Firma Digital

Conceptos Fundamentales y su aplicación en SUDOCU

Diego F. Quiroga
Dirección General de Tecnologías de Información
UNSL
dgti.sudocu@gmail.com

¿Qué es la firma digital?

Es una solución tecnológica que permite añadir a documentos *digitales* una ***huella o marca única, a través de ciertas operaciones matemáticas***.

La firma digital ***permite al receptor*** del documento:

- Identificar al firmante de forma fehaciente **(Autenticación)**
- Asegurar que el contenido no pudo ser modificado luego de la firma **(Integridad)**
- Tener garantías de que la firma se realizó bajo el control absoluto del firmante **(Exclusividad)**
- Demostrar el origen de la firma y la integridad del documento ante terceros, de modo que el firmante no pueda negar o repudiar su existencia o autoría **(No Repudio)**

La *firma digital* posee las mismas características técnicas de seguridad que una firma en papel, e incluso mayores.

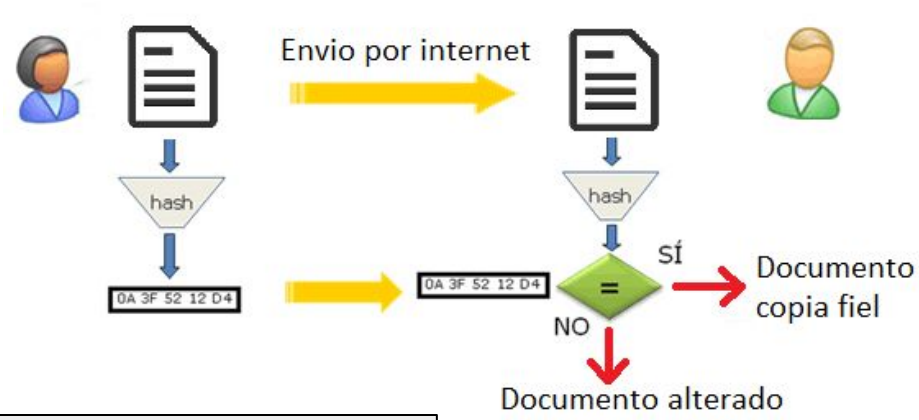
Hash (o resumen)

Es un resumen único que se relaciona a un documento digital. Se puede aplicar a cualquier tipo de documento, incluso a una cadena de texto. Se obtiene al aplicar una fórmula matemática llamada función de hash. El resultado suele expresarse en sistema hexadecimal.

Por ejemplo, el hash calculado por la función SHA1 para el texto “Hola UNSL” es:
16c6b1c40a121838049a3cc8bbdc4bbf02b49f60

Características:

- Bajo costo
- Longitud constante
- Determinista
- Unidireccional
- Resistente a colisiones

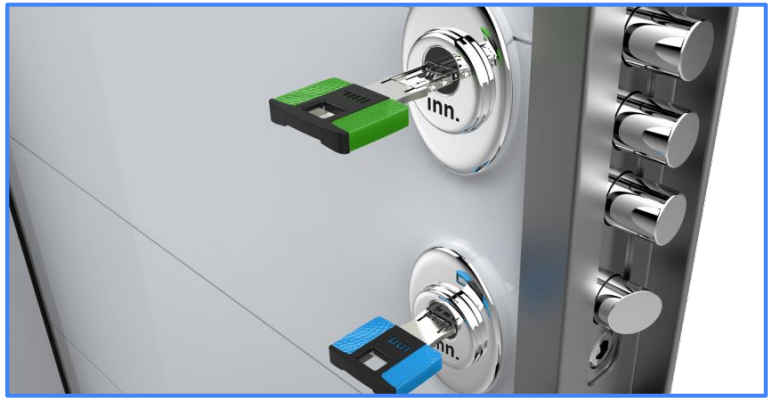


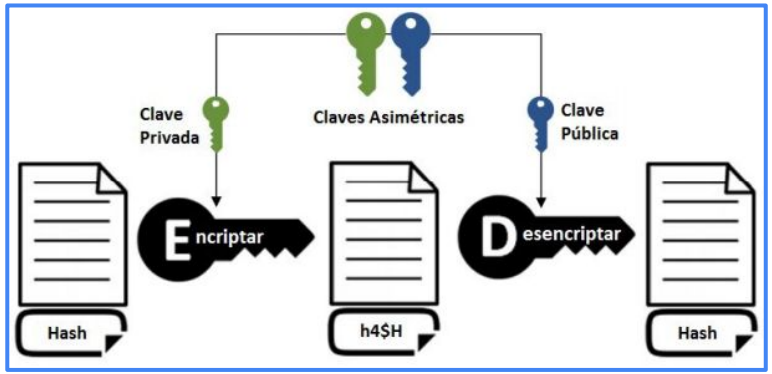
https://emn178.github.io/online-tools/sha512.html

Clave Asimétrica

- La Clave Asimétrica es un método de criptografía, en el que se generan dos números mediante una fórmula matemática compleja.
- Estos números, llamados “claves” (pública y privada), son distintos, pero están relacionados de modo tal que lo que se cifra o encripta con una clave sólo puede descifrarse con la otra.
- La clave pública se distribuye y la clave privada la conserva el propietario, protegida por una contraseña.
- El par de claves es único, y funciona siempre en conjunto: No es posible cifrar y descifrar un documento con una misma clave.

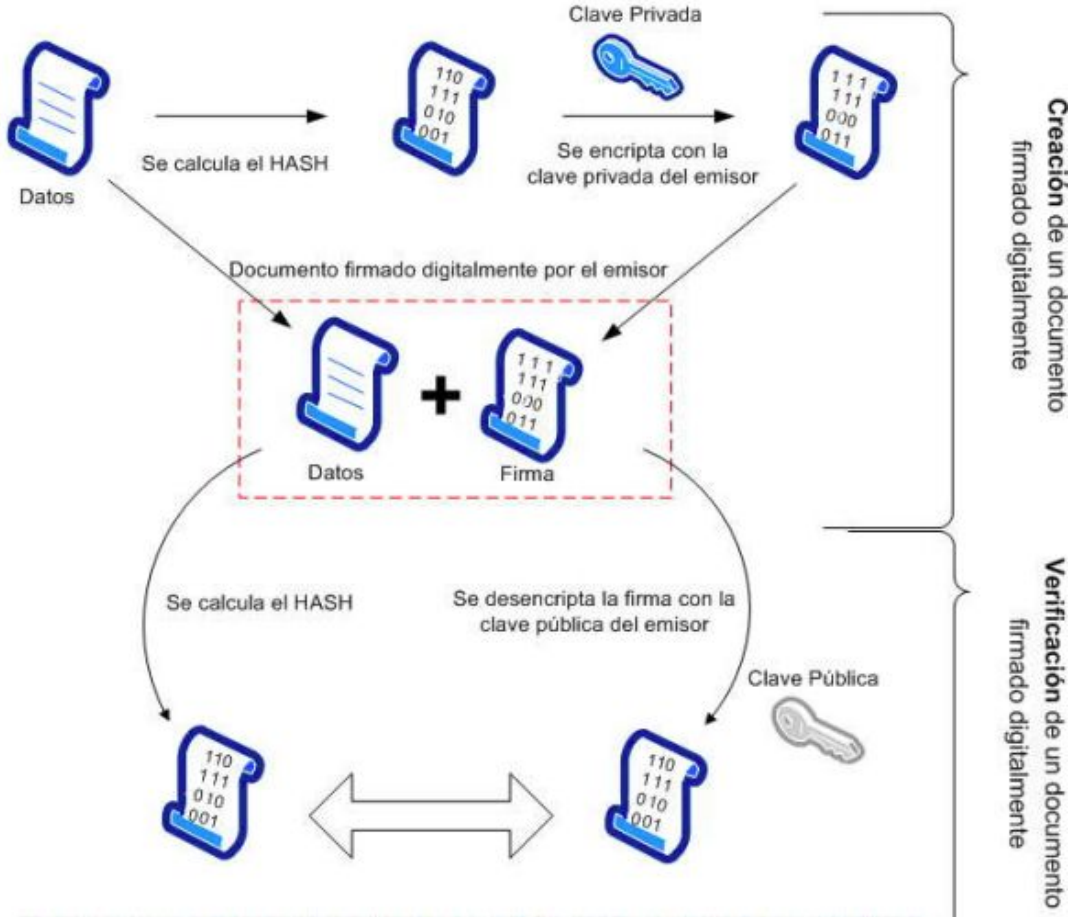
https://www.devglan.com/online-tools/rsa-encryption-decryption





Con este mecanismo se encripta el HASH del documento.

Proceso de Firma y Verificación



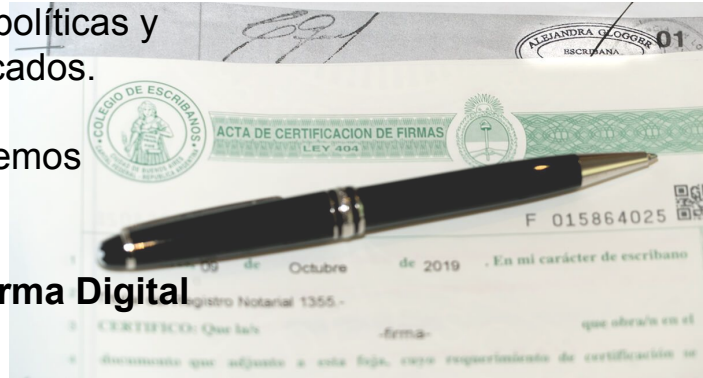
Certificados Digitales - Infraestructura PKI

Para que el procedimiento de firma y autenticación sea confiable, necesitamos la seguridad de que esa clave pública efectivamente pertenece al firmante.

Un **Certificado Digital** es un documento firmado digitalmente por una autoridad, en el cual se atestigua que una clave pública pertenece a un determinado individuo o entidad. En general, contiene:

- datos de identidad de la persona,
- su clave pública
- **Período de vigencia**,
- y el nombre de la autoridad que emitió el certificado

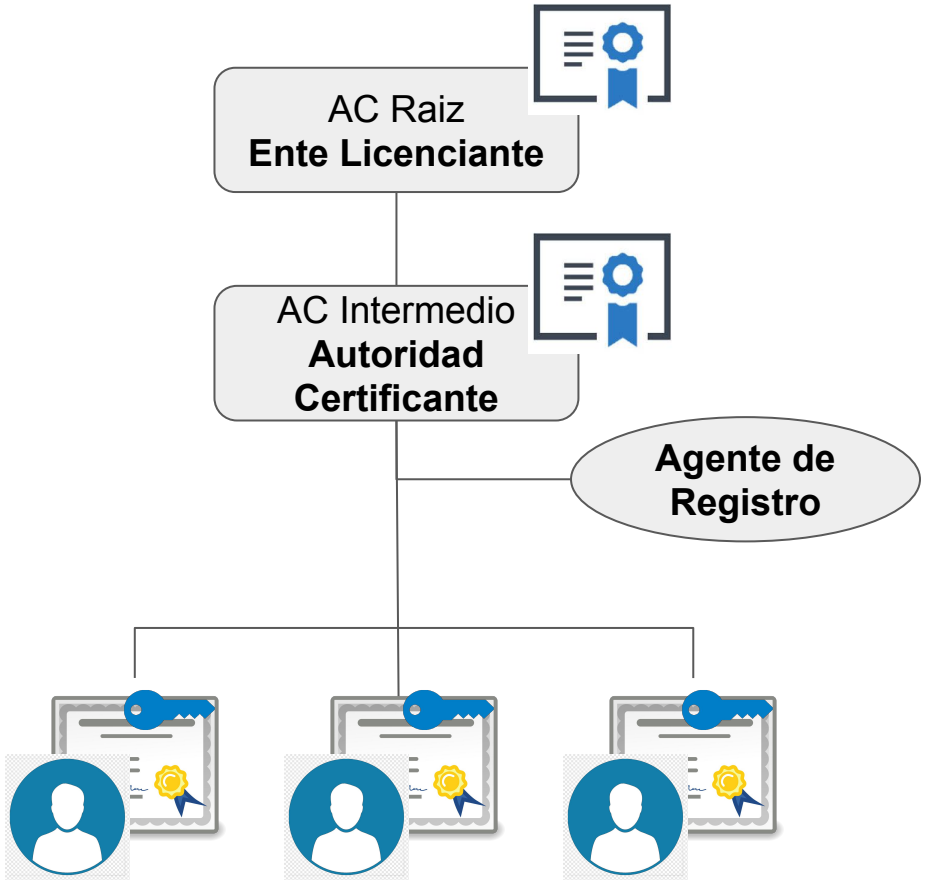
La Infraestructura de Clave Pública es el conjunto de procedimientos, políticas y roles normados que definen cómo se generan y organizan esos certificados.



Si el certificado es auténtico y confiamos en la autoridad emisora, podemos asegurar la identidad del firmante.

En nuestro país, esta regulación se conoce como Infraestructura de **Firma Digital de la República Argentina (IFDRA) - Ley 25.506 de Firma Digital**

Jerarquía de Certificados en la IFDRA

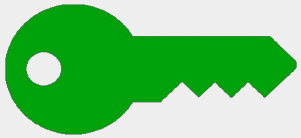


JEFATURA DE GABINETE DE MINISTROS de la Nación

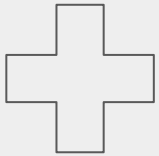
ONTI - MODERNIZACION - AFIP - OTROS

UNSL (AR de ONTI)

En resumen, como persona, ¿que tengo que tener para poder firmar digitalmente?



Clave Privada



Clave Pública

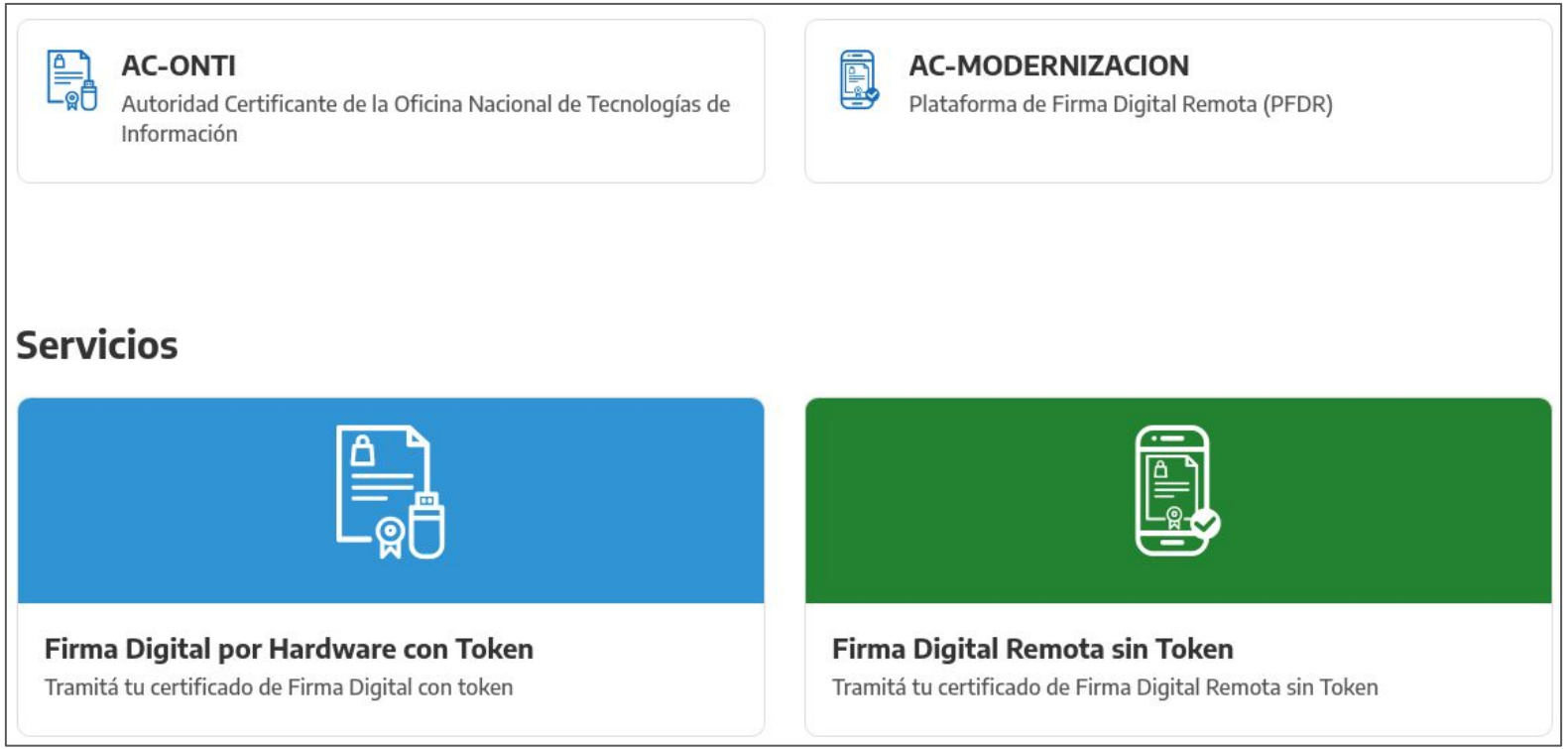
Datos Personales

Certificado Digital Firmado por una Autoridad Certificante (ONTI)

¿Dónde se guarda esta información y cómo se protege?

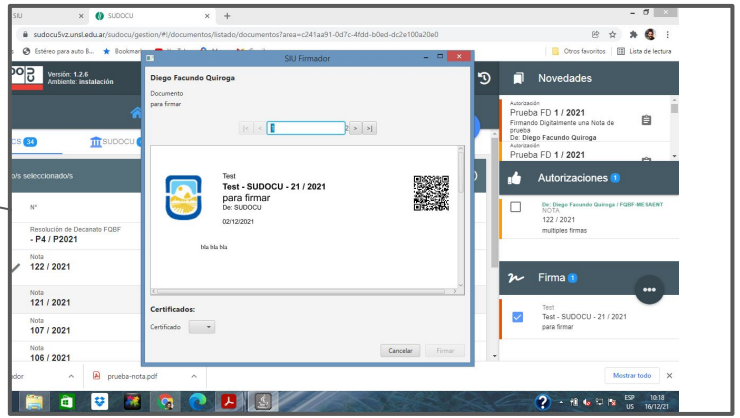
Firma digital Argentina: con Token, o en la Nube

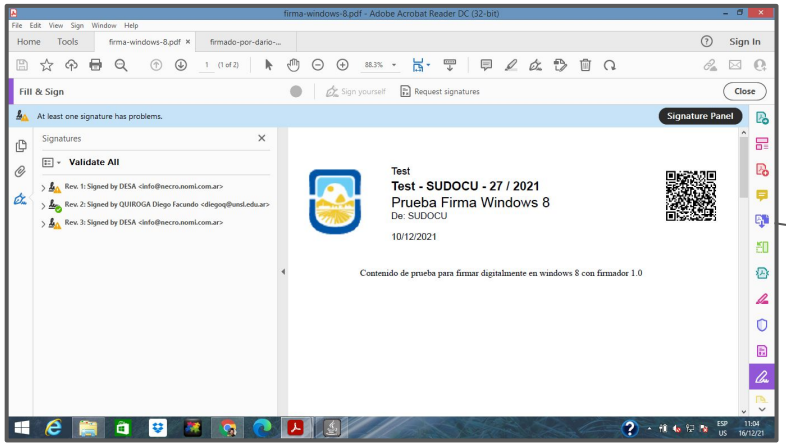
https://www.argentina.gob.ar/firmadigital



Para firmar digitalmente, o verificar la firma de un documento:

¡Necesito un software específico! que calcule el hash, lo encripte con mi clave privada y lo incluya en el documento junto a mi certificado (clave pública). Ej. **Firmador SIU**, Acrobat DC, etc.





O **un software** que calcule el hash del documento, verifique el certificado y la cadena de confianza,, desencripte el hash (de la firma) con la clave pública, y lo compare con el del documento.

La firma digital no se verifica visualmente! - Algunos formatos (PDF) permiten asociar una representación visual de la firma, que puede o no estar. Pero esta sola representación no es suficiente para que exista la firma digital.

Vamos a ver un ejemplo real en SUDOCU

https://sudocu5vz.unsl.edu.ar

1) **Vamos a Generar un Documento en SUDOCU y lo vamos a firmar con Token**

2) **Vamos a Verificar el resultado en Acrobat Reader DC**

LEY DE FIRMA DIGITAL

(Ley 25.506 Noviembre de 2001)

http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

¿Qué es la Firma Digital?

ARTICULO 2º — Firma Digital. Se entiende por firma digital al resultado de **aplicar a un documento digital un procedimiento matemático** que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital 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.

LEY DE FIRMA DIGITAL

(Ley 25.506 Noviembre de 2001)

Validez Jurídica

ARTICULO 3º — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

Conforme la Ley 25.506, la firma digital cumple las mismas exigencias que la firma manuscrita de los documentos en papel, ya que posee las mismas características técnicas de seguridad que una firma en papel, e incluso mayores.

LEY DE FIRMA DIGITAL

(Ley 25.506 Noviembre de 2001)

¿Qué es un Certificado Digital?

ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

LEY DE FIRMA DIGITAL

(Ley 25.506 Noviembre de 2001)

Firma Digital Válida

ARTICULO 9º — Validez. Una firma digital es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado; ***(certificados extranjeros)***

LEY DE FIRMA DIGITAL

(Ley 25.506 Noviembre de 2001)

Firma Digital vs Firma Electrónica

Digital ≠ Electrónica

ARTICULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, 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.

Firma Electrónica

Entonces, para poder ser considerada firma electrónica, el procedimiento debe al menos poseer las propiedades de Autenticación e Integridad, y por ende No Repudio.

La diferencia es que la **FIRMA DIGITA**L se realiza con un **Certificado Válido**. La Electrónica NO.

Ejemplos de firma electrónica son:

- Las firmas realizadas con certificados que no fueron emitidos por un Certificador Licenciado, incluyendo certificados emitidos por autoridad certificante extranjera (salvo las que cumplan los requisitos del art. 16 ley 25.506),
- certificados emitidos por un ente nacional, privado o público sin licencia,
- certificados generados por el propio firmante mediante alguna aplicación informática.
- La firma realizada con certificado válido (emitido por un Certificador Licenciado) pero expirado o revocado antes de firmar.

¡Gracias por su atención!

¿Preguntas?