Representando a los
Abogados europeos

Directrices sobre proyectos de firma electrónica y uso de ésta por abogados

I- Introducción:

Estas directrices son parte de un importante proyecto del CCBE que busca ayudar al desarrollo de un ambiente electrónico seguro y práctico para los abogados a lo largo de toda Europa. La firma electrónica, objeto de estas recomendaciones, no puede ser considerada como un asunto aislado que se detiene en las fronteras de las jurisdicciones nacionales. El establecimiento de este gran proyecto para los abogados europeos, que ayudará a facilitar las comunicaciones electrónicas y hacerlas más interoperables, es necesario para facilitar la libertad de servicio y establecimiento del ejercicio de la abogacía. También ayudará a los abogados a interactuar de manera segura y a mantener su rol como sujetos independientes del sistema judicial y dentro de las estructuras electrónicas de los Gobiernos nacionales.

Este borrador de directrices para proyectos de firma electrónica sigue la misma línea que las recomendaciones ya dadas sobre los carnets electrónicos, adoptadas por el Comité Permanente del 13 de octubre de 2006. A finales de este año se presentará un borrador sobre el Marco Comunitario para el Sistema de Carnets Electrónicos para abogados. La estructura de este sistema se basará en los estándares técnicos, principalmente en la Política Común de Certificación, para que las autoridades nacionales de certificación puedan interoperar de manera digital. Con este Sistema Europeo, el CCBE busca apoyar a sus miembros en el desarrollo del carnet electrónico mientras que al mismo tiempo se mejora la interoperabilidad de abogados por toda Europa. Estas directrices son, por tanto, un paso en la mejora del sistema y, siendo optimistas, crearán una conciencia entre abogados acerca de la necesidad de comunicaciones electrónicas seguras y las ventajas que esto traerá a la profesión.

II- Directrices:

Se recomiendan las siguientes actividades a las abogacías:

.

1. Investigar la aplicación exitosa de la firma electrónica en otros ámbitos. Este es el camino más rápido, seguro y económico para el desarrollo de nuestros propios sistemas.

2. Reducir los costes, observando qué es posible aprovechar de iniciativas ya existentes para nuestra propia iniciativa, como por ejemplo los documentos de identidad nacionales.

3. Asegurarse de que la tecnología de firma elegida produzca firmas de calidad (vg. las firmas cumplen con los requisitos del artículo 5.1 de la Directiva 1999/93/EC donde se establece un marco Comunitario para la firma electrónica, en el cual se prevé el certificado de calidad y un mecanismo seguro de creación de la firma).

4. Garantizar la interoperabilidad técnica, usando los estándares[1] aprobados para los productos de firma electrónica (vg. los números de referencia generalmente reconocidos por los estándares publicados en la Decisión de la Comisión de 14 de julio de 2003 (2003/511/EC) en consonancia con la Directiva 1999/93/EC sobre firma electrónica.

5. Hacer un borrador propio con la documentación subyacente para este proyecto (política de firmas, declaración sobre la práctica de certificado, política de certificados).

6. Llevar acabo los pasos adecuados para garantizar su archivo y validez a largo plazo (garantizando que el documento es el correcto y que no ha sido objeto de cambios o enmiendas desde su archivo).

7. Explicar a los profesionales que los proyectos de firma electrónica no deben seguir elaborándose de modo aislado sino que deben ser incorporados a una propuesta global de “oficina sin papeles”, incluyendo, por ejemplo, contenidos de gestión de empresas, archivos dirigidos a los Tribunales, etc.

8. Tener en cuenta la facilidad de uso del proyecto elegido, ya que muchos sistemas fracasan porque los abogados no saben cómo usarlos.

9. Asegurarse de que los certificados contengan los atributos relacionados con la profesión jurídica o vayan referidos a una base de datos –significa que es posible vía certificado, establecer que el propietario de un certificado es un abogado cualificado, bien en el propio certificado, o bien por una referencia a una base de datos donde se pueda encontrar la información.

10. Considerar el uso de tarjetas inteligentes para guardar las claves de firma necesarias para el proyecto.

---

[1] Anexo de la Decisión de la Comisión (2003/511/EC)

A. Lista de normas que gozan de reconocimiento general para productos de firma electrónica considerados conformes por los Estados miembros con los requisitos del anexo II f de la Directiva 1999/93/CE

- CWA 14167-1 (marzo de 2003): security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System Security Requirements

- CWA 14167-2 (marzo de 2002): security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: cryptographic module for CSP signing operations - Protection Profile (MCSO-PP)

B. Lista de normas que gozan de reconocimiento general para productos de firma electrónica considerados conformes por los Estados miembros con los requisitos del anexo III de la Directiva 1999/93/CE

- CWA 14169 (marzo de 2002): secure signature-creation devices