Secure Biometrics Match-on-Card Feasibility Study

October 11, 2007

William I. MacGregor

NIST PIV Coordinator

SBMOC Goals

- Determine the technical feasibility of Secure Biometrics Match-on-Card.
- Authentication transaction time should be less than 2.5 seconds.
- Transmitting biometric data over the contactless interface should meet following security objectives:
  - 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; and
  - communication of biometric data between the smart card and the reader shall occur only after the cardholder has indicated the reader is legitimate; and
  - communication of biometric data from the smart card to the reader shall occur only after the cardholder has entered their PIN; and
  - the approach should achieve the preceding security objectives without reader-to-smart-card authentication or associated key management infrastructure

SBMOC Process

Two Major Elements

- Functionality & Performance: Draft Report
- Biometric Fidelity & Accuracy: Undergoing Analysis

Vendor Participation

- Developed and distributed Test Approach document in April 2007
- Help Public workshop in May 2007
- Conducted Weekly Public Conference Calls
- Entered Agreement with Interested Vendors

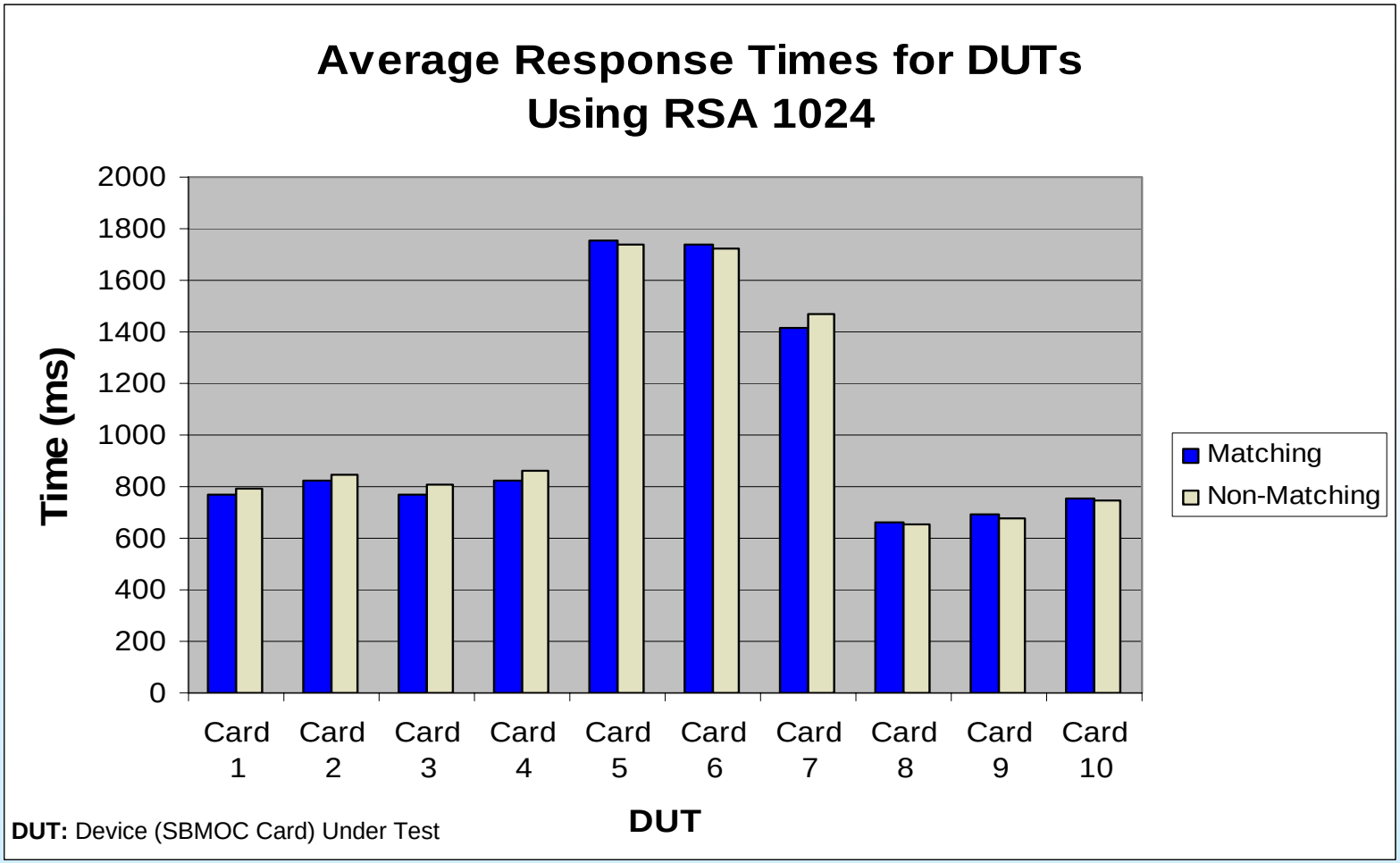
Functionality & Performance Evaluation Tests

- Developed test harness to measure performance using contactless reader
- Performed security evaluation of each submission
- Integrated specified SBMOC card edges
- Measured performance with varying security algorithms and fingerprint templates of different minutia counts (starting with powered cards)
- Summary results are subject to change; the published report will be NISTIR 7452

Card Under Test Details (Using RSA 1024)

DUT Name	Cryptographic Algorithms		Template Format	Minutiae Count
Card 1	2TDEA	RSA 1024	ISO 19794-2 Compact	27, 34, and 41
Card 2	AES-128	RSA 1024	ISO 19794-2 Compact	27, 34, and 41
Card 3	2TDEA	RSA 1024	ISO 19794-2 Compact	41
Card 4	AES-128	RSA 1024	ISO 19794-2 Compact	41
Card 5	2TDEA	RSA 1024	ISO 19794-2 Compact	27, 34, and 41
Card 6	2TDEA	RSA 1024	ISO 19794-2 Compact	27, 34, and 41
Card 7	2TDEA	RSA 1024	ANSI 378	27, 34, and 41
Card 8	2TDEA	RSA 1024	ISO 19794-2 Compact	27, 34, and 41
Card 9	3TDEA	RSA 1024	ISO 19794-2 Compact	27, 34, and 41
Card 10	AES-128	RSA 1024	ISO 19794-2 Compact	27, 34, and 41

Test Results

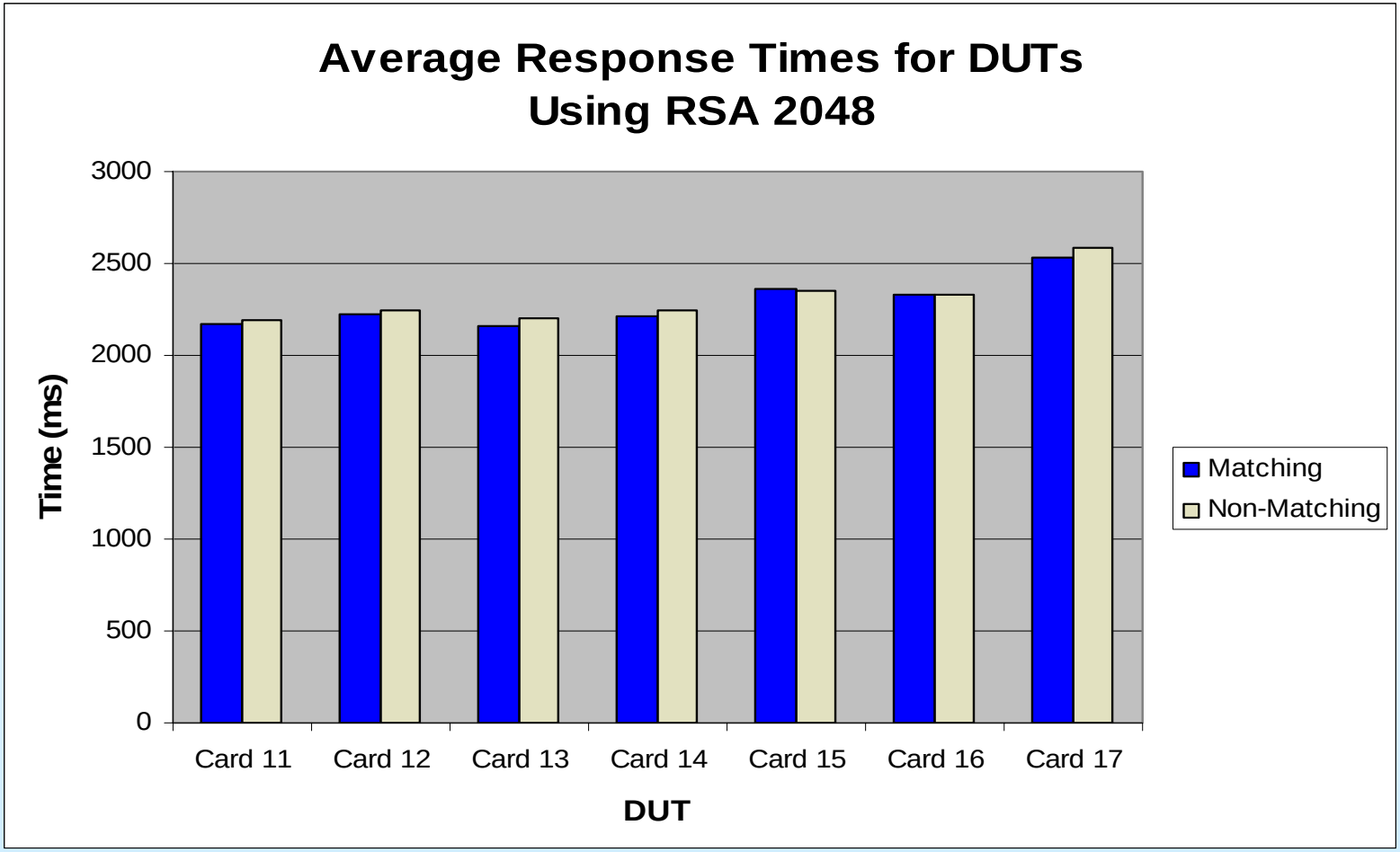


DUT: Device (SBMOC Card) Under Test

Card Under Test Details (Using RSA 2048)

DUT Name	Cryptographic Algorithms		Template Format	Minutiae Count
Card 11	2TDEA	RSA 2048	ISO 19794-2 Compact	27, 34, and 41
Card 12	AES-128	RSA 2048	ISO 19794-2 Compact	27, 34, and 41
Card 13	2TDEA	RSA 2048	ISO 19794-2 Compact	41
Card 14	AES-128	RSA 2048	ISO 19794-2 Compact	41
Card 15	2TDEA	RSA 2048	ISO 19794-2 Compact	27, 34, and 41
Card 16	2TDEA	RSA 2048	ISO 19794-2 Compact	27, 34, and 41
Card 17	2TDEA	RSA 2048	ANSI 378	27, 34, and 41

Test Results



Conclusion and Next Steps

Conclusions

- Possible to perform SBMOC operations within 2.5 seconds over contactless interface
- Data transfer secured during the transaction
- Accuracy tests are undergoing analysis

Possible Next Steps

- Report on accuracy test results
- Standardize interoperable card edge for SBMOC
- Plan integration with the PIV Standards (SP 800-73)
- Provide migration strategy for integrating SBMOC with existing PIV implementation

Thank You

- Joe Broghamer and John Schwartz for business case and leadership support
- Philip Lee for providing industry perspective, test approach, and vendor coordination
- Ketan Mehta for vendor coordination, test approach, and report development
- Trung-Hung Dang for developing the test harness and integrating vendor submissions
- NIST Director William Jeffrey, ITL Director Cita Furlani, and CSD Chief Curt Barker

Congratulations to the Participants!

Gemalto

Oberthur Card Systems

Sagem Morpho

TecSec