

A Method for Contactless Biometric Data Protection for TWIC

Presented to the NMSAC TWIC Working Group by the Security Industry Team

(Second Draft for NMSAC TWG review and comment)

1.0 Scope

This concept paper is submitted to the NMSAC TWIC Working Group (TWG) by the security industry task team to describe a method of using the TWIC card for automated physical access that enables

- cryptographic protection of the biometric data when stored on the TWIC card or when transmitted through the contactless interface,
- the avoidance of key management responsibilities for the access control system operators, and
- optimum transaction throughput

2.0 Purpose

TSA has advised the NMSAC TWG that Department of Homeland Security policy will require that the fingerprint template stored on the TWIC card be protected during contactless transmission using encryption technology that is appropriate to the operational requirements of the maritime industry. The method described in this paper is intended to meet this requirement.

3.0 Overview of Concept

The proposed method requires that the biometric templates be stored as encrypted data on the TWIC card and that the encrypted templates be freely accessed from either the contactless or contact interface. The biometric templates will be encrypted and placed in a separate container linked to the TWIC application during the process of updating the TWIC cards from Version 1 to Version 2. This update process will take place at TWIC enrollment centers and will be performed by trusted agents of the TSA. During the update process, encryption of the biometric templates will be based on a randomly generated 16 byte binary number, hereafter referred to as the TWIC Privacy Key (TPK), which is unique to each TWIC card. The encryption process will use the strong Advanced Encryption Standard (AES) encryption standard. As part of the update process, the TPK will be stored on the magnetic stripe in a track reserved by TSA for this purpose. The TPK will also be stored in a separate memory container on the TWIC card chip that can only be accessed through the contact interface. The TPK is used to decrypt the biometric templates at the time of user authentication. The TPK is not considered a “shared secret” in the cryptographic sense and therefore requires no special protection or key management protocol. Each TPK is only usable for the decryption of the templates stored on that specific TWIC card.

At the point of access using a fixed mount reader, a TWIC card holder will swipe the TWIC card through a magnetic stripe reader and will then place the TWIC card in close proximity to the contactless reader to transfer the unique ID and encrypted template to the reader. The TPK read from the magnetic stripe will be used to decrypt the template read from the contactless interface of the card. Then the card holder will place their finger on the fingerprint sensor and the reader will perform the matching function. If the match is successful, the reader will send the unique ID to the physical access control (PAC) system which will make the decision to open the gate based on the privileges associated with that unique ID.

3.1 Advantages

The primary advantage of this approach is that there is no requirement for storing secret keys in readers or requiring an elaborate scheme of key management. The proposed method will achieve the privacy and security objective by encrypting the biometric data when stored on the TWIC card such that it will remain encrypted during any contactless transmission and can only be decrypted by a reader that has obtained the TPK stored elsewhere in the card. It can be assumed that the reader is a valid TWIC reader because the card holder has made the decision to present the card to the reader for the purpose of access to a facility or vessel. Conversely, a contactless reader that does not have the ability to obtain the TPK data from the magnetic stripe or through the contact card interface would not be able to decrypt any biometric data read from the contactless interface of the card.

If a TWIC card is lost or stolen, the TPK on the card can be obtained. If the person now in possession of the card has detailed knowledge of the method used to generate the cryptographic key from the TPK, it would be feasible for that person to obtain the biometric template data over the contact or the contactless interface. But the card could not be used for access since the person now holding the card would not have the same fingerprint as the card holder. So the potential impact is limited to the privacy exposure of biometric data from one lost card and that card does not pose a security threat to the system. It should also be noted that privacy risk associated with the loss of a card would exist anyway since the name, photo and possibly other personally identifiable information is also printed on the surface of the card.

The proposed method effectively prevents “farming” a significant number of biometric templates without the card holder’s knowledge or consent because a rogue reader placed in close proximity to a TWIC card would not have the TPK from that card which is required to decrypt the templates.

3.2 Disadvantages

There are disadvantages to this approach. Requiring the reading of a magnetic stripe will impact:

- Reader cost
- Throughput
- Human factors issues associated with presentation of the card to multiple sensors

We believe that magnetic swipe reader modules are commercially available that are capable of operating in an outdoor weather exposed environment. Also, we believe that commercial reader manufacturers are including magnetic swipe readers on some of their reader models that also read contactless smart cards and fingerprints. Since most users are more familiar with the use of magnetic swipe card readers at the retail point of sale, the motion of swiping the card should be natural and fast. However, if magnetic card swipe was added as a user action at high volume entry points, throughput will still be negatively impacted.

3.3 Placing the TPK Code on the Magnetic Stripe

Due to the schedule constraints for the launch of the Version 1 TWIC cards, it may not be practical for TSA to record the TPK code on a reserved track of the magnetic stripe at the time of initial card production. If this is the case, it will be necessary to generate and transfer the TPK to the magnetic stripe during the one-time process of updating the card to a Version 2 card. This update process will be required in any case to place the TWIC application software and data objects on the Version 1 TWIC cards. We assume that this update function will occur at a TWIC enrollment center staffed by TSA trusted agents using workstations configured for this purpose. Each of these workstations would require the addition of a magnetic stripe encoding device which otherwise would not be required to update the TWIC application software and data objects onto the smart card memory chip. This update function would only be necessary for TWIC version 1 cards. New cards issued as Version 2 cards would already contain the necessary TPK data on the magnetic stripe as well as the TWIC application software and data objects.

4.0 Alternative Implementations

The proposed method offers flexibility to the operator in how it can be implemented within a facility or vessel. These alternative implementations can support readers that are connected to a PAC system with two-way communications capability, readers connected to a PAC system with a one-way communications capability and readers that are not connected to a PAC system. Following is a description of each:

4.1 Readers Connected to a PAC System with Two-way Communications

For those facilities that demand maximum throughput, we are assuming that the facility operator has a PAC system and that supports two-way communications with the reader. We also assume that the reader is capable of two-way communications with the PACS. The reader must have the ability to read contactless smart cards and fingerprints but does not need to have the capability to read magnetic stripes. The objective of this implementation is to eliminate the need to use a magnetic swipe device at the reader for every transaction in order to increase throughput. This implementation requires that each user be registered into the PAC system in advance. During the registration process, the unique identifier is read from the card's CHUID object on the smart card chip and the TPK is automatically read from the magnetic stripe or contact interface of the card. Both the unique identifier and TPK are then stored in the PAC system along with any other data related to access privileges for this card holder.

When a TWIC card is presented to the reader, the unique card holder identifier is read from the card through the contactless interface and sent to the PAC system. If the unique identifier is registered and has privilege to enter, the PAC system sends the TPK back to the reader. The reader uses the TPK to decrypt the biometric template read from the card.

The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader sends a signal to the PAC system. The PAC system opens the gate or turnstile.

Another permutation of this implementation can reduce the amount of data exchange between the reader and the PAC system. In this case, the reader has sufficient memory such that the PAC system can periodically broadcast all pre-registered user IDs and TPKs for storage at the reader. When a TWIC card is presented to the reader, the unique card holder identifier and encrypted templates are read from the card through the contactless interface. The unique ID is compared to the list stored in the reader. If the identifier is present, the reader uses the TPK code for that user (also stored in the reader) to decrypt the biometric templates read from the TWIC card. The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader sends the unique ID to the PAC system. If the unique identifier is registered and has privilege to enter, the PAC system opens the gate or turnstile.

4.2 Readers Connected to a PAC System with One-way Communications

In this implementation, the TWIC reader only has one-way communication to the PAC system (e.g. Wiegand interface). The reader then must have the capability to read magnetic swipe cards, contactless smart cards, and fingerprints. While it is assumed that users will be pre-registered into the PACS system, it will not be necessary to read and store the TPK in the card holder's record within the PACS system.

The card holder will swipe the card in the magnetic reader slot. The user then presents the card to the contactless reader surface and the reader reads the unique ID and encrypted template. The reader uses the TPK read from the magnetic stripe to decrypt the templates. The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader sends the unique identifier to the PAC system. If the unique identifier is registered and has privilege to enter, the PAC system opens the gate or turnstile.

4.3 Readers Not Connected to a PAC System

This implementation is generally associated with a handheld mobile reader device that may or may not be connected to the PAC system through a wireless interface. For initial deployment of Version 1 TWIC cards, the Coast Guard may use such handheld readers for spot checking. Since the Version 1 cards will be similar in design to the Federal Employee Personal Identity Verification (PIV) card, it will not be possible to read the biometric data except through a contact interface and then only after entry of a six digit PIN. Therefore, at a minimum, the handheld reader used for this purpose must have the capability to read contact smart cards and fingerprints and must include a keyboard for PIN entry.

If handheld readers are deployed in the context of the proposed method, they only require a change to the application software. The card holder or operator will insert the card in the contact reader slot. The reader obtains the unique identifier, TPK and encrypted templates through the contact interface. The reader decrypts the templates using the TPK. The user presents his/her finger to the sensor. The reader matches the presented fingerprint with the fingerprint templates read from the card. If the match is good, the reader checks its list of authorized users or sends a remote request to the PAC system to

confirm that the unique identifier has been granted access privileges. The response will be displayed to the operator who will then grant access.

4.4 Operational Biometric as a Viable Alternative to TPK

Another alternative implementation is available that avoids the use of the TPK for each access transaction since there is no need to transmit the biometric template from the card to the reader. This implementation has been previously discussed as the concept called “operational” biometrics and would be available for those operators with PAC systems with either one-way or two-way communications with the reader. This concept requires that each user be registered into the PAC system in advance. During the registration process, the unique identifier is read from the card’s CHUID object on the smart card chip and the encrypted biometric template on the TWIC card is also read and decrypted using the TPK stored in either the magnetic stripe or obtained through the contact card interface. The decrypted biometric templates are then stored in the PAC system along with any other data related to access privileges for this card holder. In addition to the option of using the enrolled fingerprint templates stored on the TWIC card for this registration process, it is also possible to enroll a different type of biometric to store in the PAC system (e.g., iris or hand geometry).

When a TWIC card is presented to the reader, the unique card holder identifier is read from the card through the contactless interface and sent to the PAC system as an index pointer to the biometric data stored on the PAC system. The card holder presents their finger to the sensor. The reader generates a template and sends the template to the PAC system. The PAC system matches the presented biometric to the biometric stored in the PAC system. If the match is good and the card holder has privilege to enter, the PAC system opens the gate or turnstile. It is important to note that this operational biometric implementation can be used in conjunction with Version 1 TWIC cards. The disadvantage to this approach is that some card holders might object to the operator maintaining a database of their biometric template for privacy reasons.

5.0 Conclusions

The proposed contactless biometric method using encrypted templates and a TWIC Privacy Key meets the security and privacy policy requirements of the Government while eliminating the need for storing and managing secret keys in the readers. The proposed method also provides flexibility as to the choice of implementation approaches and takes into consideration the different access control configurations and throughput requirements that facilities and vessels might have.