

December, 2007

Subject: Software House and the U.S. TWIC Program

Background:

The Transportation Worker Identification Credential (TWIC) is a vital security measure that will ensure individuals who pose a threat do not gain unescorted access to secure areas of the nation's maritime transportation system. TWICs are tamper-resistant biometric credentials for workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities and all credentialed merchant mariners.

In response to comments received on the joint TSA/CG Notice of Proposed Rule Making (NPRM) published 22 May 2006, the TWIC program was divided into two separate regulatory projects:

1. The first rulemaking of TWIC requires all personnel needing unescorted access to areas covered by the Maritime Transportation Safety Act to hold a TWIC. During this initial rollout phase, workers will present their cards to authorized personnel, who will compare the holder to his or her photo, inspect security features on the TWIC and evaluate the card for signs of tampering. The Coast Guard will verify TWICs when conducting vessel and facility inspections and during spot checks using hand-held scanners, ensuring credentials are valid. This part of the rulemaking does not require electronic access control.
 - a. The TWIC final rule for the initial rollout was posted on the TSA and Coast Guard web sites January 1, 2007 in compliance with SAFE Port Act and published in the Federal Register January 25, 2007 with an effective date of March 26, 2007.
 - b. The Captain of the Port (the lead Coast Guard official for an area) will set the date that compliance for the first phase will be met, but it must be no later than September 25th, 2008.
2. TSA has announced that a second rulemaking is expected in January 2009, which will propose enhanced access control requirements, including the use of electronic readers by certain vessel and facility owners and operators. The rule making will likely require biometrics, and the use of a TWIC Privacy Key (TPK) to ensure secure, encrypted transmission of a person's biometric fingerprint template when using a contactless interface.

TWIC Card Technical Details and Data Model

The TWIC credential is a PIV II credential with an additional application to enable contactless biometrics. It is a dual interface (contact/contactless) smart card, with the contactless interface based on the ISO 14443 standard for contactless smart card transmissions. The TWIC includes storage of biometric templates, user PIN, images and digital certificates. The card data model will follow the FIPS 201 standard, using the FASC-N (Federal Agency Smart Credential Number) for card uniqueness. A TWIC Privacy Key (TPK), unique per card, will be used to decrypt the biometric template. The TPK will be available from the card's contact interface, and will also be placed on the card's magnetic stripe.

TWIC V1.0 Data Model

Buffer Description	Maximum Length (bytes)	Contact/Contactless
Unsigned Cardholder Unique Identifier	64	Contact and Contactless
TWIC Privacy Key Buffer	40	Contact (and Magstripe also)
Card Holder Unique Identifier (CHUID)	3000	Contact and Contactless
Card Holder Fingerprints	2500	Contact and Contactless
Security Object	920	Contact and Contactless

TWIC Implementation

During the first rulemaking phase of TWIC, some owners and operators may choose to integrate TWIC cards into their existing access control systems, although owners and operators are not required to purchase, install, or maintain card readers until the second rulemaking is enacted. The Coast Guard will conduct checks using handheld readers to confirm the identity of TWIC holders during regular inspections and unannounced spot checks.

The second regulation will propose card reader requirements that utilize all of the unique technologies employed in the TWIC, including the biometric template and the TPK. While not finalized, the rulemaking will likely require a biometric match at the perimeter of the restricted area, and then standard contactless readers without biometrics may be used for internal doors and portals.



TWIC Implementation with a Software House[®] System

The current version of the Software House C·CURE[®] 800/8000 system, rev 9.1, as well as all versions of the Software House C·CURE 9000 system, support the extended card formats and government card features required by PIV II cards and the FIPS 201 standard (when using iSTAR controllers at rev 4.1 or higher). Using these versions also ensures compatibility with the current TWIC standard.

Software House Multi-Technology readers will read all fields of the FASC-N in both PIV II cards and TWIC cards, and will output the card data to the iSTAR controller in a number of different tested and supported formats, including the standard GSA 75-bit Wiegand format. Since the firmware in these readers is flashable, any future TWIC requirement that necessitates a firmware change is easily downloaded to the reader.

Software House is actively engaged in the rulemaking for TWIC and will work to support future TWIC requirements within the C·CURE platform.

Resources

TWIC information on the TSA website: www.tsa.gov/twic

U.S. Coast Guard Homeport website: homeport.uscg.mil/mycg/portal/ep/home.do

FIPS 201 information on the NIST website: csrc.nist.gov/groups/SNS/piv/index.html