@firma

Iniciación a la Firma Electrónica y Tecnologías de PKI

10 de abril de 2007

INDICE

ÍNDICE

Criterios de Seguridad según B.O.E. 26-6-2003

Autenticación

• Identifica a las entidades implicadas en una transacción y **garantiza** que estas entidades son lo que dicen ser (emisor y receptor). También conocida como “Autenticación fuerte”. Necesita del establecimiento de un **Círculo de Confianza** y de una infraestructura de Certificación (PKI) que lo mantenga y lo gestione.

Integridad

• Garantía de que una información, o un conjunto de datos en general, no es modificado en el transcurso de la comunicación desde el generador al receptor.

No repudio

• Garantía de que el emisor es el autor de la transacción que ha sido firmada.

Confidencialidad

• Capacidad de mantener la información fuera del alcance de usuarios no autorizados. Para ello se utiliza el protocolo estándar Secure Socket Layer (SSL), que mediante técnicas criptográficas oculta el contenido de la información que viaja a través de la Red.

Firma Electrónica con Certificados X.509 v3

Cifrado

- Proceso mediante el cual una determinada información se ofusca por medio de un algoritmo determinado, haciendo uso de una clave conocida.

Tipos de claves

Claves Simétricas

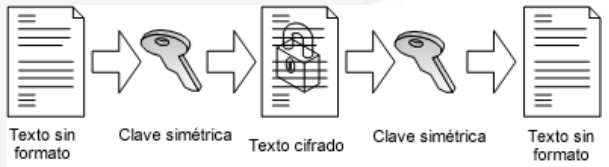
- Permiten cifrar y descifrar datos utilizando la misma clave.
- Se utilizan longitudes de clave cortas: 8, 16, 24 bits.

Claves Asimétricas

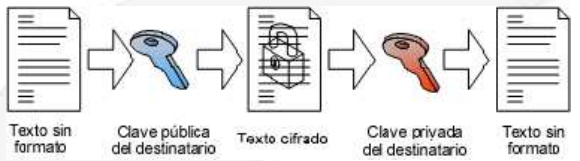
- Son claves complementarias. Solamente pueden ser generadas una a partir de la otra.
- Lo cifrado con una sólo puede descifrarse con su complementaria.
- Las claves se denominan respectivamente, pública y privada.
- La clave pública puede difundirse.
- La clave privada debe ser custodiada por su propietario.
- Longitudes de clave a partir de 512 bits (512, 1024, 2048, etc).

Tipos de cifrado

- **Cifrado simétrico (ej: 3DES, AES)**
  - Proceso eficiente
  - Misma clave para todo el proceso
  - Emisor y receptor deben conocer la clave



- **Cifrado asimétrico (ej: DSA, RSA)**
  - Proceso costoso
  - Intervienen claves asimétricas
  - La clave privada no se intercambia



- **Cifrado híbrido (ej: SSL)**
  - Aúna las ventajas de ambos
  - Eficiencia y seguridad

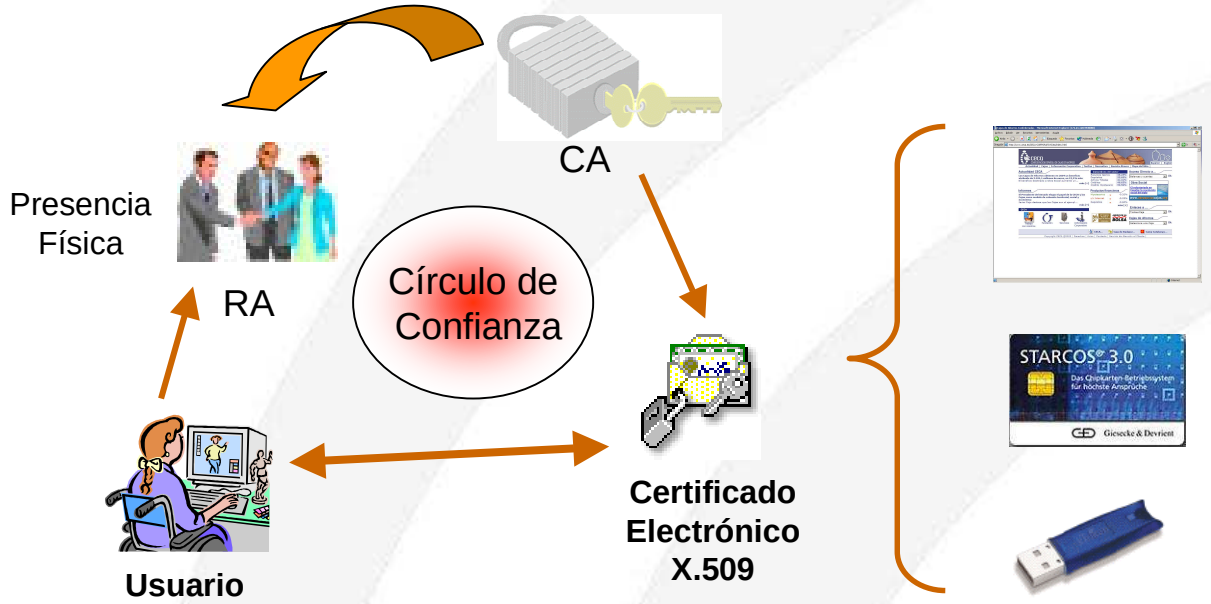
ÍNDICE

Definición Certificado Electrónico X.509

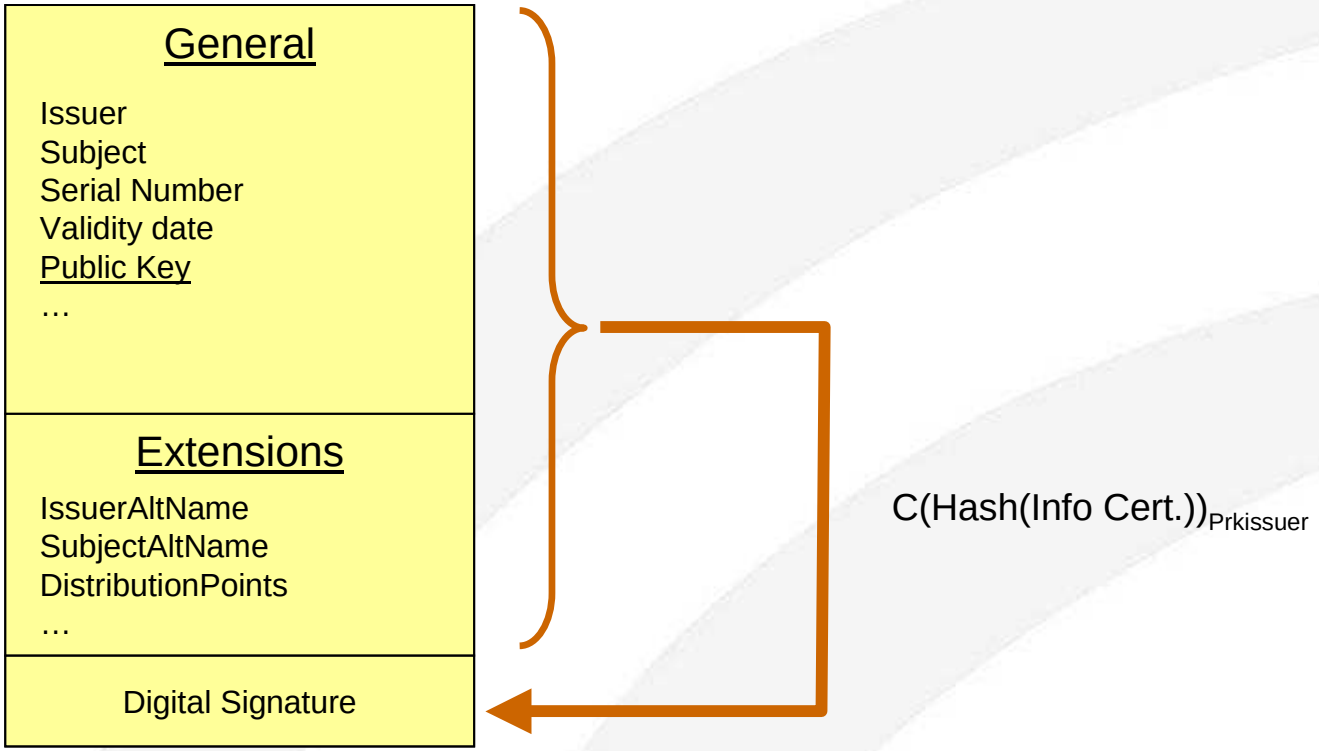
• Componentes basados en sistemas de clave pública que identifican de manera telemática a una persona física, jurídica o de representación.

• Son Emitidos por una Entidad de Certificación (CA) que garantiza la equivalencia “certificado <-> persona”. Exigen presencia física en las Autoridades de Registro (RA).

• Se almacenan en: “navegador, ficheros (formato pkcs#12) y en tokens criptográficos PKCS#15 (SmartCards, dispositivos USB, Software)”.



Estructura de un certificado digital X.509v3



Ciclo de Vida del Certificado Electrónico

• **Caducado**, cuando se ha superado la fecha de vigencia del certificado. Normalmente un certificado suele tener un período de vigencia de 2 a 3 años desde la fecha de emisión. En el caso de la FNMT, por ejemplo, son 2 años.

• **Revocado**, cuando ha sido rechazado, o bien por la Autoridad Certificadora que lo emite o bien por el propio titular. El motivo de la revocación es variado (extravío, robo, caducidad, certificado copiado por terceros, etc).

• **Suspendido,** cuando se ve afectado por una investigación o procedimiento judicial o administrativo, por lo que se procede a cancelar la validez del certificado durante un cierto período de tiempo, pudiendo volverse a levantar la suspensión dentro del período de validez del certificado.

• **Válido,** cuando no pertenece a ninguno de los estados anteriores.

Un certificado caducado, revocado o suspendido no tiene validez, por lo que las firmas realizadas con este tipo de certificados dejan de tener valor desde el momento de su revocación.

Tipos de Certificados Electrónicos

No existe un criterio estándar que nos permita clasificar de manera única todos los certificados disponibles en el mercado. La tipología de los certificados electrónicos varía en función de los PSCs que los emiten y gestionan. No obstante, podemos tomar la siguiente clasificación General:

1. **Certificados de Persona Física.** Ejem: Certificado de eDNI o de PF de FNMT.
2. **Certificados de Persona Jurídica o de Representación**. Ejem: certificado de pertenencia a organización.
3. **Certificados de Entidad.** Ejem: Certificado emitido a nombre de Consejería determinada.
4. **Certificados de Componentes**. Ejem: Certificado SSL o de firma de código.

ÍNDICE

Autoridades Certificadoras (CA's)

• Entidad que **emite el certificado**, previo visto bueno de la Autoridad Registradora.

• Proporciona las herramientas y servicios necesarios para gestionar su ciclo de vida: emisión, suspensión y revocación.

• Las Solicitudes de emisión de certificados pasan a ser gestionadas por las Autoridades Registradoras.

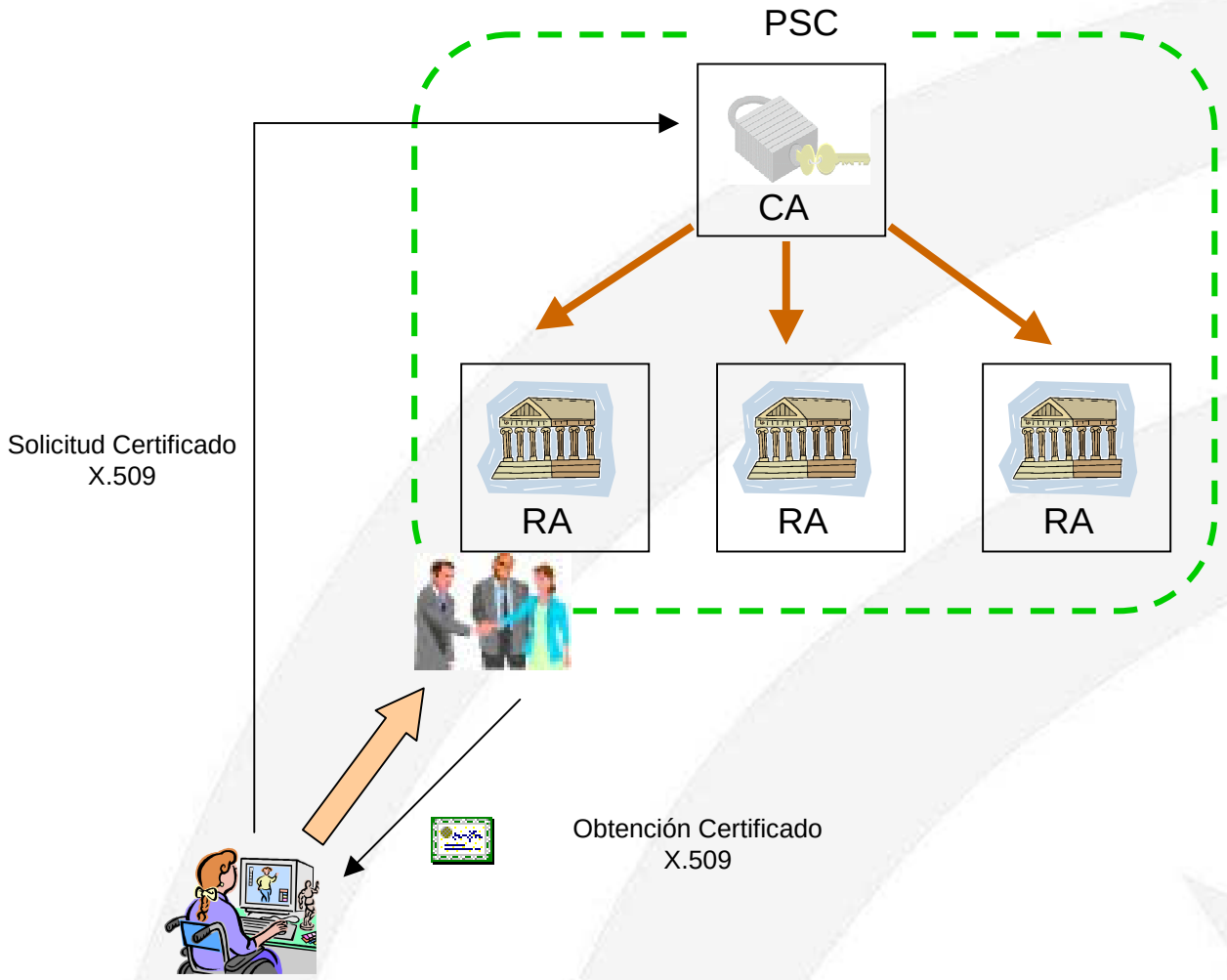
Autoridades Registradoras (RA's)

• Requiere presencia física del solicitante de un certificado en la Autoridad de Registro, donde a través de la documentación pertinente se verificará que el solicitante del certificado y la persona presentada son la misma persona y que la información es verídica.

• Son numerosas y dispersas geográficamente para facilitar la accesibilidad de los usuarios finales.

• Son formadas y certificadas por la Autoridad Certificadora que les proporciona una licencia de funcionamiento.

CAs y RAs


PSC
CA
RA
RA
RA
Solicitud Certificado
X.509
Obtención Certificado
X.509

ÍNDICE

Prestadores de Servicios de Certificación (PSCs)

- Son entidades que despliegan y mantienen Entornos de Confianza en ámbitos bien definidos
- Ponen a disposición de sus usuarios herramientas para solicitar la obtención de certificados digitales de forma telemática.
- Gestionan el ciclo de vida de los certificados electrónicos emitidos.
- Dan servicios de consulta de estado de certificados, Time Stamping, etc.
- Pueden poseer infraestructuras de Autoridad de Registro (RA), o delegar este servicio.
- Definen jerarquías de certificación que permiten dar servicio a sus usuarios.
- Definen sus políticas de funcionamiento en Documentos de Prácticas de Certificación (DPC).
- Ejemplos: FNMT, DGP (eDNI), Firma Profesional, etc.

Servicios de Certificación

•**Consulta de Estado de Certificados (CRLs).** La CA ha de publicar el estado de los certificados (válido, revocado, suspendido) mediante las herramientas y protocolos pertinentes.

- •**CRL (Certificate Revocation List)**
- •**OCSP (Online Certificate Status Protocol)**

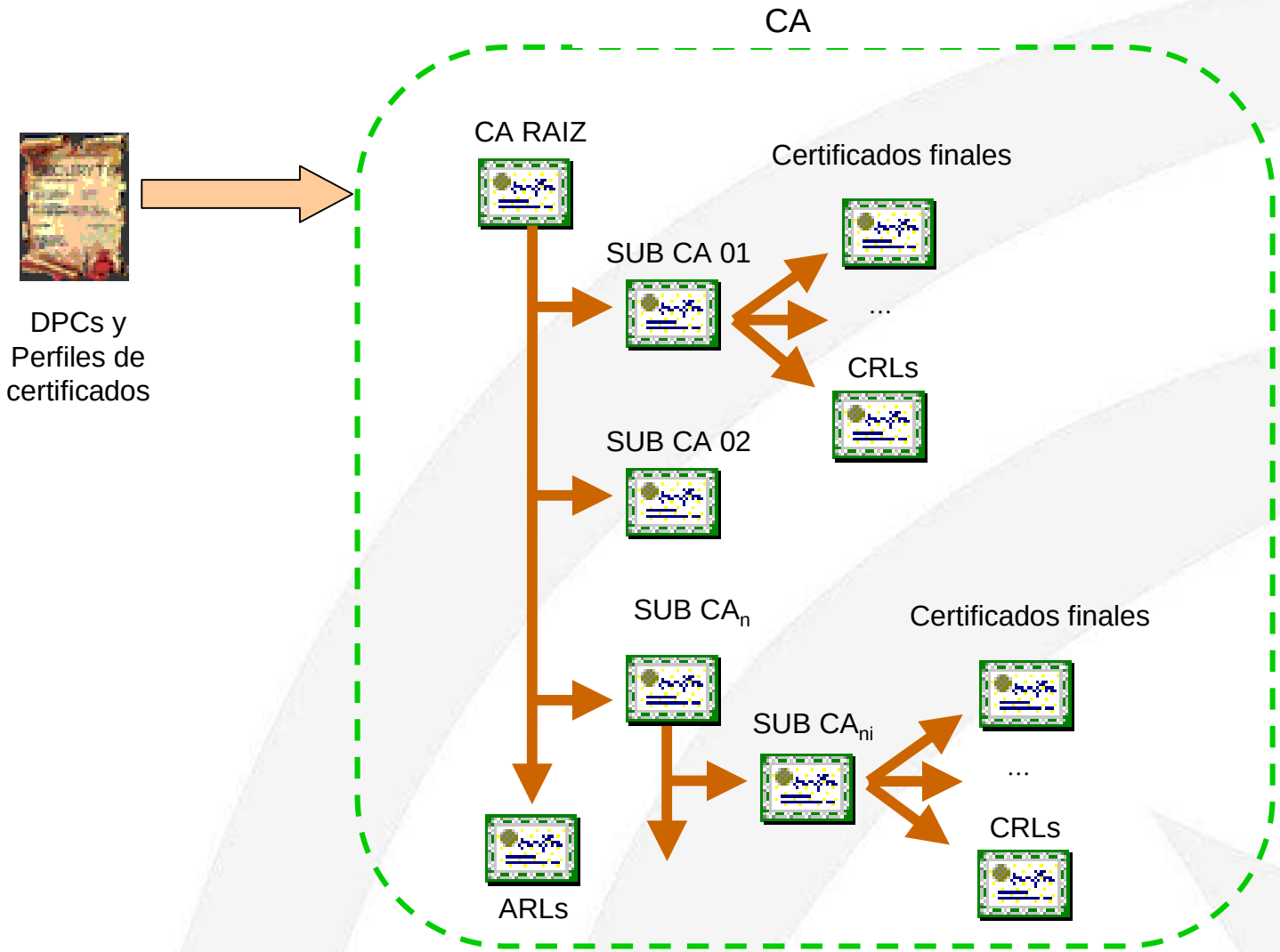
•**TimeStamping**. En toda transacción de firma se ha de constatar el instante de tiempo para que sea válida, y además ese instante de tiempo ha de estar acreditado por un Tercero de Confianza denominado Autoridad de Fechado Digital (TSA).

• **Certificación de RA's.** Formación y acreditación de Autoridades de Registro para la gestión de solicitudes de certificados. Se provee de las herramientas software y hardware necesarias a los registradores.

• **Custodia a largo plazo**. Almacenamiento y conservación de transacciones de firma en el tiempo proporcionando los métodos de disponibilidad pertinentes (según criterios de seguridad del BOE).

• **Outsourcing.** Suministro de servicios de CA para entidades privadas que lo necesiten. Incluyen un convenio de formación e implantación de RA's exclusivas para estas entidades privadas.

Jerarquías de certificación



Prestadores de Servicios de Certificación Reconocidos

Se denominan **Prestadores de Servicios de Certificación Reconocidos** a los PSCs admitidos por la ley 59/2003 de firma electrónica. El ministerio de Industria, Turismo y Comercio mantiene una lista de los PSC españoles reconocidos para trabajar con la Administración General del Estado (en adelante AGE) en la dirección:

http://www.mityc.es/DGDSI/Servicios/FirmaElectronica/Prestadores

Según la Ley 59/2003 **la equivalencia entre firma electrónica y firma manuscrita se da cuando la firma ha sido generada con un "certificado reconocido".** Los certificados reconocidos son los certificados emitidos por los PSCs Reconocidos publicados en la lista anterior.

El DNI-e

- Emitido por la Dirección General de la Policía (DGP) dependiente del Ministerio del Interior. Para ello, la DGP ha desplegado una infraestructura de PKI y se ha constituido como Prestador de Servicios de Certificación Reconocido.
- Su jerarquía de CAs está constituida por **un nodo raíz y tres sub-raíces** a partir de las cuales se generan los certificados correspondientes. Esta estructura de sub-raíces se incrementará conforme crezcan el número de DNI-e emitidos.
- Las CAs están ubicadas físicamente en el bunker del Escorial, sede oficial de la DGP. Las Autoridades de Registro (RAs) están constituidas por las comisarías expendedoras del DNI, distribuidas por toda la geografía española.
- **El DNI-e es pertenece a la clasificación de Persona Física**, no cubre la representación Jurídica.
- **Cada DNI-e contiene un par de certificados electrónicos: uno para autenticación y otro para firma electrónica.**

ÍNDICE

Validación de certificados (I)

¿Qué es la validación de un certificado?

Es la verificación de que el certificado es válido, integro y no ha sido comprometido.

¿Por qué se debe validar un certificado?

Es la forma de garantizar que en el momento de realizar una firma o una autenticación, el estado del certificado era válido y por lo tanto también la operación en la que participó.

¿Cómo se lleva a cabo?

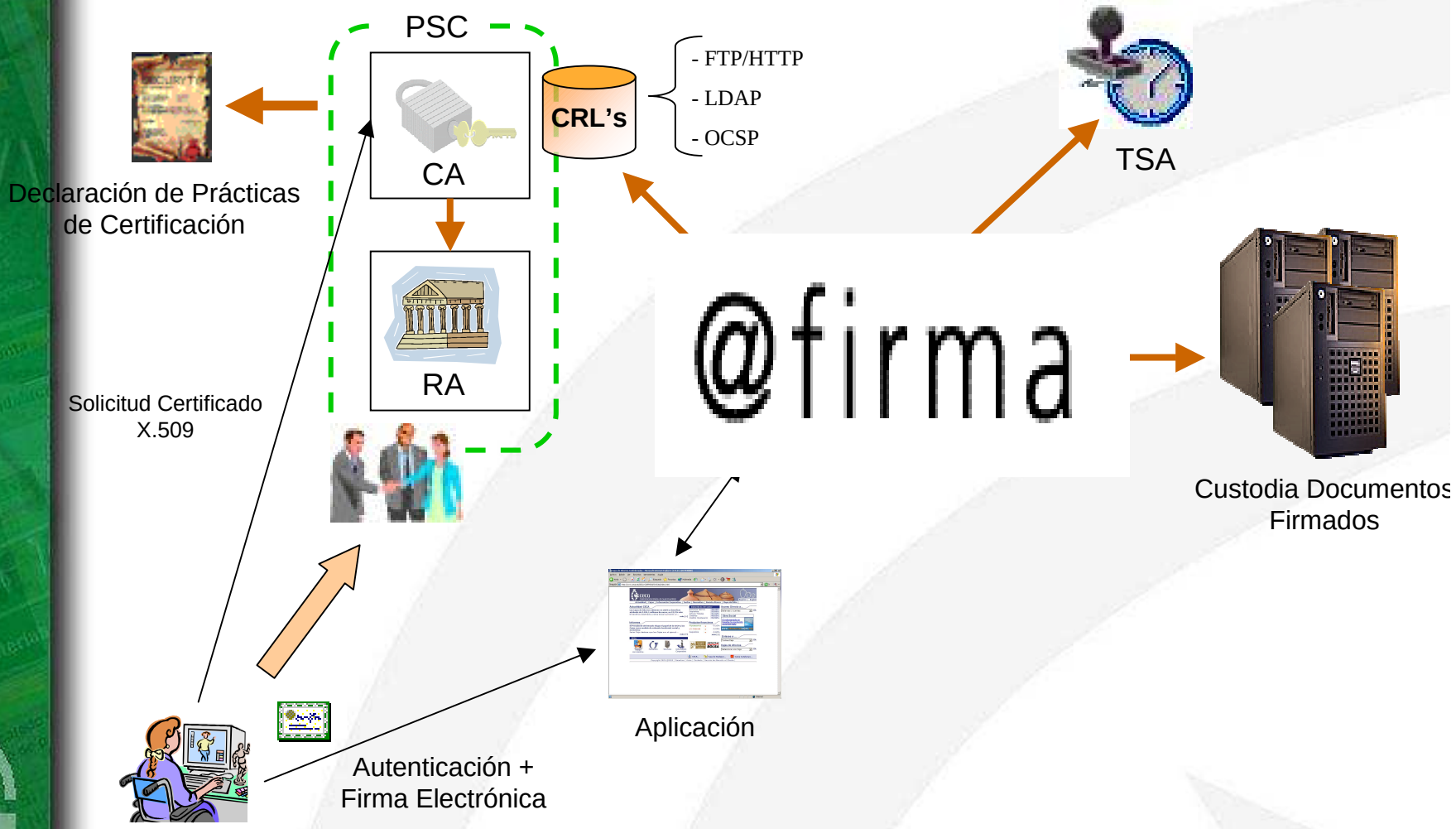
- **Validación de integridad del certificado**
  - Cumplimiento del estándar X.509v3
  - Fecha de caducidad.
  - Firma del emisor.
- **Consulta del estado del certificado**
  - Válido.
  - Revocado.
  - Suspendido.
- **Validación de la cadena de certificación**

Según RFC 3280

Validación de certificados (II). Métodos de consulta

- **CRL (Certificate Revocation List)**
  - Listas firmadas que publican los certificados comprometidos.
  - Son emitidas por el PSC emisor de los certificados.
  - Pueden ser completas, segmentadas, indirectas, etc.
  - Pueden ser publicadas por HTTP/S, LDAP, FTP, etc.
  - Tiempo de latencia alto.
- **OCSP (Online Certificate Status Protocol)**
  - Protocolo en línea para consulta de estado de certificados.
  - Es independiente del protocolo de comunicación.
  - Es el método más fiable.

@firma: Caso Práctico



ÍNDICE

Definición de Firma Electrónica

- Una firma electrónica es el resultado de aplicar una serie de operaciones criptográficas a una fuente de información (por ejemplo, un documento) utilizando para ello un certificado electrónico, para obtener dos cosas: la **Integridad** del documento firmado y el **No repudio** de la firma realizada.
- Pasos básicos de firma Electrónica:
  1. A partir del documento original se calcula un resumen mediante un algoritmo de HASH. Este “código hash” identifica de manera única el documento.
  2. Se accede al certificado del usuario para cifrar ese código hash con la clave privada. Al hacerlo se solicita la contraseña del certificado.
  3. Se firma el documento y se genera: “código hash encriptado” + certificado (sólo clave pública) + Documento Original = Firma Electrónica Avanzada.
  4. Verificación: a) Se calcula el código hash a partir del documento original, b) se desencripta el código hash encriptado con la clave pública del certificado utilizado, c) se comparan los códigos hashes de los apartados a) y b).

Tipos de Firma Electrónica

• Según el formato o estructura de firma electrónica:

- El ya obsoleto PKCS#7 y su evolución CMS mantenidas por el IETF .
- El también obsoleto formato en XML, XMLDSignature desarrollado por el W3C .
- La serie de nuevos formatos en XML, XAdES (XML Advance Electronic Signature) mantenidos por OASIS .
- Los nuevos formatos (poco maduros aún) CAdES (CMS Advance Electronic Signature).

Por otro lado, existen formatos de firma electrónica basados en formatos de documentos muy extendidos en el mercado. Ejemplos de estos formatos son:

- **Firma en PDF.** Desarrollada por Adobe y no es compatible hacia atrás en todas sus versiones. No obstante, incorpora la firma en el propio documento, la representación gráfica es bastante buena y está bastante extendido.
- **Firma en ODF** (Open Document Format). El formato ODF es utilizado por los paquetes ofimáticos OpenOffice y Staroffice. La firma electrónica en este formato está poco madura aún. Sigue la misma pauta de comportamiento que el formato PDF.

Tipos de Firma Electrónica

- Según la ubicación de la información firmada:
  - **Explícita.** Cuando la estructura de firma electrónica es independiente al documento firmado, es decir, se obtienen dos ficheros: uno con la firma y el documento original. Este tipo es el más utilizado, sobretodo en documentos de tamaño mediano-grande.
  - **Implícita.** Cuando la estructura de firma electrónica incorpora el documento firmado. Este formato se utiliza cuando los documentos a firmar son pequeños.
- Según la Jerarquía de la firma electrónica:
  - **Jerárquica o "counterSign".** Cuando la estructura de firma electrónica es secuencial y en cadena, es decir, antes de firmar una determinada persona ha de firmar otra previamente. Lo que realmente se firman son las firmas anteriores manifestando de alguna forma la conformidad con lo firmado.
  - **Paralela o "coSing".** Cuando en la estructura de firma electrónica no existe ni orden ni jerarquía, lo que realmente importa es que un conjunto de "n" personas firmen un mismo documento.

Tipos de Firma Electrónica

• Según la multiplicidad de la firma electrónica:

- **Simple.** Cuando en la estructura de firma electrónica solo existe un único firmante.
- **Mulfirma.** Cuando en la estructura de firma electrónica existen varios firmantes.

• Según la Ley 59/2003:

- **Reconocidas.** Estas firmas electrónicas son las únicas válidas legalmente ante terceros y equivalentes a la firma manuscrita tradicional. Una firma electrónica es reconocida cuando ha sido generada con un medio de creación de firmas seguro y utilizando un certificado electrónico reconocido .
- **No Reconocidas.** No tienen validez legal, aunque técnicamente se pueden probar que son fiables. Son generadas por certificados internos o de PSCs no reconocidos por la Administración Española.

Validación de la Firma Electrónica

Se puede dividir en tres fases a nivel global:

1. **Validación Básica.** Se verifica la integridad de la firma electrónica y que los datos firmados se corresponden con el original aportado en el proceso de validación.

2. **Validación del certificado empleado en la firma electrónica.** Este proceso es conlleva la validación del certificado electrónico contra el PSC correspondiente, tal y como se ha descrito en apartados anteriores.

3. **Validación del sello de tiempo.** Como es sabido todo certificado tiene asociado un estado de validez. Si una firma electrónica es realizada con un certificado válido en un instante de tiempo “X” y en el instante “X+Y” el certificado utilizado está revocado, al verificar la firma se verificaría también el certificado empleado obteniendo como resultado que está revocado y que la firma es incorrecta. Para evitar este inconveniente, todo proceso de firma electrónica necesita un elemento externo que permita verificar la validez de la firma: la fecha exacta en que se realizó.

Validación de la Firma Electrónica

Cuando se verifica una firma y se obtiene que el certificado está revocado, se comprueba si la fecha de revocación del certificado empleado es posterior a la fecha en que se realizó la firma, en cuyo caso se constataría que el certificado no estaba revocado en ese momento y la firma sería válida.

Por este motivo **toda firma electrónica debe tener un fechado electrónico**, denominado técnicamente como TimeStamping, obtenido de una fuente de tiempos segura que certifique que ese instante de tiempo es seguro e inalterable. La entidad que certifica que el instante de tiempos es seguro se denomina Autoridad de Fechado Electrónico (TimeStamping Authority, TSA).

ÍNDICE

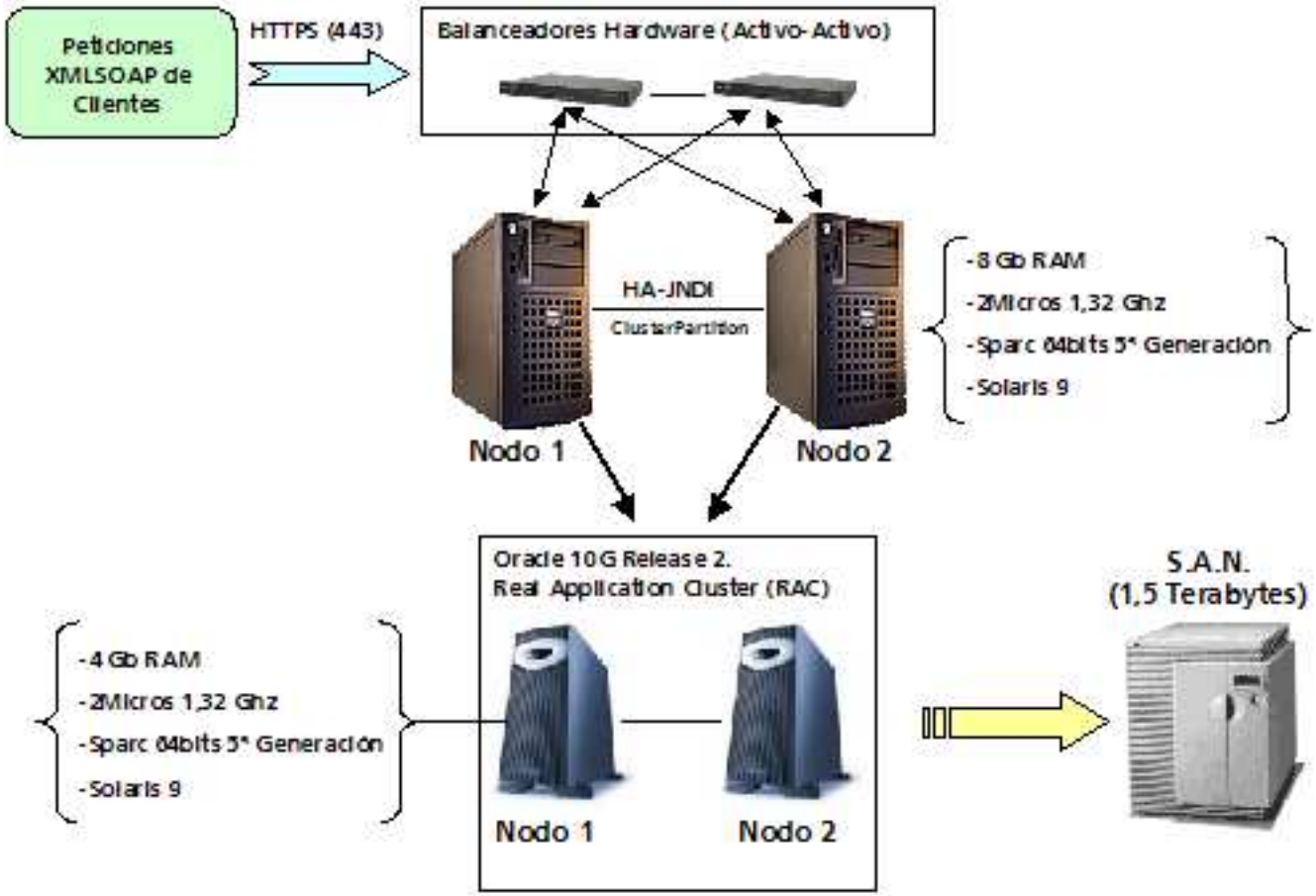
Introducción

- ¿Qué es @firma?

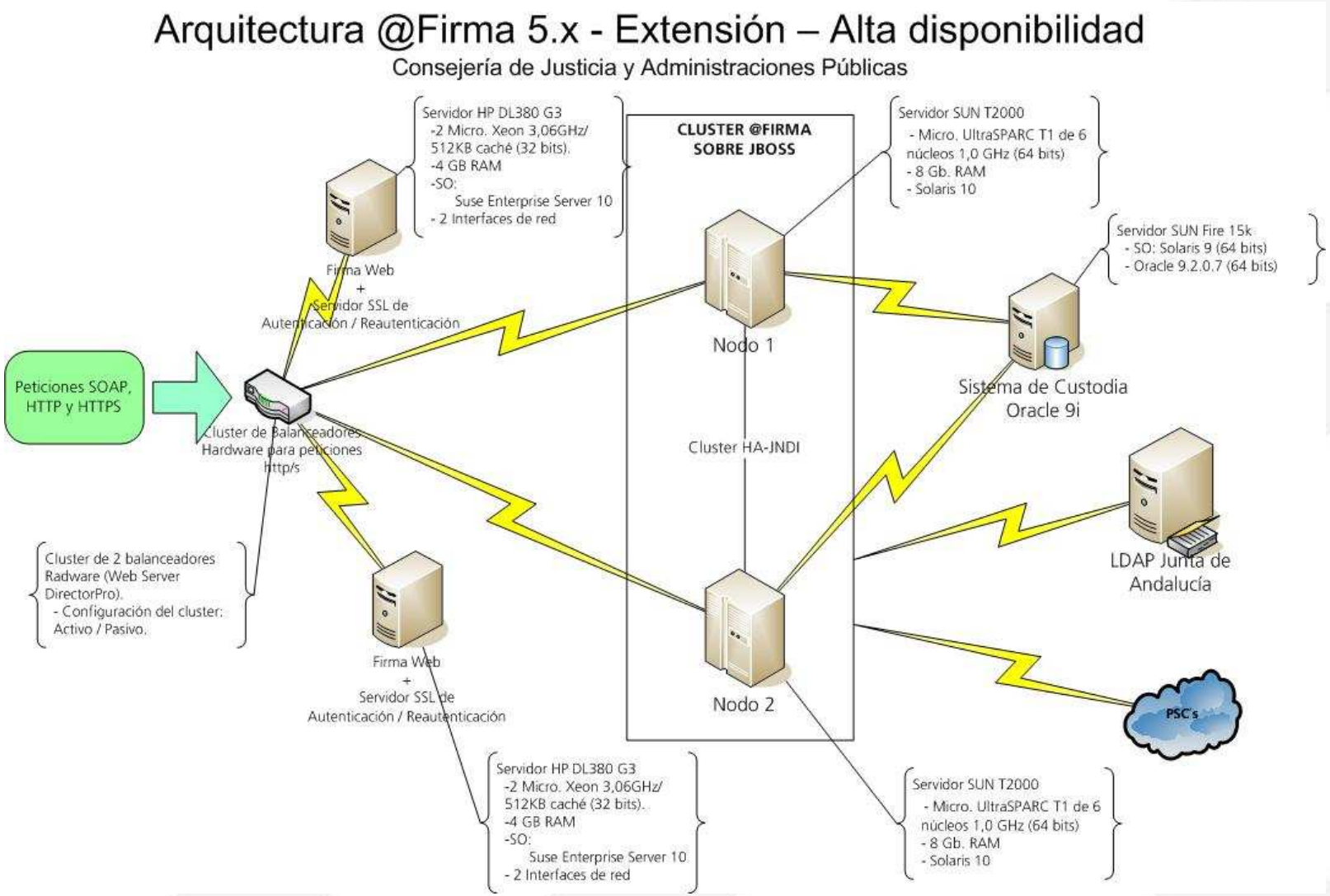
  Es una plataforma electrónica que utiliza certificados digitales X.509 v3 según las principales recomendaciones y estándares internacionales (RFC 2360, 3280, ETSI TS 101 733 v1.5.1, etc.) para la generación y validación de firmas digitales en múltiples formatos (CMS, XADES, XMLDSignature…), así como la validación avanzada de certificados digitales para garantizar en todo momento la integridad y validez de los mismos en el momento de la realización de una firma

- Versiones de @firma
  - V3.x (Fielato, Consejería de Hacienda)
  - V4.x (Junta de Andalucía, C. Justicia, C. Medio Ambiente, etc.)
  - V5.x (Ministerio de Administraciones Públicas)
- ¿Por qué existe una Extensión para la migración entre versiones?
  - Redefinición del sistema de gestión de CAs o PSCs.
  - Modificación de las interfaces de acceso WS, y eliminación de los RMI
  - Eliminación de determinados tipos de firma en el servidor (firma web).
  - Modificación de la BD de custodia.

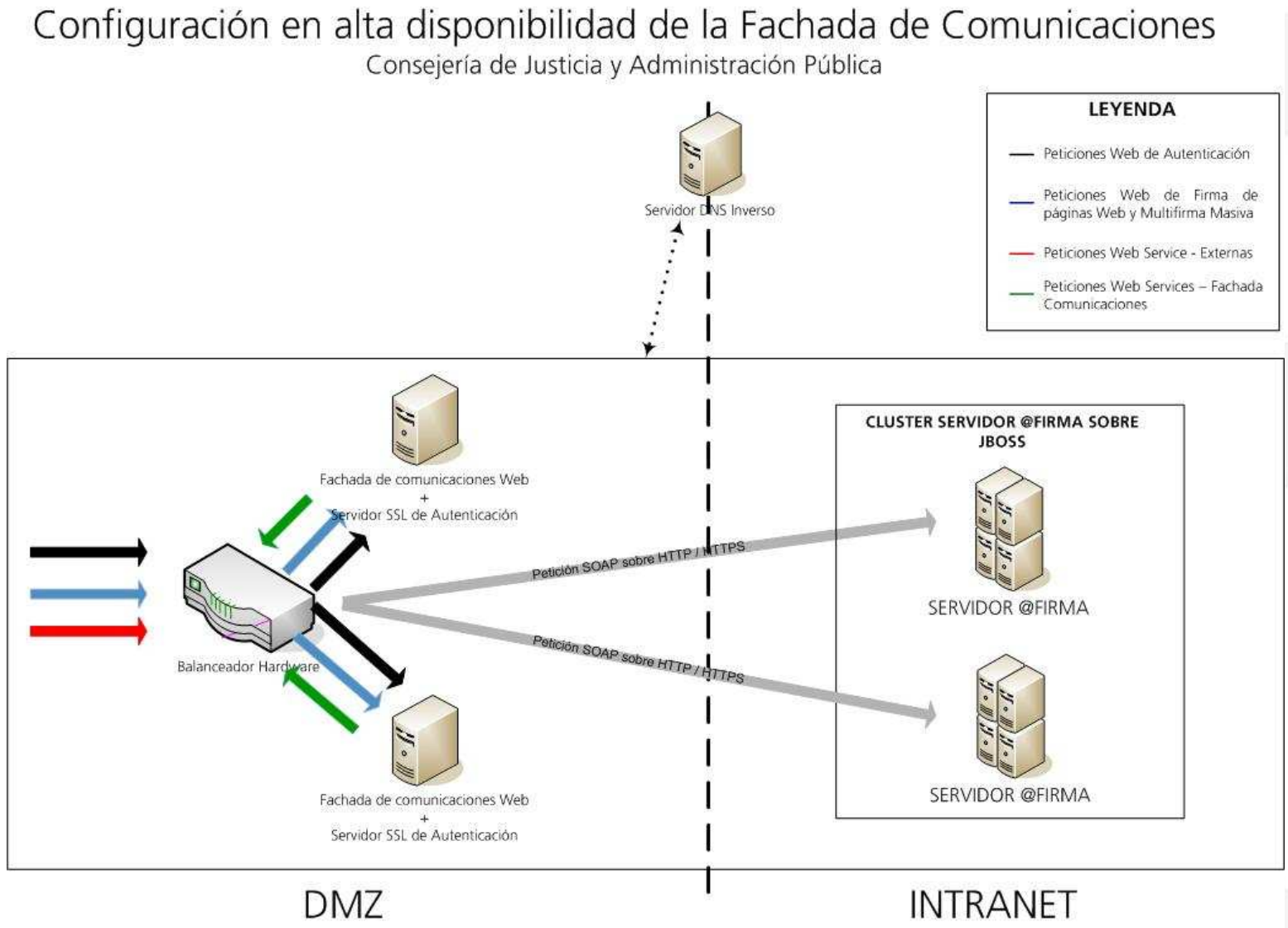
Arquitectura Hardware (I): Plataforma @firma v5.x



Arquitectura Hardware (II)



Arquitectura Hardware (III)



Servicios de @firma v5.x (I)

- Módulo de Gestión de Prestadores
  - Gestión del Árbol de Prestadores de Servicios de Certificación (PSC).
  - Gestión de los distintos tipos de certificados por cada PSC.
  - Analizador semántico de certificados y mapeo de campos.
  - Gestión de Políticas de Confianza.
  - Importación y Exportación de Elementos de Confianza entre distintas plataformas @firma.
- Módulo de Validación
  - Validación Multinivel de certificados según RFC 3280.
  - Validación del estado de revocación de certificados X.509 v3 ante un PSC mediante los protocolos CRL, OSCP y WS.
  - Servidor OCSP multiprestador.
  - Caché de estado de certificados multinivel.

Servicios de @firma v5.x (II)

- Módulo de Firma
  - **Firma, Multifirma y Multifirma web masiva (CoSign y CounterSign)**
  - **Firma, Multifirma de Ficheros en cliente (CoSign y CounterSign)**
  - **Firma de Ficheros por Certificado de Organización.**
  - **Firmas multiformato**
    - CMS, XMLDSignature, XADES, …
  - **Sellado de Tiempo.**
  - **Custodia de elementos de No repudio**
    - Con custodia de documento
    - Sin custodia de documento
  - **Justificante de firma.**
  - **Validación de Firmas.**

Servicios de @firma v5.x (III)

- Módulo de Gestión y Registro de Eventos
  - Auditoría y trazabilidad de todas las transacciones realizadas por la plataforma.
  - Generación de estadísticas sobre servicios
  - Gestión de Alarmas.
  - Herramienta Gráfica de Auditoria
  - Herramienta Gráfica de Monitorización

- Servicios de @firma Extensión JA
  - Módulo de Autenticación
    - Autenticación Web
    - Reautenticación Web
  - Módulo de Firma
    - Firma de páginas Web
    - Multifirma masiva de páginas Web
  - Módulo de Administración de la Extensión
    - Gestión de aplicaciones v4.x
    - Utilidades

@firma v4.x vs @firma v5.x (I)

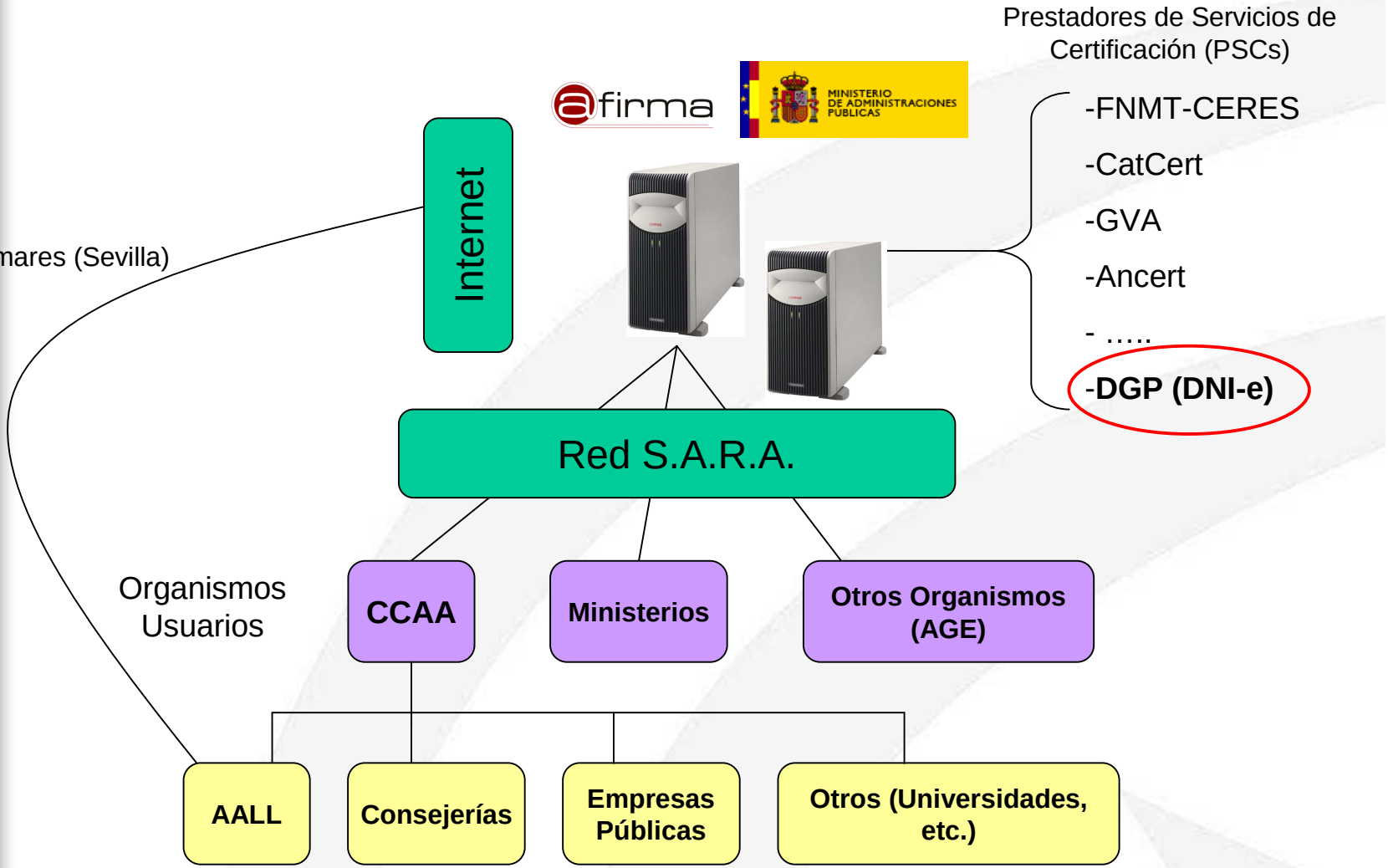
- Mejoras en @firma v5.x
  - **Módulo de Gestión de PSCs.**
    - ✓ Alta de PSCs y tipos de certificados de forma sencilla e intuitiva
    - ✓ Definición de mapeos online
    - ✓ Discriminación de tipos de certificados configurable visualmente
  - **Módulo de Validación.**
    - ✓ Validación conforme RFC 3280 (multinivel)
    - ✓ Servidor OCSP
    - ✓ Cachés de estado de certificados a dos niveles.
    - ✓ Definición de Políticas de Validación.
  - **Módulo de Firma.**
    - ✓ Nuevos formatos de Firma (CMS, XMLDSignature, XADES, etc.)
    - ✓ Custodia de elementos de no repudio.

@firma v4.x vs @firma v5.x (II)

- Mejoras en @firma v5.x (cont.)
  - **Módulo de Firma**
    - ✓ Capacidad de integración con HSMs (custodia y operaciones)
  - **Generales**
    - ✓ Firma de peticiones y respuestas del servicio (WS-Security)
    - ✓ Herramientas gráficas de usuario accesibles vía web
- Novedades en @firma v5.x
  - **Módulo de Gestión y Registro de Eventos**
    - ✓ Auditoría de transacciones
    - ✓ Generación de estadísticas e informes
    - ✓ Gestión y monitorización de alarmas en tiempo real.
  - **Módulo de Validación**
    - ✓ Importación y exportación de políticas de validación.

ÍNDICE

Modelo Centralizado ó ASP (Application Service Provider)



Modelo Centralizado ó ASP (Application Service Provider)

Ministerios:
Ministerio de Economía y Hacienda
Ministerio de Sanidad y Consumo
Ministerio de Cultura
Ministerio de Educación y Ciencia
Ministerio del Interior
Ministerio de Administraciones Públicas
Ministerio de Industria y Comercio
Ministerio de Fomento
Ministerio de la Vivienda
Ministerio de la Presidencia

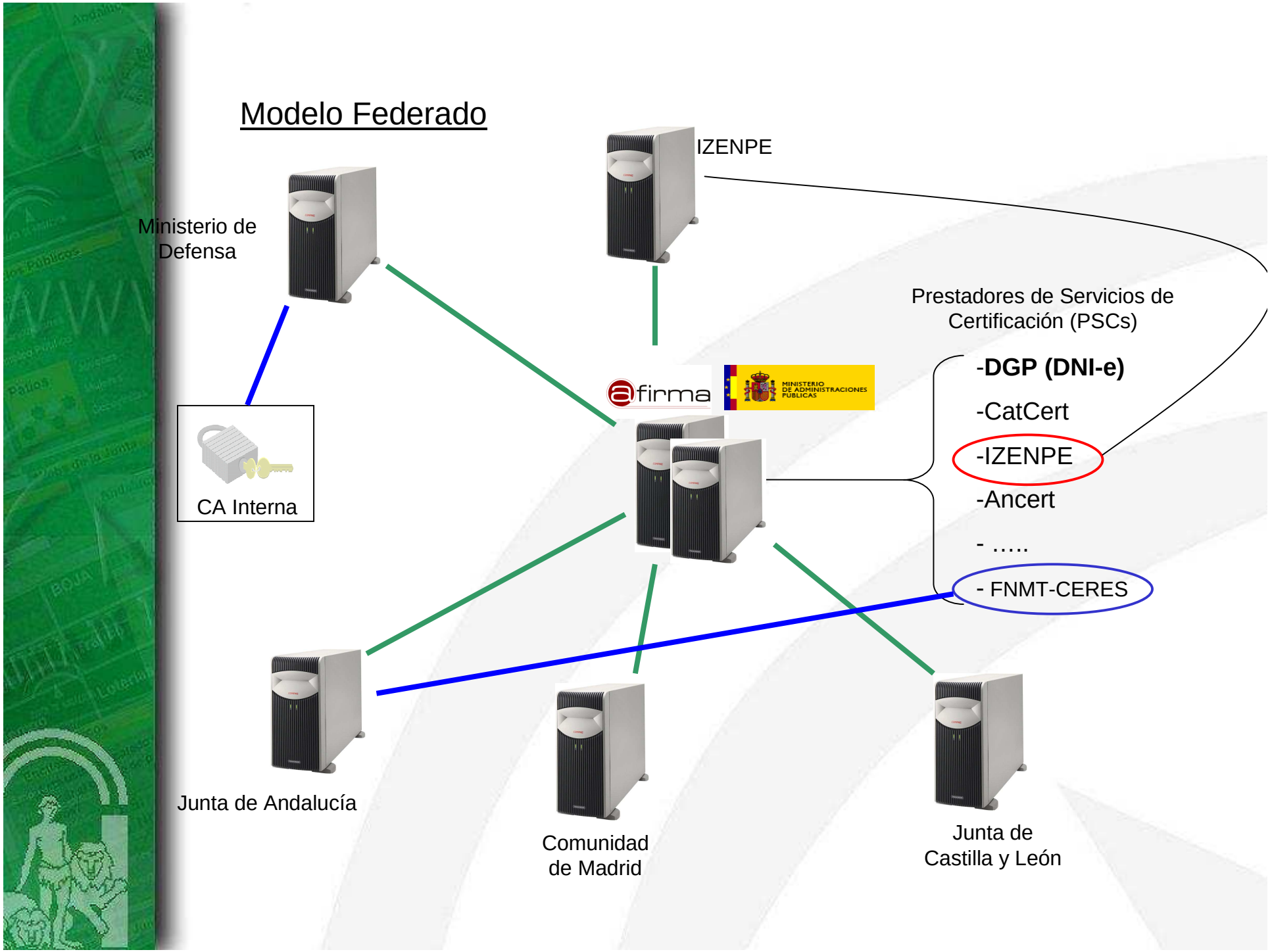
Otros organismos nacionales:
INEM
Correos
Gerencia de la Seguridad Social
DGT (Ministerio Interior)
Guardia Civil
Agencia de Protección de Datos
Confederación Hidrográfica del Guadalquivir (Ministerio MedioAmbiente)

Comunidades Autónomas:
Principado de Asturias
Cabildo de Gran Canaria
Junta de Andalucía
Junta de Castilla y León
Junta de Castilla La Mancha
Gobierno Vasco
Gobierno de Cantabria
Generalitat Valenciana

Organismos Autonómicos
CatCert (Autoridad de Certificación Catalana)
GVA (Autoridad de certificación Valenciana)

Administración Local:
Federación Española de Municipios y Provincias
Ayto. de Avilés
Ayto. Tomares
Ayto. Las Palmas
Ayto. Cáceres

Modelo Federado



Modelo Federado - Características

- Uso básico para el servicio de validación de Certificados

- Interconexión entre distintas plataformas @firma en una arquitectura distribuida

- Importación y Exportación de políticas de certificación comunes entre plataformas → Homogeneidad en los procesos de certificación

- Información Estadística Compartida → Posibilidad de Consolidar la información estadística Total desde cualquier Plataforma

- Autonomía e Independencia en cada despliegue de @firma (generación de firmas, custodia de información, etc.)

ÍNDICE

Muchas Gracias