

National Maritime Security Advisory Committee

TWIC Working Group

Maritime Operating Requirements

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.

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 strongly 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 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?*

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.

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:

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

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:

- a) Identity matching error rates (expressed as “false accept” and “false reject” error rates)
- b) Enrollment failures (expressed as “failure to enroll” errors)
- c) 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.