

Coast Guard (CG) / Transportation Security Administration (TSA)

Transportation Worker Identification Credential (TWIC)
Reader Hardware and Card Application Specification / Pilot Program
Meeting and Teleconference Summary

19 November 2007 1:00 ET

Registered Teleconference Participants

Al Perkins
Beth Rooney
Bill Eglinton
Bill Erny
Boyd Stephenson
Brad Jenson
Brian Conaway
Brook Doty
Carla J. Stewart
Catherine Cross
Colin Soutar
Craig Hill
Dale Kers
Dan O'Brien
Dave Maresh
Director of Security
Earl Agron
Eleanor Morton, Esq.
Eric Widlitz
Frances Zelazny
Geri Castaldo
Guillermo (Willie) Pacheco
Jack McClure
Jane Jordan
Jay Jones
Jeff Larson
Jeff Peters
Jerry Wright
Joe Porthouse
John Douglass & Bob Samuel
Kate McNamara
Ken Fleming
Kevin Steeprow
Len Gliatta
Lindsay McLaughlin
Lisa Hember
Martin Ouellet

Matt Shannon
Meredith Romley
Michael Kelley
Mike McMullen
Pat Hemphill
Patrick McIntyre
Peter Weaver
Poli Luis
Richard A. Hilinski
RJ Lyerly
Rob Zivney
Robert Brown
Rod Hilden
Ryan Zlockie
Steve Rummel
Sue Dernik
Teresa Wu
Thomas G. Schroeter
Timothy Bentley
Tom Pettit
Vincent Lamaestra
Walter Hamilton

Registered Attendees

Admiral Rudy K. Peschel
Adrienne Gregory
Alexandra Lemieux
Aliya Sternstein
Andrew Howell
Andrew O. Omidvar
Andrew Webb
Bert Coursey
Bob Gilson
Brian Beideman
Catherine J. Tilton
Charles Diorio
Chenchen Yuan
Cheryl Instad
Cheryle Ingstad
Consuelo Bangs
Cresence Stafford
Daniel Schleifer
David Belchick
Denise Krepp
Dominic Ingerto
Edward Langhoff

Frank Recknagel
Gena Alexa
Gregory McConnell
H. Elizabeth Wenchel
James B. Briley, Jr.
James Duncan Campbell III
Jeffrey Lynn
Jim Lyons
Joe Coccia
Joe Ryder
Kristen Taylor
LT Andrew Pate
Lynn Klar
Mark Sandvigen
Martian Janiak
Mary McCarthy
Megan Fogel
Megan Fogel
Michael Huffman
Mike Zerchen
Monty Willaford
Prabhat Agarwal
Randy Vanderhoof
Robby Moss
Robert Green
Robert Martin
Roger Morrison
Roger Roehr
Scott Glover
Scott Schneiderman
Sterling Marchand
Steve Parsons
Steve Warker
Steven Lowry
Thomas P. Marian
Tim Perry
Tom Corder
Tom Gitchel
Tony Damalas

Welcome

CAPT Mark O'Malley, Office of Port & Facility Activities, USCG

By the end of this week, 16 enrollments centers will be open throughout the country. Enrollment is going smoothly overall; enrollment time is averaging approximately 10

minutes. We appreciate you attending this session because we are looking forward to the next step: readers for the cards and, in conjunction, the pilot program.

Intentions

CDR Pete Gautier – CG Program Manager for TWIC

This is intended to be a forum for a free exchange of information between the smartcard and security industry, TSA, and the CG. We plan to discuss the TWIC version 2 Reader Specification, the pilot program, specifically the Test and Evaluation Master Plan (TEMP), envisioned test scenarios, and also provide ample time for questions and answers from participants. This meeting/teleconference is not intended to discuss the TWIC reader requirement rule-making. We are also restricted from discussing any future Request for Quotation (RFQ) concerning CG handheld readers. We will talk about the past CG handheld reader Request for Information (RFI) & RFQ.

Security and Accountability for Every (SAFE) Port Act Requirement Overview

John Schwartz – TSA Assistant Program Manager for TWIC

SAFE Port Act Presentation <http://homeport.uscg.mil>

CG Handheld Reader Requirement

LCDR Jon Maiorine – Security Standards Branch, Cargo & Facility Division, USCG

Once compliance is required under the initial TWIC Final Rule, the CG will need the capability to check TWICs using handheld readers during facility and vessel security exams. A RFI was issued on June 15, 2007 and closed on June 22, 2007 outlining CG requirements for handheld readers. Valuable and significant suggestions were received and some potential vendors identified through the RFI. A RFQ was released on September 10, 2007 and cancelled on September 11, 2007. The cancelled RFQ contained CG requirements for handheld readers including the ability to determine TWIC authenticity, conduct validity and identity verification in both the contact and contactless mode in the maritime environment, link to the TSA managed hotlist, and operate independently from a laptop or external computer with the exception of removal media, such as a thumb drive. The cancelled RFQ also identified training, service, and support requirements. A new RFQ for handheld readers will be posted in early Calendar Year 2008. The CG's requirement to check TWICs has not diminished.

Card Application & Reader Specification Overview

Gerry Smith – Senior Consultant ID Technology Partners – Technical Contract for TSA and TWIC Program

Card Application and Reader Specifications Presentation

<http://homeport.uscg.mil>

TEMP Overview

Richard Kaye – Space and Naval Warfare (SPAWAR) Systems Center – Independent Test Agent for TWIC Program

TWIC Pilot Overview Presentation <http://homeport.uscg.mil>

Guidance for TWIC Reader Pilot Program / Test Scenarios
CDR Pete Gautier

TWIC Vendor Day Scenarios Presentation <http://homeport.uscg.mil>

Question & Answer Period
LT Brooke Grant – Moderator

Q: What is the process for individuals who are unable to have their biometrics captured?

A: There is a sequence that the enrollment software goes through to identify the quality of fingerprints being captured; hopefully the software is able to find at least two viable fingers for an operational biometric to put onto the card. In an instance where it is impossible to get a biometric, a card may still be issued. Once readers are in place, a requirement and alternate process must be identified so that individuals without a quality biometric may still have access to secure areas. That process and/or requirements have yet to be determined.

Q: What is the process to obtain test cards?

A: We recognize vendors are interested in test cards. We do not have test cards at this time. We are working on a identifying a fair and equitable process to develop and distribute test cards. It is appropriate and possible for vendors to obtain TWIC cards through the enrollment centers.

Q: Is it understood or anticipated that various perimeters will be drawn and used incorporating TWIC within sections of facilities?

A: Currently the entire Maritime Transportation Security Act (MTSA) footprint, as approved in a facility's security plan, is viewed as the secure area – the area over which a facility exerts access control. There is an exception written into the rule so that facilities with a significant non-maritime transportation portion may redefine their secure area through their security plan to exclude those portions with a significant non-maritime transportation function. A facility owner/operator may chose to draw additional perimeters within their MTSA footprint and exert various levels of access control in addition to those mandated by regulation.

Q: What is the relationship between the initial technical testing by SPAWAR and the testing scenarios described by the CG?

A: The initial technical testing and the operational scenario based testing are two different phases. The initial technical testing proves the reader can perform to technical specifications. After that the reader is tested on its performance in operational situation. TSA anticipates having a list of equipment, readers and other associated equipment, that will have gone through technical testing. The technical testing includes how the equipment functions and makes the appropriate checks, whether it reads the TWIC appropriately, in addition to how it responds to various conditions through environmental testing to the specification. Pilot test participants will be responsible to make a determination based on the TWIC compatible list to what readers and associated access control equipment is best for their particular situation/configuration.

Q: What is the process to select technology for technical testing?

A: Testing will be open to any vendors who feel their equipment meets the specification or elements of the specification for applicable use. After submittal, the equipment will be tested.

Q: On which magnetic stripe track is the TWIC Privacy Key (TPK) located?

A: The TPK is located on track one.

Q: Can the PKI be used in lieu of hotlist and are OCSP Responders going to be stood up as part of the TWIC program?

A: That is a policy issue. We do not have a firm decision. Right now there is a hotlist with a simple structure, not a CRL. PKI infrastructure is on the PIV side.

Q: Is there a going to be a Qualified / Approved Product List?

A: The process is to develop a list, not specifically a qualified or approved list with the associated definitions, of readers and equipment used in pilot program. The goal is to spring that forward into a list of qualified TWIC compatible products available to maritime interests for use once the 2nd rule is effective.

Q: Who will be defining the business cases during the pilot?

A: The guidance and testing scenarios presented by CDR Gautier today are a foundation to begin the business case discussions with pilot program port and vessel interests. Individual participants are presenting test plans based on their own needs and a dialogue with occur between all parties. There is going to be a give and take between the government and pilot participants to determine what works and what makes sense.

Q: Isn't the TPK an alternative to the PKI?

A: The intent of the privacy key is to ensure a level of confidentiality on the biometric template without having to impose key management, it essentially side-steps any PKI or key management aspects and still maintains confidentiality.

Q: How important is it that readers be able to read different types of identification?

A: Our central focus with the pilot is on the ability for readers to read a TWIC card. Owners and operators will need to make their own business decisions on what they would like the readers they purchase to be able to read. Some owners and operators have indicated that the ability for readers to read various cards (FRAC, CAC, etc.) is attractive to them.

Comment: Formal request for test cards. Recommendation made in support of readers with the capability to read multiple types of biometric identification cards. Many joint use facilities servicing MSC, Navy, and Marine Corps ships carrying individuals with CAC and Defense Biometric Identification System (DBIS) cards are going to be identified in the near future. Perimeter access to those facilities should have readers that support multiplicity.

Q: Is there technology available for purchase now that can read a TWIC card in order to enter it into an existing access control system?

A: The TWIC is a PIV. Any PIV contact reader has the capability to read the PIV information on the TWIC right now, assuming the card holder consents. That information could be integrated into an existing access control system. In addition, on both the contact and contactless side, the CHUID is freely available. That number is unique and identifies a particular TWIC card. One purpose of the pilot program is to identify readers for contactless validation and verification of TWICs.

Q: Will written responses be provided to individuals who submitted questions to CG/TSA in advance of the meeting/teleconference?

A: No. It was not our intention to develop a written list of questions and answers. Our hope is that the questions will be addressed throughout the meeting/teleconference.

Q: Can you identify the specific template generator that was used to store the reference biometric templates at time of enrollment onto the TWIC cards so that reader manufacturers can use the most compatible template matcher and generator in their reader products?

A: All we are able to disclose is that the template generator and all components are from a PIV approved product list and certified by NIST.

Q: The use of human subjects for a testing of readers to determine throughput and matching accuracy is now part of the scenario testing that will occur in the initial operational assessment phase at port facilities and vessels. Is that correct?

A: Yes. That is correct.

Q: Is there any fee being charged to vendors to submit their products for the technical testing conducted by SPAWAR?

A: That has not yet been decided. Once we determine the test protocol and cost of actual testing, a determination will be made based on that and funds available.

Q: Is the TEMP going to be a public document?

A: The TEMP will be released on a need to know basis. It will be a public document; however we are not planning on posting it online or in the Federal Register because of its specific use. It will be available upon request to vendors and pilot test participants.

Q: Will the results of the initial laboratory testing be on a pass or fail basis? Or is there some quantitative scoring that will either be made public or only shared with the participating manufacturer?

A: Our specific test protocol has not yet been fully developed. Several options have been discussed. Once the test protocol is complete, we will be able to address this question. We are open to suggestions.

Q: How many document signing certificates are required to be placed onto a reader so that memory requirements can be estimated?

A: Until we get into operational scenarios, we are not comfortable saying how many certificates will be required. Since there is only a single issuing authority, it a fair characterization to say that there will be a few vice an infinite amount of certificates required.

Q: Has there been any thought given to how you will best test access to facilities with a large population requiring TWICs, specifically at shift changes, with a large population entering or exiting at the same time?

A: We do plan to test peak load situations for access control. We are taking baseline measurements and will gather initial data during the early operational assessment. The full system test and evaluation peak load data will be collected once virtually all individuals at the particular pilot location / port area have their TWICs.

Q: Are you also testing the 'hardiness' of the hardware – i.e. is the reader going to hold up after 40,000 longshoremen have passed through? In addition is the card going to last five years?

A: We do plan to test the hardiness of the reader – will it hold up over a long duration of time and over multiple uses? The plan is to have enough time and data to make a realistic

determination of the ability of the reader to perform in a maritime environment. We are not testing the durability of the card.

Q: How is a reader submitted for testing? When is the testing going to begin – what is the timeline for the different test phases?

A: We are working with SPAWAR as the test integrator to determine exact directions for submittal. We would like to start the early operational assessment in early 2008. We have not yet established a timeline or the specific test protocol, which we do need to do. We hope to begin testing as soon as possible and we are dependent on industry to submit readers as they become available.

Comment: Pilot program participants need time to procure and install the appropriate infrastructure prior to the beginning of the early operational assessment in order for it to occur.

Response: We are cognizant of the time needed by pilot program participants. That time varies based on the operation.

Q: What about environmental ‘ruggedness’ testing?

A: Environment testing will be a phase of the initial technical testing. Technical testing will occur first, then the readers will be put through environmental test protocols, and then certain technical aspects will be verified again.

Q: Is SPAWAR doing all the environmental, operational, and functional testing?

A: SPAWAR is overseeing all of the testing. The actual location where testing is conducted may vary, but SPAWAR is in charge of managing all the TWIC testing, which includes functional, environmental, and operational testing.

Q: Is the pilot program going to include components that help establish the security and privacy of incorporating TWIC readers into existing access control system? Is a template for configuration / integration of software with TWIC readers going to be provided?

A: We anticipate some pilot participants are going to work to incorporate TWIC readers into existing security and access control systems. There are ways described in CG NVIC 03-07 to maintain a chain of trust between the TWIC and an alternate access control method. That needs to be worked out at a specific facility and identified within the security plan and with the COTP.

Q: Will the volume of data generated by the installation of a typical TWIC reader system be identified during the pilot and will that information be made available?

A: Plans are in place to measure throughput time with different modalities, not actual bytes.

Q: Is there an ability to gage the storage capacity needed for card data?

A: We are not measuring the storage capacity needed during the pilot program.

Q: How do you integrate TWIC readers and the card into an existing system with interrupting the current capabilities of the system, specifically if that system also manages things other than access control?

A: Under the existing rule, you are able to continue to use a facility specific issued card to gain access if you can demonstrate that the individual to whom you have issued that facility specific card also has a TWIC. Facilities with legacy systems will need to work with their software providers and particular vendors to determine the best way to integrate TWIC requirements.

Q: What is the process to suggest a pilot site, specifically a cold water location? Who should you contact?

A: You may contact John Schwartz, whose contact information is on the TSA website, or LT Brooke Grant, whose contact information is in the Docket.

Q: What is the process to integrate the TWIC card database and legacy databases? Is that automated or manual?

A: The process of checking the hotlist could be automated. Various facility and vessel owner/operators will need to work with vendors to integrate TWIC requirements into their own existing access control system. All facilities and vessels have very unique situations and will need to determine on a case by case basis what works best with their particular infrastructure.

Q: CDR Gautier mentioned record-keeping in his presentation, i.e., tracking of date and times when a particular TWIC was read. What, if any, policies are in place on how that information will be maintained and who will have access to it?

A: Policies are not yet in place for any TWIC record-keeping requirement; we did propose some ideas on this issue in the Notice of Proposed Rule-Making (NPRM) May 2006. The government envisions that the information on TWIC reads be made available to inspectors and investigators upon request. It would be the owner/operators responsibility to maintain the information either electronically or via hard copy. We need to see how this will function during the pilot and what the ramifications will be based on the collection of this data.

Q: It takes manufacturers a great deal of time and money to finalize products. Will there be a procedure to accept BETA products for the pilot test and allow manufacturers to modify those products as we learn together to reach the best possible solution?

A: Reader manufacturers are requested to submit what they have when they can. SPAWAR intends to conduct objective testing to determine what can work and what can't. Those readers that best meet the specification will most likely be selected.

Q: Can the government provide guidance on the expected radio of fixed indoor, fixed outdoor and handheld devices in a typical TWIC deployment?

A: At this point, we are unable to do that. A good idea of nationwide ratios will be needed for the regulatory analysis of the TWIC Reader rule, but that is not something we have now.

Q: We should we contact for a copy of the TEMP?

A: Either contact John Schwartz or LT Grant. A copy will be provided once it is finalized and approved.

Q: Is there anything we need to unlock the data on the card to download into an existing system?

A: The CHUID, containing the credential number, is freely available on both the contact and contactless side. The CHUID can be used at this time to link TWICs into an existing system. Other data can be obtained through the various access rules and appropriate interfaces to gain the data.

Q: Are you testing readers for the ability to reject counterfeit cards?

A: Yes. That is within scope of the testing. We plan to test whether the four data objects on the card can be transferred from the card with no error. There also has to be a way to determine if the card is authentic.

Q: In section 11.1 of the Specification, it states, "As not all TWIC cards may be issued with the TWIC application as the default selected card-application, the reader shall explicitly select the TWIC card-application." The statement implies there is more than one version of a TWIC card, is it not true that all cards will be issued with the TWIC application as the default selected card-application?

A: Yes. At this time all cards will be issued with the TWIC application as the default selected card-application. However there are advantages for the reader to explicitly select the TWIC card-application right now and possibly in the future, which is why it was stated in the specification.

Q: In Appendix A.3 of the Specification, it states, "The reader (or bi-directional panel) would 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." If the reader is network connected to the physical access control system panel or server and the TWIC expiration date is registered in that server along with the CHUID and/or TPK, would it

then not be necessary for the reader to have access to a time or system clock nor would the reader need to send the expiration date to the system because the system already knows that date?

A: That scenario is possible. The expiration date could be registered in the server system as opposed to adding a time function to the reader itself.

Q: What is date listed on the hotlist?

A: The date listed on the hotlist is the date of revocation of the TWIC card.

Q: Is this hotlist always going to be on the pre-enrollment site or is it going to be more secure?

A: It may not move locations, but we do intend to add security elements to the hotlist.

Q: If a particular reader solution is not part of the initial test, how will it be tested in the future? Are there going to be subsequent rounds of testing?

A: There is going to be a designated time span to accept readers for testing for the pilot program. The readers that make it through the initial technical testing will be used in subsequent early operational assessment portion of the pilot.

Q: If during testing TWIC cards experience problems in either the contact or contactless mode, will they be re-issued and/or will there be a fee to those individuals with defective cards?

A: If the card fails for a reason that is not due to abuse of card by the owner it will be reissued. If the card is not functioning, whether or not the replacement fee of \$60.00 is assessed will be determined by the reason for the card failure.

Q: Is the process in place for non-functioning cards to be re-placed?

A: The process is the same as that for lost, stolen, or damaged cards. The non-functioning card will be revoked and a new card issued.

Q: Will incremental updates to the hotlist be sent out?

A: No. The hotlist will be updated daily and can be accessed online.

Q: How frequently does the hotlist need to be checked?

A: Currently there is no requirement in regulation for the hotlist to be checked. It has been established for those who wish to use it if they decide to integrate the current TWIC card into their access control systems and it is there in anticipation of future regulatory requirements. It would be premature to speak to any future policy decisions. In the

NPRM published in May 2006, the proposed frequency depended upon the Maritime Security (MARSEC) level at which the particular facility or port was operating under, and it ranged anywhere from updating daily to weekly.

Comment: Thank you to the panel for opening up this forum.

Q: What will be the future role of the National Maritime Security Advisory Committee (NMSAC) TWIC working group? What will be our means to continue the questions and dialogue with the CG and TSA?

A: Any further questions and/or comments not addressed in this meeting/teleconference may be submitted to the Docket. We want to continue to keep the lines of communication open during this entire process. Specific engagement of NMSAC and other advisory committees has already occurred for the second rule-making. We will continue to ask questions and request comments from those advisory committees.

We have learned additional information today due to the nature of your questions. We know the interest in specifics about how one gets test cards, how one submits a reader for testing, what the testing will consist of, and how we will report out that testing. We will work on those answers.

Q: Right now we are unable to write to the chip on the TWIC card and are not able to securely write to the magnetic stripe. Is there another location to write a local application to the TWIC card?

A: No. The chip is locked and secured, and by both technology and policy can not be written to. Facility operators are able to write to track two and three of the magnetic stripe. However there is no way to lock or protect what is written on the magnetic stripe portion of the card. As long as the card is in the owner's possession and they do not allow another entity to write to it, the information should be secure. It should not be able to be de-magnetized or scrambled.

Q: There is a TSA Qualified Product List (QPL) for airport readers. Will that have bearing on this test or expedite acceptance of readers?

A: We are going to consider other testing and other approved, proven readers. Technical parameters and environmental port setting parameters will vary due to the TWIC requirements.

Q: Due to environmental requirements, is it not only the reader but also the housing and panel that must be submitted for testing?

A: The reader is all inclusive of the housing that incorporates the technology. We intend to test the entire solution not just parts.

Q: If a company's reader product alone would not meet the environmental specifications, but placed into a protective housing it could, would the entire configuration need to be submitted for testing?

A: We need to wait until the test protocol is finalized and released for the specifics of what would need to be submitted. There have been numerous discussions on indoor versus outdoor readers and how information is reported out. We do not intend to have a pass / fail for any of the reader tests. We intend to indicate those readers that read the TWIC card appropriately and also report out the results from the various environmental testing. The protocol on how best to do that has not yet been determined.

Closing Remarks

CAPT Mark O'Malley

Thank you for your participation. We have received valuable information from the questions asked today. We intend to continue to move forward and identify answers to those questions that still remain. We look forward to continued dialogue.