AGENCIA ESPAÑOLA DE COOPERACIÓN INTERNACIONAL PARA EL DESARROLLO (AECID)

UNIVERSIDAD DE PANAMÁ

# La firma digital y las Administraciones Públicas

Arturo Ribagorda Garnacho
Catedrático de Universidad. Universidad Carlos III de Madrid

Universidad Carlos III de Madrid www.uc3m.es
Firma digital y certificados en las AA PP

## LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP

La seguridad de la información administrativa.
El cifrado de datos sensibles.
La firma digital.
- Qué es.
- Qué efectos tiene.
- Como se realiza.

Certificados digitales.
- Funciones.
- Tipos de certificados: personal, de servidor, …
- Contenido.
- Formatos.

Universidad Carlos III de Madrid www.uc3m.es
Firma digital y certificados en las AA PP

## LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP

Autoridades de Certificación
- Funciones.
- Tipos de Autoridades de certificación.
- Revocación de certificados.
- La constancia fiable de tiempo: sellos de tiempo y Autoridades de sellado

Infraestructuras de clave Pública (PKI).
- Estructuración de las Autoridades de certificación.
- Autoridades de validación. El caso de la Administración Pública española: La plataforma @firma.

La firma digital. Validez legal en España y en la Unión Europea.

**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

La identidad digital. Tarjetas e-ID (sanitaria, permiso de circulación, …). El documento nacional de identidad electrónico español.

La firma y los certificados en la informatización de las Administraciones. El caso español: La Ley 11/2007 de Acceso electrónico de los ciudadanos a las Administraciones Pública y su Reglamento de desarrollo.

Desarrollos legales en la protección de los datos personales.

- Directiva de la Unión Europea
- Ley española de protección de datos personales (LOPD)
- Reglamento de desarrollo de la LOPD.



ADMINISTRACIÓN ELECTRÓNICA[1]:

"El uso de tecnologías de la información y de las comunicaciones, especialmente Internet, como herramienta para mejorar la administración"

1. La administración electrónica: un imperativo. OCDE. 2004



ADMINISTRACIÓN ELECTRÓNICA

El uso de la tecnología de la información y la comunicación en las administraciones públicas para mejorar los servicios públicos y los procesos democráticos y reforzar el respaldo a las políticas públicas

LA ADMINISTRACIÓN PÚBLICA. Retos

Simplificación administrativa
Eficiencia
Coordinación
Cercanía
Transparencia
Privacidad



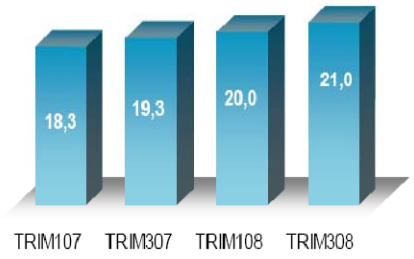
MEDIDAS DE SEGURIDAD: Legales

Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos

- R. D. 1671/2009, por el que se desarrolla parcialmente la Ley 11/2007
- R. D. 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- R. D. 4/2010, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.



A2C: % respecto de ciudadanos >15 años[1]



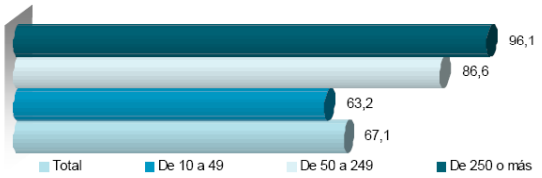

1. RED.ES-ONTSI (2008)

9

Universidad Carlos III de Madrid www.uc3m.es

## Firma digital y certificados en las AA PP

Empresas que interactúan con la A. P por Internet (%)




1. RED.ES-ONTSI (2008)

Universidad Carlos III de Madrid www.uc3m.es

Firma digital y certificados en las AA PP

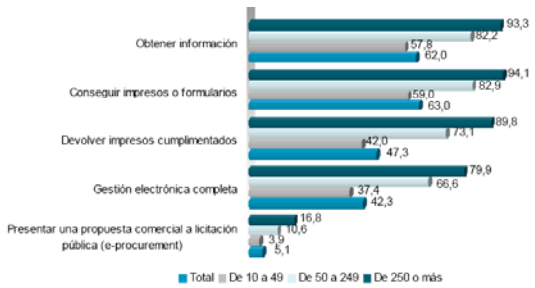
Microempresas que interactúan con la A. P. por Internet (%)


1. RED.ES-ONTSI (2008)

Universidad Carlos III de Madrid www.uc3m.es

Firma digital y certificados en las AA PP

EMPRESAS. Interacción con la A. P. por Internet (%)



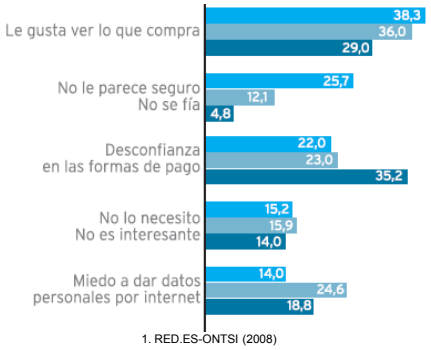

1. RED.ES-ONTSI (2008)

INDIVIDUOS. Trámites con la A. P. por Internet (%)


1. RED.ES-ONTSI (2008)



INTERNAUTAS: Razones para no comprar[1]




1. RED.ES-ONTSI (2008)

14



… Y el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en la sociedad en general y en la Administración en particular es la generación de **confianza** suficiente que elimine o minimice los riesgos asociados a su utilización. La desconfianza nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías.

LEY 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos

[…] las Administraciones deben comprometerse con su época y ofrecer a sus ciudadanos las ventajas y posibilidades que la sociedad de la información tiene, asumiendo su responsabilidad de contribuir a hacer realidad la sociedad de la información. Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de las Administraciones Públicas. Depende de la **confianza** y **seguridad** que genere en los ciudadanos […].



Artículo 4[1]. *Principios generales.*

f) Principio de **seguridad** en la implantación y utilización de los medios electrónicos por las Administraciones Públicas, en cuya virtud se exigirá al menos el mismo nivel de garantías y seguridad que se requiere para la utilización de medios no electrónicos en la actividad administrativa.

1. LEY 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos



Artículo 4. *Principios generales.*

g) Principio de **proporcionalidad** en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. Asimismo sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios en atención a la finalidad para la que se soliciten.

1. LEY 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos

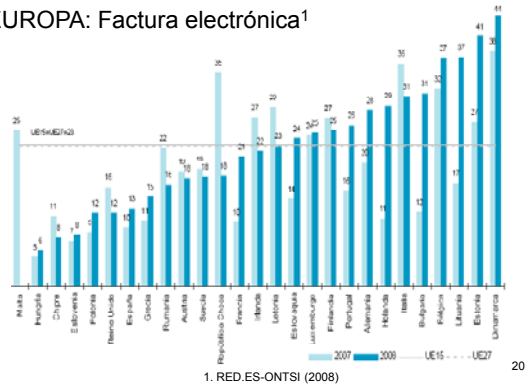
FACTURA ELECTRÓNICA[1]

[…]
A estos efectos, se entenderá que la factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la **autenticidad de su origen** y la **integridad de su contenido**, lo que impide el repudio de la factura por su emisor

1. LEY 56/07 Medidas Impulso S.I. (Art. 1)



EUROPA: Factura electrónica[1]




1. RED.ES-ONTSI (2008)

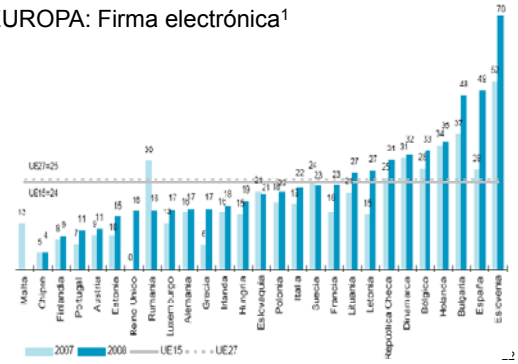
20



[…] en España se hacen unas **4.500 millones de facturas al año**, con un ahorro por factura, en el caso de hacerlas electrónicamente, de **3,4 euros**. Por tanto, la divulgación de la Factura Electrónica supone un ahorro potencial al año de más de 15.000 millones de euros para la economía española, un **1,5% del PIB** […]

[…] Con Facturae la Administración Pública crea un formato gratuito, abierto y con la garantía de la Agencia Tributaria y de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información […]

EUROPA: Firma electrónica[1]




1. RED.ES-ONTSI (2008)



**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

La seguridad de la información administrativa.

El cifrado de datos sensibles.

La firma digital.

Certificados digitales.



$\Delta$ Seguridad $\Rightarrow$ $\Delta$ Coste

$\nabla$ Rendimiento

$\nabla$ Usabilidad

24

SEGURIDAD

Objetiva

Subjetiva (Confianza)

25

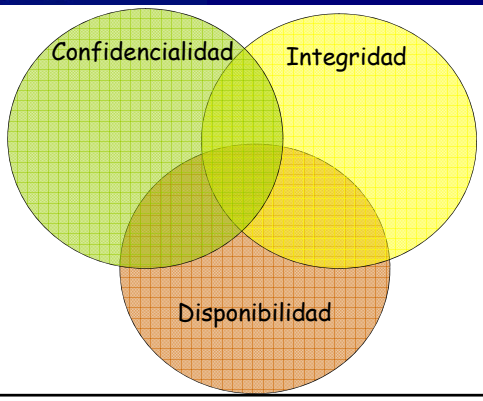


SEGURIDAD DE LOS DATOS

La seguridad de los datos trata de la protección de éstos frente a revelaciones accidentales o intencionadas a usuarios no autorizados, frente a modificaciones indebidas o frente a destrucciones.

26






27

MECANISMOS DE SEGURIDAD

- Autenticación
- Control de accesos
- Cifrado de datos
- Funciones resumen
- Firma digital
- Registro de auditoría

28



**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

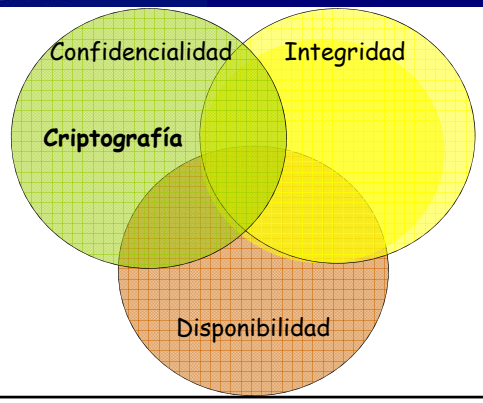
La seguridad de la información administrativa.
El cifrado de datos sensibles.
La firma digital.
Certificados digitales.



CRIPTOGRAFÍA

Disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado

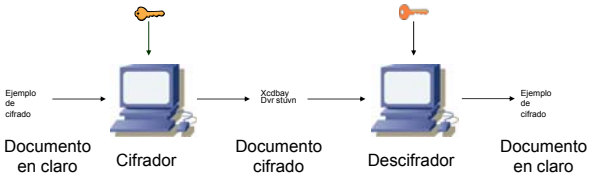
30




31



SISTEMA DE CIFRADO (Criptosistema)



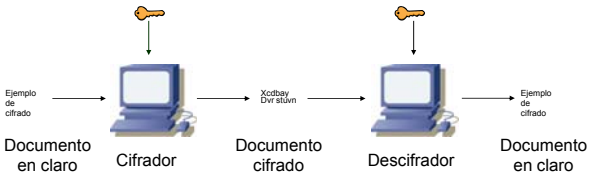

Clave de cifrado

Clave de descifrado

32



CRIPTOSISTEMA SIMÉTRICO (DE CLAVE SECRETA)




Clave de cifrado y descifrado

33

CRIPTOANÁLISIS

Análisis de un sistema criptográfico, sus entradas y salidas, o ambas, para obtener variables o datos sensibles, incluyendo el texto en claro





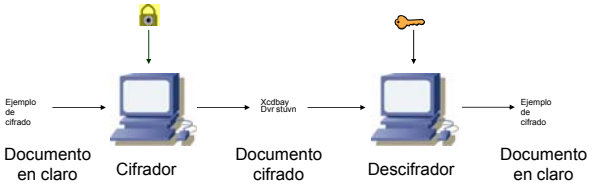
CRIPTOANÁLISIS: Principio de Kerckhoff (Auguste Kerckhoff , 1883)

La seguridad del cifrado debe de residir, exclusivamente, en el secreto de la clave





CRIPTOSISTEMA ASIMÉTRICO (DE CLAVE PÚBLICA)




Clave de cifrado (pública)

Clave de descifrado (privada)

SISTEMAS DE CIFRADO: Usos

- Simétrico o de clave secreta
  - Confidencialidad
- Asimétrico o de clave pública
  - No repudio (Firma digital)
  - Intercambio de claves secretas

37



LEY GRAL. DE TELECOMUNICACIONES[1]: Cifrado en las redes y servicios de comunicaciones electrónicas (Art. 36)

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado

1. Ley 32/03 de 3 de noviembre

38



LEY GRAL. DE TELECOMUNICACIONES[1]: Cifrado en las redes y servicios de comunicaciones electrónicas (Art. 36)

2. ... Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la AGE o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con a normativa vigente

1. Ley 32/03 de 3 de noviembre

39

CIFRADO DE LOS DATOS

Algoritmos de compresión

| | |
|---|---|
| WinRAR | AES 128 |
| WinZip | Algoritmo propietario |

Procesadores de textos

Microsoft Office Word

Adobe Acrobat Profesional



**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

La seguridad de la información administrativa.

El cifrado de datos sensibles.

La firma digital.

- Qué es.
- Qué efectos tiene.
- Como se realiza.

Certificados digitales.



NORMALIZACIÓN: Ámbito internacional

- Comisión Electrónica Internacional (*International Electrotechnical Commission,* IEC)
  - Normas sobre electrotecnia y electrónica
  - Países miembros ~ 60
- Organización Internacional de Normas. (*International Organization for Standardization*, ISO)
  - Normas resto de sectores de actividades
  - Países miembros ~ 130

42

NORMALIZACIÓN: Ámbito internacional

ISO e IEC elaboran conjuntamente las normas relativas a las T. I. (Joint Technical Comitee 1, JTC1)

http://www.iso.org/iso/jtc1_home.html



NORMALIZACIÓN: Ámbito internacional

Unión Internacional de las Telecomunicaciones (UIT)

- Sector telecomunicaciones (UIT-T)
  Antes: Comité Consultivo Internacional Telegráfico y telefónico (CCITT)
- Sector radiocomunicaciones (UIT-R)
  Antes: Comité Consultivo Internacional de Radiocomunicaciones (CCIR)
- Sector de desarrollo de las Telecomunicaciones (UIT-D)

44



ORGANISMOS NACIONALES DE NORMALIZACIÓN

| PAÍS | ORGANISMO |
|---|---|
| Alemania | Deutsches Institut für Normung (DIN) |
| España | Asociación Española de Normalización y Certificación (AENOR) |
| E U A | American National Standards Institute (ANSI) |
| Francia | Association Française de Normalisation (AFNOR) |
| Japón | Japanese Industrial Standars Committee (JISC) |
| Reino Unido | British Standards Institution (BS) |
| Rusia | Agencia Federal para la Regulación Técnica y la Metrología (GOST) |
| Suiza | Swiss Association for Standardization (SNV) |

ORGANISMOS NACIONALES DE NORMALIZACIÓN

| PAÍS | ORGANISMO |
|---|---|
| R. Panamá | Dción. Gral. Normas y Tecnología Industrial. Mterio Comercio e Industrias |
| México | Dirección General de Normas (DGN) |
| Chile | Instituto Nacional de Normalización (INN) |



ESTÁNDAR O NORMA DE FACTO

No consensuado ni legitimado por un organismo oficial de normalización

Aceptado y ampliamente utilizada por iniciativa propia de un gran número de interesados

Algunos acaban en estándares de iure

A menudo prevalecen sobre los de iure

Especialmente importantes en el ámbito de las T.I.



ESTÁNDAR O NORMA DE FACTO. Instituciones

- IETF (Internet Engineering Task Force)
  - RFC (Request for Comments)
- IEEE (Institute of Electrical and Electronics Engineers)
  - 802, 802.11, Posix, VHDL, …
- World Wide Web Consortium (W3C)
- ECMA (En origen: European Computer Manufacturers' Association)
  - ECMA 376 Office Open XML File Formats

FIRMA DIGITAL

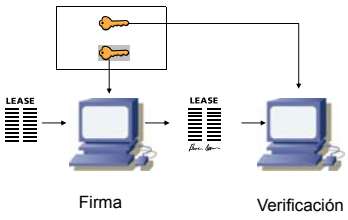
Transformación criptográfica de un conjunto de datos que lo protegen de falsificaciones y permiten al receptor de aquel conjunto probar su origen e integridad[1]

1. ISO/IEC 19790: 2006





FIRMA DIGITAL




Clave pública (Datos de verificación de firma)

Clave privada (Datos de creación de firma)





FUNCIÓN RESUMEN (HASH)[1]

Función matemática que transforma elementos de un conjunto, posiblemente muy grande, en elementos de otro conjunto mucho más pequeño

1. ISO/IEC 10181-2

FUNCIÓN RESUMEN (con clave)

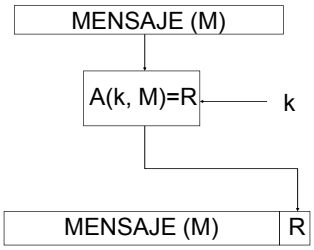
A(k, M) = R  M: preimagen de R

- A(k, M) es fácil de calcular
- R<< M
- $A^{-1}(k, R)$ es muy difícil de computar
- Si $R_1=A(k, M_1)$, es complejo hallar $M_2$/ $A(k, M_2) = R_2 = R_1$

52



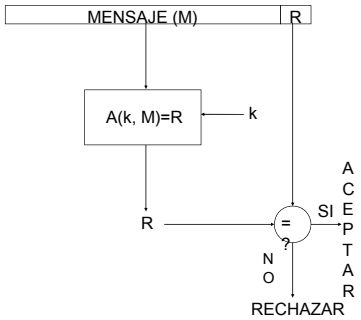
AUTENTICACIÓN (con clave): En el emisor




53



AUTENTICACIÓN (con clave): En el receptor



FUNCIÓN RESUMEN NIST

- SHA-0 NIST (FIPS 180), 1993
- SHA-1 NIST (FIPS 180-1), 1995
- SHA-2 NIST (FIPS 180-3), 2008

55



FUNCIÓN RESUMEN NIST

| Algorithm | Message Size (bits) | Block Size (bits) | Word Size (bits) | Message Digest Size (bits) |
|---|---|---|---|---|
| SHA-1 | $< 2^{64}$ | 512 | 32 | 160 |
| SHA-224 | $< 2^{64}$ | 512 | 32 | 224 |
| SHA-256 | $< 2^{64}$ | 512 | 32 | 256 |
| SHA-384 | $< 2^{128}$ | 1024 | 64 | 384 |
| SHA-512 | $< 2^{128}$ | 1024 | 64 | 512 |

56



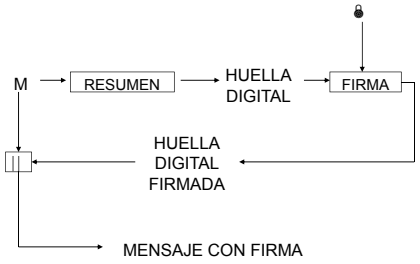
FIRMA DIGITAL

Datos añadidos a un conjunto de datos (o transformación criptográfica de éstos), que lo protegen de falsificaciones y permiten al receptor de aquel conjunto probar su origen e integridad[1]

1. ISO/IEC 19790: 2006

57

FIRMA DIGITAL: Separada del mensaje




58



SEGURIDAD EN XML

XML Encryption

- Entidad normalizadora. W3C (WG XML-Enc)
- Permite cifrar documentos enteros o sólo partes
- Permite cifrar distintos formatos: HTML, XML, datos binarios, etc.
- Se pueden anidar cifrados o firmas

59



SEGURIDAD EN XML

XML Signature

- Entidad normalizadora. W3C (WG XML-DSig) y ETSI
- Permite cifrar documentos enteros o sólo partes
- Permite cifrar distintos formatos: HTML, XML, datos binarios, etc.
- Se pueden anidar cifrados o firmas

60

XAdES: Formatos

- XAdES-BES (Basic Electronic Signature)
- XAdES-EPES (Explicit Policy Electronic Signature)
- XAdES-T (with Time Stamp)
- XAdES-C (Complete Validation Data)
- Opcionales (anexos):
  - XAdES-X (Extended Validation Data)
  - XAdES-XL (Extended Long Validation Data)
  - XAdES-A (Archival)

61



SEGURIDAD EN XML

XML Encryption

XML Signature

XML Key Management

Protocolo de distribución y registro de claves públicas

X-KRSS. Registro de clave pública

X-KISS. Información de la clave pública

62



FORMATOS DE FIRMA

- PKCS#7
- CMS (RFC 2630)
- S/MIME
- XML Signature

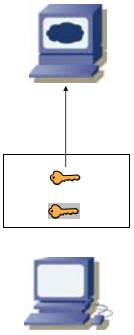
63

**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

La seguridad de la información administrativa.
El cifrado de datos sensibles.
La firma digital.
Certificados digitales.
- Funciones.
- Tipos: personal, de servidor, …
- Contenido.
- Formatos.



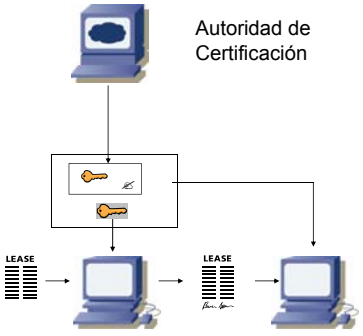
CERTIFICADO DE CLAVE PÚBLICA




65



CERTIFICADO DE CLAVE PÚBLICA




66

FIRMA DIGITAL: Almacenamiento del certificado y la clave privada

- En un fichero
- En una tarjeta de circuito integrado (tarjeta chip)





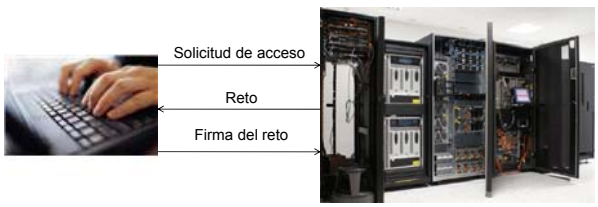
CERTIFICADO DIGITAL: ITU-T. X 509 v.3

```
Certificate             ::= SIGNED { SEQUENCE {
   Version                    Version,
   serialNumber               CertificateSerialNumber,
   signature                  AlgorithmIdentifier,
   issuer                     Name,
   validity                   Validity,
   subject                    Name,
   subjectPublicKeyInfo       SubjectPublicKeyInfo,
   issuerUniqueIdentifier     IMPLICIT UniqueIdentifier OPTIONAL,
   subjectUniqueIdentifier    IMPLICIT UniqueIdentifier OPTIONAL,
   extensions                 Extensions OPTIONAL }
```





AUTENTICACIÓN MEDIANTE LA FIRMA



CERTIFICADO DIGITAL: Extensiones

- Acerca del uso de las claves
- Acerca de las políticas de certificación
- Acerca de los atributos del titular y de la AC
- Acerca de las rutas de certificación
- Acerca de los puntos de distribución

70



CERTIFICADO DIGITAL: Uso de la clave

- Cifrado de datos (confidencialidad)
- Firma digital (integridad, no repudio)
- Autenticación

71



CERTIFICADO DIGITAL: Extensiones (uso de claves)[1]

KeyUsage ::= BIT STRING {
digitalSignature (0),
nonRepudiation (1), (renombrada contentCommitment)
keyEncipherment (2),
dataEncipherment (3),
keyAgreement (4),
keyCertSign (5),
cRLSign (6),
encipherOnly (7),
decipherOnly (8) }

ITU-T X.509 v.3

72

CERTIFICADOS RECONOCIDOS: Normas técnicas

ETSI TS 101 862: Perfil de Certificados Reconocidos

RFC 3739 Internet X.509 PKI: Perfil de Certificados Reconocidos

73



CERTIFICADO DIGITAL: Tipos

- Certificado de Autoridad de certificación
- Certificado de servidor (sede electrónica)
- Certificado de editor de software
- Certificado personal

74



CERTIFICADO DE ATRIBUTOS: Contenido

- Identificación del usuario
- Nombre de la Autoridad de Atributos (AA)
- Algoritmo de firma de la AA
- Periodo de vigencia
- Atributos

•Extensiones

75

**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

Autoridades de Certificación
- Funciones.
- Tipos de Autoridades de certificación.
- Revocación de certificados.
- La constancia fiable de tiempo: sellos de tiempo y Autoridades de sellado

Infraestructuras de clave Pública (PKI).

La firma digital. Validez legal en España y en la Unión Europea.



AUTORIDADES DE CERTIFICACIÓN

- Generación y emisión de certificados
- Revocación, suspensión, renovación y recuperación
- Generación de claves (ocasionalmente)
- Almacenamiento certificados (ocasionalmente)
- Mantenimiento de la CRL (ocasionalmente)
- Traslado de los certificados

77

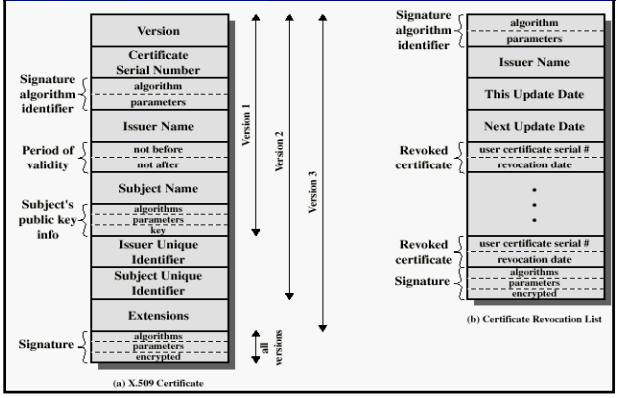


CERTIFICADO DIGITAL: Consulta de validez (Autoridades de validación)

- CRL (*Certificate Revocation Lists*)
  - ITU-T: X.509 v.3
- OCSP (*On-line Certificate Status Protocol*)
  - IETF: RFC 2560

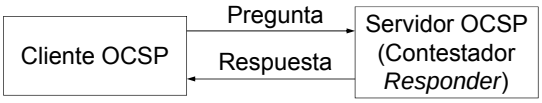
78

Formato X.509: Certificado y CRL






OCSP: Pregunta y respuesta



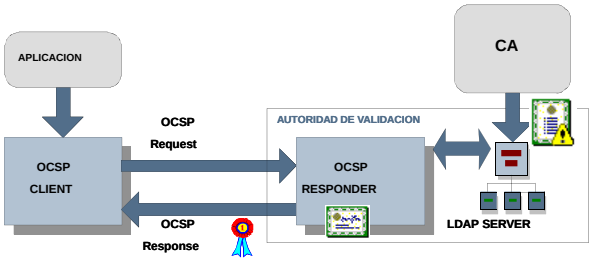

Contestador (*Responder*)

- AC emisora del certificado o un Tercero de Confianza acreditado para este fin por aquella
- Un Tercero de Confianza para el cliente

80



OCSP: Esquema general




81

OCSP frente a CRL

- Proporciona información reciente del estado del certificado.
- Elimina la necesidad de procesar las CRL´s
- Las CRL´s contienen información sensible
- Permite la verificación a posteriori de la validez de las firmas, sin archivar las CRLs.

82



CERTIFICADOS DIGITALES: CRL

- Emisor
- Algoritmo de firma de la AC
- Fecha de actualización
- Próxima actualización
- Certificados revocados
- Fecha y hora de revocación
- Extensiones

83



TERCEROS DE CONFIANZA (Trusted Third Party, TTP)

SERVICIOS

- Certificación de claves
- Fechado digital
- Notificaciones electrónicas
- Custodia de documentos
- Custodia de claves (depositadas o de recuperación)
- Directorio de claves

84

SELLADO DE TIEMPO

Servicio que permite demostrar que un conjunto de datos existía con anterioridad a un instante, habiendose mantenido inalterado desde entonces.

Se puede usar, por ejemplo, para verificar que un documento fue firmado previamente a la revocación del correspondiente certificado, para probar que un mensaje se remitió antes de expirar un cierto plazo, etc.

Este servicio está establecido en la RFC 3161.

85



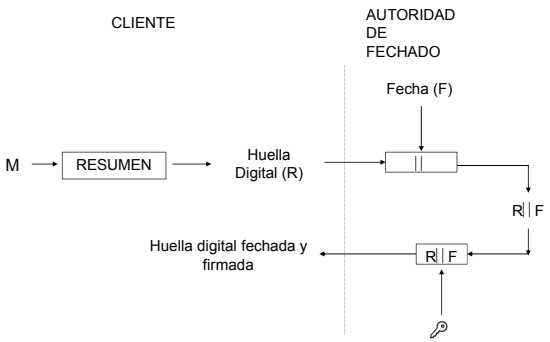
SERVICIO DE FECHADO: Técnicas

- Firma electrónica
- Registros encadenados
- Almacén de confianza

86



FECHADO: Firma electrónica



SERVICIO DE FECHADO: Normas

- ETSI TS 102 023: Policy requirements for time-stamping authorities
- ETSI TS 101 861: Time stamping profile
- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

88



**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

Autoridades de Certificación

Infraestructuras de clave Pública (PKI).

Estructuración de las Autoridades de certificación.

Autoridades de validación. El caso de la Administración Pública española: La plataforma @firma.

La firma digital. Validez legal en España y en la Unión Europea.

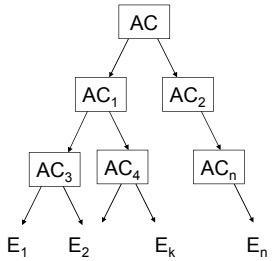


INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

Conjunto de autoridades de certificación, de registro, de sellado de tiempo, etc., así como las reglas de estructuración de éstas, y sus métodos de gestión de certificados, que establecen la validez de éstos y garantizan el reconocimiento mutuo de los mismos

90

PKI: Estructura jerárquica descendente




91



AUTORIDADES DE REGISTRO[1]

- Identificación peticionarios
- Remisión información a AC
- Recepción de los certificados emitidos por la AC
- Aceptación y traslado a AC de peticiones de suspensión, revocación y cambio de atributos

1. Oficinas de acreditación



POLÍTICA Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

¿qué se necesita hacer?

Política de seguridad

¿cómo se va a hacer?

Declaración de prácticas de certificación

93

POLÍTICA DE CERTIFICACIÓN[1]

Conjunto de reglas que establecen la adecuación de un certificado a una comunidad particular y a una clase de aplicaciones con requisitos comunes de seguridad

1. X 509 y RFC 2527





DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Documento publicado por una AC que comprende las normas, reglas y procedimientos que rigen el ciclo de vida de los certificados que expide. Además, incluye las obligaciones que contrae con los titulares de sus certificados, y de éstos con aquélla, y los márgenes de responsabilidad que asume frente a las entidades que aceptan dichos certificados





**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

Autoridades de Certificación

Infraestructuras de clave Pública (PKI).

La firma digital. Validez legal en España y en la Unión Europea.

LEGISLACIÓN

- Real Decreto-Ley 14/1999 sobre firma electrónica
- Ley modelo de la CNUDMI sobre las firmas electrónicas (2001)
- Directiva 1999/93/CE del P. E. y del Consejo por la que se establece un marco comunitario para la firma electrónica
- Ley 59/2003 sobre firma electrónica



Firma electrónica y documentos firmados electrónicamente (Art. 3)

1. 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

98



Esto es una prueba de firma electrónica.

Madrid, octubre de 2008

Fdo. Arturo Ribagorda Garnacho

Universidad Carlos III de Madrid

99

Firma electrónica y documentos firmados electrónicamente (art. 3)

2. 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

100



Prestadores de servicios de certificación (Art. 2.2)

Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica

101



Concepto de certificado electrónico y de firmante (Art. 6)

1. Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma *(clave pública)* a un signatario y confirma su identidad

102

Concepto de certificado electrónico y de firmante (Art. 6)

2. El firmante es la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa

103



Concepto y contenido de los certificados reconocidos (Art. 11)

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten

104



Certificados reconocidos (Art. 11)

2. Los certificados reconocidos incluirán, al menos:

a) La indicación de que se expiden como tales
b) El código identificativo único del certificado
c) La identificación del PSC que lo emite y su domicilio
d) La firma electrónica avanzada del PSC que lo expide
e) La identificación del firmante (personas físicas: nombre, apellidos y NIF, o seudónimo; personas jurídicas: denominación o razón social y CIF)

105

Certificados reconocidos (Art. 11)

f) Los datos de verificación de firma que corresponden a los datos de creación de firma que se encuentran bajo el control del firmante
g) Comienzo y fin del periodo de validez del certificado
h) Limites de uso del certificado, si se establecen
i) Limites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen

106



Extinción de la vigencia (Art. 8)

2. El periodo de validez de los certificados electrónicos será adecuado a los características y tecnología empleada en la generar los datos de creación de firma. En el caso de los certificados reconocidos este periodo no podrá ser superior a cuatro años

107



Certificados reconocidos (Art. 11)

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite

108

Firma electrónica y documentos firmados electrónicamente (Art. 3)

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

109



Firma electrónica y documentos firmados electrónicamente (Art. 3)

4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel

110



Firma electrónica y documentos firmados electrónicamente (art. 3)

10. A los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas.

111

– The European Telecommunication Standards Institute (ETSI)

– The European Standardization Committee (CEN)

112



ETSI TS 101 456: Requisitos de Políticas para AC que emiten certificados reconocidos

ETSI TS 102 042: Requisitos de Políticas para AC que emiten certificados de clave pública

113



ETSI TS 101 862: Perfil de Certificados Reconocidos

RFC 3739 Internet X.509 PKI: Perfil de Certificados Reconocidos

114

ETSI TS 101 456 *Policy requirements for certification authorities issuing qualified certificates*

(*European Telecommunications Standard Institute*)

- Certificados que requieren dispositivos de firma seguros (OID 0.4.0.1456.1.1)
- Certificados que no requieren dispositivos de firma seguros (OID 0.4.0.1456.1.2)

115



Anexo II f de la Directiva 1999/93/CE. Decisión de la C.E. C(2003) 2439

Security requirements for trustworthy systems managing certificates for electronic signatures

• Part 1: System Security Requirements. CWA 14167-1, marzo de 2003. (CEN Comité Europeo de Normalización)

• Part 2: Cryptographic module for CSP signing operations. Protection Profile (MCSO-PP). CWA 14167-2, marzo de 2002. (CEN Comité Europeo de Normalización)

116



Anexo III de la Directiva 1999/93/CE (Decisión de la Comisión C(2003) 2439)

Secure signature-creation devices. CWA 14169, marzo de 2002. (CEN Comité Europeo de Normalización)

Aprobada como norma española: UNE-CWA 2005

117

Disposiciones comunes a la extinción y suspensión de la vigencia de los certificados electrónicos[1] (Art. 10)

4. La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el servicio de consulta sobre vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su periodo de validez

118



Obligaciones de los PSC que expidan certificados electrónicos. (Art. 18)

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados

119



Obligaciones de los PSC que expidan certificados electrónicos.[1] (Art. 18)

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro

120

**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

La identidad digital. Tarjetas e-ID (sanitaria, permiso de circulación, …). El documento nacional de identidad electrónico español.

La firma y los certificados en la informatización de las Administraciones. El caso español: La Ley 11/2007 de Acceso electrónico de los ciudadanos a las AA PP y su Reglamento de desarrollo.

Desarrollos legales en la protección de los datos personales.

Universidad Carlos III de Madrid www.uc3m.es
Firma digital y certificados en las AA PP

**LA FIRMA DIGITAL Y LOS CERTIFICADOS EN LAS AA PP**

La identidad digital. Tarjetas e-ID (sanitaria, permiso de circulación, …). El documento nacional de identidad electrónico español.

La firma y los certificados en la informatización de las Administraciones. El caso español: La Ley 11/2007 de Acceso electrónico de los ciudadanos a las AA PP y su Reglamento de desarrollo.

Desarrollos legales en la protección de los datos personales.

Universidad Carlos III de Madrid www.uc3m.es
Firma digital y certificados en las AA PP

LEGISLACIÓN

- Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos
- Real Decreto 1671/2009 por el que se desarrolla parcialmente la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 56/2007 de Medidas de impulso de la sociedad de la información

Artículo 13. Formas de identificación y autenticación

2. Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las AA PP, de acuerdo con lo que cada Administración determine:

a) En todo caso, los sistemas de firma electrónica incorporados al DNI, para personas físicas.

[…]



Artículo 13. Formas de identificación y autenticación

b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las AA PP.

c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen



Artículo 15. Utilización de sistemas de firma electrónica avanzada.

1. Los ciudadanos, además de los sistemas de firma electrónica incorporados al DNI, […], podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos.

2. La relación de sistemas de firma electrónica avanzada admitidos, con carácter general, en el ámbito de cada A P, deberá ser pública y accesible por medios electrónicos. […]

Artículo 16. Utilización de otros sistemas de firma electrónica.

1. Las AA PP podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, tales como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.



Artículo 18. Sistemas de firma electrónica para la actuación administrativa automatizada.

1. Para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:



Artículo 18. Sistemas de firma electrónica para la actuación administrativa automatizada.

1. a) Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

Artículo 19. Firma electrónica del personal al servicio de las Administraciones Públicas.

2. Cada A. P. podrá proveer a su personal de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

3. La firma electrónica basada en el DNI podrá utilizarse a los efectos de este artículo.





Artículo 25. Plataformas de verificación de certificados y sistema nacional de verificación.

1. El Ministerio de la Presidencia gestionará una plataforma de verificación del estado de revocación de los certificados admitidos en el ámbito de la A. G. E. y […]. Esta plataforma permitirá verificar el estado de revocación y el contenido de los certificados y prestará el servicio de forma libre y gratuita a todas las Administraciones públicas, españolas o europeas.

R.D. 1671/2009





PLATAFORMA @FIRMA

- Servicios
  - Validación de certificados de múltiples PSC
  - Validación de firmas
  - Sellado de tiempo (según RFC 3161)
  - Cliente de firma (para firma de los ciudadanos)
- Requisitos de integración
  - Conexión a la red SARA

DNI electrónico[1]. Artículo 1. Naturaleza y funciones

5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel

Real Decreto 1553/2005



DNI electrónico[1]. Artículo 3. Órgano competente para la expedición y gestión

2. El ejercicio de las competencias a que se refiere el apartado anterior, incluida la emisión de los certificados de firma electrónica reconocidos, será realizado por la Dirección General de la Policía, a quien corresponderá también la custodia y responsabilidad de los archivos y ficheros, automatizados o no, relacionados con el Documento Nacional de Identidad

Real Decreto 1553/2005



DNI electrónico[1]. Artículo 9. Entrega del Documento Nacional de Identidad

2. La activación de la utilidad informática a que se refiere el artículo 1.4, que tendrá carácter voluntario, se llevará a cabo mediante una clave personal secreta, que el titular del Documento Nacional de Identidad podrá introducir reservadamente en el sistema

Real Decreto 1553/2005

DNI electrónico[1]. Artículo 11. Contenido

4. El chip incorporado a la tarjeta soporte contendrá:

Datos de filiación del titular

Imagen digitalizada de la fotografía

Imagen digitalizada de la firma manuscrita

Plantilla de la impresión dactilar del dedo índice de la mano derecha o, en su caso, del que corresponda según lo indicado en el artículo 5.3 de este R. D. Real Decreto 1553/2005



Artículo. La sede electrónica

1. La sede electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias.



Artículo 10. La sede electrónica

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

Artículo 13. Formas de identificación y autenticación

3. Las AA PP podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:
a)Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras

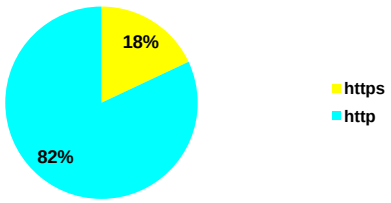


Artículo 17. Identificación de las sedes electrónicas.

Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.



AGE: Conexiones https frente a http[1]




Informe REINA 09 141

Artículo 13[1]. Formas de identificación y autenticación

3. […]
b) Sistemas de firma electrónica para la actuación administrativa automatizada.
c) Firma electrónica del personal al servicio de las Administraciones Públicas.
d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.



Artículo 18[1]. Sistemas de firma electrónica para la actuación administrativa automatizada.

1. Para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:



Artículo 18[1]. Sistemas de firma electrónica para la actuación administrativa automatizada.

1. a) Sello electrónico de Administración Pública, órgano o entidad de derecho público, basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

144

Artículo 18[1]. Sistemas de firma electrónica para la actuación administrativa automatizada.

1. b) Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

145



Artículo 18[1]. Sistemas de firma electrónica para la actuación administrativa automatizada.

3. La relación de sellos electrónicos utilizados por cada A. P., incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada A. P. adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

146



DNI electrónico[1]. Artículo 11. Contenido

4. (continuación)

Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez

Claves privadas necesarias para la activación de los certificados mencionados anteriormente

Real Decreto 1553/2005

DNI electrónico[1]. Artículo 12. Validez de los certificados electrónicos

1. Con independencia de lo que establece el artículo 6.1 sobre la validez del DNI, los certificados electrónicos reconocidos incorporados al mismo tendrán un período de vigencia de treinta meses.

A la extinción de la vigencia […], podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del DNI mientras dicho Documento continúe vigente

Real Decreto 1553/2005



Empleo de la firma electrónica en el ámbito de las AA. PP.[1] (Art. 4)

1. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que está asociada

149



ANEXO[1]: Definiciones

s) Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

150

AGE: Empleados/firma electrónica avanzada[1]

Tabla 8-4 1-1-2009

| Ministerios | Nº Empleados con firma elect. | % sobre el total de Empleados Públicos |
|---|---|---|
| Industria,Turismo y Comercio | 6.317 | 100% |
| Vivienda | 400 | 76% |
| Administraciones Públicas | 6.309 | 60% |
| Interior | 80.251 | 48% |
| Presidencia | 1.460 | 40% |
| Sanidad y Consumo | 1.216 | 32% |
| Economía y Hacienda | 9.725 | 20% |
| Justicia | 4.931 | 19% |
| Trabajo e Inmigración | 8.905 | 19% |
| Cultura | 931 | 18% |
| Defensa | 25.542 | 17% |
| Igualdad (2) | 22 | 6% |
| Asuntos Exteriores y Cooperación | 327 | 4% |
| Medio Ambiente y Medio Rural y Marino | 315 | 3% |
| Ciencia e Innovación (1) | 244 | 2% |
| Fomento | 583 | 1% |
| Educación, Política Social y Deporte | 5 | 0% |
| Total | 147.483 | 27% |

Informe REINA 09



STORK (Secure Identity Across Borders Linked)

- Uso de DNI-e en todos los países de la Unión
- Participantes: 12 Estados de la UE más Islandia

152



AGENCIA ESPAÑOLA DE COOPERACIÓN INTERNACIONAL PARA EL DESARROLLO (AECID)

UNIVERSIDAD DE PANAMÁ

## La firma digital y las Administraciones Públicas

Arturo Ribagorda Garnacho
Catedrático de Universidad. Universidad Carlos III de Madrid