

## **A Method for Contactless Biometric Data Protection for TWIC**

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

(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 transmitted over 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 is similar to the technique used for reading data from the contactless chip embedded in the U.S. electronic passport (ePassport). The ePassport technique is known as Basic Access Control (BAC). BAC uses data obtained from the printed surface of the passport to generate a cryptographic key that is used to enable secure transmission of data from the contactless chip to the passport reader. Any attempt to read data from the contactless chip without first reading the printed data is prevented.

In the proposed method, information unique to each TWIC card is printed on the surface of the TWIC card and/or stored in the magnetic stripe of the TWIC card. This data is then used in an approach similar to the ePassport BAC system to generate a secure communication session between the card and the reader for the purpose of securely transferring the biometric templates from the TWIC card to the reader for matching with the presented biometric.

The proposed method assumes that the Version 1 TWIC card will include a printed bar coded field that has a unique number that is not freely readable from the contactless interface and is of sufficient length to ensure reasonable protection against attempts to guess the encryption process through eavesdropping on a legitimate transaction. It is also suggested that the value of the bar code field also be printed in human readable form

below the bar code area to provide a redundant source of data if the bar code cannot be read for some reason.

### **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 transmission of biometric data from the card to reader. It can be assumed that the reader is a valid TWIC reader because the card holder has made the decision to present the card in close proximity to the reader for the purpose of access to a facility or vessel. Conversely, a reader that does not have the ability to obtain the BAC information printed on the surface of the card and/or stored in a magnetic stripe would not be able to read the biometric data from the contactless interface of the card.

If a TWIC card is lost or stolen, the BAC information 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 BAC data in the bar code or magnetic stripe, it would be feasible for that person to obtain the biometric template data over 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 it is not possible for a rogue reader to be placed in close proximity to a TWIC card and access the biometric data without the card holder’s knowledge or consent.

### **3.2 Disadvantages**

There are disadvantages to this approach. For high volume access points, requiring the reading of a bar code may not be practical for the following reasons:

- Reader cost
- Durability of printed bar code
- Commercial product availability
- Throughput
- Human factors issues associated with presentation of the card to multiple sensors

Each of these points can be mitigated to some degree by copying the bar code data to the magnetic stripe and then having the user swipe the magnetic stripe of the card as the first presentation action at the reader. Magnetic swipe readers are lower in cost and we believe that the magnetic stripe is less susceptible to wear as compared to printed bar codes. We also believe that magnetic swipe reader modules are commercially available that are capable of operating in an outdoor 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 would be more natural and probably faster than reading a bar code. Likewise, there should be less of an impact related to problems caused by human factors. However, if magnetic card swipe was added as a user action at high volume entry points, throughput would still be negatively impacted – just to a lesser degree.

### **3.3 Placing the BAC 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 BAC code on a reserved track of the magnetic stripe in addition to its placement in the printed bar code. If this is the case, it will be necessary to read the bar code and transfer the data 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 BAC data in both bar code form, human readable form and magnetic stripe format 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 high, medium or low volume operations. Following is a description of each:

#### **4.1 High Volume Implementation**

In a high volume implementation that demands maximum throughput, we are assuming that the facility operator has a physical access control (PAC) system (or PACS) and that the PAC system 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 BAC data is automatically read from the magnetic stripe (or bar code) of the card or entered manually from the human readable BAC data printed below the bar code. Both the unique identifier and BAC data 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. The PAC system sends the BAC code back to the reader. The reader uses the BAC code to generate a secure transmission session with the card and reads the biometric data. 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 BACs for storage at the reader. When a TWIC card is presented to the reader, the unique card holder identifier is read from the card through the contactless interface and compared to the list stored in the reader. If the identifier is present, the reader uses the BAC code for that user (also stored in the reader) to generate a secure transmission session with the card and reads the biometric data. 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.

#### **4.2 Medium Volume Implementation**

In this implementation, the TWIC reader only has one-way communication to the PACS 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 BAC data 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. The reader uses the BAC code read from the magnetic stripe to generate a secure transmission session with the card and reads the biometric data and unique identifier through the contactless interface. 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 PACS system. If the unique identifier is registered and has privilege to enter, the PACS system opens the gate or turnstile.

#### **4.3 Low Volume Implementation**

This implementation is generally associated with a handheld mobile reader device that may or may not be connected to the PACS 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 must also be capable of reading magnetic stripe cards or bar codes as well as contactless smart cards and fingerprints. The card holder or operator will swipe the card in the magnetic reader slot or scan the bar code. The card holder or operator will then present the card to the contactless reader surface or insert the card into the contact reader slot. The reader uses the BAC code read from the magnetic stripe or bar code to generate a secure contactless or contact transmission session with the card and reads the biometric data and unique identifier. 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 BAC**

Another alternative implementation is available that completely avoids the use of the BAC code 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. 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 enrolled biometric template on the TWIC card is also read and 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 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 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 Basic Access Control techniques 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 throughput requirements of high, medium and low volume access control points.