Ministero dell'Interno

Dipartimento per gli Affari Interni e Territoriali
Direzione Centrale per i Servizi Demografici

VERBALE

COMITATO TECNICO SCIENTIFICO PERMANENTE

DEL 11 FEBBRAIO 2008

In data 11 febbraio alle ore 10.00, presso la Direzione Centrale per i Servizi Demografici si è tenuta una riunione del Comitato Tecnico Scientifico Permanente avente all'ordine del giorno l'esame dei seguenti punti:

- Approvazione dei verbali delle sedute del 1e gennaio 2008 e del 4 febbraio 2008;
- Stato avanzamento lavori del file system;
- Valutazione e approvazione del modello di domanda per omologazione del chip;
- Programmazione modalità di omologazione del chip;

Alla riunione presieduta dalla D.ssa Franca Fico, Vice Prefetto Aggiunto della Direzione Centrale per i Servizi Demografici, hanno partecipato:

- L'ing. Giovanni Manca del CNIPA;
- L'Ing. Leopoldo Consiglio dell'Istituto Poligrafico e Zecca dello Stato per delega dell'Ing. Andrea De Maria
- L'Ing. Valentino Ditoma dell'Ancitel per delega dell'Ing. Turano;
- Il Prof. Guido Marinelli dell'Università degli studi di Roma "Tor Vergata";

La seduta si apre con la lettura del verbale della seduta del 14 gennaio 2008 modificato con le integrazioni apportate dal Comitato, lo stesso viene approvato e sottoscritto unitamente al verbale della seduta del 4 febbraio 2008.

Il Comitato conviene per la pubblicazione degli stessi sul sito della Direzione Centrale per i Servizi Demografici.

La D.ssa Fico rappresenta al Comitato le note pervenute dalle società concernenti le apparecchiature per l'emissione della CIE a seguito delle determinazioni assunte dal Comitato nella seduta del 25 gennaio 2008 e rese note con i documenti tecnici pubblicati sul sito.

Nello specifico le note attengono alle autodichiarazioni dei parametri aggiuntivi delle apparecchiature stampanti termografiche Digital XID 580i, 590i, DataCard SP75 e dell'apparato Biometrico CKB 10000.

Si sottopone inoltre all'attenzione del Comitato la nota di chiarimento relativa alla "lista dei requisiti minimi" per le postazioni di emissione fatta pervenire dalla società Colla&Partners.

In particolare l'Ing. Consiglio precisa che il parametro della velocità di laminazione 200mm/sec deve attribuirsi ad un refuso nel documento "Lista requisiti minimi" e "Modello di domanda di omologazione dispositivi CIE". La correzione 20mm/sec di sarà prontamente apportata dal Comitato Tecnico Scientifico Permanente.

Per quanto attiene il *"film termografico KT-YMCK (stampa diretta) e KT-YMCKT (stampa indiretta)"* l'Ing. Consiglio precisa che il punto 11 dei requisiti minimi delle stampanti termografiche riporta: "film termografico KT - YMCK (stampa diretta) e KT - YMCKT (stampa indiretta): consigliato: auto-dichiarata" e, pertanto, al fine dell'omologazione sono accettate tutte le altre tecnologie equivalenti.

Il Comitato conviene per la trasmissione della risposta formale alla Società richiedente.

La D.ssa Fico puntualizza l'approccio di massima collaborazione che il Comitato deve adottare nei confronti delle esigenze rappresentate dalle Società.

La D.ssa Fico passa all'esame del punto all'ordine del giorno relativo allo stato di avanzamento dei lavori sul File System.

Il Comitato ribadisce che pur essendo rimasti in sospeso gli aspetti concernenti la modalità di protezione e di memorizzazione dei dati biometrici, foto e impronta digitale del titolare, tale aspetto non costituisce un vincolo per l'IPZS ai fini dell'omologazione del chip.

La D.ssa Fico sottopone a valutazione del Comitato, coerentemente a quanto concordato nella seduta del 4 febbraio 2008, la nota illustrativa relativa alla protezione delle informazioni dei dati personali foto e impronta biometrica. La nota evidenzia oltre agli aspetti insoluti anche gli obblighi imposti dalla normativa, le possibilità di gestione del dato e gli eventuali costi nonché una serie di opzioni decisionali.

Il Comitato analizza il documento e dopo ampia discussione reputa necessari alcuni approfondimenti.

L'Ing. Ditoma prende in carico la revisione del documento che sarà integrato eventualmente dal resto dei presenti.

Il Comitato concorda.

La D.ssa Fico passa alla rassegna del punto all'ordine del giorno concernente la domanda di omologazione dl chip.

Il Prof. Marinelli ha rappresentato l'opportunità di acquisire con la domanda di omologazione del chip l'impegno dei produttori di fornire al Ministero dell'Interno tutte le specifiche del chip, i software e gli script che consentono di inizializzare il file system della CIE nonché il CSP in ambiente Windows il PKCS#11 in ambiente Windows, Linux e MacOSX al fine di non gravare in alcun modo per oneri sull'Amministrazione dell'Interno.

L'Ing. Consiglio evidenzia che la disponibilità delle librerie non è necessaria all'omologazione. Le librerie suddette sono un argomento da affrontare in chiave diversa stabilendo in prima battuta di chi sia la responsabilità trattandosi di componenti software necessarie al funzionamento delle CIE per l'accesso ai servizi. E'necessaria, piuttosto che una libreria per ciascun fornitore, un'unica libreria che supporti tutte le carte sia per le funzionalità di

autenticazione sia per quelle di firma. Per lo sviluppo di una libreria con tali caratteristiche è sufficiente la conoscenza delle specifiche APDU, del file system e del manuale dell'Amministratore della carta che deve essere fornito dal produttore e già richiesto nella versione attuale della domanda di omologazione. Ciò che potrebbe essere utile richiedere ai produttori di microchip nella domanda di omologazione è la disponibilità ad implementare o, in qualsiasi forma, rendere disponibili gratuitamente strumenti software che permettano l'installazione del file system di firma sulle CIE.

L'Ing. Ditoma suggerisce che il produttore dichiari che non esistono vincoli per la costruzione di librerie.

Il prof. Marinelli ritiene che in aggiunta il produttore debba anche dichiarare, in sede di domanda di omologazione, se esistono software proprietari che in qualche modo siano necessari alla creazione delle librerie per l'inizializzazione del microchip e per l'suo della CIE. Nel caso il produttore deve dichiarare la politica commerciale relativa all'uso di tali software. Ciò per evitare che in qualsiasi momento del ciclo di vita della CIE possa verificarsi la necessità di acquisire licenze d'uso non preventivate.

Il Comitato concorda.

Prende la parola l'Ing. Manca che riassume gli aspetti relativi al chip e alla sua omologazione.

Il microchip è caratterizzato da una parte hardware e da un sistema operativo. Il sistema operativo è stato standardizzato con il documento delle APDU quindi tutte le smart card funzionano, per gli obiettivi necessari alla CIE allo stesso modo. Le funzioni della carta sono assicurate dal file system che, essendo standardizzato consente accessi esterni alla CIE da un'unica libreria software sia di tipo PKCS#11 (criptoki) che di tipo CSP (per ambienti windows). In molti progetti europei questa libreria è disponibile secondo la filosofia dell'open source come sostenuto dal Progetto Porvoo. Più complesso è il meccanismo della firma digitale.

Infatti ogni smart card implementa un proprio file system per la firma digitale. Ne consegue che per non perdere la certificazione di sicurezza della smart card sulla specifica piattaforma chi scriverà sulla CIE uno specifico file system per la firma digitale dovrà riconoscere il modello e il produttore della stessa. In conseguenza di ciò anche la libreria software per interfacciare la carta è specifica per il singolo modello e produttore della carta stessa. In ambiente CNS sono state realizzate delle librerie (distribuite su licenza software a codice chiuso) che tengono conto di queste specificità e sono in grado di funzionare con tutte le smart card facenti parte di un insieme noto a priori delle stesse.

Infine L'Ing. Manca ricorda che sia la libreria "di autenticazione" che quella di "firma" devono essere considerate nello scenario degli sviluppi a supporto della distribuzione delle CIE.

In particolare rappresenta l'opportunità di definire chi fa il primo sviluppo e poi la successiva manutenzione sia correttiva che evolutiva.

Il Prof. Marinelli ricorda che i problemi di interoperabilità nell'uso della firma digitale, come noto, sono stati affrontati con l'introduzione di software gratuiti in grado di verificare firme rilasciate da diversi certificatori. Viceversa ritiene assolutamente fondamentale approfondire quanto evidenziato dall'ing. Manca relativamente ai diversi file system per la firma digitale secondo cui, per scrivere il file system della firma digitale è necessario riconoscere il modello e il produttore della smart card che ospita il file system stesso. Tali aspetti vanno assolutamente approfonditi tenendo anche conto che per la CIE devono iniziare a breve le procedure di omologazione dei nuovi microchip propedeutiche alla gara di acquisizione degli stessi.

Il Prof. Marinelli prospetta l'opportunità che il Ministero dell'Interno potrebbe farsi carico delle librerie CIE per le funzioni di autenticazione (PKCS#11 e CSP) a condizione che in primis i produttori forniscano tutte le specifiche.

All'unanimità si delibera che per le decisioni concernenti gli aspetti sopra trattati per la firma digitale, la qualificazione del chip nonché gli eventuali impatti che le modifiche del file system possano avere sul processo di certificazione Common Criteria dello stesso, il Comitato attende l'audizione con i rappresentanti di Assocertificatori prevista per la sessione del Comitato del 25 febbraio 2008, al fine di acquisire in detta sede informazioni tecniche utili.

Infine il Comitato passa alla considerazione della parte della domanda di omologazione del chip che riguarda il "materiale di test" da fornire da parte del produttore.

Si conviene, sulla base delle smart card che occorrono per il test bed dell'IPZS e per le prove sul circuito centrale di emissione, di richiedere ai produttori n. 600 supporti dei quali 400 destinati a verifiche fatte sul circuito centrale di emissione e 200 destinate alle verifiche fatte da IPZS.

Alla luce dell'analisi della bozza di domanda e delle determinazioni assunte l'IPZS prende in carico la revisione del modello di domanda di omologazione del chip da trasmettere al resto del Comitato per l'approvazione prossima.

La seduta termina alle ore 14.00 e si aggiorna al 18 febbraio 2008.

IL VERBALIZZANTE