Ministero dell'Interno

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

VERBALE

COMITATO TECNICO SCIENTIFICO PERMANENTE

DEL 10 LUGLIO 2008

In data 10 luglio 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:

- Valutazione dei test effettuati presso il CNSD;
- Valutazione e confronto sulla nota presentata dall'IPZS concernente la tempistica di acquisizione chip;
- Varie ed eventuali.

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

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

La D.ssa Fico apre la seduta con il primo punto all'ordine del giorno afferente i test effettuati presso il CNSD sugli apparati biometrici di seguito elencati:

- Apparato Biometrico ET500-2T,test del 27 giugno 2008;
- Apparato Biometrico ET500-2I, test del 27 giugno 2008;
- Apparato Biometrico ET500Plus-1T, test del 27 giugno 2008.

Sulla base dell'analisi dei verbali nonché dei supporti, il Comitato esprime i seguenti giudizi di idoneità tecnica:

- Apparato Biometrico ET500-2T: giudizio di **idoneità tecnica positivo**;
- Apparato Biometrico ET500-2I:; giudizio di **idoneità tecnica positivo;**
- Apparato Biometrico ET500Plus-1T: giudizio di **idoneità tecnica positivo**.

Il Comitato conviene, come da prassi, che i giudizi espressi siano comunicati direttamente alle Società interessate e che ne sia data evidenzia nella lista delle apparecchiature, omologate secondo i nuovi parametri, pubblicata sul sito web della Direzione centrale per i Servizi Demografici.

In relazione ai dispositivi apparati biometrici il Comitato rileva l'opportunità che la sottocommissione in fase di test presso il CNSD specifichi sul verbale il dispositivo di acquisizione della foto presente nell'apparato: fotocamera, telecamera o scanner e in caso di presenza di entrambi si richiede che siano testati.

Il Comitato specifica, inoltre, che nell'evenienza che una delle modalità di acquisizione della foto presenti delle anomalie, l'apparato è omologato esclusivamente per la modalità funzionante e la società dovrà impegnarsi a specificare tra le caratteristiche dell'apparato unicamente il dispositivo omologato dal Comitato.

La D.ssa Fico invita i presenti ad affrontare il secondo punto all'ordine del giorno: valutazione e confronto sulla nota presentata dall'IPZS concernente la tempistica di acquisizione chip, trasmessa dall'Ing. De Maria in data 2 luglio 2008.

L'Ing. De Maria passa all'esposizione della nota nel suo contenuto e richiede che la stessa sia parte integrante del verbale.

La D.ssa Fico richiede che la discussione sull'argomento si concluda con un documento illustrativo sui punti fondamentali da affrontare da presentare alle valutazione del Comitato di Indirizzo e di Monitoraggio.

La D.ssa Fico, inoltre, in relazione al DL n. 112 del 25 giugno 2008, richiede all'Istituto Poligrafico e Zecca dello Stato una analisi approfondita sulla validità della CIE a 10 anni in relazione soprattutto alle caratteristiche del supporto fisico e del chip.

L' Ing. De Maria si riserva di presentare un documento in relazione a quanto richiesto.

L'Ing. De Maria prosegue con l'esposizione della nota evidenziando in particolare tre step connessi alla tempistica di acquisizione dei chip:

- Definizione del taglio di memoria del chip da acquisire;
- Firma digitale e software per la firma digitale;
- Gestione del transitorio sino ad approvvigionamento dei nuovi chip.

Prende la parola l'Ing. Ditoma il quale evidenzia l'importanza che qualsiasi espressione del Comitato in ordine alle questioni esposte sia suffragata da motivazioni di ordine tecnico normativo.

Il comitato concorda con il suddetto avviso.

Interviene il Prof. Marinelli il quale suggerisce che, ogni nota che si riterrà di trasmettere al Comitato di indirizzo e monitoraggio dovrà essere elaborata nell'ottica del DL n.112 anche in considerazione del documento che l'IPZS produrrà in ordine alla validità del supporto CIE per un arco temporale di 10 anni.

L'Ing. Manca comunica che ad oggi non vi sono chip in cui si possa inserire la firma digitale per una durata di 10 anni.

In relazione alla definizione del taglio di memoria del chip da acquisire il Comitato si confronta alla luce di quanto disposto dal DM dell'8 novembre 2007 recante le regole tecniche della CIE, che al punto 4.3 dell'allegato B dispone che per la CIE sono ammissibili, per un periodo transitorio, tagli di memoria EEPROM da almeno 32KBytes e algoritmi RSA, per operazioni di crittografia asimmetrica, almeno a 1024 bit. A regime, tenendo conto delle tecnologie disponibili, dovranno essere utilizzati tagli di memoria EEPROM da almeno

64KBytes e con algoritmi RSA almeno a 2048 bit.

Il Comitato concorda sulla predisposizione di un documento in cui sia data evidenza del taglio di memoria necessario nel chip tenendo conto dello spazio necessario per il file system, per due strutture di firma digitale e per i servizi da caricare. Si conviene di effettuare la computazione completa nel corso della seduta successiva.

Si passa alla valutazione della gestione del software della firma digitale.

Il Comitato discute sul funzionamento separato dei PKCS11 a seconda dell'applicazione.

L'IPZS si offre di acquisire il P11 di firma (software di libreria per il caricamento e l'uso del servizio di firma digitale), il Prof. Marinelli evidenzia in merito che il P11 delle singole carte dovrebbe essere multipiattaforma e che i fornitori dovrebbero consegnarlo con le specifiche di dettaglio per il caricamento del servizio di firma e per il suo uso.

Il Comitato chiede che le librerie siano disponibili almeno per le piattaforme Windows XP da SP2, Vista, MacOS dalla versione 10.x, Linux dal Kernel 2.4.x.

Prende la parola l'Ing. De Maria il quale evidenziando che la manutenzione correttiva delle librerie è fornita dal fornitore per il tramite dell'IPZS, evidenzia che si deve decidere a chi debba essere posto in capo l'assistenza.

Dal confronto si palesa che lo strato di interfaccia per l'interoperabilità è un onere a carico del Ministero dell'Interno, rispetto a tanto il Prof. Marinelli evidenzia la necessità di definire regole specifiche che dovranno essere fornite unitamente al P11 e che richiedono una comunicazione integrata tra l'IPZS e il Ministero dell'Interno oltre che un certo numero di giorni di supporto all'integrazione da richiedere al fornitore. Inoltre il fornitore dovrà fornire, insieme al software P11 sviluppato anche tutta la documentazione di dettaglio e le componenti necessarie a che il Ministero dell'Interno abbia la piena autonomia per lo sviluppo delle procedure di interoperabilità. A tal fine IPZS si coordinerà con L'Università di Tor Vergata per la definizione

dei requisiti e delle specifiche per l'acquisizione dei microchip e del software P11 di caricamento ed uso del servizio di firma digitale.

L'Ing. De Maria riferisce che l'IPZS intende evitare il rischio che, acquisito un chip, questo non possa essere usato dai certificatori.

L'Ing. Manca ritiene che tale rischio sia nullo.

Il Comitato conviene di ultimare l'analisi degli argomenti posti all'ordine del giorno con particolare riferimento alla definizione del taglio di memoria del chip nel corso della prossima riunione.

La seduta termina alle ore 13.00 e si aggiorna al 14 luglio 2008.

IL VERBALIZZANTE