PLATAFORMA DE CERTIFICACIÓN Y FIRMA ELECTRÓNICA DEL MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES

Miguel Gendive Rivas
Subdirector General Adjunto
Subdirección General de Proceso de Datos
Ministerio de Trabajo y Asuntos Sociales

Félix Aragonés Arribas
Técnico de Sistemas
Subdirección General de Proceso de Datos
Ministerio de Trabajo y Asuntos Sociales

Palabras clave

Certificado, X509, Firma electrónica; Autenticación; LAECSP; e-Administración, OCSP, CRL, Time Stamp.

Resumen de la Comunicación

La Subdirección General de Proceso de Datos del MTAS ha puesto en marcha la Plataforma de Certificación y Firma Electrónica del Ministerio de Trabajo y Asuntos Sociales para hacer frente a los crecientes demandas de aplicaciones de Administración Electrónica.

Dentro de la plataforma de certificación se contempla la emisión de certificados de diversos tipos, para cubrir todos los aspectos especificados en LEY 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos: De autenticación y firma para los empleados del Ministerio, de autenticación de servidores, de sello o procedimiento automatizado y de firma de código.

En cuanto a la plataforma de Firma, permite ofrecer servicios de forma centralizada a todas las aplicaciones del Ministerio que necesiten funciones como información del estado de revocación de certificados, firma de documentos, tanto de servidor como de cliente, servicios de Time Stamping.

Ambas plataformas estarán replicadas en Centro de Respaldo del Ministerio, actualmente en fase de diseño, para ofrecer total garantía de continuidad ed estas funciones en caso de desastre.

Plataforma de Certificación y Firma electrónica del Ministerio de Trabajo y Asuntos Sociales.

Introducción

El creciente uso de las técnicas de firma electrónica en las aplicaciones informáticas del Ministerio, así como la necesidad de dotar a los empleados del mismo de los instrumentos de autenticación y firma necesarios para utilizarlas, condujo a la decisión de tener una plataforma propia del Ministerio que permitiera ofrecer los servicios necesarios.

Por una parte, la emisión de certificados a todos los empleados del Ministerio, así como los certificados necesarios para servidores, aplicaciones, etc. pudiendo incorporar los campos necesarios sin las rigideces que impondría usar los certificados emitidos por Autoridades de Certificación externas.

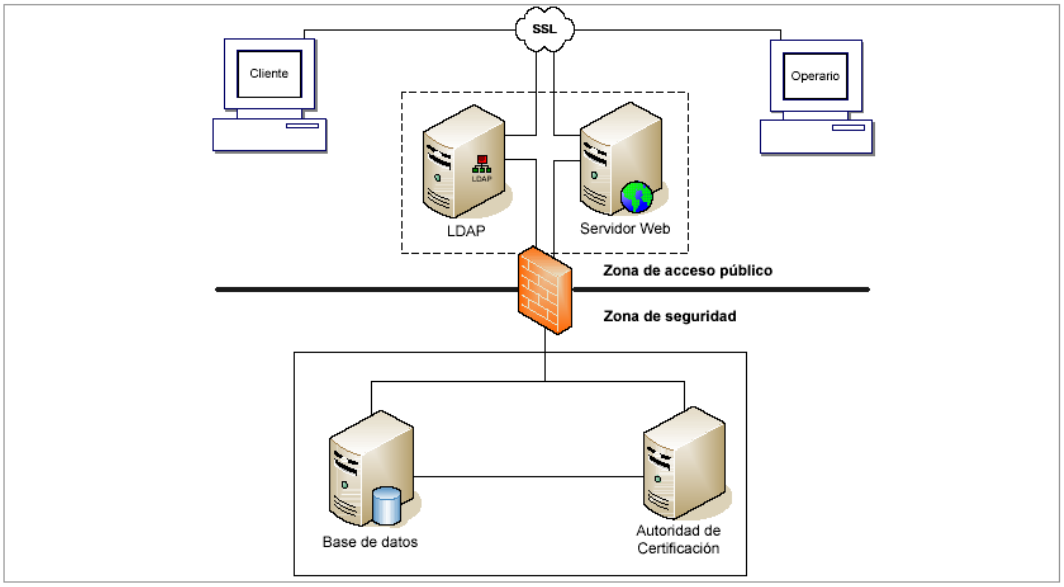
El acierto de esta decisión se ha confirmado con la reciente publicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que define una serie de certificados, algunos de ellos no contemplados hasta ahora, y que el Ministerio de Trabajo y Asuntos Sociales puede poner en marcha de forma inmediata al tener su propia Autoridad de Certificación, lo que le permite definir nuevas políticas de certificación para cubrir estos tipos de certificados.

Por otra parte, la plataforma de firma electrónica permite centralizar los servicios de validación de firmas electrónicas, estado de revocación de certificados, etc. para todas las aplicaciones que lo necesiten, sin necesidad de escribir el código correspondiente en cada aplicación. Así, por ejemplo, si se produce el reconocimiento de una nueva Autoridad de Certificación para poder usar los certificados de la misma frente a las aplicaciones del Ministerio, únicamente hace falta darla de alta en la plataforma, sin necesidad de modificar el código de las aplicaciones que la utilizan.

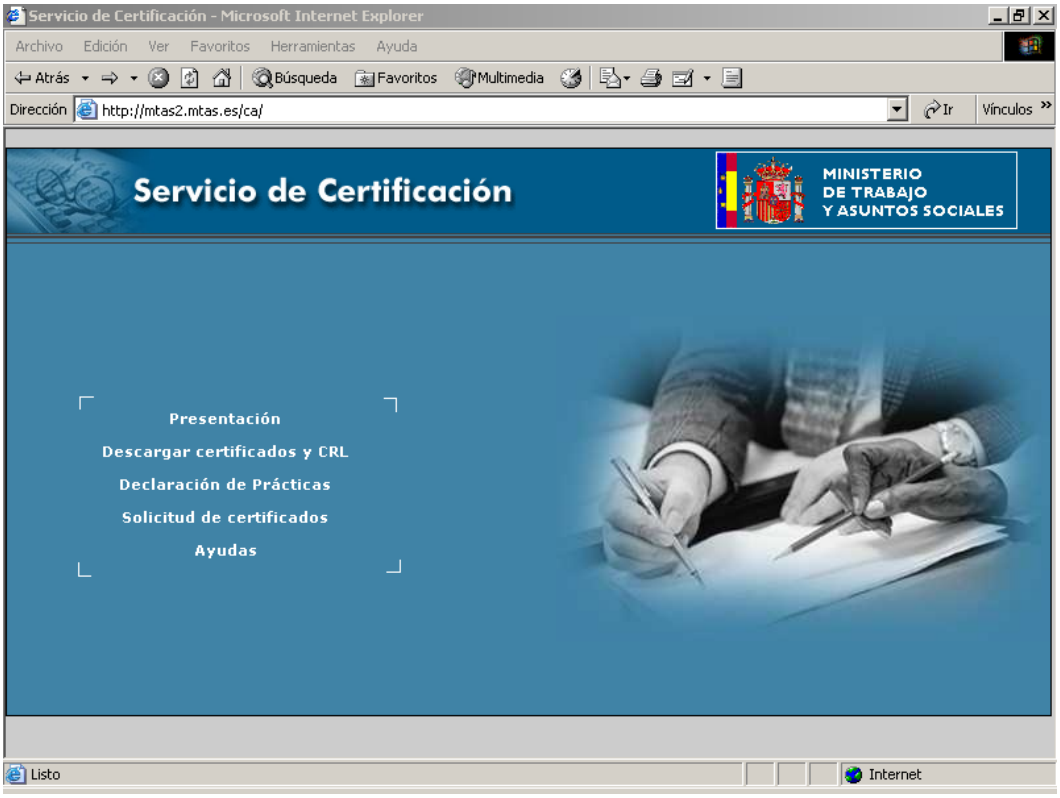
Plataforma de Certificación

La Autoridad de Certificación (en adelante AC) del MTAS permite la gestión completa del ciclo de vida de los certificados digitales. Está basada en el Servicio de Certificación de Microsoft Windows 2000/2003 Server, y se puede considerar como un módulo de extensión del producto Microsoft Certificate Server (MCS) incorporado en el Sistema Operativo. Permite la administración de una AC de forma tanto local como remota y ofrece una aplicación Web desde la que se pueden emitir certificados de clave pública X509.

La configuración básica de la plataforma es la que se observa en la figura:



- **El Servidor Web** permite el acceso, tanto de clientes para la solicitud de certificados, para aquellas políticas de certificación que lo permitan, como a los operadores para administrar políticas, validar las solicitudes de certificados, etc. También se encuentran en el servidor web la Declaración de Prácticas de Certificación de la AC del MTAS y las Políticas de Certificación de la CA para los diferentes tipos de certificados emitidos. Por último, contiene la última versión de la lista de revocación de certificados (CRL) de la AC.
- **La de base de datos** contiene información sobre las AC, políticas de certificación, y LDAPs, además de datos de solicitudes (fecha de la misma, datos enviados, estado en que se encuentran), certificados emitidos y revocados (con la causa y la fecha de la revocación).
- **El LDAP** almacena los certificados de forma jerárquica, según los datos que contienen. Es accesible desde el exterior por lo que permite la obtención de cualquier certificado para verificar una firma.



Los beneficios derivados de utilizar una AC propietaria son los siguientes:

- Permite disponer de una infraestructura PKI para emitir y gestionar nuestros propios certificados a bajo coste.
- Emisión y gestión de certificados personalizados y adaptados a las necesidades concretas del usuario y/o de las aplicaciones.
- Definición de distintas políticas para distintos departamentos.
- Cumplimiento de estándares.
- AC totalmente configurable.
- Uso de distintos tipos de soporte criptográfico: navegador, tarjeta criptográfica, llave USB,…
- Permite emitir certificados para poder utilizarlos en: autenticación en la red de la organización (en vez de usuario y contraseña), autenticación VPN, firma de correo electrónico, autenticación en Intranet y firma electrónica para aplicaciones Intranet, Extranet e Internet.
- Fácil implementación de modificaciones y extensiones.

Tipos de certificados emitidos

Aparte de certificados específicos para determinadas aplicaciones, la CA del MTAS, emite los siguientes tipos de certificados, todos ellos conformes a la norma X.509 V3, y cuyos detalles están especificados en las correspondientes Políticas de Certificación:

CERTIFICADOS	URL
CERTIFICADO PERSONAL DE AUTENTICACIÓN	http://mtas2.mtas.es/ca/dcp/pcmtasa.pdf
CERTIFICADO PERSONAL DE FIRMA ELECTRÓNICA	http://mtas2.mtas.es/ca/dcp/pcmtasfe.pdf
CERTIFICADO DE AUTENTICACIÓN DE SERVIDOR SEGURO	http://mtas2.mtas.es/ca/dcp/pcmtasas.pdf
CERTIFICADO DE AUTENTICACIÓN DE SERVIDOR PKCS10	http://mtas2.mtas.es/ca/dcp/pcmtasas10.pdf
CERTIFICADO DE SELLO DE ADMINISTRACIÓN ELECTRÓNICA	http://mtas2.mtas.es/ca/dcp/pcmtassae.pdf
CERTIFICADO DE FIRMA SOFTWARE	http://mtas2.mtas.es/ca/dcp/pcmtasfs.pdf

- **Certificados Personales**: Se ha elegido la opción de separar en dos certificados distintos las funciones de autenticación y firma, según las recomendaciones de los estándares y siguiendo el modelo del DNI electrónico. Estos certificados vienen a responder a los descritos en el artículo 19.2 de la LAECSP como certificados de empleados públicos: "*Cada Administración Pública podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios*". Además de los usos básicos de autenticación y firma, estos certificados permiten a sus poseedores otros usos como la firma de correo electrónico, inicio de sesión en el PC, etc.
- **Certificados de Autenticación de Servidor Seguro**: Estos dos tipos de certificados permiten al usuario que accede a un sitio del MTAS que tenga este certificado instalado, tener la seguridad de que accede realmente a ese sitio y que todas las comunicaciones estarán cifradas. Responden a la definición de certificados de Sede

Electrónica introducida en la LAECSP en el artículo 17: "*Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente*".

- **Certificados de sello de Administración Electrónica**: Son certificados destinados a su instalación y uso en aplicaciones que realicen firmas electrónicas sin la intervención de una persona física. Responden a lo descrito en el artículo 18.1.a relativo a Sistemas de firma electrónica para la actuación administrativa automatizada: "*Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica*".
- **Certificados de firma de software**: Destinados a asegurar a un usuario que el software que se descarga (módulos ejecutables, applets, etc) procede realmente del MTAS.

Los certificados personales de autenticación y firma los obtiene el propio usuario, mediante la tarjeta inteligente de la que se le hace entrega, garantizando de esta forma que nadie más que el propio usuario ha tenido en ningún momento la posibilidad de copiar las claves privadas.

Esta tarjeta está homologada por el Centro Criptológico Nacional con el nivel EAL4+, lo que la define como dispositivo seguro de creación de firma y permite la generación de firma electrónica reconocida, la única que tiene la misma validez jurídica que la firma manuscrita.

Plataforma de Firma

La plataforma de firma ASF (Advanced Signatura Framework) es una solución completa para la integración de la firma electrónica avanzada en una infraestructura informática de una entidad u organización, o para prestar servicios de validación y firma a terceros.

Permite la convivencia con más de una AC, independizando al resto de los sistemas de esta complejidad añadida. Contempla el ciclo de vida completo de utilización de certificados: creación de documentos firmados y/o cifrados, validación y control de éstos, validación de la vigencia de certificados, registro de la información de firma de cara al no repudio y establecimiento de políticas de firma.

Sus principales características son las siguientes:

- Múltiples estándares de firma y cifrado.
- Uso de certificados de diferentes AC.
- Validación contra múltiples AC.
- Múltiples métodos de validación. Gestión de prioridades.
- Soporte de nuevos métodos de validación.
- Definición de múltiples políticas de confianza y firma mediante un sencillo interfaz Web.
- Integración con hardware criptográfico (HSM).
- Consola de administración Web.
- Consola de consulta de operaciones firmadas.
- Soporte de dispositivos criptográficos estándares en cliente.

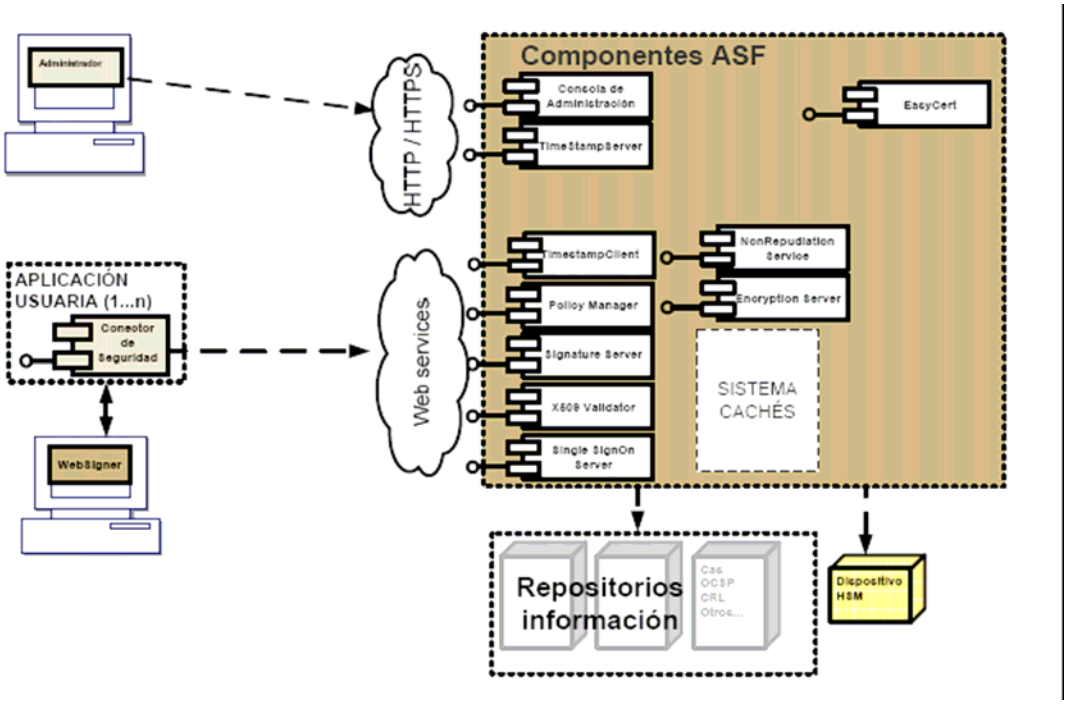
Con ASF se consigue disponer de una infraestructura común para todas las aplicaciones en las que se deseen integrar las funcionalidades de firma digital electrónica avanzada, consiguiendo unificación en los estándares utilizados en las distintas aplicaciones.

Se evitan costes adicionales en el desarrollo de las funcionalidades propias de la firma digital, tanto en las aplicaciones actuales como en las futuras, evitando la necesidad de formar a los desarrolladores en tecnología de firma a bajo nivel.

Así se consigue independizar a las aplicaciones de la incorporación de nuevas tecnologías y protocolos relacionados con la firma electrónica y aísla a las aplicaciones de las diferencias entre las distintas AC autorizadas así como entre los distintos certificados digitales que éstas emiten.

Módulos y funcionalidades

La plataforma la constituyen un conjunto de módulos que implementan de manera sencilla todos los requisitos de uso de firma electrónica avanzada multi-CA, estos módulos pueden trabajar de forma independiente según las necesidades de integración. Los módulos de la plataforma ofrecen sus servicios a través de diferentes interfaces (WebServices –SOAP/XML- o interfaces locales Java –si están dentro de la misma aplicación en el mismo servidor de aplicaciones-). Los módulos pueden distribuirse en distintos servidores comunicándose entre sí a través de protocolos seguros SSL v3.0.



La plataforma consta de los siguientes módulos:

- **X.509-Single SignOn**: Autenticación de usuarios mediante certificados digitales X.509.
- **SignatureServer**: Validación/generación de firmas (parte servidora) en múltiples formatos (PKCS#7, XMLDSig, CMS y S/MIME). Distribución de tareas sobre el resto de módulos para la obtención de información sobre los firmantes, la validez de los certificados, almacenar la operación firmada, etc.
- **X509Validator**: Validación de certificados (validez temporal y autenticidad). Validación del estado de revocación del certificado (a través de CRL, consulta HTTPS o LDAP, consulta OCSP (– Online Certificate Status Protocol), o a BD). Caché de respuestas CRL y OCSP.

- **PolicyManager**: Sistema central para el control de los usos de los certificados en las distintas aplicaciones. Obtención de información del firmante a partir del certificado. Encapsula las diferencias entre las distintas CAsACs. Actúa como punto único de administración y de definición de políticas de confianza y firma.
- **Consola de Administración**: Encargada de administrar y configurar toda la plataforma.
- **NonRepudiationService**: Registro de la información de firma para evitar el repudio. Consulta por el cliente de las operaciones almacenadas firmadas por él. Emisión de informes con la información relativa a la firma y verificación del documento.
- **EncryptionServer**: Cifrado de documentos. Gestión de certificados de cifrado y cifrado múltiple. Búsquedas de certificados en repositorios LDAP remotos. Descifrado a partir de certificados en almacén de ASF.
- **WebSigner**: Generación y verificación de documentos con firma electrónica avanzada, cifrado y descifrado, todo ello desde navegadores Web (parte cliente). Uso de firma única o múltiple mancomunada. Filtrado de certificados autorizados para el proceso.
- **DesktopSigner**: Software local para estaciones de trabajo que permite funciones de firma, validación, cifrado y descifrado de documentos almacenados en ficheros digitales. Tiene la misma funcionalidad que el módulo WebSigner pero disponiendo de interfaz propio, por lo que no necesita navegador.
- **TimeStampServer**: Introduce sellos de tiempo digitales según el RFC3161.
- **TimestampClient**: Módulo que ofrece servicios para obtener sellos de tiempo de cualquier Autoridad de Sellado de Tiempos (TSA) que cumpla el RFC3161 sin necesidad de conocer dicho estándar.

En el manejo de todos estos módulos existen una serie de almacenes de certificados, que pueden albergarse en BD o dispositivos HSM:

- Almacén de Confianza (almacena raíces de confianza, certificados de servidores SSL y de servidores OCSP).
- Almacén de Firma (certificados utilizados por SignatureServer).
- Almacén de Cifrado (certificados utilizados por EncryptionServer).
- Almacén de Peticiones (certificados utilizados para firmar peticiones OCSP, TSA, etc.)
- Almacén de Descifrado (almacena certificados utilizados por EncryptionServer para descifrar).

Validación de Certificados X.509 en el entorno del MTAS

El Ministerio de Trabajo y Asuntos Sociales cuenta con un despliegue de ASF que fundamentalmente se utiliza para la validación de certificados por parte de los servidores de aplicaciones de cara a garantizar el acceso seguro a las mismas y verificar la validez de las firmas electrónicas generadas. ASF se encuentra desplegado sobre un cluster balanceado de servidores Tomcat, configuración que proporciona alta disponibilidad y un mejor rendimiento.

A pesar de que el uso primario actual de ASF se orienta a la validación de certificados, se encuentran en fase de desarrollo diversas aplicaciones que hacen uso de los módulos de firma y está en estudio la activación del almacén de información de no repudio.

Los métodos de comprobación de la revocación de certificados definen la forma por la cual un usuario o aplicación puede obtener información relativa al estado de un determinado certificado digital. Éstas se pueden dividir en dos grandes grupos: las basadas en distribución de listas u Off-line y las que lo están en línea.

La primera opción se caracteriza por el envío de una lista de certificados revocados o CRL al usuario, mediante la cual debe de verificar el estado del certificado. Generalmente los usuarios guardan la lista en su memoria caché y no es necesario realizar transacciones en línea cuando se necesita verificar el estado de un cierto certificado. No obstante, este método no garantiza al 100% que los datos de revocación estén actualizados y es técnicamente complejo el almacenamiento de justificantes de comprobación de la validez de los certificados para posteriores auditorías.

Se trata de un modo especial la CRL correspondiente a certificados Clase 2 CA emitidos por la FNMT por el volumen de certificados de este tipo validados a diario y por la particularidad de que la CRL de la FNMT se encuentra segmentada, es decir, no es única. En este caso, se mantiene en MTAS una réplica del LDAP que aloja las CRLs de la FNMT que se actualiza periódicamente mediante modificaciones incrementales proporcionadas por la FNMT en el momento de su generación.

La segunda opción consiste en el envío de información sobre la validez de un determinado certificado o certificados que el usuario solicita en un instante concreto.

El protocolo de estado de certificados en línea (OCSP- Online Certificate Status Protocol) ha sido propuesto por el grupo PKIX del IETF, y proporciona el estado de uno o varios certificados a través de un servidor de confianza denominado OCSP Responder. OCSP se basa en mecanismos de solicitud/respuesta codificados en ASN.1 que pueden encapsularse en múltiples

protocolos de comunicaciones, aunque el más utilizado es HTTP. Un Responder OCSP puede devolver una respuesta firmada, lo cual significaría que el certificado indicado en la petición es "bueno"(good), "revocado"(revoked) o "desconocido"(unknown). También puede devolver un código de error, en cuyo caso la respuesta no tendría que estar firmada.

Todas éstas características resultan en una serie de ventajas que el protocolo OCSP muestra frente a las CRLs:

- OCSP puede proporcionar una información más adecuada y reciente del estado de revocación de un certificado.

- OCSP elimina la necesidad de que los clientes tengan que obtener y procesar las CRLs, ahorrando de este modo tráfico de red y procesado por parte del cliente.

- El contenido de las CRLs puede considerarse información sensible, luego debe protegerse adecuadamente.

- El almacenamiento de información sobre la validación de un certificado de cara a auditorías es factible.

La vía de comprobación del estado de los certificados revocados con ASF depende del tipo de certificados que se pretenda validar.

Para certificados soportados por la plataforma @firma, el método de validación primario utilizado es la consulta mediante OCSP a @firma a través de la Intranet Administrativa.

El método de validación secundario es la comprobación mediante OCSP directamente a la URL proporcionada por la Autoridad de Certificación emisora del certificado en cuestión.

En los casos en que la Autoridad de Certificación emisora no proporciona OCSP, se validan los certificados mediante el acceso a la CRL proporcionada por la Autoridad de Certificación emisora del certificado.

Por último, como ya se explicó anteriormente, el caso de la FNMT se trata de forma diferente, almacenando una réplica del LDAP en local, del cual se obtiene el estado de revocación de los certificados de esta CA.

Las consultas sobre el estado de revocación se pueden lanzar a ASF bien mediante WebSservices o bien usando a su vez el propio OCSP Responder de la plataforma.