Istruzione per garantire l'impiego dei prodotti Postecert in un ambiente sicuro.

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 una certificazione di sicurezza che offre un grado di affidabilità elevato; questi dispositivi garantiscono la riservatezza della chiave privata con cui si appone una firma e l'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 dal Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 e dalle Regole Tecniche emanate dall'Agenzia per l'Italia Digitale (AgID), come l'utilizzo di specifici algoritmi di generazione e verifica della firma digitale e marche temporali.

I software distribuiti dal certificatore Poste Italiane, 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 utilizza, come tecnologia di base, quella della Posta Elettronica Standard.

Ciascun utente può accedere alla propria casella di Posta Elettronica Certificata sia attraverso i client commerciali di posta elettronica standard (ad esempio Outlook o Thunderbird) ovvero utilizzando applicativi specifici.

A tale fine, Poste Italiane mette a disposizione un indirizzo web, accessibile in modalità sicura SSL (https://webmail.postecert.it) con il quale è possibile effettuare, ad esempio, le attività di lettura e scrittura dei messaggi e gestire il cambio password per l'accesso alla casella.

Poiché gli strumenti di gestione delle caselle di basano su applicazioni standard liberamente scelte dall'utente e non necessariamente fornite da Poste Italiane, 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.

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 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 e sia altresì attiva la tipica funzionalità di aggiornamento automatico del meccanismo di rilievo dei software malevoli;
- In merito alle versioni e agli aggiornamenti del sistema operativo installato sulla postazione utente, accertarsi che il relativo servizio "Aggiornamenti Automatici" sia attivo, in modo da garantire l'automatica applicazione delle correzioni disponibili per il proprio sistema operativo;
- Se la postazione utente è collegato ad una rete (intranet o internet) assicurarsi di aver preventivamente attivato le funzionalità di personal firewall, mirate a impedire l'utilizzo non desiderato della rete da e verso la propria postazione; in mancanza di un personal firewall di 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, in quanto principale veicolo di software malevoli (malware, virus);
- Analogamente, nell'accesso a siti internet si raccomanda di non effettuare il download o si eseguire programmi disponibili su internet (generalmente di tipo ".EXE" o di tipo ".zip") dei quali non si conosca l'origine e lo scopo.
- 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 di arrivo;

La Firma Digitale, utilizzando applicazioni e strumenti hardware specifici, e la Posta Elettronica 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.

Firma Digitale

- L'installazione di "firmaOK" o della "Postekey" deve essere effettuata unicamente dal prodotto originale (Postekey, sito postecert.poste.it);
- 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);

- 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 di accesso alla carta, si raccomanda di procedere immediatamente alla richiesta di revoca/sospensione del certificato utilizzando i canali messi a disposizione dei titolari;
- I documenti elettronici creati con i prodotti di Microsoft Word e Microsoft Excel possono contenere contenuti dinamici, come ad esempio le macro, che in fase di visualizzazione potrebbero variarne il contenuto. Il DPCM del 22 Febbraio 2013, art. 4 comma 3, sancisce che l'apposizione della firma digitale su documenti 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

Il certificatore Poste Italiane rende disponibile nell'area del sito postecert.poste.it gli ultimi aggiornamenti del software di Firma Digitale.

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 al Gestore Poste Italiane 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://webmail.postecert.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;
- Il Gestore Poste Italiane 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 riservatezza delle informazioni che vengono visualizzate o delle operazioni che vengono effettuate (ad esempio il cambio password) durante l'accesso alla propria casella;
- Nel servizio di Posta Elettronica Certificata Avanzata (dominio di posta certificata dedicato), le figure degli amministratori di sistema dell'organizzazione accedono, tramite credenziali di username e password rilasciate al momento dell'attivazione, alle funzionalità di gestione delle caselle associate al dominio in questione; tali funzionalità consentono all'amministratore la creazione e la cancellazione di caselle, il reset password e altre funzionalità rilevanti. 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 non consentirne l'utilizzo a terzi.