

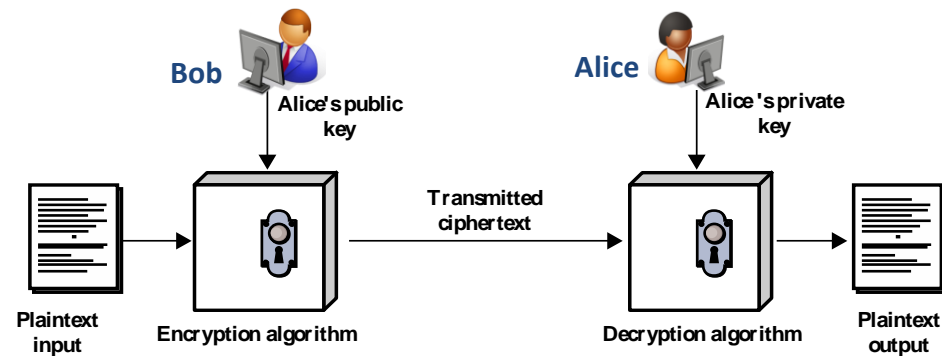
# SEGURIDAD DE LA INFORMACIÓN

## TEMA 3

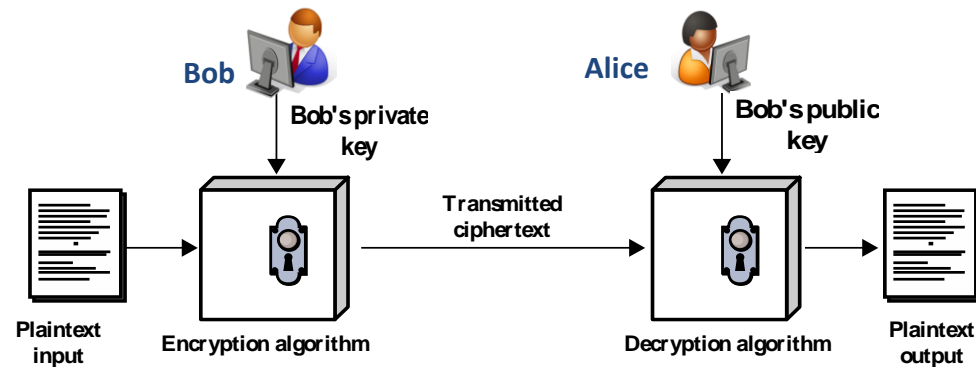
### **ESQUEMAS, PROTOCOLOS Y MECANISMOS DE SOPORTE (A LA SEGURIDAD DE APLICACIONES Y DE REDES)**

## Mecanismos e Infraestructuras de administración de claves públicas.

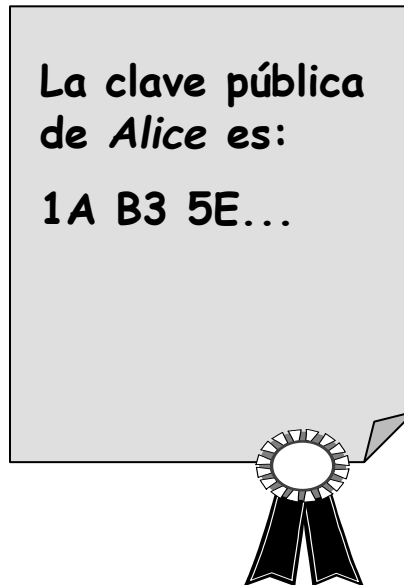
- ¿Cómo sabe *Bob* en este escenario si la clave pública de *Alice* es genuina?



- ¿Cómo sabe *Alice* en este escenario si la clave pública de *Bob* es genuina?



- Las preguntas anteriores equivalen a plantearse ¿cómo garantizar que **las claves públicas** de *Alice* y *Bob* **son auténticas**?
- Veamos, como ejemplo, el caso en el que *Bob* necesita la clave pública de *Alice*
  - *Bob* necesitaría algún documento digital con algún “**sello de garantía**”, o sea, algo equivalente a lo que en papel sería:



- En realidad, ¿qué información relevante habría de contener ese documento digital para optimizar su utilidad?
  - La **identidad del usuario** al respecto del cual se ofrece información (*Alice* en la figura anterior)
  - El valor de la **clave pública** de Alice (o sea, 1A B3 5E ...)
  - Algo que identifique unívocamente a ese documento entre otros muchos (por ejemplo, un **número de serie**)
    - ¿sirve la identidad del usuario para este menester?
      - No, porque un usuario puede tener más de un par <clave pública, clave privada>
  - Algo que indique “desde” cuándo y “hasta” cuándo es válido el documento digital (por ejemplo, una fecha de **emisión** y una de **expiración**)
  - La identidad de **quien emite** el documento
  - La **firma digital** de quien emite el documento



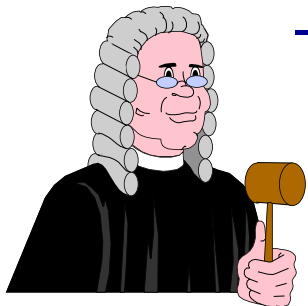
- El documento digital con esa información se denomina **certificado digital** o **certificado de clave pública**

- Es la firma digital de un documento (que contiene la información antes mencionada) la que garantiza que cierta clave pública pertenece a un determinado usuario



- Se denomina **Autoridad de Certificación** a la *tercera parte confiable* (TTP) que emite y administra los certificados digitales de los usuarios de un sistema

- Garantiza que una clave pública pertenece a cierto usuario inequívocamente identificado



- La ITU-T ha definido una estructura estándar de certificado digital que ha sido adoptada internacionalmente: **certificado X.509**

- ***Versión***: Indica el número de versión de X.509 (o sea, 1, 2 ó 3)
- ***Número de Serie***: Número de identificación único para este certificado digital, asignado por la CA
- ***Algoritmo de Firma***: Identificador del algoritmo de firma digital usado por la CA para firmar el certificado
- ***Emisor***: Nombre X.500 de la **CA emisora**
- ***Periodo de Validez***: Fecha desde el que el certificado comienza a ser válido, y día y hora de expiración

Versión
Numero de Serie
Algoritmo de Firma
Emisor
Periodo de Validez
Sujeto
Algoritmo Clave Pública
Clave Pública
Identif. único emisor
Identif. único usuario
Extensiones
Firma de la CA

- La ITU-T ha definido una estructura estándar de certificado digital que ha sido adoptada internacionalmente: **certificado X.509**

- *Sujeto*: Nombre en formato X.500 del usuario cuya clave pública se está certificando
- *Algoritmo Clave Pública*: Identificador del algoritmo de clave pública con el que se ha de utilizar la clave pública
- *Clave Pública*: Valor de la clave pública del usuario
- *Identificador único de emisor*: Cadena opcional para que el nombre de la **CA** no sea ambiguo, en caso de que esto pudiera ocurrir (versión 2)
- *Identificador único de usuario*: Cadena opcional para que el nombre del **usuario** no sea ambiguo, en caso de que pudiera ocurrir (versión 2)

Versión
Numero de Serie
Algoritmo de Firma
Emisor
Periodo de Validez
Sujeto
Algoritmo Clave Pública
Clave Pública
Identif. único emisor
Identif. único usuario
Extensiones

Firma de la CA



- La ITU-T ha definido una estructura estándar de certificado digital que ha sido adoptada internacionalmente: **certificado X.509**
  - **Extensiones**: Campo opcional para almacenar información de distinto tipo (versión 3)
  - **Firma**: **firma digital de la CA sobre el valor hash del conjunto de los demás campos del certificado**

Versión
Numero de Serie
Algoritmo de Firma
Emisor
Periodo de Validez
Sujeto
Algoritmo Clave Pública
Clave Pública
Identif. único emisor
Identif. único usuario
Extensiones
Firma de la CA



## Cristina

Entidad de certificación raíz

Caduca: jueves, 19 de marzo de 2026, 20:26:58 (hora estándar de Europa central)

✗ Este certificado raíz no es fiable

► Confiar

▼ Detalles

### Nombre del sujeto

País SP

Estado/Provincia Malaga

Localidad Malaga

Empresa UMA

Unidad organizativa UMA

Nombre común Cristina

Dirección de correo ab@lcc.uma.es

### Nombre del emisor

País SP

Estado/Provincia Malaga

Localidad Malaga

Empresa UMA

Unidad organizativa UMA

Nombre común Cristina

Dirección de correo ab@lcc.uma.es

Número de serie 00 D9 AE F5 9B 24 2D 04 FE

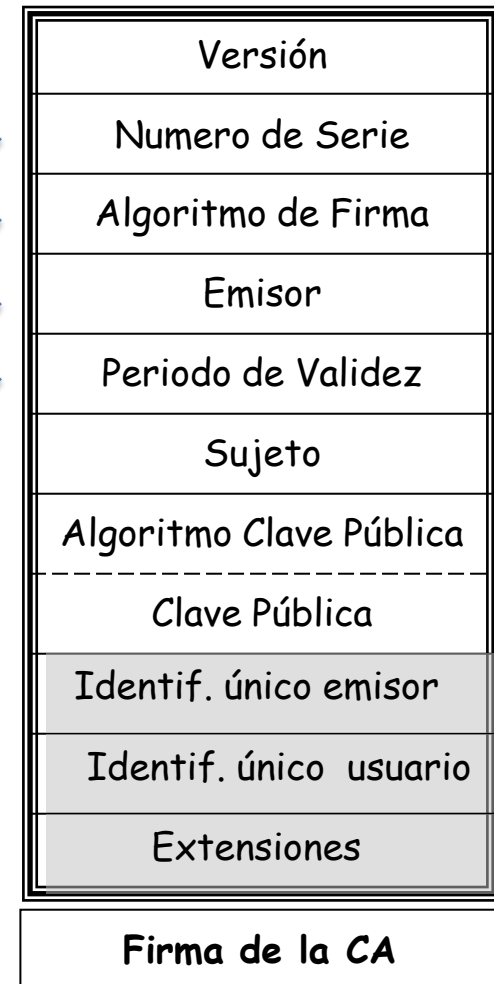
Versión 3

Algoritmo de firma SHA-1 con encriptación RSA ( 1.2.840.113549.1.1.5 )

Parámetros ninguno/a

No válido antes de lunes, 21 de marzo de 2016, 20:26:58 (hora estándar de Europa central)

No válido después de jueves, 19 de marzo de 2026, 20:26:58 (hora estándar de Europa central)





## Cristina

Entidad de certificación raíz

Caduca: jueves, 19 de marzo de 2026, 20:26:58 (hora estándar de Europa central)

✗ Este certificado raíz no es fiable

► Confiar

▼ Detalles

### Nombre del sujeto

País	SP
Estado/Provincia	Malaga
Localidad	Malaga
Empresa	UMA
Unidad organizativa	UMA
Nombre común	Cristina
Dirección de correo	ab@lcc.uma.es

### Nombre del emisor

País	SP
Estado/Provincia	Malaga
Localidad	Malaga
Empresa	UMA
Unidad organizativa	UMA
Nombre común	Cristina
Dirección de correo	ab@lcc.uma.es

Número de serie 00 D9 AE F5 9B 24 2D 04 FE

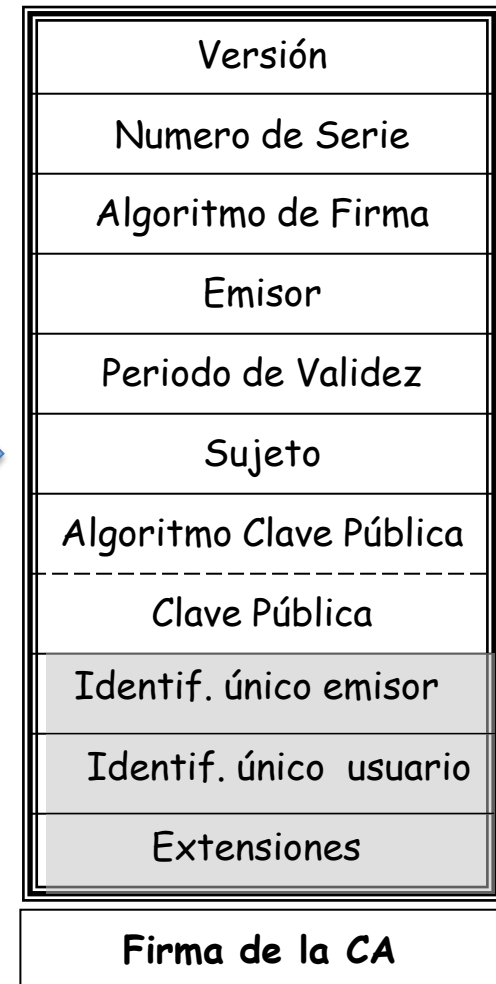
Versión 3

Algoritmo de firma SHA-1 con encriptación RSA ( 1.2.840.113549.1.1.5 )

Parámetros ninguno/a

No válido antes de lunes, 21 de marzo de 2016, 20:26:58 (hora estándar de Europa central)

No válido después de jueves, 19 de marzo de 2026, 20:26:58 (hora estándar de Europa central)



#### Información de la clave pública

<b>Algoritmo</b>	Encriptación RSA ( 1.2.840.113549.1.1.1 )
<b>Parámetros</b>	ninguno/a
<b>Clave pública</b>	128 bytes: BF F9 49 27 D5 E6 29 D5 ...
<b>Exponente</b>	65537
<b>Tamaño de la clave</b>	1024 bits
<b>Uso de la clave</b>	Cualquiera
<b>Firma</b>	128 bytes: 98 43 60 F8 B4 C4 D7 E1 ...

**Extensión** Restricciones básicas ( 2.5.29.19 )

**Crítico** NO

**Entidad de certificación** Sí

**Extensión** Identificador de clave del sujeto ( 2.5.29.14 )

**Crítico** NO

**Nombre de la clave** 24 85 28 DC 50 C1 BD 39 5D D0 D5 72 A5 09 1B F4 73 9D AF 7F

**Extensión** Identificador de clave de entidad emisora ( 2.5.29.35 )

**Crítico** NO

**Nombre de la clave** 24 85 28 DC 50 C1 BD 39 5D D0 D5 72 A5 09 1B F4 73 9D AF 7F

**Nombre de directorio**

**País** SP

**Estado/Provincia** Malaga

**Localidad** Malaga

**Empresa** UMA

**Unidad organizativa** UMA

**Nombre común** Cristina

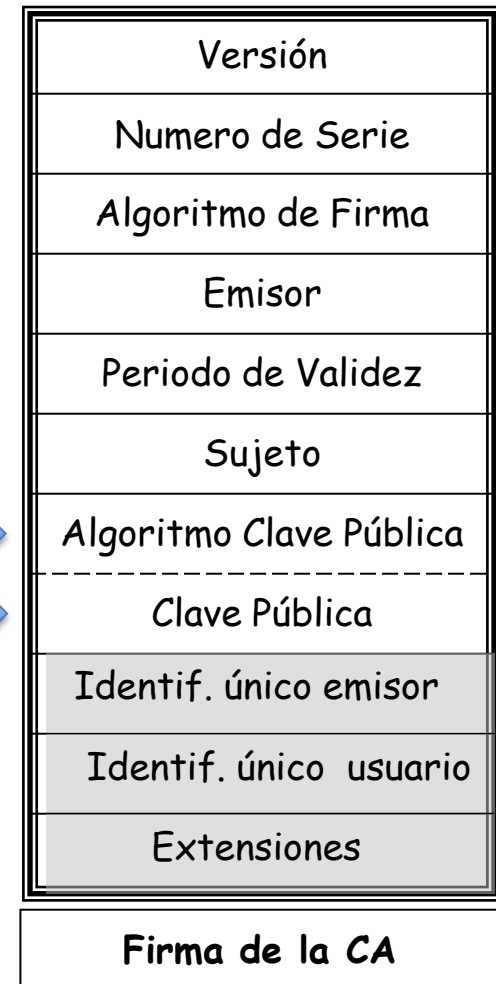
**Dirección de correo** ab@lcc.uma.es

**Número de serie** 00 D9 AE F5 9B 24 2D 04 FE

#### Huellas digitales

**SHA1** 8B 5F 16 E7 64 66 15 9C 89 F3 C1 13 44 94 44 A0 69 75 8F 90

**MD5** D6 DB ED 1D 4B DC B3 42 17 31 78 D7 70 8E 0A 96



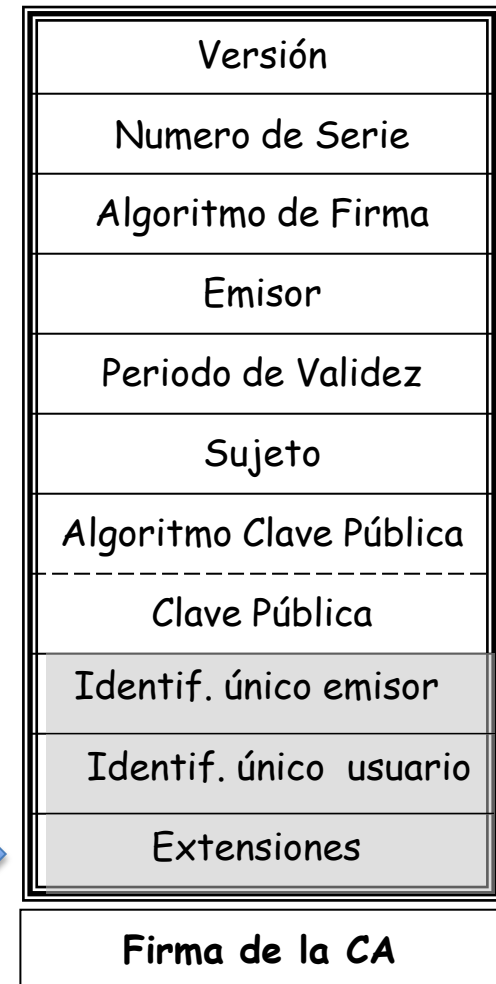
#### Información de la clave pública

<b>Algoritmo</b>	Encriptación RSA ( 1.2.840.113549.1.1.1 )
<b>Parámetros</b>	ninguno/a
<b>Clave pública</b>	128 bytes: BF F9 49 27 D5 E6 29 D5 ...
<b>Exponente</b>	65537
<b>Tamaño de la clave</b>	1024 bits
<b>Uso de la clave</b>	Cualquiera
<b>Firma</b>	128 bytes: 98 43 60 F8 B4 C4 D7 E1 ...

<b>Extensión</b>	Restricciones básicas ( 2.5.29.19 )
<b>Crítico</b>	NO
<b>Entidad de certificación</b>	SÍ
<b>Extensión</b>	Identificador de clave del sujeto ( 2.5.29.14 )
<b>Crítico</b>	NO
<b>Nombre de la clave</b>	24 85 28 DC 50 C1 BD 39 5D D0 D5 72 A5 09 1B F4 73 9D AF 7F
<b>Extensión</b>	Identificador de clave de entidad emisora ( 2.5.29.35 )
<b>Crítico</b>	NO
<b>Nombre de la clave</b>	24 85 28 DC 50 C1 BD 39 5D D0 D5 72 A5 09 1B F4 73 9D AF 7F
<b>Nombre de directorio</b>	
<b>País</b>	SP
<b>Estado/Provincia</b>	Malaga
<b>Localidad</b>	Malaga
<b>Empresa</b>	UMA
<b>Unidad organizativa</b>	UMA
<b>Nombre común</b>	Cristina
<b>Dirección de correo</b>	ab@lcc.uma.es
<b>Número de serie</b>	00 D9 AE F5 9B 24 2D 04 FE

#### Huellas digitales

<b>SHA1</b>	8B 5F 16 E7 64 66 15 9C 89 F3 C1 13 44 94 44 A0 69 75 8F 90
<b>MD5</b>	D6 DB ED 1D 4B DC B3 42 17 31 78 D7 70 8E 0A 96



#### Información de la clave pública

<b>Algoritmo</b>	Encriptación RSA ( 1.2.840.113549.1.1.1 )
<b>Parámetros</b>	ninguno/a
<b>Clave pública</b>	128 bytes: BF F9 49 27 D5 E6 29 D5 ...
<b>Exponente</b>	65537
<b>Tamaño de la clave</b>	1024 bits
<b>Uso de la clave</b>	Cualquiera
<b>Firma</b>	128 bytes: 98 43 60 F8 B4 C4 D7 E1 ...

**Extensión** Restricciones básicas ( 2.5.29.19 )

**Crítico** NO

**Entidad de certificación** Sí

**Extensión** Identificador de clave del sujeto ( 2.5.29.14 )

**Crítico** NO

**Nombre de la clave** 24 85 28 DC 50 C1 BD 39 5D D0 D5 72 A5 09 1B F4 73 9D AF 7F

**Extensión** Identificador de clave de entidad emisora ( 2.5.29.35 )

**Crítico** NO

**Nombre de la clave** 24 85 28 DC 50 C1 BD 39 5D D0 D5 72 A5 09 1B F4 73 9D AF 7F

**Nombre de directorio**

**País** SP

**Estado/Provincia** Malaga

**Localidad** Malaga

**Empresa** UMA

**Unidad organizativa** UMA

**Nombre común** Cristina

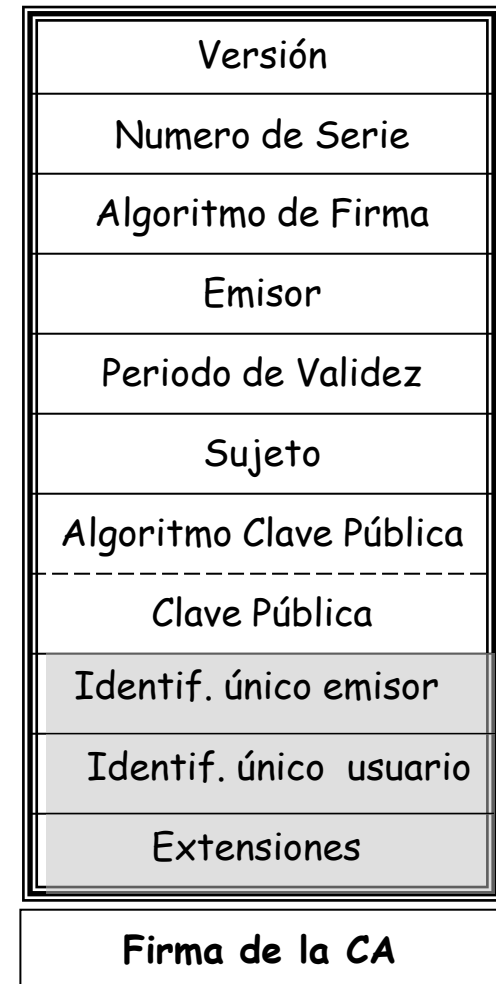
**Dirección de correo** ab@lcc.uma.es

**Número de serie** 00 D9 AE F5 9B 24 2D 04 FE

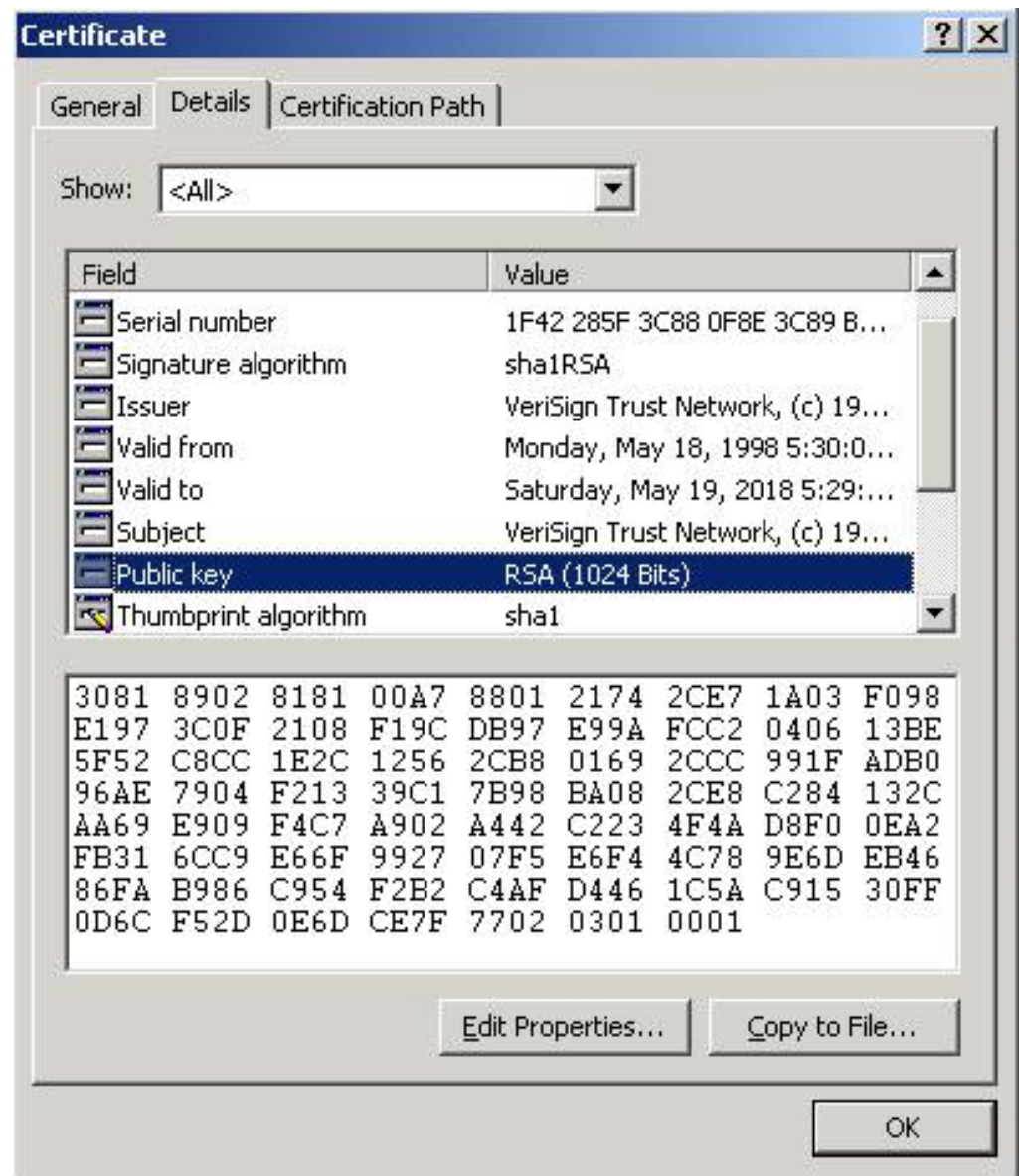
#### Huellas digitales

**SHA1** 8B 5F 16 E7 64 66 15 9C 89 F3 C1 13 44 94 44 A0 69 75 8F 90

**MD5** D6 DB ED 1D 4B DC B3 42 17 31 78 D7 70 8E 0A 96



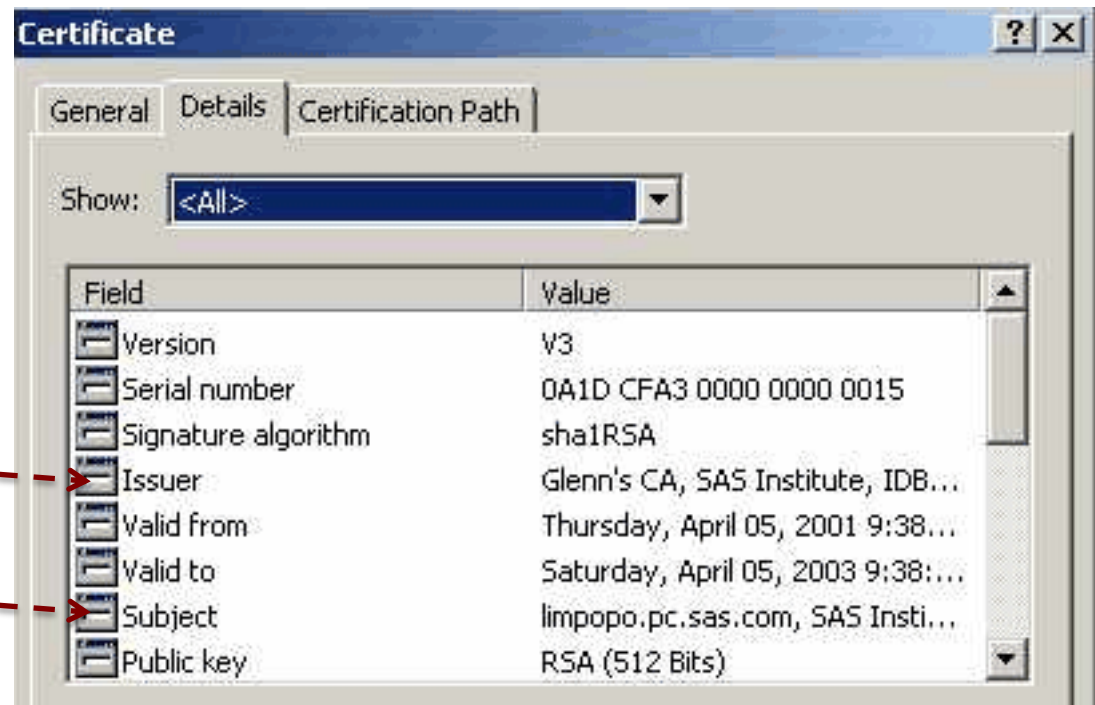
- Ejemplo de certificado X.509 instalado en un navegador



- Ejemplo de certificado X.509 instalado en un navegador:

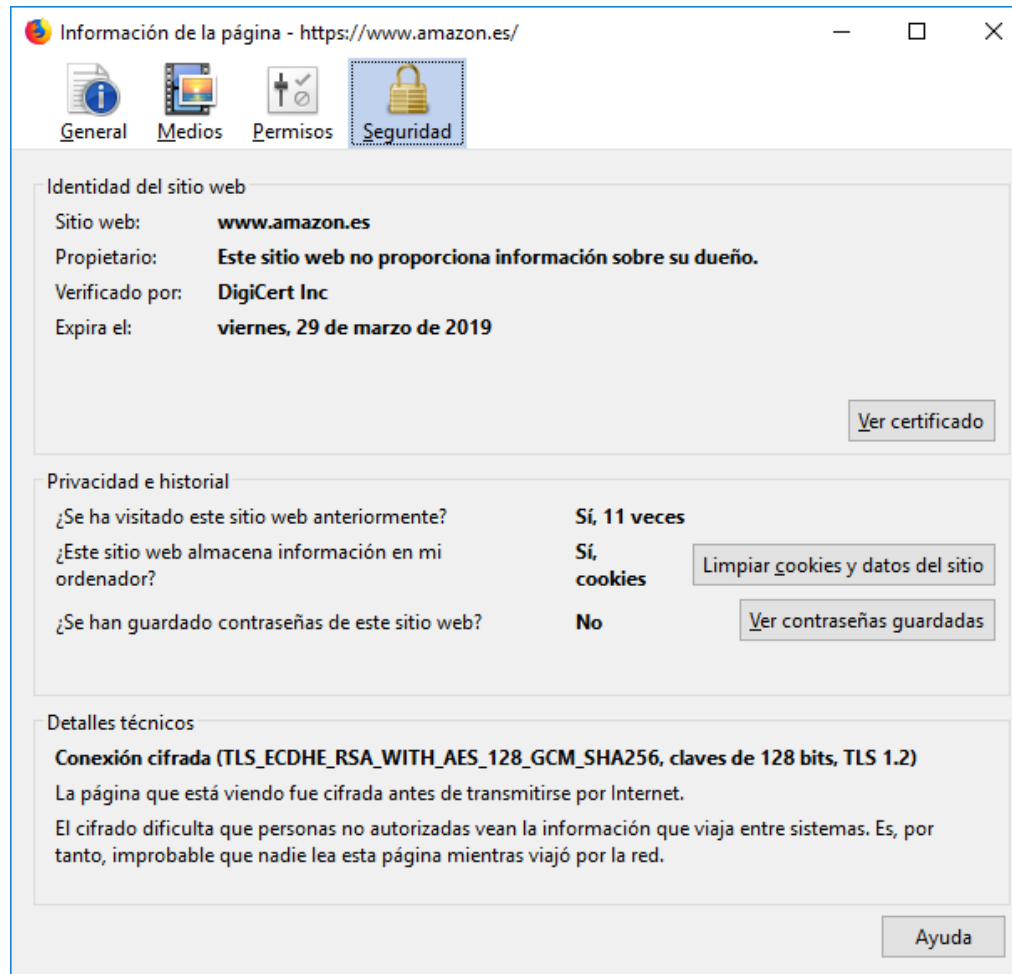
Autoridad de  
Certificación

Usuario

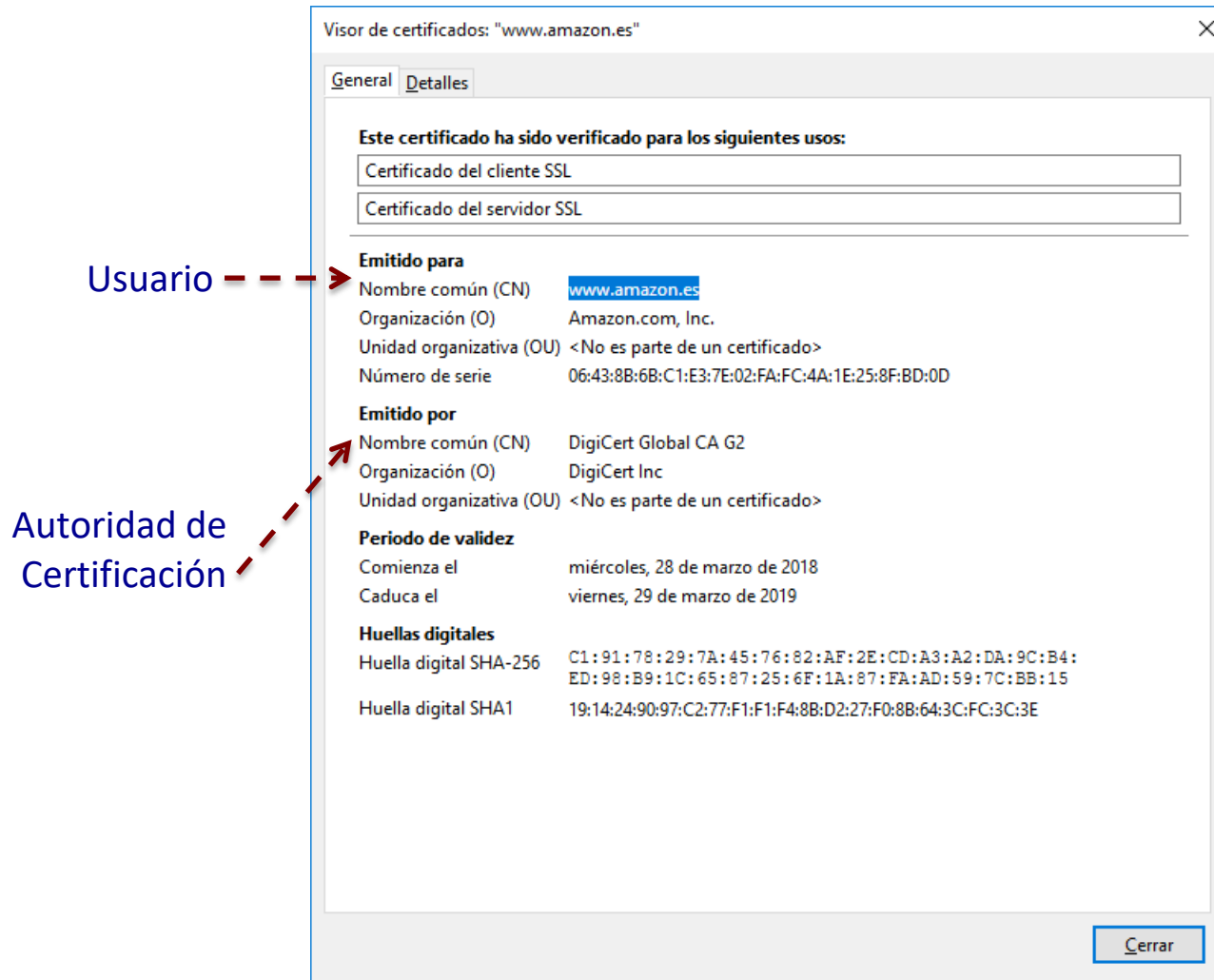




- Ejemplo de certificado X.509 de una página HTTPS:

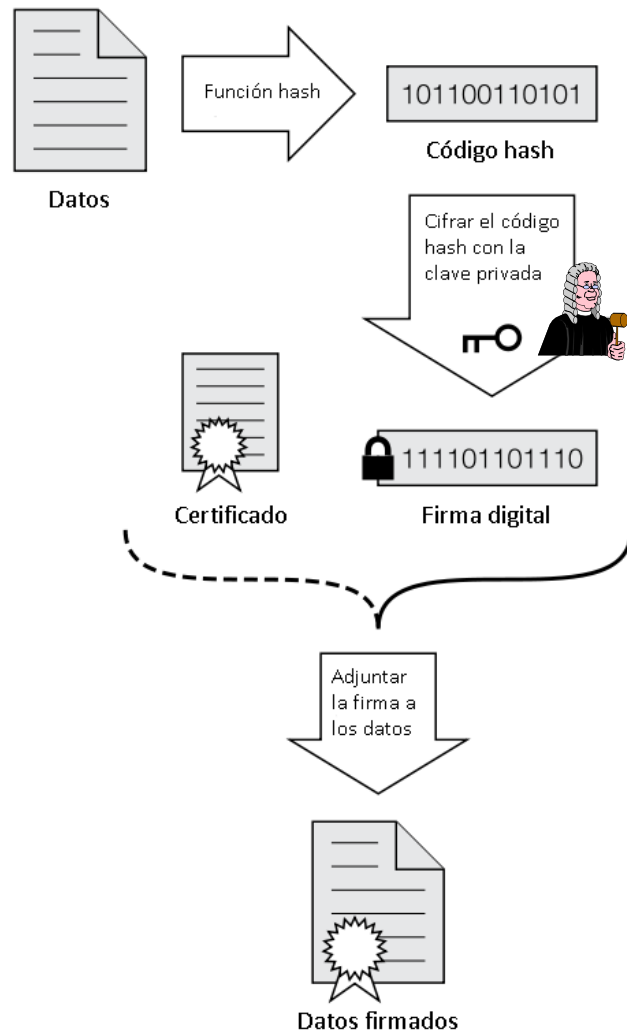


- Ejemplo de certificado X.509 de una página HTTPS:

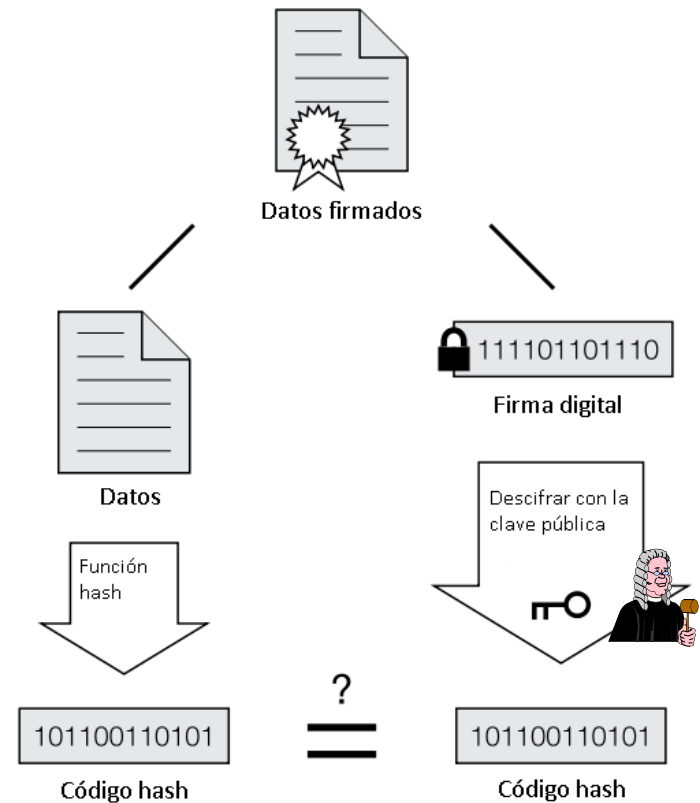




## Firma Digital



## Comprobación de una Firma



Si los códigos hash coinciden, la firma es válida

# Certificados digitales



<http://www.cacert.org>

## ¿Nuevo en CAcert?

CAcert.org es una autoridad certificadora dirigida por la comunidad que emite certificados gratuitos al público.

El objetivo de CAcert es promover el conocimiento y la educación sobre la seguridad informática a través del cifrado, ofreciendo específicamente certificados criptográficos. Estos certificados se pueden utilizar para firmar digitalmente y cifrar mensajes de correo electrónico, autenticar y autorizar usuarios que se conectan a sitios web y asegurar la transmisión de datos a través de Internet. Cualquier aplicación que tenga soporte del protocolo Secure Socket Layer (SSL o TLS) puede hacer uso de los certificados firmados por CAcert, así como cualquier aplicación que utilice certificados X.509, por ejemplo para el cifrado o firmado de código y las firmas digitales en documentos.

Si desea obtener certificados gratuito emitidos en su nombre, [únase a la Comunidad CAcert](#).

Si desea utilizar los certificados emitidos por CAcert, lea la CAcert [Root Distribution License](#). Esta licencia se aplica cuando se utilizan [claves raíz](#) de CAcert.

## ÚLTIMAS NOTICIAS

### Accréditation à / Assurance in Paris

Le prochain rendez-vous mensuel à Paris à lieu le mardi 21 mars 2017 entre 19:00 heures et 20:00 heures Nous vous proposons une rencontre pour toutes personne intéressée par CAcert. Validation, certification, accréditation de vos identités et informations sur CAcert. Bar de l'Hôtel Novotel Les Halles 8, place Marguerite de Navarre Paris 1er, Mo Châtelet Pour [...]

### CAcert 2017

February brought the start of the exhibition season for CAcert with our presence at FOSDEM – one of the biggest Europe-wide developer conferences in Brussels, Belgium. Of course we performed our well-known assurances, which is very popular at such events, with which CAcert safeguards its certificates by checking users' ID documents. This allows us to [...]

### CAcert and secure-u e.V. present at FOSDEM 2017

CAcert and secure-u e.V. will be present at FOSDEM 2017, the Free and Open Source Software Developers' European Meeting in Brussels, on February 4th and February 5th. Booth (Sat + Sun) Keysigning Party If you want to help at our booth, register yourself on our events wiki page for FOSDEM 2017 planning. CU at FOSDEM [...]

[ [MYEs Noticias](#) ]

## Dirigido a los miembros de la comunidad CAcert

¿Ha superado ya la [Prueba de Notario](#) de CAcert?

¿Ha leído ya el [Acuerdo de Comunidad](#) de CAcert?

Para encontrar la documentación general y ayuda visite el [sitio de Documentación Wiki](#) de CAcert. Para leer acerca de directrices específica, lea la [página de Directrices Aprobadas](#) de CAcert.

## Alta en CAcert.org

[Darse de alta](#)  
[Acuerdo de la comunidad](#)  
[Certificado raíz](#)

## Mi cuenta

[Iniciar sesión con contraseña](#)  
[Contraseña olvidada](#)  
[Iniciar sesión con Net Cafe](#)  
[Iniciar sesión con certificado](#)

## + Acerca de CAcert.org

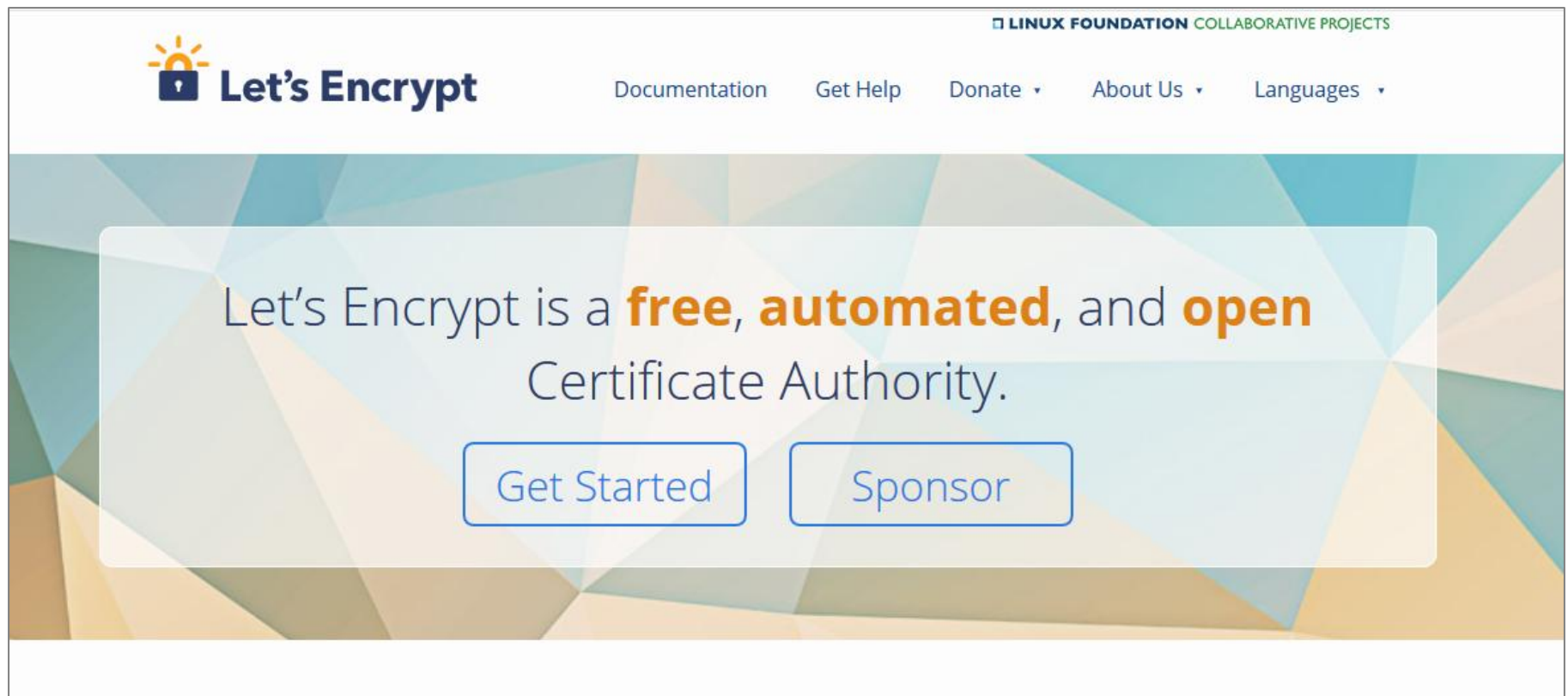
## + Traducciones


## Publicidad

# Certificados digitales



<https://letsencrypt.org/>

A screenshot of the Let's Encrypt website. The header features the Let's Encrypt logo (a sun with a padlock) and the text "Let's Encrypt". To the right of the logo is the text "LINUX FOUNDATION COLLABORATIVE PROJECTS". Further right are navigation links: "Documentation", "Get Help", "Donate", "About Us", and "Languages". The main content area has a colorful geometric background. A white box in the center contains the text "Let's Encrypt is a **free, automated, and open** Certificate Authority." Below this text are two buttons: "Get Started" and "Sponsor".

 **Let's Encrypt**

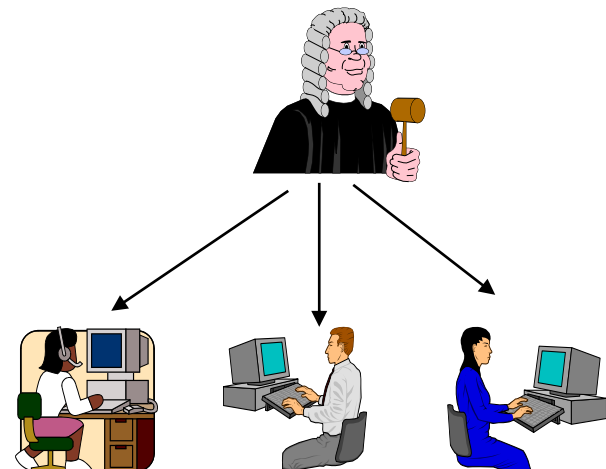
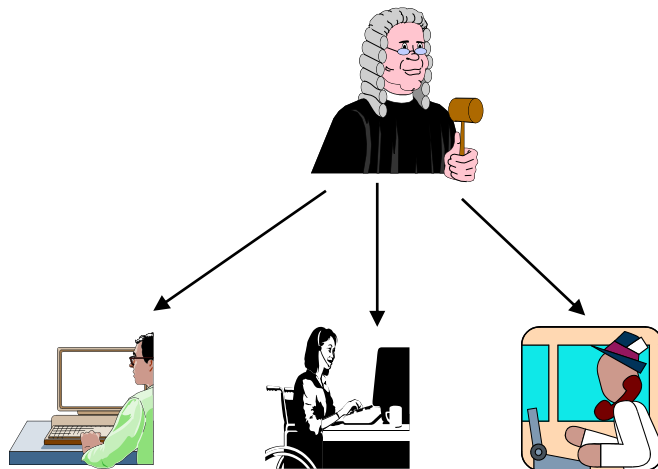
LINUX FOUNDATION COLLABORATIVE PROJECTS

[Documentation](#) [Get Help](#) [Donate](#) [About Us](#) [Languages](#)

Let's Encrypt is a **free, automated, and open** Certificate Authority.

[Get Started](#) [Sponsor](#)

- La situación ideal sería que una única CA pudiera certificar a todos los usuarios de Internet
- Sin embargo, la situación real es bien distinta, dado que existe una gran multiplicidad de grupos de usuarios en Internet, y distribuidos geográficamente, lo que implica la necesidad de **múltiples CAs**



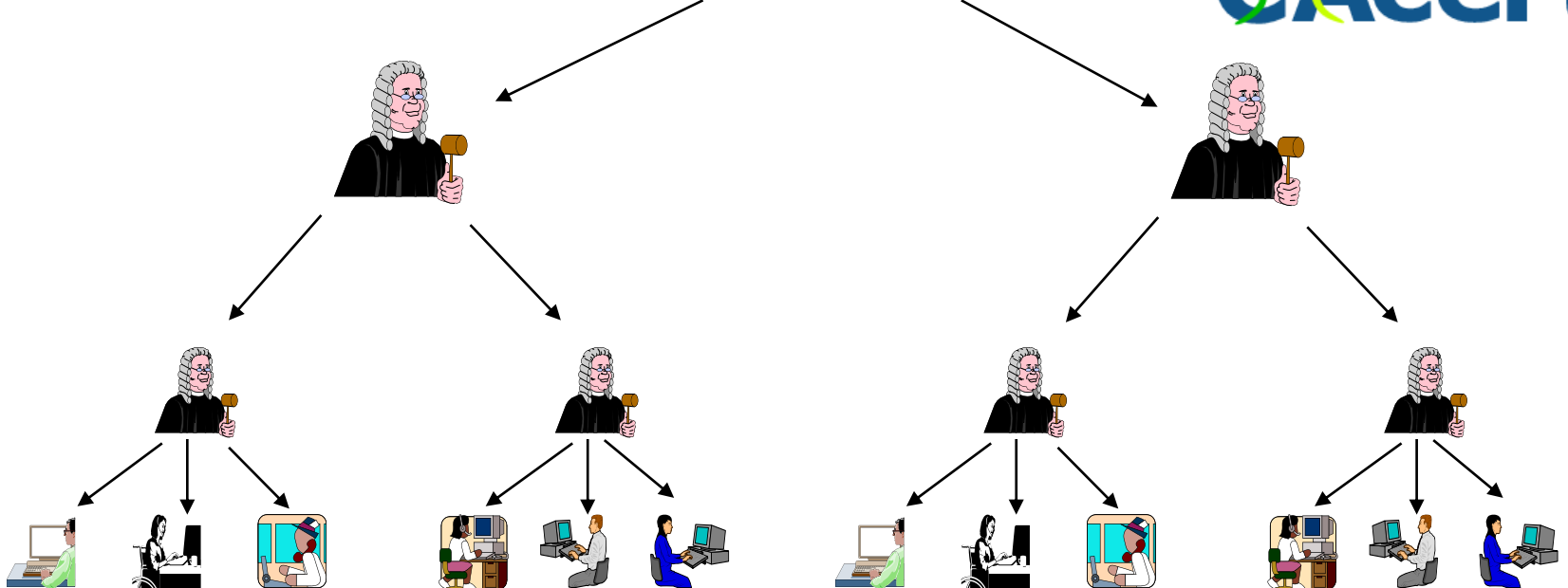
# Certificados digitales



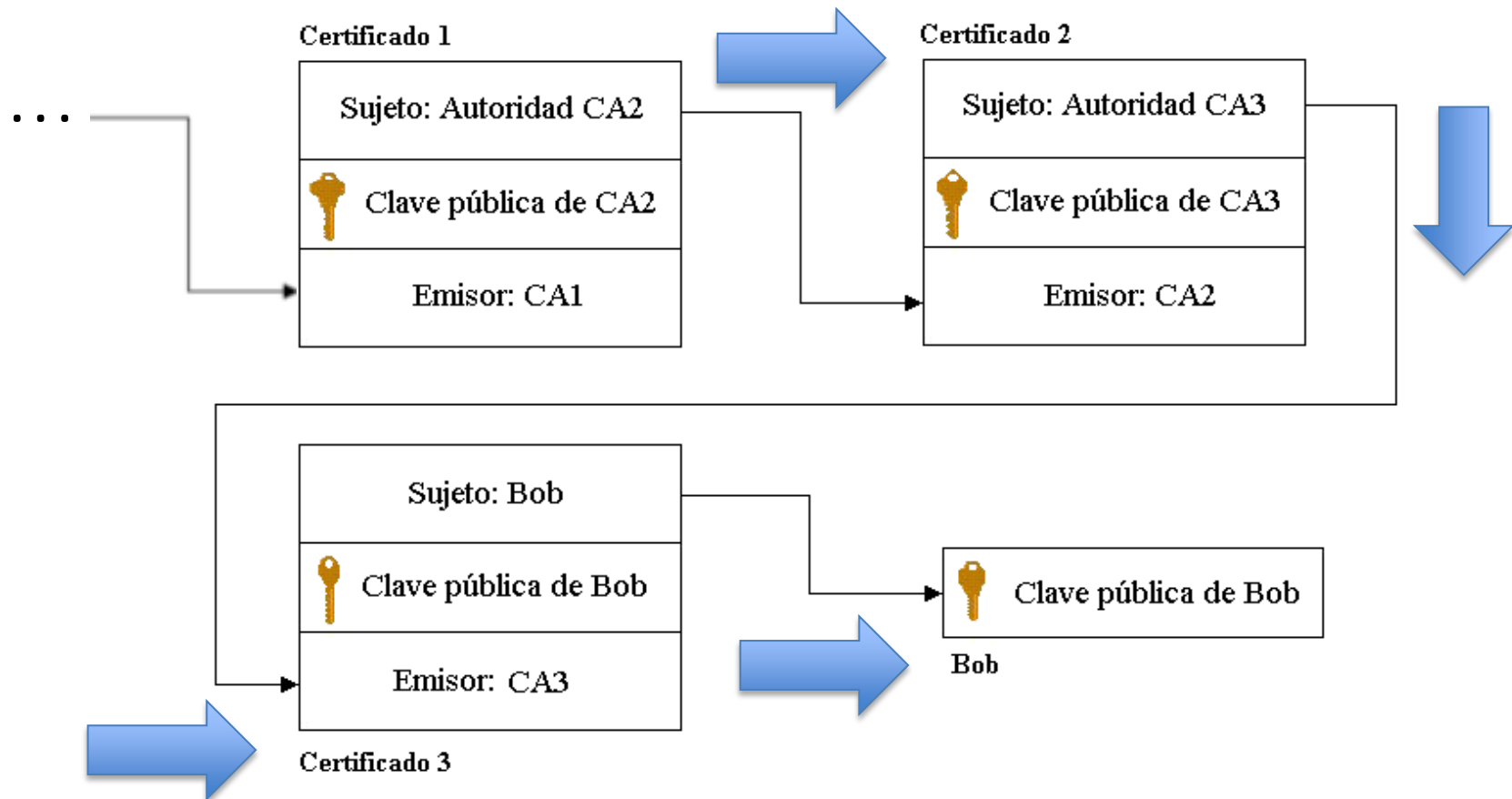
VeriSign®



CAcert

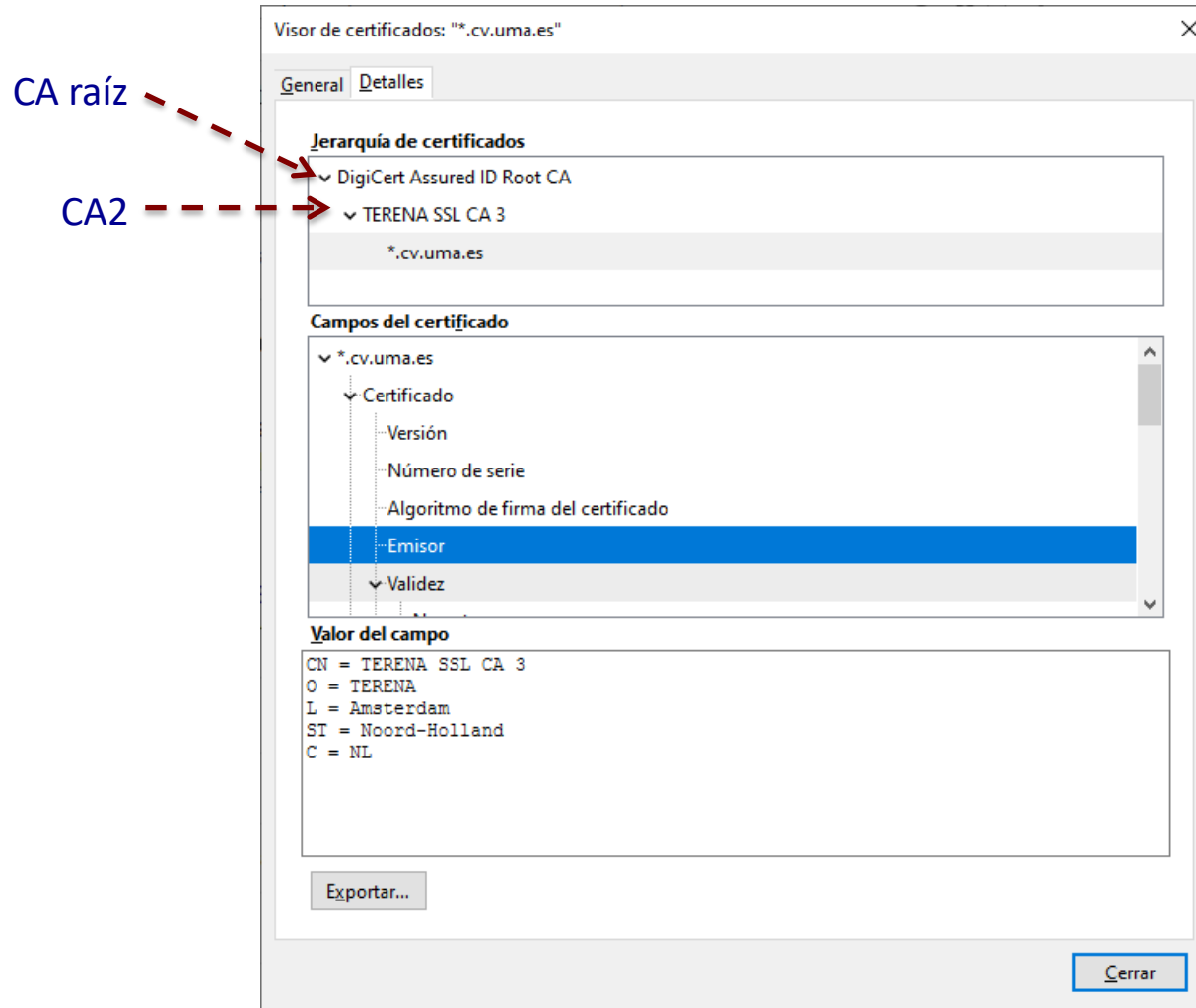


- Entre las CAs se utiliza de forma recursiva el esquema de certificación, creándose las **cadenas de confianza** (o **caminos de certificación**)





- Ejemplo de camino de certificación en un navegador:



- Esas cadenas de confianza se forman gracias a la infraestructura de CAs, denominada **Infraestructura de Clave Pública (PKI – Public Key Infrastructure)**
  - Una PKI proporciona el marco subyacente que permite la implantación de la tecnología de clave pública
- Servicios ofrecidos por una PKI:
  1. Emisión de Certificados
  2. Distribución de Certificados
  3. Obtención de Certificados
  4. Certificación Cruzada
  5. Generación de Claves
  6. Actualización de Claves
  7. Salvaguarda y Recuperación de Claves
  8. Revocación y Suspensión de Certificados

- Revocación de certificados

- Puede ser recomendable **invalidar** (revocar) **un certificado antes de la fecha de expiración** cuando:
  - la clave pública deja de ser válida
  - el usuario identificado en el certificado no se considera por más tiempo un usuario con potestad sobre la clave privada correspondiente
  - varía la información dentro del certificado
- La **CA se encarga de realizar la revocación**, bajo petición del usuario
  - ha de **publicar** esa información acerca del estado del certificado para que el resto de usuarios puedan realizar la comprobación antes de usarlo
- La comunidad Internet y la ITU-T han desarrollado el concepto de ***Lista de Revocación de Certificados, CRL***, como mecanismo de revocación
  - Una CRL es una lista (con timestamping) de certificados revocados, **firmada por la autoridad que emitió los certificados**

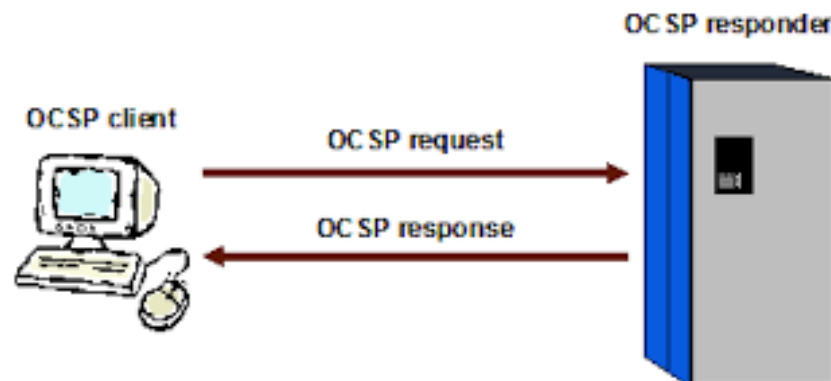
- Escenario típico de uso:
  - Para que *Bob* verifique la firma de *Alice* sobre un documento digital, no sólo ha de verificar el certificado de *Alice* y su validez; además, ha de comprobar que ese certificado no está en la CRL
    - o sea, ha de adquirir la versión más reciente de la CRL y confirmar que el número de serie del certificado de *Alice* no está en tal CRL
- Una CA emite CRLs regularmente (cada hora, día, semana,...) con independencia de que se hayan producido nuevas revocaciones
- El intervalo de emisión de CRLs depende de la política de certificación de la CA
- El certificado **se borra de la CRL cuando alcanza la fecha de expiración** (o sea, cuando se hubiese producido su caducidad natural)

- Estructura de una CRL, según el estándar X.509:



X.509 CRL  
versión 2

- El protocolo **Online Certificate Status Protocol (OCSP)** es otra solución de revocación (RFC 6960)
  - Define un formato standard para mensajes de **peticiones y respuestas**
  - Su funcionamiento se basa en que un **usuario puede confirmar on-line el status de un certificado** mediante la ejecución de una transacción con un servidor (Responder) OCSP asociado a la CA
  - La CA debe poner a disposición de todos los usuarios potenciales un **servicio online de alta disponibilidad**, y además, el servicio ha de proporcionarse dentro de un entorno seguro
  - El Respondedor OCSP puede ser o bien la misma CA o alguna entidad autorizada por ella



# Tarjetas inteligentes

- Una **tarjeta inteligente** o smartcard es una tarjeta que incluye un chip cuya función puede ser variada:
  - desde **simplemente almacenar** cierta información en su memoria interna (con o sin medidas de protección) ...
  - ... hasta realizar **complejos cálculos criptográficos** y encargarse de proteger el acceso a las claves que almacena
- Su uso se extiende hoy a muchos sectores:
  - tarjetas de fidelización
  - tarjetas bancarias
  - tarjetas de parking
  - documentos de identificación (DNI electrónico o pasaporte electrónico)
  - etc.



- Si atendemos al **método de comunicación o interfaz** con el circuito integrado, las smartcards se clasifican en:

- **Tarjetas de contacto**
- **Tarjetas sin contacto**



- Si atendemos a las **capacidades del chip**, se clasifican en:
  - **Tarjetas de memoria**: sólo contienen datos, y no albergan aplicaciones
    - Uso: identificación y control de acceso sin altos requisitos de seguridad
  - **Tarjetas microprocesadas**: albergan datos y aplicaciones
    - Uso: pago con monederos electrónicos
  - **Tarjetas criptográficas**: tarjetas microprocesadas avanzadas que incluyen módulos hardware para la ejecución de cifrados y firmas digitales
    - Uso: puede almacenar de forma segura un certificado digital (y su clave privada), así como firmar documentos o autenticarse
      - El procesador de la tarjeta realiza la firma