

Plataforma @Firma

Cambios asociados al reglamento eIDAS

GOBIERNO DE ESPAÑA



Contenido

1. INTRODUCCION:.....	3
2. SERVICIOS DE FIRMA	4
A. Validación de certificados y firmas:	4
Situación actual:	4
A partir de la entrada en vigor del eIDAS:.....	4
Adaptación @firma:	4
B. Información de tipos de certificados:	4
Situación actual:	4
A partir de la entrada en vigor del eIDAS:.....	5
Adaptación @firma:	6
3. SERVICIOS DE IDENTIDAD.....	9
A. Información de identidad del ciudadano:	9
Situación actual:	9
A partir de la entrada en vigor del eIDAS:.....	9
Adaptación @firma:	9
B. Certificados con seudónimo.....	10
Situación actual:	10
A partir de la emisión de certificados con seudónimo:.....	10
Adaptación @firma:	11
4. INFORMACION SOBRE LAS CLASIFICACIONES	11

1. INTRODUCCION:

La plataforma @firma tiene dos funciones:

- Proveedor de servicios de firma: validación del estado de revocación de los certificados y validación de firmas electrónicas en diferentes formatos.
- Proveedor de servicios de identificación: a través de la extracción de los datos de identidad de los ciudadanos de los certificados.

Los recientes cambios normativos influirán en la plataforma @firma en ambas funciones. Dichos cambios normativos son:

- Reglamento eIDAS, 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
- Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público.
- Ley 40/2015 de Régimen Jurídico del Sector Público, artículo 43.2 "Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales 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. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo al número de identificación profesional del empleado público." que considera la existencia de certificados de empleado público con la identificación profesional.
- Real Decreto 668/2015, de 17 de julio, por el que se modifica el Real Decreto 1671/2009, que al igual que la Ley 40/2015 contempla una nueva tipología de certificados, los certificados de empleado público con seudónimo.

Los principales cambios se producen a partir de la entrada en vigor del reglamento eIDAS, el 1 de Julio de 2016, ya que el eIDAS afecta a la normativa básica tanto de identificación como de firma.

2. SERVICIOS DE FIRMA

A. Validación de certificados y firmas:

A partir del 1 de Julio de 2016 es obligatoria la validación de todos los certificados europeos incluidos en las Listas de confianza (TSL) de sus Estados Miembros.

Situación actual:

@firma valida los certificados españoles y algunos certificados europeos.

A partir de la entrada en vigor del eIDAS:

Se validarán todos los certificados europeos, además de los españoles.

Adaptación @firma:

Para minimizar el impacto en las aplicaciones de administración electrónica, se han tomado una serie de medidas en @firma.

- @firma validará por defecto todos los certificados cualificados de las Cas incluidas en las TSL, tanto españoles como Europeos. Se devolverá el país origen del certificado en un campo de la respuesta de @firma.
- Las aplicaciones de administración electrónica a las que no sean de aplicación los certificados europeos, podrán solicitar, a través del servicio de soporte, la desactivación de la validación de los certificados de TSL extranjeras.

B. Información de tipos de certificados:

A raíz de la entrada en vigor del Reglamento eIDAS, desaparecen las tipologías de certificados existentes de la Ley 59/2003 (persona física, persona jurídica, entidad sin personalidad jurídica,...) y Ley 11/2007 (sello electrónico y sede electrónica), sustituyéndose por las nuevas recogidas en el eIDAS (firma, sello, autenticación web). Para minimizar el impacto en las aplicaciones de administración electrónica, se han tomado una serie de medidas en @firma.

Situación actual:

@firma devuelve el tipo de certificado como un parámetro 'Clasificación', que contiene la siguiente información:

- Clasificación = 0 – Persona física según la ley 59/2003
- Clasificación = 1 – Persona jurídica según la ley 59/2003
- Clasificación = 2 – Componente/SSL/no reconocido/sello de empresa
- Clasificación = 3 – Sede según la ley 11/2007
- Clasificación = 4 – Sello según la ley 11/2007
- Clasificación = 5 – Empleado Público según la ley 11/2007
- Clasificación = 6 – Entidad sin personalidad jurídica según la ley 59/2003

Dicho tipo lo obtiene de las listas de prestadores de servicios de certificación que mantiene el Ministerio de Industria, Energía y Turismo.

A partir de la entrada en vigor del eIDAS:

Aparecen nuevos tipos de certificados y desaparecen los específicos de la Ley 59/2003 como el de persona jurídica y el de entidad sin personalidad jurídica, que dejan de renovarse y en muchos casos pasan a considerarse certificados no reconocidos/cualificados, como en el caso de los certificados de sede electrónica y sello electrónico según la Ley 11/2007. Esto ya ha sido notificado a los prestadores de servicios de certificación y está publicado en la página de la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información relativa a la firma electrónica (<http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx>)

Los nuevos tipos según el Reglamento eIDAS son:

- 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.
- 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.
- Certificado de autenticación web. Orientado a vincular el sitio web (dominio de Internet) con la persona física o jurídica titular del certificado.
- Certificado no cualificado. Puede estar orientado tanto a personas físicas, como jurídicas, componentes, SSL. Para persona física no se contempla su uso ya que no está recogido en la legislación vigente (Ley 39/2015), al no aportar las mismas garantías que los certificados cualificados, como por ejemplo estar sometidos a una supervisión más ligera, los requisitos de verificación de la identidad de la persona a quien se expide el certificado, o proporcionar el estado de validez o revocación de forma automatizada, fiable, gratuita y eficiente. etc.

Los certificados no cualificados no se garantiza que vayan a poder ser validados.

Adaptación @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.

En @firma se están tomando las siguientes acciones para minimizar el impacto en las aplicaciones finales.

Se prevé mantener las clasificaciones actuales hasta la extinción de las CA o la caducidad de todos los certificados emitidos por ellas. Hay que tener en cuenta ciertas particularidades.

- Clasificación = 0 – Persona física. Equivale a certificado cualificado de firma de persona física del eIDAS.
- Clasificación = 1 (a extinguir) – Persona jurídica (no reconocido) – Según la información proporcionada por el MINETUR en el enlace mencionado anteriormente, a partir del 1 de Julio de 2016 los certificados de persona jurídica de la Ley 59/2003 pasan a considerarse certificados no cualificados. En @firma se mantendrá la clasificación de estos certificados (tipo 1), para que el impacto en las aplicaciones finales sea el menor posible, pero hay que tener en cuenta que a partir del 1 de julio estos certificados son no cualificados. No se darán de alta nuevos certificados en esta categoría.
- Clasificación = 2 – No cualificados. 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 las listas publicadas por la Secretaria de Estado de Telecomunicaciones y Sociedad de la Información relativa a la firma electrónica
- Clasificación = 3 – Sede según la ley 11/2007. Según la información proporcionada por el MINETUR, a partir del 1 de Julio de 2016 estos certificados pasan a considerarse certificados no cualificados. En @firma se mantendrá la clasificación de estos certificados (tipo 3), para que el impacto en las aplicaciones finales sea el menor posible, pero hay que tener en cuenta que a partir del 1 de julio estos certificados son no cualificados. No se darán de alta nuevos certificados en esta categoría.
- Clasificación = 4 – Sello según la ley 11/2007. Según la información proporcionada por el MINETUR, a partir del 1 de Julio de 2016 estos certificados pasan a considerarse certificados no cualificados. En @firma se mantendrá la clasificación de estos certificados (tipo 4), para que el impacto en las aplicaciones finales sea el menor posible, pero hay que tener en cuenta que a partir del 1 de julio estos certificados son no cualificados. No se darán de alta nuevos certificados en esta categoría.
- Clasificación = 6 (a extinguir) – Entidad sin personalidad jurídica (no reconocido) – Según la información proporcionada por el MINETUR en el enlace mencionado anteriormente, a partir del 1 de Julio de 2016 los certificados de entidad sin personalidad jurídica de la ley 59/2003 pasan a considerarse certificados no

cualificados. En @firma se mantendrá la clasificación de estos certificados (tipo 6), para que el impacto en las aplicaciones finales sea el menor posible, pero hay que tener en cuenta que a partir del 1 de Julio estos certificados son no reconocidos. No se darán de alta nuevos certificados en esta categoría.

Por tanto, 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 personalidad jurídica. Si se mantiene la clasificación por la SETSI o se cumple el perfil indicado para ello.

Para los certificados **EUROPEOS**: Las validaciones de certificados emitidos por Prestadores que figuran en las TSL europeas devolverán los tipos de certificados cualificados que indica el

eIDAS: firma, sello, autenticación web, o no cualificado (en cuyo caso no hay obligación de admisión), a través de dos campos que se tomarán de los certificados y de las TSL:

- certQualified
 - NO: El certificado no es cualificado (reconocido).
 - YES: El certificado es cualificado.
 - UNKNOWN: Se desconoce (Se considera no cualificado a menos que se indique lo contrario en certClasification).
- certClassification:
 - ESEAL: Certificado de sello electrónico. Pertenece a una persona jurídica pero NO incluye un custodio.
 - ESIG: Certificado para firma electrónica (persona física).
 - WSA: Certificado para autenticación de servidor web.
 - UNKNOWN: Se desconoce el tipo del certificado (Se considera no cualificado a menos que se indique lo contrario en certQualified).

Por tanto, si se desean admitir certificados Europeos, se pueden discriminar de los españoles por el campo indicativo del país, y obtener el tipo eIDAS del campo certClasification.

Estos campos también se devolverán para los certificados españoles, para facilitar el tratamiento a aquellas aplicaciones que necesiten admitir tanto a certificados españoles como europeos, ya que las siguientes clasificaciones son equivalentes:

- ESEAL => Clasificación = 8.
- ESIG => Clasificación = 0, 5, 7, 11, 12.
- WSA => Clasificación = 9.
- UNKNOWN => Clasificación = 2, 10.

3. SERVICIOS DE IDENTIDAD

A. Información de identidad del ciudadano:

Los certificados Europeos no tienen la obligación de incluir un identificador único de la persona poseedora del certificado. Solo están obligados a incluir el nombre y apellido, o incluso un seudónimo.

Situación actual:

@firma valida los certificados españoles de los que obtiene los datos de identidad. Nombre, apellido 1, apellido 2, DNI (NIE)...

También se validan algunos certificados Europeos que disponen de identificador único, que se devuelve en un campo específico.

@firma al validar los certificados devuelve los que se conoce como mapeos de campos de identidad del certificado. Es decir, no solo valida las firmas electrónicas, sino que actúa como proveedor de identidad para los certificados españoles dados de alta en la plataforma.

A partir de la entrada en vigor del eIDAS:

Los certificados Europeos no tienen DNI, y en la mayor parte de los casos tampoco un identificador único. Solo es obligatorio el nombre y apellido (normalmente uno) o incluso un seudónimo. Además pueden llevar otra información variada asociada a la identidad (lugar de nacimiento, fecha de nacimiento...)

Adaptación @firma:

En cuanto a la función de @firma como proveedor de identidad, la entrada en vigor del eIDAS no afecta a los certificados emitidos por Prestadores de Servicios de Certificación españoles reconocidos por el Ministerio de Industria y dados de alta en @firma. Se seguirán devolviendo los datos de identidad (Nombre, Apellidos y DNI), que coincidirán con los obtenidos a través de Cl@ve. Si se necesita obtener la identidad de un certificado español que no está dado de alta en @firma se puede solicitar dicha inclusión a través del servicio de soporte.

La obtención de la identidad a partir de la información incluida en los certificados afectará solo a las validaciones de certificados emitidos por Prestadores de Certificación europeos que figuren en la TSL del país emisor. Para la identificación de los nacionales de los Estados Miembro:

- Se recomienda utilizar Cl@ve, 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.
- Una vez identificado al ciudadano extranjero, se puede solicitar su firma y validarla a través de los servicios de @firma.

Si se quieren obtener los datos de identidad del firmante con @firma, a partir del certificado, esta información no coincidirá con la proporcionada por Cl@ve en el caso de certificados europeos. @firma devolverá la información de identidad en un campo único, tal y como figuran en el certificado, pero no los mapeos de campos de identidad del certificado, como se hace con los certificados españoles. Dentro de esta información podrán figurar nombre, apellido, seudónimo y otra información de identidad como fecha de nacimiento, lugar de nacimiento, etc, según establezca el prestador emisor del certificado, sin ningún formato u orden preestablecido.

IMPORTANTE: Para los certificados extranjeros la información de identidad obtenida del certificado típicamente no se corresponderá con la obtenida a través de Cl@ve-nodo eIDAS. Por ello se recomienda el uso de Cl@ve para la identificación de extranjeros, ya que es la única que devuelve la identidad oficial respaldada por el país origen del ciudadano.

Si resultara necesario asegurar que el firmante es el mismo que se identificó en Cl@ve, se recomienda implantar medidas adicionales, por ejemplo: poner avisos legales de que es responsabilidad del firmante asegurarse que se ha identificado correctamente, o al firmar el documento/formularios configurar que se firmen también los datos de identidad obtenidos de Cl@ve. Otra opción es obligar a realizar la identificación y la firma en la misma sesión.

También hay que considerar que cuando un extranjero se identifica a través de Clave-eIDAS obtiene un identificador de su país de origen. Si dicho ciudadano tenía un certificado español con NIE, dicho NIE no se obtendrá en la identificación a través de Cl@ve. En sucesivas versiones del sistema Cl@ve-eIDAS se buscará la posibilidad de devolver el NIE además de la identidad del país de origen, en aquellos casos en los que el ciudadano lo tuviera.

B. Certificados con seudónimo.

A raíz de la modificación del RD 1671/2009, así como de próxima entrada en vigor de la ley 40/2015, se incluye la posibilidad de emitir certificados de empleado público con seudónimo. El eIDAS también contempla que el certificado lleve un seudónimo.

Situación actual:

Este tipo de certificados no se contempla para los certificados de empleado público.

A partir de la emisión de certificados con seudónimo:

En la ley 40/2015 de Régimen Jurídico del Sector Público se contempla la posibilidad de certificados de empleado público en el artículo 43.2 “Por razones de seguridad pública los sistemas de firma electrónica podrán referirse solo el número de identificación profesional del empleado público”

Se emitirán certificados de empleado público con seudónimo, 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.

Ya existen Prestadores de Servicios de Certificación Españoles, que emiten certificados con seudónimo para personas físicas.

Adaptación @firma:

Cuando se empiecen a emitir estos tipos de certificados de empleado público se clasificarán de forma específica, si la Secretaria de Estado de Telecomunicaciones y Sociedad de la Información mantiene una lista de estos tipos de certificados que permita su identificación, en la lista relativa a la firma electrónica (<http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/FirmaElectronica.aspx>)

Se creará un nuevo tipo, previsiblemente con Clasificación =‘7’ que los identifique, para permitir a las aplicaciones tratarlos convenientemente (o rechazarlos).

Si la SETSI no mantiene dicha lista, se buscará en @firma una manera de identificarlos para permitir a las aplicaciones su tratamiento automatizado.

4. INFORMACION SOBRE LAS CLASIFICACIONES

La información sobre las clasificaciones se mantendrá actualizada en el documento: “Procedimiento de inclusión y clasificación de certificados en @firma” de acceso público en el área de descargas de la página de @firma en el CTT:

<http://administracionelectronica.gob.es/ctt/afirma>

También se notificarán todos los cambios a través de la lista de novedades de @firma:

afirma-mptapavisos@listas-ctt.administracionelectronica.gob.es