Ministero dell'Interno

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

VERBALE

COMITATO TECNICO SCIENTIFICO PERMANENTE

DEL 3 / 11 MARZO 2008

In data 3 marzo e in prosecuzione in data 11 marzo 2008 alle ore 10.00, presso gli Uffici della Direzione Centrale per i Servizi Demografici si è tenuta la riunione del Comitato Tecnico Scientifico Permanente avente all'ordine del giorno l'esame dei seguenti punti:

- Analisi e valutazione dei verbali di test di qualificazione delle apparecchiature apparati biometrici effettuati presso il CNSD e relativo giudizio di idoneità tecnica;
- Discussione sull'esito dell'incontro con i rappresentanti di Assocertificatori del 25 febbraio 2008;
- Analisi della domanda di omologazione del chip e relativi allegati alla luce di quanto emerso nella seduta del 25 febbraio u.s.;

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

Apre la seduta la D.ssa Fico sottoponendo all'esame del Comitato i verbali dei test di omologazione degli apparati per l'emissione della carta d'identità elettronica effettuati presso il CNSD.

La D.ssa Fico presenta i verbali dei test delle apparecchiature di seguito elencate unitamente alle autodichiarazioni dei parametri aggiuntivi approvati dal Comitato nella seduta del 25 gennaio 2008 e presentate dalle Società:

- Dispositivo Acquisizione Dati Biometrici Greenbit Scan-CIE DTS-F;
- Dispositivo Acquisizione Dati Biometrici FIMA CIE POINT;
- Dispositivi Acquisizione Dati Biometrici CKB 10000 e CKB 10000/A;
- Dispositivo Acquisizione Dati Biometrici E-P Terminal;
- Stampante termografica CX 330 DAAD;
- Stampante termografica Nisca PR 5350 con laminatore PR 5302;
- Dispositivo Acquisizione Dati Biometrici BTT CAMERA;
- Dispositivo Acquisizione Dati Biometrici BTT WEB;
- Dispositivo Acquisizione Dati Biometrici Biometric 6;
- Autodichiarazioni Dispositivo Acquisizione Dati Biometrici ET-500;
- Autodichiarazione Stampanti termografiche 580i, 590i, SP75.

Il Comitato decide di procedere a valutazione analizzando, mediante confronto, i verbali della check list dei test per qualificazione realizzati presso il CNSD congiuntamente alle autodichiarazioni dei parametri aggiuntivi presentate dalle società.

Il Dispositivo Acquisizione Dati Biometrici Greenbit Scan-CIE DTS-F risulta dall'analisi dei verbali dei test omologabile, tuttavia il Comitato analizzata l'autodichiarazione dei parametri aggiuntivi rileva che alcuni parametri devono essere precisati dalla società.

In particolare la nota in argomento riporta nella descrizione del lettore di smart card "*compatibilità driver TWAIN per Windows 2000, XP, Vista 32 e 64 bit*". Il Comitato Tecnico Scientifico Permanente richiede maggiori dettagli su tale affermazione ritenendo che la

caratteristica indicata non sia supportabile dal lettore / scrittore di smart card essendo essa relativa ai soli dispositivi di acquisizione.

Il Comitato ritiene, altresì, di richiedere delucidazioni relative all'affermazione "*formato ICAO imposto*" riportata nel verbale di test di omologazione del dispositivo relativamente al test relativo alla "Qualità della risoluzione" della foto.

Per quanto sopra il Comitato ritiene di dover attendere le integrazioni che la Società vorrà trasmettere al fine di poter esprimere un giudizio di idoneità tecnica in occasione della prossima seduta.

Il Dispositivo Acquisizione Dati Biometrici FIMA CIE POINT viene ritenuta, sulla base dell'analisi dei test effettuati unitamente alla autodichiarazione dei parametri aggiuntivi omologabile.

Per quanto sopra il Comitato esprime un giudizio di idoneità tecnica per detta apparecchiatura. L'apparecchiatura sarà inserita nella lista delle apparecchiature omologate pubblicata sul sito web della Direzione Centrale per i Servizi Demografici.

Il Comitato passa all'esame della check list dei test e delle autodichiarazioni dei parametri aggiuntivi concernenti i Dispositivi di Acquisizione Dati Biometrici CKB 10000 e CKB 10000/A.

Il Comitato, valutata la documentazione di cui sopra, al fine di procedere all'adozione delle deliberazioni di competenza, richiede alla Società di meglio specificare il punto 4. dell'autodichiarazione in argomento relativamente ai dispositivi CKB 10000 e CKB 10000/A. In particolare la dicitura usata è la seguente " l'apparato **è/ non è** dotato di scanner piano di formato A6 per scansione foto/firma con risoluzione ottica di 600 dpi, 24 bit colore, interfaccia USB controllabile tramite twain e driver per i sistemi operativi Windows 2000, Xp". Occorre specificare l'una o l'altra ipotesi.

Il Comitato ritiene, altresì, di richiedere l'identificazione del dispositivo oggetto di test relativamente al verbale di test del 22 febbraio 2008. In particolare la dicitura è la seguente: "Modello apparato:CKB 10000 CKB10000/A; Versione 1.4 senza pressure sensitive + webcam trust **1/3pollice o Intuix ½ pollice**". Occorre indicare l'uno o l'altro dispositivo oggetto di test**.**

Per quanto sopra il Comitato ritiene di dover attendere le integrazioni che la Società vorrà trasmettere al fine di poter esprimere un giudizio di idoneità tecnica in occasione della prossima seduta.

Il Dispositivo Acquisizione Dati Biometrici E-P Terminal risulta dall'analisi dei verbali dei test omologabile, tuttavia il Comitato analizzata l'autodichiarazione dei parametri aggiuntivi rileva dei parametri da chiarire.

Nello specifico l'autodichiarazione dell'Apparato Biometrico E-P Terminal manca della definizione dell'interfaccia di tipo twain per il lettore di impronte e per lo scanner.

Per quanto sopra il Comitato ritiene di dover attendere le integrazioni che la Società vorrà trasmettere al fine di poter esprimere un giudizio di idoneità tecnica in occasione della prossima seduta.

Dal verbale dei test della stampante termografica CX 330 DAAD risulta che le prove non sono state portate a termine e la società ripresenterà nuova domanda. Per l'autodichiarazione dei parametri aggiuntivi non si rilevano incongruenze.

Per la Stampante termografica Nisca PR 5350 con laminatore PR 5302 si attende il risultato dei test di qualità effettuati presso l'IPZS.

I Dispositivi di Acquisizione Dati Biometrici BTT CAMERA, BTT WEB, Biometric 6 risultano dall'analisi dei verbali dei test omologabili, tuttavia il Comitato al fine di procedere all'adozione delle deliberazioni di competenza, richiede alla Società di specificare il punto dell'autodichiarazione dei parametri aggiuntivi relativo all'interfaccia di tipo twain per il lettore di impronte e per lo scanner;

Il Comitato passa ad esaminare l'autodichiarazione del Dispositivo Acquisizione Dati Biometrici ET-500.

Il documento non presenta incongruenze per cui il Comitato ritiene che l'autodichiarazione sia coerente a quanto richiesto e che possa essere confermata l'omologazione per detta apparecchiatura. L'apparecchiatura sarà inserita nella lista delle apparecchiature omologate pubblicata sul sito web della Direzione Centrale per i Servizi Demografici.

In ultimo si procede alla valutazione dell'autodichiarazione Stampanti termografiche 580i, 590i, SP75.

Le autodichiarazione relative alle stampanti termografiche 580i, 590i non presentano incongruenze per quanto attiene la stampante termografica Datacard SP75 il Comitato, al fine di procedere all'adozione delle deliberazioni di competenza, ritiene di dover richiedere alla Società di meglio specificare il punto concernente il range di velocità di laminazione.

Per quanto sopra il Comitato esprime un giudizio di idoneità tecnica per le stampanti termografiche 580i, 590i mentre per la stampante termografica Datacard SP75, ritiene di dover attendere le integrazioni che la Società vorrà trasmettere al fine di poter esprimere un giudizio di idoneità tecnica in occasione della prossima seduta.

Si conviene che in caso di giudizio di **non idoneità tecnica** delle apparecchiature sottoposte a omologazione le Società, pur avendo facoltà di ripresentare domanda per le stesse apparecchiature, devono distinguere gli apparati risottoposti a test mediante specifica del numero di versione o revisione delle stesse.

Interviene il Dott. De Maria che, in relazione all'autodichiarazione dei parametri aggiuntivi richiesti alle Società, chiarisce al Comitato che i range di velocità di laminazione e di temperatura di laminazione sono da intendersi come range massimi.

In altri termini non si deve scendere sotto i 5mm/sec come velocità di laminazione né salire oltre i 20mm/sec.

Analoga specifica è avanzata da IPZS rispetto alla temperatura di laminazione: sopra i 190° si rischia la fusione del PVC, sotto i 120° si rischia una cattiva adesione della stampa.

La D.ssa Fico invita i presenti ad affrontare l'esame del punto all'ordine del giorno relativo all'esito dell'incontro con i rappresentanti di Assocertificatori del 25 febbraio 2008 con particolare attenzione all'aspetto afferente la Firma Digitale.

Dalla discussione emergono due aspetti sui quali occorre approfondire:

1. il rapporto tra Comune e certificatore stante quanto disciplinato dal Decreto Interministeriale dell'8 novembre 2007 sulle regole tecniche sulla carta d'identità elettronica che pone a capo del Comune il caricamento della firma digitale sulla carta d'identità elettronica;
2. lo schema di caricamento del servizio relativamente alla creazione della struttura, alla creazione delle chiavi e all'attivazione e consegna PIN/PUK di firma.

In particolare i requisiti da CWA14169 prevedono la Generazione onboard in ambiente sicuro, la Secure channel per la generazione e per la firma, un primo uso delle chiavi da parte del titolare ed un PIN ad ogni firma.

Dal confronto in corso del Comitato emerge il seguente possibile scenario:

- Multi fornitore
- Multi certificatore
- Caricamento del file system di firma specificato dal fornitore
- Generazione delle chiavi in IPZS, se possibile, con un ulteriore oggetto con hash della chiave pubblica firmato
- La carta viene emessa con la struttura di firma bloccata, con un meccanismo dipendente dalla carta
- Al ritiro della carta, si può attivare contestualmente la firma o meno. Se non l'attiva ritira una busta PIN/PUK di firma. Questo presuppone che il comune possa operare come

LRA. L'attivazione consiste nella richiesta del certificato di firma, firmata con la propria chiave. L'operazione può essere anche fatta in seguito

- La richiesta di certificato viene mediante un P10, fatta tramite una libreria P11 'administrator' che permette di: attivare la struttura mediante un PIN, firmare la richiesta di certificato, caricare il certificato.
- E' necessario etichettare preventivamente gli oggetti con CKA_ID predeterminati
- L'utilizzo è realizzata con una P11 di utilizzo
- Verso l'applicazione c'è un'unica interfaccia
- Verso le carte sono n interfacce (una per certificatore)

L'IPZS specifica che lo scenario prospettato presenta quattro componenti di costo: costo di caricamento struttura di firma (tempo di personalizzazione e scrittura sw di personalizzazione); costo di generazione delle chiavi (tempo di personalizzazione e scrittura sw di personalizzazione); costo libreria P11 'admin' e costo libreria P11 'usage'. Dette componenti saranno esaminate in dettaglio.

Il prof. Marinelli come già espresso in precedenti occasioni e come chiaramente emerso nella riunione del 25/2/2008 nel confronto con Assocertificatori ricorda che, poiché l'attuale normativa sulla firma digitale consente ad ogni produttore di chip di implementare un proprio file system per la firma digitale, chi scrive sulla CIE il file system per la firma digitale deve riconoscere il modello e il produttore del microchip. In conseguenza di ciò anche la libreria software (PKCS#11) per interfacciarlo è specifica per il singolo modello e produttore del microchip stesso. Infatti i PKCS#11 interagiscono con le APDU, che non sempre si comportano in modo uniforme, e quindi con i sistemi operativi dei microchip. Ogni certificatore accreditato ha di fatto scelto uno o più microchip e lo specifico software (PKCS#11) per il caricamento della firma, fornito, di norma dal produttore del chip stesso. Addirittura capita che uno stesso

produttore di chip fornisca software (PKCS#11) diversi per lotti diversi di microchip a fronte di cambiamenti minimali dallo stesso introdotti, venendosi così a configurare extra costi e ulteriori complessità organizzative. Considerando che per la CIE deve essere esperita a breve la gara per la scelta del microchip si verrebbe a prefigurare il paradosso che scegliendo a gara il produttore di microchip, l'assegnazione stessa della gara introduce una sperequazione nei confronti dei certificatori di firma digitale favorendo quelli in grado, nell'immediato, di inserire la firma digitale sulla CIE in quanto già utilizzano per la loro firma digitale il microchip del produttore vincitore della gara. Non essendo ovviamente possibile che la gara dei microchip vada di fatto ad individuare anche il fornitore di firma digitale è necessario coinvolgere i produttori di chip e i certificatori accreditati per la firma digitale al fine di individuare le opportune soluzioni di interoperabilità. Va ribadito con chiarezza che comunque una soluzione di un sostanziale mantenimento dello status quo comporterebbe l'assunzione da parte del Ministero dell'Interno e/o da parte dei comuni dell'onere dell'acquisto dei diversi PKCS#11 necessari per i diversi microchip. Per ciascuna smart card utilizzata per la CIE deve, infatti, essere possibile inserire la firma digitale rilasciata da uno qualsiasi dei certificatori accreditati. Va, ovviamente, garantita anche l'interoperabilità per l'uso della firma digitale. Ovviamente il Ministero dell'Interno deve avere certezza che non si creino situazioni anomale e deve avere garanzia della piena e libera disponibilità dei software PKCS#11, da fornire da parte dei produttori di microchip, per il caricamento e l'uso della firma digitale senza costi aggiuntivi rispetto alla fornitura dei microchip per la CIE. In tale direzione vanno le già formulate richieste di integrazione nella domanda di omologazione chip in merito all'impegno da parte di tutti i produttori che presentino domanda di omologazione a fornire al Ministero dell'Interno a titolo gratuito e con possibilità di distribuzione illimitata i software e/o gli script che consentono di inizializzare il file system della CIE e le componenti di file system e di sicurezza relative alla firma digitale, di generare le coppie di chiavi pubbliche e private a bordo della CIE necessarie ai processi di

autenticazione e di firma digitale e di fornire tutti gli altri software eventualmente necessari all'inizializzazione ed uso sia in fase di omologazione per gli opportuni test che contestualmente alle forniture al fine della libera distribuzione. Il prof. Marinelli chiarito che ci si trova ancora in una fase preliminare per la definizione della soluzione chiede quindi con urgenza a IPZS di inidicare nel loro documento soluzioni concrete ed operative soprattutto per gli elementi più critici. Chiede inoltre che tale documento comprenda un cronogramma che chiarisca le tempistiche per le relative soluzioni operative. L'urgenza di individuare una soluzione nell'imminenza delle gare per l'acquisto dei microchip ci obbliga purtroppo, considerati i tempi legati alla definizione di un file system unico per la firma digitale, soluzione naturale di tutto il problema, ad individuare una soluzione intermedia che consenta una rapida operatività della firma digitale sulla CIE garantendo trasparenza al mercato senza oneri aggiuntivi per il Ministero dell'Interno e/o i Comuni.

Il Comitato prende atto di quanto presentato e si riserva di approfondire la questione alla luce del documento che verrà presentato.

Le due sedute terminano rispettivamente alle ore 12.30 e 13.

Il Comitato si aggiorna al 13 marzo 2008.

IL VERBALIZZANTE