ALABAMA STATE PORT AUTHORITY
 REQUEST
 FOR
 BID:

TO FURNISH, INSTALL AND INTEGRATE
PORTABLE TWIC CREDENTIAL READERS,
MANAGEMENT SOFTWARE
&
WIRELESS ACCESS POINTS

JUNE 2012
# TABLE OF CONTENTS

1. INSTRUCTIONS FOR BIDDERS And INSURANCE REQUIREMENTS .............3
2. CONFIDENTIALITY AND INFORMATION SECURITY ..........................6
3. OVERVIEW .................................................................................6
4. OPERATIONAL AND PERFORMANCE OBJECTIVES ......................7
5. PROJECT REQUIREMENTS ..........................................................7
6. SCOPE OF WORK ......................................................................7
7. VERIFYING CONDITIONS ..........................................................8
8. SCHEDULE ................................................................................8
9. SUBMITTALS ............................................................................9
10. PRODUCT DELIVERY, STORAGE AND HANDLING .....................9
11. PROTECTION AFTER INSTALLATION ........................................10
12. SPECIFIED EQUIPMENT AND MATERIALS .................................10
13. FINANCIAL PROPOSAL .........................................................11
14. PRICE CERTIFICATION ..........................................................12
    FINANCIAL PROPOSAL WORKSHEET .......................................12
    TABLE A ..................................................................................14
    APPENDIX A .............................................................................
ALABAMA STATE PORT AUTHORITY ACCESS POLICY
IMPORTANT NOTICE TO BIDDERS REGARDING ACCESS TO ASPA RESTRICTED FACILITIES:

Successful bidders requiring access to the Alabama State Port Authority's Restricted Facilities to fulfill any obligations set forth in this bid must comply fully with the Authority's Access Policy found in its entirety at http://www.asdd.com/portaccess_policy.html. The Port Authority's Access Policy requires all persons permanently employed at the port, including ASPA staff, tenants and their employees, surveyors, agents, stevedores, longshoremen, chaplains, contract labor and persons requesting temporary access to the port, including delivery persons, vendors, contractors, and temporary workers must obtain and display an ASPA issued photo ID badge or visitor badge at all times when accessing or working on port property. In order to obtain an ASPA credential, applicants must also obtain a Transportation Worker Identification Credential (TWIC) and undergo mandatory Security Awareness Training. Information on the TWIC can be found at http://www.asdd.com/portaccess_twicregs.html. Information on Security Awareness Training classes and scheduling can be found at http://www.asdd.com/portaccess_securitytraining.html.

ALL PROSPECTIVE BIDDERS ARE ENCOURAGED TO REVIEW THESE POLICIES AND CONSIDER THESE REQUIREMENTS IN PREPARING BID SUBMISSIONS.

INSTRUCTIONS FOR BIDDERS
ALABAMA STATE PORT AUTHORITY

This instruction sheet is provided as a guide to facilitate the bid process and highlight important points for consideration by bidders. Each bidder is responsible for fully reading and complying with the instructions on the Alabama State Port Authority bid form. This instruction sheet is to be used as a guide only.

1. No consideration will be given to bids unless presented on the Alabama State Port Authority "Requisition & Proposal" Form with suitable attachments as deemed necessary by the bidder. Alternate bid proposals may be rendered, with proper support.

2. If your company is not prepared to submit a bid, so state and sign to avoid being deleted from the prospective bidder's list.

3. The Alabama State Port Authority reserves the right to reject any and all bids if deemed in the Alabama State Port Authorities' interest.

4. No allowance will be made for error, either omission or commission.

5. Unit price governs in errors relating to extension of prices.

6. **Bids will not be accepted via FAX.** All bids must be sealed and sent via mail or hand delivered to the International Trade Center before the specified date and time.

7. The Alabama State Port Authority accepts no responsibility for facilitating the receipt of bids.
8. **Bids over $7,500 must be notarized.**

9. Bids received after specified opening time will be returned to the bidder unopened. Bidders are requested to show a return address on the bid envelope.

10. Proposals must be filled out completely, including the name, address, telephone number, fax number (if possible) and signature of responsible person.

11. **Questions may be directed to** the Alabama State Port Authority IT Systems Specialist Senior, at (251) 441-7549, *bvalentz@asdd.com*

12. **All hand delivered bids** must be tendered to:

   Alabama State Port Authority
   ATTN Brett Valentz 250 North Water Street Suite 240 Mobile, AL 36602

13. **All regular U.S. Postal Mail** must be tendered to:

   Alabama State Port Authority
   ATTN Brett Valentz 250 North Water Street Suite 240 Mobile, AL 36602

14. **All courier / overnight deliveries** (UPS, FEDEX) must be delivered to:

   Alabama State Port Authority
   ATTN Brett Valentz 250 North Water Street Suite 240 Mobile, AL 36602

15. Note: all overnight bids must be FIRST PRIORTY OVERNIGHT. (8:30 A.M. NEXT MORNING)

16. **Notarization not required on "SALE" bids.**

17. **IMPORTANT NOTICE TO BIDDERS REGARDING EMPLOYMENT PRACTICES:**
   Effective October 1, 2011, the Beason-Hammon Alabama Taxpayer and Citizen Protection Act (“the Act”) requires that any business entity contracting with or proving any grant or incentives to the state, including the Alabama State Port Authority, certify compliance with the Act. All Bidders must certify such compliance by executing the enclosed Affidavit and returning it to the Alabama State Port Authority with your bid package. The Affidavit must be notarized.

**ALABAMA STATE PORT AUTHORITY**  
**INSURANCE REQUIREMENTS FOR CONTRACT WORK**

**INDEMNIFICATION**

The Contractor shall assume all liability for and shall indemnify and save harmless the State of Alabama and the Alabama State Port Authority (ASPA) and its officers and employees from all damages and liability for injury to any person or persons, and injury to or destruction of property, including the loss of use thereof, by reason of an accident or occurrence arising from operations under the contract, whether such operations are performed by himself or by any subcontractor.
or by anyone directly or indirectly employed by either of them occurring on or about the premises, or the ways and means adjacent during the term of the contract, or any extension thereof, and shall also assume the liability for injury and/or damages to adjacent or neighboring property by reason of work done under the contract.

**INSURANCE REQUIREMENTS**

The Contractor shall not commence work under the contract until he has obtained all insurance required under the following paragraphs and until such insurance has been approved by ASPA, nor shall the Contractor allow any subcontractor to commence work until all similar applicable insurance has been obtained by the subcontractor or the Contractor has provided coverage for the subcontractor. The Contractor shall provide, at his expense, insurance in accordance with the following:

**General Requirements (applicable to all policies)**

All policies of insurance must be written with companies acceptable to ASPA. The Contractor shall furnish to ASPA certificates of insurance, signed by the licensed agent, evidencing required coverages. ASPA reserves the right to require certified copies of any and all policies. Each policy of insurance shall provide, either in body of the policy or by endorsement, that such policy cannot be substantially altered or cancelled without thirty (30) days’ written notice to ASPA and to the insured. Except for Workers Compensation, said policies will identify Alabama State Port Authority, its officers, officials, agents, servants and employees as Primary and Non-contributory Additional Insureds in connection with work performed for, on behalf of, or on the property of ASPA.

**Commercial General Liability**

The Contractor shall take out and maintain during the life of the contract Commercial General Liability insurance, including Blanket Contractual and Completed Operations coverages, in an amount not less than $2,000,000 for any one occurrence for bodily injury, including death, and property damage liability.

**Business Automobile Liability**

The Contractor shall take out and maintain during the life of the contract Business Automobile Liability insurance covering any auto in an amount not less than $1,000,000 for any one occurrence for bodily injury, including death, and property damage liability.

**Workers Compensation (AL WC/EL and USLH required for this project)**

The Contractor shall take out and maintain during the life of the contract Workers Compensation and Employers Liability insurance providing coverage under the Alabama Workers Compensation Act in an amount not less than that required by Alabama law.
1. CONFIDENTIALITY AND INFORMATION SECURITY

This Request for Bid (RFB) contains security sensitive information which is the sole property of the Alabama State Port Authority (ASPA) and must be protected from unauthorized access. Your organization and its employees may not disclose any documents, diagrams, information, and/or information storage media made available to you by ASPA, or in conjunction with any contract arising there from except that only those employees who are authorized and required to use this materials may have access to and use it in the preparation of your bid. **Contractor must take precautions to protect the confidentiality of the information contained in this RFB and resulting bid service proposals from unauthorized access and compromise.**

All materials provided to Contractor by ASPA will be returned promptly or destroyed after the award of the bid. Contractor will include with the returned materials, a letter attesting to the complete return of materials, and documenting the destruction of copies and/or derivations. If materials are not returned, but instead destroyed, Contractor will submit a letter attesting to the destruction of all materials, copies and/or derivations.

Contractor must represent and warrant that, if their organization is awarded the Agreement by ASPA, for the Contract resulting from the Request for Bid, it will not enter into any agreements or discussions with a third party or subcontractor concerning such materials prior to receiving approval from ASPA that such third party or Subcontractor has been approved by ASPA.

Failure to comply with this confidentiality requirement will result in Contractor’s suspension from participating in future submittals as a Prime Contractor or Subcontractor.

2. OVERVIEW

**Purpose**

ASPA is soliciting this Request for Bid for a Special Systems Integrator (SSI) with a local presence and specific capabilities related to the procurement, integration and programming support of Portable TWIC Credential Readers, management software and wireless access points in a port and maritime environment. This work will be conducted at the Alabama State Port Authority.

**Background**

**The Alabama State Port Authority (ASPA) does not currently have an electronic access control system.**

This DHS, Port Security Grant Program (PSGP) funded scope of work addresses enhancement of Maritime Domain Awareness (MDA) by hardening the facility access points and by controlling and monitoring facility ingress and egress, for security as well as, life safety. In addition, MDA is enhanced by employing the use of TWIC standard based equipment and data management, which when networked could be shared with; ASPA, the Coast Guard and Law Enforcement. Furthermore, this exchange of electronic security information will serve as a “bridge” to enhance the current communications protocol and response procedures between ASPA and all other regulated entities.

The primary SRMP objective is to prevent unauthorized access to the port facility (water or land side) through target hardening, TWIC implementation and enhancement of entry points and a record of all
persons entering, and in heightened threat states, leaving. As a secondary, but equally important SRMP objective is MDA by design the portable readers will be able to look beyond the footprint of the facilities and will enhance the ASPA and U.S. Coast Guard ability to monitor and respond to suspicious activity in the sector. ASPA shall coordinate the portable TWIC reader capabilities and infrastructure closely with the U.S. Coast Guard to ensure compatibility and sharing of transmission burden.

3. OPERATIONAL AND PERFORMANCE OBJECTIVES
This project will serve to provide a TWIC screening and monitoring capability within the ASPA regulated footprint. It will include the installation of a new, secure / encrypted network of wireless access points throughout the port, connected to the ports recently contracted, near-Gigabit, security, wireless network. The portable readers can be distributed to each guardhouse at vehicle access points, as well as be available on a regular basis to “spot check” personnel attempting to gain access to the Port or personnel within the Port Facility as deemed necessary for TWIC status verification and authentication purposes. The ASPA Port Police Officers in patrol vehicles will utilize the Portable TWIC Readers for random screening to ensure TWIC authentication. Distributing portable TWIC card readers at all ASPA facility access points will comply with the TWIC procedures as listed in CFR 33 section 105.210 through 105.255.

Security Infrastructure
This component is the procurement and installation of minimal required security infrastructure to support the implementation of the portable TWIC readers. This includes, but is not limited to, the installation of conduit, communications cabling, electrical power, and wired / wireless network equipment.

Wireless Access Points
This component consists of the procurement, installation and integration of approved, encrypted, secure, wireless access points throughout the port.

Portable TWIC Readers
This component is the procurement and integration of portable TWIC readers as detailed in the Scope of Work section that follows.

4. PROJECT REQUIREMENTS
All components must be installed in a workmanlike manner, fully functioning and accepted by ASPA prior to final commissioning and payment

5. SCOPE OF WORK
The scope of this RFB is the procurement and installation / implementation of Portable TWIC Access Control Readers for the regulated entity, including the required management software and wireless access points. The following is a breakdown, and brief description, of each type of component to be implemented in this project:

Portable TWIC Readers MUST;
A. Be on the DHS/TWIC Initial Capability Evaluation List;
B. Be capable of accessing TWIC info via 1D/2D barcode, magnetic stripe, smart chip, proximity or RFID and biometrics;
C. Be capable of reading drivers licenses.
Portable TWIC Readers Request For Bids

**TWIC Reader Management Software**

- A. Be on the DHS/TWIC Initial Capability Evaluation List;
- B. Be capable of independently managing the readers and visitor/vendor records;
- C. Be capable printing FIPS-201 credentials;
- D. Be capable of connection to NCIC (option).

**Wireless Access Points**

- A. Be FIPS compliant;
- B. Be a, b, g and n capable;
- C. Be capable of 10/100/1000;
- D. Be capable of covering a minimum radius of 2000Lf (LOS).

6. **VERIFYING CONDITIONS**

Contractor(s) unfamiliar with the port should participate in a pre-bid conference and site visit (as required) on June 18, 2012 at 10 AM at the ASPA International Trade Center Building.

Before commencement of work, the Contractor will make a thorough examination of the work area and will report to ASPA, any and all conditions, which may interfere with, or otherwise affect or prevent the proper execution of the work. No work will commence until any and all such conditions have been corrected.

Failure to notify ASPA of unsatisfactory conditions will be construed as an acceptance of all conditions.

7. **OWNERS RIGHTS**

ASPA reserves the right to withdraw this RFB, reject any and all Bids, advertise for new Bids, or to proceed to accomplish the work by other means determined by ASPA, in its sole discretion, to be in the best interest of ASPA. ASPA may waive minor or technical irregularities in any Bid. A Bid, which is determined by ASPA, in its sole discretion, to be non-responsive in any material respect, may be disqualified from consideration. However, ASPA may request additional information from any Contractor in order to make a proposal responsive to this request, or to otherwise obtain clarification or additional information deemed by ASPA, in its sole discretion, necessary to analyze and compare the proposals.

By submitting a Bid in response to this RFB, and/or any communication, statement, act, or omission by representatives of ASPA, (including consultants), in the selection process, shall not vest any right, privilege, or right of action by any Contractor submitting a Bid.

8. **SCHEDULE**

The contractor shall deliver a detailed procurement, installation and integration schedule within seven (7) days after the execution of the Contract Notice of Award.

The Contractor shall schedule, layout, coordinate and install work in such time and manner not to delay, interfere or encumber the operations and safety of the site and general public.

As a deliverable, within seven (7) days after the execution of the Contract Notice of Award, Contractor shall submit to ASPA for review and acceptance, a preliminary work schedule in the form of Microsoft Project or Visio software and scheduling chart. The baseline schedule shall cover the mobilization, material procurement and installation activities as specified in this Provision.

All Bi-monthly Progress Schedule updates shall be plotted and updated against the approved Baseline Schedule.
9. SUBMITTALS
The submittal process is intended to ensure that the quantity, quality and functionality of products and materials installed on the project meet project specification. ASPA requires the Contractor to submit all components, samples, and products reviewed in the submittal process in a timely fashion.

Compliance Submittals include shop drawings, coordination drawings, product data, samples, and mockups, which are prepared by the Contractor, subcontractor, manufacturer, or supplier and submitted by the Contractor to ASPA as a method of approval of the use of equipment and materials proposed for incorporation in the work or as needed to describe installation, operation, maintenance or technical properties.

ASPA acknowledges that blueprints or rough drawings have been provided to Contractor by ASPA. Contractor shall provide drawings, diagrams and photographs, for purposes of implementing the Contract.

Such material shall include:

- Design and construction features, power requirements, control range, uniformity limits, and all pertinent dimensions
- Wiring diagrams
- Cut sheets and performance data of equipment, instrumentation and control panels
- Operation & Maintenance Manual(Submit in accordance with the general requirements of the Specification. Include instructions for operation, with pertinent control data and schematics, arrangement, and recommended maintenance or equipment.)

Submittals such as drawings, manuals, and data shall be of the quality for legibility and reproduction purposes, with every line, character and letter clearly legible, and for such drawings as reproducible prints usable for further reproduction to yield legible hard copy.

10. PRODUCT DELIVERY, STORAGE AND HANDLING
Arrange deliveries of equipment and materials in accordance with schedules, in ample time to facilitate inspection prior to installation, and to avoid work delays.

Deliver, store, and handle equipment and materials in accordance with manufacturer’s recommendations using means and methods that will prevent damage, deterioration, and loss (including theft).

Control delivery schedules to prevent long-term storage at the site and to prevent overcrowding of spaces and safety hazards. In particular, to coordinate delivery and installation to ensure minimum holding or storage items for items known or recognized to be flammable, hazardous, easily damaged or sensitive to deterioration and loss (including theft).

Avoid conflict with work of other contractors and ASPA's operations.
Deliver equipment and materials to the site in manufacturer’s sealed containers or other packaging system with identifying labels and instructions for handling, storing, unpacking, protecting and installing.

Mark deliveries of component parts of equipment to identify the equipment, to permit easy accumulation of parts, and to facilitate inspection and measurement of quantity or counting of units.

Immediately on delivery inspect shipment to assure product complies with requirements, Contract Documents, reviewed submittals, quantities are correct, containers and packages are intact, labels are legible and equipment/materials are properly protected and undamaged.

Provide equipment and personnel necessary to unload and handle equipment and materials by methods to prevent damage or soiling to equipment and materials or packaging.

Handle by methods to prevent bending or overstressing. Where lifting points are designated, lift components only at those points.

Provide additional protection to surrounding surfaces as necessary to prevent damage. Damage to surrounding surfaces or materials shall be repaired to ASPA’s satisfaction (by, or if need be on behalf of Contractor).

Store equipment and materials immediately on delivery and protect until completion of the work. (Store in accordance with manufacturer’s instruction with seals and labels intact and legible)

Store equipment and materials subject to damage by elements in weather-tight enclosures and protect from elements.

11. PROTECTION AFTER INSTALLATION
Provide covering and protection to equipment, components and devices as necessary to protect installed materials from damage from subsequent construction operations. Remove protective covers when no longer needed or as specified.

12. SYSTEM MAINTENANCE PROCEDURES
As a deliverable, the Contractor must provide a system maintenance procedure document and a written report certifying that all equipment is performing according to the operational, technical specifications and regulatory requirements.

Contractor maintenance procedure will include checking:

1. Hardware and software installation quality and function
2. Wiring, terminations and voltage supplies
3. Backup power supplies and UPS
4. Demonstrate how functional and operational objectives are met

In addition the Contractor must certify that all user manuals, system documentation (including system settings, usernames, passwords, warranty information/certificates, maintenance schedule and service contact numbers) are updated and received by ASPA.

13. SPECIFIED EQUIPMENT AND MATERIALS
The Contract is executed, on the basis of equipment and materials, as specified and of manufacturers and suppliers mentioned by name herein (without acceptance or consideration of possible substitutions
or “of equal items”). It is the Contractors responsibility to provide the items specified exactly as specified. No adjustment shall be made to this Contract for special or custom delivery, fabrication, handling or expediting of specified materials.

14. FINANCIAL PROPOSAL
The Contractor must complete the Financial Proposal Worksheet and provide all-inclusive pricing based on the combination of work categories as indicated on the Worksheet. In preparing the Financial Proposal Worksheet, the Contractor shall not change the work categories or line items on the Worksheet. This will ensure that all Financial Proposals are evaluated on the same information. The Contractor should assume that its initial Financial Proposal will be treated as its best and final offer. However, ASPA reserves the right to request additional best and final offers.

The Contractor shall submit all-inclusive pricing to include materials, equipment, transportation, overhead, payroll, general administration, licenses, fees, profit, taxes and fringe benefits.

The Price Proposal shall contain the following information.

1. Title page
2. Completed Price Certification and Financial Proposal Worksheet
3. An insurance certificate evidencing the coverage required
4. Price Proposals shall be typewritten or written legibly in ink and all erasures shall be initialed in ink by the signer.
5. Price Proposal shall be signed in (Blue) ink.

All Contractors must present pricing in the format provided. Do not alter or change any wording on the Financial Proposal Worksheet. No additions, conditions or amendments to the Financial Proposal Worksheet are permitted and such will cause the Contractor to be declared unacceptable. However, wherever possible, back-up or explanatory material may be submitted as clarification of cost/price proposed.
15. PRICE CERTIFICATION

PROPOSAL OF ______________________________________________________

Made this _______day of ______________________________, 2012

A. The undersigned hereby declares to have carefully examined this Request for Bids (RFB)

B. The undersigned proposes and agrees to furnish all services necessary for the performance of the above referenced contract in accordance with the RFB and all other contract documents referenced in the RFB

C. Contractor certifies that the pricing submitted by the Contractor via this Financial Proposal is firm for the duration of the contract term

D. Contractor certifies that its pricing on the Financial Proposal Worksheet is all-inclusive (i.e. “fully loaded”) pricing, to include, but not be limited to, materials, equipment, transportation, payroll, overhead, general administration, profit, taxes and fringe benefits.

______________________________                    __________________________
Contractor   Authorized Signature

______________________________                   ___________________________
DateTitle
FINANCIAL PROPOSAL WORKSHEET

Financial Proposals shall be submitted as follows and shall include all costs associated with the performance of this RFB. This pricing is to be all-inclusive. Contractor may be required to provide documentation, with the Financial Proposal on how each fully loaded cost was calculated.

Complete the following unit price schedule.

<table>
<thead>
<tr>
<th>Component</th>
<th>Units</th>
<th>Cost Per Unit</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portable TWIC Reader</td>
<td>7</td>
<td>$__________</td>
<td>$__________</td>
</tr>
<tr>
<td>Management Software</td>
<td>1</td>
<td>$__________</td>
<td>$__________</td>
</tr>
<tr>
<td>Installation of Management Software</td>
<td>1</td>
<td>$__________</td>
<td>$__________</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>6</td>
<td>$__________</td>
<td>$__________</td>
</tr>
<tr>
<td>Access Point Installation</td>
<td>6</td>
<td>$__________</td>
<td>$__________</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>$__________</td>
<td>$__________</td>
</tr>
</tbody>
</table>

Price Bid Compiled By: 

Title: 

Company:
# TABLE A

## ANTICIPATED PROCUREMENT PROCESS

<table>
<thead>
<tr>
<th>Stage</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution of RFB to Integrators</td>
<td>June 8, 2012</td>
<td>ASPA issues a Request for Bids to Integrators for 7 Portable TWIC Readers, Management software and 8 Wireless Access Points. Integrators will receive a complete bid package after executing a “non disclosure agreement” agreeing not to distribute or copy any portion of the bid documents and to return all bid package information after a successful bidder has been selected.</td>
</tr>
<tr>
<td>Pre-Proposal Conference at ASPA International Trade Center Building</td>
<td>1:00 p.m. June 18, 2012</td>
<td>An overview discussion of the scope of work, Contractors should plan to spend at least 2hrs on the site. Participation is not required in order to participate in the process.</td>
</tr>
<tr>
<td>RFI Cut-off for RFB</td>
<td>4:00 p.m. June 25, 2012</td>
<td>Request for information (questions) cutoff date for the RFB package.</td>
</tr>
<tr>
<td>Response to RFB</td>
<td>12:00 p.m. June 28, 2012</td>
<td>Firms submit their Bids.</td>
</tr>
<tr>
<td>Bid Evaluation</td>
<td>2:00 p.m. June 28, 2012</td>
<td>ASPA opens RFB’s and evaluates for best value recommendation to the selection committee.</td>
</tr>
<tr>
<td>Project Award</td>
<td>June 29, 2012</td>
<td>ASPA awards the Bid.</td>
</tr>
<tr>
<td>Notice to Proceed</td>
<td>June 29, 2012</td>
<td>ASPA issues official Notice to Proceed.</td>
</tr>
</tbody>
</table>
ADDENDUM TO BID

(Issued October 3, 2011)

Effective October 1, 2011, the Beason-Hammon Alabama Taxpayer and Citizen Protection Act ("the Act") requires that any business entity contracting with or proving any grant or incentives to the state, including the Alabama State Port Authority, certify compliance with the Act. Please have the appropriate individual with personal knowledge certify such compliance with the enclosed Affidavit and return it to the Alabama State Port Authority with your bid package. The Affidavit must be notarized.

(Continued on Next Page)
STATE OF ALABAMA : 
COUNTY OF MOBILE :

AFFIDAVIT AND CERTIFICATE OF COMPLIANCE

Before me, the undersigned authority, a Notary Public in and for said State and County, personally appeared ____________________, who is known to me and who, being by me first duly sworn, deposes and says as follows:

1. My name is ____________________, I am the ____________________ of ____________________ ("Company"), a company that contracts with and/or provides goods or services to the Alabama State Port Authority (ASPA) in Mobile, Alabama.

2. Company certifies that it does not knowingly employ, hire for employment or retain the services of any person who is not authorized to work in the United States as defined in 8 U.S.C. § 1324a(h)(3). Company further certifies that it is in full compliance with all federal and State of Alabama laws and regulations concerning the employment of non-citizens of the United States of America and will continue to remain in full compliance throughout the period Company contracts with or provides its goods or services to the Alabama State Port Authority.

3. Company further certifies that it is currently enrolled or will be enrolled in the E-Verify program administered by the United States Citizen and Immigration Services, the Department of Homeland Security and Social Security Administration or that it participates in the program through the Alabama Department of Homeland Security on or before January 1, 2012.

STATE OF ALABAMA :
COUNTY OF MOBILE :

The foregoing instrument was acknowledged before me this _____ day of ____________, 2011.

____________________________
NOTARY PUBLIC
State of Alabama
FORM FOR SECTIONS 9 (a) and (b) BEASON-HAMMON ALABAMA TAXPAYER AND CITIZEN PROTECTION ACT; CODE OF ALABAMA, SECTIONS 31-13-9 (a) and (b) AFFIDAVIT FOR BUSINESS ENTITY/EMPLOYER /CONTRACTOR
(To be completed as a condition for the award of any contract, grant, or incentive by the State of Alabama, any political subdivision thereof, or any state-funded entity to a business entity or employer that employs one or more employees)

State of ________________________________________________________________________
County of _______________________________________________________________________

Before me, a notary public, personally appeared ______________________________ (print name) who, being duly sworn, says as follows:

As a condition for the award of any contract, grant, or incentive by the State of Alabama, any political subdivision thereof, or any state-funded entity to a business entity or employer that employs one or more employees, I hereby attest that in my capacity as __________________________ (state position) for ____________________________ (state business entity/employer/contractor name) that said business entity/employer/contractor shall not knowingly employ, hire for employment, or continue to employ an unauthorized alien.

I further attest that said business entity/employer/contractor is enrolled in the E-Verify program.

(ATTACH DOCUMENTATION ESTABLISHING THAT BUSINESS ENTITY/EMPLOYER/CONTRACTOR IS ENROLLED IN THE E-VERIFY PROGRAM)

_________________________________ Signature of Affiant

Sworn to and subscribed before me this _____ day of ___________________, 20__.

I certify that the affiant is known (or made known) to me to be the identical party he or she claims to be.

_________________________________ Signature and Seal of Notary Public

Author: Jean Brown
Statutory Authority: Code of Alabama, sections 31-13-9 (a) and (b); Section 31-13-9 (h).
APPENDIX A

TSA/DHS TWIC Specification
&
Initial Capabilities Evaluation List

JUNE 2012
INITIAL CAPABILITY EVALUATION LIST

Updated: 12 January 2012

PURPOSE: The Initial Capability Evaluation (ICE) List includes information on all readers that demonstrated to the Transportation Security Administration and the U.S. Coast Guard successful completion of the evaluation. Broad Agency Announcements (BAA) available elsewhere on this web site contain details of the ICE and other information about the Transportation Worker Identification Credential (TWIC) reader testing program.

DISCLAIMER: This list serves no other purpose other than to identify readers that have demonstrated their ability to complete the ICE satisfactorily.

UPDATES: The ICE List will be updated from time to time as more readers complete the ICE.

DESCRIPTION OF THE ICE LISTS:

Two ICE lists are maintained.

The first list details portable and fixed readers which directly support the TWIC Privacy Key (TPK) enciphered on-card reference biometrics during registration and in operation.

The second list details portable and fixed readers which implement an alternate operational biometric solution. The TPK enciphered on-card reference biometrics is used only during registration into a Physical Access Control System (PACS) prior to having the cardholder biometrically enroll. (Such a verification and validation process of the card and cardholder prior to local enrollment into an operational biometric solution is required to preserve the Chain of Trust).
**INITIAL CAPABILITY EVALUATION LIST**

*Portable Readers Using TWIC TPK and TWIC Reference Biometrics*

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Hardware Manufacturer/ Model</th>
<th>Software Company/Product</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codebench</td>
<td>Cross Match/ Be.U Mobile</td>
<td>Codebench/ OMNิcheck</td>
<td><a href="http://www.codebench.com">www.codebench.com</a></td>
</tr>
<tr>
<td>Codebench</td>
<td>DAP/ CE3240BWE</td>
<td>Codebench/ OMNิcheck</td>
<td><a href="http://www.codebench.com">www.codebench.com</a></td>
</tr>
<tr>
<td>Codebench</td>
<td>Datastrip/ DSV2+Turbo</td>
<td>Codebench/ OMNิcheck</td>
<td><a href="http://www.codebench.com">www.codebench.com</a></td>
</tr>
<tr>
<td>Codebench</td>
<td>Datastrip/ DSV3</td>
<td>Codebench/ OMNิcheck</td>
<td><a href="http://www.codebench.com">www.codebench.com</a></td>
</tr>
<tr>
<td>Codebench</td>
<td>MaxID/ iDL500</td>
<td>Codebench/ OMNิcheck</td>
<td><a href="http://www.codebench.com">www.codebench.com</a></td>
</tr>
<tr>
<td>Codebench</td>
<td>MorphoTrak/ MorphoCheck</td>
<td>Codebench/ OMNิcheck</td>
<td><a href="http://www.codebench.com">www.codebench.com</a></td>
</tr>
<tr>
<td>CoreStreet</td>
<td>DAP/ 3240B</td>
<td>CoreStreet/ Pivman</td>
<td><a href="http://www.corestreet.com">www.corestreet.com</a></td>
</tr>
<tr>
<td>CoreStreet</td>
<td>Crossmatch/ BE.U</td>
<td>CoreStreet/ Pivman</td>
<td><a href="http://www.corestreet.com">www.corestreet.com</a></td>
</tr>
<tr>
<td>CoreStreet</td>
<td>DataStrip/ DSV2 Plus Turbo</td>
<td>CoreStreet/ Pivman</td>
<td><a href="http://www.corestreet.com">www.corestreet.com</a></td>
</tr>
<tr>
<td>Cross Match</td>
<td>Crossmatch/ BE.U SMC-800</td>
<td>CoreStreet/ Pivman</td>
<td><a href="http://www.crossmatch.com">www.crossmatch.com</a></td>
</tr>
<tr>
<td>DataStrip/Codebench</td>
<td>Datastrip/ DSV II SC</td>
<td>Codebench/ TWICCheck</td>
<td><a href="http://www.datastrip.com">www.datastrip.com</a></td>
</tr>
<tr>
<td>idSoftware</td>
<td>MC 75a</td>
<td>idSoftware/ SecureGate Ports</td>
<td><a href="http://www.idsoftware.us">www.idsoftware.us</a></td>
</tr>
<tr>
<td>MaxID</td>
<td>MaxID/ iDLMAX G</td>
<td>Corestreet/ Pivman</td>
<td><a href="http://www.maxidgroup.com">www.maxidgroup.com</a></td>
</tr>
<tr>
<td>MaxID</td>
<td>MaxID/ iDL500/ iDL500i</td>
<td>MaxID/ MaxiDentity Suite TWIC Application</td>
<td><a href="http://usa.maxidcorp.com/idl500.php">http://usa.maxidcorp.com/idl500.php</a></td>
</tr>
<tr>
<td>MaxID</td>
<td>MaxID/ iDL300</td>
<td>MaxID/ MaxiDentity Suite TWIC Application</td>
<td><a href="http://usa.maxidcorp.com/idl300.php">http://usa.maxidcorp.com/idl300.php</a></td>
</tr>
<tr>
<td>Mobilisa</td>
<td>Moblisa/ IM2700</td>
<td>Moblisa/ Defense ID</td>
<td><a href="http://www.icmobil.com">www.icmobil.com</a></td>
</tr>
<tr>
<td>MorphoTrak</td>
<td>PSION Teklogix/ Workabout Pro</td>
<td>MorphoTrak/ TWIC PIV Morphocheck</td>
<td><a href="http://www.morpho.com">www.morpho.com</a></td>
</tr>
<tr>
<td>Motorola</td>
<td>Motorola/ MC 75</td>
<td>Motorola Mobile Software</td>
<td><a href="http://www.motorola.com/biometrics">www.motorola.com/biometrics</a></td>
</tr>
</tbody>
</table>
## Fixed Readers Using TWIC TPK and TWIC Reference Biometrics

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Hardware Manufacturer/Model</th>
<th>Software Company/Product</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3M Cogent, Inc.</strong></td>
<td>MIY-ID GOV</td>
<td>3M Cogent, Inc.</td>
<td><a href="http://www.cogentsystems.com">www.cogentsystems.com</a></td>
</tr>
<tr>
<td><strong>3M Cogent, Inc.</strong></td>
<td>MIY-Card GOV</td>
<td>3M Cogent, Inc.</td>
<td><a href="http://www.cogentsystems.com">www.cogentsystems.com</a></td>
</tr>
<tr>
<td>Innometriks</td>
<td>Innometriks/Rhino-XS-TWIC</td>
<td>Innometriks/Rhino Software</td>
<td><a href="http://www.innometriksinc.com">www.innometriksinc.com</a></td>
</tr>
<tr>
<td>L-1 Identity Solutions</td>
<td>L-1 Identity Solutions / 4G PIV-TWIC Station Extreme²</td>
<td>L-1 Identity Solutions/ Secure Admin</td>
<td><a href="http://www.l1id.com/pages/666-4g-piv-twic-station-extreme">http://www.l1id.com/pages/666-4g-piv-twic-station-extreme</a></td>
</tr>
<tr>
<td>L-1 Identity Solutions</td>
<td>L-1 Identity Solutions / 4G PIV-TWIC Station²</td>
<td>L-1 Identity Solutions/ Secure Admin</td>
<td><a href="http://www.l1id.com/pages/666-4g-piv-twic-station">http://www.l1id.com/pages/666-4g-piv-twic-station</a></td>
</tr>
<tr>
<td>L-1 Identity Solutions</td>
<td>L-1 Identity Solutions / TWIC-Station</td>
<td>L-1 Identity Solutions/ Secure Admin</td>
<td><a href="http://www.l1id.com/pages/494-bioscrypt-twic-station">www.l1id.com/pages/494-bioscrypt-twic-station</a></td>
</tr>
<tr>
<td>L-1 Identity Solutions</td>
<td>L-1 Identity Solutions / TWIC-Station</td>
<td>L-1 Identity Solutions/ Secure Admin</td>
<td><a href="http://www.l1id.com/pages/494-bioscrypt-twic-station">www.l1id.com/pages/494-bioscrypt-twic-station</a></td>
</tr>
<tr>
<td>MorphoTrak</td>
<td>MorphoTrak/ MA120w</td>
<td>MorphoTrak/ MA120w</td>
<td><a href="http://www.morpho.com">www.morpho.com</a></td>
</tr>
<tr>
<td>MorphoTrak</td>
<td>MorphoTrak/ MA521</td>
<td>MorphoTrak/ MA521</td>
<td><a href="http://www.morpho.com">www.morpho.com</a></td>
</tr>
<tr>
<td>MorphoTrak</td>
<td>MorphoTrak/ OMA521 Outdoor</td>
<td>MorphoTrak/ MA521</td>
<td><a href="http://www.morpho.com">www.morpho.com</a></td>
</tr>
<tr>
<td>Veridt</td>
<td>Veridt/ 900W1020</td>
<td>Veridt/PIVCheck</td>
<td><a href="http://www.veridt.com">www.veridt.com</a></td>
</tr>
</tbody>
</table>
### Readers Using Non-TWIC Operational Biometrics

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Hardware Manufacturer /Model</th>
<th>Software Company/Product</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Techsphere</td>
<td>Techsphere/VP-II</td>
<td>Techsphere/NetControl-TWIC</td>
<td><a href="http://www.tech-sphere.com">www.tech-sphere.com</a></td>
</tr>
<tr>
<td>TopTech (Fingerprint BIO)</td>
<td>TopTech/RCU II /w veriFID</td>
<td>TopTech/TMS/VeriFID</td>
<td><a href="http://www.toptech.com">www.toptech.com</a></td>
</tr>
</tbody>
</table>

Note:  
1. The readers added for this update is shown in **bold italics**.  
2. Readers are **listed in alphabetical order by vendor name**. All readers listed have satisfactorily completed the ICE.
TWIC Reader Hardware
And
Card Application Specification

May 30, 2008

Department of Homeland Security
Transportation Security Administration
Transportation Threat Assessment and Credentialing Office
601 S. 12th Street
Arlington, VA 22202
## VERSION CONTROL

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>Initial release of the specification.</td>
</tr>
<tr>
<td>September 11, 2007</td>
<td></td>
</tr>
<tr>
<td>Version 1.1</td>
<td>Clarification and technical corrigendum of Version 1 of the specification.</td>
</tr>
<tr>
<td>March 28, 2008</td>
<td>Revisions are detailed in Section 1.3 of this document.</td>
</tr>
<tr>
<td>Version 1.1.1</td>
<td>Amendment 1 to the March 28, 2008 release of the specification for</td>
</tr>
<tr>
<td></td>
<td>additional clarification and minor reorganization of the document.</td>
</tr>
<tr>
<td></td>
<td>Revisions are detailed in Section 1.3 of this document.</td>
</tr>
</tbody>
</table>
# Table of contents

1. Overview ........................................................................................................................................... 7  
   1.1 Abstract ........................................................................................................................................ 7  
   1.2 Scope and purpose ......................................................................................................................... 7  
   1.3 Summary of Changes to the March 28, 2008 Specification .......................................................... 7  
   1.4 Summary of Changes to the September 11, 2007 Specification .................................................. 9  
   1.5 Summary of Changes to the NMSAC Specification .................................................................... 11  

2. References ......................................................................................................................................... 14  
   2.1 Normative References .................................................................................................................. 14  
   2.2 Informative References ................................................................................................................ 15  

3. Definitions ......................................................................................................................................... 16  
   3.1 Conformance levels ....................................................................................................................... 16  
   3.2 Glossary of terms .......................................................................................................................... 16  
   3.3 Acronyms and abbreviations ......................................................................................................... 17  

4. TWIC Modes of Operation ............................................................................................................. 18  
   4.1 General ........................................................................................................................................ 18  
   4.2 System Perspective ....................................................................................................................... 19  
      4.2.1 Physical Access Control ........................................................................................................ 19  
      4.2.2 Portable Identity Verification .............................................................................................. 22  

5. Fixed TWIC Reader Requirements .................................................................................................. 24  
   5.1 Physical Requirements ................................................................................................................ 24  
      5.1.1 TWIC Reader Dimensions ................................................................................................... 24  
      5.1.2 TWIC Reader Mounting ........................................................................................................ 24  
      5.1.3 Environmental ....................................................................................................................... 24  
      5.1.4 Impact Resistance .................................................................................................................. 25  
   5.2 Electrical Requirements .............................................................................................................. 25  
   5.3 Safety .......................................................................................................................................... 25  
   5.4 Electromagnetic/Vibration Compatibility ..................................................................................... 25  
      5.4.1 47CFR18 and/or CISPR 11 (Emissions) ................................................................................ 26  
      5.4.2 IEC 61000-4-2 (Electrostatic Discharge) ............................................................................. 26  
      5.4.3 IEC 61000-4-3 (Radiated RF Immunity) .............................................................................. 26  
      5.4.4 IEC 61000-4-4 (Electrical Fast Transient/Burst) ................................................................. 26  
      5.4.5 IEC 61000-4-6 (Radio Frequency Common Mode) .......................................................... 26  
      5.4.6 IEC 61000-4-5 (Surges) ....................................................................................................... 26  
      5.4.7 IEC 61000-4-8 (Power Frequency Common Mode) .......................................................... 26  
      5.4.8 IEC 61000-4-11 (Voltage Dips and Interruptions) .............................................................. 27  

6. Portable TWIC Reader Requirements ............................................................................................... 28  
   6.1 Portable TWIC Reader Specific Requirements: .......................................................................... 28  
      6.1.1 Operational Features ............................................................................................................ 28  
      6.1.2 Environmental Requirements ............................................................................................. 28  
      6.1.3 Electrical Requirements ..................................................................................................... 29  

7. TWIC Reader Operational Requirements ..................................................................................... 30  

8. Performance Requirements ............................................................................................................ 33
9. Operational Availability ........................................................................................................................................34

10. Delivery ..........................................................................................................................................................35

11. TWIC Card Application ................................................................................................................................36
   11.1 Card application Identifier ........................................................................................................................36
   11.2 Key Reference(s) ......................................................................................................................................36
   11.3 ICC Data Model .......................................................................................................................................36
   11.4 Magnetic Stripe Data Model ......................................................................................................................39
   11.5 TWIC Card Application Command Set ....................................................................................................39
       11.5.1 SELECT ...........................................................................................................................................40
       11.5.2 GET DATA ......................................................................................................................................41

Appendix A Authentication Processing (NORMATIVE) ..................................................................................43
   A.1 CHUID Verification ....................................................................................................................................46
   A.2 Active Card Authentication ........................................................................................................................47
   A.3 CHUID Verification + Biometric User Authentication .............................................................................49
   A.4 CHUID Signing Certificate + Active Card Authentication + Biometric User Authentication ..............50

Appendix B TWIC Privacy Key Network Processing (INFORMATIVE) ..........................................................52

Appendix C TWIC Reader Adaptability (NORMATIVE) ....................................................................................54
   C.1 Change of operation mode .........................................................................................................................54
   C.2 Accepting new operating modes ...............................................................................................................54

Appendix D TWIC Reader Compatibility With Other Card Types (INFORMATIVE) ......................................55

Appendix E TWIC AID Structure (NORMATIVE) ............................................................................................56
   E.1 Registered Identifier (RID) .........................................................................................................................56
   E.2 Proprietary Identifier Extension (PIX) Structure ......................................................................................56

Appendix F Use of Get Response APDU at the application layer (INFORMATIVE) .......................................58

Appendix G Interpretation of the Biometric Template CBEFF Header (NORMATIVE) ......................................60
List of figures

Figure 4.1 Generic Biometric-based Access Control System (ACS) ................................................................. 20
# List of tables

Table 4.1 TWIC Identification and Authentication Modes

Table 4.2 Biometric Access System Key Descriptions

Table 4.3 Portable Card TWIC Reader Hardware Requirements

Table 7.1 75-bit Wiegand Output Format

Table 7.2 48-bit Wiegand Output Format

Table 11.1 Unsigned Card Holder Unique Identifier

Table 11.2 TWIC Key Privacy Buffer

Table 11.3 Signed Card Holder Unique Identifier

Table 11.4 Card Holder Enciphered Fingerprint Templates

Table 11.5 Security Object

Table 11.6 Data Objects in the TWIC Card application Property Template (Tag '61')
1. Overview

1.1 Abstract

This document specifies the behavior at the card interface of the TWIC card application as well as the requirements for TWIC readers, both fixed and portable, to be used with the Transportation Worker Identification Credential (TWIC).

This specification was initially developed by the National Maritime Security Advisory Committee (NMSAC) in response to a request from the Transportation Security Administration (TSA) and the U.S. Coast Guard. The NMSAC TWIC Working Group included members of the maritime industry with support from representatives from the security technology industry who are affiliated with such organizations as the International Biometric Industry Association (IBIA), the Security Industry Association (SIA) and the Smart Card Alliance. The original specification developed by the NMSAC TWIC Working Group has been modified to accommodate TSA security and privacy requirements.

1.2 Scope and purpose

The scope of this specification is:

- TWIC reader requirements
- TWIC card application data model
- TWIC card application card edge behavior during normal operation

The mission of the TWIC program is to design and field a common credential for all transportation workers requiring unescorted physical and logical access to secure areas of the nation’s transportation system and their associated information systems. In its development, TWIC has been designed as a standards-based program, and conforms to the standards referenced in this document. This specification enables varying levels of control in support of threat level risk mitigation plans.

1.3 Summary of Changes to the March 28, 2008 Specification

Version 1.1 Amendment 1 of this specification is a further clarification of the specification that includes some reorganization of the document for purposes of clarity.

All comments, suggestions or additional change requests should be directed to the Project Editor, Gerald.Smith@associates.dhs.gov.

Summary of changes is as follows:

1) Revised Version Control table to reflect Amendment 1 changes.
2) General corrections for spacing and misspelling not caught in the March 28, 2008 release.
3) Revised the date of the document on the cover and on each page to May 30, 2008.
4) Reformatting of Table of Contents.
5) Added Section 1.3 detailing the changes from the March 28, 2008 release of the specification.
6) Revised Section 1.4 language from “Section 1.4 of this” to “Section 1.5 of this”.
7) Moved the sentence “All comments, suggestions…” from Section 1.4 to Section 1.3.
8) Section 2.1 added normative reference to SP800-96 which details APDU buffer size requirements.

9) Added Section 4.1 General to properly align Headings in Section 4.

10) Revised Table 4.1 for naming of Identification / Authentication entries, clarified comments to include referencing the appropriate section of Appendix A. [Appendix A sections reorganized and renamed to match Table 4.1].

11) Revised Table 4.1 to change “dual factor” to “two factors”.

12) Section 4.1, last paragraph added “Note: All data shall be retrieved from the TWIC card application except for operations involving Active Card Authentication”.

13) Sections 4.2.1.2 and 4.2.1.3 removed “Biometric” from the title and performed minor rewording to properly reflect the steps indicated may be executed dependent on mode as defined in Table 4.1.

14) Section 6, 4th paragraph added “A portable TWIC reader shall be capable of downloading and using the most recent TWIC Hotlist. A portable TWIC reader may support a Certificate Revocation List (CRL) subject to availability of a network connection.”

15) Section 6, sub-section 6.1.1 added the sentence “Portable TWIC readers shall have a real time clock.”

16) Section 7, Table 7.1 changed “Credential Code” to “Credential Number” to harmonize this specification with other Government PACS specifications referencing the FASC-N.

17) Section 7, added text just before the Wiegand 75-bit description of “Due to the particulars of TWIC card issuance a minimum of 4 data elements of the FASC-N should be read and forwarded to the PACS. These data elements are the Agency Code, System Code, Credential Number and the Individual Credential Issue.”

18) Section 7, paragraph below Table 7.1 changed the wording to “Fixed TWIC readers may support an additional Wiegand output format of 48 bits when”.

19) Section 7, below Table 7.2 added Note 1 detailing the format of the Credential Number the TWIC reader shall use to transmit both the Credential Number and the Individual Credential Issue values to the PACS. This combining of fields is required to enable the PACS to identify lost and stolen TWIC cards when using the GSA specified Wiegand output formats.

20) Section 7, first paragraph below Table 7.2 changed to “Fixed TWIC readers may support other additional Wiegand formats for legacy systems. Wiegand output formats not detailed in this specification may transmit the entire FASC-N or selected elements of the FASC-N.”

21) Section 7, 4th paragraph from the end changed “a log of operations” to “a time-stamped log of operations”.

22) Section 11.3, Note #2 below Table 11.4 added the guidance “Deciphering of the biometric template should be performed using the “no padding” option of the AES algorithm.” This change is made to alert TWIC reader manufacturers to the necessary decipherment mode to be used for TWIC cards issued prior to May 9, 2008.

23) Section 11.5.1, Table 11.6 changed the Application Template Length from “Var” to ‘16’ (22 decimal) as the Answer to Select is a fixed structure for this Version of the specification. Also replaced “see” with “Refer to” for this same row in the table.

24) Appendix A reorganized to have sub-sections match the entries in Table 4.1 (for clarity).

25) Appendix A, PIV and TWIC Object Identifiers, last row changed “The TWIC NACI” to “The TWIC Threat Assessment”.

26) Appendix A, sub-section A.1 4th paragraph changed to “When the TWIC reader is configured for CHUID signature verification it shall perform the following steps:”
27) Appendix A, sub-section A.1 step 3) changed to read “TWIC reader shall decode the Issuer Asymmetric Signature Object (tag: 0x3E) from the CHUID in order to retrieve the card issuer’s digital signature certificate for the document signer (guaranteeing the CHUID was created by an accredited issuer) that is used to verify the signed objects on the card “

28) Appendix A, sub-section A.1 first bulleted list added a line after Step 3 of “4) TWIC reader shall verify the CHUID signature and origin up to and including the trust anchor.”

29) Appendix A, sub-section A1. added new paragraph below the bulleted list providing an alternate way to verify the CHUID using the unsigned CHUID and the Security Data Object.

30) Appendix A, sub-section A.1 changed “Individual Credential Number” to “Individual Credential Issue” to harmonize this specification with other Government PACS specifications referencing the FASC-N.

31) Appendix A, sub-section A.1 last paragraph changed “may be used for access” to “shall be used for access”.

32) Appendix A, sub-section A.2 changed to “Active Card Authentication” and text from previous A.3 moved to this section. Table 4.1 Row 2 now matches Appendix A sub section A.2.

33) Appendix A, sub-section A.2 6th paragraph changed to “The output of a TWIC reader, upon successful authentication, depends on the infrastructure capabilities and requirements. When card authentication is performed, the TWIC reader shall obtain the encoded FASC-N and expiration date from the Card Authentication Certificate.”

34) Appendix A, Section A.3 title changed to “CHUID Verification + Biometric User Authentication”.

35) Appendix A, Section A.3 2nd paragraph changed “then matched” to “matched” to clarify the order of the steps may vary depending on TWIC reader implementation.

36) Appendix A, Section A.3 first bulleted list Step 4 added “and CHUID”.

37) Appendix A, Section A.3 Bullet 8 sub-bullet “a” first sentence changed to read as “The TWIC reader shall retrieve the expiration date from the CHUID and the document signer’s certificate from the CHUID signature field, since the CHUID shall be signed by the same entity as the biometric.”.

38) Appendix A, Section A.3 Bullet 8 sub-bullet “b” deleted as it conflicted with the amended sub-bullet “a” statement immediately above.


40) Appendix D, 3rd paragraph deleted as it conflicted with Section 4.1 that requires all but the Card Authentication certificate data to be retrieved from the TWIC card application.

1.4 Summary of Changes to the September 11, 2007 Specification

Version 1.1 of this specification is a clarification and correction of the September 11, 2007 release of the TWIC Reader Hardware and Card Application Specification. Section 1.5 of this document was not included in the editorial process so as to preserve the original comments as written in the September 11, 2007 release.

Summary of changes is as follows:

1) General editorial changes from “must” to “shall”.

2) General editorial changes from “will” to “shall”.

3) General editorial changes from “would” or “could” to “should”.
4) General editorial changes from “might” to “may”.
5) General editorial changes from “can” to “may”.
6) General editorial changes from “terminal” to “TWIC reader”.
7) General editorial changes from “device” to “TWIC reader”.
8) General editorial changes from “crypt” to “cipher”.
9) General editorial changes from “magstripe” to “magnetic stripe”.
10) General editorial changes to use “TWIC reader” instead of “reader” as appropriate for purposes of clarity.
11) General editorial changes to use the term “template” in a consistent manner throughout the document.
12) General editorial changes from “enrollment” to “registration” when referring to a PACS.
13) General editorial changes to correct spelling errors.
14) General editorial changes to provide alternate expression for the purpose of clarity.
15) General formatting changes for consistency.
16) Addition of a Version Control table at the beginning of the document.
17) Revised the date of the document on the cover and on each page to March 28, 2008.
18) Added Section 1.3 detailing the changes from the September 11, 2007 release of the specification.
19) Added definitions in Section 3.1 for the terms “informative” and “normative”.
20) General editorial changes to Table 4.2 for harmonization of the text to Figure 4.1.
21) Revised the sequence of steps in Section 4.2.1.3 to read the TPK from the magnetic stripe later in the sequence (as the magnetic stripe reading step is conditional upon TWIC reader mode and successful processing of the CHUID).
22) Modified the language in Section 5.1.2 on tamper evident means by the substitution of “will have the ability to send…” for “should have the ability to send…”.
23) Section 5.1.3.1, revised sub-headers to include the language “Use requirements” to clarify said requirements only apply when the TWIC reader is to operate in the specified environment.
24) Revised language in Section 7 related to an automated alert which now states “… lockout after a configurable number of consecutive failed biometrics matching attempts”.
25) Section 11.3 First Table header modified to indicate Maximum Length is in bytes.
26) Section 11.3 First Table corrects the length of the signed CHUID from 3000 bytes to 3377 bytes as specified in SP 800-73 Revision 1.
27) Section 11.3 First Table corrects the length of the Security Object from 920 bytes to 1000 bytes as specified in SP 800-73 Revision 1.
28) Section 11.3 First Table Note 4 revised to remove the incorrect reference to the TPK hash being present in the Security Object.
29) Section 11.3, Table 11.5 Note 1 removed the incorrect reference to the TWIC Privacy Key hash in the description of hashes represented in the Security Object.
30) Section 11.3, Table 11.5 Note 2 added the word “signed” just before CHUID for clarity.
31) Section 11.5 reworded Notes 2 and 3 for clarity.
1.5 Summary of Changes to the NMSAC Specification

Version 1.0 of this specification is based upon the NMSAC Alternate TWIC Reader Hardware and Card Application Specification, Feb 28, 2007 specifying encryption of biometric templates using a TWIC Privacy Key (TPK). Summary of additional changes is as follows:

1) Section 2.1 Normative References. NIST SP-800-76-1, NIST SP-800-73 Revision 1 and SP 800-78-1 added as normative references.
2) Section 4, TWIC Modes of Operation. Requirement for specific authentication modes to be used at specific MARSEC levels has been removed and available authentication modes have been clarified.

3) Section 4, TWIC Modes of Operation. Ability to configure specific authentication modes to be used at differing MARSEC levels has been added.

4) Section 4, TWIC Modes of Operation. Verification of CHUID signature changed to mandatory. CHUID signature is either verified once, at the time of Physical Access Control System (PACS) enrollment (white list) or by the TWIC reader each time the CHUID is read.

5) Section 5.1.1, Device Dimensions. Note added to stress contactless reader sensitivity to location and electromagnetic conditions of their environment.

6) Section 6, Portable Reader Requirements. Requirements for confidentiality and authentication added for wireless devices used in physical access systems.

7) Section 6, Portable Reader Requirements. Requirement added for handheld devices to have a contactless interface and a mag-stripe reader, or a contact interface for TPK and biometric access or a contact only interface using the PIV card application requiring PIN support to access the biometric template.

8) Section 7, Operational Requirements. Contactless transmission speed requirement changed to support 106kbit/s, 212kbit/s or 424kbit/s, based on the card's capabilities.

9) Section 7, Operational Requirements. Requirement added to reject transaction if multiple cards are simultaneously detected in the reader’s contactless field.

10) Section 8, Performance Requirements. Support for biometric liveness detection strengthened from “may” to “should” indicating a strong preference for liveness detection rather than an option.

11) Section 11, TWIC Card Application. As for PIV, the TWIC application does not need to be the default selected application. This requires an explicit Application Select of the application. It has been added to the specification the Select Application Protocol Data Unit APDU command issued by the TWIC terminal should ask only for the 9 first bytes of the TWIC application AID allowing to find out from the card the TWIC version and nature (test or not) of the application in the card.

12) Section 11.2 Key reference. An explicit reference to SP 800-78-1 has been added.

13) Section 11.3 ICC Data Model. Modification of the Transportation Worker Unique Information data object into Unsigned Cardholder Unique Identification data object in order to align TWIC on the SP800-73-2. Structure, Tag reference and Container ID aligned on the next version of SP800-73. Maximum length of buffers has been adjusted to take into account the TWIC requirements.

14) Section 11.3 The Unsigned Cardholder Unique Identifier has been aligned on the next version of SP 800-73.

15) Section 11.4 The Magstripe Model has been completed and detailed.

16) 11.5.1 Select Command. The requirement for terminals to use a partial select (TWIC AID truncated) has been added to the specification. The information returned by the Select command has been corrected to be in line with ISO/IEC 7861-4. Possible Return codes have been added.

17) 11.5.2 Get Data APDU command. Information about the Length of requested data objects as well as return codes have been added.

18) Section 11.6 Sample Card Data removed from the specification.

19) Appendix A.1, CHUID Authentication. CHUID authentication clarified.


22) Appendix A.3, Card Authentication Key Authentication. Card Authentication Key usage clarified to indicate that it is only available via the PIV application, and is not shared with the TWIC application.

23) Appendix C, MARSEC Level Processing modified to indicate the reader needs to be adaptable to various changes (security threat level and revision of software)

24) Appendix D, TWIC Reader Compatibility with Other Card Types. Reader compatibility and default card support clarified and modified to allow configuration of default AID in the reader selection mechanism.

25) Appendix E, Description of Concept for Contactless Biometric Data Protection for TWIC provided redundant and out of scope information and was deleted.

26) Appendix F (now Appendix E), Proposed TWIC AID Structure. TSA RID added, AID structure clarified.

27) Appendix F added describing the use of the Get Response APDU at the application layer interface.
2. References

2.1 Normative References

[R1] ANSI/INCITS 383, Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers


[R4] NISTIR 6529A, Common Biometric Exchange Formats Framework (CBEFF)

[R5] NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007


[R7] NIST Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for PIV, August 2007

[R8] ISO/IEC 7816, Identification cards – Integrated circuit(s) cards with contacts

[R9] ISO/IEC 14443, Identification cards – Contactless integrated circuit(s) cards – Proximity cards


[R11] FIPS 186-2, Digital Signature Standard

[R12] FIPS 197, Advanced Encryption Standard

[R13] FIPS 46-3, Data Encryption Standard

[R14] FIPS 140-2, Security Requirements for Cryptographic Modules

[R15] UL 294, Standard for Safety of Access Control System Units


[R19] IEC 61000-4-2 (Electrostatic Discharge)

[R20] IEC 61000-4-3 (Radiated RF Immunity)

1 Normative references apply only to the extent specifically cited in this document.
[R21] IEC 61000-4-4 (Electrical Fast Transient/Burst)

[R22] IEC 61000-4-6 (Radio Frequency Common Mode)

[R23] IEC 61000-4-5 (Surges)

[R24] IEC 61000-4-8 (Power Frequency Common Mode)

[R25] IEC 61000-4-11 (Voltage Dips and Interruptions)


[R28] OSHA Regulation 1910.147 De-energizing Equipment

[R29] MIL-STD 810F Series of standards are issued by the United States Army's Developmental Test Command, to specify various environmental tests to prove that equipment qualified to the standard will survive in the field


### 2.2 Informative References

[R32] FIPS Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (March 14, 2006)


[R35] ICAO 9303 Machine Readable Travel Documents

[R36] GlobalPlatform Messaging Specification, Version 1.0, Nov. 2003 (Provides a definition of all the roles and responsibilities for all the actors (systems) in a multi application smart card infrastructure and defines reference standard on information exchange (message) between actors)


[R38] ANSI/SIA OSIPS ACOV-01:200x (Under Development). The OSIPS (Open, Systems Integration and Performance Standards) data models are defining interoperability between components in traditional access control systems.
3. Definitions

3.1 Conformance levels

3.1.1 expected: A key word used to describe the behavior of the hardware or software in the design models presumed by this specification. Other hardware and software design models may also be implemented.

3.1.2 informative: portion of the document that explains the specification or provides guidance on the use of the specification.

3.1.3 may: A key word indicating flexibility of choice with no implied preference.

3.1.4 normative: portion of the document that details the requirements of the specification.

3.1.5 shall: A key word indicating a mandatory requirement. Designers are required to implement all such mandatory requirements.

3.1.6 should: A key word indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase is recommended.

3.2 Glossary of terms

3.2.1 TWIC card: A smart card that corresponds to the specifications laid out for the Transportation Workers Identity Credential Program.

3.2.2 TWIC Privacy Key: A 128-bit AES key value used to encipher the biometric templates that are stored on the TWIC card.

3.2.3 Minutiae template: A minutiae template is a mathematical representation of the friction ridge characteristics that are used to individualize a fingerprint image. Minutiae are the points where friction ridges begin, terminate, or split into two or more ridges. In many fingerprint systems, the minutiae (as opposed to the images) are compared for recognition purposes.
### 3.3 Acronyms and abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APDU</td>
<td>Application Protocol Data Unit</td>
</tr>
<tr>
<td>BAC</td>
<td>Basic Access Control</td>
</tr>
<tr>
<td>CBEFF</td>
<td>Common Biometric Exchange Formats Framework</td>
</tr>
<tr>
<td>CHUID</td>
<td>Card Holder Unique Identifier</td>
</tr>
<tr>
<td>FASC-N</td>
<td>Federal Agency Smart Credential Number</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>IBIA</td>
<td>International Biometric Industry Association</td>
</tr>
<tr>
<td>IP</td>
<td>Ingress Protection (rating)</td>
</tr>
<tr>
<td>MARSEC</td>
<td>Marine Security Level</td>
</tr>
<tr>
<td>NEMA</td>
<td>National Electrical Manufacturers Association</td>
</tr>
<tr>
<td>NMSAC</td>
<td>National Maritime Security Advisory Committee</td>
</tr>
<tr>
<td>PACS</td>
<td>Physical Access Control System</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identity Verification</td>
</tr>
<tr>
<td>SIA</td>
<td>Security Industry Association</td>
</tr>
<tr>
<td>TPK</td>
<td>TWIC Privacy Key</td>
</tr>
<tr>
<td>TSA</td>
<td>Transportation Security Administration</td>
</tr>
<tr>
<td>TWIC</td>
<td>Transportation Workers Identification Credential</td>
</tr>
</tbody>
</table>
4. TWIC Modes of Operation

4.1 General

The Coast Guard has a three-tiered system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security's Homeland Security Advisory System (HSAS). MARSEC Levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. The Commandant of the U.S. Coast Guard sets MARSEC levels commensurate with the HSAS.

The TWIC is designed to be used in various systems at different levels of security depending on the requirements of each site and under specific threat levels. This document does not make any recommendation on the specific levels which need to be used by the sites but indicates the different modes of operations available allowing each site to create its own authentication security policy in accordance with the TWIC Rule and Coast Guard requirements. TWIC physical access readers shall allow authentication modes to be configured for each MARSEC level, based upon Coast Guard and site requirements. Specific authentication modes that should be supported by TWIC physical access control readers are identified in Table 4.1, TWIC Identification and Authentication Modes.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Identification/Authentication</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CHUID Verification</td>
<td>Provides verifiable identification factor, assuming the CHUID digital signature is either verified once, when the user’s CHUID is registered in the PACS or that the CHUID is verified each time it is accessed from a TWIC card. Refer to Appendix A Section A.1</td>
</tr>
<tr>
<td>2</td>
<td>Active Card Authentication</td>
<td>Provides single factor authentication at the same level of security as for a PIV Card Authentication operation. The FASC-N and expiration date are present in the Card Authentication certificate which obviates the need to read the CHUID. Refer to Appendix A Section A.2</td>
</tr>
<tr>
<td>3</td>
<td>CHUID Verification + Biometric User Authentication</td>
<td>The cardholder’s live biometric sample is compared to a stored biometric reference. The biometric reference template may be read from a TWIC card at each use or stored in the PACS system during PACS registration of the user. Provides single factor authentication. Refer to Appendix A Section A.3</td>
</tr>
<tr>
<td>4</td>
<td>(CHUID) Signing Certificate + Active Card Authentication + Biometric User Authentication</td>
<td>Provides two factor authentication. Refer to Appendix A Section A.4</td>
</tr>
</tbody>
</table>

Table 4.1 TWIC Identification and Authentication Modes

Note: This specification presumes that Personal Identity Numbers (PINs) are not a requirement for authentication at any MARSEC level.

TWIC is based upon a PIV compatible smart card and carries both a PIV card application and a TWIC card application that may be independently selected. This allows a TWIC card to operate both
in PIV mode in PIV compatible readers as well as TWIC mode in TWIC compatible readers. TWIC contactless CHUID verification and TWIC contactless biometric user authentication are supported directly by the TWIC card application. Card authentication is not supported by the TWIC card application. That said, card authentication over the contactless interface is supported through the selection of the PIV card application.

Note: All data shall be retrieved from the TWIC card application except for operations involving Active Card Authentication.

4.2 System Perspective

This specification describes two types of TWIC readers that may be used to verify the user’s TWIC card. They are:

- Fixed Physical Access Control Reader – a TWIC reader installed in a wall, turnstile or similar type installation. It communicates with an external access control system to control a door, gate, turnstile, etc. Fixed TWIC readers may operate in indoor environments or in outdoor environments exposed to the weather.

- Portable Verification Reader – a handheld TWIC reader that may be used for portable, spot-check identity verification.

A TWIC card may also be verified using contact smart card readers attached to a personal computer in an office environment for such functions as privilege granting, registration into a physical access control system and for logical access control. This specification only describes TWIC readers that shall be used for physical access into a facility or vessel.

4.2.1 Physical Access Control

4.2.1.1 Biometric Access Control System Overview

Figure 4.1, Generic Biometric-based Access Control System provides a graphical view of the relationship between a physical access control system (as a whole), a biometric sub-system boundary, and a biometric TWIC reader. Note that this is a generic diagram and that specific implementations may vary from this particular depiction. Key elements of Figure 4.1 are described in Table 4.2, below.

Generally, a TWIC card shall be used at a door or gate that may or may not be manned. The ISO/IEC 14443 contactless interface shall be used to transfer the unique ID number assigned to the cardholder and the biometric data between a TWIC card and a TWIC reader. The cardholder biometric template stored on a TWIC card is enciphered with a key unique to each TWIC card and remains enciphered during transmission to a TWIC reader over the contactless interface. The key required to decipher the reference biometric template of the user, called the TWIC Privacy Key (TPK), shall be obtained from one of several sources. These sources include the magnetic stripe encoded on each TWIC card, the TWIC card memory (but only accessible through the contact interface) or from the physical access control system where the TPK has been registered.
Figure 4.1 Generic Biometric-based Access Control System (ACS)

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Any form of machine-readable credential (TWIC card) presented by the user to the ID TWIC reader to claim an identity.</td>
</tr>
<tr>
<td>B</td>
<td>User identity code (ID number, card number, ACS ID) read from the token by the ID TWIC reader and sent to the panel for the ACS to determine access privilege (part of typical legacy ACS).</td>
</tr>
<tr>
<td>C</td>
<td>Electrical signal from the panel used to command the door electromechanical locking mechanisms. This path may also include other signals such as door-open indicators, emergency lock override, etc. (part of typical legacy ACS).</td>
</tr>
<tr>
<td>D</td>
<td>(Physical) communication channel (Ethernet, RS-485, etc.) enabling data interchange between the panel, ACS processor and database. (Logical) communications depends on site-specific implementation and includes user identity code data from the panel and user access authorization data from the ACS processor.</td>
</tr>
<tr>
<td>E</td>
<td>Body part or human behavior presented by the applicant to the biometric sensor during enrollment (e.g., fingerprint, iris, voice, signature). This function may also include interactions between applicant and sensor, i.e., indicator lights, audio cues.</td>
</tr>
</tbody>
</table>
### Key Description

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Biometric template data from enrollment database to biometric processor for implementations using server-stored templates. (This flow is architecture-specific, may be per user transaction or periodic pre-loads).</td>
</tr>
<tr>
<td>G</td>
<td>YES/NO indication (electrical signal or message) from biometric processor to panel conveying the result of the user verification transaction.</td>
</tr>
<tr>
<td>H</td>
<td>User identity code (ID number, card number, ACS ID) read from an ID Card by the ID TWIC reader and sent to the biometric processor as claim of identity (also includes user template data for template on card architectures).</td>
</tr>
<tr>
<td>I</td>
<td>Body part or human behavior presented to the biometric sensor during an access transaction (e.g., fingerprint, iris, voice, signature, etc.). This may also include interactions between the user and sensor such as indicator lights or audio cues.</td>
</tr>
<tr>
<td>J</td>
<td>Applicant-supplied information (name, address, etc.) obtained during ACS registration via the ACS processor (part of typical legacy ACS).</td>
</tr>
</tbody>
</table>

#### Table 4.2 Biometric Access System Key Descriptions

### 4.2.1.2 Verification - Network Attached TWIC Reader

A network attached TWIC reader\(^2\) supports two-way communication between a TWIC reader and the physical access control system. A TWIC reader may use this communication channel to access the user’s TWIC Privacy Key information that was stored during the process of registering the user into the PACS. TWIC verification consists of the following steps (presuming a user has previously registered with the local PACS). When a TWIC card needs to be verified, the following steps as required shall be followed:

- Present TWIC card to a contactless TWIC reader.
- TWIC reader may read the unique ID number from the TWIC card and either sends this directly to the PACS when in “CHUID only” mode, or temporarily stores this information for transmission after a successful biometric match when in “CHUID + biometric” mode. If the TWIC reader is in “CHUID + biometric” mode, the TWIC reader may use the unique ID number from the TWIC card to retrieve the user’s TWIC Privacy Key previously stored in the PACS when the user registered into the PACS at the facility.
- The TWIC reader may alternatively execute an active card authentication (using the PIV Card Authentication Key) to authenticate the card and read the unique ID number depending on the level of security required. (Refer to Appendix A, section A.2).
- TWIC reader may additionally retrieve the user’s biometric template from the contactless interface on the TWIC card and decipher the biometric using the TWIC Privacy Key depending on the level of security required.

---

\(^2\) Note that the term, “Network Attached” here indicates a bi-directional communication path between the reader and the PACS, it is not intended to specify any particular network fabric or protocol.
• If performing a Biometric User Authentication, the TWIC cardholder presents their biometric.

• If performing a Biometric User Authentication, the TWIC reader compares the biometric against the template read from the TWIC card and signals the physical access control system.

4.2.1.3 Verification - Standalone TWIC Reader

A standalone TWIC reader is one that has no two-way communications channel available or is connected to a PACS through a one-way communications connection. In this case, when a TWIC card is presented to a contactless only TWIC reader, the TWIC Privacy Key shall be read from the magnetic stripe on the TWIC card. The following steps shall be followed:

• Present TWIC card to a contactless TWIC reader.

• TWIC reader may read the unique ID number from the TWIC card and temporarily stores this information for transmission after a successful biometric match when in “CHUID + biometric” mode. If the TWIC reader is in “CHUID only” mode no further information is required from the card.

• If performing a Biometric User Authentication, the TWIC reader reads the user’s biometric template from the contactless interface on the TWIC card and temporarily stores this information for use in a later step.

• The TWIC reader may alternatively execute an active card authentication (using the PIV Card Authentication Key) to authenticate the card and read the unique ID number depending on the level of security required. (Refer to Appendix A, section A.2).

• If performing a Biometric User Authentication, the TWIC cardholder swipes their TWIC card through magnetic stripe reader to read the TWIC Privacy Key.

• If performing a Biometric User Authentication, the TWIC reader deciphers the previously stored biometric using the TWIC Privacy Key obtained from the magnetic stripe.

• If performing a Biometric User Authentication, the TWIC cardholder presents their biometric.

• If performing a Biometric User Authentication, the TWIC reader matches the presented biometric against the template obtained from the TWIC card.

• TWIC reader displays that the verification was confirmed or denied and signals the physical access control system.

Note: As the TWIC Privacy Key is also stored in the non-volatile electronic memory of the TWIC card, the TPK may alternatively be accessed through a smart card contact interface conditional upon said interface being supported by a stand-alone TWIC reader.

4.2.2 Portable Identity Verification

A handheld TWIC reader may also be used to verify worker credentials in a portable environment. This may be in conjunction with or as a substitute for the fixed access control TWIC readers described above. Smaller installations may not have, nor need, a complete physical access control system. In this case, a portable TWIC reader should provide an alternate means of identity verification. A handheld TWIC reader is presumed to be attended and operated by a qualified verification agent.
A TWIC card may be interrogated and verified using a portable handheld unit. The interface between the TWIC card and a TWIC reader may be via the contact or the contactless interface. A portable TWIC reader is envisioned to be used in a minimum of two operational modes:

- At a gate control location to interrogate credentials within a vehicle with multiple occupants.
- Authorized security personnel performing a random challenge throughout the facility.

Access to the biometrics on a TWIC card depends on the TWIC reader card interface used. Biometrics access modes are described in Table 4.3 below.

<table>
<thead>
<tr>
<th>Interface used to access the Biometric Template</th>
<th>Requirements to access the card biometric template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Interface</td>
<td>Using the PIV card application: Presentation of a PIN is required to access the user biometric reference template stored in clear text in the PIV card application.</td>
</tr>
<tr>
<td></td>
<td>Using the TWIC card application: Obtain through the contact interface the enciphered biometric template as well as the key (TPK) used to decipher it. No PIN or other key material is required from the TWIC reader.</td>
</tr>
<tr>
<td>Contactless Interface</td>
<td>Using the TWIC card application: The enciphered biometric reference template being free readable over the TWIC contactless interface, the TPK required to decipher it may be obtained from three possible sources: the magnetic stripe of the card, the contact interface of the TWIC card application, or from the PACS system if the TPK was stored during TWIC card registration into the PACS.</td>
</tr>
</tbody>
</table>

Table 4.3 Portable Card TWIC Reader Hardware Requirements
5. Fixed TWIC Reader Requirements

There exist electrical and physical interoperability requirements for fixed TWIC readers. These requirements detail the nature of the environment and in-place technologies a fixed TWIC reader shall interoperate with to be compliant and successful.

The purpose of a fixed TWIC reader is to provide the physical interface between a TWIC card and the physical access control system controlling access to a given portal (turnstile, door, gate, ramp, etc.).

5.1 Physical Requirements

5.1.1 TWIC Reader Dimensions

There are no specific recommendations regarding TWIC reader dimensions. For practicality, TWIC readers should be reasonably compact and versatile as to mounting in relation to the access point being controlled.

5.1.2 TWIC Reader Mounting

Mountings provided shall be tamper-proof. This means that the TWIC reader should have the ability to send an external signal in the event that there is an attempt at unauthorized entry into a TWIC reader or removal of a TWIC reader.

Note: TWIC readers shall employ an ISO/IEC 14443 contactless RF technology (operating at 13.56 MHz). This RF technology is sensitive to location and electromagnetic conditions of the local environment. Installers should work in coordination with TWIC reader manufacturers to make sure no electrical field or metallic element shall interfere with the TWIC reader contactless RF communications field.

5.1.3 Environmental

5.1.3.1 Outdoor Use requirements:

TWIC readers shall conform to a NEMA 4 rating. TWIC readers shall operate within a temperature range of -20°C to +70°C (-4°F to +158°F). TWIC readers shall operate in a humidity range of 5-100%, condensing. TWIC readers shall be capable of outdoor operations in direct sunlight and shall neither require nor be affected by ambient light sources. TWIC reader components may be offered in an enclosing cabinet that achieves the rating required. TWIC readers may be required to function in a hazardous materials environment. Intrinsically safe TWIC readers may be offered to meet this requirement.

5.1.3.2 Indoor Use requirements:

TWIC readers shall operate in a humidity range of 5-90%, non-condensing.
5.1.4 Impact Resistance

TWIC reader verification functionality shall not be degraded by low frequency vibration typical at terminals stemming from sources such as vessel departure/landings, heavy foot traffic, electric carts, large HVAC systems, sub-floor bag conveyors, and outdoor truck traffic. TWIC reader manufacturers may base compliance on IEC 60068-2-64. Equivalent commercial practice or analysis may be substituted subject to approval by TSA.

5.1.4.1 Shock

TWIC reader shall survive a shock event defined by IEC 68-2-27 (1987) using one half-sine pulse with a nominal peak acceleration of 5 g (50 m/s²) and nominal pulse duration of 30 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted subject to approval by TSA.

5.1.4.2 Bump

TWIC reader shall survive 100 bumps defined by IEC 68-2-29 (1987) each with a nominal peak accelerating of 10 g (100 m/s²) and nominal pulse duration of 16 ms with no observable change in performance. Equivalent commercial practice or analysis may be substituted subject to approval by TSA.

5.2 Electrical Requirements

TWIC readers shall operate within a range of 8-48 VDC. Where necessary to operate from line voltage, a power supply approved for use with a TWIC reader shall be provided. TWIC readers may optionally support PoE or PoE+ (Power over Ethernet or Power over Ethernet Plus) in accordance with IEEE 802.3af (48VDC/15.4W max) or 802.3at (48 VDC/56W max).

TWIC readers shall not exceed a 2.0 Amperes current requirement.

TWIC readers shall provide reverse voltage protection.

TWIC readers shall be FCC certified.

TWIC readers shall return automatically to normal operation after a loss of power event.

5.3 Safety

TWIC readers shall comply with UL 294, Standard for Safety of Access Control System Units, or internationally recognized equivalent.

TWIC readers shall not possess:

- Sharp corners or edges that may puncture, cut, or tear the skin or clothing or otherwise cause bodily injury. All TWIC reader corners and edges should have at least a 1mm exposed radius of curvature.
- External wires, connectors, or cables other than the power cable, data cable and the optional TWIC Privacy Key reading sub-assembly (i.e. magnetic stripe reader).
- Loose coverings and cowlings.

5.4 Electromagnetic/Vibration Compatibility

TWIC readers shall comply with the following requirements. For immunity tests the equipments shall operate normally or, if operation is interrupted, it shall not grant access.
5.4.1 47CFR18 and/or CISPR 11 (Emissions)
   • As per Section 5.2, TWIC readers shall be FCC certified.

5.4.2 IEC 61000-4-2 (Electrostatic Discharge)
   • Contact Discharge Mode at 2 kV and 4 kV Air Discharge Mode at 2 kV, 4 kV and 8 kV.
   • Presumes 8 to 10 equipment discharge test points plus coupling planes, positive and negative discharge waveform polarities.
   • Performance Criteria B.

5.4.3 IEC 61000-4-3 (Radiated RF Immunity)
   • 10 V/meter, 80 MHz to 1 GHz.
   • Four sides of EUT, 1% steps, 2.8 sec. dwell. AM Mod., 80%, 1 kHz.
   • Performance Criteria A.

5.4.4 IEC 61000-4-4 (Electrical Fast Transient/Burst)
   • AC and DC Power Ports at 0.5kV, 1kV and 2kV.
   • Signal Lines over 3 meters at 0.25 kV, 0.5kV and 1kV.
   • Performance Criteria B.

5.4.5 IEC 61000-4-6 (Radio Frequency Common Mode)
   • 10 Vrms, 150 kHz to 80 MHz.
   • Power ports and signal lines over 3 meters, 1% steps, 2.8 sec. dwell.
   • Performance Criteria A.

5.4.6 IEC 61000-4-5 (Surges)
   • AC power port at 2kV line to earth, 1kV line to line at 0, 90 and 270 deg.
   • DC Power Ports at 0.5 kV line to earth, 0.5 kV line to line.
   • Signal Lines over 30 meters at 1 kV line to earth.
   • Positive and negative polarity, 5 surges per mode of appearance.
   • Performance Criteria A.

5.4.7 IEC 61000-4-8 (Power Frequency Common Mode)
   • 30 A/m, 50 or 60Hz.
   • Performance Criteria A.
5.4.8 IEC 61000-4-11 (Voltage Dips and Interruptions)

- 30% reduction for 0.5 periods (10 ms), Performance Criteria B.
- 60% for 5 periods (100 ms), Performance Criteria C.
- 60% for 50 periods (1 sec), Performance Criteria C.
- 95% for 250 periods (5 sec), Performance Criteria C.
6. Portable TWIC Reader Requirements

A portable TWIC reader may support a wireless interface to provide direct access to a PACS. In such a case, the wireless connection shall have the following security attributes:

- confidentiality (session key)
- active authentication of the TWIC reader or, the operator using the TWIC reader.

If a portable TWIC reader has only a contact interface, the PIV card application may be used to verify the biometric information of the user. The PIV card application requires the user PIN to be presented in order to release the reference biometric information to a TWIC reader. Using the TWIC card application over the contact interface allows the TWIC reader to access the enciphered biometric reference template along with the key (TPK) used to decipher it.

If a portable TWIC reader has only a contactless card read capability, the portable TWIC reader shall also have a magnetic stripe reader in order to access the TWIC Privacy Key. The TPK is needed to decipher the biometric information held within the TWIC card application.

A portable TWIC reader shall be capable of confirming whether a TWIC card has been revoked. A portable TWIC reader shall be capable of downloading and using the most recent TWIC Hotlist. A portable TWIC reader may support a Certificate Revocation List (CRL) subject to availability of a network connection.

6.1 Portable TWIC Reader Specific Requirements:

A portable TWIC reader shall meet the same specifications as a fixed TWIC reader, as appropriate, with the exception of the following differences:

6.1.1 Operational Features

Portable TWIC readers shall have a display suitable for user interaction.

Portable TWIC readers shall be able to display the current battery level.

Portable TWIC readers shall have a real time clock.

Portable TWIC readers may use a touch screen or other suitable means for user input/control.

Portable TWIC readers should have a hibernation mode for protection against data loss.

6.1.2 Environmental Requirements

Portable TWIC readers certified for harsh conditions shall meet the following specifications:

- MIL-STD 810F, Method 514.5 – Vibration.
- MIL-STD 810F, Method 501.4 – High temperature (to +70°C/+158°F).
- MIL-STD 810F, Method 502.4 – Low temperature (to -10°C/-14°F).
- MIL-STD 810F, Method 507.4 – Humidity.
- MIL-STD 810F, Method 503.4 – Temperature shock.
- MIL-STD 810F, Method 516.5, Procedure IV (Transit Drop Test) – 26 drops at 4 feet.
6.1.3 Electrical Requirements

Portable TWIC readers should be supplied with a rechargeable battery with 12 hours minimum operational time.

Portable TWIC readers shall be operable while charging.

Portable TWIC readers should have a maximum battery recharge time of 2 hours.
7. **TWIC Reader Operational Requirements**

TWIC reader operational requirements apply to all TWIC reader types except where noted.

The contactless smart card TWIC reader component shall conform to the ISO/IEC 14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-1.

TWIC readers shall have a maximum contactless smart card read range of 10cm.

Contactless enabled TWIC readers shall be able to communicate with a contactless card at 106kbit/s, 212kbit/s or 424kbit/s, dependent on the contactless card communications speed capabilities.

If two or more contactless smart cards are presented at the same time in a TWIC reader's contactless field, the TWIC reader shall reject all of the presented cards.

TWIC readers shall require that a TWIC card, once read, shall be removed from the RF field for at least one second before attempting to read any new contactless card. This requirement is to minimize multiple reads of the same TWIC card for a single presentation.

Fixed TWIC readers shall be capable of reading the access control data from a TWIC card, performing the necessary authentication steps, and transmitting the credential data as required by the PACS.

Due to the particulars of TWIC card issuance a minimum of 4 data elements of the FASC-N should be read and forwarded to the PACS. These data elements are the Agency Code, System Code, Credential Number and the Individual Credential Issue.

Fixed TWIC readers shall have communications ports as required by the PACS cable plant and control panels. Minimum options required are:

- Wiegand port for connection to standard access control panels.
- RS-485 or 10/100baseT (Ethernet) for connection to computer systems or access control systems.

For fixed TWIC readers, at least one Wiegand output format shall follow that specified for FIPS 201-based systems. The GSA Approved Products Listing test for Federal Employee Personal Identity Verification defines a 75-bit “transparent mode” which includes 2 parity bits and 25 bits for the date. The TWIC reader shall output the following 75-bits:

<table>
<thead>
<tr>
<th>Description</th>
<th>Position</th>
<th>Length (BITS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parity Bit P1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Agency Code</td>
<td>2-15</td>
<td>14</td>
</tr>
<tr>
<td>System Code</td>
<td>16-29</td>
<td>14</td>
</tr>
<tr>
<td>Credential Number (Note 1)</td>
<td>30-49</td>
<td>20</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>50-74</td>
<td>25</td>
</tr>
<tr>
<td>Parity Bit P2</td>
<td>75</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 7.1 75-bit Wiegand Output Format
Fixed TWIC readers may support an additional Wiegand output format of 48 bits when a TWIC reader includes a real time clock that may be used to verify the expiration date. In this case, it is presumed that the TWIC reader has the ability to process the expiration date. Some PACS control panels may not be able to support both 48-bit and 75-bit Wiegand input at the same time. In such a case, a TWIC reader shall provide a method of setting the Wiegand output format as required by the local PACS.

The 48-bit Wiegand format is the same as the 75-bit transparent mode but drops the expiration date and the two parity bits as shown below:

<table>
<thead>
<tr>
<th>Description</th>
<th>Position</th>
<th>Length (BITS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Code</td>
<td>1-14</td>
<td>14</td>
</tr>
<tr>
<td>System Code</td>
<td>15-28</td>
<td>14</td>
</tr>
<tr>
<td>Credential Number (Note 1)</td>
<td>29-48</td>
<td>20</td>
</tr>
</tbody>
</table>

Table 7.2 48-bit Wiegand Output Format

Note 1: The Credential Number field shall be used to transport the values of the Credential Number and the Individual Credential Issue (ICI) fields. TWIC Readers shall format this field as follows:

1) For an ICI value of 1, the FASC-N Credential Number shall be used without modification. The Most Significant Digit (MSD) of the Credential Number shall be either a 0 or 1 for a TWIC Card.

2) For an ICI value of 2, the MSD of the FASC-N Credential Number shall be transmitted as 2 + the value of the MSD. The transmitted Credential Number MSD shall be either 2 or 3 for a TWIC card.

3) For an ICI value of 3, the MSD of the FASC-N Credential Number shall be transmitted as 4 + the value of the MSD. The transmitted Credential Number MSD shall be either 4 or 5 for a TWIC card.

4) For an ICI value of 4, the MSD of the FASC-N Credential Number shall be transmitted as 6 + the value of the MSD. The transmitted Credential Number MSD shall be either 6 or 7 for a TWIC card.

5) For an ICI value of 5 or higher, the MSD of the FASC-N Credential Number shall be transmitted as 8 + the value of the MSD. The transmitted Credential Number MSD shall be either 8 or 9 for a TWIC card.

Fixed TWIC readers may support other additional Wiegand formats for legacy systems. Wiegand output formats not detailed in this specification may transmit the entire FASC-N or selected elements of the FASC-N.

TWIC readers should clearly and continuously display power status (on, ready or out of service).

TWIC readers may contain additional user indications including lights, text messages, and audible indicators.

TWIC reader visual indicators shall be visible in daylight.

TWIC readers should have a finger guide to aid in proper finger placement on the sensor.

For biometrically enabled TWIC readers, the fingerprint sensor should be embedded in the same chassis as the TWIC reader. If a separate fingerprint sensor module is used, the wiring between the TWIC reader and the biometric unit shall not be exposed.

TWIC readers shall allow for future enhancements to be added in the field. A mechanism should be provided that assu res that only authorized/authenticated firmware/software updates are permitted.
TWIC readers shall provide a means to create a time-stamped log of operations for use in assessing exception conditions such as fingerprint rejections.

TWIC readers shall provide an automated alert or lockout after a configurable number of consecutive failed biometric matching attempts (i.e. the facility chooses the number of attempts).

TWIC readers may support a means of alerting the PACS/operator if the TWIC reader detects tampering.

TWIC readers shall support a method of changing its mode of authentication according to the current security threat level of the protected site.
8. Performance Requirements

TWIC readers should be capable of achieving a standard maximum transaction time (defined as the time between presentation of the contactless card to a TWIC reader and completion of the biometric match) of three seconds. This does not include the time required to acquire the TPK either using a magnetic stripe or through download from a PACS.

The biometric sub-system should provide an equal error rate (EER) of 1% (i.e. 1% false rejections at a setting of 1% false acceptance) on a per transaction basis. This presumes up to three attempts as a minimum standard error rate. TWIC readers should provide a mechanism to adjust the security level sensitivity as required.

Any alternatives to the use of fingerprint biometrics shall be addressed in the local operator’s security plans.

Biometric enabled TWIC readers should provide liveness detection. This is particularly important when TWIC readers are used in unattended operations.

Biometric processes and performance are further described in ANSI/INCITS 383.

It should be noted that biometric interoperability is defined as the ability of a biometric TWIC reader to perform a match from a presented biometric with the ANSI/INCITS 378 formatted enrolled templates provided on a TWIC card by TSA. Such templates shall be in compliance with NIST Special Publication 800-76-1 INCITS 378 profile for PIV Card templates.
9. Operational Availability

Biometric enabled TWIC readers shall be able to handle 1 million touches without degradation. TWIC readers shall be designed to yield a Mean Time Between Failure (MTBF) of 25,000 hours or greater.
10. **Delivery**

TWIC readers shall include technical manuals covering installation, operation and maintenance. TWIC readers shall be packaged suitable for shipment to a designated installation point.
11. TWIC Card Application

The TWIC card application data model and card edge edition defined in this section is Version 1.1.

Annex E details the data model and card edge edition encoding convention within the Application Identifier (AID).

11.1 Card application Identifier

<table>
<thead>
<tr>
<th>TWIC card application AID</th>
<th>RID</th>
<th>PIX</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0 00 00 03 67</td>
<td>20 00 00 01 xx xx</td>
<td>Needs to be selected using a partial select with a PIX length of 4 bytes</td>
<td></td>
</tr>
</tbody>
</table>

(See Appendix E: xx xx = 81 01 = TWIC test, xx xx = 01 01 = TWIC live)

Note: Both PIV and TWIC specifications allow another application to be the default selected application in a card. As not all TWIC cards may be issued with the TWIC application as the default selected card application, TWIC readers shall explicitly select the TWIC card application.

11.2 Key Reference(s)

<table>
<thead>
<tr>
<th>Algorithm Identifier*</th>
<th>Key Reference</th>
<th>Key Name</th>
<th>Authenticatable Entity</th>
<th>Security Status</th>
<th>Retry/Reset Value</th>
<th>Number of Unblocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>08</td>
<td>‘Kp’</td>
<td>TWIC card-application Privacy Key</td>
<td>TWIC Card application Biometric data and Cardholder</td>
<td>Application</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Reference FIPS 201-1 document SP 800-78-1: algorithm identifier 08 indicates this key is to be used with an AES algorithm in ECB mode.

Notes:

1. The TPK is not used by the TWIC card application for any cryptographic function. The TPK is used by the client application to encipher (for storage in the card) or decipher (for use in a TWIC reader) the user's reference biometric template.
2. The Key reference is a field (tag 0xC1) found in the TWIC Privacy Key Buffer.

11.3 ICC Data Model

<table>
<thead>
<tr>
<th>Buffer Description</th>
<th>Data Object (BER-TLV tag)</th>
<th>Maximum Length (BYTES)</th>
<th>Access Rule</th>
<th>Contact/Contactless</th>
<th>M/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsigned Cardholder Unique Identifier</td>
<td>0x5FC104 (0x3002)**</td>
<td>64</td>
<td>Always Read</td>
<td>Contact and Contactless</td>
<td>M</td>
</tr>
<tr>
<td>TWIC Privacy Key Buffer</td>
<td>0xDFC101 (0x2001)**</td>
<td>40</td>
<td>Always Read</td>
<td>Contact (and Magnetic stripe also)</td>
<td>M</td>
</tr>
<tr>
<td>Card Holder Unique Identifier</td>
<td>0x5FC102 (0x3000)**</td>
<td>3377</td>
<td>Always Read</td>
<td>Contact and Contactless</td>
<td>M</td>
</tr>
</tbody>
</table>
The container IDs are provided in this data model as they are required for the Security Object Data Group (DG) mapping.

Notes:
1. The maximum length of data objects in the above table includes the BER-TLV structural information attached to each data object. This structural information consists at a minimum of the tag itself (three bytes), the length of the data object value which may be one or three bytes, and applet internal data information which may vary specific to an applet implementation.
2. All the Data Objects in the TWIC card application data model are elementary data objects with 3-byte ASN.1 BER-TLV encoded tags. The individual tags inside these data objects are not intended to follow ASN.1 coding rules in the interest of keeping backward compatibility with the PIV data model. As a consequence, no ASN.1 constructed data object is used in this application.
3. The signatures used in the Signed Cardholder Unique Identifier and the Card Holder Fingerprint Templates are of type RSA 2048, SHA1. The signature belongs to the Card Management System which is responsible for preparing the personalization data.
4. The calculation of hashes of the individual data objects, to be used for the creation of the Security Object, shall be based on the contents of Data Objects as stored in the TWIC card application.

Table 11.1 Unsigned Card Holder Unique Identifier

<table>
<thead>
<tr>
<th>Data Element (TLV)</th>
<th>Tag</th>
<th>M/O</th>
<th>Type</th>
<th>Max Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FASC-N</td>
<td>0x30</td>
<td>M</td>
<td>Fixed Text</td>
<td>25</td>
</tr>
<tr>
<td>GUID</td>
<td>0x34</td>
<td>M</td>
<td>Fixed Numeric</td>
<td>16</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>0x35</td>
<td>M</td>
<td>Date (YYYYMMDD)</td>
<td>8</td>
</tr>
<tr>
<td>Error Detection Code</td>
<td>0xFE</td>
<td>M</td>
<td>LRC</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: The structural information consists of two additional bytes per element (simple TLV tag byte plus one byte for length). This requires a minimum total of 57 bytes for this data object value.

Table 11.2 TWIC Key Privacy Buffer

<table>
<thead>
<tr>
<th>Data Element (TLV)</th>
<th>Tag</th>
<th>M/O</th>
<th>Type</th>
<th>Max Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TWIC Privacy Key (Kp)</td>
<td>0xC0</td>
<td>M</td>
<td>Variable</td>
<td>32</td>
</tr>
<tr>
<td>Algorithm Identifier</td>
<td>0xC1</td>
<td>M</td>
<td>Fixed Text</td>
<td>01</td>
</tr>
<tr>
<td>Key Index</td>
<td>0xC2</td>
<td>M</td>
<td>Fixed Text (00 = RFU)</td>
<td>01</td>
</tr>
</tbody>
</table>

Notes:
1. The current TPK requires only 16 bytes of data storage. An additional 16 bytes have been added to the maximum size of the TPK element (Tag 0xC0) to support future algorithms.
2. The structural information consists of two additional bytes per element (simple TLV tag byte plus one byte for length). This requires a total of 40 bytes for this data object value.
Transportation Security Administration  
May 30, 2008

TWIC Reader Hardware and Card Application Specification

Table 11.3 Signed Card Holder Unique Identifier

<table>
<thead>
<tr>
<th>Card Holder Unique Identifier</th>
<th>Tag</th>
<th>M/O</th>
<th>Type</th>
<th>Max Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Element (TLV)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FASC-N</td>
<td>0x30</td>
<td>M</td>
<td>Fixed Text</td>
<td>25</td>
</tr>
<tr>
<td>GUID</td>
<td>0x34</td>
<td>M</td>
<td>Fixed Numeric</td>
<td>16</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>0x35</td>
<td>M</td>
<td>Date (YYYYMMDD)</td>
<td>8</td>
</tr>
<tr>
<td>Issuer Asymmetric Signature</td>
<td>0x3E</td>
<td>M</td>
<td>Variable</td>
<td>2400</td>
</tr>
<tr>
<td>Error Detection Code</td>
<td>0xFE</td>
<td>M</td>
<td>LRC</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: The structural information consists of some additional bytes per element (simple TLV tag byte plus one or three bytes for length). This requires a minimum total of 12 bytes for this data object value.

Table 11.4 Card Holder Enciphered Fingerprint Templates

<table>
<thead>
<tr>
<th>Card Holder Fingerprints</th>
<th>0xDFC103</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Element (TLV)</td>
<td>Tag</td>
</tr>
<tr>
<td>Enciphered Fingerprint template (2 fingers)</td>
<td>0xBC</td>
</tr>
</tbody>
</table>

Notes:
1. The fingerprint biometric template is encoded in accordance with the INCITS 378 standard.
2. Tag 0xBC shall contain the enciphered biometric template. The CBEFF integrity option is required per SP 800-76-1, section 6. The data therefore includes the digital signature of the Card Management System. The data is padded per PKCS#7 section 10.3, note 2, and enciphered using the TWIC Privacy Key (Kp). Deciphering of the biometric template should be performed using the “no padding” option of the AES algorithm.
3. Four additional bytes of structural information are required for this data object.

Table 11.5 Security Object

<table>
<thead>
<tr>
<th>Security Object</th>
<th>0xDFC10F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Element (TLV)</td>
<td>Tag</td>
</tr>
<tr>
<td>Mapping of DG to Data Objects</td>
<td>0xBA</td>
</tr>
<tr>
<td>Security Object</td>
<td>0xBB</td>
</tr>
<tr>
<td>Error Detection Code</td>
<td>0xFE</td>
</tr>
</tbody>
</table>

Notes:
1. The security object is in accordance with Appendix C.2 of PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1. [8]. Tag “0xBA” is used to map the Data Objects in the TWIC data model to the 16 Data Groups specified in the Machine Readable Travel Document (MRTD). The objects hashed are: the Unsigned CHUID (0x3002), the Signed CHUID (0x3000), and the signed fingerprint templates (0x2003). This enables the TWIC security object to be fully compliant for future activities with identity documents.
2. The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object. The signature field of the security object shall omit the issuer’s certificate, since it is included in the signed CHUID. The Card Issuer’s Digital Signature is in accordance...
with FIPS 201-1 using the SP-800-78-1 document as reference with the key sizes in accordance to the TWIC card life.

3. Eight additional bytes of structural information are required for this data object.

11.4 Magnetic Stripe Data Model

The TWIC Privacy Key (TPK) used to encipher/decipher the reference biometric template stored in the TWIC card application is stored on the magnetic stripe of each TWIC card. The TPK shall be encoded on the magnetic stripe as follows:

- The TPK is a 16 byte string used by an AES encipherment/decipherment algorithm.
- Track 1 of the TWIC magnetic stripe shall be reserved exclusively for the TPK character string. The TPK character string shall be encoded on the high-coercivity magnetic stripe track 1 of the card as defined in ISO/IEC 7811-6.
- Each nibble of the 16 bytes of the TPK shall be encoded as ASCII alphanumeric characters (0 to 9 and A to F) giving a total of 32 characters representing the 32 hexadecimal digits of the TPK.
- The TPK shall be encoded as one data field starting with a start sentinel (‘;’) followed by 32 data characters and ending with one end sentinel (‘?’).
- An LRC field calculated in accordance with ISO/IEC 7811-2 shall be coded after the end sentinel.

11.5 TWIC Card Application Command Set

The TWIC card application shall support the following APDU commands:

- SELECT
- GET DATA

Notes:

1. As for PIV, the GET RESPONSE APDU command does not appear at the application command layer but may be required if the application layer does not use an extended length in the APDUs. The use of the GET RESPONSE APDU command by the application layer is described in Appendix F.

2. Other APDU commands may be required to handle application management features but, as they are not required for interoperability in TWIC readers, such APDU commands do not appear in this specification.

3. Beyond the tags described in this specification, some ISO/IEC 7816-6 tags may be available at the card interface in response to a GET DATA APDU command (e.g. Card Related Information). These tags are not required for interoperability in TWIC readers. Such additional tags are not described in this document as they are specific to either an applet implementation or the management features of an applet implementation.
11.5.1 SELECT

Command Syntax

<table>
<thead>
<tr>
<th>CLA</th>
<th>‘00’</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS</td>
<td>‘A4’</td>
</tr>
<tr>
<td>P1</td>
<td>‘04’  (Select by Name)</td>
</tr>
<tr>
<td>P2</td>
<td>‘00’</td>
</tr>
<tr>
<td>Lc</td>
<td>‘09’ (Select on a partial TWIC AID length)</td>
</tr>
</tbody>
</table>

Data Field: TWIC AID (= TSA RID || TWIC first four bytes of the PIX)

Le: ‘00’ or ‘xx’ - Length of TWIC card application property template if known

Note: In TWIC readers using the TWIC card, the SELECT “AID” APDU command shall always ask for a partial TWIC AID and analyze the information returned from a TWIC card when the SELECT APDU command is successful. The information returned provides the version of the TWIC card application as well as if the card is a test card or a live TWIC card. A full SELECT “AID” APDU command with a length of 11 bytes (Lc = 0x0B) shall, nevertheless, be supported by a TWIC card in order to be ISO/IEC 7816-4 compliant.

Card Application Property Template

Upon successful selection, the TWIC card application shall return the application property template described below.

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Tag</th>
<th>Length</th>
<th>M/O</th>
<th>Value field of the tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Template</td>
<td>‘61’</td>
<td>‘16’</td>
<td>M</td>
<td>Refer to ISO/IEC 7816-6</td>
</tr>
<tr>
<td>Application identifier of application</td>
<td>‘4F’</td>
<td>‘0B’</td>
<td>M</td>
<td>The PIX of the AID includes the encoding of the Version. Refer to Appendix E.</td>
</tr>
<tr>
<td>Coexistent tag allocation authority</td>
<td>‘79’</td>
<td>‘07’</td>
<td>M</td>
<td>Coexistent tag allocation authority template. (Tag ‘4F’)</td>
</tr>
<tr>
<td>Application RID coexistent with ISO/IEC 7816 name space for tags</td>
<td>‘4F’</td>
<td>‘05’</td>
<td>M</td>
<td>TSA RID</td>
</tr>
</tbody>
</table>

Table 11.6 Data Objects in the TWIC Card application Property Template (Tag ‘61’)
Response Syntax

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Card application property template (see above)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1-SW2</td>
<td>Status Word</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SW1</th>
<th>SW2</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>'6A'</td>
<td>'82'</td>
<td>Card Application not found</td>
</tr>
<tr>
<td>'6A'</td>
<td>'86'</td>
<td>P1,P2 combination not supported</td>
</tr>
<tr>
<td>'6A'</td>
<td>'87'</td>
<td>Incorrect Data Field length (Lc =0 or Lc &gt; 16)</td>
</tr>
<tr>
<td>'90'</td>
<td>'00'</td>
<td>Successful execution</td>
</tr>
</tbody>
</table>

11.5.2 GET DATA

Command Syntax

<table>
<thead>
<tr>
<th>CLA</th>
<th>‘00’</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS</td>
<td>‘CB’</td>
</tr>
<tr>
<td>P1</td>
<td>‘3F’</td>
</tr>
<tr>
<td>P2</td>
<td>‘FF’</td>
</tr>
<tr>
<td>Lc</td>
<td>‘05’ for TWIC related data objects</td>
</tr>
<tr>
<td>Data Field</td>
<td>refer to Section 11.3 ICC Data Model</td>
</tr>
<tr>
<td>Le</td>
<td>‘00’ or ‘xx’ - Number of data content bytes to be retrieved</td>
</tr>
</tbody>
</table>

Response Syntax

<table>
<thead>
<tr>
<th>Data Field</th>
<th>BER-TLV with the tag ‘53’ containing in the value field the requested data object</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1-SW2</td>
<td>Status Word</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SW1</th>
<th>SW2</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>'61'</td>
<td>'XX'</td>
<td>Successful execution where SW2 encodes the number of response data bytes not returned in the response</td>
</tr>
<tr>
<td>'62'</td>
<td>'82'</td>
<td>Warning, End of File Reached before reading the requested Le bytes. Returned data block may contain padding bytes for some types of transmission protocol</td>
</tr>
<tr>
<td>'69'</td>
<td>'82'</td>
<td>Security status not satisfied</td>
</tr>
<tr>
<td>'6A'</td>
<td>'88'</td>
<td>Data Object not found</td>
</tr>
<tr>
<td>'6C'</td>
<td>'XX'</td>
<td>Execution aborted (no data returned) SW2 encodes the number of response data bytes available not returned in the response</td>
</tr>
<tr>
<td>'90'</td>
<td>'00'</td>
<td>Successful execution</td>
</tr>
</tbody>
</table>

Notes:

1. The use of return codes SW1-SW2 = ’61 xx’ is explained in Appendix F of this document.
2. TWIC reader manufacturers should note that it is not reliable to use the Le field (expected information length) to limit the amount of time it takes to transmit information from the card. Some cards, depending on the transport protocol used may not accept truncation in the
response of the amount of data constituting a data object. In such a case the complete data object would be transmitted anyway and truncated only at the application layer presentation with no benefit in transmission time. For this reason the unsigned CHUID is part of this specification, allowing read of such information quickly. ISO/IEC 7816-4 allows the application layer to ask for a truncated value field of data objects but requires use of another format of the GET DATA APDU command (Tag list ‘5D’ instead of ‘5C’). TWIC, in the same manner as PIV, does not support this alternate form of the GET DATA APDU command.
Appendix A Authentication Processing (NORMATIVE)

In order to determine the identity of a cardholder, an access control system shall check one or more authentication factors. The overall assurance of the authentication process is determined by the number and quality of each authentication factor used. These factors are typically divided into three categories:

- Something you have - An object hard to copy (e.g. a badge, a metal key or a smart card),
- Something you know - An element hard to guess (e.g. a PIN or a password),
- Something you are - An element hard to share (e.g. your fingerprint, your iris or your voice),

A check against an authentication factor is considered “strong” if it is difficult for an attacker to gain control, clone or compromise that factor. An access control system may achieve the required level of authentication security by checking factors against the card presented, the user presenting it, and information stored in its own database.

An authentication factor is bound to an identifier used to uniquely identify an individual within a system. For example, a username used to login to a computer system is assigned to identify an individual as a user of a computer. The username is bound to a password which is used to authenticate that the person logging in to the computer is the same person who was assigned the identifier and given the password. This is a simple example of single factor authentication where the password represents a single, “something you know” authentication factor and the username represents an identifier.

Identifiers, such as the TWIC CHUID may be strengthened through the use of a digital signature. A digitally signed identifier may be verified to determine that it is a genuine identifier for an individual, that said identifier was issued by the system authority, and the identifier has not been revoked or invented. However, an identifier by itself is generally public information and does not provide authentication that the individual using the identifier is the individual to whom the identifier was issued. An authentication factor, such as a password, should also exist. Further, the knowledge to satisfy a given authentication factor challenge should be limited to either the system authority (e.g. card authentication) or the individual (e.g. PIN or biometric) for whom the identifier was issued.

A TWIC card offers three different data elements that may be used to support authentication via the contactless interface of the card:

1) CHUID data object – A strong, digitally signed identifier issued by the TWIC Program after vetting the identity of an individual and determining that said individual is trustworthy.

2) TWIC biometric template – A strong “something you are” authentication factor that is strongly bound (unique) to the individual. The TWIC biometric template is strongly bound to the CHUID (identifier) and protected against alteration (counterfeit) through digital signature.

3) PIV Card Authentication Certificate and Key – A strong “something you have” authentication factor that is strongly bound to the user’s smart card through proof of possession of a never revealed private key that exists only on the user’s smart card. The use of the card authentication certificate and associated private key provide strong proof that the smart card being presented to a TWIC reader is a genuine TWIC card that was issued to the individual by a trusted authority.

Note: The CHUID may be referred to as a “weak” authentication factor. It should be noted that without biometric verification or card authentication, the CHUID is publicly available data that is transmitted over the TWIC contactless interface in clear text and may be captured, copied to another card or replayed, along with the digital signature attached to it. Caution should be exercised in relying solely on the CHUID as a “weak” authentication factor, even in low assurance applications as it may be captured by an attacker without user consent or knowledge.
This appendix describes the process that may be used to authenticate one or more of these factors against a TWIC card. An access control system may choose to supplement or replace these authentication factors with off-card authentication information in a database. For example, a PACS PIN may be stored in the access control system and compared on entry, even though the TWIC card application does not support this capability. Such off-card authentication checks are beyond the scope of this specification.

TWIC employs the use of Public Key Infrastructure (PKI) to include signatures and certificates. TWIC issues five year certificates; the consequence of these longer life certificates is certain fields in the certificate have values that, by policy, vary from FIPS201. The following table provides the differences in the construction of TWIC Object Identifiers (OIDs) from their PIV equivalents. TWIC OIDs have the identical meaning to their PIV OID equivalents.

PIV OIDs are registered with the Computer Security Objects Registry for which NIST is the Registration Authority. The “PIV Root” is 2.16.840.1.101.3 {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)}.

TWIC OIDs are registered with the Internet Assigned Numbers Authority (IANA). The “TWIC Root” is defined as 1.3.6.1.4.1.29138 {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) twic-root (29138)}.

TWIC readers shall accept either OID value when parsing a signature or certificate from either the TWIC card application or the PIV card application.

### PIV and TWIC Object Identifiers

<table>
<thead>
<tr>
<th>ID</th>
<th>Object Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id-TWIC-digital-signature</td>
<td>1.3.6.1.4.1.29138.2.1.3.5</td>
<td>May be asserted in the Certificate Policy field of an X.509 certificate</td>
</tr>
<tr>
<td>id-TWIC-key-management</td>
<td>1.3.6.1.4.1.29138.2.1.3.6</td>
<td>May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.</td>
</tr>
<tr>
<td>ID</td>
<td>Object Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>id-TWIC-devices</td>
<td>1.3.6.1.4.1.29138.2.1.3.8</td>
<td>May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.</td>
</tr>
<tr>
<td>id-TWIC-authentication</td>
<td>1.3.6.1.4.1.29138.2.1.3.13</td>
<td>May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.</td>
</tr>
<tr>
<td>id-TWIC-cardAuth</td>
<td>1.3.6.1.4.1.29138.2.1.3.17</td>
<td>May be asserted in the Certificate Policy field of an X.509 certificate. Refer to Section 7.1.6 of the X.509 Certificate Policy for the US Federal PKI Common Policy Framework.</td>
</tr>
</tbody>
</table>

**Application Attributes**

<table>
<thead>
<tr>
<th>ID</th>
<th>Object Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pivFASC-N</td>
<td>2.16.840.1.101.3.6.6</td>
<td>The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures.</td>
</tr>
<tr>
<td>twicFASC-N</td>
<td>1.3.6.1.4.1.29138.6.6</td>
<td>The twicFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures.</td>
</tr>
</tbody>
</table>

**Extended Key Usage**

<table>
<thead>
<tr>
<th>ID</th>
<th>Object Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id-PIV-content-signing</td>
<td>2.16.840.1.101.3.6.7</td>
<td>This specifies that the public key may be used to verify signatures on PIV CHUIDS and PIV biometrics.</td>
</tr>
</tbody>
</table>
### ID | Object Identifier | Description
--- | --- | ---
id-TWIC-content-signing | 1.3.6.1.4.1.29138.6.7 | This specifies that the public key may be used to verify signatures on CHUIDS and biometrics that are present on either the TWIC or PIV card applications.
id-PIV-cardAuth | 2.16.840.1.101.3.6.8 | This specifies that the public key is used to authenticate the PIV card rather than the PIV cardholder.
id-TWIC-cardAuth | 1.3.6.1.4.1.29138.6.8 | This specifies that the public key is used to authenticate the TWIC card rather than the TWIC cardholder.

#### Certificate Extension

<table>
<thead>
<tr>
<th>ID</th>
<th>Object Identifier</th>
<th>Description</th>
</tr>
</thead>
</table>
id-PIV-NACI | 2.16.840.1.101.3.6.9.1 | The PIV NACI indicator extension indicates the status of the subject’s background investigation at the time of credential issuance. |
id-TWIC-interim | 1.3.6.1.4.1.29138.6.9.1 | The TWIC Threat Assessment indicator extension indicates the status of the subject’s background investigation at the time of credential issuance. |

### A.1 CHUID Verification

The CHUID is a freely readable data object that is digitally signed (to prevent such a number from being modified or invented by a non-authorized party), but is neither enciphered nor strongly bound to the physical card. The signed object contains the unique Federal Agency Smart Credential Number (FASC-N) identifier, which should be used as the primary identification number for the card. The FASC-N may also be found in the unsigned CHUID data object (tag = 0x5FC104).

Before using a CHUID (or the FASC-N it contains) the digital signature of the issuer should be verified in order to ensure the credential number is not altered or invented. This verification may take place when the CHUID is downloaded from a trusted source to the PACS for insertion in the authorized CHUID access control list (a white list in the PACS) or may be done when the CHUID of a new worker is registered in the PACS, or at the first time a CHUID is used by a PACS. Under no condition should a CHUID be used if its digital signature has never been verified by the PACS or a TWIC reader attached to the PACS.

The first time a CHUID is found in a PACS system (registration, download, or first use), the digital signature shall be verified.

When the TWIC reader is configured for CHUID signature verification it shall perform the following steps:

1) TWIC reader selects the TWIC card application.
2) TWIC reader gets the complete contents of the CHUID data object.
3) TWIC reader shall decode the Issuer Asymmetric Signature Object (tag: 0x3E) from the CHUID in order to retrieve the card issuer’s digital signature certificate for the document signer (guaranteeing the CHUID was created by an accredited issuer) that is used to verify the signed objects on the card.

4) TWIC reader shall verify the CHUID signature and origin up to and including the trust anchor.

5) TWIC reader searches the CHUID object to find the FASC-N tagged (0x30) value.

6) TWIC reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Issue. The TWIC reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or selected elements of the FASC-N.

Alternatively, when configured for CHUID signature verification, the TWIC reader may verify the signature of the unsigned CHUID using the Security Data Object. In this case the TWIC reader shall retrieve the card issuer’s digital signature certificate from the signed CHUID and verify the unsigned CHUID signature in the Security Data Object. Before first use of any cached card issuer’s digital signature certificate, the TWIC reader shall verify the signature and origin of this certificate. TWIC readers shall not statically configure the card issuer’s digital signature certificate. TWIC readers shall dynamically acquire new versions of the card issuer’s digital signature certificate from a TWIC card when a new version of the certificate is presented.

In some operations the FASC-N of a CHUID shall be used for access control by a PACS when previously registered (white list verification). In such a case, the TWIC reader should perform the following steps for authentication:

1) TWIC reader selects the TWIC card application.

2) TWIC reader gets the contents of the unsigned CHUID data object (which contains an unsigned FASC-n along with the expiration date).

3) TWIC reader searches the data object to find the FASC-N tagged (0x30) value.

4) TWIC reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Issue. The TWIC reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or selected elements of the FASC-N.

A.2 Active Card Authentication

In addition to a TWIC card application, every TWIC card also contains a separate application with its own application identifier (AID) that is compatible with the Personal Identity Verification (PIV) specification as referenced in the NIST FIPS 201-1 standard and its associated special publications. The PIV card application includes a Card Authentication Key and Certificate that may be used over the contactless interface for the purpose of authenticating that the card was issued by a trusted authority. This provides a mechanism that strongly binds the cardholder’s identity (via the FASC-N) to the physical card token by embedding a piece of secret data in the chip that cannot be copied via any interface. This key data may be used in conjunction with the freely readable certificate to prove that the card has not been cloned or spoofed. Note that the card authentication key is defined as a local private key to the PIV application, only available after successful selection of the PIV application and is not accessible via the TWIC card application.
This mechanism requires that a credential presented to the system (or a TWIC reader it is connected to) shall be capable of performing an asymmetric Private Key operation such as an RSA signature generation. A TWIC card is issued with the optional Card Authentication Key and Certificate as specified in NIST SP 800-73, Revision 1. The certificate profile standardizing the contents of the Card Authentication Certificate is documented by the Federal Identity Credentialing Committee’s Shared Service Provider subcommittee. Note that, unlike the Certificate/Key containers used exclusively on the contact interface of the FIPS-201 credential, the Card Authentication Certificate does not require or support a PIN to unlock the information prior to usage. This means that any contactless FIPS-201 card represents a strong single authentication factor (possession), and any additional authentication factors (PIN, biometric) need to be managed external to the card application itself (either in the PACS with a PACS PIN, or using another application such as the TWIC card application for biometric authentication of the user). To support local (on-card) second and third factor authentication with a FIPS-201 PKI credential, the PIV card application employing the contact interface of the card shall be used.

A TWIC reader (or panel, with bi-directional wiring) shall be locally configured with the public keys (or, more typically, a full X.509 certificate containing the public keys) for one or more Certificate Authorities (CAs) that are trusted for issuance of TWIC Card Authentication Certificates. This may be limited to the issuing CAs for TSA, or may include external CAs from other agencies to authenticate federated identities. This may be the same set of trusted CAs that should be stored on each TWIC reader in order to authenticate the CHUID signing certificate on a TWIC card, as required for biometric verification. The cryptographic operations performed by a TWIC reader (e.g., RSA signature verification) should be of the same type as those required by the biometric verification, and hence require an equivalent level of computing resources at a TWIC reader (e.g. a 32 bit embedded processor or cryptographic co-processor).

The public key information in a TWIC reader is not treated as secret or sensitive data, so extraction of this data from a TWIC reader does not create a security risk. However, incorrect configuration of a TWIC reader with illegitimate Authority Keys may result in that TWIC reader accepting the authenticity of illegitimate tokens.

A TWIC reader (or bi-directional panel) also needs to have access to a system clock capable of providing the current date and time. The current date and time is required to determine the expiration status of a TWIC card.

The output of a TWIC reader, upon successful authentication, depends on the infrastructure capabilities and requirements. When card authentication is performed, the TWIC reader shall obtain the encoded FASC-N and expiration date from the Card Authentication Certificate.

The entire verified Card Authentication Certificate may be passed to the access control system for more advanced processing.

1) TWIC reader selects the PIV Applet.
2) TWIC reader gets the content of the Card Authentication data object (tag = 5FC101).
3) TWIC reader retrieves the binary contents of the Certificate value (tag: 0x70).
4) TWIC reader retrieves the content of the CertInfo value (tag: 0x70).
5) If the least significant bit of the CertInfo value is ‘1’, then the contents of the Certificate value are compressed using the “gzip” algorithm, and are decompressed by a TWIC reader to produce the raw DER-encoded X.509 certificate. Otherwise, the contents of the Certificate value may be used without decompression.
6) The “issuer” name in the Certificate is compared against the “subject” name in each trusted issuing CA certificate stored on a TWIC reader. For each CA with a matching name, the Public Key is used to attempt to verify the signature on the token’s Certificate. If no matching CA certificate is found on a TWIC reader
with the same name and with a Public Key that verifies the signature on the certificate, then the Certificate is rejected.

7) If the date encoded in the Certificate’s “notBefore” validity date is after the current date/time, or if the Certificate’s “notAfter” validity date is before the current date/time, the Certificate is rejected.

8) If the Certificate’s “keyUsage” extension does not contain the “digitalSignature” flag, the Certificate is rejected.

9) If the Certificate’s “extendedKeyUsage” extension does not contain the “id-TWIC-cardAuth” keyPurposeID (1.3.6.1.4.1.29138.6.8), the Certificate is rejected.

10) If the Certificate’s “subjectAltName” extension is present with the “twicFASC-N” (1.3.6.1.4.1.29138.6.6) name entry, this value shall be retrieved from the certificate for optional transmission to a panel or back-end (e.g. IDMS infrastructure).

11) If the Certificate contains any unknown extensions with the Criticality flag set to TRUE, the Certificate is rejected.

12) TWIC reader generates a random or pseudo-random challenge of at least 127 bytes of unique data and transmits this to the TWIC card using the GENERAL AUTHENTICATE APDU command.

13) The response (i.e. the card’s signature) from the GENERAL AUTHENTICATE APDU command is verified using the Public Key from the Certificate. If verification fails, the TWIC card is rejected.

14) If verification has succeeded, the Certificate is accepted as an assurance factor. Identifying information (e.g. the Certificate, the FASC-N, or other unique identifying components) may be immediately used locally or at a panel as input for the access control rules, or supplemental second and third factors (e.g. PIN, biometric) may be independently evaluated.

If the biometric authentication factor was also verified, then the FASC-N from the biometric shall be identical to the FASC-N contained within the Card Authentication Certificate. If they do not match, then the biometric and the TWIC card do not belong together, so one shall be rejected.

A.3 CHUID Verification + Biometric User Authentication

The TWIC card application (as well as the PIV card application present in the same card) contains a biometric template of fingerprint minutiae bound to the cardholder’s FASC-N identifier via the digital signature of the card issuer. The signed fingerprint biometric template is stored in the TWIC card application in a format that is enciphered using a card-specific TWIC Privacy Key (TPK). The TPK is not available via the contactless interface, although the TPK may be retrieved via either the magnetic stripe or contact interface of a TWIC card. This retrieval of the TWIC Privacy Key from a TWIC card may occur at every TWIC reader during each access transaction, or obtained by a TWIC reader from the PACS where the corresponding TPK was stored as a one-time operation during card registration.

In order to confirm that the cardholder matches the stored biometrics, the data shall be retrieved, deciphered, verified, and matched against a live finger.

1) TWIC reader loads the TWIC Privacy Key from a TWIC card from local memory, a server, the magnetic stripe of a TWIC card, or the contact interface of a TWIC card.

2) TWIC reader selects the TWIC card application in a TWIC card.

3) TWIC reader selects the fingerprint object.

4) TWIC reader gets the contents of the fingerprint data object and CHUID.

5) The enciphered fingerprint template TLV (tag: 0xBC) is retrieved from the fingerprint data object.

6) The enciphered fingerprint template is deciphered using the TWIC Privacy Key.
7) The CBEFF record is parsed into the ANSI/INCITS 378-2004 fingerprint body, FASC-N and the digital signature.

8) TWIC reader verifies that the digital signature on the CBEFF record was produced by an authorized document signer. This requires that the TWIC reader have a verified copy of the document signer’s X.509 digital certificate. The public key from this verified document signing certificate shall verify the signed biometric data.
   a) The TWIC reader shall retrieve the expiration date from the CHUID and the document signer’s certificate from the CHUID signature field, since the CHUID shall be signed by the same entity as the biometric. The TWIC reader shall verify that the CHUID signing certificate from a TWIC card was signed by one of the trusted card issuing Certificate Authorities from TSA or another locally trusted issuer.

9) A finger is sampled from the cardholder. This image shall be matched against one of the fingerprint minutiae stored in the signed biometric object at an appropriate level of confidence (see Section 8). If the fingerprint does not match the template on the first attempt, the TWIC reader may prompt for subsequent attempts without requiring the TWIC card to be read again.

10) If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object may be used as the identification number. This value shall match the FASC-N from any other authentication factors that are matched to know that they are bound together by the card issuer.

A.4 CHUID Signing Certificate + Active Card Authentication + Biometric User Authentication

This two factor authentication mode of operation performs an active card authentication and a biometric user authentication.

Section A.2 details active card authentication.

When performing two factor authentication, the biometric user authentication process varies from Section A.3 in that only the document signing certificate is required to be read from the signed CHUID. The FASC-N and expiration shall be obtained during Active Card Authentication. The FASC-N obtained from Active Card Authentication shall be used to match the FASC-N found in the biometric data.

In order to confirm that the cardholder matches the stored biometrics, the data shall be retrieved, deciphered, verified, and matched against a live finger.

1) TWIC reader performs an Active Card Authentication.

2) TWIC reader loads the TWIC Privacy Key from a TWIC card from local memory, a server, the magnetic stripe of a TWIC card, or the contact interface of a TWIC card.

3) TWIC reader selects the TWIC card application in a TWIC card.

4) TWIC reader selects the fingerprint object.

5) TWIC reader gets the contents of the fingerprint data object.

6) The enciphered fingerprint template TLV (tag: 0xBC) is retrieved from the fingerprint data object.

7) The enciphered fingerprint template is deciphered using the TWIC Privacy Key.

8) The CBEFF record is parsed into the ANSI/INCITS 378-2004 fingerprint body, FASC-N and the digital signature.
9) TWIC reader verifies that the digital signature on the CBEFF record was produced by an authorized document signer. This requires that the TWIC reader have a verified copy of the document signer’s X.509 digital certificate. The public key from this verified document signing certificate shall verify the signed biometric data.

   a) The TWIC reader shall retrieve the document signer’s certificate from the CHUID signature field, since the CHUID shall be signed by the same entity as the biometric. The TWIC reader shall verify that the CHUID signing certificate from a TWIC card was signed by one of the trusted card issuing Certificate Authorities from TSA or another locally trusted issuer.

10) A finger is sampled from the cardholder. This image shall be matched against one of the fingerprint minutiae stored in the signed biometric object at an appropriate level of confidence (see Section 8). If the fingerprint does not match the template on the first attempt, the TWIC reader may prompt for subsequent attempts without requiring the TWIC card to be read again.

11) If the fingerprint matches successfully, then the authentication factor is successful, and the FASC-N from the data object may be used as the identification number. This value shall match the FASC-N from any other authentication factors that are matched to know that they are bound together by the card issuer.
Appendix B TWIC Privacy Key Network Processing (INFORMATIVE)

This Appendix describes a method that may be used to perform the TWIC Privacy Key retrieval from a PACS system.

The method is based on a simple XML-RPC Request/Response message. (see http://www.xmlrpc.com/)

The Base64 conversion used in this Appendix was performed using a Web-based utility located at http://www.motobit.com/util/base64-decoder-encoder.asp.

The XML-RPC example uses the following data:

1) Request data using a FASC-N of 25 hexadecimal bytes with value of ->
   D70339DAA1822C10842125A1685821084216C1B9870339A3EB

2) Return data of a TWIC Privacy Key of 16 hexadecimal bytes with value of ->
   30313233343536373839303132333435

The Base64 encoding of the FASC-N yields ->
   1wM52qGCLBCEISWhaFghCEIWwbmHAzmj6w==

The Base64 encoding of the TWIC Privacy Key yields ->
   MDEyMzQ1Njc4OTAxMjM0NQ==

An example input request using the FASC-N as a PACS record index is illustrated here:

```
POST /RPC2 HTTP/1.0
User-Agent: reader
Host: reader1
Content-Type: text/xml
Content-length: xx

<?xml version="1.0"?>
<methodCall>
  <methodName>Key Lookup</methodName>
  <params>
    <param>
      <value><base64>1wM52qGCLBCEISWhaFghCEIWwbmHAzmj6w==</base64></value>
    </param>
  </params>
</methodCall>
```

NOTE: The request Content-Length field value was not computed for this example.
The input parameter value corresponds to the unique user ID (i.e. FASC-N) that was read from a TWIC card as a binary value and base64 encoded.

The response shall be, as a minimum, a base64-encoded 128-bit (16-byte) AES decipherment key:

HTTP/1.1 200 OK
Connection: close
Content-Length: xx
Content-Type: text/xml
Date: Fri, 19 Feb 2008 19:55:08 GMT
Server: TWICLand Frontier/5.1.2-WinNT

<?xml version="1.0"?>
<methodResponse>
  <params>
    <param>
      <value><base64>MDEyMzQ1NjcXOTAxMjM0NQ==</base64></value>
    </param>
  </params>
</methodResponse>

NOTE 1: The response Content-Length field was not computed for this example.
NOTE 2: The Host may elect to transmit a fixed, maximum length TPK value field (32 bytes). Transmission of a fixed length TPK value field is encouraged for extensibility reasons. The expected TPK decoded data in the (not detailed) longer response message using the example value of the TPK should be:

3031323334353637383930313233343500000000000000000000000000000000.

TWIC readers should be able to correctly extract the TPK from either form of the XML-RPC response.
Appendix C TWIC Reader Adaptability (NORMATIVE)

C.1 Change of operation mode

TWIC readers shall support multi-mode operation and be able to accept external triggers for the mode change. A mode change should apply to applications such as a threat level change (e.g., maritime security or MARSEC levels).

C.2 Accepting new operating modes

TWIC readers should be capable of various modes whether currently defined by the Coast Guard or not. Also, it is anticipated that TWIC shall be expanded to all transportation modes in the future. Therefore, TWIC readers should be capable of supporting secure firmware modification allowing definition of new modes of operations as may be required.
Appendix D TWIC Reader Compatibility With Other Card Types (INFORMATIVE)

Some sites may need to use TWIC readers and the associated PACS with other cards in addition to the TWIC. In some situations, a TWIC reader may be required to read multiple card types such as the Department of Defense Common Access Cards (CACs) and the Federal Personal Identity Verification (PIV) cards in addition to TWIC cards. In such an environment, a TWIC reader should be capable of selecting the application identifier (AID) associated with these different card types and, on successful selection of a specific card application, behave in accordance with the requirements of the specific card application. For a site that may use multiple card types, a TWIC reader should support the configuration of default AIDs.

As no standard mechanism exists to recognize the smart card type presented based only on the ATS (answer to select) or ATR (answer to reset), each TWIC reader is forced to use a sequence in which it shall apply one or more SELECT APDU commands to connect to a particular card application. For example, at an access point where most cards are CAC cards, a TWIC reader may be configured by default to first start by selecting the CAC card application, then the TWIC card application if no CAC card application is found in the card, then the PIV card application if no TWIC or CAC card applications are found. In most situations, the TWIC card is expected to be the prevalent card used and for this reason, the TWIC AID should be configured as the first application selected by the TWIC reader unless otherwise required by local operational policy.
Appendix E TWIC AID Structure (NORMATIVE)

This section defines how the TWIC Application Identifier (AID) is defined and how it should be used in TWIC applications developed for TWIC readers.

The AID used for the TWIC application shall consist of a 5 byte Registered Identifier (RID) and a 6 byte Proprietary Identifier Extension (PIX).

E.1 Registered Identifier (RID)
TSA has obtained an international Registered Identifier (RID) in accordance with ISO/IEC 7816-5. The RID is represented here by the hexadecimal string "A0 00 00 03 67". This hexadecimal string is also called the TSA RID.

E.2 Proprietary Identifier Extension (PIX) Structure
All TSA applications using the RID "A0 00 00 03 67" shall have a similar PIX structure.

The first two bytes of the PIX are used to define the group to which the card application belongs. The values '00 00' and 'FF FF' are currently not defined and these values are reserved for future use. The following group values are defined:

- applications used by TSA employees or contractors: group = '10 00'
- applications used by non TSA employees or contractors: group = '20 00'

The next two bytes of the PIX are used to identify the application within a group. The values '00 00' and 'FF FF' are currently not defined and these values are reserved for future use. The following applications are allocated:

Applications Group '20 00'
- TWIC application number '00 01'

The final two bytes of the PIX define the class of TWIC card and release edition. Release edition references the edition of the card application data model and card edge supported. Release editions are NOT linked to the Version number of this specification.

A major release value shall be changed if the card application data model is changed due to changes in mandatory data objects OR if the card edge (i.e. APDU commands) is modified or enhanced in a manner that would impact operational use of the TWIC card. Major releases start at “1”.

A minor release value shall be changed if the card application data model is changed due to changes in optional data objects that may impact operational use of the TWIC card. Minor releases start at “1”.

The next to last byte of the PIX is used to identify the major release of the data model and card edge edition as well as the class of TWIC card. If the most significant bit of this byte is set to one ('1') the card is a test TWIC card. In this case, a TWIC reader may configure itself in a diagnostic mode and execute one or more testing/diagnostic functions (presuming such a mode is allowed and enabled) when a test TWIC card is presented. The remaining 7 bits of this byte indicate the major release of the data model and card edge edition.

The major release of the data model and card edge edition is currently defined as release '1' (or '000 0001' in binary format).
The last byte of the PIX indicates the minor release of the data model and card edge edition. The minor release values '00' and 'FF' are currently not defined and these values are reserved for future use.

The minor release TWIC data model and card edge edition is currently defined as release ‘1’ (or ‘0000 0001’ in binary format).

A TWIC reader may use the least significant 7 bits of the major release and the all bits of the minor release to form a data model and card edge edition Version designation expressed as MAJOR.MINOR.

The TWIC application data model and card edge edition is currently defined as Version 1.1.

<table>
<thead>
<tr>
<th>Bytes of the AID</th>
<th>Symbol</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 5</td>
<td>RID</td>
<td>A0 00 00 03 67</td>
<td>TSA RID</td>
</tr>
<tr>
<td>6 &amp; 7</td>
<td>Grp</td>
<td>00 00 &amp; FF FF</td>
<td>Reserved values</td>
</tr>
<tr>
<td>8 &amp; 9</td>
<td>App</td>
<td>00 00 &amp; FF FF</td>
<td>Reserved values</td>
</tr>
<tr>
<td>10</td>
<td>Major Release</td>
<td>00 &amp; 7F</td>
<td>Reserved values</td>
</tr>
<tr>
<td>1xxx xxxx</td>
<td></td>
<td>01 or 81</td>
<td>TWIC specification major release 1</td>
</tr>
<tr>
<td>11</td>
<td>Minor Release</td>
<td>00 &amp; 81</td>
<td>Reserved values</td>
</tr>
<tr>
<td></td>
<td></td>
<td>01</td>
<td>TWIC application minor release 1</td>
</tr>
</tbody>
</table>

Note: The AID may use up to 16 bytes and TSA reserves the right to use all the possible 11 bytes of the PIX in other card applications.

The AIDs that shall be recognized for a TWIC card application are:

- A0 00 00 03 67 20 00 00 01 01 01 01 Operational TWIC Card
- A0 00 00 03 67 20 00 00 01 81 01 Test TWIC card

Only one TWIC AID release edition, using the PIX structure defined in this specification, shall exist on a given TWIC card.

Note: A TWIC reader looking for a TWIC card application should always use a partial SELECT APDU command and request only the first 9 bytes of the TWIC AID (i.e. “A0 00 00 03 67 20 00 00 01”).

A TWIC card shall respond with the full AID of the TWIC card application that exists on this TWIC card (including the release edition as well as the test bit indicator). A TWIC reader shall verify if the TWIC reader supports the release edition (or test mode) returned by the TWIC card. Release editions of the data model and card edge should be upward compatible.

In the unlikely case a new TWIC card application release edition cannot be made upward compatible, (thus creating a potential problem for existing TWIC readers) a new application AID shall be defined using the TSA RID and a new PIX structure.
Appendix F Use of Get Response APDU at the application layer (INFORMATIVE)

Most cards in use today, as well as interface drivers and card readers are using short length fields in APDU coding; thus limiting the amount of data which may be received (i.e. 256 bytes) in a single APDU command. This creates a protocol limitation of data block exchanges between a TWIC reader and a TWIC card application. Such cases are explained in ISO/IEC 7816-3 and some resolution options are available in ISO/IEC 7816-4 to address this limitation.

When cards, drivers and readers are able to use the extended length format of APDUs, data blocks of up to 64K bytes of information may be exchanged without having to deal with low level data transport concerns. It is important to clearly explain this issue at the transport layer so the application layer is not adversely impacted when smart cards, in the near future, support large data block transfers.

Two different mechanisms are available in ISO/IEC 7816-4 to address this short length APDU issue:

1. Employ command chaining. This mechanism is commonly used for case 3 commands (e.g. PUT DATA with INS byte = ‘DA’) as used in PIV. Command chaining is not always supported by the same smart card for case 2 commands (e.g. GET DATA with INS byte = ‘CA’) or case 4 commands (e.g. odd INS byte GET DATA with INS = ‘CB’).
2. Use the GET RESPONSE APDU command at the application layer.

The recommended mechanism is to use the command chaining process but, as this mode is not mandated for commands retrieving information from a smart card by any ISO, PIV or TWIC specification, the smart card may not support such behavior. Unfortunately, other than trying the GET DATA APDU command with the command chaining bit set to “1”, there is no simple way to know if the smart card accepts command chaining for retrieval of information (i.e. odd INS byte GET DATA with INS = ‘CB’).

Most PIV compliant smart cards (supporting transmission protocols T=0 or T=1) use the GET RESPONSE APDU command either for each elementary block (T=0 at the transport protocol layer) or for blocks larger than 256 bytes at the application layer (T=1 and T=CL). This appendix details this GET RESPONSE mechanism with the motivation TWIC reader manufacturers may implement TWIC card interfaces in a consistent and coherent manner.

In most TWIC reader implementations, the limit between the TPDU layer (transport layer dependent on the transport protocol) and the APDU (application layer interface) may be difficult to establish. It is highly recommended for TWIC reader manufacturers to keep these two layers separated. These layers exist to some extent “between” the specified behaviors detailed in ISO/IEC 7816-3 and ISO/IEC 7816-4. Separation of these layers should allow better interoperability and less dependency on a given TWIC card implementation.

This appendix describes a way TWIC readers should implement the use of the GET RESPONSE APDU command.

The described mechanism does not address (or use) the GET RESPONSE APDU command and length management defined in secure messaging modes (e.g. as defined in ISO/IEC 7816-4 or GlobalPlatform). The description herein should be compatible with secure messaging but may not cover all secure messaging behavior of smart cards.

In the description below, it shall be presumed that:

- The TWIC reader application layer has a maximum buffer size available of 64K bytes. The TWIC reader application layer makes all information requests using the extended length format. The TWIC reader application does not know the type of protocol the card is using.
• The interface layer (driver) has a maximum buffer size of 256 bytes. All interface layer (driver) requests to the smart card are made using a short length format.

• The smart card may or may not support extended length but receives all the requests in short length formats.

• For any layer, a length of Le = ‘00’ in short format or a length of Le = ‘FF 00 00’ in extended format is always interpreted to mean "all you may get" up to the size of the requester’s receiving buffer (i.e. ‘00’ = 256 or ‘FF 00 00’ = 64K bytes).

For T=1 smart cards, the driver layer shall:
1. Issue a GET DATA APDU command to the smart card with a maximum length of Le = '00'.
2. If the data object length is smaller than 256 bytes, the smart card shall respond with the data object, the actual length of the data object in the block returned and a return code of ‘62 82’ in response indicating there are less data bytes than expected.
3. If the data object is larger than 256, the smart card shall respond with the first 256 bytes of data and send a return code of SW1-SW2 = ‘61 xx’. Note that xx = ‘00’ indicates at least 256 bytes of data is still available for transfer. The driver layer shall then re-issue a GET RESPONSE APDU command for a length of Le = ‘xx’ until it either receives the return code ‘90 00’ (all data retrieved) or until it has reached the maximum data length supported by the application layer (i.e. 64K bytes).

For T=0 smart cards, the driver layer shall translate APDUs to TPDUs:
1. Issue the GET DATA APDU command (odd INS byte) to the smart card (without any Le).
2. The smart card returns no data (as this is not possible in T=0) in response to the GET DATA APDU command and provides a return code of ‘61 xx’ indicating the command has been successful and ‘xx’ bytes of information are available. The driver then issues a GET RESPONSE APDU command with a length Le = ‘xx’. If the return codes are again ‘61 xx’, the driver loops on this function until it gets either a return code of ‘90 00’ or it reaches the maximum data length supported by the application layer (i.e. 64K).
Appendix G  Interpretation of the Biometric Template CBEFF Header (NORMATIVE)

The biometric template shall be encoded in a manner that communicates to a TWIC reader:

1) The presence of zero, one or two fingerprint minutiae patterns for use in 1:1 matching logic.
2) The quality level of said fingerprint minutiae for use in 1:1 matching logic.

The information in this Appendix is in accordance with SP 800-76-1.

TWIC readers shall first check the number of minutiae present to determine if a 1:1 match may proceed.

TWIC readers shall interpret the CBEFF header encoded information as follows:

Normal Case: At least One Usable Fingerprint Minutiae available for 1:1 matching

1) Use ANSI/INCITS 378-2004 Minutiae Template and ignore CBEFF Header Quality Field value.

Exception 1: Unusable Fingerprint Minutiae to perform a 1:1 match

1) Examine ANSI/INCITS 378-2004 Minutiae Template for:
   a) Number of Minutiae = 0
   b) Fingerprint image Quality = 20 [lowest possible]
   c) CBEFF Header Quality Field <= 0
      i) Quality Value = -1 (Meaning -> Failed to compute a value by capture S/W)
      ii) Quality Value = 0 (Meaning -> Quality too low for an effective 1:1 Match)

Exception 2: No Fingers Available at Enrollment Time. 1:1 matching not possible

1) Examine ANSI/INCITS 378-2004 Minutiae Template for:
   a) Number of Minutiae = 0
   b) Fingerprint image Quality = 20 [lowest possible]
   c) CBEFF Header Quality Field < 0
      i) Quality Value = -2 (Meaning -> Assignment not supported)

Note that, for some TWIC cards with usable fingerprint minutiae templates, the CBEFF Header Quality Field may contain the value “-2”. The number of minutiae should always be checked prior to checking the CBEFF Header Quality Field.