Smart Cards

Government programs overview

Gilles Lisimaque
Partner
ID Technology Partners, Inc.

GLisimaque@idtp.com
301-320-5146
The trends in Smart Cards

- Memory Size
- Computing Power
- Role based models
- Biometrics
- User Identification
- Privacy
- Privilege based models
- Logical Access Control
- GSM
- Physical Access Control
- Payment
- Convenience Contactless
- DRM Digital data
- Account identification
- Low cost

© 2007 All Rights Reserved
ID Technology Partners, Inc.
Smart Card: Bridge between Logical & Physical ID

- Strong online & off-line security
- Easy to use & convenient
- Portable & Personal
- Multi-Application
- Data in the card can be updated; privileges can be modified
- New applications can be programmed after the card is issued

Visual security
Electronic Certificates: Digital ID
Personal key pairs
PIN & Biometric data
Demographic data
Driver’s license (or other privilege)
Contactless: Physical access
Name and picture on the card as well as in the card
Market Forces & Privacy Concerns

- Convergence of physical and logical access control creates drastic changes in system interactions.
- Standardization of the identification tokens (smart card) simplifies interfaces and allows interoperability but may open some doors for hackers and create stronger incentives.
- The use of contactless technology for standard ID tokens has raised serious concerns for user’s privacy.
Challenges in Identification

• Contactless technology is
  – Fast
  – Convenient
  – Maintenance free

• Contactless communication is
  – Open to eavesdroppers if not protected
  – Open to data harvesting if requestor is not authenticated
  – A risk to privacy if not managed correctly
Security is not Privacy

- Contactless Financial cards broadcast the user account number to any terminal asking for it.
- Contactless Financial transaction security is managed by the back end system based on the merchant asking to be paid.
- User can be tracked without consent or knowledge as his/her PAN is provided by the card even when not taken out of the wallet.

*When asked for identification we do not show our identity document if we do not know who is asking for it.*

*Authentication of the authority of the requestor is crucial.*
Identity & Privilege Relationship

Identity Authority

- Link at enrollment and vetting
- Establish Trust
- Link at use
- Identity Assertion
- An ID card asserts the identity of the legitimate cardholder, but may not grant explicit privilege
- Attribute Certification
- Subject Verification

Application Authority

Transfer Trust

Person/Subject

© 2007 All Rights Reserved
ID Technology Partners, Inc.
Identity, Person, Claims & Privileges

Privilege derived from person’s identity

Identity Authority

Privilege based on attribute claim

Identity - Individual

Privileges pre-authorized for an individual

Privileges

Application Authority

US Customs

Access to beer

Access to Federal Buildings

Subject/Person

© 2007 All Rights Reserved
ID Technology Partners, Inc.
US Government programs (at least some of them …)

- DOD CAC card
- HSPD12 - FIPS 201 – PIV
- First responders (DHS card)
- e-Passport
- TWIC
- Registered Traveler
- U.S. Visit
- Real ID
- WHTI
Department of Defense
Common Access Card

- PKI functions
  - Encrypt/Decrypt
  - Digital Signature
  - Authentication
- E-Business
  - Defense Travel System
  - Army Portal
  - E-invoicing
- Support of Warfighter
  - Manifest/Tracking
  - Deployment readiness
  - Food Service
  - Property Accountability

© 2007 All Rights Reserved
ID Technology Partners, Inc.
DoD CAC Card

• The Card
  – JavaCard 2.1
  – Global platform
  – GSA Interoperability
  – PIV compliance
  – FIPS 140
  – 64K of memory
  – Multiple card suppliers
  – Has a Magnetic stripe
    and a 2D bar code

• Used by
  – US Navy
  – US Army
  – US Marine Corp
  – US Air force
  – US Coast Guard

• Decentralized issuance system relies on:
  – the DEERS database (Defense Enrollment Eligibility Reporting System with 23 million records)
  – The RAPIDS application and issuance stations (Real-Time Automated Personnel Identification System)
HSPD-12 PIV Card Requirements

A secure and reliable identification credential that:

• Is issued based on sound criteria for verifying an *individual employee’s identity*
• Is *strongly resistant to identity fraud*, tampering, counterfeiting, and terrorist exploitation
• Can be rapidly *authenticated electronically*
• Is issued only by providers whose reliability has been established by an official accreditation process.

Homeland Security Presidential Directive 12 (HSPD-12)
PIV Cards – ID in compliance with HSPD 12

- HSPD 12 and FIPS 201
- ID credential for all federal employees
- Replaces multiple credentials
- Machine verified
- Online and physical access control
**FIPS 201 - PIV Card Topology**

The PIV Card’s printed design requirements include:

- Designed to meet the objectives of *improved security and interoperability*
- Has a *common look* that is recognizable as a Federal identification card (e.g., consistent placement of mandatory printed components and technology)
- *Flexible design* to support individual department and agency requirements (i.e., allows for optional data)
e-Passport: How it works

1). An officer swipes the data page through a special reader to read two lines of characters at the bottom of the data page, providing key unique to the passport

2). Officer holds open passport over another reader, then checks his view of you in front of him, in the passport and on a screen

3). Data on the monitor verifies that passport was issued by legitimate authority

Slide courtesy of Montner & Associates
Transportation Worker Identification Credential

- Biometric credential for transportation workers
- Addresses vulnerabilities in national transport system
- Positively ties worker to credential and threat assessment system
Registered Traveler

- Specification created by an industry consortium formed in 2005 (RTIC) and accepted in mid 2006 by TSA-TTAC
- Members
  - 68 airports and airport authorities
  - 47 service providers
- Allows travelers whose identity has been verified by TSA to use a “fast lane” at the airport security checkpoints
- Privilege granted on biometric verification
U. S. Visit

- Fingerprint biometric ID program now in pilot at 12 U.S. airports and 2 seaports (no smart card)

- Biometric/biographic data compared to data gathered when visa issued

- Reduction in fraud, theft; protection against terrorist threats

Program using biometric verification only but no smart card
Congress passed the Real ID Act of 2005 after it was learned a 9/11 terrorist used a fake ID in a police stop before the tragedy.

Imposes strict verifications on breeder documents and expiration dates of state issued documents.

By 2008, state-issued drivers’ licenses will have to be a “real ID”.

Cards must meet minimum security requirements, including:
- Incorporation of specified data
- Use common, machine-readable technology
- Include anti-fraud security features

Smart cards are the ideal solution for Real ID but this may take a while in the United States.
Texas Medicaid Program

Background:

- Texas Legislature in 2003 mandates that Health and Human Service Commission “combat fraud, abuse, or waste in health and human services programs”

- Pilot biometric smart card ID program rolled out to 33,000 Medicaid recipients on Jan. 1, 2004

- Incorporates “match-on-card,” combining fingerprint template and the algorithm to use it

- Use of cards speeds up benefits processing while significantly reducing fraud and abuse

Due to success, Texas recently decided to roll out program to 2 million Medicare recipients statewide.

Slide courtesy of Montner & Associates
West Hemisphere Travel Initiative

- Program intended to simplify border crossing
- Allows to cross US borders (Canada and Mexico) with a simple “passport” Radio Frequency Tag (similar technology to product tags in stores)
- The identification number from the Radio Frequency Tag is picked up before reaching the border and allows the immigration officer to display from their data base the picture of the legitimate tag holder

Program using biometric verification only but no smart card
Thanks you for your attention

Gilles Lisimaque
Partner
ID Technology
Partners
GLisimaque@IDTP.com
301-320-5146
WWW.IDTP.COM

© 2007 All Rights Reserved
ID Technology Partners, Inc.