

# Match On Card MINEX 2

## CTST 2008 Conference

**Consuelo Bangs**  
**Sagem Morpho, Inc.**



Biometrics in Action

# What is MOC?

- ▶ **Match on Card (MOC) is the process of sending a biometric template from a live capture device to the card**
- ▶ **The card processor receives the biometric template and matches it to the reference biometric template stored on the card**
- ▶ **Advantages of MOC**
  - **Compatible with FIPS201, 140-2 certified cards**
  - **Addresses privacy concerns**
  - **Can be an element of increased security**
  - **Fast, accurate, and interoperable**
  - **Match-on-Card is available today**



# ■ Why Consider MOC?

## ▶ Replace need for PIN in FIPS 201

- Operational environments where PIN is cumbersome
- PIN can be compromised

## ▶ How does MOC help

- MOC provides non-repudiation and highly accurate means of authenticating card holder to card
- MOC would perform the same function of PIN, unlocking PII data on PIV card



## ■ MINEX 2 and MOC

- ▶ **February 2007 DHS sponsored demonstration of Match On Card to NIST FIPS 201, MINEX and TWIC program management.**
  - **Execution of Match On Card as a separate application on a certified FIPS201 card implemented using a GSA APL certified PACS reader**
  - **MOC with card authentication and full CHUID read were demonstrated**



## ■ ■ ■ ■ MINEX 2 and MOC

▶ **The demonstration resulted in a NIST feasibility study of match on card technology with secure messaging and MINEX 2**

- **MOC with secure messaging focused on speed of match when using encryption to protect the live biometric template sent to the card for matching**
- **MINEX 2 focused on performance accuracy and interoperability**



# ■ Why Conduct a Feasibility Study?

- ▶ **Recognition that FIPS201 does not address the wide use of contactless technology in the PACS environment**
- ▶ **MOC executed under secure messaging could be a solution to provide security for PII passed across the contactless interface**
  - **If speed and accuracy requirements are not compromised**
  - **If interoperability is maintained**



# ■ NIST Published Results - SBMOC

## ▶ SBMOC Process

- The cardholder presents their card to a contactless biometric reader.
- The cardholder presents their finger to the biometric scanner.
- The host establishes a secure session with the card.
- The host prepares an encrypted template containing the fingerprint (image or minutia) and transmits it via contactless interface to the card.

\* Reference NISTIR 7453



# ■ NIST Published Results - SBMOC

## ▶ SBMOC Process

- The card decrypts the template and compares it with the reference template stored on the card
- The card returns signed result (i.e., Yes/No) to the host
- ▶ 4 card vendors participated and all vendors were able to perform biometric match on card using secure messaging in 2.5 seconds or less with a 1 % or better error rate

\* Reference: NISTIR - 7453



# ■ NIST Published Results - BMOOC

## ▶ BMOOC Process

- Fips 201 certifiable card with reference template generated from one of 19 certified MINEX I vendors in ISO/IEC 19794-2 compact card format- vendor A
- MOC Matcher is selected by provider of card stock, compares ISO/IEC 19794-2 COMPACT CARD instances.
- Verification generator from reader manufacturer, C. It would extract INCITS 378 data from fingerprint image and convert to ISO/IEC 19794-2 COMPACT CARD

\* Reference NISTIR 7477



# ■ NIST Published Results - BMOC

- ▶ Only one MOC implementation achieved the minimum error rate specifications of the PIV program, Sagem Morpho
- ▶ The most accurate implementation, Sagem Morpho, was more accurate at  $FMR = 0.0001$  than the next best matcher at  $FMR = 0.01$ ,
- ▶ Sagem Morpho MOC matcher was the only one to meet the FNMR reequired for PIV for all 19 MINEX I certified template generators
- ▶ NIST data reports that all participating vendors' MOC algorithms performed best when matching against a reference template generated by the Sagem Morpho algorithm as compared to using a reference template from the other 19 MINEX I certified template generators

\* Reference NISTIR 7477



# Conclusions

- ▶ **Secure messaging has application for FIPS201 PACS implementation in supplying a secure means to pass PII data across the contactless interface**
- ▶ **One vendor has proven that MOC algorithms are as accurate as match off card algorithms with strong interoperability**
- ▶ **MINEX II is continuing and there is no doubt other vendors will improve the accuracy of their MOC algorithms**





**Consuelo Bangs**

**Cell: 703 786-7971**

**Voice: 703 797-2665**

**E-mail: [consuelo.bangs@morpho.com](mailto:consuelo.bangs@morpho.com)**

