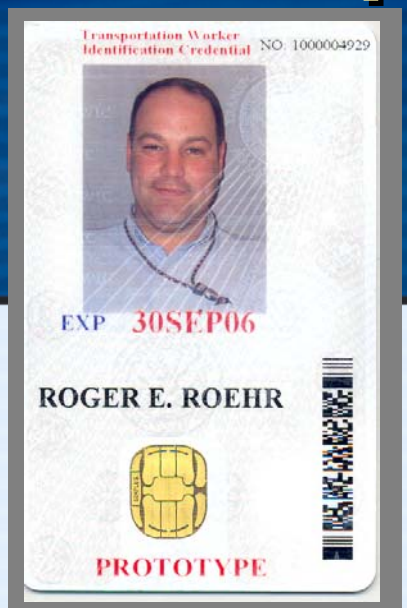
SOFTWARE HOUSE®

Biometric Access Control in TWIC Read Hardware and Card Application Specification

Roger Roehr



tyco

Agenda

- TWIC Reader speciation
- Fingerprint minutia templates
- FIPS 201 biometric solutions
- TWIC contactless biometric solutions
- Questions

Reader Specification

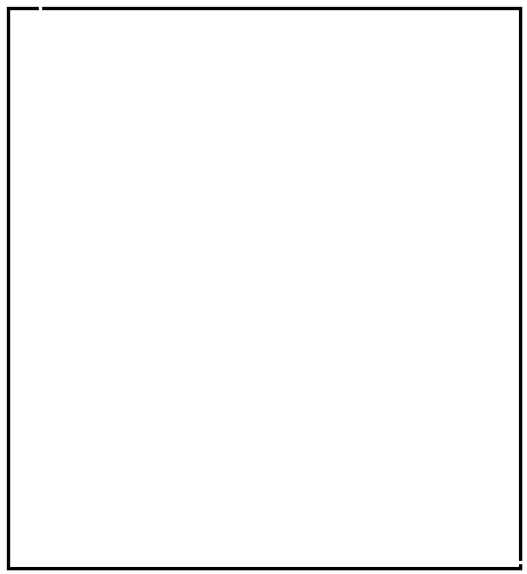
- TSA published the TWIC reader “working” specification on September 11, 2007
- Based on NMSAC TWIC Working Group alternate spec
  - Biometric data is encrypted on card
  - Does not require management of shared cryptographic keys
  - Contactless transfer of biometric data allowed without PIN
- Similar to approach in ePassport
  - TWIC “Privacy Key” unique to each card and stored on card
  - Treated as a “public key” and not as a secret
- Key accessible from magnetic stripe or contact interface
  - Can also be stored in local access control system server to eliminate need for magnetic swipe or contact read

Reader Specification (cont.)

- Three reader types defined
  - Fixed mount for outdoor use
  - Fixed mount for indoor use
  - Handheld for mobile use
- May operate standalone or network attached
  - Network attached reader should support 2-way communications to allow upload of TWIC Privacy Key from server
- Outdoor reader ruggedized for environment
  - Operating range -20ºC to +70ºC
  - Humidity range of 5-100% condensing
- Transaction time of 3 seconds
  - From presentation of contactless card to completion of biometric match
- Biometric matching equal error rate of 1% or less
- Biometric sensor should provide “liveness” detection

Finger Print Biometrics

- For FIPS-201 the Federal Government has standardized on ANSI 2004-378 fingerprint minutia templates for biometrics.

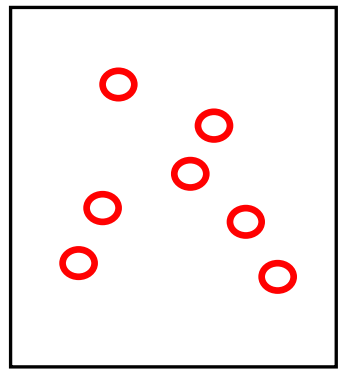


Template

Advantages of the ANSI 2004-378

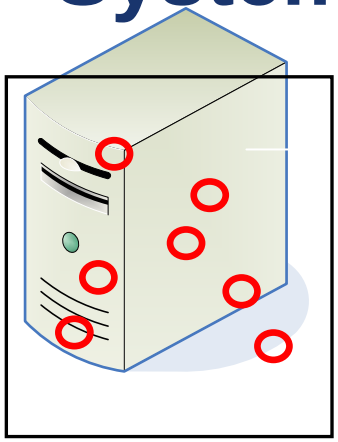
- Template generation and match algorithms have been toughly tested by NIST in the MINEX 04 test.
- The ANSI 378 template where implemented in phase 3 of the TWIC and proved successful with multiple vendor in field environments
- Keeps ports from being locked into a single vendor for biometrics

FIPS 201 Template stored on contact card after PIN



Template

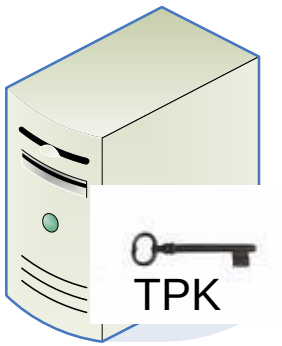
FIPS 201 Template stored on Backend System

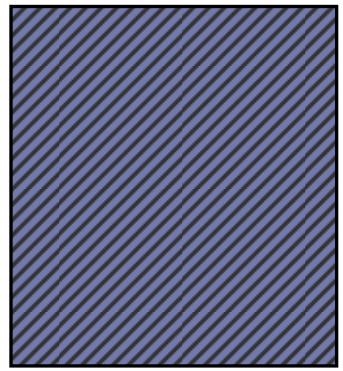


Template for card 1234

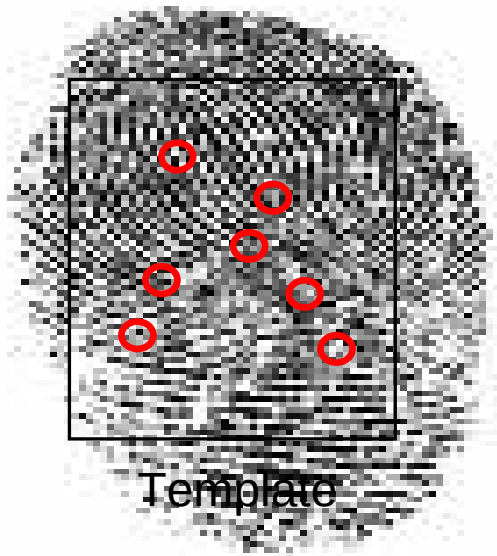
Card # 1234

Contacless Biometrics with stored TWIC Privacy Key



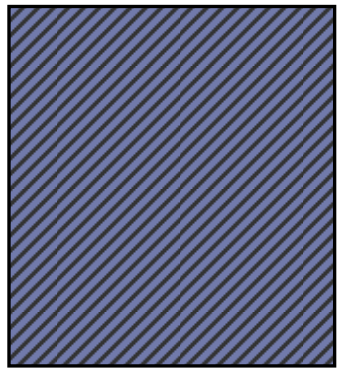


Encrypted Template

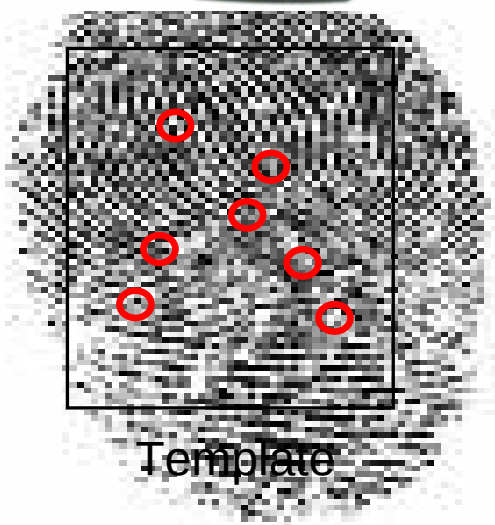


SOFTWARE HOUSE®

Contacless Biometrics reading TWIC Privacy Key First



Encrypted Template



TPK

tyco

PIV Data model from SP 800-73

Buffer Description	Container ID	Maximum Length (Bytes)	Access Rule	Contact /Contactless	M/O
Card Capabilities Container	0xDB00	266	Always Read	Contact	M
Card Holder Unique Identifier	0x3000	3377	Always Read	Contact and Contactless	M
X.509 Certificate for PIV Authentication	0x0101	1651	PIN	Contact	M
Card Holder Fingerprints	0x6010	7768	PIN	Contact	M
Printed Information	0x3001	106	PIN	Contact	O
Card Holder Facial Image	0x6030	12704	PIN	Contact	O
X.509 Certificate for Digital Signature	0x0100	1651	PIN Always	Contact	O
X.509 Certificate for Key Management	0x0102	1651	PIN	Contact	O
X.509 Certificate for Card Authentication	0x0500	1651	Always	Contact and Contactless	O
Security Object	0x9000	1000	Always Read	Contact	M

For TWIC all the optional field will be filled

Review of HSPD-12 Overview

HSPD-12

TWIC

FRAC

FIPS -201

SP-800-73-1

Interfaces for PIV

SP-800-76-1

Biometric Data Specification for PIV

SP-800-78 Cryptographic Algorithms and Key Sizes for PIV

SP-800-79

Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

SP 800-87 Codes for the Identification of Federal and Federally-Assisted Organizations

SP-800-96

PIV Card / Reader Interoperability Guidelines

SP-800-103 A Scheme for PIV Visual Card Topography

http://csrc.nist.gov/piv-program/fips201-support-docs.html

TWIC Information Links

- TSA web site: www.tsa.gov/twic
- U.S. Coast Guard Homeport web site: http://homeport.uscg.mil/mycg/portal/ep/home.do

Resources

- http://csrc.nist.gov/piv-program
- www.smart.gov
- www.idmanagement.gov
- www.smartcardalliance.org
- http://www.fixs.org/

Final Thoughts

- This is a working specification
- Current rule making and NAVIC 03-07 do not require electronic checking of TWIC.
- TWIC is going to use the Federal Agency Smart Card Number (FASC-N) this number is larger than most PACS can use.
- Ensure that your biometric reader manufacture has got a method and path to upgrade their reader.

SOFTWARE HOUSE®

Contact Info

tyco / Fire & Security

Roger Roehr

Access Control & Video Systems
Manager - Government Vertical
rroehr@tycoint.com

11317 South Shore Road
Reston, VA 20190 USA

Tele: 703 437-5651
Mobile: 703 407-8249

www.swhouse.com

tyco