DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES

FIRMA ELECTRÓNICA DE LARGA DURACIÓN

	NOMBRE	FECHA
Elaborado por:	Departamento Ceres	28 - Jul- 2008
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	**Descripción**	**Autor**
1	28 – Jul - 2008	Creación del documento	Departamento Ceres

FIRMA ELECTRÓNICA DE LARGA DURACIÓN. FIRMA LONGEVA

Comenzar recordando lo que es una firma electrónica, tomando como referencia la Ley 59/2003 de firma electrónica, y cómo se ha llegado a equiparar con la firma manuscrita, tenemos que:

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Profundizando en el tema se define lo que es firma avanzada y firma reconocida:

La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Y por último, recordemos el aspecto más interesante de una firma electrónica: y es *que la firma reconocida tendrá el mismo valor que la firma manuscrita en relación con los datos consignados en papel.*

Por tanto, se ha conseguido efectuar electrónicamente lo que hasta ahora sólo podía realizarse físicamente, pero esto añade una serie de requerimientos a la operación que no existían para el mundo físico, se tiene que poder validar esa firma, ¿y en que consiste esa validación?, resumiendo habría que asegurar dos aspectos, el primero de ellos comprobar la integridad de los datos firmados asegurando que éstos no hayan sufrido ninguna modificación y segundo, comprobar que el estado del certificado con el que se firmó era el correcto, es decir, era vigente en el momento de la operación.

Pero además se quiere llegar más lejos, porque el proceso de verificación de una firma debe poder repetirse años después de su generación y con el paso del tiempo, las claves, los algoritmos empleados, etc, se pueden considerar obsoletos o incluso podemos no tener acceso a determinados datos necesarios para la comprobación.

Para solucionar este inconveniente se precisa incorporar a la firma electrónica los elementos de tiempo y validación que permitan verificar esa firma sin ayuda externa, se deberán guardar y mantener todas las evidencias que posibilitarán su verificación posterior.

Existen diferentes versiones para los principales formatos de firma existentes denominados AdES (Advanced Electrónic Signature) que amplían las posibilidades de las firmas electrónicas [1].

De forma muy breve se apuntan a continuación los distintos formatos de firma que van incrementando la calidad de la misma hasta conseguir una firma que pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas:

1. Firma Básica (AdES - BES), firma básica para satisfacer los requisitos de la firma electrónica avanzada.
2. AdES - T, se añade un sellado de tiempo (TimeStamp) con el fin de situar en el tiempo el instante en que se firma un documento.
3. AdES - C, añade un conjunto de referencias a los certificados de la cadena de certificación y su estado, como base para una verificación longeva.
4. AdES - X, añade sellos de tiempo a las referencias creadas en el paso anterior.
5. AdES - XL, añade los certificados y la información de revocación de los mismos, para su validación a largo plazo.
6. AdES - A, permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones.

Se ha conseguido una firma longeva “auto-verificable” con el paso del tiempo.

---

[1] *XAdES (XML Advanced Electronic Signatures), ETSI TS 101 903*

CAdES (CMS Advanced Electronic Signature), ETSI TS 101 733