Procedimiento de inclusión y clasificación de certificados en @firma

Versión de trabajo actualizada (eIDAS2 · Ley 6/2020)

Plataforma de validación y firma electrónica de las AAPP

Preparado por Julián Inza (inza.blog) / Agosto de 2026

Nota sobre este documento. Se trata de una versión de trabajo no oficial, reelaborada a partir del documento «**Procedimien inclusión y clasificación de certificados en @firma**» (v3.9), disponible en https://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Descargas/Tratamiento%20de%20certificados%20en firma-v-3-8.pdf en la que se han aplicado las actualizaciones de terminología, normativa, organismos y enlaces derivadas de publicación del Reglamento (UE) 910/2014, modificado por el Reglamento (UE) 2024/1183 (eIDAS2), y de la Ley 6/2020. No reproduce el documento oficial, no incorpora identidad gráfica institucional y no constituye asesoramiento jurídico. Los enla marcados como «verificar» deben contrastarse con su ubicación vigente antes de cualquier publicación.
El documento de partida incluye información sobre actualizaciones desde 2011 a 2018.

1. Índice

2. Introducción

En este documento se detalla el procedimiento que se lleva a cabo para incluir en @firma y clasificar correctamente los certificados disponibles, teniendo en cuenta la lista de confianza (TSL), la información publicada por el organismo supervisor y la información indicada en el propio certificado.

Marco normativo de referencia: Reglamento (UE) 910/2014, modificado por el Reglamento (UE) 2024/1183 (eIDAS2), y sus reglamentos de ejecución; y Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (que derogó la Ley 59/2003). La función de supervisión corresponde al Ministerio para la Transformación Digital y de la Función Pública, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA); la plataforma @firma y la publicación de la lista de confianza dependen de la Secretaría General de Administración Digital (SGAD).

3. Consideraciones previas para el alta de un certificado

Para dar de alta un certificado de un prestador cualificado de servicios electrónicos de confianza (en adelante, PSCC; en eIDAS, *QTSP*) en @firma deben darse unas condiciones previas:

- El PSCC debe figurar en la lista de confianza (TSL) española o en el registro de prestadores publicado por el organismo supervisor `[verificar URL vigente en la sede del Ministerio para la Transformación Digital y de la Función Pública. En 2026: https://sedeaplicaciones.minetur.gob.es/Prestadores/]`.
- El PSCC ha solicitado su integración en @firma, para lo cual se ha firmado un convenio de colaboración entre la Secretaría de Estado de Función Pública y el responsable de la Autoridad de Certificación. En caso de que el prestador no esté integrado en @firma, se validarán los certificados acordes únicamente a la información incluida en la TSL, por lo que no aplicarán los apartados 5-7 de este documento.

- El PSCC ha solicitado la inclusión en @firma del certificado concreto, para lo cual es necesario que envíe cierta información a @firma:
    - Un certificado (parte pública) de ejemplo, con el que se puedan realizar los mapeos de los campos de los certificados. Este certificado de ejemplo debe cumplir una serie de características:
        - Debe tener el OID adecuado para su identificación respecto a otros certificados del mismo prestador.
        - Debe tener rellenos todos los campos que puedan existir en un certificado final. Si algún campo de un certificado real no está presente en el certificado de ejemplo, no es posible determinar el mapeo de ese campo.
    - DPC (Declaración de Prácticas de Certificación) y Política de Certificación.
    - Es deseable, para facilitar el uso del certificado por parte de las administraciones públicas, que se proporcionen certificados de pruebas, de usuarios ficticios (considerando las limitaciones definidas por e Organismo Supervisor):
        - Certificado válido (parte pública y privada).
        - Certificado revocado (parte pública y privada).
    - Los métodos de validación específicos para cada rama de la CA y los certificados con los que va firmado el OCSP/CRL.
    - La justificación de que el certificado está supervisado:
        - La ubicación exacta dentro de la TSL del certificado a dar de alta `[verificar URL vigente de la TSL española / o LOTL de la Comisión Europea. En 2026 https://tsl.digital.gob.es/TSL.pdf para PDF y https://tsl.digital.gob.es/TSL.xml para XML].`
        - La ubicación exacta dentro del registro de prestadores supervisados del certificado a dar de alta `[verificar URL vigente. En 2026 https://sedeaplicaciones.minetur.gob.es/Prestadores/].`
    - La clasificación que deberá darse al certificado:
        - Persona física, persona jurídica, empleado público… teniendo en cuenta la tabla del apartado 5 de este mismo documento.
        - El uso del certificado: firma, autenticación, ambos, otros.

Dadas las limitaciones técnicas, operativas y económicas del soporte de atención a los integradores y a las AAPP, se deben priorizar ciertas actividades para seguir ofreciendo un buen servicio:

- Se darán de alta los certificados por orden de llegada de la petición al servicio de soporte. La petición deberá incluir el certificado de ejemplo.
- Para peticiones directas de alta de certificados por parte de los PSCC, se darán de alta un número máximo de 5 nuevos certificados (5 OID) para cada PSCC cada 6 meses. Si se supera ese límite, el alta de las peticiones sucesivas deberá esperar a que el resto de peticiones de otros PSCC hayan sido atendidas.

4. Lista de certificados admitidos

La lista actualizada de los certificados incluidos en @firma, disponibles para validación por todas las aplicaciones, se encuentra publicada en la página del proyecto @firma, en el Centro de Transferencia de Tecnología (CTT) del Portal de Administración Electrónica (PAe).

Puede consultar la URL: `https://administracionelectronica.gob.es/ctt/afirma [verificar la ruta vigente del «Anexo PSC» en el Pae. En 2026: https://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Descargas/aFirma-Anexo-PSC.pdf]`

Observación. Por limitaciones del estándar OCSP, este protocolo no permite filtrar certificados por su OID. Por tanto, si distintos tipos de certificados han sido emitidos por una Autoridad de Certificación supervisada e incluida en la TSL, no se pueden distinguir los certificados cualificados (Qualified Certificates) de aquellos certificados no cualificados (non-Qualified Certificates), o incluso de certificados no supervisados, aunque estén asociados a Declaraciones de Prácticas de Certificación distintas (con distintos identificadores OID).

Por tanto, el servicio “OCSP responder” de @firma no garantiza la exclusión de certificados no cualificados o no supervisados, aunque sean emitidos por PKI supervisadas. En caso de que se quiera disponer de esta ventaja de @firma, sería necesario realizar las validaciones a través de los servicios web de @firma.

5. Clasificación de tipos de certificados

La plataforma @firma, a través del campo «clasificación» de la respuesta del WS de validación de certificado, proporciona una clasificación básica del tipo de certificado de que se trata. Los tipos son los siguientes:

- Clasificación = 0 – Persona física
- Clasificación = 1 – Persona jurídica (no cualificado)
- Clasificación = 2 – No cualificados
- Clasificación = 3 – Sede electrónica según la Ley 40/2015 (no cualificado)
- Clasificación = 4 – Sello según la Ley 40/2015 (no cualificado)
- Clasificación = 5 – Empleado público según la Ley 40/2015
- Clasificación = 6 – Entidad sin personalidad jurídica (no cualificado)
- Clasificación = 7 – Empleado público con seudónimo según la Ley 40/2015
- Clasificación = 8 – Cualificado de sello, según el Reglamento (UE) 910/2014
- Clasificación = 9 – Cualificado de autenticación de sitio web, según el Reglamento (UE) 910/2014
- Clasificación = 10 – Cualificado de servicio de sello de tiempo
- Clasificación = 11 – Persona física representante ante las Administraciones Públicas de persona jurídica
- Clasificación = 12 – Persona física representante ante las Administraciones Públicas de entidad sin personalidad jurídica

Nota. *Las referencias a la anterior Ley 11/2007 (LAECSP) se han sustituido por la Ley 40/2015, de Régimen Jurídico del Sector Público, y la Ley 39/2015, del Procedimiento Administrativo Común, que la derogaron. Esto incluye la eliminación de referencias al 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 los ciudadanos a los servicios públicos. Derogado por el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.*

Las clasificaciones devueltas por @firma coinciden con las clasificaciones de los certificados publicadas por el organismo supervisor. Pueden consultarse todos los certificados incluidos en @firma y su clasificación en el ANEXO PSC de la Declaración de Prácticas de validación de @firma [verificar URL vigente en el PAe / github.com/ctt-gob-es. En 2026 ver: https://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Descargas/aFirma-Anexo-PSC.pdf y https://administracionelectronica.gob.es/ctt/resources/Soluciones/190/Descargas/2016-Declaracion-Practicas-Validacion--afirma-9-0.pdf].

6. Mapeo tipo para cada clase de certificado

Para cada tipo de certificado dado de alta, en la respuesta de @firma se devuelven normalmente los siguientes datos:

a. Clasificación = 0 – Persona física – certificado cualificado de firma

Relativos al subject:

- subject
- nombreResponsable
- primerApellidoResponsable (si es posible su determinación unívoca a partir de los campos del certificado del PSCC)
- segundoApellidoResponsable (íd.)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI)
- ID_europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- email (si el PSCC lo incluye)
- unidadOrganizativa (si el PSCC lo incluye)
- organizacion (si el PSCC lo incluye)
- pais

Relativos al emisor (identifica la subCA emisora):

- idEmisor

- OrganizaciónEmisora

Relativos al certificado:

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

b. Clasificación = 1 – Persona jurídica (no cualificado)

Relativos al subject:

- subject
- — de la empresa — NIF-CIF (CIF de la empresa); razonSocial
- — del custodio — nombreResponsable
- primerApellidoResponsable / segundoApellidoResponsable (si es posible su determinación unívoca)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI del responsable)
- email (si el PSCC lo incluye)
- unidadOrganizativa
- organizacion
- pais

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

c. Clasificación = 2 – Componente/SSL – no cualificado

Relativos al subject:

- unidadOrganizativa
- organizacion
- pais
- subject

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

d. Clasificación = 3 – Sede electrónica (no cualificado)

Relativos al subject:

- NombreDominioIP (dominio al que pertenece la sede)
- sedeElectronica (breve descripción de la sede)
- email (si el PSCC lo incluye)
- 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

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

e. Clasificación = 4 – Sello (no cualificado)

Relativos al subject:

- DenominaciónSistemaComponente
- entidadSuscriptora
- DIR3
- NIFEntidadSuscriptora
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)

- organizacion
- pais
- subject
- — del responsable — nombreResponsable
- primerApellidoResponsable / segundoApellidoResponsable (si es posible su determinación unívoca)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI del responsable)
- ID_europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- email (si el PSCC lo incluye)

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

f. Clasificación = 5 – Empleado público

Relativos al subject:

- nombreResponsable
- primerApellidoResponsable / segundoApellidoResponsable (si es posible su determinación unívoca)
- ApellidosResponsable
- NombreApellidosResponsable
- email (si el PSCC lo incluye)
- NIFResponsable (DNI del responsable)
- ID_europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- numeroIdentificacionPersonal (NRP o NIP)
- puesto (puesto desempeñado dentro de la Administración)
- subject
- — relativos a la organización — entidadSuscriptora
- DIR3
- NIFEntidadSuscriptora
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- unidadOrganizativa
- organizacion
- pais

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

- clasificacion = 5

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

g. Clasificación = 6 – Entidad sin personalidad jurídica (no cualificado)

Relativos al subject:

- subject
- razonSocial
- NIF-CIF (CIF de la empresa)
- — del custodio — nombreResponsable
- primerApellidoResponsable / segundoApellidoResponsable (si es posible su determinación unívoca)
- ApellidosResponsable
- NombreApellidosResponsable
- email (si el PSCC lo incluye)
- NIFResponsable (DNI del responsable)
- unidadOrganizativa
- organizacion
- pais

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

h. Clasificación = 7 – Empleado público con seudónimo

Relativos al subject:

- email (si el PSCC lo incluye)
- seudonimo
- puesto (puesto desempeñado dentro de la Administración)
- subject
- — relativos a la organización — entidadSuscriptora
- DIR3
- NIFEntidadSuscriptora

- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- unidadOrganizativa
- organizacion
- pais

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

i. Clasificación = 8 – Cualificado de sello, Reglamento (UE) 910/2014

Relativos al subject:

- DenominaciónSistemaComponente
- entidadSuscriptora
- NIFEntidadSuscriptora
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- organizacion
- pais
- subject
- — del responsable — nombreResponsable
- primerApellidoResponsable / segundoApellidoResponsable (si es posible su determinación unívoca)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI del responsable)
- ID_europeo (DNI o identificador europeo, con codificación estándar según ETSI EN 319 412)
- email (si el PSCC lo incluye)

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

- validoHasta

j. Clasificación = 9 – Cualificado de autenticación de sitio web, Reglamento (UE) 910/2014

Relativos al subject:

- NombreDominioIP (dominio del sitio web, tal como figura en el Subject Alternative Names)
- email (si el PSCC lo incluye)
- entidadSuscriptora
- NIFEntidadSuscriptora
- OI_Europeo (NIF o identificador de la organización europeo, con codificación estándar según ETSI EN 319 412)
- organizacion
- pais
- subject

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

k. Clasificación = 10 – Cualificado de sello de tiempo

Relativos al subject:

- unidadOrganizativa
- organizacion
- pais
- subject

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

l. Clasificación = 11 – Persona física representante ante las AAPP de persona jurídica

Relativos al subject:

- subject
- — de la empresa — 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
- — del representante — nombreResponsable
- primerApellidoResponsable / segundoApellidoResponsable (si es posible su determinación unívoca)
- ApellidosResponsable
- NombreApellidosResponsable
- NIFResponsable (DNI)
- email (si el PSCC lo incluye)
- pais
- Documento de representación

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

m. Clasificación = 12 – Persona física representante ante las AAPP de entidad sin personalidad jurídica

Relativos al subject:

- subject
- — de la empresa — 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
- — del representante — nombreResponsable
- primerApellidoResponsable / segundoApellidoResponsable (si es posible su determinación unívoca)
- ApellidosResponsable
- NombreApellidosResponsable
- email (si el PSCC lo incluye)
- NIFResponsable (DNI del responsable)
- pais
- Documento de representación

Relativos al emisor (identifica la subCA emisora):

- idEmisor
- OrganizaciónEmisora

Relativos al certificado:

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

n. Observaciones

- El campo `certClassification` indica la clasificación del certificado acorde al Reglamento eIDAS.
- El campo ID_europeo es un identificador referente a la persona física o jurídica del certificado, basado en la norma ETSI EN 319 412-1.
- El campo `OI_Europeo` es un identificador referente a la entidad del certificado, basado en la norma ETSI EN 319 412-1.
- El campo `qscd` indica si el certificado ha sido emitido con una clave gestionada en un dispositivo cualificado de creación de firma o sello (QSCD); sus valores posibles son YES, NO y UNKNOWN. *(En versiones anteriores este campo se denominaba «sscd», en referencia al dispositivo seguro de creación de firma; la terminología adoptadas por eIDAS lo sustituye por QSCD.)*
- El campo `certQualified` indica si la TSL del país considera el certificado como cualificado; sus valores posibles son YES, NO y UNKNOWN.

7. Procedimiento de clasificación

A continuación, se detallan los pasos necesarios para incluir y clasificar un certificado en la plataforma @firma.

1. Se analiza si el emisor del certificado está en la TSL. Se recorren los TSP y, por cada uno, los TSP-Services contenidos (mientras no se haya encontrado el que corresponda con el certificado). Por cada servicio se comprueba si el tipo de servicio es alguno de estos:

- `http://uri.etsi.org/TrstSvc/Svctype/CA/QC`
- `http://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC` *(tipo heredado del modelo anterior a eIDAS; se conserva para compatibilidad con listas históricas)*

Si el tipo de servicio es CA/PKC, la subCA es no cualificada, por lo que los certificados emitidos por ella serán no cualificados: `http://uri.etsi.org/TrstSvc/Svctype/CA/PKC`

2. Se comprueba si el servicio (identificado por el SDI) está vigente mediante el SCS (Service Current Status), que indica el estado del servicio.

Con el modelo eIDAS, el estatus cualificado se expresa esencialmente como **granted** (vigente) y **withdrawn** (retirado). El resto de estados procede del modelo de supervisión/acreditación anterior a eIDAS y se conserva únicamente para la lectura de listas históricas.

Si el estado del servicio es alguno de los siguientes, se considerará que la cadena de certificación del certificado no es válida (servicio cesado o retirado):

- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn`
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased` (heredado)
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationceased` (heredado)

Y si es alguno de los siguientes, el certificado se considerará revocado:

- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionrevoked` (heredado)
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationrevoked` (heredado)
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel`

- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedbynationallaw`

Estos casos no se incluyen en @firma. Partiendo del TSP al que pertenece el certificado, se recorren sus TSP-Services y se comprueba que su estado sea válido, es decir, alguno de los siguientes:

- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted`
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel (heredado)`
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision (heredado)`
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation (heredado)`
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited (heredado)`
- `http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/setbynationallaw (heredado)`

Se comprueba que la fecha de inicio del servicio sea anterior a la fecha de validación.

3. Se analiza si el certificado es cualificado. Se examina el propio certificado. Se considerará cualificado si se cumple alguna de estas opciones:

- a) Si la extensión `QCStatements` (1.3.6.1.5.5.7.1.3) del certificado se encuentra definida e incluye la declaración `QcCompliance`.
- b) Si la extensión `CertificatePolicies` (2.5.29.32) está definida y al menos uno de los `PolicyInformation` se corresponde con:
  - `qcp-public-with-sscd (0.4.0.1456.1.1)`
  - `qcp-public (0.4.0.1456.1.2)`
  - `qcp-natural (0.4.0.194112.1.0)`
  - `qcp-legal (0.4.0.194112.1.1)`
  - `qcp-natural-qscd (0.4.0.194112.1.2)`
  - `qcp-legal-qscd (0.4.0.194112.1.3)`
  - `qcp-web (0.4.0.194112.1.4)`

Si el OID de la política de certificación es QCP/QCP+, el certificado está marcado como cualificado. *(Los nombres qcp-public-with-sscd y variantes -qscd son identificadores normalizados por ETSI; el sufijo «sscd» se mantiene por compatibilidad de nomenclatura de OID.)*

4. Si la información no viene en el certificado, se comprueba la TSL. Se analiza si alguna de las identidades digitales del servicio verifica ser la emisora del certificado. Si al menos uno de los `Qualifications` contiene algún Criteria que concuerde con el certificado, se toman los `Qualifiers` asociados (el proceso no se detiene en el primer Criteria: procesa todos los `Qualification` cuyo Criteria se cumpla). En este punto se considera encontrado el TSP correspondiente.

Si no se encuentra ningún Criteria acorde al certificado, pero Qualifications no es una extensión crítica, se considera cualificado igualmente. En otro caso, no se considera cualificado. Una vez detectado el TSP-Service que reconoce al certificado, se considerará cualificado si en alguna de las URI de los Qualifier asociados se encuentra:

- `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement`

Si en su defecto se encuentra la siguiente, se considerará no cualificado:

- `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified`

5. Se obtiene el tipo de certificado (solo para los certificados cualificados).

- a. Si la extensión `QCStatements (1.3.6.1.5.5.7.1.3)` está definida y contiene el `QCstatement QcType (0.4.0.1862.1.6)`, en función de los OID que contenga:
  - `id-etsi-qct-esign (0.4.0.1862.1.6.1)` → **ESIG**
  - `id-etsi-qct-eseal (0.4.0.1862.1.6.2)` → **ESEAL**
  - `id-etsi-qct-web (0.4.0.1862.1.6.3)` → **WSA**
- b. Si la extensión `CertificatePolicies (2.5.29.32)` está definida, según los `PolicyInformation` se considerará:
  - **ESIG** si alguno se corresponde con: `qcp-public-with-sscd, qcp-public, qcp-natural, qcp-natural-qscd`
  - **ESEAL** si alguno se corresponde con: `qcp-legal, qcp-legal-qscd`
  - **WSA** si alguno se corresponde con: `qcp-web`

- c. Si el certificado se ha reconocido en la TSL, las siguientes URI de `Qualifiers` determinan los valores del mapeo certClassification:
    - `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForLegalPerson → LEGAL_PERSON`
    - `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig → ESIG`
    - `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal → ESEAL`
    - `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA → WSA`

6. Se obtiene el detalle del tipo de certificado (solo para los cualificados emitidos por PSCC españoles). Una vez analizada toda la información de la TSL y del propio certificado, se comprueban las listas del organismo supervisor para obtener más detalle y terminar de clasificar el certificado:

- a. Certificado de Sello (**ESEAL**) español: se revisa el esquema y el registro de prestadores publicados por el organismo supervisor `[verificar URL vigente]`. Si el OID está incluido como «Certificados de Sello electrónico de la Administración Pública», se trata de un certificado de sello según la Ley 40/2015 (tipo 4). En caso de no ser español o no encontrarse en dicha lista, se trataría de un certificado de sello según el Reglamento (UE) 910/2014 (tipo 8).
- b. Certificado de autenticación de sitio web (**WSA**) español: se consulta la lista de certificados de sede del organismo supervisor `[verificar URL vigente]`. Si el OID está incluido, se trata de un certificado de sede según la Ley 40/2015 (tipo 3). En caso contrario, sería un certificado de autenticación de sitio web según el Reglamento (UE) 910/2014 (tipo 9).
- c. Certificado de firma (**ESIG**) español que **NO** posea el bit `Content Commitment` (antiguo "no repudio") si el PSCC indica que es un certificado de la normativa de administración electrónica, se revisará si tiene habilitado únicamente el bit «`Digital Signature`» o únicamente «`dataEncipherment`». Se revisará el registro de prestadores del organismo supervisor: si el OID está incluido en «Certificados electrónicos de Empleado Público», se comprobará si cumple los perfiles de empleado público con o sin seudónimo. En su caso, será un certificado de empleado público (tipo 5) o de empleado público con seudónimo (tipo 7), con funciones únicas de autenticación o cifrado respectivamente. El uso vendrá indicado en el campo UsoCertificado.
- d. Certificado de firma (**ESIG**) español que **SÍ** posea el bit `Content Commitment` (antiguo "no repudio"): es un certificado de firma. Se revisará el registro de prestadores del organismo supervisor:
    - Si el OID está incluido en «Certificados electrónicos de Empleado Público», se comprobará si cumple los perfiles de empleado público con o sin seudónimo: será un certificado de empleado público (tipo 5) o de empleado público con seudónimo (tipo 7).
    - Se revisará si cumple los perfiles de certificados de representación (ver el anexo correspondiente de **perfiles de certificados de la AGE**):
        - Si tiene el OID `2.16.724.1.3.5.8`, será un certificado de persona física representante ante las AAPP de persona jurídica (tipo 11).
        - Si tiene el OID `2.16.724.1.3.5.9`, será un certificado de persona física representante ante las AAPP de entidad sin personalidad jurídica (tipo 12).
    - Si, siendo **ESIG** con `Content Commitment,` no encaja en ninguno de los casos anteriores, estaremos ante un certificado cualificado de firma (tipo 0).
- e. Certificado desconocido (UNKNOWN): será necesario revisar si en la TSL aparece como servicio de sello de tiempo y cumple las normas técnicas para ser considerado como tal; en cuyo caso, se considerará un certificado de sello de tiempo (tipo 10).

7. Se analiza si el certificado está en un dispositivo cualificado de creación de firma o sello (QSCD).

- a. El campo `qscd → YES` cuando:
    - La extensión `QCStatements (1.3.6.1.5.5.7.1.3)` está definida y contiene el `QCstatement QcSSCD/QcEuSSCD (0.4.0.1862.1.4).`
    - La extensión `CertificatePolicies (2.5.29.32)` está definida y alguno de los `PolicyInformation` se corresponde con: `qcp-public-with-sscd (0.4.0.1456.1.1), qcp-natural-qscd (0.4.0.194112.1.2), qcp-legal-qscd (0.4.0.194112.1.3)`
- b. Si el certificado se ha reconocido en la TSL, las siguientes URI de Qualifiers determinan el valor del mapeo qscd:
    - `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD → YES`
    - `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD → NO`
    - `http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf → YES`

    - (Heredados, en desuso) `QCWithSSCD → YES` y `QCNoSSCD → NO`; estos qualifiers SSCD fueron sustituidos por sus equivalentes QSCD en ETSI TS 119 612 v2.
- c. Si aun así no se ha podido determinar que se encuentra en un QSCD, se entiende que no lo está → NO.

Nota. En el caso de que el certificado raíz o de SubCA se encuentre en la TSL pero el certificado a dar de alta no figure indicado como cualificado, sería posible darlo de alta clasificándolo como «No cualificado», siendo necesario que el PSCC notifique que pasa a cualificado en la TSL para que a su vez se actualice en la plataforma @firma.

8. Procedimiento de disconformidades

En caso de que un PSCC no esté de acuerdo con la clasificación dada a su certificado por la plataforma @firma, puede ponerse en contacto con el Centro de Atención a Integradores y Desarrolladores (CAID) abriendo una incidencia mediante el formulario correspondiente `https://soportecaid.redsara.es/ayuda/consulta/caid [verificar la ruta vigente del CAID]`.

En dicha incidencia deberá indicarse el OID del certificado o certificados que se solicita reclasificar, la justificación de que está incluido en la TSL y las razones por las que se estima que la clasificación no es correcta.