FIPS 201
Smart Card Industry Perspectives

Craig Diffie
Director, Field Marketing – Government
Axalto, North America

axalto

Homeland Security Presidential Directive -12

- Policy for a Common ID Standard for Federal Employees & Contractors
- Mandatory Gov't-wide standard for secure & reliable forms of ID
  - Issued based on sound criteria for verifying individual employee's identity
  - Strongly resistant to ID fraud, tampering, counterfeiting, and terrorist exploitation
  - Can be rapidly authenticated electronically
  - Issued only by providers whose reliability has been established by an official accreditation process
- Used in gaining physical access to facilities & logical access to information systems
- Signed 27 Aug. Six months to promulgate the standard.

What does this mean to the Smart Card Industry?

Are we better off today than we were 4 years ago?

- GAO Report – September 2004: Fed Agencies Continue to Invest in Smart Card Technology
- DoD CAC Program Implementation
- TWIC Prototype – Phase 3
- Aggregate Buy
- GSC-IS v2.1 moving to ISO/IEC 24727
- FICC/DCIS
- Electronic Passport/E-Visa/USVISIT
- Federal PACS Guidance
- USB (ISO/IEC 7816-12)

- 9/11 Commission Report/ID Theft/Phishing

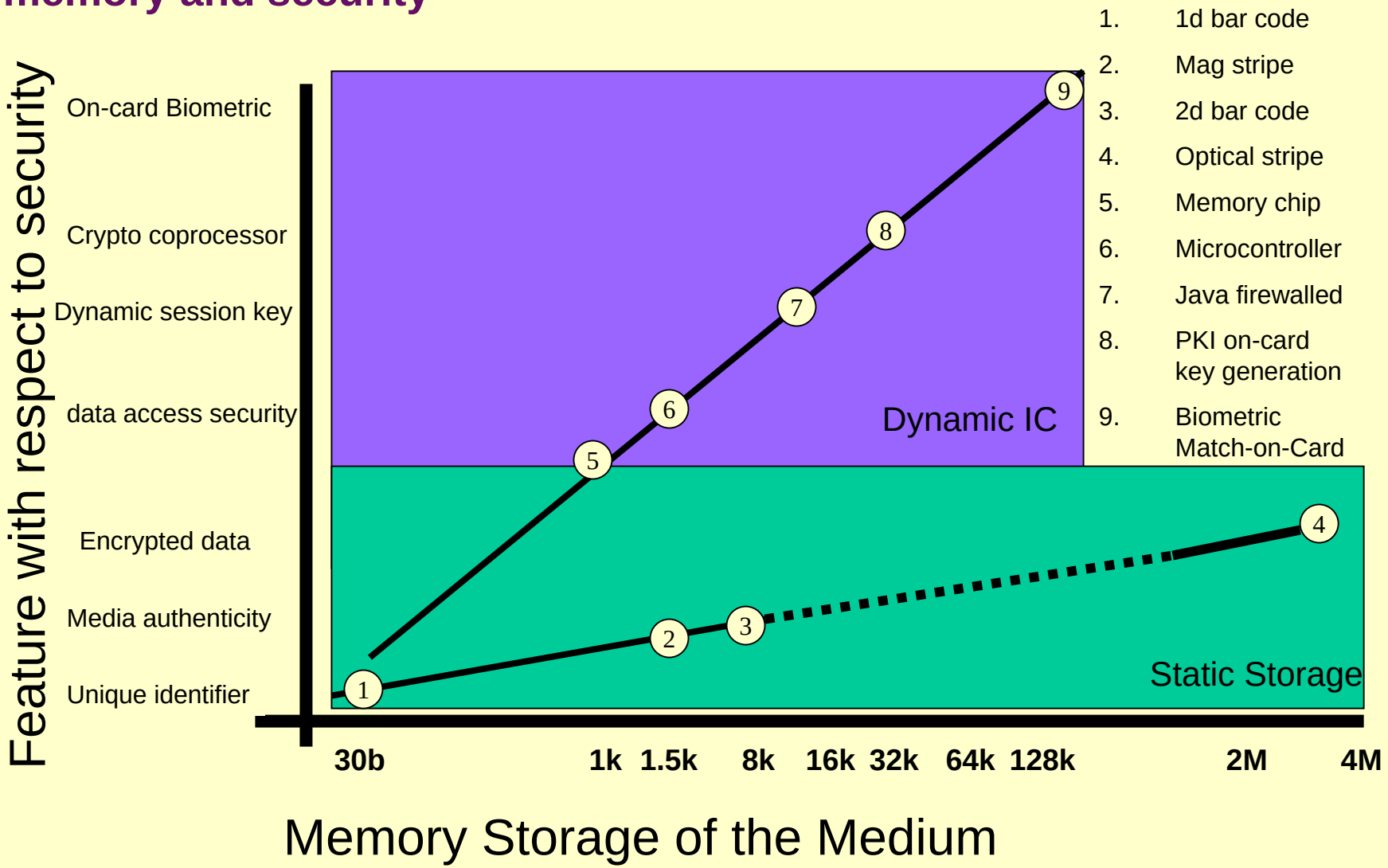
Contents

- Smart ID Card Technology
- Identification
- Biometrics
- Security
- Privacy

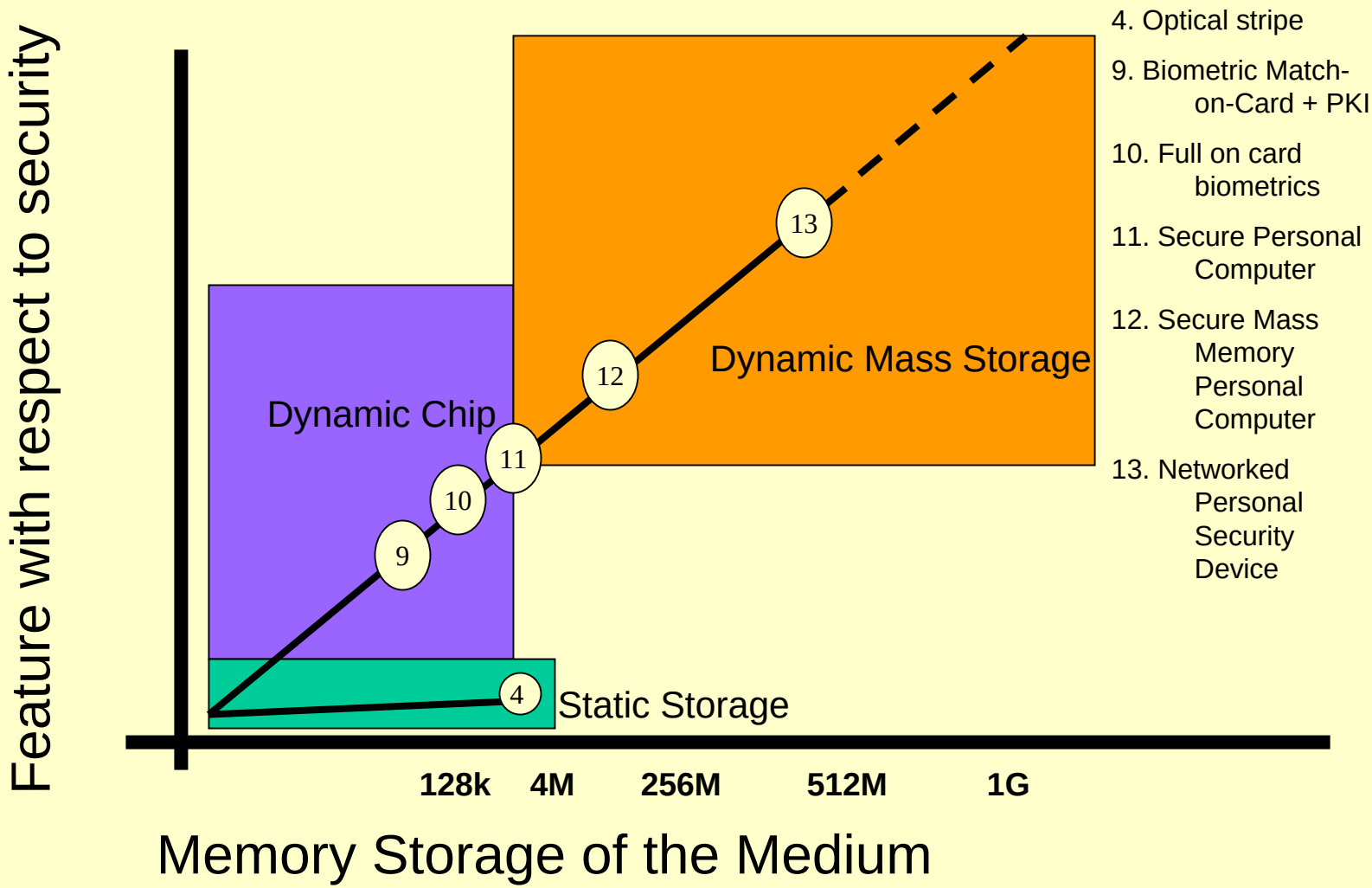
Smart ID Card Technology

Where the technology is going…

Comparison of Dynamic verse Static technology with relation to memory and security



Future Projections



Identification

Who You Are –
Who Are You?

Establishing Identity @ Application

- Policy of Credential system may require such things as:
- Presenting credentials
- Background checks
  - Criminal
  - Financial
  - Watch-list / Terrorist
- As good as…enrollment credential?
  - Birth Certificate, Passport
  - Driver's License
  - Utility Bill
  - 3rd Party attestation
- Multi-factor (scored) analysis.
- Approved/Rejected
  - Appeal?

Enrollment

- Policy of Issuer:
  - Capture of biographical data
    - Name, Address, age, affiliation etc..
  - Capture of biometric data
    - Facial photo, finger print(s), Iris scan, palm scan etc
  - Linkage of biographical and biometric data to identity within credentialing system
    - Name, ID number, card ID number, etc
  - Publishing of (some) data to operational ID system

Identity Authentication

- Once you are enrolled it’s all about authentication, not identification
- Verify and authenticate according to the enrolled credential
- On line – with reference to Issuer
- Off line – local security agent on behalf of Issuer

Biometrics

Something You Are –

And can prove

Biometric Identity Verification

With ID Cards

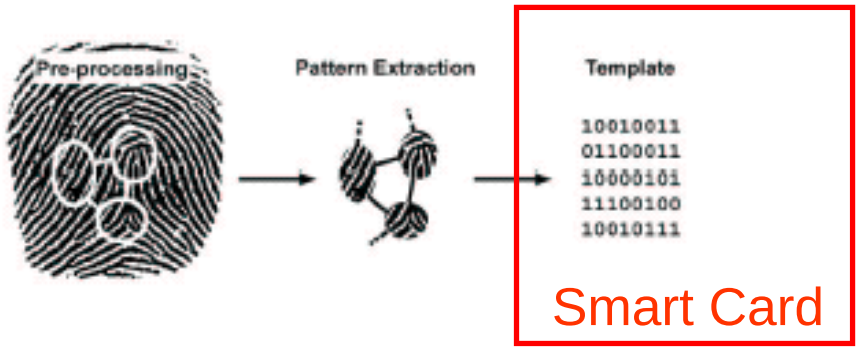
- Used to establish card holder is same person who initially enrolled
- Can be
  - On line to central Database for match
    - Card as ID number
  - Off line – match locally
    - Card serves biometric or template to local device
  - Off line – match-on-card
    - Card compares received biometric or template

Smart Card's Biometric role

- Using the secure chip allows the card to
  - Authenticate external equipment
  - Authenticate card holder with PIN &/or biometrics
    - Securely serve raw biometric data
    - Securely serve biometric templates
    - Compute match-on-card using templates
  - Perform strong one-to-one Match
- The Smart Card is the Issuer's security agent in the hands of the user.

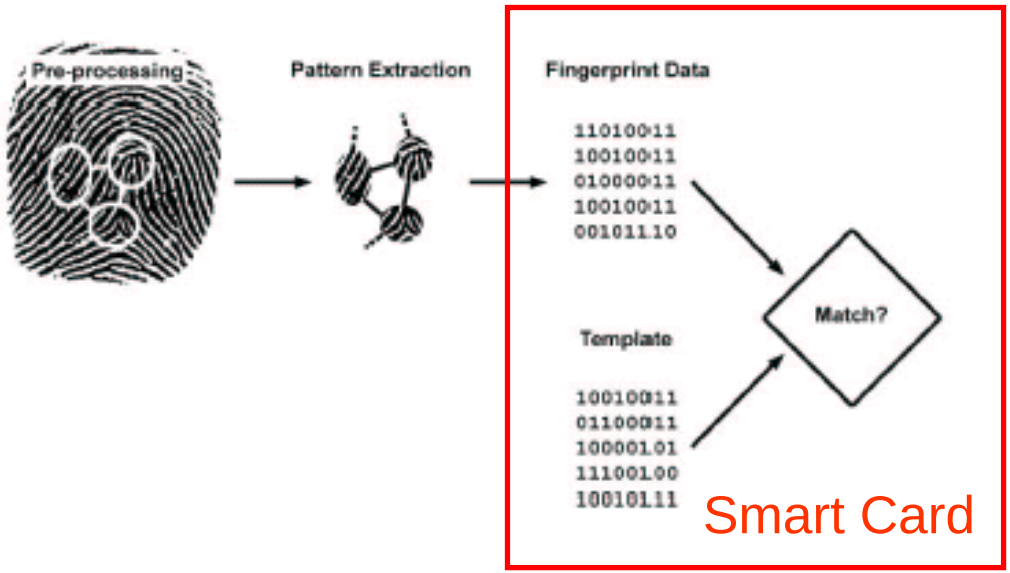
Match On Card

Enrollment



Enrollment Template Stored on Card

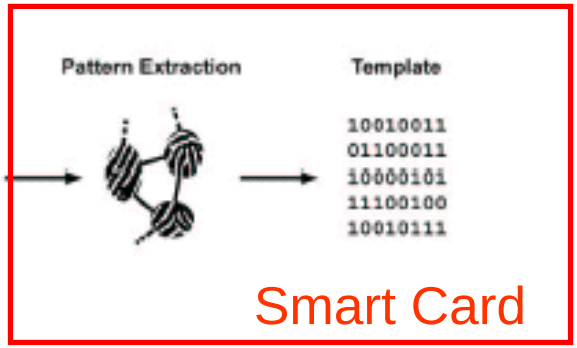
Verification



Template Comparison with Match on Card

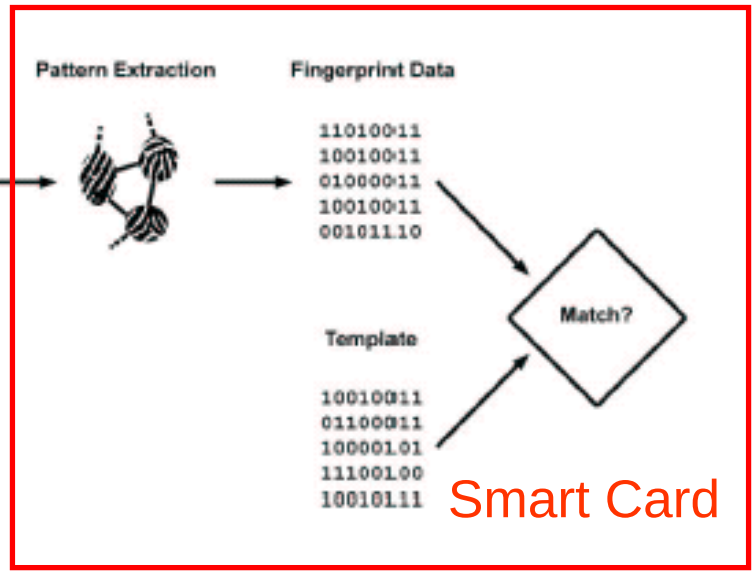
Full Biometric on Card match?

Enrollment



Extraction of Template and Storage on Card

Verification



Template Extraction and Comparison Match On card

Biometrically Agnostic

- Biometric vendor neutrality in any ID System
  - Cards deal with specifics of Biometrics
- Multiple Biometric technologies can co-reside on cards
- Cards deal with raw Biometric images from sensors
- Pre-processing not required on client/host
- Less opportunity to attack image - Privacy benefit

Security

Protecting assets –

Use it correctly

Appropriate Security

- Use security that is commensurate with the value of the assets you are trying to protect.
- Define a Security Policy that can be implemented and verified.
- Determine the role of the Smart Card for enforcing the Security Policy

Case Study : E-Passport data availability

- ICAO mandate only Digital signature of data page information
- Data Page information available as “free read”
- Non-obvious extraction/collection possible
- Open to skimming
- Open to substitution
- No chain of trust with chip/document/credential/holder

- Who is going to be **red faced** & or get a **black eye**?

Refer to Axalto White Paper:

“**Securing and Enhancing the Privacy of the E-Passport with Contactless Electronic Chips.” 24 May 2004.**

Selecting appropriate levels

- It is essential that when an Identity system using smart card technology is developed, it
  - utilizes appropriate Smart ID Card security features to protect the assets
  - respects and enforces the Privacy Policy
  - uses best practices for Biometrics
  - Provides a major part of the credential's **Chain of Trust**

To provide authenticated identity

How does a smart card contribute to the chain of trust?

Phishing Countermeasures

Announcing… “The end of username/password account access.”

- Smart ID Cards **will** provide internet account security
  - By the connection either physically or logically the smart ID card strongly authenticates the device with the user and the device with the service.
  - Local Security Agent or Identity Proxy
  - Kills Phishing, social engineering and brute force attacks

Internet Server

Security & Identity Proxy

User

Privacy

Disclosing only what needs to be disclosed -
Using only what is needed

Smart Cards are PETs

- Smart ID Cards are a **Privacy Enabling Technology**
- Ensure you perform a **Privacy Impact Assessment**
- Define a **Privacy Policy**
- Determine the role of the Smart Card for enforcing the Privacy Policy.
- Educate the population regarding the Privacy Policy, data collection & it's usage
- Don't allow the Smart ID Card to become the focus of Privacy based attacks and accusations

HSPD-12

Promulgate a Common ID Standard for Federal Employees and Contractors

Challenges to the SC Manufacturer

- New Features – acceptance then qualification
- Very little in-stock inventory
- Production Run Scheduling
- Sequencing with Production Runs of Competing Products
- Supplier and stocking issues
- Yield

Research & Development Processes

- **Internal Development** — **6-18 months**
- **Product Qualifications** — **1-2 months**
- **IV&V Labs** — **1-2 months**
- **FIPS Validation** — **5-14 months**
  - **Card**
  - **Card & Applet**
- **Common Criteria** — **12 months**
  - **Profile**
  - **Process**
  - **Entire Supporting Security Environment**

Making FIPS 201 a Win-Win Standard

- **Build on the work that has already been accomplished**
  - **GSC-IS v2.1**
  - **IAB**
  - **Successful program implementations**
- **Seek guidance from industry**
- **Provide unambiguous guidance without being prescriptive**
- **Narrow feature set choices where possible**
- **Cut away support for legacy systems where possible**
- **Don’t try to be everything for everybody**
- **No radical course changes**
- **Leave room for technology refresh**

Conclusion

Smart ID Cards are getting more powerful with more storage capacity and attract more applications.

The need for Biometric authentication of Users is increasing.

The Security of the credential is paramount once issued.

The Privacy of the information must be maintained.

Summary

“Advances in Smart Card Identity”

- Comprehensive Privacy Practices
- Appropriate use of Security features
- Implementing Biometric best practices
- Smart ID Cards enable trusted identity authentication

Smart ID Cards will/have become a trusted Identity Proxy

= An Authenticated Future

Thank You

Craig Diffie
cdiffie@axalto.com
703.371.3231 (mob)