MORPHOTRAK MATCH-ON-CARD

EFFICIENT SOLUTION TO BALANCE PRIVACY AND SECURITY

- Addresses privacy concerns
- Provides increased security
- Fast and accurate
- Most Interoperable for enrollment & verification (see MINEX II results)
- Easily integrated with legacy systems

Benefits of Match-on-Card

- The biometric template and the user's identity data are encrypted and digitally signed.
- Exchanges between the card processor and the card encoder are protected.
- At verification time, the validity of the signing authority is verified and the integrity of the data is verified with the digital signature.
- The biometric match process, embedded within the security perimeter of the card ICC, is therefore secured.
- For PIV: No need to release biometric data from PIV Card to any other system element.

SAFRAN
Morpho

MORPHOTRAK MATCH-ON-CARD

EFFICIENT SOLUTION TO BALANCE PRIVACY AND SECURITY

MorphoTrak's Match-on-Card (MOC) algorithm is capable of matching ANSI 378 to Reference template ANSI 378; ANSI 378 to Reference Template ISO 19794-2*; ISO 19794-2 to Reference Template ANSI 378 making it the most interoperable Match-on-Card algorithm in the market today.

**ISO/IEC 19794-2 specifies the compact finger minutiae based template.*

How Match-on-Card works

1. A request for the card holder's biometric is made
2. The device sends the biometric to the card
3. The card matches the live biometric sent to the biometric stored on the card
4. If the templates match, then data is released from the card

The biometric on the card is used to authenticate the card holder to the card.

Match-on-Card and Secure Messaging

The move from contact to contactless readers to read data from a smart card provides greater convenience and speed. However, data transfer across airways is less secure.

- Technology exists today to surreptitiously read data from a contactless smart card without the cardholder knowledge
- Cryptographic techniques can solve this problem by encrypting the data shared between the card and the device
- Physical Key Infrastructure (PKI) is used to create an authenticated secure session to protect the integrity and confidentiality of data sent between the device and the smart card
- The device encrypts and then sends the encrypted biometric sample to the smart card.
- The smart card decrypts the biometric sample it receives and matches it against the stored template
- The smart card then sends a simple match/no match result to the device

With each communication session the device requests a random number from the card that is used by both the card and the device to create an encrypted session. With this method, there is no need to manage keys as every session creates its own unique keys that used only once.

With Match-on-Card, there is no need to enter a PIN and secure messaging enables the use of contactless communication between card and device.

Further information on the NIST Secure Biometric Match-on-Card Assessment can be found at: http://csrc.nist.gov/groups/SNS/piv/documents/NIST-BMOC-Test-Approach.pdf

Further information on the NIST MINEX II test results can be found at: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=908096

MorphoTrak
Contact us: (800) 601-6790 - www.morphotrak.com
113 South Columbus Street Suite 400
Alexandria, Virginia U.S.A. 22314

SAFRAN
Morpho