Privacy and Secure ID Systems: The Role of Smart Cards as a Privacy-Enabling Technology

Smart Card Alliance

Secure Personal ID Task Force

February 12, 2003

New Privacy White Paper (Medich)

- **Target audiences**
  - Enterprises and government agencies who are implementing secure ID systems
  - General public
  - Privacy advocacy organizations
- **Objectives**
  - Educate the target audiences on the definitions of privacy and security and on how smart cards can protect privacy and ensure security in an ID system
  - Describe the privacy-enabling advantages of using smart cards in ID systems vs. other ID technology
  - Recommend guidelines and practices that promote privacy in an ID system

Topics & Speakers (Medich)

- Introductions
  - *Cathy Medich, Task Force Chair & Consultant*
- Defining Privacy & Security
  - *Keith Saunders, VP Business Development, MasterCard International*
- Personal Identification vs. Personal Information: The Role of Smart Cards
  - *Neville Pattinson, Director Business Development & Technology, SchlumbergerSema*
- Practical Guidelines for Privacy Protection
  - *Jeff Katz, VP Marketing, Atmel*
- Smart Card ID System Architectures & Privacy
  - *Mansour Karimzadeh, President, Smart Commerce Inc.*
- Privacy-Enabled Smart Card Applications
  - *Colleen Kulhanek, VP Marketing, Datakey*
- Conclusions

Defining Privacy & Security
(Saunders)

- Privacy can be defined as: "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others"
- Privacy protection parameters
  - When, how and why information is collected from an individual
  - When, how and why collected information is accessed by authorized entities.
  - When, how and why information is destroyed
  - How information is protected from disclosure to, or modification by unauthorized parties, throughout its life cycle
  - How an individual can control whether information is collected and how it is used and retransmitted
  - How an individual's usage preferences are enforced

Defining Privacy & Security
(Saunders)

- Information security is a vital element in the design and implementation of a privacy-sensitive system.
- Security includes:
  - Confidentiality: How is information entered, transmitted and stored so that an unauthorized entity cannot access or alter the information?
  - Integrity: How accurate is the information being held? How is information protected from tampering? How does the system ensure that information is correct and updated?
  - Availability: Who can access the information and how does the system control access?

Privacy & Security in ID Systems: Choices (Saunders)

1) Use an existing ID as the de factor choice
2) Deliberately use another ID as a policy choice
3) Design an ID system correctly
   - Include the entire system design, from the enrollment process through the use and final destruction of the ID card
   - Include policies and procedures, as well as technology
   - Select an ID technology that has strong security mechanisms and that can enhance the privacy aspects of the ID system

Personal Identification: Two Uses
Pattinson)

- **Initial identification** – typically when an individual is enrolling in an ID system
  - Presentation of original credentials to establish identity
  - Search of existing databases to validate identity
    - For example: Driver's license records, resident alien or permanent resident databases, criminal records, undesirable/ wanted database
- **Identity verification** – validating that the individual presenting an ID card is the person who owns the credentials on the ID card

The Smart Card Privacy Role for Personal Identification

- **On-card match**, with all identity information and processing done on the smart ID card and only results sent to external devices
  - Support for anonymous go/no go
- **Cost-effective offline verification**
  - Small, secure, portable and low cost smart card readers at multiple locations where identity needs to be verified
- **Convenient identity verification**, with the smart card containing all information needed to confirm the cardholder's identity
  - For example, identity verification with biometrics at unstaffed locations

The Smart Card Role for Protecting Personal Information (Pattinson)

- **Personal firewall**, protecting the individual's data through both cardholder and information requestor authentication
- **Authenticated and authorized information access**, allowing the release of only the information required for the transaction
- **Strong ID card security**
  - Tamper-resistance
  - Extreme difficulty of duplicating or forging cards
- **Data security**, ensuring the privacy, authenticity and integrity of data encoded on the ID card
  - Encryption
  - Digital signatures
  - Prevention of information sharing among applications
- **System challenges**, authenticating the legitimacy of system components

Practical Guidelines for Privacy Protection (Katz)

- Business Practice Guidelines
- System Design Considerations and Guidelines

Smart Card Alliance

Practical Guidelines for Privacy Protection (Katz)

- **Business Practice Guidelines**
  - Comprehensive privacy policy, including information handling practices
  - Staff training
  - Employee background checks
  - Collection of minimum data required
  - No display of personal data
  - Restriction of staff access to individuals' personal information
  - Individual notification before information collection: why it is being collected, what it will be used for, who will be able to see it, how it will be protected, consequences of not providing information and rights of redress.

Practical Guidelines for Privacy Protection (Katz)

- **System Design Considerations and Guidelines**
  - Encrypt all personal information being stored on all media and destroy original unencrypted information after encryption
  - Transmit only encrypted information
  - Use template technology for biometrics
  - Remove any information captured by an ID card reader or at any intermediate transmission point when transaction is complete
  - Use individual data field checklists to specify access rights
  - Enable cardholders to authorize information extraction with password, PIN or biometric verification
  - Maximize the offline portion of transactions, performing on-card verification of identity where possible
  - Construct ID verification applications that extract only the information required for the transaction
  - Construct applications so that transaction records cannot be used as surveillance tools

Smart Card ID System Architectures and Privacy (Karimzadeh)

- **Token-based architecture**
  - One or more secure tokens or credentials are stored on the smart card, each relating to an application and identifying the card to a host system.
  - All user data is held on a host system.
  - When the card is presented, the tokens – along with a secondary authentication factor - indicate the presence of a valid credential.
  - Advantages
    - The identity of the cardholder is not divulged.
    - A secure channel can be established between the host and the card.

Smart Card ID System Architectures and Privacy (Karimzadeh)

- **On-card information-based architecture**
  - The smart card holds the cardholder personal information.
  - Cardholder data is protected on the card and only visible to the cardholder and other users with the appropriate level of authorization.
  - When the card is presented to a requesting device, all processing is done on the card, with only results sent to the external device.
    - Example: On-card biometric match
  - Advantage
    - After the card is issued, no cardholder information is revealed to any external parties at any time.

Smart Card Application Examples (Kulhanek)

- **GSM Mobile Phones**
  - Implementations maintain individual privacy while enabling mobile telephone service worldwide.
  - Very restricted network equipment translates a phone number to the IMSI and does not identify the subscriber.
  - All digital speech information is encrypted.
  - Only the issuer's billing system can identify the subscriber and entity who pays for the call.
  - Pre-paid GSM implementations create total anonymity for the subscriber.

Smart Card Application Examples (Kulhanek)

- **Western Governors Association Health Passport Project (HPP)**
  - HPP allows people to use smart cards to receive benefits and give up-to-date information to their health care providers.
  - Health Passport smart cards have been issued to 25,000 pregnant women, mothers and children eligible for a variety of health care programs in North Dakota, Wyoming and Nevada.
  - Privacy and security is implemented through a combination of the cardholder's PIN and the health care provider's PIN, allowing access only to the information authorized for that person.

Smart Card Alliance

Conclusions (Medich)

- Multiple organizations – both public and private – are implementing new or upgraded ID systems.
- Privacy and security must be **designed into** the ID system, including system policies, processes, architecture and technology.
- ID system designers should base the system design and architecture on practices and guidelines that promote a privacy-friendly design.
- Smart card technology delivers a unique set of features that both improve the ID system security and protect the individual's privacy.
- Smart cards help to protect privacy, providing a privacy-enhancing platform for ID systems.

For More Information

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
USA
Tel: 1-800-556-6828
Email: info@smartcardalliance.org
www.smartcardalliance.org

The Secure Personal ID Task Force has an in-person meeting, Feb. 12, from 5:15-6:15 PM. All Alliance members are welcome to attend.