UNIVERSIDAD D SEVILLA

Políticas de Seguridad

Política de certificación de @FIRMA de la Universidad de Sevilla

Índice

1. Objeto

El objeto de este documento es establecer una base sólida que defina una política de certificación para la plataforma @firma personalizada para la Universidad de Sevilla (US). La política que se propone cumple con los siguientes requisitos imprescindibles.

- Mínima. Contempla solamente los prestadores de servicios de certificación (PSCs) utilizados en la US.
- Completa. Contempla los prestadores de servicios de certificación (PSCs) utilizados en la US.
- Correcta. Define los métodos de validación necesarios para permitir la validación de cada uno de los certificados dados de alta en la plataforma @firma.
- Autodocumentada. Incluye las referencias hacia las Declaraciones de Prácticas de Certificación (DPCs) de cada PSC.
- Segura. Solamente los administradores cualificados podrán gestionar la política de certificación.
- Mantenible. Se definen los mecanismos de mantenimiento obligatorios para tenerla siempre actualizada.
- Independiente. No dependerá de ningún organismo tercero para realizar las acciones de mantenimiento de la política de certificación.
- Extensible. La política podrá ser extendida en cualquier momento, definiendo en este mismo documento las pautas a seguir para dar soporte a nuevos PSCs.

Los conceptos básicos de la política de certificación definida comprenden los siguientes aspectos que veremos detalladamente en sus correspondientes apartados.

1. Prestadores de Servicios de Certificación (en adelante PSC)
2. Métodos de Validación.

2. Referencias

Declaración de Prácticas de Certificación de la Fábrica Nacional de Moneda y Timbre (DPC FNMT) https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

Declaración de Prácticas de Certificación del DNIE (DPC DNIE)

http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_501

Declaración de Prácticas de Certificación de CAMERFIRMA (DPC CAMERFIRMA)

http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

3. Acrónimos

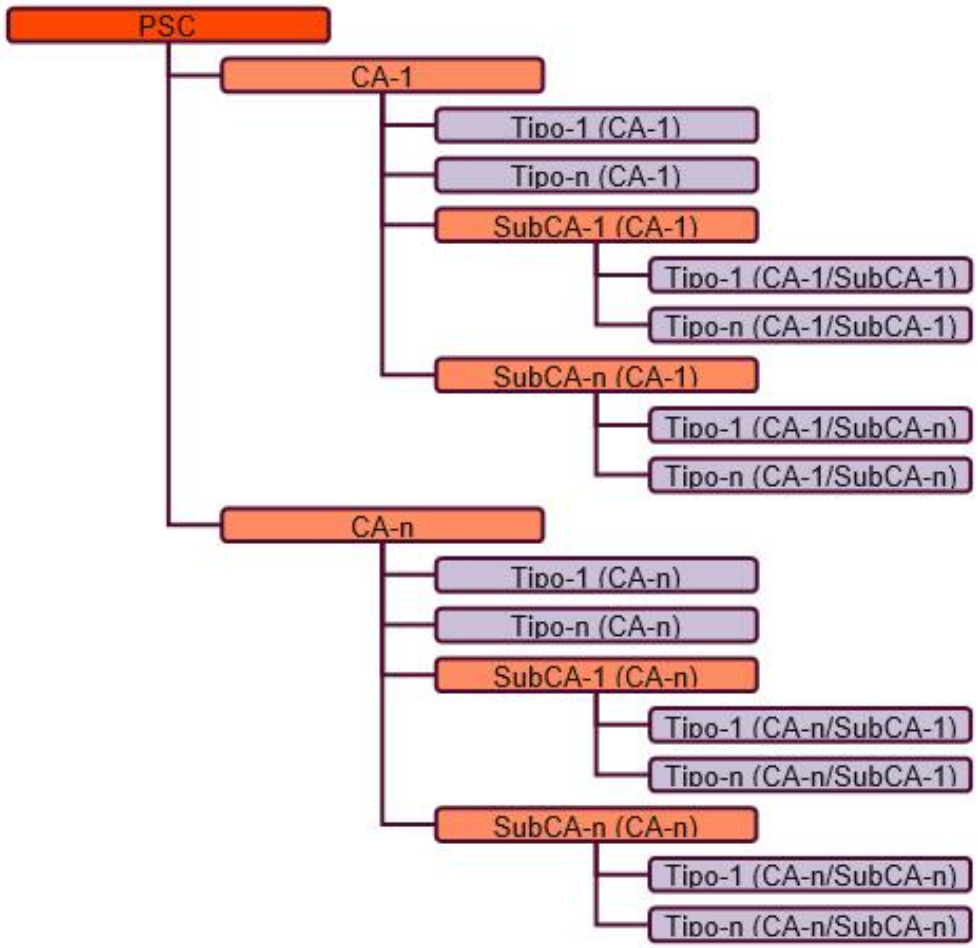
PSC	Prestador de Servicios de Certificación
CA	Autoridad de Certificación
SubCA	Sub Autoridad de Certificación
DPC	Declaración de Prácticas de Certificación
FNMT	Fábrica Nacional de Moneda y Timbre
RCM	Real Casa de la Moneda
CC	Certificados Camerales
CRL	*Certificate Revocation List*
OCSP	*Online Certificate Status Protocol*
LDAP	*Lightweight Directory Access Protocol*
DP	*Distribution Point*
PEM	*Privacy-enhanced Electronic Mail*

4. Prestadores de Servicios de Certificación

Un PSC es una entidad emisora de certificados para diferentes ámbitos. El PSC define uno o más certificados raíz como autoridades de certificación (CAs), las cuales emiten los diferentes tipos de certificados aplicables en su ámbito. A su vez, cada CA también podrá emitir una o más autoridades de certificación subordinadas (SubCAs), qué emitirán sus propios tipos de certificados.

De esta forma un PSC podrá formar una o varias jerarquías de certificación en función del número de CAs que emite, las cuales suelen tener largos periodos de vigencia, al igual que las SubCAs. Por el contrario, los tipos de certificados emitidos por cada CA o SubCA suelen tener periodos de vigencia de pocos años o meses, ya que son estos certificados finales los utilizados de forma cotidiana y por ende son susceptibles de sufrir revocaciones por diferentes motivos de seguridad.

Un ejemplo genérico para la jerarquía de un PSC es la siguiente:



Los PSCs distribuyen las claves públicas de sus CAs y SubCAs para permitir la confianza de estas en los diferentes sistema de PKI, como es el caso de @firma, que utilizará estos certificados para configurar los PSCs soportados por la plataforma. Toda la información del PSC (CAs, SubCAs y tipos de certificados) es publicada en una o varias Declaraciones de Prácticas de Certificación (DPCs), un documento que indica cuales son los propósitos y extensiones

configuradas en cada certificado y que supone una información imprescindible para configurar correctamente la plataforma @firma.

De todas las claves que incluyen los certificados debemos centrarnos principalmente en el identificador de política (p.e. 1.3.6.1.4.1.5734.3.3.4.4.1), ya que identifica de manera única cada certificado de un PSC que veremos en las jerarquías de los apartados correspondientes a cada PSC. Esto es muy importante ya que será el campo utilizado para que la plataforma @firma pueda discriminar que tipo de certificado llega con cada petición y así poder aplicarle los procedimientos correspondientes.

Una vez definida la estructura de los PSCs procedemos a enumerar los prestadores reconocidos por la Universidad de Sevilla y que veremos detalladamente en los siguientes apartados.

- FNMT. Fábrica Nacional de Moneda y Timbre.
- eDNI. Documento Nacional de Identidad Electrónico.
- Camerfirma. Cámara de Comercio.

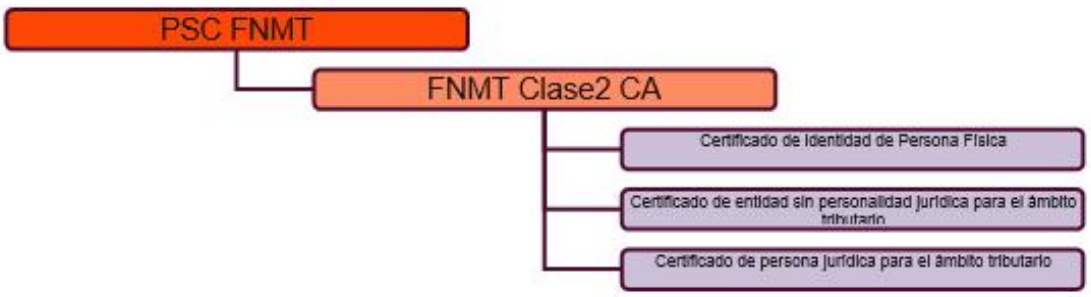
4.1. Fábrica Nacional de Moneda y Timbre (FNMT)

La FNMT emite diferentes CAs con sus tipos correspondientes, de las cuales la Universidad de Sevilla reconoce las siguientes.

1. FNMT Clase2 CA. Autoridad de certificación en vía de extinción y que debe ser soportada por compatibilidad con las personas, entidades y componentes que aún tienen en vigor sus certificados. Las consiguientes emisiones de estos certificados serán sobre la nueva CA definida al respecto por la FNMT y que vemos a continuación.
2. AC FNMT-RCM. Autoridad de certificación actual de la FNMT y que emite certificados para muy diversos ámbitos y que serán reconocidos por la US.

4.1.1. FNMT Clase2 CA

Esta Autoridad de Certificación fue emitida el 18 de marzo de 1999 y tiene una vigencia de 20 años, caducando el 18 de marzo de 2019. Aunque esta CA está siendo discontinuada, se mantiene por compatibilidad con los certificados vigentes en la actualidad y hasta el día de su caducidad. Ha de tenerse en cuenta que las renovaciones de estos certificados ya están siendo emitidos por la nueva CA especificada en el siguiente apartado 4.1.2.

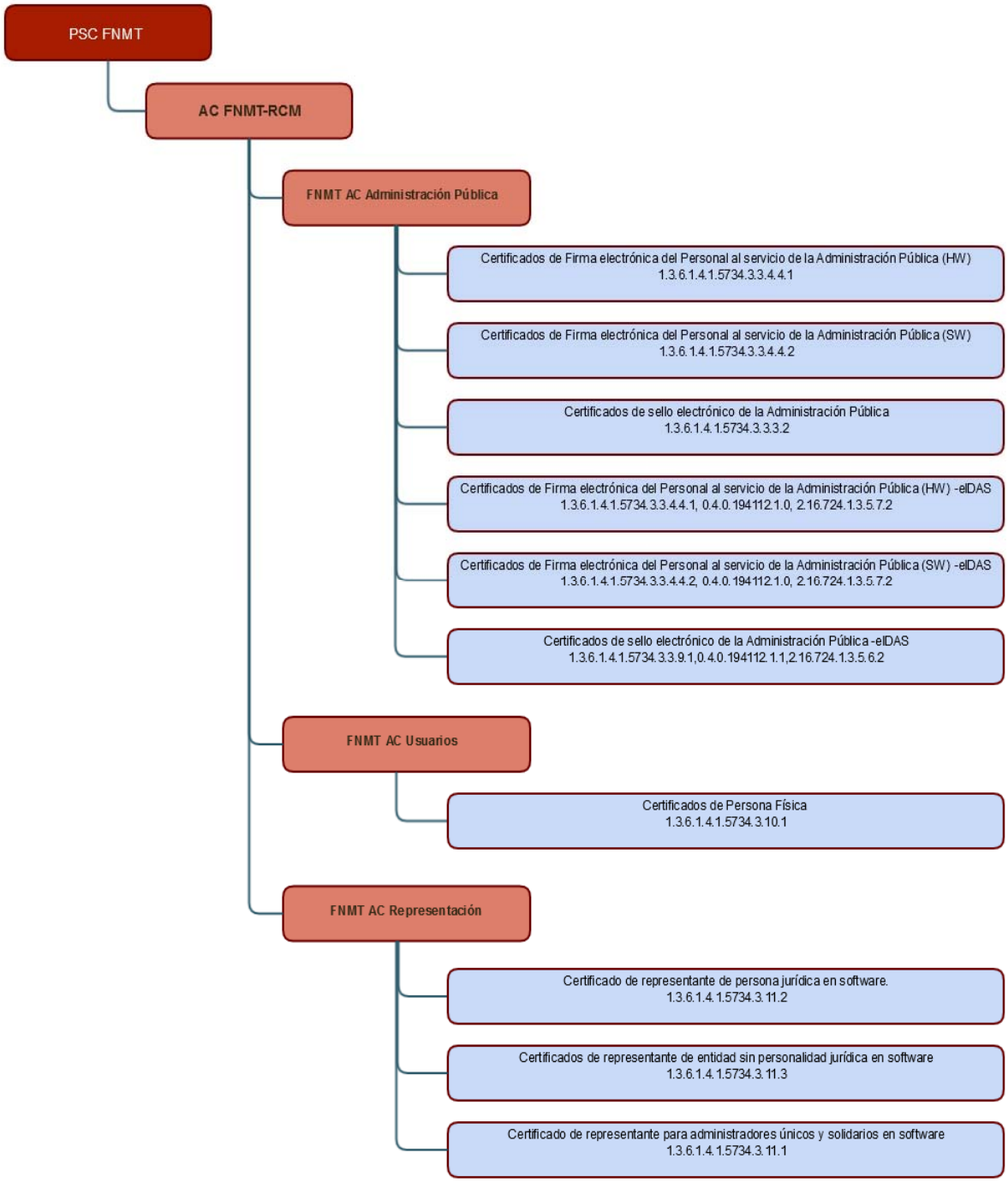


Los certificados de FNMT Clase2 CA no incluyen un identificador de política válido para identificar inequívocamente cada tipo de certificado emitido, de forma que para la configuración de @firma usaremos los siguientes discriminadores.

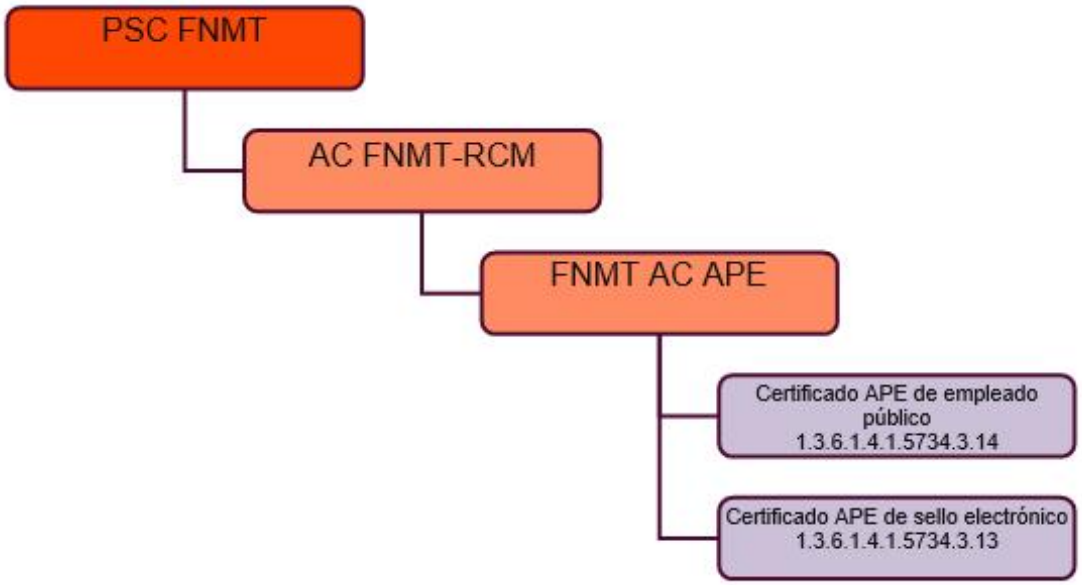
- Certificado de identidad de Persona Física.
  - EXTENSION::1.3.6.1.4.1.5734.1.33 = PERSONA FISICA
- Certificado de entidad sin personalidad jurídica para el ámbito tributario.
  - EXTENSION::1.3.6.1.4.1.5734.1.33 = CERTIFICADO DE ENTIDAD CARENTE DE PERSONALIDAD JURIDICA EXCLUSIVO PARA EL AMBITO TRIBUTARIO
- Certificado de persona jurídica para el ámbito tributario.
  - EXTENSION::1.3.6.1.4.1.5734.1.33 = CERTIFICADO EXCLUSIVO PARA EL AMBITO TRIBUTARIO

4.1.2. AC FNMT RCM

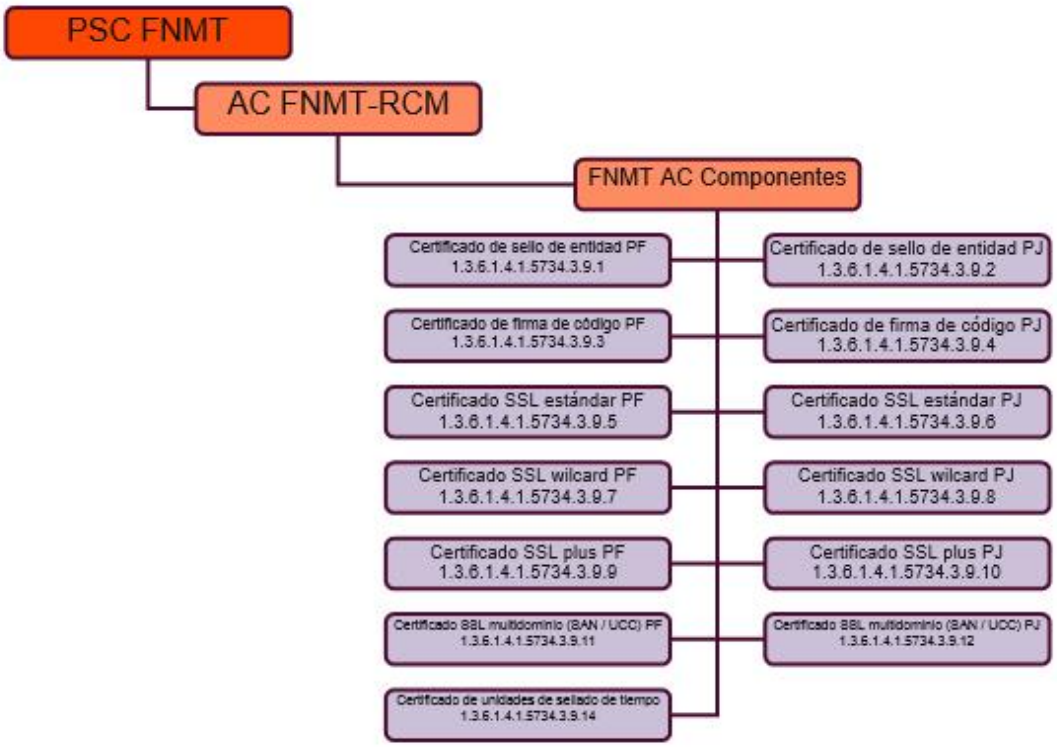
Esta Autoridad de Certificación fue emitida el 29 de octubre de 2008 y tiene una vigencia de aproximadamente 22 años, caducando el 1 de enero de 2030. La CA contempla todos los tipos de certificados emitidos por la FNMT, incluyendo los emitidos por otras CA en proceso de discontinuación. En la siguiente jerarquía de la FNMT se muestran solo los certificados finales para uso en firma electrónica o autenticación, conformando el conjunto de certificados más actualizado de la FNMT como prestador.



Además de la jerarquía anterior que muestra el estado actual y vigente de la FNMT como prestador en lo referente a certificados para firma electrónica y autenticación, existe otra SubCA obsoleta que debe mantenerse por compatibilidad con los certificados de Administración Pública emitidos anteriormente.

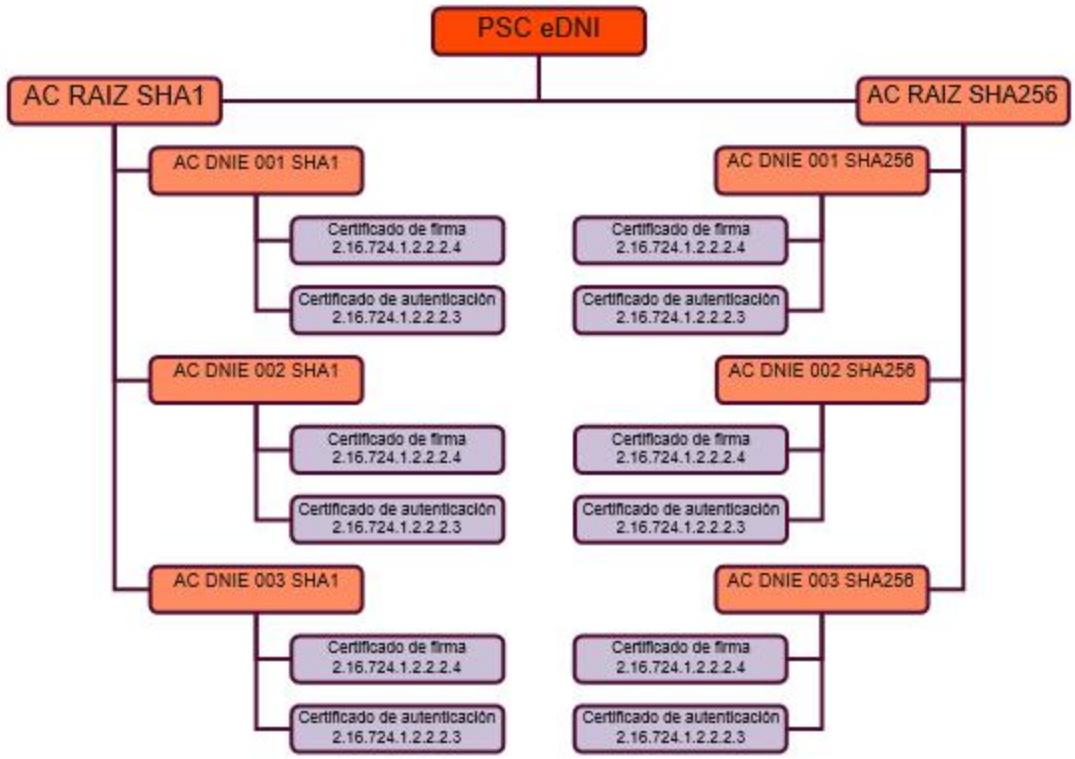


Por último, se muestra la SubCA correspondiente a los certificados de componentes emitidos por esta CA y aunque es muy poco probable que se intente validar uno de estos certificados por @firma, serán incluidos como certificados reconocidos por la US.



4.2. Documento Nacional de Identidad Electrónico (eDNI)

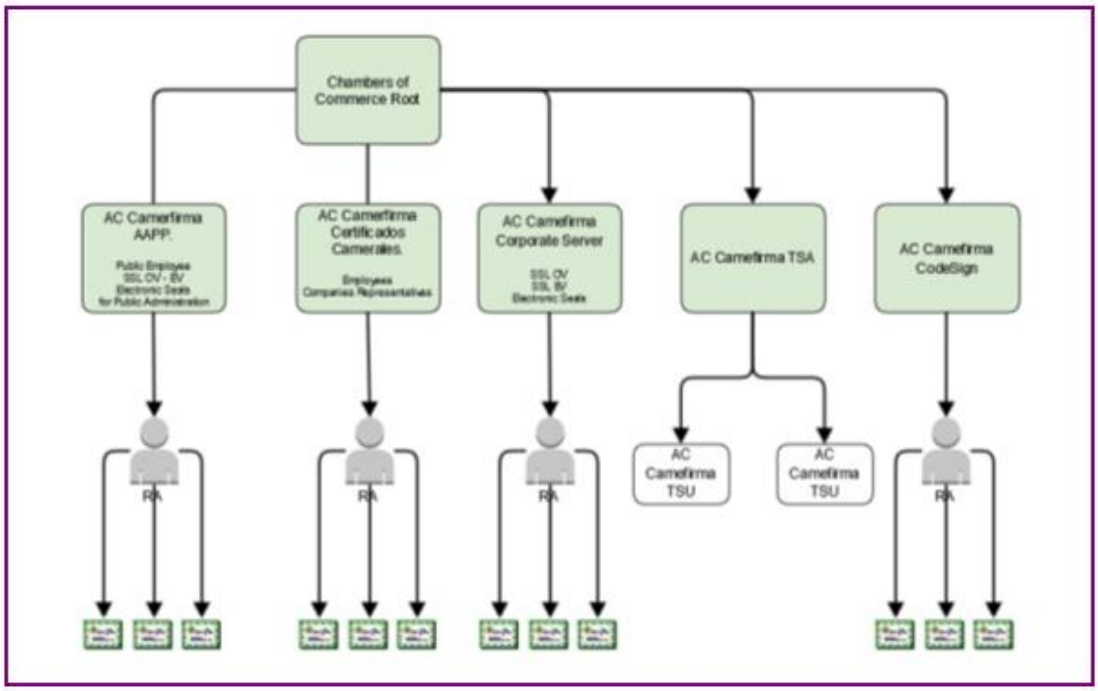
Este PSC emite una Autoridad de Certificación para ciudadanos vigente desde el 8 de febrero de 2006 y con una vigencia de aproximadamente 30 años, caducando el 16 de febrero de 2036. La CA presenta dos jerarquías para un mismo propósito pero con dos niveles de potencia de cifrado, SHA1 y SHA256. En cualquier caso la plataforma @firma5.5 no está preparada para soportar las dos jerarquías a la vez, debido a que se basa en el nombre del emisor para dar de alta las CAs, SubCAs y tipos de certificado y teniendo en cuenta que tanto la jerarquía SHA1 como la SHA256 usan los mismos nombre de emisor, bastará con dar de alta una de las dos para soportar ambas.



4.3. Cámara de Comercio (Camerfirma)

La Cámara de Comercio como PSC contempla varias Autoridades de Certificación con diferentes propósitos, pero la US solo contemplará la CA correspondiente a los Certificados Camerales (CC), qué son los encargados de emitir certificados de usuario y de representación. Aun así las CAs emitidas por Camerfirma son las siguientes:

- AC Camerfirma Certificados Camerales (CC de 2003 y 2008)
- AC Camerfirma Administración Pública
- AC Camerfirma Corporate Server
- AC Camerfirma CodeSign
- AC Camerfirma TSA

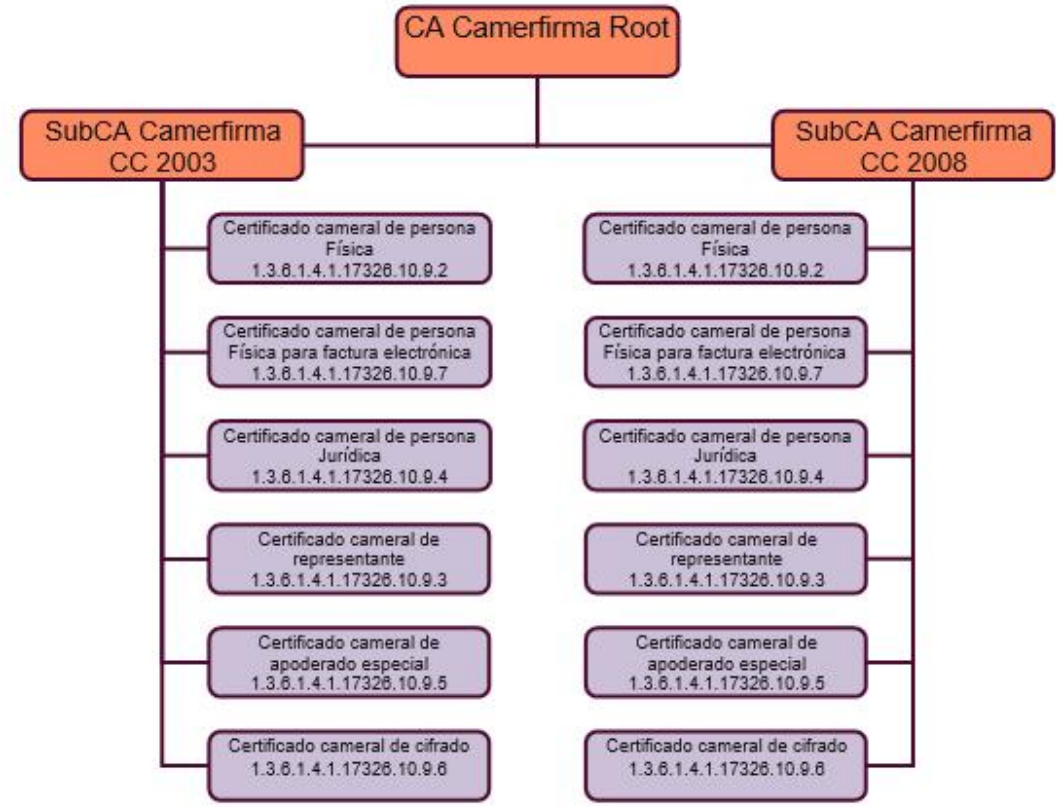


La particularidad principal de este PSC es que emite dos jerarquías de CAs diferentes para emitir los mismos tipos de certificado, la de 2003 y la de 2008. En concreto, el periodo de vigencia para la CA de certificados camerales se corresponde con los siguientes datos:

- Jerarquía de 2003: 34 años de vigencia.
  - Desde: 30 de septiembre de 2003
  - Hasta: 30 de septiembre de 2037
- Jerarquía de 2008: 30 años de vigencia aproximadamente.
  - Desde: 1 de agosto de 2008
  - Hasta: 30 de julio de 2038

A diferencia que los certificados del PSC eDNI, Camerfirma utiliza emisores diferenciados para las CAs de 2003 y 2008, permitiendo dar de alta las dos jerarquías en la plataforma @firma y de este modo soportar los certificados finales emitidos por cualquiera de ellas.

El árbol de emisión de certificados para los certificados camerales que se aplicarán en @firma de la US podemos verla en el siguiente jerarquía, correspondientes a las CAs de 2003 y 2008.



Este PSC emite además 4 subtipos de certificado para cada certificado final en la jerarquía, exceptuando el certificado cameral de cifrado, de forma que los identificadores de políticas especificados en la jerarquía anterior quedan extendidos como se muestra en los siguientes apartados.

4.3.1. Subtipos del certificado cameral de persona Física

Se corresponde con el identificador de política 1.3.6.1.4.1.17326.10.9.2, que se desglosa en los siguientes subtipos emitidos por la AC Camerfirma de Certificados Camerales.

- CAM-PF-SW-KPSC (1.3.6.1.4.1.17326.10.9.2.1.1): Claves almacenadas en software y generadas por el PSC.
- CAM-PF-SW-KUSU (1.3.6.1.4.1.17326.10.9.2.1.2): Claves almacenadas en software y generadas por el titular.

- CAM-PF-HW-KPSC (1.3.6.1.4.1.17326.10.9.2.2.1): Claves almacenadas en hardware y generadas por el PSC.
- CAM-PF-HW-KUSU (1.3.6.1.4.1.17326.10.9.2.2.2): Claves almacenadas en hardware y generadas por el titular.

4.3.2. Subtipos del certificado cameral de persona Física de pertenencia a empresa para emitir factura electrónica

Se corresponde con el identificador de política 1.3.6.1.4.1.17326.10.9.7, que se desglosa en los siguientes subtipos emitidos por la AC Camerfirma de Certificados Camerales.

- CAM-PFF-SW-KPSC (1.3.6.1.4.1.17326.10.9.7.1.1): Claves almacenadas en software y generadas por el PSC.
- CAM-PFF-SW-KUSU (1.3.6.1.4.1.17326.10.9.7.1.2): Claves almacenadas en software y generadas por el titular.
- CAM-PFF-HW-KPSC (1.3.6.1.4.1.17326.10.9.7.2.1): Claves almacenadas en hardware y generadas por el PSC.
- CAM-PFF-HW-KUSU (1.3.6.1.4.1.17326.10.9.7.2.2): Claves almacenadas en hardware y generadas por el titular.

4.3.3. Subtipos del certificado cameral de persona Jurídica

Se corresponde con el identificador de política 1.3.6.1.4.1.17326.10.9.4, que se desglosa en los siguientes subtipos emitidos por la SubCA Camerfirma de Certificados Camerales.

- CAM-PJ-SW-KPSC (1.3.6.1.4.1.17326.10.9.4.1.1): Claves almacenadas en software y generadas por el PSC.
- CAM-PJ-SW-KUSU (1.3.6.1.4.1.17326.10.9.4.1.2): Claves almacenadas en software y generadas por el titular.
- CAM-PJ-HW-KPSC (1.3.6.1.4.1.17326.10.9.4.2.1): Claves almacenadas en hardware y generadas por el PSC.
- CAM-PJ-HW-KUSU (1.3.6.1.4.1.17326.10.9.4.2.2): Claves almacenadas en hardware y generadas por el titular.

4.3.4. Subtipos del certificado cameral de representante

Se corresponde con el identificador de política 1.3.6.1.4.1.17326.10.9.3, que se desglosa en los siguientes subtipos emitidos por la SubCA Camerfirma de Certificados Camerales.

- CAM-PR-SW-KPSC (1.3.6.1.4.1.17326.10.9.3.1.1): Claves almacenadas en software y generadas por el PSC.
- CAM-PR-SW-KUSU (1.3.6.1.4.1.17326.10.9.3.1.2): Claves almacenadas en software y generadas por el titular.
- CAM-PR-HW-KPSC (1.3.6.1.4.1.17326.10.9.3.2.1): Claves almacenadas en hardware y generadas por el PSC.
- CAM-PR-HW-KUSU (1.3.6.1.4.1.17326.10.9.3.2.2): Claves almacenadas en hardware y generadas por el titular.

4.3.5. Subtipos del certificado cameral de apoderado especial

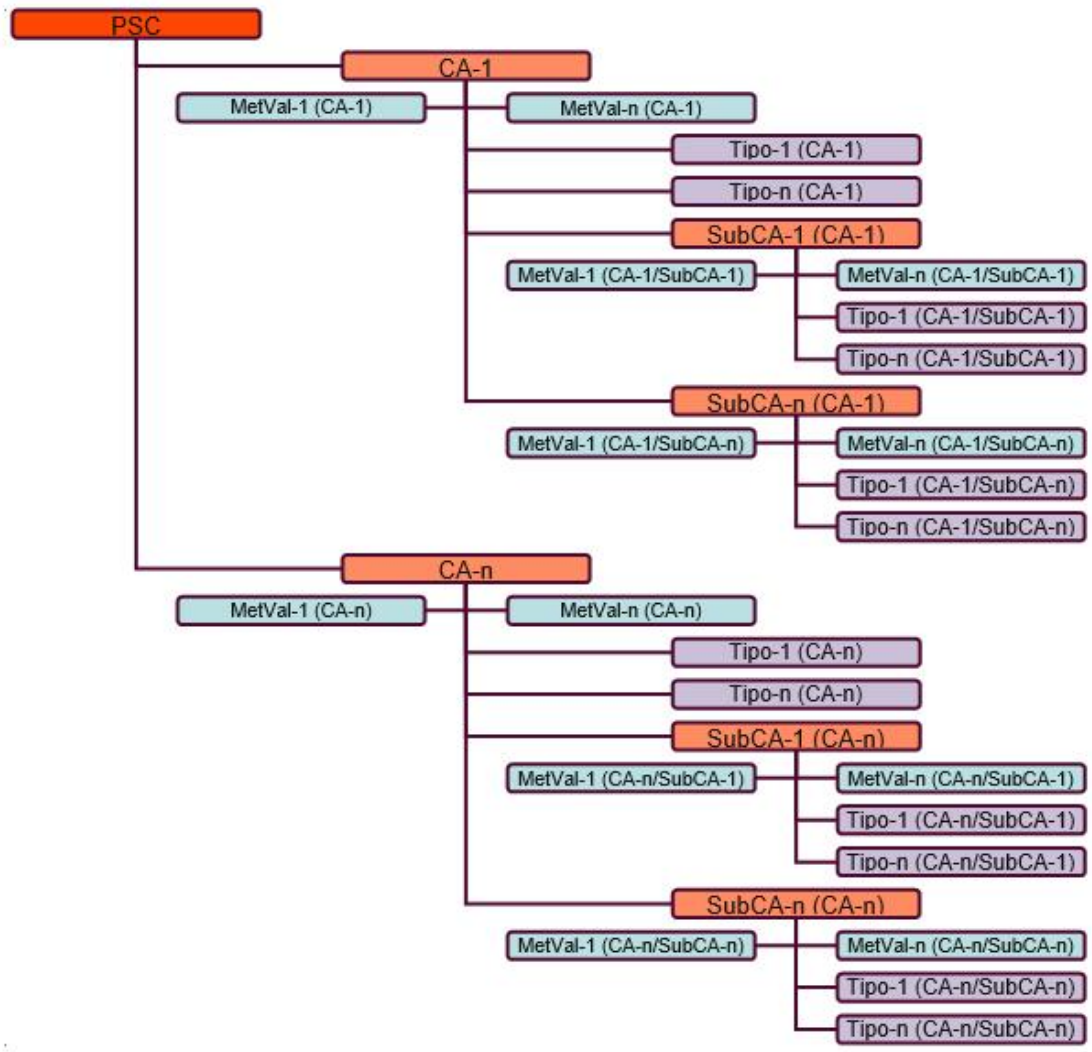
Se corresponde con el identificador de política 1.3.6.1.4.1.17326.10.9.5, que se desglosa en los siguientes subtipos emitidos por la SubCA Camerfirma de Certificados Camerales.

- CAM-AP-SW-KPSC (1.3.6.1.4.1.17326.10.9.5.1.1): Claves almacenadas en software y generadas por el PSC.
- CAM-AP-SW-KUSU (1.3.6.1.4.1.17326.10.9.5.1.2): Claves almacenadas en software y generadas por el titular.
- CAM-AP-HW-KPSC (1.3.6.1.4.1.17326.10.9.5.2.1): Claves almacenadas en hardware y generadas por el PSC.
- CAM-AP-HW-KUSU (1.3.6.1.4.1.17326.10.9.5.2.2): Claves almacenadas en hardware y generadas por el titular.

5. Métodos de validación

Una vez definidos los PSCs soportados por la plataforma @firma de la US, se procede a definir los métodos de validación necesarios para una correcta gestión de cada tipo de certificado.

Un método de validación podrá ser una CRL o un OCSP, pero en cualquier caso se aplican sobre cada CA y SubCA, de forma que validarán el estado de revocación de cada uno de los certificados emitidos por las mismas. Además, cada CA o SubCA podrá definir más de un método de validación, que serán configurados secuencialmente, de forma que si un método falla se pasará a usar el siguiente, tal y como se muestra en el siguiente diagrama.



Una vez conocemos la forma de configurar un método de validación procedemos a definir los métodos de validación de cada PSC.

5.1. Fábrica Nacional de Moneda y Timbre (FNMT)

Como ya vimos anteriormente este prestador emite dos CAs principales y cada una de ellas tendrá sus propios métodos de validación. La URL de acceso para todos los certificados de la FNMT y sus renovaciones es la siguiente:

https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

5.1.1. FNMT Clase 2 CA

Esta CA emite directamente los tipos de certificado y no emite ninguna SubCA, de forma que los posible métodos de validación serán configurados directamente sobre esta CA y servirán para validar todos los tipos de certificado emitidos por la misma.

5.1.1.1. Validación de certificados emitidos por FNMT Clase2 CA

Se configuran varios métodos de validación, dos mediante OCSP y otro secundario mediante la CRL de réplica de la Junta de Andalucía. La US dispone de un certificado de servicios avanzados de la FNMT para firmar las peticiones OCSP y obtener acceso al mismo, de forma que la lista de prioridades para los métodos de validación es la siguiente.

1. OCSP_FNMT_CLASE2_NEW
2. OCSP_FNMT_CLASE2
3. CRL_FNMT_CLASE2_JA

Validación mediante CRL: CRL_FNMT_CLASE2_JA

El acceso a la CRL para validar los certificados emitidos por la CA que nos atañe se realiza mediante el protocolo LDAP, publicado por la Junta de Andalucía a modo de réplica del LDAP de la FNMT. El acceso es público, pero su actualización se realiza cada 12h.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: LDAP Segmentado
- Usar DP del certificado: Si
- URL del servicio: crl.juntadeandalucia.es:1705
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_fnmt_clase2_ja
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_fnmt_clase2_ja
Validez: 10 años
Emisor: OU=FNMT Clase 2 CA,O=FNMT,C=ES
Asunto: OU=FNMT Clase 2 CA,O=FNMT,C=ES
URL: https://www.sede.fnmt.gob.es/documents/11614/116099/FNMTClase2CA.cer

Validación mediante OCSP: OCSP_FNMT_CLASE2_NEW

El acceso a este servicio OCSP para la validación de certificados emitidos por FNMT Clase2 CA se realiza mediante conexión segura, aceptando solo peticiones firmadas con certificados habilitados al respecto. De esta forma, antes de poder utilizar el servicio de OCSP mencionado será necesario solicitar el acceso y recibir la clave privada necesaria para firmar las peticiones.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocspc2.cert.fnmt.es/ocspc2/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: Si (seleccionar alias 'clienteocsp')
- RequestorName obligatorio: Si
- Identificador de aplicación: rfc2560

Antes de poder seleccionar la clave para firmar las peticiones será necesario incluir el PKCS#12 correspondiente en el KeystoreClienteOCSP. La US dispone del certificado necesario con la siguiente información.

Alias: clienteocsp
Validez: 3 años
Emisor: OU=AC Componentes Informáticos,O=FNMT-RCM,C=ES
Asunto: CN=AFIRMA.US.ES,SERIALNUMBER=Q4118001I,OU=SERVICIO DE INFORMATICA,O=UNIVERSIDAD DE SEVILLA,L=SEVILLA,C=ES

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_clase2_new

Validez: 4 años

Emisor: c=es,o=fnmt,ou=fnmt clase 2 ca

Asunto: cn=Servidor de OCSP - Fabrica Nacional de Moneda y Timbre Q2826004J,ou=Internos,ou=FNMT Clase 2 CA,o=FNMT,c=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_Clase2CA_Nuevo

Validación mediante OCSP: OCSP_FNMT_CLASE2

El acceso al servicio OCSP para la validación de certificados emitidos por FNMT Clase2 CA está securizado, aceptando solo peticiones firmadas con certificados habilitados al respecto. De esta forma, antes de poder utilizar el servicio de OCSP mencionado será necesario solicitar el acceso y recibir el certificado con la clave privada necesaria para firmar las peticiones.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://apus.cert.fnmt.es/appsUsuario/ocsp/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: Sí (seleccionar alias 'clienteocsp')
- RequestorName obligatorio: Si
- Identificador de aplicación: rfc2560

Antes de poder seleccionar la clave para firmar las peticiones será necesario incluir el PKCS#12 correspondiente en el KeystoreClienteOCSP. La US dispone del certificado necesario con la siguiente información.

Alias: clienteocsp

Validez: 3 años

Emisor: OU=AC Componentes Informáticos,O=FNMT-RCM,C=ES

Asunto: CN=AFIRMA.US.ES,SERIALNUMBER=Q4118001I,OU=SERVICIO DE INFORMATICA,O=UNIVERSIDAD DE SEVILLA,L=SEVILLA,C=ES

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_clase2

Validez: 3 años

Emisor: c=es,o=fnmt,ou=fnmt clase 2 ca

Asunto: cn=Servidor de OCSP - Fabrica Nacional de Moneda y Timbre Q2826004J,ou=Internos,ou=FNMT Clase 2 CA,o=FNMT,c=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_Clase2CA

5.1.2. AC FNMT RCM

Como hemos visto en el apartado de PSCs, esta CA emite varias SubCAs que a su vez emiten los tipos de certificados finales correspondientes para cada una de ellas. Al presentar una jerarquía de CA, SubCAs y tipos de certificado, se deberán configurar los posibles métodos de validación en cada CA y SubCA dada de alta.

5.1.2.1. Validación de las SubCAs emitidas por AC FNMT RCM

Para validar las SubCAs configuramos los dos métodos de validación que ofrece la FNMT. El primario será el método de validación público mediante OCSP y como secundario el método de validación mediante CRL. Con estos métodos de validación podremos conocer el estado de las SubCAs emitidas.

Los métodos de validación mediante CRL y OCSP publicados por la FNMT para este propósito son públicos, pero solo se aplican para la validación de las SubCAs y no para la validación de certificados finales.

- FNMT AC Administración Pública
- FNMT AC Usuarios
- FNMT AC Representación
- FNMT AC ISA (Comisión Europea)
- FNMT AC APE
- FNMT AC Componentes

Validación mediante CRL: CRL_FNMT_RCM

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_fnmt_rcm
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_fnmt_rcm

Validez: 22 años

Emisor: OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES

Asunto: OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Raiz_FNMT-RCM_SHA256.cer

Validación mediante OCSP: OCSP_FNMT_RCM

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_rcm

Validez: 6 meses

Emisor: OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES

Asunto: CN=SERVIDOR OCSP AC RAIZ FNMT-RCM,OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_ACRAIZ_FNMTRCM

5.1.2.2. Validación de los certificado emitidos por la SubCA FNMT AC Administración Pública

Se utilizan dos métodos de validación configurados sobre la SubCA FNMT AC Administración Pública, uno primario mediante OCSP y otro secundario mediante CRL.

Validación mediante CRL: CRL_FNMT_RCM_AP

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: Si
- URL del servicio: http://www.cert.fnmt.es/crlsacap/CRL1.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_fnmt_rcm_ap
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_fnmt_rcm_ap

Validez: 12 años

Emisor: OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES

Asunto: CN=AC Administración Pública,SERIALNUMBER=Q2826004J,OU=CERES,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Administracion_Publica_SHA256.cer

Validación mediante OCSP: OCSP_FNMT_RCM_AP

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocspap.cert.fnmt.es/ocspap/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_rcm_ap

Validez: 6 meses

Emisor: CN=AC Administración Pública,SERIALNUMBER=Q2826004J,OU=CERES,O=FNMT-RCM,C=ES

Asunto: CN=SERVIDOR OCSP AC Administración Pública,SERIALNUMBER=Q2826004J,OU=CERES,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_AP

5.1.2.3. Validación de los certificado emitidos por la SubCA FNMT AC Usuarios

El método de validación mediante CRL para los certificados emitidos por la SubCA FNMT AC Usuarios es privado y solo tienen acceso los organismos de Administración Pública, de forma

que la US solo utilizará el método de validación OCSP, habilitado para otros organismos y para el cual la US ya dispone de la clave de firma que permite acceder al servicio.

URL SubCA FNMT AC Usuarios:
https://www.sede.fnmt.gob.es/documents/11614/116099/AC_FNMT_Usuarios.cer

Validación mediante OCSP: OCSP_FNMT_RCM_USU

El acceso al servicio OCSP para la validación de certificados emitidos por FNMT AC Usuarios está securizado, aceptando solo peticiones firmadas con certificados habilitados al respecto. De esta forma, antes de poder utilizar el servicio de OCSP mencionado será necesario solicitar el acceso y recibir el certificado con la clave privada necesaria para firmar las peticiones.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocspusu.cert.fnmt.es/ocspusu/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: Si (seleccionar alias 'clienteocsp')
- RequestorName obligatorio: Si
- Identificador de aplicación: rfc2560

Antes de poder seleccionar la clave para firmar las peticiones será necesario incluir el PKCS#12 correspondiente en el KeystoreClienteOCSP. La US dispone del certificado necesario con la siguiente información.

Alias: clienteocsp

Validez: 3 años

Emisor: OU=AC Componentes Informáticos,O=FNMT-RCM,C=ES

Asunto: CN=AFIRMA.US.ES,SERIALNUMBER=Q4118001I,OU=SERVICIO DE INFORMATICA,O=UNIVERSIDAD DE SEVILLA,L=SEVILLA,C=ES

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_rcm_usu

Validez: 6 meses

Emisor: CN=AC FNMT Usuarios,OU=Ceres,O=FNMT-RCM,C=ES

Asunto: CN=Servidor OCSP AC FNMT Usuarios,OU=Ceres,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_AC_FNMT_Usuarios

5.1.2.4. Validación de los certificado emitidos por la SubCA FNMT AC Representación

Se utilizan dos métodos de validación configurados sobre la SubCA FNMT AC Representación, uno primario mediante OCSP y otro secundario mediante CRL.

Validación mediante CRL: CRL_FNMT_RCM_REP

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: Si
- URL del servicio: http://www.cert.fnmt.es/crlsrep/CRL1.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_fnmt_rcm_rep
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_fnmt_rcm_rep

Validez: 14 años y 6 meses

Emisor: OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES

Asunto: CN=AC Representación,OU=CERES,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Representacion.cer

Validación mediante OCSP: OCSP_FNMT_RCM_REP

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocsprep.cert.fnmt.es/ocsprep/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_rcm_rep

Validez: 6 meses

Emisor: CN=AC Representación,OU=CERES,O=FNMT-RCM,C=ES

Asunto: CN=Servidor OCSP AC FNMT Representación,SERIALNUMBER=Q2826004J,OU=Ceres,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_AC_Representacion

5.1.2.5. Validación de los certificado emitidos por la SubCA FNMT AC Componentes

Se utilizan dos métodos de validación configurados sobre la SubCA FNMT AC Componentes, uno primario mediante OCSP y otro secundario mediante CRL.

Validación mediante CRL: CRL_FNMT_RCM_COMP

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado

- Tipo de acceso: HTTP
- Usar DP del certificado: Si
- URL del servicio: http://www.cert.fnmt.es/crlscomp/CRL1.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_fnmt_rcm_comp
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_fnmt_rcm_comp
Validez: 15 años
Emisor: OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES
Asunto: CN=AC Componentes Informáticos,O=FNMT-RCM,C=ES
URL: https://www.sede.fnmt.gob.es/documents/11614/116099/AC_Componentes_Informaticos_SHA256.cer

Validación mediante OCSP: OCSP_FNMT_RCM_COMP

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocspcomp.cert.fnmt.es/ocsp/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_rcm_comp

Validez: 6 meses

Emisor: CN=AC Componentes Informáticos,OU=CERES,O=FNMT-RCM,C=ES

Asunto: CN=Servidor OCSP AC Componentes Informáticos,OU= AC Componentes Informáticos,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_AC_Componentes_Informaticos

5.1.2.6. Validación de los certificado emitidos por la SubCA FNMT AC APE

Se utilizan dos métodos de validación configurados sobre la SubCA FNMT AC APE, uno primario mediante OCSP y otro secundario mediante CRL.

Validación mediante CRL: CRL_FNMT_RCM_APE_OLD

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: Si
- URL del servicio: http://www.cert.fnmt.es/crlsape/CRL1.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_fnmt_rcm_ape_old
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_fnmt_rcm_ape_old

Validez: 15 años

Emisor: OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES

Asunto: CN=AC APE,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116099/AC_APE.cer

Validación mediante OCSP: OCSP_FNMT_RCM_APE_OLD

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocspape.cert.fnmt.es/ocspape/OcspResponder
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_fnmt_rcm_ape_old

Validez: 6 meses

Emisor: CN=AC APE,O=FNMT-RCM,C=ES

Asunto: CN=DESCRIPCION SERVIDOR OCSP APE - ENTIDAD FNMT-RCM - CIF Q2826004J,OU= AC APE,O=FNMT-RCM,C=ES

URL: https://www.sede.fnmt.gob.es/documents/11614/116107/OCSP_APE

5.2. Documento Nacional de Identidad electrónico (eDNI)

En este apartado se describen los métodos de validación utilizados para la correcta configuración del PSC eDNI. La URL de acceso para todos los certificados de eDNI y sus renovaciones es la siguiente:

http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_076

5.2.1. AC RAIZ

Como hemos visto en el apartado de PSCs, esta CA emite varias SubCAs que a su vez emiten los tipos de certificados finales correspondientes para cada una de ellas. Al presentar una jerarquía de CA, SubCAs y tipos de certificado, se deberán configurar los posibles métodos de validación en cada CA y SubCA dada de alta.

5.2.1.1. Validación de las SubCAs emitidas por AC RAIZ

Para validar las SubCAs configuramos un único método de validación mediante CRL directamente sobre la CA que nos incumbre, lo queos permitirá conocer el estado de las SubCAs emitidas.

El servicio de validación mediante CRL publicado por la DNIE para este propósito es público, pero solo se aplica para la validación de las SubCAs y no para la validación de certificados finales. Concretamente, se trata de un método de validación mediante CRL que comprueba el estado de las siguientes SubCAs.

- AC DNIE 001
  - URL SHA1: http://www.dnielectronico.es/ZIP/ACDNIE001-SHA1.zip
  - URL SHA2: http://www.dnielectronico.es/ZIP/ACDNIE001-SHA2.zip
- AC DNIE 002
  - URL SHA1: http://www.dnielectronico.es/ZIP/ACDNIE002-SHA1.zip
  - URL SHA2: http://www.dnielectronico.es/ZIP/ACDNIE002-SHA2.zip
- AC DNIE 003
  - URL SHA1: http://www.dnielectronico.es/ZIP/ACDNIE003-SHA1.zip
  - URL SHA2: http://www.dnielectronico.es/ZIP/ACDNIE003-SHA2.zip

Validación mediante CRL: CRL_DNIE_RAIZ

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP

- Usar DP del certificado: No
- URL del servicio: http://crls.dnie.es/crls/ARL.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_dnie_raiz
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL, que se corresponde con el certificado raíz de DNIE con algoritmo de *hash* SHA1, el utilizado para dar de alta la jerarquía de este PSC.

Alias: crl_dnie_raiz
Validez: 30 años
Emisor: CN=AC RAIZ DNIE,OU=DNIE,O=DIRECCION GENERAL DE LA POLICIA,C=ES
Asunto: CN=AC RAIZ DNIE,OU=DNIE,O=DIRECCION GENERAL DE LA POLICIA,C=ES
URL SHA1: http://www.dnielectronico.es/ZIP/ACRAIZ-SHA1.CAB
URL SHA2: http://www.dnielectronico.es/ZIP/ACRAIZ-SHA2.CAB

5.2.1.2. Validación de los certificados emitidos por la SubCA AC DNIE 001, 002 y 003

La Dirección General de la Policía ofrece un servicio OCSP público común para las 3 SubCAs disponibles en este PSC, por tanto, se define un método de validación mediante OCSP que será utilizado por las 3 SubCAs de la misma forma. No se configurará ningún método de validación mediante CRL, debido a que este servicio es de acceso restringido.

Validación mediante OCSP: OCSP_EDNI2

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Usar Distribution Point(DP): Sí
- Tipo de acceso: HTTP

- Usar DP del certificado: No
- URL del servicio: http://ocsp.dnie.es
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir los certificados correspondientes en el AlmacenConfianzaOCSP.

La información de los certificados incluidos en el AlmacenConfianzaOCSP es la siguiente.

Alias: c=es,cn=av dnie fnmt,o=direccion general de la policia,ou=dnie,ou=fnmt - sha2 - 30/06/17

Validez: 6 meses

Emisor: CN=AC DNIE 001,OU=DNIE,O=DIRECCION GENERAL DE LA POLICIA,C=ES

Asunto: CN=AV DNIE FNMT,OU=FNMT,OU=DNIE,O=DIRECCION GENERAL DE LA POLICIA,C=ES

URL: https://www.dnielectronico.es/descargas/certificados/Ocsp%20Responder%20AV%20DNIE-FNMT_SHA2.rar

5.3. Cámara de Comercio (Camerfirma)

En este apartado se describen los métodos de validación utilizados para la correcta configuración del PSC Camerfirma. La URL de acceso para todos los certificados de Camerfirma y sus renovaciones es la siguiente:

http://www.camerfirma.com/area-de-usuario/jerarquia-politicas-y-practicas-de-certificacion/

5.3.1. CA Camerfirma root 2003 y 2008

Como hemos visto en el apartado de PSCs, Camerfirma emite dos CAs con el mismo propósito, una desde 2003 y otra desde 2008, las cuales a su vez emiten varias SubCAs que emiten los tipos de certificados finales correspondientes para cada una de ellas. La US solo dará soporte a las SubCAs de Certificados Camerales correspondientes a 2003 y 2008 y por tanto solo será necesario definir los métodos de validación de las CAs y las SubCAs mencionadas.

5.3.1.1. Validación de SubCAs emitidas por CA Camerfirma root (2003)

Para validar las SubCAs de 2003 configuramos un único método de validación mediante CRL directamente sobre la CA que nos atañe y que nos permitirá conocer el estado de las SubCAs emitidas en 2003. Camerfirma no proporciona ningún mecanismo de validación mediante OCSP para comprobar el estado de las SubCAs emitidas en 2003, el único servicio habilitado es mediante CRL.

- AC Camerfirma Certificados Camerales (CC de 2003)
- AC Camerfirma Administración Pública
- AC Camerfirma Corporate Server
- AC Camerfirma CodeSign
- AC Camerfirma TSA

Validación mediante CRL: CRL_CAMERFIRMA_ROOT_2003

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://crl.chambersign.org/chambersroot.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_camerfirma_root_2003
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_camerfirma_root_2003
Validez: 34 años

Emisor: CN=Chambers of Commerce Root,OU=http://www.chambersign.org,O=AC Camerfirma SA CIF A82743287,C=EU

Asunto: CN=Chambers of Commerce Root,OU=http://www.chambersign.org,O=AC Camerfirma SA CIF A82743287,C=EU

URL: http://docs.camerfirma.com/publico/DocumentosWeb/ocsp/ROOT_CHAMBERS_OF_COMMERCE.crt

5.3.1.2. Validación de SubCAs emitidas por CA Camerfirma root (2008)

Para validar las SubCAs emitidas en 2008, Camerfirma ofrece un servicio de CRL y una réplica de la misma, de forma que configuramos los métodos de validación mediante CRL directamente sobre la CA que nos atañe. Además, Camerfirma proporciona soporte de validación OCSP para las SubCAs emitidas en 2008, de forma que será configurado como método de validación primario.

- AC Camerfirma Certificados Camerales (CC de 2008)
- AC Camerfirma Administración Pública
- AC Camerfirma Corporate Server
- AC Camerfirma CodeSign
- AC Camerfirma TSA

Validación mediante CRL: CRL_CAMERFIRMA_ROOT_2008

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://crl.camerfirma.com/chambersroot-2008.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_camerfirma_root_2008
- Tipo de autenticación: Sin autenticación

- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_camerfirma_root_2008

Validez: 30 años

Emisor: CN=Chambers of Commerce Root – 2008,O=AC Camerfirma S.A.,SERIALNUMBER=A82743287,L=Madrid (see current address at www.camerfirma.com/address),C=EU

Asunto: CN=Chambers of Commerce Root – 2008,O=AC Camerfirma S.A.,SERIALNUMBER=A82743287,L=Madrid (see current address at www.camerfirma.com/address),C=EU

URL: http://docs.camerfirma.com/publico/DocumentosWeb/ocsp/ROOT_CHAMBERS_OF_COMMERCE_2008.crt

Validación mediante CRL: CRL_CAMERFIRMA_ROOT_2008_REPL

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://crl1.camerfirma.com/chambersroot-2008.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_camerfirma_root_2008
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Validación mediante OCSP: OCSP_CAMERFIRMA_ROOT_2008

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado

- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocsp.camerfirma.com
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_camerfirma_root_2008

Validez: 3 años

Emisor: CN=Chambers of Commerce Root – 2008,O=AC Camerfirma S.A.,SERIALNUMBER=A82743287,L=Madrid (see current address at www.camerfirma.com/address),C=EU

Asunto: Description=Chambers of Commerce OCSP,SERIALNUMBER=A82743287,O=AC Camerfirma SA,E=info@camerfirma.com,CN=OCSP Responder Chambers of Commerce Root – 2008,C=ES

URL: http://docs.camerfirma.com/publico/DocumentosWeb/ocsp/OCSP_RESPONDER_CHAMBERS_OF_COMMERCE_ROOT-2008_20140313_20170313.crt

5.3.1.3. Validación de certificados emitidos por la SubCA Camerfirma CC (2003)

Los métodos de validación mediante CRL y OCSP para los certificados emitidos por la SubCA Camerfirma CC (2003) son públicos, de forma que configuramos el acceso mediante OCSP como primario y el acceso mediante CRL como secundario.

Validación mediante CRL: CRL_CAMERFIRMA_CC_2003

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP

- Usar DP del certificado: Si
- URL del servicio: http://crl.camerfirma.com/ac_camerfirma_cc.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_camerfirma_cc_2003
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_camerfirma_cc_2003

Validez: 30 años

Emisor: CN=Chambers of Commerce Root,OU=http://www.chambersign.org,O=AC Camerfirma SA CIF A82743287,C=EU

Asunto: CN=AC Camerfirma Certificados Camerales,O=AC Camerfirma SA,SERIALNUMBER=A82743287,L=Madrid (see current address at www.camerfirma.com/address),E=ac_camerfirma_cc@camerfirma.com,C=ES

URL: http://docs.camerfirma.com/publico/DocumentosWeb/ocsp/AC_CAMERFIRMA_CC.crt

Validación mediante CRL: CRL_CAMERFIRMA_CC_2003_REPL

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: Si
- URL del servicio: http://crl1.camerfirma.com/ac_camerfirma_cc.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_camerfirma_cc_2003
- Tipo de autenticación: Sin autenticación

- Almacenar CRL: No

Validación mediante OCSP: OCSP_CAMERFIRMA_CC_2003

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocsp.camerfirma.com
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_camerfirma_cc_2003

Validez: 4 años

Emisor: CN=AC Camerfirma Certificados Camerales,O=AC Camerfirma SA,SERIALNUMBER=A82743287,L=Madrid (see current address at www.camerfirma.com/address),E=ac_camerfirma_cc@camerfirma.com,C=ES

Asunto: Description=Chambers of Commerce OCSP Responder 2012,O=AC Camerfirma SA,CN=OCSP Responder AC Camerfirma,C=ES

URL: http://docs.camerfirma.com/publico/DocumentosWeb/ocsp/OCSP_RESPONDER_AC_CAMERFIRMA_CC_20121026_20161025.crt

5.3.1.4. Validación de certificados emitidos por la SubCA Camerfirma CC (2008)

Los métodos de validación mediante CRL y OCSP para los certificados emitidos por la SubCA Camerfirma CC (2008) son públicos, de forma que configuramos el acceso mediante OCSP como primario y el acceso mediante CRL como secundario.

Validación mediante CRL: CRL_CAMERFIRMA_CC_2008

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: Si
- URL del servicio: http://crl.camerfirma.com/camerfirma_cc-2009.crl
- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_camerfirma_cc_2008
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Antes de poder seleccionar el emisor será necesario incluir el certificado correspondiente en el AlmacenConfianzaCRL.

Alias: crl_camerfirma_cc_2008

Validez: 10 años

Emisor: CN=Chambers of Commerce Root – 2008,O=AC Camerfirma S.A.,SERIALNUMBER=A82743287,L=Madrid (see current address at www.camerfirma.com/address),C=EU

Asunto: CN=Camerfirma Certificados Camerales – 2009,L=Madrid (see current address at https://www.camerfirma.com/address),SERIALNUMBER=A82743287,O=AC Camerfirma S.A.,C=ES

URL: http://docs.camerfirma.com/publico/DocumentosWeb/ocsp/AC_CAMERFIRMA_CC-2009.crt

Validación mediante CRL: CRL_CAMERFIRMA_CC_2008_REPL

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: CRL
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: Si
- URL del servicio: http://crl1.camerfirma.com/camerfirma_cc-2009.crl

- Validar la CRL obtenida: Si
- Usar DeltaCRL: No
- Emisor de la CRL: crl_camerfirma_cc_2008
- Tipo de autenticación: Sin autenticación
- Almacenar CRL: No

Validación mediante OCSP: OCSP_CAMERFIRMA_CC_2008

El alta del método de validación se establece con los siguientes atributos.

- Tipo de método: OCSP
- Estado: Habilitado
- Tipo de acceso: HTTP
- Usar DP del certificado: No
- URL del servicio: http://ocsp.camerfirma.com
- Algoritmo de firma: sha1WithRSAEncryption
- Firma peticiones: No
- RequestorName obligatorio: No

Por último y para confiar en la respuesta del OCSP será necesario incluir el certificado correspondiente en el AlmacenConfianzaOCSP.

Alias: ocsp_camerfirma_cc_2008

Validez: 3 años

Emisor: CN=Camerfirma Certificados Camerales – 2009,L=Madrid (see current address at https://www.camerfirma.com/address),SERIALNUMBER=A82743287,O=AC Camerfirma S.A.,C=ES

Asunto: SERIALNUMBER=A82743287,E=info@camerfirma.com,CN=OCSP Responder - Camerfirma Certificados Camerales – 2009,O=AC Camerfirma SA,C=ES

URL: http://docs.camerfirma.com/publico/DocumentosWeb/ocsp/OCSP_RESPONDER_AC_CAMERFIRMA_CC-2009_20140313_20170313.crt

Apéndice: Lenguaje de género

Esta política ha sido redactada con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.