# Certificados digitales

# CONFIANZA

**Uno de los principales desafíos a que se enfrentan los medios telemáticos es asegurar la identidad de las partes que intervienen en cualquier operación, tanto del usuario que accede a un servicio como la organización que lo presta.**

"El acceso a la información y los servicios de un usuario final necesita más que nunca de un grado de fiabilidad y confianza en el medio. Para ello, cualquier operación que se realice a través de medios electrónicos requiere "asegurar la integridad del contenido y autenticar al remitente y al receptor."

# ASEGURAR LA IDENTIDAD

## SERVICIOS WEB

**En el acceso a cualquier página web, la identidad de los actores es conocida pero debe demostrarse:**

**Autentica al organismo**

En primer lugar, la institución debe aportar pruebas de que es realmente el titular de la página web.

**Autentica al ciudadano**

La persona que solicita acceso deberá demostrar que tiene derecho a tal acceso.

# ASEGURAR LA IDENTIDAD

## ES NECESARIO GARANTIZAR LA CONFIANZA DE LAS PARTES

En la identidad de entidades y usuarios
**AUTENTICACIÓN**

En la privacidad de la información
**CONFIDENCIALIDAD**

En que los datos no sean modificados
**INTEGRIDAD**

En que las partes no se desdigan
**NO REPUDIO**

# SOLUCIÓN TECNOLÓGICA

La solución adoptada para garantizar la seguridad en el uso de medios electrónicos está basada en la **criptografía** (del griego kryptos, «ocultar», y grafos, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

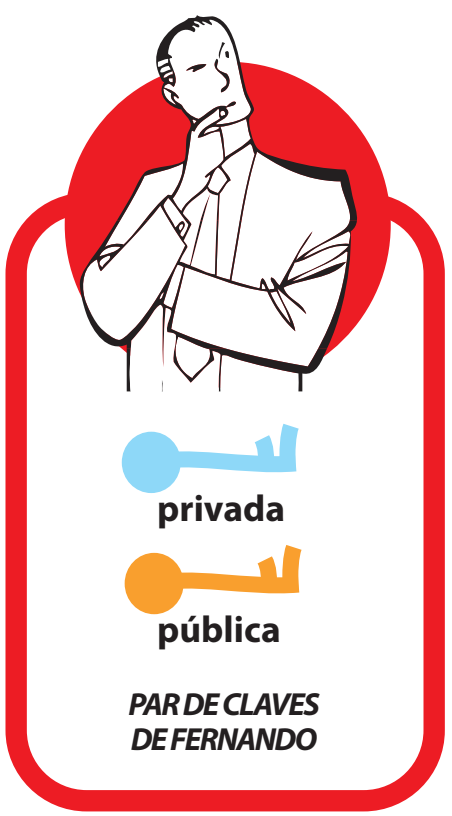
Los Certificados Digitales están basados en la utilización de técnicas de criptografía **ASIMÉTRICA**, en la que existe una **CLAVE PÚBLICA** a disposición de todo el mundo y que sirve para identificar al titular del certificado y una **CLAVE PRIVADA** que solamente conoce en titular del certificado y le sirve para **FIRMAR ELECTRÓNICAMENTE**.

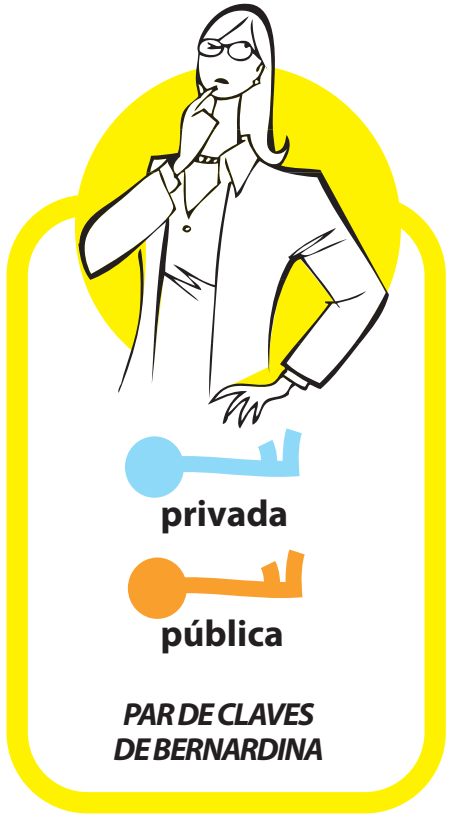
# CRIPTOGRAFÍA ASIMÉTRICA

## Cifrado asimétrico

**El cifrado asimétrico o de llave pública se basa en el concepto de un par de llaves (claves)**. Cada mitad del par (una llave) puede cifrar información que sólo la otra parte (la otra llave) podrá descifrar. Una parte del par de llaves, la llave privada, sólo es conocida para el propietario designado; la otra parte, la llave pública, se publica abiertamente, pero continúa asociada al propietario.

**El cifrado asimétrico garantiza la confidencialidad, autenticidad y el no repudio.**

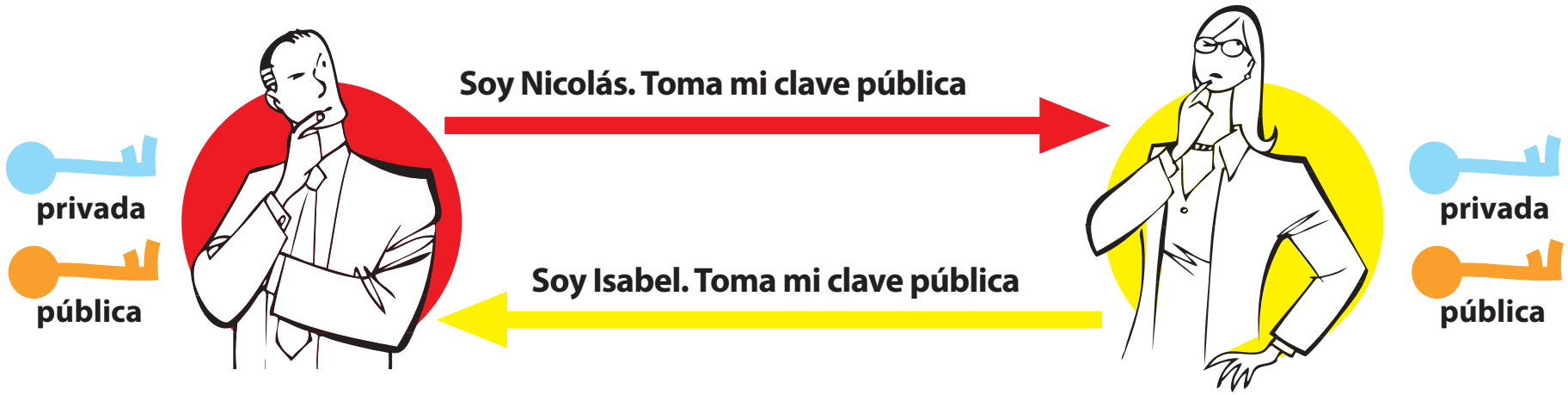


# CRIPTOGRAFÍA ASIMÉTRICA

## PROCESO DE CIFRADO

### Compartir clave públicas



# CRIPTOGRAFÍA ASIMÉTRICA

**Mediante el uso de CERTIFICADOS DIGITALES se pueden llevar a cabo las siguientes operaciones:**

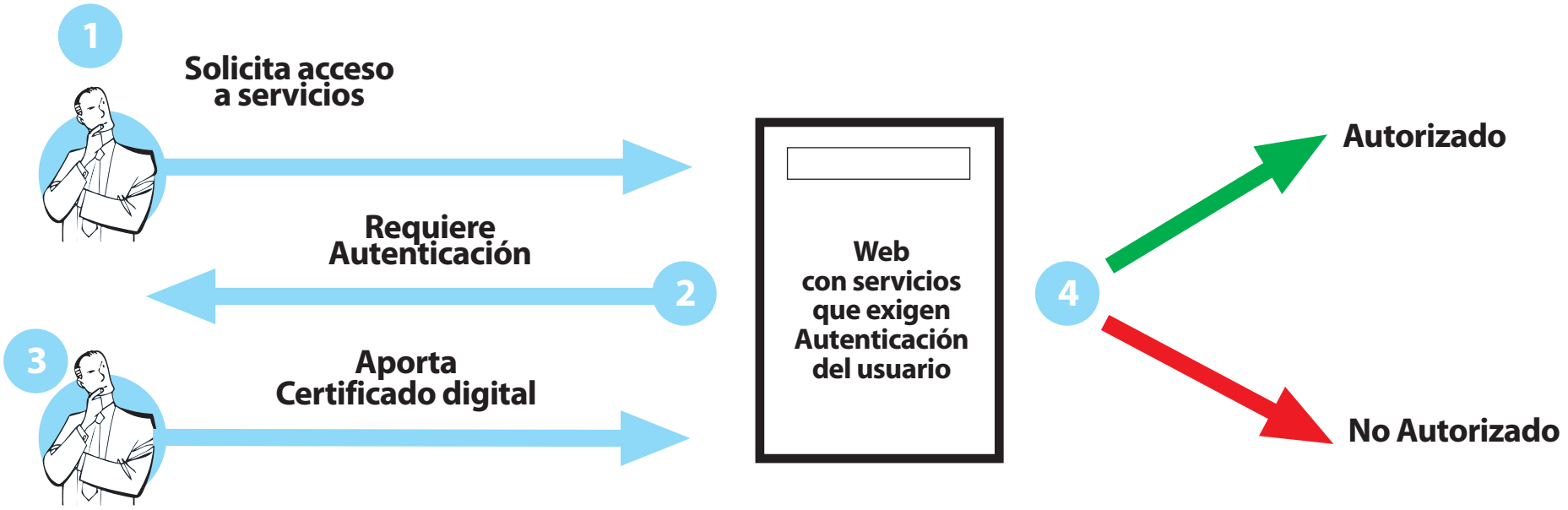
**AUTENTICACIÓN**, para acceder a servicios que están restringidos y que solicitan validar la identidad del usuario que accede a ellos (Ministerios, Comunidades Autónomas, Ayuntamientos, Entidades Bancarias, …).

**CIFRADO DE INFORMACIÓN**, tales como correos electrónicos, archivos almacenados en nuestro ordenador, …

**FIRMA ELECTRÓNICA**, de documentos requeridos para presentar solicitudes ante la Administración, transacciones bancarias,...

# CRIPTOGRAFÍA ASIMÉTRICA

## PROCESO DE AUTENTICACIÓN

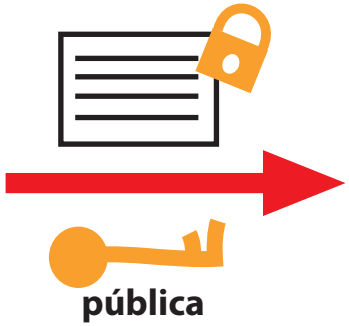


# CRIPTOGRAFÍA ASIMÉTRICA

## PROCESO DE CIFRADO

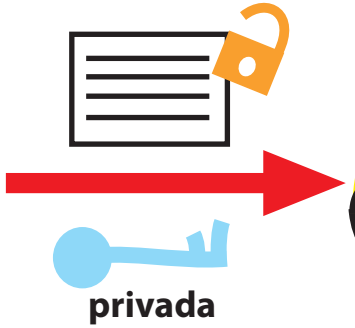
**CIFRADO**

**Cifrado del mensaje con la clave pública de Isabel**




**Envío del mensaje cifrado**

**Descifrado del mensaje con la clave privada de Isabel**




# CRIPTOGRAFÍA ASIMÉTRICA

## PROCESO DE FIRMA ELECTRÓNICA

**La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.**

**Información original en Icaro**

**Firma**

**0A 3F 15 12 D4**

**Información original en Icaro**

**Firma**

**0A 3F 15 12 D4** **=**

**Idéntico Documento**

**Distinto Documento**

**Tutorial : Certificados digitales**

efactura
portal de la factura electrónica

# ORDENAMIENTO JURÍDICO

Para que los recursos tecnológicos encargados de mostrar y demostrar la identidad de personas y organizaciones tengan validez legal, ha sido preciso un importante esfuerzo en el ordenamiento jurídico español, cabe destacar el **Real Decreto-Ley 14/1999, de 17 de septiembre**, que otorga los mismos efectos jurídicos a la Firma Electrónica que a la manuscrita.

Así mismo, el 19 de diciembre de 2003 se publicó la **Ley 59/2003**, de firma electrónica que, entre otros conceptos, define certificado electrónico, firma electrónica, certificado reconocido y Documento Nacional de Identidad electrónico.

**La validación legal de la firma electrónica elimina las barreras legales y potencia el desarrollo de negocios a través de Internet.**

# ORDENAMIENTO JURÍDICO

La Ley 59/2003, de 19 de diciembre, de firma electrónica recoge en su artículo 1 el Objeto de la Ley:

1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

2. Las disposiciones contenidas en esta ley no alteran las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos

# CERTIFICADOS DIGITALES

A continuación se relacionarán los conceptos recogidos en la Legislación Vigente en materia de Firma Electrónica.

**FIRMA ELECTRÓNICA**

**CERTIFICADO DIGITAL**

**AUTORIDAD DE CERTIFICACIÓN**

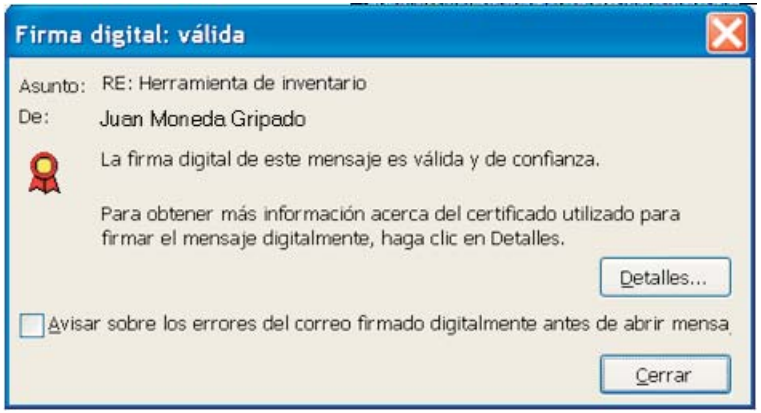
**DNI ELECTRÓNICO**

# CERTIFICADOS DIGITALES

**FIRMA ELECTRÓNICA** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante (integridad)

**FIRMAR ELECTRÓNICAMENTE** es el proceso en el que el signatario utiliza una clave secreta que le vincula al documento.

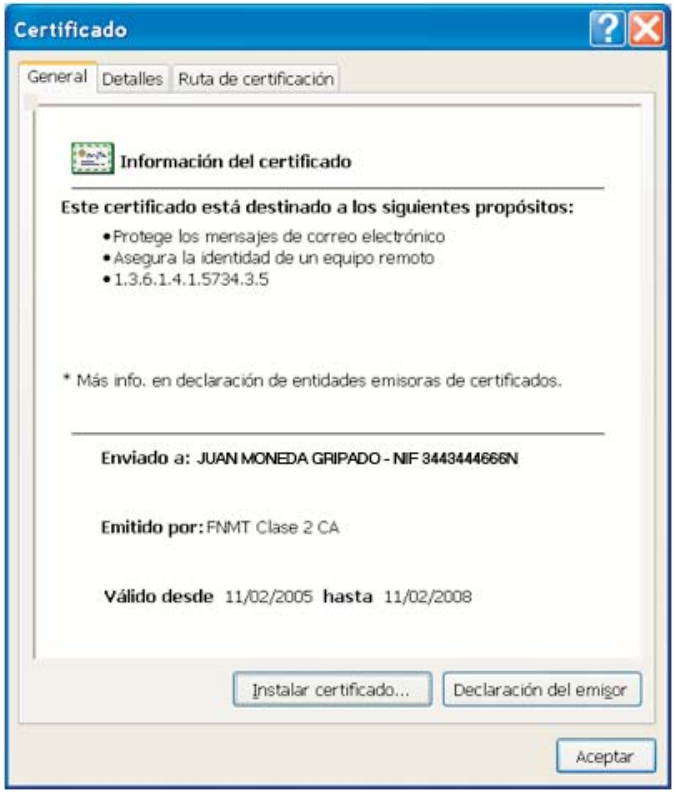
**LA VALIDEZ DE LA FIRMA** podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.



# CERTIFICADOS DIGITALES

**CERTIFICADO DIGITAL** es un archivo **FIRMADO** con la clave privada de una **AUTORIDAD DE CERTIFICACIÓN** y que contiene la clave pública de dicha identidad y los atributos del titular del certificado.

certificado.cer



# AUTORIDAD DEL CERTIFICADO

- Es necesario un elemento que evite que un participante suplante a otro.
- Debe ser un elemento en el que todos los participantes confien.
- El elemento certifica con su firma que un participante es quien dice ser.
- La llave pública del elemento debe ser conocida por todos y es la única que necesita ser conocida previamente.
- Este elemento se llama Autoridad de Certificación.

# CERTIFICADOS DIGITALES

El **certificado digital** es un vínculo entre una **clave pública y una identidad de usuario**, que se consigue mediante una firma digital por una tercera parte o autoridad de certificación en la que **TODOS** confían.

El uso de **certificados** basado en la **criptografía asimétrica**, está diseñado sobre una **Entidad de Certificación** en la que confían todos los usuarios que emite los certificados, para entenderlo podemos utilizar el símil de una caja con dos llaves diferentes, una publica que conoce todo el mundo y otra privada que el dueño debe mantener en secreto.

# CERTIFICADOS DIGITALES

El **Documento Nacional de Identidad Electrónico** es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

# Fin del tutorial

## Certificados digitales