# Smart Card Technology Roadmap for Secure ID Applications

Randy Vanderhoof

Executive Director

Smart Card Alliance

Agenda

- Primary standards & specifications:
  - ISO 7816, PCSC, X509
  - Open Card platforms (Javacard & Multos)
- Security standards and their challenges
  - FIPS 140, Common Criteria
- Specifications for interoperability
  - Global Platform
  - GSA specification
- Industry Specifications
  - GSM (presented in another EI201 Session)
  - EMV
- References for use with RFPs

NIST Workshop: July 9, 2003

Smart Card
Alliance
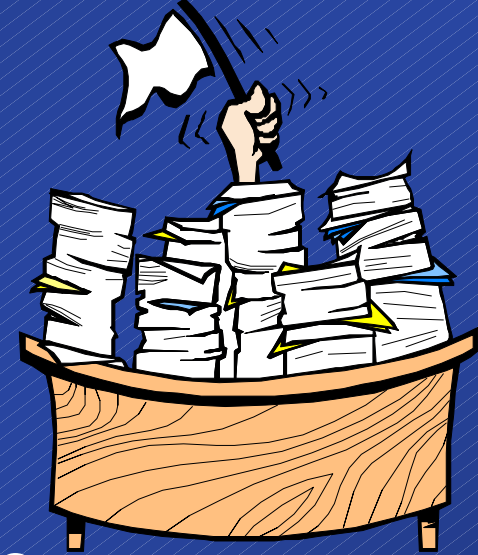
Where do standards apply?

ISO 7816	-Interface between the card & the terminal
PC/SC	-Common driver interface for all smart card readers connected under Windows
X509	-Digital Signature format & associated certificates
Open OS	-In the smart card only, allows a common application development platform for in-card applications
FIPS 140	-Tamper resistance of a cryptographic device
Common Criteria	-Threat evaluations and secure application protections
GSC specification	-Common way to find data files in cards & common application structures for US Government applications
Global Platform	-Card application management and issuance in the card as well as in the back-end
EMV	-Hardware specifications for smart cards and terminals
	-Multi application selection for smart cards
	-Credit & Debit: commands and related transaction flow

NIST Workshop: July 9, 2003

Smart Card
Alliance

Smart Cards for Logical Security

- PC/SC allows applications to be independent of the smart card reader (Windows drivers structure for hardware)

- Microsoft Crypto API allows applications to use crypto services of various crypto devices

- X.509 standard format for digital certificates

> Still no standard mechanism to launch an application when a given smart card is inserted in reader PC

NIST Workshop: July 9, 2003

Smart Card Alliance

New Yorker Magazine - 1993

"On the Internet, nobody knows you're a dog."

THIS is the problem!

Smart Card
Alliance

Issues for IT Security

- Moving beyond user name and password
- Managing internal and remote IT access
- Developing a systems view of physical and logical security
- Servicing beyond the network edge

Smart Card
Alliance

Smart Cards for Physical Security

- It is the "What We Own", or "Token" of ID Systems

- It is an intelligent, highly tamper resistant Token, allowing us to provide proof of who we are and the role we play

- It is a Highly Secure, portable credential platform providing
  - On-card security functions &
  - Intelligent interactions with reader

NIST Workshop: July 9, 2003

Smart Card Alliance

Smart Card Role in an ID System

- **A personal database**
  - Store and safeguard information on an individual basis
  - Local, portable storage of an individual's private information
- **A personal firewall**
  - Intelligent guardian of cardholder data – verifying that requestors are authorized to access information
  - Cardholder control of release of information
- **A personal terminal**
  - Validation of the authenticity and trustworthiness of card readers or terminals
  - Strong validation of cardholder as rightful owner of the ID card

NIST Workshop: July 9, 2003

Smart Card
Alliance

Personal ID Cards

- **Personal Identification Cards**
  - Specific rights, privileges, and responsibilities
  - Driver's license, membership card for an organization or club, credit card, border crossing document, badge for paid event, etc.

- **Secure Personal Identification Cards**
  - Extension to Personal Identification Cards
    - Includes best security technologies available – smart cards and biometrics
    - Certifies identification and authentication of <u>user</u> and granted <u>privileges</u>
    - Confirms authenticity of <u>credential</u> through use of security markings
  - Multiple applications on the same credential

ID systems that require the highest degree of security are combining smart card and biometric technologies.

NIST Workshop: July 9, 2003

Smart Card Alliance

Technology Availability Readers and Reader ICs

- Multiple providers of off the shelve reader products:
  - General purpose
  - Public transportation
  - Access Control
  - Retail industry

- Integrated ICs supporting:
  - ISO14443
  - ISO15693
  - ISO14443 and ISO15693

NIST Workshop: July 9, 2003

Smart Card Alliance

Contactless comparison chart

Features	14443	15693	Proximity
Standards	ISO 14443 ISO 7810	ISO 15693 ISO 7810	None (de facto)
Frequency	13.56 MHz	13.56 MHz	125 kHzFrequency
Read range	~10 centimeters (~3-4 inches)	~1 meter (~3.3 feet)	~1 meter (~3.3 feet)
Chip types supported	Memory Wired logic Microcontroller	Memory Wired logic	Memory
Encryption and authentication functions	MIFARE, DES/3DES, AES, RSA, ECC	Supplier specific, DES/3DES	Supplier specific
Memory capacity range	64 to 64K bytes	256 and 2K bytes	8 to 256 bytes
Read/write ability	Read/write	Read/write	Read only
Data transfer rate (Kb/sec)	Up to 106 (ISO) Up to 848 (available)	Up to 26.6	Up to 4
Anti-collision	Yes	Yes	Optional
Card-to-reader authentication	Challenge/Response	Challenge/Response	Password
Hybrid card capability	Yes	Yes	Yes
Contact interface support	Yes	No	No

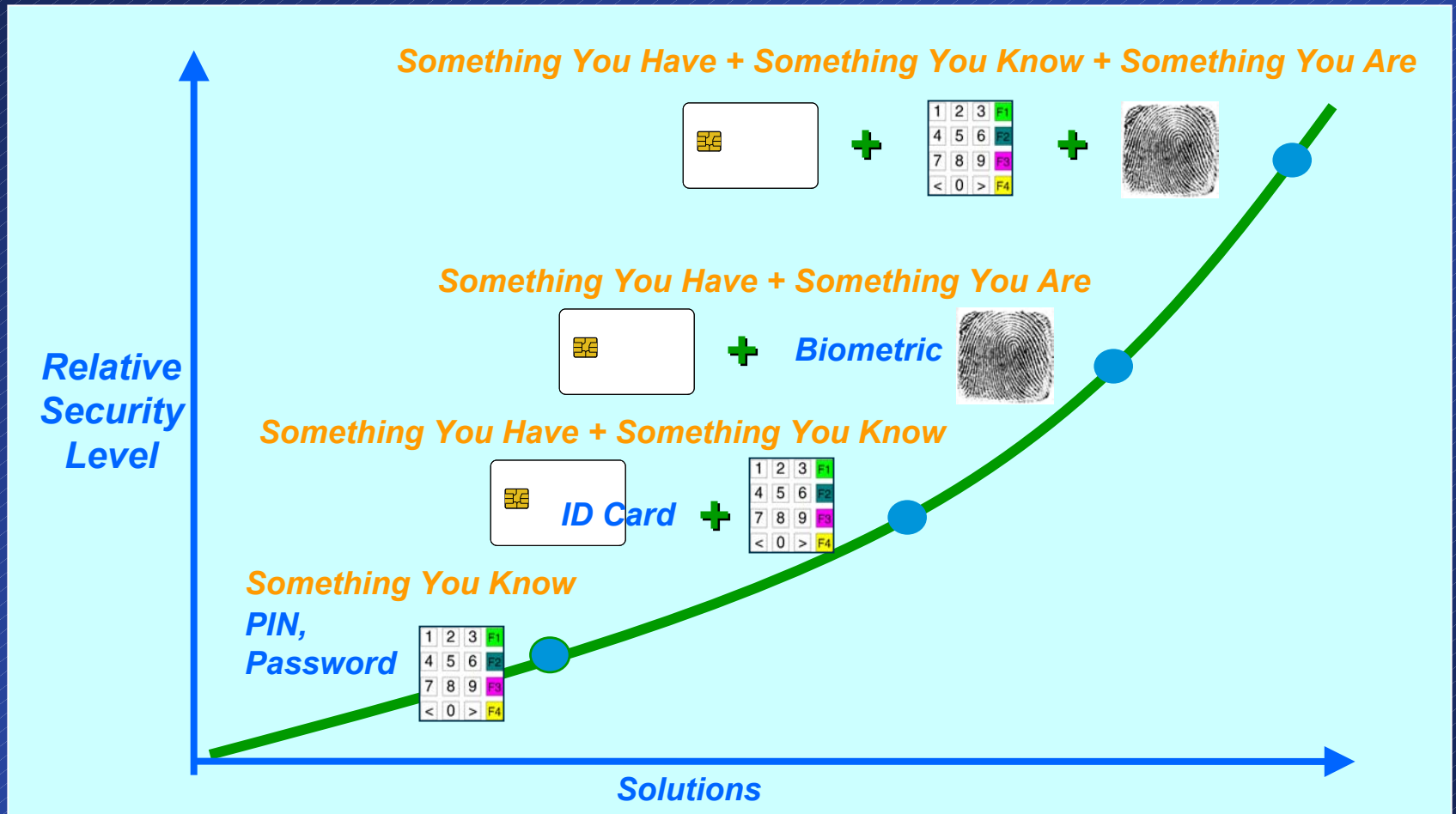*NIST Workshop: July 9, 2003*

Smart Card Alliance

Challenges Facing the Secure Identification Industry?

- When is visual authentication <u>not</u> enough?

- The maturity of machine-readable technology with more standards-based choices at lower costs

- The recognized need that exists to bind the identity of the cardholder to the card – how do you do it?

- How do you increase security without sacrificing speed and convenience?

- Managing <u>scalable</u> ID solutions that need <u>multiple</u> <u>t</u>echnologies with <u>security and privacy</u> from <u>point of issuance</u> to the <u>network edge</u>
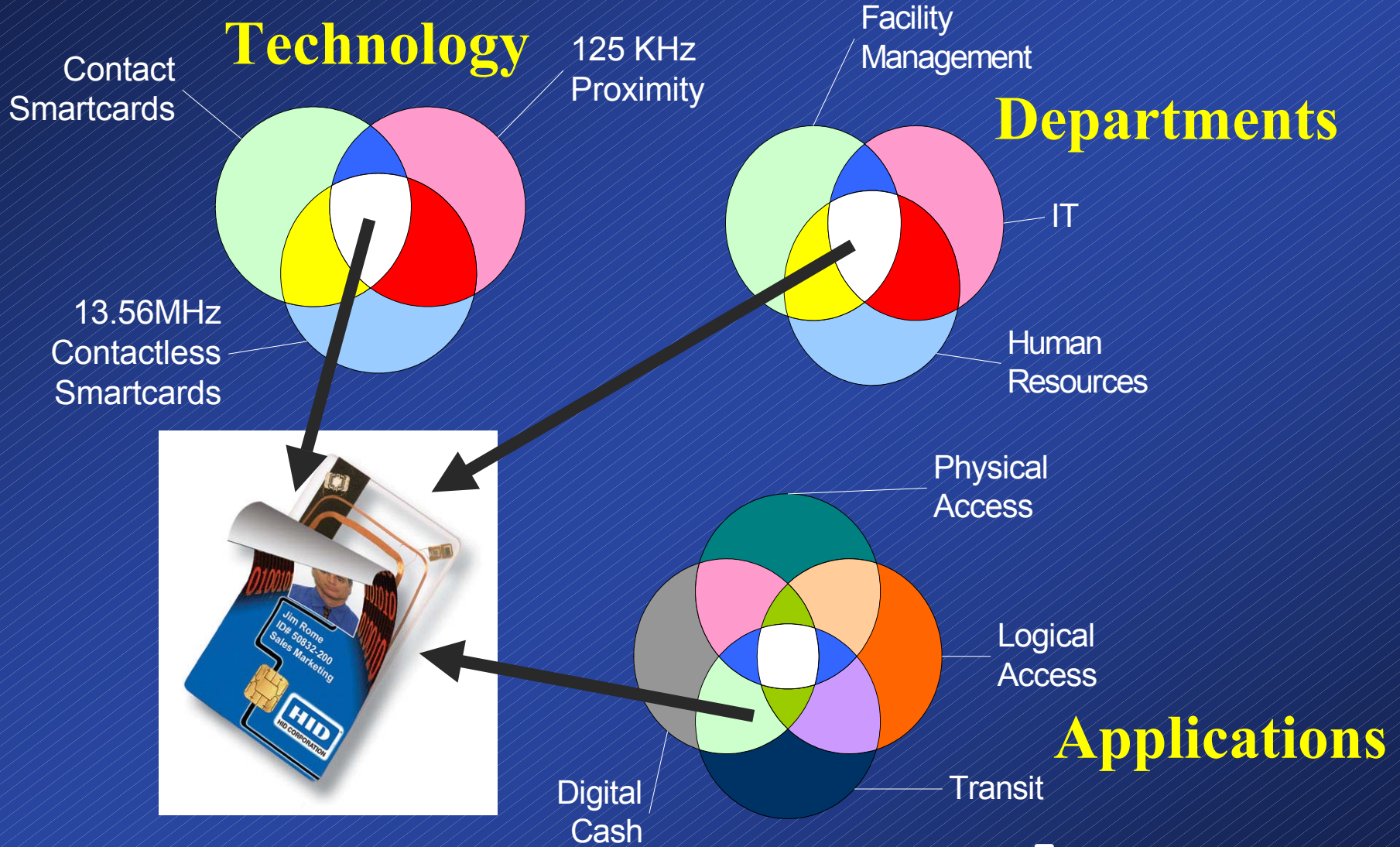
...demands intelligent, secure, portable, rewritable platform

NIST Workshop: July 9, 2003

Smart Card
Alliance

Enhanced Security Design Options

Relative Security Level

Something You Have + Something You Know + Something You Are

Something You Have + Something You Are

Biometric

Something You Have + Something You Know

ID Card

Something You Know

PIN, Password

Solutions

NIST Workshop: July 9, 2003

Smart Card Alliance

Smart Badge Convergence

Technology

Contact Smartcards

125 KHz Proximity

13.56MHz Contactless Smartcards

Departments

Facility Management

IT

Human Resources

Applications

Physical Access

Logical Access

Transit

Digital Cash

Courtesy of Assa Abloy

NIST Workshop: July 9, 2003

Smart Card Alliance

Conclusion:
What about Interoperability ?

- There are different aspects to interoperability
- Solutions available
  - Development in the cards have been simplified thanks to Java
  - Card edge interface and data formats are clarified with GSC-IS
  - Multi application selection is possible for cards and applications compatible with the Open Platform mechanism
  - Multi application card management with Global Platform
- Issues still pending
  - Management of biometrics templates and storage options
  - Agreement on policy issues for cross-certification of credentials

Smart Card
Alliance