DIGITAL SIGNATURE

INDICE

CHE COS'È?

La **digital sign** (firma digitale) è un meccanismo crittografico che consente di verificare l'autenticità e l'integrità di un documento o di un messaggio elettronico. Si tratta di una tecnologia che garantisce che il documento non sia stato modificato e che provenga effettivamente dal mittente dichiarato.

COME CREARLA?

1. Ottieni un certificato digitale: Devi registrarti presso una Certification Authority (CA), come Aruba, Infocert o Poste Italiane. Fornirai i tuoi documenti per l'identificazione, e in cambio otterrai un certificato digitale contenente una chiave pubblica e una chiave privata. Questo certificato può essere rilasciato su un dispositivo fisico (smart card o chiavetta USB) o su un servizio cloud.

COME CREARLA?

2. Installa il software di firma digitale: La CA ti fornirà un software o ti indicherà uno strumento compatibile per firmare i documenti, come Dike (Infocert), ArubaSign (Aruba), o PosteKey (Poste Italiane). Se hai ricevuto un dispositivo fisico (come una smart card), avrai bisogno di un lettore per utilizzarlo con il software.

COME CREARLA?

3. Firma i tuoi documenti: Apri il software, carica il documento da firmare (formato PDF, DOC, ecc.), seleziona la tua chiave privata e inserisci il PIN o la password associati. Il software genera la firma digitale e la applica al documento.

COME CREARLA?

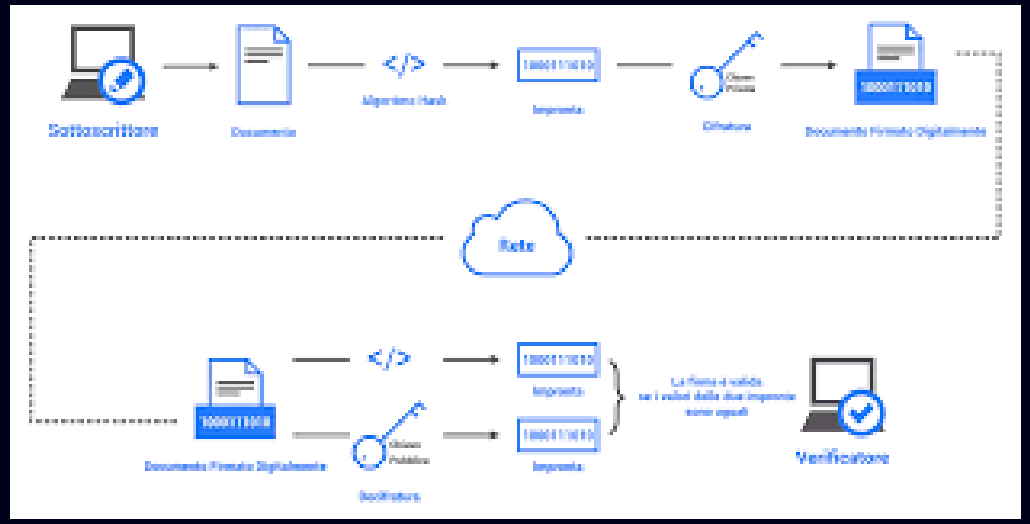
4. Verifica della firma: Il documento firmato digitalmente include un codice crittografico che può essere verificato da chiunque usando la tua chiave pubblica. Il destinatario può verificare che il documento non sia stato alterato e che la firma provenga effettivamente da te.

La firma digitale fornisce autenticità, sicurezza e valore legale, ed è utilizzata in contesti ufficiali e legali.

FUNZIONAMENTO ALL'INTERNO DEL DOCUMENTO

1. Generazione dell'Hash

- Quando firmi digitalmente un documento, il software di firma digitale crea un hash (riassunto crittografico) del documento. L'hash è una stringa univoca di numeri e lettere generata a partire dal contenuto del documento.
- Questo hash rappresenta una sorta di "impronta digitale" del documento: anche una piccola modifica nel documento genererebbe un hash completamente diverso.

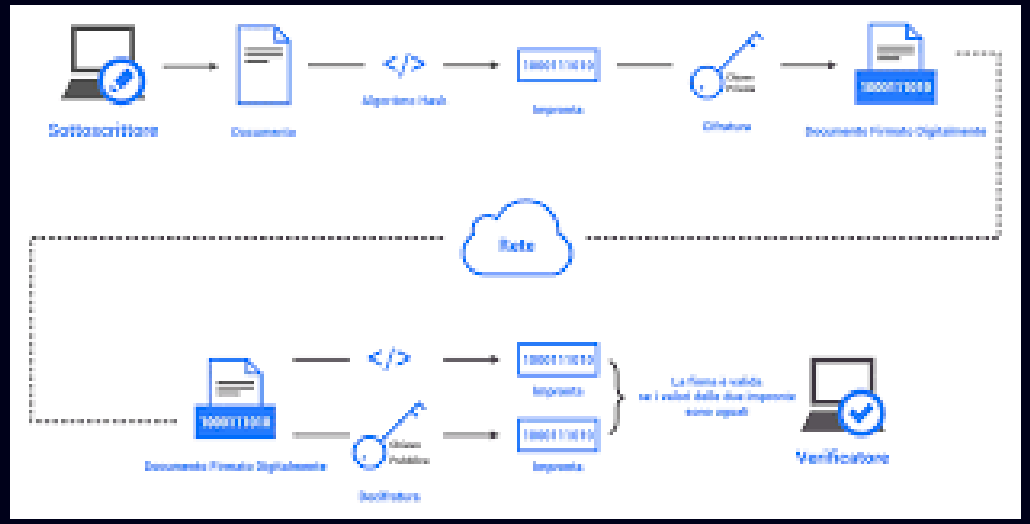


FUNZIONAMENTO ALL'INTERNO DEL DOCUMENTO

2. Cifratura dell'Hash con la Chiave Privata

- Il firmatario utilizza la propria chiave privata per cifrare l'hash. Questo passaggio è fondamentale perché la chiave privata è segreta e associata solo al proprietario.

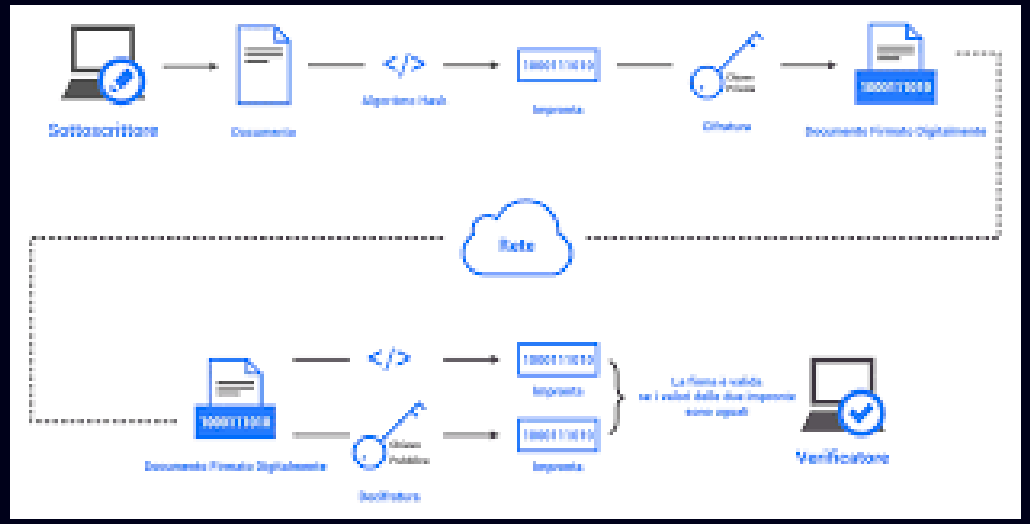
- L'hash cifrato diventa la firma digitale vera e propria e viene inserito all'interno del documento. Viene anche incluso il certificato digitale del firmatario, che contiene la chiave pubblica per la verifica.



FUNZIONAMENTO ALL'INTERNO DEL DOCUMENTO

3. Aggiunta della Firma al Documento

- La firma digitale e il certificato vengono allegati al documento, ma il contenuto del documento non viene alterato o cifrato. Il documento rimane leggibile e modificabile, ma la firma digitale è legata alla sua versione esatta al momento della firma.



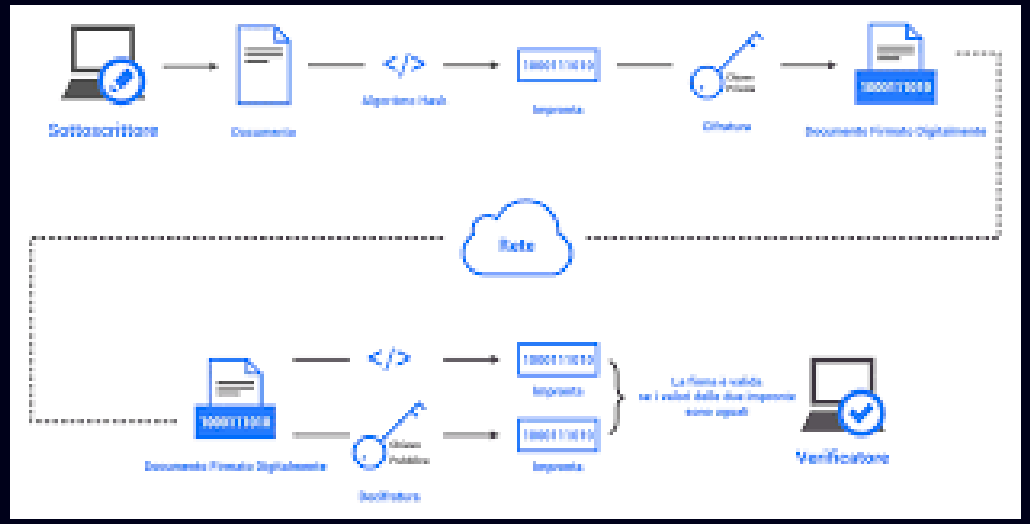
FUNZIONAMENTO ALL'INTERNO DEL DOCUMENTO

4. Verifica della Firma Digitale

- Quando qualcuno riceve il documento firmato, può usare la chiave pubblica del firmatario (inclusa nel certificato) per decifrare l'hash della firma digitale.

- Poi il destinatario genera un nuovo hash dal documento ricevuto. Se l'hash decifrato dalla firma coincide con quello appena generato, significa che:

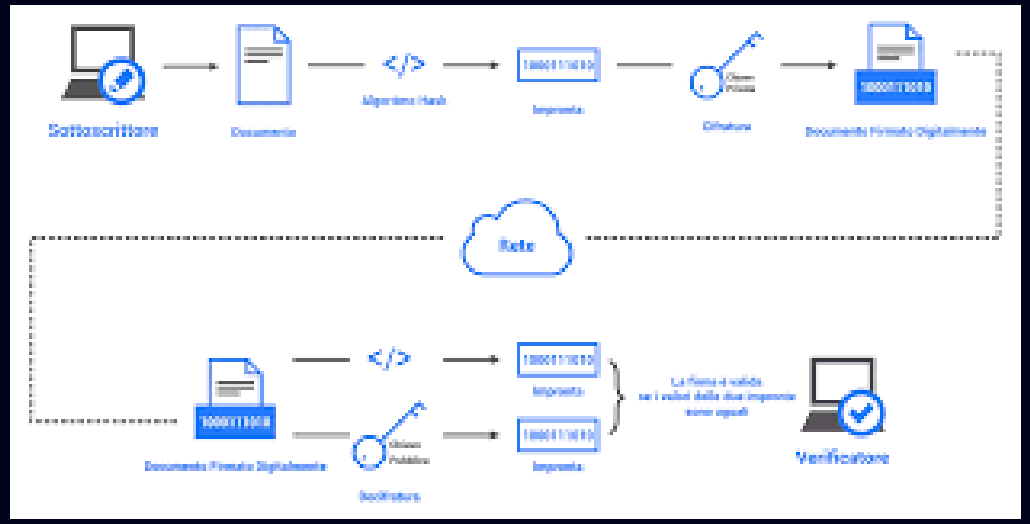
1. Il documento non è stato modificato (integrità garantita).
2. La firma proviene effettivamente dal proprietario della chiave privata (autenticità garantita).



FUNZIONAMENTO ALL'INTERNO DEL DOCUMENTO

5. Non Ripudio

- Poiché solo il firmatario possiede la chiave privata, non può negare di aver firmato il documento. Questo principio si chiama non ripudio.



VANTAGGI

Vantaggi:

- Verifica dell'identità: Conferma che il documento arriva dal mittente.

- Controllo dell'integrità: Dimostra che il contenuto non è stato alterato.

- Non negabilità: Il mittente non può negare di aver firmato, poiché solo lui possiede la chiave privata usata.

LA DIFFERENZA TRA FIRMA DIGITALE E FIRMA ELETTRONICA

La differenza tra firma digitale e firma elettronica riguarda il livello di sicurezza e di autenticità che offrono:

1. Firma Elettronica:

- È un concetto più ampio e generico. Si riferisce a qualsiasi tipo di firma applicata in formato digitale, come inserire una scansione della propria firma manoscritta, fare clic su un pulsante "Accetto" o firmare con uno stilo su un dispositivo touch.
- Non garantisce necessariamente l'autenticità o l'integrità del documento firmato.
- Può essere facilmente riprodotta o falsificata.
- È utilizzata per transazioni meno formali o dove non è richiesta una sicurezza elevata.

LA DIFFERENZA TRA FIRMA DIGITALE E FIRMA ELETTRONICA

2. Firma Digitale:

- È un tipo specifico di firma elettronica che utilizza tecniche crittografiche (chiavi pubbliche e private) per garantire sicurezza, autenticità e integrità del documento.
- Offre un livello elevato di protezione, poiché garantisce che il documento non sia stato modificato e che provenga dal mittente.
- È legalmente vincolante in molti Paesi, inclusa l'Unione Europea, dove è regolata dal Regolamento eIDAS.
- Non può essere facilmente falsificata, poiché richiede la chiave privata del firmatario per essere creata.

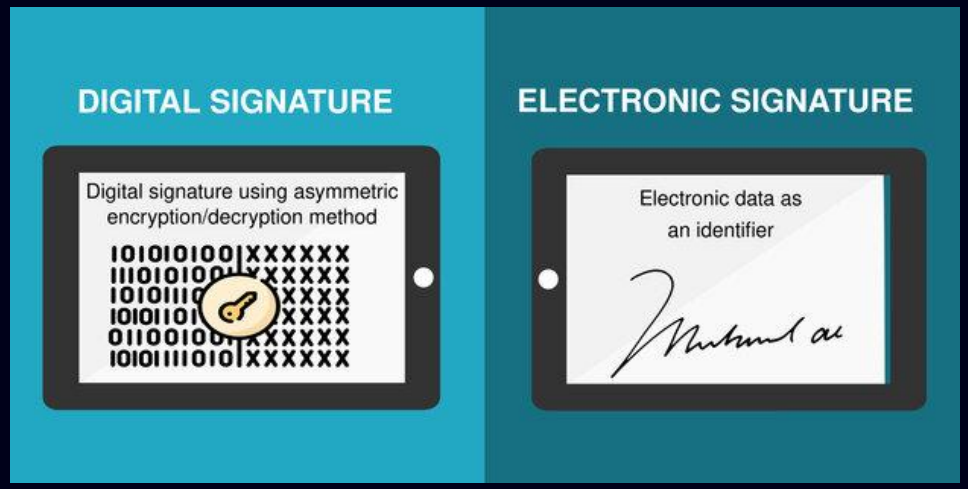
La firma digitale è quindi una forma avanzata e sicura di firma elettronica.

LA DIFFERENZA TRA FIRMA DIGITALE E FIRMA ELETTRONICA

Riassunto delle differenze:

- Firma elettronica: Più semplice, meno sicura, non sempre garantisce autenticità e integrità.

- Firma digitale: Più complessa, altamente sicura, garantisce l'origine e l'integrità del documento grazie alla crittografia.



AZIENDE INFORMATICHE CHE UTILIZZANO LA DIGITAL SIGNATURE

Alcune aziende che offrono o utilizzano ampiamente la firma digitale (digital signature), una tecnologia sempre più diffusa per autenticare documenti in modo sicuro e legalmente valido:

1. **DocuSign**

- Una delle piattaforme più conosciute al mondo per la gestione e la firma digitale di documenti. Molte aziende in vari settori (finanziario, legale, immobiliare) utilizzano DocuSign per la firma di contratti e documenti legali.

AZIENDE INFORMATICHE CHE UTILIZZANO LA DIGITAL SIGNATURE

2. Adobe Sign

- Parte del pacchetto Adobe, questa piattaforma è utilizzata per gestire firme elettroniche e digitali in modo sicuro. Molte aziende di diversi settori utilizzano Adobe Sign per snellire i processi di approvazione e gestione documentale.

3. Aruba PEC

- Un'azienda italiana specializzata in soluzioni di certificazione digitale, tra cui PEC (Posta Elettronica Certificata) e firme digitali. Molte imprese italiane utilizzano i suoi servizi per garantire la validità legale dei documenti elettronici.

4. InfoCert

- Un altro grande provider italiano di soluzioni di firma digitale, identificazione elettronica e servizi fiduciari. Molte aziende italiane e pubbliche amministrazioni utilizzano InfoCert per la firma digitale e la conservazione elettronica a norma.

AZIENDE INFORMATICHE CHE UTILIZZANO LA DIGITAL SIGNATURE

5. Yousign
- Una piattaforma europea di firma digitale utilizzata da piccole e medie imprese (PMI) e professionisti per firmar e autenticare documenti in modo semplice e sicuro. La piattaforma è diffusa in diversi paesi, tra cui l'Italia.

6. SignNow
- Piattaforma usata da aziende per gestire firme elettroniche in documenti PDF, contratti e accordi. Viene utilizzata soprattutto per la semplicità di integrazione con altri strumenti aziendali, come Salesforce e Google Drive.

7. Namirial
- Azienda italiana che offre una vasta gamma di servizi di firma digitale, compresi soluzioni di identità digitale e conservazione a norma. Namirial è fortemente presente in settori come la finanza, la sanità e la pubblica amministrazione.

AZIENDE INFORMATICHE CHE UTILIZZANO LA DIGITAL SIGNATURE

8. HelloSign (parte di Dropbox)

- Una piattaforma di firma elettronica popolare tra aziende e professionisti, specialmente per la sua integrazione con Dropbox. Molte startup e PMI utilizzano HelloSign per gestire accordi digitali.

9. Zucchetti

- Grande azienda italiana di software che offre anche soluzioni per la firma digitale. I suoi sistemi di gestione documentale vengono utilizzati da diverse imprese italiane, spesso in ambito fiscale e contabile.

10. Kofax SignDoc

- Un'altra soluzione globale di firma digitale, utilizzata da aziende in settori quali finanza, sanità e pubblica amministrazione per la gestione dei flussi di lavoro e l'autenticazione sicura dei documenti.

SETTORI CHE UTILIZZANO LA DIGITAL SIGNATURE

Settori che utilizzano frequentemente la firma digitale:

- Banche e Finanza: Per contratti di mutuo, aperture di conti, prestiti e transazioni.
- Sanità: Per la firma di documenti medici e la gestione di cartelle cliniche.
- Legale: Studi legali utilizzano firme digitali per contratti e documenti ufficiali.
- Pubblica Amministrazione: Molti enti pubblici richiedono la firma digitale per certificati, atti e contratti con i cittadini e le aziende.
- Assicurazioni: Per la firma di polizze, contratti e reclam