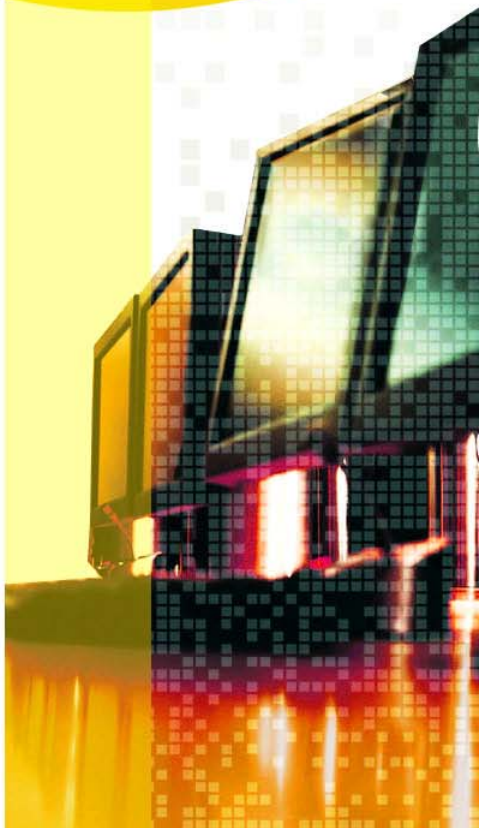
Firma Electronica Avanzada

Vivir Mejor

Vivir Mejor

Qué es y para qué sirve la Firma Electrónica Avanzada

La Firma Electrónica Avanzada es un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa.



Vivir Mejor

Su diseño se basa en estándares internacionales de infraestructura de claves públicas en donde se utilizan dos claves o llaves para el envío de mensajes

CLAVE PUBLICA

CLAVE PRIVADA

Vivir Mejor

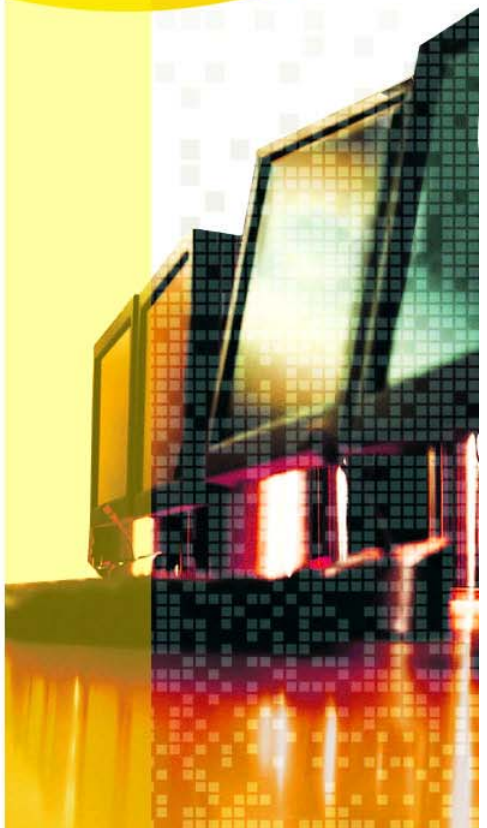
Clave Publica

Disponible en Internet para consulta de todos los usuarios de servicios electrónicos, con la que se descifran datos.

Clave Privada

Únicamente es conocida por el titular de la firma, que sirve para cifrar datos.

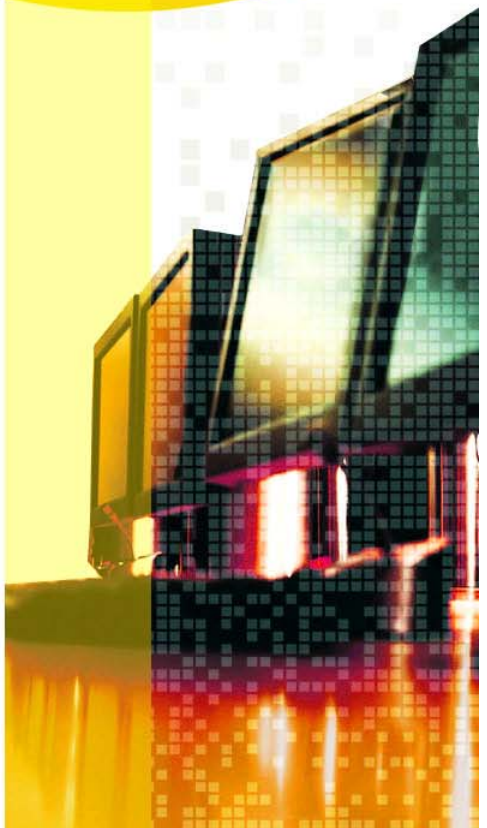
Usando la Clave Publica
Comprueba la Firma



Vivir Mejor

¿Qué es un certificado Digital?

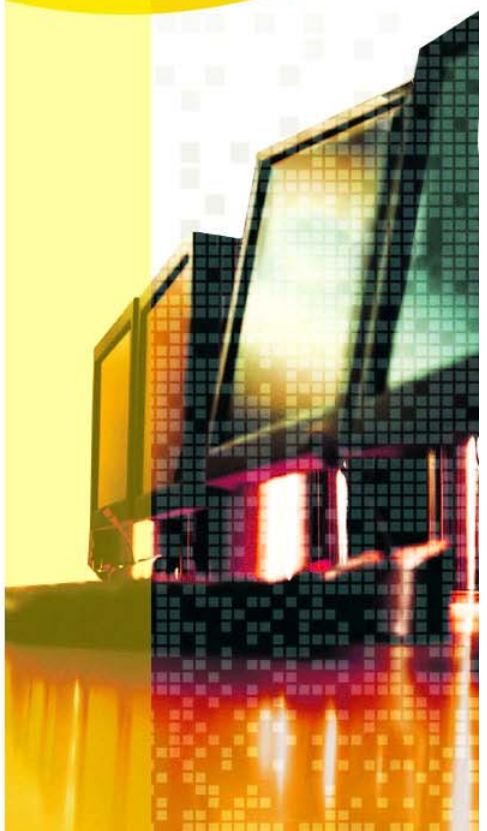
Un certificado digital es un documento electrónico mediante el cual un tercero confiable garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.



Quiénes deben obtenerla

- **De acuerdo con las reformas al Código Fiscal de la Federación, publicadas en el Diario Oficial el 28 de junio y 27 de diciembre de 2006, todos los contribuyentes están obligados a tramitarla.**

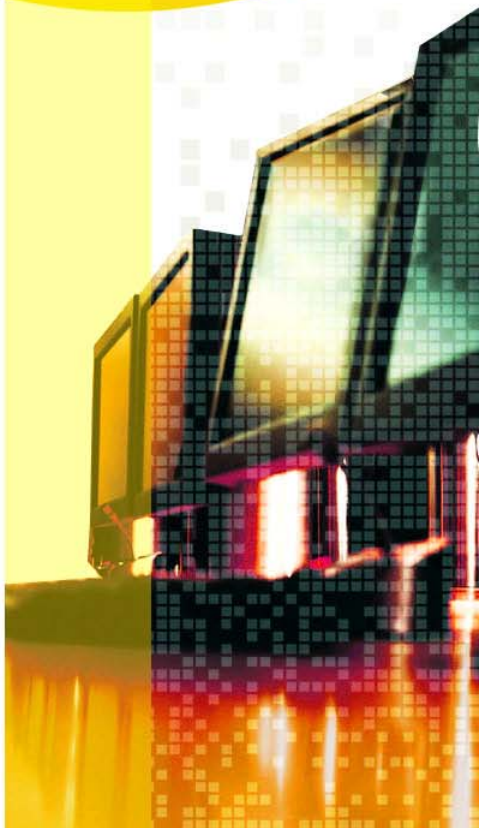
  El Servicio de Administración Tributaria liberará gradualmente los trámites y servicios en donde el uso de la Fiel será obligatorio.



Vivir Mejor

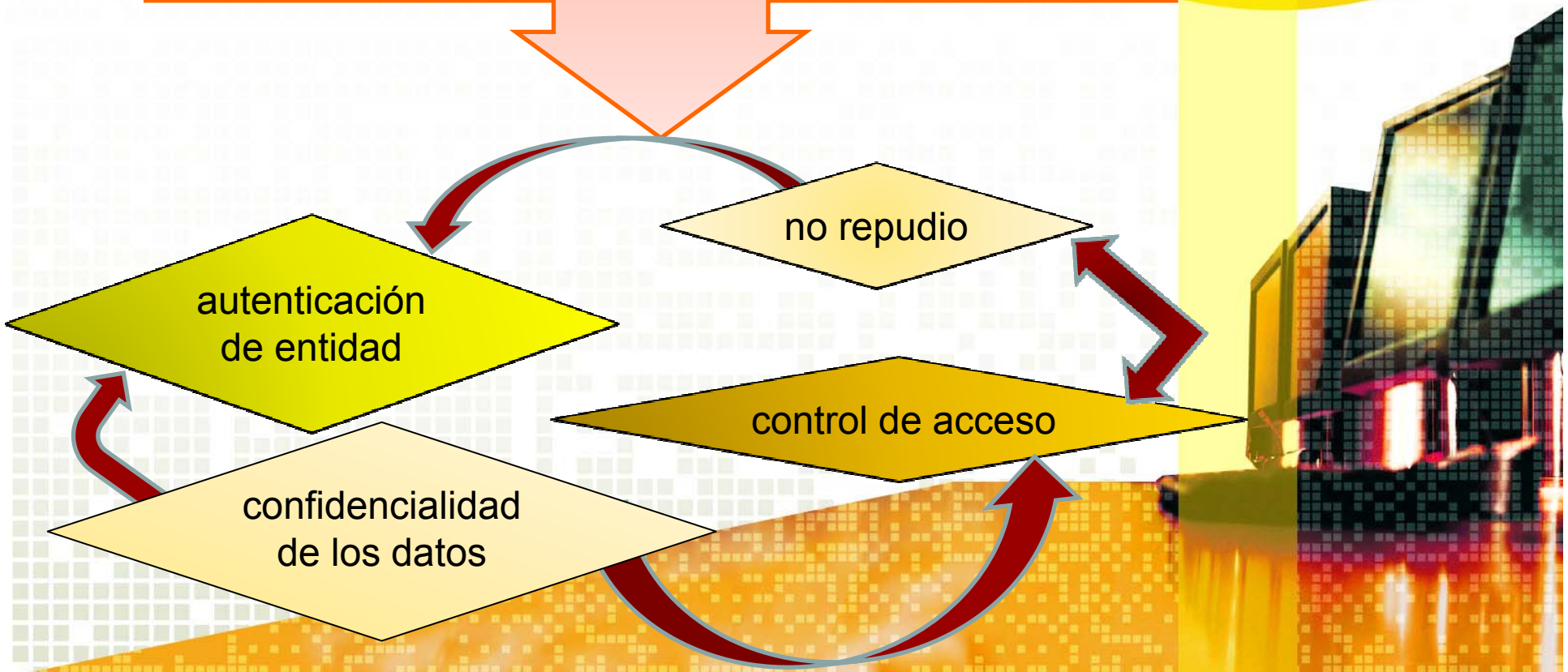
Integridad

Para hacer una breve explicación, al momento de cifrar un mensaje se obtiene un conjunto de datos ilegibles o inentendibles que carecen de sentido. Para poder descifrar dicho mensaje es necesaria la utilización de la clave pública.



Funcionamiento

Para proteger las comunicaciones de los usuarios en las redes es necesario dotar a las mismas de los siguientes servicios de seguridad:



Vivir Mejor

Para proporcionar estos servicios de seguridad es necesario incorporar dos mecanismos:

Cifrado:

Utilizando sistemas criptográficos simétricos o asimétricos

Control de acceso:

Mecanismo que se utiliza para legalizar las capacidades de una entidad con el fin de asegurar los derechos de acceso a recursos que posee

Vivir Mejor

La firma digital supone el cifrado, con una componente secreta del/la firmante, de la unidad de datos.

Consiste en un bloque de caracteres que acompaña a un documento acreditando quién es su autor que no ha existido ninguna manipulación posterior de los datos.

Vivir Mejor

Existen dos tipos de firma electrónica

De clave simétrica

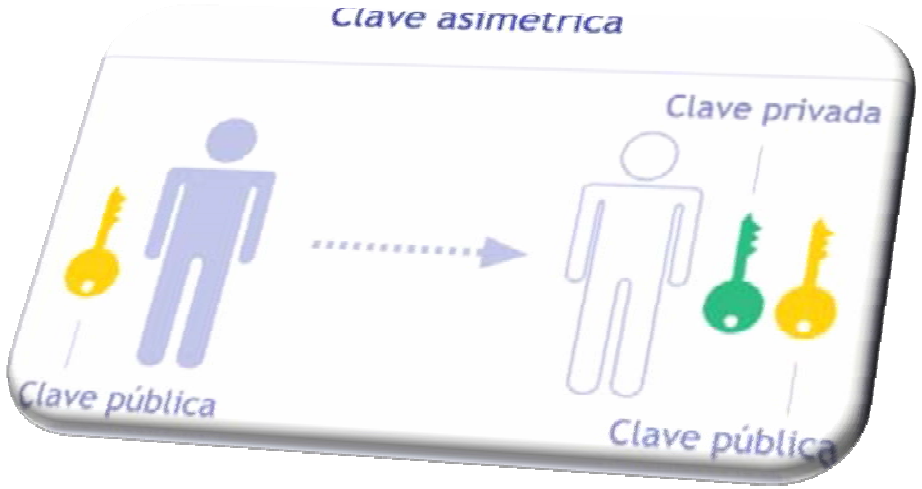
Fueron las primeras en utilizarse. Supone que habiendo dos partes interesadas en el contenido de una comunicación o transacción electrónica, la clave que se utiliza para decodificar el mensaje, será sólo una, que ambas partes poseerán.

De infraestructura de clave pública o simétrica.

La firma electrónica tiene un valor equivalente al de la firma manuscrita, pudiendo darse a conocer a los demás la primera y debiéndose guardar por el interesado la segunda, sin revelarla a los demás.

Vivir Mejor


Clave simetrica

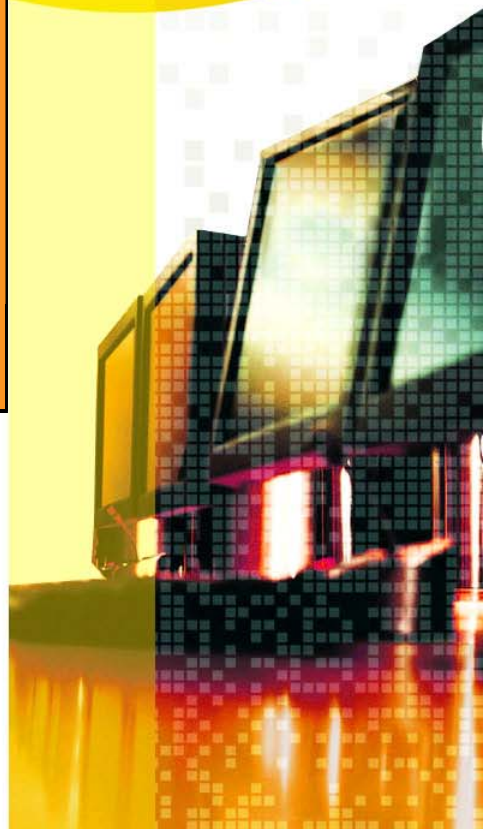

Clave asimetrica
Clave privada
Clave pública
Clave pública

Vivir Mejor

Certificados

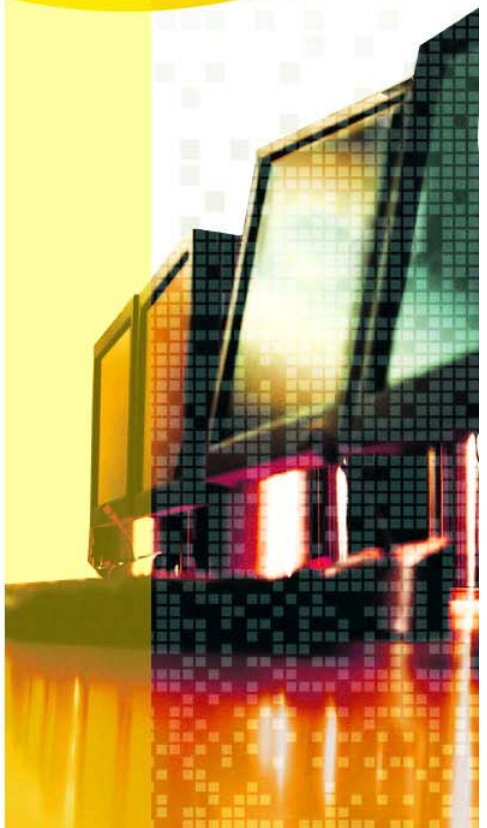
La Ley lo define como la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

Los certificados no son más que registros electrónicos que atestiguan que una clave pública pertenece a un determinado individuo o entidad e intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.



Vivir Mejor

Los certificados contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado.



Vivir Mejor

Tipos de certificados

Identifican y conectan un nombre a una clave pública.

Certificados de identificación

Certificados que colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para dar fe de la validez de un determinado hecho.

Certificados de autorización

Certificados que permiten determinar día y hora en que el documento fue digitalmente firmado

Digital-time stamp certificates

Ofrecen otro tipo de información correspondiente al usuario, como por ejemplo la dirección comercial, antecedentes, catálogos de productos

Vivir Mejor

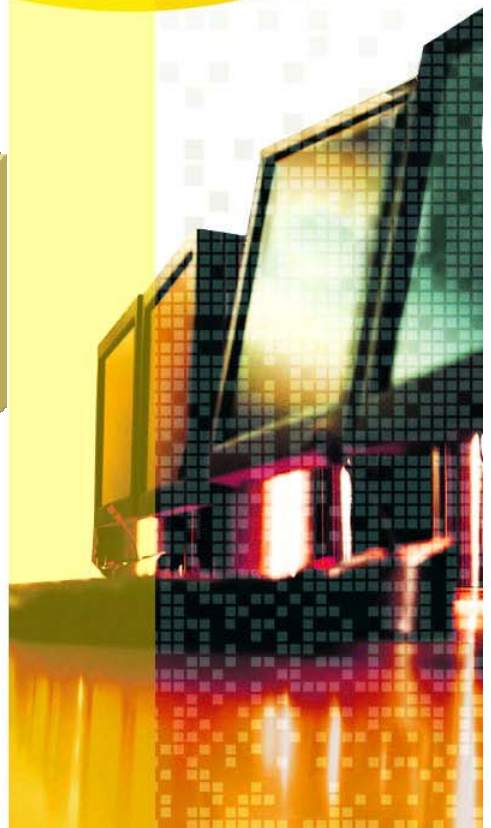
Obtención de certificados

Un certificado se puede obtener directamente de la Autoridad de Certificación o a través de otras empresas que se hayan constituido como entidades colaboradoras en el registro de certificados.

Vivir Mejor

Para la emisión de un certificado es preciso la identificación del usuario frente a la Autoridad de Registro o una Entidad Colaboradora en el Registro. Según el certificado solicitado se deberá presentar la documentación requerida

La Autoridad de Registro y las ECR se encargan por tanto de identificar de manera inequívoca a los/as usuarios/as para que, posteriormente, éstos puedan obtener los certificados.



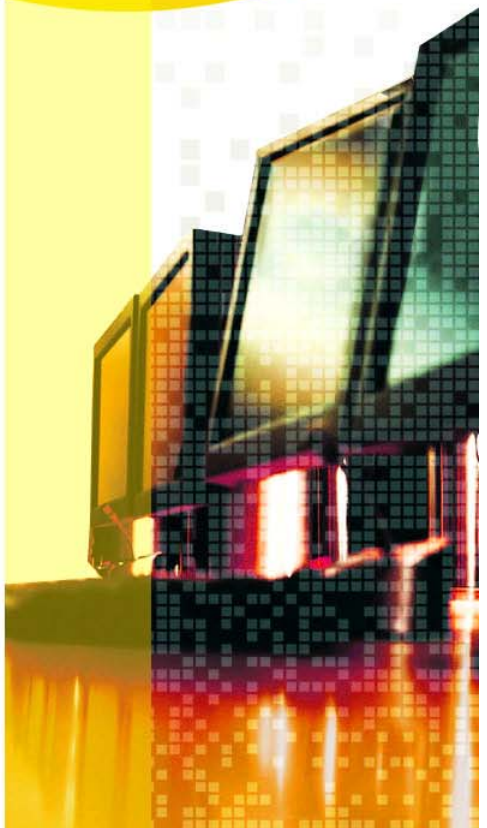
Vivir Mejor

El procedimiento es el siguiente:

El usuario presenta la documentación, bien de forma o físicamente según el nivel de seguridad, se verifica la identidad y se proporciona un ID o identificador y una contraseña.

La solicitud se realiza por tanto de forma y las claves se generan automáticamente en el mismo ordenador desde el que se realiza la solicitud.
La clave pública se enviaría posteriormente a la Autoridad de Certificación también de forma automática.

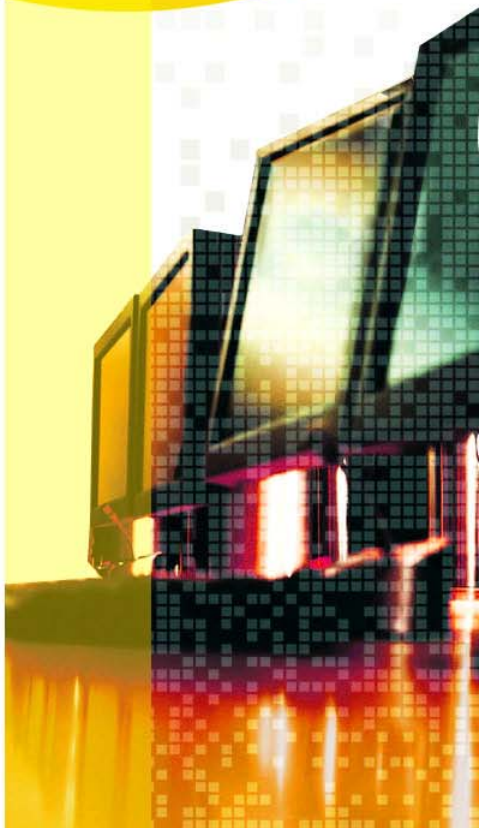
1



Vivir Mejor

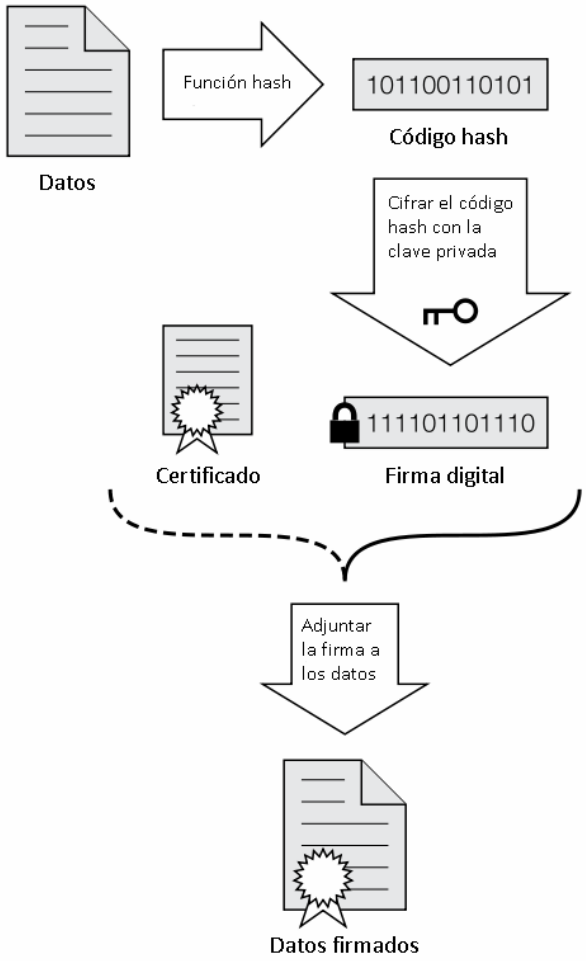
1

Se procede mediante el ID y la contraseña a realizar la solicitud a la Autoridad de Certificación y ésta, tras verificar los datos que el solicitante le proporciona ID, contraseña emite el certificado.

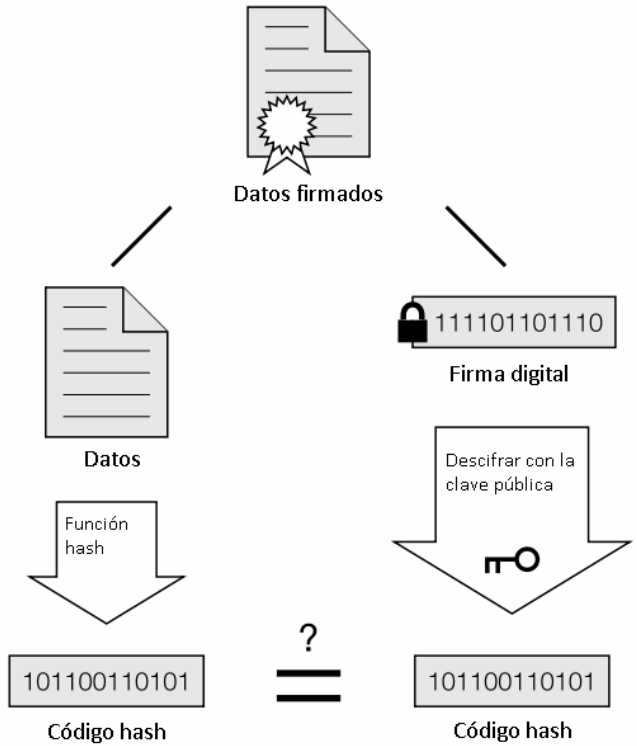


Vivir Mejor

Firma Digital



Comprobación de una Firma



Si los códigos hash coinciden, la firma es válida