Plataforma @firma

Nueva política de validación de certificados electrónicos: **default**

José Ignacio Cortés Santos

Dirección General de Transformación Digital

Consejería de Hacienda , Industria y Energía

Sevilla, 20 de Febrero de 2019

ÍNDICE

Firma electrónica

Autenticación y Firma electrónica. Definiciones

Autenticación

- Proceso que permite identificar a las entidades implicadas en una transacción y garantiza que estas entidades son quienes dicen ser.
- Utiliza certificados digitales para su objetivo.
- Aporta mayor información y contenido al proceso de autenticación a una aplicación.

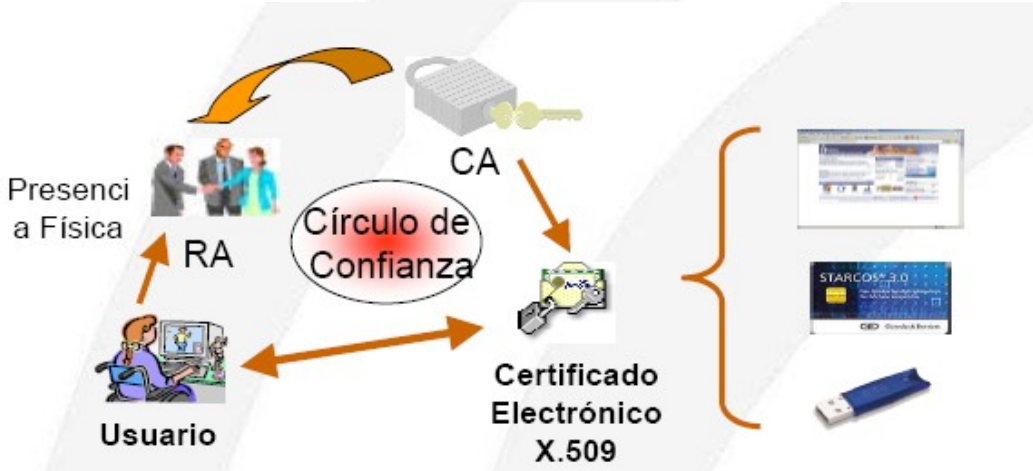
Firma electrónica

- Una firma electrónica es el resultado de aplicar una serie de operaciones criptográficas a una entidad de información utilizando para ello un certificado electrónico, para obtener dos cosas: la integridad del documento firmado y el no repudio de la firma realizada.

Certificados digitales

Definición

- Un certificado digital es un documento electrónico que relaciona una clave pública a un conjunto de información que identifica a una entidad (una persona, por ejemplo) que está en posesión de la correspondiente clave privada.
- Son emitidos por una Entidad de Certificación (CA) que garantiza la equivalencia entre el certificado y la entidad.
- Se almacenan en navegadores, ficheros (formato PKCS#12) y tokens criptográficos PKCS#15 (Tarjetas inteligentes, tokens USB, etc).



Certificados digitales

Ciclo de Vida del Certificado Electrónico

• **Caducado**, cuando se ha superado la fecha de vigencia del certificado. Normalmente un certificado suele tener un período de vigencia de 2 a 4 años desde la fecha de emisión. En el caso de la FNMT, los certificados de persona física, por ejemplo, son 4 años.

• **Revocado**, cuando ha sido rechazado, o bien por la Autoridad Certificadora que lo emite o bien por el propio titular. El motivo de la revocación es variado (extravío, robo, caducidad, certificado copiado por terceros, etc).

• **Suspendido,** cuando se ve afectado por una investigación o procedimiento judicial o administrativo, por lo que se procede a cancelar la validez del certificado durante un cierto período de tiempo, pudiendo volverse a levantar la suspensión dentro del período de validez del certificado.

• **Válido,** cuando no pertenece a ninguno de los estados anteriores.

Un certificado caducado, revocado o suspendido no tiene validez, por lo que las firmas realizadas con este tipo de certificados dejan de tener valor desde el momento de su revocación.

Certificados digitales

Validación de certificados (I)

¿Qué es la validación de un certificado?

Es la verificación de que el certificado es válido, integro y no ha sido comprometido.

¿Por qué se debe validar un certificado?

Es la forma de garantizar que en el momento de realizar una firma o una autenticación, el estado del certificado era válido y por lo tanto también la operación en la que participó.

¿Cómo se lleva a cabo?

Validación de integridad del certificado

- Cumplimiento del estándar X.509v3
- Fecha de caducidad.
- Firma del emisor.

Consulta del estado del certificado

- Válido.
- Revocado.
- Suspendido.

Validación de la cadena de certificación.

Según RFC 3280

Certificados digitales

Validación de certificados (II). Métodos de consulta

- **CRL (Certificate Revocation List)**
  - Listas firmadas que publican los certificados comprometidos.
  - Son emitidas por el PSC emisor de los certificados.
  - Pueden ser completas, segmentadas, indirectas, etc.
  - Pueden ser publicadas por HTTP/S, LDAP, FTP, etc.
  - Tiempo de latencia alto.
- **OCSP (Online Certificate Status Protocol)**
  - Protocolo en línea para consulta de estado de certificados.
  - Es independiente del protocolo de comunicación.
  - Es el método más fiable.

Certificados digitales

Políticas de validación (I)

De entre las funcionalidades que ofrece @firma, destacan estas tres relacionadas con las políticas de validación de certificados en @firma:

Autenticación

- Proceso que permite autenticar o identificar de forma fehaciente a una entidad basándose en la comprobación de su certificado digital.
- Es el mecanismo empleado por la **fachada de tickets**.

Validación de firmas

- Proceso que permite determinar si una firma es válida o no.
- Se comprueba tanto la validez de la firma (formato y atributos) como la validez de los certificados contenidos en el momento de la firma (si hay referencia temporal) o en el momento de la validación (si no hay referencia temporal).

Validación de certificados

- Proceso que permite determinar si un certificado es válido (en estado no caducado ni revocado ni suspendido).
- Requiere el tratamiento de los datos contenidos en el certificado y su presentación a las aplicaciones de forma homogénea. Este proceso se conoce con el nombre de "**mapeo**".

Certificados digitales

Políticas de validación (II)

Se define como "**Política de validación**" a los criterios configurados en una implantación de @firma que permiten validar certificados y mapear sus atributos.

Mecanismos de validación de certificados

- Para cada tipo de certificado admitido por @firma se requiere tener configurada toda la jerarquía de certificación de cada prestador (raíz e intermedias), definiendo y configurando para cada tipo de certificado emitido por cada entidad los mecanismos de validación disponibles (OCSP, CRL, WS), así como el orden de cada uno de ellos.
- En caso de fallar un mecanismo de validación, la plataforma intentará utilizar el siguiente disponible en función del orden indicado.

Mapeo de certificados

- Para cada tipo de certificado admitido por @firma se requiere tener disponible un certificado "tipo" que se utiliza como plantilla para indicar los atributos del certificado y su modo de presentación a las aplicaciones.
- Este proceso es manual. Es necesario un "mapeo" de atributos por cada tipo de certificado admitido (aquel cuyo identificador de política sea diferente).

Certificados digitales

Políticas de validación (III)

Una política de validación puede ser exportada e importada en otras implantaciones de @firma.

Se trata de un fichero que contiene la siguiente información:

Jerarquía de prestadores

- Se define la jerarquía completa de los certificados reconocidos, tanto la CA raíz como todas las CA's intermedias que expidan certificados que se van a reconocer.

Mecanismos de validación

- Se define para cada CA raíz e intermedia los mecanismos de validación admitidos (OCSP, CRL, WS) así como el orden de ejecución. Esto incluye los almacenes de confianza.

Mapeo de certificados

- Se definen un conjunto de atributos comunes a todos los certificados reconocidos, así como su significado.
- Para cada tipo de certificado se indican qué atributos de los comunes indicados en la política de validación son obligatorios, opcionales o no aplicables.

Certificados digitales

Políticas de validación (IV)

La plataforma @firma v6 corporativa define dos políticas de validación de certificados diferentes:

Default JA

- Es la política de validación heredada de las versiones anteriores de @firma.
- En @firma v5 se amplió el número de atributos de la política, manteniéndose los atributos de la v4 por compatibilidad. Se denominó “default”.
- En @firma v6 se renombró la política a “default JA” para indicar de forma clara que se correspondía con el mapeo de atributos realizado por la Junta de Andalucía.
- Es la utilizada por defecto en todas las aplicaciones integradas con la implantación corporativa de @firma.

Default

- Es la política de validación del Ministerio de Hacienda y Administraciones Públicas.
- Se actualiza quincenalmente
- Es la utilizada en algunos sistemas corporativos como Notific@, PEG, VEA y Compuls@.

ÍNDICE

Política de validación “Default JA”

Política de validación Default JA (I)

Es la política de validación utilizada por defecto.
Última versión **v48**: 11/12/2018

Consta de los siguientes componentes:

Política de firma (sólo para administradores de @firma)

- Fichero xml que contiene la política de validación.
- Dependiente de la versión de @firma. Sólo se distribuyen para la versión 5.

Manual de política

- Documento PDF donde se documentan los cambios respecto a la política anterior.

Mapeo de certificados reconocidos por @firma

- Documento PDF donde se detalla el mapeo de cada tipo de certificado reconocido, ordenado por prestador.

Política de validación “Default JA”

Política de validación Default JA (II). Mapeo de certificados.

La política de validación “Default JA” tiene las siguientes características:

- El mapeo realizado es propio de la Junta de Andalucía, a partir de los certificados “tipo” ofrecidos por los distintos prestadores de certificación reconocidos (aquellos publicados en la siguiente web: https://sedeaplicaciones2.minetur.gob.es/prestadores/).
- No todos los certificados reconocidos por Industria son admitidos en @firma.
- La política se actualiza cuando hay modificaciones sensibles en los mapeos o se incorporan nuevos certificados.
- Cada tipo de certificado se identifica de forma unívoca mediante un valor numérico (TIPOAFIRMA) o de texto (tipoCertificado).
- Las aplicaciones que requieren filtrar los tipos de certificados admitidos requieren disponer de una lista de tipos de certificados admitidos por la aplicación, que se tiene que mantener conforme aumenta el número de certificados reconocidos.
- El mapeo de certificados es un extenso documento donde los certificados se clasifican por prestador en primer lugar, por subCA (autoridad de certificación intermedia) y por último por cada tipo de certificado (identificado por la política del certificado).

Política de validación “Default JA”

Política de validación Default JA (III). Mapeo de certificados.

Los atributos de los certificados definidos en la política “default JA” pueden ser

- LIBRES: Un valor arbitrario (tipoCertificado, TIPOAFIRMA).
- SIMPLES: Un valor obtenido de un atributo del certificado sin transformación.
- CONCATENACION: Un valor obtenido mediante la unión de más de un atributo del certificado.
- COMPLEJA: Un valor obtenido a partir de parte de la cadena de un atributo del certificado.
- EXPRESIÓN REGULAR: Un valor obtenido a partir de atributos del certificado mediante la aplicación de expresiones regulares.

Política de validación “Default JA”

Política de validación Default JA (IV). Mapeo de certificados.

La política de validación “Default JA” define los siguientes atributos para los certificados admitidos:

Atributos de @firma v4

- Se representan en mayúsculas.

Atributos de @firma v5

- Formado por los atributos de @firma v4 y extendidos por otros que se representan en minúsculas.

Política de validación “Default JA”

Política de validación Default JA (V). Atributos de @firma v4

Atributos obligatorios:

- **ANAGRAMA**: Anagrama del titular del certificado.
- **TIPOAFIRMA**: Valor numérico único para cada tipo de certificado.

Atributos opcionales

- **CADUCIDAD** → Representa si el certificado está o no caducado.
- **CARGO** → Cargo de la persona responsable del certificado.
- **CIFENTIDAD** → CIF de la entidad representada por el responsable.
- **CIFVINCULADA** → CIF de la entidad vinculada.
- **ENTIDADVINCULADA** → Entidad vinculada del certificado.
- **FECHACREACION** → Fecha de creación del certificado.
- **FECHACADUCIDAD** → Fecha de caducidad del certificado.
- **NIF-CIF** → NIF del responsable o el CIF de la entidad en el caso de ser un certificado de representante.
- **NIFREPRESENTADO** → NIF del responsable del certificado.
- **NOMBREENTIDAD** → Nombre de la entidad representada por el certificado.
- **NOMBREYAPELLIDOSREPRESENTADO** → Nombre y apellidos de la persona representada.
- **PAIS** → País representado por el certificado.
- **POBLACION** → Población representada por el certificado.
- **PROVINCIA** → Provincia representada por el certificado.
- **TIPOVINCULACION** → Tipo de vinculación del representante y la entidad.
- **TITULO** → Título del representado por el certificado

Política de validación “Default JA”

Política de validación Default JA (VI). Atributos de @firma v5

Atributos obligatorios:

- **NIFResponsable / NIFResponsableER** → NIF del responsable del certificado.
- **nombreResponsable** → Nombre del responsable del certificado.
- **primerApellidoResponsable** → Primer apellido del responsable del certificado.
- **segundoApellidoResponsable** → Segundo apellido del responsable del certificado.

Atributos opcionales

- **EntidadJuridica** → Nombre de la entidad representada por el certificado.
- **CIFEntidadER** → Se mapea de CIF de la organización representada en el certificado mediante ER.
- **NombreApellidosResponsable** → Nombre y apellidos del responsable del certificado.
- **ApellidosResponsable** → Apellidos del responsable del certificado.
- **numeroSerie** → Número de serie del certificado.
- **Direccion** → Dirección del propietario o entidad vinculada al certificado.
- **OrganizacionEmisora** → Organización emisora del certificado.
- **politica** → Identificador de política del certificado.
- **razonSocial** → Empresa vinculada al certificado.
- **clasificacion** → Autoridad de certificación emisora del certificado.
- **email** → Dirección de correo electrónico del responsable del certificado.
- **extensionUsoCertificado** → Uso extendido del certificado.
- **fechaNacimiento** → Fecha de nacimiento del responsable del certificado.
- **fnmtApeNip** → Número de identificación del empleado público.
- **fnmtApeUnidadOrganizativa** → Unidad organizativa de la APE.
- **idEmisor** → Identificador de emisor del certificado.
- **Subject** → Identificador de asunto del certificado.
- **situacionLaboral** → Situación laboral del empleado público.
- **ServicioSello** → Servicio de sello electrónico.
- **tipoCertificado** → Tipo en el que se encuadra el certificado.
- **usoCertificado** → Usos válidos del certificado.
- **validoDesde** → Fecha de creación del certificado.
- **validoHasta** → Fecha de caducidad del certificado.

ÍNDICE

Política de validación “Default”

Política de validación Default (I)

Es la política de validación utilizada por el Ministerio de Hacienda y Administraciones Públicas.

Consta de los siguientes componentes:

Política de firma (sólo para administradores de @firma)

- Fichero zip que contiene la política de validación en ficheros json.
- Dependiente de la versión de @firma. Sólo se distribuyen para la versión 6.

Manual de cambios

- Hoja de cálculo donde se describen de forma cronológica los cambios respecto a la política anterior.

Procedimiento de inclusión y clasificación de certificados

- Documento PDF donde se describe el mapeo de cada certificado atendiendo a su clasificación.

Anexo – Prestadores de Servicios de certificación

- Documento PDF donde se indican los certificados admitidos por la política organizados por prestador y tipo de certificado atendiendo a su clasificación.

Política de validación “Default”

Política de validación Default (II). Mapeo de certificados.

La política de validación “Default” tiene las siguientes características:

- El mapeo es realizado por el Ministerio de Hacienda y Administraciones Públicas e incluye a **todos** los prestadores de certificación reconocidos (aquellos publicados en la siguiente web: https://sedeaplicaciones2.minetur.gob.es/prestadores/).
- La política se actualiza quincenalmente.
- El mapeo de certificados es un pequeño documento donde los certificados se clasifican por el tipo de certificado conforme a la clasificación de certificados realizadas por Industria.
- Se incluye un documento anexo donde se detallan los certificados admitidos por @firma por cada prestador y la clasificación que tienen: forja-ctt.administracionelectronica.gob.es/webdav/site/ctt-map/users/soporte_afirma/public/@FirmaV5p0_ANEXO_PSC.pdf

Política de validación “Default”

Política de validación Default JA (III). Clasificación.

Todos los certificados admitidos por @firma se clasifican según el reglamento eIDAS (Reglamento UE Nº 910/2014):

- **0**: Persona física
- **1**: Persona jurídica (no cualificado)
- **2**: No cualificados
- **3**: Sede según la ley 40/2015 (no cualificado)
- **4**: Sello según la ley 40/2015 (no cualificado)
- **5**: Empleado público según la ley 40/2015
- **6**: Entidad sin personalidad jurídica (no cualificado)
- **7**: Empleado público con seudónimo según el RD 1671/2009
- **8**: Cualificado de sello, según el reglamento UE 910/2014
- **9**: Cualificado de autenticación, según el reglamento UE 910/2014
- **10**: Cualificado de servicio cualificado de sello de tiempo
- **11**: Persona física representante ante las Administraciones Públicas de persona jurídica.
- **12**: Persona física representante ante las Administraciones Públicas de entidad sin persona jurídica.

ÍNDICE

Ventajas uso política “Default”

La política de validación “Default” tiene las siguientes ventajas:

- Simplificación del tratamiento de los certificados por parte de las aplicaciones al limitar los tipos de mapeos a trece.
- Se incluyen todos los certificados reconocidos por Industria.
- Simplicidad de mantenimiento de controles de filtro de certificados admitidos al limitar estos a los valores de clasificación de certificados.
- Facilita la interoperabilidad con las aplicaciones del Estado y otras que utilicen la implantación de @firma estatal tanto centralizada como federada siempre y cuando utilicen la misma política.

Las desventajas que presenta esta política son principalmente las siguientes:

- Requiere una pequeña adaptación de las aplicaciones que ya utilizan la política “default JA” para adaptarla a los nuevos campos y atributos mapeados.
- Sólo es aplicable a aplicaciones integradas en @firma v6.

Ventajas uso política “Default”

Comparativa política default JA - default

Característica	Default JA	Default
Reconoce todos los certificados reconocidos por Industria	**NO**	**SI**
Permite clasificar los certificados conforme a clasificación eIDAS	**NO**	**SI**
Interoperable con @firma MINHAP	**No de forma directa**	**SI**
Frecuencia de actualización	**Variable**	**Quincenal**
Compatibilidad con @firma	**V4, v5 y v6**	**v6**
Filtro de tipo de certificados para aplicaciones	**Por tipo de Certificado**	**Campo Clasificación**
Requiere adaptar la aplicación al incorporar nuevos certificados a la política de validación	**Sí, si la aplicación dispone de filtro de certificados deberá decidir si incluye o no los nuevos certificados en la lista de “admitidos” por la aplicación**	**No, los nuevos certificados al estar clasificados no requieren de ninguna acción especial por parte de las aplicaciones**

ÍNDICE

Mapeo tipo para cada clase de certificado

Clasificación 0 – Persona física cualificado

Atributos relativos al subject

- subject
- nombreResponsable
- primerApellidoResponsable (si es posible de forma unívoca desde los atributos del certificado)
- segundoApellidoResponsable (si es posible de forma unívoca desde los atributos del certificado)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI)
- ID_europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- email (si el PSC lo incluye en sus certificados)
- unidadOrganizativa (si el PSC lo incluye en sus certificados)
- organizacion (si el PSC lo incluye en sus certificados)
- pais

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificacion = 0
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 1 – Persona jurídica (no cualificado)

Atributos relativos al subject

- subject
- NIF-CIF (CIF de la empresa)
- razonSocial
- nombreResponsable
- primerApellidoResponsable (si es posible de forma unívoca desde los atributos del certificado)
- segundoApellidoResponsable (si es posible de forma unívoca desde los atributos del certificado)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI del responsable)
- email (si el PSC lo incluye en sus certificados)
- unidadOrganizativa
- organizacion
- pais

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificacion = 1
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 2 – Componente/SSL (no cualificado)

Atributos relativos al subject

- unidadOrganizativa
- organizacion
- pais
- subject

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificacion = 2
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 3 – Sede (no cualificado)

Atributos relativos al subject

- NombreDominioIP (dominio al que pertenece la sede)
- sedeElectronica (breve descripción de la sede indicando un nombre)
- email (si el PSC lo incluye en sus certificados)
- entidadSuscriptora (entidad propietaria del certificado)
- DIR3
- NIFEntidadSuscriptora (Número único de identificación de la entidad)
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- organizacion
- pais
- subject

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificacion = 3
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 4 – Sello (no cualificado)

Atributos relativos al subject

- DenominaciónSistemaComponente (breve descripción del sistema o componente)
- entidadSuscriptora (entidad propietaria del certificado)
- DIR3
- NIFEntidadSuscriptora (Número único de identificación de la entidad)
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- organizacion
- pais
- subject
- nombreResponsable
- primerApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- segundoApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI del responsable)
- ID_ europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- email (si el PSC lo incluye en sus certificados)

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación = 4
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 5 – Empleado público

Atributos relativos al subject

- nombreResponsable
- primerApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- segundoApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- ApellidosResponsable
- NombreApellidosResponsable
- email (si el PSC lo incluye en sus certificados)
- NIFResponsable (DNI del responsable)
- ID_ europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- numeroIdentificacionPersonal (se corresponde con el NRP o NIP)
- puesto (puesto desempeñado por el suscriptor del certificado dentro d la administración)
- subject
- entidadSuscriptora (entidad propietaria del certificado)
- DIR3
- NIFEntidadSuscriptora (Número único de identificación de la entidad)
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- unidadOrganizativa (dentro de la Administración, en la que está incluida el suscriptor)
- organizacion
- pais

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación =5
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- CertQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 6 – Entidad sin personalidad jurídica (no cualificado)

Atributos relativos al subject

- subject
- razonSocial
- NIF-CIF (CIF de la empresa)
- nombreResponsable
- primerApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- segundoApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- ApellidosResponsable
- NombreApellidosResponsable
- email (si el PSC lo incluye en sus certificados)
- NIFResponsable (DNI del responsable)
- unidadOrganizativa
- organizacion
- pais

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación =6
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- usoCertificado
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 7 – Empleado Público con Seudónimo

Atributos relativos al subject

- email (si el PSC lo incluye en sus certificados)
- seudonimo
- puesto (puesto desempeñado por el suscriptor del certificado dentro de la administración)
- subject
- entidadSuscriptora (entidad propietaria del certificado)
- DIR3
- NIFEntidadSuscriptora (Número único de identificación de la entidad)
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- unidadOrganizativa (dentro de la Administración, en la que está incluida el suscriptor)
- organizacion
- pais

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación =7
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- usoCertificado
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 8 – Cualificado de sello (UE 910/2014)

Atributos relativos al subject

- DenominaciónSistemaComponente (breve descripción del sistema o componente)
- entidadSuscriptora (entidad propietaria del certificado)
- NIFEntidadSuscriptora (Número único de identificación de la entidad)
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- organizacion
- pais
- subject
- nombreResponsable
- primerApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- segundoApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI del responsable)
- ID_ europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- email (si el PSC lo incluye en sus certificados)

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación = 8
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 9 – Cualificado de autenticación de sitio web (UE 910/2014)

Atributos relativos al subject

- NombreDominioIP (dominio del sitio web, tal y somo figura en el Subject Alternative Names)
- email (si el PSC lo incluye en sus certificados)
- entidadSuscriptora (entidad propietaria del certificado)
- NIFEntidadSuscriptora (Número único de identificación de la entidad)
- OI_Europeo (NIF o identificador europeo, con codificación estándar según ETSI EN 319 412)
- organizacion
- pais
- subject

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación = 9
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 10 – Cualificado de sello de tiempo

Atributos relativos al subject

- unidadOrganizativa
- organizacion
- pais
- subject

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación = 10
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 11 – Persona física representante de persona jurídica

Atributos relativos al subject

- subject
- NIF-CIF (CIF de la empresa)
- razonSocial (Organization Name)
- unidadOrganizativa
- organizacion
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412. Organization Identifier)
- nombreResponsable
- primerApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- segundoApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI)
- email (si el PSC lo incluye en sus certificados)
- pais
- Documento representación

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación = 11
- usoCertificado
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- validoDesde
- validoHasta

Mapeo tipo para cada clase de certificado

Clasificación 12 – Persona física representante de entidad sin PJ

Atributos relativos al subject

- subject
- razonSocial (Organization Name)
- NIF-CIF (CIF de la empresa)
- unidadOrganizativa
- organizacion
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412. Organization Identifier)
- nombreResponsable
- primerApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- segundoApellidoResponsable (si es posible su determinación unívoca a partir de los campos contenidos en el certificados del PSC)
- ApellidosResponsable
- NombreApellidosResponsable
- email (si el PSC lo incluye en sus certificados)
- NIFResponsable (DNI del responsable)
- pais
- Documento representación

Atributos relativos al emisor

- idEmisor
- OrganizaciónEmisora.

Atributos relativos al certificado

- clasificación = 12
- extensionUsoCertificado
- numeroSerie
- politica
- certClassification
- certQualified
- qscd
- tipoCertificado (nombre común en la plataforma @firma)
- usoCertificado
- validoDesde
- validoHasta

ÍNDICE

Migración de aplicaciones

Esquema general

Modificar el filtrado de certificados admitidos por la aplicación

- Determinar el conjunto de certificados que se admitirá en la aplicación, de modo que se eliminen los filtros por los campos **TIPOAFIRMA** y **tipoCertificado** o **politica** y se filtre únicamente por el campo **clasificacion**.

Revisar los atributos mapeados

- Es necesario revisar en la aplicación los atributos que se utilizan tras la validación de un certificado y comprobar si con la nueva política se mantienen los atributos o son diferentes. En la mayoría de los casos no se requerirá ninguna modificación o la única modificación será el cambio de nombre de un atributo. En raras ocasiones el atributo puede no existir, por lo que el cambio en la aplicación puede ser algo más complejo.

Solicitar cambio de mapeo en @firma

- Si la aplicación ya está dada de alta en @firma, bastará con abrir una incidencia en itracker solicitando el cambio de la política de validación “default ja” a “default”. Primero en pruebas y posteriormente en producción.
- Los manuales de mapeo de ambas políticas están publicados en la Web de Soporte de Administración Electrónica, en la sección dedicada a @firma.

Migración de aplicaciones

Comparativa de atributos comúnmente utilizados (PF)

Característica	Default JA	Default
Nombre del titular	**nombreResponsable**	**nombreResponsable**
Apellidos del titular	**ApellidosResponsable**	**ApellidosResponsable**
DNI	**NIFResponsable**	**NIFResponsable**
email	**email**	**email**
Validez	**validoDesde/validoHasta**	**validoDesde/validoHasta**

Migración de aplicaciones

Comparativa de atributos comúnmente utilizados (RPJ)

Característica	Default JA	Default
NIF Entidad PJ	**CIFEntidad**	**NIF-CIF**
Razón social	**EntidadJuridica**	**razonSocial**
Nombre del titular	**nombreResponsable**	**nombreResponsable**
Apellidos del titular	**ApellidosResponsable**	**ApellidosResponsable**
DNI	**NIFResponsable**	**NIFResponsable**
email	**email**	**email**
Validez	**validoDesde/validoHasta**	**validoDesde/validoHasta**

Migración de aplicaciones

Esquema temporal

Nuevas aplicaciones

- A partir de hoy, todas las solicitudes de alta de aplicaciones en cualquier entorno de @firma 6 irán con la política de validación "**default**".

Aplicaciones existentes en @firma v6

- Las actuales aplicaciones dadas de alta en cualquier entorno de @firma v6 deberán migrar o actualizarse a la nueva política de validación.
- A partir de este momento se garantiza el mantenimiento de la política de validación "default ja" en lo relativo a la incorporación de nuevos certificados.

Muchas gracias

José Ignacio Cortés Santos

josei.cortes@juntadeandalucia.es

Dirección General de Transformación Digital

Consejería de Hacienda , Industria y Energía