Transportation Worker Identification Credential

Working Technical Specification & Evaluation / Qualification Overview

U.S. Department of Homeland Security
Transportation Security Administration

Gerald Smith
SME to the TWIC PMO
ID Technology Partners

April 21, 2010

AGENDA

- TWIC Reader Hardware and Card Application Specification Overview
- TWIC Evaluation and Qualification Steps Review

TOPIC

- TWIC Reader Hardware and Card Application Specification Overview
- TWIC Evaluation and Qualification Roadmap Overview

History of the Working Specification

- Initial specification was developed by the National Maritime Security Advisory Committee (NMSAC) TWIC Working Group
  - TSA baseline was from the 28 February 2007 "Alternate" NMSAC Specification
  - TSA published Version 1.0 on 9/11/2007
- Current version is Version 1.1 Amendment 1 dated 05/30/2008
  - Specification frozen to allow vendors a stable base from which to develop solutions

The TWIC Working Specification

- TWIC Working Specification is public
  - Available at -> http://www.tsa.dhs.gov/assets/pdf/twic_reader_card_app_spec.pdf
- TWIC Working Specification details
  - Reader Types (Fixed or Portable)
    - Functional and Environmental Requirements
  - TWIC Card Application
    - Data Model
    - Supported Command/Response Messaging

TWIC Terminology aligned to SP 800-116

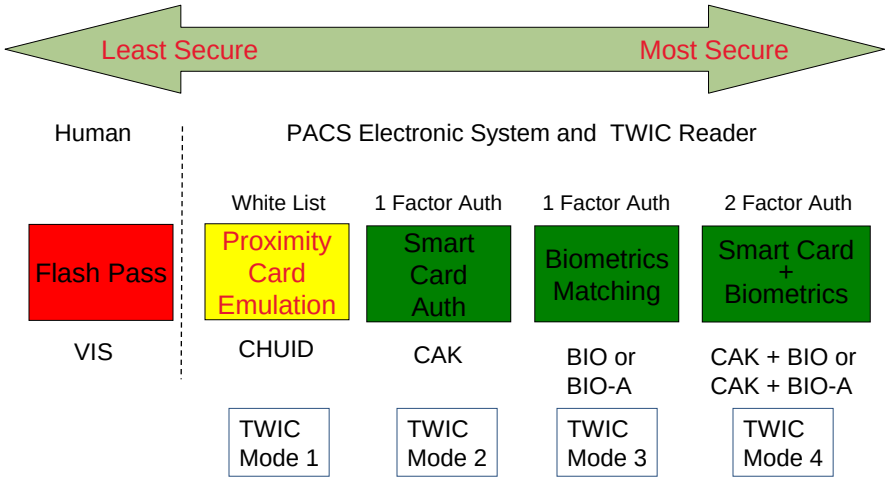
- ✓ VIS –> Visual Inspection
  - A FIPS 201 identification mechanism in which the visual identity verification of a TWIC Card is done by a human guard.
- ✓ CHUID –> Static ID Match
  - A FIPS 201 identification mechanism that is implemented by transmission of the CHUID data object from the TWIC Card to a PACS, or the TWIC Card data object of the same name.
- ✓ CAK –> Card Authentication Asymmetric Key Challenge
  - A n authentication mechanism that is implemented by an asymmetric key challenge/response protocol.
- ✓ BIO –> Biometric (Finger) Match
  - A FIPS 201 authentication mechanism that is implemented by using a Fingerprint data object sent from the TWIC Card to the PACS.
- ✓ BIO-A –> BIO "Attended" [Observed by a human Guard]
  - A FIPS 201 authentication mechanism that is implemented by using a Fingerprint data object sent from the TWIC Card to the PACS.

Highlights from the Working Specification

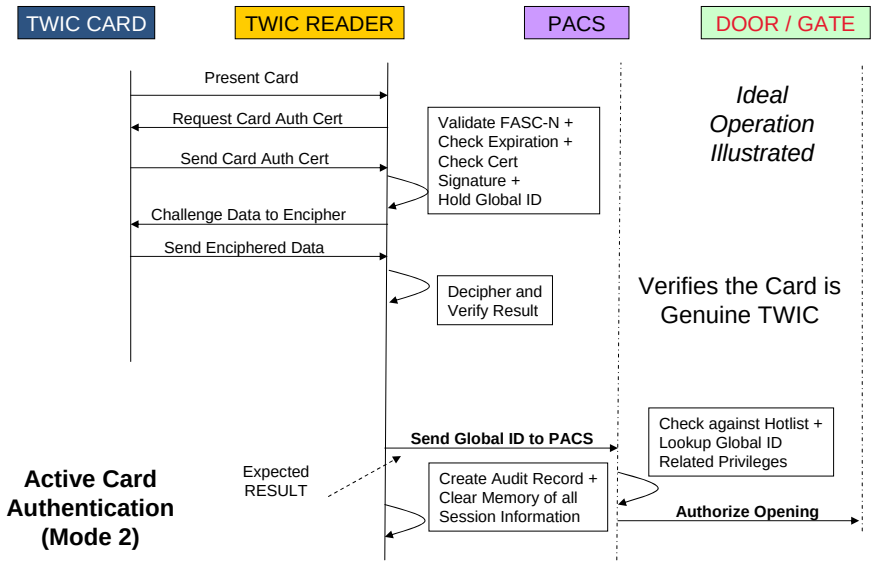
Four Modes of Identification/Authentication

MODE	TWIC Identification / Authentication Description	Desired Result
1	Card Holder Unique ID (CHUID) Identification	Match Static ID to a unique entry on a PACS white list
2	Active Card Authentication (CAK)	Verify the Card is issued by TSA TWIC
3	Biometric User Authentication BIO or BIO-A	Verify the Card Holder biometrics match the reference on the card
4	CAK + BIO Authentications or CAK + BIO-A Authentications	Verify the Card Holder is bound to a TSA TWIC issued card

Highlights from the Working Specification



Transaction Scenario (CAK Example)



TWIC Reader Overview (Unique Needs)

- Unique to TWIC is the ability to support the TWIC Privacy Key (TPK) usage for transmission of the fingerprint minutiae biometrics reference data across the contactless interface without need to present a PIN
- Fixed TWIC Readers are required to function in harsh environmental conditions

TWIC Reader Overview (Fixed vs. Portable)

- Fixed Readers are envisioned to be stationary with one (or more) connections to a PACS
  - Access decision is made by the PACS; not the TWIC reader
- Portable Readers are envisioned to be used by Operators
  - Access decision is made by the Operator in association with the reader

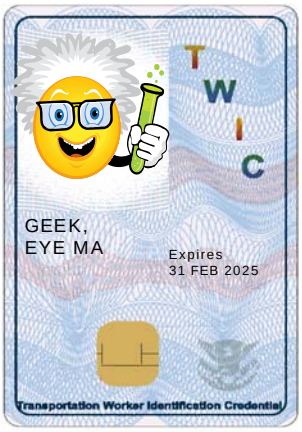
TWIC Reader Overview (Weigand Interface)

- Weigand Interface (a ONE WAY interface) is required for all Fixed TWIC readers
  - Intent is to support existing PACS installations
  - Current TWIC Working Specification attempts to preserve the NMSAC recommendations BUT
    - TWIC Issuance model requires the PACS to check the Initial Credential Issuance (ICI) field which is NOT supported in the GSA 75 bit (or 48 bit) format.
    - The specification suggests a solution that preserves the GSA format.
  - TPK usage is a challenge for Fixed Readers supporting ONLY Weigand output (i.e. Magnetic Stripe Reader becomes mandatory)

TWIC Fingerprint Minutiae Biometrics

- Fingerprint Minutiae available in 2 places
  - Resides in the TWIC Card Application as an enciphered object that can be read without privilege using either contact or contactless interface
    - The Decipher symmetrical key (TPK) is available only via the Contact interface / Magnetic Stripe Track 1
  - Resides in the PIV Card Application as a clear text object that can be read only via the contact interface AFTER successful presentation of the card specific PIN
- Fingerprint Minutiae Templates
  - Two views format uses the ANSI 378 format
  - One view format uses the ANSI 378 format
  - Zero views format uses an ISO CBEFF format with a null Biometrics Data Block (refer to TWIC Technical Advisory)

TWIC Smart Card



- Aligned with FIPS 201
- 64K of non-volatile memory
- Dual interfaces share memory
  - Contact interface (ISO/IEC 7816)
  - Contactless interface (ISO/IEC 14443/A)
- 1D Bar Code / Magnetic Stripe
- Physical security features
  - Tamper resistant
  - Color shifting inks
  - Hologram
- Logical security features
  - Enciphered fingerprint templates
  - Signed data (CHUID, Biometrics)
  - Security Data Object supported
  - PKI certificates (on PIV Card Application)

Digital Signature AND Secure Hash computed on most Data Objects

- Most objects are signed using the Issuer private key associated with the Content Signing Certificate found in the (signed) CHUID
- These same objects also have a Secure Hash computed and stored in the Security Data Object
  - TWIC Card Application support a Security Data Object
  - PIV Card Application support a Security Data Object
- The intent was to offer TWIC readers an option on how to verify data integrity for Data Objects
  - TWIC Reader Pilot and Specification Conformance Testing have shown that TWIC Readers perform a check of the digital signature associated with a data object; the secure hash is not checked.

Looking Ahead

- TWIC will migrate from the Working Specification to one or more FINAL specifications
  - Time frame is a function of many variables including:
    - Final Reader Rule Timing
    - Lessons learned from the TWIC Reader Pilot Effort
- Observations on how to proceed
  - Augmenting the FINAL specification to cover identified gaps in the Working Specification (e.g. PACS Registration, Chain of Trust)
  - One Specification or Multiple?
    - One specification reorganized for clarity / relevance OR
    - One Specification per Reader Type

TOPIC

- TWIC Reader Hardware and Card Application Specification Overview
- TWIC Evaluation and Qualification Roadmap Overview

TWIC Evaluation / Qualification Steps

- TWIC Evaluation / Qualification Steps
  - Initial Capability Evaluation (ICE) (2008)
    - ICE List is the output of this process
  - Specification Conformance Testing (SCT) (2009)
    - Limited to providing input into a Report to Congress addressing industry readiness to support TWIC
    - Both Functional and Environmental Testing Performed
  - Final Reader Assessment (FRA) (in Process)
    - Qualified Product List

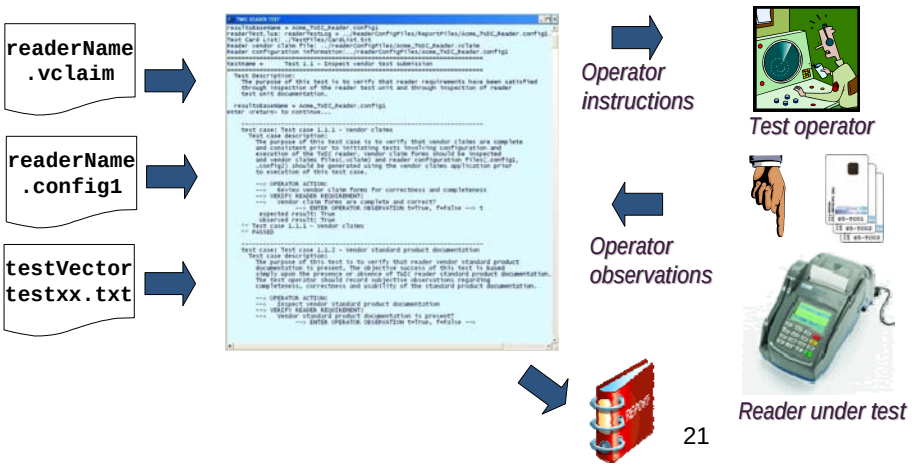
ICE

- ICE is a scenario based approach evaluating readiness of TWIC Readers for possible use in the TWIC Reader Pilot effort
  - ICE Scenarios and the Process for application to TSA can be found here listed as "Current Broad Agency Announcement" -> http://www.tsa.dhs.gov/what_we_do/layers/twic/pilot_test.shtm
  - Successful evaluation allows the entity submitting a solution for ICE to be placed on the ICE List located at -> http://www.tsa.dhs.gov/assets/pdf/twic_ice_list.pdf
- 23 entities currently on the ICE List (01/20/2010); two support operational biometrics
- NOTE: ICE will be **phased out** as the pilot concludes and a Final Reader Assessment capability is developed.

Functional SCT

- Functional Testing Approach
  - First a Vendor claims what parts of the TWIC Working Specification are supported
  - These Vendor claims are then used to generate all tests to be performed (automated script generation)
  - Vendor allowed to submit up to Two unique configurations per specific TWIC Reader
  - Each vendor configuration is tested along side a Reference Implementation as an aid to the Test Operator
- F-SCT did not permit redress but did provide a vendor specific debrief from the Test entity
- Results to be aggregated for use in a Report to Congress

Functional SCT



Source: TSA / ID Technology Partners

Environmental SCT

- Environmental Testing Approach
  - Testing per the (challenging) environmental requirements as specified in the Working Specification
  - Testing beyond the specified requirements were also performed
  - Tests were “black and white” as each test was well defined per MIL-STD 810F.
- E-SCT did not permit redress but did provide a vendor specific debrief from the Test entity

Final Reader Assessment (Future)

- Process still under development
- Purpose of this workshop is to gather ideas and suggestions for what should be considered for FRA

Conclusion

- TWIC Program has unique requirements
- Evaluation and limited testing have been performed to date in support of the TWIC Pilot initiative
- This workshop is about gathering input on the Final Reader Assessment Process

Contact Information

Gerald Smith

Gerald.Smith@Associates.DHS.gov

Tel at TSA: (571) 227-5252

OR

Gsmith@idtp.com