- Possibilità di firmare molteplici documenti senza richiedere l'inserimento del PIN;
- Modifica del PIN e sblocco della SmartCard tramite inserimento del PUK direttamente sulla Smartcard Crittografica;
- Supporto integrato all'uso di servizi di Marcatura Temporale con accesso libero via http
- Supporto Integrato all'uso di servizi di marcatura temporale con accesso riservato tramite Login e Password sempre via http (ad esempio il servizio di Marcatura di Infocamere);
- Funzione per ottenere il Riferimento Temporale tramite servizi di terzi così come previsto dalle normative, utilizzabile in alternativa alla marca Temporale;
- Creazione delle Impronte dei File in formato binario o esadecimale, con la possibilità di creare un File contenitore per tutte le impronte generate;
- Supporto diretto dei certificati privati su SmartCard tramite protocollo CSP, con possibilità di utilizzare virtualmente qualsiasi smartcard Crittografica fornita di CSP utilizzabile da terze parti;
- Funzioni di verifica per firme, marche temporali e impronte senza necessità di avere certificati e lettori collegati al PC;
- Verifiche anche on line della CRL (Certification Revocation List), della validità delle firme e dei certificati;
- Funzioni di scrittura/lettura e formattazione su Smartcard con CHIP di memoria non crittografiche e di cifratura *bufferizzata* per la cifratura massiva di File in conformità al MEF 27.07.2005;

Realizzare applicazioni di firma digitale

Le funzioni di Dimatek 3.3.1 permettono di realizzare rapidamente applicazioni che permettono di firmare un documento con un certificato installato su un Server Web senza dover spedire il documento originale, e quindi in modo molto efficiente ed immediato. L'utilizzo di questa funzionalità è molto semplice e si realizza con 3 sole funzioni DmtHash, DmtsigningHash e DmtMergeSigned più altre tre opzionali per verificare le singole operazioni effettuate: DmtVerifyHash e dmtVerifysignHash e dmtVerifysignedFile.

Una volta scelto il documento da firmare sul PC Client, si passerà la stringa, con il nome completo del File, alla funzione DmtHash che restituirà l'impronta del documento da inviare via HTTP al Server Web. Quest'ultimo, alla ricezione del messaggio, chiamerà la funzione DmtsigningHash, la quale firmerà l'impronta ricevuta e restituirà il risultato al Client. Ricevuta la risposta, l'applicazione Client chiamerà le funzioni opzionali DmtVerifyHash e DmtVerifysignHash che verificheranno la correttezza dell'impronta firmata. Se i due risultati sono verificati con successo, si passa al passo conclusivo, con la creazione della Busta P7M. Avendo a disposizione l'impronta originale, l'impronta firmata e il documento Originale, con la certezza che siano tutti integri e conformi agli originali, l'applicazione chiamerà la funzione DmtMergeSigned, la quale restituirà un file P7M composto da firma, impronta e documento originale.

Come si può facilmente intuire con questo metodo sarà possibile firmare anche documenti di grandi dimensioni e in gran quantità, con possibilità di utilizzare più certificati contemporaneamente. Tra l'applicazione Server e quella client ci sarà solo un passaggio di stringhe cifrate, non intercettabili e veloci da trasmettere.

Dimatek è disponibile in Licenza Limitata disponibile solo su un singolo PC, Licenza Singola Distribuzione con la quale si può distribuire illimitatamente la libreria abbinata però ad una solo Software e Licenza Multi Distribuzione con la quale la software house può distribuire illimitatamente Dimatek con diverse applicazioni software.

FIRMARE CON LA PROPRIA SMARTCARD

Grazie a DIMATEk è possibile apporre la propria firma autenticata sui documenti utilizzando i certificati privati della propria SmartCard emessa da Infocamere, dalle Poste (PostCert), da Actalis o da altre organizzazioni autorizzate. L'unica accortezza è quella di installare il CSP (Context Service Provider) fornito con la SmartCard che si intende utilizzare. Ad esempio, per utilizzare le SmartCard i modelli 1601, 1602 e 1603 di Infocamere è sufficiente installare il CSP CV_installation_user_infocamerecard16xx.zip, scaricabile dalla sezione Download del sito www.dataflex.it e quindi importarne i certificati tramite l'apposita Utility. Dopo di che, si dovrà configurare opportunamente la funzione DMTCREATE passandole il parametro che indica la Directory ove è stato collocata la DLL chiamata CVP11_M4.dll. Per la SmartCard 1401, si potrà invece utilizzare la funzione di setup del CSP da scaricare dall'indirizzo www.evolutionweb.com/public/CardOS_API221.zip e quindi lanciare il programma sicardintro.exe che in automatico carica i certificati della SmartCard nello Store My. La DLL da usare con Dmtcreate in questo caso sarà si_pkcs11.dll.

La libreria DIMATEK è già stata adottata da dozzine di società per le loro applicazioni software di firma Digitale, Archiviazione Sostitutiva o Fatturazione elettronica tra le quali: Banca Ifis, Brain System, Buffetti, Connect Informatica, Dylog Italia, Ergon Informatica, Ideasolution, Kartha, Sesamo Software, Sea Software.