MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Servicios seguros y confiables: DNI electrónico

Antonio Alcolea Muñoz

Dirección General para el Desarrollo de la Sociedad de la Información
Secretaría de Estado de Telecomunicaciones y para el Desarrollo de la Sociedad de la Información

2ª Jornada sobre Televisión de Servicio: T-ciudadano

Barcelona, 15 de junio de 2006

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Visión de los Servicios Interactivos (SI)

- Accesibles por el 99% de los hogares en 2010.
- Modelo de negocio complejo
  - prestadores de servicios interactivos, operadores de contenidos y de red, proveedores de publicidad, etc.
- Entorno tecnológico convergente
  - Multicanal: TD Terrestre / Satélite / Cable / ADSL, Internet, Redes Móviles, etc.
  - Multiplataforma y multidispositivo: TV, PC, Móvil, PDA, Home Media Platforms, consola juegos, etc
- Banda ancha en el canal de retorno
- Tendencia a la personalización / individualización
- Seguros y confiables > factor crítico de éxito

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Seguridad y Confianza en los SI

- Requisitos de seguridad de la información en los SI
  - Autenticación de origen
  - Autenticación del prestatario del servicio
  - No repudio de las transacciones
- Su implementación contribuye a la generación de confianza entre usuarios y prestadores de servicio, y por tanto impulsa:
  - el comercio electrónico y la banca electrónica evitando el fraude online y la ciberdelincuencia
  - la implantación de la administración electrónica,
  - el desarrollo de servicios personales, por ejemplo, e-Health.
  - la protección eficaz frente a contenidos ilícitos y nocivos

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Descripción y Funcionalidad del DNIe

- El DNI electrónico (DNIe) es una infraestructura pública de seguridad de la información que permite:
  - Acreditar electrónicamente y de forma indubitada la identidad de la persona
  - Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita
- Marco jurídico:
  - Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
    - Directiva 1999/93/CE del Parlamento Europeo y del Consejo, por la que se establece un marco comunitario para la firma electrónica.
  - Real Decreto 1553/2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica.
- Otras disposiciones
  - Decisión 2003/511/CE, de 14 de julio de 2003, relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica
    - CWA 14169, dispositivos seguros de creación de firma

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Fortalezas del DNIe

- Gran aceptación social: forma parte de nuestra operación diaria y de nuestra cultura
- 97% de las bases de datos tiene el número del DNI como clave
- Infraestructura pública de seguridad
- Basada en estándares de PKI y de tarjeta inteligente
- Permite autenticación del titular
- Permite la firma electrónica reconocida
  - Certificados reconocidos
  - La DG de la Policía cumple las obligaciones de la Ley para los PSC que emiten certificados reconocidos y la ETSI TS 101 456.
  - La tarjeta criptográfica es un dispositivo seguro de creación de firma electrónica certificado CWA 14169
- Estará disponible en todos los hogares y para todos los usuarios.
  - 2008+ despliegue completo
- Más de 140 servicios ya disponibles de eAdmon

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Tarjeta Criptográfica - soporte

http://www.dnielectronico.es/Asi_es_el_dni_electronico/presen_graf.html

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Tarjeta Criptográfica - soporte

http://www.dnielectronico.es/Asi_es_el_dni_electronico/presen_graf.html

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Certificados electrónicos

- Dos certificados diferentes
  - autenticación y firma electrónica
- Información personal
  - Nombre y apellidos, DNI, y fecha de nacimiento
- Certificados reconocidos
  - ETSI TS 102 280, RFC3739,
  - Artículo 11 de la Ley 59/2003
- Usos
  - Autenticación (Digital Signature): garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática.
  - Firma electrónica (Non Repudiation): permite al ciudadano firmar tramites o documentos electrónicos
- Algoritmos criptográficos
  - SHA-1, SHA-256
  - RSA clave de 2048 bits
- Accesibles con un PIN / Biometria

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Tarjeta criptográfica - chip

- Chip  ST19WL34 y ICC ST19WL34
- Certificación EAL4+ según perfil de protección CEN CWA14169 por el Centro Criptológico Nacional (CNI)
- Es un dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3, de la Ley 59/2003
  - Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.
  - Que exista seguridad razonable de que dichos datos no puedan ser  derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.
  - Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.
  - Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Servicios de la Infraestructura DNIe

- Autoridades de Validación
  - Carácter universal, gratuíto, y disponibles al público
  - Inicialmente:
    - Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda
    - Ministerio de Administraciones Públicas
  - OCSP
  - Futuro: especialización / segmentación (ciudadanos, empresas, administración pública), evolución multi-PSC
- CAU
  - 24 / 7 , universal, gratuito, integral (atiende cualquier tipo de incidencia de primer nivel sobre la infraestructura del DNIe)
- Portal www.dnielectronico.es
- Oficina Técnica

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Lectores de tarjeta inteligente

- Lector **ISO 7816** – para Smart Card Clase A y B.
- Soportará tarjetas asíncronas basadas en protocolos T=0 (GSM, Visacash, Euro6000, Tarjeta criptográfica FNMT) y T=1 (German Geldkarte)
- Soporte a velocidades de comunicación mínimas de 9.600 bps.
- Puerto USB, RS232 y sobre teclado.
- Alimentación interna sin mantenimiento
- Compatibilidad EMI CE 89/336
- Standard ISO 7816 1/2/3 , EMV3.0, GSM11.11
- Compatibilidad sistema Windows.
- Estándares soportados:
  - PC/SC, CSP, PKCS#11

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Conclusión: la oportunidad del DNIe

- El DNI electrónico (DNIe) es una infraestructura pública de seguridad de la información que proporciona confianza en la prestación de servicios de comunicaciones electrónicas y de la sociedad de la información.
- La incorporación de DNIe en los SI permite cumplir con los requisitos de seguridad de la información, y aportar confianza en la prestación de servicios de calidad.
- La televisión digital es uno de los mejores vehículos para promover el uso del DNIe y avanzar en el desarrollo de la Sociedad de la Información, en particular, en la consecución de las políticas de e-Inclusión.

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

# Servicios seguros y confiables: DNI electrónico

Gracias por su atención

Antonio Alcolea Muñoz
aalcolea@mityc.es