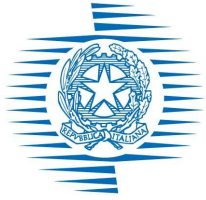


Le nuove tecnologie per la gestione dell'identità: l'utilizzo dei dati biometrici

Alessandro Alessandroni
Ufficio Osservatorio del mercato
Coordinatore CDC e GDL Biometria
alessandroni@cnipa.it

9 maggio 2006



relatori

Stefano Aprile

Responsabile Area Pareri e Cooperazione Applicativa Intersettoriale DGSIA Ministero della Giustizia

Giuseppe Fortunato

Componente Garante per la Protezione dei Dati Personali

Maurizio Leoni

Vice Capo Reparto del TEI Stato Maggiore della Difesa - Caserma De Cicco

Stefano Petecchia

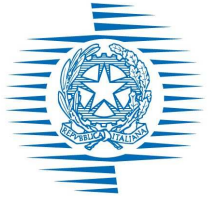
Dirigente Superiore Fisico della Polizia di Stato Ministero dell'Interno - Polizia Scientifica

Pietro Porcarelli

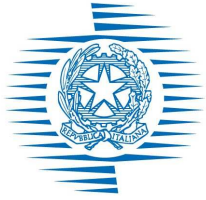
Project Manager N-VIS Direzione Generale Italiani all'estero e le Politiche Migratorie Ministero degli Affari Esteri

Gioacchino Carlo Trizzino

Vice Direttore Generale per gli Italiani all'estero e le Politiche Migratorie Ministero degli Affari Esteri



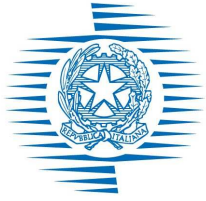
1 - Concetti base



Riconoscimento con tecnologie biometriche

Le tecnologie biometriche sono finalizzate all'identificazione o alla verifica automatica di identità degli individui attraverso la valutazione di caratteristiche fisiche o comportamentali.

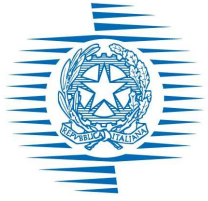
Consentono di basare il riconoscimento non su qualcosa che si possiede (token, smart card) o qualcosa che si conosce (password), ma su caratteristiche proprie dell'individuo



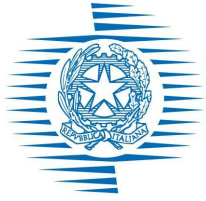
Caratteristiche biometriche più utilizzate

- Fisiche
 - Caratteristiche dell'iride (8.8%)
 - Geometria della mano (10.8%)
 - Struttura del volto (14%)
 - Impronte digitali (45.2%)
- Comportamentali
 - Voce (5.6%)
 - Apposizione della firma (2.3%)

2004 Biometric Technology Revenues (non AFIS)
International Biometric Group



2 - Le applicazioni nella PA



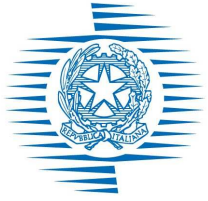
Campi d'applicazione

Applicazioni consolidate

- Identificazione criminale (AFIS)
- Controllo accesso (fisico) aree riservate

Applicazioni emergenti

- Accesso logico
- Abilitazione all'utilizzo di smart card (es.: per firma digitale)
- Videosorveglianza
- Identificazione civile: documenti di identità e di viaggio (passaporto, CIE, permesso soggiorno, visti....)



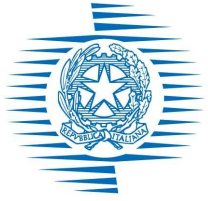
Applicazioni biometriche per la PA

Accesso fisico

Accesso fisico: procedura di accertamento della titolarità del soggetto all'ingresso in un locale, edificio, comprensorio o area

Applicazioni

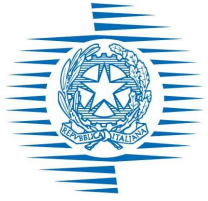
Controllo degli accessi e rilevazione di presenza in aree riservate con elevati livelli di sicurezza



Applicazioni biometriche per la PA

Accesso logico

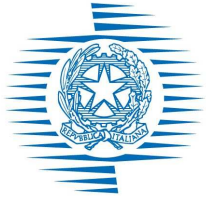
- **Accesso logico:** procedura di accertamento della titolarità del soggetto ad usufruire di una risorsa informatica
- Esempi di accesso logico sono
 - Accesso al proprio personal computer
 - Accesso ad un server
 - Accesso ad una rete



Applicazioni biometriche per la PA

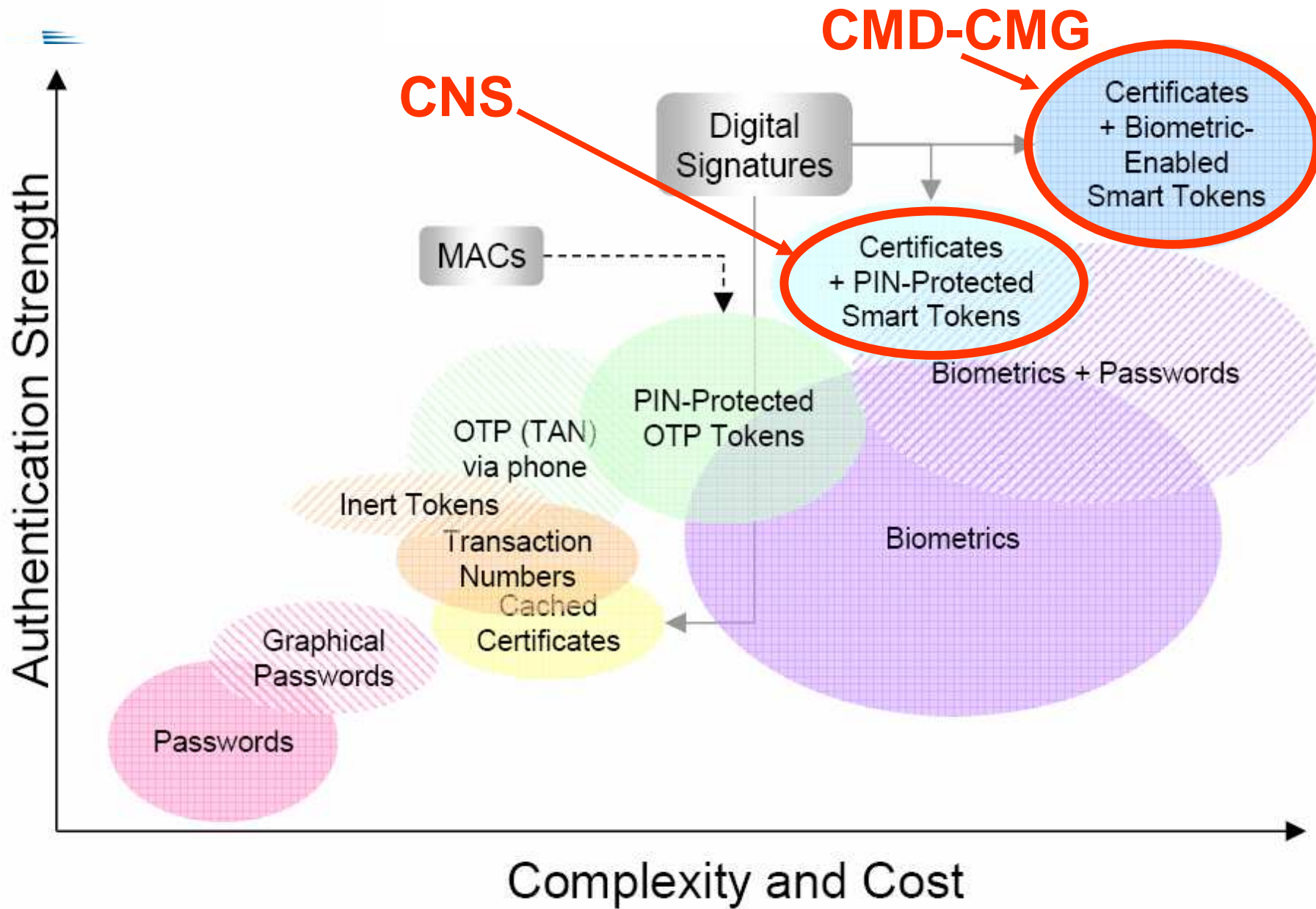
Uso con smart card

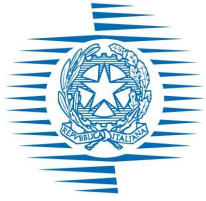
- Uso in aggiunta o in sostituzione del PIN
 - Accesso alle funzioni di firma digitale
 - Accesso a carte multiservizi (es. accesso fisico, logico e firma digitale)
 - “Carte del dipendente” e impiego nella CNS
- Uso nelle smart card per i nuovi documenti di viaggio e di identità



Le “carte multiservizi” dei dipendenti pubblici

- La Carta Multiservizi della Difesa (CMD)
 - Identificazione (a vista, elettronica, in rete)
 - Firma digitale
 - Dati sanitari
 - Dati di vestiario e matricolari
- La Carta Multiservizi della Giustizia (CMG)
 - Accesso logico
 - Firma digitale



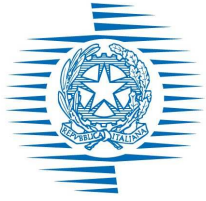


Il Passaporto Elettronico in Italia



Obiettivi

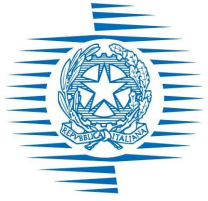
- Recepire la direttiva europea (standard ICAO)
- Mantenere l'esenzione dal Visto con gli USA
- Semplificare e rendere più efficaci i controlli utilizzando:
 - un sistema di emissione sicuro che elimini i rischi derivanti da falsificazione, contraffazione e furto.
 - identificatori biometrici per garantire l'identificazione certa del possessore
- Garantire la riservatezza delle informazioni utilizzando meccanismi di accesso ai dati innovative e sicure



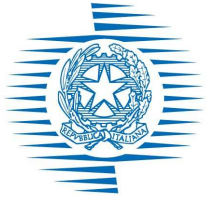
Il Permesso di Soggiorno Elettronico

Obiettivi

- Recepire la direttiva europea adottando uno strumento che rispetti gli standard indicati dall'UE
- Garantire la compatibilità con la CIE
- Semplificare e rendere più efficaci i controlli, utilizzando:
 - un sistema di emissione sicuro che elimini i rischi derivanti da falsificazione, contraffazione e furto
 - identificatori biometrici per garantire l'identificazione certa del possessore

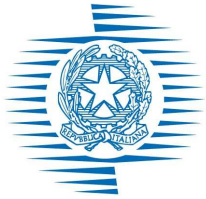


3 – Iniziative Cnipa e aspetti rilevanti



Iniziative CNIPA

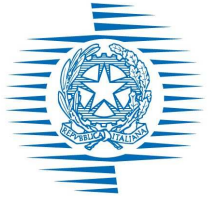
- Il **centro di competenza** sulla biometria (da novembre 2003)
 - Supporto diretto ai progetti della PA
 - Condivisione di *best practice*
 - **Laboratorio** per la verifica di metodologie di test
 - Osservatorio tecnologico e normativo
- Il **gruppo di lavoro** per la redazione di linee guida sulle tecnologie biometriche



Iniziative CNIPA

- Documenti prodotti
 - Linee guida per l'impiego delle tecnologie biometriche nella PA (2004) – Quaderni CNIPA n.9
 - Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni. Indicazioni operative (2005) - Quaderni CNIPA n.17
 - Atti del convegno Cnipa La biometria entra nell'e-government. Roma, 23.11.04 – (Quaderni CNIPA n.15)

www.cnipa.gov.it



aspetti rilevanti

- Aspetti tecnici
 - Accuratezza del riconoscimento (errori)
 - Sicurezza/vulnerabilità
 - Standard/interoperabilità
 - Test e certificazioni

- Aspetti non tecnici
 - Privacy
 - Aspetti medici (diretti, indiretti)
 - Accessibilità
 - Accettabilità