Sella Technology Solutions

Procedura per l'accesso al modello cifrato

La soluzione di firma elettronica avanzata erogata da Sella Technology Solutions si avvale della Certification Authority Infocert per la conservazione delle chiave di cifratura dei documenti.

Secondo quanto previsto dalla procedura interna InfoCert PR525, la Banca utilizzatrice del servizio di firma effettua richiesta di verifica del documento con apposito modulo predisposto da InfoCert tramite messaggio di posta elettronica certificata (PEC).

Tutte le attività sono svolte presso la sede di Infocert che predispone una postazione apposita così come descritto nei paragrafi successivi.

1.1. Dotazione informatica (hardware e software)

Presso i locali tecnici InfoCert sarà predisposta una postazione fisica per la verifica dei documenti firmati con firma elettronica avanzata.

Le impostazioni della postazione saranno quelle previste per la certificazione del sistema EAL4+, con i seguenti requisiti:

- Microsoft Windows 7 Enterprise Edition (32-bit and 64-bit versions)
- Lingua: English
- Versione: 6.1.7600

Il sistema avrà due soli utenti:

- Administrator: gestito dal responsabile della procedura InfoCert;
- Verificatore: gestito da InfoCert e rilasciato all'utente finale con impostazioni delle password di livello adeguato e scadenza obbligatoria.

Sul sistema saranno installati i soli programmi necessari alla verifica:

- Forensic tool, per il Gruppo Sella il programma è "Encalligrapher"; il software di verifica ENCalligrapher è fornito da Sella Technology Solutions S.p.A. ed installato da InfoCert nella postazione con il fine esclusivo dell'attività di verifica; al termine dell'attività il software verrà disinstallato da InfoCert;
- Adobe Reader X con le opportune patch e plug-in per la verifica e visualizzazione dei file firmati;
- Dike Ultima Versione, per la verifica delle firme digitali.
- Antivirus aggiornato

La postazione verrà dedicata alla Banca o al Perito per verificare le firme elettroniche avanzate, e non sarà connessa a Internet.

Per la configurazione di questa postazione si seguiranno le procedure dei manuali Microsoft per la certificazione, e sarà stato effettuato un hardening della postazione rispetto alla configurazione utilizzata in sede di certificazione della stessa Microsoft. Verrà eseguita la Windows 7 Baseline Security, nonché

l'impostazione del pacchetto di Windows 7, integrato con lo strumento Microsoft Security Compliance Manager. Il PC è utilizzato esclusivamente per l'attività di Delivery delle chiavi crittografiche ed è conservato in apposito luogo sicuro dal responsabile del servizio di Assistenza e Delivery InfoCert.

Oltre alla postazione, la dotazione per attivare la procedura richiede anche la presenza di:

- Lettore di smart card: USB standard InfoCert;
- Stampante a nastro;
- Due Buste cieche per stampa codici segreti;
- Buste standard InfoCert per l'inserimento di buste cieche.

Al termine della procedura la macchina verrà formattata a basso livello con software opportuno.

1.2. Verifica documento cifrato

Il funzionario della sicurezza della Certification Authority, accedendo alla postazione attraverso l'utenza dedicata procederà:

1. alla verifica e all'apertura della busta contente il dispositivo sicuro conservato da InfoCert, se il software di verifica presente nella WS è in grado di accedervi col protocollo PKCS#11 ovvero all'esibizione dal sistema di conservazione a norma del certificato PKCS#12;
2. alla verifica e all'apertura della busta delle password /PIN portata con sé dal Notaio il quale procederà egli stesso ad imputare la password/PIN;
3. all'avvio dello strumento software di verifica;
4. al caricamento del documento da verificare da supporto esterno;
5. allo sblocco della chiave di decifratura con le credenziali da parte del Notaio;
6. all'effettuazione della Perizia da parte del Perito grafologo nominato dall'azienda/ente;
7. al cambio password della Master Key, eseguito dal Notaio. Alla presenza della Banca e del Notaio si provvede al cambiamento della password di protezione utilizzata in precedenza.

Sarà cura del Perito la redazione del documento di perizia, anche presso il proprio studio con i dati raccolti. Nel caso il Perito non abbia terminato la perizia o non sia presente, il Notaio ha a disposizione un software di cifratura con cui, impostata a sua scelta una password, cifra i documenti decifrati precedentemente, che rende disponibili al soggetto indicato dal Cliente assieme alla chiave di decifrazione.

1.3. Emissione nuova password e ripristino della postazione

Concluse le operazioni per l'apertura del file da verificare, si effettua il ripristino della protezione (Password) del file PKCS #12 contenente la chiave privata.

Il funzionario della sicurezza della CA, tramite il software KeyPairDelivery richiederà al Notaio di impostare nuovi PIN/PUK, che rimarranno di sua esclusiva conoscenza, per il dispositivo sicuro utilizzato o una nuova PSW per il PKCS#12. Al termine il funzionario della sicurezza della CA distruggerà le buste cieche utilizzate e consegnerà le nuove buste prodotte al Notaio per la conservazione.

Il Notaio verificherà l'integrità delle nuove buste e le conserverà presso i propri Uffici; il file PKCS #12 contenente la coppia di chiavi ed il certificato saranno caricati nel sistema di conservazione a norma InfoCert. Tutti i file vengono cancellati dalla postazione e viene completata la stesura del verbale in forma cartacea: il funzionario CA effettuerà il resoconto delle operazioni effettuate, che sarà sottoscritto da tutti i partecipanti.