CRIPTOGRAFIA APLICADA

Ing Germán Bollmann

1

AGENDA

FIRMA DIGITAL
Certificados Digitales
Componentes y Estándar PKCS
Diez riesgos sobre las PKI
OCSP
Ejemplos de Uso
Problemas
Herramientas / TIPS

2

FIRMA DIGITAL

3

Firmas tradicionales (en papel)

- Es auténtica. Convence al destinatario que el firmante verdaderamente firmó el documento.
- Es infalsificable. Prueba que el firmante, y nadie más, ha firmado el documento.
- No es reusable. Es parte del documento firmado y no puede trasladarse a otro.
- El documento es inalterable. No se lo puede cambiar después de firmado.
- La firma no se puede repudiar (negar que se haya firmado)

4

Objetivo

Poder enviar un documento firmado a través de medios electrónicos de manera que ese documento cuente, por lo menos, con las mismas características técnicas de seguridad y legales que tiene un documento firmado hológrafamente.

Resumen: Modelar digitalmente las mismas características de un documento con firma hológrafa.

Firma Digital - Definición

- La firma digital es una solución tecnológica que permite **autenticar el origen** y **verificar la integridad del contenido** de un mensaje de manera tal que ambas características sean demostrables ante terceros.

5

Firma Digital - Propiedades

- *Autenticidad:* Poder atribuir el documento únicamente a su autor de forma fidedigna, de manera de poder identificarlo.
- *Integridad:* Estar vinculada a los datos del documento digital, poniendo en evidencia su alteración luego de que fue firmado.
- *Exclusividad:* Garantizar que la firma se encuentre bajo el absoluto y exclusivo control del firmante.
- *No repudio:* Garantizar que el emisor no pueda negar o repudiar su autoría o existencia; ser susceptible de verificación ante terceros.

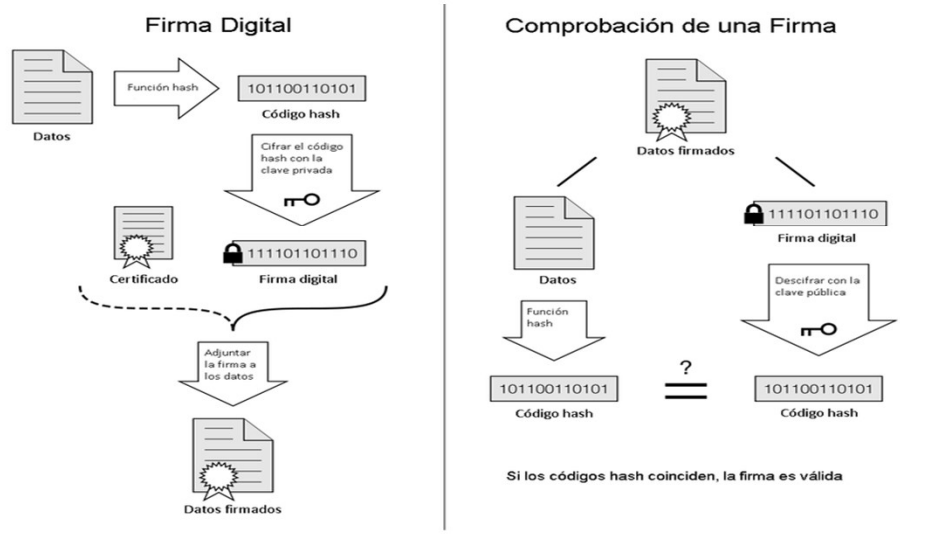
6

Qué no es una Firma Digital

- Una firma digitalizada (una firma manuscrita escaneada).
- Una contraseña o password.
- Un sistema biométrico.
- Un sistema de autenticación: este requisito sólo no alcanza.
- Una firma electrónica.
- Un documento encriptado (solo se garantiza la confidencialidad).

7

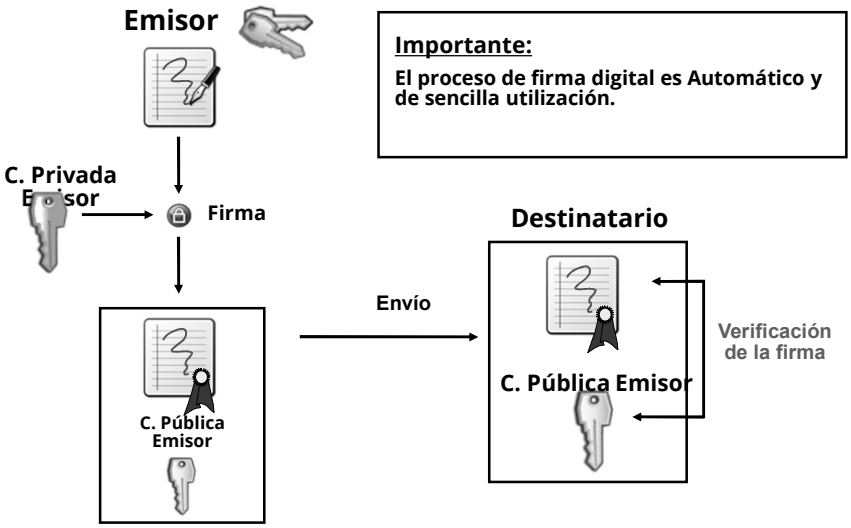
Esquema de funcionamiento



https://es.wikipedia.org/wiki/Archivo:Firma_Digital.png

8

Firma Digital: Procedimiento

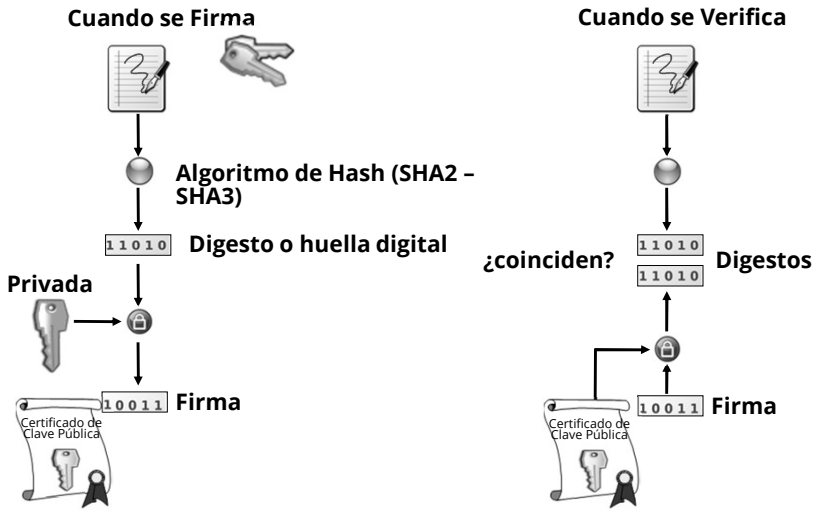


Importante:

El proceso de firma digital es Automático y de sencilla utilización.

9

Firma Digital: ¿Como funciona?



10

¿Firma Digital, Firma Electrónica o Digitalizada?

Se parecen semánticamente, pero son muy diferentes

.

Según la legislación Argentina **la firma digital** *es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control*. Esta firma debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita *identificar al firmante* y *detectar cualquier alteración* del documento digital posterior a su firma.

En tanto la **firma electrónica** es el *conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónico*s, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

La firma digitalizada es *una firma escaneada, que no tiene validez legal* y suele usarse para acompañar campañas de marketing o publicitarias, ya que se acostumbra a adjuntarla a mensajes de estas áreas.

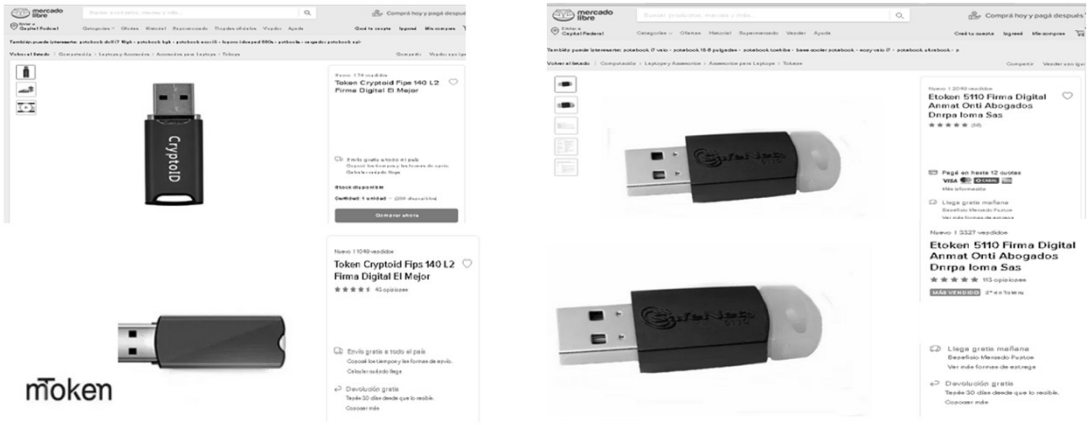
11

¿Qué es?

https://ticsalborada1.fandom.com/es/wiki/18._Conductas_de_seguridad._Seguridad_activa:_Firma_digital_y_certificado_digital.

12

Firma Digital por Hardware (Token Criptográfico)



https://articulo.mercadolibre.com.ar/MLA-614463038-etoken-5110-firma-digital-anmat-onti-abogados-dnrpa-ioma-sas-_JM#position=1&type=item&tracking_id=2f4fb393-8a4c-4607-853c-921766ea4b27

https://articulo.mercadolibre.com.ar/MLA-868016383-token-cryptoid-fips-140-l2-firma-digital-el-mejor-_JM#position=13&search_layout=stack&type=item&tracking_id=104090f1-135e-401d-84f5-d3d7166f9b5e
https://articulo.mercadolibre.com.ar/MLA-614463038-etoken-5110-firma-digital-anmat-onti-abogados-dnrpa-ioma-sas-_JM#position=9&search_layout=stack&type=item&tracking_id=104090f1-135e-401d-84f5-d3d7166f9b5e

13

Token: Características del Producto

Sistemas Operativos:
- Windows 2000, Windows Server 2003, Windows Server 2008, XP, Vista, Windows 7, 8,10 , Linux, Mac OS X

Soporte API y estándares:
- PKCS#11 v2.01, Microsoft CAPI, PC / SC, almacenamiento de certificados X.509 v3, SSL v3, IPSec / IKE

Algoritmos de seguridad incorporados:
- RSA 2048-bits, DES, 3DES (Triple DES), SHA 256

Certificaciones de seguridad:
- FIPS 140-2 L3 (dispositivo completo) (Las certificaciones difieren por modelos, favor consultar)

Soporte de especificaciones ISO:
- Soporte para especificaciones ISO 7816-1 a 4

Cubierta:
- Plástico duro moldeado, a prueba de manipulación

Retención de datos en memoria de tarjeta inteligente:
- Al menos 10 años

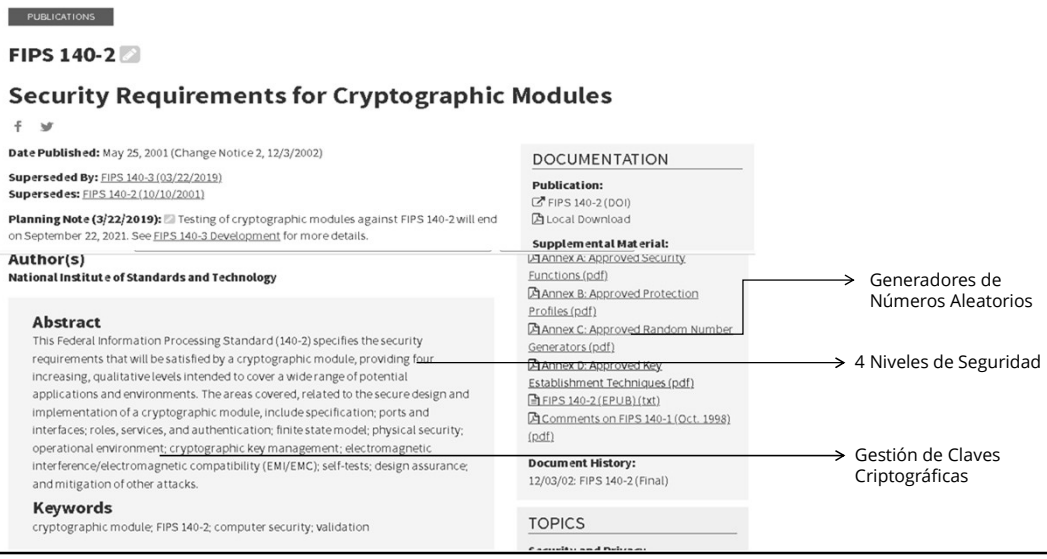
Reescritura de celda de memoria de tarjeta inteligente:
- **Al menos 500,000**

Estos tokens son recomendados por la ONTI (Oficina Nacional de Tecnologías de Información) ente que se encarga de homologar y aprobar todo lo relacionada a Firma Digital en Argentina.

https://articulo.mercadolibre.com.ar/MLA-614463038-etoken-5110-firma-digital-anmat-onti-abogados-dnrpa-ioma-sas-_JM#position=1&type=item&tracking_id=2f4fb393-8a4c-4607-853c-921766ea4b27

14

FIPS - 140



PUBLICATIONS

FIPS 140-2

Security Requirements for Cryptographic Modules

Date Published: May 25, 2001 (Change Notice 2, 12/3/2002)

Superseded By: FIPS 140-3 (03/22/2019)
Supersedes: FIPS 140-2 (10/10/2001)

Planning Note (3/22/2019): Testing of cryptographic modules against FIPS 140-2 will end on September 22, 2021. See FIPS 140-3 Development for more details.

Author(s)
National Institute of Standards and Technology

Abstract
This Federal Information Processing Standard (140-2) specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

Keywords
cryptographic module; FIPS 140-2; computer security; validation

DOCUMENTATION

Publication:
FIPS 140-2 (DOI)
Local Download

Supplemental Material:
Annex A: Approved Security Functions (pdf)
Annex B: Approved Protection Profiles (pdf)
Annex C: Approved Random Number Generators (pdf)
Annex D: Approved Key Establishment Techniques (pdf)
FIPS 140-2 (EPUB) (txt)
Comments on FIPS 140-1 (Oct. 1998) (pdf)

Document History:
12/03/02: FIPS 140-2 (Final)

TOPICS

Generadores de Números Aleatorios

4 Niveles de Seguridad

Gestión de Claves Criptográficas

15

Certificados Digitales

16

¿Qué son los certificados digitales?

- Un certificado digital es un documento que contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y que es firmado por una Autoridad de Certificación (AC).
- Como emisor y receptor confiarán en esa AC, el usuario que tenga un certificado expedido por ella se autenticará ante el otro, en tanto que su clave pública está firmada por dicha autoridad.
- Una de las certificaciones más usadas y un estándar en la actualidad en infraestructuras de clave pública PKIs (Public-Key Infrastructure) es X.509.

http://www.ietf.org/html.charters/pkix-charter.html

17

Certificado digital X.509

- X.509 está basado en criptografía asimétrica y firma digital.
- En X.509 se define un framework (una capa de abstracción) para suministrar servicios de autenticación a los usuarios del directorio X.500.
- La autenticación se realiza mediante el uso de certificados.

- Un certificado contiene: el nombre de la AC, el nombre del usuario, la clave pública del usuario y cualquier otra información como puede ser un un indicador de tiempo o *timestamp*.
- El certificado se cifra con la clave privada de la AC.
- Todos los usuarios poseen la clave pública de la AC.

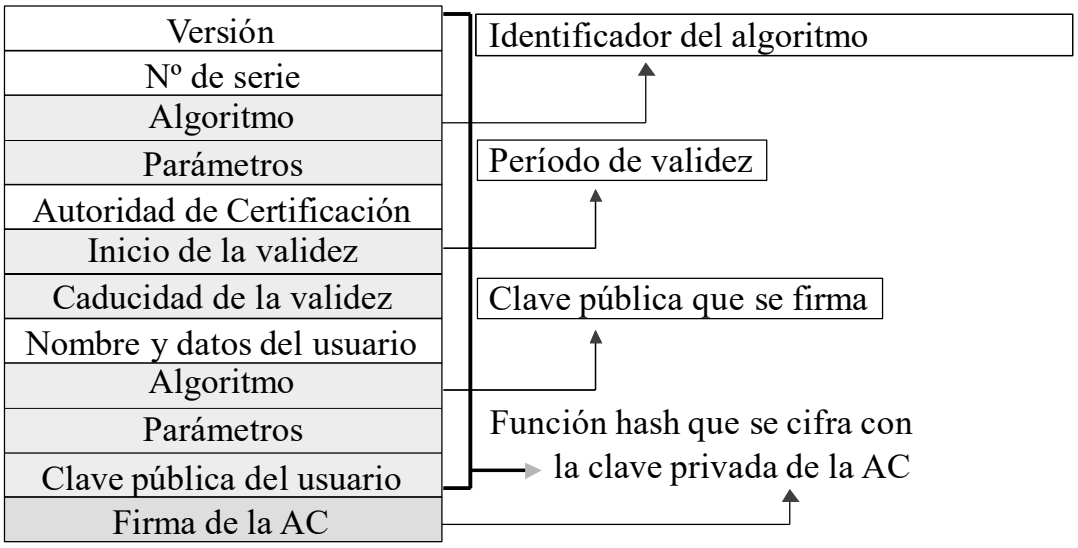
18

Certificado digital x.509

Versión	Versión del formato X.509 (hasta v3).
Nº de serie	Valor único del certificado dentro de la CA.
Algoritmo Parámetros	Identificación del algoritmo de firma utilizado.
Emisor del certificado	Nombre X.509 de la AC.
Inicio de la validez Final de la validez	Fecha inicial y fecha final del certificado
Nombre distinguido del usuario	Identidad a la que se remite el certificado (personal, corporación, etc.).
Algoritmo Parámetros Clave pública	Clave pública del usuario, junto con el algoritmo asociado (es obligatorio el uso de RSA).
Firma	Firma digital del certificado, realizada por la AC sobre el hash de datos públicos.

19

Certificado digital x.509



20

Campos del certificado digital X.509

V: Versión del certificado (actualmente V3).
SN: Número de serie.
AI: identificador del algoritmo de firma que sirve para identificar el algoritmo usado para firmar el paquete X.509.
CA: Autoridad certificadora.
T_A: Periodo de validez.
A: Propietario de la clave pública que se está firmando.
P: Clave pública más identificador de algoritmo utilizado y más parámetros si son necesarios.
Y{I}:Firma digital de Y por I usando la clave privada de la unidad certificadora.

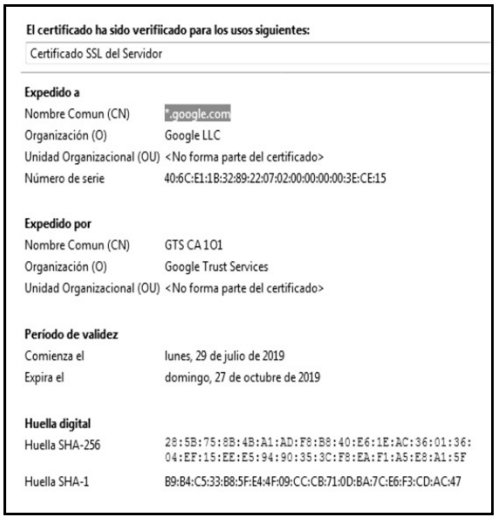
CA<<A>> = CA { V, SN, AI, CA, T_A, A, AP }

Y<<X>> es el certificado del usuario X expedido por la autoridad certificadora Y.

21

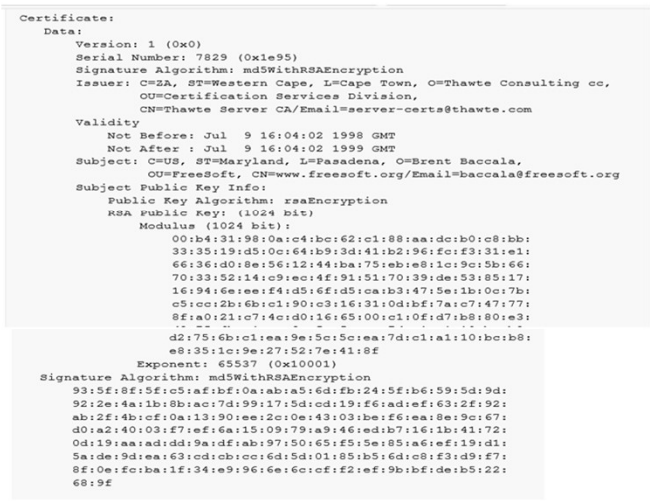
Certificado Digital X509

Serial Number
Certificate Algorithm: - Algorithm - Parameters
Issuer
Period of Validity: - Not Before Date - Not After Date
Subject
Subject's Public Key: - Algorithm - Parameters - Public Key
Signature



22

Detalles del Certificado Digital X509



```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 7829 (0x1e95)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
        Validity
            Not Before: Jul  9 16:04:02 1998 GMT
            Not After : Jul  9 16:04:02 1999 GMT
        Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                 OU=FreeSoft, CN=www.freesoft.org/Email=baccala@freesoft.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                    33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                    66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                    70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                    16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                    c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                    8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                    d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                    e8:35:1c:9e:27:52:7e:41:8f
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
        92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
        ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
        d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
        0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
        5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
        8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
        68:9f
```

23

Clases de Certificados

Según el tipo de Autenticación

Clase 1: corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.
Clase 2: la Autoridad Certificadora comprueba además el Documento de identidad o permiso de conducir que incluya fotografía, el número de la Seguridad Social y la fecha de nacimiento.
Clase 3: en la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante un servicio (Equifax, Datacredito).
Clase 4: que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización.

24

Tipos de Certificados

Según la naturaleza del Autenticado

Certificado personal, que acredita la identidad del titular.
Certificado de pertenencia a empresa, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
Certificado de representante, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
Certificado de persona jurídica, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
Certificado de atributo, el cual permite identificar una cualidad, estado o situación. Este tipo de certificado va asociado al certificado personal. (p.ej. Médico, Director, Casado, Apoderado de..., etc.).
Además, existen otros tipos de certificado digital utilizados en entornos más técnicos:
Certificado de servidor seguro, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

25

Revocación de Certificados

- **El usuario del certificado cree que su clave privada ha sido robada.**
- **Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica.**
- **El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.**
- **Una orden judicial.**
- **Etc.**

26

Revocación de Certificados

La lista de revocación de certificados **CRL (Certificate 'Revocation List**) es un registro utilizado en la operación de algunos sistemas usualmente los de infraestructura de clave pública **(PKI),** para mantener un listado de aquellos certificados (más concretamente sus números de serie) que han sido revocados y, por tanto, ya no son válidos y en los que no se debería confiar.

27

Autoridades de Certificación

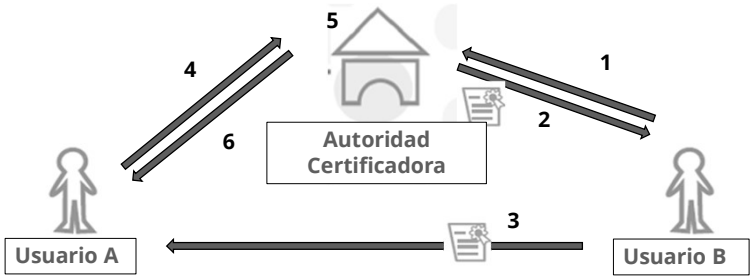
¿Qué son?

- Son entidades de confianza encargadas de certificar que una clave pública es válida y que pertenece a una determinada persona, Web o máquina, es decir, autentica la clave pública del usuario o sistema.
- Documento firmado por una CA (autoridad de certificación) que contiene diversos datos, al menos:
  - Identificación de una entidad (usuario)
  - su clave pública
- Emisor y receptor deben confiar en esa CA

- Pero además
  - Sólo la AC puede modificar el certificado del usuario sin que se detecte.
- Es fundamental tener
  - Confianza en las AC, de manera que los usuarios las reconozcan y dispongan del certificado de dicha autoridad de certificación. Por ello, deben acreditarse.

28

Protocolo de autenticación



1. Pido un certificado
2. La AC valida mi identidad y me otorga un certificado
3. Presento un certificado con mi identidad al usuario A
4. El usuario A no me conoce así que pregunta a la AC para verificar mi identidad
5. La AC comprueba que mi certificado es válido
6. La AC le dice al Usuario A que mi certificado es válido

29

Componentes y Estándar PKCS

30

Componentes

Los componentes más habituales de una infraestructura de clave pública son:

- La **autoridad de certificación** (o, en inglés, *CA, Certificate Authority*): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- La **autoridad de registro** (o, en inglés, *RA, Registration Authority*): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.
- **Los repositorios:** son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el **repositorio de certificados** y el **repositorio de listas de revocación de certificados.** En una lista de revocación de certificados (o, en inglés, *CRL, Certificate Revocation List*) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

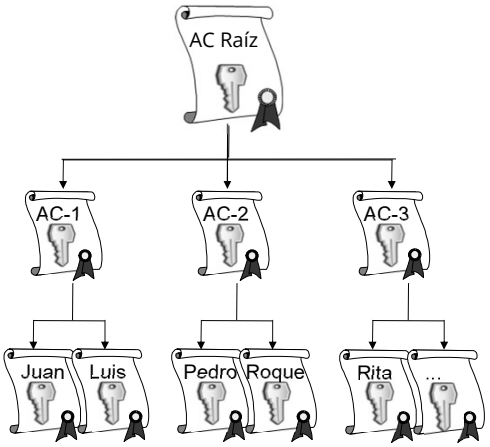
31

Componentes

- La **autoridad de validación** (o, en inglés, *VA, Validation Authority*): es la encargada de comprobar la validez de los certificados digitales.
- La **autoridad de sellado de tiempo** (o, en inglés, *TSA, Time Stamp Authority*): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
- Los **usuarios y entidades finales** son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.)

32

Jerarquía de AC's



33

Estándar PKCS

- PKCS: Public-Key Cryptography Standards, son un conjunto de especificaciones técnicas desarrolladas por RSA y otros desarrolladores de informática cuyo objeto es uniformizar las técnicas y protocolos de la criptografía pública.
- Publicación de la primera versión 1.0 se hace en el año 1991.
- PKCS forma parte de distintos estándares de hecho como ANSI PKIX, X9, SET, S/MIME y SSL.
- A la fecha existen 14 documentos con títulos genéricos que van desde PKCS #1 a PKCS #15.
- El de mayor trascendencia podría ser PKCS #11 llamado CRYPTOKI.
- Mantendremos los títulos originales en su versión en inglés de RSA Security Inc. Public-Key Cryptography Standards PCKS.

http://www.rsasecurity.com/rsalabs/pkcs/
https://es.wikipedia.org/wiki/PKCS

34

Diez riesgos sobre las PKI

35

Diez riesgos sobre las PKI

1. **¿En quien debo confiar?**
   Hoy en día existen multitud de entidades de certificación pero,
   ¿quién te garantiza que los datos que certifican son correctos (por ejemplo, un email o un nombre)?
   ¿Quién las ha situado en el contexto comercial en el que se encuentran?
2. **¿Quién tiene acceso a mi clave?**
   La criptografía de clave pública o asimétrica supone la existencia de dos claves: una *pública* y disponible de forma universal, y otra *privada* y bajo el control exclusivo del usuario. Pero, hoy en día, la *clave secreta* o *privada* no está segura. Los sistemas operativos y los navegadores adolecen de multitud de problemas de seguridad, además de existir virus y troyanos. Por tanto, no se puede garantizar que un documento firmado con una clave secreta constituya una firma confiable.
3. **¿Cómo de seguro es el ordenador verificador?** Como ocurre con el caso anterior, el ordenador que realiza la verificación del certificado puede haber sido manipulado. Puede, por ejemplo, haberse instalado una entidad de certificación espúrea en el navegador, algo absolutamente trivial.
4. **¿Qué "Jesús Cea" es el correcto?**
   Habitualmente los certificados se expiden a un nombre determinado, sin tener en cuenta que pueden existir diferentes personas con dicho nombre. En caso de disponer de información adicional, como su dirección de correo electrónico, tenemos que saber también si ésta es correcta o no, amén de vincular al usuario con datos que pueden quedar anticuados en un plazo breve.

36

Diez riesgos sobre las PKI

5. **¿La entidad de certificación es realmente una autoridad?** Por lo general, una entidad de certificación tradicional emite un certificado cubriendo datos sobre los que no tiene control. Por ejemplo, un certificado fusionando el nombre y la dirección de correo electrónico de un usuario no tiene en cuenta si el usuario se llama real y legalmente así, ni considera la posibilidad de que el email cambie o el ISP dé de baja la cuenta y la reasigne a otro usuario (o que todo el ISP desaparezca, por ejemplo).
6. **¿El diseño de seguridad considera al usuario?** Son muy pocos los usuarios, por ejemplo, que verifican los certificados del servidor remoto cuando establecen una conexión SSL con su navegador.

37

Diez riesgos sobre las PKI

7. ¿**Autoridades de certificación** o autoridades de certificación con **autoridades de registro**?
8. **¿Cómo identifica la autoridad de certificación al usuario?**

   Antes de emitir un certificado, la autoridad de certificación debe **tener la certeza de que los datos que certifica son correctos**.
9. **¿Los certificados son seguros?** El uso de certificados no garantiza la seguridad. Una cadena es tan fuerte como su eslabón más débil.
10. **¿Por qué existen entidades de certificación?** La conclusión más clara que se puede extraer de la lectura de este ensayo, elaborado por dos expertos de gran prestigio, es doble: los certificados deben ser expedidos por organismos oficiales con control sobre la información que están certificando (por ej., el Ministerio de Hacienda y el Número de Identificación Fiscal) y, por otra parte, es necesario almacenar los certificados personales en medios seguros tales como tarjetas Chip. En este contexto, iniciativas oficiales tales como el proyecto CERES español, por ejemplo, pueden ser la respuesta.

38

Consideraciones

Consideraciones para usuarios de certificados digitales

- La clave privada es generada, almacenada y utilizada en la estación de trabajo del usuario.
- Se debe proteger la clave privada, para esto se pueden utilizar contraseñas.
- La Autoridad Certificante NO posee copia de la clave privada, por lo tanto no puede restaurarla si se pierde.
- El certificador NO interviene en las comunicaciones entre las partes.
- No es necesario un certificado por cada documento a firmar digitalmente.
- La firma digital no se puede imprimir.

39

OCSP

40

OCSP

OCSP *(Online Certificate Status Protocol)* es un protocolo para determinar el estado de vigencia de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). Fue creado para solventar ciertas deficiencias de las CRL.

Cuando se despliega una PKI, es preferible la validación de los certificados mediante OCSP sobre el uso de CRL por varias razones:

- OCSP puede proporcionar una información más adecuada y reciente del estado de revocación de un certificado.
- OCSP elimina la necesidad de que los clientes tengan que obtener y procesar las CRL, ahorrando de este modo tráfico de red y procesado por parte del cliente.
- El contenido de las CRL puede considerarse información sensible, análogamente a la lista de morosos de un banco.
- OSCP puede implementar mecanismos de tarifa para pasarle el costo de la validación de las transacciones al vendedor, más bien que al cliente.

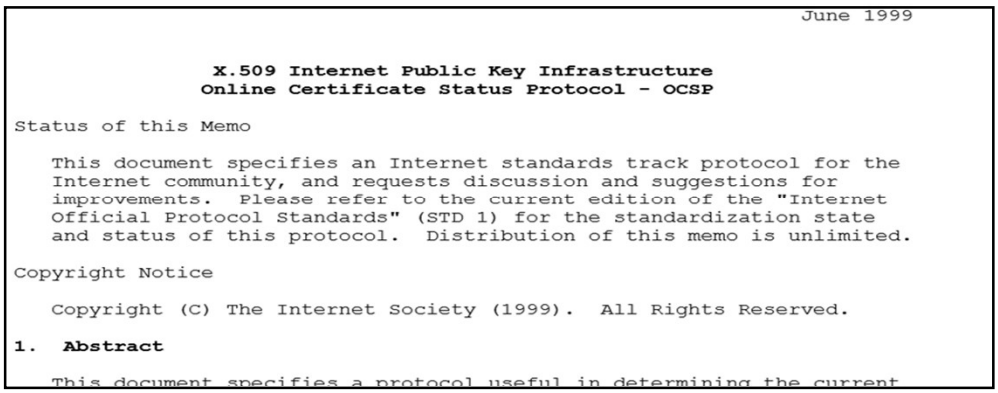
41

OCSP

- OCSP soporta el encadenamiento de confianza de las peticiones OCSP entre los "responders". Esto permite que los clientes se comuniquen con un "responder" de confianza para lanzar una petición a una autoridad de certificación alternativa dentro de la misma PKI.
- Una consulta sobre el estado de un certificado sobre una CRL, debe recorrerla completa secuencialmente para decir si es válido o no. OCSP, en el fondo, usa un motor de base de datos para consultar el estado del certificado solicitado, con todas las ventajas y estructura para facilitar las consultas. Esto se manifiesta aún más cuando el tamaño de la CRL es muy grande.

42

Protocolo OCSP



June 1999

X.509 Internet Public Key Infrastructure
Online Certificate Status Protocol - OCSP

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

1. Abstract

This document specifies a protocol useful in determining the current

43

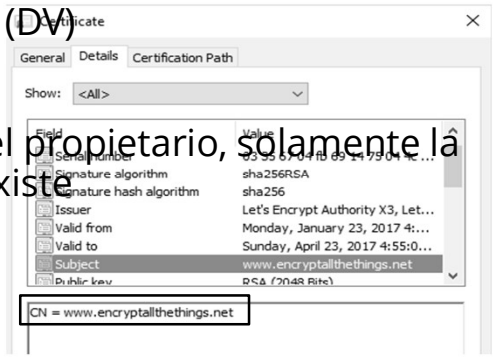
¿Cuando un sitio web es confiable?

44

Domain Validation (DV)

Solamente Validación de Dominio (DV)

Sin información de la identidad del propietario, solamente la confirmación de que el dominio existe



45

Organization validation (OV)

Organización Validada (OV)

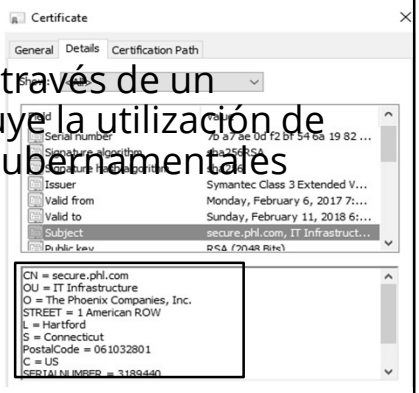
OV: Confirmación básica de la identidad a través de una verificación simple, corroborada a través del contacto con el cliente en función de datos suministrados por un tercero confiable

46

Extended Validation (EV)

- Validación Extendida (EV)

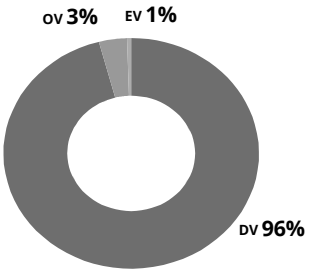
EV: Confirmación sólida de la identidad a través de un extenso proceso de verificación, que incluye la utilización de datos de terceros confiables y registros gubernamentales



47

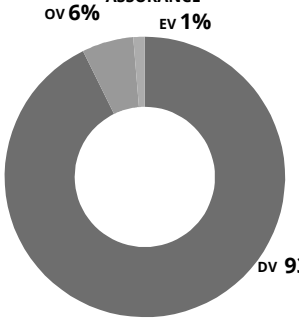
Uso de los Certificados

ARGENTINA % BREAKDOWN BY CERTIFICATE ASSURANCE



Certificate Assurance	No. of Certificates
EV	274
OV	1,810
DV	49,190
Total	**51,274**

LATIN AMERICA % BREAKDOWN BY CERTIFICATE ASSURANCE



Certificate Assurance	No. of Certificates
EV	5638
OV	25,319
DV	395,591
Total	**426,548**

Fuente: Netcraft Report (February 2017)

48

Ejemplos de Uso

49

Ejemplos de Uso

Los sistemas de PKI, de distintos tipos y proveedores, tienen muchos usos, incluyendo la asociación de una llave pública con una identidad para:

- Cifrado y/o autenticación de mensajes de correo electrónico (ej., utilizando OpenPGP o S/MIME).
- Cifrado y/o autenticación de documentos (ej., la firma XML * o Cifrado XML * si los documentos son codificados como XML).
- Autenticación de usuarios o aplicaciones (ej., logon por tarjeta inteligente, autenticación de cliente por SSL).
- Bootstrapping de protocolos seguros de comunicación, como Internet key exchange (IKE) y SSL.

50

Seguridad de los certificados

La seguridad en la infraestructura PKI depende en parte de cómo se guarden las claves privadas.

Existen dispositivos especiales denominados *tokens de seguridad* para facilitar la seguridad de la clave privada, así como evitar que ésta pueda ser exportada. Estos dispositivos pueden incorporar medidas biométricas, como la verificación de huella dactilar, que permiten aumentar la confiabilidad, dentro de las limitaciones tecnológicas, en que sólo la persona dueña del certificado pueda utilizarlo.

Criptografía

51

Certificado de Antecedentes Penales


Trámite: P1431039

CONSTANCIA DE EMISION DE
CERTIFICADO DE ANTECEDENTES PENALES
Art. 8 inciso f) LEY Nro. 22.117
Art. 52 C.P. (Modificado por Ley 23.057)

SE DEJA CONSTANCIA que : JUAN PEREZ
NACIONALIDAD Argentina, FECHA DE NACIMIENTO 20/10/1980
DOCUMENTO D.N.I. 23.444.666
NO REGISTRA ANTECEDENTES PENALES a informar por esta Repartición.
Se expide el presente a los efectos de ser presentado ante las autoridades que correspondan.

Buenos Aires, 19 de mayo de 2006

Firmado conforme Ley 25.506 por : Francisco Vallejos
Coord. Noche – Area At. Usuario

Código de seguridad

6C430647AA625626F86F6A69B1F04EF3062F7A50

52

Problemas

53

Problemas de la vida real

2001. Verisign emite 2 certificados a nombre de Microsoft a “desconocidos”

- Los certificados de Verisign no incluían link a una CRL
- Internet Explorer no chequeaba CRLs

2006. Phishing contra “Mountain America Credit Union”

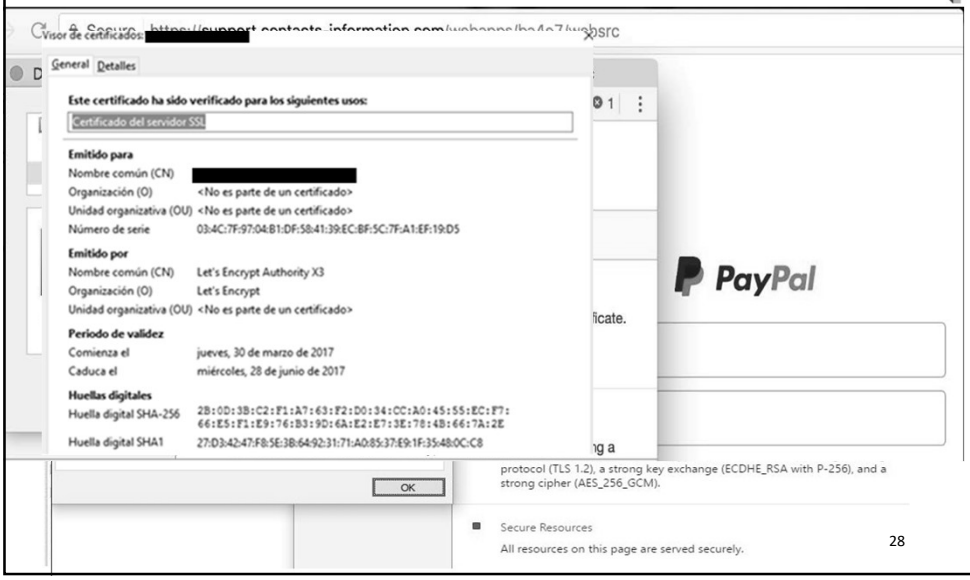
- Sitio y certificado de www.mountain-america.net
- ¿Quién puede registrar un determinado nombre?

¿Marzo? 2011: Atacantes hackean una cuenta de un partner de una autoridad de certificación, Comodo, y generan 8 certificados (mail.google.com, www.google.com, etc.)

Julio/Agosto 2011: “Hackers” logran penetrar la red de DigiNotar (una CA) y generar más de 200 certificados para distintos sitios

54

Problemas



28

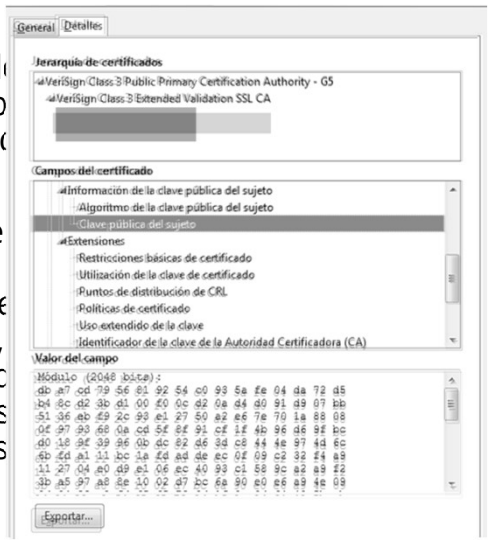
55

56

Relación entre los ataques cíclicos y los certificados x.509

Ahora veremos que también será posibl
usando nuevamente la misma clave púb
contra de toda la lógica de los sistemas
clave pública.

El problema que se nos presenta es que
conozca las claves usadas en el proceso
clave, podría en teoría recuperar el secre
públicas de un destinatario es muy fácil,
certificado digital X.509 al alcance de toc
como se observa en la siguiente figura, s
ataques a claves con números grandes s



57

Relación entre los ataques cíclicos y los certificados x.509

Como $C = N^e \bmod n$, con N un valor secreto, vamos a realizar cifrados sucesivos de los criptogramas C_i resultantes con la misma clave pública e. Si en uno de estos cifrados obtenemos nuevamente el cifrado C original con el que se ha iniciado el ataque, resulta obvio que el valor del paso anterior será el secreto N buscado.

$C_i = C^e_{i-1} \bmod n$; para i = 1, 2, ..., con $C_0 = C$

Si en el cifrado iésimo se encuentra el criptograma C inicial, entonces el cifrado anterior (i-1) será el número secreto, como se muestra en el siguiente ejercicio.

58

Relación entre los ataques cíclicos y los certificados x.509

Alicia desea comunicarse en secreto con Bernardo, para ellos utilizarán una clave secreta K. Alicia elige un nro y lo han cifrado con los datos públicos de Bernando que se conocen (sus claves públicas n = 187 y e = 7).

Alicia envia el mensaje cifrado C = 50 para que Bernardo lo descifre con su privada.

Aunque para este caso sería elemental encontrar los primos p y q (osea factorizando el módulo 187 = 11 x 17) vamos a ver qué sucede haciendo un ataque por cifrado cíclico.

Para ello usaremos simplemente la calculadora de Windows.
1ra operación: $C^e \bmod n = 50^7 \bmod 187 = 118$
2da operación: $C^e \bmod n = 118^7 \bmod 187 = 101$
3ra operación: $C^e \bmod n = 101^7 \bmod 187 = 84$
4ta operación: $C^e \bmod n = 84^7 \bmod 187 = 50$

Como en la cuarta operación se ha llegado al valor 50 con el que partimos en el ataque, resulta claro que la clave secreta era K = 84.

59

INCIDENCIA DEL VALOR CAPTURADO EN EL ATAQUE

Con el programa genRSA crea las siguientes claves y haz un ataque cíclico con los valores que se indican.

Anota el número de vueltas que debe realizar el programa hasta dar con el secreto.

Clave 1) p = 367, q = 487, e = 713. Valores de ataque: 20, 22, 24, 26, 27, 29 y 30. Número cifrados: 500

Clave 2) p = 1949, q = 1889, e = 51. Valores de ataque: 10, 13,16, 17, 19 y 20. Número cifrados: 3.000

60

INCIDENCIA DEL VALOR CAPTURADO EN EL ATAQUE

Por lo tanto, si un ataque prospera en torno a las 300.000 vueltas, deberás esperar en el mejor de los casos al menos 10 minutos.

El problema de este tipo de ataque es que, además de necesitar como dato el criptograma, es decir que es necesario capturar previamente esa información, no resulta sencillo llevarlo a un escenario de ataque distribuido pues los subgrupos que se forman son muy grandes cuando aumenta el tamaño de la clave. Existe una proporcionalidad entre el tamaño del módulo n y el tamaño de la ventana de cifrados del ataque, con lo cual va a ser muchísimo más difícil atacar, por ejemplo, una clave de 100 bits que una de 80.

Por otra parte como ya hemos visto, existe también una gran dispersión en el número de cifrados necesarios para que prospere el ataque ante claves de iguales dimensiones. En las siguientes figuras se muestran dos tablas que muestran este efecto.

61

Side Channel Attacks

Si bien en este curso no vamos a profundizar en estos ataques, pero debemos conocer su existencia.

Una primitiva criptográfica (algoritmo) debe ser implementada en un programa que ejecutara en un procesador dado, o de forma más general en un ambiente dado. En consecuencia, presentara ciertas características de implementación (hardware).

Los ataques físicos toman ventaja de las características de implementación para quebrar el criptosistema.

Es por esto que estos ataques son menos generales, dado que son específicos a cierta implementación, pero pueden ser mucho más poderosos que el criptoanálisis clásico.

Es por esto que deben ser tenidos en cuenta a la hora de fabricar los dispositivos que ejecutaran (o almacenaran información de) los algoritmos.

62

Side Channel Attacks

Los ataques Físicos usualmente se clasifican de la siguiente manera:

Invasivos o No-invasivos:

- Los ataques invasivos desarman el dispositivo para acceder al núcleo (chip) y de esta forma tener acceso directo a sus componentes. Por ejemplo, puede ser un cable conectado a un puerto para obtener la transferencia de datos.
- Los ataques no-invasivos explotan solamente la información disponible externa la cual usualmente se emite de forma involuntaria por el dispositivo. Por ejemplo, tiempo de cómputo, consumo eléctrico, emisión de sonidos, temperatura de la CPU, etc.

Activo o Pasivo

- Los ataques activos tratan de manipular el dispositivo para lograr un mal funcionamiento deseado y as explotarlo. Por ejemplo, inducir errores en los cálculos.
- Los ataques pasivos simplemente observan el comportamiento de los dispositivos durante el procesamiento sin alterarlo.

63

Herramientas / TIPS

64

Son seguros los ¿WWW...? Que navegamos

A. Nombrar o ingresar a sitios web

https://www.ssllabs.com/

B Buscar y validar que tipo de Certificados digitales

65

Buscador de certificados

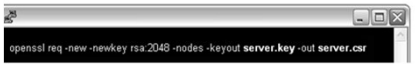
https://ssl-tools.net/certificates

66

Pasos para crear un certificado

1. **Cómo crear su CSR (Windows / Unix)**
   Esto genera un request en Base64
2. **Se envía el CSR a la empresa emisora de los certificados**
3. **instalar y configurar su certificado SSL en la plataforma web**
   1. **Instalar certificado SSL**
   2. **Asignar certificado SSL**
   3. **Enlaces del sitio web**
   4. **Exportar certificados**


```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```



Links https://www.digicert.com/kb/csr-creation-ssl-installation-iis-10.htm
https://www.digicert.com/kb/csr-ssl-installation/apache-openssl.htm
https://www.digicert.com/kb/ssl-support/pfx-import-export-iis-

67

Seguridad en la navegación Web

Buenas prácticas de seguridad en la navegación Web:

- ✓ No hagas clic en enlaces dentro del correo electrónico. Si es necesario verificar, es mejor escribir la dirección manualmente en el navegador.
- ✓ Evitar acceder a sitios desconocidos o no confiables.
- ✓ No aceptar la instalación automática de software.
- ✓ No dejar información sensible en páginas o foros.
- ✓ Si debe enviar información sensible: sólo hacerlo en sitios seguros (https) y verificar que el certificado sea del sitio al que desea ingresar
- ✓ Consulte con su administrador sobre configuración segura del navegador
- ✓ No descargar archivos ejecutables.

68

¡Gracias!

69