Secure Biometrics Match-on-Card Workshop

May 24, 2007

Workshop Goals

- Determine the technical feasibility of person authentication using a conceptual approach, “Secure Biometric Match-On-Card.”
- Two major elements:
  - Functionality & Performance AM
  - Biometric Fidelity & Accuracy PM
- Discussion:
  - Identify issues and concerns
  - Answer questions about the process
  - List dependencies and impacts

AM Agenda

- Goals – MacGregor
- Business Process – Mehta
- Test Methodology – Dang
- Next Steps – Lee

Goals – Functionality and Performance

- Conceptual requirements in white paper
- Core requirements
  - Public domain sBMOC card edge
  - MOC capability using standard templates
  - Firmware builds on PIV card stock
  - Contact and contactless operation
  - Meets security objectives set by white paper
- Authentication transaction < 2.5 seconds

Goals – Detailed Requirements

- MOC meets accuracy & fidelity requirements
- Test with RSA 1024 and 2048
- X.509v3 certificate
- Symmetric encryption (if used) chosen from 2TDEA, 3TDEA, AES 256
- ANSI or ISO minutiae templates
- 2.5 sec criterion applies to successful match
- ISO/IEC 7816 & 14443 communication
- No essential technical conflicts with PIV

Goals – Security Objectives

- SO1: communication of biometric data shall occur only over a trusted channel that is not susceptible to eavesdropping attacks in the reader-to-card direction, nor spoofing or replay attacks in the card-to-reader direction
- SO2: communication of biometric data between the PIV Card and smart card reader shall occur only after the cardholder has indicated the reader is legitimate
- SO3: communication of biometric data from the PIV Card to the reader shall occur only after the cardholder has entered their PIN
- SO4: the approach should achieve the preceding security objectives without reader-to-smart-card authentication or associated key management infrastructure.

Goals – Non-Requirements

- Strict adherence to APDU's in white paper
- Card-to-reader session before finger scan
- Integration with PIV card-app or keys

Business Process – Participation

- This is a public discussion.
- This forum is of interest to vendors developing Biometric Match-on-Card products.
- NIST can accept non-proprietary products / information through this public forum.
- If proprietary material needs to be shared, NIST can enter an agreement with the vendor in the following two ways:
  - Use the existing CRADA agreement and modify the statement of work.
  - Create a new CRADA agreement.

Business Process – Submissions

- Smart cards with sBMOC firmware
- Documentation describing
  - Personalization method
  - sBMOC card edge
- Tools or services
  - For PKI personalization
  - For biometric personalization

Business Process – Expectations

- Vendor Expectations:
  - Provide troubleshooting support needed to integrate the product with the test harness.
  - Provide loaner equipment for about three months.
- NIST Expectations:
  - Develop the test harness.
  - Incorporate protocols necessary to carry out the feasibility demonstration.
  - Perform security review of the protocol.
  - Produce the analysis report.

Business Process – Report Results

- The report will NOT include:
  - any vendor identifying information.
  - Results of security analysis of each configuration.
- Benchmark performance measurements will be documented.
  - # of successful submissions
  - transaction times
  - constructive findings
- Performance measurement of the interface to the card and accuracy of Biometric match will be reported.
- Test methodology and configuration details will be included.

Business Process – Possible Schedule*

- t+0 Invitation to participate in FR
- t+30 All “intentions” received
- t+60 All “submissions” received
- t+90 All tests complete

*Pending decisions on structure of participation.

Test Methodology – Objectives

- Obtain timing metrics to perform Biometric Match-On-Card (BMOC) over a contactless interface
- Observe differences in transaction times for matching and non-matching biometric templates
- Observe effects of minutia count on transaction times
- Observe effects of PKI key strength on transaction times

Test Methodology – Approach

- Develop test fixture to measure transaction times per the guidelines set forth in NIST "Test Plan for Secure Biometrics Match-on-Card (sBMOC) Feasibility Study"
- Measure card-edge transaction times to perform BMOC
- Measure total host processing time
  - Time from when BMOC card application is selected up to the time when the BMOC verification command returns a response
  - Includes time to perform data encryption/verification on the host side

Test Methodology – Approach (continued…)

- Validate card-edge time metrics using protocol analyzer. Other validation methods may be used also (e.g., card reader firmware that provides timestamps on the card-edge).
- Test initially with RSA 1024. RSA 2048 will be tested if card supports it.

Test Methodology – Configuration

- Include multiple card readers – test cases will be repeated with each card reader
- Include multiple cards
- Include matching and non-matching biometric templates
- Include biometric templates with varying minutia counts
- X.509 PKI certificate loaded on cards will differ only in public key to minimize variance

Test Methodology – Test Case #1

- Configuration
  - 1 matching sample template with minutia count of A
  - 1 non-matching sample template with minutia count of A
  - RSA 1024 public/private key pair

- Goals
  - Observe effects of matching/non-matching biometric templates on transaction times
  - Observe effects of minutia count A on transaction times
  - Observe effects of PKI key strength on transaction times

Test Methodology – Test Case #2

- Configuration
  - 1 matching sample template with minutia count of B
  - 1 non-matching sample template with minutia count of B
  - RSA 1024 public/private key pair

- Goals
  - Observe effects of matching/non-matching biometric templates on transaction times
  - Observe effects of minutia count B on transaction times
  - Observe effects of PKI key strength on transaction times

Test Methodology – Test Case #3

- Configuration
  - 1 matching sample template with minutia count of C
  - 1 non-matching sample template with minutia count of C
  - RSA 1024 public/private key pair

- Goals
  - Observe effects of matching/non-matching biometric templates on transaction times
  - Observe effects of minutia count C on transaction times
  - Observe effects of PKI key strength on transaction times

Test Methodology – Test Case #4

- Configuration
  - 1 matching sample template with minutia count of A
  - 1 non-matching sample template with minutia count of A
  - RSA 1024 public/private key pair
  - Protocol analyzer
- Goals
  - Validate time metrics obtained by test fixture

Test Methodology – Test Case #5 (Optional)

- Configuration
  - 1 matching sample template with minutia count of A
  - 1 non-matching sample template with minutia count of A
  - RSA 1024 public/private key pair
  - Card reader firmware that implements timestamp information on card-edge

- Goals
  - Validate time metrics obtained by test fixture

Test Methodology – Test Case #6 (Optional)

- Configuration
  - 1 matching sample template with minutia count of A
  - 1 non-matching sample template with minutia count of A
  - RSA 2048 public/private key pair

- Goals
  - Observe effects of PKI key strength on transaction times

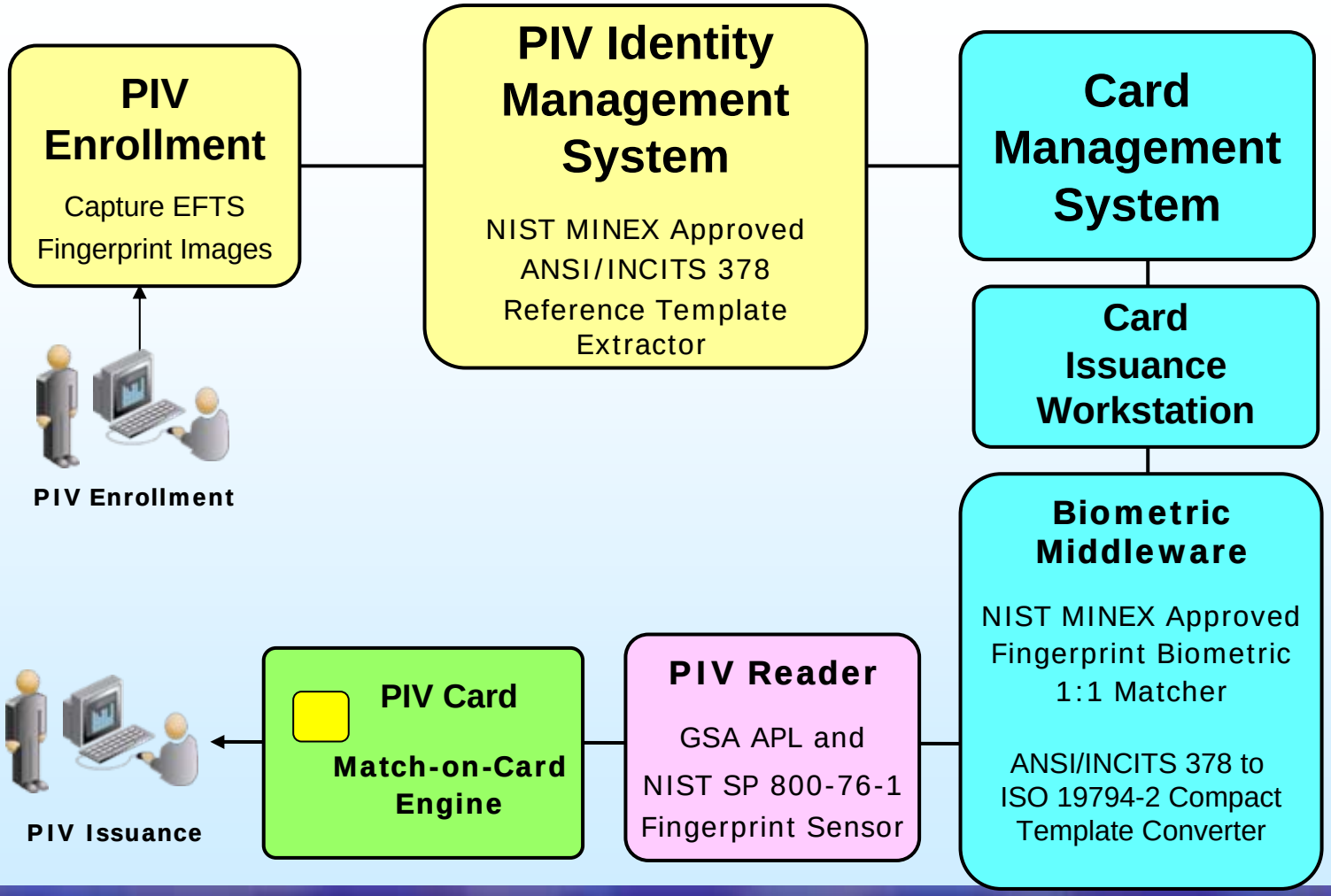
Next Steps

- Extraction of Reference Templates via MINEX Approved Algorithms in PIV-I Work Flow
- Personalization of BMOC PIV Card via COTS CMS
- BMOC Enabled Client Middleware
- BMOC and Secure Messaging Enabled Physical Access Reader
- BMOC Enabled Logical Access Reader
- Multiple Sources of BMOC PIV Cards, Readers and Client Middleware

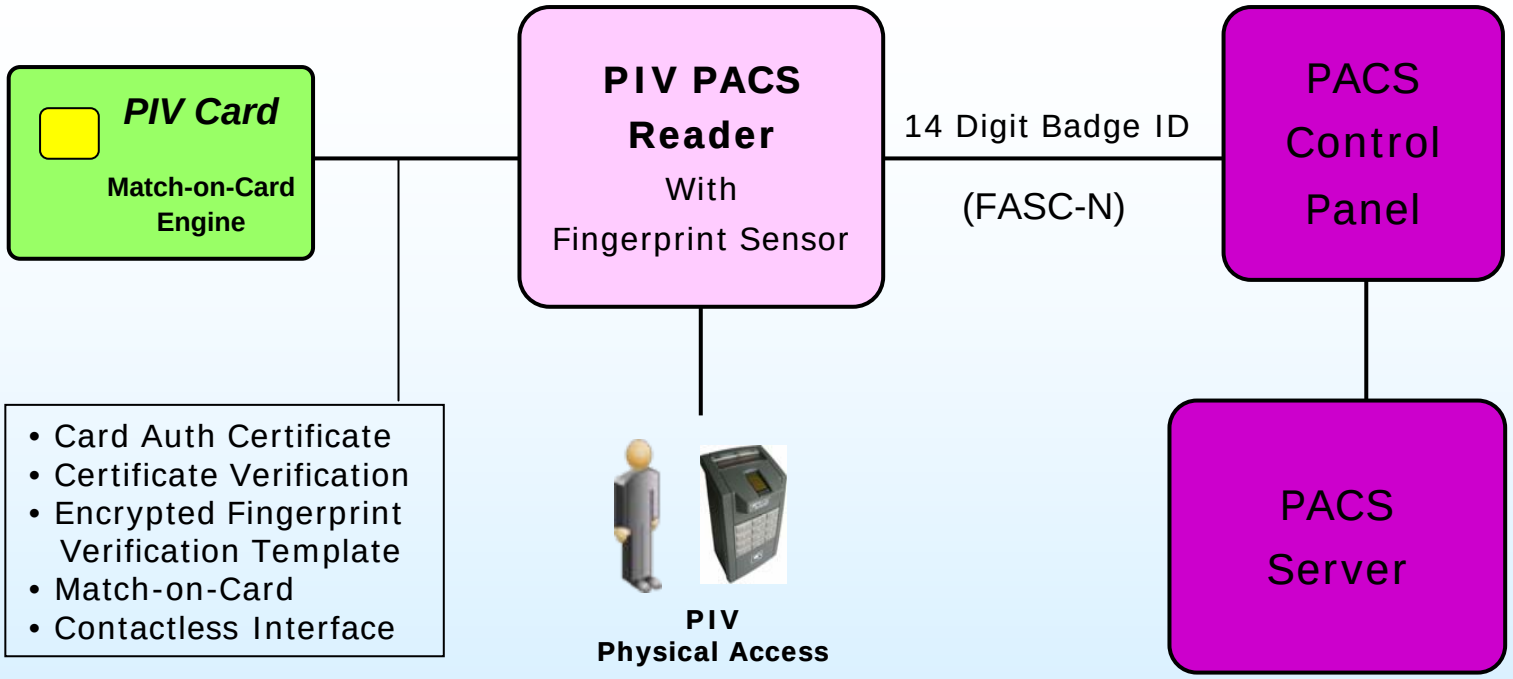
Next Steps

- Standards Works
  - FIPS 201-1
  - SP 800-73-1
  - FIPS 140-2/3, ISO 7816 and Others ?
- What Secure BMOC Activity Should Affect?
- How to Integrate with PIV?

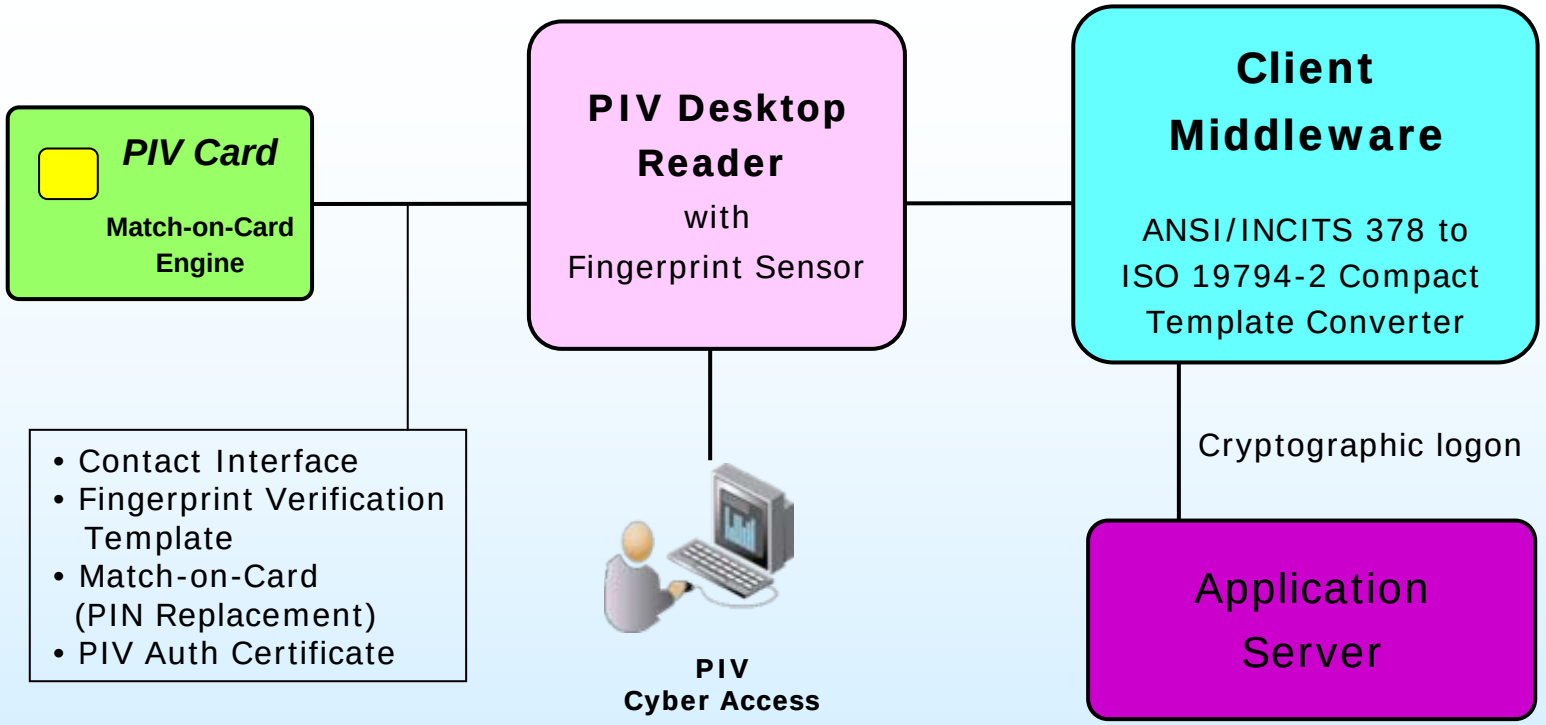
PIV Enrollment and Card Issuance Process Flow



Biometric Usage: Physical Access



Biometric Usage: Logical Access



Thanks for Helping!

Bill MacGregor
william.macgregor@nist.gov
(301) 975-8721