

# Interagency Advisory Board

*Meeting Agenda, June 23, 2009*

1. **Opening Remarks**
2. **The Four Bridges Forum**
  - a) *Tim Pinegar, FCBA*
  - b) *Jeff Nigrini, Certipath*
  - c) *Gary Secrest, SAFE-BioPharma*
  - d) *Scott Rea, HEBCA*

-----BREAK-----

3. **PIV Standards Update (Bill MacGregor, NIST)**
4. **Federally Interoperable Credentialing in Illinois (*Dennis Glavin, CGN PM*)**
5. **Closing Remarks (*Tim Baldrige, NASA*)**

# **NIST PIV Status Update**

**William I. MacGregor**

**National Institute of Standards and Technology**

**IAB Meeting, 23Jun2009**

# Overview

- ***DONE*** SP 800-85A-1 & TestRunner to labs
- SP 800-73-3 Focused Update
- “Use of ISO/IEC 24727” (NISTIR title)
- PLAID Workshop at NIST
- PLAID Experimental Implementation
- PIV Card Trust Validation Refimp
- Biometric Match-On-Card
- BIO Authentication Demonstration

# SP 800-73-3 Focused Update

*Public Comment Draft in preparation, deltas:*

- Definition of UUID consistent with NFI spec
  - For Non-Federal cards used with PIV System
  - Not a proposal to change PIV Cards
- KMK: use with ECDH and RSA transport
  - Fully defined
- KMK: on-card retention of historical keys
  - Allow with certs on- or off-card

# “Use of ISO/IEC 24727”

*NISTIR in preparation*

- Based on lab demo of ISO/IEC 24727 middleware accessing a PIV Card
- Document describes the demo structure and purpose
- If possible, we will package and publish the demo source code
- Windows and Linux platforms, PC/SC below and CAPI or PKCS #11 above

# Protocol for Lightweight Authentication of Identity (PLAID)

- Workshop to be hosted by Australian Gov. at NIST, 13-15 July 2009
- Two days hands-on with PLAID, one day of talks on motivation, design, applications
- See [http://csrc.nist.gov/news\\_events/plaid-workshop/](http://csrc.nist.gov/news_events/plaid-workshop/)
- Registration required, limited space basis

# PLAID Experimental Implementation

- Attempt to use PLAID authentication for a secure messaging tunnel to a PIV Card
- Being built on PIV development card

# Thanks for listening!

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

<http://csrc.nist.gov>