

CRIPTOGRAFÍA Y SUS APLICACIONES

NICOLÁS MACIA

ÍNDICE DE TEMAS

- Firma digital
- Certificados digitales
- PKI
- PGP

FIRMA DIGITAL

- La firma digital permite asociar un documento digital con su autor.
- Utiliza el modo autenticación:
 - El emisor genera la firma digital usando su clave privada para cifrar el hash del mensaje
 - El receptor puede verificar la firma comparando:
 - El resultado del hash del mensaje recibido
 - El hash obtenido al descifrar con la clave pública del emisor la firma digital

¿QUÉ ES LA FIRMA DIGITAL?

- Desde el punto de vista legal produce los mismos efectos que la firma hológrafa pero sobre un formato digital.
- Desde el punto de vista técnico es una secuencia de bits resultante de aplicar un conjunto de algoritmos criptográficos que permiten identificar al autor y verificar la integridad del contenido firmado.

PROPÓSITOS DE LA FIRMA DIGITAL

- Atribuir el documento a su autor de manera fehaciente (autenticidad del autor)
- Verificar que el contenido del documento no fue alterado (integridad del documento).
- Garantizar que el autor no pueda negar haber firmado el documento o mensaje (no repudio de la acción).

PERO,

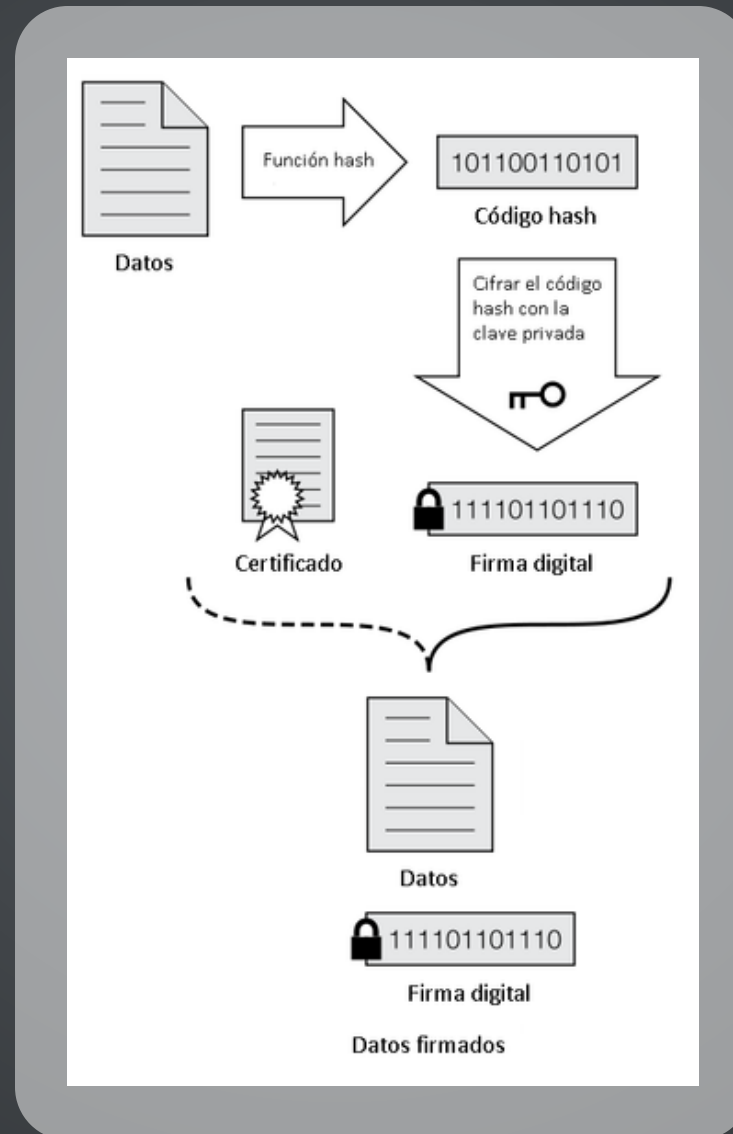
**NO HAY GARANTIAS SOBRE CUAL ES LA CLAVE DE UNA
PERSONA EN PARTICULAR**

¿QUÉ SE NECESITA PARA FIRMAR?

- Un par de claves
- Un certificado digital que permita asociar a un firmante con su clave pública

Los certificados digitales son estructuras que permiten asociar una clave pública con la identidad de una persona

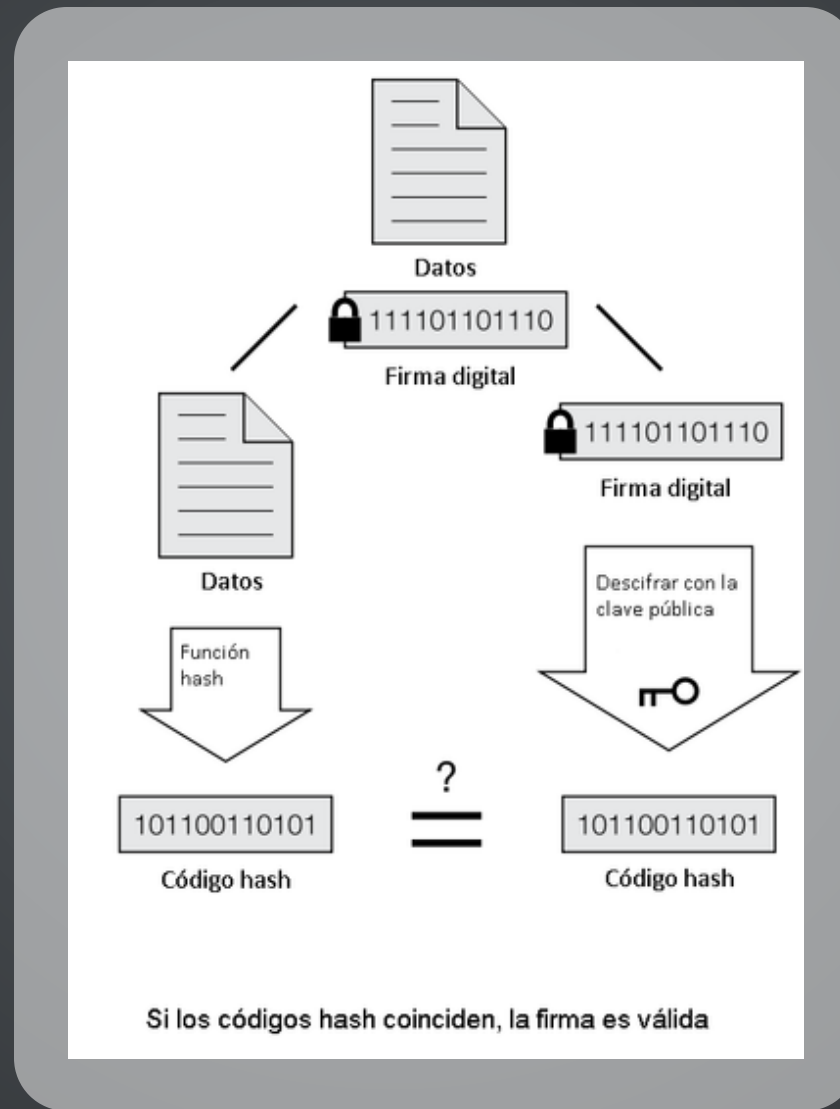
PROCESO DE FIRMA



PROCESO DE FIRMA

- Para crear una firma digital hay que crear un resumen del mensaje original o “hash”. La función de resumen reduce el mensaje a una cadena de caracteres de tamaño fijo.
- El emisor cifra el resumen del mensaje con su clave privada.
- El mensaje original y el hash firmado se envían al destinatario
 - El mensaje se podría haber enviado cifrado si se deseaba conservar también la confidencialidad

PROCESO DE VERIFICACIÓN



PROCESO DE VERIFICACIÓN

- Se recibe tanto los datos como la firma digital
- A partir de los datos se calcula el hash que se obtiene a partir de los mismos
- La clave pública del emisor se utiliza para descifrar la firma digital y obtener el hash calculado por el emisor
- Se verifica si los hashes son iguales
 - Si coinciden significa que la firma es válida y que el mensaje no fue alterado

CERTIFICADO DIGITAL

- El certificado digital es una estructura de datos que contiene:
 - La identidad del poseedor
 - La clave pública del poseedor
 - Período de validez del certificado
 - Identidad del emisor del certificado
 - Firma digital (emitida el emisor del certificado)

Visualizador de certificados: *.facebook.com

General

Detalles

Este certificado se verificó para los siguientes usos:

Certificado del servidor SSL

Emitido a

Nombre común (CN)	*.facebook.com
Organización (O)	Facebook, Inc.
Unidad organizativa (OU)	<No forma parte de un certificado>

Proporcionada por

Nombre común (CN)	DigiCert SHA2 High Assurance Server CA
Organización (O)	DigiCert Inc
Unidad organizativa (OU)	www.digicert.com

Período de validez

Emitido el	lunes, 19 de julio de 2021, 21:00:00
Vence el	lunes, 18 de octubre de 2021, 20:59:59

Visualizador de certificados: *.facebook.com

General

Detalles

Jerarquía de certificados

▼ Buildroot Object Token DigiCert High Assurance EV Root CA

▼ DigiCert SHA2 High Assurance Server CA

*.facebook.com

Campos del certificado

Algoritmo de clave pública del sujeto

Clave pública del sujeto

▼ Extensiones

ID de clave de la Entidad de certificación

ID de clave del sujeto del certificado

Nombre alternativo del sujeto del certificado

Uso de la clave del certificado

Uso extendido de la clave

Puntos de distribución de la CRL

Valor de campo

```
04 B1 8E 70 66 57 E5 AB A6 B1 D7 45 1D 3D 9B E7
FE EA B5 94 49 15 9A 52 29 D8 FF CA C9 79 D2 72
15 2B EA DD 5F 6C 1F ED 22 2F CE 11 D4 35 64 06
0E B4 AB 2B 4E D4 BB 2A 7C 67 62 A8 F8 D3 B1 4B
FC
```

Exportar...

Visualizador de certificados: *.facebook.com

General **Detalles**

Jerarquía de certificados

- ▼ Bundles Object Token: DigiCert High Assurance EV Root CA
 - ▼ DigiCert SHA2 High Assurance Server CA
 - *.facebook.com

Campos del certificado

- ▼ Uso extendido de la clave
- Puntos de distribución de la CRL
- Directivas del certificado
- Acceso a la información de la autoridad
- Restricciones básicas del certificado
- OID.1.3.6.1.4.1.11129.2.4.2
- Algoritmo de firma del certificado
- Valor de firma del certificado**
- ▼ Huellas digitales

Valor de campo

```
63 A1 FA C9 DD 06 B5 55 96 EE 5C 00 4C F4 BE D9
DD 3C 25 7E E3 3B E8 AA 10 F7 DF 72 6D C9 33 65
AC 8A 5B 0B 39 C8 68 3E C5 ED 4C 5C EB 40 1A D7
21 B3 3D 85 CF 21 36 4C A0 4C D0 C1 00 F9 FF A8
A2 E5 54 53 DD CD 79 1B 1B 79 79 8C 7F 95 B4 A3
66 66 3F 06 C2 CD D9 25 86 AB 2B 81 60 C7 C7 BC
```

Exportar...

PKI – INFRAESTRUCTURA DE CLAVE PÚBLICA

- Es la infraestructura encargada del manejo de certificados digitales.
- Su objetivo consiste en emitir y gestionar certificados digitales X.509 que asocian el par de claves a su poseedor.
- La confianza se basada en la confianza que le damos a determinados organismos conocidos como autoridades de certificación.

SOBRE LAS AUTORIDADES DE CERTIFICACIÓN

- Son las que emiten los certificados digitales de los diferentes sitios web que usamos a diario
- El certificación digital de las mismas está autofirmado por ellas mismas
- Nuestro navegador confía en cualquier cosa que es firmada con la clave privada de las autoridades de certificación

ALGUNAS AUTORIDADES DE CERTIFICACIÓN EN LAS QUE CONFIAMOS

Configuración

Tú y Google

Autocompletar

Verificación de seguridad

Privacidad y seguridad

Diseño

Motor de búsqueda

Navegador predeterminado

Al iniciar

Configuración avanzada

Extensiones

Acerca de Chrome

Buscar en configuración

org-China Financial Certification Authority

org-Chunghwa Telecom Co., Ltd.

org-Comodo CA Limited

org-COMODO CA Limited

org-Cybertrust, Inc

org-D-Trust GmbH

org-Dhimyotis

org-DigiCert Inc

org-DigiNotar

NO ES DE CONFIANZA

 DigiNotar Root CA

org-DigiNotar B.V.

NO ES DE CONFIANZA

 DigiNotar PKIoverheid CA Organisatie - G2

org-Digital Signature Trust Co.

org-Disig a.s.

org-E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.

org-eMudhra Inc

org-eMudhra Technologies Limited

org-Entrust, Inc.

org-Entrust.net

PROBLEMA CONOCIDO CON UNA AUTORIDAD DE CERTIFICACIÓN

DigiNotar

From Wikipedia, the free encyclopedia

DigiNotar was a [Dutch certificate authority](#) owned by [VASCO Data Security International, Inc.](#)^{[1][2]} On September 3, 2011, after it had become clear that a security breach had resulted in the [fraudulent](#) issuing of [certificates](#), the [Dutch government](#) took over operational management of DigiNotar's systems.^[3] That same month, the company was declared bankrupt.^[4]

An investigation into the hacking by Dutch-government appointed Fox-IT consultancy identified 300,000 [Iranian Gmail](#) users as the main target of the hack (targeted subsequently using [man-in-the-middle](#) attacks), and suspected that the Iranian government was behind the hack.^[5] While nobody has been charged with the break-in and compromise of the certificates (as of 2013), cryptographer [Bruce Schneier](#) says the attack may have been "either the work of the [NSA](#), or exploited by the NSA."^[6] However, this has been disputed, with others saying the NSA had only detected a foreign [intelligence service](#) using the fake certificates.^[7] The hack has also been claimed by the so-called Comodohacker, allegedly a 21-year-old Iranian student, who also claimed to have hacked four other certificate authorities, including [Comodo](#), a claim found plausible by [F-Secure](#), although not fully explaining how it led to the subsequent "widescale interception of Iranian citizens".^[8]


After more than 500 fake DigiNotar certificates were found, major web browser makers reacted by blacklisting all DigiNotar certificates.^[9] The scale of the incident was used by some organizations like [ENISA](#) and [AccessNow.org](#) to call for a deeper reform of [HTTPS](#) in order to remove the weakest link possibility that a single compromised CA can affect that many users.^{[10][11]}

Contents [\[hide\]](#)


- Company
 - History
 - Bankruptcy
 - Refusal to publish report
- Issuance of fraudulent certificates
 - Steps taken by the Dutch government
- See also
- References
- Further reading
- External links



COSTO DE UN CERTIFICADO WILCARD



CERTIFICATE SERVICES
Purchase Certificate

 Log In

1 Order

2 Contacts

3 Options

4 Payment

5 Confirmation

Product Selection

☐ Standard OV SSL

☐ Advantage OV SSL

☐ Multi-Domain EV SSL

☐ Multi-Domain OV SSL

☒ Wildcard OV SSL

☐ Document Signing Individual

☐ Document Signing Group

☐ SMIME Personal

Provides flexibility and ease of use in environments that see frequent change. By specifying *.example.com in the certificate, Wildcard OV SSL certificates will dynamically support an unlimited number of subdomains.

- Organization Validated (OV) SSL
- Supports multiple wildcard domains
- Unlimited subdomains

New Certificate Price

699⁰⁰ USD





Cost for 1 year

☐ Organization is outside of US, UK or Canada


Enter Promo Code

Apply


Why Entrust?

- 24x5 Support 
- Unlimited Reissues 
- Unlimited Server Licensing 
- SHA-2/2048-Bit Keys 

COSTO DE UN CERTIFICADO PARA USO PERSONAL



CERTIFICATE SERVICES
Purchase Certificate

 Log In

1 Order

2 Contacts

3 Options

4 Payment

5 Confirmation

Product Selection

☐ Standard OV SSL

☐ Advantage OV SSL

☐ Multi-Domain EV SSL

☐ Multi-Domain OV SSL

☐ Wildcard OV SSL

☐ Document Signing Individual

☐ Document Signing Group

☒ SMIME Personal

Enables users to digitally sign and encrypt email and attachments with the strongest levels of confidentiality and security. The recipient can verify the sender's identity and ensure the message was not tampered with during transmission.

- Ensures private, authenticated email communication
- Establishes trust between email client and browser, preventing annoying trust dialogs
- Enables digital signatures which prove the origin of emails and guarantee the integrity of their content

New Certificate Price

24⁰⁰ USD


Cost for 1 year


☐ Organization is outside of US, UK or Canada


Enter Promo Code


Apply

Why Entrust?

• 24x5 Support 

• Unlimited Reissues 

• Unlimited Server Licensing 

• SHA-2/2048-Bit Keys 



USOS DE PKI



Autenticación
del usuario



Firma de
Documentos



Emisión de
Certificados x509

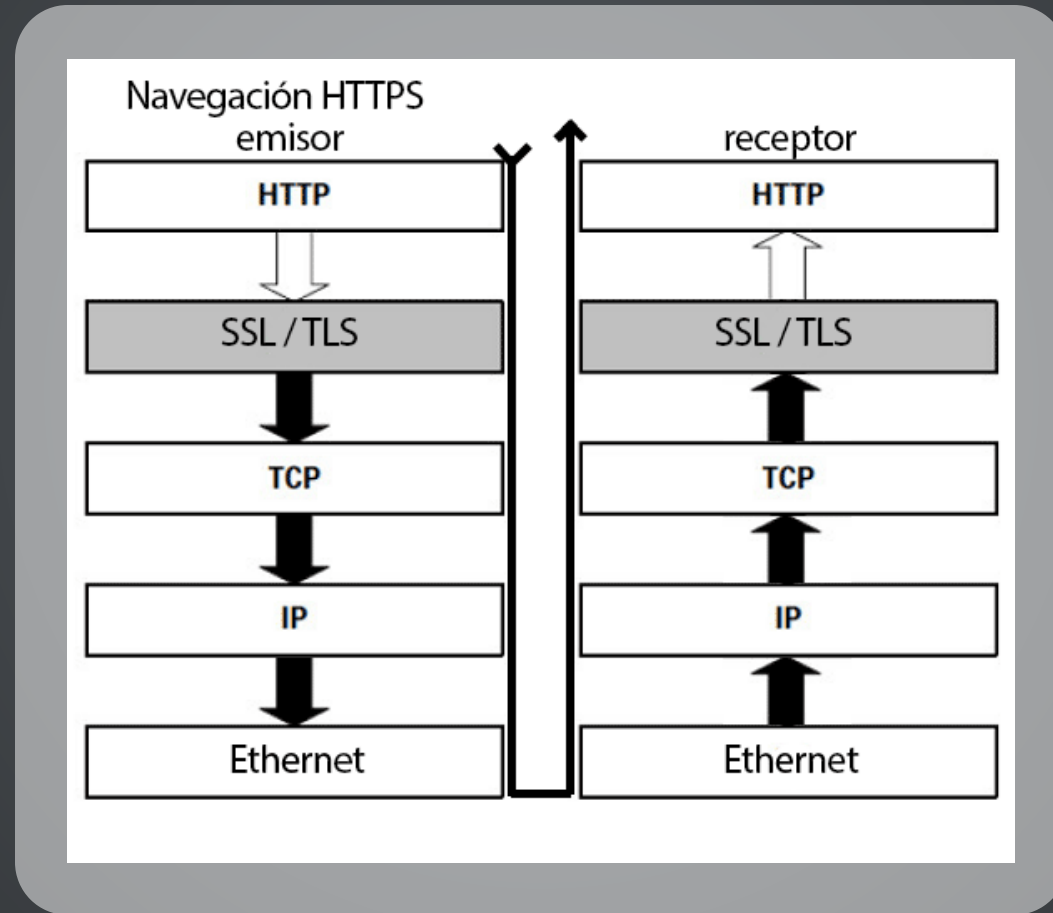


Comunicaciones
seguras



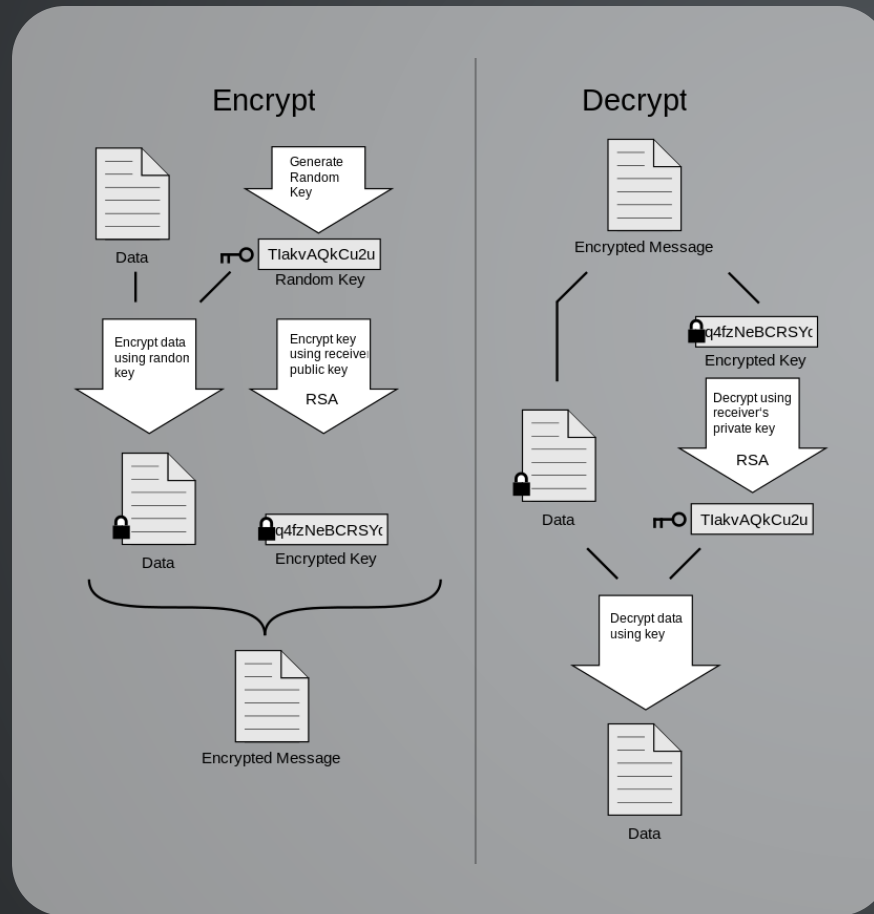
Correo
Electronico seguro

USOS DE PKI - HTTPS



PGP (PRETTY GOOD PRIVACY)

- PGP es un criptosistema híbrido. Cifrado en PGP



ESQUEMAS DE CONFIANZA EN PGP

- En PGP, una clave es válida si yo mismo la firmo.
- Alternativamente, se pueden manejar otros esquemas de confianza:
 - Puedo confiar en lo que otro usuario firme.
 - Puedo manejar otros esquemas de confianza con multiples firmas
- ¿yo como lo uso?



RESUMEN REDES DE CONFIANZA

- PKI provee un esquema centralizado de confianza en el que confiamos ciegamente en una serie de autoridades de certificación
- En PGP no hay autoridades de certificación.
- PGP provee un esquema descentralizado de confianza:
 - En PGP cada individuo es su propia CA.
 - Cada individuo es responsable de certificar/firmar lo que considere.

