



Ministero dell'Interno

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

VERBALE **COMITATO TECNICO PERMANENTE** **DEL 17 DICEMBRE 2007**

In data 17 dicembre 2007 alle ore 10.30, presso la Direzione Centrale per i Servizi Demografici si è tenuta una riunione del Comitato Tecnico Permanente avente all'ordine del giorno l'esame dei seguenti punti:

- Evoluzione dei metacomandi CIE;
- Approvazione della versione definitiva del file system;
- Approvazione versione finale specifiche APDU.
- Valutazione definitiva dei requisiti minimi hardware e software concernente i dispositivi di acquisizione dati biometrici alla luce delle osservazioni fatte pervenire dalle società.
- Varie ed eventuali.

Alla riunione presieduta dalla D.ssa Fico, Vice Prefetto Aggiunto, Responsabile del Servizio Carta d'Identità, hanno partecipato:

- L'Ing. Giovanni Manca del CNIPA
- L'Ing. Andrea De Maria dell'Istituto Poligrafico e Zecca dello Stato;
- L'Ing. Leopoldo Consiglio dell'Istituto Poligrafico e Zecca dello Stato;
- Il Prof. Guido Marinelli dell'Università degli studi di Roma "Tor Vergata";
- Il Dott. Fabrizio Abratis del Ministero dell'Interno.



Ministero dell'Interno

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

Aprire la seduta la D.ssa Fico chiedendo ai partecipanti lo stato del documento definitivo del file system anche alla luce dei commenti e delle delucidazioni fatte pervenire dall'Università Tor Vergata nella persona del Prof. Marinelli.

Il Comitato concorda di analizzare punto per punto le delucidazioni richieste.

Ai quesiti i rappresentanti dell'IPZS rispondono puntualmente.

1. File dati personali aggiuntivi:

La funzione del file è permettere la scrittura delle annotazioni analogamente a quanto accade per la versione cartacea della carta d'identità. Dette annotazioni sono riportate durante la fase di scrittura del DF1.

Il file attualmente presente nel DF2 non è né utilizzato né codificato. Nel caso fosse utile per i servizi aggiuntivi, è prevista la possibilità di creare file dati aggiuntivi a chi scrive il DF2 sotto la supervisione del Ministero dell'Interno e del Comune che ha emesso la CIE.

Il Comitato concorda di eliminare il file Dati Personali Aggiuntivi presente nel DF2 e di aggiungere un file Dati Personali Annotazioni nel DF1. Quest'ultimo file non concorre al calcolo dell'hash utilizzato nella composizione del Common Name del Certificato di autenticazione in quanto i dati in esso contenuti non sono verificabili (e quindi certificabili) al momento dell'inserimento. Il file è protetto da PUK in scrittura fino al Comune, viene lockato in scrittura in fase di emissione, ed è protetto in lettura da PIN utente. Dimensione del file: 256 byte netti.

2. DIMENSIONE DEL FILE EF_ATR:

La dimensione del file EF_ATR dipende dagli elementi che il produttore del sistema operativo vi inserisce. Esiste la possibilità che si inserisca l'intero ATR o i soli caratteri storici. E' necessario che il produttore dichiari la modalità di scrittura del contenuto del file. Si ritiene di non richiedere che le modifiche del file si rispecchino in modifiche



Ministero dell'Interno

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

dell'ATR.

3. Posizione delle operazioni proposte su Kia Kic:

Kia e Kic sono stati invertiti perchè nella versione precedente erano errati. Questo risulta specificato anche nelle note di rilascio del draft.

4. Criteri di protezione del DF1:

I criteri già esposti via mail vengono ribaditi per completezza dall'IPZS. Nella precedente versione e nel vecchio file system della CIE, la condizione di accesso AC_ADMIN del DF era impostato, in fase di inizializzazione, al valore PUK_USER (11h) e, successivamente, impostato in fase di personalizzazione a NEVER (FF). Tale passaggio non risulta necessario in quanto le modifiche alle condizioni di accesso necessarie sui file in DF1 sono, dal punto di vista della sicurezza, regolate dalla AC_ADMIN del file stesso. Lasciare aperta la condizione del suddetto accesso nel DF1 potrebbe inficiare la sicurezza degli oggetti nello stesso DF nella parte di ciclo di vita della carta tra l'inizializzazione e la fine della personalizzazione.

Si concorda, pertanto, di lasciare sulla versione 2.0 RC-1 del file system CIE AC_ADMIN=NEVER (FF) in entrambi le fasi.

5. Generate Key Pair:

Nella modalità proposta nel documento si va in direzione di maggiore sicurezza. In sede di Comitato è stato richiesto di uniformare i criteri di generazione delle chiavi a quelli utilizzati per gli altri file: AC_GENKEYPAIR=PUK_USER in fase di inizializzazione da "lockare" a NEVER in fase di personalizzazione. Al fine di consentire la modifica della condizione di accesso di cui sopra, è necessario, in fase di personalizzazione, lasciare aperta (PUK_USER)



Ministero dell'Interno

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

la condizione AC_UPDATE del master file. Detta modalità comporterebbe una diminuzione della sicurezza dell'intera carta. Nella versione Draft C, è stato posto AC_GENKEYPAIR=PUK_USER in fase di inizializzazione senza prevederne il lock in fase di personalizzazione in modo da avere il Master File con condizioni di accesso sempre a NEVER. Questa situazione non inficia in alcun modo la sicurezza generale della carta in quanto, la condizione di accesso AC_GENERATEKEYPAIR=PUK_USER, non consente comunque di rigenerare la coppia di chiavi considerando che la chiave pubblica corrispondente (EF_KeyPub) ha AC_UPDATE=NEVER.

Il prof. Marinelli chiede assicurazioni in merito al fatto che le condizioni di accesso modificate, così come descritto nei precedenti punti, permettano comunque la corretta personalizzazione della carta e la scrittura sul chip di tutti gli elementi necessari. IPZS fornisce tale assicurazione.

Su proposta del Prof. Marinelli si concorda di inserire nelle references del file system il riferimento al decreto sulle regole tecniche della carta d'identità elettronica del 9 novembre 2007.

Alla luce delle annotazioni e dei chiarimenti sopra esposti il draft del File System viene definitivamente approvato dal Comitato previo assenso inoltrato via mail dai convenuti per la pubblicazione come Release Candidate 1.

La D.ssa Fico passa all'esame dell'argomento all'ordine del giorno relativo all'approvazione della versione finale del documento sulle specifiche APDU.

Il Comitato approva e sottoscrive il documento sulle specifiche APDU pubblicate in RC-1.

Si esamina il punto concernente la valutazione definitiva dei requisiti minimi hardware e software relativa ai dispositivi di acquisizione dati biometrici alla luce delle osservazioni fatte



Ministero dell'Interno

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

pervenire dalle società.

Interviene l'Ing. Manca il quale fa presente, alla luce delle osservazioni fatte pervenire dalle società nonché delle valutazioni del CNIPA, l'opportunità di precisare alcuni aspetti della lista relativamente all'esatta dicitura di alcuni requisiti suggerendo di riferirsi alle modalità utilizzate nei capitolati CONSIP.

Il prof. Marinelli precisa che i requisiti pubblicati tengono conto della compatibilità con la fase di sperimentazione. In fase di gara IPZS dovrà fornire requisiti più puntuali.

Per quanto attiene i PC, l'IPZS viene incaricata di verificare le prescrizioni di CNIPA sulle forniture hw.

Si conviene di sostituire i requisiti minimi della scheda rete del PC 10/100/1000 con 10/100, di eliminare la porta SCSI qualora i lettori di banda ottica vengano forniti con-controller SCSI "in bundle".

Il Comitato conviene, inoltre, che sia possibile ridurre il requisito per il processore a 3Ghz. Andrà comunque tenuto conto dei benchmark del CNIPA per quanto riguarda l'equivalenza tra processori di diverse marche e di diversa tecnologia. Per quanto attiene l'acquisizione della firma il Comitato decide che va meglio esplicitato che tavoletta 'pressure sensitive' e scanner piano sono alternativi, anche se la normativa già lo chiarisce, in quanto alcuni fornitori hanno chiesto conferma in merito.

Relativamente all'apparato per fingerprint, nel corso dell'incontro che si terrà presso il CNIPA il 21 dicembre 2007, sarà fornito un documento di requisito minimo che verrà valutato per l'eventuale integrazione dei requisiti minimi hw/sw.

Per le motivazioni sopra esposte si conviene che il documento dei requisiti minimi sarà inviato all'Ufficio CIE dopo il 21 dicembre.

Si conviene di pubblicare il documento con le precisazioni apportate alla luce delle valutazioni sulle osservazioni fatte pervenire dalle società.



Ministero dell'Interno

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

L'Ing. Manca propone di lasciare il documento comunque invariato alla data del 1 ottobre 2007 dal momento che le precisazioni apportate non hanno impatti significativi sugli apparati per usi futuri.

Il Comitato concorda.

Si affronta l'argomento concernente la modalità di acquisizione delle foto. Il Comitato concorda che il requisito sulla dimensione del CCD, presente nel documento pubblicato, non è vincolante, ma solo raccomandato.

La D.ssa Fico richiede di conoscere la situazione del mercato.

Il Prof. Marinelli sottolinea che attualmente sono presenti sul mercato dei software che consentono un controllo di qualità automatico delle foto acquisite. Sarebbe auspicabile dotare le postazioni di emissione di detto software se la concorrenza è ampia e i costi ridotti.

Collegialmente il Comitato ritiene di dover acquisire fotografie di qualità sia per ottenere una stampa di adeguata qualità sia per avere una foto su chip utilizzabile per controlli automatici.

Come evidenziato dal Prof. Marinelli, per raggiungere detti standard, occorrerebbe utilizzare un software di controllo qualità che è di tipo commerciale. Considerando l'impatto economico della soluzione e che la decisione è di tipo politico, si conviene di rinviare la soluzione alle valutazioni del Comitato di Indirizzo e Monitoraggio.

L'Ing. De Maria chiede se la foto e l'impronta debbano essere protetti da PIN.

L'Ing. Manca ritiene che l'aspetto debba essere vagliato con il Garante della Privacy.

Il Prof. Marinelli, ricordando che la domanda riguarda la protezione in lettura, ritiene che il template dell'impronta andrebbe protetto ma che anche questo aspetto andrebbe rinviato alle valutazioni del Comitato di Indirizzo e Monitoraggio.

Il Comitato concorda, rispetto alle osservazioni sulla lista dei requisiti hardware e software pervenute dalle aziende produttrici e distributrici, di integrare tale lista pubblicata sul sito allegando alla stessa un documento che chiarisca le motivazioni delle integrazioni e delle



Ministero dell'Interno

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

modifiche e fornisca le adeguate risposte ai quesiti posti dai produttori/distributori dei dispositivi.

La sessione si scioglie alle ore 13.30 e si aggiorna a data da destinarsi.

IL VERBALIZZANTE