



Ministero dell'Interno

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

VERBALE **COMITATO TECNICO SCIENTIFICO PERMANENTE** **DEL 25 FEBBRAIO 2008**

In data 25 febbraio 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:

- Discussione e analisi degli aspetti concernenti la firma digitale, la qualificazione del chip e eventuali impatti che le modifiche del file system possono avere sul processo di certificazione Common Criteria dello stesso mediante incontro e confronto con i rappresentanti di Assocertificatori invitati alla seduta;
- Sottoscrizione del verbale della seduta dell'11 febbraio 2008;
- Sottoscrizione della domanda di omologazione del chip e relativi allegati al fine della tempestiva pubblicazione;
- Proposte di calendarizzazione delle attività del Comitato alla luce delle priorità individuate per l'evoluzione del progetto Cie;

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;
- Il Prof. Guido Marinelli dell'Università degli studi di Roma "Tor Vergata"



Ministero dell'Interno

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

Alla riunione hanno partecipato inoltre l'Ing. Leopoldo Consiglio dell'IPZS e i rappresentanti di Assosertificatori: la D.ssa Cinzia Villani, il Dott. Paolo Cascino e la D.ssa Assunta Alfano.

Aprè la seduta la D.ssa Fico la quale in qualità di Presidente del Comitato rivolge un saluto di benvenuto ai rappresentanti di Assocertificatori invitati alla sessione odierna del Comitato auspicando che, quello in corso, possa essere il primo di una serie di incontri di collaborazione e confronto reciproco.

La D.ssa Fico presenta agli ospiti il progetto CIE anche sotto il versante normativo con riferimento al Decreto Interministeriale dell'8 novembre 2007 recante "Regole Tecniche sulla carta d'identità elettronica" evidenziando che in detto disposto normativo sono individuati gli organi deputati a compiti specifici all'interno del progetto. Il Decreto disciplina, altresì, l'evoluzione tecnica afferente ai supporti, al chip nonché alle procedure di omologazione delle apparecchiature e del chip. Precisa, inoltre, che l'incontro odierno ha lo scopo di chiarire aspetti relativi alla firma digitale. La D.ssa Fico presenta il resto del Comitato agli ospiti e affida la parola all'Ing. Manca.

L'Ing. Manca presenta i componenti di Assocertificatori evidenziando che l'Associazione si palesa come input per l'interfaccia con il mercato in tema di vigilanza e controllo effettuata dal CNIPA. Evidenzia, inoltre, il rapporto di interoperabilità costruttiva con il mercato, 15 vigilanze su 18 soggetti, nonché la collaborazione con esiti positivi che il CNIPA intrattiene con l'Assocertificatori.

L'Ing. Manca descrive a livello tecnico i compiti in capo al Comitato Tecnico Scientifico Permanente. Con riguardo all'inserimento della firma digitale nel chip, fa notare che nei vecchi supporti non era presente la componente di file system per la firma digitale ma vi sono potenzialità correttive per la fase a regime. Sottolinea, inoltre, che le rappresentanze tecniche in



Ministero dell'Interno

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

seno al Comitato, operando in un contesto istituzionale, hanno quale ancoraggio e riferimento il Decreto Interministeriale dell'8 novembre 2007.

La parola passa alla D.ssa Cinzia Villani di Assocertificatori la quale ringrazia per l'opportunità data dal confronto con un tavolo di lavoro presidiato dal Ministero dell'Interno. Rappresenta al Comitato l'esperienza di firma digitale con la CNS per la quale sono stati emessi 12 milioni di certificati. Su alcune migliaia di queste carte è presente la firma digitale qualificata. Inoltre è disponibile una libreria PKCS#11 per le operazioni di gestione della firma nella CNS stessa.

La D.ssa Villani prosegue evidenziando che rispetto alle normative del CNIPA il certificatore ha l'obbligo di identificare con certezza il titolare della carta, detta procedura richiede che il certificatore conservi per 20 anni la copia cartacea del documento d'identità del titolare.

Le ipotesi prospettate fanno capo al caso in cui l'inserimento della firma digitale avvenga contestualmente all'emissione della CIE e nella fattispecie non vi sarebbero problemi per l'identificazione del cittadino in quanto sarebbe presente di fronte all'ufficiale di anagrafe che lo ha identificato per l'emissione del documento. Differente si presenta la situazione per l'inserimento della firma successivamente all'emissione della CIE.

Prende la parola la D.ssa Fico che sottolinea quale esigenza del Ministero dell'Interno quella di evidenziare le criticità afferenti all'inserimento della firma digitale nel chip della CIE. La D.ssa Fico affida la parola ai partner istituzionali del Ministero.

Interviene il Prof. Marinelli che riassume la riflessione e l'analisi della firma digitale con la CIE evidenziando due ordini di problemi: uno afferente all'inserimento della firma digitale nella CIE ed uno relativo all'utilizzo della stessa con la CIE. Nello specifico il Prof. Marinelli chiede se vi è la possibilità concreta che un certificatore possa inserire la firma digitale su un qualsiasi chip tra quelli certificati common criteria per la firma digitale e quale tipologia di



Ministero dell'Interno

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

vincoli esiste tra produttore di chip e certificatore di firma. Evidenzia altresì che attualmente per la normativa vigente è il Comune a dover inserire la firma nella CIE.

Prende la parola l'Ing. Manca che evidenzia l'opportunità di gestire in modo unico il file system di firma digitale. Inoltre evidenzia anche il fatto che l'intero Comitato Tecnico Scientifico Permanente aveva discusso in senso positivo su questo aspetto.

Interviene la D.ssa Alfano la quale ribadendo che il file system ad oggi non permette l'inserimento della firma nella CIE, evidenzia che per i nuovi supporti il Comune emette contestualmente le due tipologie di certificati (firma e autenticazione); differente è il processo per i vecchi supporti.

L'Ing. Manca evidenzia che in questo caso occorre gestire un percorso differente con i due file system relativi alle smart card emesse nella seconda fase sperimentale. Dovrà essere gestito il caricamento successivo della firma digitale gestendone anche gli aspetti organizzativi oltre a quelli tecnologici. Diversa procedura con le nuove carte per le quali si potrebbe predisporre un'unica libreria di interfaccia per le operazioni di autenticazione e firma anche se ovviamente la valutazione deve essere fatta in modo ampio e valutando anche i costi delle varie operazioni. L'Ing. Manca conclude ricordando che in tutti gli scenari le carte sono riconoscibili mediante l'ATR (Answer To Reset) che è stato standardizzato dal Comitato Tecnico Scientifico Permanente.

La D.ssa Alfano chiede se vi è la disponibilità alla predisposizione del file system per la firma digitale nel chip della CIE durante la fase di inizializzazione della carta.

Risponde in senso positivo il Dott. De Maria.

Il Dott. De Maria chiarisce che per la creazione di un unico file system occorre un unico processo di certificazione protection profile per il quale occorre tempo. I produttori di chip dovranno certificare di nuovo common criteria i loro chip.



Ministero dell'Interno

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

In attesa che tale processo vada a compimento, si continueranno ad avere diversi file system utilizzati dai diversi certificatori. Quindi le carte che si emetteranno nell'immediato futuro non avranno un unico file system bensì si procederà a caricare la firma secondo le modalità del singolo certificatore.

Interviene il Prof. Marinelli il quale ribadisce il quesito concernente la possibilità di caricare la firma digitale su un chip differente da quello usualmente utilizzato dal certificatore. Chiede cosa si deve fare per garantire che tutti i certificatori siano in grado di caricare la loro firma digitale su tutti i chip attualmente certificati common criteria per la firma digitale. Chiede inoltre chi lo deve fare, se il produttore di chip o il certificatore di firma digitale. È chiaro che avere una modalità di caricamento indipendente dal produttore di chip è più generale che costringere ogni certificatore a predisporre con interfacce diverse per ogni chip.

La D.ssa Villani risponde che il certificatore acquista unitamente al chip il relativo PKCS11. Spesso capita (caso chip Siemens) che, pure a parità di produttore e di chip, venga fornito dal produttore di chip un PKCS11 differente a seconda della destinazione del lotto di chip.

Prende la parola la D.ssa Fico chiedendo esplicitamente se, per l'avviso dei rappresentanti di Assocertificatori, vi siano dei criteri o requisiti che occorre richiedere ai fornitori di chip.

La D.ssa Alfano risponde che è importante la disponibilità del fornitore a fornire un unico PKCS11 per il chip e di darne evidenza al certificatore che si assume la responsabilità verso il titolare della firma.

Interviene la D.ssa Fico la quale chiede se i vincoli evidenziati siano noti in fase di omologazione del chip.

La D.ssa Alfano sottolinea che i fornitori devono consentire la gestione del pregresso attraverso un utilizzo standard delle librerie.



Ministero dell'Interno

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

Prende la parola il Dott. De Maria il quale specifica che per la fase di omologazione viene richiesto ai fornitori il software per il caricamento della firma digitale, mentre vi sono differenze per la fase di utilizzo. Prospetta la possibilità di interfacciarsi con l'Assocertificatori al fine di visionare la documentazione presentata dai fornitori.

Interviene il Prof. Marinelli il quale partendo dal presupposto che il PKCS11 dovrebbe essere standard per tutti i chip chiede la motivazione, anche alla luce delle criticità evidenziate nella seduta odierna, per la quale non viene richiesto ai fornitori nella domanda di omologazione. Reputa inoltre che i fornitori debbano fornire anche i codici sorgenti del PKCS11 o della interfaccia necessaria per il caricamento della firma digitale.

La D.ssa Fico propone al tavolo, alla luce delle esigenze manifestate, la possibilità di predisporre una riunione del Comitato ad hoc per delineare uno scenario percorribile in un'ottica di massima trasparenza anche con i certificatori.

La D.ssa Villani prospetta quali argomenti di confronto la procedura da adottare nel caso di CIE revocate o da rinnovare e la necessità di considerare che la durata di validità della CIE sia pari a quella del certificato.

Il Prof. Marinelli ipotizza la possibilità di valutare se Assocertificatori possa fornire il suo parere, non vincolante, durante il processo di omologazione dei chip.

La D.ssa Fico ritiene che il Comitato si riunisca per deliberare sulle questioni emerse nella seduta odierna al fine di procedere nella valutazione di una ipotetica futura collaborazione con Assocertificatori.

La riunione termina alle ore 12.30 e si aggiorna al 3 marzo 2008.

IL VERBALIZZANTE