

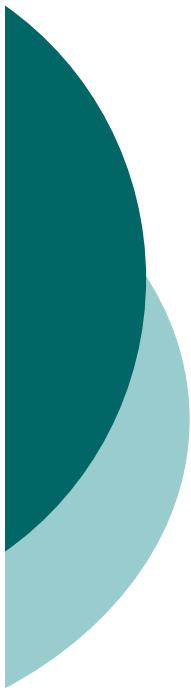


Universidad
de Alcalá

Dpto. Ciencias de la Computación

Sistemas Empresariales

Administración Electrónica – II
Plataformas, componentes, certificados



Índice

- 1. Elementos para la Implementación de la eAdmin**
- 2. Plataformas**
- 3. Componentes**
- 4. Integración con el Backoffice**
- 5. Identidad digital y certificados**

1.- Elementos

Visión Global



Componentes + Procesos
Plataforma

1.- Elementos

Componentes



Sede Electrónica



Gestor de formularios



Registro electrónico



Pasarela de pagos



Gestor de expedientes



Notificación electrónica



Identificación electrónica



Archivo electrónico



Interoperabilidad

.....

Fuente:



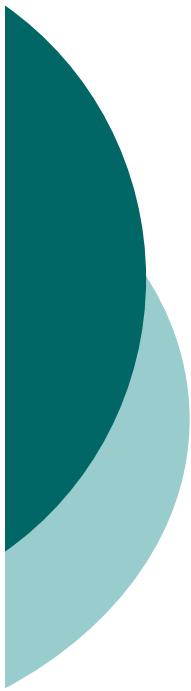
1.- Elementos

Procesos

| | | | | | | | | | | | | | | |
|---|---|---|---|--|--|---|---|---|---|---|---|---|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  | | |
| Arbitrajes | Autorizaciones | Certificaciones | Contratación pública | Convenios | | | | | | | | | | |
| Expropiaciones | Gestión de personal | Notificación electrónica | Presentación de documentación | Prestaciones sociales y sanitarias | | | | | | | | | | |
| Recursos administrativos | Responsabilidad patrimonial | Sanciones | Subvenciones | Sugerencias, quejas y reclamaciones | | | | | | | | | | |

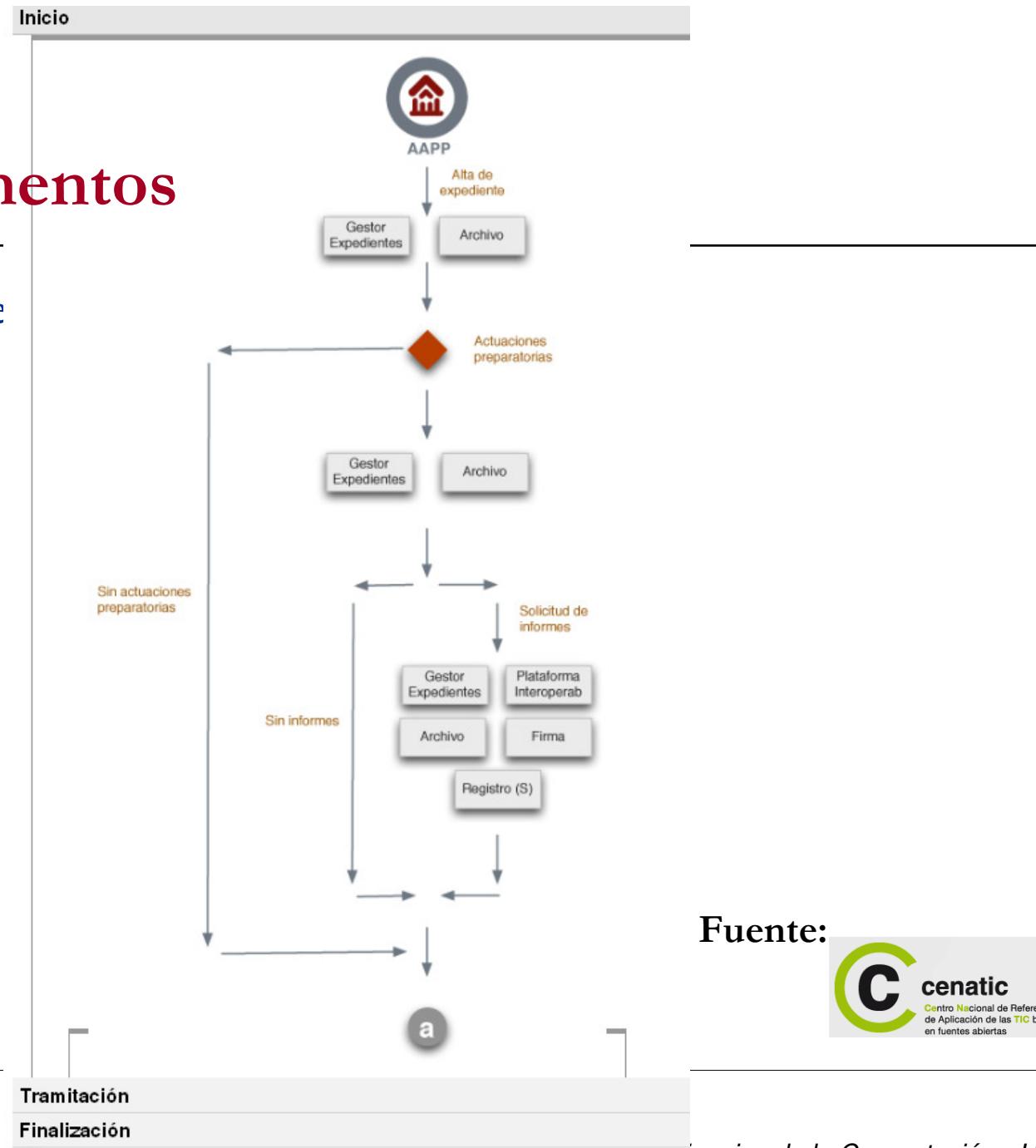
Fuente:





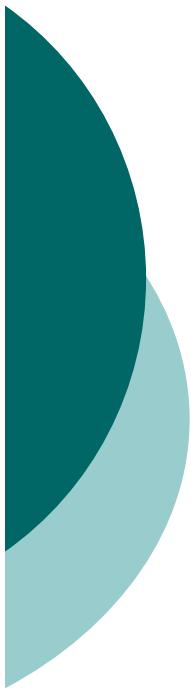
1.- Elementos

Ejemplo de proceso



Fuente:





Índice

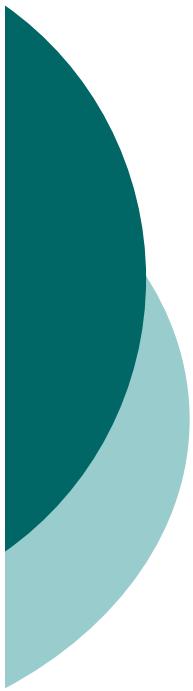
1. Elementos para la Implementación de la eAdmin
2. Plataformas
3. Componentes
4. Integración con el Backoffice
5. Identidad digital y certificados

2.- Plataformas

Plataforma

Componentes + Procesos

Plataforma



2.- Plataformas

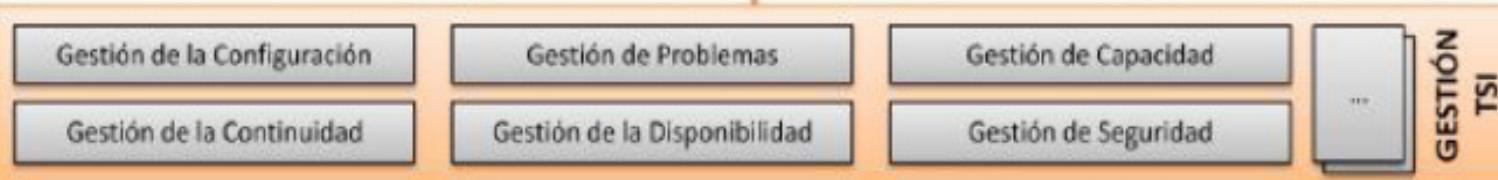
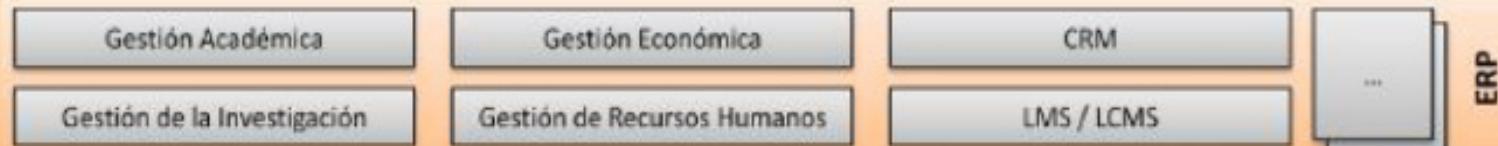
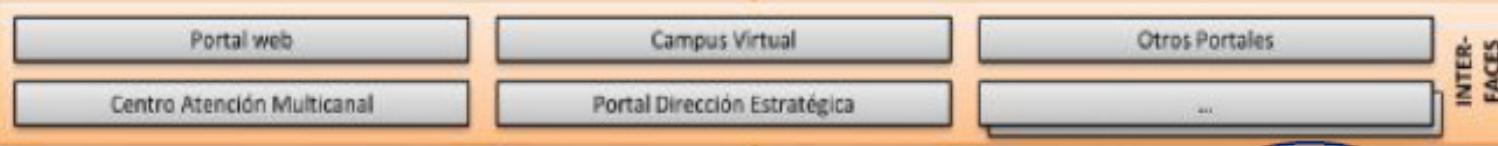
Plataforma

- Conjunto de **herramientas pensadas para ser transversales** a toda la administración, proporcionando homogeneidad, puntos únicos de acceso, e interoperabilidad entre organismos y sistemas de información.
- Estas herramientas, poco a poco están sustituyendo a las verticales de cada Organismo, en su mayoría desarrolladas como proyectos a medida que nacen y mueren en él.

LIBRO BLANCO DE LA
UNIVERSIDAD DIGITAL 2010

INTEROPERABILIDAD CON INSTITUCIONES, ORGANISMOS Y SERVICIOS

Preuniversitarios, Empresas, Estudiantes, PDI, PAS, Órganos de Gobierno, Consejos Sociales, Titulados, Egresados, Instituciones, Fundaciones, Centros, Administración, Clientes, Sociedad...



Ejemplos de plataformas

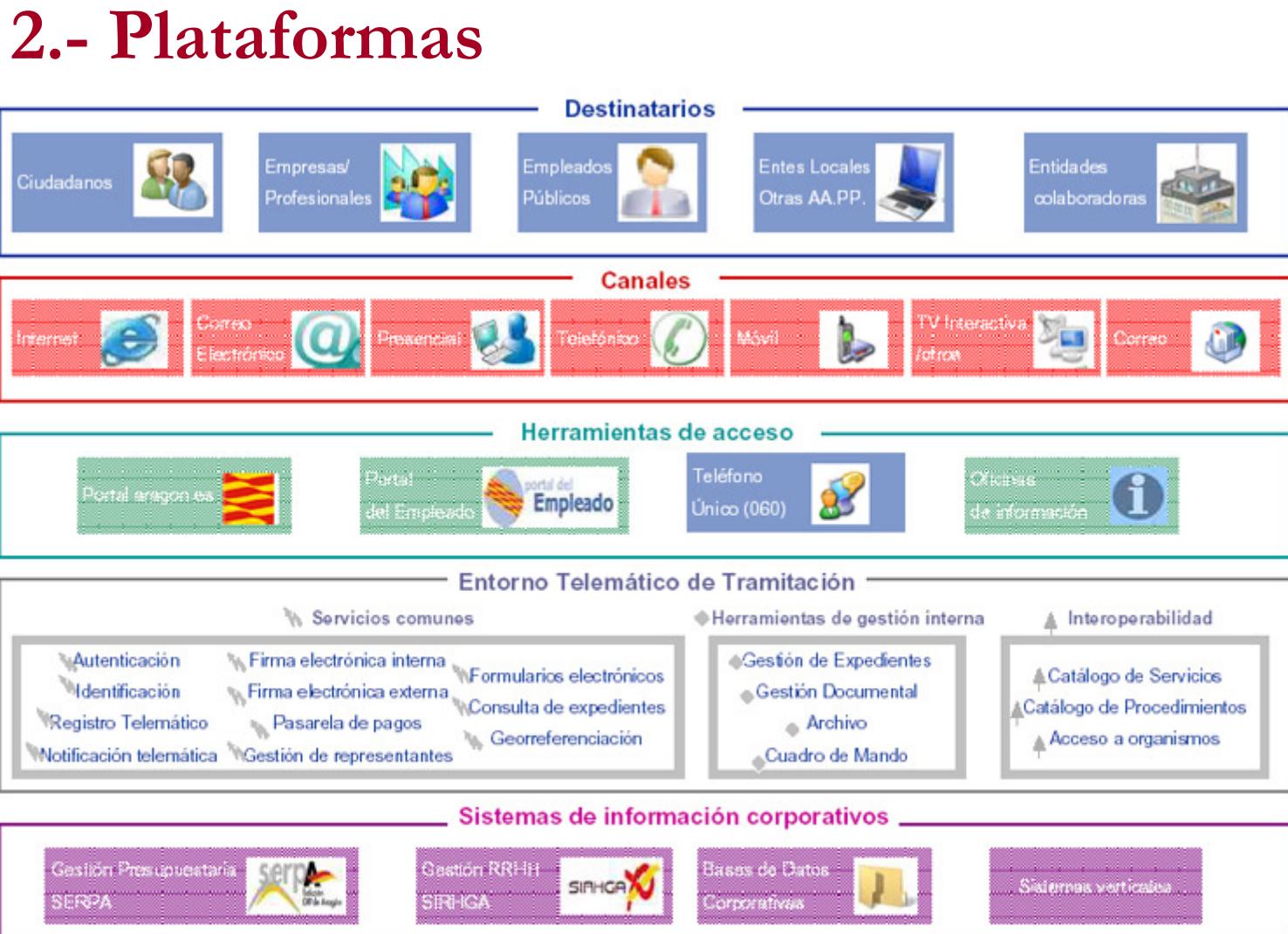
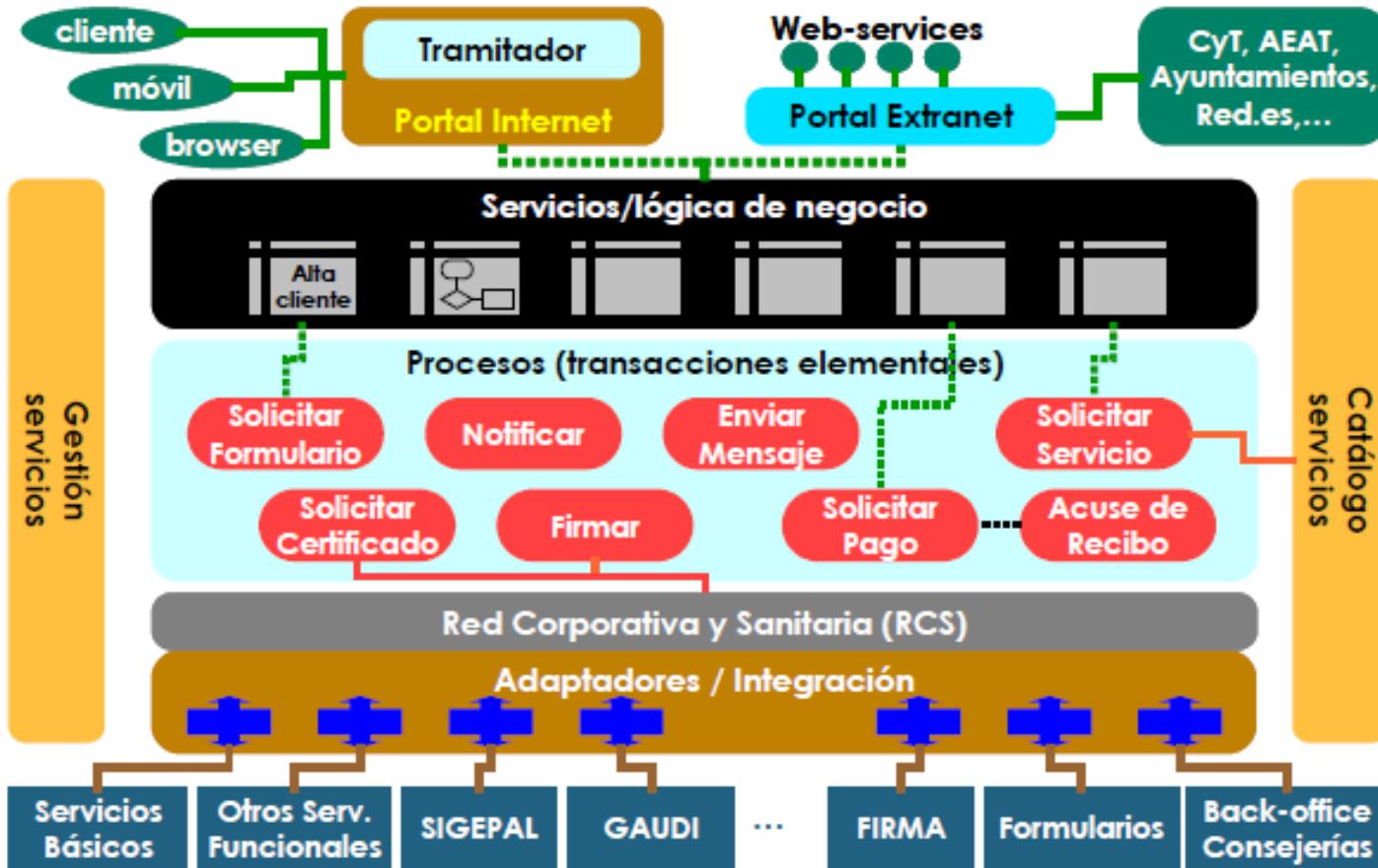


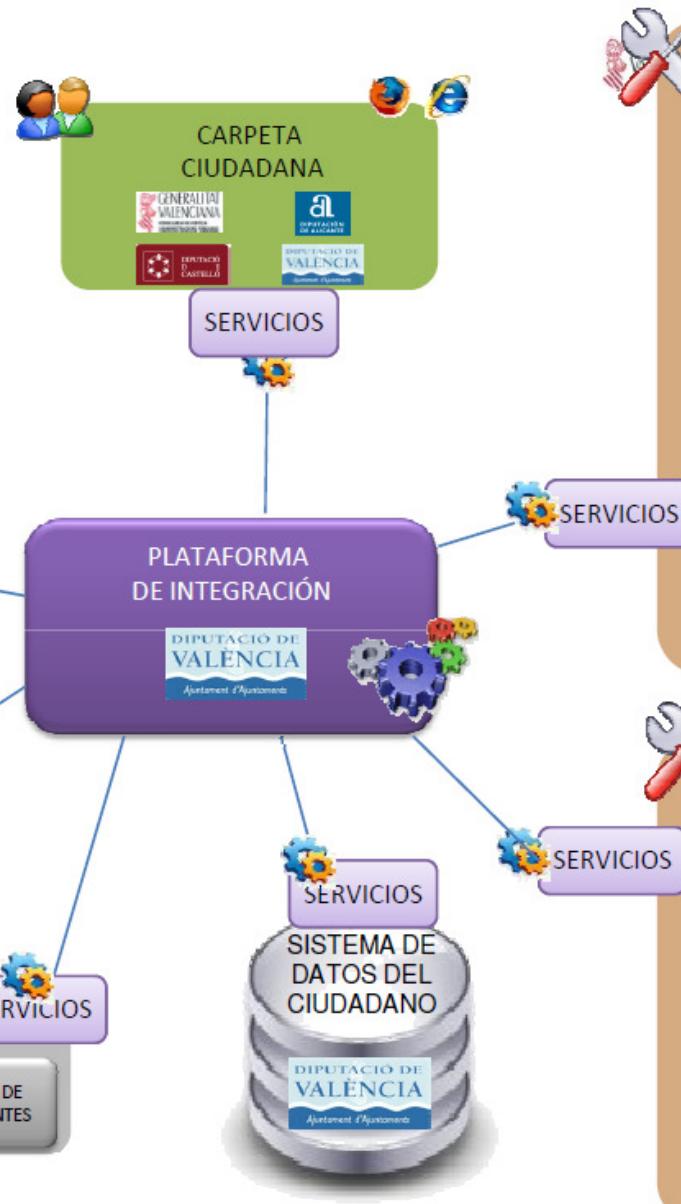
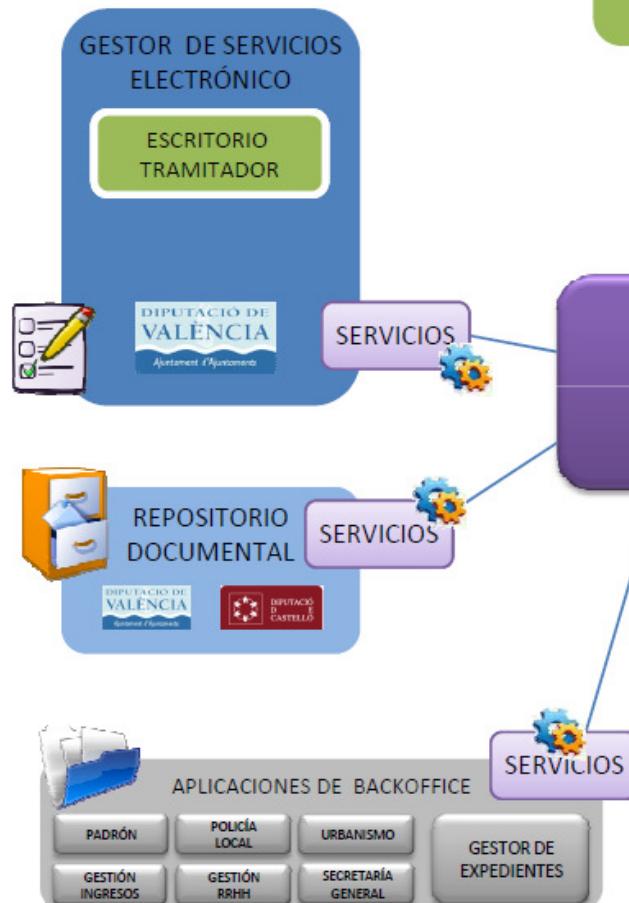
Figura 4: Modelo de Administración Electrónica

2.- Plataformas

3. Arquitectura de Administración electrónica de la CARM

Ejemplos de plataformas





APLICACIONES ADMINISTRACIÓN ELECTRÓNICA

CONTRATACIÓN
ELECTRÓNICA

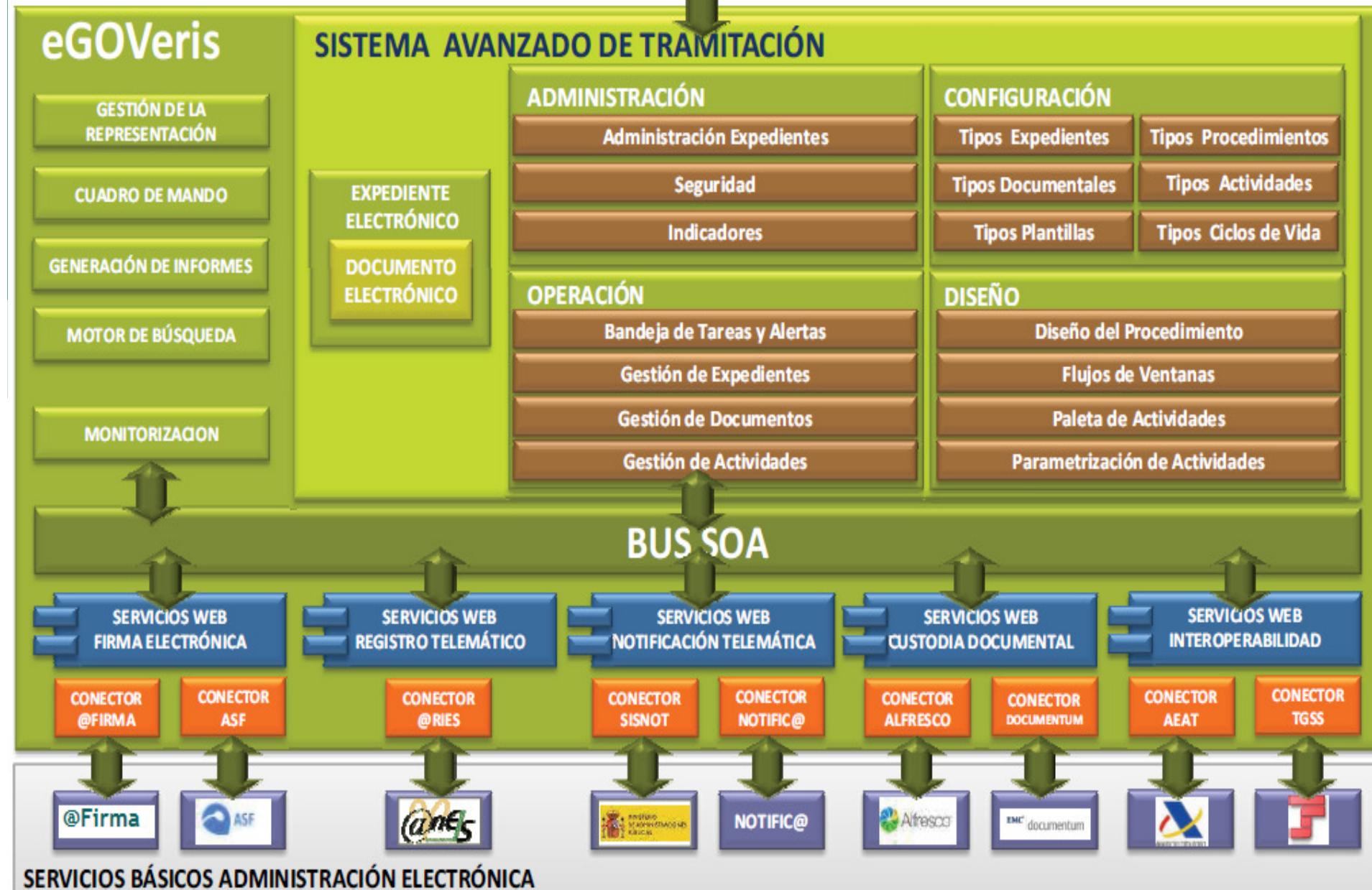
FACTURACIÓN
ELECTRÓNICA

AYUDAS Y
SUBVENCIONES

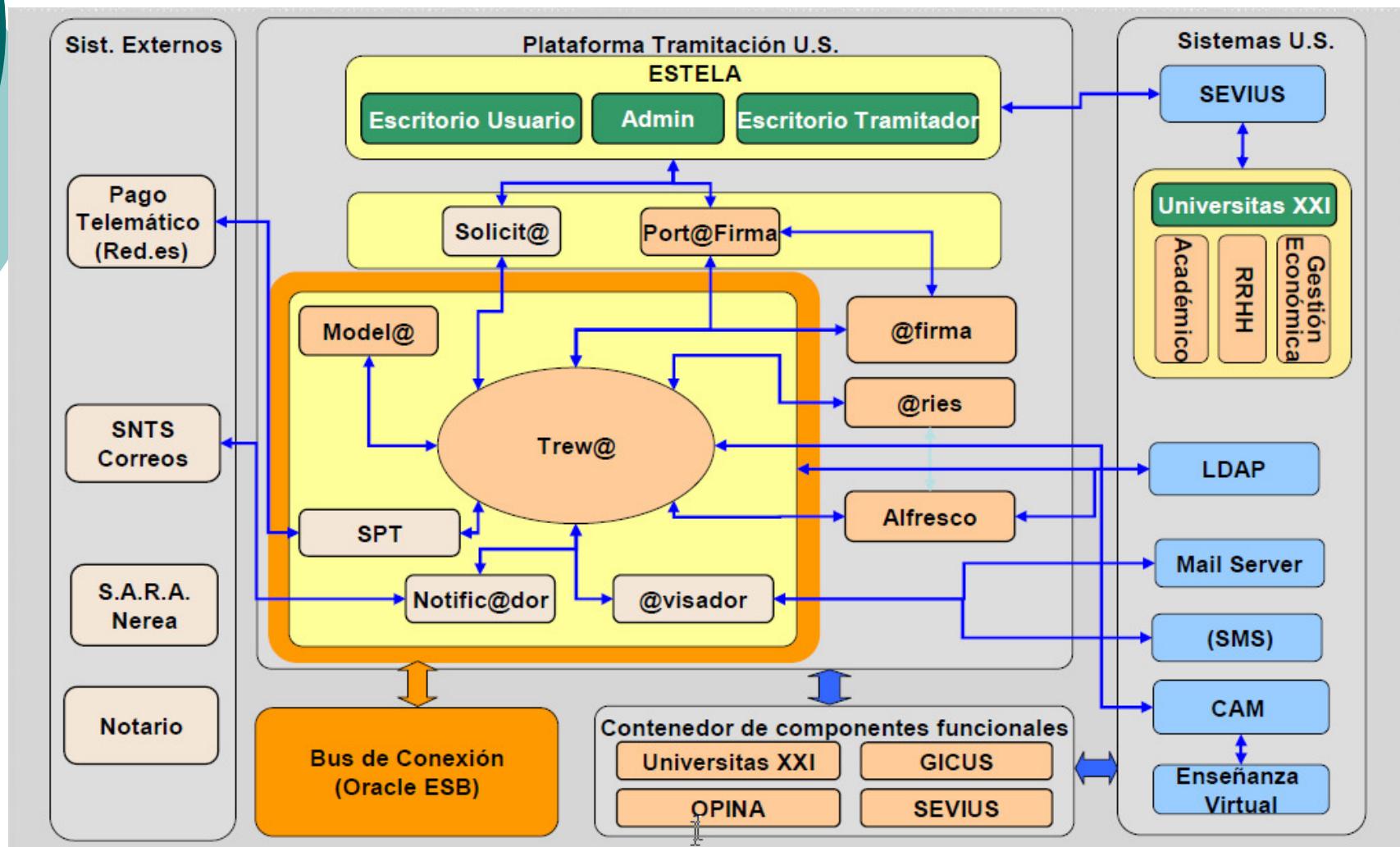
RECLAMACIONES
PATRIMONIALES

SANCIONES

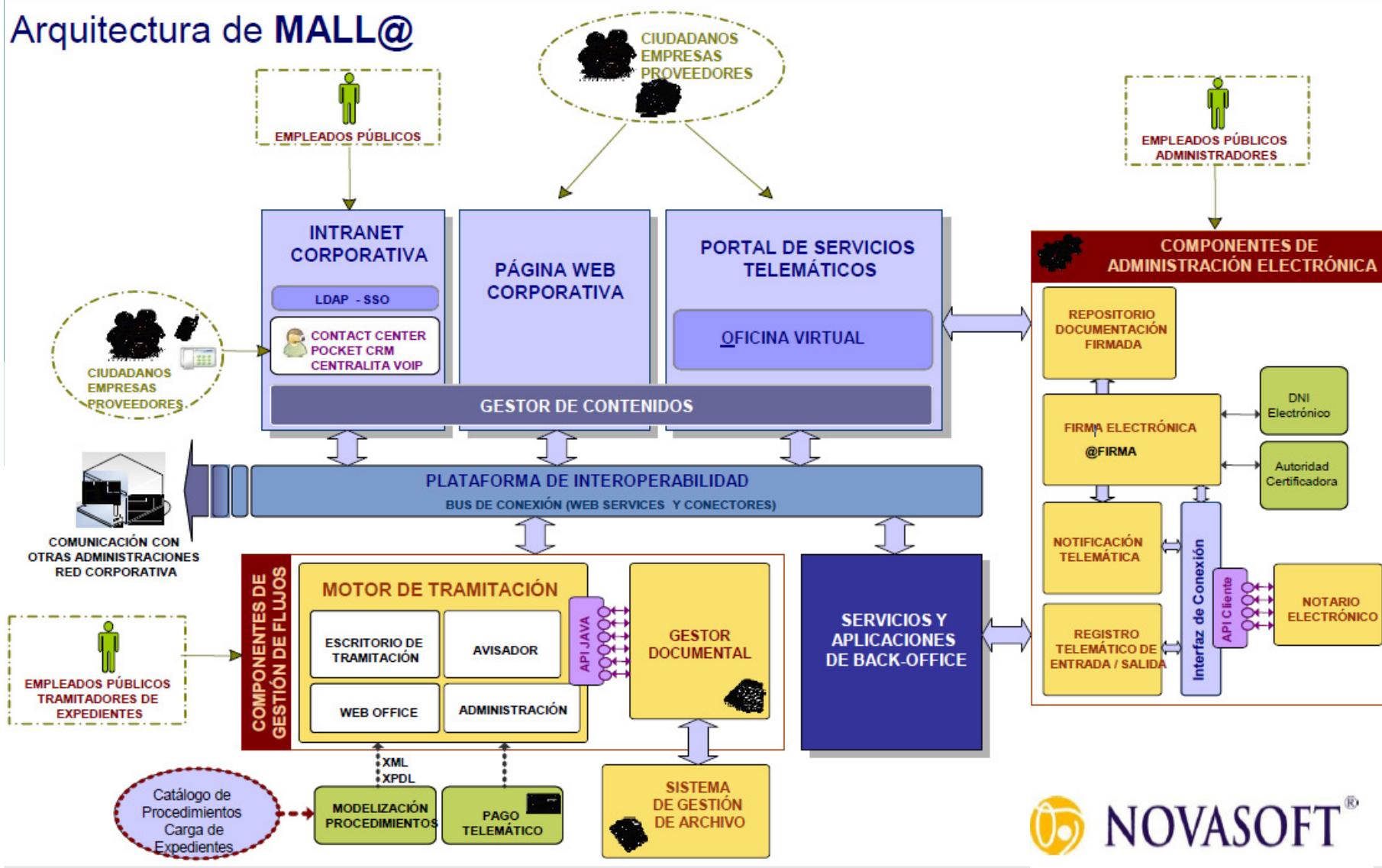
...



2.- Plataformas

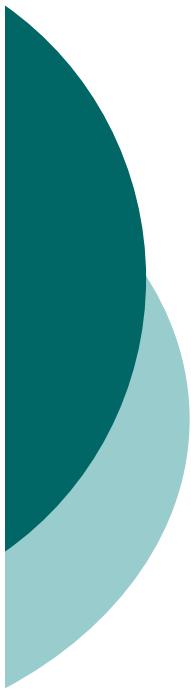


Arquitectura de MALL@



NOVASOFT®





Índice

1. Elementos para la Implementación de la eAdmin
2. Plataformas
3. Componentes
4. Integración con el Backoffice
5. Identidad digital y certificados

3.- Componentes

Componentes



Sede Electrónica



Gestor de formularios



Registro electrónico



Pasarela de pagos



Gestor de expedientes



Notificación electrónica



Identificación electrónica



Archivo electrónico



Interoperabilidad

.....

Fuente:



3.- Componentes: Sede Electrónica



- La sede electrónica o portal del ciudadano es la **herramienta que sirve de puerta de acceso al ciudadano** para toda aquella información y servicios on-line que se ponen a su disposición de forma actualizada y, preferentemente, personalizada.
- Entre los servicios que pueden ofrecerse se encuentran: la **iniciación de trámites, la consulta de estado de expedientes**, los foros de colaboración, descargas, soporte técnico, servicios cartográficos, visitas virtuales, etc.

Fuente:





3.- Componentes: Gestor de formularios

- El gestor de formularios **engloba al conjunto de herramientas que facilitan la construcción, conservación, presentación y utilización de formularios** dentro de la plataforma de administración electrónica.
- El formulario es una pieza fundamental para la presentación y envío de la información de solicitudes, escritos o comunicaciones por parte del interesado hacia el registro.
- En nuestro caso la herramienta es **Solicit@**

Fuente: The logo for cenatic features a large green letter 'C' with a smaller black 'C' nested inside it. To the right of the 'C' is the word 'cenatic' in a bold, sans-serif font. Below the 'C' and 'cenatic' is a smaller line of text: 'Centro Nacional de Referencia de Aplicación de las TIC basadas en fuentes abiertas'.

3.- Componentes: Registro electrónico



- Las tareas fundamentales del registro electrónico son **tomar una referencia de tiempo, anotar el asiento de la entrada/salida, guardar los datos de la presentación de información, y devolver un acuse de recibo** con el número de registro y momento de la presentación.
- El registro podrá asimismo incluir funcionalidades adicionales, como por ejemplo, el sellado de tiempo para obtener la referencia temporal, el cotejo/compulsa electrónica de documentos presentados físicamente o el funcionamiento como registro único para toda la Administración.
- En nuestro caso el Registro es **SIGEM**.

Fuente:





3.- Componentes: Pasarela de pagos

- Su tarea fundamental es **permitir el pago online en aquellos trámites que así lo requieran**. Para ello, la plataforma debe estar integrada con, entre otros elementos, la sede y la firma electrónica, además de existir acuerdo con diferentes entidades bancarias.
- En nuestro caso será TPV Santander o Pasarela de pagos de Red.es

Fuente:



3.- Componentes: Gestor de expedientes



- Con el trámitador o gestor de expedientes se tiene una situación similar a la de la sede electrónica, es decir, aunque es posible el diseño a medida de una herramienta que gestione los flujos de cada trámite, existen soluciones prefabricadas que facilitan la implantación de procedimientos de manera automatizada. Son los “Workflow” y los BPMS (Business Process Management Suite).
- **Estas herramientas**, por medio de un “motor de workflow” situado en el servidor de la red, **van encaminando los expedientes de acuerdo con las reglas establecidas**.
- En nuestro caso el motor es **Trew@**

Fuente:





3.- Componentes: Notificación electrónica

- Es el sistema que **permite el envío de comunicaciones** escritas y mensajes en general a los interesados siguiendo las reglas y protocolos oficiales de la notificación electrónica (Real Decreto 209/2003, de 21 de febrero).
- Deberá por una parte **realizar el aviso al receptor de la notificación** (interesado) y por otra **permitir el acceso electrónico a la lectura de las notificaciones**. El sistema deberá tener constancia de la recepción, acceso y lectura de las notificaciones por parte del usuario.
- En nuestro caso herramienta interna de la plataforma e integración con SISNOT (Servicio de Notificaciones Telemáticas Seguras)



3.- Componentes: Identificación y firma electrónica

- La **identificación y autenticación** de ciudadanos y empresas, así como la de funcionarios públicos y sedes electrónicas se realiza con ayuda de la plataforma de firma electrónica.
- Asimismo, las **operaciones de firmado** de documentos por parte de ciudadanos y empleados públicos también se incluye dentro de las funcionalidades de la plataforma de firma electrónica.
- Las funcionalidades anteriores son normalmente cubiertas por una única solución dentro del mercado. Sin embargo, a menudo las Administraciones disponen de otros componentes adicionales como por ejemplo el que facilita la gestión de las operaciones de firma, permitiendo la visualización del conjunto de documentos pendientes de firma y, si procede, su firma por lotes (**portafirmas**).
- **@firma** y **Portafirm@s** en nuestro caso

Fuente:





3.- Componentes: Archivo electrónico

- Es el sistema que **ofrece almacenamiento seguro para los documentos y ficheros relacionados con cada expediente**, gestionando el ciclo de vida de cada documento desde su creación y registro hasta su archivo definitivo (preservación y custodia).
- Además de la funcionalidad de **almacenamiento** permite la **recuperación** y **consulta** de los documentos de cada procedimiento administrativo tanto por parte de los **empleados** de la Administración como de los **interesados** en el procedimiento.
- **Alfresco** será nuestra herramienta.

Fuente:



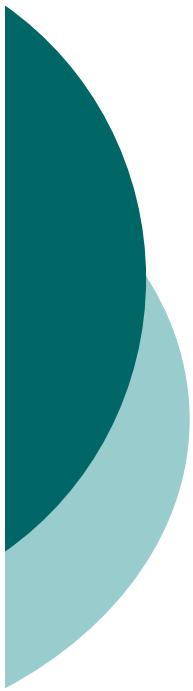


3.- Componentes: Interoperabilidad

- Implementa un **sistema de intercambio de datos** que evita el requerimiento de información al ciudadano que se encuentra ya en poder de otros departamentos dentro de la misma Administración o de otras Administraciones.
- En nuestro caso integración con UXI, integración en servicios de la Red Sara .

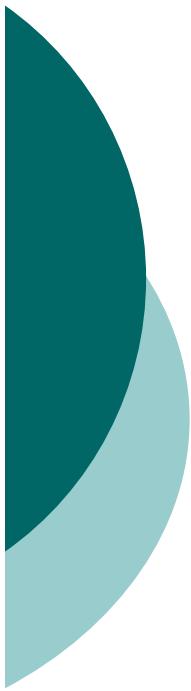
Fuente:





3.- Componentes

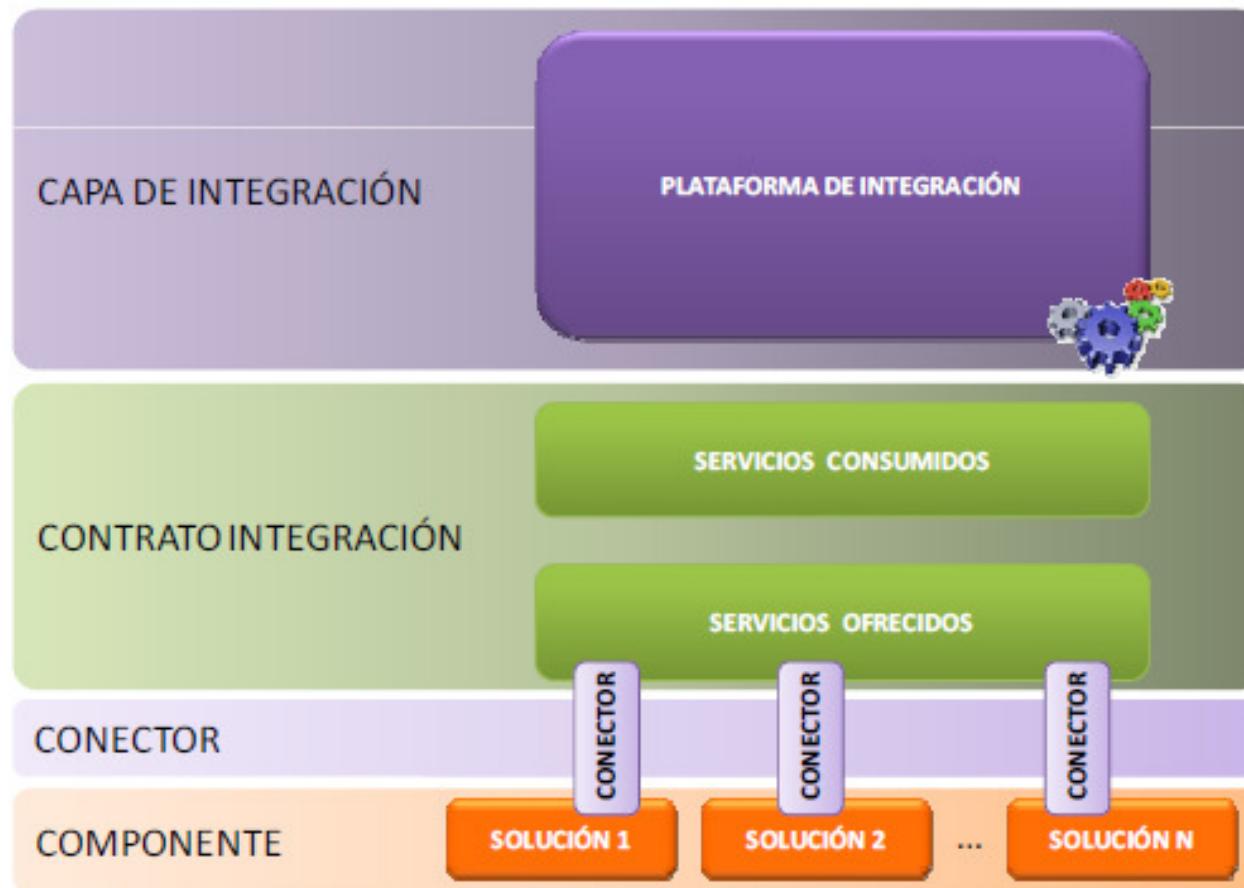
- Toda la información en:
 - <http://www.cenatic.es/laecsp>
 - <https://ws024.juntadeandalucia.es>



Índice

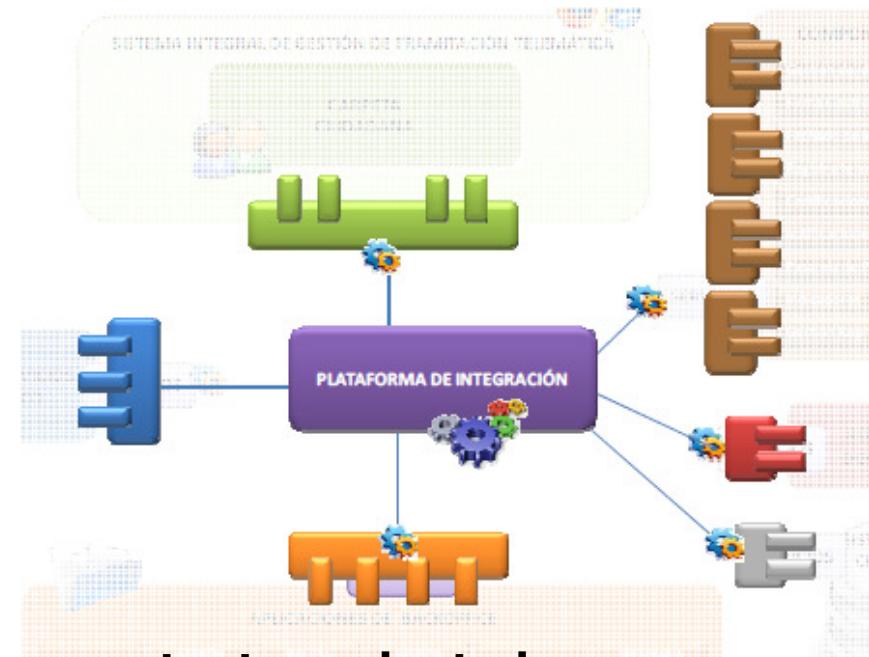
1. Elementos para la Implementación de la eAdmin
2. Plataformas
3. Componentes
4. Integración con el Backoffice
5. Identidad digital y certificados

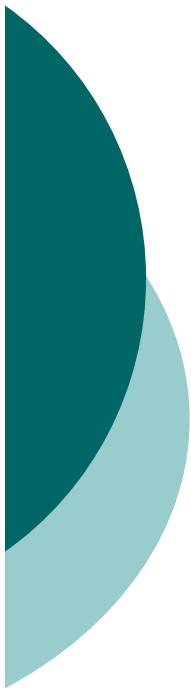
4.- Integración con el Backoffice



4.- Integración con el Backoffice

- Puesto que las soluciones seleccionadas en cada componente no conocen de forma nativa el interface definido, **será necesario construir un adaptador que relacione dicho “contrato” (interface) con la solución concreta.**
- Potencialmente **se podrán crear tantos adaptadores como soluciones a un componente concreto** se deseen integrar en la plataforma. De esta forma se asegura que la plataforma permite continuar utilizando los componentes ya seleccionados por las distintas administraciones de forma independiente.





Índice

1. Elementos para la Implementación de la eAdmin
2. Plataformas
3. Componentes
4. Integración con el Backoffice
5. Identidad digital y certificados



Introducción

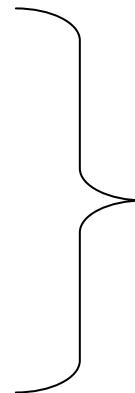
Una gestión telemática a través de Internet implica, entre otros:

- **Identificación:** *de remitente y destinatario, estando los datos de identidad completos, sin ambigüedad a la hora de establecer la identidad de una persona física o jurídica.*
- **Autentificación:** *garantía de conocer fehacientemente la identidad de una persona física o jurídica*
- **No repudio:** *imposibilidad de rechazar la autoría de una determinada acción o documento*
- **Confidencialidad:** *sólo se muestran los datos o páginas al usuario autorizado a ello*
- **Integridad:** *la información no fue manipulada y corresponde a su estado original*

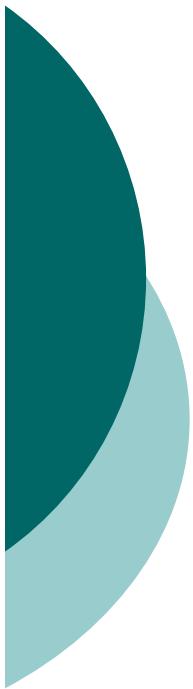
Introducción

Para alcanzar estos objetivos,..... surgen:

- Identificación
- Autentificación
- No repudio
- Confidencialidad
- Integridad

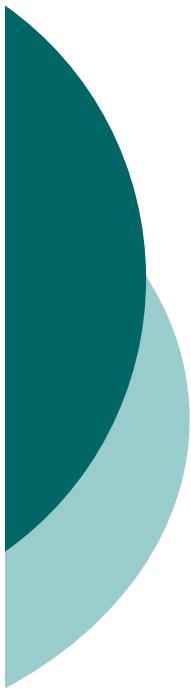


Certificados Electrónicos
Firma Electrónica



Introducción

- Con ayuda de los **certificados electrónicos** se puede realizar la protección de la información mediante un cifrado o transformación criptográfica (ocultamiento o enmascaramiento de la información de forma que no sea legible sin realizar la operación inversa) de los mensajes, haciendo su contenido ilegible salvo para el destinatario.
- Con ayuda de los mismos **certificados electrónicos** y aplicando un algoritmo de **firma electrónica**, obtenemos de un texto, una secuencia de datos que permiten asegurar que el titular de ese certificado ha ‘firmado electrónicamente’ el texto y que éste no ha sido modificado.



Identificación



Identificación

Identidad Digital

La identificación electrónica debe permitir verificar la identidad de una persona que no se halle en presencia de otra.



Identificación

Identidad Digital vs. Presencial

En el **mundo físico** la comprobación se hace contrastando algún **rasgo físico o de comportamiento** con algún patrón o comportamiento certificado por un **tercero de confianza**.

Ej. **DNI**: un tercero de confianza (Ministerio del Interior) certifica determinados rasgos o de conducta de una persona:

- Rasgos físicos: foto de la cara y huella dactilar
- Rasgos de conducta: firma manuscrita



Identificación

Necesidad de la Identidad Digital

-Hay multitud de relaciones no presenciales que necesitan identificación:

- Compras por correo/internet
- Transacciones por teléfono
- Operaciones a través de SMS/Internet

-La LOCM (Ley de Ordenación del Comercio Minorista) establece que cuando el importe de una compra hubiese sido cargado utilizando el número de una **tarjeta de crédito, sin que ésta hubiese sido presentada directamente o identificada electrónicamente**, su titular podrá exigir la **inmediata anulación del cargo**.



Identificación

Sistemas de identificación no presenciales

- **Secreto compartido:** los dos lo saben
 - Claves de acceso, códigos pin, tarjetas de coordenadas
 - Puede tener la consideración de firma electrónica⁽¹⁾
 - Problema: sólo pueden conocer dos partes, no sirve para relacionarse con un tercero.



(1) Se ajusta a la definición que de la misma da la Ley 59/2003, "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"

Identificación

Sistemas de identificación no presenciales

- Algún **rasgo propio y único de la persona que puede ser comparado con un patrón:**
 - Sistemas **biométricos**: reconocimiento del iris, de la huella, de la voz, etc.
 - Poco práctico en relaciones múltiples (proveedores de identidad, lectores en dispositivos, etc.)
- En un futuro...



Identificación

Sistemas de identificación no presenciales

- Elemento (físico o lógico) que sólo tiene una persona y que pone a disposición de otra
 - Certificados digitales
 - DNI-e





Identificación

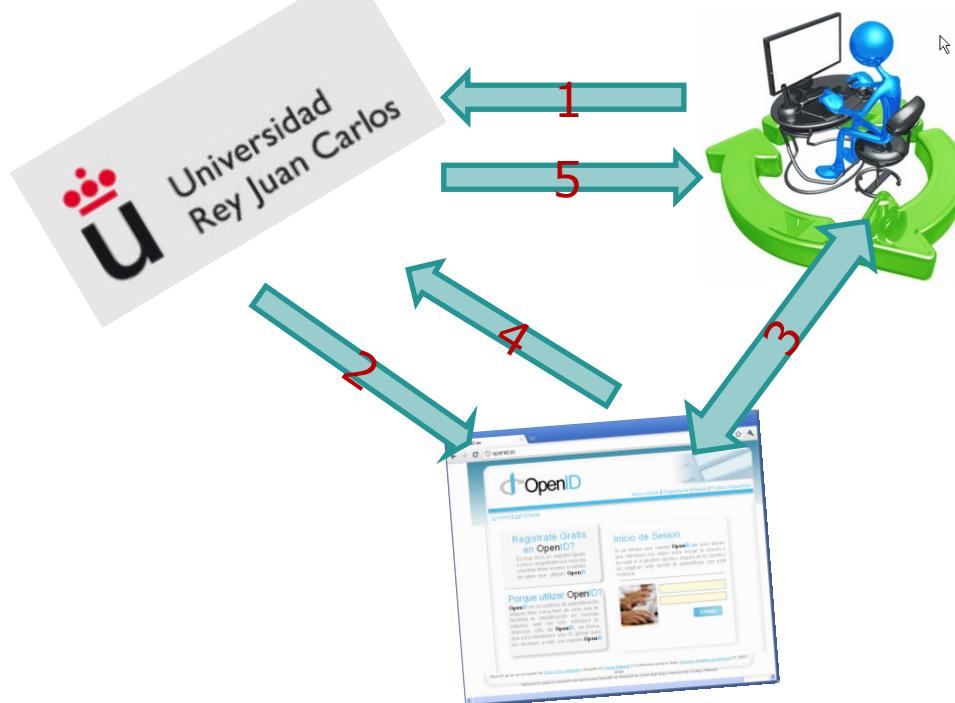
Verificación de identidades: Autentificación

- Si hay numerosas formas de tener una identidad digital, ¿cómo puedo yo asegurar que quien se relaciona conmigo es quién dice ser?.
- Los alumnos y empleados se validan con cuentas que ha proporcionado la propia universidad, pero con la eAdmin se podrán relacionar con nosotros cualquier ciudadano (empresas, opositores, futuros alumnos, etc.).
- Si alguien se identifica con un DNIe debo validarla contra el Ministerio de Interior.
- Si alguien paga con una tarjeta debo validarla contra la entidad bancaria.
- ... (problema debo poder hablar con cada posible emisor de identidades para poder validarlas).

Autenticación

Federación de Identidades

Prestador del servicio:SP



1. El usuario solicita identificarse al SP
2. El SP solicita la identificación al IDP
3. El IDP solicita al usuario las credenciales para autenticarse
4. El IDP informa al SP del resultado de la autenticación y de la información del usuario
5. En función del resultado el SP permite el acceso al usuario

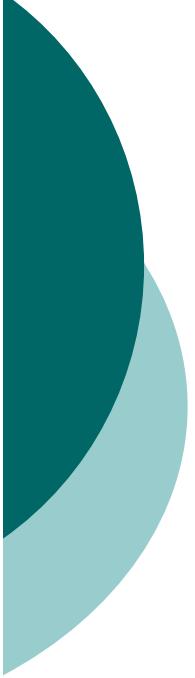
Proveedor de identidad: IDP

Autenticación

Confianza en los proveedores de Identidad

- ¿En qué se basa la confianza en un proveedor de identidad?
 - La fortaleza del **proceso de registro**
 - La fortaleza del **sistema de autenticación**





Autentificación

Fortaleza proceso de registro

- Para obtener el DNI electrónico hay que ir a comisaria. (Fuerte).
 - Para obtener un certificado digital de la FNMT hay que personarse en una oficina de registro. (Fuerte).
 - Para obtener una tarjeta de crédito hay que abrir una cuenta en un banco, en persona, y recibir el pin en el domicilio. (Fuerte).
 - Para crear una cuenta en multitud de sitios web (facebook, google, etc...) tan sólo hay que tener una dirección de correo electrónico. (Débil).
-

Autenticación

Fortaleza autenticación: autenticación por multifactor

- Autenticación mediante dos factores:
 - Algo que tengo: **tarjeta de crédito**
 - Algo que se: un número **pin**
- Autenticación triple factor:
 - Algo que tengo: **tarjeta**
 - Algo que se: una clave tipo **pin**
 - Algo que soy: la **huella dactilar**



Autenticación

El ideal

Utilizar autenticación multifactor (tipo DNIe) para cualquier necesidad de identificación electrónica



Login or Signup *recommended*
Select one of these third-party accounts

Sign in using your account with



Certificado digital

La solución para garantizar la seguridad en el uso de medios electrónicos está basada en una técnica que se denomina:

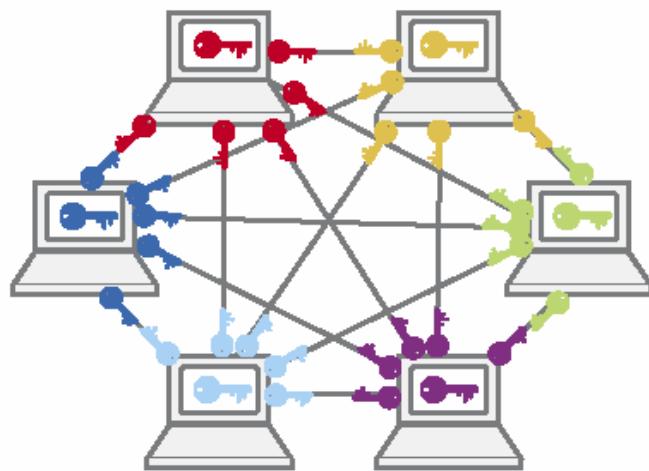
Criptografía



‘La criptografía (del griego κρύπτω krypto, «oculto», y γράφω graphos, «escribir», literalmente «escritura oculta») es la técnica, bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje.’

Certificado digital

Existe la **Criptografía Simétrica** y la **Criptografía Asimétrica**.

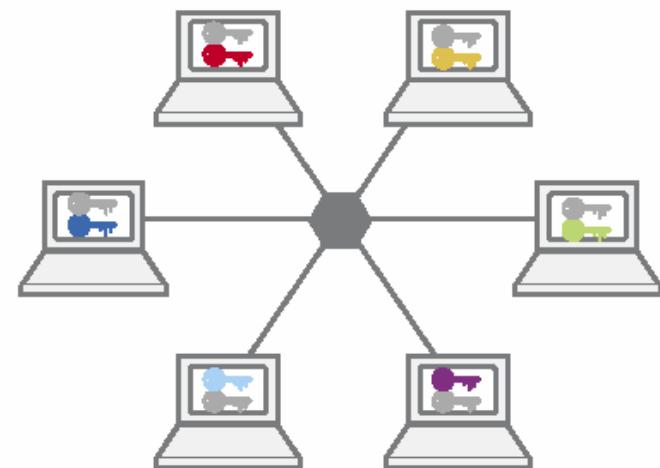


SIMÉTRICO

En la Criptografía Simétrica, se pueden calcular el número de llaves necesarias con la ecuación

$$\frac{n \cdot n - 1}{2}$$

En un caso con 1000 usuarios, se generarán 499500 llaves



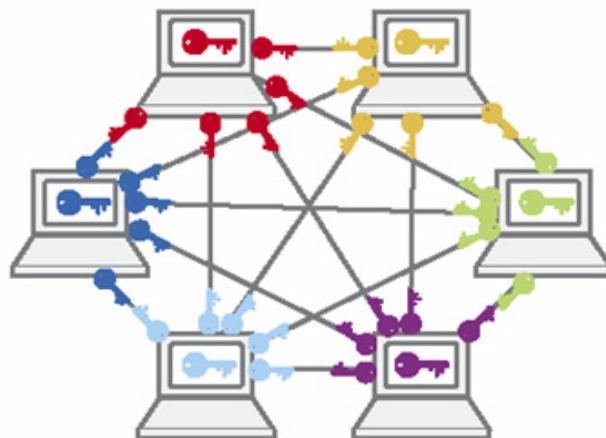
ASIMÉTRICO

En la Criptografía Asimétrica, se utilizan sólo un par de llaves para cada usuario, por lo tanto para n cantidad de usuarios, se necesitarán n pares de llaves

En un caso con 1000 usuarios, se generarán 1000 llaves

Certificado digital

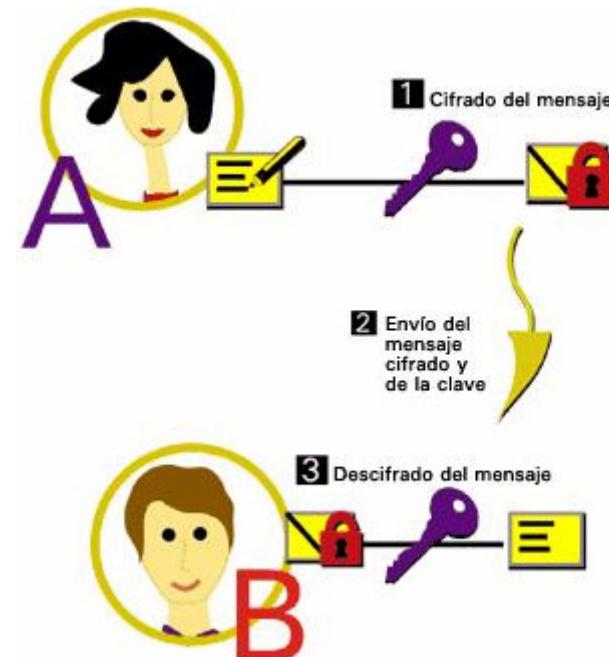
Criptografía Simétrica



SIMÉTRICO
En la Criptografía Simétrica, se pueden calcular el número de llaves necesarias con la ecuación

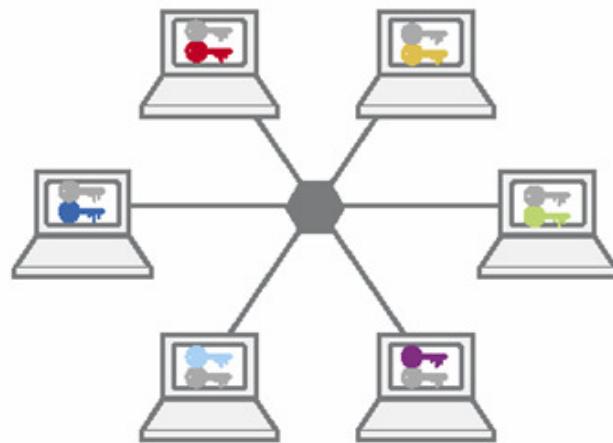
$$\frac{n \cdot n - 1}{2}$$

En un caso con 1000 usuarios, se generarán 499500 llaves



Certificado digital

Criptografía Asimétrica



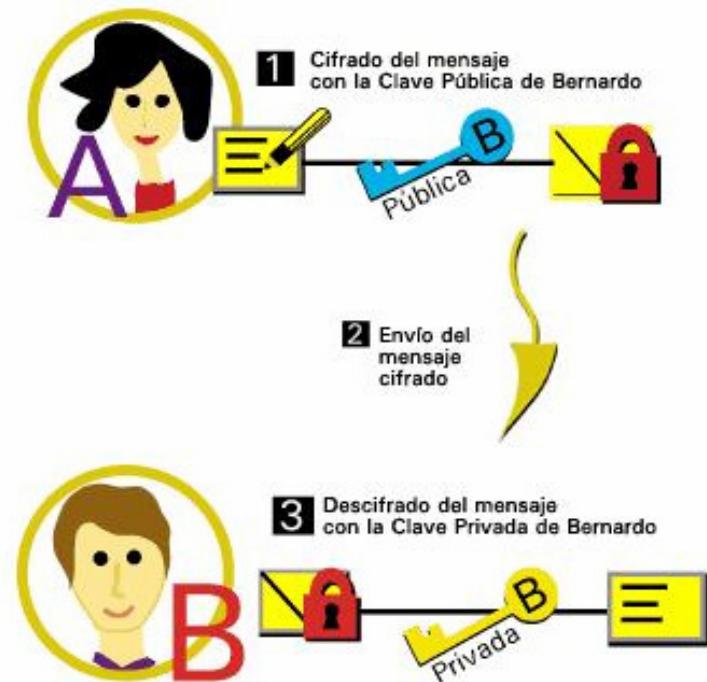
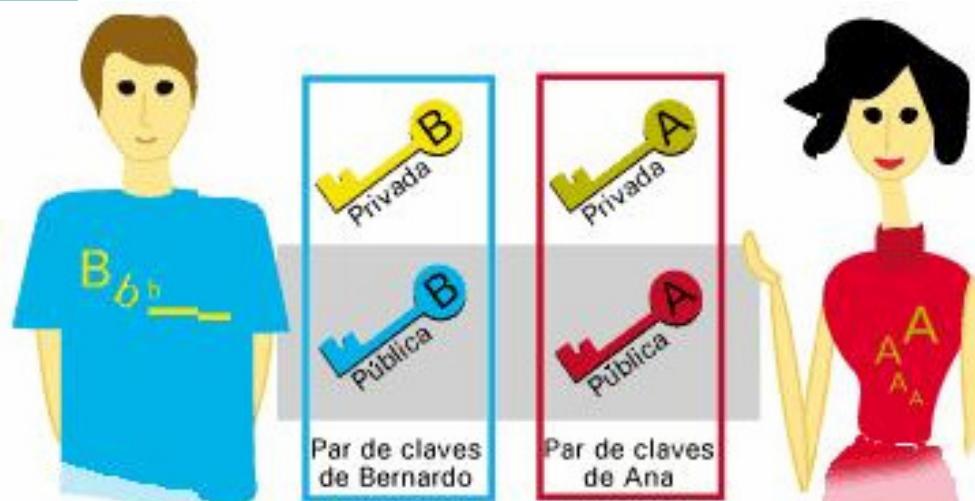
ASIMÉTRICO
En la Criptografía Asimétrica, se utilizan sólo un par de llaves para cada usuario, por lo tanto para n cantidad de usuarios, se necesitarán n pares de llaves

En un caso con 1000 usuarios, se generarán 1000 llaves



Certificado digital

Los Certificados Digitales están basados en la utilización, en este caso, de la **Criptografía Asimétrica**.





Certificado digital

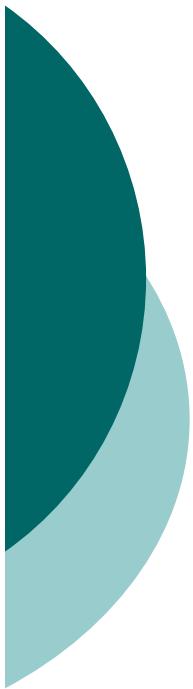
- Posee dos claves:
 - **Clave privada:** hay que protegerla.
 - **Clave pública:** para distribuirla entre los que deban comunicarse con el propietario del certificado.
- Estas claves no son claves “al uso”, **no es “el PIN”**, que el usuario pueda o deba recordar, pero sí debe proteger su uso y/o distribución.
 - La clave pública se distribuye.
 - La clave privada no se distribuye, sólo se usa.



Certificado digital

Mediante el uso de certificados, con criptografía asimétrica, se pueden llevar a cabo las siguientes operaciones:

- Autentificación
- Cifrado
- Confidencialidad
- Firma electrónica
- No repudio
- Integridad



Certificado digital

- Un **certificado digital** es un documento electrónico mediante el cual un **tercero de confianza** (una **autoridad de certificación**) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.
 - Este tercero de confianza exige los requisitos para identificar con garantías absolutas al sujeto del certificado. Si es una persona física se le exigirá que se persone con su DNI.
-



PSC (*Prestador del Servicio de Certificación*)

- Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
- Se define en la Ley 59/2003 de Firma Electrónica y en otras normativas relacionadas con la certificación digital.
- Son servicios de Certificación los siguientes:
 - **Autoridad de Certificación (AC)** → *responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica*
 - **Tercero de confianza**
 - **Servicios de Custodia de Documentos Electrónicos**
 - **Servicios de Consulta de Atributos**
 - **Autoridad de Validación**
 - **Autoridad de Sellado de Tiempo**



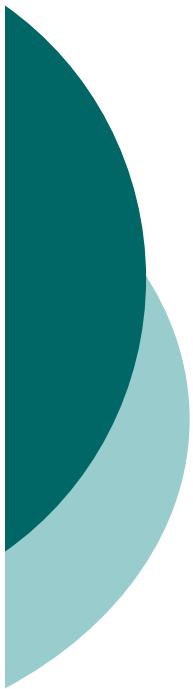
Certificados cualificados (*reconocidos*)

- Directiva 1993/93/CE y Ley 59/2003 de firma electrónica
 - **Incluirán al menos los siguientes datos:**
 - La indicación de que se expedan como tales.
 - El código identificativo único del certificado.
 - La identificación del PSC (*Prestador del Servicio de Certificación*) que expide el certificado y su domicilio.
 - La firma electrónica avanzada del PSC que expide el certificado.
 - La identificación del firmante.
 - Los datos de verificación de firma (clave pública)
 - El comienzo y el fin del periodo de validez del certificado.
 - Los límites de uso del certificado, si se establecen.
 - **Los PSC (*Prestadores de Servicios de Certificación*) deberán:**
 - Comprobar la identidad y circunstancias.
 - Verificar que la información del certificado es exacta.
 - Asegurarse que el firmante está en posesión de los datos de creación de firma (la clave privada).
 - Un certificado cualificado ha pasado por un **registro fuerte**. En consecuencia, los IDP (Proveedor de servicios de Identificación) que usen certificados cualificados y sistemas de autenticación multifactor serán los más confiables.
-



Titulares de los Certificados Cualificados

- Conforme a la Directiva 1993/93/CE sólo pueden ser firmantes las personas físicas, actuando en nombre propio o en representación de una entidad.
- Conforme a la Ley 59/2003, de firma electrónica:
 - Las personas físicas, actuando en nombre propio o en representación de una entidad.
 - Las personas jurídicas.
 - Las entidades carentes de personalidad jurídica a las que se refiere el actual artículo 35.4 Ley General Tributaria.



Terceras Partes de Confianza

¿Cómo confiar si un determinado certificado es válido o si está falsificado?.

- La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado.
- La validez del certificado en un entorno de clave pública es esencial ya que se debe conocer si se puede confiar o no en que el destinatario de un mensaje será o no realmente el que esperamos.



Terceras Partes de Confianza

¿Cómo confiar si un determinado certificado es válido o si está falsificado?

- La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la confianza en **terceras partes**.
- La idea consiste en que dos usuarios puedan confiar directamente entre sí, si ambos tienen relación con una tercera parte ya que ésta puede dar fé de la fiabilidad de los dos.



Terceras Partes de Confianza

¿Cómo confiar si un determinado certificado es válido o si está falsificado?

- La necesidad de una Tercera Parte Confiable (TPC ó TTP, Trusted Third Party) es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada.
- Además, la mejor forma de permitir la distribución de los claves públicas (o certificados digitales) de los distintos usuarios es que algún agente en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

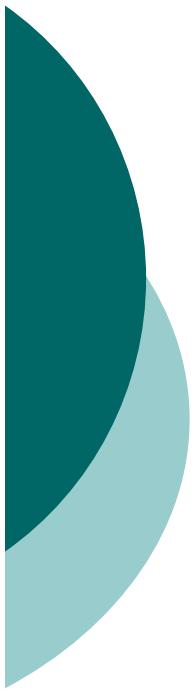




Terceras Partes de Confianza

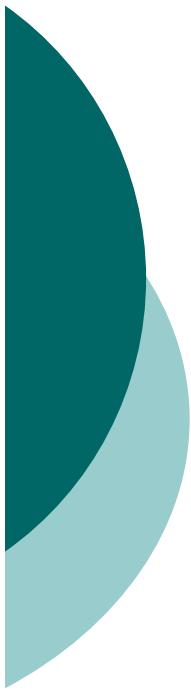
¿Cómo confiar si un determinado certificado es válido o si está falsificado?

- En conclusión, se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si dicho certificado está avalado por una tercera parte en la que sí confiamos.
- La forma en que esa tercera parte avalará que el certificado es de fiar es mediante su firma digital sobre el certificado.
- Por tanto, podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos.
- La TPC que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave pública se conoce con el nombre de **Autoridad de Certificación (AC)**.



Infraestructura de Clave Pública

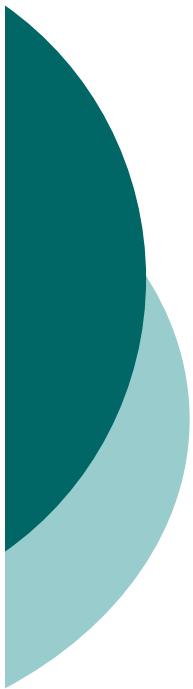
- El modelo de confianza basado en Terceras Partes Confiables de Confianza es la base de la definición de las **Infraestructuras de Clave Pública** (ICPs o PKIs, Public Key Infrastructures).
- Una infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.



Infraestructura de Clave Pública

Algunos de los servicios ofrecidos por una ICP son los siguientes:

- Registro de claves: emisión de un nuevo certificado para una clave pública.
- Revocación de certificados: cancelación de un certificado previamente emitido.
- Selección de claves: publicación de la clave pública de los usuarios.
- Evaluación de la confianza: determinación sobre si un certificado es válido y qué operaciones están permitidas para dicho certificado.
- Recuperación de claves: posibilitación de recuperar las claves de un usuario.



Infraestructura de Clave Pública

Las ICPs están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:

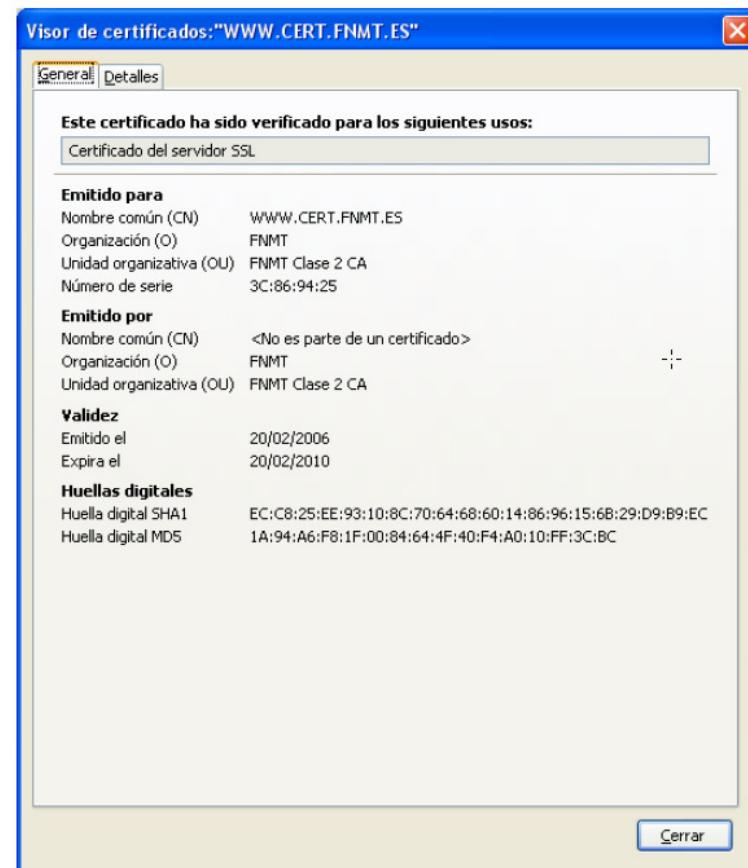
- Autoridad de Certificación
- Autoridad de Registro
- Otras Terceras Partes Confiables como por ejemplo las Autoridades de Fechado Digital

Un certificado

De persona



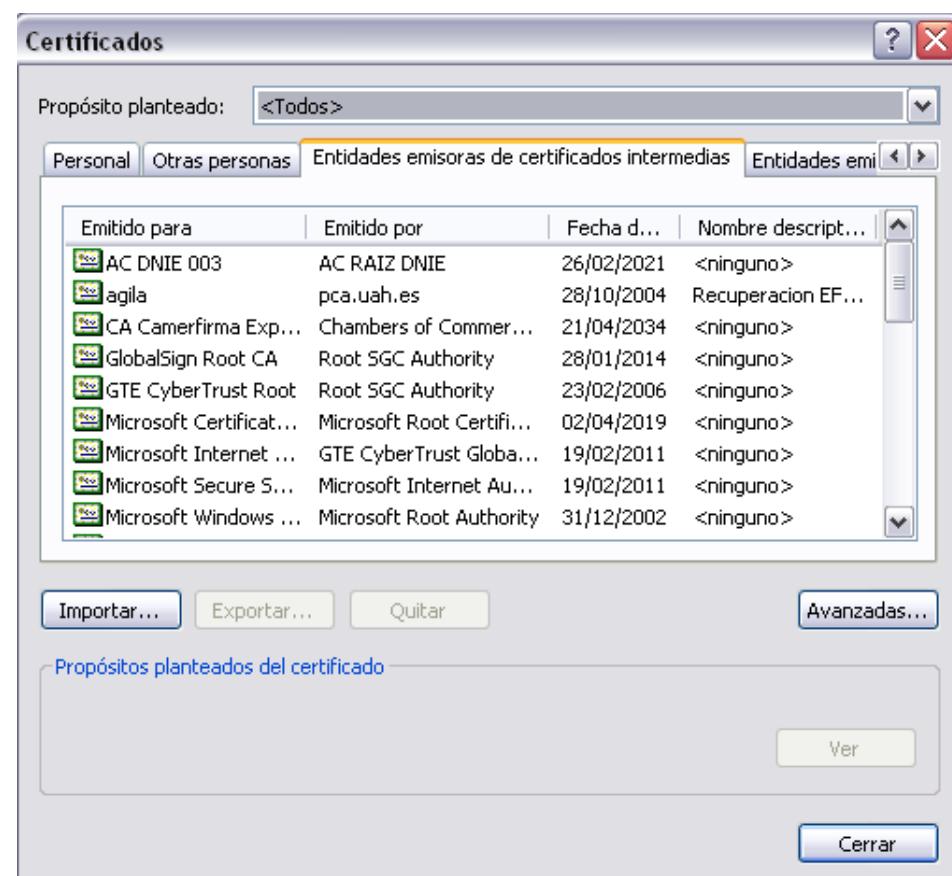
De servidor



Un certificado

- Ver Certificados en Explorer

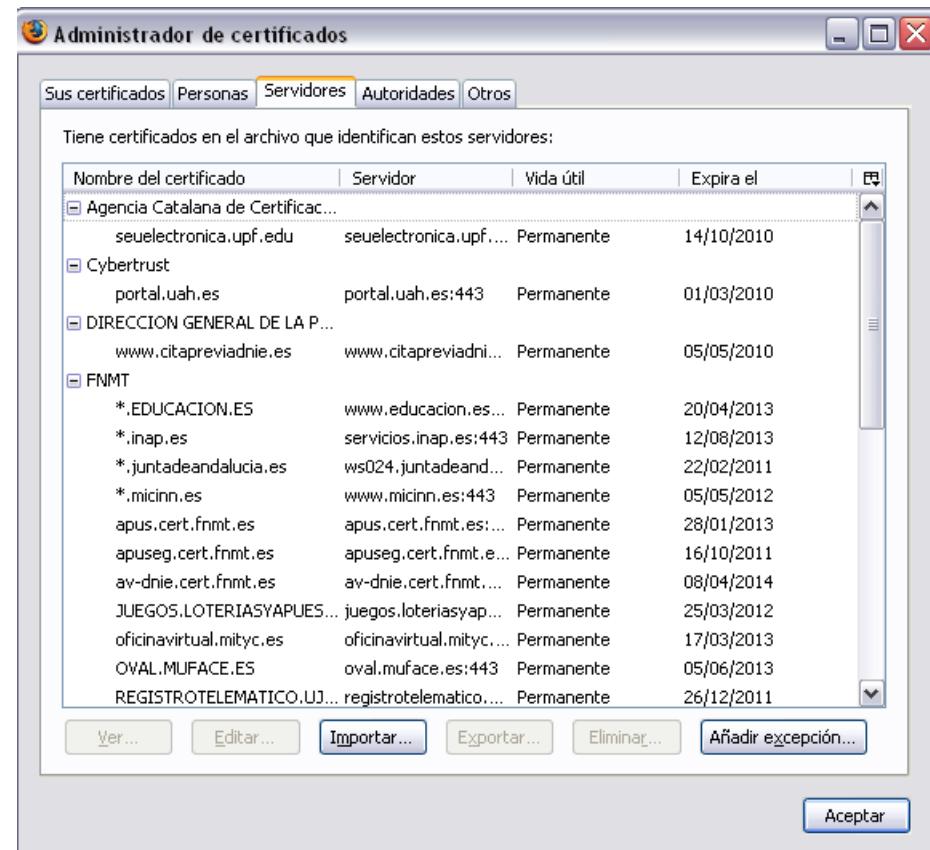
Herramientas>
Opciones_de_Internet
Contenido>
Certificados



Un certificado

- Ver Certificados en Firefox

Herramientas>
Opciones
Avanzado>
Ver Certificados





Un certificado

Veamos el certificado de servidor

- Acceder a www.seg-social.es
- Visualizar información de seguridad

Explorer: Archivo > Propiedades

Firefox: Herramientas > Información de la página



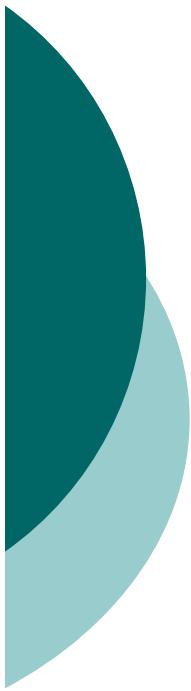
Un certificado

Veamos el certificado de servidor

- Acceder a www.seg-social.es > Sede Electrónica
- Visualizar información de seguridad

Explorer: Archivo > Propiedades

Firefox: Herramientas > Información de la página >
Seguridad > Ver Certificado



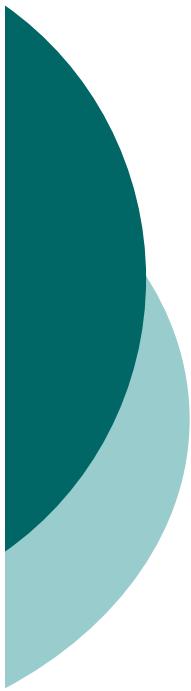
Autoridades de Certificación

- Se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si dicho certificado está avalado por una tercera parte en la que sí confiamos. La forma en que esa tercera parte avalará que el certificado es de fiar es mediante su firma digital sobre el certificado. Por tanto, podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos.
 - La Tercera Parte de Confianza (TPC) que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave pública se conoce con el nombre de Autoridad de Certificación (AC).
-



Autoridades de Certificación

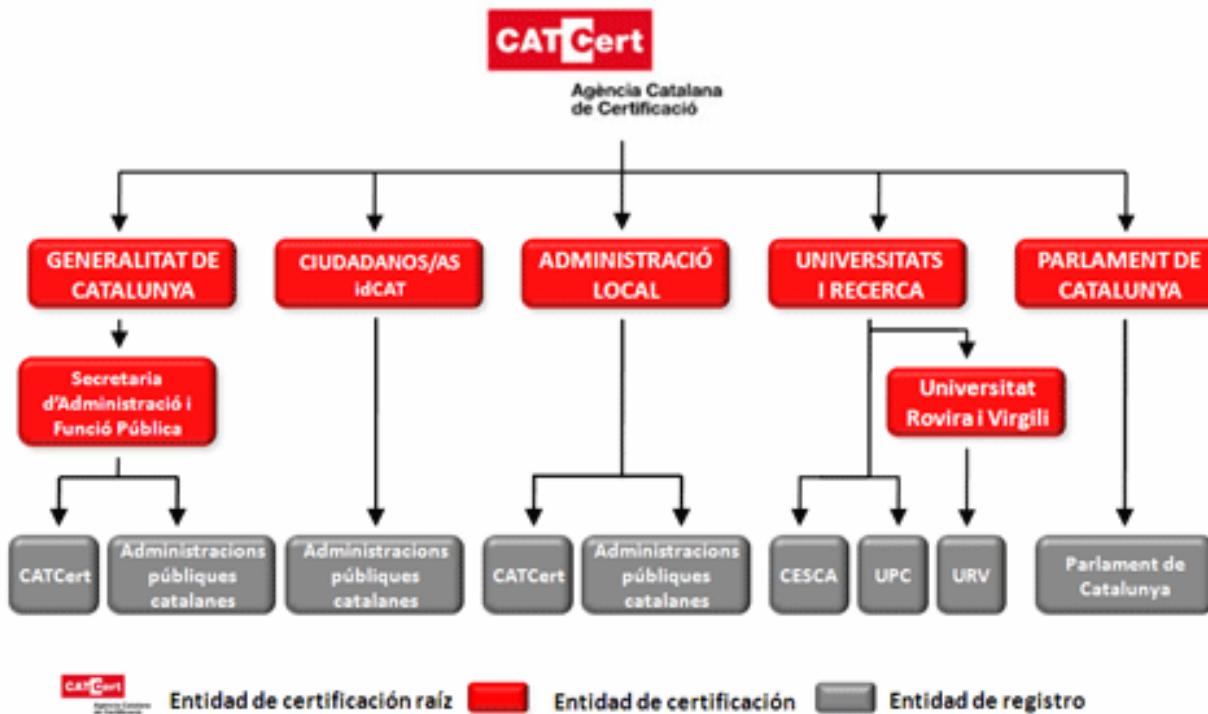
- Una Autoridad de Certificación (**CA**) **avalía la identidad de los sujetos a los que expide los certificados**, actuando de forma parecida a un notario que da fe de un hecho jurídico.
- Para ello firma con su clave privada los certificados emitidos, avalando así la identidad del dueño del certificado emitido.
- Pone a disposición su propio certificado con su clave pública, lo que permitirá validar sus firmas electrónicas.
- Ofrece servicios para la verificación de la validez del certificado, ya que aunque el certificado indica su plazo de expiración puede ser revocados en cualquier momento (p.ej por extravío del mismo).



Autoridades de Certificación

- Aunque generalmente se emiten certificados a sujetos, también es posible emitir certificados para autoridades de certificación de un rango menor, lo cual puede ser operativo para delegar y distribuir la expedición de certificados.
- Este mecanismo responde a la idea de **jerarquías de certificación**, es decir puede haber una cadena en la que las sucesivas CA de la cadena jerárquica avalan la identidad de las CA del nivel jerárquico inferior.
- Por tanto al validar un certificado se recorre la cadena de confianza jerárquica hacia arriba, hasta la **autoridad de certificación raíz** del árbol.

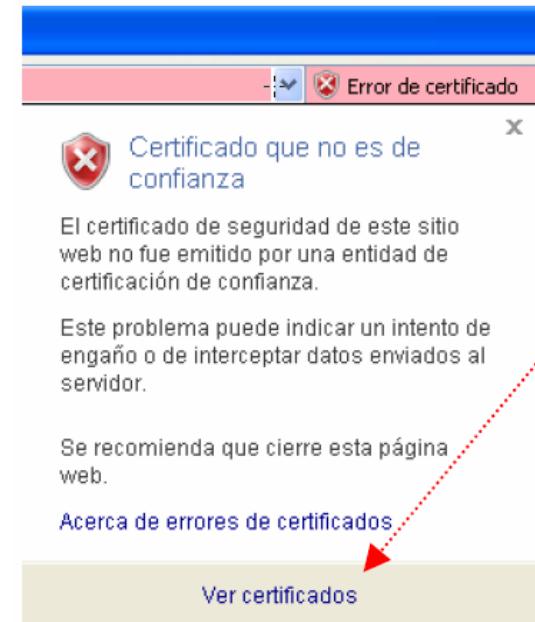
Autoridades de Certificación

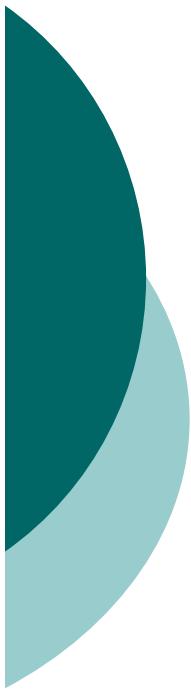


- CatCert es una CA: La Universidad Rovira i Virgili es una CA intermedia que emite certificados

Autoridades de Certificación

- Necesito instalar en el navegador las CAs raíz e intermedias (ya vienen precargadas las habituales).
- ¿Por qué?: es una forma de decir que “confiamos” en esas Autoridades de Certificación.
- ¿Qué ocurre si no lo hago? Me sale un error parecido al de la figura
- Ej: <https://correo.m.uson.mx>
- Ej: <https://www.ga-millennium.net/>





Autoridades de Certificación

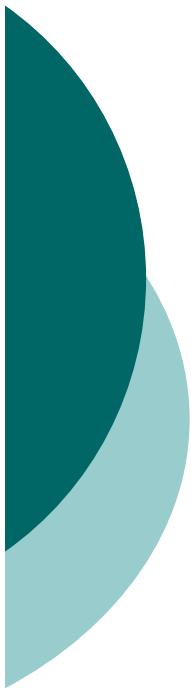
- **Práctica:** veamos las CAs instaladas en el navegador
 - **MS Explorer:** Herramientas > Opciones Internet > Contenido > Certificados
 - **Firefox:** Herramientas > Opciones avanzadas > Certificados > Autoridades
- ¿Está FNMT, CatCert, DNIe?
- Veamos sus propiedades: ¿cuándo expira la validez del certificado de la CA raíz del DNI?



Autoridades de Certificación

Práctica: instalación de certificado raíz de la FNMT

- Ir a <http://www.cert.fnmt.es/> > Obtenga Certificado de Usuario > Descarga de contratos
- MS Explorer: Herramientas > Opciones Internet > Contenido > Certificados
- Firefox: Herramientas > Opciones avanzadas > Certificados > Autoridades
 - Entidades emisoras raíz de confianza > Importar

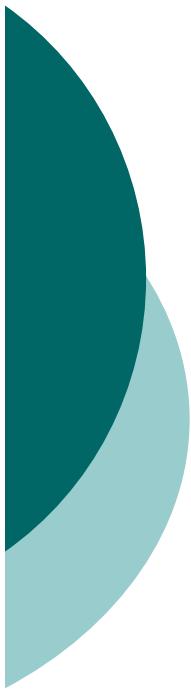


Gestión de personas

- La eAdministración ha de pensar no sólo en gestionar las identidades de los usuarios, sino que debe gestionar sus capacidades: conocer quién es, qué puede hacer y cuándo lo puede hacer.

Gestión de personas = identidades + capacidades
(ej. un empleado = quién es + cargo que ocupa)

- La gestión de personas resuelve no sólo la autenticación, acceso y auditoría en los sistemas de información, sino que también resuelve qué puede hacer, y si una persona posee las capacidades necesarias para realizar un trámite, acto o procedimiento.



Capacidades en certificados digitales

- Hemos hablado que un certificado digital **identifica** a una persona, pero también puede incluir sus **capacidades**.
- Certificados de atributos:
 - Permite **identificar una cualidad**, estado o situación (p.ej médico, director, casado, representa a, etc.)
 - Este tipo de certificado va asociado al certificado personal.
 - No se ha extendido su uso



El certificado de empleado público

- Es un Certificado de atributos
- Previsto en el artículo 19 de la LAECSP, para el personal al servicio de la Administración.
- Se emplea para la identificación de un empleado público en cualquiera de sus categorías: funcionario, laboral fijo, etc., e incluye tanto al titular como a la entidad pública en la que presta servicios el empleado



El certificado de sede

- Los certificados reconocidos de Sede Electrónica sirven para **identificar un portal web y establecer comunicaciones seguras**, de tal forma que se garantiza la privacidad e integridad de la información que se ofrece, excluyendo la posibilidad de ser víctimas de un fraude.



El certificado de sello de órgano

- Los certificados de Sello de Órgano se utilizan para identificar y firmar actos administrativos por medio de sistemas informáticos sin intervención directa de la persona física competente.
- Ejs.
 - Firma de un resguardo de un registro de entrada en el registro electrónico.
 - Firma de un sello de tiempo de una publicación en el perfil del contratante.

La identidad hay que renovarla...

- Los **certificados tienen una vigencia**
- Lista de certificados revocados (CRL: Certificate Revocation List)
 - Incluye toda la lista de certificados no válidos de una Autoridad de Certificación.
 - Cuando se valida un certificado se consulta en línea esta lista.
 - La validación en línea se hace mediante protocolo OCSP.
 - También podemos **revocar** un certificado (por extravío p.ej)





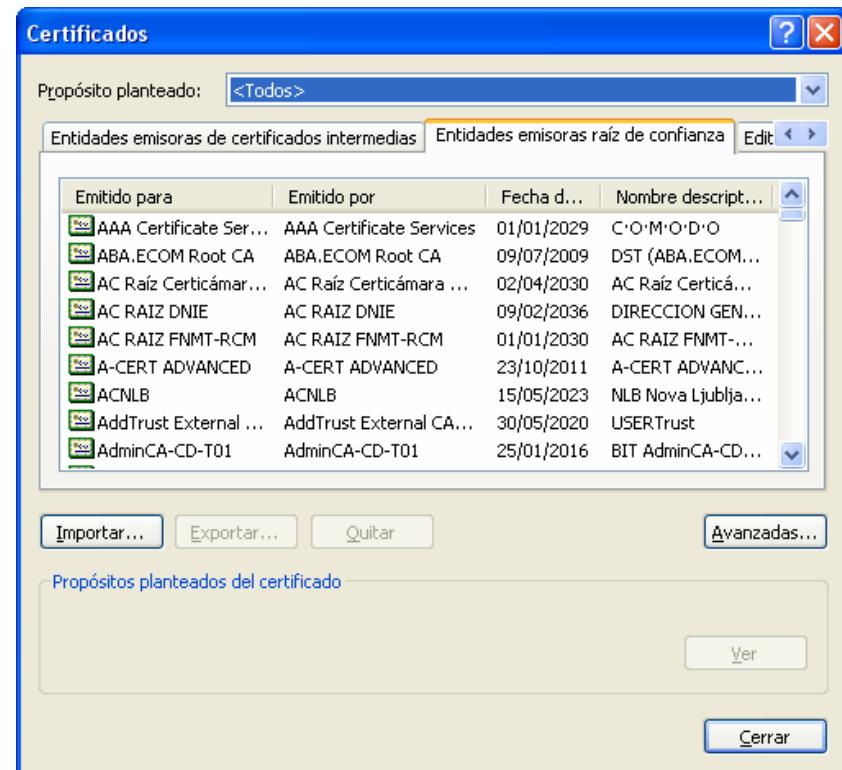
¿Cómo se verifica un certificado?

- Cada vez que se usa un certificado, nuestro ordenador (o el componente que lo utilice) comprueba dos cosas:
 - Autenticidad
 - Vigencia

Verificando autenticidad certificado

■ Para la **autenticidad** es suficiente contar con la instalación en el equipo informático que se esté usando del certificado raíz de la Autoridad de Certificación (CA) que emitió el certificado.

■ Si no tenemos instalada la CA, el certificado se puede comprobar pero saldrá un mensaje de que no se confía en él.





Verificando vigencia

- La **vigencia** se comprueba de dos formas:
 - **Consultando las fechas de validez** del certificado (están en el propio certificado).
 - **Validando que no esté revocado:** haciendo una consulta en línea a la CRL (Lista de Certificados Revocados) de la Autoridad de Certificación.
 - Esto lo hace automáticamente el navegador o la aplicación que hace uso del certificado.

¿Cómo se obtiene un certificado? Ej. FNMT

- Paso 1: Lo **solicito** en www.cert.fnmt.es > ciudadanos > obtener certificado

The screenshot shows the CERES website interface. At the top, there's a navigation bar with links to 'Mapa', 'Contacto', 'Enlaces', 'Legislación', and 'Noticias'. Below this is a main menu with options like 'Obtener el CERTIFICADO DE USUARIO CON SU DNIe', 'Obtener el CERTIFICADO DE USUARIO', 'Qué es CERES', 'Ciudadanos', 'Empresas', 'Adm. Pública', 'Certificado de usuario', 'Modificar datos', 'Verificar estado', 'Renovación de certificado', 'Anulación de certificado', 'Firma Electrónica Móvil', 'Contacto', 'Soporte Técnico', 'Otros servicios', and 'Preguntas Frecuentes'. A large green button labeled 'CIUDADANOS' is prominent. On the left, a sidebar lists various services: 'CERTIFICADO DE USUARIO', 'Solicitud del certificado', 'Acreditación de la identidad', 'Descarga del certificado', 'Copia de la clave privada', 'CERTIFICADO DE USUARIO EN TARJETA CRÍPTOGRAFICA', 'USUARIOS DE WINDOWS VISTA CON INTERNET EXPLORER 7 O INTERNET EXPLORER 8', 'CERTIFICADO DE USUARIO CON DNIe', and 'DESCARGA DE CONTRATOS'. The main content area contains instructions for obtaining a certificate, a 'NIF/NIE DEL TITULAR DEL CERTIFICADO' input field, a dropdown for 'Longitud clave' set to '2048 (Grado elevado)', and a 'Enviar petición' button.

The screenshot shows a 'SOLICITUD DEL CERTIFICADO' form. It displays the message 'El código de solicitud para el NIF 00000000T es:' followed by a large blue highlighted number '296550335'.

- Imprimo el código de solicitud y me voy a una oficina de registro

¿Cómo se obtiene un certificado?

Ej. FNMT

- Paso 2: Me **persono** en una oficina de registro (AEAT, Segsocial, UAH...) y acredito mi identidad presentando el DNI.
- Paso 3: me **descargo** el certificado
www.cert.fnmt.es > descarga certificado

| | | | |
|------------------------------|----------------------------|---------------------------|------------------------------|
| Qué es CERES | Ciudadanos | Empresas | Adm. Pública |
| Certificado de usuario | Obtener el certificado | Renovación de certificado | Anulación de certificado |
| Modificar datos | Verificar estado | Soporte Técnico | Preguntas |
| Contacto | Otros servicios | | |

 Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

CIUDADANOS

OBTENER CERTIFICADO
 DESCARGA DEL CERTIFICADO

Para descargar el certificado debe usar el mismo ordenador que en el paso de Solicitud.

FORMULARIO DE DESCARGA

Rellene el siguiente formulario y pulse el botón "Enviar petición" para completar la obtención del Certificado de Usuario de la FNMT.

más sobre el proceso de descarga del certificado de usuario

NIF
Código



¿Cómo se obtiene un certificado? Ej. FNMT

■ **Paso 4:** se instala el certificado en el navegador o en la tarjeta criptográfica.

Notas:

-La descarga del certificado debe hacerse desde el mismo ordenador y navegador desde el que se cursó la solicitud.

-Es posible solicitar el certificado en tarjeta criptográfica (dispositivo seguro de creación de firma).



Certificados en tarjeta criptográfica

- DNIe, Tarjeta criptográfica CERES, Tarjeta Universitaria Santander con certificado incluido...
- Las claves residen en el chip y los procesos de cifrado y firma se hacen en el chip.
- La clave privada nunca sale del chip y está protegida mediante un PIN





Certificados en navegador: importante

- Si el certificado reside en el navegador:
 - Hay que hacer una **copia de seguridad** exportando la clave privada. Es conveniente hacerlo protegiéndolo con una contraseña por si alguien se hace con el archivo que no pueda usarlo.
 - Si el ordenador no es personal, **proteger** el uso del certificado mediante una **contraseña**.



Certificados en navegador: importante

Práctica

- http://www.cert.fnmt.es/content/pages_std/docs/ManualFirmaElectronica.pdf



Certificados en navegador: importante

- Si no hago copia de seguridad:
 - Si formateo del ordenador perderé el certificado.
 - No podré utilizar el certificado en otro ordenador.
- Si no protejo el uso con una clave:
 - Cualquiera que tenga acceso a mi usuario del ordenador podrá hacerse pasar por mí.



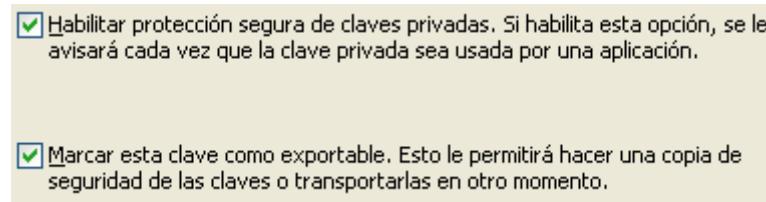
Certificados en navegador: importante

- La copia de seguridad debe custodiarse en lugar seguro.
- Especialmente grave es hacer la copia de seguridad sin contraseña y dejarla en una memoria USB que puede perderse, prestarse, etc.
- Si el certificado sin protección cae en manos de otra persona, **podrá hacerse pasar por uno mismo.**



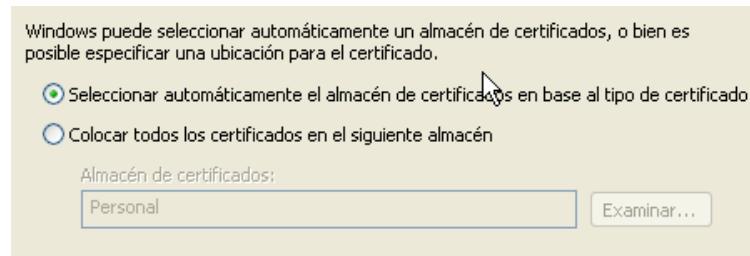
Certificados en navegador: importación en Explorer

- Internet Explorer:
 - Herramientas > Opciones de Internet > Pestaña Contenido > Certificados.
 - Pulsar sobre el botón importar.
 - Poner la contraseña si el certificado estaba protegido con contraseña e importante marcar



Certificados en navegador: importación en Explorer (2)

■ Seleccionar



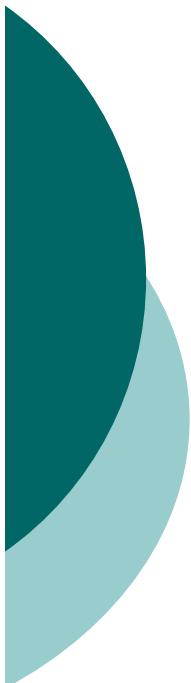
■ Importante: activar petición de clave con cada uso de la clave privada (poner un PIN). De esta forma cada vez que el navegador vaya a firmar o cifrar nos pedirá la contraseña.





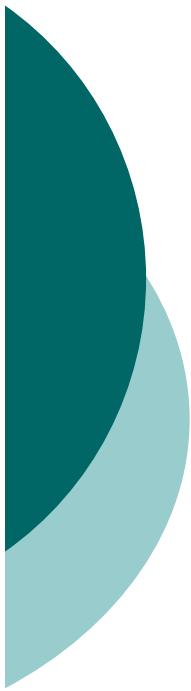
Certificados en navegador: importación en Firefox

- Firefox:
 - Herramientas > Opciones > Pestaña Avanzado > Ver Certificados
 - Pulsar sobre el botón importar.
 - Seguir instrucciones, seleccionar exportar clave pública e introducir una contraseña para proteger la clave. Si el certificado ya ha sido exportado previamente con clave habrá que introducirlo.



Certificados en navegador: exportación en Explorer

- Copia de seguridad en Internet Explorer:
 - Herramientas > Opciones de Internet > Pestaña Contenido > Certificados
 - Seleccionar el certificado en la pestaña Personal y pulsar sobre el botón exportar.
 - Seguir instrucciones, seleccionar exportar clave privada e introducir una contraseña para proteger la clave.



Certificados en navegador: exportación en Firefox

- Copia de seguridad en Firefox:
 - Herramientas > Opciones > Pestaña Avanzado > Ver Certificados
 - Seleccionar el certificado en la pestaña Sus Certificados y pulsar sobre el botón Hacer Copia
 - Seguir instrucciones, seleccionar exportar clave privada e introducir una contraseña para proteger la clave.

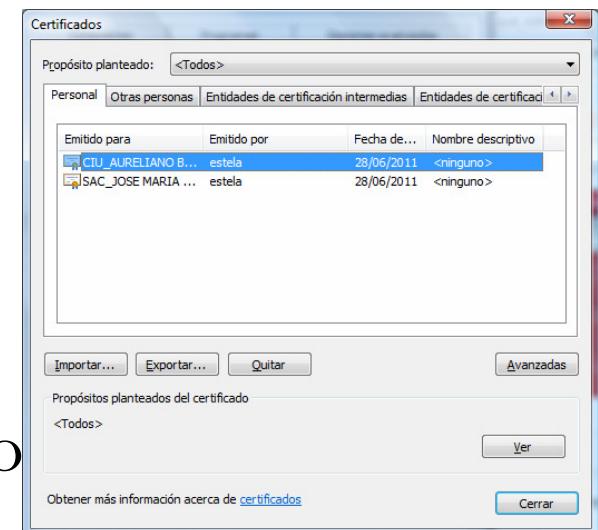


Certificados en navegador: almacenes

- Internet Explorer utiliza el almacén de certificados de Windows, Google Chrome también.
- Firefox utiliza uno propio.
- Esto implica que si queremos utilizar el certificado en ambos navegadores habrá que importarlo en ambos.

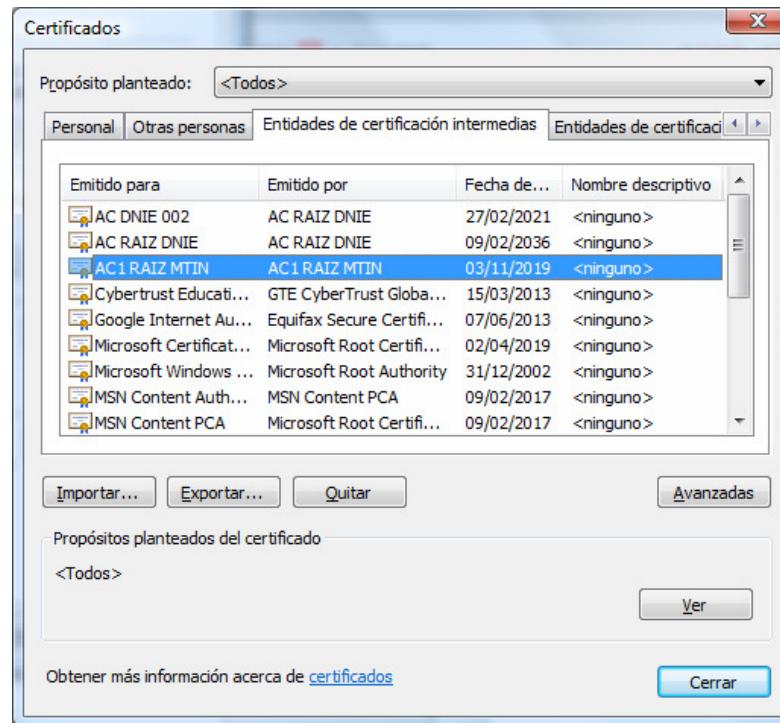
Certificados en navegador: práctica

- Importar/exportar certificados en Internet Explorer y en firefox
- Importar uno con protección de la clave privada y otro no.
- Comprobar efecto:
 - Valide.redsara.es
 - Firmar un documento con un certificado
 - Firmar un documento con otro certificado
 - ¿Diferencias?



Certificados en navegador: práctica

- Importar CA del Ministerio de Trabajo
http://ca.mtin.es/es/CA_MTIN/certificados.htm





Práctica: certificados Junta Andalucía

Accede al curso

<https://ws024.juntadeandalucia.es/cursoCertificados/inicio.htm>

Repasa los contenidos y contesta a las preguntas planteadas