



Servicio de Firma Electrónica Remota sobre Dispositivo Seguro Centralizado (SSCD)

Título del documento:	Servicio de Firma Electrónica Remota sobre SSCD
Nombre del fichero:	Servicio Firma Electronica Remota.doc
Versión:	1.0
Estado:	VIGENTE
Fecha:	25/8/2008
Autor:	JOSE VILATA

Revisión, Aprobación		
Revisado por:		Fecha:
Aprobado por:		Fecha:

Historial de cambios			
Versión	Fecha	Descripción de la acción	Páginas
■	■	■	
■	■	■	

Tabla de Contenidos

1	INTRODUCCIÓN.....	4
2	DESCRIPCIÓN DEL SERVICIO.....	4
3	ACCESO AL SERVICIO. BALANCEO DE CARGA.....	5
	ANEXO RELATIVO A NORMATIVA DE DISPOSITIVOS SEGUROS DE CREACIÓN DE FIRMA .	7

1 Introducción

El servicio de Firma Remota EDICOM “**EDICOM CRYPTO SERVER (ECS)**” permite realizar firma electrónica reconocida con certificados almacenados en dispositivos seguros de firma (SSCD) a través de un interfaz WebService sobre HTTPS.

El servicio ECS utiliza a su vez los siguientes servicios de EDICOM relacionados con la seguridad y firma electrónica:

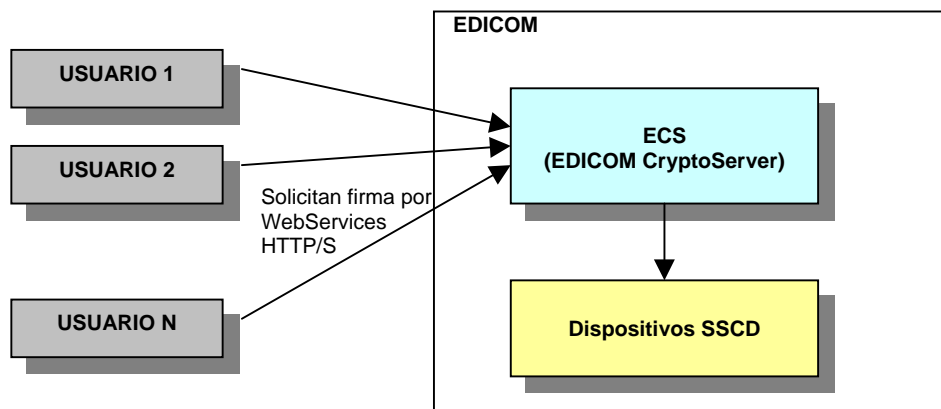
- Entidad certificadora ACEDICOM para la generación de certificados reconocidos.
- Servicio de TimeStamp (TSA) para realizar sellado de tiempo.
- Servicio OCSP para información de revocación de certificados

2 Descripción del servicio


El servicio ECS (Edicom Crypto Server) permite operaciones criptográficas de firma en una arquitectura cliente servidor, bien desde dentro del entorno ASP de EDICOM (intranet privada) o desde Internet (acceso público).

Mediante ECS la tecnología de firma electrónica reconocida mediante dispositivos seguros tipo smartcards o HSM queda totalmente solucionada y sin ninguna complicación añadida para el software cliente, pasándole por tanto la responsabilidad de la gestión o el acceso a estos dispositivos al propio ECS con todas las ventajas de administración que ello conlleva para el cliente de ECS ya que no debe preocuparse por la seguridad física de dispositivo de firma así como también le abstrae de la complejidad técnica del acceso concurrente a dicho dispositivo de firma desde múltiples sitios.

En el caso de que el cliente que solicita la firma no esté en el entorno ASP de EDICOM (intranet) , llamaremos a esta firma “Firma Electrónica Remota”.



ARQUITECTURA SERVICIO ECS (EDICOM CRYPTOSERVER)

	SERVICIO DE FIRMA ELECTRÓNICA REMOTA SOBRE SSCD	
	Edición 1	Página 5

En el modo actual de funcionamiento de ECS, todos los pares de claves se encuentran almacenados en el dispositivo seguro centralizado SSCD. La generación de estas claves es un proceso totalmente ajeno a ECS y sigue los Procedimientos operativos correspondientes de la Autoridad de Certificación ACEDICOM.

El cliente ECS, normalmente el módulo crypto del software Ediwin, conectará por WebServices con ECS para solicitar una firma.

Existen dos niveles de autenticación:

- Autenticación a nivel de servicio ECS. Permite acceso al servicio ECS.
- Autenticación con el dispositivo seguro de firma (SSCD). Además de la autenticación de ECS, en la solicitud de firma el cliente mandará las credenciales para que ECS se autentique con el SSCD. En esta autenticación también va incluido el PIN asociado a la clave privada.

El servicio ECS registra cada petición de firma, con una serie de información adicional.

3 Acceso al servicio. Balanceo de carga

Para dotar al servicio de firma de máxima disponibilidad se ha replicado por completo la infraestructura en cada uno de los CPDs de EDICOM, como es habitual en todos los servicios de ASP o SEDEB2B en Edicom.

La naturaleza intrínseca de los dispositivos seguros de firma SSCD impide una arquitectura de máxima disponibilidad usando los mismos pares de claves. De modo que se ha optado por una solución en la que a cada cliente de ECS se le generan dos certificados (con sus correspondientes pares de claves), cada uno de ellos en un entorno distinto.

En el SSCD centralizado que hay en el entorno de ACEDICOM01 tenemos usuarios, claves y certificados firmados por la Autoridad de Certificación ACEDICOM01 y en el entorno de ACEDICOM02 tenemos los mismos usuarios (se crean 2 veces), claves nuevas y certificados firmados por la Autoridad de Certificación ACEDICOM02.

En todo este servicio existe el concepto de **firma delegada**, que básicamente consiste en firmar documentos de un cliente con un certificado a nombre de Edicom (una persona de Edicom) todo acordado en el correspondiente contrato previo. A nivel de ECS la firma delegada simplemente supone que varios cliente compartirán las credenciales de ECS y de SSCD centralizado.

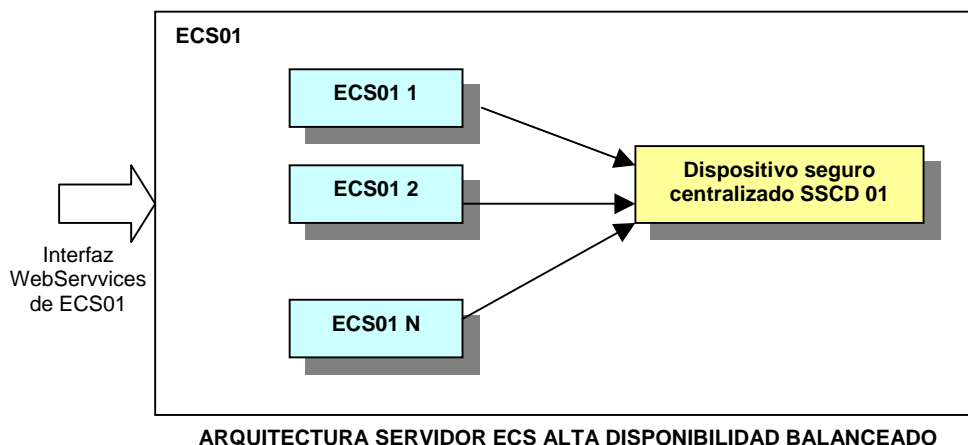
Por tanto un usuario de ECS podría firmar indistintamente con el certificado firmado por ACEDICOM01 o por el firmado por ACEDICOM02. Para evitar que en una situación normal se vayan alternando las claves con el que un usuario firma sus documentos, situación que puede provocar incidencias en algunos de los destinatarios de los documentos firmados, existe el concepto de **Dispositivo o entorno “preferido”**, que indica cuál es el certificado con el que ECS debe firmar preferiblemente.

Para evitar tener una arquitectura activo/pasivo, a unos usuarios se les configurará como entorno preferido el 01 y a otros el 02.

Cuando hablamos de entorno 01 nos referimos a:

- Claves almacenadas en dispositivo seguro centralizado (SSCD)
- Certificado firmado por ACEDICOM01

Cada servidor ECS tiene conectividad únicamente con el dispositivo centralizado (SSCD) que se encuentra en su mismo entorno:




Ante una petición de firma recibida por ECS nos podemos encontrar con varios casos:

- Acierto: El certificado con el que se solicita se encuentra en el entorno del ECS que recibe la petición
- Habilitado: A nivel lógico tenemos habilitado el dispositivo centralizado SSCD asociado al certificado.
- Estado: Estado del dispositivo centralizado SSCD: ERR o OK.
- Result: OK, ERR
- Info: Cambio -> Le indica al cliente que el dispositivo de su certificado está temporalmente OFFLINE

Podemos configurar el cliente ante offline del dispositivo primario como sigue:

- OK acepto el nuevo certificado -> Volverá a intentarlo con el nuevo. En este segundo intento se producirá el acierto de ECS y le pedirá firmar con un

	SERVICIO DE FIRMA ELECTRÓNICA REMOTA SOBRE SSCD	
	Edición 1	Página 7

certificado que no es el suyo principal. ECS marcará como “ENUSO” el de backup. Esto sirve para que cuando el suyo principal esté online, se pueda hacer la vuelta atrás en la configuración. ECS le indicará lo mismo al cliente, que ese no es el certificado con el que debería firmar, cambiará la configuración, etc..

- No hago nada. (no cambia su configuración). Seguirá intentándolo y obteniendo error.


ECS tiene la información del estado actual y de la configuración habitual. Gracias a esta información es posible una vuelta atrás automáticamente de la configuración de los clientes (siempre que lo acepten).

Anexo relativo a normativa de dispositivos seguros de creación de firma

Edicom proporciona en su plataforma un servicio de creación de firma basado en **dispositivo seguro** que goza de la certificación CWA 14169 y por lo tanto con plenas garantías en el ámbito de la Unión Europea.

La Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, establece un marco comunitario para la firma electrónica (en adelante, la Directiva). En su artículo 3, la Directiva expone que la conformidad de los dispositivos seguros de creación de firma será determinada por los organismos designados por los Estados miembros, siendo la Comisión quien ha de fijar los criterios para que los Estados miembros establezcan si procede designar un determinado organismo. Por otro lado, obliga a que la conformidad señalada por dichos organismos ha de ser reconocida por todos los Estados miembros. Así mismo, con el fin de armonizar los requisitos técnicos, la Directiva habilita a la Comisión para poder determinar, y publicar en el Diario Oficial de las Comunidades Europeas (DOCE), los números de referencia de las normas que gozan de reconocimiento general para los productos de firma electrónica, indicando que los Estados miembros presumirán que los productos de firma electrónica que se ajusten a dichas normas son conformes con los requisitos que establece la Directiva para su consideración como dispositivos seguros de creación de firma.

Por otro lado, era necesario que los requisitos generales definidos en la Directiva para dispositivos seguros de creación de firma se encontraran concretados en una norma que sirviera de referencia para evaluar la conformidad de un dispositivo concreto y que esta norma fuera publicada en el Diario Oficial de las Comunidades Europeas (DOCE) por la Comisión, tal y como hemos visto anteriormente que prevé la Directiva. Con este objetivo, entre otros, la Comisión hizo un llamamiento a la industria y a los organismos

	SERVICIO DE FIRMA ELECTRÓNICA REMOTA SOBRE SSCD	
	Edición 1	Página 8

de normalización europeos para que analizaran si las normas ya existentes cubrían los requisitos exigidos por la Directiva.

Este análisis identificó áreas no suficientemente cubiertas y por tanto que era necesario elaborar nuevas normas que se ajustaran a las necesidades de la Directiva. En consecuencia con este análisis, surgió la Iniciativa Europea para la Normalización de la Firma Electrónica (EES SI) en el marco del Órgano de Normalización de las Tecnologías de la Información y la Comunicación (ICTSB), dividiéndose los trabajos de normalización técnica entre dos de los organismos de normalización europeos oficialmente reconocidos: el Comité Europeo de Normalización (CEN) y el Instituto Europeo de Normalización de las Telecomunicaciones (ETSI).

El resultado de estos trabajos son una serie de especificaciones técnicas que abarcan la mayoría de las áreas de requisitos señaladas por la Directiva y entre ellas el Acuerdo de trabajo de CEN, CWA 14169, relativo a dispositivos seguros de creación de firma. Esta especificación, siguiendo el modelo de Criterios Comunes para la Evaluación de la Seguridad de las Tecnologías de la Información, más conocido por Criterios Comunes (CC), adopta la forma de un Perfil de Protección (PP) con un Nivel de Garantía de Evaluación 4+. Tras su aceptación en el seno del comité de firma electrónica, que según el artículo 9 de la Directiva debe asistir a la Comisión y que está compuesto por representantes de los Estados miembros y de la Comisión, ésta aprobó en julio de 2003 una "Decisión relativa a la publicación de los números de referencia" de las normas que gozan de reconocimiento general para productos de firma electrónica, donde se incluía el CWA 14169 como norma técnica de reconocimiento general para dispositivos conformes con los requisitos del anexo III de la Directiva, es decir para dispositivos seguros de creación de firma.