PRESERVACIÓN LEGAL DE LARGA DURACIÓN PARA DOCUMENTOS ELECTRÓNICOS

SANTIAGO NAVARRO
navarros@keensoft.es

Preservación legal de larga duración para documentos electrónicos

Santiago Navarro (navarros@keensoft.es)

Jaca, 23 de julio de 2013

cursos de verano
UNIVERSIDAD DE ZARAGOZA

Presentación. keensoft

Business Intelligence y *Big Data*

Estudiamos sus datos y objetivos de empresa, diseñamos los indicadores necesarios y el modo de exponerlos para obtener un análisis rápido y útil. Implantamos soluciones software para explotar los datos y obtener la información que permite alcanzar las metas propuestas.

Gestión de conocimiento

Intranet colaborativa

Desarrollamos intranets de trabajo para potenciar la productividad de su entidad. La oficina cero-papel complementada con la interactividad colaborativa reduce los tiempos de espera y agiliza sus procesos.

Gestión Documental

Diseñamos sistemas de gestión documental basados en tecnologías y plataformas existentes adaptándolas a sus necesidades. Agilice su negocio evitando los tiempos improductivos de búsqueda de información.

Gestión de Archivo

Gestione su archivo de un modo eficiente y seguro garantizando su contenido. Aumente la accesibilidad de la información archivada permitiendo el autosuministro de la misma.

Custodia electrónica legal

Es necesario establecer mecanismos para garantizar la autenticidad de los documentos electrónicos guardados. Para ello keensoft hemos desarrollado un repositorio de custodia electrónica que garantiza la validez legal de la documentación electrónica a lo largo del tiempo de vigencia.

Movilidad

Creación de sitios web adaptativos para su información pueda ser consultada correctamente desde cualquier dispositivo.

Desarrollamos soluciones en movilidad a partir de aplicaciones ya existentes actualmente o totalmente nuevas. Aplicamos nuestro conocimiento técnico en dirección de proyectos y de tecnologías emergentes para garantizar un rápido desarrollo en las plataformas más extendidas.

Asesoría y consultoría tecnológica

Centrados especialmente en el software de gestión empresarial analizamos las necesidades de nuestros clientes, asesoramos sobre las soluciones que pueden impulsar su empresa.

Garantizamos el éxito de los proyectos informáticos mediante la auditoria de sus planes, realizando revisiones independientes de los proyectos en marcha o asesorando como un importante apoyo a su equipo.

Dirección de proyectos

Dirigimos su proyecto de tecnologías de la información garantizando la consecución de sus objetivos y por tanto su éxito. Seguimiento de requisitos, aprobación de entregables, reporte de información, evaluación de riesgos y apoyo en la decisión.

Creamos una oficina de proyectos dentro de su compañía para la gestión de las aplicaciones multidepartamentales y donde la integración de las diferentes soluciones es vital. Coordinación de proveedores, agrupación de requisitos comunes y sincronización de entregables.

Presentación. keensoft

Índice

- Preservación legal de larga duración
  - Definición
  - Necesidad
- Documento electrónico
  - Tipos
  - Legalidad
  - Metadatos
- Firma electrónica
  - Funcionamiento
  - Sello de tiempo y OCSP
  - CSV y copias electrónicas autenticas
- Archivo electrónico de larga duración
  - Escenario
  - Esquema
  - Evidencias digitales
- Aplicación en la Administración

Preservación legal de larga duración

Preservación legal de larga duración

- Definición
  - ***preservar. (Del lat. praeservāre).***
  - 1. tr. Proteger, resguardar anticipadamente a una persona, animal o cosa, de algún daño o peligro
  - ***legal. (Del lat. legālis).***
  - 1. adj. Prescrito por ley y conforme a ella.
  - 2. adj. Perteneciente o relativo a la ley o al derecho.
  - 3. adj. Verídico, puntual, fiel y recto en el cumplimiento de las funciones de su cargo

  - *"El acto de mantener la información de modo independiente, entendible y con autenticidad garantizada por evidencias por un largo periodo de tiempo para una comunidad"*[1]

  - La información digital es más fácil de alterar que el papel o microfilm. Los soportes de almacenamiento digital tienen menos esperanza de vida y requieren de determinadas tecnologías para acceder a la información.

[1] Alliance for Permanent Access http://www.alliancepermanentaccess.org

Preservación legal de larga duración

- Necesidad
  - Ley 11/2007 , de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)
    - *Artículo 6. Derechos de los ciudadanos." Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos"*
    - *Disposición final tercera "En el ámbito de la Administración General del Estado y los organismos públicos vinculados o dependientes de ésta, los derechos reconocidos en el artículo 6 de la presente ley podrán ser ejercidos en relación con la totalidad de los procedimientos y actuaciones de su competencia a partir del **31 de diciembre de 2009.**"*
    - http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf
  - Administración electrónica
    - Total de personas que han utilizado Internet en los últimos 12 meses 24.802.451
      - Obtener información de páginas web de la Administración 59,4 %
      - Descargar formularios oficiales 41,0 %
      - Enviar formularios cumplimentados 32,2 %
    - Fuente: Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares 2012. INE. http://www.ine.es/prensa/np738.pdf

Preservación legal de larga duración

- Necesidad
  - Actos jurídicos relevantes en el procedimiento administrativo
    - Actos de los Ciudadanos
      - Actos de declaración de voluntad
      - Actos de comunicación previa
      - Actos de declaración responsable
      - Actos de queja o sugerencia
    - Actos de la Administración
      - Actos administrativos
        - ✓ Los actos consultivos.
        - ✓ Los actos de visto bueno de la Administración.
        - ✓ Los actos de foliado.
        - ✓ Los actos de fiscalización.
        - ✓ Los actos de propuesta.
        - ✓ Los actos de dación de fe.
        - ✓ Los actos de solicitud de la Administración.
        - ✓ Los actos de declaración responsable de la Administración
      - Actos negociales de la Administración
  - Dependiendo del riesgo evaluado se podrán realizar la presentación y conservación de un modo u otro pero en todos casos la utilización de la firma electrónica es el medio establecido para ser legalmente aceptados.

Preservación legal de larga duración

- Necesidad de preservación física
  - Puntos clave
    - Conservación. Preservar tanto el contenido como la apariencia de los mismos.
    - Copias de seguridad. Proceso de hacer duplicados exactos del objeto digital.
    - Actualización. Copia de información digital de un soporte de almacenamiento a largo plazo a otro del mismo tipo, sin ningún cambio en los documentos
    - Metadatos conservación de los metadatos del de producción o como mínimo unos metadatos básicos que serán ampliados en catalogación e identificación.
      - Información sobre el contenido
      - Información para la conservación
  - Conservación de los contenidos
    - Preservación de la tecnología.
    - Migración.
    - Utilización de estándares
    - Emulación.
    - Almacenamiento.
  - Conservación de los soportes
    - Capacidad
    - Control de errores
    - programas de reemplazamiento
    - Condiciones de almacenamiento y manejo
    - Redundancia y copias de seguridad

Preservación legal de larga duración

- Necesidad de preservación legal
  - La Directiva 1999/93/CE *"A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica."*
  - LEY 59/2003, de 19 de diciembre, de firma electrónica regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. *"El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años".*
  - La validez de los documentos firmados electrónicamente depende de la imposibilidad de alteración del contenido sin detección del mismo. Para ello la firma electrónica ha establecidos medios que evitan dichas acciones.
  - Una de ellas radica en la necesidad de confirmar de forma periódica los documentos firmados su validez. Dado que la tecnología y la capacidad de procesamiento de los equipos evolucionan rápidamente la inviolabilidad del sistema de firma debe ser ratficado cada 4 años o menos. De este modo se hace imposible que la evolución de la tecnología avance hasta permitir la suplantación de un documento firmado electrónicamente por otro.

Documento electrónico

Documento electrónico

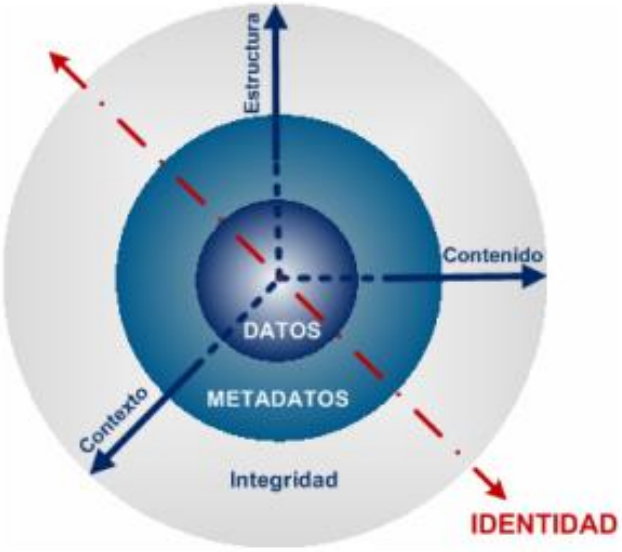
- Según la ley 11/2007 LAECSP, *"Documento electrónico. Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado."*
- Nos interesan en este caso los documentos que pueden ser utilizados como evidencias (records). UNE-ISO 30300:2011 "*Documentos (records) información creada, recibida y conservada como evidencia y como activo en el desarrollo de sus actividades o en virtud de sus obligaciones legales."*
- Así pues vamos a tratar en el documento electrónico o digital que incorpora una o varias firmas electrónicas tal y como describe el mismo la Guía de Aplicación de la NTI del documento electrónico [1] *"Un documento administrativo electrónico es, por tanto, el objeto digital administrativo que contiene la información objeto (datos y firma) y los datos asociados a ésta (metadatos)"*

- *"Un documento electrónico reside, desde el mismo instante de su captura, en el sistema de gestión de documentos de una determinada organización, donde permanecen inalteradas las características de autenticidad, fiabilidad e integridad, que confieren al documento valor probatorio, en el marco de la política de gestión de documentos electrónicos correspondiente"*

[1] http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_documento-electronico-INTERNET.pdf

Documento electrónico

- **El contenido**, conjunto de datos en que se sustancia la información
- **La firma electrónica** conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que:
  - Permite detectar cualquier cambio ulterior de los datos firmados,
  - Está vinculada al firmante de manera única y a los datos a los que se refiere
  - y ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- **Los metadatos**, elemento que proporciona contexto al contenido, estructura y firma de un documento, contribuyendo al valor probatorio y fiabilidad de éste a lo largo del tiempo como evidencia electrónica de las actividades y procedimientos.



Dimensiones y componentes del documento electrónico.

http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_documento-electronico-INTERNET.pdf

Documento electrónico

- Características de los documentos electrónicos
  - Dinámicos, pueden variar de una visualización a otra
  - Son procesables, la estructura y el contenido se conforman en el momento de la visualización.
  - Resultado de combinación de distintas fuentes como registros de una base de datos.
  - Diferentes morfologías (imagen, texto, video, …)
  - Formado por diferentes adjuntos (correo electrónico)
  - Almacenamiento distribuido
  - Necesita elementos hardware y software para su visualización.
- Requisitos de los documentos electrónicos
  - Confidencialidad y acceso.
  - Integridad
  - Autenticidad
  - Fiabilidad
  - Usabilidad y disponibilidad
  - Contextualidad

Documento electrónico

- **Metadatos mínimos**[1]
  - Versión NTI
  - Identificador. ES_<Órgano>_<AAAA>_<ID_específico>
  - Órgano. Directorio Común de Unidades Orgánicas y Oficinas (DIR3) http://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=dir3#.UezHBI17KAg
  - Fecha de captura. Formato ISO 8601 AAAAMMDD T HH:MM:SS
  - Origen. 0 = Ciudadano, 1 = Administración
  - Estado de elaboración
  - Nombre de formato. Catálogo de estándares de la NTI
  - Tipo documental
  - Tipo de firma. CSV o Formatos de firma electrónica definidos en la NTI
  - Valor CSV (si tipo firma CSV)
  - Definición generación CSV (si tipo firma CSV)
  - Identificador de documento origen. Si 'Estado de elaboración' = copia electrónica autentica (total o parcial)
- **Metadatos adicionales**

[1] http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_documento-electronico-INTERNET.pdf

Firma electrónica

Firma electrónica

- Objetivos
  - Firma
    - Autenticidad. El emisor del mensaje es quien dice ser.
    - Integridad. Mensaje no alterado.
    - No Repudio. El mensaje fue emitido por el emisor.
  - Cifrado
    - Confidencialidad. Información solo de emisor a receptor.

Firma electrónica

- Como funciona

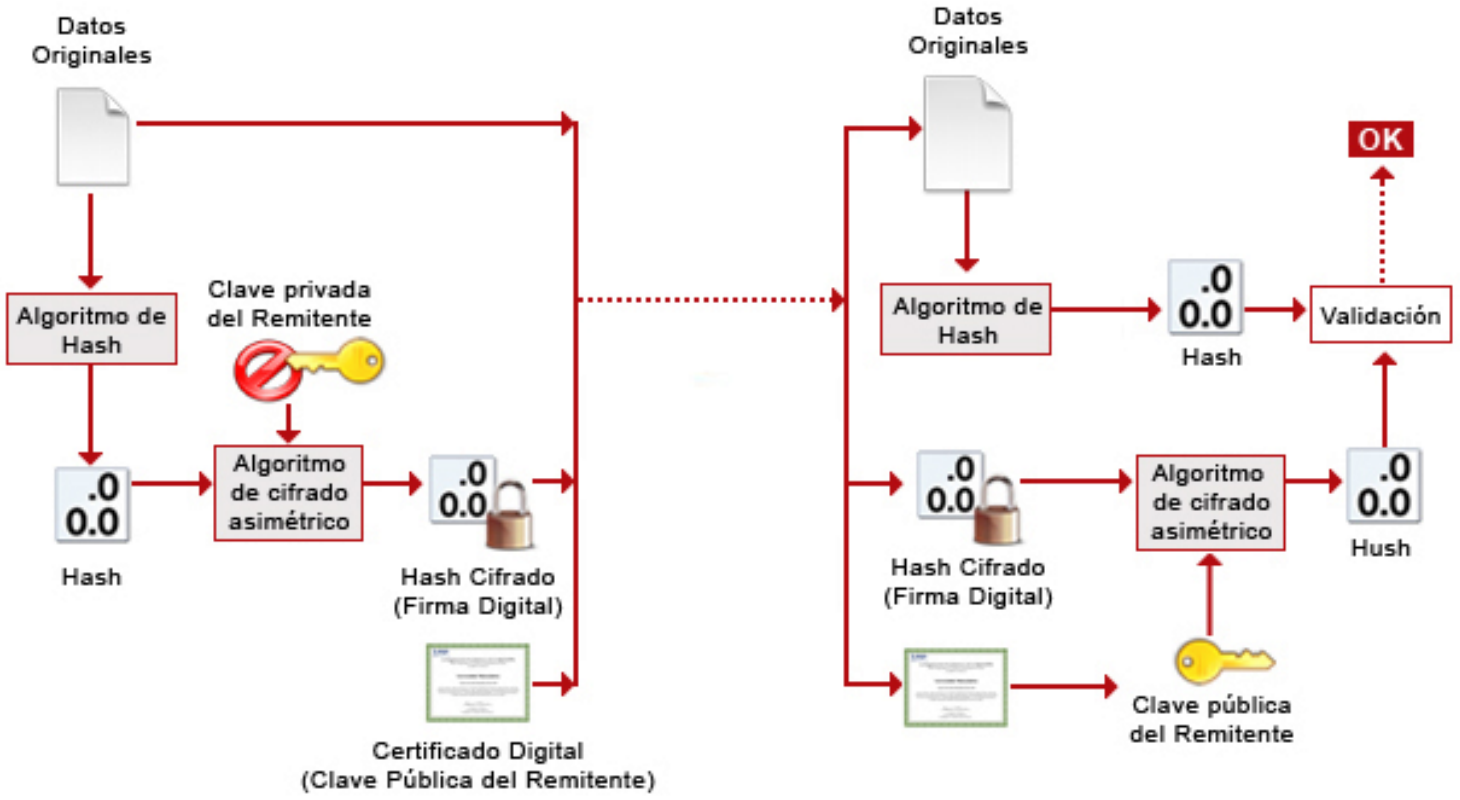
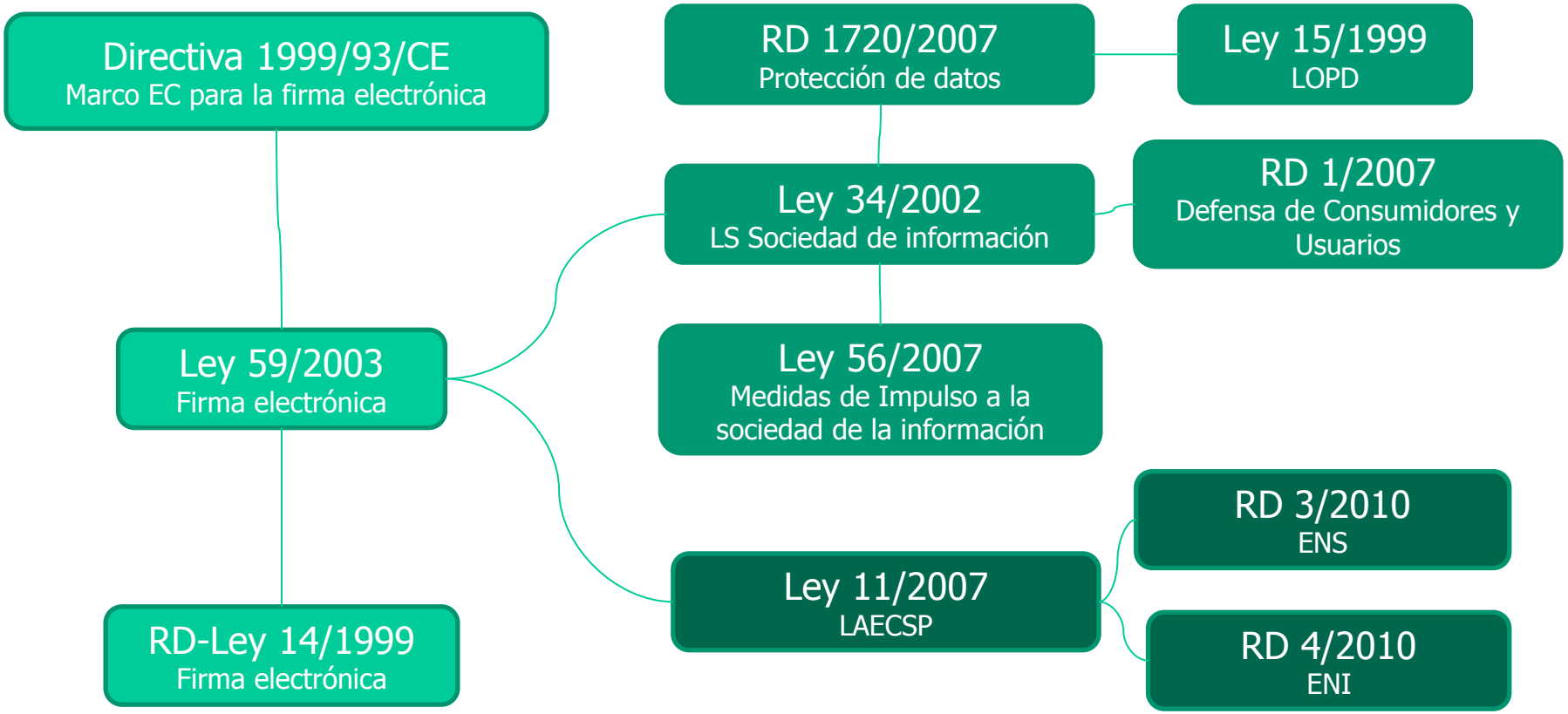


Gráfico: INTECO (Instituto de Tecnologías de la Comunicación) http://www.inteco.es

Firma electrónica

- Marco normativo



Firma electrónica

- Prestadores de servicio
  - CA. Autoridad de certificación.
  - RA. Autoridad de registro.
  - VA. Autoridad de validación.
  - TSA. Autoridad de Sello de Tiempo.
  - LTA. Servicio de Custodia Longeva.

- https://sedeaplicaciones2.minetur.gob.es/prestadores/

Firma electrónica

- Tipos de certificados de firma
  - Personas
    - Certificado-tipo de persona física.
    - Certificado-tipo de persona jurídica.
    - Certificado-tipo de entidad sin personalidad jurídica.
    - Certificado-tipo de representante.
    - Certificado-tipo de personal al servicio de una organización.
    - Certificado-tipo de personal al servicio de la Administración.
  - Organismos
    - Certificado-tipo de sede electrónica.
    - Certificado-tipo de sello electrónico de Administración, órgano o entidad de derecho público.
    - Certificado-tipo de entidad de sellado de fecha y hora.
  - Maquinas
    - Certificado-tipo de servidor seguro.
    - Certificado-tipo de aplicación segura.
    - Certificado-tipo de firma software.

Firma electrónica

- Formatos de firma
  - Desde el punto de vista del fichero resultante
    - *Attached* (Firmas implícitas)
    - *Detached* (Firmas explicitas)
  - Formatos
    - Binarias (PKCS#7, CMS, CADES, PAdES, FirmaPDF)
    - XML (XMLDSig, XAdES)
    - Correo (S/MIME)
  - Validación
    - Básicas (PKCS#7, CMS, XMLDSig, S/MIME, FirmaPDF)
    - Avanzadas (CADES, PAdES, XAdES)
  - Numero de firmas
    - Secuenciales
    - Paralelas

Firma electrónica

- Ejemplo firma XAdES BES

```
<?xml version="1.0" encoding="UTF-8"?>
<documento id="documento">
    <titulo id="titulo">Documento de pruebas</titulo>
    <descripcion id="descripcion">Documento destinado a realizar pruebas de firma</descripcion>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:etsi="http://uri.etsi.org/01903/v1.3.2#" Id="Signature504735">
        <ds:SignedInfo Id="Signature-SignedInfo1024952">
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference Id="SignedPropertiesID429729" Type="http://uri.etsi.org/01903#SignedProperties" URI=
            "#Signature504735-SignedProperties48056">
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue><!-- Digest del elemento referenciado en Base64 --></ds:DigestValue>
            </ds:Reference>
            <ds:Reference URI="#Certificate1237555">
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue><!-- Digest del elemento referenciado en Base64 --></ds:DigestValue>
            </ds:Reference>
            <ds:Reference Id="Reference-ID-200615" URI="">
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue><!-- Digest del elemento referenciado en Base64 --></ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue Id="SignatureValue552465">
            <!-- Valor de la firma en Base64 -->
        </ds:SignatureValue>
        <ds:KeyInfo Id="Certificate1237555">
            <ds:X509Data>
                <ds:X509Certificate>
                    <!-- Certificado firmante en Base64 -->
                </ds:X509Certificate>
            </ds:X509Data>
            <ds:KeyValue>
```

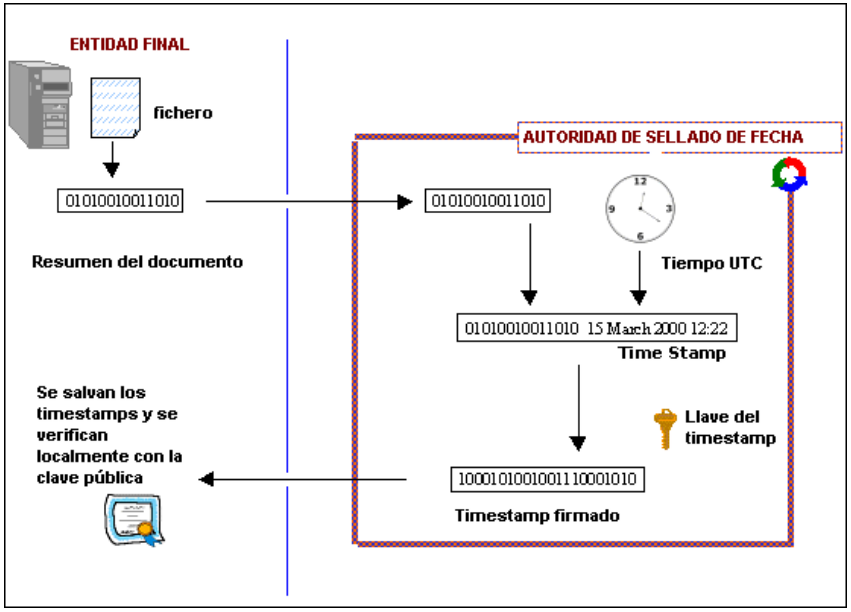
Firma electrónica

- Ejemplo firma XAdES BES

```
            <ds:Modulus><!-- Módulo de la clave RSA en Base64 --></ds:Modulus>
            <ds:Exponent><!-- Exponente de la clave RSA en Base64 --></ds:Exponent>
        </ds:RSAKeyValue>
    </ds:KeyValue>
</ds:KeyInfo>
<ds:Object Id="Signature504735-Object873466">
    <etsi:QualifyingProperties Target="#Signature504735">
        <etsi:SignedProperties Id="Signature504735-SignedProperties48056">
            <etsi:SignedSignatureProperties>
                <etsi:SigningTime><!-- Fecha y hora de la firma --></etsi:SigningTime>
                <etsi:SigningCertificate>
                    <etsi:Cert>
                        <etsi:CertDigest>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                            <ds:DigestValue><!-- Digest del certificado en Base64 --></ds:DigestValue>
                        </etsi:CertDigest>
                        <etsi:IssuerSerial>
                            <ds:X509IssuerName><!-- Nombre de emisión del certificado firmante --></ds:X509IssuerName>
                            <ds:X509SerialNumber><!-- Número de serie del certificado firmante --></ds:X509SerialNumber>
                        </etsi:IssuerSerial>
                    </etsi:Cert>
                </etsi:SigningCertificate>
            </etsi:SignedSignatureProperties>
            <etsi:SignedDataObjectProperties>
                <etsi:DataObjectFormat ObjectReference="#Reference-ID-200615">
                    <etsi:Description><!-- Descripcion del objeto firmado ---></etsi:Description>
                    <etsi:MimeType><!-- Tipo MIME del objeto firmado --></etsi:MimeType>
                </etsi:DataObjectFormat>
            </etsi:SignedDataObjectProperties>
        </etsi:SignedProperties>
    </etsi:QualifyingProperties>
</ds:Object>
```

Firma electrónica

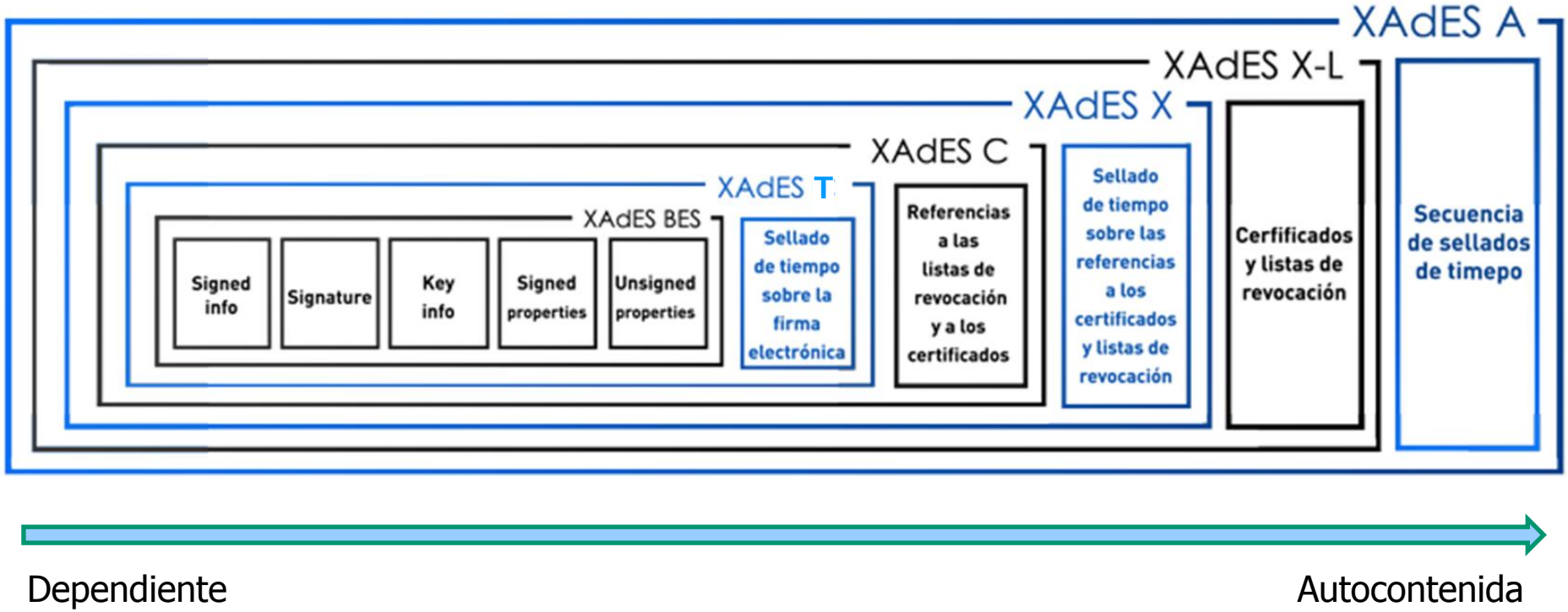
- Sello de tiempo



- OCSP *Online Certificate Status Protocol*
  - RFC 2560 http://tools.ietf.org/html/rfc2560
  - Se trata de un protocolo que permite la verificación del estado de un certificado en el momento de la consulta.
  - Es un método alternativo a las listas CRL (*Certificate Revocation List*)
  - La respuesta del servidor se codifica en formato ASN1 (*Abstract Syntax Notation One*) y puede ser guardada y adjuntada a una firma para construir una firma autocontenida.

Firma electrónica

- Formato de firma electrónica avanzada

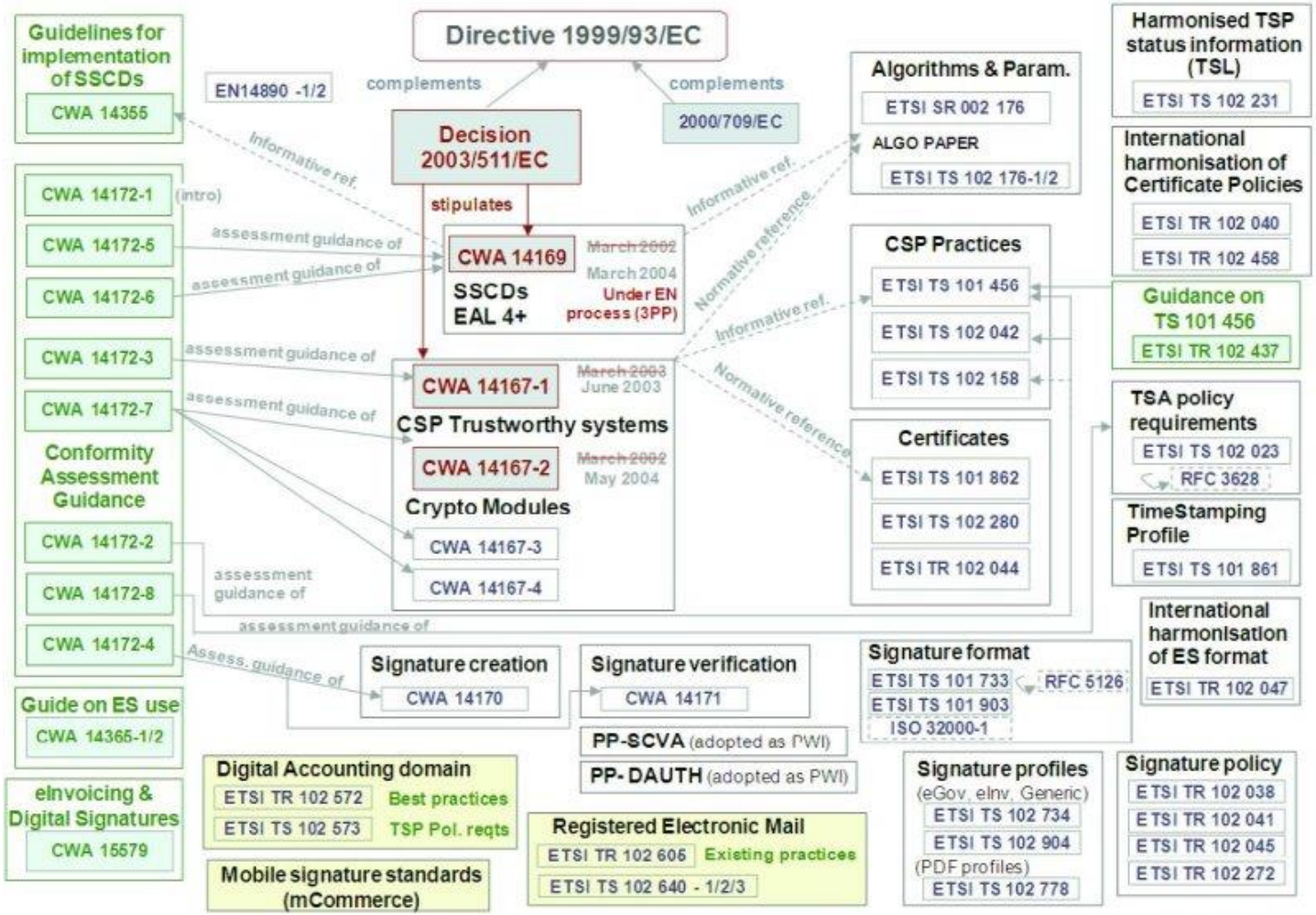


Firma electrónica

- Formato de firma electrónica avanzada Longeva ADES-A
  - Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, ésta deberá:
    - Ser complementada con información del estado del certificado en el momento
    - Información no repudiable (metadatos) con sello de tiempo
    - Certificados de la cadena de confianza
  - Para mantener la firma válida en el tiempo debe incluir evidencias de ello antes de que sea vulnerable (caducidad).
  - Se debe aplicar mecanismos de resellado, para añadir, de forma periódica, un sello de fecha y hora de archivo con un algoritmo más resistente

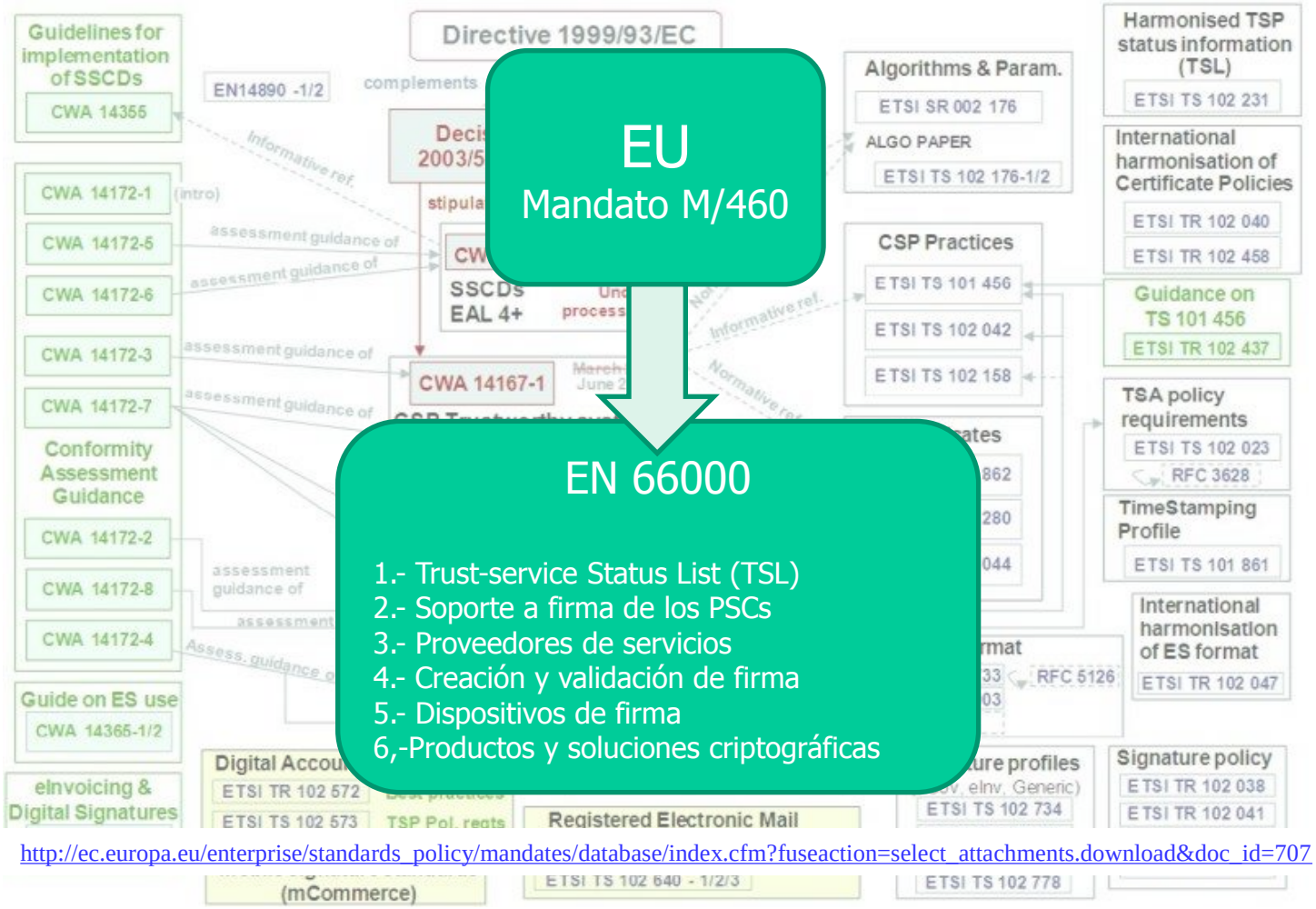
Firma electrónica

- Marco normativo. Estándares



Firma electrónica

- Marco normativo. Estándares



http://ec.europa.eu/enterprise/standards_policy/mandates/database/index.cfm?fuseaction=select_attachments.download&doc_id=707

Firma electrónica

CSV Código Seguro de Verificación

- Ley 11/2007, LAESCP, Artículo 18. Sistemas de firma electrónica para la actuación administrativa automatizada.

"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:

…

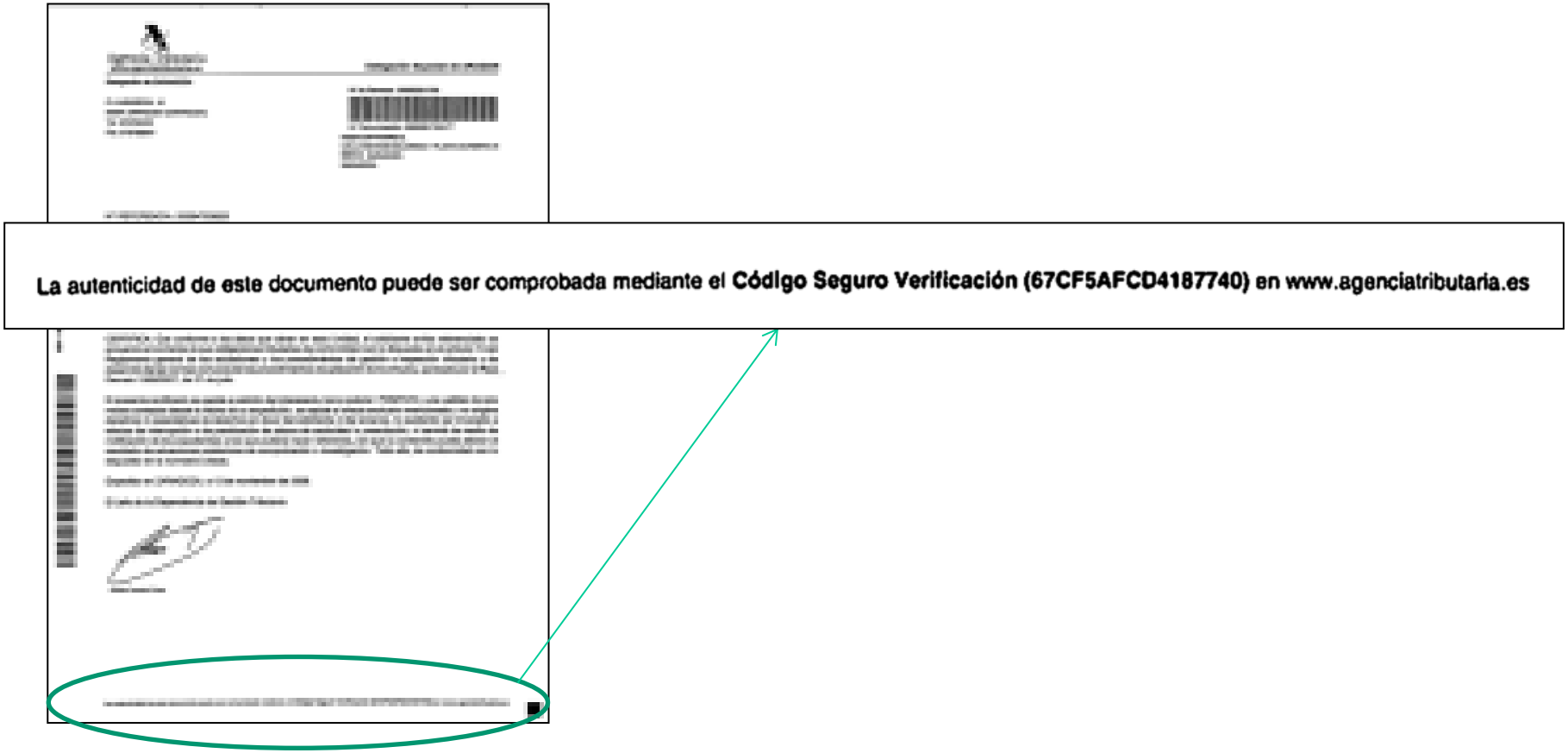
Código seguro de verificación vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente."

- Ley 11/2007, LAESCP, Artículo 30

"Las copias realizadas *en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas* ***siempre que incluyan la impresión de un código*** *generado electrónicamente u otros sistemas de verificación* ***que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos*** *de la Administración Pública, órgano o entidad emisora."*

Firma electrónica

- CSV Código Seguro de Verificación



Firma electrónica

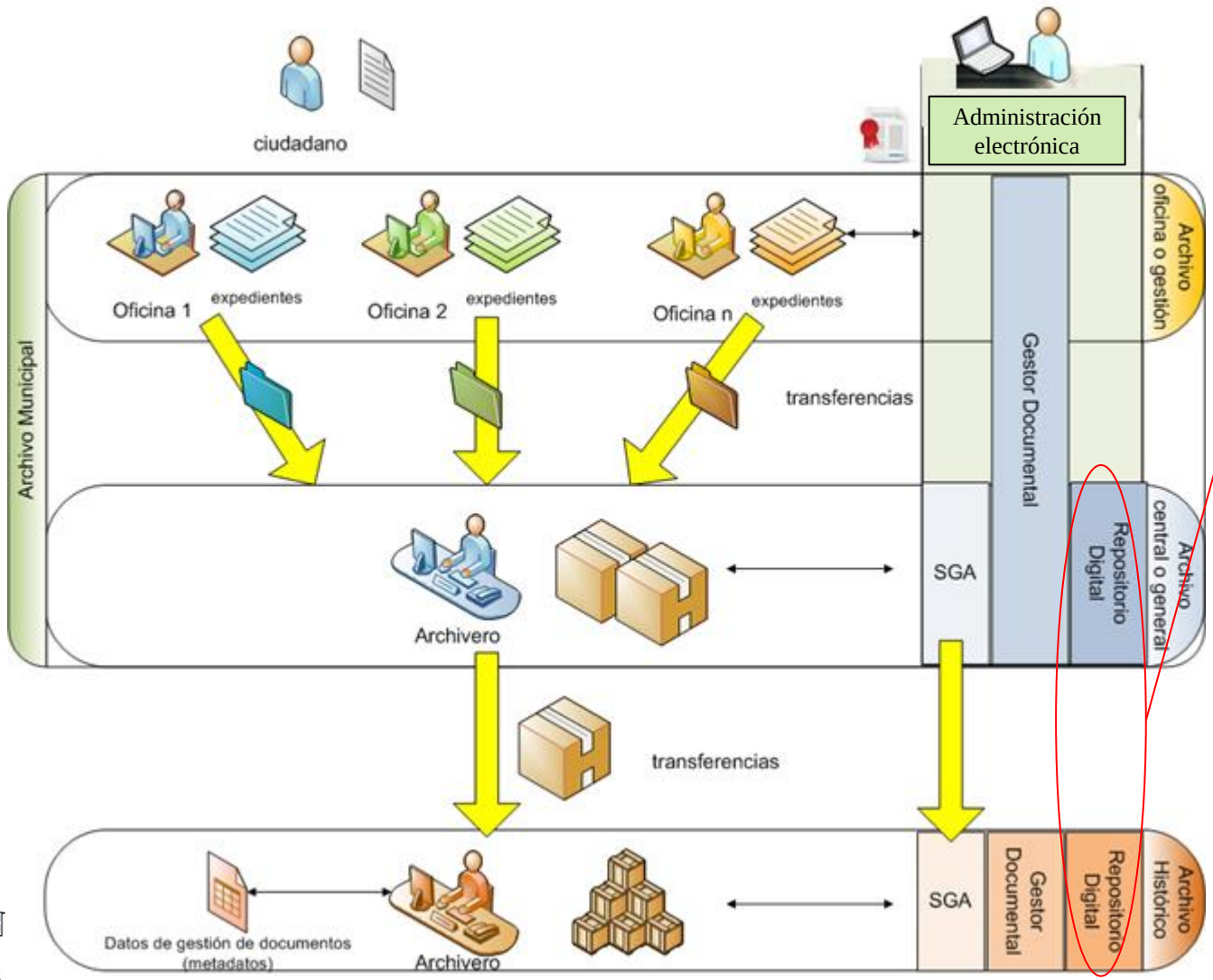
- Copia electrónica

Ref. normativa (Artículos)			DOCUMENTO ORIGEN			DOCUMENTO OBTENIDO		Descripción – TIPO DE COPIA
Ley 11/2007	R.D. 1671/2009	R.D. 4/2010	Generado por	Localización	Soporte	Soporte	¿Cambio formato?	
30.1	43 y 49	21 y 23	ADMON.	ADMON.	ELECT.	ELECT.	✗	**NO ES UNA COPIA AUTÉNTICA:** - Si el contenido y formato del documento a generar es igual al del original, debe tratarse como una representación del documento electrónico original: es un documento original.
			CIUDADANO	ADMON.	ELECT.	ELECT.	✗	
			ADMON.	ADMON.	ELECT.	ELECT.	✓	**Copia electrónica auténtica con cambio de formato.**
			CIUDADANO	ADMON.	ELECT.	ELECT.	✓	
30.2	44	21 y 23	ADMON.	ADMON.	PAPEL	ELECT.	-	**Copia electrónica auténtica de documento papel.**
30.3	44	21 y 23	CIUDADANO	ADMON.	PAPEL	ELECT.	-	
30.3	50	21 y 23	CIUDADANO	CIUDADANO	PAPEL	ELECT	-	
30.1	43 y 49	21 y 23	ADMON.	ADMON.	ELECT.	ELECT	OPCIONAL	**Copia electrónica parcial auténtica.**
30.5	45	21 y 23	ADMON.	ADMON.	ELECT.	PAPEL	-	**Copia papel auténtica de documentos públicos administrativos electrónicos.**
			CIUDADANO	ADMON.	ELECT.	PAPEL	-	

Gráfico: Guía de aplicación de la norma de interoperabilidad. Procedimientos de copiado autentico y conversión entre documentos electrónicos, http://www.mpt.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_copiado-conversion-doc-elec-INTERNET.pdf

Archivo electrónico de larga duración

Archivo electrónico de larga duración. Escenario



El repositorio digital tiene el cometido de almacenar la información de los expedientes del modo adecuado para que su validez legal permanezca en el tiempo

Archivo electrónico de larga duración

- Desde la aprobación de la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* la interacción de los ciudadanos de forma electrónica a los servicios de la administración es un derecho.
- Consecuencia de ello se requiere de un mecanismo para poder guardar la documentación electrónica que forma parte de un expediente con las mismas garantías que un expediente en papel.
- En el caso de los expedientes electrónicos los principales problemas existentes para son:
  - La obsolescencia de los algoritmos utilizados para realizar firma electrónica debido al aumento de la capacidad computacional de los equipos. Esto permitiría falsificar el documento
  - La limitación del ciclo de vida de los certificados utilizados que exige su renovación no superior a 4 años.
- Por este motivo es necesario establecer mecanismos para garantizar la autenticidad de los documentos electrónicos guardados.
- El *Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica* indica dos posibles aproximaciones para dar solución a este objetivo:
  - Uso de formato de firma longeva o de archivo.
  - Conservación y custodia de las firmas en archivos digitales garantizando la fecha de ingreso y la no modificación de los mismos

Archivo electrónico de larga duración

- **Objetivos funcionales**
- El servicio de archivo electrónico y la preservación digital de larga duración es una necesidad estratégica para el desarrollo de la administración electrónica con las garantías legales exigibles.
- El archivo de larga duración permite:
  - Custodia de los documentos electrónicos con la garantía del mantenimiento de su validez legal a lo largo del tiempo
  - Soluciones de protección ante la obsolescencia tecnológica
  - Servicio de evidencia electrónica con validez legal
- Así pues el sistema de preservación digital de la información debe tener las siguientes funciones:
  - Basado en el modelo OAIS (ISO 14721:2003) *Open Archival Information System*
  - Control de formatos: normalización y migración
  - Control de acceso (LDAP)
  - Registro de accesos
  - Gestión de la obsolescencia. Conversión de formatos
  - Metainformación sobre preservación (PREMIS)
  - Almacenamiento de documentos encriptados

Archivo electrónico de larga duración

- Para construir el sistema nos basaremos en el sistema OAIS

- Como puede verse en el esquema la información que entra en el sistema se encuentra paquetizada de modo que puede tratarse de un modo "abstracto" sin conocer su contenido.
- El sistema tratará los expedientes electrónicos como paquetes de entrada y salida

REFERENCE MODEL FOR AN OPEN ARCHIVAL INFORMATION SYSTEM (OAIS)
http://public.ccsds.org/publications/archive/650x0m2.pdf

Archivo electrónico de larga duración

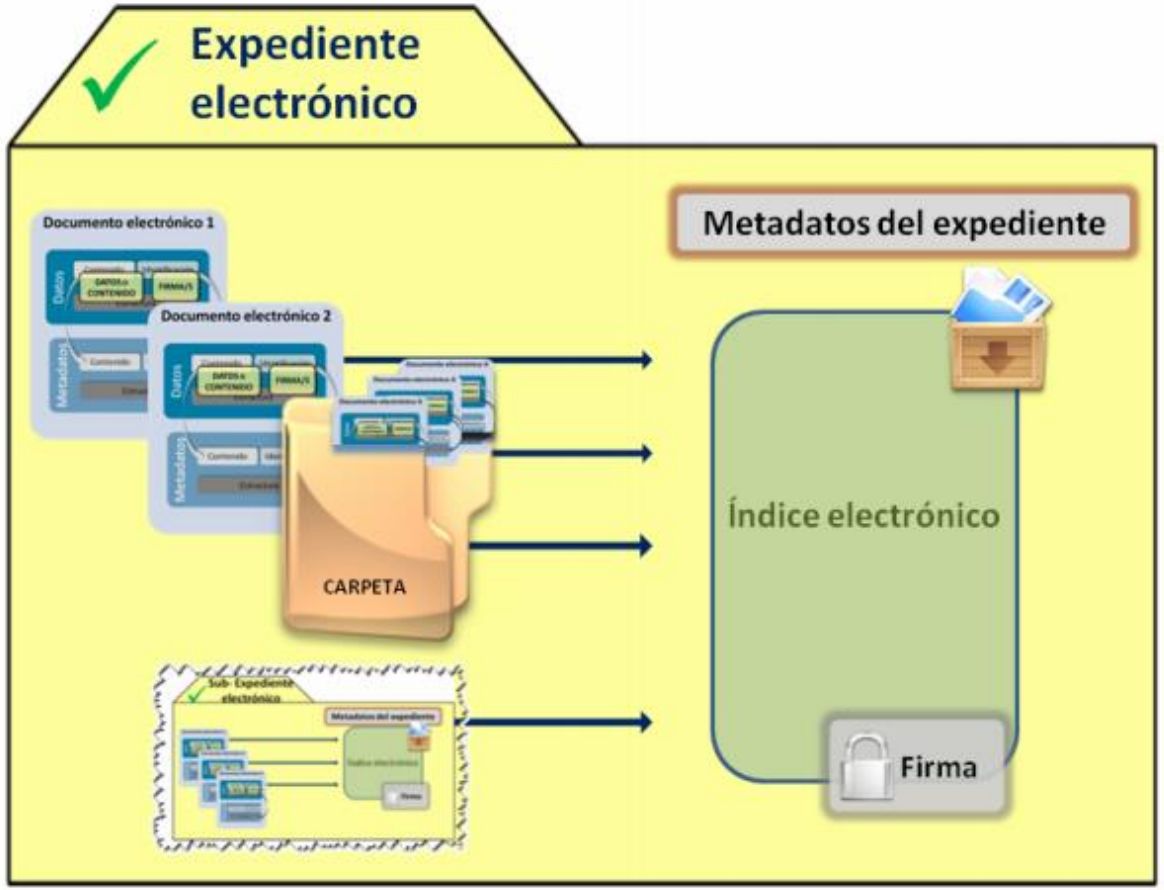
- De este modo el objeto de información del archivo almacenado es una composición de:
  - Documento guardado
  - Metadatos de preservación de la información
  - Metadatos del paquete de información
  - Metadatos descriptivos
  - Documento en formato preservable

  Todo ello en un formato XML

- Cada paquete de información es ingresado en un formato que permita gestionar los datos complejos de metadatos + objeto digital que forman un expediente (METS)

Archivo electrónico de larga duración

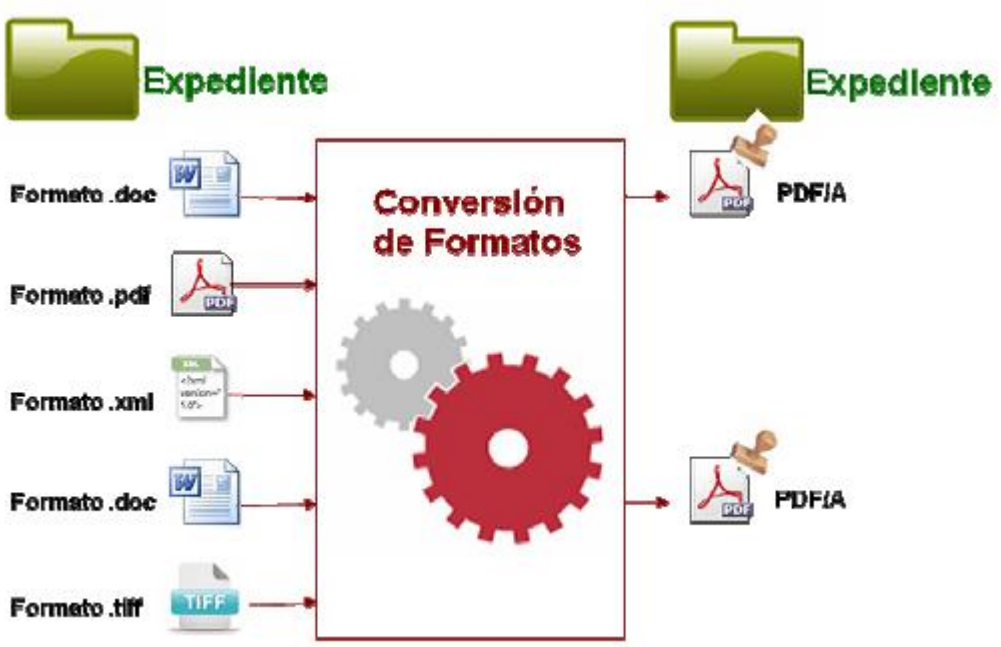
- Expediente Electrónico



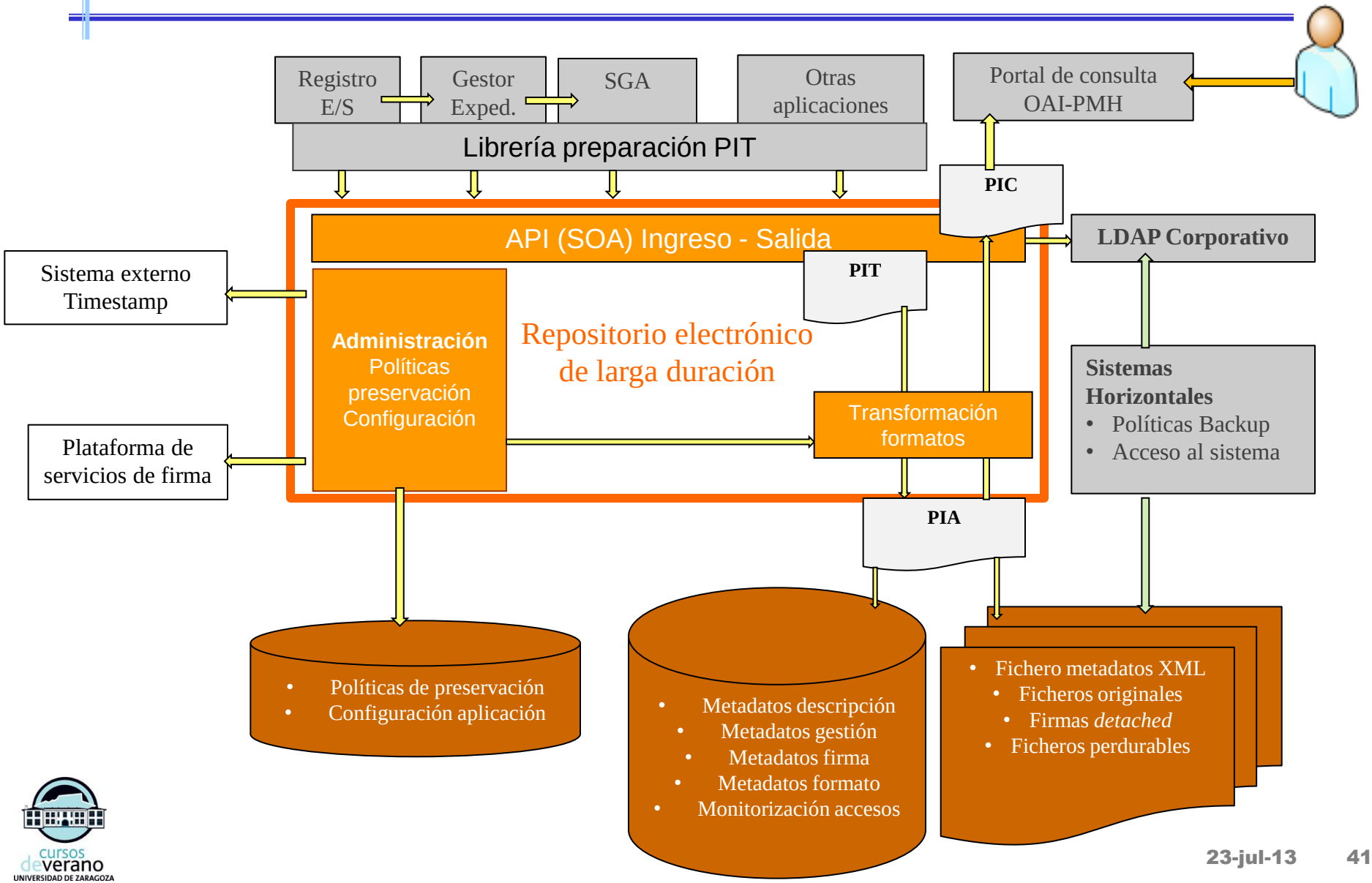
Modelo del ENI Esquema Nacional de Interoperabilidad
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=145

Archivo electrónico de larga duración

- Uno de los aspectos más importantes es disponer de un sistema de vigilancia de la obsolescencia de la información.
- Para ello se deben establecer filtros de conversión que garanticen que la información será siempre visible.
- Aun con todo siempre se guardará la información original accesible para que pueda obtenerse la fuente del proceso.

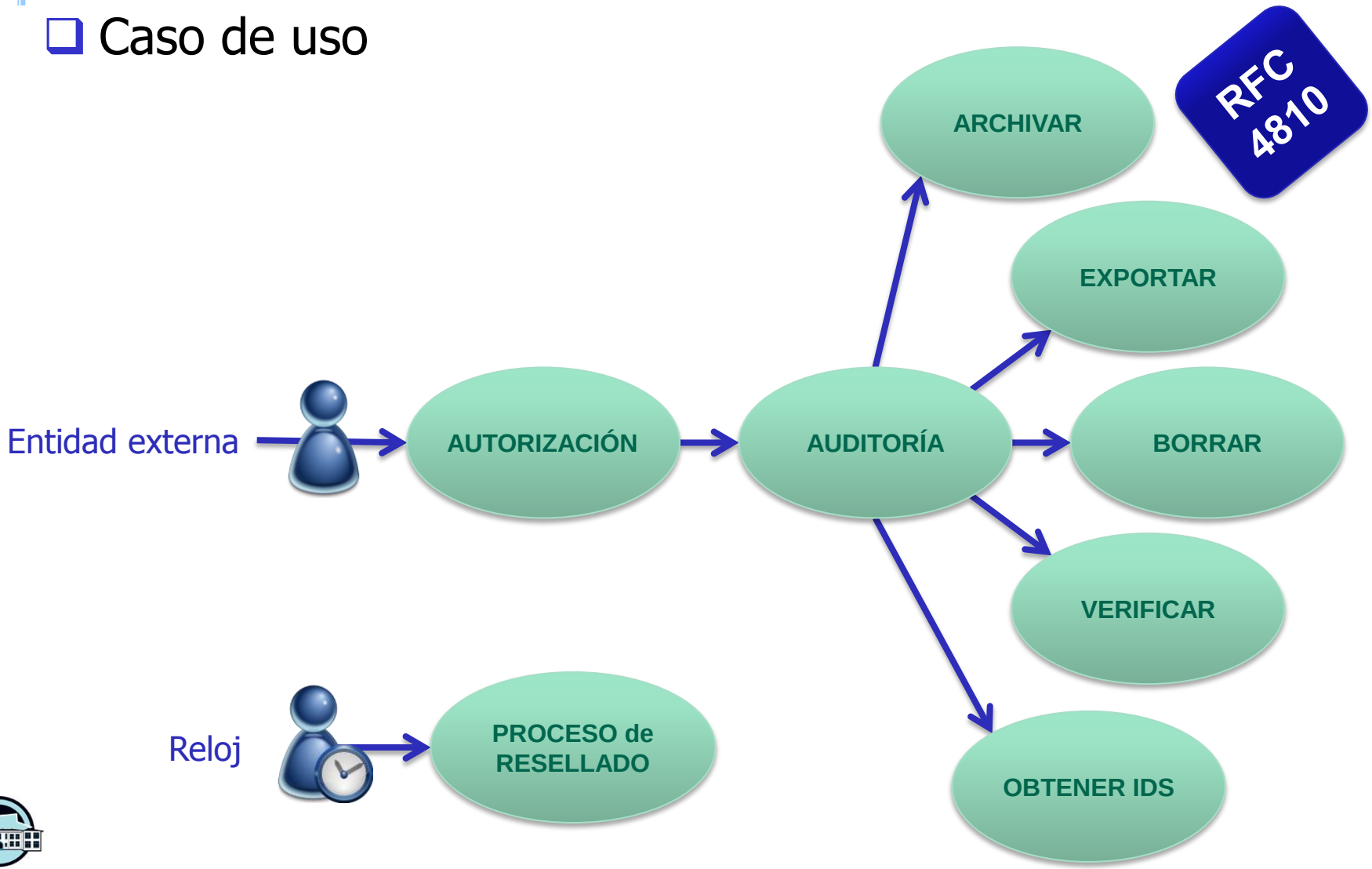


Archivo electrónico de larga duración. Esquema



Archivo electrónico de larga duración.

- Caso de uso

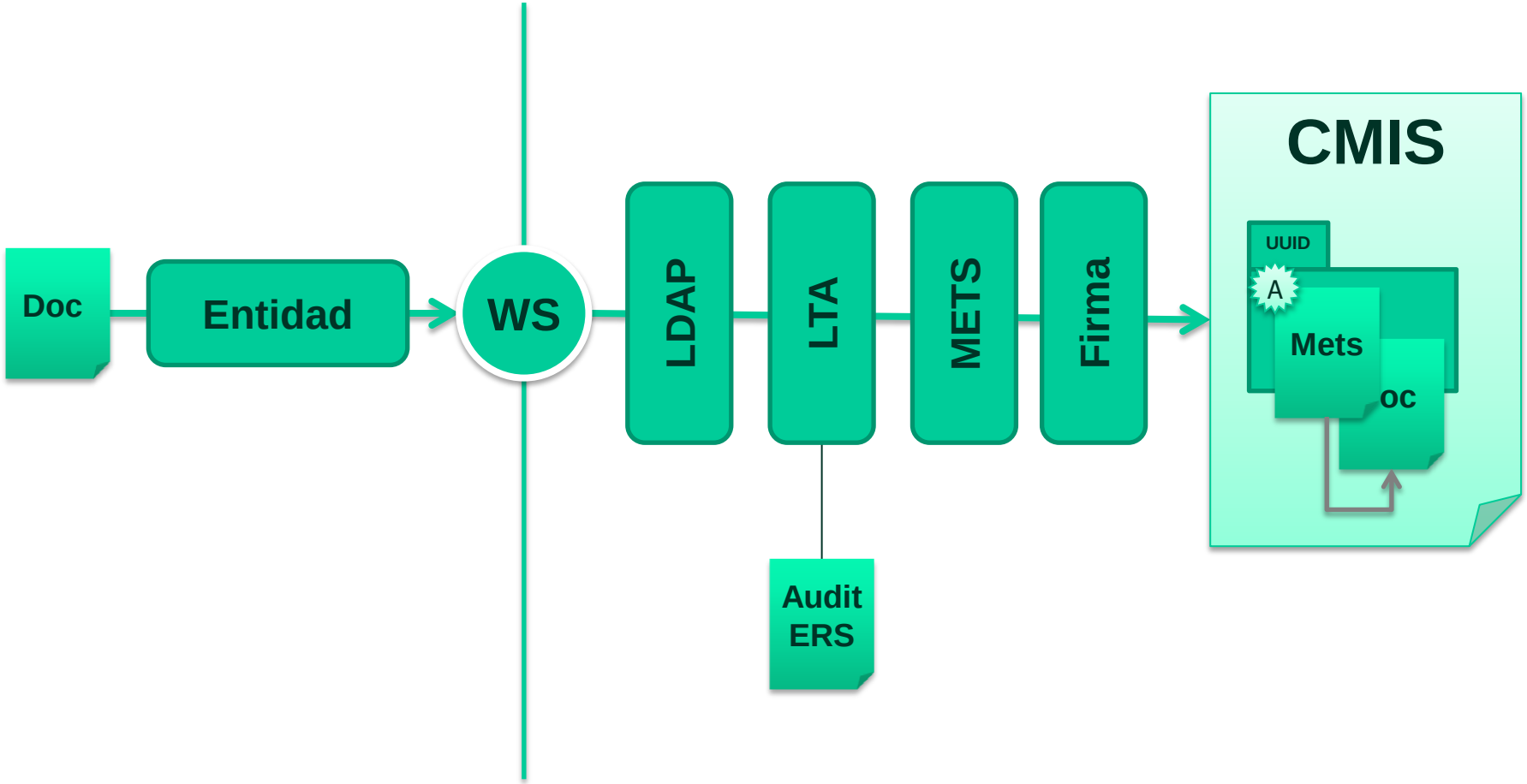


Archivo electrónico de larga duración.

- Funcionalidades
- Ingreso
  - Creación de peticiones de transferencia de documentos / expedientes
  - Aprobar, rechazar y aceptar las solicitudes de transferencia de documentos / expedientes
- Consulta
  - Consulta en línea de los documentos
  - Descarga del informe de evidencia
- Validación
  - Informe del estado del documento
- Preservación
  - Gestión y ejecución de políticas de migración de documentos, de consistencia y de
  - Resellado.
  - Gestión de los formatos de los ficheros
- Eliminado
  - Eliminación de los documentos manteniendo las evidencias y traza de su existencia

Archivo electrónico de larga duración.

- Funcionamiento



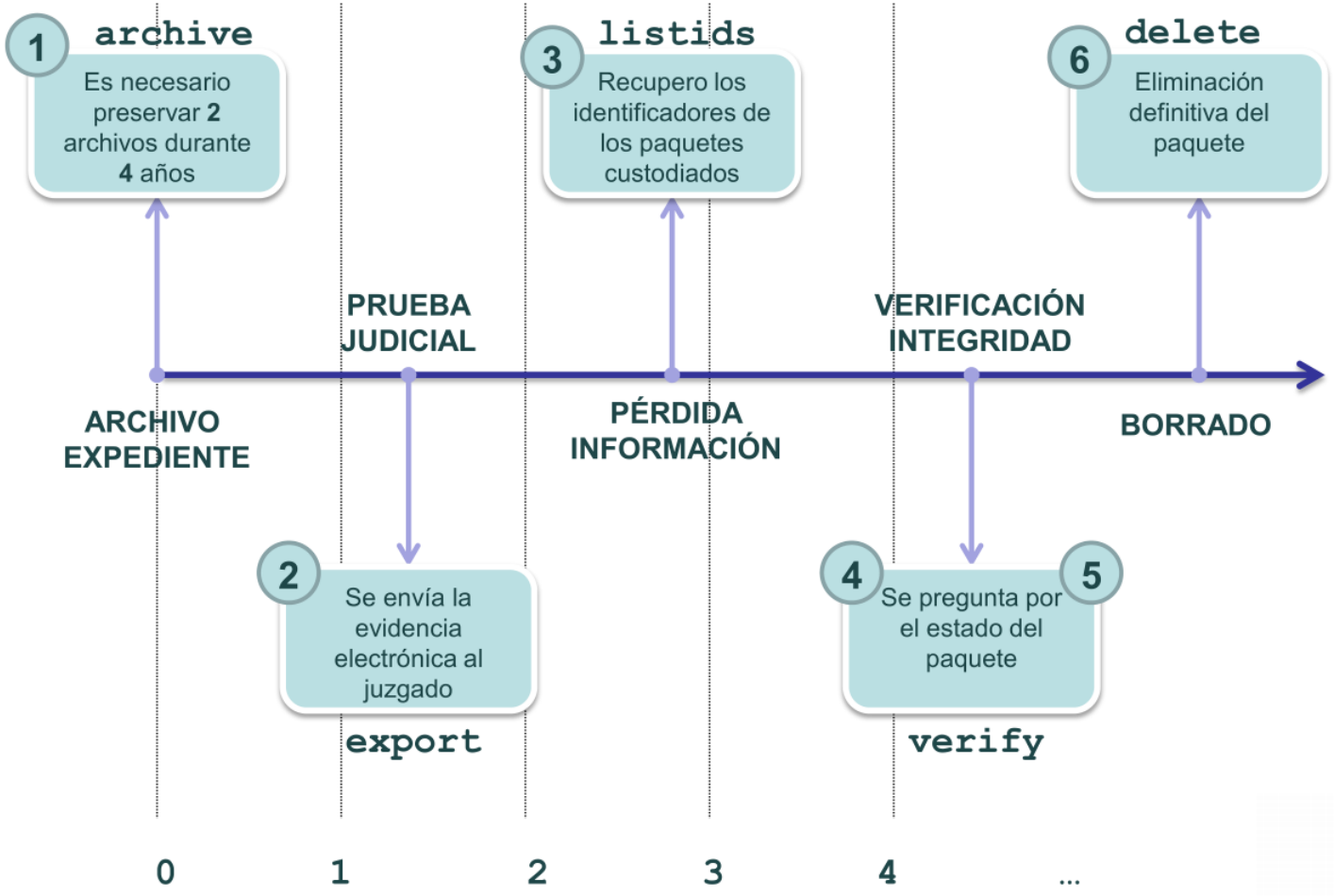
Evidencias electrónicas

- En muchos casos, los usuarios deben ser capaces de demostrar la existencia, la integridad y la validez de los datos, incluyendo los datos firmados durante períodos de tiempo largo o indeterminado.
- RFC 6283 XMLERS especifica la sintaxis y procesamiento de reglas XML para la creación de evidencia de no repudio a largo plazo de la existencia y la integridad de los datos. http://www.rfc-base.org/rfc-6283.html
- Se basa en el formato ERS (Evidencia Record Sintaxis) RFC 4998. http://tools.ietf.org/html/rfc4998

- El funcionamiento de las evidencias se basa en la construcción de una cadena de evidencias selladas de tiempo que permite garantizar que el documento no ha sido vulnerable en ningún momento.

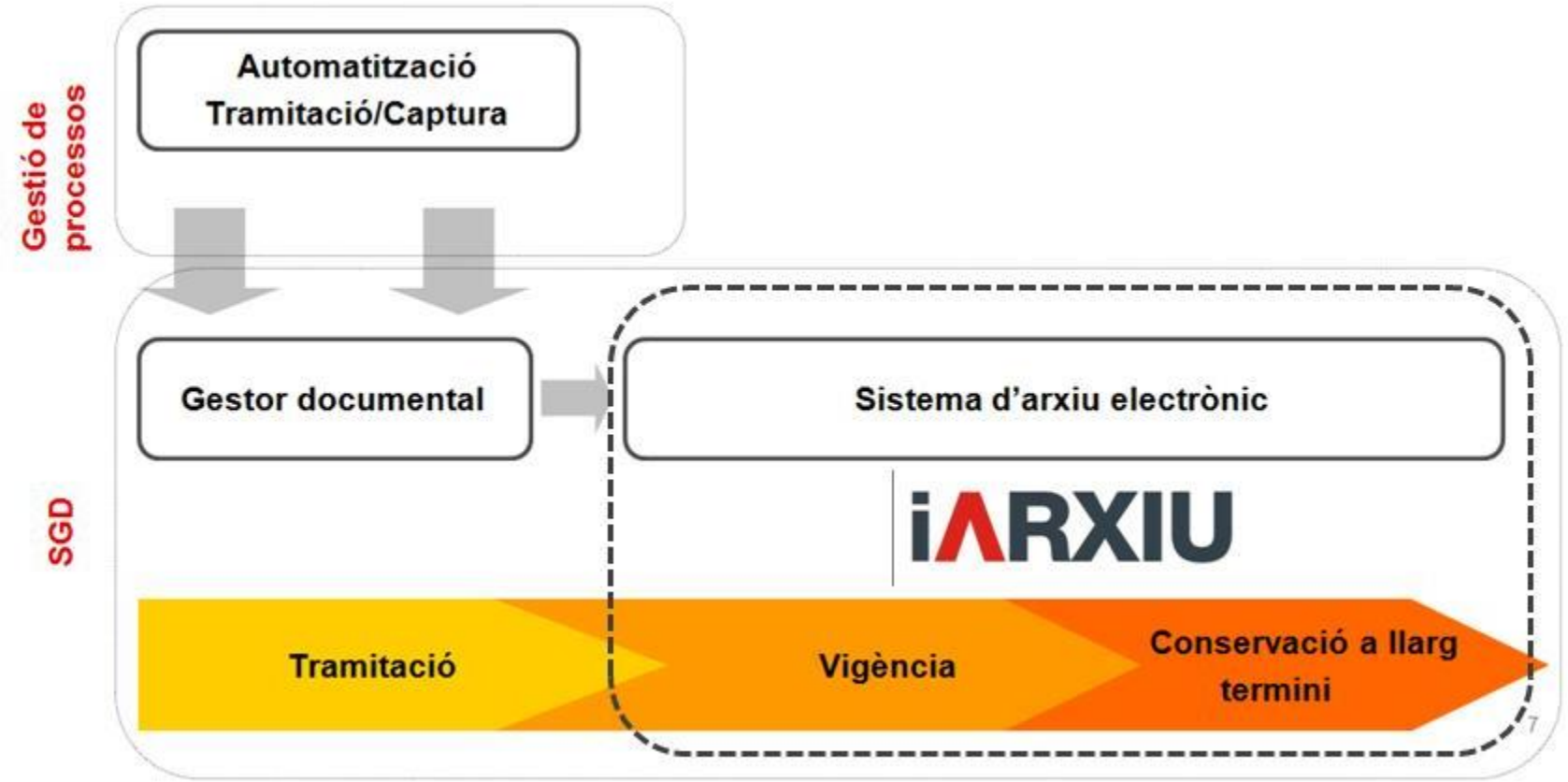
Archivo electrónico de larga duración.

- Ejemplo de funcionamiento



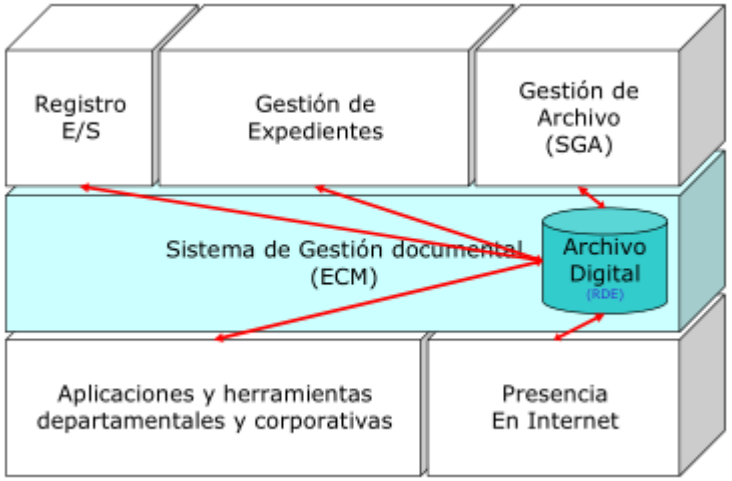
Archivo electrónico de larga duración.

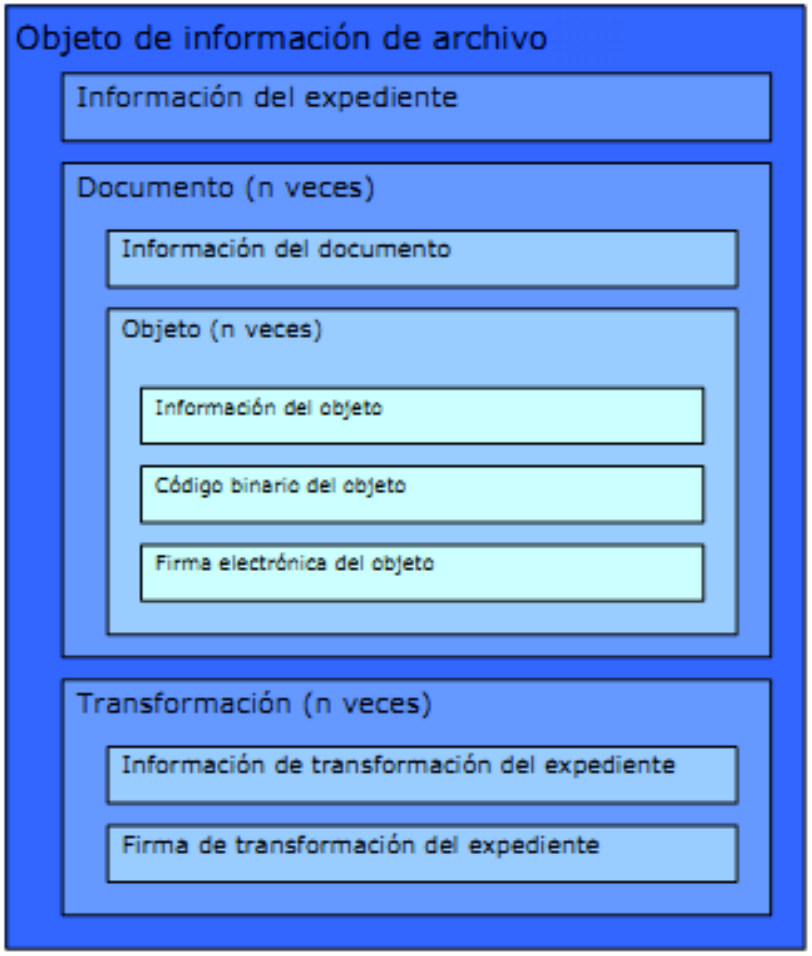
- iArxiu. Generalitat de Catalunya



Archivo electrónico de larga duración.

- DOKUSI. Gobierno Vasco





Archivo electrónico de larga duración.

- Perdur@. Diputación de Teruel