Dirección de Tecnologías de la Información y las Comunicaciones
C/ María de Molina, 50. 28071. Madrid.

Procedimiento de inclusión y clasificación de certificados en @firma.
Versión 3.9

Historia del documento:		
Fecha:	Versión:	Descripción:
27/10/2011	V2.0	Actualización
14/12/2011	V2.1	Actualización
09/02/2012	V2.2	Actualización
21/02/2012	V2.3	Actualización
24/04/2012	V2.4	Actualización
29/06/2012	V2.5	Actualización de URL de MINETUR
27/07/2012	V2.6	Actualización de nombres de campos mapeados
28/02/2013	V2.7	Actualización de URL's de MINETUR
14/04/2016	V3.0	Actualización del documento con los nuevos cambios a nivel europeo
16/04/2016	V3.1	Actualización
27/05/2016	V3.2	Actualización
21/06/2016	V3.3	Actualización de los certificados de sede y sello
28/06/2016	V3.4	Actualización URL del Anexo de certificados incluidos en @firma
27/07/2016	V3.5	Revisión de errores
26/09/2016	V3.6	Se actualizan los nombres de los mapeos y se revisan errores
27/06/2017	V3.7	Actualización
28/11/2017	V3.8	Actualización URLs
02/02/2018	V3.9	Actualización de los mapeos

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 TSL, la información del MINETUR y la información indicada en el propio certificado.

3. Consideraciones previas para el alta de un certificado

Para dar de alta un certificado de un PSC en @firma deben darse unas condiciones previas:

- El PSC debe estar dado de alta en la web de certificados supervisados por industria: (https://sedeaplicaciones.minetur.gob.es/Prestadores/) o el la TSL.

- El PSC ha solicitado su integración en @firma, para lo cual se ha firmado un convenio de colaboración entre la Secretaria 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 acorde únicamente a la información incluida en la TSL, por lo que no aplicarán los apartados 5-7 de este documento.

- El PSC ha solicitado la inclusión en @firma del certificado concreto, para lo cual es necesario que envíe cierta información a @firma:

  - Un certificado (parte pública) ejemplo, con el que se puedan realizar los mapeos de los campos de los certificados. Es necesario destacar que este certificado ejemplo debe cumplir una serie de características:
    - Debe tener el OID adecuado para su identificación respecto a otros certificados del mismo prestador
    - Debe tener todos los campos que puedan existir en un certificado final rellenos. En caso de que algún campo de un certificado real no estén presente en el certificado ejemplo, no es posible determinar el mapeo de ese campo.

  - DPC y Política de certificación.

  - Es deseable, para facilitar el uso del certificado concreto por parte de las administraciones públicas, que se proporcionen certificados de pruebas, de usuarios ficticios.
    - 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 (https://sede.minetur.gob.es/Prestadores/TSL/TSL.pdf) del certificado a dar de alta.
- La ubicación exacta dentro de la web de la Ley 59/2003 del certificado a dar de alta (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.

Dada 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 ejemplo.

- Para peticiones directas de alta de certificados por parte de los PSCs, se darán de alta un número máximo de 5 nuevos certificados (5 OIDs) para cada PSC cada 6 meses. Si se supera ese límite, el alta de las peticiones sucesivas deberá esperar a que el resto de peticiones de otros PSC 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 disponible en la página del proyecto @firma, en el centro de Transferencia de Tecnología, del Portal de Administración Electrónica:

Puede consultar la URL: http://administracionelectronica.gob.es/PAe/aFirma-Anexo-PSC

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 por el MINETUR y por tanto 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 por el Ministerio de Industria, Energía y Turismo, 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 según la ley de firma 59/ 2003 y la Ley 11/2007, aunque sean emitidos por PKI supervisadas.

En caso 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 que se trata.

Los tipos son los que se incluyen a continuación:

- Clasificación = 0 – Persona física
- Clasificación = 1 – Persona jurídica (no cualificado)
- Clasificación = 2 – No cualificados
- Clasificación = 3 – Sede 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 el RD 1671/2009
- Clasificación = 8 – Cualificado de sello, según el reglamente UE 910/2014
- Clasificación = 9 – Cualificado de autenticación, según el reglamente UE 910/2014
- Clasificación = 10 – Cualificado de servicio cualificado 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 persona jurídica

Las clasificaciones devueltas por @firma coinciden con las clasificaciones de los certificados indicados por el MINETUR. Pueden consultar todos los certificados incluidos en @firma y su clasificación en el ANEXO PSC’s de la Declaración de Practicas de validación de @firma:

http://forja-ctt.administracionelectronica.gob.es/webdav/site/ctt-map/users/soporte_afirma/public/@FirmaV5p0_ANEXO_PSC.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 para cada tipo de certificado:

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 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)
  - 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
- 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 (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)
        - email (si el PSC lo incluye en sus certificados)
        - unidadOrganizativa
        - organizacion
        - pais
    - Relativos al emisor:
        - idEmisor
        - OrganizacionEmisora
    - 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:
    - idEmisor
    - OrganizacionEmisora
- 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 (no cualificado)

- 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

- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora
- 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 (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
  - --- del responsable ---
  - 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)
- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora

- Relativos al certificado:
  - clasificación = 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 (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
  - ---- Relativos a la organización -------
  - 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
- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora
- Relativos al certificado:
  - clasificación =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 (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
- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora
- Relativos al certificado:
  - clasificación =6
  - extensionUsoCertificado
  - numeroSerie
  - politica
  - certClassification
  - certQualified
  - qscd
  - tipoCertificado (nombre común en la plataforma @firma)
  - usoCertificado
  - validoDesde
  - validoHasta

h. Clasificación = 7 – Empleado Público con Seudónimo

- 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
  - ---- Relativos a la organización -------
  - 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

- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora
- Relativos al certificado:
  - clasificación =7
  - extensionUsoCertificado
  - numeroSerie
  - politica
  - certClassification
  - certQualified
  - qscd
  - tipoCertificado (nombre común en la plataforma @firma)
  - usoCertificado
  - validoDesde
  - validoHasta

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

- 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
  - --- del responsable ---
  - 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)
- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora
- Relativos al certificado:
  - clasificación = 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 (UE 910/2014)

- 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 de la organización europeo, con codificación estándar según ETSI EN 319 412)
  - organizacion
  - pais
  - subject
- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora
- Relativos al certificado:
  - clasificación = 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:
  - idEmisor
  - OrganizaciónEmisora
- Relativos al certificado:
  - clasificación = 10

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

I. 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 (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
- Relativos al emisor:
  - idEmisor
  - OrganizaciónEmisora
- Relativos al certificado:
  - clasificación = 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 persona 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 (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
- Relativos al emisor:
  - idEmisor
  - OrganizacionEmisora
- Relativos al certificado:
  - clasificación = 12
  - extensionUsoCertificado
  - numeroSerie
  - politica
  - certClassification
  - certQualified
  - qscd
  - tipoCertificado (nombre común en la plataforma @firma)
  - usoCertificado
  - validoDesde
  - validoHasta

n. Observaciones:

- El campo certClassification indica la clasificación del certificado acorde al eIDAS.
- El campo “ID_europeo” es un identificador referente a la persona física o jurídica del certificado basado en la normativa ETSI EN 319 412-1.
- El campo “OI_Europeo” es un identificador referente a la entidad del certificado basado en la normativa ETSI EN 319 412-1.
- El campo qscd indica si el certificado ha sido emitido en un dispositivo seguro, sus valores posibles son YES, NO y UNKNOWN.
- El campo certQualified indica si la TSL del país considera el mismo como certificado cualificado, sus valores posibles son YES, NO y UNKKOWN.

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 de estos se analizan los TSP-Services contenidos (mientras no se haya encontrado el que corresponda con el certificado). Por cada uno de estos se comprueba si el tipo de servicio es alguno de estos: CA/QC, o NationalRootCA-QC.

   http://uri.etsi.org/TrstSvc/Svctype/CA/QC

   http://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC

   Si el tipo de servicio es CA/PKC, la subCA es no cualificada, por lo que los certificados emitidos por ella será no cualificados:

   http://uri.etsi.org/TrstSvc/Svctype/CA/PKC:

2. Se comprueba si el servicio (identificado por el SDI) está supervisado.

   (o si tiene el estado de cualificado) mediante el SCS (Service Current Status) que indica el estado del servicio.

   Si el estado del Servicio es alguno de los siguientes, se considerará que la cadena de certificación del certificado no es válida:

   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationceased

   En cambio, si el estado del Servicio es alguno de los siguientes, se considerará que el certificado se encuentra revocado:

   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionrevoked
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationrevoked
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn

   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedatnationallevel
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedbynationallaw

   Estos dos casos no se incluyen en @firma.

   Partiendo del TSP en el que se ha detectado que el certificado pertenece, se recorren los TSP-Services contenidos y por cada uno de estos se comprueba que su estado sea correcto, es decir, que sea uno de los siguientes:

   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/recognisedatnationallevel
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited
   http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/setbynationallaw

   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 debe mirar en el propio certificado. Se considerará cualificado si se cumple alguna de las siguientes opciones:

   a) Si la extensión QCStatements (1.3.6.1.5.5.7.1.3) del certificado se encuentra definida. Incluye la declaración QcCompliance.

   b) Se encuentra definida la extensión CertificatePolicies (2.5.29.32), y al menos uno de los PolicyInformation definidos 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.

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, y se toman los Qualifiers asociados (a tener en cuenta que el proceso no para con el primer Criteria encontrado, sino que procesa todos los Qualification cuyo Criteria se cumpla). En este punto ya se considera que se ha encontrado el TSP correspondiente al certificado.

   Si no se ha encontrado ningún Criteria acorde al certificado, pero Qualifications no es una extensión crítica, se considera cualificado igualmente el certificado.

   En otro caso no se considera cualificado.

   Una vez se detecta 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:
   http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified
   se considerará como **no cualificado**

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) del certificado se encuentra definida, y además esta contiene el QCstatement QcType (0.4.0.1862.1.6), en función de las 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. Se encuentra definida la extensión CertificatePolicies (2.5.29.32), y según los PolicyInformation definidos se considerará:
   - **ESIG** si alguno de los Policy Information 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-natural-qscd (0.4.0.194112.1.2)
   - **ESEAL** si alguno de los Policy Information se corresponde con:
     qcp-legal (0.4.0.194112.1.1)
     qcp-legal-qscd (0.4.0.194112.1.3)
   - **WSA** si alguno de los Policy Information se corresponde con:
     qcp-web (0.4.0.194112.1.4)

c. Si se ha reconocido el certificado en la TSL, las siguientes URIs de Qualifiers determinarían los valores indicados para el 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 certificados cualificados emitidos por PSC españoles)

Una vez se ha analizada toda la información de las TSL y del propio certificado, es necesario comprobar las listas de MINETUR para obtener más detalle y terminar de clasificado el certificado:

a. En caso de que se trate de un certificado de Sello (**ESEAL**) español se revisa:

   - la página del MINETUR del esquema (http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/SchemeService_es.aspx),
   - la página de los prestadores, la Categoría de servicio según la Ley 11/2007 https://sedeaplicaciones.minetur.gob.es/Prestadores/

   Si el OID está incluido como “Certificados de Sello electrónico de la Administración Pública”, se trata de un certificado de sello según la ley 11/2007 **(tipo 4).**

   En caso de no ser español o no encontrarse en dicha lista, se trataría de un certificado de sello según el reglamente UE 910/2014 (**tipo 8**).

b. En caso de que se trate de un certificado de autenticación de sitio web (**WSA**) español consultar la página del artículo 30.2 del MINETUR de los certificados de sede (https://sedeaplicaciones.minetur.gob.es/Prestadores/): Si el OID está incluido, se trata de un certificado de sede según la ley 11/2007 **(tipo 3)**.

En caso de no ser español o no encontrarse en dicha lista, se trataría de un certificado de autenticación de sitio web según el reglamente UE 910/2014 (**tipo 9**).

c. En caso de que se trate de un certificado de firma (**ESIG**) español, y NO posea el bit Content Commitment (Sin repudio) si el PSC indica que es un certificado de la ley 11/2007, se revisará si el certificado tiene habilitado únicamente el bit "Digital Signature" o únicamente "dataEncipherment ".

   Se revisará la página del MINETUR de los prestadores, la Categoría de servicio según la Ley 11/2007

   https://sedeaplicaciones.minetur.gob.es/Prestadores/

   Si el OID está incluido en el apartado "Certificados electrónicos de Empleado Público", se revisará si el certificado cumple los perfiles de empleado público con o sin seudónimo.

   Si es así, se tratará bien de un certificado de empleado público según la ley 11/2007 **(tipo 5)** o bien de un certificado de empleado público con seudónimo según el RD 1671/2009 **(tipo 7)** con funciones únicas de autenticación o cifrado respectivamente. El uso del certificado vendrá indicado en el campo UsoCertificado.

d. En caso de que se trate de un certificado de firma (**ESIG**) español, y SÍ posea el bit Content Commitment (Sin repudio), se trata de un certificado de firma.

   - Se revisará la página del MINETUR de los prestadores, la Categoría de servicio según la Ley 11/2007 :

     https://sedeaplicaciones.minetur.gob.es/Prestadores/

     Si el OID está incluido en el apartado "Certificados electrónicos de Empleado Público", se revisará si el certificado cumple los perfiles de empleado público con o sin seudónimo y si es así, se tratará bien de un certificado de empleado público según la ley 11/2007 **(tipo 5)** o bien de un certificado de empleado público con seudónimo según el RD 1671/2009 **(tipo 7)**.

   - Se revisará si cumplen los perfiles de certificados de representación (ver Anexo I del documento "Perfiles de certificados def (ANEXO II) v2.0._10_FINAL"):
     - si tiene el OID "2.16.724.1.3.5.8", se tratará de un certificado de persona física Representante ante las Administraciones Públicas de persona jurídica **(tipo 11).**
     - si tiene el OID "2.16.724.1.3.5.9", se tratará de un certificado de persona física Representante ante las Administraciones Públicas de entidad sin personalidad jurídica **(tipo 12)**.

- En caso de que no cumpla de que cumpla los apartados anteriores (tipo ESIG, con Content Commitment) sin tratarse de los anteriores casos, estaremos ante un certificado cualificado de firma **(tipo 0)**.

e. En caso de que se trate de un 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 seguro:
   a. El campo SSCD -> YES:
      - Si la extensión QCStatements (1.3.6.1.5.5.7.1.3) del certificado se encuentra definida, y además esta contiene el QCstatement QcEuSSCD (0.4.0.1862.1.4)
      - Se encuentra definida la extensión CertificatePolicies (2.5.29.32), 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 se ha reconocido el certificado en la TSL, las siguientes URIs de Qualifiers determinarían los valores indicados para el mapeo sscd:
      http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD --> YES
      http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD--> NO
      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

   c. Si aun así no se ha podido determinar que se encuentra en un SSCD, se entiende que no lo está --> NO

Nota: En el caso de que el certificado raíz se encuentre en la TSL pero el certificado a dar de alta no se encuentre indicado como cualificado, sería posible dar de alta el mismo pero clasificándolo como “No cualificado”, siendo necesario que el PSC notifique que el mismo, cambia a cualificado en la TSL para que a su vez sea actualizado en la Plataforma @firma.

8.Procedimiento de disconformidades

En caso de que un PSC no esté de acuerdo con la clasificación que se ha dado a su certificado por parte de la Plataforma @firma, puede ponerse en contacto con el Centro de Atención a Integradores y Desarrolladores (CAID) del MINHAP abriendo incidencia mediante el formulario localizado en https://soportecaid.redsara.es/ayuda/consulta/caid

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