Linee guida per l'utilizzo di strumenti crittografici nelle applicazione del MEF

(*versione ridotta*)

Ver. 2.0

Data: 26/01/2007

Redatto da: (vers. 2.0) *Luana Angelone, Diodato Marano, M. Raffaella Migliorini*

Approvato da: *M. Raffaella Migliorini*

TABELLA DELLE VERSIONI

Data	Versione	Descrizione delle modifiche	Cap. /Sez. modificati
Dicembre 2004	1.0	Nascita documento	tutti
Gennaio 2007	2.0	Integrazioni Inserimento par. Allegati Aggiornamenti Sostituzione “Thin Client” con “Layer Unico” Inserimento par. Routine di verifica firma (piattaforma UNIX) Eliminazione par. “Scenario di evoluzione”	1.1 1.2 2; 3; 3.1; 3.1.1; 3.2 3.1.2 3.2.2

INDICE

1 Introduzione 4
1.1 Definizioni ed Acronimi 4
1.2 Allegati 5
2 Descrizione del contesto 6
3 Situazione Attuale 8
3.1 Piattaforma Client 8
3.1.1 Firma e Cifra e Marca Temporale 8
3.1.2 Layer Unico 9
3.2 Piattaforma Server 9
3.2.1 Routine di Verifica Firma (piattaforma Mainframe) 10
3.2.2 Routine di Verifica Firma (piattaforma UNIX) 11
3.2.3 Alimentazione CRL 11
3.2.4 Firma Automatica 12
3.3 Utilizzo della smart card come strumento autenticazione 12
3.3.1 RACF 12
3.3.2 Single Sign-On Server 12

1 Introduzione

Il seguente documento ha l'obiettivo di illustrare le linee guida per il disegno e l'utilizzo degli strumenti di crittografia nelle applicazioni dei differenti Dipartimenti del Ministero dell'Economia e delle Finanze.

Saranno descritti il contesto normativo, i prodotti adottati, le modalità di utilizzo e le procedure attivate a supporto.

1.1 Definizioni ed Acronimi

Certificato, Certificato Digitale, Certificato X.509 ***[Digital Certificate]***
Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica; nel certificato compaiono altre informazioni tra cui:
- il Certificatore che lo ha emesso
- il periodo di tempo in cui il certificato può essere utilizzato;
- altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificatore ***[Certification Authority – CA]***
Il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati.

Chiave Privata e Chiave Pubblica
La coppia di chiavi crittografiche asimmetriche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici.

Dispositivo di firma ***[Token]***
E' un apparato elettronico in grado di conservare in modo protetto le chiavi private e di generare al suo interno firme digitali. Il dispositivo di firma utilizzato dall'utente è costituito da una carta plastica delle dimensioni di una carta di credito in cui è inserito un microprocessore. E' chiamato anche **carta a microprocessore** o **smart-card**.

Firma digitale ***[digital signature]***
Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Lista dei Certificati Revocati o Sospesi ***[Certificate Revocation List – CRL]***
E' una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza.
L'operazione è chiamata revoca se definitiva, sospensione se temporanea.

Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla lista CRL, che viene quindi pubblicata nel registro dei certificati.

PKI (Public Key Infrastructure): gerarchia di autorità di certificazione, fiduciate tra loro mediante protocolli di autenticazione standardizzati, che fornisce servizi di certificazione, distribuzione, verifica e revoca per le chiavi pubbliche utilizzate per la firma digitale e la crittografia.

RACF (Resource Access Control Facility): prodotto di Access Management su piattaforma mainframe per la gestione degli utenti/password e delle loro autorizzazioni.

SSO Server (Single Sign-on server): prodotto Oracle di Access Management per la gestione degli utenti/password e del Single Sign-on per le applicazioni web-based.

CSP (Cryptographic Service Provider): strato di componenti software/hardware che fornisce servizi di crittografia e sicurezza digitale in un Personal Computer; consente la gestione di certificati digitali, crittografia e firma digitale, dispositivi di firma ecc.

MSCAPI (Microsoft CryptoAPI): strato software ad alto livello del sistema operativo Microsoft Windows contenente le funzioni di interfaccia con i vari CSP presenti nel sistema.

PKCS (Public Key Cryptography Standards): serie di protocolli standard sviluppati da RSA Security / RSA Labs che coprono vari aspetti della sicurezza digitale.

1.2 Allegati

[...]

2 Descrizione del contesto

Il Centro Tecnico per la Rete Unitaria della Pubblica Amministrazione (CT-RUPA oggi CNIPA) è l'Ente preposto alle attività di certificazione per i soggetti che utilizzano la RUPA. Per tale ragione esso è iscritto, secondo quanto previsto dal quinto comma dell'articolo 16 del DPCM dell'8 febbraio 1999, nell'Elenco pubblico dei Certificatori, tenuto dal CNIPA ai sensi dell'articolo 27, comma 3, del DPR 445.

Per intraprendere l'attività di certificazione, il Centro Tecnico ha inteso avvalersi della facoltà, prevista dall'articolo 62 del DPCM, di utilizzare i servizi offerti da un Certificatore ufficiale, selezionato, attraverso una procedura concorsuale, da espletarsi tra quelli iscritti nell'elenco pubblico alla data di presentazione dell'offerta. La procedura si è conclusa nell'ottobre 2000, con l'aggiudicazione della fornitura alla Società Postecom S.p.A.

Il MEF, come soggetto utilizzatore dei servizi RUPA, ha aderito al servizio di certificazione delle chiavi reso disponibile alle Amministrazioni attraverso la definizione di un accordo, detto "Protocollo d'intesa", in cui sono stabiliti i principi e le modalità di interazione tra le parti.

Nell'ambito del protocollo d'intesa avviene la nomina dei referenti. I Referenti sono le figure, nominate all'interno dell'Amministrazione d'appartenenza, ai fini di costituire l'interfaccia attiva fra i Titolari e il Certificatore.

In questa prima fase sono stati messi a disposizione delle Pubbliche Amministrazioni, che ne avessero fatto richiesta, circa 60.000 smart card (comprensiva di certificati di cifra e firma) e relativo kit (costituito da: lettore *smart card*, CDROM con CBT e software)
Al momento di questa revisione (dicembre 2006) il contratto di fornitura tra CNIPA e Postecom per i servizi di Certification Authority è stato prorogato fino ad Ottobre 2007.

Dal punto di vista tecnologico in base ad una analisi di mercato il MEF individuò nel prodotto Multifunction Buffer Manager (MBM) della Telvox (società del gruppo SCAI Informatica) come l'ambiente di programmazione per lo sviluppo delle applicazioni lato server che avessero necessità di :
- ottimizzare la trasmissione dati mediante processi di compressione;
- applicare sicurezza simmetrica ed asimmetrica ai dati;
- trasformare i dati per facilitare i flussi tra applicazioni operanti in sistemi operativi uguali o differenti.

Le caratteristiche fondamentali del framework MBM sono:
- essere scritto in "C" ANSI;
- essere multipiattaforma (è disponibile sulla maggior parte dei sistemi operativi esistenti (MVS, AS400, Windows, AIX, Digital Hp etc...) presentando sempre la stessa interfaccia di programmazione, semplificando, dal punto di vista del programmatore le complessità insite negli algoritmi crittografici ;
- tutte le funzioni implementate fanno riferimento a normative emesse da:
    - ANSI = American National Standards Institute;

- CCITT = Comité Consultatif International Téléphonique et Télégraphique;
- DODCSC = Department of Defense - Computer Security Center;
- FIPS = Federal Information Processing Standards;
- ISO = International Standards Organization;
- ITU = International Telecommunication Union;
- NIST = National Institute of Standards and Technology;
- UN-ECE = United Nations - Economic Commission for Europe.

3 Situazione Attuale

In questo capitolo si descrive lo stato dell'arte sia per le piattaforme client che per quella server e si da un breve accenno alle procedure automatiche attivate a supporto di queste.

3.1 Piattaforma Client

Quanto segue è già efficace per le postazioni di lavoro del II Dipartimento. Quanto indicato, invece, è in corso di realizzazione per le postazioni del IV Dipartimento.

Nel corso del 2006 si è provveduto ad una ulteriore standardizzazione dei client mediante l'adozione del software Layer Unico CNIPA, il quale consente di virtualizzare l'accesso alle diverse Smart Card utilizzando, anziché le diverse funzioni delle librerie PKCS specifiche dei vari token, le funzioni fornite da un'unica libreria PKCS "virtuale".

Nella configurazione base di ciascuna postazione di lavoro sono supportati i seguenti componenti:

Hardware			
Lettori di Smart Card con supporto Layer Unico			
	Gemplus PC Twin USB		Lettore Smart Card USB esterno (default)
	Gemplus GemPC410		Lettore Smart Card seriale esterno
	GemPCSerial		Lettore Smart Card seriale esterno
Schede Smart Card (token) con supporto Layer Unico			
	Gemplus GemGATE CardOS M4		Attualmente non usata
	Gemplus GemGATE 32K		
	Incard Incrypto34v2DSD 2		Attualmente non usata
	Incard Incrypto34v2DSD		
	Siemens Siemens CIE		Attualmente non usata; non supportata da FCMT

Eventuali ulteriori token possono essere supportati dal Layer Unico registrando le opportune informazioni nel registro di sistema e installando le specifiche librerie PKCS.

La libreria Microsoft Capicom fornisce un'interfaccia COM alle MSCAPI ed è utilizzata nei processi di gestione automatizzata dei certificati presenti sulle postazioni client, principalmente per quanto riguarda la firma software delle applicazioni Consip.

3.1.1 Firma e Cifra e Marca Temporale

L'applicazione stand-alone Firma e Cifra e Marca Temporale (FCMT) è parte integrante del kit di firma e consente di firmare, cifrare e verificare documenti in formato elettronico, nonché di effettuare le operazioni di gestione delle smart card (cambio pin, sblocco ecc.). L'applicazione è presente su tutte le postazioni.

3.1.2 Layer Unico

La libreria Layer Unico è fornita a corredo della infrastruttura a chiave pubblica per la Rete Unitaria della Pubblica Amministrazione per agevolare lo sviluppo di applicativi implementanti funzionalità di accesso/verifica della Smart Card, di firma digitale e di lettura delle informazioni di certificati.

In tale contesto lo sviluppatore di applicazioni si disinteressa completamente di come le funzioni crittografiche vengano implementate e si concentra unicamente sul disegno della GUI e sulle modalità di integrazione delle richieste degli utenti con le funzionalità offerte dalla libreria Layer Unico.

In particolare il Layer Unico fornisce agli sviluppatori una interfaccia attraverso la quale è possibile realizzare le seguenti funzioni:

" Firma di un documento.
" Controllo del PIN della Smart Card.
" Lettura/scrittura nell'area pubblica della Smart Card.
" Lettura/scrittura nell'area privata della Smart Card.
" Lettura delle informazioni contenute in un certificato.
" Verifica della presenza/assenza della Smart Card.

Le primitive messe a disposizione dalla libreria Layer Unico possono essere invocate dalla applicazione crittografica mediante chiamata diretta alla DLL e sono disponibili per i linguaggi C, Visual Basic e Java.

La implementazione di Layer Unico è conforme agli standard PKCS11 e PKCS7 per quanto riguarda gli accessi alla Smart Card e la firma digitale.

3.2 Piattaforma Server

A supporto dello sviluppo delle applicazioni lato server è stato adottato il framework MBM della società Telvox che offre servizi di calcolo specializzati alle differenti applicazioni secondo il seguente modello:

Figura 1

A partire da queste componenti sono state sviluppate procedure , il cui disegno è stato realizzato in forma "generalizzata", in modo da costituire un patrimonio comune per tutte le applicazioni che vogliano integrare queste funzionalità nel proprio codice.

Di seguito una breve descrizione di quanto sviluppato come componente server ed i riferimenti necessari per il loro riutilizzo.

3.2.1 Routine di Verifica Firma (piattaforma Mainframe)

Sulla piattaforma OS/390 è presente una routine (SXPK07), sviluppata in COBOL che, sulla base di un parametro fornito in input dal programma chiamante, realizza le funzioni cardine per il processo di verifica delle firme.

Verifica ridotta (VERIRID)

Questo servizio permette l'estrazione del dato firmato da un PKCS#7 fornito in input. Il dato viene convertito dalla codifica ASCII alla codifica EBCDIC (secondo il code-page 037) tramite una tabella di conversione fornita in input.
Inoltre il servizio verifica la firma utilizzando il certificato presente nel PKCS#7.

Dal certificato viene estratto il valore del campo 'authorityKeyIdentifier' e, in base a questo, viene effettuata la verifica del certificato mediante la chiave pubblica (caricata in memoria nella fase di inizializzazione) avente tale valore di SKI.

Verifica estesa (VERIEST)

Il servizio, esegue le stesse operazioni del servizio VERIRID ed, in aggiunta, verifica la non-revoca del certificato rispetto alle CRL reperite. Prima di questo, estrae dal certificato l'URL della CRL corrispondente (cioè quella destinata a contenere l'eventuale revoca del certificato) e controlla che sia tra quelli da cui viene effettuato lo scarico periodico. Restituisce, infine, al chiamante il

CODICE FISCALE presente nel Common Name del Subject del certificato estratto dal PKCS#7 ricevuto.

Verifica CRL (VERICRL)

Esegue le operazioni di verifica di una o più CRL ricevute in ingresso. In particolare:
- verifica la firma della CRL.
- verifica il certificato della CA relativo alla firma della CRL.
- controlla che la validità della CRL non sia scaduta da più di 3 ore (tale valore, impostato in un parametro interno al software, è di facile modificabilità).

3.2.2 Routine di Verifica Firma (piattaforma UNIX)

La componente generalizzata di controllo della firma digitale, realizzata per la piattaforma UNIX, offre un servizio, disponibile sia come Web Services che come API Java che, dato un documento elettronico firmato digitalmente in formato PKCS#7, offre le seguenti funzionalità:

1. verifica integrità del documento;
2. verifica validità temporale del certificato del firmatario (non scaduto);
3. verifica Trust certificato del firmatario (certificato emesso da una CA accreditata CNIPA);
4. verifica validità CRL (certificato non sospeso, non revocato);
5. estrazione del documento;
6. estrazione informazioni del certificato di firma (nome, cognome, codice fiscale, CA, data inizio validità, data fine validità)

La componente è realizzata con librerie C interfacciate da classi Java tramite Java Native Interface. E' stata progettata per essere eseguita su server AIX 5.2 con IBM Java Virtual Machine 1.4.2

L'accesso al servizio può avvenire in 2 modi:
1. Le applicazioni Java presenti sullo stesso server potranno utilizzare direttamente i metodi esposti dalle classi del package JVerify.jar.
2. Tutte le altre applicazioni (non Java o residenti su server esterni) dovranno accedere tramite i Web Services della Web Application JVerifyDigitalSignWeb che ad ogni richiesta effettueranno la chiamata al metodo corrispondente del package Java.

3.2.3 Alimentazione CRL

Il processo di aggiornamento della Copia della CRL presso il MEF è una procedura che effettua il download periodico delle CRL dai siti dei certificatori per renderle disponibili alle applicazioni residenti sul sistema centrale che, per motivi di sicurezza, non hanno la possibilità di prelevarle direttamente dal web.

3.2.4 Firma Automatica

Per "firma automatica" si intende un'operazione di firma generata da un processo automatico per cui l'oggetto prodotto è integro, non ripudiabile ed in formato PKCS#7 ma non ha validità di firma autografa.

A partire da questa premessa, in ambito MEF, è stata messa a punto una procedura di Firma Automatica per sfruttare i meccanismi d'integrità sottesi all'utilizzo di chiavi asimmetriche a garanzia della trasmissione di dati tra amministrazioni in orari non presidiati.

La firma automatica è attualmente utilizzata per lo scambio di dati verso Banca d'Italia per i flussi relativi alle Contabilità speciali.

A supporto di questa procedura è stata generata, sul sistema mainframe, una coppia di chiavi, associata al responsabile della sicurezza RGS, e con il CNIPA è stato definito il processo di generazione e richiesta del Certificato per questa coppia di chiavi. Il certificato è stato generato e risiede su dataset protetti del sistema mainframe (OS/390).

3.3 Utilizzo della smart card come strumento autenticazione

Nell'ambito MEF la smart card viene utilizzata in diversi scenari di identificazione con modalità di funzionamento che differiscono sensibilmente in considerazione delle diverse epoche di realizzazione. Il primo è legato alle applicazioni che utilizzano il database RACF come "user repository" e le transazioni CICS come "business logic". Tra queste ci sono applicazioni dell'area Spese sia client/server quali Mandato Informatico e Perenti sia applicazioni "web based" quali Ordini di Accreditamento o Tesoreria.

Il secondo scenario di riferimento, per tutti i nuovi sviluppi dalla fine del 2002, è legato a tutte le applicazioni "web based" che si che utilizzano l'SSO Server come "user repository" e per le quali viene implementato un effettivo meccanismo di "strong authentication". Nei paragrafi successivi si dettagliano meglio i due scenari indicando il processo implementato ed i componenti coinvolti.

3.3.1 RACF

Prodotto per il controllo degli accessi alle risorse su piattaforma z/OS.

3.3.2 Single Sign-On Server

Come Access Manager viene utilizzato il prodotto SSO Server di Oracle. Nella versione in uso è supportata l'autenticazione multilivello.
Il livello 1 corrisponde all'utilizzo di user id e password, il livello 2 all'utilizzo della smartcard.
Il livello 2 implementa una strong authentication basata sul protocollo di handshake del SSL versione 3.

Questo protocollo di handshake consente al client ed al server di autenticarsi a vicenda e di negoziare un algoritmo di cifratura e le chiavi di cifratura da utilizzare per la protezione dei dati trasmessi.

La scelta del livello di identificazione sarà a carico dell'applicazione che può scegliere di richiedere l'autenticazione forte per alcune funzioni o per tutte.

L'SSO Server del MEF per questa funzione[1] accetta tutti e soli i certificati/smart card emesse dai certificatori qualificati CNIPA e la CNS.

[1] I certificatori qualificati CNIPA sono gli unici che garantiscono l'interoperabilità tra gli strumenti crittografici (smart card) e quindi il tracciato dei certificati e campi del filesystem.