Ministero dell'Interno

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

VERBALE

COMITATO TECNICO SCIENTIFICO PERMANENTE

DEL 14 LUGLIO 2008

In data 14 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 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".

In via preliminare all'analisi degli argomenti all'ordine del giorno, la D.ssa Fico presenta il materiale fatto pervenire dalla ST Incard in relazione alla domanda di omologazione del chip.

Il Comitato conviene che il materiale passi all'esame della Commissione per la verifica e omologazione del chip.

La D.ssa Fico invita i presenti a proseguire l'analisi, già iniziata nel corso della riunione del 10 luglio 2008, concernente la tempistica di acquisizione chip, con particolare riferimento alla computazione del taglio di memoria del chip.

Il Comitato avanza considerazioni di ordine tecnico con riferimento al confronto tra CIE e CNS e a quanto stabilito per quest'ultima dalla Regione Lombardia.

Si passa al calcolo puntuale per componenti della memoria necessaria: il file system attuale della CIE con esclusione della firma richiede **21.588** byte. Sommando a tale computo lo spazio necessario per due strutture di firma con due certificati e tre coppie di chiavi il taglio di memoria necessario risulta di almeno **29.360** byte.

Il suddetto calcolo prospettato da IPZS sarà trasmesso e acquisito agli atti del Comitato.

Interviene il Prof. Marinelli il quale ritiene che la memoria libera sulla CIE debba essere perlomeno pari a quella presente sulla CRS o sulla CIE attuale.

L'Ing. Manca riferisce che nella CRS sono disponibili 6Kb al netto di tutti i servizi aggiuntivi.

Il prof. Marinelli ribadisce gli spazi di memoria necessari: 22 KB per il file system, 8Kb per due strutture di firma e 10 Kb per i servizi aggiuntivi.

Il Comitato conviene di richiedere 10 Kb di memoria per i servizi aggiuntivi al pari di quelli presenti sulla CIE attuale giungendo a definire il taglio di memoria libera per il chip in **40 Kb.**

Il Comitato passa alla valutazione dello SHA-2.

In relazione all'argomento l'Istituto Poligrafico e Zecca dello Stato ritiene che non sia necessaria la presenza di questo algoritmo sulla carta, poiché nei protocolli di autenticazione e di firma l'hash viene sempre calcolato fuori dalla carta, mai dalla carta. Infatti, nel set di APDU CIE non sono presenti comandi per calcolare l'hash. Pertanto, questo non sarà un requisito per i chip da acquisire, così come non lo era lo SHA-1.

Riguardo alla questione sulla lunghezza delle chiavi, (1024 bit o 2048 bit), l'Ing. De Maria fa presente che, sebbene i vari fornitori abbiano chip che supportano chiavi a 2048 bit, non c'è una soluzione standard, né tantomeno comune a più fornitori. Per poter utilizzare chiavi

a 2048 bit si dovrebbero quindi aggiornare i comandi APDU della CIE in modo da supportare le lunghezze estese.

La posizione espressa dal Prof. Marinelli richiama un rinvio della discussione sullo sha-2 tra qualche mese, mentre ad avviso del Prof. la questione della lunghezza della chiave a 2048 dovrà essere riaffrontata a breve soprattutto alla luce della normativa che prevede una proroga della carta d'identità a dieci anni.

L'Ing. Ditoma ribadisce la sua posizione che va nell'ottica di decisioni che siano scientificamente plausibili e giustificabili e che possono prescindere dalla situazione di mercato.

Il Comitato si confronta anche rispetto alle *Java Card* per le quali si richiama l'attenzione sulle performances che, di norma, risultano inferiori a quelle delle "native card".

Per quanto attiene la firma digitale l'Ing. Manca afferma che non sussistono limitazioni se il chip è a norma di legge.

il Comitato è dell'avviso che sia fortemente improbabile che i certificatori siano disposti ad assumersi la responsabilità di un certificato di firma che duri dieci anni.

Il Comitato prospetta l'opportunità di avere due o tre coppie di chiavi a 1024.

La discussione non viene definita in quanto si necessita una maggiore definizione degli scenari di mercato relativi alla firma.

La seduta termina alle ore 13.00 e si aggiorna al 29 luglio 2008.

IL VERBALIZZANTE