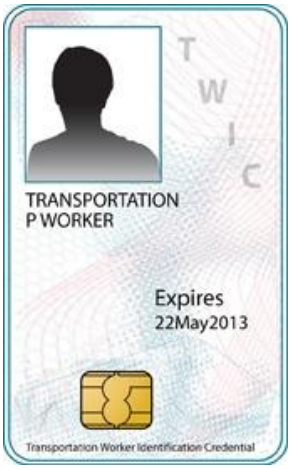
Maritime Security Enhanced through Biometric Readers

On August 23, 2016 the U.S. Coast Guard published its long-awaited final rule outlining the requirements for electronic biometric readers used in conjunction with the Transportation Worker Identification Credential (TWIC®). *[Include hyperlink to rule at: https://www.federalregister.gov/articles/2016/08/23/2016-19383/transportation-worker-identification-credential-twic-reader-requirements]* The TWIC is a government-issued smart card that must be carried by all maritime workers that require unescorted access to secure areas of regulated U.S. maritime facilities and vessels. The TWIC was mandated by Congress through the Maritime Transportation Security Act of 2002. The Transportation Security Administration (TSA) is responsible for enrollment and issuance of TWIC cards and for conducting background checks to determine an applicant's eligibility. The U.S. Coast Guard is responsible for setting and enforcing TWIC card usage as well as facility and vessel access requirements.

TSA began issuance of TWICs in 2007 and over 2 million cards have been issued. Most applicants pay a fee of $128 for a TWIC card that is good for 5 years. The TWIC is a sophisticated smart card that is aligned with the standardized Personal Identity Verification (PIV) card issued to all federal workers and contractors. The TWIC can be electronically read to determine card validity and for verification of the card holder by matching a presented fingerprint with the fingerprint data stored on the card.



The Coast Guard has labored for the last ten years to finalize regulations that require electronic validation of TWIC cards when accessing maritime secure areas. Until this new rule, the only requirement was for visual inspection of TWIC cards by security personnel at entry points. Visual card inspection is accomplished by viewing the security features on the card (such as the watermark), checking the expiration date on the face of the card, and comparing the photograph on the TWIC with the individual's face. However, there is no way to visually check if the TWIC has been revoked by the TSA since it was issued. Using the TWIC in this manner as a "flash pass" did not take advantage of the advanced electronic features on the card.

So what took so long? The Coast Guard actually began its public rule making process for electronic reading of TWIC cards in May 2006. There have been hundreds of public comments received and many of the comments expressed concern over the costs associated with adding electronic readers to the existing maritime infrastructure. Many maritime facilities and vessels do not have automated physical access control systems (PACS), and the Coast Guard had to carefully balance the cost burden of electronic TWIC validation with the security benefits. As a result of a lengthy risk-based cost analysis and public comment review, the Coast Guard's final rule mandates electronic TWIC inspection – but only for the highest risk maritime facilities and vessels. Those facilities and vessels not in the high-risk category are free to continue using visual TWIC inspection; or they may implement electronic TWIC readers on a voluntary basis.

The new Coast Guard rule estimates that 525 facilities and 1 vessel fall into the high-risk category and are required to use an electronic TWIC validation process prior to each entry into a secure area. According to the Coast Guard, this represents only about 5% of the TWIC card holders but addresses about 80% of risks of a transportation security incident – such as a terrorist attack.

The electronic TWIC validation process consists of three discrete parts: (1) Card authentication, in which the TWIC is identified using public key cryptography as an authentic card issued by the TSA; (2) a card validity check, in which the TWIC is compared to the TSA-supplied list of cancelled TWICs to confirm that it has not been revoked and is not expired; and (3) identity verification, in which the TWIC is matched to the person seeking access through use of a biometric fingerprint template stored on the TWIC.

The Coast Guard acknowledges that each of these methods is an improvement over visual TWIC inspection since the electronic TWIC inspection uses methods of validation that are not easily manipulated through counterfeiting or physical alteration. Further, electronic validation ensures that the card being presented has not been revoked by TSA as a result of being reported as lost or stolen, or through TSA's determination that the card holder is no longer eligible due to a criminal conviction or suspected terrorist activity. And finally, biometric matching provides a higher level of identity assurance than visual photo comparison.

In addition to the security benefits, electronic TWIC validation may improve the efficiency of security staff by relieving them of the burden of visual TWIC inspection and permitting them to focus on other more specialized duties related to access control. It should also be noted that even if an individual possesses a valid TWIC, the maritime operator still has the discretion to grant unescorted access privileges. Electronic TWIC validation ensures that facility security personnel do not grant unescorted access to individuals that have not been vetted or have been determined as unfit for access to secure areas.

The TSA has published a *TWIC Reader Hardware and Card Application Specification* to assist manufacturers of TWIC readers in developing products that meet the requirements for electronic TWIC inspection. The TSA has also implemented a voluntary program where TWIC reader manufacturers can submit their products to an independent laboratory for testing and evaluation for conformance with the Specification. Once a product has successfully completed this rigorous

test and evaluation process, it will be added to the TSA's TWIC Reader Qualified Technology List (QTL).

As of this writing, there are six portable and eight fixed-mount TWIC readers on the TSA's TWIC Reader QTL. Both the QTL and the Specification can be downloaded from the Coast Guard's Homeport Web site at https://homeport.uscg.mil and selecting "TWIC" under the featured Homeport links. It should be noted that the Coast Guard's final TWIC reader rule does not require that TWIC readers be included on the QTL. Instead, it allows some flexibility in the approach that a maritime operator can choose in implementing electronic TWIC validation by leveraging existing PACS components. However, maritime operators that choose to implement TWIC readers would be wise to consider those products that have completed the independent QTL test and evaluation process.

The TWIC reader rule has been a long time coming. But even though it is now official, the Coast Guard will still delay the effective date by two years to allow time for maritime operators to comply with the rule. So it will not go into effect from an enforcement perspective until August 23, 2018. Even so, this new rule clearly demonstrates that the Coast Guard believes that the use of biometric readers can and should be a part of the nation's maritime security system.

About the author:

Walter Hamilton is a recognized industry authority and subject matter expert on biometric technology. He currently serves as Vice Chairman of the International Biometrics + Identity Association (IBIA), a Washington, DC-based non-profit trade association that supports the use of technology to determine identity and enhance security, privacy, productivity and convenience. He previously served seven terms as IBIA's Chairman and President. Mr. Hamilton is also a Senior Consultant with Identification Technology Partners (IDTP), a consulting firm in the identity management field. Mr. Hamilton has been committed to advancing biometric use and is an advocate for the adoption of open standards - crucial for industry development. In his consulting activity with IDTP, Mr. Hamilton is currently engaged with U.S. government clients supporting the implementation of biometric technology in the maritime and aviation transportation security sectors. Prior to joining IDTP in 2006, Mr. Hamilton served as Vice President and General Manager; Biometric Solutions for Saflink Corporation. Prior to joining Saflink in 1995, Mr. Hamilton completed a distinguished 30-year career with Unisys Corporation