SOMMARIO

Introduzione

Spesso la tecnologia, quando è complessa, si presenta avvolta da un'aura misteriosa, quasi magica, che la fa apparire accessibile solo alla stretta cerchia iniziatica degli esperti. Esistono fortunatamente da tempo i divulgatori, una progenie forse ispirata da Prometeo, che rubò il fuoco agli dèi per donarlo agli uomini, che si impegna a infrangere quell'aura e mostrare come i concetti e le idee alle basi del funzionamento della tecnologia possano essere esposti in modo comprensibile e intuitivo per chiunque.

Nel redigere questo fascicolo l'intento è stato proprio quello di far svanire le nebbie attorno a due strumenti che sono divenuti sempre più indispensabili nella nostra quotidianità: la firma e l'identità digitali.

Fare operazioni di questo genere è sempre pericoloso come navigare nello stretto di Messina, rischiando di essere risucchiato dai vortici di Scilla o di Cariddi. Da un lato c'è infatti il rischio di semplificare troppo l'esposizione, venendo criticati dai tecnici per omissioni e banalizzazioni. Dall'altro si può scivolare anche involontariamente in qualche tecnicismo che rimane oscuro per il lettore non esperto.

Il rischio meritava comunque di essere affrontato, poiché su questi argomenti abbondano le risorse per gli addetti ai lavori, ma non è facile trovare materiale divulgativo raccolto in modo organico e completo.

Ci affidiamo quindi all'accoglienza e al giudizio dei lettori, sia tecnici che novizi, dai quali speriamo di ricevere stimoli per un'eventuale riedizione aggiornata.

Capitolo 1

Le firme elettroniche

1.1 UN PO' DI STORIA

Firmare è un verbo latino con due significati. Il primo è rendere saldo, rafforzare, fortificare, ed è usato in riferimento al corpo o a un insediamento, ma anche all'animo umano. Il secondo significato è confermare, assicurare, garantire, provare. Il vocabolario della lingua latina Castiglioni, Mariotti riporta tra gli esempi d'uso un'espressione pregnante di Cornelio Tacito: *"tabulis aliquid firmare"*, confermare qualche cosa con l'autorità dei pubblici registri. Queste parole del più grande storico romano, vissuto quasi 2.000 anni fa, riassumono il significato profondo di un gesto che ha una precisa finalità giuridica e sociale, anche se col passare dei secoli ci è divenuto ormai naturale. Un gesto usato abitualmente da tutti con lo scopo di dare ad un documento la validità e la forza vincolante necessaria in qualsiasi atto negoziale, dal più importante, come il rogito presso un notaio, al più banale, come l'autorizzazione al pagamento con carta di credito sul display di un supermercato.

Vivendo a cavallo tra due epoche, prima e dopo la digitalizzazione, ci troviamo così inaspettatamente ad usare sia documenti cartacei che documenti informatici, e a dover progressivamente abituarci ad abbandonare i primi per i secondi, in quanto più economici e veloci da trasferire, meno ingombranti, più ecologici. E sebbene sullo schermo luminoso un documento informatico sembri identico alla sua copia cartacea, la differenza emerge in modo spiazzante proprio nel momento in cui lo si voglia firmare elettronicamente.

Siamo in realtà vittima di una dimenticanza. Per quanto infatti scrivere ci sembri naturale, avendolo imparato da piccoli, non dovremmo dimenticare che la scrittura è in realtà un'invenzione *tecnologica* dell'uomo. Ed è nata inizialmente per documentare e tener conto dei beni materiali delle classi regali e sacerdotali, quindi poi per fissare le leggi che regolano l'ordinamento sociale, nonché per tramandare tutto ciò che prima era affidato alla memoria e al racconto orale. Essa esiste da più di 5.000 anni e come ogni tecnologia si è evoluta nei secoli cambiando più volte gli strumenti e i supporti materiali. Negli ultimi decenni si sta trasformando ancor più profondamente e rapidamente per effetto della digitalizzazione, un cambiamento davvero epocale per l'umanità. Così, abbandonando sempre più spesso carta e penna a favore di schermo e tastiera, dobbiamo tutti imparare anche un nuovo modo per sottoscrivere i documenti informatici.

La tecnologia che consente di firmare elettronicamente è stata inventata negli anni '70 e si è subito diffusa tra gli specialisti, ma l'utilizzo con valore legale ha richiesto il recepimento da parte delle istituzioni. A tale proposito la normativa italiana può vantare di essere stata tra le prime al mondo, con la L. 15.03.1997, n. 59, a conferire valore giuridico non solo ai documenti ma anche alle sottoscrizioni digitali. In Italia poi abbiamo subito recepito la direttiva comunitaria del 1999 e emanato nel 2005 un Codice dell'Amministrazione Digitale (CAD), per disciplinare il valore giuridico degli atti della pubblica amministrazione. L'applicazione del CAD ebbe subito una importante diffusione anche in tutto il settore privato in quanto consentì alle aziende di digitalizzare una parte significativa della documentazione, specialmente quella fiscale, tramite la "conservazione digitale a norma", facendo quindi nascere uno specifico mercato dei servizi di conservazione.

Infine, per favorire il commercio e le transazioni elettroniche in tutto il mercato unico europeo, nel 2014 il Parlamento e il Consiglio UE emanano il Regolamento eIDAS (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices), che viene direttamente applicato a tutti gli stati membri senza la necessità di atti di recepimento da parte di essi. Questa normativa, per il suo carat-

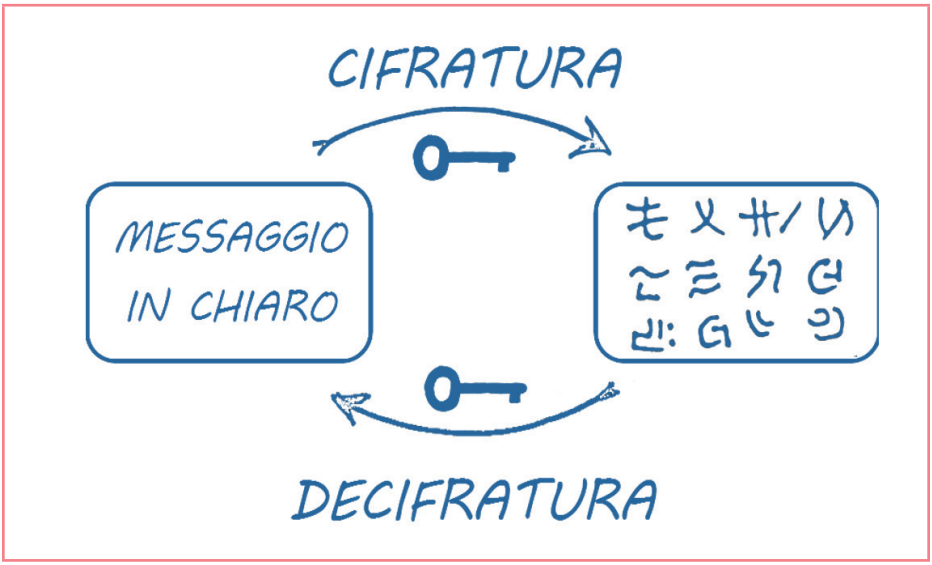
tere innovativo e per i livelli di sicurezza garantiti, è di fatto considerata un punto di riferimento ineludibile e un modello per la regolamentazione anche fuori dall'UE. Il Regolamento eIDAS intende realizzare una piena interoperabilità giuridica e tecnica tra i paesi membri dell'UE per le attività di identificazione, autenticazione e sottoscrizione. Esso cioè tratta già anche dell'identità digitale, non solo della firma, poiché le due tecnologie sono strettamente correlate. Lo scopo ultimo è quello di instaurare la certezza giuridica nell'ambito delle transazioni online, al fine di diffondere fiducia verso l'uso delle transazioni elettroniche, nei consumatori e nelle imprese.

1.2 CENNI TECNICI

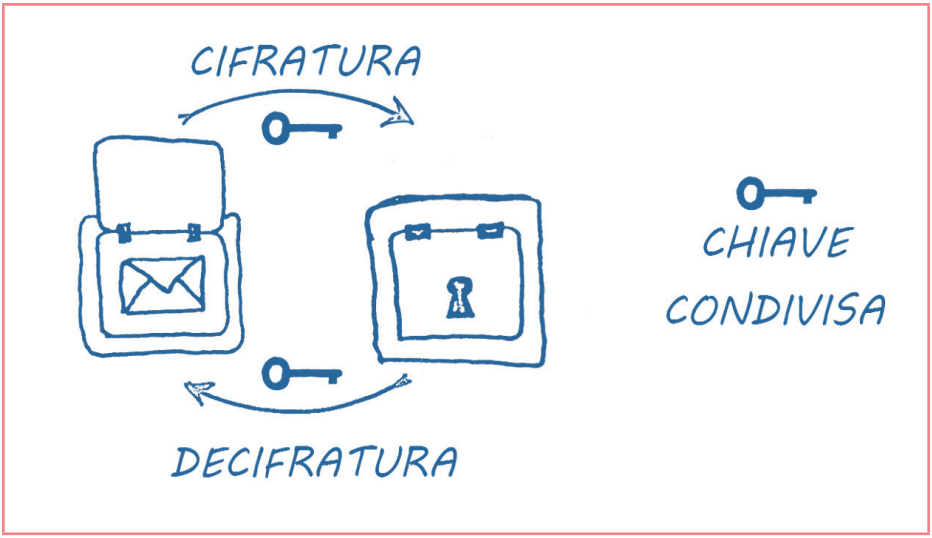
Per parlare della tecnologia su cui si basa la firma elettronica è necessario qualche accenno alla crittografia, materia avvolta da un oscuro alone di mistero. Non ci addentreremo nei dettagli e nelle formule matematiche, ma cercheremo di dare una rappresentazione semplice e quanto più fedele dei meccanismi fondamentali che riguardano la firma elettronica.

Le operazioni informatiche complesse usate in crittografia si chiamano algoritmi crittografici e alcuni di essi consentono di trasformare un messaggio in modo che non sia più comprensibile a un avversario che lo intercetti. Si parla così di "messaggio in chiaro" e di "messaggio cifrato" per distinguere il messaggio originale, prima dell'operazione di cifratura, e il risultato finale.

L'operazione che viene effettuata utilizza inoltre un valore segreto, una sorta di password, che viene chiamata **chiave crittografica**, condivisa dal mittente e dal destinatario. Quest'ultimo può usare la chiave crittografica per effettuare l'operazione inversa e decifrare il messaggio cifrato riportando il messaggio "in chiaro". In questo modo chiunque intercetti il messaggio cifrato, non conoscendo la chiave crittografica, non può venire a conoscenza del contenuto.

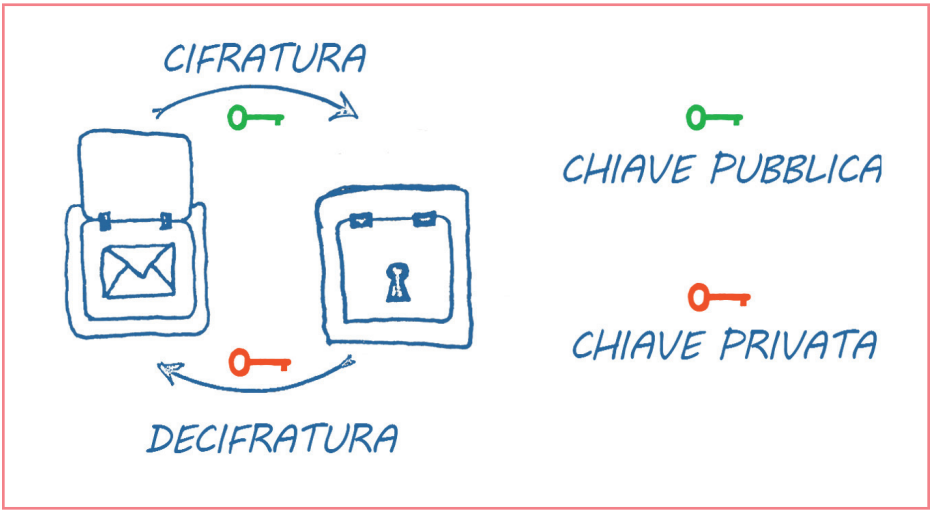


L'uso del termine chiave è una metafora abbastanza efficace. Possiamo immaginare infatti che il messaggio sia chiuso in uno scrigno e che il mittente e il destinatario posseggano ciascuno una copia della chiave che apre e chiude lo scrigno. Chi intercetta lo scrigno non potendolo aprire non è in grado di leggere il messaggio.

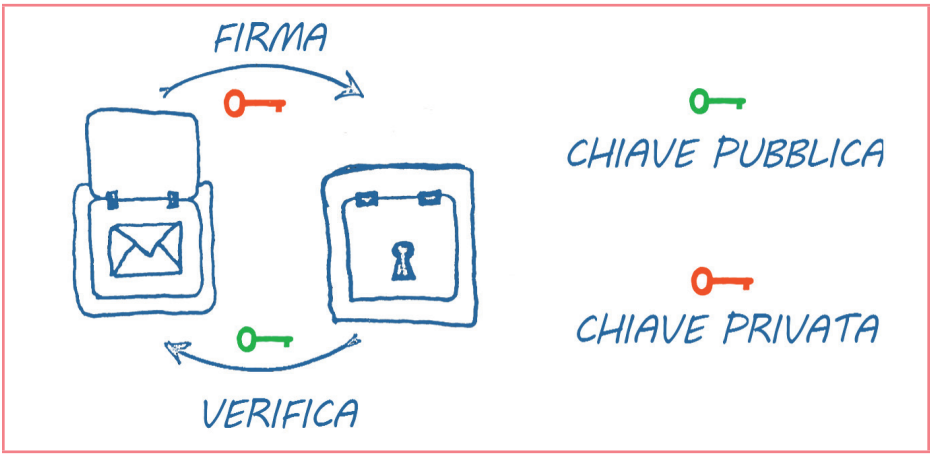


Fin qui abbiamo descritto la crittografia detta **simmetrica**. Ma nel 1976 è stata inventata una nuova tecnica crittografica detta **asimmetrica**, o a chiave pubblica. Il suo funzionamento si basa sull'uso di due chiavi differenti e correlate, progettate in modo tale che se una delle due chiude lo scrigno, solo l'altra può aprirlo.

In questo modo il destinatario conserva la chiave segreta che apre lo scrigno, detta **chiave privata**, mentre distribuisce una copia dell'altra chiave, la **chiave pubblica**, che può aprirlo, a chiunque voglia inviargli un messaggio riservato. Il mittente usa dunque la chiave pubblica per chiudere il messaggio nello scrigno, con la certezza che il destinatario, possedendo solo lui la chiave privata, è l'unico che potrà aprirlo e leggerne il contenuto.



Quando è stata inventata questa tecnologia, ci si è subito accorti che il possesso esclusivo della chiave privata da parte di un soggetto poteva essere usato non solo per garantire la riservatezza dei messaggi a lui inviati, ma anche per ottenere l'equivalente elettronico della firma. Infatti se chi possiede la chiave privata chiude con essa un messaggio nello scrigno, solo la chiave pubblica corrispondente potrà aprirlo. Dunque si ha la certezza che solo il possessore della chiave privata poteva fare tale operazione, si ha cioè la garanzia dell'identità del mittente, che in tal modo ha sostanzialmente firmato il messaggio.



Inoltre va sottolineato che chiunque possegga la chiave pubblica corrispondente può *verificare* che lo scrigno è stato chiuso dall'unica persona che possiede la chiave privata.

Una firma elettronica è quindi una struttura di dati particolare, che nel disegno abbiamo rappresentato con lo scrigno, il cui formato è definito da uno standard crittografico chiamato Cryptographic Message Syntax (CMS).

I dispositivi

Gli strumenti per controllare in modo sicuro una chiave privata e firmare dei documenti informatici in passato erano prevalentemente le smart-card crittografiche, poi divenute chiavette USB per maggiore semplicità di utilizzo; ma oggi sono prevalentemente gli smartphone, uno strumento che è sempre con noi a portata di mano.

Le **smart-card** utilizzate per la firma elettronica sono simili a molte di quelle che abbiamo in tasca (bancomat, carta di credito, carta nazionale dei servizi, carta d'identità elettronica): una tessera di plastica con all'interno una SIM analoga a quella telefonica. L'inconveniente maggiore era la necessità di un lettore apposito da collegare al PC, per questo motivo si è passati alle chiavette o token USB. Rimaneva però spesso il problema di compatibilità del software con il sistema in uso, o l'impossibilità di utilizzo su tablet o smartphone. Questi motivi, uniti alle molteplici cause di malfunzionamento che affliggono spesso la manutenzione dei PC, hanno fatto sì che oggi si preferisca utilizzare lo smartphone come dispositivo fisico associato al possesso esclusivo della credenziale di firma.

Delegare la firma

L'uso dello smartphone presenta anche il vantaggio di abolire l'usanza tanto sciagurata quanto diffusa di affidare la smart-card o il token USB al proprio commercialista (assieme al PIN). Usanza sciagurata in primo luogo per il titolare, perché se un malintenzionato venisse in possesso del dispositivo e del PIN, potrebbe commettere ogni sorta di illecito senza possibilità di ripudio da parte del titolare che si troverebbe a far fronte ad ogni conseguenza civile e penale.

Ed è sciagurata anche per l'affidatario, dato che in taluni casi si può configurare o un improprio rapporto di delega (non ammessa ad esempio per la firma dei bilanci), oppure un reato di falso, poiché: *"il consenso o l'acquiescenza della persona di cui sia falsificata la firma, non svolge alcun rilievo, in quanto la tutela penale ha per oggetto non solo l'interesse della persona offesa, apparente firmataria del documento, ma anche la fede pubblica, la quale è compromessa nel momento in cui l'agente faccia uso della scrittura contraffatta per procurare a sé un vantaggio o per arrecare ad altri un danno; pertanto anche l'erroneo convincimento sull'effetto scriminante del consenso costituisce una inescusabile ignoranza della legge penale."* (Cassazione penale, Sezione V, Sentenze 27.08.2013, n. 35543 e 10.03.2009, n. 16328).

Dispositivi per la firma	
Smart card	Necessità di lettore esterno, necessità di software sul pc, in caso di smarrimento va emesso un nuovo certificato.
Token usb	Software già presente nella chiavetta, non necessità di lettore esterno in quanto è lui stesso il lettore e si collega con usb, in caso di smarrimento va emesso un nuovo certificato.
Con questi dispositivi sono probabili malfunzionamenti dovuti a SIM sporche, driver non riconosciuti dal sistema operativo, malfunzionamento dei dispositivi stessi.	
Firma in cloud (o firma remota)	Il software che elabora il file è sullo smartphone o sul pc collegato a internet, mentre il dispositivo di firma, fisicamente al sicuro sui server del fornitore del servizio, viene attivato tramite lo smartphone o ricevendo un SMS di verifica su un telefono tradizionale. In caso di smarrimento del telefono non è necessaria l'emissione di un nuovo certificato.
La firma in cloud o firma remota ha meno probabilità di malfunzionamenti, in quanto la procedura non coinvolge dispositivi fisici ed è composta da smartphone e pc che comunicano a distanza.	

Come si fa

Qualunque sia il dispositivo utilizzato, per apporre la firma elettronica è necessario l'uso di software specifici con i quali si compiono solitamente le operazioni seguenti:

1. selezione del file da firmare;
2. *(opzionale)* posizionamento nel documento della **firma visibile** *(vedi oltre)*;
3. inserimento di una password o PIN.

Quando si utilizza lo smartphone come dispositivo il PIN può essere inserito su una apposita app mobile, oppure l'app mobile genera una password temporanea (OTP, One Time Password, vedi oltre) da inserire nel software sul PC.

Per completare il quadro in ambito crittografico bisogna aggiungere solamente un'ultima operazione molto importante: il calcolo dell'impronta (che gli anglofoni chiamano "hash"). Si tratta di un algoritmo che a partire da un file di qualunque dimensione produce un messaggio di lunghezza predefinita. Ad esempio l'immagine precedente può avere come impronta un valore come il seguente:

4e604bd0453f781658026e1a4608f6c5e9f063a6c238afb972ee9cfc367c7c1f

che può sembrare una sequenza casuale di lettere e numeri ma in sostanza è un numero enorme, risultato di un calcolo molto preciso effettuato a partire dai bit che compongono il file del documento. Calcolare l'impronta di un file risulta molto utile per l'uso della firma elettronica in quanto consente di chiudere nello scrigno, cioè firmare, un messaggio piccolo, con un notevole guadagno di prestazioni.

Oltre al fatto di avere una lunghezza predefinita, l'impronta possiede un'altra proprietà estremamente utile. Se il file di partenza cambia anche di poco, persino di un solo bit, il valore dell'impronta cambia completamente. Il calcolo in questo caso funziona in modo simile all'ultimo carattere del codice fiscale, che viene calcolato in base a tutti i caratteri precedenti. Questo consente di controllare e quindi garantire l'integrità dei documenti che vengono firmati elettronicamente.

La biometria

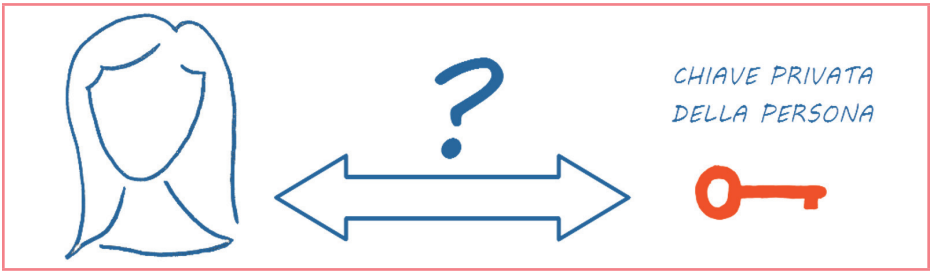
A conclusione di questo capitolo va fatto un cenno anche ad un'altra tecnologia, alternativa alla crittografia, molto usata per la firma e l'identità elettroniche: la biometria. La differenza fondamentale tra i due approcci consiste nel modo in cui si collegano i dati alle persone. Nella crittografia la chiave è un dato associato alla persona tramite il possesso, cioè il collegamento tra dati e persona si fonda sul controllo esclusivo della chiave. Nella biometria si usano dei dispositivi particolari che "leggono" alcuni dati presenti nel nostro corpo, come l'impronta digitale, la retina, il timbro della voce, il gesto della mano che firma con un pennino. A differenza della chiave crittografica, si ottengono però dei dati ogni volta un po' diversi poiché la lettura è imprecisa e anche il nostro corpo può cambiare nel tempo. Nonostante questi inconvenienti, grazie alla statistica è possibile comunque usare questi dati per identificare in modo univoco una persona con un grado di probabilità accettabile, e in certi casi può essere più conveniente.

Il livello di sicurezza della biometria è diverso rispetto a quello della crittografia non solo per questioni statistiche, ma anche per motivi architetturali. Si può in molti casi far leggere a un dispositivo un dato contraffatto. Jan Krissler, ricercatore ed ethical hacker tedesco, nel 2014 ha raccolto l'impronta digitale di Ursula von der Leyen, allora ministro della difesa tedesco, usando semplicemente alcune fotografie ad alta risoluzione fatte a distanza durante un evento pubblico. Krissler ha dimostrato come fosse possibile partendo da tali immagini realizzare una falsa impronta digitale con cui sbloccare un iPhone 5S.

Un altro aspetto di non poco conto che dovrebbe farci preferire la crittografia alla biometria è che in caso di furto posso sempre revocare una chiave privata, così che da quel momento non sia più associata alla mia persona. Proviamo invece a immaginare il caso, oggi difficile ma non escludibile a priori, del furto dei parametri che identificano una firma grafometrica. Se qualcuno riuscisse a utilizzarli per guidare una mano artificiale, potrebbe apporre firme apparentemente autografe su supporto cartaceo. Sarebbero in tal caso riconoscibili come false da un perito calligrafo?

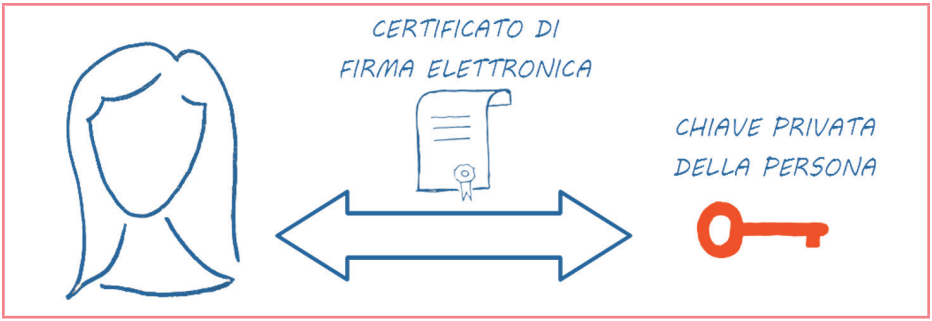
1.3 LA NORMATIVA DI RIFERIMENTO

Abbiamo visto come l'autenticità di una firma elettronica, usando la crittografia, dipenda dal collegamento tra la chiave privata usata per firmare e l'identità della persona. Ma come si può garantire tale collegamento?



Per realizzare un collegamento affidabile tra una persona e una chiave è necessario il dispiegamento di una tecnologia raffinata, per cui nel Regolamento eIDAS i prestatori di servizi fiduciari (Trust Service Provider, abbreviato in TSP) occupano un posto centrale. Essi offrono infatti un servizio tecnologico cruciale emettendo i certificati di firma. Il certificato è un documento informatico che collega in modo affidabile l'identità di una persona alla sua chiave pubblica.

In questo modo l'identità risulta associata in modo certo anche alla chiave privata corrispondente di cui la persona ha il controllo esclusivo. E il prestatore di servizi fiduciari diventa così il custode e il garante di questa associazione che è fondamentale per l'autenticità e la non ripudiabilità della firma elettronica, cioè per il suo valore legale.



Il ruolo del TSP è talmente critico che la normativa ha pensato bene di introdurre la sottocategoria dei prestatori di servizi fiduciari qualificati (Qualified Trust Service Provider, brevemente QTSP) i quali sono soggetti a vigilanza da parte di un organismo istituzionale nazionale, che in Italia è l'Agenzia per l'Italia Digitale (AgID). L'organo di vigilanza controlla periodicamente che il QTSP rispetti un insieme di requisiti di sicurezza e conformità obbligatori per l'esercizio di tale attività.

L'elenco dei QTSP italiani è consultabile all'URL:
https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/IT
L'elenco completo dei QTSP presenti nell'UE è consultabile all'URL:
https://esignature.ec.europa.eu/efda/tl-browser

I certificati emessi dai QTSP sono così chiamati certificati *qualificati* di firma elettronica. E una firma elettronica apposta con una chiave privata associata ad un certificato qualificato è definita *firma elettronica qualificata*. Solo grazie a tutte queste garanzie, in termini di sicurezza e trasparenza, il Regolamento eIDAS può quindi sancire finalmente che "una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa" (art. 25, c. 2). Per completezza si può aggiungere anche che in caso di disconoscimento, diversamente dalla firma autografa, l'onere della prova è a carico del firmatario. Pertanto si potrebbe dire che offra persino maggiori garanzie.

L'obbligo di riconoscere le firme elettroniche qualificate introdotto nel Regolamento eIDAS (art. 25, c. 3) deve essere onorato, altrimenti, oltre a non consentire l'esercizio di un diritto dei cittadini dell'unione, si incorre in una procedura di infrazione. Sono piuttosto rari oggi gli uffici della PA non ancora in grado di accettare un documento firmato elettronicamente. Nella maggior parte dei casi viene pretesa. Ma a dispetto dei diritti, come in ogni situazione, in caso di contrasto spesso vince chi ha più potere negoziale.

Bisogna fare molta attenzione alla terminologia nelle traduzioni. Il Codice per l'Amministrazione Digitale nel 2005 ha infatti usato il termine *firma digitale* per descrivere quello che poi il Regolamento eIDAS nel 2014 ha chiamato invece *firma elettronica qualificata*. Per tale motivo in Italia spesso si usa ancora il termine firma digitale come sinonimo di firma elettronica qualificata. Bisogna però evidenziare che al contempo l'espressione *digital signature* viene usata in inglese solitamente in ambito tecnico per indicare la firma elettronica realizzata con la crittografia a chiave pubblica, senza alcun riferimento ad un particolare valore legale: essa non corrisponde quindi affatto a ciò che in Italia viene indicato con l'espressione *firma digitale*.