



La importancia de la decisión
correcta.

eID para eGov, experiencias en
España

Manuel Torres – 16 de Agosto de 2013

- Las nuevas tecnologías de la información requieren de elementos que permitan garantizar a la sociedad de mecanismos que aseguren la privacidad, libertad y derechos de los que ya goza en el entorno físico.
 - 11 países de la Unión Europea disponen de una forma de identificación electrónica ciudadana, 11 de los 18 restantes han anunciado planes para su despliegue durante los próximos años
 - ✓ España, dispone del mayor proyecto a nivel mundial de identificación ciudadana con más de 40 millones de ciudadanos españoles, para los que ya se han emitido más de 35 millones de tarjetas de e-ID.
- La mayoría de países europeos dispone de más de un Prestador de Servicios de Certificación:
 - En España existen 30 Prestadores de Servicios de Certificación reconocidos, de los cuáles 12 pertenecen al sector público:
<http://www11.mityc.es/prestadores/busquedaPrestadores.jsp>

- Las cédulas personales fueron el origen del Documento Nacional



Contenido del Chip

- Certificado y claves de Autenticación
- Certificado y claves de No-Repudio
- Certificado de la CA Emisora
- Datos de filiación del Ciudadano
- Imagen de la Fotografía
- Imagen de la firma Manuscrita
- Plantilla de impresión Dactilar
- Aplicación Match On Card



Medidas de Seguridad Física



Tintas OVI

- Impresión con cambio de color

Estructura de superficie

- Guilloches y microimpresión
- Fácil verificación visual y táctil

Tintas UV/IR

- Sólo visibles con luz ultravioleta o infrarroja
- Tintas Fluorescentes

Chip criptográfico

- Para autenticación mediante comparación biométrica almacenada en el chip
- Datos criptografiados



Holograma/Kinegrama

- Estructura holográfica artística
- Protegido por overlay de 100nm

Imagen láser cambiante (CLI)

- Elementos de información diferentes y específicos combinados en una estructura grabada a láser.
- Fotografía MLI

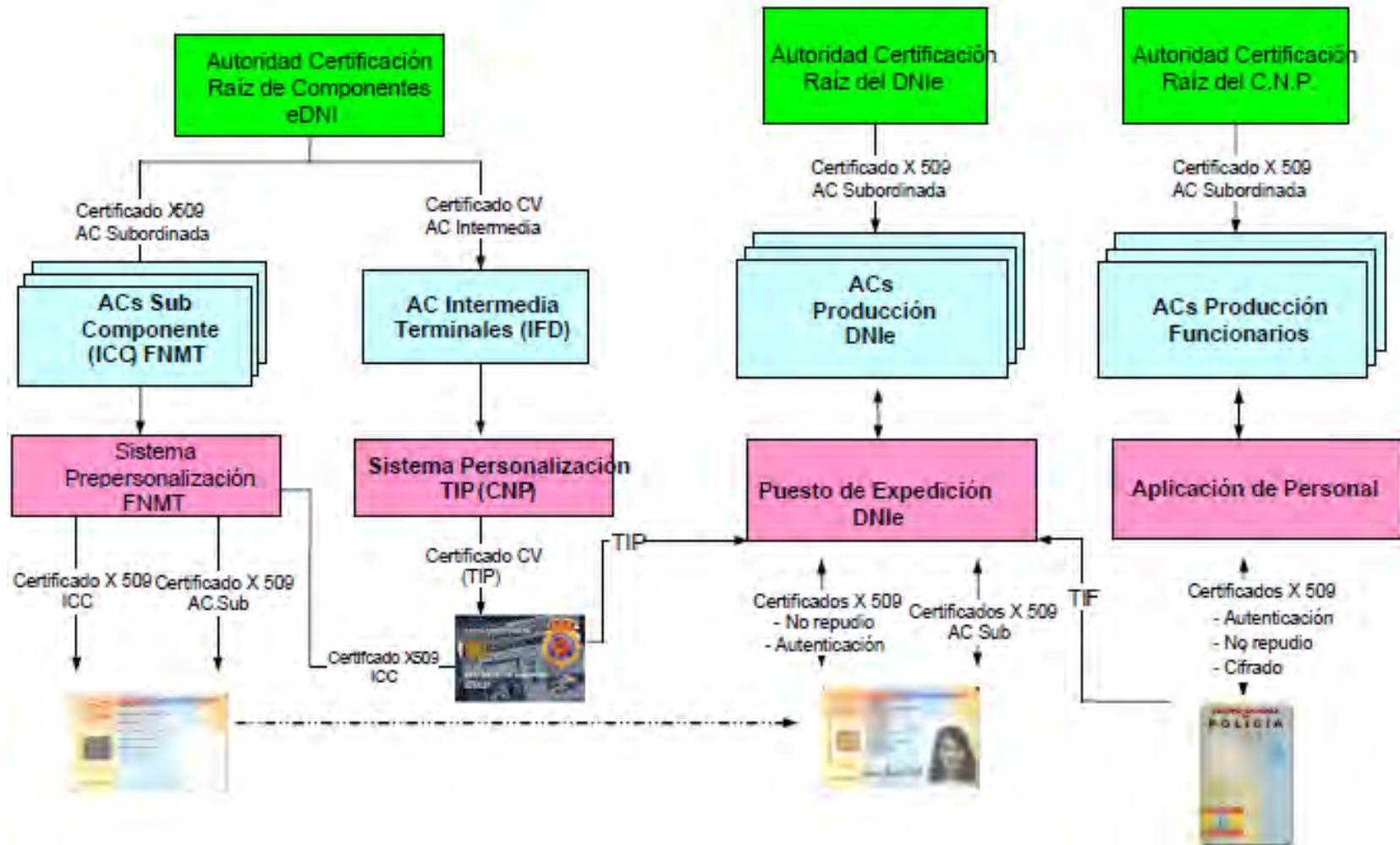
Fondo de Seguridad

- Formas de guilloches que pueden incorporar logotipos
- Impresión irisada.

Fotografía

- Grabada con tecnología láser en el interior de la tarjeta
- Protección contra falsificación
- Integración de la imagen en el fondo impreso de la tarjeta.
- Borde del retrato superpuesto y fondo de seguridad

Infraestructura de Clave Pública en el DNle



La tarjeta



Certificación CC Chip



Certificación CC SO Tarjeta



Certificación del Sistema de Expedición

AENOR

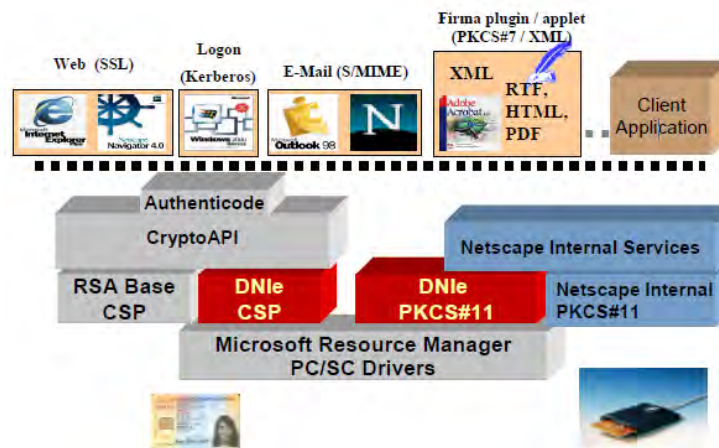
Inicio > Certificación > Buscar certificados

Ficha del Certificado de la Empresa

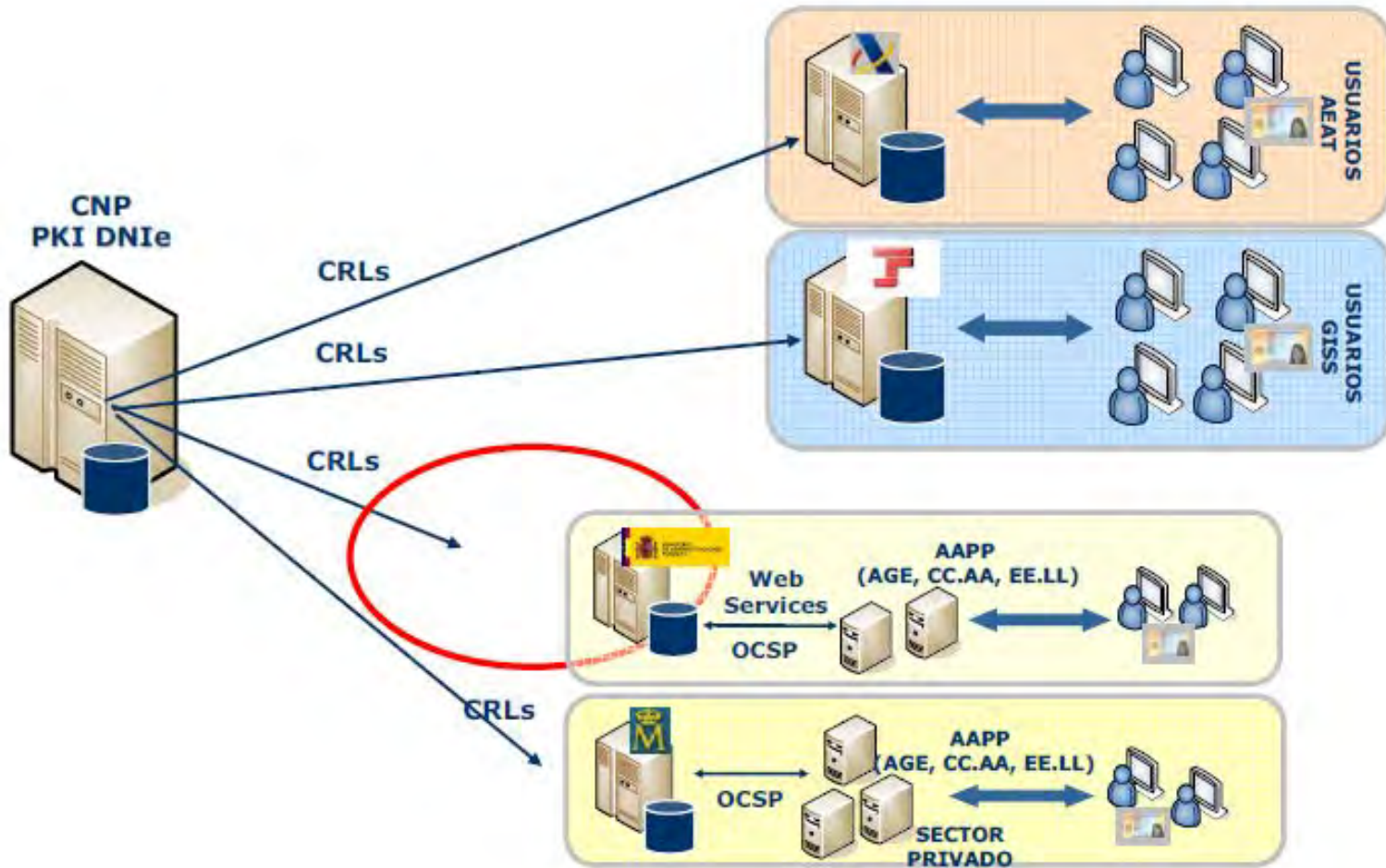
Empresa	DIRECCIÓN GENERAL DE LA POLICÍA,
Certificado	SI-0011/2011
Norma	UNE-ISO/IEC 27001:2007
Alcance	Los sistemas de información que dan soporte a las actividades de gestión de la explotación de los servicios centrales del proceso de expedición del DNIe, según la declaración de aplicabilidad vigente.
Centros incluidos:	1
DIRECCIÓN GENERAL DE LA POLICÍA	
Dirección	CPD EL ESCORIAL. CR. GUADARRAMA-EL ESCORIAL, S/N
CP	28280
Localidad	MADRID
País	España

Volver

Soporte tecnológico de Uso



Esquema Validación del DNIe



- **A2C – Administration to Citizen**

- El DNle se ha convertido en un referente en la administración pública, participando activamente en la provisión de servicios de identificación, Autenticación y firma electrónica en la mayoría de los proyectos estratégicos lanzados por las administraciones

- **Catalizador: Ley 11/2007**

- **B2C – Business to Consumer**

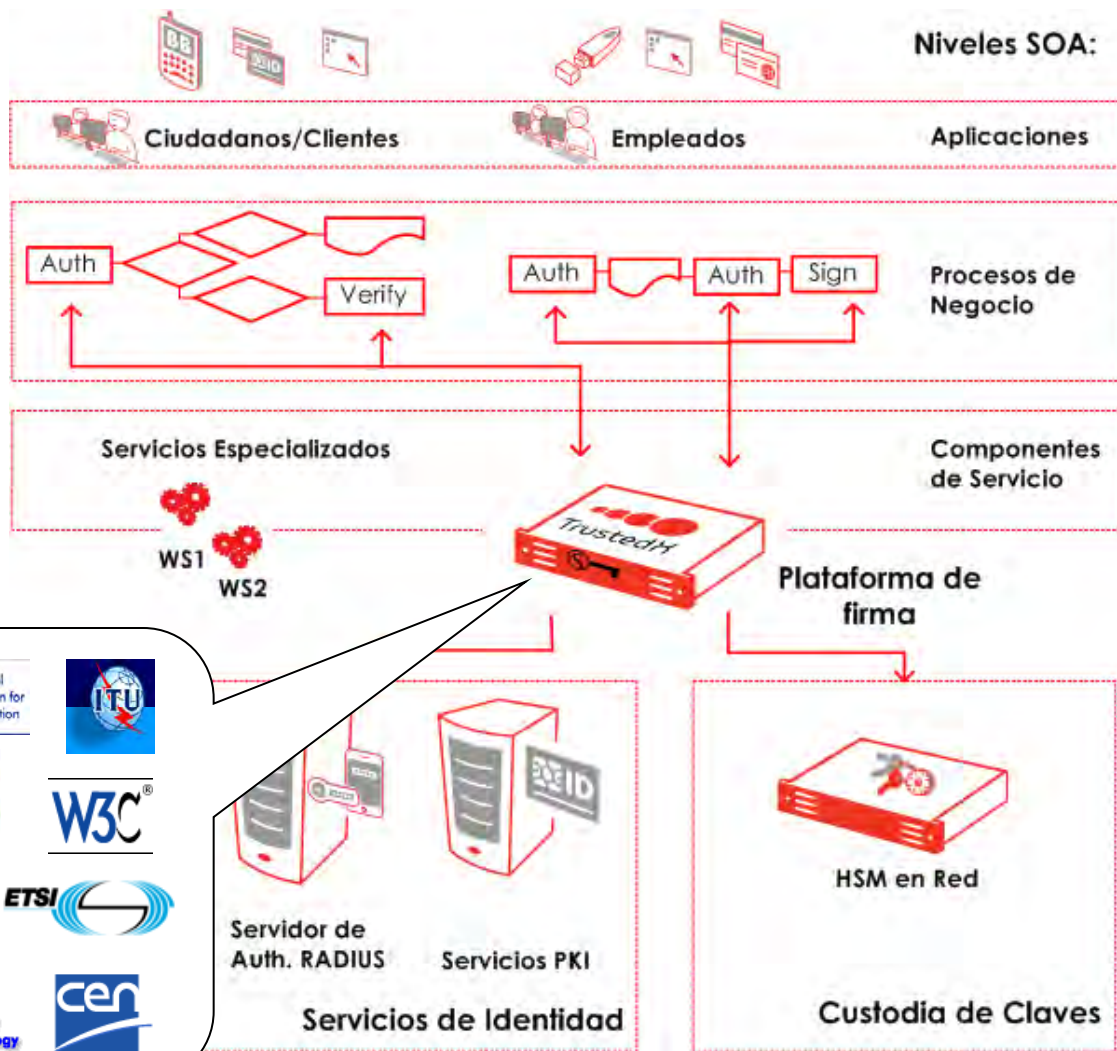
- Tímidamente se observa un paulatino uso del DNle en los servicios ofrecidos por Entidades financieras y por Utilities debidas principalmente al cumplimiento de la LISI.
- Permite una mejora de los procesos de negocio y habilita nuevos canales.

- El DNle no es competencia a los PSC (Prestadores de Servicios de Certificación) reconocidos
 - Impulsa su demanda y les aporta un valor añadido.

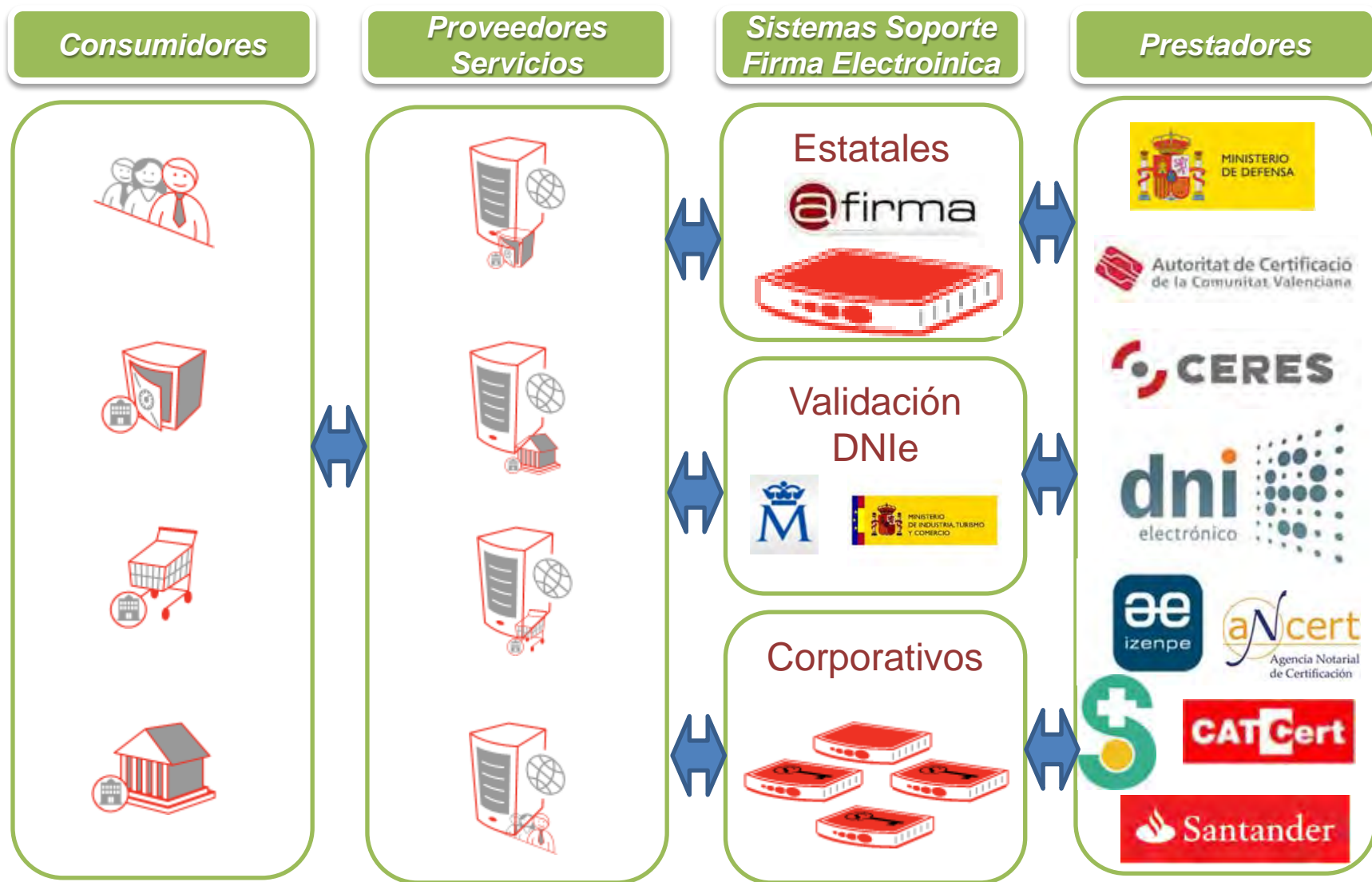
<http://www.cert.fnmt.es/index.php?cha=cit&sec=4&page=184&lang=es>

- Una organización no puede obligar a utilizar el DNle a sus empleados
 - Puede disponer de una jerarquía de certificación interna para utilizarla en los procesos corporativos de negocio.
- La organización que se vea afectada por la LISI tendrá que disponer de los medios necesarios para reconocer los certificados reconocidos por el Ministerio de Industria, no sólo los del DNle.
- Tanto el DNle como los certificados de los PSC son la materia prima
 - Es necesario una infraestructura de servicios para incluirse en los procesos de negocio corporativos.

Enterprise Trust Integration



Soporte a Proveedores de Servicios para el uso de la Firma electrónica



- En general la sociedad española ha aceptado de buen grado la implantación del DNle, si bien hay que considerar:
 - Los aspectos de seguridad establecidos en el DNle suponen un paso adelante en la “autenticidad” del documento y posibilita asociarlo inequívocamente a su “dueño” mediante medidas biométricas lo que permite al ciudadano demostrar su identidad.
 - <http://zonatic.usatudni.es/es/actualidad/blog-noticias-discusion/el-dnie-permite-un-control-de-fronteras-rapido-y-automatico-en-los-aeropuertos-de-madrid-y-barcelona.html>
 - Si bien el número de DNle y de servicios van aumentando,
 - http://www.dnielectronico.es/servicios_disponibles/
 - <http://www.usatudni.es/dnie/servicios/195>
- la utilización del DNle por parte de los ciudadanos en el ámbito puramente “internet” ofrece paupérrimas cifras:
 - Solo el 3% de los usuarios con DNle dispone de Lector de Tarjetas.
 - De estos apenas la mitad han hecho uso del DNle.

- **2013**
 - **Evolución de Algoritmos y Claves.**
 - Cambio de SHA1 a SHA2
 - Incremento del tamaño de claves 2048 a 4096 en Certificados de CA's
 - **Solicitud de renovación por Internet.**
 - Actualmente sólo en puesto automáticos en dependencias policiales
 - Requiere presentación telemática de documentación
- **2014**
 - **Certificado de Identificación para Menores.**
 - Modificación del artículo 1.4 del Real Decreto 1553/2005, por el que se regula la expedición del documento nacional y sus certificados de firma electrónica, para que permita la identificación electrónica del titular del DNI aunque este sea menor de edad.
 - **Inclusión del Correo Electrónico en el certificado (voluntario).**
 - **Funcionalidad del DNI como documento de viaje.**
 - Chip con dos interfaces (Contacto + NFC) y doble funcionalidad
 - Adaptación a los requisitos establecidos por la ICAO y la UE para los documentos de viaje electrónicos.

- **Interoperabilidad a nivel Europeo.**
 - **Stork (Secure Identity Across Borders Linked)**
<https://www.eid-stork.eu/>
 - eID Interoperability for PEGS (Pan-European eGovernment Services) (<http://ec.europa.eu/idabc/servlets/Doc?id=29621>)
- **Incorporación del DNle en todos los procesos de negocio.**
- **Utilización de aplicaciones Certificadas.**
- **Desarrollos para nuevos dispositivos.**
- **Voto electrónico a través de Internet**
- **etc**

- En general podemos decir que el DNle no ha hecho más que nacer, al que le queda un largo recorrido que implicará su crecimiento, adaptación y evolución.
- No debemos ver el DNle como componente aislado, debemos considerarlo como un conjunto de elementos que han de sincronizarse para funcionar apropiadamente.
- Garantizar la interoperabilidad con otros servicios de identificación digital.
- Deben existir servicios que garanticen la no-repudiabilidad de las firmas electrónicas siguiendo los estándares que garantizan la longevidad de las mismas.

Muchas gracias:

Manuel Torres
Regional Sales Director
manuel.torres@safelayer.com
www.safelayer.com
+34 917 080 480

*©1999-2013 Safelayer Secure Communications, S.A. Todos los Derechos Reservados.
Este material es propiedad intelectual de Safelayer Secure Communications S.A.
No se permite la reproducción total o parcial de este material sin el previo consentimiento de
Safelayer.*