DRAFT

Test Approach v0.3

For

Secure Biometrics
Match-on-Card (SBMOC)

Feasibility Study

Prepared for:
National Institute of Standards and Technology

June 2007

Table of Contents

1. PURPOSE

FIPS 201-1 and associated NIST Special Publications define a method to perform biometric authentication of a PIV cardholder when the PIV Card is inserted into a contact smart card reader. In some use cases, however, contactless (Radio Frequency or RF) operation is required. Security concerns have hindered communication of biometric data transfer over the contactless interface. The transaction data can be protected by secure messaging and data encryption, but these methods can impact performance. To understand the effects of security on performance, NIST will conduct a technical feasibility study of secure data transfer over the contactless interface to perform Secure Biometric Match-On-Card (SBMOC) operations. Eventually, NIST may propose an extension of the FIPS 201 standard that achieves secure biometric authentication in the contactless mode of operation, but such a proposal is not an immediate goal of this study.

The study will use PKI to create an authenticated, secure session (like an SSL/TLS session) that protects the integrity and confidentiality of messages sent from the terminal to a smart card, and the integrity and authenticity of messages sent from the smart card to the terminal. The protocol never releases biometric data from the smart card, called the Device Under Test (DUT) in this document. Instead, the DUT receives an encrypted sample template from a biometric reader, performs a match against a reference template stored on the DUT, and returns a logically signed Yes/No result to the reader.

Preliminary tests of BMOC operation have shown that a BMOC operation for physical access could be performed within 500 milliseconds without secure messaging. Tests of PKI transaction times suggest that the approach could meet a success criterion of less than 2.5 seconds per transaction.

2. SECURITY OBJECTIVES

FIPS 201-1 permits biometric data to be released only across the contact interface of a PIV Card, and only after activation of the PIV Card through presentation of the cardholder's PIN. These restrictions achieve two security objectives: communication of biometric data occurs only over a trusted communication channel that is not easily subject to eavesdropping attacks (namely, the wired contacts inside the smart card reader); and the PIV cardholder implicitly attests to the legitimacy of the smart card reader, as they indicate by entering the PIN on the smart card reader keypad. FIPS 201-1 enables biometric authentication to occur without imposing a technical requirement for automatic authentication of smart card readers to PIV Cards. Such a requirement, it was believed, would add unacceptable key management costs. (The PIV fingerprint object is digitally signed, and the signature can be used to verify authenticity and integrity of the data.) This feasibility study will evaluate the impact of a secure protocol on transaction performance, when the protocol meets these 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; and

- SO2: communication of biometric data between the smart card and smart card reader shall occur only after the cardholder has indicated the reader is legitimate; and

- SO3: communication of biometric data from the smart card to the reader shall occur only after the cardholder has entered their PIN; and

- SO4: the approach should achieve the preceding security objectives without reader-to-smart-card authentication or associated key management infrastructure.

These security objectives are aligned with the high-level security objectives of FIPS 201-1. They protect both the integrity of the biometric authentication transaction and the privacy of the cardholder's biometric data, while avoiding the potential cost of reader authentication key management.

3. FUNCTIONAL AND PERFORMANCE OBJECTIVES

The Device Under Test (DUT) shall be a smart card having ISO/IEC 7810 physical and mechanical characteristics.

The Device Under test shall be capable of contact (via ISO/IEC 7816-3 methods, consistent with NIST SP800-73-1) and contactless (via ISO/IEC 14443 methods, consistent with NIST SP800-73-1).

Preferably, the DUT is listed on the GSA HSPD-12 Approved Product List, and modified only by the addition of BMOC firmware. The DUT may also be a type of smart card not on the GSA APL list. In this case, NIST will determine if the DUT could host a PIV card-application at reasonable development cost, and if so, the DUT will be tested.

The DUT may not have an NPIVP or a CMVP certificate. In this case, NIST will determine if the DUT could pass NPIVP and CMVP testing at reasonable development cost, and if so, the DUT will be tested.

The DUT should perform a Biometric Match-On-Card authentication transaction and meet the security objectives described in Section 2.

The biometric matching algorithm on the DUT should demonstrate accuracy meeting the criteria of SP800-76-1 Section 8.10 by testing in either the NIST MINEX II or Ongoing MINEX activity. (Note: accuracy testing may run concurrently with performance and security testing.)

The fingerprint sample template sent from the reader to the DUT should be represented following either ISO 19794-2 finger minutiae card or ANSI 378 format. Any extensions or options must be fully documented in the submitted protocol documentation.

Both RSA 1024 and RSA 2048 should be available as asymmetric algorithm alternatives unless one of these is not available on the DUT.

AES (preferred), 3TDEA, or 2TDEA (deprecated) should be implemented at the symmetric encryption algorithm.

The target transaction time for the SBMOC Technical Feasibility Study is 2.5 seconds or less and is measured from steps 3 through 9 in Section 5. Performance will be measured and reported separately for matching and non-matching cases.

4. TEST PLAN

This test plan identifies the tasks necessary to design, develop and install the BMOC Performance Test Platform at the NIST test facility located in Gaithersburg, MD.

The submission package to NIST will include:

- An executed copy of the Materials Transfer Agreement;
- Documentation of the ISO/IEC 7816 command sequence implementing the SBMOC protocol, and at least one complete protocol sequence as an example;
- Three DUTs (smart cards) capable of performing the SBMOC protocol;
- Documentation of the loading process for biometric templates onto the smart card, both initially and as a replacement after the initial load.

Additional software tools or examples maybe supplied with the submission package.

Once a complete submission package has been received, NIST will begin a security analysis of the SBMOC protocol to determine if it meets the security-related objectives of Sections (2) and (3). NIST will construct the client-side protocol implementation in the test framework. NIST will develop a new client-side protocol implementation for each submitted DUT (this will insure that NIST is able to construct working client-side software from the protocol documentation).

The test fixture will record the duration of each command-response transaction between the host and the card. A test record will therefore contain a complete log of all APDUs exchanged, and timing on each request-response pair individually. A trial will run tests and reference templates, and with non-matching sample and reference templates, to highlight any differences in transaction time arising form the match result. If the reference template object contains multiple templates, trials will be designed to disclose the effects of multiple templates (e.g., separate trials matching first template vs. second on variance, break down communication and processing time per request-response cycle, document the amount of data transmitted (in both directions) during the protocol scenario, and estimate the command-response time per sub-activity (e.g., "read certificate, "general authenticate", "verify").

5. PROTOCOL IMPLEMENTATION

The performance tests will measure the duration of phases during the SBMOC transaction. The rationale for the approach relies on two observations. First, the PIV System trust model is founded on PKI, and by design, any PIV Card can authenticate itself to another system element at a medium high assurance level using a private key and certificate stored on the card. Second, if a biometric match operation is performed on the PIV Card using SBMOC technology, there is no need to release biometric data from the PIV Card to any other system element (thus satisfying SO3 in Section 2).

Variations in protocol implementation are acceptable provided that the objectives in Sections 2 and 3 are achieved.

In outline, the use scenario is as follows. The cardholder presents their card to a contactless biometric reader, and presents their finger to the biometric scanner. The scanner obtains a fingerprint image which is transformed into the sample template, encrypted, and transmitted via contactless into the PIV Card. The PIV Card decrypts the template, matches the sample template against the reference template stored on the PIV Card, and returns a signed "Yes" or "No" result to the smart card reader.

An example of a more detailed protocol is included next.

1. The cardholder presents their PIV Card to the contactless smart card reader.
2. The host system selects the SBMOC application on the card.

   ```
   e.g., using the SELECT APDU
   ```

3. The smart card reader performs Get Data to read the PKI certificate from the PIV Card, and validates the PKI certificate.

e.g., using the GET DATA APDU followed by GET RESPONSE APDU(s)

4. The host system requests a nonce (a random card data) from the card. The card responds with 8-bytes Rc(1) and 16 bytes Rc(2). Rc(1) is used to authenticate the host and Rc(2) is used to derive the session keys.

   e.g., using the GET CHALLENGE APDU

5. The card and host system generate encryption and MAC session keys.

   GENERAL AUTHENTICATE – Used to communicate the session keys in an ciphered data block encrypted by the card public key. The encryption uses the following input data:
   - Random number for encryption session key (PSKenc)– 16 bytes
   - Random number for MAC session key (PSKmac) – 16 bytes
   - Rc(1) – 8 bytes padding received from GET CHALLENGE APDU
   - PKCS #1 padding

   GENERAL AUTHENTICATE returns the encryption and MAC session keys.

   e.g., using the GENERAL AUTHENTICATE APDU

6. A secure session is established between the card and the host system. Both the card and the host system use the Rc(2) as a key to compute encryption session key and MAC session key. The algorithm is: SKmac = 3DES(PSKmac, Rc(2)) and SKenc = 3DES(PSKenc, Rc(2)).
7. The cardholder presents their finger to the fingerprint scanner.
8. The fingerprint scanner scans the finger, and generates the sample template from the image. Alternatively, the finger print template is retrieved from a file.
9. The smart card reader encrypts the sample template using the session encryption key.
10. The host system sends the template to the card for authentication

    - VERIFY – Used to send encrypted biometric template for authentication. The input data should be of the following format: 0x7F 0x2E || length || 0x81 || length || encrypted biometric template (pad the template with zero at the end to make it multiple of 8 bytes. The response of 90 00 means the biometric template matched. The message also responds with 9 bytes of MAC for further verification by the host system.

      e.g., using the VERIFY APDU

The time to complete each of the request-response transactions, and the total time to complete steps 2-10 will be recorded. Repeated measurements will be made to estimate variance. Trials will be conducted with templates that match, and with templates that do not match. The public key algorithm used will be RSA, and trials will be conducted at 1024 and 2048 bit key lengths.

6. PUBLICATION OF RESULTS

A submission is successful if it achieves the objectives in Sections 2 and 3 when tested. At the completion of testing, NIST will publish a summary report indicating the number of successful submissions, and for each successful submission, and for both RSA 1024 and 2048, and for matching and non-matching tests:

1. the average total time for the transaction;
2. average time to establish a secure session;
3. average time to transmit the reference template to the smart card;
4. average time to compute the match;
5. average time to transmit the result from the smart card;
6. whether or not the smart card has passed NPIVP testing;
7. whether or not the smart card has passed CMVP testing.

The average total time (1) will be approximately (2) + (3) + (4) + (5).

NIST may also publish summary observations and recommendations resulting from the protocol security analyses, without reference to specific submissions.

In conformance with the “no endorsement” policy of NIST, the names of participants will not be published.