BibLus-net

LA FIRMA DIGITALE

Premessa

A seguito dell'evoluzione normativa nazionale in materia di certificazione energetica, buona parte delle regioni italiane prevede la possibilità, e in alcuni casi l'obbligatorietà (Campania, Emilia Romagna, Friuli Venezia Giulia, Liguria, Lombardia, Marche, Piemonte, Veneto), di gestire l'Attestato di Prestazione Energetica in formato elettronico.

Nello specifico, una volta prodotto l'APE la procedura che il certificatore dovrà seguire è la seguente, **anche se può cambiare da regione a regione**:

- stampare, timbrare, firmare manualmente il certificato e farne una scansione;
- apporre la firma digitale al documento scansionato;
- trasmettere ed archiviare il documento sul sistema informativo regionale.

In questo speciale proponiamo un approfondimento sulla firma digitale, con le risposte alle domande più frequenti.

Caratteristiche della firma digitale

La firma digitale, o più in generale firma elettronica, rappresenta l'insieme di una serie di dati in forma elettronica utilizzati come metodo di identificazione informatica.

La firma digitale di un documento informatico si propone di soddisfare 3 esigenze, che non tutte le tipologie riescono in realtà a soddisfare, quali:

- autenticità: consentire al destinatario di verificare l'identità del mittente;
- non ripudio: far in modo che il mittente non possa disconoscere un documento da lui firmato;
- integrità: impedire che il destinatario possa alterare un documento firmato da qualcun altro.

Come funziona

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

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

Questo metodo è conosciuto come crittografia a doppia chiave e garantisce la piena sicurezza visto

che la chiave pubblica non può essere utilizzata per ricostruire la chiave privata.

Per generare una firma digitale è necessario utilizzare un particolare kit, generalmente costituito da una chiavetta USB o lettore smart-card, che deve essere richiesto ad uno dei soggetti autorizzati inseriti nell'apposito elenco dei certificatori accreditati.

Essa verrà rilasciata in seguito all'invio di documenti attestanti l'identità del richiedente, il quale verrà associato univocamente alla firma elettronica rilasciata.

Il processo di informatizzazione della pubblica amministrazione e non solo, di cui l'AgID si fa promotrice istituzionale, si pone quindi come obiettivo quello di incentivare, coordinare e promuovere le tecnologie ITC necessarie per la semplificazione e per il risparmio: la firma digitale è uno di questi importanti strumenti.

Un tipico schema di firma elettronica basata sulla tecnologia della chiave pubblica consiste di 3 algoritmi:

- un algoritmo per la generazione della chiave che produce una coppia di chiavi: PK (Public Key) e SK (Secret Key). PK è la chiave pubblica di verifica della firma mentre SK è la chiave privata posseduta dal firmatario, utilizzata per firmare il documento
- un algoritmo di firma che, presi in input un messaggio m e una chiave privata SK produce una firma
- un algoritmo di verifica che, presi in input il messaggio m, la chiave pubblica PK e una firma σ, accetta o rifiuta la firma

Differenze tra firma elettronica e firma convenzionale

Nella tabella seguente si riportano le differenze tra la firma autografa e quella elettronica (fonte Wikipedia).

	FIRMA AUTOGRAFA	FIRMA ELETTRONICA
CREAZIONE	manuale	mediante algoritmo di creazione
APPOSIZIONE	sul documento: la firma è parte integrante del documento	fuori dal documento, ad esempio in una firma elettronica semplice l'autenticazione attraverso user id o password o come allegato: in tal caso il documento firmato è costituito dalla coppia (documento, firma)
VERIFICA	confronto con una firma autenticata: metodo insicuro basato su perizia calligrafica	uso di valutazioni tecniche (metodo insicuro) o mediante algoritmo di verifica pubblicamente noto e certificazione (metodo sicuro)
DOCUMENTO COPIA	distinguibile	indistinguibile
VALIDITÀ TEMPORALE	illimitata	limitata
AUTOMAZIONE DEI PROCESSI	non possibile	possibile

Valore giuridico della firma digitale in Italia

Nell'ordinamento giuridico italiano il termine firma digitale sta a indicare un tipo di firma elettronica qualificata, basato sulla crittografia asimmetrica, alla quale si attribuisce una particolare efficacia probatoria, tale da potersi equiparare, sul piano sostanziale, alla firma autografa.

La firma elettronica è disciplinata dal "Codice dell'amministrazione digitale" (Decreto Legislativo 7 marzo 2005, n. 82) che ha subito nel corso del tempo varie modifiche (da ultimo a opera del D. Lgs. 18 ottobre 2012 n. 179 nel testo integrato dalla Legge di conversione 17 dicembre 2012 n. 221).

Certificatori

La titolarità della firma elettronica qualificata è garantita dai "certificatori" (disciplinati dagli articoli 26-32bis), soggetti con particolari requisiti di onorabilità, che garantiscano affidabilità organizzativa, tecnica e finanziaria.

In particolare i certificatori hanno il compito di tenere i registri delle chiavi pubbliche, al fine di verificare la titolarità del firmatario di un documento elettronico.

I certificatori, inoltre, possono essere accreditati presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (DigitPA) e in tal caso vengono chiamati certificatori accreditati.

Ragione Sociale	Indirizzo della sede legale	Rappresentante legale	Man. oper. certificatore	Data iscrizione	MAN.OPER. SOTTOSCRITTO AGID
ACTALIS S.p.A.	Via dell'Aprica, 18 – 20158 Milano	Omero Narducci, Amministratore delegato	http://ca.actalis.it/	28-03-02	Manuale
Aruba Posta Elettronica Certificata S.p.A.	Via Sergio Ramelli, 8 – 52100 Arezzo (IT)	Simone Braccagni, Amministratore unico	https://ca.arubapec.it/	06-12-07	Manuale
Banca d'Italia	Via Nazionale, 91 - 00184 Roma, IT	il Governatore pro tempore	http://www.bancaditalia.it/	23-01-08	Manuale
Banca Monte dei Paschi di Siena S.p.A.	P.zza Salimbeni, 3 - 53100 Siena, IT	Giuseppe Mussari, Presidente	http://infinita.mps.it/Supporto/FirmaDigitale/Documentazione.htm	03-04-08	Manuale
Cedacri S.p.A. (già Cedacrinord S.p.A.)	via del Conventino, 1 - 43044 Collecchio (Parma)	Sergio Capatti, Presidente	http://www.cedacricert.it/	15-11-01	Manuale
Comando C4 Difesa - Stato Maggiore della Difesa	Via Stresa, 31/B - 00135 Roma, IT	Contrammiraglio Edoardo Compiani, Comandante C4 Difesa	http://www.pkiff.difesa.it/	20-09-06	Manuale
Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili	Piazza della Repubblica, 59 - 00185 Roma, IT	Claudio Siciliotti, Presidente	http://www.certicomm.it/	10-07-08	Manuale
Consiglio Nazionale del Notariato	via Flaminia, 160 - 00196 Roma, IT	Giancarlo Laurini, Presidente	http://ca.notariato.it/	12-09-02	Manuale
Consiglio Nazionale Forense	via Arenula, 71 - 00196 Roma (IT)	Guido Alpa, Presidente	http://www.consiglionazionaleforense.it/site/home/cnf/certification-autority.html	10-12-03	Manuale
ICBPI - Istituto Centrale delle Banche Popolari Italiane S.p.A.	Corso Europa, 18 - 20122 Milano	De Censi Giovanni (Presidente)	https://ca.icbpi.it/	17-12-12	Manuale
In.Te.S.A. S.p.A.	Corso Orbassano, 367 - 10137 Torino IT	Antonio Taurisano, Direttore Generale e Amministratore Deleg	http://e-trustcom.intesa.it/	22-03-01	Manuale
Infocert S.p.A.	Piazza Sallustio, 9 - 00187 Roma (IT)	Fernando Zilio, Presidente CdA	https://www.firma.infocert.it/	19-07-07	Manuale
Intesa Sanpaolo S.p.A.	P.za San Carlo, 156 - 10126 Torino, IT	Messina Carlo, Consigliere delegato e CEO	http://ca.intesasanpaolo.com/	07-04-04	Manuale
Lombardia Informatica S.p.A.	via Don Minzoni,24 - 20158 Milano	Lorenzo Demartini, Presidente	http://www.lispa.it/CA/CPS/	16-12-10	Manuale
Namirial S.p.A.	Via Caduti sul Lavoro, 4 - 60019 Senigallia (AN), IT	Paolo Giacometti, Amministratore Unico	http://www.firmacerta.it/index.php?page=1	03-11-10	Manuale
Postecom S.p.A.	Viale Europa, 175 - 00144 Roma IT	Vincenzo Pompa, Amministratore Delegato	http://www.poste.it/	20-04-00	Manuale
Telecom Italia Trust Technologies S.r.l.	S.S. 148 Pontina - Km 29,100 - 00040 Pomezia (RM), IT	Leopoldo Genovesi, Amministratore Delegato	http://www.trusttechnologies.it/	01-01-14	Manuale

FAQ Generali sulla firma digitale

Che cos'è la firma digitale?

La firma digitale è l'equivalente informatico di una tradizionale firma apposta su carta.

La sua funzione è quella di attestare la validità, la veridicità e la paternità di un documento, come una lettera, un atto, un messaggio o, in generale, qualunque file di dati (testo, immagini, musica, ecc.). Come tale, non va confusa con altri oggetti omofoni definiti genericamente "elettronici", come ad esempio la firma autografa scannerizzata e conservata come immagine. La firma digitale è infatti il risultato di una procedura informatica basata su un sistema di codifica crittografica a chiavi asimmetriche (una pubblica e una privata), che consente:

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

Qual è il valore legale della firma digitale?

I presupposti giuridici che rendono possibili transazioni legali fatte grazie a queste tecnologie, si fondano soprattutto sull'articolo 15 comma 2 della legge 15 marzo 1997 n. 59, la cosiddetta "Bassanini 1", che recita:

"Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge...". L'attuale Codice dell'Amministrazione Digitale, D. Lgs. 7 marzo 2005, n. 82 dispone inoltre, all'art. 21, comma 2, che "il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia [della forma scritta] prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria".

Quale può essere l'utilizzo della firma digitale?

La firma digitale può essere apposta su qualunque documento informatico. Alcuni esempi:

- bilanci e atti societari
- fatture elettroniche
- notificazioni al Garante della Privacy
- iscrizione al registro dei revisori contabili
- comunicazioni degli operatori finanziari con l'Agenzia delle Entrate
- richiesta di pareri al CNIPA

Quali sono gli obblighi e le responsabilità dell'utente?

L'utente deve:

- verificare le informazioni contenute nel certificato relative alla chiave pubblica della coppia di chiavi utilizzata;
- verificare la data di scadenza del certificato;
- verificare lo stato del certificato (se e' valido, se e' stato revocato o sospeso).

Che cos'è la Marcatura Temporale?

La marcatura temporale di un documento informatico consiste nella generazione, da parte di una terza parte fidata, di una firma digitale del documento (anche aggiuntiva rispetto a quella del sottoscrittore) cui è associata l'informazione relativa ad una data e ad un'ora certa. La marcatura temporale consente quindi di stabilire l'esistenza di un documento informatico a partire da un certo istante temporale e di opporlo a terzi.

Che cos'è un Ente Certificatore?

Nello scenario delineato occorre garantire l'identità dei soggetti che utilizzano la firma digitale, fornire protezione nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività connesse, assicurare la solidità e sicurezza dei sistemi operativi e della struttura organizzativa.

Questo rende necessario ricorrere all'intervento delle cosiddette "Terze Parti Fidate", cioè soggetti terzi che si trovano in posizione di neutralità rispetto agli utilizzatori della firma digitale: sono quelli che la legge italiana definisce "Certificatori", mentre negli Stati Uniti sono detti "Autorità di Certificazione" (Certification Authority e nell'uso corrente CA).

Che cosa fa un Ente Certificatore?

I Certificatori svolgono, tra gli altri, i seguenti compiti fondamentali:

- verificano ed attestano, emettendo un apposito certificato digitale, l'identità del titolare ed eventualmente la veridicità di una serie di altre informazioni;
- stabiliscono il termine di scadenza dei certificati;
- pubblicano il certificato e la chiave pubblica;
- ricevono la segnalazione di eventuali smarrimenti, furti, cancellazioni, divulgazioni improprie di chiavi private e pubblicano quindi la lista dei certificati revocati o sospesi in conseguenza di tali fatti.

Cosa è il certificato di sottoscrizione?

E' un certificato presente all'interno del dispositivo di firma (Smart Card o token USB), rilasciato dall'ente certificatore autorizzato. Esso è un insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica. Nel certificato compaiono altre informazioni tra cui il Certificatore che lo ha emesso, il periodo di tempo in cui il certificato può essere utilizzato, ecc. Lo scopo di questo certificato è di dare il valore della "forma scritta" ai documenti informatici.

Cosa è il certificato di autenticazione?

E' un certificato che può essere presente all'interno del dispositivo di firma (Smart Card o token USB), rilasciato dall'ente certificatore autorizzato. Nel certificato compaiono altre informazioni tra cui il Certificatore che lo ha emesso, il periodo di tempo in cui il certificato può essere utilizzato, ecc. Lo scopo di questo certificato è quello di firmare messaggi di posta elettronica (garanzia dell'identità del mittente); può anche essere usato per accedere a siti web (al posto di user/password). A questo certificato, al momento del rilascio, viene associato un indirizzo di posta elettronica in modo univoco, quindi il certificato potrà essere usato solo con quell'indirizzo.

Che cosa sono le Smart Card?

Le Smart Card e i token USB, dispositivi di firma utilizzati per la firma digitale e i servizi di identificazione, sono apparati elettronici in grado di conservare in maniera protetta le chiavi private e di generare al loro interno la firma digitale. Utilizzano microprocessori basati su standard previsti dalla legge, nei quali sono implementate avanzate tecnologie crittografiche in un ambiente con standard di sicurezza molto restrittivi.

Chi può richiedere la Smart Card?

I requisiti necessari per richiedere all'Ente Certificatore InfoCert un dispositivo di firma digitale sono:

- aver compito 18 anni;
- essere in possesso del codice fiscale;
- essere in possesso di un documento di identità in corso di validità.

Condo Free

www.condofree.net

PROCEDURE STANDARDIZZATE

www.procedurestandardizzate.net

CONTRIBUTI TERREMOTO

www.contributiterremoto.net

50 DETRAZIONE

www.detrazione50.net

65 DETRAZIONE

www.detrazione65.net

IL CONTO TERMICO

www.ilcontotermico.net

Building Free

www.buildingfree.net