FIRMA DIGITALE

COS'È LA FIRMA DIGITALE?

La **firma digitale** è uno schema matematico per dimostrare l'autenticità di un messaggio o di un documento digitale inviato attraverso un canale non sicuro.

QUANDO SI USA LA FIRMA DIGITALE?

Le firme digitali si basano su protocolli crittografici comunemente usati nella distribuzioni di software, nelle transazioni finanziarie e in altri casi in cui si debba rilevare la falsificazione o l'alterazione del messaggio.

VALORE GIURIDICO DELLA FIRMA DIGITALE IN EUROPA

A livello europeo il sistema delle firma elettroniche e quindi anche della firma digitale va ricondotto alla direttiva 1999/93/CE, Direttiva del Parlamento europeo e del Consiglio relativa ad un quadro comunitario per le firme elettroniche.

Pubblicata nella G.U.C.E. 19 gennaio 2000, n. L 13. è entrata in vigore il 19 gennaio 2000. Particolare importanza ha l'articolo 5 della direttiva, che prevede obblighi degli Stati membri relativi sia alle «firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura» sia ad altri sistemi di firma (che oggi vengono genericamente chiamati deboli o semplici).

VALORE GIURIDICO DELLA FIRMA DIGITALE IN ITALIA

L'Italia si è adeguata alla direttiva nel 2002 (D. lg. 23 gennaio 2002, n. 10) ed oggi nel codice dell'amministrazione digitale si usano i termini di **firma elettronica semplice**, **firma elettronica avanzata** e **firma elettronica qualificata**: quest'ultima differisce dalla **firma digitale** in quanto la firma digitale è l'unica che, per espresso dettato normativo, è vincolata ad una precisa tecnologia (crittografia asimmetrica).

TIPI DI FIRMA ELETTRONICA

Attualmente la legge italiana prevede 4 tipologie di firma elettronica:

- firma elettronica generica
- firma elettronica avanzata
- firma elettronica qualificata
- firma digitale

FIRMA ELETTRONICA GENERICA

(chiamata anche nella prassi firma elettronica "semplice"): l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

FIRMA ELETTRONICA AVANZATA

Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

FIRMA ELETTRONICA AVANZATA

Deve:

- garantire una connessione univoca al firmatario
- essere creata con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

FIRMA ELETTRONICA QUALIFICATA

Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato rilasciato da un certificatore accreditato e realizzata mediante un dispositivo sicuro per la creazione della firma.

FIRMA ELETTRONICA QUALIFICATA

La firma elettronica qualificata ha in più della firma elettronica avanzata:

- l'utilizzo di un dispositivo di firma sicuro
- e di un certificato qualificato rilasciato da un certificatore autorizzato.

FIRMA DIGITALE

Particolare tipo di firma elettronica qualificata basata su un sistema di **chiavi crittografiche**, una pubblica e una privata correlate tra loro che consente:

- al titolare, tramite la chiave privata, di rendere manifesta la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
- al destinatario, tramite la chiave pubblica, di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

FIRMA DIGITALE

La firma digitale è quindi solo un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro.

Tutti gli altri metodi di identificazione informatica sono firme elettroniche semplici.

VALORE GIURIDICO DELLA FIRMA DIGITALE IN ITALIA

- Nell'ordinamento giuridico italiano il termine firma digitale sta a indicare un tipo di firma elettronica qualificata, basato sulla crittografia asimmetrica, alla quale si attribuisce una particolare efficacia probatoria, tale da potersi equiparare, sul piano sostanziale, alla firma autografa.
- Oggi, la legge che disciplina la firma elettronica è il "Codice dell'amministrazione digitale" (Decreto Legislativo 7 marzo 2005, n. 82) che ha subito nel corso del tempo varie modifiche.

FIRMA DIGITALE

La Firma Digitale è l'equivalente informatico di una tradizionale firma autografa apposta su carta e possiede le seguenti caratteristiche:

- **Autenticità** (la firma digitale garantisce l'identità del sottoscrittore)
- **integrità** (la firma digitale assicura che il documento non sia stato modificato dopo la sottoscrizione)
- **non ripudio** (la firma digitale attribuisce piena validità legale al documento, pertanto il documento non può essere ripudiato dal sottoscrittore)

AUTENTICAZIONE

Le firme digitali si utilizzano per autenticare il mittente. Quando si ha garanzia che la **chiave privata** di firma digitale sia in possesso **unicamente dell'utente** al quale è stata attribuita, una firma valida impone che il messaggio sia stato spedito proprio da quell'utente. L'autenticità del mittente è importante specialmente nel contesto finanziario.

Ad esempio, se la filiale di una banca inviasse istruzioni alla sede centrale chiedendo una modifica sul conto corrente di un utente ma la sede centrale mettesse in dubbio la paternità del messaggio, proseguire nella richiesta di modifica del conto potrebbe costituire un errore gravissimo.

INTEGRITÀ

- In molti contesti, il mittente e il destinatario di un messaggio devono avere la certezza che lo stesso non sia stato alterato durante la trasmissione.
- Se un messaggio è firmato digitalmente, ogni cambiamento nel messaggio successivo all'atto della firma, rende nulla la firma.
- Inoltre, non esiste un modo efficiente per modificare un messaggio e la sua firma al fine di produrre un nuovo messaggio con una firma valida, poiché ciò è considerato non realizzabile computazionalmente dalla maggior parte delle funzioni di hash.

HASH

- Nel linguaggio matematico e informatico, l'**hash** è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita.
- **Algoritmo di hash** elabora qualunque mole di bit e restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output è detto *digest*.
- L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output

NON RIPUDIO

- Il non ripudio, più precisamente detto non ripudio dell'origine, è un aspetto importante della firma digitale poiché grazie a questa proprietà, un'entità che ha firmato alcune informazioni non può in un secondo momento negare di averle firmate.
- Essere in possesso solo della chiave pubblica non mette in condizioni un attaccante di falsificare una firma valida.

GENERAZIONE DELLA FIRMA DIGITALE

Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche attribuite in maniera univoca ad un soggetto, detto titolare:

- La **chiave privata** è conosciuta solo dal titolare ed è usata per generare la firma digitale da apporre al documento.
- La **chiave pubblica** è usata per verificare l'autenticità della firma.

SISTEMA CRITTOGRAFICO

Un sistema crittografico garantisce la riservatezza del contenuto dei messaggi, rendendoli incomprensibili a chi non sia in possesso di una "chiave" per interpretarli.

CHIAVE PRIVATA E CHIAVE PUBBLICA

- Per ogni utente, le due chiavi vengono generate da un apposito algoritmo con la garanzia che la *chiave privata* sia la sola in grado di poter decifrare correttamente i messaggi cifrati con la *chiave pubblica* associata e viceversa.
- il mittente utilizza la *chiave pubblica del destinatario* per la cifratura del messaggio da spedire, quindi spedisce il messaggio cifrato al destinatario; il destinatario riceve il messaggio cifrato e adopera la propria chiave privata per ottenere il messaggio "in chiaro".

FIRMA ELETTRONICA

Un tipico schema di firma elettronica basata sulla crittografia a chiave pubblica si compone dei seguenti algoritmi:

- Un **algoritmo per la generazione della chiave**
- un **algoritmo di firma**
- un **algoritmo di verifica**

ALGORITMO PER LA GENERAZIONE DELLA CHIAVE

Seleziona in modo casuale una chiave privata da un insieme di possibili valori, e restituisce una coppia di chiavi, la chiave privata con cui si firma il documento e la corrispondente chiave pubblica di verifica della firma.

ALGORITMO DI FIRMA

L'algoritmo di firma crea una firma elettronica che dipende dal contenuto del documento a cui deve essere allegata, oltre che dalla chiave dell'utente.

Una coppia (documento, firma) rappresenta un documento firmato, ovvero un documento a cui è stata allegata una firma.

ALGORITMO DI VERIFICA

Presi in input un messaggio, la chiave pubblica e la firma, accetta o rifiuta la firma che compare nel messaggio.

Sono richieste le seguenti due proprietà:

- l'autenticità di una firma generata da un messaggio fisso e da una chiave privata deve essere verificata facendo uso della corrispondente chiave pubblica.
- dovrebbe essere impossibile generare una firma valida per un messaggio senza avere a disposizione la chiave privata.

L’impiego della Firma Digitale permette di **snellire** significativamente i rapporti tra Pubbliche Amministrazioni, i cittadini o le imprese, riducendo drasticamente la gestione in forma cartacea dei documenti, proprio come indicato nelle Linee Guida per l’utilizzo della Firma Digitale, emanate da AGID (Agenzia per l'Italia Digitale, ex DigitPA)

VERIFICA DELL'AUTENTICITÀ

Chiunque può verificare l'autenticità di un documento:

- decifra la firma del documento con la *chiave pubblica del mittente*, ottenendo l'impronta digitale del documento,
- confronta quest'ultima con quella che si ottiene applicando la funzione hash al documento ricevuto;
- se le due impronte sono uguali, l'autenticità e l'integrità del documento sono garantite.

OPERAZIONI DI FIRMA E VERIFICA

Le operazioni di firma e di verifica possono essere demandate ad appositi programmi forniti, in caso di firme elettroniche avanzate o qualificate, dall'ente certificatore oppure dal proprio provider di posta elettronica, che, con una semplice configurazione, le effettuerà automaticamente.

RISCHI PER LA SICUREZZA

- Tutti i crittosistemi a chiave pubblica e privata si basano sul fatto che la chiave privata non sia divulgata. Una chiave privata può essere memorizzata sul computer dell'utente a cui è stata rilasciata, e protetta da una password locale, ma ciò comporta due svantaggi:
- l'utente può firmare solo documenti su quel particolare computer;
- la sicurezza della chiave privata dipende interamente dalla sicurezza del computer.

SICUREZZA DEL SISTEMA

Perché il sistema risulti sicuro, è necessario che solo l'utente stesso *e nessun altro* abbia accesso alla chiave privata. Il modo più semplice per ottenere questo è far sì che l'unica copia della chiave sia "in mano" all'utente (il quale deve impedirne l'accesso a terzi).

UTILIZZO DI SMART CARD

Un’alternativa più sicura consiste nel memorizzare la chiave privata su una smart card.

Molte smart card sono progettate per resistere efficacemente alla distruzione.

l’hash calcolato a partire dal documento viene inviato alla smart card, la cui CPU firma l’hash usando la chiave privata in essa memorizzata, e restituisce l’hash firmato. Prima di ogni utilizzo, l’utente deve attivare la sua smart card inserendo un numero identificativo personale o codice PIN. Anche se non è implementato su tutti i dispositivi, è possibile programmare la smart card in modo che la chiave privata non sia accessibile all’esterno.

In caso di furto, chi entra in possesso del dispositivo avrà comunque necessità del codice PIN per generare una firma digitale; l’utente che subisce il furto, procede immediatamente a revocare la validità del certificato collegato alla sua smart card.

CARTA NAZIONALE DEI SERVIZI(CNS)

- strumento che consente l'identificazione certa dell'Utente (Titolare del Certificato) in rete ai servizi on-line ed ai siti web della Pubblica Amministrazione, del Registro Imprese, INPS, ex- Inpdap, Equitalia ecc.
- La CNS è sempre più richiesta sia dai cittadini che dalle aziende e per alcune categorie professionali, come avvocati, geometri, architetti ecc.
- È diventato uno strumento necessario per autenticarsi ai propri punti di accesso telematici o scambiare informazioni con le PA.
- Il Certificato CNS viene rilasciato su supporto Smart/SIM Card unitamente al certificato di Firma Digitale.

	Firma autografa	Firma elettronica
Creazione	Manuale	mediante algoritmo di creazione
Apposizione	sul documento: la firma è parte integrante del documento	fuori dal documento (autenticazione attraverso user id o password o come allegato)
Verifica	confronto con una firma autenticata: metodo insicuro basato su perizia calligrafica	uso di valutazioni tecniche (metodo insicuro) o mediante algoritmo di verifica pubblicamente noto e certificazione (metodo sicuro)
Documento copia	distinguibile	Indistinguibile
Validità temporale	illimitata	limitata
Automazione dei processi	non possibile	possibile


GRAZIE!