SEGURIDADE INFORMÁTICA

Unidade 02. Criptografía

Índice

1. Técnicas criptográficas

1.1 Introdución

Hoxe en día, os datos e as comunicacións necesitan ser cifradas, xa que a información é poder e para sacar o máximo dunha información hai que compartila. O momento no que se produce esta transferencia de información en algún soporte é o momento de maior vulnerabilidade para a mesma, xa que outros individuos non autorizados poderían roubar ou escoitar dita información.

Así, a criptografía está presente en accións que se realizan a cotío, como acceder a sitios web usando https ou a presentación de documentos na administración pública vía telemática empregando o dni-e ou certificados dixitais da FNMT (Fábrica Nacional de Moeda e Timbre).

1.2 Criptoloxía

A criptoloxía é a práctica e o estudo da ocultación de información. É a ciencia de cifrar e descifrar información mediante técnicas especiais, empregándose para facer ininteligibles mensaxes para receptores non autorizados. Búscase facer un intercambio de mensaxes que só poidan ser lidos por persoas ás que van dirixidos e que posúen os medios para descifralos.

A criptoloxía pode dividirse en dúas ramas:

- Criptografía: centrada nas técnicas para cifrar a información.
- Criptoanálise: centradas nas técnicas e mecanismos para decodificar a información, rompendo os procedementos de cifrado e recuperar a mensaxe orixinal.

Poden atoparse exemplos de uso de técnicas criptográficas na antigüidade, como a 'escítala espartana' o 'método Polybios', o "cifrador do César' ou o 'cifrador de Vigènere', onde se empregaba a substitución e a trasposición das letras da mensaxe orixinal para obter outra mensaxe inintelixible.

Escítala. Fonte: Wikipedia. Licenza CC BY-SA 3.0

Todos estos métodos criptográficos foron perfeccionándose e mellorándose segundo avanzaban os anos, e é na 2ª Guerra Mundial cando se fai imprescindible o uso das máquinas criptográficas para evitar que o inimigo interceptase a información das operacións de ataque que se pretendían realizar. Unha delas foi a máquina *Enigma*, que se amosa na imaxe:

Máquina Enigma: Museo nazionale della scienza e della tecnologia Leonardo da Vinci, Milano. Fonte: Wikipedia.

Hoxe en día, a criptografía que se emprega data dos anos 70. Estas técnicas aplícanse cada día no mundo da tecnoloxía en multitude de usos como as comunicacións militares, protocolo https, protocolo ssh, envío de correos electrónicos cifrados ou as telecomunicacións en xeral.

A información orixinal que debe protexerse denomínase *texto plano* (texto en claro). O cifrado é o proceso de converter o texto plano nun texto imposible de ler chamado *texto cifrado* ou *criptograma*. Para obter un texto cifrado, aplícase un algoritmo de cifrado, utilizando unha clave, ao texto plano:

Para recuperar a mensaxe orixinal, aplicarase o algoritmo de descrifrado ao criptograma (texto cifrado) empregando a clave:

Os principais obxectivos que busca a criptografía son:

- **Confidencialidade**: a información revélase unicamente aos usuarios autorizados. Por exemplo; usando https para acceder a un sistema de webmail, os datos de usuario/contrasinal irán cifrados por un túnel de comunicacións establecido entre o navegador do usuario e o servidor. Conséguese así que o navegador e o servidor poidan intercambiar información pero que esa información non sexa lexible para os demais (se se capturasen os paquetes da comunicación veríanse os datos cifrados).
- **Integridade**: garante a exactitude da información contra a alteración, perda ou destrución da información. Por exemplo, cando se firma electronicamente un documento, apórtase un 'resumo' que garante que se o documento orixinal fose modificado, poderíase detectar

a manipulación ao non coincidir o resumo do documento orixinal co resumo do documento modificado.

- **Autenticación**: comprobación da identidade. Por exemplo, ó usar ssh para conectarse a un equipo remoto, o cliente comproba a identidade dixital do servidor ssh para asegurarse que se está conectando ao servidor de verdade e non a un impostor.
- **Non repudio** (irrenunciabilidade ou vinculación): vincula un documento ou transacción a unha persoa ou equipo. Por exemplo, na firma electrónica de documentos garántese o non repudio no emisor; é dicir, empréganse mecanismos tales que se garante que un documento firmado electronicamente por unha persoa usando a súa identidade dixital está asociado a esa persoa, non sendo posible que fose asinado por outra.

Dependendo do número de claves utilizadas polos algoritmos de cifrado/descifrado, existen dous tipos de métodos criptográficos:

- Criptografía de clave simétrica, que utiliza unha única clave.
- Criptografía de clave asimétrica, que utiliza dúas claves.

Como se verá máis adiante, existen sistema chamados de criptografía híbrida, que empregan os dous sistemas (simétrico e asimétrico) na procura dun mellor rendemento.

1.3 Criptografía de clave simétrica

Na criptografía de clave simétrica emprégase **unha única clave** para cifrar e descifrar mensaxes. Unha vez que as dúas partes que se van comunicar posúen a mesma clave, o remitente cifra unha mensaxe con ela, envíaa ao destinatario e este descífraa coa mesma clave.

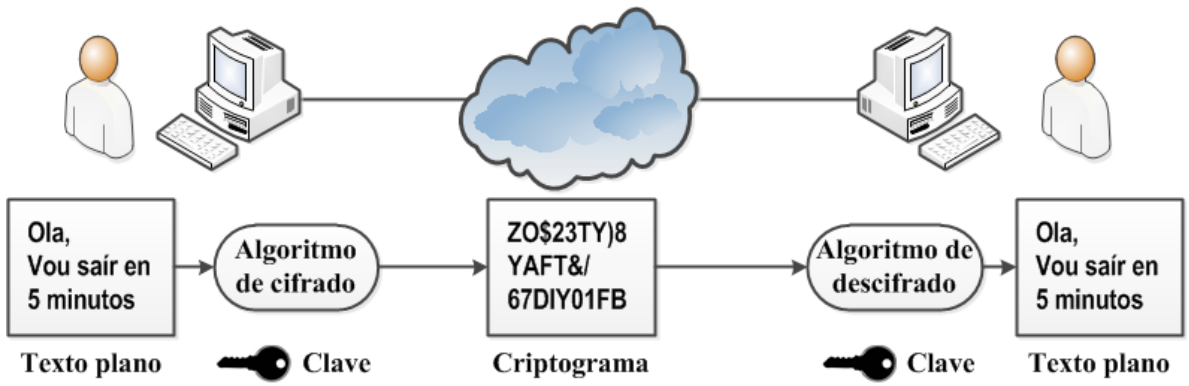


Fig. Criptografía de clave simétrica

Un problema que teñen os sistemas de clave simétrica é o intercambio de claves; xa que, antes de poder enviar información, os participantes teñen que intercambiarse a clave. Se a clave cae en malas mans toda comunicación que use esa clave comprometida non será segura; xa que, persoas non autorizadas poderán acceder aos contidos transmitidos. Se se atopa un sistema seguro para intercambiar a clave, este sistema é o máis eficaz.

Un bo sistema de cifrado centra toda a seguridade na clave e non no algoritmo; é dicir, non debería ser de ningunha axuda para un atacante coñecer o algoritmo que se está usando. Só se o atacante obtivese a clave, serviríalle coñecer o algoritmo. Dado que toda a seguridade está na clave, é importante que sexa moi difícil adiviñar o tipo de clave. Isto quere dicir que o abanico de claves posibles (espazo de posibilidades de claves) debe ser amplo.

Na seguinte táboa pode compararse a lonxitude de clave e o número de claves posibles:

Tamaño (lonxitude da clave)	Número de claves posible
8	$2^8 = 256$
40	$2^{40} = 1.099.511.627.776$
56	$2^{56} = 72.057.594.037.927.900$
64	18.446.744.073.709.600.000
128	340.282.366.920.938.000.000.000.000.000.000.000.000
256	1,16E+077
512	1,34E+154

Os computadores modernos poden descifrar claves con extrema rapidez, e esta é a razón pola cal o tamaño da clave é importante nos criptosistemas modernos. O algoritmo de cifrado DES usa unha clave de 56 bits, o que significa que hai 2^{56} claves posibles. Aínda que pode parecer un número moi grande de posibles claves, un computador xenérico pode comprobar o conxunto posible de claves en cuestión de días e un equipo especializado en horas.

Algoritmos de cifrado de deseño máis recente como AES, 3DES, Blowfish e IDEA usan claves de maior lonxitude, o que dificulta enormemente os ataques ó prolongalos no tempo. A modo de exemplo, o algoritmo AES (Advanced Encryption Standard) permite o uso de claves de 128, 192 e 256 bits. AES é un estándar de cifrado no Goberno dos Estados Unidos de América e para os documentos clasificados como TOP SECRET é obrigatorio o uso de claves de 192 ou 256 bits.

Exemplo de criptografía simétrica

Un exemplo de criptografía simétrica é a autenticación dun móbil GSM: por que sabe que é o noso número, aínda que metamos o cartón SIM noutro teléfono. O procedemento é o seguinte:

- A nosa tarxeta SIM contén un identificador T e unha clave K.
- Ese identificador T e a clave K aparecen asociados ao noso contrato nos servidores de autenticación da operadora da que somos clientes.
- Cando acendemos o teléfono, conéctase á rede da operadora e solicita entrar co identificador T. O seu servidor de autenticación recibe a petición e xera un número aleatorio A (chamado desafío), que nos envía.
- Unha vez recibido, no noso teléfono aplicamos un determinado algoritmo simétrico sobre ese número A, utilizando a clave K (ciframos o número A coa clave K). O resultado é o número B. Enviamos o número B ao servidor de autenticación.
- Cando o recibe, el tamén aplica o mesmo algoritmo coa mesma clave. Se o resultado é igual a B, confírmase que somos os donos do identificador T. Asígnanos o noso número 6XXXXXXX, e xa podemos facer e recibir chamadas.
- Se cambiamos de teléfono, non importa porque o número vai asociado á SIM.

Con esta solución estamos protexidos dunha posible captura de tráfico inarámico mediante un sniffer de rede:

Podería capturar o número A. Pero é un simple número aleatorio: sen o algoritmo e a clave, o atacante non poderá xerar a resposta correcta B.

Podería capturar tamén o número B e xa tería a resposta correcta cando o servidor envía o número A. Pero a probabilidade de que o servidor repita o mesmo número A para este abonado é moi baixa. É dicir, se o atacante elabora unha tarxeta SIM preparada para responder B cando lle pregunten A, é moi pouco probable que teña éxito.

1.4 Criptografía de clave asimétrica

Os sistemas criptográficos de clave simétrica teñen o problema da distribución da clave entre os participantes da comunicación. Nos sistemas de clave asimétrica non existe este problema e cada participante ten un parella de claves propias:

- Clave privada:
  - O seu propietario debe mantela en segredo a toda costa.
  - Permite cifrar mensaxes (que poderán ser descifrados coa clave pública).
  - Permite descifrar mensaxes cifrados coa clave pública do propietario.
- Clave pública:
  - Debe repartirse a todos os usuarios cos que se queira comunicar.
  - Úsase para enviar mensaxes cifradas ó propietario, que só el poderá descifrar usando a súa clave privada.
  - Úsase para descifrar mensaxes enviadas polo propietario e cifrados coa clave privada.

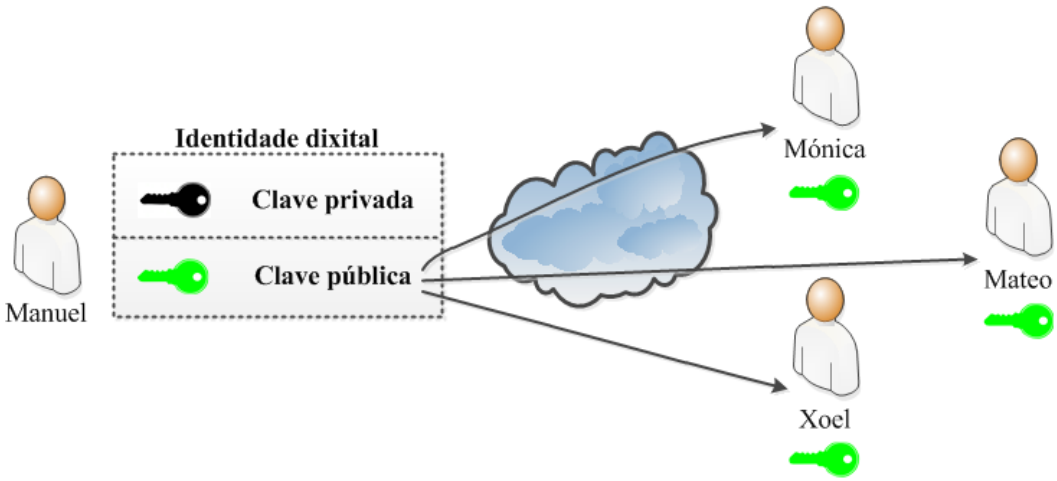


Fig. Criptografía de clave asimétrica

Na seguinte imaxe pode verse o que sucede se Mónica envía unha mensaxe a Manuel cifrándoa coa clave pública de Manuel. O que consegue é que unicamente Manuel a poida descifrar usando a súa clave privada (a de Manuel). Ninguén, agás o que teña a clave privada de Manuel poderá descifrar a mensaxe; polo tanto, conseguiuse a confidencialidade.

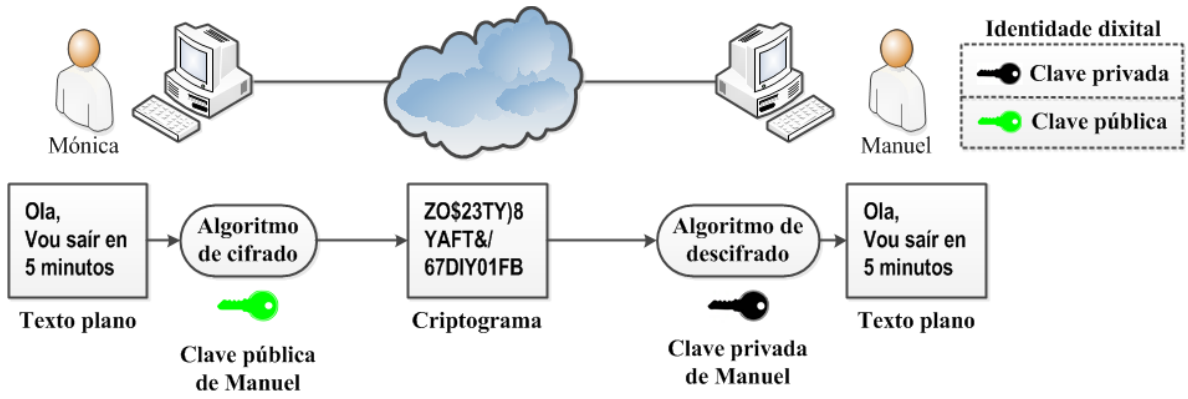


Fig. Confidencialidade usando criptografía de clave asimétrica

Agora Manuel envía unha mensaxe cifrada coa súa clave privada a Mónica. Mónica, usando a clave pública de Manuel, será capaz de descifrar a mensaxe e terá a seguridade de que a mensaxe foi enviada por Manuel; xa que, ninguén agás Manuel posúe a clave privada (de Manuel). Conséguese a identificación e a vinculación (non repudio) do remitente.

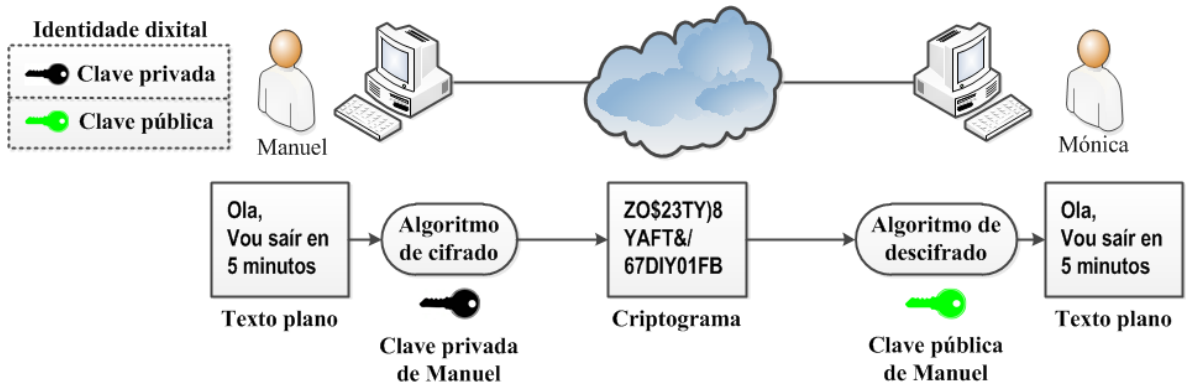


Fig. Identificación e vinculación usando criptografía de clave asimétrica

Unha vez entendidas as posibilidades que ofrece o uso das claves privadas e públicas de Manuel, plantéxase a situación onde Manuel e Mónica queren comunicarse buscando á vez confidencialidade, identificación e vinculación. Para acadalo:

- Manuel ten a súa clave privada que non comparte con ninguén.
- Manuel envía a súa clave pública a Mónica.
- Mónica ten a súa clave privada que non comparte con ninguén.
- Mónica envía a súa clave pública a Manuel.
- Mensaxes de Manuel a Mónica:
  - Manuel cifra a mensaxe coa súa clave privada e despois a cifra coa clave pública de Mónica.
  - A mensaxe dobremente cifrada envíase a Mónica.
  - Unha vez que lle chega a mensaxe a Mónica, ésta descifra a mensaxe coa súa clave privada e o resultado procede a descifralo coa clave pública de Manuel. Unha vez aplicado este procedemento, Mónica recupera a mensaxe orixinal de Manuel.
- Mensaxes de Mónica a Manuel:
  - Mónica cifra a mensaxe coa súa clave privada e despois a cifra coa clave pública de Manuel.

– A mensaxe dobremente cifrada envíase a Manuel.
– Unha vez que lle chega a mensaxe a Manuel, éste descifra a mensaxe coa súa clave privada e o resultado procede a descifralo coa clave pública de Mónica. Unha vez aplicado este procedemento, Manuel recupera a mensaxe orixinal de Mónica.

O que se consegue con este sistema é:

- Ao cifrar en primeiro lugar coa clave privada do remitente, o destinatario poderá estar seguro de que a mensaxe realmente procede do remitente; e polo tanto, garántese a identificación e vinculación do remitente.
- Ao cifrar en segundo lugar coa clave pública do destinatario, asegúrase que unicamente o destinatario pode ver o contido da mensaxe (grazas a que a única clave que pode descifrar a mensaxe é a privada do destinatario); e polo tanto, garántese a confidencialidade do envío.

Na seguinte imaxe pode verse o proceso a seguir no envío de mensaxes de Manuel a Mónica:

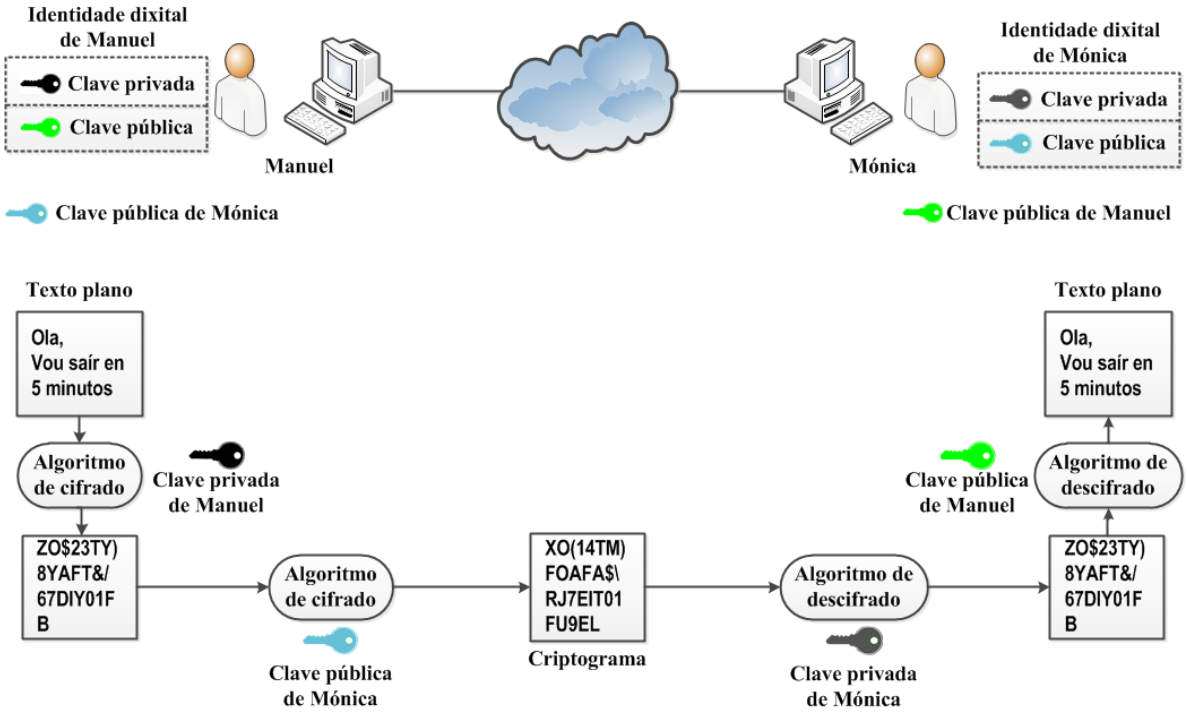


Fig. Confidencialidade, identificación e vinculación usando criptografía de clave asimétrica

Os métodos criptográficos garanten:

- Que esa parella de claves só se poida xerar unha vez, de modo que se pode asumir que non é posible que dúas persoas obtivesen casualmente a mesma parella de claves.
- Que a partir da clave pública non se pode deducir nada da clave privada.
- Que o que cifra a clave pública só pode ser descifrado coa privada e o que cifra a clave privada só o descifra a pública.

Agora o intercambio de claves xa non é problema xa que a pública está pensada para repartirse. O que se é crítico é manter a clave privada a bo recaudo. Exemplos de métodos de cifrado asimétricos son Diffie-Hellman, RSA, DSA e ElGamal.

1.5 Sistemas criptográficos híbridos

Debido a que os sistemas de cifrado asimétricos son computacionalmente máis custosos que os simétricos e que estes últimos teñen o problema de intercambio de claves, inventáronse os sistemas de criptografía híbrida. Nestes sistemas híbridos, ao comezo da comunicación emprégase un sistema de claves asimétricas para intercambiar de forma segura unha clave simétrica de sesión, que se usará para cifrar o resto da comunicación de forma máis eficiente. Un exemplo de implementación práctica deste tipo de sistema pode atoparse no protocolo SSH.

Na seguinte figura pode verse un resumo do proceso:

- Paso 1: Manuel envía a clave pública a Mónica.
- Paso 2: Mónica xera unha clave de sesión que é cifrada usando a clave pública de Manuel e a envía a Manuel. Este procede a descifrala usando a súa clave privada.
- Paso 3: unha vez que os dous participantes da comunicación xa coñecen a clave de sesión, poden proceder a enviar mensaxes cifradas e descifralas usando a mesma clave (criptografía simétrica).

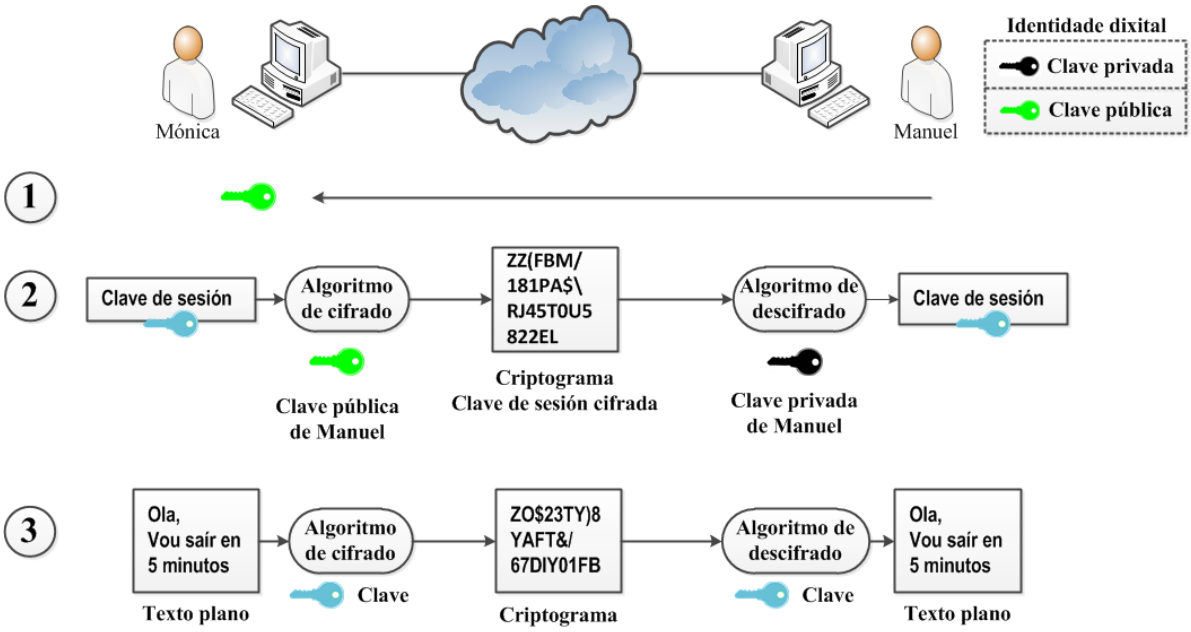
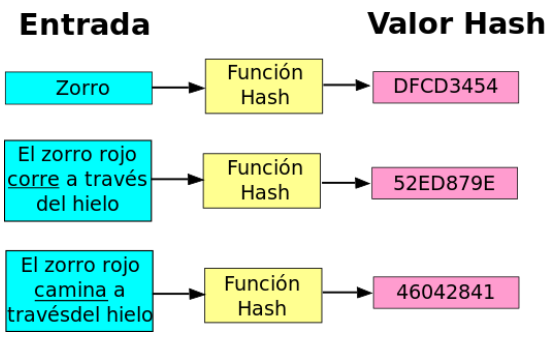


Fig. Criptografía híbrida

1.6 Funcións Hash

Unha función hash é unha función matemática que converte un conxunto de datos noutro, normalmente nunha cadea de lonxitude fixa. O valor devolto pola función hash chámase resumo, checksum, suma hash ou hash. As funcións hash tamén son coñecidas como funcións resumo ou funcións digest. A seguinte imaxe exemplifica o funcionamento dunha función hash:



Funcionamento das funcións hash. Wikipedia. Licenza CC BY-SA 3.0.

A modo de exemplo, calcularase o hash MD5 dun arquivos usando o comando md5sum en Linux Ubuntu:

```
$ cat arquivo.txt
ola mundo
$ md5sum arquivo.txt
2c61dba1b7d13d2224bb94a08044cc96  arquivo.txt
```

Se o contido do arquivo cambia, tamén cambiará o hash:

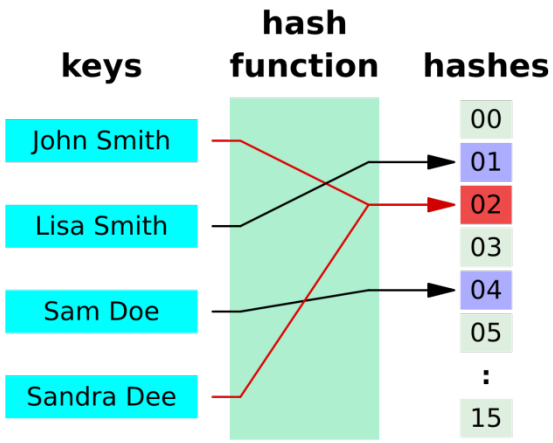
```
$ cat arquivo.txt
ola mundo
adeus mundo
$ md5sum arquivo.txt
aec5dd5542ecd96b30b773a475624c7d  arquivo.txt
```

Unha función hash funciona nunha soa dirección, e polo tanto, é imposible calcular os datos orixinais a partir do valor resumo. Ó aplicar unha función hash a un documento ou ficheiro o valor resumo é unha cadea que identifica inequívocamente o contido. Este feito fai que as funcións hash se usen para:

- Comprobación da integridade dun ficheiro: as funcións hash permiten saber se un ficheiro sufriu modificacións; xa que, un cambio no contido do ficheiro tradúcese nun valor resumo diferente. Esto permite usar as funcións hash para:
  - Comprobar se un arquivo descargado/enviado/almacenado se corrompeu (erros fortuitos). Por exemplo, verificar a validez dunha imaxe iso descargada antes de queimala nun CD.
  - Comprobar se o contido de arquivos de configuración, binarios do sistema, etc. sufriu modificacións. Por exemplo, calcúlase o hash de determinados arquivos de configuración e binarios do sistema. Se o equipo fose asaltado e o atacante realizase modificacións nalgún arquivo de configuración ou binario, podería detectarse xa que os hashes deses arquivos cambiaron. Esta técnica é usada por sistemas HIDS (host-based intrusion detection system) como tripwire e OSSEC.
- Identificación de ficheiros: como o hash depende do contido do arquivo é posible identificar arquivos con independencia do seu nome e/ou ubicación. Un exemplo desta funcionalidade pódese atopar no software Hispalis da Garda Civil. Hispalis rastrexa os hashes dos arquivos que se intercambian en redes P2P e compáraos cos hashes de vídeo e fotografías de carácter pedófilo das súas bases de datos. Se coincide o hash dun arquivo da rede P2P co hash dun arquivo da base de datos da Garda Civil quere dicir que na rede P2P hai material ilegal.

- Almacenamento de contrasinais: en lugar de almacenar o contrasinal dos usuarios, almacénase o hash do contrasinal. Cando un usuario quere autenticarse indicando o seu contrasinal, calcúlase o hash e compárase co valor do hash almacenado.

Unha colisión hash prodúcese cando dúas entradas diferentes a unha función hash producen o mesmo valor resumo. No exemplo da seguinte imaxe pode verse unha colisión; xa que, dous valores diferentes de entrada (John Smith e Sandra Dee) levan ó mesmo hash.



Función hash. Wikipedia. Licenza Dominio Público.

Cando o rango de posibles valores resumo é menor que o rango de posibles valores de entrada haberá colisións. En criptografía, acéptase o uso de funcións hash especialmente deseñadas para garantir que as colisións son computacionalmente imposibles; é dicir, o tempo para lograr unha colisión hash é tan grande que non se considera factible. Exemplos de funcións hash usadas en criptografía son MD5 (Message Digest Algorithm), SHA (Secure Hash Algorith) e RIPEPMD-160.

A finais de 2008, e tras descubrirse varios erros no deseño, MD5 foi considerado criptograficamente roto e non apto para o seu uso polo departamento de seguridade nacional de EEUU. Algo semellante sucedeu con SHA-1 polo que a partir do ano 2010 recomendouse o uso de SHA-2.

Hai que valorar a importancia das colisións en funcións hash. Unha colisión hash supón que dous documentos con contidos diferentes teñen o mesmo resumo hash. Outra cousa é que o contido deses arquivos teñan algún sentido. Sen embargo, e como xa se indicou no punto anterior, recoméndase o uso de funcións hash sen problemas coñecidos.

2. Sistemas de identificación dixital

2.1 Xestión de claves públicas

Na actividade anterior estudamos as técnicas criptográficas de clave simétrica e asimétrica.

Grazas á criptografía de clave asimétrica un individuo pode posuír unha identidade dixital baseada nas súas dúas claves (a súa clave privada e a súa clave pública). O que interesa agora é poder asignar de forma unívoca esa identidade dixital a un determinado individuo. Hai dúas aproximacións:

- Redes de confianza: é un modelo descentralizado onde os individuos envían a súa clave pública a aquelas persoas coas que se relaciona ou as publica nalgún servidor accesible. É o modelo adoptado por PGP e OpenPGP.
- PKI (Public Key Infraestructure): é un modelo centralizado onde unha organización se encarga de rexistrar e manter unha base de datos de claves públicas. Esta organización manterá unha infraestrutura para recibir solicitudes, verificar identidades e emitir documentos dixitais que certifiquen o rexistro da clave pública coa identidade do solicitante. A esa infraestrutura (hardware, software, persoal, políticas e procedementos) denomínase Infraestrutura de Clave Pública ou PKI.

2.2 Certificado dixital

Un certificado dixital é un documento electrónico, emitido mediante unha PKI, mediante o cal unha entidade (chamada de forma xenérica terceiro de confianza) garante o vínculo entre a identidade dun suxeito e unha clave pública (e polo tanto coa súa privada correspondente). Basicamente, é un documento que asocia unha identidade real cunha identidade dixital emitido por unha organización que se encargou de verificar esa asociación.

Un certificado dixital contén xeralmente información do tipo:

- Datos do usuario: nome, apelidos, correo electrónico, organización á que pertence, posto ou cargo profesional, etc.
- Clave pública, lonxitude e algoritmo usado na súa xeración.
- Datos da entidade que emitiu a certificado.
- Validez.
- Uso/s para os que foi rexistrada/autorizada a clave.

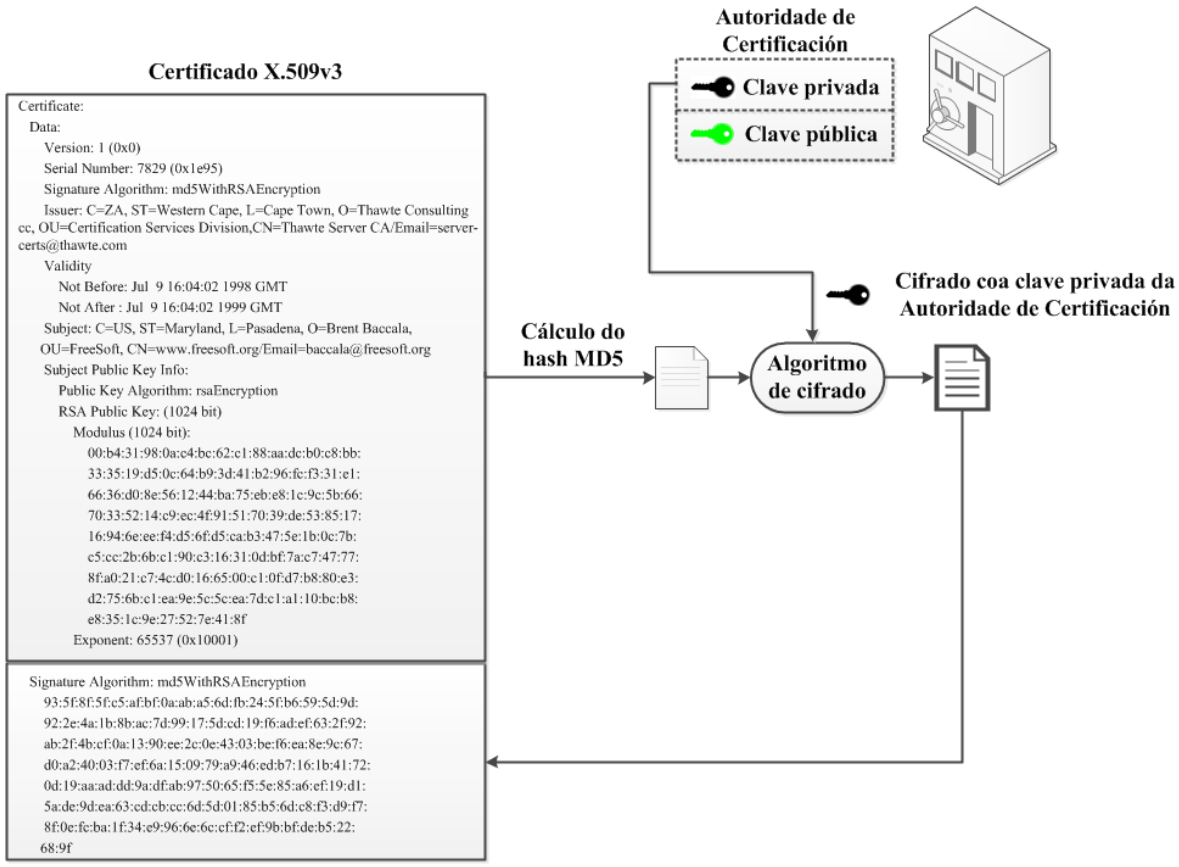
Debe quedar claro que as claves criptográficas e os certificados están relacionados pero non son o mesmo. As claves pública/privada son secuencias e a súa misión é permitir o cifrado/descifrado da información usando os algoritmos criptográficos correspondentes. En cambio, a misión dos certificados é identificar ao propietario do certificado, quedando asociado a unha parella de claves.

A UIT (Unión Internacional de Telecomunicacións) definiu o estándar X.509 de certificados dixitais para buscar unha homoxeneización e interoperabilidade entre os certificados emitidos por diferentes organizacións. O estándar define o contido común dos certificados permitindo o seu emprego por aplicacións de diferentes fabricantes. O formato dos certificado X.509v3 pódese ver a continuación cun exemplo:

Campos	Certificado
▪ Versión ▪ Número de serie ▪ ID do algoritmo ▪ Emisor ▪ Validez Non antes de Non despois de ▪ Suxeito ▪ Información de clave pública do suxeito Algoritmo de clave pública Clave pública del suxeito ▪ Identificador único de emisor (opcional) ▪ Identificador único de suxeito (opcional) ▪ Extensións (opcional) ▪ Algoritmo usado para firmar o certificado ▪ Firma dixital do certificado	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

Este certificado de exemplo foi emitido pola autoridade Thawte para www.freesoft.com. Na parte final do certificado pode verse a clave pública de www.freesoft.com e a firma dixital.

A firma dixital permite asegurar a integridade do certificado e posibilitar as comprobacións de que non se realizaron cambios dende a súa emisión. Para asinar o certificado utilízase outra parella de claves xeradas con esta finalidade e asociadas á entidade certificadora.



Para verificar a integridade dun certificado, calcúlase o hash e compróbase co valor da firma (previo descifrado coa clave pública da entidade).

A clave pública desta parella de claves da entidade inclúese nun certificado autofirmado (asinado pola mesma clave privada asociada á clave pública que contén) e que se distribuirá para que calquera usuario poida comprobar que un certificado foi asinado pola entidade. Este certificado chámase certificado raíz da entidade de certificación e a súa clave privada utilízase para asinar os certificados dixitais que emite a entidade, ou ben para xerar outro certificado intermedio co que asinar os certificados dixitais que emiten.

Na seguinte táboa aparece un certificado autofirmado onde pódese comprobar que o Emisor (Issuer) e o suxeito (Subject) son iguais:

Campos	Certificado
▪ Versión ▪ Número de serie ▪ ID do algoritmo ▪ Emisor ▪ Validez Non antes de Non despois de ▪ Suxeito ▪ Información de clave pública do suxeito Algoritmo de clave pública Clave pública del suxeito ▪ Identificador único de emisor (opcional) ▪ Identificador único de suxeito (opcional) ▪ Extensións (opcional) ▪ Algoritmo usado para firmar o certificado ▪ Firma dixital do certificado	Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) 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: Aug 1 00:00:00 1996 GMT Not After : Dec 31 23:59:59 2020 GMT **Subject: 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** Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c: 68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:

Campos	Certificado
	85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06: 6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2: 6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b: 29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90: 6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f: 5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36: 3a:c2:b5:66:22:12:d6:87:0d Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: critical CA:TRUE Signature Algorithm: md5WithRSAEncryption 07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9: a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48: 3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88: 4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9: 8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5: e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9: b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e: 70:47

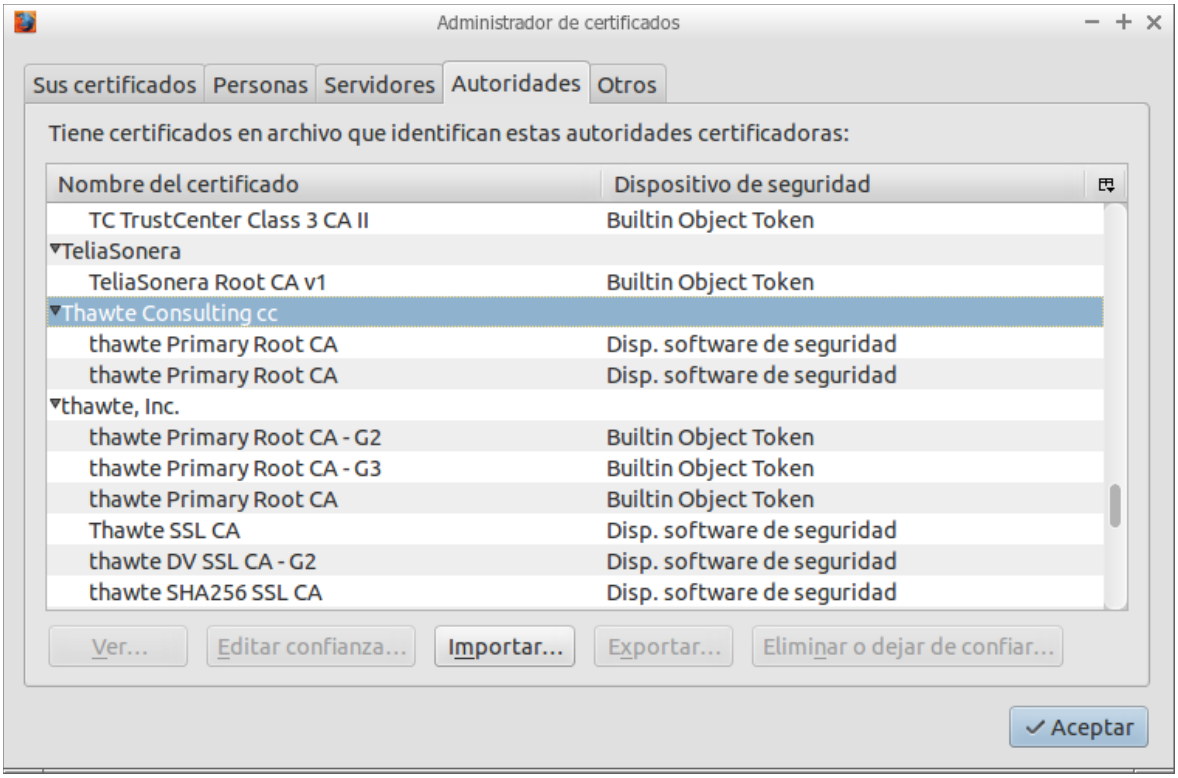
É de vital importancia para a entidade certificadora custodiar a clave privada da súa certificado raíz; xa que, se esta clave fose comprometida, poderíanse emitir certificados dixitais no seu nome, perdéndose a confianza na entidade. Nunha PKI, os procesos de xeración, custodia e uso desta clave son moi delicados, polo que hai protocolos a seguir que para garantir a súa protección e uso correcto, así como equipos específicos para custodiar e realizar operacións coa clave.

As extensións máis usadas para os certificados X.509 son:

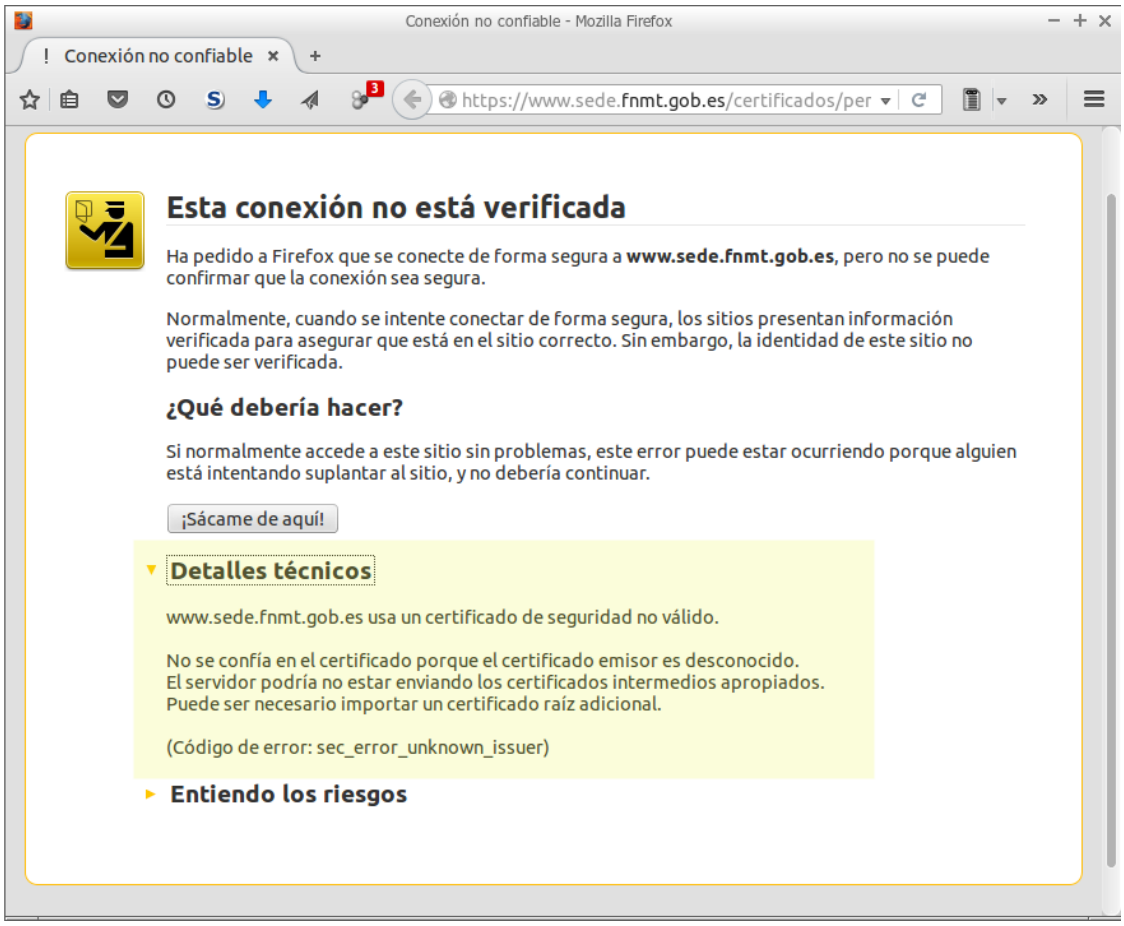
- .pem: certificado codificado en formato Base64 entre as liñas "-----BEGIN CERTIFICATE-----" e "-----END CERTIFICATE-----".
- .cer, .crt, .der: certificados en formato binario ou codificados Base64.
- .p7b, .p7c: asociado ao formato de arquivo PKCS#7.
- .p12: asociado ao formato de arquivo PKCS#12.

> PKCS#7 e PKCS#12 definen o formato de ficheiro para almacenar claves e certificados. Para saber máis sobre PKCS (Public-Key Cryptography Standards) pode visitarse a páxina https://es.wikipedia.org/wiki/PKCS

Normalmente os certificados raíz están incluídos nos navegadores web e no software de realización/verificación de firmas electrónicas, permitindo que este software realice as verificacións oportunas. A modo de exemplo pode verse na seguinte imaxe a ventá de xestión de certificados do navegador Firefox á que se chega a través de Preferencias → Avanzado → Ver certificados.

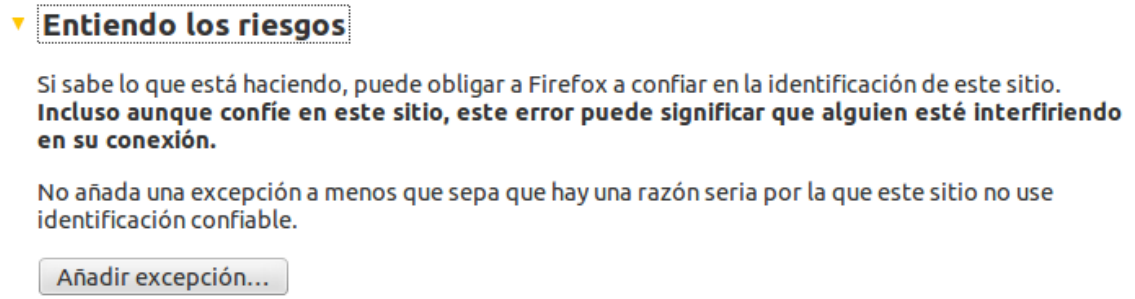


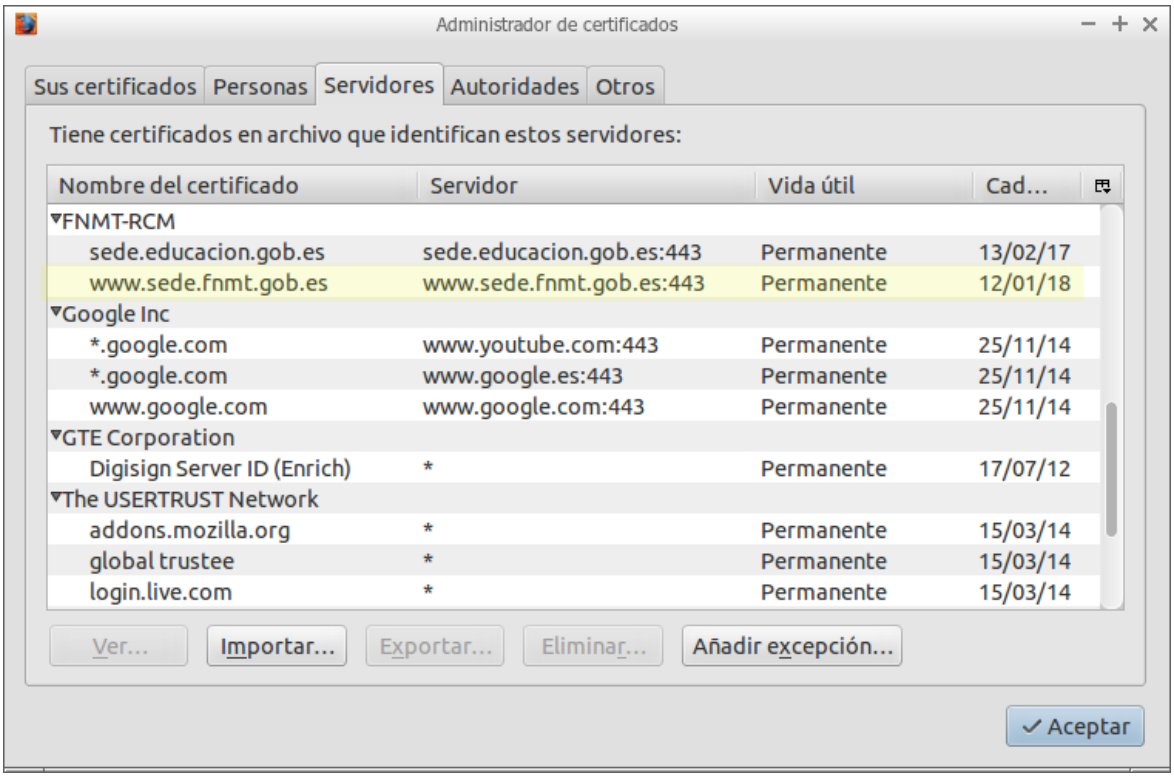
No caso de ter que verificar a validez dun certificado e non dispor do certificado raíz da entidade certificadora producirase un erro:



Para solucionar este tipo de erros pódese optar por unha das seguintes solucións:

– Aceptar como válido o certificado do máquina á que se está a conectar.

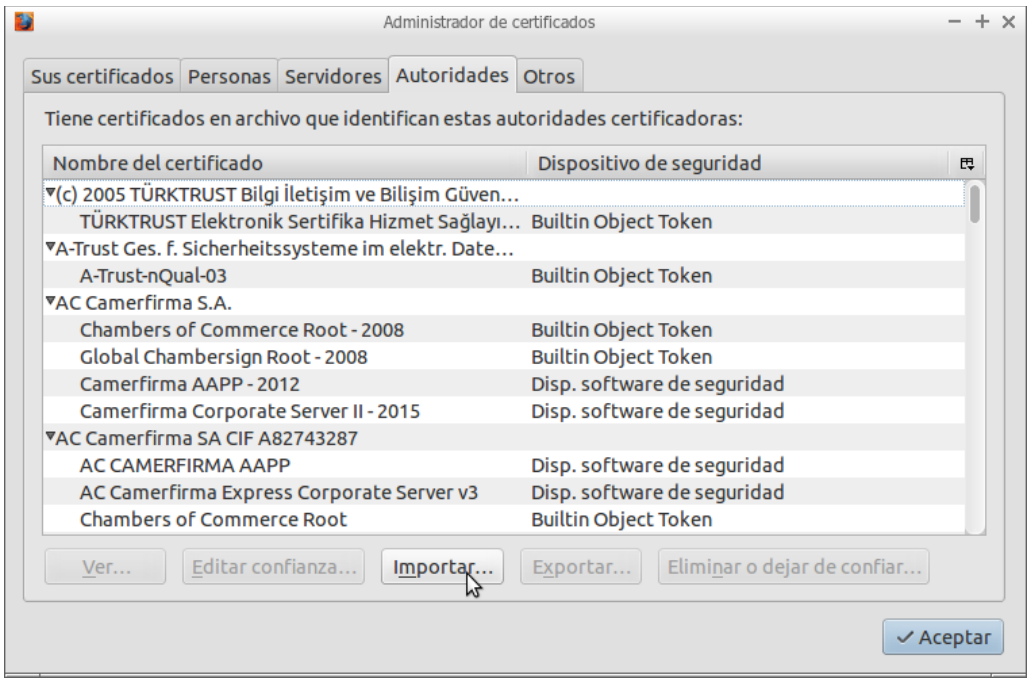




Esta solución ten o problema de que se está a aceptar un certificado sen facer a verificación da firma dixital usando o certificado raíz da entidade certificadora. Polo tanto, pódese estar aceptando un certificado falso emitido por un atacante que suplanta a identidade do equipo.

No caso de traballar con certificados autoxerados (non emitidos por entidades de certificación) esta sería a forma de aprobalos para que non apareza a mensaxe de advertencia cada vez que se conecte ao servidor en cuestión.

– A segunda solución consiste en instalar o certificado raíz da entidade de certificación emisora do certificado do servidor. Deste xeito, o navegador poderá verificar a validez do certificado do servidor. Ademais, isto permite verificar a validez de calquera certificado emitido pola entidade e elimínase o problema de suplantación de identidade descrito no punto anterior. Na pestana Autoridades do navegador Firefox pódense importar novos certificados raíz pulsando en Importar:



No seguinte artigo fálase do erro ssl sec_error_untrusted_issuer devolto polos navegadores: http://www.securitybydefault.com/2010/03/errores-ssl-en-navegadores-cuales-son-y.html

No seguinte artigo fálase do erro ssl sec_bad_cert_domain devolto polos navegadores: http://www.securitybydefault.com/2010/04/errores-ssl-en-navegadores-cuales-son-y.html

Ao longo da explicación anterior falouse de certificados emitidos a persoas e servidores. Os certificados dixitais poden clasificarse en función do seu titular:

- Certificados emitidos a persoas físicas:
  - Certificado persoal, que inclúe datos persoais do titular.
  - Certificado profesional, que inclúe datos persoais do titular e da empresa/organismo.
- Certificados emitidos a persoas xurídicas (empresas ou organismos).
- Certificados emitidos a equipos informáticos:
  - Certificados emitidos a servidores para cifrado de comunicacións ssl/tls.
  - Certificados emitidos a equipos para autorizar o seu acceso á rede.

2.3 Infraestructura de Clave Pública (PKI)

Á infraestrutura de hardware, software, persoal, políticas e procedementos necesarios para xestionar con garantías as operacións relacionadas coa vinculación de identidades e claves públicas denomínase Infraestructura de Clave Pública o PKI (Public Key Infraestructure).

Grazas á PKI, a firma dixital poderá garantir:

- Autenticación da identidade das partes.
- Confidencialidade da información transmitida entre as partes.
- Integridade da información, engadindo a capacidade de detectar se un documento ou información manipulouse dende o momento da súa sinatura.

- Vinculación ou non repudio, impedindo negar ás partes implicadas a súa participación e o contido dunha determinada transacción.

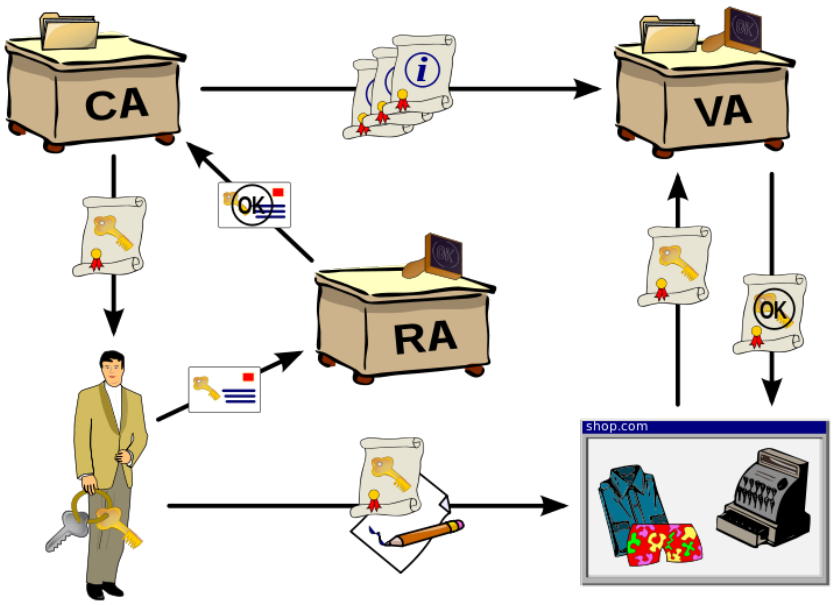
Nunha PKI atópanse os seguintes compoñentes:

- Autoridade de Certificación (Certification Authority – CA): encárgase de emitir os certificados.
- Autoridade de Rexistro (Registration Authority – RA): encárgase de verificar os datos dos solicitantes.
- Autoridade de Validación (Validation Authority – VA): encárgase da xestión dos certificados revocados (que perderon a súa validez).
- Autoridade de Selado de Tempo (Time Stamping Authority – TSA): garante a existencia e o contido dun documento nun instante de tempo determinado.

A entidade que emite os certificados ou Autoridade de Certificación recibe a petición dun usuario para que emita un novo certificado dixital que asegure que a clave pública perténcelle. Antes de emitir o certificado, hai que comprobar a identidade do solicitante. A comprobación pode realizala directamente a CA ou delegala na Autoridade de Rexistro (RA). Este labor de comprobación é de vital importancia; xa que, del depende a exactitude dos datos contidos nos certificados dixitais. A confianza que xera unha CA vai depender en gran medida deste labor de comprobación.

> Nos seguintes artigos do blog de seguridade informática Securitybydefault trátase a problemática dos certificados dixitais emitidos por entidades que non realizan moitas verificacións fronte aos certificados con validación extendida: Fraude online con firma dixital e ssl e certificados dixitais con validación extendida.

Xa confirmada a identidade, procédese a emitir un certificado dixital cos datos de identificación do usuario e a súa clave pública. Este certificado asínase coa clave privada da CA de xeito que calquera poderá comprobar que a validez do certificado usando a clave pública da CA distribuída a través do certificado raíz da entidade.



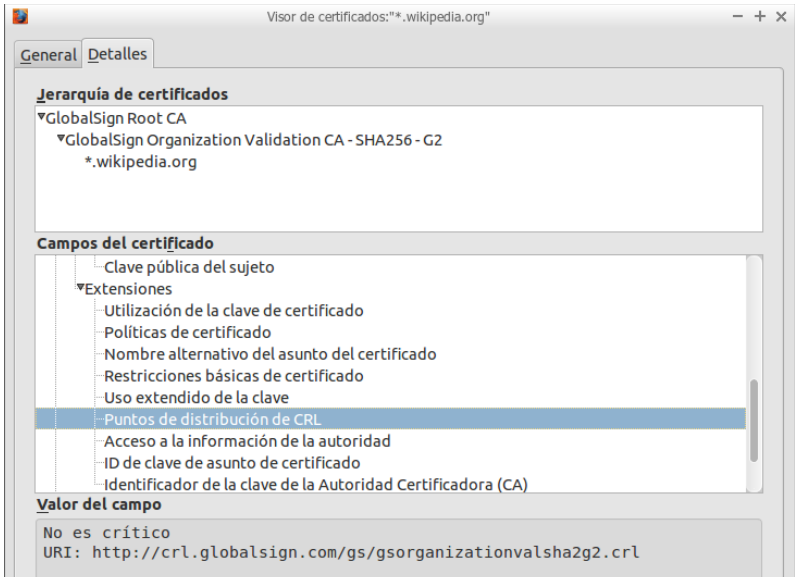
Principios dunha PKI. Wikipedia. Licenza CC BY-SA 3.0

Para xerar os certificados envíaselle á CA unha petición CSR (Certificate Signing Request) en formato PKCS#10, que contén a información do usuario e a súa clave pública. Unha vez verificada a información e o cumprimento dos requisitos (pago, firma de contratos) envíase o certificado ao usuario ou ben se lle proporciona unha ligazón de descarga.

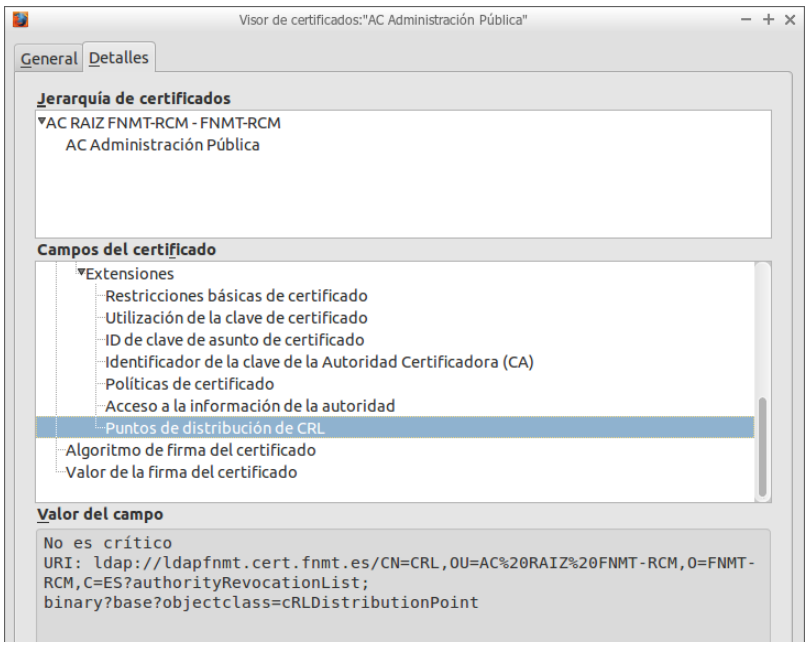
Un usuario terá as súas claves privada-pública, ben por que as xera el mesmo (p.e. xéraas o navegador do usuario) ou ben porque as xera a propia CA e llas entrega (p.e. DNIe).

Todos os certificados X.509v3 teñen unha validez temporal expresada cun par de datas (Validez: Non antes de e Non despois de). Pola contra, pode ocorrer que un certificado sexa revocado (por exemplo, a clave privada do usuario foi comprometida, un traballador para o que foi emitido o certificado xa non ocupa o posto, etc.). A CA deberá facer as comprobacións necesarias e tomar a decisión de revocar ou non un certificado.

No caso de ser revocado, o certificado incluirase nunha lista CRL (Certificate Revocation List) que contén os números de serie dos certificados revocados, data, hora e causa da revocación. Periodicamente, a CA asinará coa súa clave privada a lista CRL para garantir a súa integridade e procederá a facela pública nun servidor web, ldap ou a través do OCSP (Online Certificate Status Protocol). Desta forma, grazas ao atributo CDP (CRL Distribution Point) do certificado as aplicacións coñecen a ubicación do ficheiro CRL e poden verificar a validez ou a revocación do certificado.



Exemplo de distribución da lista CRL a través dun servidor web.



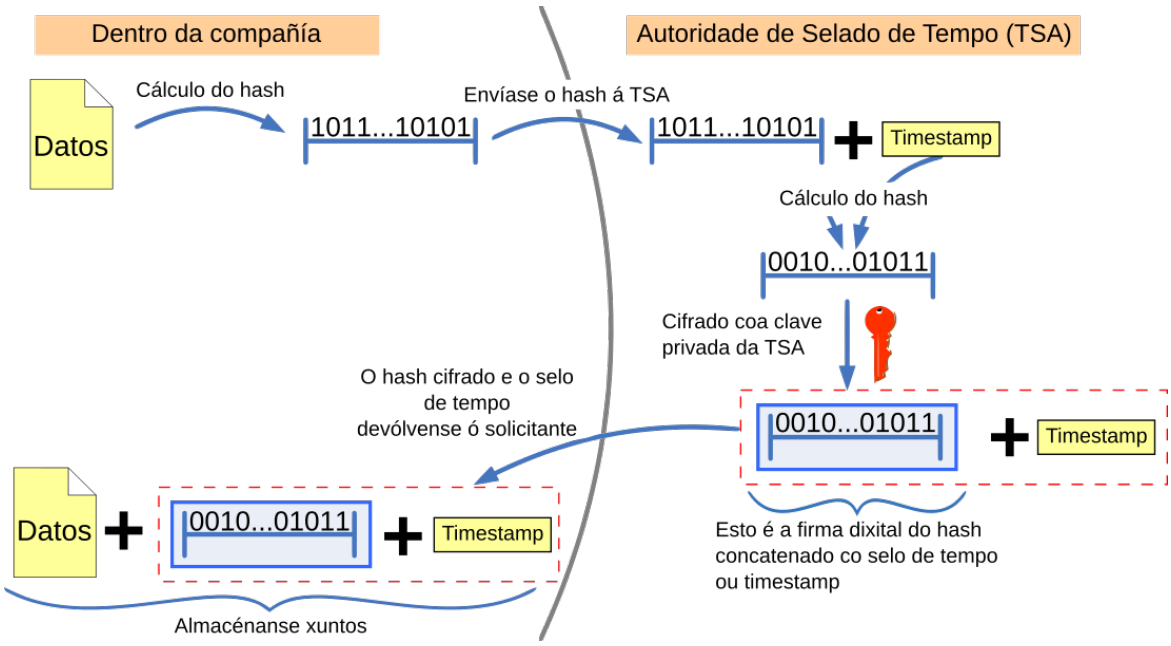
Exemplo de distribución da lista CRL a través dun servidor LDAP.

No caso de que unha entidade xestione unha grande cantidade de certificados (p.e. a FNMT xestiona millóns deles), a lista CRL alcanzará un tamaño considerable, facendo que o proceso de descarga e verificación da revocación por parte das aplicacións sexa lenta. Para estes casos pódese:

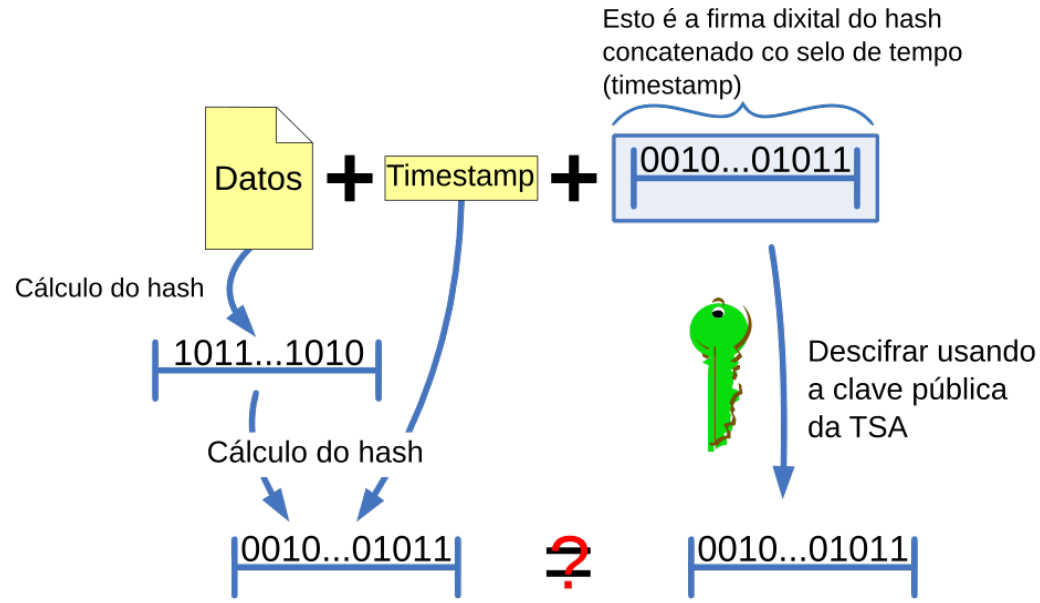
- Usar CRL particionadas, onde a CRL é dividida en sublistas dun tamaño limitado.
- Traballar con listas de actualizacións (Delta CRL) que recollen os últimos cambios. Para verificar o estado dun certificado habería que descargarse a lista orixinal e as actualizacións.
- Usar o protocolo OSCP, que viaxa sobre paquetes http, para interrogar á CA sobre o estado dun certificado. Esta responde indicándolle se está revocado ou non.

A CA pode delegar noutras entidades chamadas Autoridades de Validación (VA) a publicación desta información.

A Autoridade de Selado de Tempo (TSA) actúa como un terceiro de confianza para probar a existencia dun documento antes de certa data e que os seu contido non foi modificado dende entón. Grazas ao selado de tempo é posible controlar cando foi emitida unha factura, cando foi presentada unha solicitude ou unha reclamación. Nas seguintes imaxes pode verse como unha TSA aplica un selo temporal (timestamp) e como se pode verificar:



Proceso de obtención dun selo de tempo. Imaxe modificada por Manuel González Regal a partir do traballo de Bart Van den Bosch. Licenza CC BY-SA 2.0 BE.



Proceso de verificación dun selo de tempo. Imaxe modificada por Manuel González Regal a partir de Checking timestamp.svg. Wikipedia. Licenza CC BY-SA 3.0.

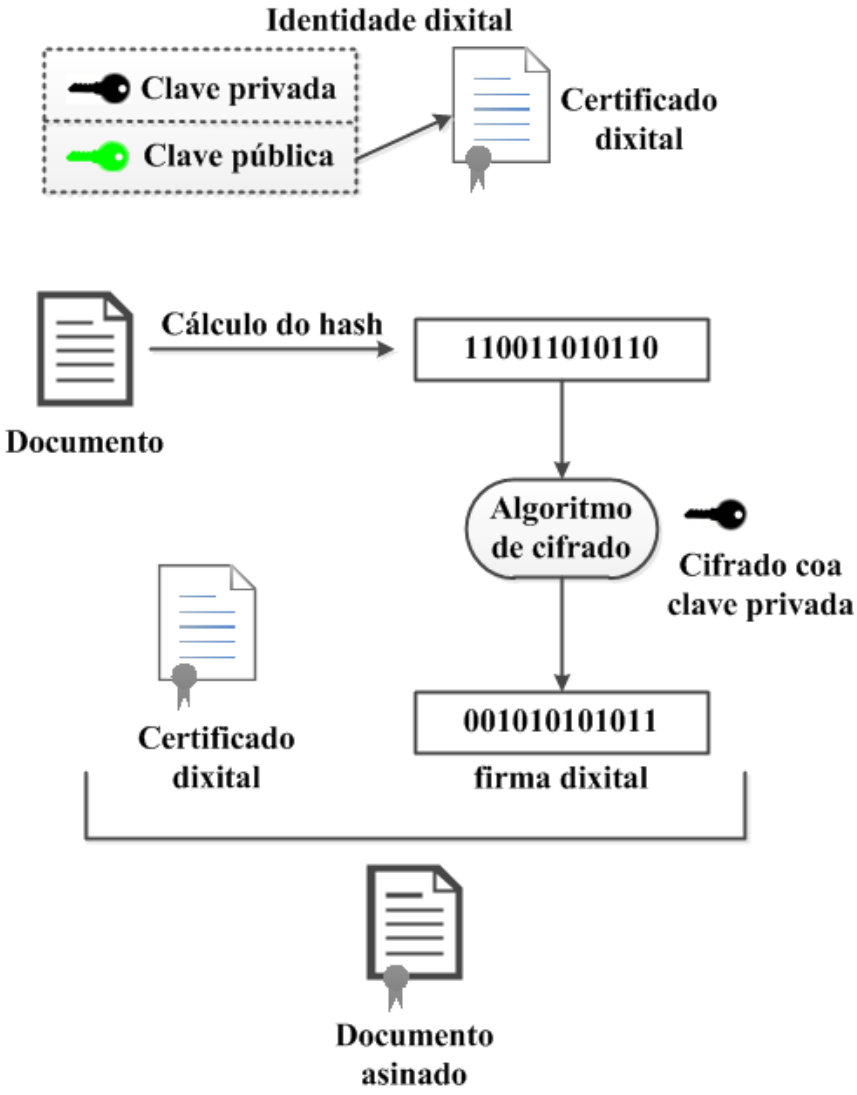
O selado de tempo proporciona un engadido na firma dixital; xa que, esta por si soa non proporciona información sobre o momento de creación da firma.

2.4 Sinatura electrónica

Para firmar dixitalmente un documento hai que ter unha identidade dixital (clave privada e pública) vinculada á nosa identidade por un terceiro de confianza. É dicir, precísase un certificado dixital e a clave privada asociada.

O proceso para firmar dixitalmente un documento segue os seguintes pasos:

- En primeiro lugar, calcúlase o resumo hash do documento.
- En segundo lugar, o hash calculado é cifrado usando a clave privada do asinante. Este resultado é a firma dixital 'en bruto'.
- En terceiro lugar, para permitir e facilitar as tarefas de verificación da firma, gárdase de forma anexa ao documento asinado a firma dixital 'en bruto' e información adicional (certificado do asinante, instante de realización da firma, vixencia do certificados, etc.). A firma dixital 'en bruto' e todos eses metadatos forman o que se coñece como firma dixital. Na seguinte imaxe pódese ver un resumo do proceso de firma dixital dun documento:



En función, de como se garda esa información adicional, fálase de:

- Firma disociada: gárdase de forma independente noutro ficheiro, sendo responsabilidade do usuario manter xuntos o documento e o ficheiro coa firma.
- Firma embebida: gárdase ao comezo ou ao remate do documento. Este formato facilita que o documento e a firma estean unidos, pero pode alterar a estrutura propia do ficheiro. Algúns formato, como o pdf, xa contemplan a posibilidade de incluír dentro do propio documento a firma dixital.

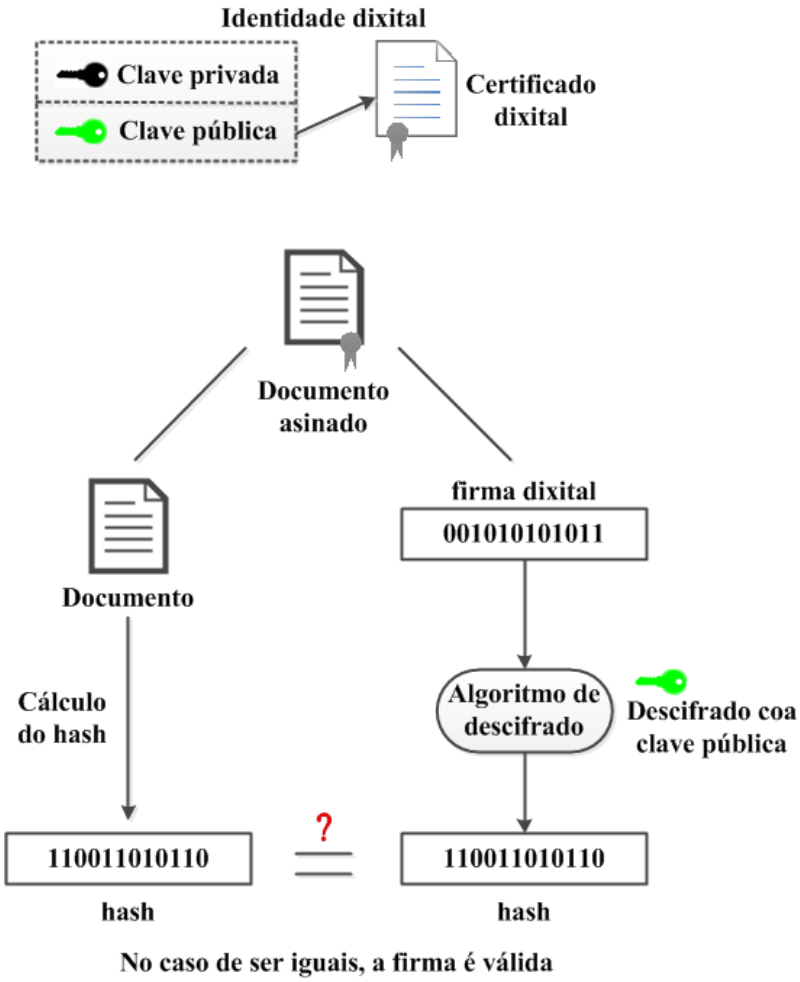
Existen diversos formatos para a firma dixital, entre os que destacan: S/MIME, PDF Signature, CAdES, XAdES, PAdES, ODF, …

> Para saber máis sobre formatos de firma pódese visitar o sitio web http://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html

Para comprobar unha firma dixital os pasos a seguir son:

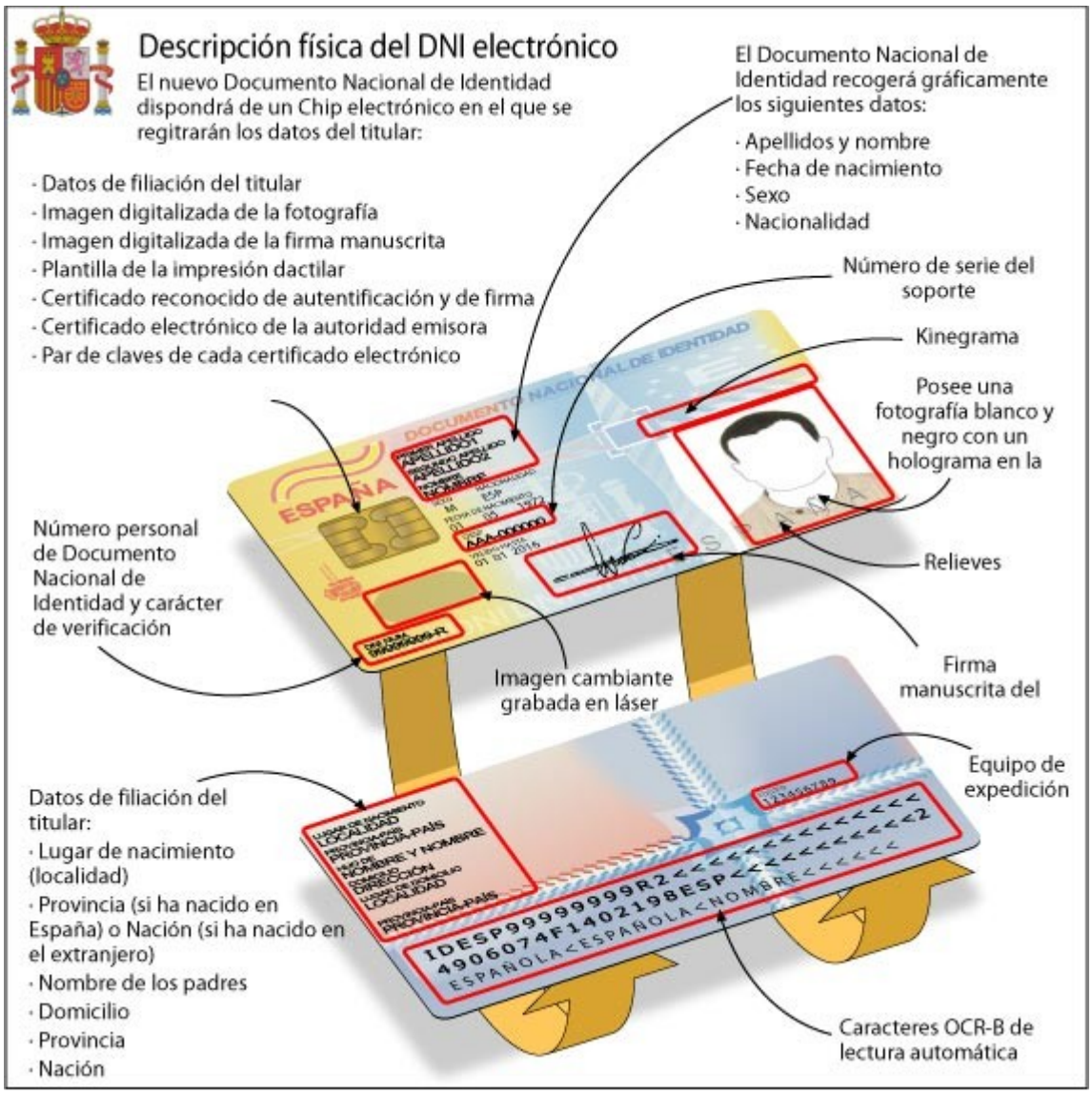
- En primeiro lugar, calcúlase o hash dos datos (o que correspondería co documento orixinal).
- En segundo lugar, emprégase a clave pública do asinante para descifrar a firma (o hash do documento orixinal cifrado coa clave privada).
- En terceiro lugar, se ao comparar os dous hashes coinciden, o documento recibido correspóndese co orixinal.

Na seguinte imaxe pódese ver un resumo do proceso de comprobación da firma dixital dun documento:

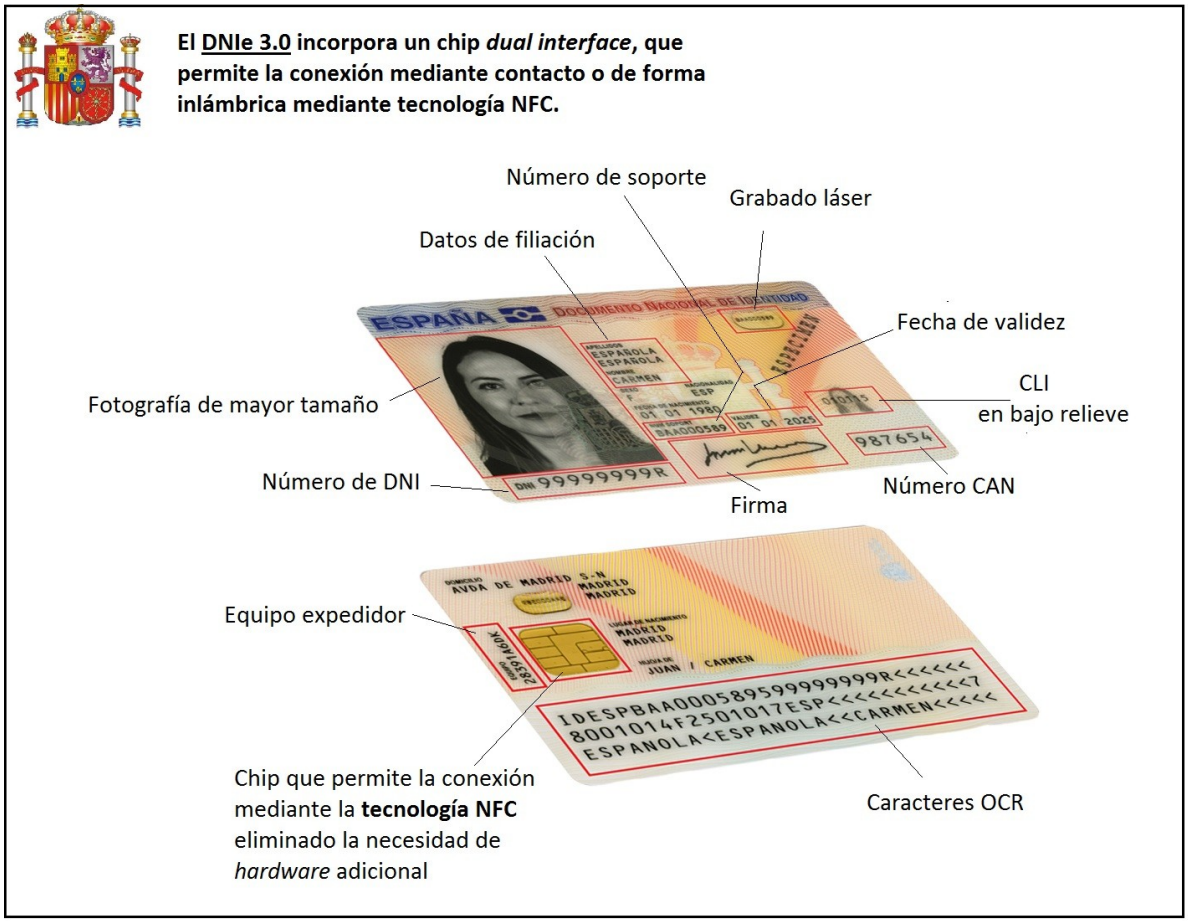


DNI Electrónico

O DNI electrónico é un Documento Nacional de Identidade coa mesma función que o DNI tradicional; é dicir, acreditar fisicamente a identidade do titular.



DNI electrónico. Ministerio do Interior. Dirección Xeral da Policía. http://www.dnielectronico.es



DNI electrónico 3.0. Ministerio do Interior. Dirección Xeral da Policía. http://www.dnielectronico.es

Pero ademais, o DNI electrónico leva un chip criptográfico que lle permite:

- Acreditar electrónicamente e de forma inequívoca a identidade do titular.
- Firmar dixitalmente documentos, dándolles validez xurídica equivalente á proporcionada pola firma manuscrita.

Estas novas funcionalidades do DNI electrónico permiten que os usuarios poidan, entre outras cousas:

- Realizar trámites coas Administracións Públicas a través de Internet de forma segura e a calquera hora e día da semana (consulta informe de vida laboral, consulta puntos do permiso de conducir, declaración do IRPF, solicitude de becas, etc.).
- Asinar electronicamente documentos.
- Identificarse, eliminándose a necesidade de usar contrasinais.
- Enviar correos electrónicos certificados.

O chip criptográfico almacena a seguinte información:

- Un certificado electrónico para autenticación do cidadán.
- Un certificado electrónico para firma electrónica recoñecida.
- Claves públicas e privadas de autenticación e firma electrónica.
- Certificado da Autoridade de Certificación emisora.
- Plantilla biométrica da impresión dactilar.

- Fotografía dixitalizada do cidadán.
- Imaxe dixitalizada da firma manuscrita.
- Datos da filiación do cidadán, correspondentes co contido personalizado na tarxeta.

O chip encárgase de realizar calquera operación criptográfica que precise o uso das claves privadas, non permitindo que as claves privadas abandonen en ningún momento o interior do chip. Polo tanto, o chip actúa por unha banda como almacén seguro de claves e por outra como procesador de operacións criptográficas. Para a realización de operacións criptográficas é preciso proporcionar o PIN de usuario para verificar que realmente se é o dono lexítimo do DNI.

Os certificados electrónicos do DNI Electrónico teñen unha validez de 30 meses dende a súa emisión. É posible renovar os certificados sen necesidade de renovar o DNI usando os PAD (Puntos de Actualización do DNIe) nas comisarías de policía.

> Para saber máis das características e funcionalidades do DNI electrónico pódese visitar o sitio web http://www.dnielectronico.es