

# **Biometric Match-On-Card NIST R&D Roadmap**

**William I. MacGregor**

**National Institute of Standards and Technology**

**IAB Meeting, 5Mar2009**

*NIST builds on the experience and unmet needs of pioneers like the Department of State*

## Desired Changes to PIV

- Improved Usability
  - Activates PIV Card as a PIN Substitute
- Improved Security & Privacy
  - No Release of Biometric Data from Card
  - This implies **Match-On-Card** (MOC)
- Is there a contactless biometric requirement?
  - Could motivate encryption and digsig
  - Not a DoS requirement

# Most Requirements Don't Change

- Backward Compatibility
  - With deployed PIV Cards and systems
- Authentication Mechanism Model
  - Choices for multi-factor authentication
- FIPS 140-2 Level 2 Conformance
  - Sets operator authentication strength
- Metrics & Testing for Biometric Components
  - *Ongoing MINEX* program, extensions

# NIST Process

- R&D activity: NISTIRs, papers & presentations
- Best Practice Guidelines: Special Publications
- Standards: ANSI & ISO, and rarely...
  - Federal Information Processing Standards (FIPS)

*All of these documents are published.*

*FIPS and SP have public comment periods.*

# NIST R&D Activity to Date

- MINEX II program in Information Access Division
  - NISTIR 7485 *Performance of Fingerprint Match-on-Card Algorithms Evaluation Plan* (Aug 2007)
  - NISTIR 7477 *Performance of Fingerprint Match-on-Card Algorithms Phase II Report* (Feb 2008)
- Feasibility Study in Computer Security Division
  - NISTIR 7452 *Secure Biometric Match-on-Card Feasibility Report* (Nov 2007)
- Cooperation with *ISO/IEC 24787 Information technology—Identification cards—On-Card biometric comparison (JTC1/ SC 17/WG 11)*
  - *Comments from ANSI/INCITS B10 and M1*
  - *Liaison with ANSI/INCITS B10.12*

# Way Forward

- FY09 Revisit and formalize requirements
- FY09 Recommend an implementation approach
  - Consider ISO/IEC 24787 mapping
  - Propose any modifications needed in
    - SP 800-73
    - SP 800-76
    - FIPS 201
- Enable a direction based on the merits

# Thanks for listening!

William I. MacGregor & Tanya Brewer  
IDMS R&D Co-Leads  
(301) 975-8721 & (301) 975-4534

<http://csrc.nist.gov>