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

Ver. 1.0

TABELLA DELLE VERSIONI

Versione	Data	Descrizione delle modifiche
1.0	Dicembre 2004	Nascita documento

INDICE

1 Introduzione

Il seguente documento ha l'obiettivo di illustrare le linee guida per il disegno e l'utilizzo degli strumenti di crittografia e di descrivere lo stato dell'arte nel loro utilizzo nelle applicazioni dei differenti Dipartimenti del Ministero dell'Economia e delle Finanza.

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
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.

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.

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)

Tra gli strumenti base messi a disposizione dal CT-RUPA, a supporto delle applicazioni, era presente una macrolibreria per la gestione del dispositivo di firma (Cryptographic Server) configurabile come:

- **Network Cryptographic Server (NCS)**: componente server che integra il motore crittografico; attende e serve connessioni client via TCP/IP, traducendo le richieste client pervenute in operazioni crittografiche.

- **StandAlone Cryptographic Server (SCS)**: componente server che integra il motore crittografico; attende e serve connessioni client via TCP/IP provenienti da *localhost*, traducendo le richieste client pervenute in operazioni crittografiche.

Questa macrolibreria si rivelò non applicabile alla realtà MEF in quanto la natura sostanzialmente asincrona del motore crittografico era difficilmente conciliabile con le transazioni on-line delle applicazioni. Il MEF chiese quindi al CT-RUPA la realizzazione di una componente client ad hoc che esponesse un set limitato di funzionalità ma che fosse direttamente richiamabile dalle applicazioni. CT-RUPA, a fronte di questa richiesta, disegnò e realizzò il ***"Thin Client"*** una libreria di funzioni crittografiche lato client.

Anche dal punto di vista server l'adozione della macrolibreria, così come fornita da CNIPA, presentava difficoltà. Si effettuò quindi una analisi di mercato che 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 ambito normativo e con gli strumenti (tecnici e consulenziali) messi a disposizione da questo accordo dal 2000 ad oggi sono state implementate le funzionalità crittografiche nelle seguenti applicazioni MEF: Si.Co.Ge., Ordine Prelevamento Fondi, Conti di Tesoreria, Ruoli di Spesa Fissa e sono state aggiornate quelle del Mandato Informatico.

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 per le quali, a fronte del progetto di "Adeguamento dell'infrastruttura del II Dipartimento", si è raggiunto un elevato grado di standardizzazione nella dotazione di base. Quanto indicato, invece, è in corso di realizzazione per le postazioni del IV Dipartimento.

Nella configurazione base di ciascuna postazione di lavoro sono presenti:
software
- GemPKCS 4.6
- Gemplus Diagnostico SMART Card
- Postecom Criptoki 1.00.008
- driver per il lettore di smart card

hardware
- lettore di smartcard Gemplus 410PC (l'ultimo lotto di fornitura è dotato di lettore su porta USB Gemplus 430PC)

Le librerie del Thin Client (ovvero tutte le librerie ThinApi*.*) sono presenti sulla postazione multifunzionale indipendentemente dall'installazione delle applicazioni che andranno poi ad utilizzarle.

3.1.1 Firma e Cifra

L'applicazione stand-alone ***Firma e Cifra*** è parte integrante del kit di firma e consente di firmare, cifrare e verificare documenti in formato elettronico. L'applicazione è presente, al momento, esclusivamente sulle postazioni dei Referenti dell'Amministrazione.

3.1.2 Thin Client

La libreria **Thin Client**, 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.

3.1.2.1 Ambito operativo

L'ambito operativo della libreria è illustrato dal seguente diagramma.

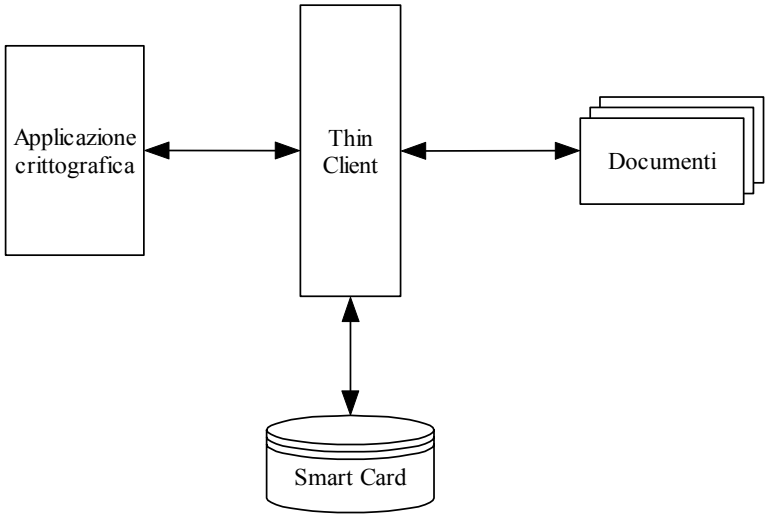


Figura 1 – Ambito operativo di Thin Client

Come rappresentato dal diagramma, la componente *Thin Client* è una interfaccia software utilizzata dalle applicazioni, per realizzare un determinato insieme di funzioni crittografiche.

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 *Thin Client*.

In particolare *Thin Client* 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 *Thin Client* 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 *Thin Client* è conforme agli standard PKCS11 e PKCS7 per quanto riguarda gli accessi alla Smart Card e la firma digitale.

In particolare l'interfaccia PKCS11 è garantita dall'adozione della libreria *gclib.dll* fornita a corredo dei lettori di Smart Card Gemplus, mentre la conformità PKCS7 è garantita dall'adozione di *OpenSSL Tookit*.

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 2

Sono attualmente disponibili le seguenti componenti del framework Multifunction Buffer Manager:

Componente	***Mainframe***	***UNIX (*)***	***Windows***
CODA (Compressione dati e conversione formato fisico del file)	√		
TA (Trasformazione alfabeti)	√	√	
HASH (Hashing)	√	√	
CSYM (Crittografia simmetrica)	√		
ASN1 (Analizzatore asn.1)	√		
X509RSA (Gestione chiave rsa - pkcs #1)	√		√
X509REQ (Gestione richiesta di certificato - pkcs #10)	√		√
X509CRT (Gestione certificato - itu x509 v3)	√	√	√
X509CRL (Gestione lista certificati revocati - itu x509 v2)	√	√	√
P7DATA (Imbustamento flusso dati in formato pkcs #7 - data)	√		√
P7SIGND (Imbustamento flusso dati in formato pkcs #7 - signed data)	√	√	√
P7SIENV (Imbustamento flusso dati in formato pkcs #7 - signed and enveloped data)	√		√

(*) Hp 9000 Server di Front-end con Banca d'Italia

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

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 cinque macrofunzioni cardine per il processo di verifica delle firme.

Inizializzazione (INIZIA)

Questo servizio, che deve essere richiamato prima di qualsiasi altro, effettua una serie di operazioni propedeutiche all'esecuzione dei servizi VERIRID e VERIEST.

Innanzitutto, permette l'acquisizione ed il caricamento in memoria (in un'area comune con il programma chiamante) delle chiavi pubbliche delle CA e dei valori dei campi 'subjectKeyIdentifier' (SKI) relativi, estraendoli dai certificati stessi delle CA dopo averne verificato la consistenza

Controlli aggiuntivi sui certificati di CA (ad esempio, il controllo che non esista duplicazione sugli SKI dei certificati di CA gestite) sono considerati propedeutici a questo servizio: s'intende, cioè, che siano stati svolti all'atto del caricamento del data set contenente tali certificati.

Il numero massimo di certificati di CA gestiti dalla routine è 30. Tale valore può essere modificato effettuando un intervento di manutenzione di lieve entità sulla routine.

Il servizio, inoltre, acquisisce e rende disponibili all'ambiente di lavoro MBM le CRL, se presenti, da utilizzare per la verifica della non-revoca dei certificati e carica in memoria (in un'area comune con il programma chiamante) il puntamento (handle) restituito dall'ambiente MBM relativo ad una singola CRL insieme all'identificativo della chiave di firma della CRL stessa (AuthorityKeyIdentifier).

Il servizio gestisce fino ad un massimo di 10 CRL. Tale valore può essere modificato effettuando un intervento di manutenzione sulla routine.

Oltre a ciò, viene caricata in memoria una tabella, a partire da un file (eventualmente fornito in input), contenente la lista degli URL da cui viene effettuato lo scarico periodico delle CRL.

Verifica ridotta (VERIRID)

Questo servizio (da richiamare dopo il servizio INIZIA) 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, da richiamare dopo il servizio INIZIA in alternativa la servizio VERIRID, esegue le stesse operazioni del servizio VERIRID ed, in aggiunta, verifica la non-revoca del certificato rispetto alle CRL reperite nel servizio INIZIA. 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.

Terminazione (TERMINA)

Tale servizio provvede a liberare dall'ambiente MBM le aree dati relative alle CRL caricate nel servizio INIZIA

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).

Questo servizio è (l'unico) richiamabile dal chiamante senza che questi abbia preventivamente invocato il servizio INIZIA.

In allegato si riporta il documento *"Disegno e Modalità d'uso routine verifica firma ambiente host" sviluppato nell'ambito delle attività svolte per il MEF nell'area applicativa Spese (Agosto 2001)* che analizza il dettaglio della routine.

3.2.2 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.

Il processo di aggiornamento della Copia della CRL presso il SIRGS è composto da due fasi:

- operazione di HTTP GET della CRL dal sito http://LDAPCA.RUPA.IT Attualmente le CRL di esercizio sono su http://ca.rupa.it/crl3
- copia del file scaricato in //Server/directory/nome fisso dove il server è un FTP server visibile sulla rete interna

Il processo può gestire CRL provenienti da certificatori diversi fino ad un massimo di 10 CRL, ognuna identificata da una URL diversa, indipendentemente dal numero di CA di appartenenza. Al disopra di questi valori sarà necessario eseguire un adeguamento dei programmi che effettuano il processo di alimentazione delle CRL.

Il processo è attivato in maniera automatica dallo schedulatore del sistema operativo che attualmente ospita il programma. In particolare, essendo obbligo del certificatore (CTRupa) aggiornare la CRL almeno ogni 4 ore, il processo è attualmente schedulato con frequenza oraria, in modo tale da avere una CRL sufficientemente aggiornata e da sopperire ad eventuali momentanee problematiche di download dai siti certificatori. La frequenza di aggiornamento può essere modificata senza interventi sulle procedure.

In questa maniera si rende disponibili, a tutte le applicazioni di verifica della firma digitale, una versione adeguatamente aggiornata delle CRL sul sito FTP interno del SIRGS. Le applicazioni suddette (Spese, SICOGE, etc...) dovranno, come primo passo delle operazioni di verifica, prelevare una copia delle ultime CRL disponibili dal sito FTP interno.

Il processo è articolato nelle seguenti fasi:
- la procedura presente sulla macchina ftp.tesoro.it viene attivata dallo schedulatore di sistema ogni ora;
- la procedura legge un file presente sulla macchina dove vengono riportate sino a 10 URL corrispondenti ad altrettante CRL da scaricare;
- le CRL disponibili vengono scaricate tramite ftp binario sul server con il nome 1.txt --> 10.txt;
- ogni ora le CRL vengono così ricoperte con l'ultima versione presente sui siti dei certificatori.

Le procedure applicative su OS390 che devono effettuare la verifica della validità dei documenti firmati come prima cosa si collegano alla macchina 213.175.11.180 via FTP binario e scaricano le CRL presenti sui dataset applicativi di propria competenza. A questo punto, effettuano la prima fase delle verifiche ovvero controllare se per tutte le CA da elaborare esiste la corrispondente CRL, se le CRL sono integre (si tratta di un documento firmato...) e se la CRL è ancora valida.

3.2.3 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

Nei due processi che saranno descritti è stata implementata una forma di "autenticazione forte" basata sulla realizzazione di un meccanismo di "one-time password".
Nell'area privata del filesystem della smart card è stato inizializzato ed inserito un campo di 32 byte che contiene:

<utenza mainframe><password><password –1><password di reset>

Le procedure custom leggono questo campo e realizzano, con variazioni legate alla diversa realtà tecnologica, i processi qui descritti

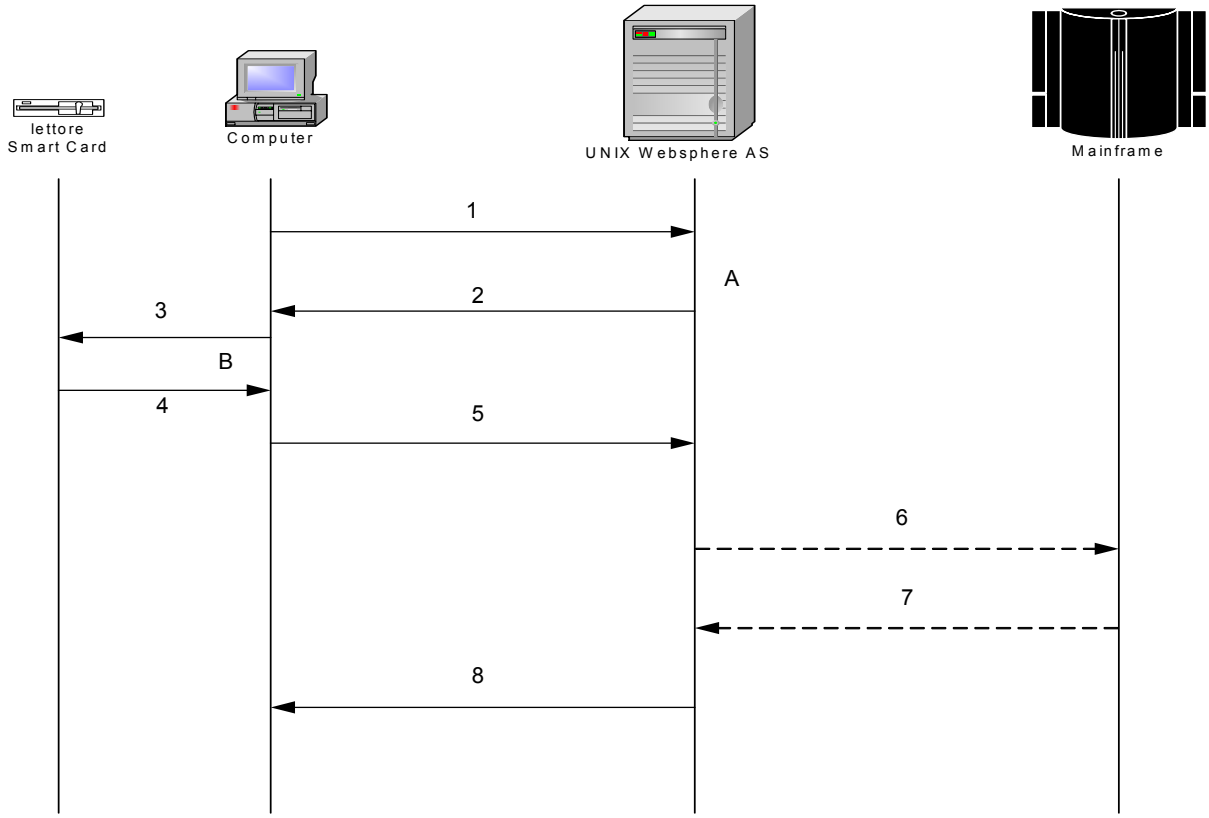
3.3.1.1 Processo di autenticazione per applicazioni client/server (Mandato Informatico)

La sequenza di operazioni per l'identificazione dell'utente per le applicazioni Mandato Informatico e Perenti è la seguente:

- l'utente richiede l'applicazione Mandato Informatico, Perenti con 'doppio click' sull'icona corrispondente sul desktop della PDL
- l'utente inserisce la Smart Card nel lettore e digita il PIN relativo. Nel caso venga immesso per tre volte un PIN errato, la Smart Card, che effettua la verifica, rifiuta ulteriori tentativi diventando inutilizzabile;
- superati i controlli locali (Smart Card + PIN), l'applicazione apre la comunicazione con il mainframe inviando User Id, PW corrente e PW nuova (per la futura sessione). La prima è prelevata dal filesystem della smart card la seconda viene generata nella smart card;
- PW corrente e PW nuova vengono ricevute da RACF che verifica la correttezza della PW corrente, la aggiorna sostituendola con la nuova ed invia un codice di ritorno che permette di stabilire se l'aggiornamento della PW è avvenuto o meno con successo. Nel caso di conferma dell'avvenuto aggiornamento, la nuova PW viene memorizzata sulla Smart Card come PW corrente per la successiva sessione e la precedente password viene memorizzata sulla Smart Card come <password –1>.

3.3.1.2 Processo di autenticazione applicazioni web based (OPF Tesoreria)

La sequenza di operazioni per l'identificazione dell'utente per le applicazioni "web based" ma che operano su mainframe è realizzata tramite una servlet ed un'applet, quest'ultima firmata per autorizzarne l'esecuzione, scaricata nel browser utente .



1 - il browser richiede un collegamento ad un URL via HTTP al server WEB
A- l'URL corrisponde all'attivazione di un Servlet (A) di LOGIN che governa in modo programmatico l'identificazione e l'autorizzazione accesso
2- viene scaricato l'applet (B) di LOGIN che ha il compito di accedere alla Smart Card
3- l'applet accede alla Smart Card, decritta i campi userid e la password dall'area privata
4-5 La userid e la password sono passati al servlet (sul canale crittato)
6-7 Il servlet attiva il metodo ESI verso il CICS/RACF per l'identificazione dell'utente
8 Il servlet gestisce l'esito dell'operazione di ESI:
esito positivo (utente identificato) - richiede al RACF l'ufficio/i corrispondente all'utente e memorizza userid, la password e ufficio come attributi di HttpSession, abbandona la sessione HTTP e invia all'utente il menù principale dell'applicazione
esito negativo (utente non identificato) - segnala la violazione di accesso e chiude la connessione

E' supportata la funzionalità di "Change password".

3.3.2 Single Sign-On Server

Nella versione dell'access manager, attiva da fine novembre 2004, per le applicazioni "web based" è stato introdotto un meccanismo di identificazione 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.

[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.

4 Scenario di evoluzione

Lo scenario di evoluzione più significativo riguarda la componente client. Il ***"Thin Client"*** ha funzionalità limitate non comprendendo funzionalità di cifratura ed è sempre più necessario poter integrare le funzionalità crittografiche native della piattaforma Windows con la smart card in dotazione al personale MEF ed in generale affrancarsi dalla necessità di utilizzare un unico dispositivo di firma, anche in previsione della Carta di Identità Elettronica.

Il CT-RUPA ha quindi avviato una revisione del cosiddetto "***Layer Unico"*** che è un software che permette di avere dei servizi di firma digitale e cifratura elettronica da effettuare tramite smart card senza che tali servizi siano dipendenti dal tipo di smart card utilizzato, ossia un layer unico per il PKCS#11 che superi le limitazioni legate alla scarsa interoperabilità tra smart card di diversi fornitori. Il "***Layer Unico"*** implementa, inoltre, uno strato SW che permette la firma e cifra secondo lo standard PKCS#7 in ambiente Microsoft tramite l'utilizzo di un CSP (Crypto Service Provider) che si appoggia sulle Crypto API fornite da Microsoft.

Le applicazioni potranno utilizzare i servizi offerti dalle smart card ~~in~~ attraverso **tre** modalità distinte di accesso:

- Tramite chiamate ad API standard PKCS # 11
- Tramite chiamate al CSP
- Tramite chiamate alle API per la crittografia, disponibili nei sistemi Microsoft, e tramite i Macrocomandi

L'altro scenario, meramente tecnologico, è legato alla presenza sul mercato di lettori di tipo USB che rendono più agevole la connessione del lettore alle postazioni di lavoro. Per il II Dipartimento è attualmente in valutazione il dispositivo USB SIMPOCKET COMBO della Eutron. Si tratta di un token USB, avente sia la funzionalità di lettore di S/C che quella di memoria Flash (con capacità da 16MB a 512MB). Le caratteristiche costruttive del dispositivo consentono di inserire la S/C all'interno di una apposita fessura, oppure, in alternativa, estrarre il chip da una smart-card fustellata e posizionarlo in un apposito alloggio.