PILLOLE DI VIAGGIO PER PARTIRE ALL'ESPLORAZIONE DEL MONDO DEI SIGILLI E DELL'ARTE DI DISTINGUERSI

Questa iniziativa è inserita nel programma
QUANTE STORIE NELLA STORIA 2023

https://patrimonioculturale.regione.emilia-romagna.it/

quantestorienellastoria

Quante storie nella Storia

QUANTE STORIE NELLA STORIA

8-14 MAGGIO 2023

22ª Settimana della didattica e dell'educazione al patrimonio in Archivio

L’uso del sigillo nei documenti medievali e moderni

a cura di Francesca Del Giacco

Cos'è un sigillo? Nella enciclopedia Treccani leggiamo che il termine “sigillo” (dal latino “sigillum” diminutivo di “signum”, segno) indica una “impronta ottenuta su un supporto malleabile mediante l’apposizione di una matrice recante i segni distintivi di un’autorità, di una persona fisica o morale (una figura, uno stemma, una o più iniziali, o una legenda), per testimoniarne la volontà certificatrice”. Per quale motivo veniva apposto un sigillo sui documenti? Nel mondo greco e latino il sigillo aveva soprattutto una funzione di tutela dell’integrità del testo e di individuazione certa dei testimoni (che avevano messo il proprio sigillo): per verificare l’autenticità di un documento valore prevalente veniva infatti riconosciuto alla sottoscrizione autografa e alla scrittura dello scrivano. Durante il Medioevo, invece, a causa del progressivo processo di de-alfabetizzazione, il sigillo divenne prevalente ed assunse quasi la stessa valenza di una firma in quanto comprensibile da tutti, anche da chi non sapeva né leggere né scrivere. Più tardi (dal Quattrocento)

riassunse rilevanza la sottoscrizione autografa ma ormai era a tal punto consolidata l'importanza del sigillo - soprattutto in documenti emanati da una autorità pubblica o ecclesiale (proprio come avviene ai giorni nostri) – che ne rimase diffuso l'uso. Quanto era grande un sigillo? Le dimensioni variavano molto: tuttavia possiamo dire che, per solito, quelli in metallo oscillavano tra i 30 e i 40 mm. Durante il X secolo ne furono impressi di 70 mm, arrivando ai 135 mm durante il Quattrocento.

Le materie più comuni per la preparazione dei sigilli erano la cera o il metallo (quasi sempre il piombo): non mancarono tuttavia anche sigilli in oro (noti già ai tempi di Carlo Magno) limitatamente però a documenti particolarmente solenni ed emanati, per lo più, da re e imperatori …. ma non si difettava in arguzia! I sigilli in oro massiccio erano una rarità: nella maggior parte dei casi si trattava di lamine d'oro che nascondevano un cuore interno di materiale ben più povero, quale ad esempio il semplice gesso. I sigilli in metallo erano chiamati anche bullae per la forma quasi sferica che avevano prima di essere impressi, termine dal quale derivò poi il nome del documento sigillato in questo modo: bolla papale, bolla di canonizzazione, bolla di scomunica, ecc…

I sigilli in cera erano colorati. Oltre a un colore naturale (quasi bianco) o giallastro erano utilizzati anche il rosso (ottenuto mescolando la cera con l'ossido di piombo o con il cinabro) o il verde (ottenuto mescolando la cera con l'ossido di rame): quest'ultimo colore era utilizzato insieme a fili di seta colorati dalla cancelleria di Filippo Augusto di Francia per distinguere i documenti a carattere permanente. Il colore rosso era tipico dei sigilli segreti e dei segnetti ovvero di piccoli sigilli ottenuti mediante l'impressione della forma negativa dell'anello che il signore portava al dito (come vediamo fare in tanti film). Quando usati per sigillare un documento ripiegato in più parti, i sigilli in ceralacca dovevano essere "rotti" per poter accedere al contenuto del documento come si vede dal frammento di cui in figura 1.

figura 1: sigillo in ceralacca di colore rosso

Uno dei sigilli in cera più noti è senz'altro l'annulus piscatoris, usato dal Papa per i brevi e per la corrispondenza privata, che prendeva il nome dall'immagine dell'Apostolo nell'atto di gettare le reti con, lungo il bordo dell'immagine, il nome del pontefice (figura 2).

figura 2: esempi di annulus piscatoris

Anche forma e impronta dei sigilli erano diverse: di forma prevalentemente tonda, se ne trovano tuttavia anche in forma ogivale (utilizzato in particolare da ecclesiastici o da corporazioni o confraternite con l'immagine del santo protettore), in forma di scudo (a richiamare lo stemma gentilizio dei nobili), quadrata, esagonale o ottagonale.
A seconda della forma, abbiamo poi diversi "tipi" di sigillo: di tipo araldico (con figura del blasone), di tipo monumentale (con strutture architettoniche quali una chiesa o un castello),

di tipo navale, di tipo agiografico o antropomorfo, di tipo fantastico (con figura di animale, segno geometrico o una stella) e tanti altri … di quelli di tipo equestre (con figura di un nobile abbigliato elegantemente) ne esistevano ben tre sotto-tipi (con veste da parata, da guerra o da caccia)!

A seconda di come erano apposti al documento i sigilli potevano essere aderenti o pendenti: nel primo caso aderivano direttamente al documento, nel secondo invece pendevano da esso attraverso l'uso di una cordicella di canapa, di fili di seta o di strisce di pergamena. Per evitare che il supporto si strappasse, in quest'ultimo caso il lembo inferiore del supporto poteva essere ripiegato a formare una plica (figura 3).

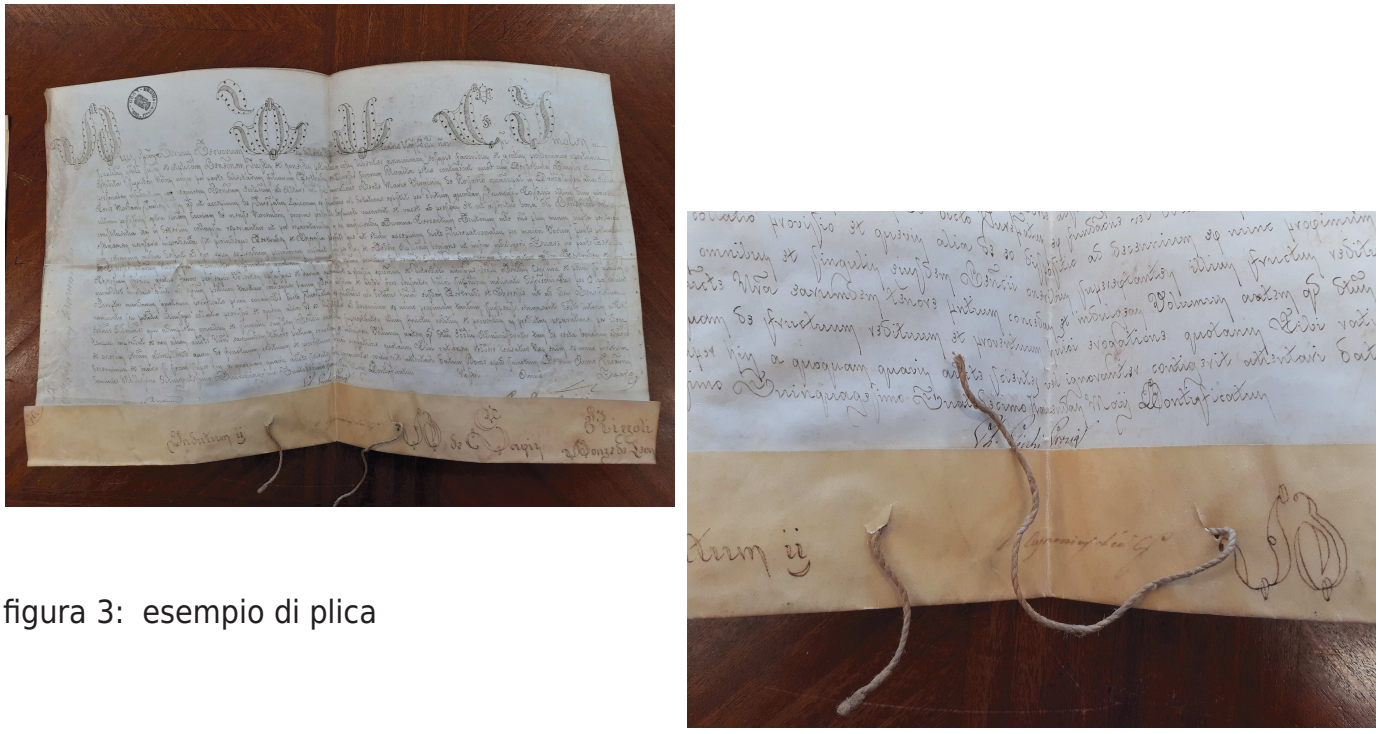
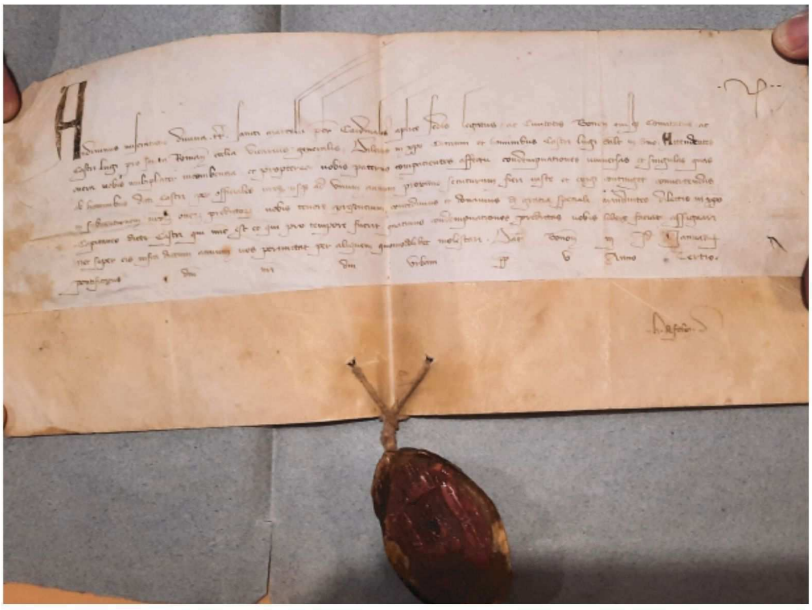


figura 3: esempio di plica



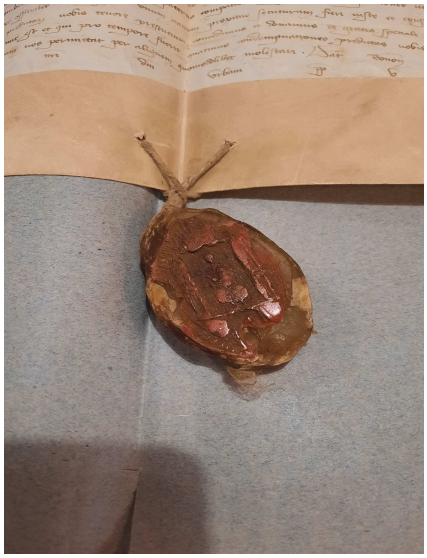


figura 4: esempio di sigillo pendente

A partire dal Quattrocento si diffonde l’uso di proteggere i sigilli di cera pendenti mediante una custodia o teca di metallo, di legno oppure di pergamena.

Per i documenti in carta, a partire dal Cinquecento, entrò in uso un tipo particolare di sigillo, denominato sigillum sub charta, ottenuto appoggiando un pezzetto di carta sullo strato di cera versato direttamente sul documento e imprimendo il sigillo sul pezzetto stesso: nascono così piccole opere d’arte, vere e proprie perle d’archivio (figura 5). Questo tipo di sigillo può essere considerato l’antenato degli attuali timbri a inchiostro e timbri a secco che lasciano una impronta direttamente sul foglio di carta mediante inchiostro nel primo caso e mediante una compressione meccanica nel secondo (sono questi i timbri che possiamo

trovare sulle vecchie carte di identità o sulle vecchie patenti o sui vecchi certificati d’anagrafe dei Comuni).

figura 5: esempi di sigillo sub charta

Nei sigilli poteva essere presente anche una legenda ovvero una scritta composta di solito dal nome o dal titolo della persona proprietaria del sigillo: può consistere in un una invocazione, in un motto o simile. Per solito essa si svolge in senso orario a ridosso dell'impronta o nell'esergo (spazio ai bordi lasciato libero dall'immagine dell'impronta). In molti casi le lettere incise cominciano con una piccola croce simbolo di devozione alla divinità.

Ci sono poi altri tipi di sigillo: sottosigillo (sigillo più semplice e più piccolo del principale generalmente apposto sulla stessa striscia di pergamena del primo ma più in basso), controsigillo (impronta fatta sullo stesso sigillo ma nel retro per completare la convalida e/o per evitare falsificazioni), sigillo minore (di dimensioni ridotte appartenente a una autorità pubblica o a una istituzione), sigillo segreto (impresso sulla cera di colore rosso appartenente ad una persona fisica e utilizzato per i documenti che non passavano attraverso gli uffici di cancelleria) e segnetto (il più piccolo dei sigilli che si otteneva premendo l'impronta dell'anello – annulus signatorius – su lettere e documenti per lo più di carattere familiare).

Infine, quanti erano i sigilli su di uno stesso documento? Per solito, uno. Quando però dovevano intervenire più attori,

allora ne troviamo uno per ogni sottoscrittore: a volte anche tantissimi!

figura 6: esempio di documento con più sigilli

Per chi desiderasse approfondire l’argomento, consigliamo la lettura di “Il documento medievale e moderno. Panorama storico della diplomatica generale e pontificia”, F. De Lasala S.I. – P. Rabikauskas S.I., Editrice Pontificia Università Gregoriana/Istituto Portoghese di S. Antonio, Roma, 2003.

Il monogramma

a cura di Gabriella Cainazzo

Il termine «monogramma» viene dal latino tardo *monogramma*, ed è parola ricalcata sull'aggettivo greco *monogrammatos* (μονογράμματος, «formato di una sola lettera»), composto di *mono*- (μονο-, «uno solo») e *gramma* (γράμμα, «segno, figura, lettera»); indica quindi un insieme di più lettere scritte in maniera da essere congiunte e sovrapposte fra di loro, così da risultare in un unico segno grafico, che poi può prendere la forma di una croce o di una figura geometrica - quadrato, rettangolo, cerchio - ed è usato di solito per rendere un nome di persona.

La letteratura storica vuole per lo più che il monogramma tragga le sue origini dalla diffusione della moneta in sostituzione del baratto, usato per i nomi di re e di città incisi sulle monete coniate, comparendo nello specifico verso il V secolo a. C. sulle monete greche. Per questo solitamente si fa risalire il suo uso alle civiltà greca e romana, ma va comunque ricordato anche l'Egitto; in particolar modo abbiamo testimonianze di uso del monogramma sotto la dinastia tolemaica, durante il regno di Tolomeo III Evergete (246-221 a. C.), quando fu così abbreviato sulle monete di

bronzo coniate da questo regnante l'aggettivo chrēstós (Χρηστός), cioè «buono», qualità con cui era appellato. Questo sovrano aveva anch'egli radici ellenistiche, perché discendente di Tolomeo, generale macedone e compagno d'armi di Alessandro Magno che conquistò l'Egitto nel 332-331 a. C., la cui dinastia impose il suo governo sull'Egitto fino al 30 a. C., quando fu definitivamente conquistato dai Romani dopo il regno di Cleopatra.

Questo insieme di lettere congiunte e sovrapposte a formare un solo segno grafico è quindi una "firma" che attraverso l'uso della scrittura (grafemi) e l'ausilio di forme geometriche identifica e rende riconoscibile una persona, un'istituzione, una corporazione o una società. Il suo uso è attestato attraverso fonti materiali e iconografiche con sempre maggior frequenza a partire dalla parte orientale dell'Impero Romano, soprattutto con l'avvento del Cristianesimo che vi ricorre per indicare il nome di Cristo. Il monogramma di Cristo, detto *Chrismon*, è infatti il simbolo cristologico formato da due grandi lettere greche *chi* (X) e *ro* (P) come iniziali per abbreviare il nome Χριστός (*Christos*); a volte il *Chrismon* è affiancato da altre due lettere greche, *alfa* (A) e *omega* (Ω), usate a ricordare Cristo come principio e fine di tutte le cose.

Tutto ciò è a volte inscritto in un cerchio con più raggi, che trae la sua derivazione - per effetto di contaminazione culturale - dalla ruota cosmica di tradizione della civiltà egizia. Il monogramma di Cristo fino all'inizio del III secolo d. C. lo si trova soltanto su sarcofagi, e quindi in contesti di uso privato, e non ancora nell'iconografia dei luoghi di culto cristiani.

Questo certamente anche alla luce del fatto che bisogna attendere l'editto di Milano dell'imperatore Costantino I (313 d. C.) perché sia permesso il culto cristiano in luoghi pubblici. E così si incomincerà a trovare da allora il simbolo cristologico nelle basiliche ma anche sulle monete coniate dallo stesso Costantino (322-333 d. C.) e sugli stendardi militari di tutti gli imperatori - divenuti cristiani - romani e bizantini, come a invocare l'aiuto di Cristo in battaglia e a ricordare a tutti come lo stesso Costantino avesse avuto la visione di quella croce come segno celeste di Dio durante un sogno alla vigilia della battaglia di Ponte Milvio da cui uscì vittorioso.

Evidentemente questo uso da parte dei sovrani si estese ben presto alla composizione appunto di monogrammi realizzati con tutte le lettere del loro intero nome, che divennero l'equivalente della loro firma sui documenti ufficiali per

garantirne l’autenticità, il simbolo del loro potere nei monumenti fatti costruire, il loro emblema sulle monete fatte coniare.

Tra le prime testimonianze di monogrammi utilizzati dai sovrani che hanno regnato sul nostro territorio, si ha il semplice *chrismon* utilizzato per il mausoleo di Galla Placidia a Ravenna e in molte chiese fatte innalzare da Giustiniano; ma un primo, splendido esempio di monogramma personale e completo è offerto dal re degli Ostrogoti Teoderico, il cui nome *Theodericus* ci è tramandato in forma monogrammatica dalla moneta da un quarto di siliqua da lui fatta coniare (493-518 d. C.) e dai capitelli riutilizzati nelle colonne del Palazzetto Veneto di Piazza del Popolo, sempre a Ravenna.

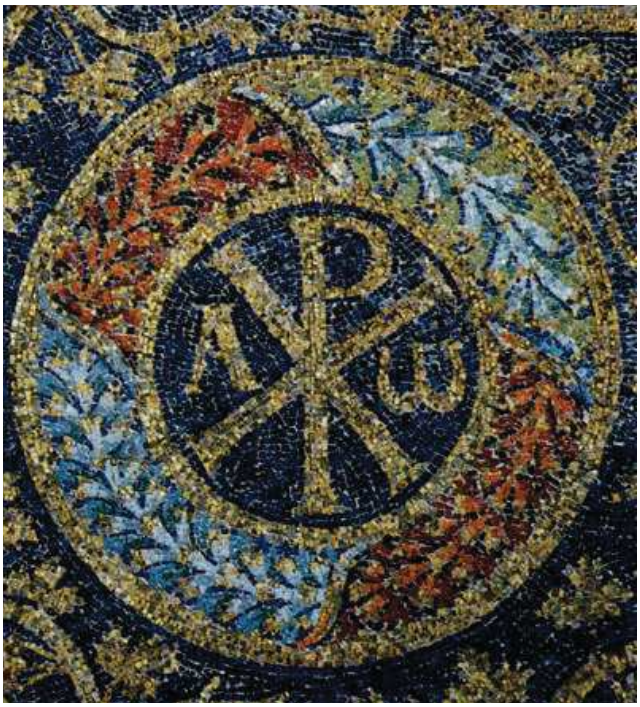


Figura 1: il chrismon del mausoleo di Galla Placidia a Ravenna.

Figura 2: un *chrismon* costantinopolitano dell’epoca di Giustiniano.

Figura 3: moneta con il monogramma di Teoderico.

Figura 4: uno dei capitelli col monogramma di Teoderico in Piazza del Popolo a Ravenna.

Tanto è rimasta forte la consapevolezza dell'antichissima tradizione di questa presenza nei monumenti ravennati, che ancora all'inizio del XX secolo, quando fu ricostruita l'antica cappella arcivescovile, per riempire uno spazio altrimenti vuoto perché erano andati perduti i mosaici originali, si volle omaggiare l'arcivescovo Pasquale Morganti (1904-1921) disegnandogli un monogramma con il suo nome all'uso antico (*Paschalis*).

Figura 5: il monogramma della Cappella Arcivescovile di Ravenna dedicato a Pasquale Morganti.

Il monogramma medievale noto ai più, sia per eleganza sia per equilibrio dal punto di vista estetico, è certamente quello dell'imperatore Carlo Magno. Si tratta della sintesi grafica del nome *Karolus* in forma di croce; questo non soltanto perché egli fu il fondatore del Sacro Romano Impero, ma perché - come sappiamo in particolare da Eginardo, suo biografo -

Carlo Magno di fatto non scriveva, e per dare autenticità alla sua firma apponeva soltanto un tratto autografo a completare la lettera «O».

L'antica città di Aquisgrana, capitale dell'impero di Carlo Magno (l'odierna Aachen in Germania), ha incastonato nella pavimentazione delle aree pedonali che circondano l'antica cappella palatina, oggi cattedrale, rotonde placchette in ottone con impresso il monogramma carolingio.

Come possiamo vedere dalle presenti immagini, abbiamo attestazioni di documenti con il monogramma autografo di Carlo Magno anche nella nostra regione, e poco lontano da noi: infatti alcune pergamene sono conservate presso l'abbazia di Nonantola, in provincia di Modena, e altre presso l'Archivio di Stato di Modena.

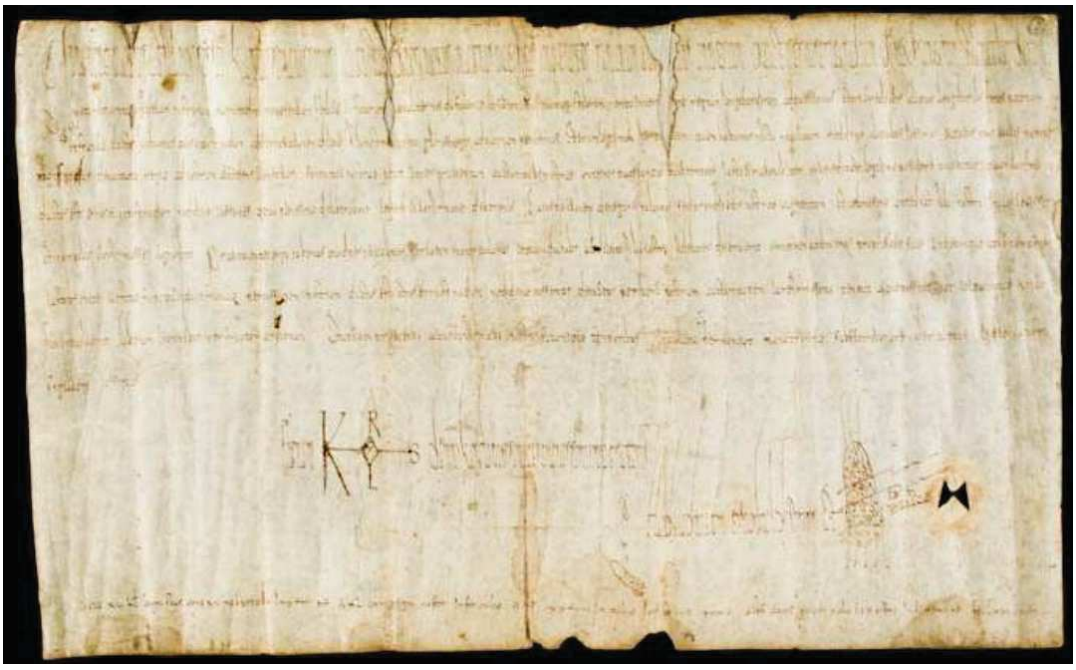


Figura 6: il documento dell'808 dell'Archivio di Stato di Modena (*Casa e Stato*, Membranacei, cass. 1, doc. 5) recante il monogramma di Carlo Magno.

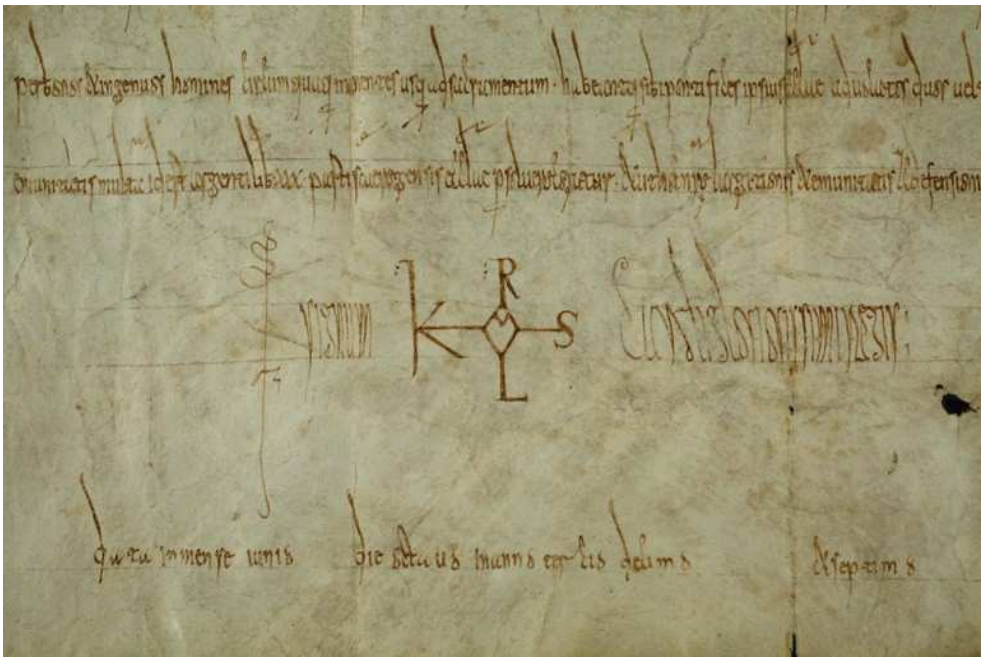


Figura 7: un monogramma di Carlo Magno (particolare ingrandito).

Il tardo Medioevo e il primo Rinascimento sono i periodi di massima fioritura dell'uso del monogramma sotto vari aspetti: oltre a rimanere simbolo dei nomi di sovrani, viene sempre più utilizzato per altri fini pratici, divenendo spesso parte dei *signa* dei notai, ricorrendo nell'iconografia degli emblemi delle corporazioni artigiane e delle compagnie o congregazioni laiche e religiose, negli stemmi delle famiglie, in dipinti e in affreschi a rappresentare il nome dell'artista che ha realizzato l'opera o del committente che l'ha pagata, nei libri a stampa a identificare l'editore, nelle filigrane della carta, negli *ex libris* a indicare il proprietario del volume, nonché con scopi puramente ornamentali - a mo' di vezzo - come nella corrispondenza privata.

Straordinario successo ebbe il cosiddetto “monogramma bernardiniano”, cioè le lettere «IHS», documentato fin dai primi secoli dell’era cristiana come *nomen sacrum* per abbreviare il nome greco di Gesù (*iota*, *eta* e *sigma* come prime tre lettere di ΙΗΣΟΥΣ, “Iesous”), e diffuso a partire dal 1424 dalla predicazione del frate francescano san Bernardino da Siena nella forma in cui la sigla è circondata da un sole a dodici raggi. Lo stesso sant’Ignazio di Loyola lo scelse prima come proprio sigillo e poi come simbolo della Compagnia di Gesù, per cui tuttora lo si trova in tantissime chiese dei Gesuiti.

Figura 8: una formella in marmo con il monogramma bernardiniano.

Figura 9: il monogramma del pittore tedesco Albrecht Dürer (1471-1528)

Figura 10: il monogramma del pittore francese Henri de Toulouse-Lautrec (1864-1901).

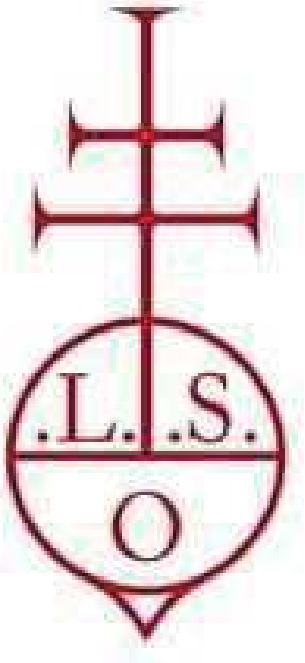


Figura 11: l’emblema della casa editrice Olschki, fondata nel 1886.

Figura 12: la filigrana di una cartiera del XVIII secolo.

Nell’età contemporanea, segnata dalla rivoluzione industriale e dalla nascita delle moderne imprese commerciali pubbliche e private, il concetto stesso del monogramma ha conosciuto nuova vita nella forma del logo (abbreviazione del termine *logotipo*, dal greco λόγος-, *logos*, che significa “parola”, e τύπος-, *typos*, che significa “lettera”). La moderna grafica pubblicitaria ha contribuito a rivitalizzare e a diffondere il monogramma come simbolo delle case di moda, dei prodotti cosmetici e di tanti altri oggetti di uso quotidiano; spesso il logo moderno si presenta propriamente come un acronimo, o sigla, utilizzando soltanto le iniziali delle diverse parole.

Un esempio specifico per le imprese private è fornito dall’emblema della società statunitense General Electric, fondata da Thomas Alva Edison, che fin dal 1898 utilizza un logo con le sue iniziali costantemente aggiornato per stare al passo delle tendenze artistiche.

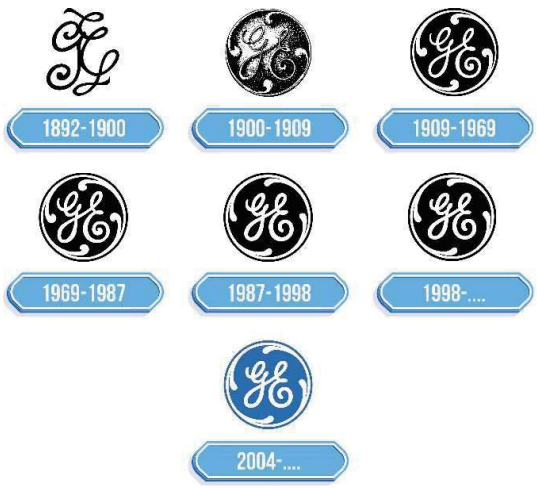


Figura 13: l’evoluzione grafica del logo della General Electric.

Figura 14: una serie di loghi di alcune delle più note imprese contemporanee.

In conclusione, per rendere omaggio a due fra le più importanti istituzioni del nostro Stato, è bello ricordare i loghi - estremamente sobri e classici nelle loro forme - del Senato della Repubblica e della Camera dei Deputati.

Figura 15: gli emblemi del Senato delle Repubblica e della Camera dei Deputati.

E adesso spazio alla tua fantasia…

...costruisci il tuo MONOGRAMMA!

Firma digitale e sigillo elettronico

a cura di Daniele Margotti

Tutto inizia con la crittografia

Luca e Paolo vogliono inviarsi messaggi in codice attraverso Internet, ma non hanno modo di scambiarsi, tramite un canale sicuro, una chiave crittografica senza il rischio che venga intercettata e utilizzata per leggere le loro comunicazioni segrete. Come possono fare? Molto semplice: utilizzando la **crittografia a chiave asimmetrica**!

Con questo tipo di crittografia non è necessario avere una chiave condivisa e scambiarsela: ognuno genera una propria coppia di chiavi, una **pubblica** (disponibile a tutti) e una **privata** (da tenere segreta e al sicuro), le quali vengono utilizzate rispettivamente per criptare e decrittare i messaggi. Le due chiavi sono legate fra loro, ma dalla chiave pubblica è **impossibile** risalire alla chiave privata: questo perché sono create utilizzando due numeri primi molto grandi, e nella chiave pubblica è presente solo il loro prodotto. Dal punto di vista matematico la moltiplicazione è un’operazione molto facile, mentre non esiste un’operazione altrettanto veloce per individuare tutti i fattori primi di un numero, se non procedendo per tentativi; e se i numeri primi

sono molto grandi (non i classici numeri primi che conosciamo, come 3, 5, 7, 11 o 13, ma parliamo di numeri di cento cifre), anche i computer più potenti possono metterci anni o decenni. Le funzioni matematiche che stanno alla base della crittografia a chiave asimmetrica garantiscono che i testi criptati con la chiave pubblica possono essere decrittati **solo ed esclusivamente** con la corrispondente chiave privata. Così Luca può utilizzare la chiave pubblica di Paolo per mandargli un messaggio: se questo dovesse essere intercettato da un pirata informatico, quest'ultimo non sarà in grado di leggerlo, perché non ha la chiave privata di Paolo.

Facciamo un esempio?

Questa è la prima strofa della poesia "San Martino" di Giosuè Carducci, criptata con una chiave pubblica; senza la chiave privata, è impossibile risalire al contenuto.

La nebbia a gl'irti colli piovigginando sale, e sotto il maestrale urla e biancheggia il mar;
-----BEGIN PGP MESSAGE----- Version: BCPG v1.39 hI4DGGlj3Ykpg2sQAf9mSHtIuOp0CZUUwWWPZV8EjPxwnNnN

```
haU0C7fuDwAAkCsxTrUWSfGGXU1Wpg2ERCvQ1ni7N0YVN7GZ
O0fY8wJFAf4holgXvvQS8FnTnwcr/q/gw+v9eUGPkXs35EUL
MKSKJxlhGCIMrdRZf4W0RC9uc5exzhk03O1JopmrnZpZKDZl
0qUBMqrsQkhCPxhsLC7/wcXFxcWKCjiR6NJ1P89+T3CqePSE
VC7hOrtVOH7qvztsD4CQM+PaOHgo8qIWblKypAB9IHfPYJDu
ZjmfTaQHlfyirJS7d7VcMnILDuyPvTd+b1Ta5OPWSEY9Zivq
KWv0l2xJ07Ie8F4oG39uyT8lhvEk2Y/4kikIke/kps9XMllM
vsCOrX6tBovddkgAzYmDh1NRUPA8dHw==B3qx
-----END PGP MESSAGE-----
```

L’utilizzo della chiave pubblica, però, non è sufficiente: se il messaggio viene intercettato, pur non essendo possibile leggerlo, può comunque essere sostituito con un altro messaggio, perché la chiave pubblica di Paolo è disponibile a tutti, pertanto Paolo non ha la certezza che il messaggio arrivi proprio da Luca. Quindi Luca dovrà codificare il suo messaggio utilizzando **anche** la sua chiave privata. Solo così Paolo potrà verificare che il messaggio sia effettivamente di Luca: utilizzando la chiave pubblica di Luca, infatti, Paolo avrà la certezza che il messaggio è stato autenticato con la chiave privata di Luca, che nessun altro possiede.

Nella vita di tutti i giorni utilizziamo già la crittografia a chiave asimmetrica senza accorgercene; sono i programmi a gestirla in maniera trasparente, ad esempio quando

visitiamo i siti che iniziano con https:// (e sono contraddistinti da un lucchetto), oppure quando usiamo sistemi di messaggistica come Whatsapp:

Arriviamo alla firma digitale

Torniamo all'esempio di prima: e se Luca decidesse di usare solo la sua chiave privata? In questo caso il messaggio sarebbe leggibile da tutti (tramite la sua chiave pubblica), ma sarebbe attribuibile solo a lui (perché nessun altro ha la sua chiave privata): Luca ha quindi **firmato digitalmente** quel messaggio.

Nella realtà di tutti i giorni, i "certificati di firma" (costituiti da chiave pubblica e privata), per avere valore legale, non possono essere generati dalle singole persone, ma vengono

rilasciati da Enti o aziende (chiamati Autorità di Certificazione) come la Camera di Commercio, le Poste Italiane, Aruba, e altri, riconosciuti a livello nazionale.

Il certificato di firma digitale viene anche controfirmato dall'Autorità di Certificazione che lo rilascia, al fine di attestare l'identità del titolare: all'interno del certificato di firma, infatti, sono indicati il nome, il cognome e il Codice Fiscale del titolare.

Il certificato di firma digitale viene solitamente rilasciato in una Smart Card con microchip, come questa:

La chiave privata rimane all'interno della Smart Card e non può essere visualizzata, al fine di garantire la sicurezza della firma; inoltre l'utilizzo della Smart Card richiede l'inserimento di un PIN.

Ma c'è un problema: la crittografia a chiave asimmetrica è lenta, richiede una grossa potenza di calcolo, spesso bisogna firmare file molto grandi (anche svariati Megabyte), e il

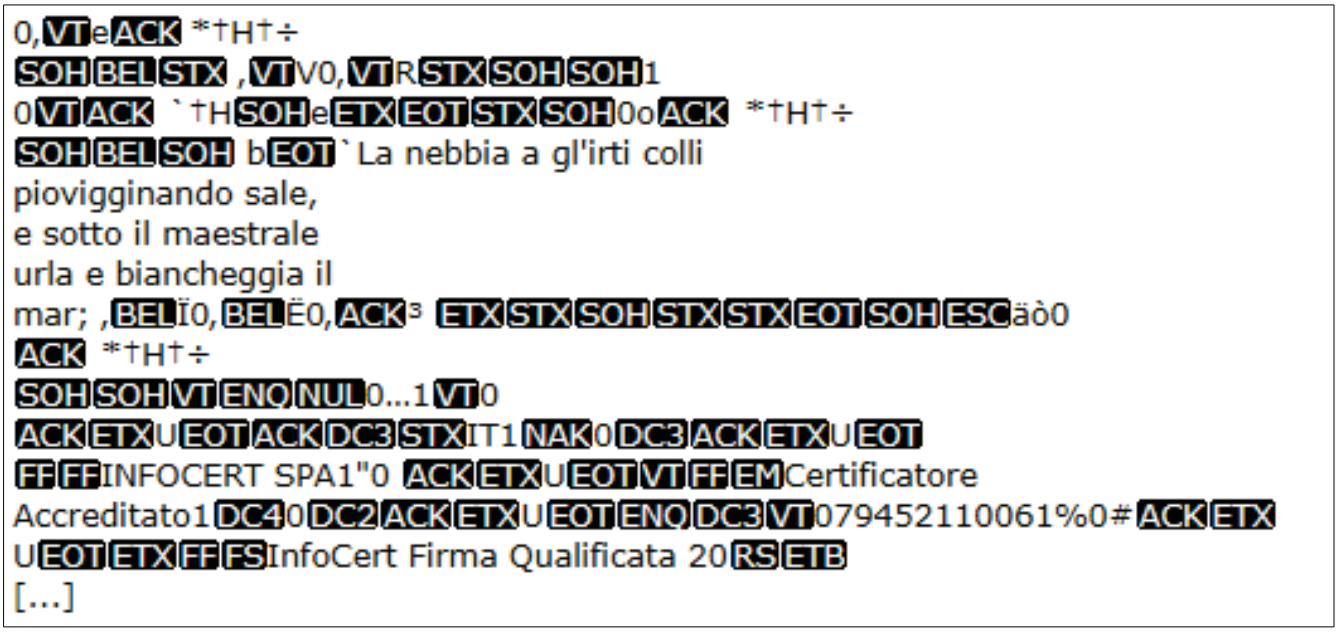
microchip non riesce a farlo. Quindi si è stabilito di firmare **l’impronta** del file, anziché il file stesso.

L’impronta (in gergo tecnico, “hash”) è una stringa esadecimale (cioè, in base 16) di lunghezza fissa, generata con funzioni matematiche che garantiscono che due file non possano avere la stessa impronta, e che una minima variazione nel contenuto del file comporti la generazione di un’impronta completamente differente. La lunghezza è di 256 bit, e corrisponde a un numero enorme di combinazioni: $1{,}1579 \times 10^{77}$, che è un numero di 78 cifre, sufficiente per far sì che ogni possibile file abbia un’impronta diversa; per fare un confronto, il numero stimato di atomi nell'universo è di circa 10^{80}. Nella tabella qui di seguito si può vedere come una piccola modifica al testo (la “m” iniziale di “maestrale” che passa da minuscola a maiuscola) generi un’impronta completamente diversa:

La nebbia a gl'irti colli piovigginando sale, e sotto il **maestrale** urla e biancheggia il mar;	La nebbia a gl'irti colli piovigginando sale, e sotto il **Maestrale** urla e biancheggia il mar;
Impronta: **78B23BC29E656A76DE24197646385714D9C06839ADF7DD42F8594B8D6B85E1FA**	Impronta: **588497EA9B40FFDDEC6BABA48F583611D3F857CFB5EE4B615061E02EE7949114**

Torniamo alla nostra Smart Card: il microchip riesce a firmare velocemente e senza problemi una stringa di 256 bit, e le funzioni matematiche di calcolo dell'impronta ci garantiscono che firmare l'impronta equivale a firmare il documento di partenza.

Ecco come si presenta un file firmato:

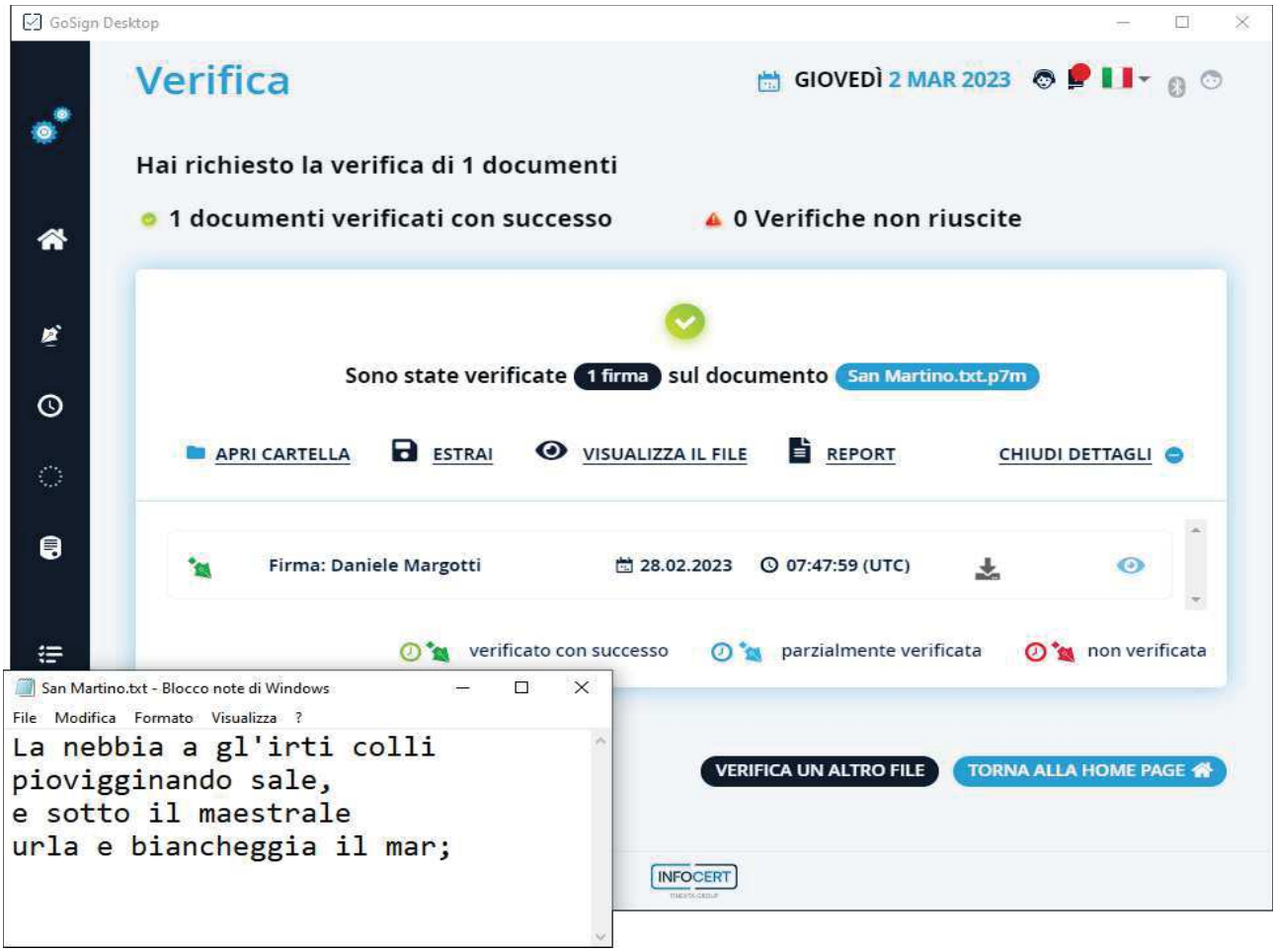


Il testo originale è leggibile (a differenza di un testo crittografato), e quei caratteri incomprensibili sono la chiave pubblica del certificato di firma (necessaria per verificare la firma) e l'impronta firmata.

Non spaventatevi!

Quello è solo il contenuto in "linguaggio macchina", e nessuno vi chiederà mai di interpretarlo.

I programmi di gestione e verifica della firma digitale sono in grado di mostrare, automaticamente e in maniera chiara, sia il firmatario che il documento firmato:



Dal punto di vista giuridico, i requisiti che assolve la firma digitale sono:

- **integrità**: la certezza che il documento non sia stato manomesso o modificato dopo la sottoscrizione (perché ogni modifica genera un’impronta diversa);
- **autenticità**: garanzia dell’identità di chi firma, perché i dati del firmatario sono presenti all’interno del certificato di firma rilasciato da un’Autorità di Certificazione;

- non ripudio: il documento informatico sottoscritto ha piena validità legale e non può essere ripudiato dal firmatario.

Concludiamo col sigillo elettronico

Un documento informatico prodotto da una Pubblica Amministrazione è descritto da alcuni dati obbligatori (oggetto, data e numero della registrazione di protocollo, destinatario) ed è composto da uno o più file (ad esempio, una lettera di accompagnamento, una relazione, un preventivo, e così via).

Per “sigillare” nel tempo tutte queste informazioni, e impedire che uno qualsiasi degli elementi venga modificato, si utilizza il **sigillo elettronico**.

Il sigillo elettronico non è altro che un file XML: è stato scelto questo formato perché, al suo interno, è possibile elencare tutti gli elementi che identificano e compongono il documento.

Assieme al nome dell’Ente e ai dati obbligatori, vengono elencati anche i singoli file con la loro impronta (calcolata come abbiamo visto poco fa), e il file XML così generato viene firmato digitalmente. In questo modo, una qualsiasi modifica ad uno degli elementi (sia quelli descrittivi, sia i file

veri e propri) non può essere effettuata senza invalidare il sigillo elettronico; e anche quest'ultimo, essendo firmato digitalmente, non può essere manomesso, garantendo così l'integrità dei dati del documento informatico a cui è associato.

Non esiste solo la firma digitale

Abbiamo parlato della firma digitale, e abbiamo visto i vantaggi e la sicurezza che può garantire.
Tutto questo però non è gratis: ottenere una firma digitale da un'Autorità di Certificazione ha un costo, non solo per il rilascio, ma anche per il rinnovo, visto che per motivi di sicurezza il certificato di firma ha una scadenza di tre anni.
In caso di smarrimento o furto della Smart Card, è possibile richiedere la revoca del certificato, per impedire che qualcun altro firmi al posto nostro: in questo caso le Autorità di Certificazione aggiornano le loro "liste di revoca", in cui sono elencati tutti i certificati revocati o sospesi prima della scadenza, e i software di firma impediranno l'utilizzo di questi certificati.

Nell'ordinamento giuridico italiano sono previste varie tipologie di firme elettroniche.

La prima è la **firma elettronica semplice**, ed è quella che usiamo più spesso. Per firma elettronica semplice si intende un "insieme di dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare". Alcuni esempi sono il nome utente e la password per accedere a un servizio online o alla propria casella di posta elettronica, oppure il PIN del Bancomat. Questo è il tipo di firma più debole, perché non prevede un'identificazione sicura e univoca di chi firma, e quindi non assicura l'autenticità, il non ripudio e l'integrità del documento: in caso di contestazioni, il suo valore probatorio è determinato dal giudice.

Un gradino più sopra c'è la **firma elettronica avanzata**: prevede l'identificazione di chi sta firmando, la corrispondenza univoca tra chi sta firmando e la firma, il controllo esclusivo da parte del firmatario sul sistema di generazione della firma, e l'integrità del documento. L'esempio più comune è la "firma grafometrica", che si realizza con un gesto manuale che emula quello di una firma a penna su un foglio di carta, utilizzando un pennino su un tablet o una tavoletta grafica. Viene detta anche "biometrica" perché il dispositivo su cui si firma è in grado di

registrare i parametri biometrici fondamentali per rendere autentica una firma grafometrica (ritmo, accelerazione, inclinazione, pressione e velocità), oltre al tracciato grafico della firma. I parametri biometrici sono codificati, assieme all'impronta del documento, utilizzando la chiave pubblica di chi fornisce il servizio di firma: in questo modo i dati sono legati in modo indissolubile al documento, ma sono crittografati per evitare che possano essere letti e usati per apporre la stessa firma su altri documenti. In caso di contenzioso, i dati biometrici vengono decrittati con la chiave privata e sottoposti a perizia calligrafica (analogamente a quanto si fa con la firma su carta) per stabilire chi è il vero firmatario. Se invece il dispositivo non è in grado di rilevare i dati biometrici (come il palmare del corriere su cui si firma con un dito), la firma non può definirsi grafometrica.

Un altro esempio di firma elettronica avanzata è la ricezione di un codice OTP (One Time Password) che arriva via SMS sul cellulare del firmatario, e che va comunicato alla controparte per completare la procedura di firma elettronica.

Anche la PEC (Posta Elettronica Certificata) è un esempio di firma elettronica avanzata, in quanto viene rilasciata solo previa identificazione del titolare che la richiede.

Un ulteriore passo nella sicurezza e nella certificazione della firma si ha con la **firma elettronica qualificata**: questa ha tutte le caratteristiche della firma elettronica avanzata, ma deve essere basata su un certificato qualificato rilasciato da un certificatore accreditato e realizzata mediante un dispositivo sicuro per la creazione della firma.
Tra i dispositivi sicuri, oltre alle Smart Card, ci sono i “Token di sicurezza”, ovvero quei piccoli dispositivi che generano codici casuali validi pochi secondi, e che servono ad esempio per confermare l’accesso al proprio Home Banking o l’invio tramite questo servizio di un pagamento o di un bonifico.

Abbiamo poi la **firma digitale**, che ormai conosciamo bene, e che è definita come “un 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 e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici”.

Infine esiste anche la **firma SPID**, che si basa sull'identità digitale del soggetto che la appone. SPID è il Sistema Pubblico di Identità Digitale, utilizzabile per accedere ai servizi online della Pubblica Amministrazione attraverso un'unica credenziale per l'autenticazione, anziché un nome utente e una password diversi per ogni sito. Per utilizzare questa modalità di firma è necessario autenticarsi con SPID sul sito del gestore che offre questo servizio: dopo aver caricato il documento da firmare, questo verrà firmato con il certificato di firma del gestore, il quale avrà però indicato i dati anagrafici del firmatario e la sua volontà di firmare il documento. La firma con SPID è idonea a garantire la sicurezza, l'integrità e l'immodificabilità del documento, così come anche la sua riconducibilità manifesta ed inequivoca all'autore.

Comune di Lugo

Archivio Storico

Biblioteca Comunale Trisi Lugo