CAPITOLATO TECNICO

PER LA FORNITURA DELLE SMART CARD NECESSARIE PER L'ATTIVAZIONE DEI SISTEMI DI EMISSIONE DEI TITOLI DI ACCESSO AGLI SPETTACOLI PUBBLICI

§§§§§§

1. Premesse

Conformemente a quanto indicato nel provvedimento del 23 luglio 2001, "*Attuazione delle disposizioni recate dagli articoli 6 e 18 del decreto legislativo 26 febbraio 1999, n. 60, e del decreto ministeriale 13 luglio 2000, concernente le caratteristiche degli apparecchi misuratori fiscali, il contenuto e le modalità di emissione dei titoli di accesso per gli intrattenimenti e le attività spettacolistiche e le modalità di trasferimento dei dati alla SIAE*", le carte di attivazione dovranno consentire:

- la generazione di un sigillo fiscale relativo ad ogni biglietto emesso mediante tecniche crittografiche a chiave simmetrica;
- l'implementazione di due contatori: uno indicante la sommatoria totale dei titoli emessi l'altro il numero progressivo da stampare su tali titoli;
- la firma digitale del giornale di fondo del sistema di emissione e la firma digitale dei messaggi di posta elettronica inviati al sistema centralizzato di raccolta dati, mediante tecniche crittografiche a chiave asimmetrica.

2. Oggetto della fornitura:

La presente fornitura ha ad oggetto l'acquisizione:

- di un massimo di n. 24.000 SMART CARD comprensiva della relativa attività di personalizzazione elettrica (firmware) e grafica (offset a colori solo fronte) dei supporti;
- di software a corredo per lo sviluppo di applicazioni correlate all'utilizzo delle carte e per le operazioni di collaudo della fornitura;
- delle attività di supporto ed aggiornamento del software di cui al punto precedente.

3. Descrizione sintetica del ciclo di vita della carta a microcircuito

Le carte a microcircuito richieste saranno utilizzate per l'attivazione dei sistemi di biglietteria automatizzata conformi alle disposizioni normative citate in premessa.

I sistemi sopra citati che fanno uso delle carte, attivi alla data, sono circa 6.000; sono prodotti da diverse società e classificabili in circa 127 distinti modelli.

La carta, consentirà al titolare, a seguito della digitazione del relativo PIN fornito a parte, di attivare il sistema di biglietteria automatizzata, consentendo in particolare:

a) la lettura del contenuto del file di configurazione a bordo della carta;

b) l'attivazione del sistema mediante:

b.1) in caso di nuova attivazione, l'assegnazione alla macchina del

titolare del *Numero Sistema* presente sulla smart card nel file di configurazione di cui al punto precedente;

b.2) in caso di sistema già attivo, la verifica del *Numero Sistema* presente sulla carta con il *Numero Sistema* già attribuito alla macchina del titolare per la quale questa è unicamente abilitata a funzionare;

c) l'emissione dei titoli di accesso per gli intrattenimenti e le attività spettacolistiche.

Per ciascuno dei titoli emessi il sistema dovrà rilasciare, utilizzando le funzioni della Smart Card, un apposito Sigillo Fiscale, da stampare insieme ai dati noti (data, ora, importo, progressivo titolo) al fine di consentire le successive operazioni di verifica sulla correttezza dell'emissione.

La carta sarà necessaria per "firmare" quotidianamente i file di LOG delle transazioni e la Lista unica dei Titoli di Accesso, che dovranno essere registrati su supporto non modificabile (CD-R/DVD+/-R ecc.) ai fini della conservazione.

Inoltre sarà necessaria anche per firmare periodicamente i file che il titolare dovrà inviare ai server SIAE (Riepiloghi Giornalieri, Riepiloghi Mensili, e Riepilogo Controllo Accessi).

Allo scadere del certificato a bordo della carta ovvero alla comparsa di problemi funzionali (es: uno dei due contatori non più in grado di auto-

incrementarsi a seguito di emissione titoli) la carta viene restituita al CMS della SIAE che la conserverà per il tempo necessario per le eventuali verifiche o controlli ad opera del personale preposto.

4. Specifiche tecniche

Al fine di consentire le operazioni indicate in premessa, le carte devono rispondere alle specifiche tecniche di seguito riportate:

1) essere conformi allo standard ISO 7816-1, -2, -3, -4,-8;
2) avere una capacità di memoria EEPROM non inferiore a 64KBytes;
3) essere conformi ai Common Criteria EAL4+ o equivalente, secondo il protection profile CWA14169;
4) implementare gli algoritmi di crittografia a chiave simmetrica DES e 3DES: tali algoritmi simmetrici sono essenziali per l'emissione del "sigillo fiscale" di seguito descritto;
5) implementare le funzionalità di firma secondo l'algoritmo RSA con chiavi a 1024bit, 2048bit o superiore esclusivamente a fronte della digitazione dell'apposito codice di identificazione personale (PIN);
6) effettuare la generazione a bordo della coppia di chiavi pubblica/privata per la firma;
7) poter ospitare almeno tre certificati conformi allo standard X.509v3 (uno relativo al titolare del sistema di vendita, uno relativo alla CA emittente ed uno relativo alla SIAE);
8) in considerazione del fatto che la firma dovrà poter far parte di un messaggio S/MIME il meccanismo di *padding* per le operazioni RSA

dovrà essere conforme allo standard PKCS #1;

9) implementare gli algoritmi di *hash* Sha128 e Sha256. L'integrazione dell'algoritmo di *hash* all'interno della carta implica che quest'ultima possa operare in maniera sostanzialmente autonoma per la produzione della firma con tecnologia a chiavi asimmetriche a partire dal solo input costituito dal documento da firmare;

10) implementare il meccanismo per la generazione del sigillo fiscale e dell'incremento dei contatori (vedi punto successivo) mediante un'operazione singola da richiamare mediante apposita APDU; tale operazione non dovrà richiedere un tempo superiore a 150 millisecondi misurati includendo i tempi di Input/Output.

11) implementare un meccanismo di contatore progressivo positivo in nessun caso decrementabile: tale meccanismo dovrà garantire che la sequenza di generazione dei numeri non possa venire alterata dopo che la carta sia stata inizializzata correttamente e quindi ogni biglietto emesso porti con sé un numero progressivo e consecutivo diverso. Nell'area specifica del contatore la EEPROM dovrà essere garantito un numero di cicli di scrittura/cancellazione non inferiore ai 4.000.000 (quattro milioni);

12) implementare il calcolo del codice di sicurezza del titolo d'accesso secondo le specifiche indicate al paragrafo 8 denominato: "APDU calcolo Sigillo Fiscale ed incremento contatori".

L'aggiudicatario apporterà le necessarie modifiche al software ed al firmware per garantire la compatibilità delle carte con gli apparati già installati. Non saranno richieste modifiche tali da pregiudicare la

rispondenza delle carte ai requisiti elencati nel presente capitolato.

5. Modalità di fornitura delle carte a microcircuito

Nell'ambito del quantitativo complessivo oggetto dell'affidamento, le carte dovranno essere fornite, a seguito di appositi ordini dell'amministrazione e nei quantitativi ivi richiesti, entro 20 giorni lavorativi dalla ricezione della richiesta da parte dell'Agenzia delle Entrate.

I supporti saranno oggetto di un doppio "step" di personalizzazione a cura rispettivamente del Fornitore e di SIAE.

Il Fornitore dovrà effettuare:

- la configurazione in fabbrica delle Smart Card con il File System che sarà fornito dalla SIAE;
- la serigrafia dei supporti secondo il logo fornito tra gli allegati tecnici; le carte dovranno inoltre recare un seriale alfanumerico composto di un carattere alfabetico (al momento è una "A") seguito da numero progressivo composto da sette cifre decimali il cui valore iniziale verrà indicato in fase di richiesta di prima fornitura. Tutte le forniture successive dovranno seguire la numerazione senza salti;
- la pre-impostazione di PIN e PUK uguali per tutte le carte secondo modalità fornite all'atto della richiesta.

Le carte di attivazione (Smart Card) dovranno essere inviate direttamente al CMS (Card Management System) della SIAE mediante corriere in contenitori da 100 pezzi chiusi con sigilli di sicurezza e con evidenziati i

numeri seriali iniziale e finale contenuti all'interno.

Presso la SIAE avverrà la successiva fase di personalizzazione elettrica e grafica (mediante tecnologia termica o laser) a carico dell'Amministrazione.

In particolare saranno effettuate le seguenti operazioni:

a) Attribuzione (modifica) di un numero pseudocasuale al PIN ed al PUK;

b) Inserimento della chiave segreta per il calcolo del sigillo in zona di memoria protetta;

c) Creazione del file di "configurazione" a bordo della carta riepilogativo dei dati del titolare, del *Numero Sistema* abilitato e degli estremi della richiesta di attivazione;

d) Generazione a bordo della carta della coppia di chiavi, pubblica e privata;

e) Attribuzione del certificato X509v3 da parte dell'ente certificatore incaricato;

f) Valorizzazione finale delle condizioni di accesso del file-system e degli oggetti di sicurezza (chiave sigillo fiscale, PIN, PUK e chiave privata di firma);

g) Stampa sul supporto plastico dei dati del titolare con inchiostro nero in termografia o mediante tecnologia laser;

h) Verifica leggibilità elettrica della zona pubblica della carta;

i) Spedizione della carta al titolare richiedente mediante corriere espresso.

6. Software a corredo

Per lo sviluppo delle applicazioni correlate all'utilizzo delle carte di attivazione dovranno essere forniti i seguenti software completi di documentazione, esempi pratici d'uso, di licenza d'uso illimitata e trasferibile a terzi ed, unicamente per i seguenti punti: c) e d), anche dei codici sorgenti, al fine di garantire la verificabilità e la correttezza del codice stesso:

a) una libreria compatibile con l'interfaccia Cryptoki (definita dallo standard PKCS#11);

b) un modulo CSP (Cryptographic Service Provider) in grado di rendere utilizzabili le CryptoAPI Microsoft agli applicativi presenti sul sistema operativo Microsoft Windows XP / 7 / 8 / 10;

c) una libreria ANSI C (o C++) denominata LibSIAE.dll, disponibile in formato sia sorgente che binario per gli ambienti Microsoft Windows, GNU-Linux ed Apple Mac OS X e che sia in grado di operare nell'area del sigillo. Tale libreria dovrà rispettare la documentazione prevista in allegato per la LibSIAE.dll al fine di garantire la continuità con gli applicativi già sviluppati;

d) una libreria in ambiente Microsoft Windows ed una per l'ambiente GNU-Linux (in particolare per le distribuzioni Ubuntu 16. 4 / Fedora 24 / openSUSE 42.1) in grado di consentire la creazione di documenti firmati in formato PKCS#7 (per la creazione e conservazione dei "log" firmati) ed in grado di consentire la creazione di messaggi email in formato S/MIME firmati mediante l'utilizzo di crittografia RSA a chiavi

asimmetriche. Tale libreria dovrà essere fornita in codice sia sorgente che binario per tutti gli ambienti descritti con licenza d'uso liberamente trasferibile a terzi. Tale libreria dovrà supportare le operazioni di creazione di file firmato nel formato PKCS#7, richiesta dei certificati a bordo della carta, richiesta di lettura file di configurazione della carta, generazione di messaggi di posta elettronica firmati e connessioni SSL/TLS utilizzando le chiavi presenti a bordo della carta;

7. Manutenzione e supporto tecnico

Dovrà essere fornita la manutenzione del software con i seguenti livelli di servizio:

- Per i malfunzionamenti segnalati :
  - presa in carico del problema entro la giornata lavorativa di comunicazione delle anomalie;
  - risoluzione entro tre giorni lavorativi successivi.
- Per l'assistenza relativa ad adeguamenti tecnologici :
  - presa in carico del problema entro la giornata lavorativa di comunicazione;
  - risoluzione entro trenta giorni lavorativi successivi; eventuali motivazioni per tempistiche diverse devono essere documentate per iscritto al fine di concordare le nuove tempistiche con l'Agenzia delle Entrate.

Il mancato rispetto dei Service Level Agreement (SLA) indicati comporterà l'applicazione di una penale, in misura giornaliera, corrispondente all'1 per

mille dell'ammontare netto contrattuale.

Sarà inoltre necessario fornire documentazione e supporto tecnico per l'utilizzo del software fornito per un periodo pari a quello di validità del contratto.

8. APDU calcolo Sigillo Fiscale ed incremento contatori

E' necessario implementare una apposita APDU (APDU_CMP_SIGILLO) in grado di eseguire le seguenti operazioni:

a) Calcolo del sigillo fiscale;

b) Incremento contatore Balance (cumulo somme titoli emessi);

c) Incremento contatore Titoli emessi (numero progressivo).

Tali operazioni, dettagliate successivamente, dovranno essere trasparenti all'utente e essere effettuate in seguito ad un unico singolo comando, comunque non frazionabile.

a) Calcolo del sigillo fiscale

Dal punto di vista crittografico il sigillo fiscale è un MAC (Message Authentication Code). Ciò implica che la carta dovrà essere in grado di memorizzare in maniera non esportabile né direttamente accessibile dall'esterno la chiave simmetrica per l'emissione del sigillo. La generazione di un sigillo fiscale sotto forma di MAC implica inoltre che l'operazione di verifica del sigillo potrà essere effettuata solo ed esclusivamente da chi conosce anche la chiave simmetrica con cui è stato calcolato il sigillo stesso.

Il Sigillo Fiscale sarà calcolato con un meccanismo challenge-response mediante un algoritmo simmetrico 3DES CBC nella maniera seguente:

$SF = F (DatiINPUT, K^i)$

dove:

SF = Sigillo Fiscale (response della funzione ovvero MAC)

DatiINPUT = numero seriale smart card, numero progressivo titolo, data, ora, importo del titolo

F = algoritmo simmetrico 3DES CBC

K^i = chiave 3Des della carta “i-esima” differenziato con algoritmo segreto. La chiave é disponibile in apposita zona protetta sul file-system accessibile in lettura unicamente a questa funzione interna.

La sfida (challenge) è quindi costituita dall’insieme dei dati specificati nel provvedimento in premessa e qui sopra evidenziati (DatiINPUT) insieme alla chiave i-esima (K^i) presente a bordo della smart card, mentre la risposta (response) è costituita dal risultato del calcolo del MAC.

b) **Incremento contatore Balance (numerico di 4Byte):**

Al valore espresso in centesimi di euro vengono aggiunti mediante somma algebrica i centesimi della corrente transazione.

Non è possibile in alcun modo decrementare il contatore (gli storni vengono gestiti contabilmente con apposita funzione esterna alla Smart Card) Il

campo è un numerico senza segno e l'importo della transazione di emissione può essere unicamente maggiore od uguale a 0 (zero).

c) **Incremento contatore Titoli (numerico di 4Byte):**

Il contatore del numero di titoli emessi viene incrementato di una unità ad ogni richiesta di sigillo fiscale.

Non è possibile in alcun modo decrementare il contatore. Il campo è un numerico senza segno.

9. Difettosità

Si intende per difettosità:

- l'impossibilità di inizializzare la carta all'inizio del ciclo di vita;
- l'impossibilità di eseguire correttamente una firma digitale;
- il mancato raggiungimento del numero minimo di cicli di aggiornamento dei contatori a bordo della carta, stabilito in 4.000.000 (quattro milioni) per ciascuno.

Per entrambi i casi la percentuale massima di difettosità non deve essere superiore a 0.1% (1 per mille) sul totale della fornitura.

10. Collaudo della fornitura

Il collaudo avverrà da parte della SIAE estraendo un numero non inferiore a 5 campioni prelevati casualmente dalla fornitura e facendo seguire l'iter completo di personalizzazione ed utilizzo degli stessi.

Dovrà essere fornito un software, in ambiente Microsoft Windows, in grado di eseguire tale collaudo. Tale software sarà comprensivo del codice sorgente e di una documentazione che ne descriva le funzioni con riferimenti alle fasi dello stesso ad eccezione del solo punto a).

Fasi di collaudo:

a) personalizzazione sia elettrica che grafica presso i locali CMS della SIAE.

b) verifica di lettura del contenuto pubblico

c) verifica funzionalità di PIN LOCK ed UNLOCK mediante PUK

d) verifica delle capacità di firma digitale

e) verifica di emissione sigilli fiscali con rispetto del limite di numero minimo di iterazioni dei contatori previsto alla lettera precedente;

f) verifica della velocità di emissione dei sigilli fiscali con rispetto dei tempi di emissione indicati al precedente punto 10) par. 4;

g) verifica di funzionalità di invio di email firmate digitalmente. Verifica di compatibilità della carta con i sistemi esistenti.

Le operazioni di collaudo sopra descritte saranno effettuate in ambiente Windows mediante Personal Computer che utilizzeranno un lettore Smart Card ISO7816 con interfaccia USB ed apposito software.

Durante le attività di collaudo, potranno essere interessati anche alcuni utilizzatori degli attuali sistemi di biglietteria, al fine di verificare sul campo il corretto funzionamento dei supporti forniti.

In caso di esito negativo delle attività di verifica, l'aggiudicatario dovrà provvedere a rimuovere le anomalie e ad effettuare una nuova consegna entro un massimo di 20 giorni dalla data di ricezione della comunicazione dell'esito negativo della verifica stessa.

11. Allegati tecnici

Tutti gli allegati tecnici, al fine di garantire un congruo livello di riservatezza, saranno forniti unicamente alla firma del contratto di appalto con "Non Disclosure Agreement".

Tali allegati saranno:

- File System SIAE (File System per l'applicazione SIAE);
- File di personalizzazione grafica che dovrà essere applicato in serigrafia su supporti plastici in grado di essere successivamente personalizzati con tecnologia "laser" ovvero "termografica".
- File libSIAECard contenente le specifiche per le librerie e l'ambiente di collaudo.

-- o --