

# A sinatura dixital

## ¿Qué é a sinatura dixital?

**A sinatura dixital é como a nosa sinatura manuscrita.** Sirve para asinar os nosos documentos, mensaxes...

### Índice

- 1 ¿Qué é a sinatura dixital?
- 2 ¿Qué preciso para asinar un documento dixitalmente?
- 3 ¿Cómo funciona?

- Permite acreditar a nosa **Identidade**. Unha sinatura válida implica que se nos pode atribuír de forma indubidable ese documento electrónico como autores de esa sinatura.
- Implica que non podemos negar en ningún caso que o documento foi asinado por nós. **Non podemos repudialo**.
- A sinatura dun documento permítenos confirmar a súa **Integridade**. Se sufrise algunha modificación dende o momento da súa sinatura ata que se consulta de novo ou outra persoa o recibe, a sinatura xa non será válida.

---

*Para poder acreditar a nosa Identidade precisaremos dun "Identificador" que está contido no noso certificado dixital*

---

## ¿Que preciso para asinar un documento de forma dixital?

- O igual que coa nosa sinatura manuscrita precisarei dun elemento de escritura para asinar (bolígrafo, pluma...) Neste caso precisamos un **programa** para facer e verificar a sinatura dixital.
- Precisarei dun **certificado dixital**: Para asinar terei que acreditarme. Mediante o certificado establezo a miña *identidade*.

O certificado dixital á súa vez é un documento dixital asinado electrónicamente por una autoridade de confianza que establece que "eu son quen digo ser" o que me permite identificarme na comunidade electrónica.

---

*A sinatura non é un elemento que copiamos e peguemos.*

*Teremos que asinar cada documento*

---

## ¿Como funciona?

1º Asinamos o documento co noso programa de sinatura:

- Seleccionaremos o documento que queremos asinar
- Solicitáranos o certificado dixital para identificarnos
- O *programa* creará unha sinatura (un conxunto de datos en forma electrónica) para engadir ao documento ou mensaxe...

2º Verifícase a sinatura: Neste proceso comprobarase que o contido non foi modificado e que foi asinado por quen di.

- Cando envío un documento asinado, a persoa que o recibe comprobará co seu *programa de sinatura e verificación* que ese documento foi asinado por min.

**Para saber máis....**



# Para saber máis...

## A sinatura dixital

# Características da sinatura dixital

*A sinatura dixital é no mundo electrónico o mesmo que a nosa sinatura manuscrita*

A sinatura, é unha secuencia de datos, resultado de aplicar un conxunto de algoritmos matemáticos ao devandito documento. Estes algoritmos permiten ofrecer garantías de seguridade sobre o documento obxecto de sinatura. Permítennos acreditar:

- A **Identidade** da persoa autora da sinatura. Implica poder atribuír de forma indubidable o documento electrónico recibido a unha determinada persoa como autora da sinatura.
- A **Integridade** do documento. Implica a certeza de que o documento é exactamente o mesmo documento que se asinou, sen que sufrira alteración ningunha dende o momento da sinatura.
- A **non repudiación** ou non rexeitamento en orixe. Implica que o asinante do documento non poida negar en ningún caso que o documento foi asinado por el.

## ¿En que se basea a sinatura dixital?

A sinatura dixital baséase na utilización combinada de dúas técnicas distintas:

- A criptografía asimétrica ou de clave pública para cifrar mensaxes
- O uso das chamadas funcións hash ou funcións resumo.

**O resumo cifrado é a sinatura dixital.**

### As funcións Hash.

Xunto á criptografía asimétrica utilízanse na sinatura dixital as chamadas funcións hash ou funcións resumo. As mensaxes que se intercambian poden ter un gran tamaño, por iso non se cifra a mensaxe enteira senón un resumo do mesmo obtido aplicando á mensaxe unha función hash.

Con independencia do tamaño que teña a mensaxe, mediante a función hash convértese nunha mensaxe cunha dimensión fixa (xeralmente de 160 bits). Para iso, a mensaxe orixinaria divídese en partes cada unha das cales terá ese tamaño de 160 bits, e unha vez dividido combínanse elementos tomados de cada unha das partes resultantes da división para formar o mensaxe-resumo ou hash, que tamén terá unha dimensión fixa e constante de 160 bits. Este resumo de dimensión fixa é o que se cifrará utilizando a clave privada do emisor da mensaxe.

Como ferramenta de seguridade, a sinatura baséase en técnicas criptográficas. A criptografía, segundo a RAE, é "a arte de escribir con clave secreta ou de forma enigmática". Funcionalmente, a criptografía é un conxunto de técnicas que, mediante a utilización de algoritmos e métodos matemáticos, serven para cifrar e descifrar documentos.

Tradicionalmente falouse de **dous tipos** de sistemas criptográficos:

- 1.– Os simétricos ou de clave privada.
- 2.– Os asimétricos ou de clave pública.

1) Os chamados sistemas *criptográficos simétricos* son aqueles nos que dúas persoas (A e B), que se van intercambiar mensaxes entre si, utilizan ambos os dous a mesma clave para cifrar e descifrar a mensaxe. Así, o emisor da mensaxe (A), cifrao utilizando unha determinada clave, e unha vez cifrado, envía a B. Recibido a mensaxe, B descifrao utilizando a mesma clave que usou A para cifralo. Destacan entre os sistemas criptográficos simétricos os coñecidos cos nomes de DEAS, TDES e AES.

Os principais **inconvenientes** do sistema simétrico son os seguintes:

- A necesidade de que A (emisor) e B (receptor) intercámbiense previamente por un medio seguro a clave que ambos os dous van utilizar para cifrar e descifrar as mensaxes.
- A necesidade de que exista unha clave para cada par de persoas que se vaian intercambiar mensaxes cifradas entre si.

Estas dificultades apuntadas determinan que os sistemas de cifrado simétricos *non sexan axeitados para ser utilizados en redes abertas como Internet*, onde intercambiarse previamente claves de cifrado non é seguro nin operativo.

2) Os sistemas *criptográficos asimétricos* ou de clave pública son aqueles en que cada unha das dúas persoas (A e B), que se van intercambiar mensaxes entre si, dispoñen dun par de *claves diferentes* (privada e pública) que teñen as seguintes características:

- Unha das claves, a privada, que é secreta debe ser custodiada polo seu propietario. Esta é a que se vai utilizar para asinar mensaxes.
- A segunda clave, a pública, é ou pode ser coñecida por calquera e pode utilizarse para cifrar a mensaxe de modo que só poida ser lido polo propietario de dita clave –xa que só el poderá descifrar a mensaxe usando a súa clave privada–.
- As mensaxes asinadas cunha clave privada só poden validarse empregando a clave pública de quen enviou a mensaxe.

A utilización do par de claves (privada e pública) implica que:

*Para enviar unha mensaxe confidencial (cifrada):*

- A (emisor) cifra unha mensaxe utilizando para iso a clave pública de B (receptor) e, unha vez cifrado, envía a B.
- B é o único que pode descifrar a mensaxe recibida utilizando a súa clave privada.

*Para enviar unha mensaxe asinada:*

- A (emisor) asina unha mensaxe utilizando para iso a súa clave privada e, unha vez asinado, envía a B (receptor).

- B valida a sinatura recibida utilizando a clave pública de A.

Se a mensaxe é validada significa necesariamente que esa mensaxe foi asinada coa clave privada de A (é dicir, que provén de A) e que non sufriu ningunha alteración durante a transmisión de A cara a B, porque se fose alterado por un terceiro, a mensaxe non sería validada coa clave pública de A.

Deste xeito, cúmprense dúas das características apuntadas: a integridade (certeza de que a mensaxe non foi alterada) e non repudiación en orixe (imposibilidade de que A negue que a mensaxe recibida por B foi cifrada por A coa clave privada deste). A terceira característica (identidade do emisor da mensaxe) obtense mediante a utilización dos certificados dixitais.

## O proceso de sinatura dixital

- 1º Asínanse os documentos. Lévese a cabo por medio da clave privada, engadindo a sinatura á mensaxe enviada.
- 2º Verifícase a sinatura: Utilízase a clave pública. Neste proceso compróbase que o contido non foi modificado.

### 1º) O proceso de Sinatura

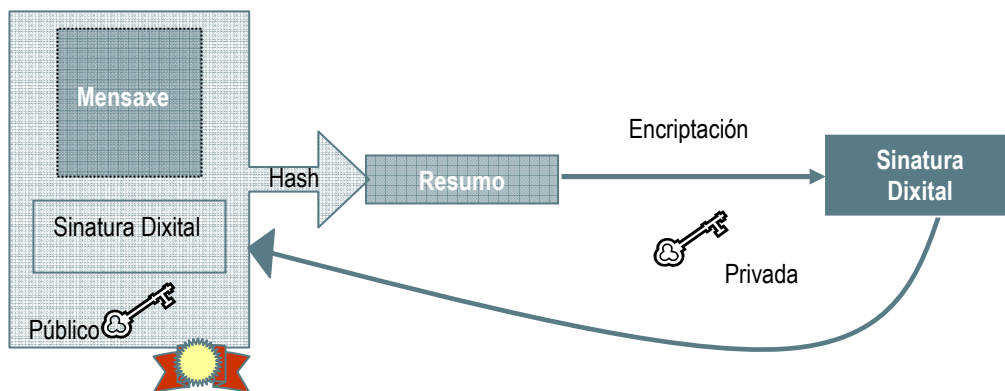


Figura 1. O proceso de sinatura

- En lugar de cifrar toda a mensaxe faise sobre un "resumo" da información (hash).
- O resumo cifrase por medio da clave privada.
- Os datos cifrados resultantes engádense á mensaxe orixinal (sinatura)
- Finalmente, engádese a clave pública do remitente, para que o destinatario poida comprobar a sinatura.
- Envíase ao destinatario o paquete composto pola mensaxe orixinal, a sinatura e a clave pública.

## 2º) Verificación de sinatura

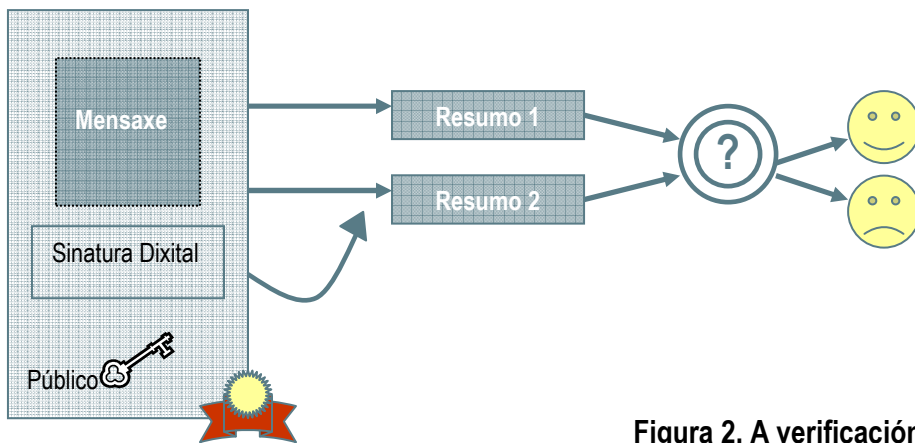


Figura 2. A verificación da sinatura

Si a persoa que recibe a mensaxe ten a miña clave pública poderá comprobar co seu *programa de sinatura e verificación* que ese documento foi asinado por min.

O que fará o seu programa ó verificar a sinatura será:

- Descifrar o resumo mediante a clave pública
- Volver a resumir a mensaxe orixinal
- Comparar o resumo obtido co resumo recibido

Se ambos son iguais, a sinatura é válida e asegura que se recibiu a mesma mensaxe que se enviou e que o noso mensaxe non foi modificado.

## Certificados dixitais e Autoridades de Certificación

Un certificado dixital é un documento asinado electrónicamente. Inclúe, entre outros elementos, unha clave pública e unha privada que están emparelladas. Grazas a unha autoridade de confianza que así o acredite, poderemos confiar en que se corresponden coa identidade dunha persoa física ou xurídica determinada.

O certificado, é fundamental no proceso de sinatura. O uso do certificado dixital permítenos identificar o emisor das mensaxe a través da clave pública contida no seu certificado. Neste sentido sen o certificado, non poderíamos garantir a autenticación de orixe e o non repudio.

A **Autoridade de Certificación (CA)** é a axencia responsable de emitir os certificados e debe ser unha entidade en quen as partes involucradas confían. Para iso, o contido dun certificado inclúe a *sinatura dixital da Autoridade de Certificación*.

O **contido** dun certificado é variado, pero como norma xeral contén:

- A clave pública e o nome do propietario; pode tamén incluír a clave privada
- A data de expedición
- Período de validez do certificado
- Un número de seriado
- A identificación da Autoridade de Certificación.

O **formato** dos certificados está definido polo estándar internacional ITU-T X.509 que especifica como xestionar os contidos dun certificado, creando o que se denomina unha Infraestrutura de Clave Pública (PKI, Public Key Infrastructure). A estrutura dos certificados X.509v3 está detallada na RFC2459.

## Referencias e recursos

### CERES, Criptografía básica:

- [http://www.cert.fnmt.es/popup\\_frame.php?p=42&l=es](http://www.cert.fnmt.es/popup_frame.php?p=42&l=es)

### Consellería de Facenda:

- Información sobre certificados de Usuario dá FNMT:  
<http://www.conselleriadefacenda.es/web/portal/oficina-virtual-obtencion-certificados>
- Procedemento resumido para obter un certificado de Usuario  
[http://host.cixtec.es/EntradaOficinaVirtual/OV/ga/OV\\_obtencion.htm](http://host.cixtec.es/EntradaOficinaVirtual/OV/ga/OV_obtencion.htm)