Firma Semplice Adobe: la firma digitale per tutti

La soluzione che facilita e rende intuitivo l'uso della firma digitale

Nell'ultima decade, i processi di business sono stati influenzati dalla tecnologia digitale ad una velocità impressionante. Oggi, milioni di persone in Europa e nel mondo sono coinvolti in processi Business-to Consumer (B2C), Government-to-Consumer (G2C) e Business-to-Business (B2B) attraverso Internet.
Muovendo da un mondo cartaceo alla promettente "electronic society", le firme elettroniche rappresentano un catalizzatore a supporto delle comunicazioni, transazioni e commerci elettronici. La disponibilità di firme elettroniche ha guidato lo sviluppo di applicazioni di eBusiness e e Government come dimostrano numerose realizzazioni messe in atto negli ultimi anni.

La firma digitale qualificata rappresenta in Europa la firma elettronica col massimo valore legale. Per la generazione e la custodia sicura delle chiavi di firma richiede l'uso di un apposito dispositivo hardware (SSCD), tipicamente una smartcard oppure una "chiavetta" USB. Per poter usare tale dispositivo, l'utente deve installare appositi driver sul proprio computer. Questa fase iniziale è gestibile in molti contesti, specialmente quando gli utenti non sono troppo numerosi, utilizzano PC di configurazione nota ed operano nell'ambito di un'organizzazione che può dar loro assistenza tecnica. Questo vale anche per le successive fasi del suo impiego.
Quando invece gli utenti sono molto numerosi (da migliaia fino a milioni di utenti) ed operano in ambienti eterogenei, gli strumenti tradizionali di firma digitale possono rivelarsi problematici, oltre che eccessivamente costosi.

LA FIRMA DIGITALE REMOTA

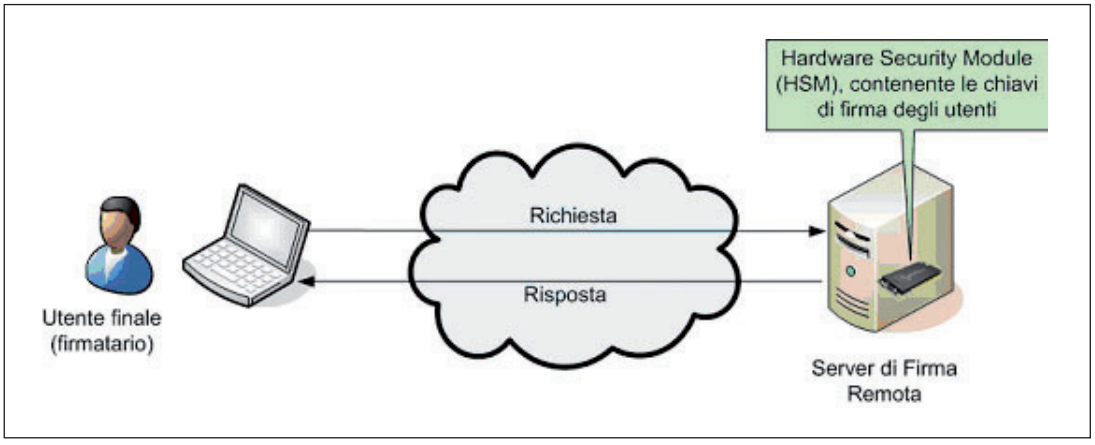
Per facilitare l'adozione della firma digitale in tali contesti, può essere utile cambiare approccio, per esempio adottando una soluzione di firma remota. Con firma remota si intende un'operazione di firma digitale eseguita con una chiave privata non residente su un dispositivo locale dell'utente (come la smartcard), bensì custodita presso un provider remoto all'interno di un HSM (dispositivo crittografico hardware). Questa tecnica consente di eliminare alla radice tutte le complessità legate all'uso di dispositivi locali e quindi consente di semplificare drasticamente l'esperienza d'uso dell'utente, rendendo la firma digitale accessibile anche per utilizzi sporadici e da parte di soggetti non in grado di sostenere operazioni di installazione software e hardware pur semplici.
Mediante tecniche sicure e affidabili l'utente accede al dispositivo di firma remoto attraverso la rete Internet e con una semplice operazione di autenticazione è in grado di sottoscrivere digitalmente qualsiasi documento.

LO STANDARD DI FIRMA DIGITALE PDF

Lo standard PDF (ISO 32000), riconosciuto in Italia e in molti altri paesi del mondo, supporta nativamente funzioni di firma digitale e marca temporale. A differenza di altri formati che realizzano la firma digitale mediante una tecnica di imbustamento (es. P7M), il PDF incorpora la firma digitale nel documento stesso rendendo l'esperienza dell'utente simile alla firma su carta, sia con semplici documenti testuali che con complessa Modulistica Intelligente, consentendo di soddisfare anche casi d'uso articolati come i processi approvativi o autorizzativi.
L'uso della firma digitale con Adobe Acrobat e Adobe Reader è molto semplice. Predisponendo o tracciando a mano sulla pagina un campo-firma è possibile contestualizzare la firma digitale nel contenuto del documento e l'operazione di sottoscrizione si limita ad un clic di mouse sul campo stesso.

LA SOLUZIONE FIRMA SEMPLICE

Firma Semplice è la soluzione di firma digitale remota PDF proposta da Adobe. La caratteristica saliente è l'utilizzo delle applicazioni Adobe Acrobat e Adobe Reader per apporre firme e marche temporali in conformità allo standard ISO 32000 e alla specifica ETSI TS 102 778. Questo non solo consente di apporre firme digitali su documenti PDF con la massima facilità e naturalezza ma, grazie alla diffusione e alla gratuità di Adobe Reader, le funzionalità di Firma Semplice sono già disponibili per milioni di utenti.
Per utilizzare Firma Semplice, l'utente deve sottoscrivere un rapporto di fornitura del servizio di certificazione presso un Certificatore Accreditato al CNIPA. Il servizio prevede una fase di identificazione e registrazione che si completa con l'emissione del certificato di firma e la consegna delle credenziali di accesso. Il tutto si traduce in una semplice configurazione che viene convalidata con una autenticazione di conferma.
Al termine l'utente avrà a disposizione il proprio strumento di Firma Semplice e richiamando la funzione di firma di Adobe Acrobat potrà utilizzarla immediatamente.
Al clic di mouse su un campo-firma appare una finestra di dialogo personalizzata dal Certificatore che eroga il servizio di firma remota e che richiede l'autenticazione all'utente. Una volta effettuata con successo l'autenticazione, il server dialoga con Adobe Acrobat, genera e restituisce la firma digitale; questa viene incorporata nel documento PDF e viene rappresentata visivamente secondo le preferenze dell'utente.



LE MODALITÀ DI AUTENTICAZIONE

Presso il provider, ogni utente ha a disposizione all'interno dell'HSM la propria coppia di chiavi RSA di firma digitale e il corrispondente certificato. Per poter effettuare la firma l'utente deve sottoporsi ad autenticazione, ovvero deve dimostrare al provider di essere il legittimo titolare delle credenziali di firma. La soluzione Firma Semplice supporta diverse tecniche di autenticazione che consentono di soddisfare esigenze applicative e operative molteplici.
La più semplice modalità di autenticazione si basa sull'invio al server del proprio nome-utente (user-id) e di una password statica. Questa soluzione, tuttavia, non consente di operare in regime di firma digitale qualificata. Per rispettare i requisiti di sicurezza imposti dalle norme vigenti, è necessaria un'autenticazione a due fattori, quali ad esempio un dato che solo l'utente conosce oppure un oggetto che solo l'utente possiede. Le modalità che consentono di ottenere una firma remota qualificata sono: autenticazione CID e autenticazione OTP.

AUTENTICAZIONE CID (CALLER IDENTIFIER)

Questa modalità di autenticazione richiede all'utente di effettuare una chiamata al numero telefonico del servizio mediante il proprio telefono cellulare, qualche istante prima di inviare la password statica del proprio account di firma remota. La telefonata viene ricevuta dal provider, che ne verifica la provenienza dal numero di telefono (Caller IDentifier, CID) preventivamente associato all'utente in fase di registrazione e autorizza l'operazione di firma digitale.
I due fattori di autenticazione sono in questo caso la password statica (informazione che solo l'utente conosce) e il numero di telefono (dato dalla SIM che solo l'utente possiede).
Questo tipo di autenticazione viene anche detta "Call drop" oppure "Call truncation" in quanto non viene attivata una conversazione e la telefonata, dopo qualche secondo, viene chiusa dal server. L'utente non riceve mai una risposta alla propria chiamata, pertanto non incorre in alcun costo telefonico. Tra i vantaggi di questa tecnica vi sono l'estrema economicità e praticità in quanto non è richiesta l'uso di alcun dispositivo fisico di autenticazione ed è molto facile da usare, semplice come fare una telefonata.

AUTENTICAZIONE OTP (ONE TIME PASSWORD)

Questa modalità di autenticazione richiede che l'utente utilizzi, in aggiunta alla password statica, anche una password dinamica. Essa viene generata mediante un apposito dispositivo OTP (generatore di password monouso) che viene fornito all'utente.
I due fattori di autenticazione sono tre, in questo caso: la password statica (informazione che solo l'utente conosce), il dispositivo OTP (oggetto che solo l'utente possiede) e la password dinamica (informazione che solo il proprio dispositivo OTP può generare, per una sola volta).
Questa soluzione è particolarmente vantaggiosa quando l'utente è già dotato di un token OTP (per esempio per accedere a servizi di Internet banking), ma il dispositivo può essere sostituito da un generatore OTP software da caricare sul proprio smartphone o palmare, unendo sicurezza assoluta, economicità e praticità della soluzione.

SICUREZZA E CONFORMITÀ DI FIRMA SEMPLICE

Il Certificatore Accreditato che eroga il servizio Firma Semplice è tenuto ad adottare tutti i requisiti e accorgimenti richiesti dalla normativa vigente che regolamenta l'attività di certificazione. Dal punto di vista della sicurezza fisica i dispositivi HSM e i server che gestiscono le operazioni di autenticazione vengono tipicamente ospitati in locali controllati e protetti da sistemi antintrusione; gli accessi sono consentiti solo agli operatori autorizzati e sono automaticamente registrati ed archiviati.
La comunicazione tra il client (Adobe Acrobat) e il server di firma del provider è protetta mediante SSL (Secure Socket Layer), con chiavi di cifratura di almeno 128 bit. Questo riduce

drasticamente il rischio di attacchi di tipo Man-In-The-Middle (MITM). Le chiavi di firma degli utenti sono gestite da HSM (Hardware Security Module) di alta qualità e prestazioni, dotati di certificazione Common Criteria di livello EAL4+, a garanzia del pieno rispetto dei requisiti di sicurezza imposti dalle norme vigenti.
Il certificato di firma viene rilasciato all'utente previa identificazione certa del medesimo, nel rispetto del Manuale Operativo del Certificatore. Il certificato contiene un identificativo di policy (OID) specifico per la firma automatica in modalità remota, e può includere limitazioni d'uso e di valore delle transazioni secondo necessità.
Il server di firma remota assicura che l'uso di una chiave di firma venga permesso solo a seguito dell'autenticazione sicura dell'utente titolare della chiave. L'autenticazione (sia essa CID o OTP), non può essere elusa dal provider, nemmeno dall'amministratore del sistema. Il Certificatore inoltre definisce e si impegna a rispettare una Security Policy dei propri servizi di firma remota.

La policy descrive le funzionalità di sicurezza di cui è dotato il sistema, le misure adottate per contrastare le minacce di sicurezza e le regole di sicurezza organizzativa ed operativa.

FIRMA SEMPLICE IN ANTEPRIMA A OMAT

In occasione di Omat 2009 Roma viene presentato il primo servizio di Firma Semplice, realizzato dalla collaborazione tra Adobe, Actalis e AndXor.

Adobe (www.adobe.com/it) presenta le funzionalità di Firma Semplice disponibili all'interno della famiglia di prodotti Adobe Acrobat 9:

- Adobe Acrobat 9 Pro, la suite completa per la creazione, conversione e gestione di documenti elettronici in formato PDF;
- Adobe Reader 9, il visualizzatore gratuito che è anche in grado di realizzare firme digitali attraverso specifiche abilitazioni (Reader Extensions)
- I prodotti saranno presentati su piattaforme Windows, MacOSX e Linux.

Actalis (www.actalis.it) offre un servizio di Firma Semplice caratterizzato da:

- alte prestazioni (transazioni per unità di tempo),
- elevata scalabilità (numero di utenti e chiavi gestibili),
- alta disponibilità, grazie ad un'architettura HW potente e ridondata;
- massima flessibilità (modalità di autenticazione e modalità di integrazione)
- piena integrazione con i restanti servizi PKI di Actalis (WebRA, OCSP, time-stamping)

AndXor (www.andxor.it) mette a disposizione gli apparati Krypto Evolution che supportano il protocollo sicuro di comunicazione di Firma Semplice:

- Apparato completo, auto-consistente, centralizzato, scalabile e sicuro, KryptoEvolution è la soluzione ideale per affrontare le problematiche di Firma Digitale in maniera semplice ed efficace;
- Gestione di chiavi RSA per la cifratura e la firma digitale fino a 4096 bit;
- Integra una scheda HSM certificata secondo Common Criteria EAL4+.

Adobe

Adobe Systems Italia
Centro Direzionale Colleoni, Pal. Taurus A3
V.le Colleoni, 5 - 20041 Agrate Brianza (MB)

www.adobe.com
www.adobe.com/it