

NATIONAL MARITIME SECURITY ADVISORY COMMITTEE

Recommendations on Developing a Contactless Biometric Specification for the Transportation Worker Identification Credential

February 28, 2006

Background

The National Maritime Security Advisory Committee (NMSAC) is chartered to advise, consult with, report to, and make recommendations to the Secretary of the Department of Homeland Security on matters relating to maritime security.

At the November 14, 2006 NMSAC meeting, DHS provided a briefing on the status of the Transportation Worker Identification Credential (TWIC). Specifically, the Committee was informed that the TWIC rulemaking would be split into two distinct rulemakings; the first rulemaking for TWIC enrollment and issuance and the second for card readers and access control requirements. At the November meeting, TSA discussed technology standards proposed for TWIC and acknowledged that there is a general consensus that current technology is not suitable for application in the maritime environment.

Accordingly, DHS asked NMSAC to consider establishing a working group to assist DHS in two areas: (1) to make sure that the Federal Government understands the full operational impact card readers will have on the maritime industry; and (2), to ensure that the Government fully understands the environmental extremes encountered in the maritime environment on a daily basis. The specific task required that NMSAC develop a contactless biometric reader specification for the Department.

NMSAC agreed to accept the task and form a TWIC Working Group (TWG).

Process

The TWG includes approximately 130 individuals, not including the federal government participants, and is organized into a maritime team and a security technology industry team. The maritime group is comprised of public and private terminal owners and operators, vessel owners and operators, maritime labor and employer organizations, trade associations, and a host of others. These individuals, with counsel of the security industry team members spent the months of December 2006 and January 2007 developing a series of operating requirements (Appendix I) which would guide the development of the technical documentation. The Maritime Operating Requirements document contains specific recommendations to DHS regarding deployment and usage of TWIC readers.

It should be noted that a minority group of members of the maritime team submitted a report discussing, among other items, several issues related to this task. This is attached as Appendix II.

Based on the parameters outlined by the maritime team, security industry representatives developed two separate Smart Card Reader Hardware Specification documents (Appendices III and IV).

The Reason for Presentation of two Documents

While the large and diverse group of individuals was able to quickly achieve consensus on a variety of matters, there remains one significant area of concern. This relates specifically to TWIC Guiding Principle (b), as provided by DHS to the NMSAC. The principle states that the specification developed by NMSAC shall incorporate “appropriate security and privacy controls.”

Specifically, there is a disparity between the NMSAC recommendation and the Department of Homeland Security guidance that the specification include a requirement to encrypt the fingerprint template. It must be noted that this guidance was supplied only after the maritime industry representatives completed the process of deliberating on the operational issues associated with the TWIC program and further that DHS provided no corresponding rationale to support the position it has taken.

As a result, the National Maritime Security Advisory Committee strongly and unequivocally recommends that DHS adopt as the TWIC reader specification, that contained in Appendix III, “TWIC Reader Hardware and Card Specification,” which was developed under the principle that utilizing a fingerprint template provides appropriate and reasonable security and privacy controls.

A. Privacy and Security Considerations – NMSAC supports the inclusion of measures to protect individual privacy and acknowledges that this prerequisite, along with the need to enhance commerce and improve transportation security, has been included as a required goal of the TWIC program since it was announced in February of 2002.

The specification included as Appendix III meets this privacy requirement.

It is our understanding that all personally identifiable information about an individual gathered during enrollment will be retained by TSA in its central data bank. The card itself is expected to show and/or contain a photo, a unique cardholder identification number, and the individual’s biometric fingerprint template.

In its design, TSA wisely elected to utilize the fingerprint template rather than a full fingerprint image specifically to address both privacy and operational efficiency concerns. Since only a fingerprint template will be passed between the card and the TWIC reader, the information cannot be reverse-engineered to a full fingerprint image.

Even if the template were “stolen” during contactless transmission to a TWIC reader, and even if somehow it could be used to replicate the original fingerprint, for which we understand no technology currently exists, the “thief” would not be able to use this illegal TWIC as the

fingerprint image would not match his own when presented to a biometric reader in conjunction with a TWIC. In addition, an individual interested in “stealing” a fingerprint would meet much less technical resistance and obtain a more accurate representation by lifting it from an object in a public place such as a car door, window or drinking glass.

B. Operational Considerations – There are several concerns with encrypting the fingerprint template.

By encrypting the template stored on the TWIC, every transaction will require encryption and decryption, each of which affords time and opportunity for a problem to arise. In addition, prior to encryption and decryption, some form of authentication or “handshake” between the card and reader is necessary to validate that the transaction about to take place is legitimate. In order for such authentication to take place, some form of key management must be in place. Thus, if a key is compromised at one instance, it affects every reader in that “key community.”

In summary,

- Adding encryption generally makes the TWIC system more complex and therefore more difficult to develop, use, manage, and maintain.
- Adding encryption will slow processing time to read cards at vessels/facilities.
- The use of keys places an administrative burden and certain liabilities (e.g., responsibility to ensure the key is not compromised) on those charged with key management. Vessel and facility operators are neither prepared nor able to accept these responsibilities.
- Adding encryption will increase TWIC costs.

Therefore, as stated in the requirements document, *“Given the limited amount of information transmitted between the TWIC and the reader, the Working Group does not believe encryption will provide any additional security benefit, but it will increase both cost and processing time.”* The NMSAC TWIC Working Group closely studied the issue and as a group concluded that the operational complexities increase by a level of magnitude and to the point where they are not proportionate with any perceived benefit of encrypting the biometric template. In short, there is no empirical evidence that encrypting the fingerprint template affords any additional protection of personal privacy.

The TWG came to this conclusion early in the process and asked DHS for a clear statement of the agency’s privacy policy at its first meeting on November 28, 2006. Unfortunately, DHS was unable to provide this guidance until after the maritime group completed its work on January 30, 2007. It was, however, received prior to the completion of the technical documentation, allowing the security team members to include protocols for encryption in its specification. Accordingly, the specification included in Appendix IV “Alternate Reader Hardware and Card Specification” does not meet the requirements of the maritime members of the TWG (See Appendix I, Questions 5 and 6). It does, however, address the DHS position that encryption should be required and it is only included as an alternate to the NMSAC recommendation at the specific request and suggestion of DHS.

Alternate Options

Appendix IV: Security Industry Proposed Solution – The security team was placed in the unenviable position of trying to meet conflicting requirements. The team developed a proposal that members believed to be a compromise approach to eliminating key management issues associated with encryption, which were among the maritime industry’s greatest concerns (see Appendix IV, Section E.1, page 48, for a text description of the proposed methodology).

However, it introduced a new concept which had not been previously discussed: this proposed solution would couple the use of a contactless chip with the use of a magnetic stripe. In summary, the approach to biometric encryption would require that an individual both swipe a magnetic stripe *and* present a TWIC in the proximity of a reader, as well as place his or her finger on the biometric sensor. This does not meet the task of “developing a contactless biometric specification for the TWIC.” The alternate approach does provide a mechanism to store the decryption key in facility access control systems, which would eliminate the need to swipe the magnetic stripe under certain circumstances; however the TWG was not provided sufficient time to discuss either the privacy concerns associated with storing data in facility systems or the impact of implementing this solution on maritime operations and its resultant effect on U.S. commerce.

As a result, the NMSAC can neither endorse nor support the Alternate TWIC Specification.

Other Solutions – During the course of its deliberations, the TWG briefly discussed other potential options to store and utilized encrypted biometric data, such as that used in the ePassport system, or installing an application on the TWIC card which would validate the fingerprint presented to a sensor within the card itself rather than within the reader. These technologies may have the potential to meet both maritime industry and DHS requirements, yet in the absence of early guidance from DHS, they have not been thoroughly explored or evaluated.

Recommendations for Moving Forward

NMSAC understands and supports the need to ensure all appropriate security and privacy protections are implemented, and we also understand the requirements in FIPS 201-1 and related Special Publications. However, we believe that both industry and government lack quantifiable and demonstrable information that would more fully justify encrypting the biometric template during the card reader transaction. Such quantifiable and demonstrable information would help ensure the Department fully understands the impact that this “protection” would have on our nation’s commerce and help strike the right balance between enhancing commerce and improving security.

Recommendation: Therefore, in the absence of such information and if DHS is in fact going to require that the biometric template be encrypted, we recommend the Department use the opportunity that the pending card reader pilot program affords to conduct a thorough assessment, from an operational perspective, of the cost, risk, and benefit of encrypting or not encrypting the biometric template. This complete assessment is warranted to demonstrate and document (1) the protections that encryption would afford the biometric template, (2) the impact that encryption

may have on performance (i.e., commerce), (3) the impact of (digital) key management on both the Department and maritime industry, and (4) the level of effort (time, cost, expertise) that would be required to introduce a threat to a regulated entity in the absence of encryption.

Given the guidance in FIPS 201-1 and associated special publications (i.e., SP 800-76), the results of such an operational analysis would be highly instructive to the entire federal government and would serve as an excellent guide as the Department develops and promulgates guidance related to biometrics technology. Additionally, the recommended assessment would be timely. The results of this critical assessment would be instrumental in guiding the development of the pending second phase (reader) rulemaking process by ensuring the Department made all necessary and appropriate considerations.

In the absence of such analysis, our nation is at risk of adversely impacting commerce and unintentionally creating more security risks than might be mitigated by TWIC implementation.

Recommendation: During the upcoming pilot program, it is our understanding that TSA is planning to coordinate the deployment of the TWIC readers nearly concurrently with the second generation TWIC cards. DHS should take steps to ensure that fully-functional Generation 2 TWIC cards are available for manufacturers to use to test the readers and applications prior to beginning the pilot program. We suggest that TSA and those of its contractors responsible for card production and card issuance/activation work closely with the security industry to provide test cards in sufficient time to allow adequate manufacturer testing of the readers prior to launching the pilot tests.

Recommendation: In addition to the above, we believe we would be remiss in our duty if we did not suggest that DHS reverse its approach to TWIC Phase II implementation. Specifically, rather than develop a TWIC reader specification first and subsequently finalize policy decisions and promulgate a rulemaking on reader usage, NMSAC recommends that DHS first resolve the TWIC policy questions (e.g., use of readers at low risk vessel and facilities, access record keeping, etc), and then incorporate the appropriate technology to support them.

Conclusion

The NMSAC continues to support the TWIC program and appreciates the opportunity to provide guidance on the TWIC reader specification. Under the circumstances, we believe the accepting the recommendations included herein, as well as those included in Appendices II and III will pave the way for a more smooth transition to TWIC reader implementation.

APPENDIX I

National Maritime Security Advisory Committee TWIC Working Group

Maritime Operating Requirements

QUESTION 1 – REVIEW OF GUIDING PRINCIPLES. Within the Task Statement presented to the National Maritime Security Advisory Committee (NMSAC) on November 14, 2006, the Transportation Security Administration (TSA) and Coast Guard prepared a list of six principles (letters a – f) which the Department of Homeland Security (DHS) believes should guide the development of Transportation Worker Identification Credential (TWIC) technologies. The working group discussed these principles and suggested the modifications as below.

GUIDING PRINCIPLES

- a. Non-proprietary
- b. Incorporating reasonable security and privacy controls
- c. Technically interoperable and aligned with Federal Information Processing Standard (FIPS) 201-1
- d. Capable of being a platform for future capabilities, including TSA-approved applications/data developed by the maritime industry which can be added to the TWIC

Recommendation: TSA should design the card in such a way that updates can be added in the field without requiring replacement of previously issued cards. The Working Group further recommends that TSA add no additional functionality beyond that required by the Maritime Transportation Security Act into the TWIC without the opportunity for public review and comment of the proposed functionality.

- e. Capable of supporting maritime operations
- f. Suitable for manufacturing

The Working Group added the following principles:

- g. The goal should remain to keep costs as low as possible; this applies to both the proposed reader and the impact of the reader on the infrastructure (e.g., electrical requirements)
- h. Operate over the full spectrum of technological environments¹
- i. Cardholder Unique Identification (CHUID) and Federal Agency Smart Credential Number (FASC-N) can be used for other applications without changing the TWIC
- j. Reader should not rely on any card feature or data that is not defined for the TWIC program by TSA
- k. The TWIC card should accommodate visible data elements compatible with International Labor Organization (ILO) seafarer's identity document

¹ That is, hi-tech operations must be able to take full advantage of the increased efficiencies afforded by the technology, and lo-tech sites must be able to implement the card and readers with minimum financial investment.

[Note: Questions 2, 3 and 15 were eliminated as unnecessary for the working group to address.]

DISCUSSION ITEMS

QUESTION 4 – TWIC DATA MODEL. *To the extent practical, TSA should describe its draft concept of a TWIC card data model. NMSAC should make recommendations for any changes or additions to this data model that are needed to support operational requirements.*

Recommendation: Given that defining the data model is a requirement to completing the reader specification, the security industry representatives have volunteered to consult with TSA and the National Institute of Standards and Technology (NIST) to describe a TWIC applet and data model. The data model should be provided to the maritime industry representatives for review and comment by February 15, 2007.

QUESTION 5 – PRIVACY. *While DHS will ultimately define the privacy policy associated with TWIC, NMSAC is being asked to define the basic privacy principles that will govern the operational use of TWIC cards. For example, it could be required that a TWIC card never disclose information to an unknown reader and that any transmissions between a card and a reader must be protected through some cryptographic means.*

Recommendations: The following recommendations are premised on the fact that the TWIC will not pass an image of the fingerprint, but rather the template only; accordingly the information cannot be reverse engineered to a full fingerprint image. However, to the extent that protective measures can be implemented to meet all the other requirements outlined in this document, such as cost, response time, and failure rate, the Working Group would be willing to consider approval of such measures. Otherwise, the Working Group adopts the following:

The Working Group recognizes that there are many who believe biometric data should be encrypted. However, given the limited amount of information transmitted, and based on the information on cryptography and associated key management provided, the maritime industry representatives on the TWIC Working Group believe encryption will not necessarily provide any additional security benefit but will increase both cost and processing time.

Guiding Principle (b.) states that TWIC will incorporate “reasonable security and privacy controls.” The Working Group does not believe the additional cost, processing time of issuing and using the TWIC, as well as the additional costs and liabilities associated with key management are reasonable measures given the nominal protection afforded by encrypting the fingerprint template.²

QUESTION 6 – KEY MANAGEMENT. *Assuming that some scheme of mutual authentication is to be defined for secure communication between the TWIC card and the reader over the contactless interface, consideration should be given to how cryptographic keys are distributed and loaded onto the TWIC card and the card readers. What will be the role and responsibility of the local facility/vessel operator in this process? What will be the role and responsibility of TSA and its card issuing contractor? Who is liable if a key is revealed, disclosed or leaked? What*

² Subsequent to the finalization of this document, the DHS provided clear guidance that encryption of the biometric template will be required. The TWIC Working Group will present additional recommendations with regard to this subject in its final presentation to NMSAC.

are the operational impact issues when a key is determined to have been exposed? How is reader maintenance managed in terms of potential key exposure? What happens if a working terminal (containing keys) is lost, stolen or misplaced?

Recommendations: Contactless card readers can readily perform the necessary function of checking the authenticity of the data within a TWIC through the utilization of a public key that does not require active key management by the maritime industry.

Given that the Working Group is not recommending that the biometric data contained with the card be encrypted, determining key management protocols should be unnecessary under this process.

Additionally, inasmuch as there are methods other than encryption that can offer reasonable protection against the unauthorized access to biometric data maintained within a TWIC and that those methods would not require key management, those methods should be explored and potentially utilized.

However, if encryption that requires key management is mandated, such key management should be simple, cost effective, and performed by TSA or its trusted agent. TSA is in the best position to perform this function and mitigate the impact, if any, of key compromise. Facility or vessel owners or operators cannot be required to perform key management functions as such management is operationally infeasible for large scale deployment, outside the expertise of facilities and vessels, and potentially less secure. Moreover, facility or vessel owners or operators disclaim and cannot assume any liability for key compromise as the production, performance, and authorized use of keys will be solely in the control of TSA.

QUESTION 7 – COMMUNICATION WITH TSA. *NMSAC should describe the suggested communication interfaces between the local facility/vessel operator and the TSA central issuance and TWIC database management that are necessary to maintain access a list of revoked TWIC credentials and to manage, to the extent it may be required, the creation of site-specific cryptographic keys.*

Recommendations:

- Look at FAA Computerized Access Control System
- Support ANSI X12
- Offer XML web-portal/web-services interface
- Investigate information coding by geographic location or employment type in TSA database to assist in focusing queries and expedite the downloading of data.

QUESTION 8 – ENVIRONMENTAL, ELECTRICAL AND SAFETY REQUIREMENTS. *The environmental, electrical and safety requirements for readers should be defined or specific environmental standards should be called out. Note that these requirements may be different between fixed mount and hand held mobile reader devices.*

Recommendations: Overall, there should be a minimum operating requirement which then can be expanded upon for specific areas of operation. For example, a container terminal should not be required to have the same HAZMAT environment/intrinsically safe device that may be employed on an oil tanker.

1. Environmental

- Readers must function in the most extreme weather conditions. Security team members to make reasonable assumptions on probable ranges based on discussions.
- Readers must be resistant to: dirt, grease, dust, vibration, rain, snow, direct sunlight, salt air, fog, sea spray, humidity, magnetic forces, blunt force, tampering, and petroleum product film such as diesel fuel, lubricating oil and other contaminants.
- Must be rated to work in hazmat environments.
- The Security group should spec three types: interior, exterior, and portable readers.

2. Electrical

- Readers should have FCC ratings
- Readers should have UL Class 2 ratings

3. Ergonomics

- Readers should have a finger guide
- Indicators should be visible in daylight
- Readers should be similar in color and design to facilitate use
- Indicators should have audible tones

4. Electrostatic

- Reader must withstand a 15KV hit with a static gun

5. Electric & radiated RF immunity

- Meet FCC standards
 - Temperature – test for cold/heat, temperature ranges
 - Humidity – 95% relative, non-condensation
 - Dust – IP & NEMA
 - Shock & vibration – UL Test
 - Corrosive testing - Salt & fog (30 day test)
 - Intrinsically safe readers should be available
- UL tested
- Meet CG & electrical standard.

The mil Std 810 process could be used to guide the evaluation of products.

QUESTION 9 – POWER. *Define the requirements for input power.*

Recommendations:

- 2 amp, maximum requirement; vendors may offer additional options
- Max 24 V DC +/- 10% (6-16 volts should be acceptable)
- Reverse voltage protection

QUESTION 10 – POWER LOSS RECOVERY. *Should the reader include a capability of storing, retrieving and automatically recalibrating to the properly calibrated biometric sub-system configuration after disruption of power?*

Recommendations:

- Automatic recovery, return to standby
- Handheld reader
 - 12 hours minimum operational time
 - Max of 2 hour recharge
 - battery pack
- Reader should have hibernation mode for data loss protection

Since the TSA system will only be used for the keys and status information, there should be no effect on local operations and systems, except that vessels/facilities will be unable to download the watch list. There should be sufficient redundancy and backup servers in the prime vendors contract to minimize if not eliminate this potential problem.

The security group will make reasonable assumptions on nos. 9 and 10 and address in the technical specification.

QUESTION 11 – OPERATIONAL AVAILABILITY. *Following is an example of an operational availability requirement developed by TSA for biometric devices used in airport access control systems. NMSAC should define a similar requirement for TWIC readers.*

Biometric device reliability (Mean-Time-Between-Failure), maintainability (Mean-Time-To-Repair), and maintenance concept as designed should yield at least a 99.86% operational availability rate (Ao), whereas the cumulative down-time per unit during operational duty hours for all maintenance should not exceed 10 duty hours annually assuming a 20-hour duty day for 365 days each year. Ao is defined as:

$$A_o = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \text{ for any single device, any duty day}$$

Where downtime is the total amount of time the unit is not available for use during the duty day.

Recommendations:

- Biometric – 1 million touches. Technical specifications should challenge vendors to develop range of readers with different levels of durability/reliability. Market place will determine which ranges are most suitable.
- 25,000/ 2-1/2 year mean time between failures (MTBF)
- Testing must be performed against specs
- Readers must be easily interchangeable to allow for speedy repair/replacement.

QUESTION 12 – USER INTERACTION INDICATORS. *Define the requirements for displaying status of any or all of the following: Power on; Ready for use; Battery level (handheld devices); Access granted; Access denied; Text messages (e.g., try again, see security officer, etc.).*

Recommendations: The following are minimum requirements; vendors may offer additional features.

- Combine power-on/ready-for-use
- Indicator (e.g., amber) to show the reader is working and processing information
- Battery power level on handheld
- Access granted/denied

- Indicators must be detectable in bright sunlight and at night
- Text message not required
- Instructional information must not be printed on paper unless it can be protected from the elements and vandalism
- Additional features might include additional lights, multiple text messages, voice indicators

QUESTIONS #13 – BIOMETRIC ERROR RATES. *The basic purpose of utilizing a biometric sub-system as part of an access control system is to verify the identity of the person attempting to gain access to a secure area. There are several fundamental metrics that quantify the performance of a biometric sub-system:*

- Identity matching error rates (expressed as “false accept” and “false reject” error rates)*
- Enrollment failures (expressed as “failure to enroll” errors)*
- Inability of the technology to adequately acquire a biometric sample (expressed as “failure to acquire” errors)*

NMSAC should define the minimum performance standards in categories a) and c). Enrollment (category b) is the responsibility of TSA. However, enrollment failures will create an exception condition that may require an operational policy change. Below is an example of standards as defined in a) for verification error rates for biometric readers developed by TSA for airports:

To qualify as an acceptable biometric device, the device should operate at error rates at or below a transaction False Reject Rate (FRR) of 1% when the security threshold is set at a False Accept Rate (FAR) of 1%. Expressed another way, an acceptable biometric device should have an Equal Error Rate (EER) of 1% or less. TSA’s guidance assumes that up to three attempts should be allowed for each verification transaction.

Recommendation: Initial recommendation is a 1% (per transaction basis – allows up to three attempts) as a minimum standard for error rate (comparable with airport operations standard). Some maritime operators will require that this standard be exceeded.

QUESTION 14 – PERFORMANCE/TRANSACTION TIME. *There should be a minimum requirement for throughput using fixed base readers for both pedestrians and vehicles. For example, this can be defined as the number of vehicles per hour and/or the elapsed time for a specific authentication transaction from the moment that a user places the TWIC card in proximity of the reader until the time that the gate, portal, or door is opened. Below is an example of a standard set by TSA for the use of biometric readers for access control at airports:*

To qualify as an acceptable biometric device, testing should indicate that the device can process biometric device transactions with an average duration of less than 6 seconds. The start time for the transaction should be the presentation of the claim of identity (such as card swipe, presenting smart card or bar code). The end time for the transaction should be when a verification decision is reached.

Recommendation: To qualify as an acceptable biometric device, testing should indicate that the device can process biometric device transactions with an average duration of no more than 3 seconds. The start time for the transaction should be the presentation of the claim of identity (presenting smart card). The end time for the transaction should be when a verification decision is reached.

QUESTION 16 – SECURITY LEVELS BASED ON THREAT. *Should possession of a TWIC card in conjunction with biometric authentication (2-factor authentication) be a minimum requirement at all threat levels (MARSEC 1, 2 or 3) or will possession of a TWIC card alone (single factor authentication) be considered sufficient at reduced threat levels (e.g., MARSEC 1)? In times of elevated security levels (e.g., MARSEC 3), will there be an additional requirement for personnel to enter a Personal Identification Number (PIN) in addition to presentation of the card and the biometric match as an added authentication factor (3-factor authentication)? If so, consideration should be given to the operational impact in dealing with forgotten PINs under such a policy – particularly when you consider that users may not have used their PIN in a long time. Is there any tangible security benefit to requiring PINs at any threat level?*

Recommendation:

- MARSEC I: Card only (i.e., read of the CHUID only through the contactless interface)
- MARSEC II & III: Card + biometric (requires that all TWIC readers include a fingerprint sensor; this can be bypassed during MARSEC I conditions)

The Working Group does not recommend that a PIN be used at any point in the TWIC verification process.

QUESTION 17 – EXCEPTION PROCEDURES/FAILURE TO ENROLL BIOMETRIC. *There will be a small number of users that are unable to successfully enroll their biometric characteristic due to a variety of factors. For example, some fingerprint patterns are difficult to measure due to age, injury or skin condition. Administrators should have procedures in place to handle such exception conditions. Alternatives to consider could include:*

- Allow card and PIN
- Consider including ability to provide biometric enrollment as a job-related requirement in the job description and deny assignment if not capable
- Restrict such individuals to access the secured areas at guard-attended access portal locations only.

Recommendations:

- If an individual is truly unable to enroll, the TWIC card should include a code that tells the reader that no biometric match will be attempted. Alternatives to use of fingerprint biometrics will be addressed in the individual security plans.
- It is important that TSA/Trusted agents receive appropriate training to reduce the percentage of individuals who are unable to enroll. It is noted that in the Tampa and Manatee, Florida areas, with approximately 20,000 applicants, less than 1% were unable to enroll.

QUESTION 18 – EXCEPTION PROCEDURES/FALSE REJECTIONS. *Administrators should expect false rejects in a biometric sub-system. These false rejects could be due to improper presentation of the biometric characteristic to the sensor (such as improper finger placement) or poor quality template capture during enrollment. The biometric sub-system should provide a capability to allow the user to make multiple attempts to authenticate with their biometric. To mitigate this issue, TSA has indicated that two fingerprints will be enrolled. If the primary biometric does not work, then the user can try their secondary biometric. The reader should accommodate this protocol. If multiple attempts with primary and secondary biometric*

enrollments are not successful, then the user will need to contact a security or administrative person for assistance in gaining access. NMSAC will need to review and comment on the false rejection rate standard set by TSA for biometric matching (after multiple attempts) and determine whether this meets operational needs and what exception procedures will need to be followed to minimize the impact to facility and vessel access control operations.

Recommendations:

- Automated alert or lockout after X attempts – facility chooses (within an acceptable range)
- Continuous log for patterns (option)

Alternatives to use of fingerprint biometrics will be addressed in the individual security plans.

QUESTION 19 – INTERFACE TO EXISTING ACCESS CONTROL SYSTEMS. *Existing access control systems may have limited data input capability for resolving the unique card holder number. Since TWIC cards are based on a very large theoretical population, there may be a conflict between the TWIC numbering scheme and the ability of the Access Control System (ACS) to accommodate the scheme. NMSAC should review the TWIC card holder numbering scheme and give consideration to either (i) recommending a TWIC numbering scheme that fits existing ACS capabilities or (ii) providing guidance for upgrading or replacing existing access control systems.*

The data output from the TWIC reader to the ACS may need to support multiple interfaces (e.g., Weigand, Ethernet, RS 485, etc.) to accommodate the widest number of legacy ACS installations. The minimum data output requirements should be defined. It may be necessary to perform a survey of a representative sample of facilities and vessels to determine the typical range of ACS in place, if any.

Recommendations:

- Use existing numbering scheme for TWIC in FIPS 201
- Use white paper by Smart Card Alliance
- Input reader to access control system data transfer protocol
- The TWIC identifier will provide a unique identifier based on the first three fields of the FASC-N as follows: Agency Code (TWIC specific, 4 digits, 14 bits), System/Site Code (4 digits, 14 bits), Credential Number (6 digits, 20 bits). This will be a 14 digit number, transmitted between the reader and the PACS as 48 bits.

QUESTION 20 – MAINTAINING READER SOFTWARE/FIRMWARE. *What should be the procedures and flexibility for reader firmware upgrades? It is more efficient to download firmware/software updates from a central location to each reader since the process of upgrading individual readers at the reader location can be labor intensive. However, downloading of cryptographic keys may have security implications that must be considered.*

Recommendations:

- Standard needs to address security and functionality to upgrade (e.g., two-way communications, direct connection to a reader port or through a programmable card). This provides more flexibility for the facility/vessel to accommodate existing PACS infrastructure.

- A security verification process should be considered for the firmware/software updates to ensure that only authorized/authenticated firmware/software updates are permitted. This ensures that the firmware/software loaded is not corrupt (intentionally or unintentionally).

QUESTION 21 – OPERATIONAL AND REFERENCE BIOMETRICS. *In the TWIC Prototype Phase, TSA explored the possibility of allowing facilities and vessels to (i) use the required “reference” fingerprint biometric stored on the TWIC card for authentication or (ii) enrolling “operational” biometric data into a locally controlled database within the ACS and using the TWIC card as an “index pointer” to the biometric record stored off of the TWIC card. The advantage of the reference biometric concept was that no external database or secondary biometric enrollment was required. The advantage of the operational biometric concept was that other biometric modalities besides fingerprint could be used at the local facility or vessel (e.g., hand geometry, iris, face, etc.) for authentication of users. A third approach would be to give local facilities and vessel operators the capability to store the operational biometric in the TWIC card itself. However, this raises issues related to conflicts for those users that have to access multiple facilities and where several of these facilities may want to use incompatible operational biometrics stored on the TWIC card. Biometric data occupies significant storage space on the card and it is unlikely that space will be available for multiple operational biometric schemes. NMSAC should make a recommendation to TSA as to whether the government should endorse the local decision to use either reference or operational biometrics.*

Recommendations:

- TWIC data model should read reference biometrics from both contact and contactless sides.
- No PIN required
- No additional biometrics on card beyond the digital photograph
- Available to facility or vessel if so chooses

QUESTION 22 – MIGRATION. *Consideration should be given to the process of phasing in new TWIC readers at a time when a portion of the user population may still be using legacy ID badges and/or readers.*

Recommendation: The Working Group believes individual operators (and/or local Captains of the Port if appropriate) should determine migration pathways.

APPENDIX II

To: The National Maritime Security Advisory Committee (NMSAC)

From: Passenger Vessel Association
International Organization of Masters, Mates & Pilots
Marine Engineers' Beneficial Association
Offshore Marine Service Association

Subject: TWIC Contactless Biometric Specification Development Working Group

As groups representing both vessel operators and professional mariners, we are writing to provide additional comments on the development of the Transportation Worker Identification Credential (TWIC) reader.

At the November 14, 2006 meeting of the NMSAC, the TSA and the U.S. Coast Guard prepared a list of six principles which DHS believes should guide the development of TWIC technologies. The Coast Guard and TSA tasked NMSAC with development of a contactless specification that would allow secure, contactless communications between the TWIC card and a TWIC reader without having to insert the card into the reader.

The TWIC is a requirement of the Marine Transportation Security Act (MTSA) of 2002.

1. Prior to any follow-on rulemaking on the TWIC reader agencies should partner with affected industries to determine the effectiveness of the proposed reader technology in a functioning maritime environment.

The MTSA requiring the TWIC does not authorize, nor does it mention, a TWIC reader. Rather, Section 70105 of Title 46, U.S. Code, simply refers to a "Biometric Security Card." The law creates a mechanism for vessel owners, operators and other parties to ensure that employees who require unescorted access to the secure areas of regulated vessels or facilities have passed background security checks.

The concept of the TWIC reader was initiated by the TSA in NPRM TSA-2006-24191. Because of the negative public, industry and congressional response to the proposal regarding the readers, the final rule defers action on the readers to a subsequent rulemaking. In the preamble to the final TWIC rule, TSA says it will publish a follow-on rulemaking detailing specifications for the TWIC readers. The task statement reports that "The results of this pilot (*Safe Port Act requirement*) will inform the second TWIC rulemaking, which is intended to incorporate contactless card reader capability to meet the demands of TWIC application in the maritime environment." Notwithstanding statements such as this, that indicate that TSA has predetermined the use of TWIC readers, public comments submitted to the TWIC rulemaking docket were opposed to the use of readers.

While TSA has been meeting with and working closely with the biometric industry to prepare a regulatory basis for the use of this technology, no similar effort has been expended to determine the efficacy of such devices in the context of vessels. There has not been an accurate cost-benefit analysis for the use of reader systems on vessels. There has been no risk-based analysis such as that encouraged by the Government Accounting Office in report GAO-07-386T before expenditures are made. The cost-benefit analysis carried out as part of the Notice of Proposed Rulemaking grossly underestimated the cost of the readers and provided no quantifiable benefit. The analysis failed to incorporate all the additional requirements that would emerge as part of the reader systems, including computer network systems, data communications systems, maintenance costs and additional personnel for supervision and maintenance.

Before taking further regulatory initiatives the TSA and the Coast Guard should partner with vessel operators. The TSA and Coast Guard should use the expertise of the various vessel operating communities to determine whether or not any use of TWIC readers is justified on any vessels. If readers are justified on any vessels, a risk-based threat assessment should be performed to determine on which, if any, vessels a TWIC reader would provide a quantifiable risk-reward benefit.

A proposed rule issued by the Department of Homeland Security (**Docket: DHS-2006-0073 / RIN 1601-AA41**) uses the DHS Risk Assessment Methodology (RAMCAP), covering Chemical Buffer Zone Protection Program systems for developing risk matrices. RAMCAP, under the proposed rule, would be used to assign a risk level at a facility which would determine appropriate security measures to be included in the facility's security plan. The approach is one of determining the level of risk on a tiered basis using as many as five tiers from high risk to low or no risk, and applying security measures, including access control procedures on the basis of potential risk for various tiers. There is a wide disparity in the risk potential represented by different facilities and vessels in our diverse maritime industry. It should be recognized that the security regimes and access controls that are justified for a high risk facility may often be inappropriate and impractical from a cost/benefit basis in a low risk environment. Industry could help the Coast Guard adapt RAMCAP or develop a similar system for vessels.

2. The department should add the internationally accepted mariner identification methodology to the TWIC.

During the discussions of the working group, the issue of international mariner identification was raised. It is important to note that the MTSA included a requirement for the United States to negotiate an international seafarer identification document. Incorporation of this feature into the TWIC will make access to shore leave for U.S. mariners aboard U.S. vessels in foreign ports possible. This will help facilitate the operation of U.S. commercial vessels and those contracted to the Department of Defense.

Such an international standard has been developed. The International Civil Aviation Organization (ICAO) standard is the standard contemplated in ILO C-185. While the United States has not yet ratified ILO C-185 due to issues unrelated to the use of the document as a means of identification, the standard does exist and U.S. mariners in foreign ports will come up against it.

As the use of the ICAO standard will not impact the functionality of the TWIC card, and since the card has been designed to allow for its inclusion, it is incumbent on the TSA to include this functionality on the card.

3. The TSA requested that the Working Group advise DHS on “the full operational impact the card readers will have on the maritime industry.”

It is impossible to advise DHS on the “full operational impact” of the card readers in the context of a process apparently being driven by the technology.

Although the vessel operating members of this group do not have the technical expertise to support or reject the technical aspects of a contactless standard, they can clearly envision routine operating situations in which the physical environment of vessels will exceed the design operating parameters considered herein. For example, they can clearly foresee situations in which the ability to add “local applications” to the card will negatively affect mariners. The vessel operating community is also concerned that there are vessels that, due to their size, capacity, cargo and/or route, do not pose a significant enough risk to support the inclusion of TWIC readers in their routine operations.

The two moderators of this Working Group did an exceptionally good job of keeping the group “on task.” In an effort to assist the moderators and not impede the group’s progress, participants with significant questions on the basic concept of readers on vessels did not persistently voice their concerns.

During discussions on the contactless standard, proponents of this technology continually voiced their assumptions of an upward spiral of applications on the TWIC card and applications for readers. One of the most disturbing assumptions was that this technology would be used on doors and gates for automatic access control. In fact, such technology is inappropriate for most vessels and facilities. The TSA and the Coast Guard should partner with vessel operators to determine which if any applications of the TWIC card other than confirmation of the required background screening are appropriate. Only after the completion of such a collaborative evaluation can industry advise the TSA and the Coast Guard on the true operational impact (\$ = cost) of the proposed reader technology.

4. We are concerned with guiding principle “d,” which states that the TWIC should be capable of being a platform for future capabilities.

Congress' vision for the TWIC program was to secure port facilities by establishing a system for vetting those who would require unescorted access to secure areas. Congress never envisioned that the TWIC would be used for any other purpose.

Our concerns over this guiding principle arise from uncertainty surrounding the intended "future capabilities."

First, no state, municipality, or port facility should have the capability to write to the TWIC card or impose requirements beyond what is required by TSA to issue the card. To allow this might interfere with the ability of mobile TWIC holders (mariners, truckers, etc.) to enter onto a facility in cases in which the individual's TWIC card is missing some locally required piece of data.

Second, allowing state, local jurisdictions or port facilities to require certain information on the card would contradict TSA's privacy policy which was clearly stated in the agency's *Privacy Impact Assessment for the Transportation Worker Identification Credential Program*, December 29, 2006, Section 1, paragraph 5. TSA states: "Limiting the amount of personal data TSA receives to what is necessary to conduct a security threat assessment and satisfy MTSA serves the agency's operational purposes and minimizes the privacy risks for TWIC applicants."

Thank-you for allowing us to submit this minority addendum to the workgroup report. As representatives of vessel operators and mariners we felt that certain points, some not directly related to the task statement, required restatement and emphasis to ensure that America's vibrant merchant marine is not damaged by the implementation of this initiative.

Signed:

Passenger Vessel Association
International Organization of Masters, Mates & Pilots
Marine Engineers' Beneficial Association
Offshore Marine Service Association

APPENDIX III

TWIC Reader Hardware and Card Application Specification

February 28, 2007

Sponsor

National Maritime Security Advisory Committee TWIC Working Group

Abstract: The document describes the hardware requirements for smart card readers supporting the Transportation Worker Identification Credential (TWIC). This credential is used to access secure areas and information in transportation facilities according to a facility's security plan control requirements.

Keywords: TWIC, smart card, biometrics, fingerprint.

Status summary

Contacts

Lisa Humber, Co-Chair, National Maritime Security Advisory Committee
TWIC Working Group
Maritime Exchange for the Delaware River and Bay
Tel: (215) 925-2615

Basil Maher, Co-Chair, National Maritime Security Advisory Committee
TWIC Working Group
Maher Terminals, Inc.
Tel: (908) 665-2100

Walter Hamilton, Technical Lead, National Maritime Security Advisory Committee
TWIC Working Group
International Biometric Industry Association
Cell: (425) 503-0985

Table of contents

Contacts2

1. Overview7

 1.1 Scope and purpose7

2. References8

 2.1 Normative References8

 2.2 Informative References9

3. Definitions10

 3.1 Conformance levels10

 3.2 Glossary of terms10

 3.3 Acronyms and abbreviations11

4. TWIC Modes of Operation12

 4.2 System Perspective12

 4.2.1 Physical Access Control12

 4.2.2 Portable Identity Verification14

 4.3 Portable Verification15

5. Fixed Reader Requirements16

 5.1 Physical Requirements16

 5.1.1 Device Dimensions16

 5.1.2 Environmental16

 5.1.3 Impact Resistance16

 5.2 Electrical Requirements17

 5.3 Safety17

 5.4 Electromagnetic/Vibration Compatibility17

 5.4.1 47CFR18 and/or CISPR 11 (Emissions)17

 5.4.2 IEC 61000-4-2 (Electrostatic Discharge)17

 5.4.3 IEC 61000-4-3 (Radiated RF Immunity)17

 5.4.4 IEC 61000-4-4 (Electrical Fast Transient/Burst)18

 5.4.5 IEC 61000-4-6 (Radio Frequency Common Mode)18

 5.4.6 IEC 61000-4-5 (Surges)18

 5.4.7 IEC 61000-4-8 (Power Frequency Common Mode)18

 5.4.8 IEC 61000-4-11 (Voltage Dips and Interruptions)18

6. Portable Reader Requirements19

 6.1 Portable Reader Specific Requirements:19

 6.1.1 Operational Features19

 6.1.2 Environmental Requirements19

 6.1.3 Electrical Requirements19

7. Operational Requirements20

8. Performance Requirements22

9. Operational Availability23

10. Delivery24

11. TWIC Card Application25

11.1 Card-application Identifier25

11.2 Data Model25

11.3 TWIC card-application command set:26

 11.3.1 SELECT card command.....26

 11.3.2 GET DATA card command.....27

11.4 Sample Card Data.....28

 11.4.1 Transportation Worker Unique Information Data Object (0xDFC100)28

 11.4.2 Card Holder Unique Identifier Data Object (0x5FC102)28

 11.4.3 Cardholder Fingerprints Data Object (0xDFC101)29

 11.4.4 Security Object Data Object (0xDFC10F)30

Appendix A Authentication Processing.....31

 A.1 CHUID Authentication.....31

 A.2 TWIC Biometric Authentication31

 A.3 Card Authentication Key Authentication.....32

Appendix B MARSEC Level Processing35

Appendix C TWIC Reader Compatibility With Other Card Types36

Appendix D Description of Concept for Operational Biometrics.....37

Appendix E Proposed TWIC AID Structure38

List of figures

Figure 4.1 Generic Biometric-based Access Control System.....13

List of tables

Table 4.1 MARSEC Requirements.....12
Table 4.2 Biometric Access System Key Descriptions.....14
Table 7.1 75-bit Wiegand Output Format.....20
Table 7.2 48-bit Wiegand Output Format.....21
Table 11.1 Data Objects in the TWIC Card-application Property Template (Tag '61').....27

1. Overview

1.1 Scope and purpose

This document specifies the requirements for smart card readers, both fixed and portable, supporting the Transportation Worker Identification Credential (TWIC). The mission of the TWIC program is to design and field a common credential for all transportation workers requiring unescorted physical and logical access to secure areas of the nation's transportation system and their associated information systems. In its development, the TWIC has been designed as a standards-based program, and conforms to the standards referenced in this document. This specification enables varying levels of control in support of threat level risk mitigation plans.

This specification has been developed by the National Maritime Security Advisory Committee (NMSAC) in response to a request from the Transportation Security Administration (TSA) and the U.S. Coast Guard. The NMSAC TWIC Working Group is comprised of members of the maritime industry with support from representatives from the security technology industry who are affiliated with such organizations as the International Biometric Industry Association (IBIA), the Security Industry Association (SIA) and the Smart Card Alliance.

2. References

2.1 Normative References³

- [R1] Security Policy for DAL C3 Applet Suite, Dreifus Associates, Ltd.
- [R2] ANSI/INCITS 383, Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers
- [R3] ANSI/INCITS 378-2004, Information Technology – Finger Minutiae Format for Data Interchange
- [R4] ANSI/INCITS 358-2002, Information Technology – BioAPI Specification
- [R5] NISTIR 6529A, Common Biometric Exchange Formats Framework (CBEFF)
- [R6] ISO/IEC 7816, Identification cards – Integrated circuit(s) cards with contacts
- [R7] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards
- [R8] SIA AC-01 (1996.10), Access Control – Wiegand Card Reader Interface Standard
- [R9] FIPS 186-2, Digital Signature Standard
- [R10] FIPS 197, Advanced Encryption Standard
- [R11] FIPS 46-3, Data Encryption Standard
- [R12] FIPS 140-2, Security Requirements for Cryptographic Modules
- [R13] UL 294, Standard for Safety of Access Control System Units
- [R14] EN 50081-1 (1992), European Standard, “Electromagnetic Compatibility – Generic Emission Standard, Part 1: Residential, Commercial and Light Industry”
- [R15] IEC 60068-2-64, “Environmental Test – Part 2: Test Methods – Test FH: Vibration Broadband Random (Digital Control) and Guidance
- [R16] IEC 61000-6-1 “Electromagnetic Compatibility – Generic Immunity \Standard, Part 1: Residential, Commercial and Light Industry”
- [R17] IEC 61000-4-2 (Electrostatic Discharge)
- [R18] IEC 61000-4-3 (Radiated RF Immunity)
- [R19] IEC 61000-4-4 (Electrical Fast Transient/Burst)
- [R20] IEC 61000-4-6 (Radio Frequency Common Mode)
- [R21] IEC 61000-4-5 (Surges)
- [R22] IEC 61000-4-8 (Power Frequency Common Mode)
- [R23] IEC 61000-4-11 (Voltage Dips and Interruptions)
- [R24] IEC 68-2-27 (1987), International Electrotechnical Commission, “Basic Environmental Testing Procedures, Part 2: Tests – Test Ea and Guidance: Shock”
- [R25] IEC 68-2-29 (1987), International Electrotechnical Commission, “Basic Environmental Testing Procedures, Part 2: Tests- Test Eb and Guidance: Bump”
- [R26] OSHA Regulation 1910.147 De-energizing Equipment
- [R27] MIL-STD 810F Series of standards are issued by the United States Army's Developmental Test Command, to specify various environmental tests to prove that equipment qualified to the standard will survive in the field

³ Some normative references may only apply to certain reader configurations

[R28] NEMA 250-1997 standard (<http://www.nema.org>)

2.2 Informative References

- [R29] FIPS Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March 14, 2006)
- [R30] FIPS 201 Errata FIPS 201-1 Change Notice (<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>)
- [R31] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS), Version 2.2 (see http://smart.gov/whats_new.cfm)
- [R32] ICAO 9303 Machine Readable Travel Documents
- [R33] Global Platform Messaging Specification, Version 1.0, Nov. 2003 (Provides a definition of all the roles and responsibilities for all the actors (systems) in a multi application smart card infrastructure and defines reference standard on information exchange (message) between actors)
- [R34] TSA *Guidance Package – Biometrics for Airport Access Control* (30 September 2005)
- [R35] ANSI/SIA OSIPS ACOV-01:200x (Under Development). The OSIPS (Open, Systems Integration and Performance Standards) data models are defining interoperability between components in traditional access control systems.

3. Definitions

3.1 Conformance levels

3.1.1 expected: A key word used to describe the behavior of the hardware or software in the design models *assumed* by this specification. Other hardware and software design models may also be implemented.

3.1.2 may: A key word indicating flexibility of choice with *no implied preference*.

3.1.3 shall: A key word indicating a mandatory requirement. Designers are *required* to implement all such mandatory requirements.

3.1.4 should: A key word indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase *is recommended*.

3.2 Glossary of terms

3.2.1 TWIC card: A smart card that corresponds to the specifications laid out for the Transportation Workers Identity Credential Program.

3.2.2 Minutiae template: A minutiae template is a mathematical representation of the pattern of ridge endings and branches in a fingerprint.

3.3 Acronyms and abbreviations

BAC	Basic Access Control
CHUID	Card Holder Unique Identifier
FIPS	Federal Information Processing Standard
IBIA	International Biometric Industry Association
IP	Ingress Protection (rating)
MARSEC	Marine Security Level
NEMA	National Electrical Manufacturers Association
NMSAC	National Maritime Security Advisory Committee
PACS	Physical Access Control System
PIV	Personal Identity Verification
SIA	Security Industry Association
TSA	Transportation Security Administration
TWIC	Transportation Workers Identity Credential

4. TWIC Modes of Operation

The Coast Guard has a three-tiered system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security's Homeland Security Advisory System (HSAS). MARSEC Levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. The Commandant of the U.S. Coast Guard sets MARSEC levels commensurate with the HSAS. The requirement for using various authentication mechanisms at certain MAESEC levels has yet to be decided. For the purposes of this specification, it is assumed that the MARSEC levels correspond to the following operational requirements:

MARSEC Level	Requirement
I	Card only (i.e., read of the CHUID only through the contactless interface)
II & III	Card + biometric (this will require that all TWIC readers include a fingerprint sensor; this can be bypassed during MARSEC I conditions).

Table 4.1 MARSEC Requirements

Note: This specification assumes that Personal Identity Numbers (PINs) are not a requirement for authentication at any MARSEC level

4.2 System Perspective

This specification describes two types of devices can be used to verify the user’s TWIC card. They are:

- Fixed Physical Access Control Reader – a TWIC reader installed in a wall, turnstile or similar type installation. It communicates with an external access control system to control a door, gate, turnstile, etc. Fixed readers can operate in indoor environments or in outdoor environments exposed to the weather.
- Portable Verification Device – a handheld device that can be used for portable, spot-check identity verification.

A TWIC card can also be verified using reader devices attached to a personal computer in an office environment for such functions as privilege granting, registration into a physical access control system and for logical access control. This specification only describes readers that will be used for physical access into a facility or vessel.

4.2.1 Physical Access Control

4.2.1.1

The following diagram provides a graphical view of the relationship between the physical access control system (as a whole), the biometric sub-system boundary, and the biometric reader device. Note that this is a generic diagram and that specific implementations may vary from this particular depiction.

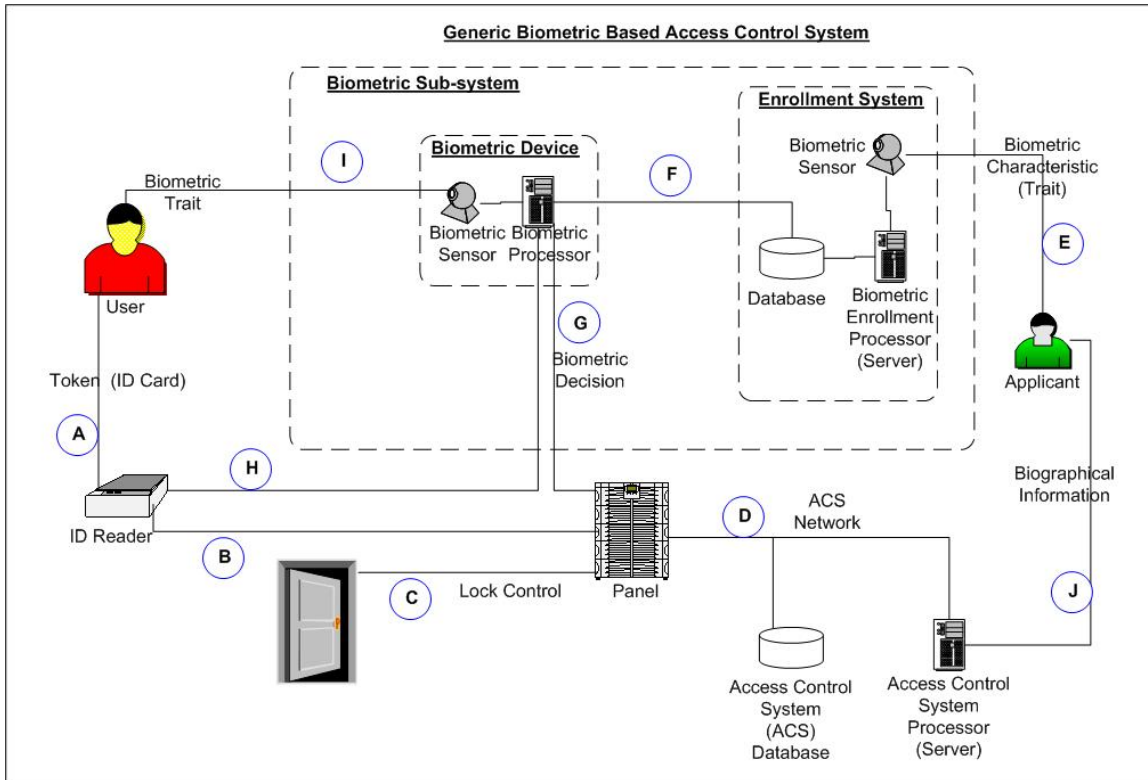


Figure 4.1 Generic Biometric-based Access Control System

Where:

Key	Description
A	Any form of machine-readable credential (TWIC card) presented by the user to the ID reader to claim an identity.
B	User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the panel for the ACS to determine access privilege (part of typical legacy ACS).
C	Electrical signal from the panel used to command the door electromechanical locking mechanisms. This path may also include other signals such as door-open indicators, emergency lock override, etc. (part of typical legacy ACS).
D	(Physically) communication channel (Ethernet, RS485, etc.) enabling data interchange between the panel and ACS processor and database. (Logically) depends on site-specific implementation and includes user identity code from panel and user access authorization from ACS processor.
E	Body part or human behavior presented by the applicant to the biometric sensor during enrollment (e.g., fingerprint, iris, voice, signature). This function may also include interactions between applicant and sensor, i.e., indicator lights, audio cues.
F	Biometric template data from enrollment database to biometric processor for implementations using server- stored templates. (This flow is architecture-specific, may be per user transaction or periodic pre-loads.)
G	Y/N indication (electrical signal or message) from biometric processor to panel conveying the

	result of the user verification transaction.
H	User identity code (ID number, card number, ACS ID) read from the token by the ID reader and sent to the biometric processor as claim of identity (also includes user template data for template on card architectures).
I	Body part or human behavior presented to the biometric sensor during an access transaction (e.g., fingerprint, iris, voice, signature, etc.). This may also include interactions between applicant and sensor such as indicator lights or audio cues.
J	Applicant-supplied information (name, address, etc.) obtained during ACS enrollment via the ACS processor (part of typical legacy ACS).

Table 4.2 Biometric Access System Key Descriptions

Generally a TWIC card will be used at a door or gate that may or may not be manned. The ISO 14443 contactless interface will be used to transfer the unique ID number assigned to the cardholder and the biometric data between the TWIC card and the reader.

4.2.1.2 Physical Access Reader

The physical access reader provides the interface between the user and a physical access control system (PACS). A reader can be either network attached or standalone. A network attached reader⁴ supports two-way communication between the reader and the physical access control system (PACS). A standalone reader is one that has no two-way communications channel available or is connected to a PACS through a one-way communications connection (such as a Wiegand interface).

Assuming a user is enrolled in a physical access system, when a TWIC card is presented the reader must follow these steps:

- Present card to contactless reader
- Reader reads unique ID number from the card and either sends this directly to the PACS when in “card only” mode, or temporarily stores this information for transmission after a successful biometric match when in “card + biometric” mode.
- If the reader is in “card + biometric” mode, the reader obtains the user’s biometric template from the contactless interface on the card.
- User presents their biometric.
- Reader matches the presented biometric to the template read from the card and:
 - a) Reader displays the verification was confirmed or denied.
 - b) Reader signals the physical access control system to grant or deny entry.

4.2.2 Portable Identity Verification

A handheld reader can also be used to verify worker credentials in a portable environment. This can be in conjunction with or as a substitute for the fixed access control readers described above. Smaller terminal installations might not have, nor need, a complete physical access control system. In this case, a portable reader would provide an alternate means of identity verification.

⁴ Note that the term, “Network Attached” here indicates a bi-directional communication path between the reader and the PACS, it is not intended to specify any particular network fabric or protocol.

4.3 Portable Verification

A TWIC card can be interrogated and verified using a portable handheld unit. The interface between the TWIC card and the reader may be via the contact and/or the contactless interface. The mobile device is envisioned to be used in a minimum of two operational modes:

- At a gate control location to interrogate credentials within a vehicle with multiple occupants
- Authorized security personnel performing a random challenge throughout the facility

Access to the biometrics on the card depends on the type of card reader used by the portable device. If the card reader is contactless, the biometric data is read through the contactless interface. If the card reader is contact, the biometric data is read through the contact interface.

5. Fixed Reader Requirements

Beyond these control objectives are electrical and physical interoperability requirements. These are objectives that state the nature of the environment and technologies in place that the fixed reader must interoperate with to be compliant and successful.

The purpose of the fixed reader unit is to provide the physical interface between the TWIC card and the physical access control system controlling access to that portal (turnstile, door, gate, ramp, etc.).

5.1 Physical Requirements

5.1.1 Device Dimensions

There are no specific recommendations regarding device dimensions. For practicality, the biometric device should be reasonably compact and versatile as to mounting in relation to the access point being controlled.

Mountings provided shall be tamper-proof. This means that the reader will have the ability to send an external signal in the event that there is an attempt at unauthorized entry into or removal of the device.

5.1.2 Environmental

5.1.2.1 Outdoor:

The reader shall conform to a NEMA 4 rating.

The reader shall operate within a temperature range of -20°C to +70°C (-4°F to +158°F).

The reader shall operate in a humidity range of 5-100%, condensing.

The reader shall be capable of outdoor operations in direct sunlight and shall neither require nor be affected by ambient light sources.

The reader components may be offered in an enclosing cabinet that achieves the rating required.

The reader may be required to function in a hazardous materials environment. Intrinsically safe readers may be offered to meet this requirement.

5.1.2.2 Indoor

The reader shall operate in a humidity range of 5-90%, non-condensing.

5.1.3 Impact Resistance

Biometric device identification function shall not be degraded by low frequency vibration typical at terminals stemming from sources such as vessel departure/landings, heavy foot traffic, electric carts, large HVAC systems, sub-floor bag conveyors, and outdoor truck traffic. Alternatively, reader manufacturer may base compliance on IEC 60068-2-64 or equivalent commercial practice or analysis.

5.1.3.1 Shock

Reader shall survive a shock event defined by IEC 68-2-27 (1987) using one half-sine pulse with a nominal peak acceleration of 5 g (50m/s^2) and nominal pulse duration of 30 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted.

5.1.3.2 Bump

Reader shall survive 100 bumps defined by IEC 68-2-29 (1987) each with a nominal peak accelerating of 10 g (100 m/s²) and nominal pulse duration of 16 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted.

5.2 Electrical Requirements

The reader shall operate within a range of 8-48 VDC. Where necessary to operate from line voltage, a power supply approved for use with the reader shall be provided. The reader shall optionally support PoE or PoE+ (Power over Ethernet or Power over Ethernet Plus) in accordance with IEEE 802.3af (48VDC/15.4W max) or 802.3at (48 VDC/56W max).

Current requirements shall not exceed 2.0 Amps.

The reader shall provide reverse voltage protection.

The reader shall be FCC certified.

The reader shall return automatically to normal operation after loss of power.

5.3 Safety

The reader shall comply with UL 294, Standard for Safety of Access Control System Units, or internationally recognized equivalent.

The reader shall not possess:

- Sharp corners or edges that can puncture, cut, or tear the skin or clothing or otherwise cause bodily injury. All device corners and edges should have at least a 1mm exposed radius of curvature.
- External wires, connectors, or cables other than the power and data cable.
- Loose coverings and cowlings

5.4 Electromagnetic/Vibration Compatibility

Readers shall comply with the following requirements. For immunity tests the equipments shall operate normally or if operation is interrupted it shall not grant access.

5.4.1 47CFR18 and/or CISPR 11 (Emissions)

5.4.2 IEC 61000-4-2 (Electrostatic Discharge)

Contact Discharge Mode at 2 kV and 4 kV Air Discharge Mode at 2 kV, 4 kV and 8 kV

Assumes 8 to 10 equipment discharge test points plus coupling planes, positive and negative discharge waveform polarities. Performance Criteria B

5.4.3 IEC 61000-4-3 (Radiated RF Immunity)

10 V/meter, 80 MHz to 1 GHz,

Four sides of EUT, 1% steps, 2.8 sec. dwell. AM Mod., 80%, 1 kHz.

Performance Criteria A

5.4.4 IEC 61000-4-4 (Electrical Fast Transient/Burst)

AC and DC Power Ports at 0.5kV, 1kV and 2kV

Signal Lines over 3 meters at 0.25 kV, 0.5kV and 1kV Performance Criteria B

5.4.5 IEC 61000-4-6 (Radio Frequency Common Mode)

10 Vrms, 150 kHz to 80 MHz,

Power ports and signal lines over 3 meters, 1% steps, 2.8 sec. dwell.

Performance Criteria A

5.4.6 IEC 61000-4-5 (Surges)

AC power port at 2kV line to earth, 1kV line to line at 0, 90 and 270 deg.

DC Power Ports at 0.5 kV line to earth, 0.5 kV line to line

Signal Lines over 30 meters at 1 kV line to earth

Positive and negative polarity, 5 surges per mode of appearance. Performance Criteria A

5.4.7 IEC 61000-4-8 (Power Frequency Common Mode)

30 A/m, 50 or 60Hz

Performance Criteria A

5.4.8 IEC 61000-4-11 (Voltage Dips and Interruptions)

30% reduction for 0.5 periods (10 ms), PerformanceCriteria B

60% for 5 periods (100 ms), Performance Criteria C

60% for 50 periods (1 sec), Performance Criteria C

95% for 250 periods (5 sec), Performance Criteria C

6. Portable Reader Requirements

The reader may support a wireless interface to provide direct access to the Physical Access Control System.

The reader shall be capable of confirming whether a TWIC card has been revoked.

6.1 Portable Reader Specific Requirements:

The portable reader shall meet the same specifications as the fixed reader where appropriate with the exception of the following differences:

6.1.1 Operational Features

The portable reader shall have a display suitable for user interaction

The portable reader shall be able to display the current battery level.

The portable reader may use a touch screen or other suitable means for user input/control.

The portable reader should have a hibernation mode for protection against data loss.

6.1.2 Environmental Requirements

A portable reader certified for harsh conditions must meet the following specifications:

- MIL-STD 810F, Method 514.5 – Vibration
- MIL-STD 810F, Method 501.4 – High temperature (to +70°C/+158°F)
- MIL-STD 810F, Method 502.4 – Low temperature (to -10°C/-14°F)
- MIL-STD 810F, Method 507.4 – Humidity
- MIL-STD 810F, Method 503.4 – Temperature shock
- MIL-STD 810F, Method 516.5, Procedure IV (Transit Drop Test) – 26 drops at 4 feet

6.1.3 Electrical Requirements

The portable reader should be supplied with a rechargeable battery with 12 hours minimum operational time.

The portable device shall be operable while charging.

The portable device should have a maximum battery recharge time of 2 hours.

7. Operational Requirements

The contactless reader component shall conform to the ISO14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-1.

The reader shall have a maximum read range of 10cm when used with the contactless card media.

The reader shall require that a card, once read, must be removed from the RF field for one second before it will be read again to prevent multiple reads from a single card presentation.

The reader shall be capable of reading the access control data from the card, performing the necessary authentication steps, and transmitting the credential data as required by the PACS.

The reader shall have communications ports as required by the PACS cable plant and control panels. Minimum options required are:

- Wiegand port for connection to standard access control panels.
- RS-485 or 10/100baseT (Ethernet) for connection to computer systems or access control systems.

The Wiegand output format shall follow that specified for FIPS 201-based systems. The GSA Approved Products Listing test for Federal Employee Personal Identity Verification defines a 75-bit “transparent mode” which includes 2 parity bits and 25 bits for the date. The reader shall output the following 75-bits:

Description	Position	Length
Parity Bit P1	1	1
Agency Code	2-15	14
System Code	16-29	14
Credential Code	30-49	20
Expiration Date	50-74	25
Parity Bit P2	75	1

Table 7.1 75-bit Wiegand Output Format

The reader may also support a 48-bit Wiegand output format when the reader includes a real time clock that can be used to verify the expiration date. In this case, it is assumed that the reader has the ability to process the expiration date. Some PACS control panels may not be able to support both 48-bit and 75-bit Wiegand input at the same time, so the reader must provide a method of setting this as appropriate. The 48-bit Wiegand format is the same as the 75-bit transparent mode but drops the expiration date and the two parity bits as shown below:

Description	Position	Length
Agency Code	1-14	14
System Code	15-28	14
Credential Code	29-48	20

Table 7.2 48-bit Wiegand Output Format

The reader may support other alternate Wiegand formats for legacy systems at a particular location as required.

The reader should clearly and continuously display power status (on, ready or out of service).

The reader may contain additional user indications including lights, text messages, audible indicators, etc.

Reader visual indicators shall be visible in daylight.

The reader should have a finger guide to aid in proper finger placement on the sensor.

For biometrically enabled readers, the fingerprint sensor should be embedded in the same chassis as the reader. If a separate fingerprint sensor module is used, the wiring between the reader and biometric unit must not be exposed.

The reader shall allow for future enhancements to be added in the field. A mechanism should be provided that assures that only authorized/authenticated firmware/software updates are permitted.

The reader shall provide a means to create a log of operations for use in assessing exception conditions such as fingerprint rejections.

The reader shall provide an automated alert or lockout after a configurable number of biometric matching attempts (facility chooses).

The reader may support a means of alerting the PACS/operator if the reader has been tampered with.

The reader shall support a method of changing the MARSEC level (see Appendix B for further details).

8. Performance Requirements

The reader should be capable of achieving a standard maximum transaction time (defined as the time between presentation of the contactless card to reader and completion of the biometric match) of three seconds.

The biometric sub-system should provide an equal error rate (EER) of 1% (1% false rejections at a setting of 1% false acceptance) on a per transaction basis. This assumes up to three attempts as a minimum standard error rate. The reader should provide a mechanism to adjust the security level sensitivity as required.

Any alternatives to use of fingerprint biometrics will be addressed in the local operator's security plans.

Biometric devices may provide liveness detection as a manufacturer's option.

Biometric processes and performance is further described in ANSI/INCITS 383.

It should be noted that biometric interoperability is defined as the ability of a biometric reader to perform a match from a presented biometric with the ANSI/INCITS 378 formatted enrolled templates provided on the TWIC card by the TSA.

9. Operational Availability

The biometric reader shall be able to handle 1 million touches without degradation.

The reader shall be designed to yield a Mean Time Between Failure (MTBF) of 25,000 hours or greater.

10. Delivery

The reader shall include technical manuals covering installation, operation and maintenance of the units. Units will be packaged suitable for shipment to installation point.

11. TWIC Card Application

11.1 Card-application Identifier

TWIC card-application AID		
RID	PIX	State
A0 00 00 0x xx	xx xx xx xx xx xx (See Appendix E)	Default Selected

11.2 Data Model

Buffer Description	Data Object (BER-TLV tag)	Maximum Length	Access Rule	Contact/Contactless	M/O
Transportation Worker Unique Information	0xDFC100 (0x2000)**	32	Always Read	Contact and Contactless	M
Card Holder Fingerprints	0xDFC101 (0x2001)**	896	Always Read	Contact and Contactless	M
Card Holder Unique Identifier	0x5FC102 (0x3000)**	3000	Always Read	Contact and Contactless	M
Security Object	0xDFC10F (0x9000)**	920	Always Read	Contact and Contactless	M

** for Security Object DG mapping use only

Note: All the Data Objects in the TWIC card-application data model are elementary data objects with 3-byte ASN.1 BER-TLV encoded tags. Please be aware that individual tags inside these data objects may not be subjected to follow ASN.1 coding rules in the interest of keeping backward compatibility with PIV data model.

Transportation Worker Unique Information		0xDFC100			
Data Element (TLV)	Tag	M/O	Type	Max Bytes	
FASC-N	0x30	M	Fixed Text	25	
Expiration Date	0x35	M	Date (YYYYMMDD)	8	

Card Holder Unique Identifier		0x5FC102			
Data Element (TLV)	Tag	M/O	Type	Max Bytes	
FASC-N	0x30	M	Fixed Text	25	
GUID	0x34	M	Fixed Numeric	16	

Expiration Date	0x35	M	Date (YYYYMMDD)	8
Issuer Asymmetric Signature	0x3E	M	Variable	2816
Error Detection Code	0xFE	M	LRC	0

Card Holder Fingerprints		0xDFC101		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Fingerprint template (2 fingers)	0xBC	M	Fixed	862

Security Object		0xDFC10F		
Data Element (TLV)	Tag	M/O	Type	Max Bytes
Mapping of DG to Data Objects	0xBA	M	Variable	10
Security Object	0xBB	M	Variable	900
Error Detection Code	0xFE	M	LRC	0

Note: The security object is in accordance with Appendix C.2 of PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1. [8] Tag “0xBA” is used to map the Data Objects in the TWIC data model to the 16 Data Groups specified in the Machine Readable Travel Document (MRTD). This enables the security object to be fully compliant for future activities with identity documents.

The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object. The signature field of the security object shall omit the issuer's certificate, since it is included in the CHUID. Card Issuer's Digital Signature is in accordance with FIPS 201-1.

The calculation of hashes of the individual data, which are then to be used for creation of Security Object shall be based on the contents of Data Objects as stored in the TWIC card-application.

11.3 TWIC card-application command set:

- SELECT
- Get Data

11.3.1 SELECT card command

Command Syntax

CLA	'00'
INS	'A4'
P1	'04'
P2	'00'
Lc	'0B'
Data Field	TWIC AID (= TWIC RID TWIC PIX)
Le	Length of TWIC card-application property template

Card-application Property Template

Upon selection, the TWIC card-application shall return the application property template described below.

Application identifier of application	'4F'	M	The PIX of the AID includes the encoding of the version of the TWIC card-application.
---------------------------------------	------	---	---

Coexistent tag allocation authority	'79'	M	Coexistent tag allocation authority template. See Sec 3.1.
-------------------------------------	------	---	--

Table 11.1 Data Objects in the TWIC Card-application Property Template (Tag '61')

Response Syntax

Data Field	Card-application property template
SW1-SW2	Status Word

SW1	SW2	Description
'6A'	'82'	Card-Application not found
'90'	'00'	Successful execution

11.3.2 GET DATA card command**Command Syntax**

CLA	'00'
INS	'CB'
P1	'3F'
P2	'FF'
Lc	'05'
Data Field	'See table A
Le	Number of data content bytes to be retrieved

Table A: Data Field

Name	Tag	M/O	Comment
Tag List	5C	M	BER-TLV tag of the data object to be retrieved in clear

Response Syntax

Data Field	BER-TLV with the tag '53' containing in the value field the requested data object
SW1-SW2	Status Word

SW1	SW2	Description
'61'	'XX'	Successful execution where SW2 encodes the number of response data bytes still available
'69'	'82'	Security status not satisfied
'6A'	'82'	Data Object not found
'90'	'00'	Successful execution

03 55 04 03 13 08 46 41 53 43 4E 20 43 41 30 1E 17 0D 30 35 30 35 32 37 31 34 35 37 32 30
5A 17 0D 31 35 30 38 31 39 31 34 35 37 32 30 5A 30 2F 31 0B 30 09 06 03 55 04 06 13 02 55
53 31 0D 30 0B 06 03 55 04 0A 13 04 4E 49 53 54 31 11 30 0F 06 03 55 04 03 13 08 46 41 53
43 4E 20 43 41 30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 81 89
02 81 81 00 91 CF 6E F0 4D D3 F2 EB 46 1E B9 1B A4 25 47 E4 88 8D E6 89 85 A8 E5 86 E7
E8 9D EA 62 7B 73 74 7B 89 55 13 82 B6 45 53 99 F2 36 72 6A 48 7A 59 ED C8 F0 70 3C 04
2C 33 AD 21 0C 32 00 BD F1 F4 F1 FA 9B 02 CB 3F AA 7B 89 C1 A4 D0 D4 C8 29 94 7A B0
E2 3E 69 C6 3C 71 43 DF A6 1D 55 18 21 CC AE 40 E3 CD 89 E2 62 A2 10 68 67 3B 56 24
4E C1 43 ED A4 48 64 73 E4 78 4C 0B 0E 69 6A 30 61 11 02 03 01 00 01 A3 81 C2 30 81 BF
30 1D 06 03 55 1D 0E 04 16 04 14 D6 42 7A 0E A3 07 B0 FC 23 93 B4 4D 9C F6 8B 22 C8 0F
89 40 30 0E 06 03 55 1D 0F 01 01 FF 04 04 03 02 01 06 30 0F 06 03 55 1D 13 01 01 FF 04 05
30 03 01 01 FF 30 7D 06 08 2B 06 01 05 05 07 01 0B 04 71 30 6F 30 6D 06 08 2B 06 01 05 05
07 30 05 86 61 6C 64 61 70 3A 2F 2F 77 77 77 2E 65 78 61 6D 70 6C 65 2E 63 6F 6D 2F 63 6E
3D 46 41 53 43 4E 25 32 30 43 41 2C 6F 3D 4E 49 53 54 2C 63 3D 55 53 3F 63 41 43 65 72 74
69 66 69 63 61 74 65 3B 62 69 6E 61 72 79 2C 63 72 6F 73 73 43 65 72 74 69 66 69 63 61 74
65 50 61 69 72 3B 62 69 6E 61 72 79 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 03 81 81
00 21 EE F6 02 D8 A0 CD E5 A7 34 F9 87 ED B8 76 D5 AC D2 A3 0A F7 EF 36 83 3E 67 6F
E2 42 B3 34 92 46 C1 F5 5A 80 05 22 FF 97 66 25 02 0D 21 02 6A B7 BD 49 CB 95 5E 8F C7
82 6A 2A A9 CD 03 35 4D F5 7C CA 4C EB 0B 61 DB 8F 9E C2 D6 7C 80 41 79 5F 5D 28 25
4C 8E 33 72 20 B1 6B A2 18 5F 25 95 B6 8C 2C 6E 07 78 C9 32 15 35 28 A9 46 B1 28 68 7F
08 14 12 C7 4A 1A B2 5F ED 34 57 22 6B A5 08 31 82 01 78 30 82 01 74 02 01 01 30 34 30 2F
31 0B 30 09 06 03 55 04 06 13 02 55 53 31 0D 30 0B 06 03 55 04 0A 13 04 4E 49 53 54 31 11
30 0F 06 03 55 04 03 13 08 46 41 53 43 4E 20 43 41 02 01 01 30 09 06 05 2B 0E 03 02 1A 05
00 A0 81 9B 30 17 06 09 2A 86 48 86 F7 0D 01 09 03 31 0A 06 08 60 86 48 01 65 03 06 01 30
1C 06 09 2A 86 48 86 F7 0D 01 09 05 31 0F 17 0D 30 37 30 32 31 36 30 32 34 37 35 34 5A 30
23 06 09 2A 86 48 86 F7 0D 01 09 04 31 16 04 14 C2 B8 30 EC 7F AE 26 92 CD B4 B7 CD 39
84 DA 5B 8F 1E F4 22 30 3D 06 08 60 86 48 01 65 03 06 05 31 31 30 2F 31 0D 30 0B 06 03 55
04 0A 13 04 4E 49 53 54 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 11 30 0F 06 03 55 04 03
13 08 46 41 53 43 4E 20 43 41 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 04 81 80 16 A7
B9 DC 8A 37 1F 50 A6 25 7C 6E 84 A9 C4 28 57 68 C4 83 D0 C1 39 63 DE E8 CE 40 3C FB
17 A9 6C B1 8B 93 16 2E 0B 27 0C 11 B7 BF E0 EE 73 CC C6 8F F6 91 B7 3A 08 EC 56 BB
D2 1F 34 DD 1A B4 A3 5D DB 51 DB E6 CC 18 3D DA BF 80 09 8D E2 C8 79 05 97 B0 B1
C5 B4 D3 95 13 DE 95 B8 BE 24 6C 2F 0F DC B2 A4 41 EE 6E 33 22 71 6B A5 CD 93 59 76
B9 87 AF 33 89 D4 13 7A C8 CE 28 1B 45 41 E5 FE 00

11.4.3 Cardholder Fingerprints Data Object (0xDFC101)

BC 82 02 A0 03 0D 00 00 02 48 00 00 00 1B 02 01 14 06 01 05 0E 1D 00 5A 14 06 04 0A 0D
30 25 5A 14 0B 04 0A 0D 30 25 5A 00 00 08 80 FE 4E 49 53 54 20 43 72 65 61 74 6F 72 00 00
00 00 00 00 D4 32 48 58 21 0C 2D 31 71 B5 25 A1 68 5A 08 C9 2A DE 0A 61 84 32 48 43 E2
00 00 00 00 46 4D 52 00 20 32 30 00 02 48 00 00 00 00 00 02 00 01 E0 00 C5 00 C5 02 00
07 00 32 29 41 35 00 51 04 00 41 21 00 7A 04 00 40 C2 00 7B 6D 00 41 3C 00 80 5B 00 41 2D
00 90 01 00 80 D1 00 A5 0B 00 41 6B 00 B0 4D 00 41 21 00 BF 62 00 40 EB 00 C6 10 00 40
FB 00 DF 0B 00 41 33 00 E5 AD 00 40 A8 00 E8 73 00 81 57 00 EB 98 00 81 00 00 F1 07 00
81 16 00 F2 62 00 81 4C 00 F3 4C 00 41 20 00 F7 68 00 41 02 00 F9 6B 00 81 43 00 FD 56 00
81 68 01 09 A3 00 81 7C 01 0F 49 00 80 B8 01 2F 1D 00 40 9E 01 49 1D 00 41 25 01 51 82 00
80 A9 01 53 66 00 80 9C 01 54 6B 00 80 C0 01 5B 1A 00 41 3B 01 61 9C 00 81 12 01 69 22 00

41 14 01 76 1A 00 41 27 01 79 AC 00 80 B3 01 7F 12 00 81 3B 01 82 53 00 81 65 01 86 4C 00
80 E1 01 90 11 00 80 E0 01 9E 0B 00 41 65 01 A5 51 00 40 C3 01 B0 08 00 40 F6 01 BB 04 00
80 EC 01 C7 01 00 41 38 01 C8 58 00 00 02 10 32 32 41 31 00 15 A4 00 80 EF 00 1F AD 00
41 3C 00 39 4A 00 41 56 00 39 47 00 81 01 00 40 AD 00 81 17 00 4D 51 00 41 4B 00 4D 9C 00
41 59 00 64 44 00 81 4F 00 70 9E 00 40 BA 00 81 06 00 80 AE 00 8A 04 00 80 B1 00 97 5A 00
41 6A 00 9A 41 00 41 19 00 A1 4C 00 81 41 00 A5 9D 00 40 A3 00 AD 02 00 40 B5 00 B9 68
00 41 46 00 BA 42 00 40 B2 00 C1 0B 00 40 E3 00 C7 01 00 40 C9 00 C9 0B 00 40 A7 00 D3
06 00 81 03 01 0D 9B 00 80 FA 01 1B 3F 00 81 30 01 1F 79 00 41 11 01 2B 1D 00 81 1D 01 2F
1A 00 41 41 01 31 36 00 81 2D 01 35 0F 00 81 3F 01 3A 59 00 81 1E 01 3F 09 00 81 43 01 46
5A 00 81 32 01 4B 00 00 40 FF 01 4F 0F 00 41 61 01 52 A1 00 81 4D 01 57 A8 00 81 1D 01 59
62 00 41 7E 01 5A 44 00 41 66 01 5D 4C 00 41 69 01 5E 9B 00 80 CB 01 61 0F 00 81 00 01 63
0A 00 81 5F 01 67 4D 00 81 2B 01 6E 5F 00 80 C0 01 79 0E 00 81 7F 01 7A 45 00 81 70 01 81
4D 00 81 35 01 87 62 00 81 18 01 98 05 00 81 2A 01 9B 5E 00 00 00

11.4.4 Security Object Data Object (0xDFC10F)

BA 0C 01 20 00 02 20 01 03 30 00 04 20 03 BB 82 02 15 30 82 02 11 06 09 2A 86 48 86 F7 0D
01 07 02 A0 82 02 02 30 82 01 FE 02 01 03 31 0B 30 09 06 05 2B 0E 03 02 1A 05 00 30 81 B1
06 06 67 81 08 01 01 01 A0 81 A6 04 81 A3 30 81 A0 02 01 00 30 09 06 05 2B 0E 03 02 1A 05
00 30 81 8F 30 19 02 01 01 04 14 1D 63 83 1D CF 5C 23 EB B6 76 B9 9C 48 57 87 C4 44 6D
C3 EC 30 19 02 01 02 04 14 AC 5A EB 84 03 8C 39 03 5A 0A D2 0B 6C 75 68 0B 95 EC 23 52
30 19 02 01 03 04 14 D0 CF D0 B6 5B 72 CD 99 55 24 A1 DF 3E D5 34 3C 3F A8 E2 3130 19
02 01 04 04 14 AD C6 BD B6 40 BD D7 ED 17 81 16 59 19 A2 08 D9 0F 57 B6 98 30 05 02 01
06 04 00 30 05 02 01 07 04 00 30 05 02 01 08 04 00 30 05 02 01 09 04 00 30 05 02 01 0A 04 00
31 82 01 36 30 82 01 32 02 01 01 30 34 30 2F 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 0D 30
0B 06 03 55 04 0A 13 04 4E 49 53 54 31 11 30 0F 06 03 55 04 03 13 08 46 41 53 43 4E 20 43
41 02 01 01 30 09 06 05 2B 0E 03 02 1A 05 00 A0 5A 30 15 06 09 2A 86 48 86 F7 0D 01 09 03
31 08 06 06 67 81 08 01 01 01 30 1C 06 09 2A 86 48 86 F7 0D 01 09 05 31 0F 17 0D 30 37 30
32 31 36 30 33 30 33 33 38 5A 30 23 06 09 2A 86 48 86 F7 0D 01 09 04 31 16 04 14 C9 7C 5E
9C 3D 5C A5 9D AA 8B 9B D0 0A F3 E1 7F 8C F3 14 B5 30 0D 06 09 2A 86 48 86 F7 0D 01
01 01 05 00 04 81 80 21 CB 42 CA 32 AE E1 46 2D CC 37 B6 F2 1C 84 91 AB CB B2 44 43
3E EC 5F 8F 88 01 21 01 95 C5 C4 0B AD EB B1 00 EB 2C 3A 84 85 29 FF 71 36 E7 91 60 2B
82 41 C1 96 83 4C BD 53 D5 74 DA A3 C6 3C 4E 92 B9 27 E3 28 FB 56 BC E3 CA B8 7D 49
C2 46 6E 7D 4A 52 75 B1 EA 26 FD AB F0 9C 57 12 01 7F 2C C7 AD AA 32 62 C0 CB 43 57
9F 3F 34 32 6C E6 13 5B 0C AD 7C A9 2B A1 8A 5D E5 29 27 B8 4B C7 FE 00

Appendix A Authentication Processing

In order to determine the **identity** of a cardholder, an access control system must check one or more **authentication factors**. The overall assurance of the authentication process is determined by the number and quality of each authentication factor used. These factors are typically divided into three categories:

Something you have:	E.g. a badge, a metal key or a smart card
Something you know:	E.g. a PIN or a password
Something you are:	E.g. your fingerprint, your iris or your voice

A check against an authentication factor is considered “strong” if it would be hard for an attacker to compromise. An access control system may achieve the required level of authentication security by checking factors against either the card or its own database.

The proposed TWIC card itself offers three different authentication factors that may be used via the contactless interface of the card:

1. CHUID data object – weak “something you have” authentication factor
2. TWIC biometric template – strong “something you are” authentication factor
3. PIV Card Authentication Certificate and Key – strong “something you have” authentication factor

This appendix describes the process that would be required to authenticate one or more of these factors against the card. An access control system could choose to supplement or replace these with off-card authentication information in a database if desired. For example, a PIN could be stored in the access control system and compared on entry, even though the card does not support this capability internally. However, these off-card authentication checks are outside the scope of this document.

A.1 CHUID Authentication

The CHUID is a freely readable data object that is digitally signed (to prevent forgery of the data itself), but is neither encrypted nor strongly bound to the physical card. The signed object contains the unique FASC-N identifier, which should be used as the primary identification number for the card.

In order to check the CHUID authentication factor from a TWIC card, an access control system may perform the following steps.

- 1) The reader selects card’s TWIC applet
- 2) The reader selects CHUID object.
- 3) The reader gets the contents of the CHUID data object.
- 4) The reader searches the CHUID object to find the FASC-N tagged (0x30) value.
- 5) The reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number. The reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or all or part of selected elements of the FASC-N.
- 6) The reader may decode the Issuer Asymmetric Signature Object (tag: 0x3E) from the CHUID in order to retrieve the certificate for the document signer that is used to verify the signed objects on the card.

The CHUID authentication factor has the advantage of being relatively simple and quick to retrieve. This factor is considered relatively weak, since it would be very easy to copy a CHUID from a valid card and then copy it to a cloned or emulated card. This copy could be done without possession of the card by getting near a cardholder with a contactless reader.

A.2 TWIC Biometric Authentication

The TWIC contains a pair of fingerprint biometrics bound to the cardholder's FASC-N identifier via the digital signature of the card issuer. The signed fingerprint templates are not encrypted and are free read from the contactless interface.

In order to confirm that the cardholder matches the stored biometrics, the data must be retrieved and then matched against a live finger.

- 1) The reader selects the card's TWIC applet
- 2) The reader selects the fingerprint object.
- 3) The reader gets the contents of the fingerprint data object.
- 4) The fingerprint template TLV (tag: 0xBC) is retrieved from the fingerprint data object.
- 5) The CBEFF template is parsed into the ANSI/INCITS 378-2004 fingerprint body, FASC-N and the digital signature.
- 6) The reader verifies that the digital signature on the CBEFF was produced by an authorized document signer. This requires that the reader have a verified copy of the document signer's X.509 digital certificate. The public key from this verified document signing cert must verify the signed biometric data. There are two options for the reader to obtain the document signing certificate for the card.
 - a) The reader could retrieve the document signer's certificate from the CHUID signature field, since the CHUID must be signed by the same entity as the biometric. The reader must verify that the CHUID signing certificate from the card was signed by one of the trusted card issuing Certificate Authorities from the TSA or another locally trusted issuer. The CHUID signing certificate must also be verified for expiration, and the certificate must contain the id-PIV-content-signing keyPurposeID extendedKeyUsage extension.
 - b) The reader could be locally configured with a copy of every trusted document signing certificate. This may improve performance, since the certificate does not need to be retrieved from the card, but may increase the local management burden as document signing certificates are added and removed.
- 7) An index finger is sampled from the cardholder. This image must be matched against one of the fingerprint templates stored in the signed biometric object at an appropriate level of confidence (see section 8). If the fingerprint does not match the template on the first attempt, the reader may prompt for subsequent attempts without requiring the card to be re-read.
- 8) If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object can be used as the identification number. This value must match the FASC-N from any other authentication factors that are matched to know that they are bound together by the card issuer.

A.3 Card Authentication Key Authentication

In addition to a TWIC application, every TWIC card also contains a separate application with its own application identifier (AID) that conforms to the Personal Identity Verification (PIV) specification as referenced in the NIST FIPS 201-1 standard and its associated special publications. The PIV-like applet includes a Card Authentication Key and Certificate that can be used from the contactless interface for the purpose of authenticating that the card was issued by a trusted authority and not cloned or faked. This provides a tool that strongly binds the cardholder's identity (via the FASC-N) to the physical card token by embedding a piece of secret data in the chip that cannot be copied via any interface. This key data can be used in conjunction with the freely readable certificate to prove that the card has not been cloned or spoofed.

This process requires that a credential presented to the system must be capable of performing an asymmetric Private Key operation such as RSA signature generation. This requires that the token be issued with the optional Card Authentication Key and Certificate as specified in NIST SP 800-73. The certificate profile standardizing the contents of the Card Authentication Certificate is documented by the Federal Identity Credentialing Committee's Shared Service Provider subcommittee.

Note that, unlike the Certificate/Key containers used exclusively on the contact interface of the FIPS-201 credential, the Card Authentication Certificate does not require or support a PIN to unlock for usage. This means that the contactless FIPS-201 card only internally represents a strong single factor (possession), and any additional authentication factors (PIN, biometric) would need to be managed externally to the card itself. To support local (on-card) second and third factor authentication with a FIPS-201 PKI credential, the contact interface of the card must be used.

The reader (or panel, with bi-directional wiring) must be locally configured with the public keys (or, more typically, a full X.509 certificate containing the public keys) for one or more Certificate Authorities that are trusted for issuance of TWIC Card Authentication Certificates. This could be limited to the issuing CAs for the TSA, or could include external CAs from other agencies to authenticate federated identities. This would likely be the same set of trusted CAs that must be stored on the reader in order to authenticate the CHUID signing certificate on a card, as required for biometric verification. The cryptographic operations performed by the reader (e.g., RSA signature verification) would be of the same type as those required by the biometric verification, so would require an equivalent level of computing resources at the reader (e.g. a 32 bit embedded processor or cryptographic coprocessor).

The public key information in the reader is not treated as a secret or sensitive data, so extraction of this data from a reader would not create a security risk, but incorrect configuration of a reader with illegitimate Authority Keys could result in that reader accepting the authenticity of an illegitimate token.

The reader (or bi-directional panel) would also need to have access to a system clock capable of providing the current date and time in order to determine the expiration status of the credential.

The output of the reader upon successful authentication would depend on the infrastructure capabilities and requirements. At a minimum, the reader could produce the encoded FASC-N for the card, which is pulled from the Card Authentication Certificate. Alternately, the entire verified Card Authentication Certificate could be passed to the access control system for more advanced processing.

- 1) The reader selects the PIV Applet
- 2) The reader selects the Card Authentication container (Container ID 0x0500).
- 3) The reader retrieves the binary contents of the Certificate value (tag: 0x70).
- 4) The reader retrieves the content of the CertInfo value (tag: 0x71).
- 5) If the least significant bit of the CertInfo value is '1', then the contents of the Certificate value are compressed using the "gzip" algorithm, and are decompressed by the reader to produce the raw DER-encoded X.509 certificate. Otherwise, the contents of the Certificate value can be used without decompression.
- 6) The "issuer" name in the Certificate is compared against the "subject" name in each trusted issuing CA certificate stored on the reader. For each CA with a matching name, the Public Key is used to attempt to verify the signature on the token's Certificate. If no matching CA certificate is found on the reader with the same name and with a Public Key that verifies the signature on the certificate, then the Certificate is rejected.
- 7) If the date encoded in the Certificate's "notBefore" validity date is after the current date/time, or if the Certificate's "notAfter" validity date is before the current date/time, the Certificate is rejected.
- 8) If the Certificate's "keyUsage" extension does not contain the "digitalSignature" flag, the Certificate is rejected.
- 9) If the Certificate's "extendedKeyUsage" extension does not contain the "id-PIV-cardAuth" keyPurposeID (2.16.840.1.101.3.6.8), the Certificate is rejected.
- 10) If the Certificate's "subjectAltName" extension is present, with the "pivFASC-N" name entry, this value shall be retrieved from the certificate for optional transmission to a panel or back-end (e.g. IdMS infrastructure).
- 11) If the Certificate contains any unknown extensions with the Criticality flag set to TRUE, the Certificate is rejected.
- 12) The reader generates a random or pseudo-random challenge of at least 127 bytes of unique data and transmits this to the container's GENERAL AUTHENTICATE command.
- 13) The response (i.e. the card's signature) from the GENERAL AUTHENTICATE command is verified using the Public Key from the Certificate. If verification fails, the card is rejected.
- 14) If verification has succeeded, the Certificate is accepted as an assurance factor. Identifying information (e.g. the Certificate, the FASC-N, or other unique identifying components) may be immediately used locally or at a panel as input for the access control rules, or supplemental second and third factors (e.g. PIN, biometric) may be independently evaluated.
- 15) If the biometric authentication factor was also verified, then FASC-N identifier from the biometric must be identical to the FASC-N contained within the Card Authentication Certificate. If they do not match, then the biometric and card does not belong together, so one must be rejected.

Appendix B MARSEC Level Processing

The reader needs to support multi-mode operation and be able to accept external triggers for the mode change. A mode change would apply to applications such as a threat level change (e.g., maritime security or MARSEC levels). The reader would need to be capable of various modes whether currently defined by the Coast Guard or not. Also, it is anticipated that TWIC will be expanded to all transportation modes in the future. Therefore, readers should be capable of supporting multiple authentication factors as may be required.

Appendix C TWIC Reader Compatibility With Other Card Types

It is important to recognize those situations where a TWIC reader may be required to read multiple card types such as Department of Defense Common Access Cards (CACs) and Federal Personal Identity Verification (PIV) cards as well as TWIC cards. In such an environment, a reader should be capable of discovering the application identifier (AID) associated with these different card types and then behaving according to the requirements of that card type. For a card that might have multiple card types, the TWIC reader should default to the TWIC AID.

Appendix D Description of Concept for Operational Biometrics

An alternative implementation is available that avoids the 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 that have 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 biometric template on the TWIC card is also read. The 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.

Appendix E Proposed TWIC AID Structure

This section presents how the TWIC Application Identifier is defined and how it should be used in the TWIC applications developed in readers and terminals.

The AID used for the TWIC application will consist of a 5 bytes RID and a 6 bytes long PIX.

RID Current Status:

TSA has applied for a Registered Identifier (RID) according to ISO/IEC 7816-5 which will be communicated to the group as soon as it is available. This RID is, for the time being, represented by the string "A0 00 00 0x xx" in this document. It is also called the TSA RID.

In the mean time, until the final TSA RID is known, the following temporary RID can be used for tests: 'F0 54 57 49 43' (The value 'Fx' indicates a non registered value for the RID and last four bytes are ACSII for 'TWIC').

PIX Structure:

All TSA applications using the RID "A0 00 00 0x xx" will have a similar structure.

The first two bytes of the PIX are used to define the group to which the application belongs. The values '00 00' and 'FF FF' are not defined for now and reserved. The following group values are defined:

- applications used by TSA employees or contractors: group = '10 00'
- applications used by non TSA employees or contractors: group = '20 00'

The following two bytes of the PIX are used to identify the application within a group. The values '00 00' and 'FF FF' are not defined for now and reserved. The following applications are allocated:

Group '20 00'

- TWIC application number '00 01'

The following byte of the PIX is used to identify the release of the specification as well as the nature of the card. If the first most right bit of this byte is set to one ('1') it indicates the card is a test card. If the rightmost bit is set to zero it is a normal application card. This allows the terminal to set itself in diagnostic mode and execute some more testing/diagnostic functions (when not disabled) when a test card is presented. The current release is defined as release '1'.

The following and last byte of the PIX is used by the card to indicate the version of the specification. The values '00' and 'FF' are so far reserved for future use and not defined. The current TWIC card specification is version '01'.

Bytes of the AID	Symbol	Value	Comment
1 to 5	RID	A0 00 00 0x xx	TSA RID
		F0 54 57 49 43	Temporary TSA RID for test purpose
6 & 7	Grp	00 00 & FF FF	Reserved values
		10 00	TSA employees & contractor group
		20 00	non TSA employees or contractors group

8 & 9	App	00 00 & FF FF	Reserved values
		00 01	TWIC application in group 20 00
10	Release	00 & 7F	Reserved values
		1xxx xxxx	If bit on indicates test card
		01 & 81	TWIC specification release 1
11	Version	00 & FF	Reserved values
		01	TWIC application version 01

The current possible AIDs for a TWIC card are:

A0 00 00 0x xx 20 00 00 01 01 01	Normal TWIC Card
A0 00 00 0x xx 20 00 00 01 81 01	Test TWIC card
F0 54 57 49 43 20 00 00 01 01 01	Temporary AID TWIC Card
F0 54 57 49 43 20 00 00 01 81 01	Temporary AID Test TWIC card

Only one TWIC AID (using the same RID) per card will ever exist but a given card may have a different TWIC application version than another card.

Application cards issued for normal use should not use the temporary RID.

Note: The terminal looking for the TWIC application should use a partial select command and ask for the partial AID on the first 9 bytes.

The card will respond with the full AID of the TWIC application it has (including release and version as well as the test bit indicator) and the terminal will have to verify it can work with the version in the card. Specifications expect to be upward compatible.

In case a new TWIC application specification cannot be made upward compatible, (thus creating a potential problem for existing terminals) a new application will have to be used (App bytes of the PIX)

