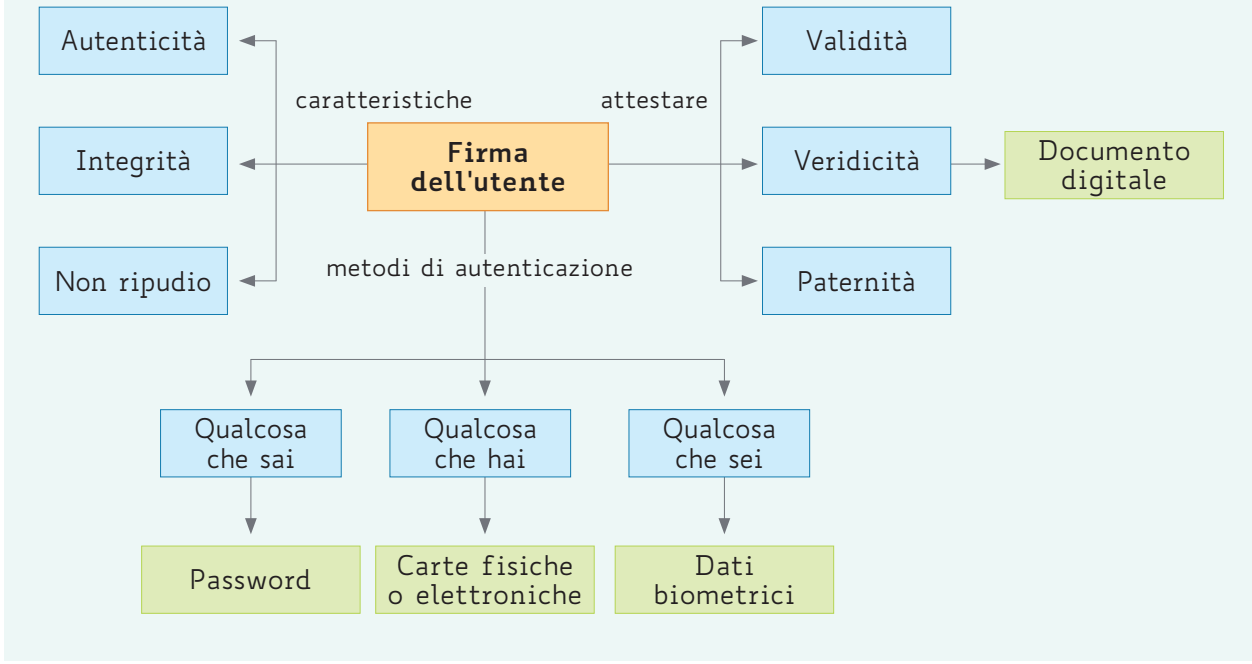
Firma elettronica, digitale, certificati e PEC

didattica inclusiva



Firma elettronica e digitale

Crittografare un messaggio completo può risultare a volte troppo dispendioso e richiedere tempi molto lunghi; spesso, inoltre, non serve la **segretezza**, ma basta l'**autenticazione** e la **certezza** che il messaggio non venga modificato.

In questi casi, è sufficiente che il messaggio venga "imbustato" all'interno di un "contenitore digitale" che prende il nome di firma digitale e che, oltre a permettere di riconoscere se il documento stesso è stato modificato o meno dopo l'apposizione della firma, è soprattutto in grado di attestare la validità, la veridicità e la paternità di un documento elettronico. Quindi, grazie a essa, è possibile risalire con certezza all'identità del firmatario.

La **firma elettronica** è stata introdotta nella normativa europea dalla **Direttiva 1999/93/CE**, e la sua validità e utilizzo nell'ordinamento italiano sono disciplinati dal D.lgs. 7 marzo 2005, n. 82, il cosiddetto Codice dell'Amministrazione Digitale, modificato dal D.lgs. 4 aprile 2006, n. 159.

Le espressioni firma elettronica e firma digitale a volte sono erroneamente considerate equivalenti, ma in realtà non lo sono: vediamo in cosa differiscono.

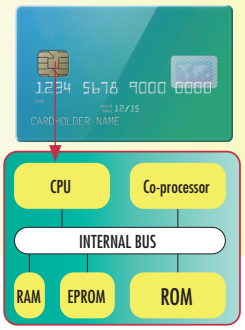
Firma elettronica

La **firma elettronica** è un'espressione generica priva di qualsiasi valenza tecnico-giuridica e fa riferimento a **qualsiasi tecnica finalizzata all'autenticazione elettronica** che consenta di associare dati ad altri dati, come ad esempio la **firma** a un **documento**.

I metodi di autenticazione elettronica utilizzati per le **firme elettroniche** possono essere raggruppati in tre categorie:

1. "**qualcosa che sai**" (password);
2. "**qualcosa che sei**" (dati biologici);
3. "**qualcosa che hai**" (una tessera magnetica o una smart card).

La legge italiana definisce così un **dispositivo di firma idoneo**: «un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali. Il dispositivo di firma è il supporto candidato alla conservazione della chiave privata e deve dunque essere non riproducibile e, in parte, non modificabile.
La chiave deve inoltre essere protetta da una procedura di identificazione del titolare (tipicamente l'inserimento di un PIN) e deve essere fatta in modo da non lasciare alcuna traccia della chiave privata sul sistema di validazione.
La **smart card** è il supporto più diffuso che risponde a tutti questi requisiti: è una tessera plastificata, con dimensioni di una carta di credito, su cui è integrato un **microchip programmabile**, con una memoria (**ROM**) che contiene il sistema operativo e i programmi "fissi", una memoria (**PROM**) che contiene il numero seriale della smart card, e una terza memoria (**EPROM**) che contiene i dati del proprietario e i meccanismi di protezione che ne evitano la clonazione.



Firma digitale

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

- **autenticità**, garantisce cioè l'identità del sottoscrittore;
- **integrità**, assicura cioè che il documento non sia stato modificato dopo la sottoscrizione;
- **non ripudio**, attribuisce cioè piena validità legale al documento, che non può essere ripudiato dal sottoscrittore.

La firma digitale si riferisce quindi a uno specifico tipo di firma elettronica, e cioè a quello che utilizza il sistema di crittografia a doppie chiavi asimmetriche, una pubblica e una privata.

La **chiave privata** è in genere memorizzata in una **smart card**.

La firma digitale consente:

- la **sottoscrizione di un documento informatico**;
- la **verifica**, da parte dei destinatari, **dell'identità** del soggetto sottoscrittore;
- la **certezza** che l'informazione contenuta nel documento non sia stata alterata.

Il cittadino può in questo modo firmare digitalmente documenti informatici in modo da garantire l'autenticità del sottoscrittore, l'integrità e il non ripudio dei documenti in questione inviati alle **Pubbliche Amministrazioni**: tale prassi permette quindi di snellire significativamente i rapporti tra **PA**, cittadini e imprese, riducendo drasticamente la gestione dei documenti in forma cartacea, proprio come indicato nelle Linee Guida per l'utilizzo della **firma digitale** emanate da **AgID** (**Agenzia per l'Italia Digitale, ex DigitPA**).

Per generare una firma digitale è necessario utilizzare, come accennato, una coppia di **chiavi digitali asimmetriche** (**chiave privata** e **chiave pubblica**), attribuite in maniera univoca a 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** viene distribuita ed è usata per verificare l'**autenticità** della firma.

Obblighi comunitari

La direttiva comunitaria 1999/93/CE ispirata al principio di "neutralità tecnologica", si "accontenta" della firma elettronica, avendo il legislatore adottato «un approccio aperto alle varie tecnologie e servizi che consentono di autenticare i dati in modo elettronico».

Il legislatore comunitario, nel predisporre la disciplina della **firma elettronica**, si è preoccupato soltanto della funzione che tale firma deve svolgere, evitando qualsiasi riferimento alle tecniche informatiche utilizzate al fine della sua creazione, permettendo così una facile apertura al progresso tecnologico.

Funzionamento della firma digitale

Firmare un documento elettronico è un'attività assai semplice e veloce e per eseguirla è necessario essere dotati di un **kit per firma digitale** (o **firma remota**), composto da un dispositivo sicuro di generazione delle firme (**smart card**), dal **lettore** di smart card e dal **software di firma e verifica**.

Un dispositivo di firma sicuro deve essere rilasciato da un apposito ente certificatore, in grado di verificare l'identità del richiedente prima di consegnargli la carta abilitata alla firma. Oltre alla carta, l'utente viene dotato di codice segreto (**PIN**, **Personal Identification Number**) personale, da utilizzarsi contemporaneamente alla smart card.

La Carta Nazionale dei Servizi (CNS), è un dispositivo (una smart card o una chiavetta usb) rilasciato dalle Camere di Commercio e concepito per accedere ai servizi online della Pubblica Amministrazione su tutto il territorio nazionale. Consente l'identificazione certa dell'utente in rete e offre anche la possibilità di firma digitale, oltre a ulteriori servizi resi disponibili dalle diverse amministrazioni.

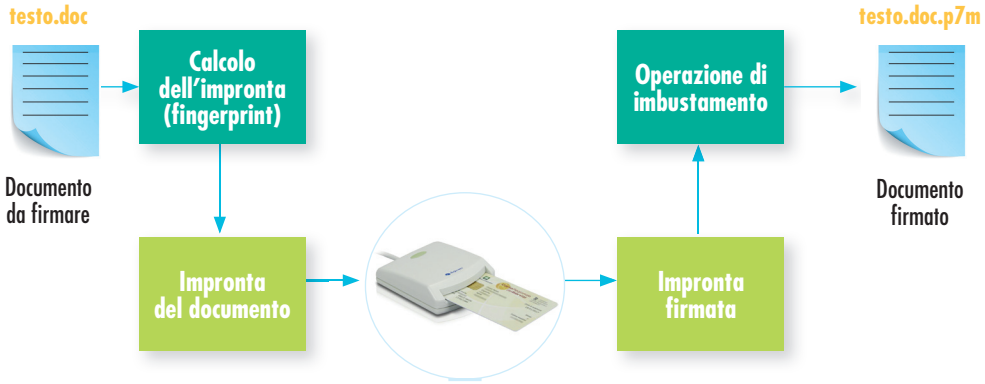
La Tessera Sanitaria è il documento personale che ha sostituito il tesserino plastificato del codice fiscale; viene rilasciata a tutti i cittadini italiani aventi diritto alle prestazioni fornite dal Servizio Sanitario Nazionale (SSN). A partire dal 2011, la Tessera Sanitaria-Carta Nazionale dei Servizi (TS-CNS), è dotata di microchip.

Dopo aver installato il kit sul proprio computer, attraverso il software di firma sarà possibile selezionare il documento elettronico da sottoporre a firma digitale e, previa attivazione di un account, alla **marcatura temporale**.

Durante l'apposizione della firma, il file viene "incapsulato" in una "**busta crittografica**" e il risultato è un nuovo file, con estensione **.p7m**: la **firma digitale** in formato .p7m consente di firmare qualunque tipo di file (.rtf, .doc, .tiff, .xls, .pdf ecc.).

Il formato **p7m**, noto come formato **pkcs#7**, è quello previsto dalla normativa vigente sull'interoperabilità della firma digitale ed è quello che le Pubbliche Amministrazioni sono obbligate ad accettare.

È il formato disponibile fin dagli albori, in uso dal 1999, al quale si aggiunsero, sette anni più tardi, i formati di firma PDF e XML.



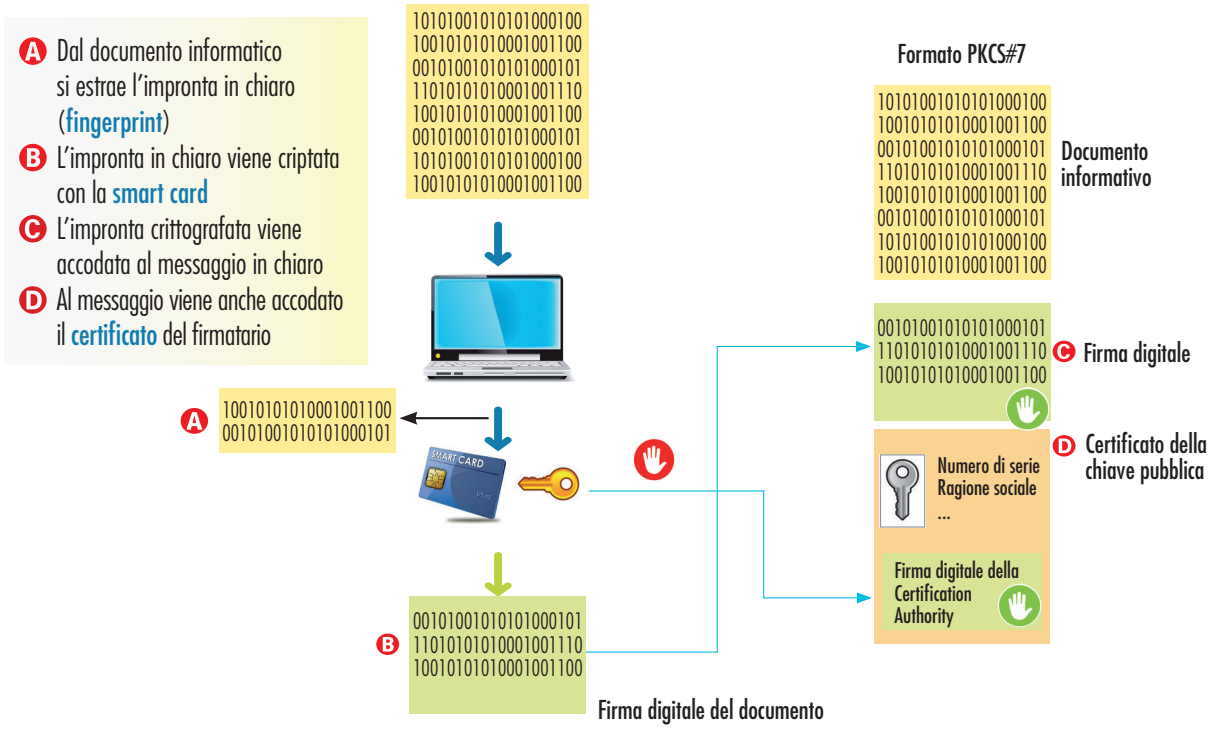
Gli enti di certificazione forniscono appositi programmi o servizi online per verificare l'identità del firmatario e la validità della firma apposta nel file **p7m**, permettendo di "aprire" il contenuto della "capsula **p7m**" e di leggere i dati che contiene.

Descriviamo il funzionamento della procedura di firma nell'esempio che segue.

Esempio

Quando A vuole mandare a B un messaggio autenticato e integro aggiunge la firma (fingerprint), la cripta con la sua chiave privata e la "aggancia" in fondo al messaggio in chiaro: il destinatario B, per decriptare la firma, deve utilizzare la chiave pubblica di A e solo questa è in grado di riconoscere il mittente, che quindi viene identificato come certo.

Nel dettaglio, la procedura di **firma** è la seguente.



Con questo sistema è possibile anche verificare l'integrità del documento in quanto, se il **fingerprint** ricalcolato sul messaggio ricevuto non corrisponde a quello inviato, questo non risulta autenticato e quindi sicuramente il messaggio è stato alterato.

Firma elettronica remota

Una modalità innovativa di **firma digitale** è quella che prende il nome di **firma remota**, che garantisce la stessa sicurezza e gli stessi effetti di legge della tradizionale firma digitale, ma offre diversi vantaggi:

- non richiede l'installazione di hardware e driver dedicati;
- è indipendente dall'ambiente operativo dell'utente.

Firma remota
È una firma digitale eseguita con una chiave privata residente su un dispositivo remoto, detto **HSM (Hardware Security Module)**, e quindi senza bisogno di utilizzare una smart card.

I dati da firmare sono inviati all'**HSM** utilizzando la rete internet e sempre tramite questa la risposta ritorna all'utente, come illustrato in figura.

Il dialogo tra l'applicazione **client** e il **server di firma** può essere così sintetizzato:

- l'**utente si autentica** nei confronti del **server**;
- il **client** richiede la **firma digitale**, **inviando** il **digest** del documento al server;
- il **server** calcola la firma e la restituisce al **client**, dove viene salvata.

Digest
È il risultato (l'output) dell'applicazione dell'algoritmo hash (chiave pubblica) al file del documento al quale è stata applicata la firma digitale. In pratica il digest è rappresentato da una stringa di dimensioni variabili, una sequenza di numeri e lettere che identifica in modo univoco il documento e il suo contenuto.

I **kit di firma remota** sono composti da un **certificato** di **firma digitale**, che risiede presso un server sicuro **HSM**, e da un dispositivo **OTP** (**One-Time Password**), che permette al titolare di autenticarsi con le proprie credenziali e di firmare i propri file da qualsiasi postazione connessa a internet.

Grazie all'utilizzo di un meccanismo OTP per l'autenticazione dell'utente, questo sistema risulta sicuro, tecnologicamente innovativo, facile da usare e con numerosi vantaggi operativi, in particolare quello di disporre in ogni momento e in ogni luogo della propria firma digitale su diversi ambienti (Windows, Mac).

Il servizio di **firma remota** rivoluziona il mondo della **firma digitale**, coniugando la portabilità a un sistema di autenticazione forte, cioè un'autenticazione a due fattori, basata sull'utilizzo congiunto di due metodi di autenticazione individuale.

Token OTP con display per la firma remota

Il dispositivo **OTP con display**, dotato di chip e schermo **LCD**, è uno strumento totalmente sicuro: genera una password con valore momentaneo (pochi secondi), valida per un'unica sessione e non riutilizzabile. Inoltre, un numero seriale univoco ne garantisce l'unicità e l'impossibilità di duplicazione.

Token OTP USB per la firma remota

Il dispositivo **OTP USB** unisce agli standard di sicurezza **One-Time Password** la comodità di inviare il codice di autenticazione generato direttamente al computer, tramite la porta **USB**. Non ha al suo interno alcuna batteria, in quanto si alimenta dal computer e non necessita di installare alcun driver per il suo funzionamento.

Il certificato digitale

Nei sistemi sino a ora descritti abbiamo trascurato un problema: per verificare il mittente (p.e. **Anna**), il ricevente (p.e. **Bruno**) utilizza la sua **chiave pubblica**, con la quale può "aprire" e autenticare il messaggio che gli è pervenuto. Ma Bruno come fa a essere certo che la chiave gli sia pervenuta effettivamente da Anna e non da un intruso "mascheratosi" da Anna? La soluzione di questo problema, che consiste nel **certificare l'identità del mittente**, si risolve attivando una particolare procedura per la consegna della chiave pubblica da Anna a Bruno: la chiave viene racchiusa all'interno di un **certificato digitale** che, oltre a essa, contiene le informazioni sul mittente.

Questo certificato deve essere a sua volta validato da un **ente certificatore** (**CA**, **Certification Authority**) che **garantisce l'identità del proprietario del certificato** firmandone le chiavi pubblica e privata con la propria chiave privata: in questo modo, ne rende impossibile per chiunque la manomissione.

Per sostituirsi ad Anna, quindi, un malintenzionato dovrebbe effettuare le seguenti operazioni:

- **violare la cifratura della CA** che protegge le due chiavi;
- sostituire le chiavi originali con delle **chiavi fasulle**;
- **ricodificare il tutto** con la chiave privata della Certification Authority.

Possiamo perciò essere abbastanza tranquilli, perché risulta molto complicato anche per un abile hacker effettuare tutte queste operazioni.

Il **certificato digitale**, contenuto nella **smart card** del titolare e firmato digitalmente dal certificatore, è un documento digitale che contiene i seguenti dati:

- **dati del proprietario**, tra i quali nome, cognome e data di nascita del titolare e la sua chiave pubblica;
- **dati del certificato**, tra cui la data di scadenza e il numero di serie del certificato;
- **dati della Certification Authority**, ovvero la ragione sociale del certificatore, il codice identificativo del titolare presso il certificatore e la firma digitale.

Il **certificato** è un piccolo file contenente **informazioni** essenziali **per la verifica della firma**, e cioè:

- il **nome** e il **codice fiscale** dell'utente **titolare** (p. es. Mario Rossi);
- il **nome** dell'**azienda** di appartenenza, se applicabile;
- il **nome** dell'**ente certificatore**;
- la data di **inizio** e la data di **fine validità**;
- la **chiave pubblica** del titolare;
- altre informazioni di servizio.

Le pratiche relative all'identificazione dell'utente prima delle emissione del certificato vengono fatte dalla **Registration Authority** che, in base alla tipologia di soggetto che richiede il certificato, svolge le necessarie indagini e attiva le relative procedure per l'identificazione certa del richiedente. La **Certification Authority** si occupa invece più specificatamente del "ciclo di vita del certificato", gestendone la sua pubblicazione online e la relativa manutenzione.

I certificati hanno una scadenza temporale e periodicamente vanno rinnovati e aggiornati. Inoltre, ricordiamo che una coppia di chiavi a 1024 bit può avere validità massima di 2 anni.

Registration Authority e **Certification Authority**, per la delicatezza del ruolo che svolgono, sono enti pubblici o privati accreditati e selezionati, che devono aver richiesto e ottenuto il riconoscimento del possesso dei requisiti più elevati in termini di qualità e di sicurezza.

Un **certificato digitale** può avere diversi formati. I più diffusi sono:

- chiavi **PGP/GPG**;
- certificati **X.509**.

La differenza sostanziale tra un certificato **PGP/GPG** e uno di tipo X.509 è che è possibile creare il proprio certificato PGP/GPG in modo autonomo e in pochissimi istanti, mentre per X.509 è necessario rivolgersi a un ente addetto allo scopo.

PGP (**Pretty Good Privacy**) è uno dei più celebri software per la crittografia a chiave pubblica, utilizzato soprattutto per codificare le email. Con **PGP** è infatti possibile crittografare un messaggio e apporre la propria firma digitale, rispondendo in questo modo alle esigenze fondamentali di riservatezza e sicurezza della corrispondenza privata.
Si basa su un approccio ibrido, con crittografia pubblica e simmetrica, e lo si deve a **Phil Zimmermann**, che in un primo tempo lo rilasciò nel 1991 come prodotto freeware.
GPG è la sua versione **OpenSource**.

L'insieme costituito da tutte le parti – utenti e Authority, nonché tecnologie che utilizzano, servizi che offrono e politiche di gestione che attuano – è detto **PKI** (**Public Key Infrastructure**).

Richiesta di un certificato digitale

Vediamo brevemente come ottenere un certificato digitale: la procedura è abbastanza standard e le piccole differenze tra le diverse **CA** possono riguardare i dati da fornire o il procedimento di generazione e comunicazione della coppia di chiavi asimmetriche. Possiamo individuare quattro passi, qui di seguito descritti.

1. **Generazione della coppia di chiavi asimmetriche da utilizzare per cifrare le comunicazioni**: le comunicazioni tra **CA** e richiedente devono essere protette e quindi viene generata una coppia di chiavi dalla **CA** direttamente seguendo la procedura indicata sul suo sito.
2. **Comunicazione del richiedente di informazioni circa la propria identità alla Certification Authority**: ricevute le chiavi, è possibile comunicare le informazioni riguardanti il richiedente, quali ad esempio il nome di dominio, l'indirizzo email, il nome e il cognome del richiedente ecc. Questa fase è detta di **enrollment** e le modalità con cui va eseguita sono definite da un apposito standard (**PKCS-10**).

3. **Verifica da parte della Registration Authority dei dati ricevuti**: le operazioni di controllo dei dati pervenuti alla **CA** possono variare a seconda del soggetto e del tipo di certificato richiesto e in questa fase possono essere richiesti anche ulteriori dati, come ad esempio l'iscrizione alla Camera di Commercio o la partita IVA; se il controllo va a buon fine, la **Certification Authority** genera il certificato e lo firma digitalmente con la propria chiave privata: viene cifrato per garantire che i dati in esso contenuti non vengano modificati.
4. **Invio del certificato firmato al richiedente**, che provvederà a installarlo o a farlo installare sul proprio server.

Posta Elettronica Certificata (PEC)

La **Posta Elettronica Certificata** (detta anche posta certificata o **PEC**) è un sistema di comunicazione simile alla posta elettronica standard, con alcune caratteristiche di sicurezza e di certificazione della trasmissione che rendono i messaggi "garantiti", in modo che il mittente sia univocamente definito e conosciuto.

Un documento inviato con la **PEC** assume il medesimo **valore legale** di una **raccomandata con avviso di ricevimento** (ricevuta di ritorno). Le caratteristiche e il valore legale della PEC sono stati definiti nel **D.P.R. 11 febbraio 2005 n. 68** e nei due documenti tecnici collegati, dove sono indicate le regole per la formazione, la trasmissione e la validazione della posta elettronica certificata.

Il Codice dell'Amministrazione Digitale (D.lgs. n. 82/2005, modificato e integrato dal D.lgs. n. 235/2010) ribadisce il valore legale della PEC come strumento di trasmissione telematica: la normativa completa, con modifiche e integrazioni, è disponibile sul sito dell'Agenzia per l'Italia digitale all'indirizzo www.agid.gov.it.

Inoltre, la nota del Ministero dello Sviluppo Economico del 16 luglio 2013 n. 120610 (circolare Min. Svil. Ec. 9 maggio 2014 prot. n. 77684) sottolinea che ogni impresa deve avere un indirizzo di PEC iscritto nel Registro delle Imprese (**INI-PEC**) riconducibile solo a essa, cioè non è più possibile iscrivere una medesima **PEC** collegata a due distinte imprese. Quindi, per ogni impresa, sia essa **individuale** sia **societaria**, deve essere iscritto, nel Registro delle Imprese, un indirizzo di PEC unico e, in caso di inadempienze, per la stessa impresa verrà avviata la procedura di cancellazione dal Registro delle Imprese, ai sensi dell'art. 2191 c.c.

Presso il Ministero dello Sviluppo Economico è stato istituito un archivio denominato **Indice Nazionale degli Indirizzi di Posta Elettronica Certificata (INI-PEC)** il cui accesso è libero, cioè Pubbliche Amministrazioni, professionisti, imprese, gestori o esercenti di pubblici servizi e tutti i cittadini possono visualizzarlo nel web senza necessità di autenticazione.

La certificazione della posta, cioè l'attestazione delle credenziali del mittente e del destinatario, viene effettuata da appositi **gestori** (che devono rispettare tutti i requisiti previsti dall'art. 14 del D.P.R. 11 febbraio 2005 n. 68) riconosciuti dall'Agenzia per l'Italia digitale e inclusi in un elenco specifico, l'**Elenco Pubblico dei Gestori accreditati**.

Tutti i gestori di servizi web offrono ai loro clienti la PEC a costi molto contenuti. Per i professionisti, molte associazioni di categoria la rendono disponibile gratuitamente, così come molte Camere di commercio. InfoCert è gestore accreditato di PEC iscritto nell'Elenco Pubblico dei Gestori accreditati, presente nel sito DigitPA, e il suo servizio di Posta Elettronica Certificata è Legalmail.

Come funziona la PEC

Una trasmissione può essere considerata **posta certificata** solo se le caselle del mittente e del destinatario sono entrambe caselle di **posta elettronica certificata**.

I gestori di posta certificata sono obbligati a mantenere registrati tutti i principali eventi che riguardano la trasmissione per 30 mesi, da fornire come prova da parte degli interessati, e devono avere l'accortezza di mantenere il proprio orologio "allineato" con gli istituti ufficiali che garantiscono l'ora esatta, in modo che tutte le transazioni (invii, ricevute, buste...) contengano sempre l'ora esatta.

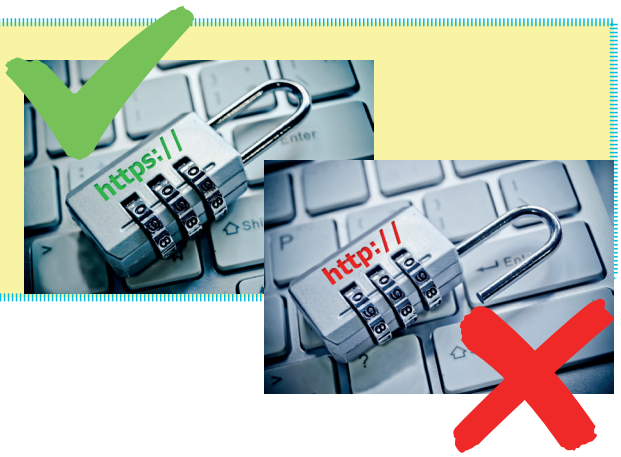
Vediamo, in forma schematica, come avviene una trasmissione.

Accesso e identificazione

Dopo aver predisposto il documento da inviare, il mittente deve essere identificato dal proprio provider tramite due modalità:

1. user_ID e password;
2. certificati digitali.

Clienti e gestori dei servizi di posta certificata utilizzano esclusivamente protocolli sicuri (p.e. https, smtps, pop3s, imaps, dove la "s" finale attesta la sicurezza del protocollo) per scambiarsi il documento, in modo da impedire qualsiasi manomissione del messaggio da parte di terzi.



Certificazione dell'invio

Quando si spedisce un regolare messaggio da una casella di posta certificata (punto 1 dello schema riassuntivo a pagina seguente) si riceve dal proprio provider di posta certificata una **ricevuta di accettazione**, firmata dal gestore, che attesta il momento della spedizione e i destinatari (distinguendo quelli normali da quelli dotati di PEC). La ricevuta di accettazione contiene la data e l'ora dell'invio, mittente, destinatario, oggetto del messaggio.

Integrità del messaggio

Il gestore di posta certificata del mittente crea un nuovo messaggio, detto "**busta di trasporto**" (punto 2 dello schema), che contiene il messaggio originale e i principali dati di spedizione.

La busta di trasporto viene firmata dal provider per garantire che il contenuto non venga compromesso durante la trasmissione: il provider del destinatario può constatare la sua integrità verificando la firma del mittente.

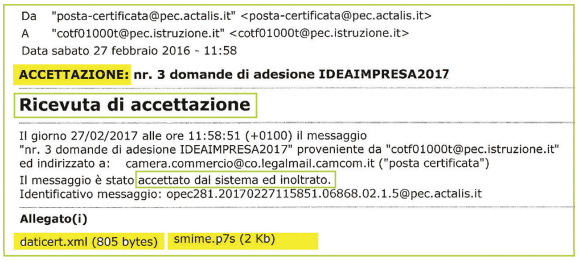
Certificazione della consegna

Il destinatario riceve il **messaggio di posta certificata** nella propria casella, inserito nella sua **busta di trasporto**" tramite il proprio provider (punto 3 dello schema) se tutti i controlli fatti danno esito positivo; il provider provvede anche a inviare al gestore del mittente la **ricevuta di consegna** (punto 4 dello schema), che è un normale messaggio email firmato dal gestore che attesta: la consegna, data e ora della consegna, tutto ciò che è stato consegnato.

Una caratteristica della PEC è che il mittente riceve tutto il messaggio, compresi gli eventuali allegati, in modo che egli possa ricevere una prova, firmata dal provider del destinatario, di tutto il contenuto che è stato recapitato.

Il gestore del mittente inoltra il documento al proprio cliente (punto 5 dello schema), che riceve così due messaggi:

1. **ricevuta di accettazione**, che ne conferma la trasmissione;
2. **avvenuta consegna**, che ne attesta la ricezione da parte del destinatario.



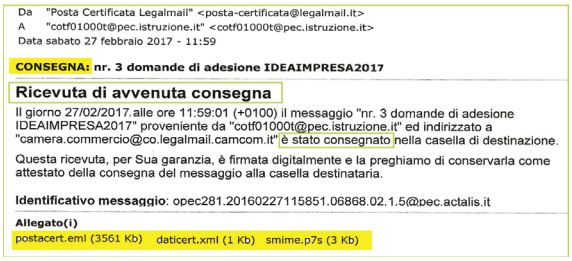
Da "posta-certificata@pec.actalis.it" <posta-certificata@pec.actalis.it>
A "cotf01000t@pec.istruzione.it" <cotf01000t@pec.istruzione.it>
Data sabato 27 febbraio 2016 - 11:58

ACCETTAZIONE: nr. 3 domande di adesione IDEAIMPRESA2017

Ricevuta di accettazione

Il giorno 27/02/2017 alle ore 11:58:51 (+0100) il messaggio
"nr. 3 domande di adesione IDEAIMPRESA2017" proveniente da "cotf01000t@pec.istruzione.it"
ed indirizzato a: camera.commercio@co.legalmail.camcom.it ("posta certificata")
Il messaggio è stato accettato dal sistema ed inoltrato.
Identificativo messaggio: opec281.20170227115851.06868.02.1.5@pec.actalis.it

Allegato(i)
daticert.xml (805 bytes) smime.p7s (2 Kb)



Da "Posta Certificata Legalmail" <posta-certificata@legalmail.it>
A "cotf01000t@pec.istruzione.it" <cotf01000t@pec.istruzione.it>
Data sabato 27 febbraio 2017 - 11:59

CONSEGNA: nr. 3 domande di adesione IDEAIMPRESA2017

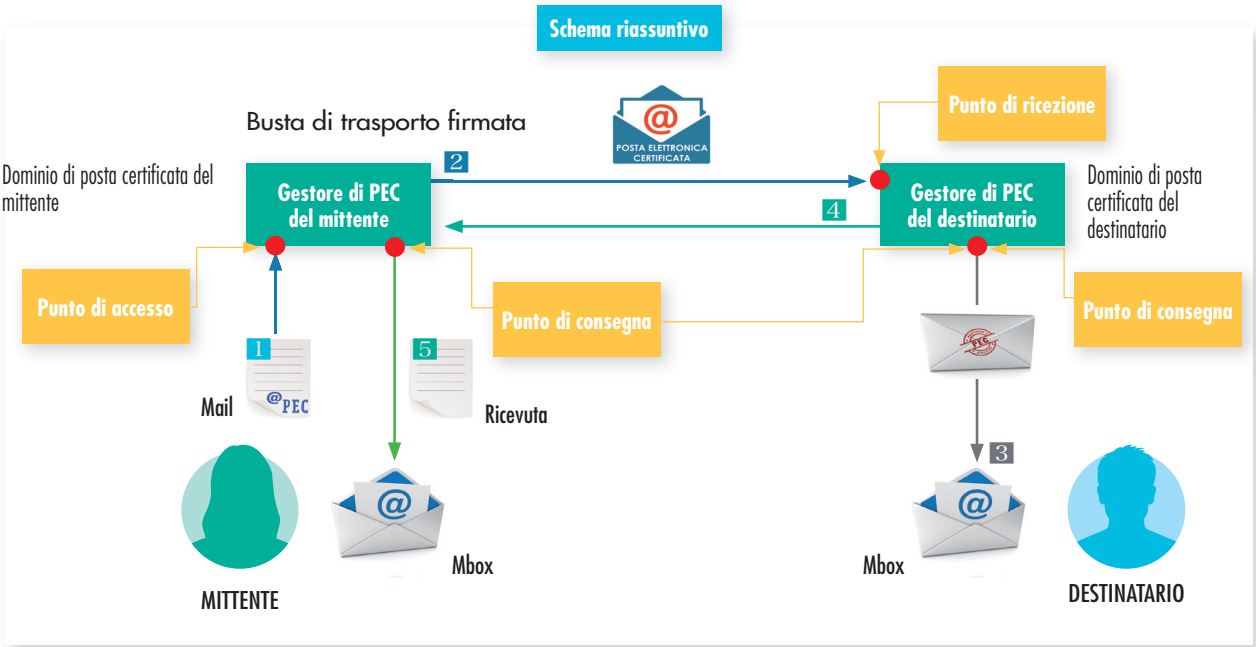
Ricevuta di avvenuta consegna

Il giorno 27/02/2017 alle ore 11:59:01 (+0100) il messaggio "nr. 3 domande di adesione IDEAIMPRESA2017" proveniente da "cotf01000t@pec.istruzione.it" ed indirizzato a "camera.commercio@co.legalmail.camcom.it" è stato consegnato nella casella di destinazione.

Questa ricevuta, per Sua garanzia, è firmata digitalmente e la preghiamo di conservarla come attestato della consegna del messaggio alla casella destinataria.

Identificativo messaggio: opec281.20160227115851.06868.02.1.5@pec.actalis.it

Allegato(i)
postacert.eml (3561 Kb) daticert.xml (1 Kb) smime.p7s (3 Kb)



Vantaggi della PEC

L'utilizzo della **PEC** ha evidenti **vantaggi**, che si possono così sintetizzare:

- **risparmio di denaro**: invio di un numero illimitato di comunicazioni senza alcun costo di spedizione; non si devono acquistare buste, lettere, francobolli; non si devono occupare spazi per conservare i documenti cartacei o le ricevute delle poste;
- **risparmio di tempo**: si possono spedire documenti dal proprio PC e le ricevute arrivano subito; non si perde tempo a inviare fax o fare code alle poste.

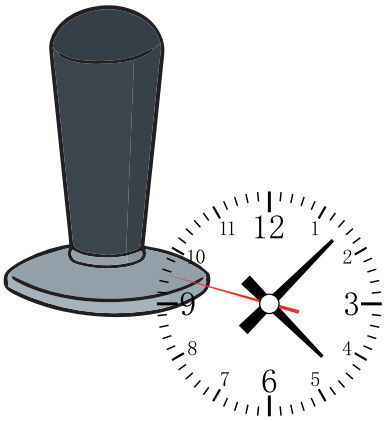
La marca temporale

La **marca temporale** è un servizio che permette di **associare data e ora certe e legalmente valide** a un **documento informatico**: viene offerto come servizio da un **certificatore accreditato**, consentendo quindi di associare al documento una validazione temporale opponibile a terzi.

Il servizio di **marcatura temporale** può essere utilizzato sia su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida, sia su documenti informatici sui quali è stata apposta la **firma digitale**: in tal caso, la **marca temporale** attesterà il preciso momento temporale in cui il documento è stato creato, trasmesso o archiviato (**cfr.** art. 20 comma 3 D.lgs. n. 82/2005 - Codice dell'Amministrazione Digitale).

Come sancito dall'art. 49 del D.P.C.M. del 30/03/2009, le marche temporali emesse devono essere conservate in appositi archivi per un periodo non inferiore a 20 anni.

Il servizio di **marca temporale**, detto anche **Digital Time Stamping** (**DTS**), ha un ruolo importante ai fini del non ripudio delle transazioni: lo scopo di un servizio **DTS** è quello di dimostrare che un certo dato di interesse (documento, messaggio ecc.) esisteva a un certo istante **T** di tempo.



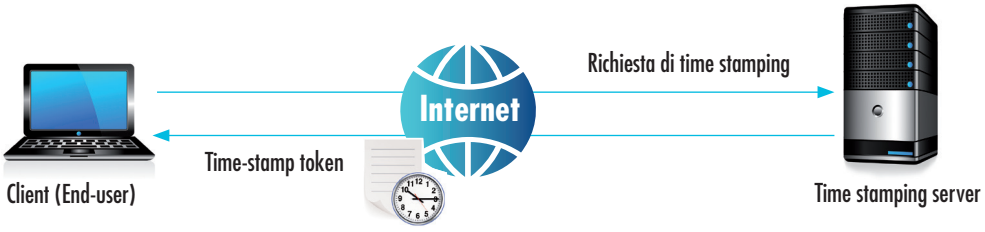
Un altro importante utilizzo della marcatura temporale si ha nelle applicazioni di "deposito" di documenti (p.e. bilanci, brevetti, dichiarazioni fiscali ecc.) per via telematica, quando il momento dell'invio o della ricezione sono di importanza critica.

Apporre una marca temporale è molto semplice: il **richiedente** (**end-user** o client) **genera** un **parametro univoco** calcolato dal dato originale (un valore chiamato **hash**) e **lo invia a un server di time stamping** gestito da una terza parte fidata (**Time Stamping Authority** o **TSA**) che eroga il servizio.

Il server concatena il valore dell'**hash** con il dato temporale (data e ora) ottenuto da una fonte affidabile e quindi firma il tutto con la propria chiave privata.

Il risultato, chiamato time-stamp token, viene inviato al client.

La seguente figura illustra la semplice interazione su cui si basa un servizio di **time-stamping**.



Lo standard **Rfc 3161** definisce il protocollo di comunicazione fra **client** e **server**, ovvero le strutture dati scambiate e le modalità di trasporto.

Esercizi per la verifica

Domande a risposta aperta

1. Cosa differenzia la firma elettronica dalla firma digitale?
2. Come viene apposta la firma digitale?
3. Cosa sono i dispositivi OPT?
4. In cosa consiste il certificato digitale?
5. Che cosa è la PEC e che validità può avere?
6. A cosa serve la marca temporale?

Vero/Falso

1. La firma digitale è stata introdotta nella normativa europea dalla Direttiva 1999/93/CE. V F
2. Per la legge italiana la smart card è un dispositivo di firma idoneo. V F
3. Una funzione di hash è chiamata "one way hash" se non è reversibile. V F
4. L'impronta digitale o message digest è composta da un numero limitato di caratteri. V F
5. Il fingerprint viene criptato con la chiave privata e agganciato in fondo al messaggio in chiaro. V F
6. La smartcard è necessaria per decrittare un documento cifrato. V F
7. Nel MD5 ogni messaggio ha un padding per raggiungere un multiplo di 512. V F
8. Con l'MD5 occorrono circa 100 ore per trovare collisioni. V F
9. L'algoritmo SHA-0 fu violato nel 2005 da un gruppo di crittoanalisti cinesi. V F
10. SHA-2 si trova alla base di applicazioni per la sicurezza come PGP e SSL. V F
11. Una coppia di chiavi a 1024 bit può avere validità massima di 3 anni. V F
12. Tra i formati di certificato digitale più diffusi troviamo il X.609. V F

Risposta singola (○) o multipla (□)

1. La firma digitale si basa su un sistema di codifica a chiavi asimmetriche che consente:
   - a la sottoscrizione di un documento informatico.
   - b la verifica, da parte dei destinatari, dell'identità del soggetto sottoscrittore.
   - c la verifica, da parte del mittente, dell'avvenuta consegna al destinatario.
   - d la certezza che l'informazione contenuta nel documento non sia stata alterata.

2. Per la legge italiana un dispositivo di firma idoneo è (indicare l'affermazione errata):
   - ⓐ un apparato elettronico programmabile solo all'origine.
   - ⓑ un apparato elettronico facente parte del sistema di validazione.
   - ⓒ un apparato elettronico in grado almeno di conservare in modo protetto le chiavi private.
   - ⓓ un apparato elettronico in grado di generare al suo interno firme digitali.
   - ⓔ una tessera plastificata, con le dimensioni di una carta di credito.

3. L'estensione di un file firmato digitalmente è:
   - ⓐ p7m
   - ⓑ pm7
   - ⓒ m7p
   - ⓓ mp7

4. L'acronimo PGP deriva da:
   - ⓐ Privacy Good Pretty.
   - ⓑ Pretty Good Privacy.
   - ⓒ Privacy Global Pretty.
   - ⓓ Pretty Global Privacy.