CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Le potenzialità della CIE per il riconoscimento in rete: accesso ai servizi, livelli di autenticazione e firma digitale.

Giovanni Manca
Ufficio Standard e tecnologie di identificazione

AGENDA

- ***L'identità digitale in Italia (CIE – CNS).***
- ***Il riconoscimento in rete.***
- ***La firma digitale nella CIE.***
- ***Il futuro prossimo dell'identità digitale.***

L’identità digitale in Italia (CIE – CNS).

La Carta d'Identità Elettronica (CIE)

- ***La CIE è una carta ibrida composta da due differenti tecnologie: un circuito elettronico e una banda ottica.***
- ***Sulla parte anteriore della carta, nella parte superiore ci sono la foto e i dati personali del titolare. Nella parte inferiore, la cosiddetta ICAO MRZ (International Civil Aviation Organization - Machine Readable Zone) che consente la lettura automatica degli stessi dati, codificati su tre righe e stampati in OCRB (secondo le disposizioni ICAO).***
- ***Sul retro della carta, oltre ad altri dati personali, sono installati il circuito elettronico, la banda ottica e un ologramma di sicurezza.***
- ***Il circuito elettronico ha una capacità di almeno 32k ed è conforme agli standard ISO della famiglia 7816.***

La CIE – parte anteriore

La CIE – parte posteriore

La Carta Nazionale dei Servizi (CNS)

- ***E' emessa da una pubblica amministrazione.***
- ***Non identifica "a vista" ma solo nell'accesso ai servizi erogati in rete dalla pubblica amministrazione.***
- ***L'emissione di queste carte è stata decisa per accelerare la diffusione di uno strumento per l'identificazione "forte" dell'utente dei servizi in rete.***
- ***La CNS deve essere predisposta per contenere le informazioni crittografiche da utilizzare per la firma digitale.***

La CNS – Parte anteriore

La CNS – parte posteriore

Qualche numero

- **Circa 2.300.00 di CIE inserite nel circuito di emissione della seconda parte della sperimentazione.**
- **A maggio 2007 sono state emesse circa 15 milioni di CNS.**
- **Le carte per la firma digitale sono circa 3.000.000 delle quali circa 400.000 sono CNS.**

Il riconoscimento in rete.

Protocolli per il riconoscimento in rete (1)

- **Il protocollo di riconoscimento in rete è standard da anni e si chiama Secure Socket Layer (SSL).**
- **Tale protocollo prevede la possibilità di associare l'identità dell'utente ad una smart card (per es. la CIE).**
- **Il titolare accede ai servizi perché la possiede e perché ne conosce il PIN.**
- **Il sistema di accoglienza riconosce le credenziali dell'utente e in base ad esse assegna le corrette autorizzazioni**

Protocolli per il riconoscimento in rete (2)

- **Il servizio viene quindi erogato sulla catena di credenziali:.**
  - Identità (Codice Fiscale).
  - Autenticità delle credenziali (protocollo SSL).
  - Autorizzazioni (diritti di utilizzo delle risorse sulla base delle credenziali precedenti).

Protocolli per il riconoscimento in rete (3)

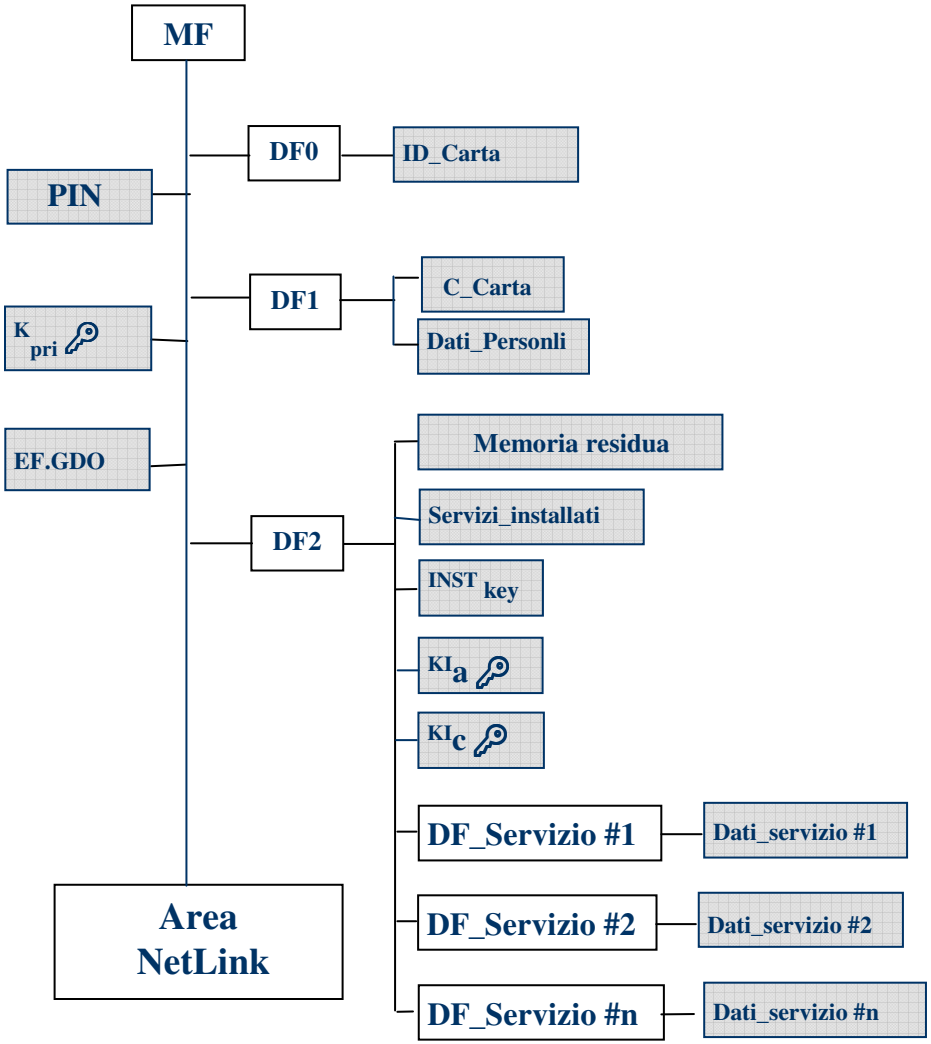
- **La mia identità è unica.**
- **Tutti gli erogatori di servizi riconoscono la mia identità.**
- **Solo i servizi per i quali sono autorizzato vengono erogati.**
- **Le autorizzazioni possono cambiare nel corso di una stessa giornata. Si pensi ad esempio al limite di prelievo di contante con il bancomat.**

La firma digitale nella CIE.

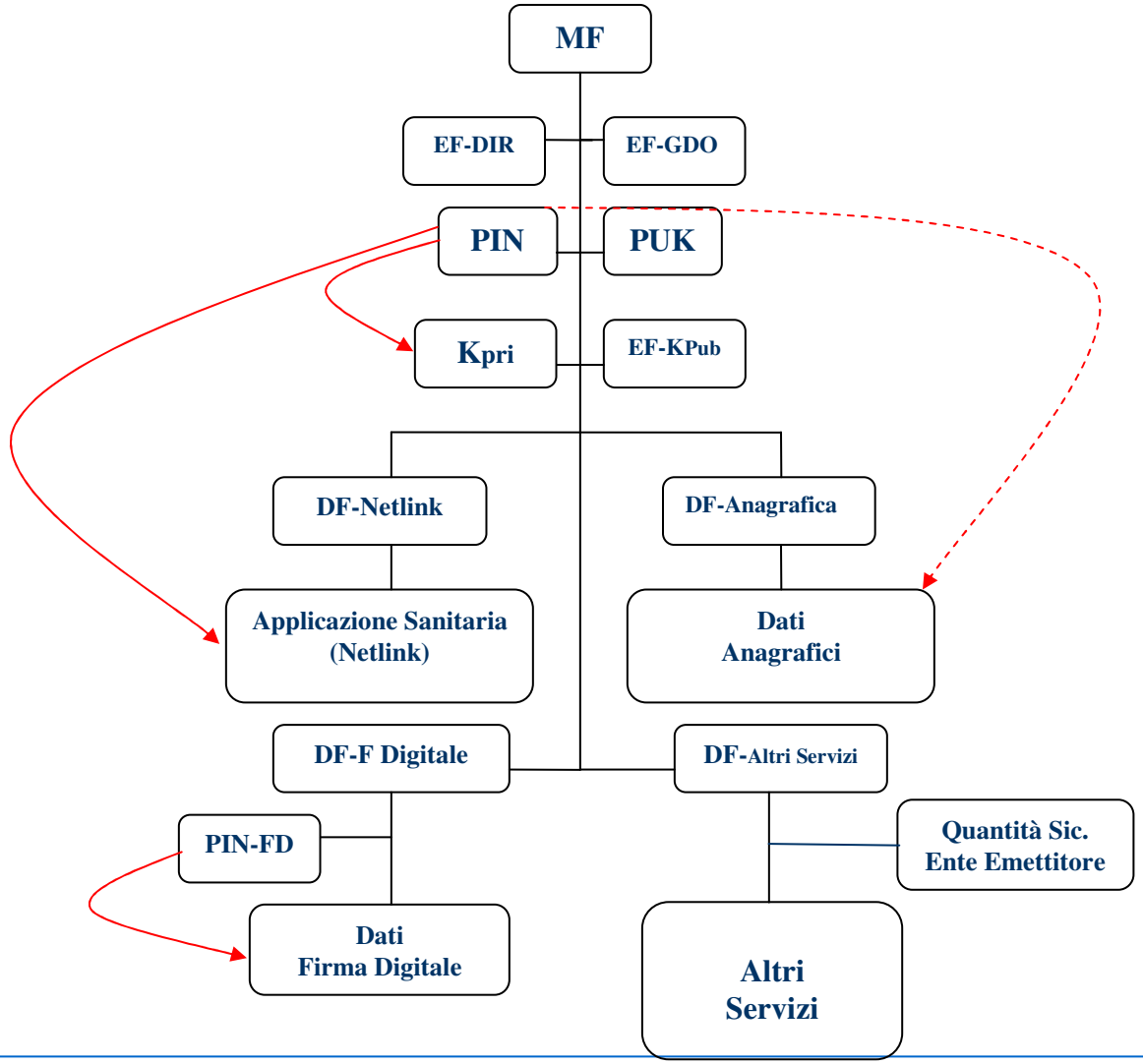
Cosa è la firma digitale nella CIE

- **La firma digitale nella CIE è in una dizione corretta "l'utilizzo della CIE come dispositivo sicuro per la creazione della firma".**
- **La CIE è progettata affinché i dati per l'utilizzo sopra citato possano essere inseriti successivamente all'emissione da parte del Comune.**
- **Tali dati devono essere inseriti da un certificatore accreditato ai sensi del codice dell'amministrazione digitale.**
- **La normativa tecnica di riferimento definisce i dettagli operativi per condurre tali operazioni.**

Schema della CIE (2^ sperim.)



La firma digitale nella CNS



Sintesi del processo di inserimento

- **Le chiavi per la firma digitale sono inserite all'interno della CIE come servizio "qualificato".**
- **Sono definite le modalità di scrittura sulla CIE di tali informazioni. Tali modalità non modificano il livello di sicurezza della CIE.**
- **Tali modalità dovranno essere concordate con i certificatori accreditati.**
- **Una serie di esperimenti che hanno avuto successo si sono svolti con la CNS.**

Il futuro prossimo dell'identità digitale.

Convergenza verso MRTD o… ?

- **Il Passaporto Elettronico (Machine Readable Travel Document - MRTD) sembra risolvere il problema dell'identità digitale.**
- **Nella sua struttura dati logica (LDS) gestisce i dati anagrafici, le informazioni biometriche e altro.**
- **MRTD risolve anche gli aspetti di scambio dati utilizzando meccanismi interoperabili a radio frequenza nel rispetto della privacy.**
- **Nello stesso chip possiamo installare dati per l'identificazione, l'autenticazione e la firma digitale e la tecnologia consente di far coesistere la radio frequenza (contactless) con le smart card tradizionali (contact).**

Lo stato dell'arte

- **Almeno quattro fornitori compatibili con le specifiche ISO/IEC 7816 "interpretate" per la CNS.**
- **19 certificatori accreditati, 2 in fase di accreditamento.**
- **Il Ministero dell'interno può diventare un certificatore accreditato.**
- **Più complesso è lo scenario per i servizi non associati all'identità in rete (sistemi di pagamento, trasporti, salute, ecc).**

Conclusioni

- **La nuova CIE costituisce il punto di riferimento per l'accesso ai servizi erogati in rete.**
- **I volumi in gioco sono notevoli. Nel primo anno a regime supereremo ampiamente il progetto europeo di riferimento che è il BELPIC (eID belga).**
- **Nel medio periodo la CIE dovrà contenere un dispositivo RFID.**
- **Potrebbero arrivare indicazioni (così dicono i piani di e-gov comunitari) dalla UE entro il 2010.**

Per maggiori informazioni

www.cnipa.gov.it

manca@cnipa.it