ISTRUZIONI E SOLUZIONI PER GARANTIRE LA MASSIMA SICUREZZA NELL'IMPIEGO DEI PRODOTTI POSTECERT FIRMA DIGITALE E POSTA ELETTRONICA CERTIFICATA

Roma, 9 febbraio 2009

Firma Digitale

La Firma Digitale, basata su un certificato qualificato, utilizza dispositivi crittografici chiamati Smart Card.

La Smart Card per la Firma Digitale è dotata di certificazioni di sicurezza che offrono un grado di fiducia elevato (impossibilità di conoscere la chiave privata con cui si appone la firma, impossibilità di copiarla o di intercettarla).

Per firmare digitalmente un documento elettronico è necessario disporre di un software adatto ad interagire con la Smart Card.

I software rilasciati dai Certificatori Accreditati devono rispettare quanto delineato dalle Regole Tecniche emanate dal C.N.I.P.A. come l'utilizzo di specifici algoritmi di generazione e verifica della Firma Digitale e marche temporali.

I software distribuiti da Postecom, attraverso il kit di Firma Digitale o posteKey sono conformi ai requisiti normativi vigenti.

Per il particolare utilizzo del software distribuito con la Firma Digitale, si raccomanda di seguire le regole minime di sicurezza descritte nel seguito del presente documento.

Posta Elettronica Certificata

La Posta Elettronica Certificata utilizza, come tecnologia di base, quella della posta elettronica standard.

Ciascun utente può accedere alla propria casella di Posta Elettronica Certificata attraverso i client commerciali di posta elettronica standard (ad esempio Outlook o Thunderbird) ovvero utilizzando specifici applicativi ad hoc. A tale fine, Postecom mette a disposizione un indirizzo web, accessibile in modalità sicura SSL (https://pec.poste.it), con il quale è possibile effettuare, ad esempio, le attività di lettura/scrittura dei messaggi e cambio password.

Poiché gli strumenti di gestione delle caselle si basano su applicazioni standard liberamente scelti dall'utente e non necessariamente forniti da Postecom, diventa un elemento cruciale per l'affidabilità del processo, la sicurezza della propria postazione.

Per i motivi sopra esposti e per un corretto utilizzo della Firma Digitale e della Posta Elettronica Certificata è bene osservare le norme minime di sicurezza di seguito riportate.

LA SICUREZZA DELLA PROPRIA POSTAZIONE

L'attuazione di alcune regole comportamentali adottate nella gestione del personal computer assumono una importanza rilevante per la riduzione del rischio di malfunzionamenti nell'utilizzo dei servizi Postecert di Firma Digitale e Posta Elettronica Certificata.
Nella gestione tradizionale dei documenti, l'apposizione della firma viene generalmente effettuata rispettando un insieme di cautele derivanti dall'importanza del documento che si sta firmando. Così pure, vengono conservati al sicuro, rispetto a possibili appropriazioni di terzi, gli strumenti come timbri, punzoni, carta intestata e quant'altro contribuisce alla formazione del documento.
Analogamente, opportune regole di sicurezza vanno tenute in considerazione nel caso di una postazione che possa essere utilizzata per trasmettere telematicamente documenti informatici attraverso caselle di Posta Elettronica Certificata ovvero per la Firma Digitale di un documento elettronico.

Di seguito le principali regole di comportamento che è necessario osservare:

- la postazione di lavoro deve essere opportunamente configurata in modo che l'accesso ad essa avvenga solo previo inserimento di un "codice identificativo" (*nome utente*) e un "codice di accesso" (*password*). Il "codice di accesso" è da ritenersi strettamente personale e deve essere custodito in modo tale da evitarne la conoscenza a terzi non autorizzati all'accesso alla postazione. Inoltre, il "codice di accesso" deve essere non predicibile, e rinnovato periodicamente;

- è molto importante proteggere la propria postazione di lavoro con l'utilizzo di un idoneo software Antivirus accertandosi che questo sia sempre attivo ed aggiornandolo periodicamente;

- in merito alle versioni e agli aggiornamenti del sistema operativo Microsoft installato sulla postazione utente, accertarsi che il relativo servizio "Aggiornamenti automatici" sia attivo, oppure controllare periodicamente quanto disponibile sul sito: http://windowsupdate.microsoft.com ed eseguire gli aggiornamenti ad alta priorità segnalati;

- se il PC è collegato ad una rete (Intranet o Internet) assicurarsi di aver preventivamente attivato il personal firewall già presente nei più recenti sistemi operativi Microsoft. In mancanza di un personal firewall si consiglia di dotarsi di uno degli strumenti di mercato dedicati alla protezione della postazione;

- l'installazione di programmi di provenienza non fidata deve essere assolutamente evitata;

- nell'utilizzo della posta elettronica, si raccomanda di non effettuare il *download* o l'apertura di file o prodotti di natura incerta e provenienti via posta elettronica da mittenti sconosciuti; tali file, generalmente di tipo ".EXE" o di tipo ".ZIP", possono essere portatori di programmi che compromettono la funzionalità della postazione di lavoro e di tutti gli applicativi installati; tra le misure precauzionali, è inoltre buona norma disattivare la funzione di visualizzazione in anteprima dei messaggi in arrivo;

- analogamente, nell' accesso a siti Internet si raccomanda di non effettuare il *download* o di eseguire programmi disponibili su Internet (generalmente di tipo ".EXE" o di tipo ".ZIP") dei quali non si conosca l'origine e lo scopo.

La Firma Digitale, utilizzando applicazioni e strumenti hardware specifici, e la Posta Certificata, avvalendosi di client di posta standard per l'accesso al servizio, presentano ulteriori regole di comportamento come di seguito sinteticamente riportato per ogni servizio Postecert.

- l'installazione di "firmaOK!gold" o della "PosteKey" deve essere effettuata unicamente dal prodotto orginale (CD-Rom o PosteKey);

- in caso di dubbi sull'integrità della postazione o del software su di essa installato, si raccomanda di verificare la sicurezza dell'ambiente in cui il processo di firma viene eseguito e di controllare e provvedere periodicamente agli aggiornamenti presenti sul sito (disponibili nell'area Download a partire dal sito postecert.poste.it);

- in caso di utilizzo di firmaOK!gold controllare periodicamente, mediante l'applicazione "Verifica integrità di firmaOK!gold", che il software per l'apposizione della Firma Digitale sia una versione controllata;

- per l'uso delle Smart Card si raccomanda di custodire i codici di utilizzo (PIN) o di sblocco della Smart Card (PUK) con la massima diligenza e a non consentirne l'utilizzo a terzi. In caso di smarrimento della Smart Card o delle credenziali segrete di accesso alla carta, si raccomanda di procedere immediatamente alla richiesta di revoca/sospensione del certificato qualificato utilizzando i canali messi a disposizione dei titolari;

- i documenti elettronici creati con i prodotti Microsoft Word e Microsoft Excel possono contenere elementi dinamici, come ad esempio *macro*, che in fase di visualizzazione potrebbero variarne il contenuto. Il DPCM 13/01/2004, art. 3 comma 3, sancisce che l'apposizione della Firma Digitale su documenti elettronici contenenti "macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati", non produce gli effetti previsti dalla normativa vigente per la firma elettronica qualificata.

Gli aggiornamenti ai clienti

Postecom rende disponibile nell'area del sito postecert.poste.it gli ultimi aggiornamenti del software di Firma Digitale.

Nella suddetta area viene anche messo a disposizione uno strumento di verifica dell'integrità dell'applicativo "firmaOK!gold" in grado di segnalare all' utente eventuali modifiche apportate al software originale distribuito. Utilizzando tale applicativo, l'utente può eseguire il controllo della sua postazione informatica prima di avviare il processo di firma e ogni qualvolta lo ritenga opportuno e, comunque, a seguito di una nuova configurazione del software installato sul proprio computer.

POSTA ELETTRONICA CERTIFICATA

- nell'utilizzo della casella di Posta Elettronica Certificata, è necessario custodire la password di accesso con la massima diligenza e non consentirne l'utilizzo a terzi. In caso di smarrimento, furto o perdita della stessa, si raccomanda di comunicare tempestivamente l'evento a Postecom in modo da richiedere il rilascio di una nuova password;

- per una corretta gestione della propria casella, è buona norma cambiare periodicamente la password, almeno ogni 6 mesi, utilizzando l'apposita funzionalità disponibile all'indirizzo https://pec.poste.it.

- per considerare correttamente concluso il processo di trasmissione telematica di documenti informatici tramite Posta Elettronica Certificata, è necessario che sia il mittente che il destinatario siano titolari di caselle di Posta Elettronica Certificata;

- Postecom mette a disposizione un indirizzo web per l'accesso alla propria casella di Posta Elettronica Certificata tramite il protocollo sicuro SSL. Tale protocollo garantisce la sicurezza delle informazioni che vengono visualizzate o delle operazioni che vengono effettuate (ad esempio per il cambio password) durante l'accesso alla propria casella;

- nel caso di Posta Elettronica Certificata Avanzata (dominio di posta certificata dedicato), gli Amministratori di Sistema accedono, tramite credenziali di username e password rilasciate al momento dell'attivazione, ad un indirizzo web per la creazione, cancellazione, reset password ed in generale gestione delle caselle associate al dominio in questione. Gli Amministratori del Sistema sono appositamente individuati e delegati dal Cliente intestatario del dominio e si impegnano a custodire la password con la massima diligenza e a non consentirne l'utilizzo a terzi.

Servizio di Assistenza alla Clientela
Per ogni ulteriore informazione in merito all'utilizzo delle soluzioni Postecert di Firma Digitale e Posta Elettronica Certificata, si raccomanda di contattare l'Assistenza Clienti al numero telefonico 803.160, selezionando l'opzione 3 "Servizi Internet", attivo dal lunedì al sabato dalle ore 8:00 alle 20:00.