificado que identifique a nuestra entidad (mediante su CIF) y el departamento o sistema de información responsable de la custodia y uso del certificado. En entornos de pruebas y administraciones públicas más laxas podrán admitir otro tipo de certificados, como los de Certificado de autenticación web, de componente o SSL, pero no está recomendado su uso para estos fines. En ningún caso se utilizará un certificado de persona física, de empleado público o de representante.

La generación y la custodia de las claves atenderán a lo dispuesto por la medida 4.3.11 Protección de claves criptográficas [op.exp.11] del ENS.

► **¿En qué casos se debe solicitar la revocación de un certificado de empleado público o de representante?**

- En caso de detectar que las claves del certificado o de la Autoridad de Certificación han sido comprometidas.
- Por pérdida o daños en el soporte del certificado.
- Al finalizar la relación contractual del empleado con la Administración Pública para la que emitió el certificado o por un cambio o extinción de puesto o cargo que se vea reflejado en el certificado.
- A la finalización de la representación o extinción de la entidad representada.
- Por inexactitudes en los datos aportados para la obtención del certificado.

¿Es necesario que mi entidad defina una Política de Firma propia?

No es necesario. Las Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados de la Administración General del Estado, mediante resolución del órgano responsable de su aprobación.

Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales siempre que las características particulares de los procedimientos administrativos bajo su competencia lo hicieran necesario.

¿Qué certificado debe utilizar mi entidad para relacionarse con otras administraciones?

Dependiendo de la administración destino con la que nos relacionemos, se nos exigirá bien un certificado de empleado público o bien un certificado de representante.

Algunas administraciones admiten únicamente el certificado de representación a los efectos de recepción de documentación, en tanto que no disponen de un registro electrónico de apoderamientos.

CERTIFICADO DE REPRESENTANTE

Certificado de Representante: ¿A quién va dirigido?

Este certificado está dirigido a una persona representante de una entidad con o sin personalidad jurídica con capacidad para obligarse en su nombre.

¿Qué tipos de certificados de representante existen?

Según la clasificación que realiza @firma atendiendo al reglamento UE 910/2014 (EIDAS), hay dos clases de certificado de representante:

- Certificado de persona física Representante ante las Administraciones Públicas de persona jurídica. Si se mantiene la clasificación por la SETSI o se cumple el perfil indicado para ello.
- Certificado de persona física Representante ante las Administraciones Públicas de entidad sin persona jurídica. Si se mantiene la clasificación por la SETSI o se cumple el perfil indicado para ello.

¿Cuáles son los aspectos más relevantes a la hora de solicitar un certificado de Empleado Representante?

- Certificado cualificado de Autoridad de Certificación cualificada (es validado en VALIDE).
- El ámbito/uso del certificado.
- Admisión por parte de las Administraciones y aplicaciones con las que nos vamos a relacionar (*).
- Soporte (hardware/software).
- Vigencia.
- Precio.

(*) Es posible que alguna Administración Pública no está admitiendo todos los certificados cualificados de todas las Autoridades de Certificación cualificadas, a pesar de su obligatoriedad, por lo que es recomendable comprobar tal extremo previamente a la adquisición del certificado.

Teniendo en cuenta estos aspectos, es recomendable acudir a las páginas web de las Autoridades de Certificación reconocidas para consultar los diferentes tipos de certificado de representante que se pueden solicitar y en qué soporte y condiciones.

A continuación, se recoge una muestra representativa de certificados de representación de los principales prestadores de servicios de certificación que han accedido a colaborar en esta enciclopedia:

ACCV

- 1.3.6.1.4.1.8149.3.29.1.0 - de entidad jurídica en dispositivo seguro
- 1.3.6.1.4.1.8149.3.30.1.0 - de entidad jurídica en soporte software
- 1.3.6.1.4.1.8149.3.31.1.0 - de entidad sin personalidad jurídica en software
- 1.3.6.1.4.1.8149.3.32.1.0 - de entidad sin personalidad jurídica en soporte software

CERES – FNMT

- 1.3.6.1.4.1.5734.3.11.1 - De administrador único o solidario de persona jurídica
- 1.3.6.1.4.1.5734.3.11.2 - De persona jurídica
- 1.3.6.1.4.1.5734.3.11.3 - De entidad sin personalidad jurídica

CAMERFIRMA

- 1.3.6.1.4.1.17326.10.16.1.3.1.1 - Representante de ESPJ con Poderes Generales de Representación en QSCD
- 1.3.6.1.4.1.17326.10.16.1.3.1.2 - Representante de ESPJ con Poderes Generales de Representación
- 1.3.6.1.4.1.17326.10.16.1.3.2.1 - (2.16.724.1.3.5.8) - Representante de PJ para trámites con la AAPP en QSCD
- 1.3.6.1.4.1.17326.10.16.1.3.2.2 - (2.16.724.1.3.5.8) - Representante de PJ para trámites con la AAPP
- 1.3.6.1.4.1.17326.10.16.1.3.3.1 - Representante de ESPJ para Apoderados
- 1.3.6.1.4.1.17326.20.16.1.3.1.1 - (2.16.724.1.3.5.8) - Representante de PJ con Poderes Generales de Representación en QSCD
- 1.3.6.1.4.1.17326.20.16.1.3.1.2 - (2.16.724.1.3.5.8) - Representante de PJ con Poderes Generales de Representación)
- 1.3.6.1.4.1.17326.20.16.1.3.2.1 - Representante de ESPJ para trámites con la AAPP en QSCD
- 1.3.6.1.4.1.17326.20.16.1.3.2.2 - Representante de ESPJ para trámites con la AAPP
- 1.3.6.1.4.1.17326.20.16.1.3.3.1 - (2.16.724.1.3.5.8) - Representante de PJ para Apoderados en QSCD
- 1.3.6.1.4.1.17326.20.16.1.3.3.2 - (2.16.724.1.3.5.8) - Representante de PJ para Apoderados
- 1.3.6.1.4.1.17326.20.16.1.3.3.2 - Representante de ESPJ para Apoderados

CONSORCI AOC (CATCERT)

- 1.3.6.1.4.1.15096.1.3.2.8.1.1 Certificado cualificado de representante ante las Administraciones Públicas

FIRMA PROFESIONAL

- 1.3.6.1.4.1.13177.10.1.11.1 - Legal en DCCF portable
- 1.3.6.1.4.1.13177.10.1.11.2 - Legal en otros dispositivos
- 1.3.6.1.4.1.13177.10.1.11.3 - Legal en DCCF centralizado
- 1.3.6.1.4.1.13177.10.1.12.1 - Representante Voluntario portable
- 1.3.6.1.4.1.13177.10.1.12.2 - Representante Voluntario en otros dispositivos
- 1.3.6.1.4.1.13177.10.1.12.3 - Representante Voluntario en DCCF centralizado
- 1.3.6.1.4.1.13177.10.1.13.1 - Representante entidad sin personalidad jurídica en DCCF portable
- 1.3.6.1.4.1.13177.10.1.13.2 - Representante entidad sin personalidad jurídica en otros dispositivos
- 1.3.6.1.4.1.13177.10.1.13.3 - Representante entidad sin personalidad jurídica en DCCF centralizado

UANATACA

- 1.3.6.1.4.1.47286.1.8.1 Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en software
- 1.3.6.1.4.1.47286.1.8.2.2 Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en QSCD (tarjeta)
- 1.3.6.1.4.1.47286.1.7.1 Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en software
- 1.3.6.1.4.1.47286.1.7.2.2 Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en QSCD (tarjeta)
- 1.3.6.1.4.1.47286.1.2.1 Certificado cualificado de Persona Física Representante en software
- 1.3.6.1.4.1.47286.1.2.2.2 Certificado cualificado de firma de Persona Física Representante en QSCD (tarjeta)

► Información sobre los nuevos certificados de representante

Conforme a la nueva normativa europea, el 1 de julio de 2016 dejaron de emitirse certificados de firma electrónica a favor de personas jurídicas o entidades sin personalidad jurídica, de la Autoridad de Certificación Clase 2 CA; si bien estos certificados (conforme a las directrices del Ministerio de Industria, Energía y Turismo) podrán seguir utilizándose hasta su caducidad o revocación. Para sustituir a dichos certificados, se podrán utilizar certificados de firma electrónica de representante de personas jurídicas o entidades sin personalidad jurídica.

Ante ese nuevo escenario, para sustituir a dichos certificados, las Autoridades de Certificación están emitiendo nuevos certificados de firma electrónica de representante de personas jurídicas o entidades sin personalidad jurídica.

Por ejemplo, CERES FNMT-RCM ha desarrollado una nueva Autoridad de Certificación, con algoritmos y claves criptográficas más robustas, que emite desde el 6 de junio de 2016 tres nuevos tipos de certificado:

- Certificado de Representante para Administrador Único o Solidario.
- Certificado de Representante de Persona Jurídica.
- Certificado de Representante de Entidad sin Personalidad Jurídica.

► ¿Qué ámbito tienen los nuevos certificados de representante?

Los certificados de representación de Persona Jurídica y Entidad sin Personalidad Jurídica pueden ser utilizados para las relaciones con cualquier Administración Pública, y algunos de ellos para relacionarse con otras empresas.

Por ejemplo, en el caso de certificados de representante de CERES FNMT-RCM:

- Los nuevos certificados de representación de persona jurídica pueden ser utilizados para la relación con cualquier Administración.
- Los nuevos certificados de representación de administrador único o solidario pueden ser utilizados para las relacionarse con las AAPP y con empresas privadas (contratación de bienes o servicios).
- Se emite conforme al Reglamento Europeo de Identificación Electrónica (eIDAS), obteniendo así validez a nivel europeo.

Ver la pregunta frecuente ¿Cuáles son los aspectos más relevantes a la hora de solicitar un certificado de Empleado Representante?

► ¿Cómo puedo validar los nuevos certificados de representante?

Si usted desea validar un certificado de Representante o un documento firmado por un certificado de Representante, puede hacerlo a través de Valide (https://valide.redsara.es/valide/).

► ¿Qué certificado de representante debo solicitar?

Debe consultar las políticas de certificación de cada Autoridad de Certificación para conocer los tipos de certificado de representación que se pueden solicitar y el uso de cada uno de ellos.

Por ejemplo, en el caso de CERES FNMT-RCM, emite tres tipos de certificados de representación (que sustituyen a los antiguos certificados de Persona Jurídica). Según la letra inicial del NIF de su entidad puede saber qué certificado puede solicitar.

- Certificado de Representación de Administrador Único y/o Solidario: se emiten, para la relación de las Personas Jurídicas a través de sus Representantes legales en sus relaciones con las administraciones públicas o en la contratación de bienes o servicios propios o concernientes a su giro o tráfico ordinario. Este certificado puede ser obtenido por las sociedades anónimas (A) y limitadas (B) si el representante de la sociedad es administrador único o solidario inscrito correctamente en el Registro Mercantil.

- Certificado de Representación de Persona Jurídica: Este certificado se expide a las personas físicas como representantes (cuando no se trate de Administradores únicos o solidarios) de las personas jurídicas para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas. Según la letra inicial del NIF de su entidad pueden solicitar este tipo de certificado: A, B, C, D, F, G, J, N, Q, R, S, P, V
- Certificado de Representación de Entidad sin Personalidad Jurídica: Este certificado se expide a las personas físicas como representantes de las entidades sin personalidad Jurídicas para su uso en sus relaciones con aquellas Administraciones Públicas, Entidades y Organismos Públicos, vinculados o dependientes de las mismas. Q: Organismos públicos. Según la letra inicial del NIF de su entidad pueden solicitar este tipo de certificado: E, H, N, P, S, U, V y W.

Puede consultar la denominación de las diferentes entidades atendiendo a la inicial de su NIF en la página de la Agencia tributaria: *NIF de personas jurídicas y entidades*

► ¿Qué tipo de certificado debo solicitar si el administrador de mi empresa es otra empresa?

Si el administrador de su empresa es otra empresa y aunque ésta tenga un representante como administrador único debe solicitar el certificado cualificado de Representante de Persona Jurídica.

► ¿Qué documentación debo aportar a la hora de solicitar un certificado de representante?

Debe consultar las políticas de certificación de cada Autoridad de Certificación para conocer los tipos de certificado de representación que se pueden solicitar y la documentación que se debe aportar.

En el caso de CERES FNMT-RCM, puede consultar en https://www.sede.fnmt.gob.es/preguntas-frecuentes/certificado-de-representante la documentación que se debe presentar a la hora de solicitar un certificado de representante:

- ¿Qué documentación debe aportar un organismo o entidad pública?
- ¿Qué documentación debe aportar una sociedad civil?
- ¿Qué documentación debe aportar una asociación?
- ¿Qué documentación debe aportar una entidad con NIF N?
- ¿Qué documentación debe aportar un Consejo de Administración sin Consejero Delegado?
- ¿Qué documentación debe aportar si el administrador de una empresa es otra empresa?
- ¿Qué documentación debe aportar una fundación?
- ¿Qué documentación debe aportar una comunidad de propietarios/as?
- ¿Qué documentación hay que aportar para solicitar un certificado de representación de persona jurídica?
- ¿Qué documentación hay que aportar para solicitar un certificado de entidad sin personalidad jurídica?

- ¿Puede un poder notarial autorizar a más de un apoderado?
- ¿Puede subapoderarse?
- ¿Tiene caducidad un poder notarial?

SEDE ELECTRÓNICA

► **¿Cuáles son los aspectos más relevantes a la hora de solicitar un certificado de Sede Electrónica?**

- Certificado cualificado de Autoridad de Certificación cualificada.
- Es validado en VALIDE como certificado de Sede Electrónica.
- Soporte por parte de los navegadores sin intervención del usuario.
- Soporte (hardware/software).
- Vigencia.
- Precio.

► **Vamos a renovar el certificado de la Sede Electrónica de mi entidad. Hasta la actualidad lo estábamos protegiendo con un certificado de servidor seguro. ¿Qué tipo de certificado se debe utilizar?**

Para la protección de la navegación de la Sede Electrónica y para asegurar la autenticidad y autoría de la información que en ella se muestra se debe utilizar un certificado electrónico cualificados de autenticación de sitios web o certificado cualificado de Sede electrónica de la Administración Pública, que identifique unívocamente el dominio de la sede electrónica (no se aceptan certificados con subdominios comodín o wildcard) y la entidad a la que pertenece la Sede Electrónica (con denominación y CIF).

Ver pregunta frecuente "A partir de la aplicación en su totalidad del Reglamento Eidas ¿Cuáles son los certificados válidos o reconocidos en la plataforma @firma?"

En todo caso, existe un servicio de validación de Sede Electrónica para comprobar que está protegida con un certificado adecuado: https://valide.redsara.es/valide/validarSede/

Además, es importante que nos aseguremos de que el certificado está emitido por una Autoridad de Certificación cuyos certificados estén admitidos por defecto en la mayoría de navegadores, sistemas operativos y aplicaciones (java, activex, etc). De esta manera evitaremos que aparezcan mensajes de advertencia en los navegadores de los usuarios que les den a entender que el certificado utilizado para proteger la Sede es inseguro.

- **En las Sede Electrónica de nuestra entidad, una vez que se autentica un usuario con su certificado se le identifica mediante NIF. Si accede un ciudadano o empresa europeos con certificado cualificado ¿cómo lo identificamos unívocamente? ¿Cómo adaptamos nuestro sistema de autenticación?**

Los certificados Europeos no tienen DNI, y en la mayor parte de los casos tampoco un identificador único de la persona poseedora del certificado. Solo están obligados a incluir el nombre y apellido, o incluso un seudónimo. Además pueden llevar otra información variada asociada a la identidad (lugar de nacimiento, fecha de nacimiento…)

Se recomienda el uso de Cl@ve, en detrimento de un sistema propio de validación, ya que a través de la conexión con los nodos eiDAS del resto de países permitirá obtener los identificadores nacionales del resto de países europeos.

- **Desde la Sede Electrónica de mi ayuntamiento se generan documentos certifican información recogida en nuestras bases de datos ¿Con qué tipo de certificado se deben firmar?**

Para el uso de firma en actuaciones automatizadas (que se generan automáticamente según información recogida en el Sistema de Información), tales como un justificante de registro, un certificado de estar dado de alta en el padrón en un determinado instante, etc., se debe utilizar un Certificado cualificado de sello. Además se debe informar en la Sede Electrónica acerca del todos los sellos electrónicos que utiliza nuestra entidad, indicando el número de serie de cada uno de los sellos.

La generación y la custodia de las claves del certificado de sello atenderán a lo dispuesto por la medida 4.3.11 Protección de claves criptográficas [op.exp.11] del ENS.

Ver pregunta frecuente "A partir de la aplicación en su totalidad del Reglamento Eidas ¿Cuáles son los certificados válidos o reconocidos en la plataforma @firma?"

Ver pregunta frecuente "¿Cómo puedo saber el número de serie de un certificado?"

SOLICITUD DE UN CERTIFICADO

- **¿Dónde puedo solicitar un certificado?**

En la página web de las diferentes Autoridades de Certificación se puede encontrar información acerca de los diferentes tipos de certificado y el procedimiento de solicitud de los mismos.

Además, se indica la forma de identificación y acreditación del solicitante.

- **¿Por qué necesito acreditarme?**

La acreditación es necesaria para asegurar la identidad del solicitante del certificado, y en su caso, su capacidad de representación del titular del certificado y para poder discriminar que clave debe ser certificada por la Autoridad de Certificación.

¿Es gratuita la obtención del certificado de persona física?

Por lo general sí, pero depende de la Autoridad de Certificación y los convenios establecidos con las diferentes administraciones en las que se establecen como Autoridades de Registro.

Por ejemplo, en el caso de los certificados de persona física de más amplia emisión - CERES FNMT-RCM - el registro de usuarios y su expedición no generarán coste económico para los interesados.

¿Se puede solicitar un certificado de representante de personas físicas?

Según el Reglamento EIDAS no son certificados de firma cualificados, por lo que no es posible obtener este tipo de certificados, aun cuando la persona que actúe por representación pueda acreditar que es el representante legal o voluntario del representado.

Esta opción, que en principio puede parecer válida, se ha descartado por el riesgo legal que se pueda hacer de dicha representación en cuanto al uso no autorizado o fraudulento del certificado (si el representado ha fallecido, revocación del poder o la sentencia no adquirió firmeza).

¿Puede firmar el representante de un tercero el contrato de solicitud de un certificado de firma electrónica?

Sí, pero solo a los efectos de solicitar el certificado, no de usarlo.

¿Se puede acreditar en la Oficina de Registro sin personación física del solicitante?

Sí, si la firma ha sido legitimada en presencia notarial.

¿Podría solicitar un certificado digital un usuario menor de edad?

Los certificados sólo podrán solicitarlos los mayores de 18 años o menores emancipados, y según las consideraciones siguientes:

- La mayoría de edad es:
  - » Para españoles: 18 años
  - » Para extranjeros: entre 18 y 21 años. En caso de dudas, el solicitante deberá aportar la acreditación de su mayoría de edad, según el país de origen, mediante certificado de su embajada o consulado.
- Menores emancipados. Pueden solicitar el certificado, pero han de acreditar su emancipación:
  - » Españoles: certificado literal del Registro Civil
  - » Para extranjeros: entre 18 y 21 años. Según el país de origen, mediante el certificado correspondiente de su embajada o consulado.

¿Qué hago si mi Certificado aparece como caducado o aún no válido?

Puede haber tres motivos para este mensaje:

- El certificado tiene validez un periodo de tiempo después de su emisión, si Ud. lo obtiene antes de que comience este periodo puede obtener este mensaje, en cuyo caso deberá esperar a que se cumpla la fecha y hora de validez.
- La fecha y/o la hora de su equipo es incorrecta. Compruebe este hecho y modifíquelas si es necesario.
- Realmente el certificado está caducado. Deberá reiniciar el procedimiento para obtener otro.

¿Cómo realizar la legitimación de firma ante notario? ¿Tiene caducidad la legitimación de firma?

Ha de ser el propio solicitante y futuro titular del certificado (para el Certificado de Usuario, Persona Física) o el representante (para el Certificado de Representante de Persona Jurídica o el de la Entidad Sin Personalidad Jurídica) quien deberá acudir personalmente a una oficina de registro a acreditar su identidad. En el caso de que no pudiera hacerlo por cualquier circunstancia, podrá ir una tercera persona en su nombre, previa legitimación de la firma ante notario.

La legitimación de firma es un testimonio que acredita el hecho de que una firma ha sido puesta en presencia del notario, o el juicio de éste sobre su pertenencia a persona determinada (en el caso de expedición de certificados, la Ley exige que sea en presencia notarial). El notario no asumirá responsabilidad por el contenido del documento cuyas firmas legitime.

En la legitimación se consigna la fecha en que fue realizada, pero no de caducidad. Es necesario, por tanto, comprobar que el resto de documentación aportada no infringe los plazos de validez que establecen los procedimientos de registro.

También en algunos casos de representación voluntaria, a juicio de la oficina de registro, si la documentación ofrece dudas sobre su validez puede solicitar la actualización de la misma.

SOLICITUD DE UN CERTIFICADO – CERES FNMT-RCM

¿Dónde puedo acreditarme para obtener un Certificado emitido por CERES FNMT-RCM?

La acreditación para la emisión de los Certificados de usuario, podrá ser realizada en la red de oficinas implantadas por aquellos Organismos que previamente hayan firmado un acuerdo de colaboración con CERES FNMT-RCM y habilitadas por estos Organismos, o en las Oficinas Consulares de carrera de España en el extranjero, no siendo posible en los registros aduaneros. Puede consultar la lista de oficinas.

¿Dónde puedo obtener información acerca de los procedimientos de solicitud de un certificado a la Autoridad de Certificación CERES FNMT-RCM?

Puede obtener más información en la página web de la Fábrica Nacional de Moneda y Timbre: https://www.sede.fnmt.gob.es/

Además, en la parte inferior puede acceder a las preguntas frecuentes, https://www.sede.fnmt.gob.es/preguntas-frecuentes , entre las que puede resolver dudas sobre el procedimiento de solicitud:

- ¿Qué documentación hay que presentar en la Oficinas de Acreditación para la solicitud de un Certificado FNMT de Persona Física?
- ¿Cuándo he de renovar mi Certificado?
- ¿Puedo renovar mi certificado de persona física de clase 2 CA?
- Información adicional sobre la renovación de Certificados
- Proceso de renovación de un Certificado en Mozilla Firefox
- Proceso de renovación de un Certificado en Windows Vista con Internet Explorer
- ¿Cómo revocar un certificado de persona física por defunción del titular?
- Procedimiento para anular o revocar un certificado de persona física de una persona fallecida.
- ¿Qué pasos he de seguir para revocar un Certificado de Persona Física?
- Servicio de revocación telefónica
- Proceso de revocación de Certificados emitidos por la FNMT Clase 2 CA
- ¿Qué pasos he de seguir para obtener un Certificado FNMT de Persona Física? (falta)
- ¿Qué es el Código de Solicitud?
- ¿Qué pasos debo seguir para solicitar un Certificado FNMT de persona física o el certificado de representación de administrador único o solidario con mi DNIe?
- ¿Qué pasos debo de seguir si resido fuera de España y deseo obtener el Certificado de usuario de la FNMT?
- ¿Cómo me acredito para obtener el Certificado de usuario emitido por FNMT?
- ¿Puedo realizar varias peticiones de certificados en un mismo dispositivo?
- Si tengo varios códigos de solicitud, ¿Cuál presento en la acreditación?
- ¿Por qué no puedo renovar mi certificado de persona física de clase 2 si proviene de una renovación anterior o de una solicitud con DNIe?
- Configuración de los antivirus para la solicitud y la descarga.
- ¿Qué navegadores puedo utilizar para obtener mi Certificado con un sistema operativo Linux?

¿Dónde puedo obtener información acerca de resolución de errores y consultas técnicas relativos a certificados emitidos por CERES FNMT-RCM?

Puede obtener soporte técnico a través la página web de CERES FNMT-RCM en el enlace https://www.sede.fnmt.gob.es/preguntas-frecuentes/problemas-y-dudas

Puede resolver, entre otras dudas o problemas, las siguientes cuestiones:

- Error: Su clave privada no ha sido generada.
- Error: Se ha producido un error en la descarga: error 2147024891
- Error: Ha ocurrido un error tratando de instalar los certificados
- Error: Este certificado no puede ser instalado porque Ud. no posee la correspondiente clave privada que se creó cuando solicitó el certificado.
- Error: Esta conexión no está verificada (Firefox).
- Error: 424 en la descarga
- Error al generar el certificado, verifique la configuración de su navegador. ERROR :-2146827859
- Descarga de certificados con Google Chrome portable 48
- Al intentar obtener mi Código de Solicitud en múltiples ocasiones obtengo el mensaje: Su clave privada no ha sido generada.
- ¿Qué hago si al solicitar un código de solicitud de persona física con Firefox, relleno los datos y al enviar me aparece el error Se ha producido un error en la aplicación: Consulte con el administrador del sistema?
- ¿Qué hago si tras pulsar el botón de Firmar en una renovación, revocación o modificación de datos personales, aparece el siguiente mensaje: El certificado no es válido. Ha ocurrido un error al firmar el contenido. Error: No coinciden los tipos?
- ¿Qué debo hacer para poder acceder en MAC con Chrome, a toda la funcionalidad de la web de CERES?
- ¿Qué hago si al intentar descargar el certificado obtengo el mensaje VBScript: Error al descargar el certificado?
- Error al exportar certificado personal CERES FNMT-RCM desde Firefox “Se produjo un fallo por motivos desconocidos al guardar la copia de seguridad del archivo PKCS #12”.
- ¿Qué hago si pulso el botón de firmar con Mozilla Firefox y la aplicación no hace nada?

CERTIFICADOS EN EL NAVEGADOR

¿Qué tipos de certificado de firma digital, atendiendo al soporte, puedo utilizar en el navegador?

Desde un navegador web se pueden utilizar certificados de firma en soporte software, que se instalan en el almacén de claves del navegador, o certificados en soporte hardware, comúnmente en tarjetas inteligentes.

El uso de tarjetas inteligentes es más seguro dado que la clave privada de la firma digital no puede extraerse de la tarjeta y su uso siempre está protegido por un código PIN.

¿Qué pasos en general debo seguir para poder utilizar un certificado software en un navegador en Windows?

Para poder utilizar un certificado de firma en software, debemos instalarlo o importarlo en el almacén de claves del navegador. Además es necesario que importemos en el almacén de claves del navegador los certificados raíz de la Autoridad de Certificación que emitió el certificado.

Es importante que en el momento de importar el certificado en el navegador los protejamos mediante una clave o PIN y que el navegador nos solicite esa clave en cada uso.

¿En qué formatos puedo exportar/importar un certificado software?

Los certificados pueden ser exportados en diversos formatos de archivo. Lo más típicos son:

- Clave pública: .CER (DER, CER) y .P7B (PKCS#7)
- Clave pública y privada: .P12 y .PFX (PKCS#12)

¿Cuál es la diferencia de exportar el certificado software con clave privada o sin ella?

Se puede exportar el certificado con su clave privada solo para su uso personal o como copia de seguridad. La clave privada servirá para realizar firma digital. Si se exporta un certificado sin la clave privada no podernos utilizarlo para firmar. Los formatos típicos de una exportación de certificado con clave privada son p12 y pfx.

La parte pública del certificado, sin la clave privada, podrá exportarse para entregarlo a todo aquel que quiera comunicarse con nosotros de forma segura (para que pueda verificar una firma o para que pueda cifrar contenido que intercambie con nosotros). Los formatos típicos de exportación de la parte pública de un certificado son p7b, der y cer.

Es importante realizar una copia de seguridad de los certificados software junto con la clave privada y custodiarlos en lugar seguro siempre protegidos por contraseña. Nunca se debe entregar copia de la clave privada a nadie bajo ningún concepto.

¿Qué pasos debo seguir para instalar/importar los Certificados Raíz de una Autoridad de Certificación en Windows?

Primero debemos acceder a la página web de la Autoridad de Certificación para consultar y descargar los certificados raíz e intermedios según el tipo de certificado de firma que vayamos a utilizar.

Por ejemplo, en caso de que deseemos utilizar certificados de CERES FNMT-RCM, debemos instalar los certificados raíz disponibles en https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

Algunas Autoridades de Certificación proporcionan un programa o instalador que importa automáticamente los certificados raíz en los navegadores del equipo.

En el caso de la requerirse la instalación manual de los certificados raíz para su uso en Internet Explorer o en Chrome, es suficiente con abrir cada uno de los certificados descargados y pulsar sobre Instalar certificado y seguir las siguientes instrucciones:

1. Pulsar en siguiente
2. Seleccionar la opción "Seleccionar automáticamente el almacén de certificados en base al tipo de certificado" y pulsar en siguiente
3. Pulsar en finalizar

En caso del Navegador Mozilla Firefox, consulta la pregunta frecuente "Qué pasos debo seguir para instalar/importar los Certificados Raíz de una Autoridad de Certificación en el navegador Mozilla Firefox".

¿Puedo tener más de un Certificado instalado en mi navegador?

Sí, podrá tener más de uno. El número exacto dependerá de la versión de su navegador.

¿Se puede tener el mismo Certificado en varios navegadores?

Sí, una vez que se haya descargado el certificado, se puede instalar en varios navegadores utilizando las opciones de exportación e importación de certificados.

CERTIFICADOS EN EL NAVEGADOR – INTERNET EXPLORER (WINDOWS)

¿Cómo puedo importar un certificado de firma en Internet Explorer?

Para importar un certificado en Internet Explorer debemos realizar los siguientes pasos:

1. Acceder al menú Herramientas - Opciones de Internet - Contenido - Certificados. La pestaña "Personal" (por defecto) muestra una pantalla con la relación de Certificados personales instalados en nuestro navegador.
2. Pulsamos el botón "Importar", aparecerá un Asistente que nos guiará durante toda la importación del certificado. Pulsamos el botón "Siguiente" y en examinar seleccionamos la ruta y el nombre del fichero del certificado que queremos importar y pulsamos "Siguiente". Si al situarnos en la ruta o carpeta donde está almacenado el certificado no lo vemos, cambiaremos el filtro de ficheros de la parte inferior y seleccionaremos Todos los archivos (*.*).

3. En la siguiente ventana se nos pide la contraseña con la que está protegido el fichero, la introducimos y marcamos la casilla “Marcar la clave privada como exportable” para que podamos volver a exportar el certificado con su clave privada y “Habilitar protección segura...”. Pulsamos “Siguiente”.
4. A continuación nos indica donde podemos colocar el certificado importado, dejaremos la opción por defecto y pulsaremos “Siguiente” y “Finalizar”
5. Por seguridad estableceremos una contraseña a nuestro certificado pulsando “Nivel de seguridad” para ponerlo en alto. Asignamos una contraseña y su confirmación. Pulsamos finalizar y nos pedirá que le asignemos la contraseña o PIN con la que deseemos proteger la clave (no tiene por qué ser la misma que la contraseña que hemos introducido en el paso 3).
6. Finalizamos el asistente.

Si todo es correcto aparecerá un cuadro informándonos de que el certificado ha sido importado correctamente

¿Cómo puedo exportar un certificado de firma en Internet Explorer?

Para exportar certificados personales en Internet Explorer debemos seguir los siguientes pasos:

1. Acceder al menú Herramientas, Opciones de Internet. Una vez allí, seleccionaremos la pestaña “Contenido”. En el apartado de Certificados pulsaremos el botón de “Certificados” y una vez en la ventana pulsaremos la pestaña “Personal”. Aquí se nos muestra una pantalla con la relación de Certificados personales instalados en nuestro navegador. Seleccionamos el que queremos exportar y pulsamos el botón “Exportar”.
2. A partir de este momento nos guiará un asistente de Windows.
3. Exportación de Certificados con la clave Privada
4. Dejaremos las opciones tal y como se nos muestran por defecto y pulsamos “Siguiente”
5. Llegamos a una pantalla donde se nos pide una contraseña y su validación para proteger el archivo que contiene el Certificado exportado. Las introducimos y pulsamos el botón “Siguiente”
6. En el siguiente cuadro de dialogo indicaremos la ruta y el nombre del archivo que queremos que contenga el certificado exportado, pulsaremos el botón “Siguiente”
7. A continuación se nos muestra una ventana con las características del certificado exportado, pulsaremos el botón “Finalizar” y nos aparece un mensaje de aviso diciendo que la clave privada va a ser exportada, pulsamos “Aceptar” y si la operación ha sido correcta se nos mostrará un cuadro informándonos de que el certificado ha sido exportado con éxito.

NOTA: Haga una copia de seguridad a disco de su certificado junto con la clave privada y guárdela en lugar seguro. Nunca entregue copia de su clave privada a nadie bajo ningún concepto.

¿Cómo puedo eliminar un certificado en Internet Explorer?

Para eliminar Certificados Personales en Internet Explorer debemos seguir los siguientes pasos:

1. Acceder al menú Herramientas, Opciones de Internet.
2. Seleccionaremos la pestaña "Contenido". En el apartado de Certificados pulsaremos el botón de "Certificados" y una vez en la ventana pulsaremos la pestaña "Personal". Aquí se nos muestra una pantalla con la relación de Certificados personales instalados en nuestro navegador.
3. Seleccionamos el que queremos eliminar y pulsamos "Quitar".
4. Nos aparecerá un mensaje de advertencia "No puede descifrar datos cifrados usando los certificados ¿Desea eliminar los Certificados?". Si pulsamos el botón "SI", nuestro Certificado se habrá eliminado de nuestro navegador.

¿Cómo puedo establecer una contraseña de uso de mi certificado en Internet Explorer?

Si su certificado está instalado en internet Explorer y al usarlo en alguna página que lo requiera no le solicita contraseña, pero la quiere establecer siga los siguientes pasos.

1. Exporte CON CLAVE PRIVADA su certificado desde Internet Explorer. Ver pregunta frecuente "Cómo puedo exportar un certificado de firma en Internet Explorer"
2. Vuelva a importar su certificado siguiendo las instrucciones de la pregunta frecuente "Cómo puedo importar un certificado de firma en Internet Explorer"

¿Cómo debo configurar mi navegador para que me solicite seleccionar el certificado que desee utilizar en Internet Explorer?

Deberá acceder a Herramientas/ Opciones de Internet/ Seguridad/ Internet y pulsar en el botón Nivel personalizado

Seleccione la opción desactivar en la categoría "No pedir la selección del certificado del cliente cuando exista uno o ningún certificado".

¿Cómo puedo comprobar la fecha de caducidad de mi certificado en Internet Explorer?

Para comprobar la caducidad de los certificados personales en Internet Explorer deberemos seguir los siguientes pasos:

1. Accedemos al menú Herramientas, Opciones de Internet.
2. Seleccionamos la pestaña Contenido.
3. Pulsamos el botón de Certificados
4. Seleccionamos la pestaña Personal, en la que se muestra la relación de certificados personales instalados en nuestro navegador
5. Hacemos doble clic sobre el certificado que queremos comprobar.
6. La caducidad del certificado coincide con la fecha del fin de validez.

¿Cómo habilitar todos los propósitos de un Certificado en Microsoft Internet Explorer?

Los pasos a seguir son los siguientes:

1. En el menú Herramientas, seleccionamos Opciones de Internet, y una vez aquí seleccionamos la pestaña de Contenido.
2. En la sección correspondiente a Certificados pinchamos sobre el botón llamado Certificados, seleccionamos la pestaña Personal (u otra aquella pestaña en la que se encuentre el certificado al que queremos habilitar todos los propósitos).
3. Pinchamos 2 veces sobre el certificado correspondiente, seleccionamos la pestaña Detalles, y pinchamos en el botón Modificar Propiedades. Dentro del apartado Propósitos de los certificados, deberemos marcar la opción: Habilitar todos los propósitos para este certificado.

¿Por qué al importar una copia de seguridad de mi certificado en Internet Explorer se instala en la pestaña de Otras personas y no en Personal?

El problema que le ocurre puede estar debido a que la copia de seguridad que usted quiere importar tiene extensión CER/p7b (el icono es un diploma) y no es correcta.

La correcta es PFX / p12 (el icono es un sobre con una llave superpuesta). Esto sucede porque al realizar el proceso de exportación (copia de seguridad) no se marcó la opción de "Exportar clave privada".

Esto implica que la importación de una copia .cer se instale siempre en la pestaña de "Otras Personas" y el certificado no es operativo al no tener clave privada. Si no puede volver a realizar una exportación del certificado original, tendrá que solicitar uno nuevo a la Autoridad de Certificación.

¿Qué hago si al intentar exportar mi certificado con clave privada en Internet Explorer me aparece el error: "Error en la exportación. Tipo especificado no es válido"?

Este error es debido a que está intentando exportar su certificado con clave privada desde la tarjeta. No es posible la exportación del certificado con clave privada desde la tarjeta.

Cuando uso mi certificado en I.E. muestra la siguiente ventana: Se están firmando datos con su clave privada de intercambio. Contraseña para/Clave privada de CryptoA junto con un cuadro de texto para introducir una contraseña ¿A qué se refiere?

Esta contraseña protege la clave privada asociada a su certificado. La contraseña es personal del usuario y se establece justo antes de obtener el código de solicitud cambiando el nivel de seguridad de "Medio" (opción por defecto) a "Alto" o bien cuando finaliza el proceso de importación de una copia de seguridad estableciendo igualmente un nivel de seguridad "Alto".

Instalación/Actualización de los certificados raíz de una Autoridad de Certificación en Internet Explorer

Ver pregunta frecuente "Qué pasos debo seguir para instalar/importar los Certificados Raíz de una Autoridad de Certificación en Windows".

¿Cómo puedo establecer un nombre descriptivo al certificado para que me lo muestre Internet Explorer al solicitarme el certificado?

Para cambiar el nombre a mostrar para que lo pueda identificar mejor haga lo siguiente:

- Abra Internet Explorer y pulse Herramientas / Opciones / Contenido / Certificados
- Haga doble clic en el certificado que desee modificar el nombre o alias
- Pulse la pestaña Detalles y el botón Editar propiedades
- En Nombre descriptivo escriba el nombre que quiera que se le muestra cada vez que tiene que elegir un certificado para acceder a alguna aplicación (hacer esto no modificará el certificado sino el nombre o alias a mostrar). Pulse aceptar.

Si desea eliminar el nombre o alias asignado y volver al nombre inicial solo tiene que borrar todo el contenido de Nombre descriptivo y aceptar las ventanas.

CERTIFICADOS EN EL NAVEGADOR – MOZILLA FIREFOX (WINDOWS Y LINUX)

¿Cómo puedo importar mi certificado con Mozilla Firefox?

Para importar un certificado al almacén de Firefox correctamente, la copia de seguridad debe tener contraseña asignada, o lo que es lo mismo, cuando se exportó se le asignó una contraseña y no se dejó en blanco.

- Acudir al almacén de certificados del navegador Mozilla Firefox:
- Herramientas / Opciones / Avanzado, pestaña de Cifrado o Certificados (según versión) / Ver Certificados, pestaña “Sus Certificados”.
- Para Firefox v56 o superior: Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados / botón Ver certificados, pestaña “Sus Certificados”.
- Pulse en el botón “Importar”
- Busque la ubicación (disco duro, cd, memoria USB, unidad de red) de la copia del certificado que quiere importar.
- Inserte la contraseña maestra de su navegador (si estableció alguna). Si es la primera vez que usa este navegador con certificados, inserte una contraseña y la confirmación, esta contraseña será requerida cada vez que quiera usar su certificado en las webs que lo requieran.
- Inserte la contraseña con la que protegió su copia de seguridad

Si todo el proceso es correcto, recibirá el siguiente mensaje:

- “Se han restaurado satisfactoriamente su(s) certificado(s) de seguridad y clave(s) privada(s).”

¿Cómo puedo exportar mi certificado con Mozilla Firefox?

Acudir al almacén de certificados del navegador Mozilla Firefox:

- Herramientas / Opciones / Avanzado, pestaña de Cifrado o Certificados (según versión) / Ver Certificados, pestaña "Sus Certificados".
- Para Firefox v56 o superior: Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados / botón Ver certificados, pestaña "Sus Certificados".
- Seleccione su certificado y pulse "Hacer copia".
- Indique dónde quiere realizar su copia de seguridad (disco duro, cd, unidad de red, etc.)
- Inserte la contraseña maestra de su navegador (si estableció alguna).
- Inserte una contraseña y la confirme para proteger la copia de seguridad que va a realizar.

Si todo el proceso es correcto, recibirá el siguiente mensaje:

- "La copia de seguridad de su(s) certificado(s) de seguridad y clave(s) privada(s) se ha realizado con éxito."

¿Cómo puedo exportar sin clave privada mi certificado con Mozilla Firefox?

Acceder a la ruta del contenedor de certificados:

- Herramientas / Opciones / Avanzado, pestaña de Cifrado o Certificados (según versión) / Ver Certificados, pestaña "Sus Certificados".
- Para Firefox v56 o superior: Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados / botón Ver certificados, pestaña "Sus Certificados".
- A continuación se le abrirá una pantalla que muestra dos pestañas: General y Detalles.
- Elegimos la pestaña de Detalles y pulsamos el botón Exportar.
- Se nos abre una ventana emergente donde nos indica donde queremos guardar la copia que vamos a realizar (por defecto el nombre de la copia lo pone el propio asistente; y son los datos del certificado) y pulsamos guardar.
- Antes de guardar, en tipo de archivo seleccionamos la opción más adecuada según el tipo de copia a realizar.

¿Cómo puedo eliminar mi certificado con Mozilla Firefox?

Acudir al almacén de certificados del navegador Mozilla Firefox:

- Herramientas / Opciones / Avanzado, pestaña de Cifrado o Certificados (según versión) / Ver Certificados, pestaña "Sus Certificados".
- Para Firefox v56 o superior: Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados / botón Ver certificados, pestaña "Sus Certificados".

- Seleccione su certificado y pulse “Eliminar”.
- Preguntará si está seguro de eliminar el certificado, damos al botón de “Aceptar”

Su certificado habrá sido eliminado correctamente.

¿Cómo puedo establecer un nombre identificativo a mi certificado para utilizarlo en Firefox si actualmente se identifica con números?

Si al utilizar su certificado con Mozilla Firefox en cualquier aplicación le aparece su certificado identificado por números, tiene la opción de establecerle un nombre identificativo siguiendo las siguientes instrucciones:

- Instale su certificado en el navegador Internet Explorer.
- Vaya a Herramientas - Opciones de internet - Contenido - Certificados
- Seleccione el certificado instalado y haga doble clic sobre él
- Pulse la pestaña Detalles y el botón “Editar propiedades”
- Establezca el nombre deseado en el campo “nombre descriptivo”; este será el nombre que verá cuando utilice su certificado con Firefox. Recomendamos establecer el nombre completo y NIF. Acepte las ventanas.
- Exporte de nuevo su certificado con clave privada y vuelva a importarlo a Mozilla Firefox.
- Cuando lo use ya estará identificado correctamente.

¿Qué es la Master Password o Contraseña Maestra en Mozilla Firefox?

La contraseña maestra (Master Password) es la contraseña del almacén de certificados del navegador Mozilla Firefox y por defecto no está establecida, siempre es el usuario quien la establece.

Esta contraseña maestra es una característica del navegador, no del certificado, y sirve para proteger los datos sensibles almacenados como por ejemplo todos los certificados.

Generalmente la contraseña maestra se establece justo antes de obtener el código de solicitud en pantalla o bien cuando se realiza la importación de un fichero de copia de seguridad de un certificado de firma digital.

Esta contraseña es requerida cada vez que se accede al almacén de certificados de este navegador y es la misma contraseña para todos los certificados que tenga almacenados en esa sesión/perfil de navegador. El sistema le solicitará esta contraseña hasta que cancele la acción. Si no recuerda la contraseña (que es personal del usuario) tendrá que restablecerla.

Si restablece la contraseña pierde todos los certificados instalados en el navegador y las solicitudes de certificados, asegúrese de tener copias de seguridad de los certificados. Para restablecer la contraseña:

- en la barra de direcciones de Firefox escriba lo siguiente y después pulse “Intro”:

  » chrome://pippki/content/resetpassword.xul

- A continuación pulse “Restablecer”

¿Cómo puedo restablecer la contraseña maestra en Firefox?

Si resetea la contraseña pierde todos los certificados instalados en el navegador y las solicitudes de certificados, asegúrese de tener copias de seguridad de los certificados. Para restablecer la contraseña:

- en la barra de direcciones de Firefox escriba lo siguiente y después pulse " Intro ":

  » chrome://pippki/content/resetpassword.xul

- A continuación pulse "Restablecer"

¿Qué pasos debo seguir para instalar/importar los Certificados Raíz de una Autoridad de Certificación en el navegador Mozilla Firefox?

Primero debemos acceder a la página web de la Autoridad de Certificación para consultar y descargar los certificados raíz e intermedios según el tipo de certificado de firma que vayamos a utilizar.

Por ejemplo, en caso de que deseemos utilizar certificados de CERES FNMT-RCM, debemos instalar los certificados raíz disponibles en https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

Algunas Autoridades de Certificación proporcionan un programa o instalador que importa automáticamente los certificados raíz en los navegadores del equipo.

En el caso de la requerirse la instalación manual de los certificados raíz para su uso en Mozilla Firefox, debe realizar los siguientes pasos:

- Herramientas / Opciones / Avanzado, pestaña de Cifrado o Certificados (según versión) / Ver Certificados.
- Para Firefox v56 o superior: Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados / botón Ver certificados.
- Seleccione la pestaña autoridades, de ser así, pulse el botón importar.
- Seleccione la ubicación de uno de los certificados raíz y pulse el botón abrir.
- Marque las casillas correspondientes a los diferentes propósitos y pulse el botón aceptar.
- Realice los mismos pasos con el resto de certificados que indique la Autoridad de Certificación.

Por ejemplo, en el caso de CERES FNMT-RCM, es necesario importar: AC Raíz FNMT-RCM, AC Usuarios, AC Representación, AC Administración Pública y AC Componentes Informáticos.

Al firmar con Mozilla Firefox se produce el error: "Su certificado no ha permitido generar una firma válida" ¿Qué pasos debo seguir para resolver dicha problemática?

Generalmente ese problema se produce porque no se encuentran instalados en Mozilla Firefox los Certificados Raíz de la Autoridad de Certificación que emitió la firma que está utilizando.

Vea la pregunta frecuente "¿Qué pasos debo seguir para instalar/importar los Certificados Raíz de una Autoridad de Certificación en el navegador Mozilla Firefox?"

¿Cómo puedo comprobar la fecha de caducidad de mi certificado en Mozilla Firefox?

Para comprobar la caducidad de los certificados personales en Firefox debemos seguir los siguientes pasos:

- Herramientas / Opciones / Avanzado, pestaña de Cifrado o Certificados (según versión) / Ver Certificados.
- Para Firefox v56 o superior: Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados / botón Ver certificados.
- Pulsamos la pestaña Sus Certificados. Aquí se nos muestra una relación de los certificados personales instalados en el navegador
- Hacemos doble clic en el certificado que queremos comprobar la caducidad y en el campo Validez se nos muestra la fecha de inicio y de fin de validez.

¿Cómo puedo acceder al almacén de claves de Mozilla Firefox en Linux y en MAC?

- En LINUX: la ruta es Editar/ Preferencias/ Avanzado/ Cifrado o Certificados/ Ver Certificados.
- En MAC: la ruta es Firefox/ Preferencias/ Avanzado/ Cifrado o Certificados/ Ver Certificados.

CERTIFICADOS EN EL NAVEGADOR – GOOGLE CHROME (WINDOWS Y LINUX)

¿Cómo puedo importar un certificado digital con Google Chrome en Windows?

Google Chrome en Windows utiliza el almacén de claves de Internet Explorer. Siga los pasos que se indican en la pregunta frecuente "¿Cómo puedo importar un certificado de firma en Internet Explorer?"

¿Cómo puedo exportar un certificado digital con Google Chrome en Windows?

Google Chrome en Windows utiliza el almacén de claves de Internet Explorer. Siga los pasos que se indican en la pregunta frecuente "¿Cómo puedo exportar un certificado de firma en Internet Explorer?"

¿Cómo puedo eliminar un certificado digital con Google Chrome en Windows?

Google Chrome en Windows utiliza el almacén de claves de Internet Explorer. Siga los pasos que se indican en la pregunta frecuente "¿Cómo puedo eliminar un certificado en Internet Explorer?"

¿Cómo puedo establecer una contraseña de uso de mi certificado en Google Chrome en Windows?

Google Chrome en Windows utiliza el almacén de claves de Internet Explorer. Siga los pasos que se indican en la pregunta frecuente "¿Cómo puedo establecer una contraseña de uso de mi certificado en Internet Explorer?"

¿Cómo importar un certificado con Google Chrome en Linux?

- Para importar un certificado con Google Chrome y Linux diríjase a "Personalizar y Configurar Google Chrome" / Configuración
- En Opciones Avanzadas / HTPPS/SSL pulsamos "Administrar certificados"
- En la pestaña "Tus certificados" pulsamos el botón "importar", seleccionamos ver "Todos los archivos".
- Elegimos el fichero que queremos importar, introducimos la contraseña de exportación y pulsamos aceptar.

¿Cómo exportar un certificado con Google Chrome en Linux?

- Para exportar un certificado con Google Chrome y Linux diríjase a "Personalizar y Configurar Google Chrome" / Configuración
- En Opciones Avanzadas / HTPPS/SSL pulsamos "Administrar certificados"
- En la pestaña "Tus certificados" seleccionamos el certificado que queremos exportar y pulsamos el botón Exportar, escribimos el nombre que queremos asignar al archivo y la ruta donde guárdalo. Pulsamos Guardar.

CERTIFICADOS EN EL MÓVIL/TABLET – ANDROID (GOOGLE)

¿Cómo se importa un certificado personal a un dispositivo Android?

Si dispone de copia de seguridad de su certificado digital en su PC u otro dispositivo puede importarlo al almacén de certificados de Android.

Procedimiento:

- Copie el archivo de su copia de seguridad a la raíz de su dispositivo, el archivo puede tener extensión *.p12 o *pfx.
- En su dispositivo acceda a Ajustes - Seguridad - Almacenamiento de credenciales. Pulsar en "Instalar desde la memoria del teléfono" o "desde la tarjeta SD". Elija la copia de seguridad que desea instalar (en caso que haya más de una) e introduzca la contraseña de exportación. Pulse aceptar.
- Asigne un nombre sin espacios al certificado. Elija VPN y aplicaciones. Pulse aceptar.

¿Cómo puedo borrar certificados en Android?

Si ya dispone de su copia de seguridad en un PC o en otro almacenamiento y quiere borrar sus certificados del dispositivo Android haga lo siguiente:

- Vaya a Ajustes - Seguridad - Almacenamiento de credenciales – Credenciales de usuario
- Al pulsar en cada uno de los certificados aparece la opción de "Eliminar" o "Listo"(continuar).

¿Cómo puedo firmar documentos desde Android?

Para poder firmar documentos desde Android, es necesario que utilice una aplicación específica de firma.

El Gobierno de España distribuye la aplicación Cliente móvil @firma a través del Play Store de Google. Es necesario que instale su certificado de firma digital en el dispositivo Android para realizar firmas electrónicas con esta aplicación.

¿Qué otras aplicaciones del Gobierno de España que hacen uso de firma electrónica puedo instalar en Android?

- Notificaciones Electrónicas - DEH
- Port@firmas móvil
- Cl@ve PIN
- Agencia Tributaria

¿Es necesario instalar el certificado de AC Raíz FNMT-RCM en Android si utilizo un certificado de firma de emitido por CERES FNMT-RCM?

Sí, es necesario instalar el certificado AC Raíz FNMT-RCM en Android.

Para ello es necesario descargar el certificado AC Raíz FNMT-RCM en su PC y a continuación copiarlo al dispositivo. Después haga clic sobre él para que se instale.

Si descarga el certificado directamente desde el dispositivo Android éste le pedirá que le asigne un nombre, por ejemplo AC Raíz FNMT RCM, pulse aceptar.

NOTA: Puede ser que el dispositivo le solicite modificar el bloqueo de su pantalla para que le permita utilizar el almacenamiento de credenciales.

A partir de la versión 8 de Android el certificado AC Raíz FNMT-RCM ya vendrá instalado por defecto.

¿Para qué plataformas está disponible la aplicación de "Obtención certificado FNMT"?

Este método de obtención se ha retirado de forma temporal, para realizar un mantenimiento de la aplicación (no hay fecha prevista para la nueva versión).

CERTIFICADOS EN EL MÓVIL/TABLET – IOS (APPLE)

¿Cómo se importa un certificado personal a un dispositivo IOS?

Los certificados de firma no se instalan en los dispositivos IOS de forma general, sino que es necesario instalarlos en cada una de las aplicaciones instaladas que requieran su uso.

Para ello seguiremos las siguientes instrucciones desde un PC:

- Ejecutar iTunes. Si no estuviera instalado, descargamos e instalamos la última versión del programa iTunes en el pc desde: https://www.apple.com/es/itunes/download/.
- Conectamos el iPhone/iPad al pc mediante cable USB.
- Pulsamos sobre el icono del dispositivo iPhone/iPad.
- Aparecerá una opción que se denomina Archivos compartidos, pulsamos sobre esa opción.
- Dentro de Archivos compartidos seleccionamos la aplicación que hace uso de la firma digital, pulsamos en Añadir archivo.. y seleccionamos el certificado.

Los formatos de certificados admitidos son p12 y pfx, protegidos por contraseña.

¿Qué aplicaciones del Gobierno de España que hacen uso de firma electrónica puedo instalar en IOS?

- Cliente @firma
- PAG SNE
- Agencia Tributaria
- Cl@ve PIN
- Portafirmas @firma

CERTIFICADOS EN LA NUBE

¿En qué consiste la centralización de certificados en la nube?

Consiste en la emisión y uso de nuestros certificados electrónicos desde la nube de una Autoridad de Certificación cualificada.

Por ejemplo, las Autoridades de Certificación CAMERFIRMA e IVNOSYS ofrecen servicios de centralización de certificados en la nube, siguiendo dos aproximaciones:

- CAMERFIRMA: El proceso de firma o autenticación hace uso del certificado digital, como si estuviese instalado en la maquina local. El uso de la clave privada requiere de una primera autenticación del usuario ante la plataforma de gestión. Las claves de firma se custodian por un dispositivo seguro, bajo una contraseña que solo conoce el titular del certificado.

- IVNOSYS: unificación y monitorización de todos los certificados digitales, dotando de fiabilidad, seguridad y eficiencia a los procesos, gracias al almacenamiento en la nube de dicha documentación. La firma que se realiza con certificado digital en la nube, permitiendo la aceptación y gestión de documentos desde cualquier lugar y con la mayor seguridad jurídica.

► ¿Cuáles son las ventajas de la centralización de certificados en la nube?

- La gestión de claves centralizada permite a una organización gestionar de una manera centralizada todos los certificados emitidos a sus trabajadores.
- Mejora la seguridad en la custodia de la claves privadas de los certificados.
- Facilita la movilidad de los usuarios entre diferentes equipos de la organización manteniendo los certificados accesibles.
- Trazabilidad en el uso de los certificados digitales de la organización.
- Ahorro importante de costes.

TARJETAS INTELIGENTES

► ¿Qué es una Tarjeta Inteligente?

Una tarjeta inteligente es un dispositivo físico de seguridad, del tamaño, forma y aspecto de una tarjeta de crédito, resistente a la adulteración y copia. Ofrece funciones para almacenar y procesar de manera segura determinada información, certificados de firma digital entre otros. Al igual que las tarjetas SIM de teléfonos móviles, las tarjetas inteligentes están protegidas por un código PIN y un código PUK.

En lo relativo a firma digital, las tarjetas inteligentes custodian de forma segura la clave pública y privada de los certificados de firma, imposibilitando la exportación y uso de la clave de firma fuera de la tarjeta (protección por hardware).

Cada vez que se haga uso de la tarjeta para realizar una firma se solicitará el código PIN que protege a la tarjeta.

► ¿Las tarjetas criptográficas tienen fecha de caducidad?

Las tarjetas criptográficas no caducan, lo que caduca es el certificado que contiene.

► ¿Puedo utilizar tarjetas inteligentes en dispositivos móviles o tabletas?

Sí, si la tarjeta dispone de tecnología RFID/NFC y el móvil o tablet dispone de lector NFC.

Es por ello que podemos utilizar el DNI electrónico 3.0 en dispositivos móviles con soporte NFC. Puede consultar esta guía de uso para conocer el funcionamiento del DNI 3.0: https://www.dnielectronico.es/PDFs/uso_nfc.pdf

¿Puedo exportar un certificado y su clave privada obtenido en tarjeta?

No, un certificado obtenido en tarjeta no se puede exportar con clave privada.

¿Qué software es necesario tener instalado para utilizar las tarjetas inteligentes en Windows?

Es necesario disponer del siguiente software instalado:

- Los drivers del lector de tarjetas que vienen junto con el lector o los puede descargar de la web del fabricante.
- Los drivers y el módulo criptográfico de la tarjeta, que se puede descargar desde la web de la Autoridad de Certificación o de la web del fabricante de la tarjeta.

Por ejemplo, para tarjetas CERES FNMT-RCM hay que instalar el módulo criptográfico TC-FNMT RCM se puede descargar desde https://www.sede.fnmt.gob.es/descargas/descarga-software

En caso de que tuviera instaladas versiones antiguas de los drivers del lector, de los drivers de la tarjeta o del módulo criptográfico, es necesario desinstalarlos previamente desde “Programas y Características”

¿Cómo puedo cambiar el PIN de mi tarjeta?

Debe acceder al software de gestión del módulo criptográfico, que difiere según el fabricante de cada tarjeta.

Para cambiar el PIN de su tarjeta es necesario que disponga del código PIN actual o el código de desbloqueo (PUK) que obtuvo junto a la tarjeta:

- En caso de que conozca el PIN: se solicitará que introduzca el PIN actual el nuevo código PIN, que por motivos de seguridad se introducirá dos veces.
- En caso de que desconozca el PIN actual: Se solicitará que introduzca el código de desbloqueo (PUK) y el nuevo código PIN, que por motivos de seguridad se introducirá dos veces.

Por ejemplo, para cambiar el PIN conociendo el PIN actual en tarjetas CERES FNMT-RCM siga los siguientes pasos:

- Vaya a Inicio > Programas > FNMT-RCM > Utilidades > Cambio de PIN. Le aparecerá un asistente para cambiar el PIN.
- Pulse siguiente, escriba el PIN actual de su tarjeta y el PIN nuevo que desee con su confirmación.
- Pulse siguiente.
- Si el cambio se ha realizado con éxito le aparecerá un mensaje: El PIN se ha actualizado correctamente.

¿Cómo puedo cambiar el PIN de mi tarjeta con Mozilla Firefox?

Inserte la tarjeta, abra Mozilla Firefox y acuda al almacén de certificados del navegador:

- Herramientas / Opciones / Avanzado, pestaña Certificados, botón "dispositivos de seguridad"
- Para Firefox v56 o superior: Herramientas / Opciones / Privacidad y Seguridad / Certificados / botón "dispositivos de seguridad"
- Seleccione en el menú de la izquierda el objeto del módulo PKCS#11 correspondiente.
- A la derecha seleccione "Cambiar contraseña", introduzca el PIN actual y el nuevo dos veces. Si todo es correcto se le informará que la contraseña maestra ha sido cambiada correctamente, esto quiere decir que el PIN de la tarjeta se ha cambiado correctamente.

Por ejemplo, para tarjetas CERES FNMT-RCM el objeto se denomina TC-FNMT v1 o similar.

¿Cuántos intentos de PIN y código de desbloqueo admite la tarjeta criptográfica?

Para acceder a cualquier aplicación con la tarjeta criptográfica es necesario introducir el PIN de la misma.

El PIN y el código de desbloqueo (PUK) se entregan en una carta junto con la tarjeta cuando la adquiere. Las tarjetas suelen venir con un número de serie impreso que debe coincidir con el número de serie de la carta.

NOTA: Dependiendo de la forma que la adquirió puede que este número de serie no se refleje.

Tenga en cuenta que si introduce 3 veces seguidas y erróneamente el PIN de la tarjeta ésta se bloqueará. Con el código de desbloqueo (PUK) puede desbloquearla, pero si introduce 3 veces seguidas y erróneamente el código de desbloqueo la tarjeta se bloqueará definitivamente sin posibilidad de recuperación.

Cuando reciba su tarjeta si lo desea puede modificar el PIN por uno personalizado con la aplicación de Cambio de PIN.

La Autoridad de Certificación no guarda ni el PIN ni el código de desbloqueo en ningún caso por lo que no se lo podrá facilitar si lo extravía.

¿Cómo puedo desbloquear mi tarjeta criptográfica?

- Para desbloquear su tarjeta es necesario que tenga a mano el código de desbloqueo (PUK) que obtuvo junto a la tarjeta.
- Debe acceder al software de gestión del módulo criptográfico, que difiere según el fabricante de cada tarjeta.
- Se solicitará que introduzca el código de desbloqueo (PUK) y el nuevo código PIN, que por motivos de seguridad se introducirá dos veces.

Por ejemplo, para tarjetas CERES FNMT-RCM ya instaladas en el equipo: Inicio > Programas > FNMT-RCM > Utilidades > Desbloqueo de Tarjeta.

¿Puedo obtener el código de desbloqueo de mi tarjeta criptográfica si no dispongo del mismo?

Las Autoridades de Certificación no conservan ningún código asociado a la tarjeta, estos datos son únicos y se facilitan con la tarjeta sin existir copia de los mismos.

¿Puedo instalar un certificado obtenido vía software/navegador en la tarjeta?

Sí, para ello tiene que exportar con clave privada el certificado instalado en el navegador (durante el proceso se le solicitará introducir una contraseña). Puede exportarlo a una ubicación del disco duro o a un pendrive y después importarlo a la tarjeta.

Dependiendo de su navegador el proceso de exportación se realizará de una forma o de otra. Si necesita ayuda, acuda a la categoría "Exportación e importación de certificados" para conocer más acerca de este proceso.

¿Cómo importar el certificado a la tarjeta?

Para importar un certificado de firma en la tarjeta, es necesario que disponga de los certificados de clave pública y clave privada en formato pfx o p12 e importarlos desde el software de gestión del módulo criptográfico, que difiere según el fabricante de cada tarjeta.

Por ejemplo, para importar un certificado en tarjetas CERES FNMT-RCM siga los siguientes pasos:

- Debe tener instalada la última versión del módulo criptográfico Ceres, en caso de no tenerla consulte la siguiente página web https://www.sede.fnmt.gob.es/descargas/descarga-software
- Debe acceder a Inicio> Programas> FNMT-RCM> Utilidades> ejecutar "Importador de certificados"
- Aparecerá un asistente de importación con la pantalla principal de bienvenida, en este paso damos al botón de siguiente, pulsamos el botón de examinar y buscamos el fichero pfx/p12 (previamente exportado de su navegador), lo seleccionamos, pulsamos aceptar y Siguiente.
- En la siguiente ventana se introducirá la contraseña del almacén de claves p12/pfx y pulsaremos en siguiente.
- Si todo va bien se solicitará el PIN de la tarjeta.
- El proceso de importación finalizará indicándole si ha sido satisfactorio o, en caso contrario, si ha ocurrido un error.

¿Cómo puedo importar mi certificado a una tarjeta criptográfica con Mozilla Firefox?

NOTA: Recuerde que para importar un certificado a una tarjeta criptográfica con Firefox correctamente, la copia de seguridad debe tener contraseña asignada, esto es, que cuando se exportó se le asignó dicha contraseña y no se dejó en blanco.

- Inserte la tarjeta, abra Mozilla Firefox y acuda al almacén de certificados del navegador:
- Herramientas / Opciones / Avanzado, pestaña Cifrado o Certificados (según versión) / Ver Certificados, pestaña de "Sus Certificados".

- Para Firefox v 56 Menú Herramientas / Opciones / Privacidad y Seguridad / Certificados - botón Ver certificados, pestaña de "Sus Certificados".
- Pulse en el botón "Importar"
- Busque la ubicación (disco duro, cd, memoria USB, unidad de red) de la copia de su certificado que quiere importar (con extensión *.pfx o *.p12).
- Elija el objeto el objeto del módulo PKCS#11 correspondiente. Inserte el PIN de la tarjeta.
- Inserte la contraseña con la que protegió su copia de seguridad.

Por ejemplo, para tarjetas CERES FNMT-RCM el objeto se denomina TC-FNMT v1 o similar.

Si todo el proceso es correcto, recibirá el siguiente mensaje: "Se han restaurado satisfactoriamente su(s) certificado(s) de seguridad y clave(s) privada(s)."

► ¿Cómo puedo eliminar un certificado instalado en tarjeta?

Si usted utiliza su tarjeta con FIREFOX, directamente desde el almacén de certificados (con la tarjeta insertada en el lector) puede eliminar el certificado pulsando en el botón "Quitar". Si su navegador Firefox no lee su tarjeta realice la configuración según instrucciones del fabricante o la Autoridad de Certificación.

Si usa Internet Explorer no lo va a poder eliminar directamente desde el almacén de certificados de este navegador. En este caso, debe usar el software de la tarjeta proporcionado por el fabricante o la Autoridad de Certificación.

En el caso de las tarjetas CERES FNMT-RCM debe instalar la UTILIDAD PARA GESTIÓN DE CERTIFICADOS EN TARJETA CRIPTOGRÁFICA CERES: https://www.sede.fnmt.gob.es/documents/10445900/10528994/Gestor_de_Certificados.zip

► ¿Cuántos certificados puede almacenar la tarjeta criptográfica?

Se pueden instalar varios certificados en una tarjeta criptográfica, dependiendo de la capacidad de almacenamiento de la misma y del tamaño/longitud de clave criptográfica que se utilice.

Por ejemplo, las tarjetas CERES FNMT-RCM en su versión actual admiten hasta 10 certificados electrónicos estándar X.509.v3 de 2048 bits. En versiones anteriores admiten hasta 6.

TARJETAS INTELIGENTES – CERES FNMT-RCM

► ¿Dónde puedo obtener información acerca de Tarjetas Inteligentes CERES FNMT-RCM y acerca de resolución de problemas con las mismas?

Puede obtener soporte técnico a través la página web de CERES FNMT-RCM en el enlace https://www.sede.fnmt.gob.es/preguntas-frecuentes/acerca-de-las-tarjetas-inteligentes

Puede resolver, entre otras dudas o problemas, las siguientes cuestiones:

- ¿Puedo usar la tarjeta CERES en una distribución de Linux?
- ¿Dónde puedo adquirir una Tarjeta criptográfica CERES?
- Instalación manual del módulo criptográfico en Firefox para Windows
- Instalación manual del módulo criptográfico en Firefox para Linux
- Instalación manual del módulo criptográfico en Firefox para MAC

CERTIFICADOS Y FIRMA DIGITAL EN EL CORREO ELECTRÓNICO

► ¿Cómo puedo asegurar la confidencialidad de los correos electrónicos que envío?

Se puede asegurar la confidencialidad de los correos electrónicos cifrando el mensaje.

Ver pregunta frecuente: ¿Qué es la encriptación o cifrado?

► ¿Cómo puedo firmar los correos electrónicos que envío y asegurar su integridad?

Mediante el uso de una firma digital, que es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

La firma digital no implica que el mensaje esté cifrado, esto es, un mensaje firmado será legible en función de que esté o no cifrado.

Ver pregunta frecuente: ¿Qué es la Firma Digital?

► ¿Qué necesita un Certificado para usarse en correo electrónico seguro?

Para poder utilizar su certificado éste debe tener ciertas características, la principal es que tenga una dirección de correo electrónico incluida en el propio certificado y sea la misma dirección de correo electrónico que la que tenga configurada en su cliente de correo, según lo establecido por el protocolo S/MIME descrito en el RFC 1521 (http://www.ietf.org/).

En el momento de la acreditación en la oficina de registro solicite al registrador que le incluya el correo electrónico en el certificado para poder firmar correos, el registrador marcará una casilla habilitada para tal fin en la aplicación de registro.

► Si tengo un Certificado sin dirección de correo electrónico asociada, ¿qué debo hacer?

Si el certificado no tiene ninguna dirección de correo asociada, y si Ud. desea utilizar las ventajas que ofrece el certificado en el uso del correo electrónico seguro, deberá solicitar la revocación del mismo y solicitar otro certificado mediante los procedimientos habituales, es decir, solicitando un nuevo código de solicitud, acreditándose en una oficina de registro comunicando al registrador que le incluya la dirección de correo electrónico en el certificado para poder firmar correos y posteriormente descargando el certificado.

Recepción de un mensaje firmado y posibles errores

A la hora de recibir un mensaje nos podemos encontrar con una serie de errores.

- **Se modificó el contenido después de firmar el mensaje**: Si aparece este mensaje marcado, nuestro mensaje ha sido modificado, no confiar en dicho mensaje.
- **Certificado no confiable**: Este tipo de error suele darse porque no tenemos instalado el certificado raíz de la Autoridad de Certificación.
- **Certificado revocado**: Al indicarnos que el identificador digital ha sido revocado, no debemos confiar en ese certificado.
- **Certificado caducado**: Si nos aparece este mensaje de error, comprobaremos que el certificado está realmente caducado o que la fecha de nuestro equipo está mal. Para verificar la fecha del certificado pulsaremos en la parte de abajo en uno de los botones que dice Ver certificado, ahí podemos observar la validez de este.
- **La dirección de correo del certificado no es la misma que la del remitente**: Nos indica que el remitente está haciendo uso de su certificado con otra cuenta distinta a la que adjunto en su certificado.

¿Qué debo hacer si envío un correo firmado digitalmente y al receptor le aparece un aviso de seguridad indicándole que el mensaje fue alterado?

Si usted tiene la certeza de que no ha modificado el mensaje después de haberlo firmado, verifique lo siguiente:

- Existencia de filtros de contenido en servidores de correo o cortafuegos que no reconozcan la firma y descarten el mensaje (debido a la estructura del mensaje, pueden considerar la firma como un adjunto desconocido).
- Existencia de filtros que modifiquen el contenido del correo e invaliden la firma. Por ejemplo, algunos antivirus introducen una línea con un mensaje que anuncia que el mensaje no contiene virus. Téngase en cuenta que modificar o insertar un solo carácter invalida la firma, y el cliente de correo mostrará un mensaje advirtiendo que el mensaje ha sido modificado cuando realmente no ha sido así.

Para estas dos opciones si usted tiene antivirus y/o filtros anti-spam, puede intentar enviarse un correo a sí mismo con estos elementos desactivados.

CERTIFICADOS Y FIRMA DIGITAL EN EL CORREO ELECTRÓNICO – OUTLOOK 2010/2013

Manual uso de correo seguro de Outlook 2013

Descargue el manual de uso de correo seguro en Outlook 2013

Manual uso de correo seguro de Outlook 2010

Descargue el manual de uso de correo seguro en Outlook 2010

¿Para qué necesito certificados ajenos en Outlook 2010 / 2013?

Si deseamos enviar un mensaje a alguien de modo que solo el destinatario pueda leerlo, el mensaje debe ser cifrado. Para poder cifrar el mensaje es necesario tener el certificado del destinatario.

¿Cómo se obtiene un certificado ajeno de un mensaje firmado?

Si recibimos un mensaje firmado y queremos obtener su certificado seguiremos los siguientes pasos:

- Abrir el mensaje.
- Si el mensaje está firmado aparecerá un icono de color rojo. Pulsaremos sobre él y en Detalles haremos clic sobre el Firmante.
- Pulsamos el botón “Ver detalles” y “Ver certificado”.
- En la pestaña Detalles mediante el botón Copiar en archivo podremos copiar el certificado del remitente.

¿Cómo se cifra por defecto todos los mensajes salientes en Outlook 2010 / 2013?

Para poder enviar un correo cifrado, dicho correo se cifra con la parte pública del certificado del destinatario.

- Abra su libreta de direcciones y pulse en el contacto que desee enviar el correo.
- En la ficha “Mostrar” pulse en Certificados. En Importar seleccione el certificado (*.cer) de su contacto. Guarde los cambios y cierre su libreta de direcciones.

Para cifrar el correo siga las siguientes instrucciones:

- Acceder a Archivo - Opciones - Centro de Confianza.
- Pulse el botón “Configuración del Centro de Confianza” y la opción “Seguridad del correo electrónico”.
- Marque la casilla “Cifrar contenido y datos adjuntos para mensajes salientes”.
- Envíe el correo a su destinatario.

¿Cómo se cifra un correo en el momento de su envío en Outlook 2010 / 2013?

Para poder enviar un correo cifrado, dicho correo se cifra con la parte pública del certificado del destinatario.

- Abra su libreta de direcciones y pulse en el contacto que desea enviar el correo.
- En la ficha “Mostrar” pulse en Certificados. En Importar seleccione el certificado (*.cer) de su contacto. Guarde los cambios y cierre su libreta de direcciones.

Para cifrar un correo siga las siguientes instrucciones:

- Redacte su correo.
- Acceder a Archivo - Propiedades. En el botón "Configuración de Seguridad" marque la casilla Cifrar el contenido del mensaje y los datos adjuntos. Pulse aceptar y cerrar.
- Envíe su correo.

► Agregar un certificado para firmar a tu cuenta de Outlook 2010 / 2013

- Acceder a Archivo - Opciones - Centro de Confianza.
- Pulse el botón "Configuración del Centro de Confianza" y la opción "Seguridad del correo electrónico".
- Pulse el botón Importar o exportar. En examinar seleccione la copia de seguridad de su certificado (Éste deberá tener extensión *.pfx ó *.p12), asigne su contraseña y un nombre que identifique su certificado. Pulse Aceptar y confirme.

NOTA: Al importar su certificado en Outlook 2010 éste también se importará a su navegador Internet Explorer. Si su certificado ya está en el navegador no hace falta agregarlo.

► Configuración para firmar por defecto en Outlook 2010 / 2013

- Acceder a Archivo - Opciones - Centro de Confianza.
- Pulse el botón "Configuración del Centro de Confianza" y la opción "Seguridad del correo electrónico".
- Marcar la casilla "Agregar firma digital a los mensajes salientes".

NOTA: Recuerde que para poder firmar un correo es imprescindible que su certificado digital contenga una dirección de correo electrónico y ésta sea la misma que la que está configurada en su cliente de correo.

► ¿Cómo se firma en Outlook 2010 / 2013?

Si el certificado que va a utilizar para firmar está instalado en su navegador Internet Explorer siga las siguientes instrucciones para firmar un correo.

- Redacte su correo.
- Acceder a Archivo - Propiedades. En el botón "Configuración de Seguridad" marque la casilla "Agregar firma digital a este mensaje".
- En el botón "Cambiar configuración" compruebe que en el apartado Certificados y algoritmos que está seleccionado su certificado. En el caso de tener instalado más de un certificado en su navegador pulse el botón "Elegir" y le aparecerá un listado de todos los certificados, elija el certificado con el que quiere firmar. Acepte las ventanas y pulse Enviar.

NOTA: Recuerde que para poder firmar un correo es imprescindible que su certificado digital contenga una dirección de correo electrónico y ésta sea la misma que la que está configurada en su cliente de correo.

CERTIFICADOS Y FIRMA DIGITAL EN EL CORREO ELECTRÓNICO – WINDOWS LIVE MAIL

► Recepción de un mensaje firmado y posibles errores (Windows Live Mail)

A la hora de recibir un mensaje nos podemos encontrar con una serie de errores.

- **Se modificó el contenido después de firmar el mensaje**: Si aparece este mensaje marcado, nuestro mensaje ha sido modificado, no confiar en dicho mensaje.
- **Certificado no confiable**: Este tipo de error suele darse porque no tenemos instalado el certificado de la Autoridad de Certificación (CA) que emitió el certificado. Para evitar este tipo de error lo más aconsejable es descargarse el certificado CA.

► ¿Cómo puedo agregar el certificado de un contacto en mi libreta de direcciones para poder enviarle un correo cifrado?

Su contacto le debe enviar su certificado sin clave privada por correo electrónico o enviarle un correo firmado.

En cualquiera de los dos casos debe guardar el certificado en disco.

- Abrir Windows Live Mail - Libreta de direcciones, seleccionar el contacto y pulsar en “Agregar información de contacto”.
- Pulse en el apartado Identificadores, en el botón Importar e importe el certificado.
- Pulse el botón Guardar.

► ¿Cómo configuro mi cuenta de correo en Windows Live Mail para poder cifrar un correo electrónico?

- Pulse en Herramientas > Cuentas. Seleccione su cuenta y pulse en Propiedades.
- En la pestaña Seguridad, en el apartado de “Preferencias de cifrado” seleccione el certificado con el que va a cifrar.
- Pulse Aceptar y cierre las ventanas.
- Redacte su correo, pulse Herramientas > Cifrar.
- Su correo se enviará cifrado.

NOTA: Recuerde que el certificado que elija para cifrar debe estar asignado a su contacto en la libreta de direcciones. *Ver pregunta “¿Cómo puedo agregar el certificado de un contacto en mi libreta de direcciones para poder enviarle un correo cifrado?”*

Si quiere configurar su cuenta para que todos los mensajes que envíe estén cifrados por defecto haga lo siguiente:

- Pulse en Herramientas > Opciones de Seguridad
- En la pestaña Seguridad, apartado “correo seguro” marque la casilla “Cifrar contenido y datos adjuntos de todos los mensajes salientes”.

¿Cómo configuro mi cuenta de correo en Windows Live Mail para poder firmar un correo electrónico?

- Debe tener configurada una cuenta de correo con su correo electrónico en Windows Live Mail.
- Cuando esté configurada debe dirigirse a Herramientas > Cuentas. Seleccione su cuenta y pulse Propiedades.
- En la pestaña Seguridad, en el apartado "Certificado de firma" debe seleccionar el certificado que está instalado en su navegador y que tiene asignada la misma dirección de correo electrónico.

NOTA: Si no dispone de la misma cuenta de correo asignada a su certificado que la que tiene configurada como cuenta en Windows Live Mail debe revocar su certificado y obtener uno nuevo con esta dirección.

- Acepte y cierre las ventanas.
- Redacte su correo electrónico y pulse Herramientas > Firmar digitalmente. Le pedirá la contraseña de su certificado (en caso de que tenga establecida una contraseña).
- El correo que envíe estará firmado por usted.

Si quiere configurar su cuenta para que todos los mensajes que envíe estén firmados por defecto haga lo siguiente:

- Pulse en Herramientas > Opciones de Seguridad
- En la pestaña Seguridad, apartado "correo seguro" marque la casilla "firmar digitalmente todos los mensajes salientes".

CERTIFICADOS Y FIRMA DIGITAL EN EL CORREO ELECTRÓNICO – WINDOWS MAIL

Recepción de un mensaje firmado y posibles errores (Windows Mail)

A la hora de recibir un mensaje nos podemos encontrar con una serie de errores.

- **Se modificó el contenido después de firmar el mensaje:** Si aparece este mensaje marcado, nuestro mensaje ha sido modificado, no confiar en dicho mensaje.
- **Certificado no confiable:** Este tipo de error suele darse porque no tenemos instalado el certificado de la Autoridad de Certificación. Para evitar este tipo de error lo más aconsejable es descargarse e instalar el certificado raíz de la Autoridad de Certificación.
- **Certificado revocado:** Al indicarnos que el identificador digital ha sido revocado, no debemos confiar en ese certificado.
- **Certificado caducado:** Si nos aparece este mensaje de error, comprobaremos que el certificado está realmente caducado o que la fecha de nuestro equipo está mal. Para verificar la fecha del certificado pulsaremos en la parte de abajo en uno de los botones que dice Ver certificado, ahí podemos observar la validez de este.
- **La dirección de correo del certificado no es la misma que la del remitente:** Nos indica que el remitente está haciendo uso de su certificado con otra cuenta distinta a la que adjunto en su certificado.

¿Cómo se obtiene un certificado ajeno de un mensaje firmado en Windows Mail?

Normalmente Windows Mail está preparado por defecto para almacenar automáticamente los certificados que nos llegan, pero si no es así, modificaremos nosotros los parámetros siguiendo los siguientes pasos:

- Abrir Windows Mail.
- Pulsar en herramientas.
- Pulsar en opciones.
- Pulsar en seguridad.
- Pulsar en avanzadas.
- Marcar una opción que dice agregar certificados de remitentes a mi libreta de direcciones automáticamente.
- Una vez seleccionado esta opción, la obtención de un certificado ajeno se realizará de forma automática cada vez que alguien nos mande un mensaje firmado.

Si no queremos almacenar todos los certificados que nos llegan sino los que nos interesa:

- desmarcaremos la opción agregar certificados de remitentes a mi libreta de direcciones automáticamente

Para agregar de forma manual el certificado desde el correo firmado::

- Pulsaremos en el distintivo que aparece a mano derecha y se abrirá un menú desplegable y buscaremos una de las opciones que dice ver propiedades de seguridad.
- Dentro del siguiente menú pulsaremos una de las pestañas que dice seguridad y dentro de esta ventana una opción que se encuentra en la parte de abajo que dice agregar a libreta de direcciones.

¿Cómo importar un certificado ajen o cuando lo tenemos en un archivo para cifrar mensajes (Windows Mail)?

- Lo primero que debemos hacer es guardar en la libreta de direcciones la dirección de correo del propietario del certificado.
- Si el certificado viene adjunto a un mensaje, lo guardaremos en disco.
- Nos situaremos sobre la dirección de correo de la persona de la cual queremos obtener su certificado.
- Pulsaremos el botón derecho del ratón y se nos abrirá una ventana y pulsaremos propiedades.
- A continuación pulsaremos una pestaña que dice identificadores digitales y allí pulsaremos importar, buscaremos el certificado donde lo habíamos guardado anteriormente o en el disquete y pulsaremos abrir.
- Nos aparecerá en un cuadro de diálogo el certificado y pulsaremos aceptar.

Desde ese momento ya podremos hacer uso de él para cifrar los mensajes que remitamos al contacto.

¿Cómo se firma en Windows Mail?

Una vez que tenemos el mensaje, para firmarlo buscaremos en la barra de herramientas de Windows Mail un botón que dice firmar, lo pulsaremos y automáticamente aparecerá un símbolo (distintivo) indicando que dicho mensaje es firmado por el emisor.

Configuración para firmar por defecto en Windows Mail

Para que nuestros mensajes enviados sean firmados automáticamente seleccionaremos una opción siguiendo estos pasos:

- Abrir Windows Mail.
- Pulsar en herramientas.
- Pulsar en opciones.
- Pulsar en seguridad.
- Dentro de seguridad hay dos opciones en la parte de abajo que dicen firmar digitalmente todos los mensajes salientes y cifrar contenido y datos adjuntos de todos los mensajes salientes.
- Marcando la opción firmar digitalmente, los mensajes posteriores llevarán automáticamente nuestra firma digital.

¿Cómo importar un certificado propio en Windows Mail para firmar correos electrónicos?

Para poder obtener el certificado propio seguiremos los siguientes pasos:

- Abrir Windows Mail.
- Pulsar en herramientas.
- Pulsar en opciones.
- Pulsar en seguridad.
- Pulsar en identificadores digitales.
- Pulsar Importar. Nos aparecerá una ventana de dialogo que es el asistente el cual nos muestra información acerca de certificados y almacenes de certificados, pulsaremos siguiente. A continuación nos aparecerá un cuadro de diálogo donde seleccionaremos el directorio y el fichero que contienen el certificado a importar pulsando examinar.
- Una vez seleccionado pulsaremos el botón de abrir, acto seguido nos aparecerá un cuadro de diálogo en el que escribiremos la contraseña con la que se ha protegido el fichero que contiene el certificado, marcaremos las dos opciones que aparecen y pulsaremos siguiente.
- La siguiente ventana nos da la posibilidad de seleccionar un almacén de certificados. Dejaremos el que nos muestra por defecto y pulsaremos siguiente.
- A continuación finaliza el asistente, pulsaremos finalizar y nos aparecerá una ventana para poder modificar el nivel de seguridad de la clave.

- Por defecto aparece con un nivel de seguridad medio, pero es recomendable cambiarlo a nivel alto.
  - » Pulsamos nivel de seguridad.
  - » Marcamos nivel alto y pulsamos siguiente.
- En la siguiente ventana pulsaremos finalizar.
- A continuación nos aparecerá otra ventana de dialogo donde nos pedirá la contraseña con la que se ha protegido el fichero que contiene el certificado y pulsaremos aceptar. Nos mostrara un mensaje comunicándonos que la importación ha sido un éxito y veremos nuestro certificado en la ventana de dialogo y finalmente pulsaremos cerrar.

Desde este momento ya estamos preparados para firmar mensajes.

CERTIFICADOS Y FIRMA DIGITAL EN EL CORREO ELECTRÓNICO - THUNDERBIRD

► ¿Para qué necesito Certificados ajenos (Thunderbird)?

Si deseamos enviar un mensaje a alguien de modo que solo el destinatario pueda leerlo, el mensaje debe ser cifrado. Para poder cifrar el mensaje es necesario tener el certificado (solo parte pública) del destinatario.

► ¿Cómo se cifra con Thunderbird?

Para cifrar un correo cifrado debe agregar el certificado del destinatario al almacén de certificados.

- En Thunderbird pulse Editar / Propiedades.
- Seleccione “Seguridad” dentro de la cuenta de correo que tenga configurada.
- Pulse “Ver Certificados” y en la pestaña “Otras personas” importe el certificado (solo parte pública) del destinatario.
- Redacte un correo y escriba la dirección del destinatario.
- Despliegue las opciones del botón Seguridad mediante la flecha y marque “Cifrar este mensaje”.
- Al pulsar el botón Seguridad le aparecerá el certificado con el que cifrará el certificado. Pulse Aceptar.

Si envía el correo se enviará cifrado.

► ¿Para qué necesito mi certificado y una clave privada en Thunderbird?

Para poder realizar las de firma es imprescindible tener mi certificado y una clave privada.

Si no poseo mi certificado no podré firmar ningún mensaje y no podré leer los mensajes que me lleguen cifrados por mi certificado.

¿Cómo se firma con Thunderbird?

Para poder firmar con Thunderbird debe asignar su certificado personal a su cuenta de correo. Para ello:

- Diríjase a Herramientas / Configuración de las Cuentas.
- En el menú izquierdo despliegue el correo que desea configurar. Seleccione seguridad.
- En el apartado Firmado digital seleccione su certificado, con el que desea firmar. Si no le aparece ninguno pulse el botón Importar e importe su copia de seguridad (*.pfx o *.p12)
- Redacte un correo, y en el botón Seguridad marque “Firmar digitalmente este correo”

El mensaje enviado será firmado.

¿Cómo se instalan los certificado raíz de una Autoridad de Certificación en Thunderbird?

Primero debemos acceder a la página web de la Autoridad de Certificación para consultar y descargar los certificados raíz e intermedios según el tipo de certificado de firma que vayamos a utilizar.

En Thunderbird, haga clic sobre su cuenta de correo / Ver configuración de esta cuenta.

Dentro de Seguridad pulse el botón “Ver Certificados”.

En la pestaña Autoridades, pulse en “Importar” y seleccione los certificado raíz

CERTIFICADOS Y FIRMA DIGITAL EN EL CORREO ELECTRÓNICO - MAC

Uso del certificado en correo electrónico con MAC

Al configurar su cuenta de correo en su cliente de correo electrónico en MAC es necesario escribirla en mayúsculas para que coincida con el correo electrónico que aparece en el certificado.

Para poder firmar correos electrónicos desde MAC, debe instalar primero un certificado de firma digital con su clave privada. Para ello puede consultar las siguientes preguntas frecuentes de este documento:

- ¿Cómo puedo importar mi certificado en el llavero de Mac?
- ¿Cómo se instala el módulo criptográfico en MAC?

AUTOFIRMA

¿Qué es la aplicación Autofirma?

Autofirma es una aplicación de firma realizada por el Gobierno de España.

Su principal objetivo es ofrecer al usuario un sistema de firma en el que éste pueda firmar cualquier tipo de documento de manera sencilla, tanto desde un navegador web como mediante una aplicación de escritorio. También está ideada para autenticarse mediante certificado en páginas web que se integren con ella.

Para firmar una documento mediante la aplicación de escritorio, simplemente se debe indicar el fichero a firmar y la aplicación escoge automáticamente el formato de firma qué debe aplicar, liberando así, al usuario de cualquier duda técnica.

¿Desde dónde se puede descargar la aplicación Autofirma?

La aplicación Autofirma se puede descargar desde el portal firmaelectronica.gob.es [http://firmaelectronica.gob.es/Home/Descargas.html].

¿Qué tipos de documentos se pueden firmar con Autofirma?

Formatos de documentos con firma nativa:

- Documentos PDF – Firma PADES
- Documentos OOXML de Microsoft Office – OOXML
- Documentos ODF de LibreOffice u OpenOffice
- Facturas electrónicas – FacturaE

Además, se podrá firmar cualquier tipo de documento con los siguientes formatos de firma:

- XADES
- CADES

¿Cuál es la configuración necesaria para utilizar Autofirma con Internet Explorer, Google Chrome y Mozilla Firefox en Windows?

Antes de comenzar recomendamos tener el Sistema Operativo lo más actualizado posible con las actualizaciones y parches de seguridad de Windows.

Para configurar AUTOFIRMA en los navegadores de su PC deberá seguir los siguientes pasos:

- Descargar la aplicación AUTOFIRMA

[http://firmaelectronica.gob.es/Home/Descargas.html]

- Cerrar todos los navegadores.
- Instalar aplicación Autofirma.

- Seguir los pasos que se vayan indicando y permitir la configuración automática de AUTOFIRMA en el sistema y los navegadores.

A partir de este momento puede utilizar AUTOFIRMA en los navegadores instalados en tu PC.

NOTA: es necesario instalar en los navegadores los certificados raíz de las Autoridades de Certificación que han emitido los certificados de firma que vamos a utilizar con AUTOFIRMA.

¿Cómo puedo calcular con Autofirma la huella digital de un fichero?

- Abra la aplicación Autofirma
- Pulse en Herramientas > Huellas Digitales > Fichero > Calcular Huella Digital

¿Cómo puedo comprobar con Autofirma si una huella digital se corresponde con un fichero?

- Abra la aplicación Autofirma
- Pulse en Herramientas > Huellas Digitales > Fichero > Comprobar Huella Digital

Tengo problemas con Autofirma y/o mi navegador no es capaz de ejecutar el programa para firmar un documento o identificarme en una web ¿cómo se puede restaurar la instalación?

AutoFirma permite generar firmas electrónicas como parte de un trámite web compatible de administración electrónica. Para ello es necesario que su sistema se encuentre correctamente configurado.

Si instala un nuevo navegador web, se da de alta un nuevo usuario en el sistema o tiene problemas al firmar en un trámite web, utilice la función de Restaurar Instalación para restaurar la comunicación entre AutoFirma y sus navegadores web:

- Abra Autofirma
- Seleccione el menú Herramientas
- Seleccione Restaurar instalación
- Pulse sobre Iniciar restauración
- Acepte todas las acciones según le vayan preguntando

No encuentro la funcionalidad de validar certificados de una firma en la última versión ¿Por qué?

Se ha eliminado la opción de validación de certificados desde el panel de información de firma, ya que no se puede verificar que la información de validación proporcionada sea de confianza. Autofirma únicamente valida que la firma sea correcta en cuanto a su estructura.

Para validar verazmente la firma junto con sus certificados, debe utilizar el servicio gratuito VALIDE (https://valide.redsara.es).

¿AUTOFIRMA tiene algún límite de tamaño máximo de documento a firmar?

Dependiendo de la arquitectura de la versión de Autofirma, si es de 32 bits o de 64 bits, puede tener algún tipo de limitación. Por ejemplo, si es de 32 bits, el tamaño máximo del archivo que puede manejar AUTOFIRMA es de 2GB. En arquitectura de 64 bits no hay límite.

Las firmas XADES y CADES de documentos grandes pueden validarse sin problema en la plataforma VALIDE.

Sin embargo, las firmas PADES de documentos pdf superiores a 8MB no pueden validarse desde la plataforma VALIDE.

¿Es suficiente validar la estructura de una firma para determinar que una firma es válida a los efectos de integridad, autenticidad y no repudio?

No, no es suficiente. Al validar la estructura de firma comprobamos que el documento firmado es íntegro.

Es necesario además validar los certificados con los que se ha realizado la firma, con el objeto de comprobar su autenticidad (emitidos por una Autoridad de Certificación reconocida) y validez (la firma se realizó con certificados no caducados ni revocados). Para realizar estas comprobaciones, podemos utilizar el servicio de verificación VALIDE (https://valide.redsara.es).

OFFICE

¿Cómo puedo firmar en Word 2010 / 2013?

Para proteger la autenticidad del contenido de un documento, puede agregar una firma digital invisible. Los documentos firmados incluirán el botón Firmas en la parte inferior del documento. Además, en los documentos firmados, aparecerá información de firma en la sección Información de la vista Backstage.

- Haga clic en la pestaña Archivo. Aparecerá la vista Backstage.
- Haga clic en Información.
- En la sección Permisos, haga clic en Proteger documento, Proteger hoja de cálculo o Proteger presentación.
- Desde el menú, seleccione Agregar una firma digital.
- Lea el mensaje de Microsoft Word, Excel o PowerPoint y después haga clic en Aceptar.
- En el cuadro de diálogo Firmar, en el cuadro Razón para firmar este documento, escriba la razón.
- Haga clic en Firmar.

Una vez insertada la firma digital en un archivo, aparecerá el botón Firmas y el archivo será de sólo lectura para evitar que se realicen futuras modificaciones.

¿Cómo puedo firmar en Word 2007?

Si no necesita insertar líneas de firma visibles en un documento, pero desea proporcionar seguridad en cuanto a la autenticidad, integridad y origen de un documento, puede agregar una firma digital invisible al documento. Puede agregar firmas digitales invisibles a documentos de, libros de Excel y presentaciones de PowerPoint.

A diferencia de una línea de firma de Office, una firma digital invisible no se ve en el contenido del propio documento, pero los destinatarios del documento pueden determinar si se ha firmado digitalmente viendo la firma digital del documento o buscando el botón Firmas en la barra de estado situada en el lado inferior de la pantalla.

Una vez firmado digitalmente un documento, será de sólo lectura para impedir la realización de modificaciones.

- Haga clic en el botón de Microsoft Office, seleccione Finalizar y, a continuación, haga clic en Agregar una firma digital.
- Si desea consignar la razón de firmar el documento, escriba esta información en el cuadro situado en Razón para firmar este documento en el cuadro de diálogo Firmar.
- Haga clic en Firmar.

¿Cómo puedo firmar en Word 2003?

Para agregar una firma digital a su documento en Microsoft Office Word 2003 o en Word 2002, siga estos pasos:

- En el menú Herramientas, haga clic en Opciones.
- En la ficha seguridad, haga clic en Digital Signatures.
- Haga clic en Agregar. Si el documento ha cambiado y aún no se ha guardado, o si no se guarda en el formato de documento de Word, recibirá el mensaje siguiente: Este documento debe guardarse como un documento de Word antes de que se pueda firmar digitalmente. ¿Desea guardar el documento?
- Haga clic en Sí para mostrar el cuadro de diálogo Guardar como. Debe guardar el archivo en el formato de documento de Word o el formato plantilla de documento para agregar la firma digital.
- Después de guardar el documento, se muestra el cuadro de diálogo Seleccionar certificado.
- Haga clic para seleccionar el certificado que desea utilizar y, a continuación, haga clic en Aceptar. Haga clic en Aceptar para cerrar el cuadro de diálogo Firmas digitales.
- Ahora está firmado el documento de Word.

ADOBE ACROBAT READER

¿Cómo puedo firmar un documento PDF con Adobe Acrobat Reader DC?

Ponemos a su disposición un documento con las instrucciones para firmar y validar una firma en Adobe Acrobat Reader DC.

Firmar un documento PDF utilizando Adobe Acrobat Reader DC [https://www.sede.fnmt.gob.es/documents/10445900/10528353/Firmar_documento_PDF_Adobe_Acrobat_Reader_DC.pdf]

¿Cómo puedo actualizar los certificados raíz de las Autoridades de Certificación en Adobe Reader?

Para actualizar los certificados raíz debe seguir los siguientes pasos:

- Abrir Adobe Reader y pulsar Edición – Preferencias.
- Pulsar en la categoría "Administrador de confianza" y en el apartado de Actualizaciones automáticas de certificados de confianza aprobados por la Unión Europea pulsar el botón "Actualizar ahora".
- Cuando se actualice mostrará un mensaje de "La configuración de seguridad se ha actualizado correctamente".

Instalar el certificado raíz del certificado de firma de un fichero PDF firmado

Cuando recibes un PDF firmado, se puede añadir el certificado raíz del Certificado de firma en las identidades de confianza, los pasos son los siguientes.

Adobe Acrobat Reader DC

- Abrir el documento.
- Seleccionar del menú principal la pestaña Edición / Preferencias / Firmas, o bien seleccionando el icono "Firmas" que se muestra en la parte izquierda del documento.
- Seleccionar la firma (se mostrará el icono o uno similar, junto a la firma para indicar que la identidad del firmante es desconocida porque no se ha incluido en la lista de identidades de confianza y ninguno de sus certificados principales es una identidad de confianza).
- Sobre la firma, pulsar el botón derecho del ratón y elegir la opción "Mostrar propiedades de la firma" del menú que se despliega. Pulsar botón "Mostrar certificado del firmante". Se abrirá la ventana visor de certificados.
- En la pestaña Confianza pulsar el botón "Agregar a certificados de confianza". Pulse Aceptar.
- Debe estar marcada la casilla "Utilizar este certificado como raíz de confianza"
- Pulsar "Aceptar" para cerrar la ventana y de nuevo "Aceptar" en la ventana Visor de certificados.

Adobe Reader 11.x

- Abrir el documento.
- Seleccionar del menú principal la pestaña Ver / Paneles de navegación / Firmas, o bien seleccionando el icono "Firmas" que se muestra en la parte izquierda del documento.
- Seleccionar la firma (se mostrará el icono o uno similar, junto a la firma para indicar que la identidad del firmante es desconocida porque no se ha incluido en la lista de identidades de confianza y ninguno de sus certificados principales es una identidad de confianza).
- Sobre la firma, pulsar el botón derecho del ratón y elegir la opción "Mostrar propiedades de la firma" del menú que se despliega. Pulsar botón "Mostrar certificado del firmante". Se abrirá la ventana visor de certificados.
- En la pestaña Confianza pulsar el botón "Agregar a certificados de confianza". Pulse Aceptar.
- Debe estar marcada la casilla "Utilizar este certificado como raíz de confianza"
- Pulsar "Aceptar" para cerrar la ventana y de nuevo "Aceptar" en la ventana Visor de certificados.

Adobe Reader 9.x

- Abrir el documento.
- Seleccionar del menú principal la pestaña Ver / Paneles de navegación / Firmas, o bien seleccionando el icono "Firmas" que se muestra en la parte izquierda del documento.
- Seleccionar la firma (se mostrará el icono o uno similar, junto a la firma para indicar que la identidad del firmante es desconocida porque no se ha incluido en la lista de identidades de confianza y ninguno de sus certificados principales es una identidad de confianza).
- Sobre la firma, pulsar el botón derecho del ratón y elegir la opción "Mostrar propiedades de la firma" del menú que se despliega. Se abrirá la ventana Propiedades de la firma. En la pestaña Resumen, pulsar el botón "Mostrar certificado".
- Se abrirá la ventana Visor de certificados, en ella se muestra, en el panel de la izquierda, la lista de certificados que componen la ruta de certificación completa.
- Seleccionar el certificado raíz (el primero en la jerarquía). Seleccionar la pestaña Confianza y pulsar el botón "Agregar identidades de confianza".
- Se abre la ventana Importar configuración de contactos, en ella, marcar en la sección Confianza la casilla "Utilizar este certificado como raíz de confianza".
- Pulsar "Aceptar" para cerrar la ventana Importar configuración de contactos y de nuevo "Aceptar" en la ventana Visor de certificados.
- Una vez que se ha establecido la confianza en los certificados raíz del certificado de firma, pulsar "Cerrar" en la ventana Propiedades de la firma.

AUTENTICA

¿Qué es Autentica?

El servicio AutenticA es un servicio de autenticación, autorización y Single Sign On (SSO) de empleados públicos de las Administraciones Públicas, altos cargos y usuarios relacionados, en el acceso a aplicaciones internas de las diferentes administraciones

¿Qué tipos de autenticación existen?

Se contemplan dos sistemas de autenticación; autenticación a través de certificado electrónico verificado por la entidad verificadora @firma y autenticación a través de usuario y contraseña.

¿Cómo me doy de alta o a otro usuario?

Un usuario puede solicitar el alta a través del módulo de autoregistro. El alta de otro usuario sólo la puede llevar a cabo un administrador estándar o un administrador delegado.

¿Qué es el autoregistro y para qué sirve?

El autoregistro es un sistema que hace posible que un usuario potencial solicite darse de alta en el sistema mediante un formulario. Una vez validado ese formulario por parte de un administrador, se llevará a cabo el alta de dicho usuario de manera definitiva.

¿Puedo consultar más preguntas frecuentes sobre Autentica?

Sí, en la parte inferior de la página https://autentica.redsara.es encontrarás un enlace a las preguntas frecuentes

CARPETA DEL PUNTO DE ACCESO GENERAL

Soy ciudadano/a o autónomo ¿Qué necesito para poder acceder a las notificaciones e información accesibles desde la Carpeta del Punto de Acceso General?

Para consultar la información personal recogida en la Carpeta del Punto de Acceso General es necesario identificarse mediante Certificado de Persona Física.

Soy trabajador de una empresa privada ¿Qué necesito para poder acceder a las notificaciones e información de mi entidad recogidas en la Carpeta del Punto de Acceso General?

Para consultar la información de mi empresa recogida en la Carpeta del Punto de Acceso General es necesario identificarse mediante Certificado de Representación Persona Jurídica / Administrador Único y Solidario.

Si nos identificamos con certificado de persona física, incluidos los certificados corporativos de Persona Física, accederemos a la información personal asociada a nuestro NIF.

- **Soy un empleado público ¿Qué certificado se requiere para consultar las notificaciones e información de mi entidad recogidas en la Carpeta del Punto de Acceso General?**

Para consultar la información de mi entidad recogida en la Carpeta del Punto de Acceso General es necesario identificarse mediante Certificado de Representación Persona Jurídica / Administrador Único y Solidario.

Si nos identificamos con certificado de persona física, incluidos los de empleado público, accederemos a la información personal asociada a nuestro NIF.

DIRECCIÓN ELECTRÓNICA HABILITADA (DEH)

- **Soy ciudadano o autónomo ¿Qué necesito para poder acceder a las notificaciones accesibles desde la Dirección Electrónica Habilitada?**

Para consultar la información personal recogida en la DEH es necesario identificarse mediante Certificado de Persona Física.

- **Soy trabajador de una empresa privada ¿Qué necesito para poder acceder a las notificaciones accesibles desde la Dirección Electrónica Habilitada?**

Para consultar la información de mi empresa recogida en la Carpeta del Punto de Acceso General es necesario identificarse mediante Certificado de Representación Persona Jurídica / Administrador Único y Solidario.

Si nos identificamos con certificado de persona física, incluidos los certificados corporativos de Persona Física, accederemos a la información personal asociada a nuestro NIF.

- **Soy un empleado público ¿Qué necesito para poder acceder a las notificaciones accesibles desde la Dirección Electrónica Habilitada?**

Para consultar la información de mi entidad recogida en la Carpeta del Punto de Acceso General es necesario identificarse mediante Certificado de Representación Persona Jurídica / Administrador Único y Solidario.

Si nos identificamos con certificado de persona física, incluidos los de empleado público, accederemos a la información personal asociada a nuestro NIF.

CERTIFICADOS SSL/TLS Y DE AUTENTICACIÓN DE SITIO WEB

- **¿Diferencias entre Certificado cualificado de autenticación de sitio web, según el reglamento UE 910/2014 y certificado de servidor seguro SSL/TLS?**

El Certificado cualificado de autenticación de sitio web, además de identificar el sitio web mediante su nombre de dominio, identifica a la persona física o jurídica titular del certificado.

► **¿Cuáles son los aspectos más relevantes a la hora de solicitar un certificado de autenticación de sitio web, según el reglamento UE 910/2014?**

- Certificado cualificado de Autoridad de Certificación cualificada (es validado en VALIDE).
- Soporte por parte de los navegadores sin intervención del usuario.
- Vigencia.
- Precio.

► **¿Cuáles son los aspectos más relevantes a la hora de solicitar un certificado de SSL/TLS?**

- Soporte por parte de los navegadores web o aplicaciones sin intervención del usuario.
- Vigencia.
- Precio.

► **¿Existe alguna Autoridad de Certificación que proporcione certificados digitales de servidor seguro (SSL/TLS), gratuitos y aceptados por la mayoría de los navegadores?**

Si, "Let's Encrypt", una Autoridad de Certificación gratuita, automatizada y abierta. Podemos obtener más información en https://letsencrypt.org/

Sus certificados tienen una validez de 90 días, por lo que se basan en un proceso automatizado de emisión de certificados.

Es importante remarcar que no se deben utilizar en las Sedes Electrónicas de las Administraciones Públicas ni en sitios web en los que se requiera el uso de certificados cualificados según el reglamento UE 910/2014 (EIDAS).

Ver preguntas frecuentes del "Reglamento UE 910/2014 (EIDAS)".

Fuentes de la elaboración de las preguntas frecuentes: Preguntas frecuentes de la FNMT-RCM; webs de las Autoridades de Certificación colaboradoras de esta guía; Guías y Documentación publicada por la Administración General del Estado; Wikipedia (en relación con sellado de tiempo y OCSP); e información de elaboración propia.

3 Tutoriales de uso

En este apartado se incluyen varios enlaces, listas de reproducción y videos de diferentes canales de Youtube relacionados con el uso de certificados electrónicos, DNI, cl@ve, carpeta ciudadana, criptografía y firma electrónica, etc.

Fundación Vodafone España

Listado de videotutoriales de Servicios Electrónicos de la Administración Pública orientado a ayudar en el uso de las tecnologías a personas con discapacidad, mayores o cualquiera con dificultades de acceso a las nuevas tecnologías (uso, renovación y recuperación de certificados DNI y FNMT, cl@ve)

https://www.youtube.com/playlist?list=PLYmp78TPQAIMHMspDCile2YxByWWrbwcE

David Bueno Vallejo

Listado de Tutoriales de Administración Electrónica. Uso DNI Electrónico, Instalación y uso de cl@ve PIN y cl@ve Permanente, Carpeta Ciudadana, Contratación del Estado, etc.

https://www.youtube.com/playlist?list=PLnNbmcjjevxtQOctYY7Z9IUt5YrzrjSPv

Unidad Innovación UMU

Listado de Tutoriales del curso de Iniciación a la Administración Electrónica de la Universidad de Murcia. E-Admon., firma electrónica, criptografía, certificados digitales, notificaciones electrónicas, firma de documentos, etc-

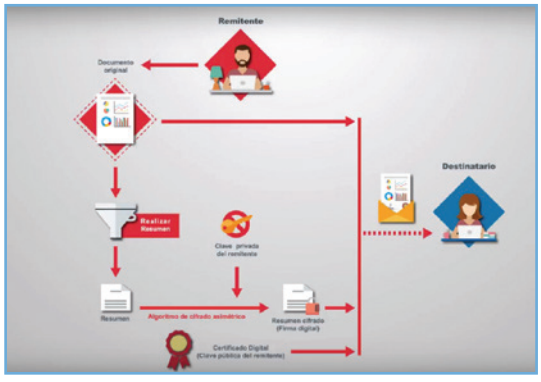
https://www.youtube.com/playlist?list=PLiQuUxsEGhjs93UKD2TOvObATCGwg97Ih

Agencia Tributaria

1. Listado de videos relacionados con Cl@ve

2. Listado de videos relacionados con la obtención y uso de certificados electrónicos

1 - https://www.youtube.com/playlist?list=PLIPJ-e4_kcL9nVnWnApflE8yMRt5idxdW
2 - https://www.youtube.com/playlist?list=PLIPJ-e4_kcL_Hco69bE0Se6qUSEzbC-BC



INCIBE

Video sobre el funcionamiento de la firma electrónica de documentos

https://www.youtube.com/watch?v=vaGTDS8UTs0

4 Enlaces de interés

Proceso de Firma

- La Firma Electrónica.

http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html

- ETSI TS 101 733 V2.1.1. Electronic Signatures and Infraestructures (ESI); CMS Advanced Electronic Signatures (CAdES).

http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.01.01_60/ts_101733v020101p.pdf

- ETSI TS 102 176-1 V2.0.0. Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.00.00_60/ts_10217601v020000p.pdf

- FIPS PUB 180-4. Secure Hash Standard (SHS). Algoritmo de la Función Hash SHA-1, SHA-256, SHA-512

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

- Criptografía: Algoritmos de cifrado de clave asimétrica.

https://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/

- LEY 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf

Política de Firma

- **Política de Firma Electrónica y de Certificados.**

http://administracionelectronica.gob.es/ctt/politicafirma

- **Política de firma electrónica y de certificados en la Administración General del Estado**

https://sede.administracion.gob.es/PAG_Sede/LaSedePAG/PoliticaFirmaElectronicaYCertificadosAGE.html

- **Nueva Guía de aplicación de la Norma técnica de interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración**

https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2017/Julio/Noticia-2017-07-11-Nueva-Guia-aplicacion-NTI-Politica-firma-y-sello-electronicos-y-certificados-Administracion.html#.WpwVSqjOWUk

- **Real Decreto 4/2010. Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica**

http://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331

- **Bases de la firma electrónica: Criptografía**

https://www.youtube.com/watch?v=tIrw65hBbDM

- **Portal de Administración electrónica**

https://administracionelectronica.gob.es/pae_Home#.W0yMf9QS-mw

- **Implantación de la Ley 39/2015 y Ley 40/2015**

https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Leyes-39-y-40-2015.html#.W0yMwdQS-mw

- **Punto de Atención al Emprendedor**

http://www.paeelectronico.es/es-ES/Paginas/principal.aspx

- **Carpeta Ciudadana de las Administraciones Públicas: Administración Electrónica**

https://www.youtube.com/watch?v=JkUo2ZodOP8

- **Certificado electrónico Agencia Tributaria**

https://www.agenciatributaria.es/AEAT.internet/Inicio/Ayuda/Certificado_electronico/Certificado_electronico.shtml

- **Certificados y sede electrónica de la FNMT**

https://www.sede.fnmt.gob.es/certificados

- **Certificados electrónicos Comunidad de Madrid**

http://www.madrid.org/cs/Satellite?c=CM_Tramite_FA&cid=1142570526216&noMostrarML=true&pageid=1331802501637&pagename=PortalCiudadano%2FCM_Tramite_FA%2FPCIU_fichaTramite&vest=1331802501621

- **Instalación y uso del DNI Digital**

https://www.youtube.com/watch?v=QYDgn5X09_0&t=3s

- **Tutorial Instalación y uso de clave (cl@ve Pin y cl@ve permanente)**

https://www.youtube.com/watch?v=rg0RC-G4YS4

- **FEMP**

http://www.femp.es/

Glosario

A

AAPP: Administraciones Públicas

AALL: Administraciones Locales

ACCV: Autoritat de Certificació de la Comunitat Valenciana

Administración electrónica: Uso de las TIC en las AAPP, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas (fuente CE)

Autenticación: Procedimiento informático que permite asegurar que un usuario de un sitio web u otro servicio similar es auténtico o quien dice ser.

Autoridad Certificadora: Entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública

Autoridad de Registro: Entidad que identifica de forma inequívoca al solicitante de un certificado. La Autoridad de Registro suministra a la Autoridad de Certificación los datos verificados del solicitante a fin de que la Autoridad de Certificación emita el correspondiente certificado.

Autoridad de Validación: Prestador de servicios de certificación que asegura la autenticidad, validez e integridad de las transacciones más críticas, como aquellas de transferencia de valores, compra, venta a través de la red

C

Catcert: Agencia Catalana de Certificación

Carpeta Ciudadana: Entorno digital de comunicación entre una administración y el ciudadano que ofrece servicios de administración electrónica

Certificados digitales: o certificado electrónico, es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Certificados electrónicos reconocidos o cualificados: son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Clave concertada: Sistema que permite la identificación de una persona que desea realizar trámites administrativos sin necesidad de disponer de certificado electrónico. Para utilizar el sistema de claves concertadas, en primer lugar deberá realizar la solicitud de clave. Recibirá tres correos electrónicos, el último de los cuales contendrá la clave de acceso. Con esa clave, el ciudadano podrá realizar la solicitud o solicitudes del procedimiento concreto para el cual se solicitó la clave.

Claves privadas/ públicas: Esquema de encriptación en el que cada persona tienes dos claves, una pública y otra privada, para el envío de mensajes, la clave publica la pueden saber algunas personas, pero la clave privada solo debe saberla la personapropietaria de dicha clave.

Confidencialidad: se entiende en el ámbito de la seguridad informática, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros

D

Digital: se usa comúnmente para referirse a todos aquellos sistemas que representan, almacenan o usan la información en sistema binario, esto es, a casi todos los aparatos electrónicos e informáticos que nos rodean actualmente.

DNI-e: Documento Nacional de Identidad Electrónico

Documentos electronicos: también conocido como documento digital, es un documento cuyo soporte material es un dispositivo electrónico o magnético, y en el que el contenido está codificado mediante algún tipo de código digital, que puede ser leído, interpretado, o reproducido mediante sensores electrónicos (magnéticos, ópticos o mecánicos).

E

eIDAS: electronic IDentification, Authentication and trust Services, es el sistema europeo de reconocimiento de identidades electrónicas, Reglamento de la UE sobre un conjunto de normas para la identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado único europeo.

ENI: Esquema Nacional de Interoperabilidad

ENS: Esquema Nacional de Seguridad

Expediente Electrónico: conjunto de datos registrados en un soporte durante el seguimiento y hasta la finalización de una actividad institucional o personal, y que comprende un contenido, un contexto y una estructura suficiente para constituir una prueba o una evidencia de esa actividad

F

Factura Electrónica: Una factura electrónica es una factura que se expide y recibe en formato electrónico

Firma Biométrica: Tecnología que permite capturar la firma manuscrita utilizando dispositivos especiales para ello (tabletas digitalizadoras), que capturan, además del propio grafo “imagen” de la firma, los rasgos biométricos del firmante, es decir, las características de la firma que lo identifican de forma unívoca, por tratarse de rasgos que son inherentes a la persona y permiten autenticar la identidad.

FNMT: Fábrica Nacional de Moneda y Timbre.

H

HSM: Hardware Security Module, dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas

I

Identidad Digital: ó Identidad 2.0 es todo lo que manifestamos en el "ciberespacio" e incluye tanto nuestras actuaciones como la forma en la que nos perciben los demás en la red.

Integridad: garantía de que el documento recibido coincide con el documento emitido sin posibilidad alguna de cambio

Interoperabilidad: capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos

N

Notificación electrónica: es la publicación en la Sede Electrónica de una comunicación administrativa con consecuencias jurídicas, como pueden ser el comienzo del plazo para contestar o presentar documentación, presentar alegaciones o recursos, etc.

P

PAE: Portal de Administración Electrónica

Plataforma de Firma: son las herramientas que hacen efectiva la firma de archivos mediante los certificados digitales

Plataformas comunes: Aquellas que integran en un único punto servicios comunes.

Política de firma: modelo de esquema de referencia para la identificación y autenticación electrónica,

PSC: Prestador de servicios de certificación

R

Redes abiertas: entornos y plataformas virtuales en los que es posible una comunicación entre personas libremente

Registro Telemático/electrónico: Es un sistema habilitado expresamente para la recepción y salida de solicitudes, escritos y comunicaciones a través de internet

Repudio: que no proporciona pruebas de la integridad y origen de los datos y/o una autentificación que con un alto aseguramiento pueda ser reafirmado como genuino.

Revocación de certificado: es anular su validez antes de la fecha de caducidad que consta en el mismo.

S

Secure Sockets Layer (SSL): Proceso que administra la seguridad de las transacciones que se realizan a través de Internet

Sede electrónica: Sitio web que está a disposición de la ciudadanía en Internet y del cual es titular una administración pública encargada de gestionarlo y administrarlo, y por medio del cual la ciudadanía y las empresas pueden acceder a su información y a los servicios y trámites electrónicos puestos a disposición.

Sello electrónico: Es un sistema de firma electrónica que permite autenticar una actuación administrativa automatizada.

Servicios electrónicos: servicios prestados por vía electrónica que abarcarán los prestados a través de Internet o de una red electrónica que, por su naturaleza, estén básicamente automatizados y requieran una intervención humana mínima, y que no tengan viabilidad al margen de la tecnología de la información.

Soportes criptográficos: Servicio por medio del cual se proporciona a los usuarios la posibilidad de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por la persona a quien está dirigido o que detenta la clave

Suspensión de certificado: Dejar sin efectos un certificado durante un período de tiempo y en unas condiciones determinadas

T

Trámites telemáticos: trámite que se realiza a través de medios electrónicos, pudiendo obtener apropiado registro de lo realizado.

Trazabilidad: En expedientes u archivos electrónicos. Cualidad por la que es posible hacer un seguimiento de las fases en las que los documentos electrónicos se encuentran.

V

Validación: de una firma electrónica es el proceso por el que se comprueba la identidad del firmante, l la integridad del documento firmado y la validez temporal del certificado utilizado.

Grupo de trabajo Identidad Digital

Denominación del Grupo:

Grupo de trabajo para la elaboración de una Enciclopedia de Servicios de Certificación para las AALL.

Coordinación y desarrollo:

- Sergio Caballero Benito, Ayuntamiento de Alcobendas
- Virginia Moreno Bonilla, Ayuntamiento de Leganés

Responsable FEMP:

- Pablo Mª Bárcenas

Integrantes:

- Antonio Bastante, Diputación Provincial de Ciudad Real
- David Bueno, Ayuntamiento de Málaga
- Eduardo Tuñón, Asociación Navarra de informática municipal (ANIMSA)
- Fernando Gallego, Ayuntamiento de Picanya
- Javier de la Villa Regueiro, Diputación Provincial de León
- Javier Peña, Diputación Provincial de Burgos

Colaboraciones:

- Aitor Cubo, Ministerio de Política Territorial y Función Pública.
- Carlos Galán, Universidad Carlos III/ Agencia de Tecnología Legal
- Rafael Pérez Galindo, Ministerio de Economía y Empresa.

Prestadores de Servicios de Certificción

- AGÈNCIA CATALANA DE CERTIFICACIÓ (CATCERT)
- AUTORITAT DE CERTIFICACIÓ DE LA COMUNITAT VALENCIANA (ACCV)
- CAMERFIRMA
- FÁBRICA NACIONAL DE MONEDA Y TIMBRE (FNMT-CERES)
- FIRMA PROFESIONAL
- IVNOSYS
- UANATACA

LA ENCICLOPEDIA DE LOS SERVICIOS DE CERTIFICACIÓN PARA LAS ADMINISTRACIONES LOCALES

La Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias viene detectando carencias importantes en cuanto al conocimiento que tienen las Entidades Locales sobre las distintas posibilidades que se ofrecen en materia de Identidad Digital, así como sus diferentes usos.

Los servicios de certificación en todas sus modalidades se han convertido en pieza clave para poder realizar cualquier actuación en el ámbito de la transformación digital. Y es tal la diversidad de elementos de certificación que se hace necesario definir, argumentar y documentar de forma clara cada uno de ellos.

Surge por tanto, dentro la Comisión de Sociedad de la Información y Tecnologías de la FEMP, un grupo de trabajo que se plantea como objetivo la creación de un documento completo, consensuado con la mayoría de entidades certificadoras, para ayudar a las Administraciones Locales a interpretar de forma práctica y homogénea las obligaciones derivadas del uso de los certificados y la firma electrónica.

Dicho grupo ha definido, clasificado y descrito, con el afán de familiarizar a los empleados públicos, ciudadanía y empresas con los certificados electrónicos reconocidos por la amplia mayoría de las Administraciones Públicas.

Adicionalmente, se contestan preguntas con las que los usuarios se enfrenta en su día a día laboral/personal, como por ejemplo; ¿Qué es el certificado digital?¿Cómo renovar un certificado digital? ¿Cómo renovar la firma electrónica?... etc.

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

RED DE ENTIDADES LOCALES POR LA TRANSPARENCIA Y PARTICIPACIÓN CIUDADANA

Depósito Legal: M-33768-2018