Firma Digitale

E’ il risultato di una serie di complesse procedure crittografiche, informatiche ed amministrative.

Normata e riconosciuta legalmente in Italia dal 1999, è l’equivalente elettronico della tradizionale firma autografa su carta.

È associata stabilmente al documento elettronico sulla quale è apposta e ne attesta:

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

Come funziona

Firmare un documento elettronico è un’attività assai semplice e veloce e per eseguirla è necessario essere dotati di un PC o simili (smartphone, tablet ,…) e un Kit per Firma Digitale o Firma Remota.

Firma Digitale con smart card

Il Kit per Firma Digitale è composto da:

- Dispositivo sicuro di generazione delle Firme (Smart Card)
- Lettore di Smart Card
- Software di Firma e Verifica

Installato il Kit sul proprio computer/device, attraverso il Software di Firma, sarà possibile selezionare il documento elettronico da sottoporre a Firma Digitale ed eventualmente alla Marcatura Temporale.

Al momento della Firma del documento, il software chiederà l’inserimento del codice di protezione del dispositivo (PIN) e - se correttamente inserito – si procederà con la creazione del file firmato digitalmente.

La smart card è strettamente personale ed è responsabilità del suo titolare utilizzarla e conservarla in modo sicuro. Stessa attenzione deve essere posta per il codice di accesso che deve essere ricordato oppure deve essere conservato in luogo protetto, accessibile solo al titolare e diverso dal luogo in cui è normalmente conservata la smart card.

La smart card e/o il codice di accesso NON possono essere affidati o comunicati a terzi.

In caso di smarrimento o furto o sospetto utilizzo da parte di altri soggetti della propria smart card l’utente dovrà :

1) Sporgere DENUNCIA alle autorità di pubblica sicurezza

2) presentarsi con copia della denuncia all'ufficio che gliel'ha rilasciata per richiedere la revoca della carta smarrita / rubata e il rilascio di una nuova carta

In Istituto la "firma digitale con smart card" è distribuita insieme alla Carta Nazionale dei Servizi (CNS), carta a microprocessore simile a una carta di credito, che viene fornita a coloro che necessitano di usufruire dei servizi erogati on line dalla pubblica amministrazione o di utilizzare la firma in applicativi che richiedano esclusivamente tale tipo firma (es. per la firma delle fatture)

Firma Digitale Remota

Il servizio di Firma Remota rivoluziona il mondo della Firma Digitale: per la sottoscrizione dei documenti digitali non è più necessaria la Smart Card ma è sufficiente utilizzare un computer collegato ad Internet, le credenziali d'accesso (utente e password), una OTP (One Time Password) generata attraverso un apposito dispositivo (Token OTP con Display o App per Smartphone)

ed un Software di Firma, attraverso il quale sarà possibile selezionare il documento elettronico da sottoporre a Firma Remota.

Le OTP (password dinamiche) sono considerate il sistema più sicuro per l'accesso ai sistemi informatici e vengono generate direttamente all'interno dei dispositivi OTP. Trattandosi di password momentanee (scadono alcuni secondi dopo essere state generate) non rendono necessaria all'utente finale la memorizzazione, eliminando di conseguenza i problemi ed i rischi relativi all'utilizzo delle tradizionali password statiche.
Il kit di Firma Digitale Remota non comprende il certificato di autenticazione di tipo CNS, pertanto il kit non può essere utilizzato per effettuare l'accesso ai portali web della Pubblica Amministrazione che richiedono l'autenticazione tramite Smart Card.

Il dispositivo per generare la OTP è strettamente personale ed è responsabilità del suo titolare utilizzarlo e conservarlo in modo sicuro. Stessa attenzione deve essere posta per le credenziali d'accesso che devono essere ricordate oppure deve essere conservate in luogo protetto, accessibile solo al titolare e diverso dal luogo in cui è normalmente conservata il dispositivo OTP.

Il dispositivo per generare la OTP e/o le credenziali d'accesso NON possono essere affidati a terzi.

In caso di smarrimento o furto del dispositivo OTP è necessario contattare l'ufficio che l'ha rilasciato in modo da poter bloccare tale dispositivo ed ottenene uno nuovo.

Modalità di firma

- **Firma Singola**: i documenti vengono firmati singolarmente e richiedono l'inserimento del PIN/OTP per ogni documento firmato
- **Firma Multipla**: Una lista di documenti è presentata al firmatario che ha facoltà di aprirli uno per uno, ma vengono firmati richiedendo una sola volta il codice di accesso (PIN/OTP)
- **Firma Massiva o Automatica:** modalità che ben si applica a situazioni con grandi moli di documenti per i quali la firma rappresenta solo una semplice vidimazione del processo a monte della produzione del documento stesso. I documenti di un determinato flusso risultano firmati da un unico soggetto che è il titolare della firma massiva o automatica.

- **Firme Parallele, Controfirme, "a matrioska"**: nel caso in cui ad un medesimo documento debbano essere apposte più firme digitali si utilizza questo tipo di firma che consente di dimostrare che più persone abbiano assunto la paternità e/o la responsabilità del documento, eventualmente in momenti diversi, così come spesso avviene nel caso della tradizionale firma autografa (es. referto di Anatomia Patologia con refertatore principale e vari lettori)

I tipi di firma digitale riconosciuti dalla normativa vigente

- CAdES (es. FileFirmato.p7m)
- PAdES (es. FileFirmato.PDF)
- XAdeS (es. FileFirmato.XML)

Si rimanda ad altra documentazione la descrizione di dettaglio degli standard sopra citati.

E possibile associare alla firma digitale anche la marcatura temporale che consente di collocare nel tempo a norma di legge il momento della firma, consentendo quindi di ottenere una validazione temporale opponibile a terzi a tutti gli effetti. (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005).

La firma digitale in Istituto oggi

L'Istituto ha deciso di utilizzare la **firma digitale remota** all'interno dei principali applicativi aziendali mentre si dovrà utilizzare la firma digitale tramite smart card per i quei processi di firma che lo richiedono obbligatoriamente.
E' quindi possibile effettuare la firma digitale utilizzando:

- il software Aruba Sign / File Protector per la firma di singoli documenti
- la funzionalità di firma digitale remota disponibile o in fase di implementazione sui principali applicativi aziendali per la quale si rimanda alla documentazione specifica

I documenti firmati all'interno dell'azienda possono appartenere ad una delle seguenti tipologie :

- documenti provenienti da enti o ditte esterni a cui l'utente deve apporre la propria firma nell'ambito delle proprie funzioni istituzionali
- documenti prodotti da procedure aziendali (referti, registri operatori, ecc) di cui l'utente firmatario assume la responsabilità
- documenti singoli prodotti dal firmatario con strumenti di informatica individuale (es Word)

In Azienda, analogamente a quanto già avviene per la firma autografa, è possibile firmare solo i documenti di cui l'utente può assumere responsabilità e titolarità nell'ambito del proprio ruolo aziendale.
Al di fuori dell'Istituto la firma digitale fornita da AOU San Martino-Ist può essere utilizzata anche per scopi personali ma solo nel caso in cui la firma non sia stata associata allo specifico ruolo ricoperto all'interno dell'azienda (es. firma come Direttore U.O.). Al momento non sono state rilasciate carte associate ad un ruolo specifico.
Qualunque documento elettronico prodotto in azienda e firmato digitalmente deve essere per legge sottoposto ad un particolare processo di archiviazione detto "conservazione sostitutiva".
Allo scadere del rapporto di lavoro con l'azienda e comunque in tutti i casi di uso illecito / abuso le credenziali di firma verranno revocate dall'Istituto. Prima del termine del rapporto di lavoro il dipendente deve riconsegnare all'ufficio che gli ha rilasciato il certificato di firma tutto il kit in suo possesso (carta, otp, ecc) e firmare un opportuno modulo in modo che sia possibile procedere alla revoca del suo certificato.

Come richiedere la firma digitale

La firma remota è in fase di distribuzione per tutti quei dipendenti che devono sottoscrivere i documenti prodotti digitalmente dalle procedure aziendali (es. medici di laboratorio, anatomo patologi, chirurghi, radiologi, ecc.) per le quali è stata implementata tale funzionalità.
Per esigenze particolari di firma al di fuori di questi flussi la richiesta di attribuzione del kit di firma deve essere effettuata utilizzando il sistema di help desk informatico con categoria FIRMA DIGITALE ed indicando chiaramente lo scopo per cui deve essere utilizzata.
La richiesta verrà valutata in modo da poter valutare l'opportunità del rilascio ed il tipo di firma più adatto e nel caso di esito positivo l'utente verrà indirizzato verso l'ufficio preposto.

FAQ

Domanda :

Perché devo compilare e firmare un modulo intestato ad Aruba Pec S.p.A ? Il mio referente deve essere l'Azienda ospedaliera e non Aruba Pec S.p.A., è l'Azienda che deve fare un contratto con i fornitori di un servizio informatico e non il singolo dipendente.

Risposta :

L'Istituto con delibera n.1270/2013 ha stipulato un contratto nei confronti di Aruba Pec S.p.A. in quanto i certificati di firma devono essere rilasciati da un ente certificato riconosciuto dalla normativa e il nostro Istituto non è abilitato a tale rilascio. All'interno dell'Istituto sono stati individuati alcuni operatori con profilo CDRL in grado di emettere, utilizzando l'apposita procedura messa a disposizione da Aruba, dei certificati di firma digitale a pieno valore legale. Tutte le

pratiche amministrative e legali connesse a tale rilascio sono svolte da tali operatori e dai loro assistenti, abilitati alla consegna dei certificati di firma previo riconoscimento de visu del dipendente a cui deve essere consegnata.

Domanda :

Posso utilizzare il certificato di firma anche per firmare singoli documenti ?

Risposta :

E' possibile utilizzare i due software messi a disposizione dall'Istituto (File Protector per smarcard, ArubaSign per firma remota) per firmare documenti singoli a patto che tali documenti siano firmati dall'intestatario della firma in veste personale e che lo stesso ne curi la conservazione.

ulteriori FAQ saranno pubblicate sul sito intranet dell'Istituto