SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE ACCESS CONTROL COUNCIL WHITE PAPER

TWIC® Card/Reader Use with Physical Access Control Systems: A Field Troubleshooting Guide

A Guide to Effective Diagnosis and Correction of TWIC® Card/Reader Field Issues

Version 1.0

May 2018

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce, and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Foreword

This document relates to the Transportation Worker Identification Credential (TWIC®). For Personal Identity Verification (PIV) card-related issues refer to the Secure Technology Alliance "PIV Card/Reader Challenges with Physical Access Control Systems: A Field Troubleshooting Guide," available at https://www.securetechalliance.org/piv-card-reader-challenges-with-physical-access-control-systems-a-field-troubleshooting-guide/.

Although the TWIC card is similar to the PIV card, and this document is also similar, there are significant differences. The Secure Technology Alliance PIV card/reader white paper was issued in 2012. This TWIC white paper incorporates subsequent lessons learned and is focused on issues specifically related to TWIC cards/readers for the field troubleshooter audience.

TWIC is a registered trademark of the United States of America, as represented by the Department of Homeland Security.

Table of Contents

1 Compilation of End User Observations, Potential Causes, and Corrective Actions 5
1.1 System Testing Recommendations 5
1.2 Test Lab 5
1.3 Reported Field Issues 6
2 Card and Card Reader Interaction Issues 7
2.1 Card Presentation Issues 7
2.1.1 TWIC Card and Reader Radio Frequency (RF) Field 7
2.1.2 TWIC Card Read Range 8
2.2 Card Reader Issues 8
2.2.1 Insufficient Power Source to Card Reader 8
2.2.2 Incompatible Card Reader Model/Versions 9
2.2.3 Reader Configuration and CHUID 9
2.2.4 Improper Reader Assembly Configuration 9
2.2.5 Unsuccessful Access Attempts 10
2.2.6 Card Reader Installation Issues 10
2.2.7 Card Reader Environmental Issues 11
2.3 Potential Card Anomalies, Card-Related Usage and Interoperability Issues 12
2.3.1 Damaged Card Antenna for Contactless Interface 12
2.3.2 Incorrect Protocol Data Decoding 12
2.3.3 Misinterpretation of TWIC Data Objects 12
3 Potential PACS Control Panel Issues 14
3.1 Incompatible PACS Configuration 14
3.2 Inconsistent Card Performance at Different Access Control Points 14
3.3 Inability to Process the TWIC Identifier (FASC-N) 15
4 PACS Card Registration Issues 16
4.1 Version Incompatibility 16
4.2 Incorrect Encoding 16
4.3 Inability to Process the TWIC Identifier (FASC-N) 16
4.4 TWIC Identifier (FASC-N) Already in the PACS Database 16
5 Publication Acknowledgements 17

6 Appendix A: Basic Troubleshooting 19
6.1 Level One Troubleshooting 19
6.2 Level Two Troubleshooting: Card and Reader Data Operation 20
6.2.1 Generic Tools for Smart Card TWIC Tests 21
6.2.2 Level Two Diagnostic Tests 24
6.3 Level Two Troubleshooting: Power Issues 26
6.4 Level Two Troubleshooting: PACS Registration Issues 27
6.5 Escalation 28
7 Appendix B: Technical Details 29
7.1 Timing Impact 29
8 Appendix C: Qualified TWIC Readers 30

1 Compilation of End User Observations, Potential Causes, and Corrective Actions

This white paper focuses on troubleshooting Transportation Worker Identification Credential (TWIC®) cards and readers. The document categorizes observed symptoms, lists some probable causes, and suggests corrective actions as well as some basic troubleshooting techniques that may easily be performed on site. This white paper is intended to help physical access control system (PACS) operators and users diagnose the cause of the different issues and quickly identify corrective actions. The goals of the recommended procedures are to minimize interruption of daily operations and reduce the need to replace system components such as cards and/or readers.

In a spirit of industry cooperation, the instances described in this paper have been submitted by manufacturers of cards, readers, and PACS; system integrators; installation companies; and credential issuers. The Secure Technology Alliance appreciates the honest and open communication from individuals and organizations that volunteered and supported the inclusion of sensitive product performance information. This white paper represents an excellent example of widespread industry and government cooperation to identify a corrective path towards resolving component compatibility issues that may be experienced by end users, system installers, and service personnel.

1.1 System Testing Recommendations

When deploying a PACS that is composed of many components which were likely obtained from several vendors and installed by contractors, it is important to understand that being tested for a specific environment does not necessarily guarantee component interoperability with other components of the PACS at any given site. It is critical that the PACS implementer perform end-to-end tests to ensure correct configuration and operation of the assembled solution prior to going live with users. These tests will ensure that all acquired components operate together at the same level of functionality in accordance with currently published TWIC specifications, and that the installation has been performed correctly to deliver reliable operation.

After initial installation, any new components being introduced, such as new readers, reader firmware updates, updated PACS software, new generations of TWIC cards, or other type of cards used in the same system (e.g., proximity cards), should also undergo testing to validate interoperability prior to rollout of the new components into an existing installation. It is particularly important to understand that new cards issued by other entities may introduce compatibility issues outside of the implementer's control.

1.2 Test Lab

Some organizations may take the initiative to create an offline testing environment in a lab setting to allow interoperability testing before introducing new components into live systems in the field. Creating this environment is recommended, as over the course of an installation lifetime, requirements in the TWIC Card and Reader Specification[1] card profiles may change. The organization should consider taking into account the specified life of the cards in the field (up to five years), which requires keeping functionalities available with old as well as new cards when they appear. Components that support new functionality

[1] This document can be found at https://homeport.uscg.mil/Lists/Content/DispForm.aspx?ID=2767.

should be acquired for interoperability testing and debugging prior to introduction into live field installations. If the changes are significant, a comprehensive, planned approach to upgrading the field installations should be undertaken to avoid compromising the integrity of the installed systems in use.

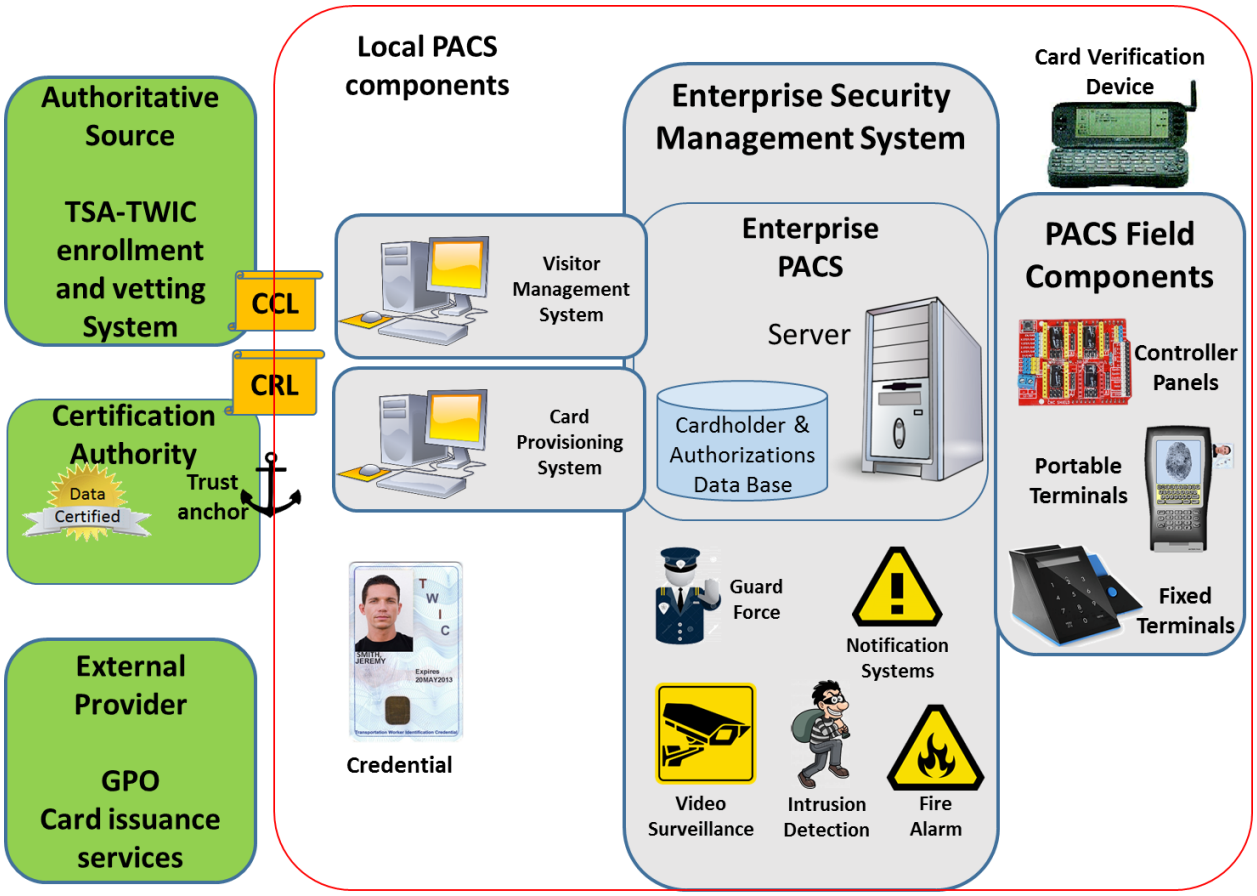

Figure 1. Example of a Typical PACS Using TWIC Cards

It should be noted that even though TWIC cards are visually or functionally similar to PIV cards, the main difference is the issuance model for the TWIC card. The TWIC card is issued by the United States Government, Department of Homeland Security, Transportation Security Administration (TSA) for eligible applicants (not limited to government employees and contractors) and is used by various independent entities in the maritime industry, who are not involved in the issuance of the cards.

1.3 Reported Field Issues

Usage difficulties when TWIC cards are used with contactless readers that are covered in this white paper include:

- Intermittent operation, such as the reader not reading the TWIC card or only sometimes reading the card.
- The card and card reader interaction producing inconsistent numbers or a non-compliant data stream.
- The reader shutting down after unsuccessful attempts to read the card.
- The PACS failing to register some cards (e.g., adding TWIC cards to PACS database).

2 Card and Card Reader Interaction Issues

Symptom: Reader does not read the card; reader does not read the card properly or produces inconsistent data.

Potential causes and basic corrective actions are listed in Sections 2.1 to 2.3 below. The main sources for these symptoms are related to card presentation, reader-card incompatibility, and card-related issues.

2.1 Card Presentation Issues

2.1.1 TWIC Card and Reader Radio Frequency (RF) Field

For contactless operation, the card and reader each contain an antenna to communicate. The communication involves a startup handshake (initiation) step and then a data exchange step. Due to security measures implemented, this is not instantaneous and may take a second or so. The user may not be holding the TWIC card within the card reader RF field long enough for the reader to properly read and process the card data.

The longer card-to-reader initialization time needed for TWIC cards (compared to proximity cards) sometimes causes a user to remove the card from the reader's RF field too soon. The early removal of the card interrupts the initialization/communication process before it is complete. This may cause further delays, as the reader will try to re-establish the connection to the card when the card is presented again. The initialization process may vary slightly with each reader location. The cardholder's patience may also vary during the day, thereby contributing to the perception of intermittent operation.

TWIC cardholders might move between multiple sites with readers and PACS from different manufacturers that operate differently. TWIC users might be new to a site so prior training for using cards with site-specific readers might not be an actionable solution. The TWIC reader that was present indoors at issuance is probably quite different from the one found outdoors on a site.

Some sites require a TWIC card to get into the facility and use a 125KHz Proximity card within the facility for access to restricted areas, with the PACS providing the authorization decisions. These sites might have readers with two different RF frequencies – one for TWIC and one for 125KHz – in the same reader. Features such as reader presentation, orientation, hold time, and read range will be different. So, managing user presentation of a card will be critical to success.

Corrective Actions:

Consider signage with non-language-specific visuals to support ideal orientation of the card to the reader, location of the TWIC sweet spot on the reader for the card, the best way to hold the card for a successful read, and the presence of any audio/visual indicators to observe.

When possible, train cardholders on proper card presentation and expectations of transaction time. Training should be provided when the card is enrolled in a PACS and when the cardholder indicates they are having problems using the card. Show the cardholder what audible and visual feedback is available from the reader to indicate when communication is complete and the card can be removed from the RF field.

Observe the behavior of the visual or audio prompts[2].

Be sure that cardholders understand that they must remove the TWIC card from the electronically-opaque sleeve if one is used. Such sleeves block RF communications. The TWIC card should be presented separated from other cards that may be carried together and that may cause interference.

See Appendix B (section 7) for information about why it takes longer to read a TWIC card than it does to read a 125 KHz proximity card.

2.1.2 TWIC Card Read Range

The TWIC card must be held at the correct distance from and orientation to the reader.

TWIC cards have a short read range and typically must be held at a specific distance from the reader; the distance varies with manufacturer and reader model. Some readers are designed to require the card touch the reader while others allow a range of nearly 2cm (approximately 1 inch). Others still want the card to be more precisely at 1 centimeter in order for the initialization process to be initiated and communications completed. Some manufacturers suggest holding the card one finger width from the reader, but this has problems in that everyone does not have the same size finger. It is equally important that all card surfaces be equidistance from the reader surface. So, it is important to not hold the card between a finger and thumb away from the reader while tapping the other edge of the card on the reader.

Card orientation is equally important. As both the card and reader typically contain oval antennae, it is necessary to hold the card in the right orientation (usually aligning the rectangle of the card with the rectangle of the reader) for best read range. Also, it helps to hold the card on the edge, as having too much hand and finger proximity across the surface of the card can interfere with antenna functionality and separation distance.

Corrective Action: Show the cardholder how to hold the card, perhaps by the edges, so that the card orientation is aligned with orientation and distance that works best with the reader. End user education regarding new card technology is critical when transitioning from one technology to another. Signage placed in strategic areas to provide a reminder of how to use the card correctly will help to eliminate user errors.

See Appendix B for information about why it takes longer to read a TWIC card than it did to read a 125 KHz proximity card.

2.2 Card Reader Issues

2.2.1 Insufficient Power Source to Card Reader

Various TWIC card readers often have different power requirements than legacy proximity or magnetic stripe card readers. Because the TWIC cards and card readers have increased processing capabilities, there is a greater demand for power.[3]

Corrective Action: Contact the reader supplier and verify the card reader voltage and amperage requirement. Confirm that installed power supplies meet power requirements during operation including

[2] See Level One Troubleshooting, Basic Test 6.1, for additional information.

[3] The "TWIC® Card and Reader Specification" provides detailed information about power required for the reader.

all environmental conditions the reader may be exposed to. This includes any interface components required to connect a TWIC reader to a PACS controller, such as a reader interface module. The power supply must be sized to accommodate all components that are attached. Assume they will all operate simultaneously.

If additional power is necessary, it is strongly recommended that the reader interface module and the card reader share the same power supply.

2.2.2 Incompatible Card Reader Model/Versions

A non-TWIC compatible card reader may have been mistakenly installed, or the reader may have been compatible at time of installation but is not compatible with more recently issued cards.

Corrective Action: Contact the reader supplier and verify the card reader firmware against TWIC card versions currently deployed. Replace the reader or update the firmware as required. Most reader suppliers offer various processes for updating firmware and software. Be sure to explore options for field-based upgrades as well as factory-based upgrades.

See Appendix A for second level troubleshooting assistance. Contact the system supplier and provide the diagnostic details for factory assistance and availability of potential updates.

2.2.3 Reader Configuration and CHUID

The reader may be configured to read and send to the PACS only partial data from the Card Holder Unique Identifier (CHUID) field of the TWIC card. The partial data may not provide a sufficiently unique ID across the TWIC cardholder population.

Such a TWIC reader configuration may have been implemented due to PACS limitations; some PACS cannot process the minimum TWIC data required for a unique ID for all cardholders in the user population. This configuration issue might be able to be corrected without component replacement. However, some reported symptoms of intermittent card operation are caused by installation errors affecting one or more readers, creating the impression that the card reader is releasing inconsistent data to the relying system.

Corrective Action: Verify the reader and, if required, the control panel configuration for the inoperable reader location. Document the configuration details and compare these with the configuration settings for those readers that operate as expected. Note and document all differences in configuration. Change as required to achieve normal operation.

See Appendix A (section 6.2), Level Two Troubleshooting, for additional details.

If the issue is related to a PACS that cannot support the required level of uniqueness (length of identifier) then a software patch from the PACS supplier or a different product may be required to address the issue.

2.2.4 Improper Reader Assembly Configuration

The PACS supplier may use their own method to configure the various readers to select the appropriate data from the card, format that data, and transmit the collected data to the PACS control panel. A reader assembly may include firmware loaded and stored within a reader interface component that may be co-located with the reader itself, or in close proximity to the access control point, or even in the PACS control panel.

The reader assembly may not be properly configured for the TWIC data model, for how the card data is extracted from the card, or for how reader data output is formatted for the PACS.

Stack errors (read sequence), data parsing, data formats, and parity checking are a few examples of reader parameters that may require configuration by the installer. Accidentally omitting or incorrectly configuring any of these parameters on one or a few readers will contribute to the perception of intermittent card/reader operation. This may be relatively easy to correct without component replacement.

Corrective Action: Verify the reader and, if required, the reader interface unit and the PACS control panel configurations for the inoperable reader location. Document the configuration details and compare with the configuration settings for those readers that operate as expected. Note and document all differences in configuration. Change as required to achieve normal operation. See Appendix A, Level Two Troubleshooting (section 6.2), for additional details.

2.2.5 Unsuccessful Access Attempts

Reader may be disabled based on unsuccessful attempts to gain access.

Some PACS have a security feature that can be configured to disable the reader after a certain number of unsuccessful attempts to gain access. This may require operator action to restore the reader, or the reader may reset after a specific time window. Depending on authorization policies implemented, some PACS may be configured to lockout the credential instead of,[4] or in addition to, the reader.

Corrective Action: Verify the assigned access privileges for the cardholder. If the card is read properly but the cardholder is not authorized for access at the specific location, the cardholder should be contacted for an interview about why these attempts were made. The system activity log will include the reason for the "access denied" decision. A disabled reader may affect other users who are attempting to use the reader to gain access to the area behind the disabled reader until the reader is enabled.

Verify that the PACS is configured for the correct number of attempts prior to disabling a reader after a specified number of access requests and resulting in an "access denied" decision. Setting this parameter too low may result in a reader or user being locked out after a limited number of attempts. Correct as required.

2.2.6 Card Reader Installation Issues

Readers are sometimes installed near metal beams or on other metallic objects (e.g., aluminum mullions, steel plates). Metallic objects may cause radio frequency (RF) reflections and distortions that have a greater impact on the TWIC card's 13.56 MHz RF frequency transactions than on the legacy 125 KHz frequency transactions. If installers are not aware of how metal within the immediate reader environment impacts a high frequency transaction, card/reader transactions could be compromised. This will contribute to the impression of intermittent operation and failures. Metal in the environment can cause the operational frequency of the card/reader to shift significantly from the 13.56 MHz design parameters.

Improper grounding can also have an impact, especially in a metallic environment. Although there might be a ground wire or terminal at the reader for connection, it is not uncommon for such connections to not

[4] The "TWIC® Card and Reader Specification" stipulates that a reader shall reject the same card if presented less than one second after the first presentation.

be connected all the way back to an acceptable ground (e.g., cold-water pipe) essential for correct operation.

Options for Actions and Corrections:

- The statement of work (SOW) for new installations and upgrades must include clearly defined card reader requirements that are aligned with the functional needs for the site. These should include reader model, firmware version, environmental usage conditions and installation practices.
- Education of card, reader, and integrator sales and technical staff is imperative. Most PACS manufacturers require their value-added resellers (VARs) to be trained and certified and to maintain their competencies with additional supplementary training on new products and implementations on a regular basis. Installers' knowledge of TWIC implementations should be verified before they begin installation, as well as required in the SOW.
- Both local and/or support staff and installers should be required to inspect and identify component versions prior to installation. Expectations for performance and interoperability should be shared with manufacturers and installers.
- Prior to deployment, requirements for component testing should be defined as part of a pre-installation test procedure. Manufacturers design mounting hardware to minimize unpredictability and maximize consistency of the immediate reader RF environment. If possible, testing should be completed at each reader location. Inquire of the reader manufacturer if the specified reader has an auto-tuning or field-tuning option for the contactless antenna or if the reader has a firmware update that addresses the issue. If the reader is not functioning properly and cannot be tuned or updated, inquire if there is a different reader that may be less susceptible to the RF environment.
- Install dual-interface (contactless and contact) readers so that the contact reader may be used as a backup if the contactless interface, for some reason, does not function satisfactorily.
- Acquire and use certified TWIC test cards to validate new card reader installations and reader upgrades. Test cards are available from TSA-TWIC Program Management Office (PMO).[5] U.S. Coast Guards do have a complete set of TWIC test cards able to verify the functionality and conformity of an operational PACS using TWIC cards.
- To mitigate metal environment effects, installers can either add non-metallic spacers or locate the readers farther away. Non-metallic spacers of ½ inch to 1 inch are often used.

2.2.7 Card Reader Environmental Issues

Readers installed in a harsh outdoor environment may be subject to operating issues due to heat, humidity, rain, pollution, or other weather-related factors. Under various conditions (heat, cold, water), the internal frequency of the reader may shift, and it may then start rejecting the cards if they happen to be tuned on the edge of the defined frequency range.

If a given reader (or series of readers) starts to reject cards under certain conditions, such as with temperature, time of the day (e.g., when the sun is high) or very dry conditions, confirm that reader operational parameters are consistent the specific operating environment

[5] Contact information can be found at https://www.tsa.gov/for-industry/TWIC-card-reader-technology or using e-mail at TWIC-Technology@tsa.dhs.gov

The TWIC card and reader specification has a section defining the conditions under which outdoor fixed TWIC readers shall operate.[6]

***Corrective Action*:** Protecting readers from direct sun exposure, making sure they are enclosed in a ventilated case, and eventually protecting them against rain (e.g., if they reject cards when it is raining) are actions which can be taken to improve the reader behavior even when the outdoor conditions are extreme. Readers may need to be relocated.

2.3 Potential Card Anomalies, Card-Related Usage and Interoperability Issues

If a reader is tested and found to be operational, a card-related issue may be causing the usage difficulties. Below is a short list of reported usage symptoms, basic troubleshooting steps, and potential card-related issues.

Symptom: Card is not read at any reader.

2.3.1 Damaged Card Antenna for Contactless Interface

A damaged card antenna prevents the card from establishing contactless communication with the reader. The most common failure mode is the weakening or breaking of the bond between the antenna and the integrated circuit chip on a dual-interface card. The symptoms might be intermittent at first, making troubleshooting a challenge, or causing the user to believe it is a reader problem rather than a card problem. This failure can be caused by stress, such as sitting on a card in a wallet, using the card as an ice scraper, having pressure from read heads in a contact interface reader, bending the card when presenting it to a reader, or continuously removing and re-inserting the card from the card holder.

Corrective Action:

- First try a known good card on that specific reader; if the reader works, please see below.
- See Appendix A (section 6.1) for level one troubleshooting assistance. Contact the TWIC enrollment center to test the card and eventually replace the card.

2.3.2 Incorrect Protocol Data Decoding

Card readers may not have a complete implementation of the data structure implemented in TWIC cards.[7] If readers don't implement this correctly, it may cause a time-out and prevent the reader from establishing communication with the card.

Corrective Action: See Appendix A (section 6.2) for second level troubleshooting assistance. Contact the system supplier and provide diagnostic details for factory assistance and possible availability of updates. The reader may need further analysis or a firmware update by the reader manufacturer.

2.3.3 Misinterpretation of TWIC Data Objects

Readers or other relying party system components may not recognize some elements of the TWIC data model from the presented card because some data objects are not structured exactly as the reader

[6] See TWIC Card and Reader Specification, section 5.1.3 for fixed readers operating outdoors.

[7] Information is encoded on TWIC cards using Tag-Length-Value structures defined in the ASN.1 Standard.

expects. This may be caused by variations in the number of elements in a given data object or a variation in the version of the TWIC data model. This may cause a mismatch between the card data structure and the reader's interpretation of the card data.

Corrective Action: See Appendix A (section 6.2) for second level troubleshooting assistance and collect diagnostic details. Contact the system supplier and provide the diagnostic details for factory assistance and possible availability of updates.

3 Potential PACS Control Panel Issues

PACS control panels might have incorrect firmware versions or firmware variations within the PACS environment.

Symptoms: The reader model is correct and the reader firmware is correct. However, the system denies access to the cardholder at authorized access control points.

3.1 Incompatible PACS Configuration

PACS can be configured to support a specific reader through field hardware dip switch settings, downloadable host configurations, field configurations, or even firmware updates. All these need to be evaluated if operation is not as expected. As PACS are designed to perform both authentication and authorization, the authorization settings can be as significant as the authentication settings when troubleshooting.

The PACS control panel firmware version may not be fully compatible with the presented TWIC card or reader. This could be a result of accidentally installing an earlier version of the controller.

Corrective Action: Contact the PACS control panel manufacturer to verify correct configuration and firmware version capability to process the TWIC identifier. Reconfigure or update as required.

Some PACS control panels may need to remain configured as "card only" readers even when a TWIC card uses a PIN presentation in the field. This is because the TWIC card will verify the PIN and release the unique Identifier to the reader.

See Appendix A (section 6.2) for second level troubleshooting assistance and collect diagnostic details. Contact the system supplier and provide the diagnostic details for factory assistance and availability of updates.

3.2 Inconsistent Card Performance at Different Access Control Points

The PACS system components are all the same brand, and all readers are the same brand and model and have the current configuration and firmware version. The card works at some access control points, but not all.

Assuming these conditions are not due to environmental issues (see section 2.2.7), in this case, all PACS control panels may not have the same configuration, or the same firmware. This may be the case at sites where a PACS has been installed and, over a period of years, expanded with then-current controllers. Controllers installed earlier may not have been installed by the same company or may not have been updated during system expansions.

Corrective Action: Contact the PACS control panel manufacturer to verify configuration and firmware version capability to process the TWIC identifier (e.g., FASC-N, UUID). Update as required.

See Appendix A (section 6.2) for second level troubleshooting assistance to collect specific diagnostic details. Contact the system supplier and provide the diagnostic details for factory assistance and availability of updates.

3.3 Inability to Process the TWIC Identifier (FASC-N)

PACS controllers may be unable to process the TWIC identifier (Federal Agency Smart Credential - Number (FASC-N)) due to its size or structure. In such cases, the reader may have been configured to translate, transpose, or simplify the card identifier. Using abbreviated identifiers may lead to collisions (i.e., multiple identical numbers) in the PACS user database. This can be the result of the reader configuration, the PACS configuration, the card registration process or a mixture of these.

Corrective Action: Review the TWIC Card and Reader Specification for guidance regarding options for bit length and format of the card unique identifier. 48 bits is the minimum required to support the first three fields of the FASC-N uniquely identifying a card. Some PACS cannot handle this bit length. Contact the reader manufacturer to discuss possible solutions.

4 PACS Card Registration Issues

Registration is the process of adding a TWIC card to the PACS user database and assigning access authority to an identifier associated with the card.

Symptom: The TWIC card cannot be registered (enrolled) in the PACS.

4.1 Version Incompatibility

There may be version incompatibility between the card and PACS database or with the data model that prevents PACS enrollment. The specific card version may not have been previously encountered by the PACS.

Corrective Action: See Appendix A (section 6.2) for second level troubleshooting assistance to collect diagnostic details. Contact the system supplier and provide the diagnostic details for factory assistance and possible availability of updates.

4.2 Incorrect Encoding

The issuer of the card (TSA) may have encoded the credential incorrectly which would then prevent PACS registration. PACS registration may include reading, matching biometrics, verifying validity periods and storing certificates. Note that encoding issues are rare.

Corrective Action: See Appendix A (section 6.2) for second level troubleshooting assistance and collect diagnostic details. Contact the system supplier and provide the diagnostic details for factory assistance and possible availability of updates.

4.3 Inability to Process the TWIC Identifier (FASC-N)

The PACS may be unable to process the TWIC identifier (FASC-N). Using abbreviated identifiers may lead to collisions (i.e., duplicate numbers) in the PACS. Data may be entered in the PACS manually, harvested from the card, or imported from an authoritative database.

Corrective Action: Contact the PACS manufacturer to discuss potential updates.

4.4 TWIC Identifier (FASC-N) Already in the PACS Database

It has happened that mistakes have been made by the system issuing TWIC cards, resulting in duplicate FASC-N card identifiers. This will be detected by a PACS if a same card identifier has been previously registered for another cardholder. In such a situation, the TWIC card should be re-issued.

Corrective Action: Contact a TWIC enrollment center to get a replacement TWIC card.

5 Publication Acknowledgements

This guidance document was developed by the Secure Technology Alliance Access Control Council in the collaboration of the TSA-TWIC PMO to help users diagnose the cause of the TWIC card/reader issues with PACS and provide troubleshooting guidance to quickly identify corrective actions.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance thanks the Council members for their contributions. Participants involved in the development of the 2012 version of the initial white paper included: 3M Cogent, Inc.; AMAG Technology; Booz Allen Hamilton; Codebench, Inc.; CSC; Damalas LLC; Deloitte & Touche LLP; Eid Passport; Exponent, Inc.; Gemalto; Giesecke & Devrient; GSA; HID Global; HP Enterprise Services; IDenticard Systems, Inc.; Identification Technology Partners; Identiv; IDmachines; IQ Devices; NASA; NXP Semiconductors; IDEMIA; Quantum Secure Inc.; RM Industries; Roehr Consulting; SafeNet, Inc.; Leidos ; Secure Mission Systems; SHAZAM; Tyco Software House; U.S. Department of Defense/Defense Manpower Data Center; U.S. Department of State; XTec, Inc.

Special thanks go to **Lars Suneborn**, (Identiv in 2012, Secure Technology Alliance in 2017), who managed the project, recruited participation, contributed content and reviewed this document.

The Secure Technology Alliance thanks the following Council members who contributed to the 2018 TWIC-specific update project:

- **Clay Estes**, HID Global
- **Mike Kelley**, Parsons
- **Gilles Lisimaque**, ID Technology Partners
- **Tom Lockwood**, NextgenID
- **Adam Shane**, Leidos
- **Lars Suneborn**, Secure Technology Alliance
- **Rob Zivney**, ID Technology Partners

The Secure Technology Alliance thanks the following Council members who contributed to writing and/or reviewing this guidance document, the 2012 PIV predecessor version, or both:

- **Christa Addy**, SHAZAM
- **David Andreski**, HID Global
- **Tim Baldridge**, Dept. of Defense/DMDC
- **Don Campbell**, Eid Passport
- **Bob Chesteen**, 3M Cogent
- **Walter Cody**, AMAG Technology, Milestone
- **Nathan Cummings**, HID Global
- **Sal D'Agostino**, IDmachines
- **Tony Damalas**, Damalas LLC
- **Kevin Doty**, HP Enterprise Services
- **Michel Escalant**, Gemalto
- **John Esser**, Oberthur Technologies
- **Frazier Evans**, Booz Allen Hamilton
- **Anna Fernezian**, CSC
- **John Fessler**, Exponent
- **Bob Fontana**, Codebench, retired
- **LaChelle LeVan**, Independent, GSA
- **Michael Lewis**, Dept. of Defense
- **Gilles Lisimaque**, ID Technology Partners
- **Diana Loughner**, IDenticard
- **Stafford Mahfouz**, Tyco Software House
- **Brad McGoran**, Exponent
- **Cathy Medich**, Secure Technology Alliance
- **Bob Merkert**, RM Industries
- **Mike Mostow**, AMAG Technology, CNL
- **Matthew Neumann**, Giesecke & Devrient
- **Neville Pattinson**, Gemalto
- **Zeca Pires**, Datacard Group
- **Rick Pratt**, XTec, Inc.
- **Roger Roehr**, Roehr Consulting
- **Steve Rogers**, IQ Devices
- **Jason Rosen**, NASA

- **Marty Frary**, Independent
- **Christophe Goyet**, Oberthur Technologies
- **Marlon Guarino**, Dept. of Defense/DMDC
- **Walter Hamilton**, ID Technology Partners
- **David Helbock**, XTec, Inc.
- **Daryl Hendricks**, GSA
- **Won Jun**, QuantumSecure
- **Mike Kelley**, Secure Mission Systems
- **Russ Kent**, HP Enterprise Services
- **Harold Kocken**, Deloitte & Touche LLP
- **Kevin Kozlowski**, XTec, Inc.
- **Lolie Kull**, HP Enterprise Services
- **Gurpreet Manes**, SafeNet
- **Dan Schleifer**, IDmachines
- **Adam Shane**, AMAG Technology, Leidos
- **Mark Steffler**, Quantum Secure
- **Mike Sulak**, Dept. of State
- **Lars Suneborn**, Identiv/Hirsch
- **Rick Uhrig**, XTec, Inc.
- **Chris Williams**, SAIC
- **William Windsor**, GSA
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, Identiv/Hirsch

Trademark Notice

6 Appendix A: Basic Troubleshooting

6.1 Level One Troubleshooting

No specific test equipment or skill is required for level one troubleshooting. The assumption for these tests is the availability of both a known good card and a transparent[8] contactless reader attached to a simple diagnostic tool that captures, formats, and transmits the card's free-read data (such as the concatenated FASC-N string that consists of the four-digit agency code, four-digit system code, and six-digit credential number, a total of 14 digits, or 48 bits) to the PACS.

The term "known good card"[9] refers to a TWIC card that has previously been authenticated, whose authentication certificate is not revoked, whose FASC-N is not on the Cancelled Card List (CCL), and that has been correctly registered with the PACS.

Other types of readers may follow the same test process.

Reported symptom: The card does not work; the reader does not read the card.

- Remove the TWIC card from its plastic card holder and check if the card can be read. If the card still doesn't work, proceed with Basic Test 1-1.

Basic Test 1-1: Is the card being activated by the reader?

Some readers are capable of reading both 125 KHz and 13.56 MHz frequencies. Those readers may use the same visual indicator for both interfaces, making it difficult to determine which frequency activated the indicator.

TWIC cards only incorporate the standard ISO/IEC 14443 frequency of 13.56 MHz. The TWIC card used for this test should be presented alone to the reader. According to the TWIC Card and Reader Specification, a TWIC reader shall reject more than one card presented at the same time, and even a good card, if presented again less than one second after the first attempt.

Does the reader react to the card when the card is presented to the reader?

Present the TWIC® card to the reader and observe the reader indicator light (or sound). Different reader brands and models use different methods and colors; however, there is usually a light that changes color when the reader detects the presence of a card. If the indicator light changes when the card is presented, this likely means the reader detects the presence of the card, and that the card transmits information and communicates with the reader.

If not successful when the card is close to the reader's surface, try to present the card at about ½ inch from the reader surface, holding the card by its edges. Depending on the reader manufacturer and model, the card may need to be a little closer or farther away.

Does the reader visual or audible indicator change?

---

[8] A "transparent" reader handles only the exchange transmission protocol but is not involved in parsing or interpreting any application data. Such a reader could be used for any ISO/IEC 14443 compliant contactless smart card or device with the corresponding software in the computer/panel it is connected to.

[9] A good known card is a TWIC card issued to a person.

Answer: Yes. Go to Basic Test 2-1, Level Two Troubleshooting.

Answer: No. Go to Basic Test 1-2.

Symptoms may vary; however, removing the card from the reader's RF field and presenting a different, known good card, if available, are good first troubleshooting steps to validate the reader. Observe the reader behavior and if the known good card works as expected, the indication is that there is a card problem. Retest the card at other reader locations and observe the reader behavior.

Basic Test 1-2: Test the card with direct pressure on the ICC

Place the card so that the card's integrated circuit chip (ICC) is located between the index finger and the thumb of the hand holding the card. Move the card to the surface of the reader and put some pressure on the ICC without bending the card itself. This is one way to test for a broken antenna bond, as the pressure may reestablish a broken connection temporarily.

Does the reader visual or audible indicator change (communication is established)?

Answer: Yes. This indicates that the card is defective (intermittent behavior). Replace the card.

Answer: No. Card is not communicating with the reader. Go to Basic Test 1-3.

Basic Test 1-3: Repeat the test with a known good card

Present a different, known good card.

Does the reader visual or audible indicator change?

Answer: Yes. Conclusion: The reader is likely operational with this version of the card. Check the PACS log to ensure that card number is being read correctly.

Answer: No. Suspect a reader problem. Go to Basic Test 1-4.

Basic Test 1-4: Repeat the test with a known good reader

Repeat Basic Tests 1-1 and 1-2 at a different location. Is the result the same as in Basic Tests 1-1 and or 1-2?

Answer: Yes. Conclusion: The card may be defective. Further tests of the card are appropriate. This may require additional equipment or assistance from the card issuer (TSA). Contact the TSA as soon as possible as problems often occur in batches and the problem may already be known.

Answer: No. The tests produce correct results for a good card and good reader. Conclusion: The reader is operational with the version of the card just presented. Check the PACS log to ensure that the card number is being read correctly and that credential number is authorized for the door.

6.2 Level Two Troubleshooting: Card and Reader Data Operation

Level two tests require some basic skills and the ability to use some diagnostic tools. Diagnostic tools for TWIC® cards are commercially available and may allow some diagnostics of a TWIC card. Contact the PACS manufacturer, the systems integrator/installer or Secure Technology Alliance, for information about available diagnostic tools. Diagnostic tools will typically display the card data that is read by a reader and

transmitted to a display for viewing. Card data that is displayed may include some card information such as the Card Unique Identifier, its expiration date, and other data objects.

Quite often, diagnostic tools require a "good" card to establish a reference to make sure the test is meaningful.

The following section presents some diagnostic tools which are publicly available and may be used for the level two diagnostics.

6.2.1 Generic Tools for Smart Card TWIC Tests

6.2.1.1 Smart Card Tool Set from www.scardsoft.com

This tool can be used for any ISO/IEC contact or contactless smart card when used with a PC/SC reader. It is a very low-level tool which allows communication with the card but does not analyze or interpret (by default) the application information provided by the card.

In order to test if a TWIC card works using this tool, it is recommended that a batch be created with the following two APDU commands:

1. Select TWIC card application: 00 A4 04 00 09 A0 00 00 03 67 20 00 00 01
2. Get CHUID Data Object: 00 CB 3F FF 05 5C 03 5F C1 02 00

The typical response of the card when the second command is successful (return code 90 00) would be the signed CHUID data object as shown in this example**: 53 82 08** B3 30 19 **D7 03 39 D8 41 46 6C 14 40 35 45 A1 68 58 21 9C E7 39 CE 61 87 03 39 A3 EE** 34 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 08 32 30 32 30 30 31 32 31 3D 00 3E 82 08 74 30 82 08 70 06 09 2A 86 48 86 F7 0D 01 07 02 A0 82 08 61 30 82 08 5D 02 01 03 31 0B 30 09 06 05 2B 0E 03 02 1A 05 00 30 0A 06 08 60 86 48 01 65 03 06 01 A0 82 06 04 30 82 06 00 30 82 04 E8 A0 03 02 01 02 02 04 53 5A E8 26 30 0D 06 09 …… (Only the first 127 bytes are shown, the bold red bytes being the FASC-N value code in hexadecimal.)

6.2.1.2 Smart Card Tool from Mgtek (www.mgtek.com/smartcard)

Created to manage smart cards used with Window operating systems, the tool may be used to check if a PIV/TWIC card is working. The tool is designed to cache the smart card PIN in the Microsoft directory and may not be very convenient to use in testing many smart cards. It may ask for the PIN of the card before trying to work with the card presented.

6.2.1.3 SmartUtil from JW Secure (www.jwsecure.com/technologies/smartutil/)

The tool is mainly focused on cards containing certificates for authentication. It is a low-level analysis tool not specifically tailored to PIV or TWIC® cards and may not provide much information about the card content such as its FASC-N.

The screen snapshot in Figure 2 shows the response of the tool when a valid TWIC card is presented.

Note: If the card is not responding, the tool is not very clear about the information. It just says, "no card," as when no card is inserted in the contact reader or presented to the contactless interface.

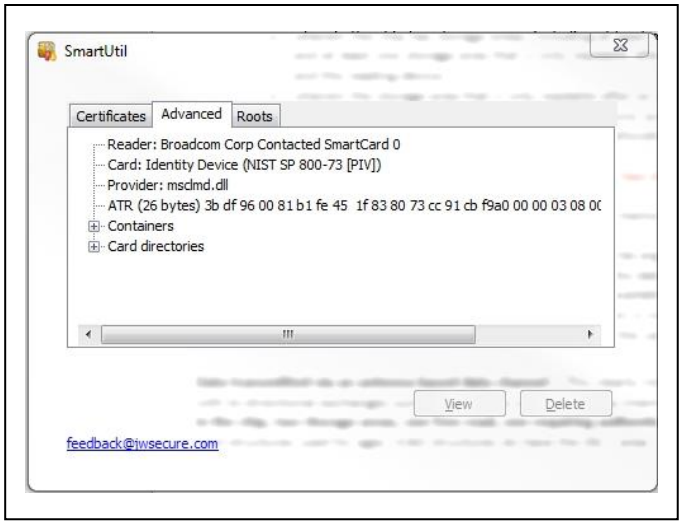

Figure 2. Tool Response with Valid TWIC Card

6.2.1.4 PIVCheck from https://www.hidglobal.com/products/software/pivclass/pivclass-validation-workstation

This tool has been designed to diagnose PIV, TWIC, and First Responder Authentication Credential (FRAC) cards and the Common Access Card (CAC). The tool can be deployed on a laptop, a PC or a handheld terminal. The tool requires the PIN to be presented in order to completely test the card presented.

It allows verification if the card presented has a correct structure (CHUID check), valid authentication certificates, and the cardholder fingerprints, and is not cancelled (it checks the TWIC CCL as well). This tool can verify the user's fingerprint as well when equipped with a fingerprint reader.

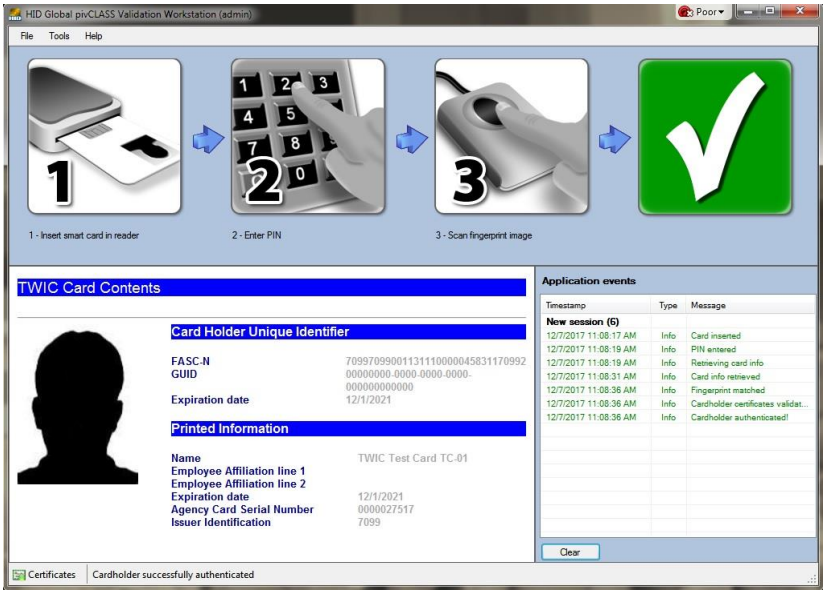

Figure 3. PIVCheck Tool

6.2.1.5 ID-CAT from ID Technology Partners (www.idtp.com/idcat/)

This is a complete and very detailed tool designed specifically for TWIC cards, but it also can be used to diagnose PIV cards. The tool can support contact as well as contactless readers, checks the TWIC cards presented against the Card Cancelled List (CCL), and verifies all of the structures of the PIV as well as TWIC data structures of the card. If the PIN is presented, the private information from the PIV card application is also displayed by the tool (e.g., cardholder picture).

When a card is tested, the tool creates a log of all the exchanges (APDU trace) and can take a digital representation of the card data (called card image in a log) for further analysis.

Like most other smart card tools, the software requires the computer operator to disable/tweak the Microsoft smart card driver/tools to operate correctly under Windows 7 or Windows 10.

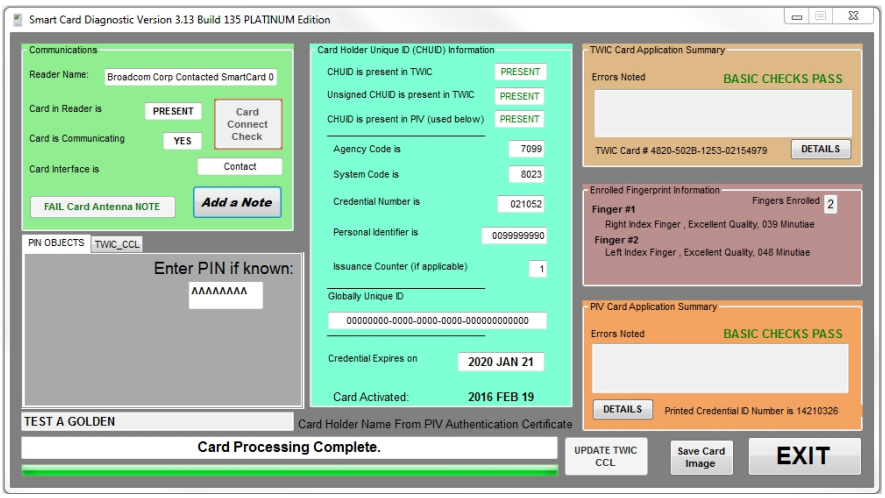

Figure 4. Resulting Screen Shot When a Good TWIC Card Is Presented

Figure 5 shows the message given by the utility when the card presented on a contact reader does not work (unresponsive card).

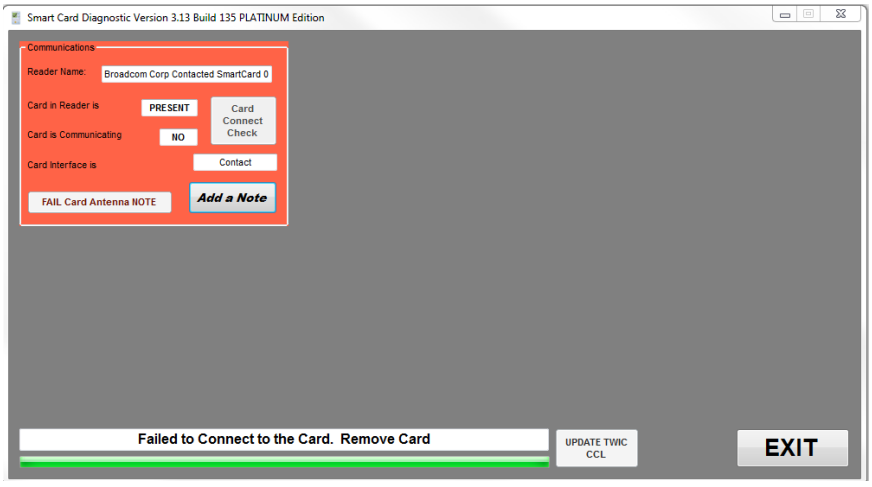

Figure 5. Resulting Screen Shot When an Unresponsive Card Is Presented

6.2.2 Level Two Diagnostic Tests

This section outlines several general tests that can be performed with the diagnostic tools described above using a contactless reader. The process for using diagnostic tools is similar for most diagnostic procedures. In addition, a simple field strength test card that visually shows the strength of the RF field generated by the reader may be a very valuable tool.[10] Please refer to the ISO/IEC 14443-2 standard for the minimum field specification.

Some PACS architectures use a reader interface module that may be located near the card reader to convert the actual data (e.g., Wiegand or ABA) sent from the reader to a vendor-specific format. These modules may contain configuration parameters. For the purpose of this document, when present, such modules are considered part of the reader assembly (see Section 2.2.4). Further troubleshooting details on reader interface modules are out of scope for this document and should be conducted with assistance from a factory-trained technician.

Baseline Test Process

This test is intended to verify that data can be read from both the contact and contactless interfaces of a reportedly defective card and that the CHUID data from both interfaces matches.

1) Connect the contact and contactless reader to the diagnostic tool.
2) Insert a known good card in the contact smart card reader.
3) Observe the display and document the relevant FASC-N data (Agency Code, System Code, and Credential Number).
4) Remove the card from the contact interface reader and present the card to the contactless reader.
5) Read the card and observe the display.
6) The Agency Code, System Code, and Credential Number should be identical to that produced from the same card using the contact interface.

This establishes a baseline for tests of reportedly defective cards as well as for further tests of reportedly defective installed readers.

Repeat the test with a reportedly defective card (one that produced a “no” answer to Basic test 1-1 and/or 1-2.)

Basic Test 2-1

Does the reportedly defective card produce the same values when used in the contact and contactless reader?

Answer: Yes. Conclusion: The card is likely operational. Go to Basic Test 2-2 for reader tests.

Answer: No. Conclusion: The card needs further analysis. Document the observed data, if any, that the diagnostic tool received and displayed. Contact the card issuer.

[10] Such a tool is sold, for example, by the company MicroPross – see www.micropross.com/products.

Basic Test 2-2

This test is intended to verify operation of suspect readers with known good cards.

Most PACS applications feature a method to display card data as received from a card reader installed at an access control point. This will be called the ***diagnostic display*** in this section.

1) While one person (person A) is observing the incoming data at the PACS diagnostic display, another person (person B) takes the known good card to the reportedly defective reader installed at an access control point.
2) Person B notifies person A that he/she has reached the suspect reader.
3) Person A instructs person B to present the known good cards, one at a time, in a predetermined sequence.
4) As person B presents the cards to the reader, person A monitors and documents the received card data on the diagnostic display. This data is then compared with the data documented in the baseline test process described above.

Does the diagnostic display show the expected data received from the known good card?

Answer: Yes. Conclusion: The reader is operational and compatible with the known good cards. Check the PACS log to ensure that the card number is being read correctly and that the credential number is authorized for the door.

Answer: No. The test produces no data. Conclusion: The reader is defective. Check the reader field strength with a field strength test card/tool. If the field strength is appropriate, remove the reader and repeat the test with the reader in a different location. Contact the PACS service provider; provide the test process and results.

Answer: No. The test produces data that is different than expected. Conclusion: The reader configuration/firmware may not be compatible with all card versions or the wiring between the reader and controller may not have been properly terminated. Document the differences in data observed in the diagnostic display. Contact system supplier. Provide the test process and results.

Basic Test 2-3

This test is intended to verify the suspect PACS reader configuration using a known good card.

- Repeat basic test 2-1, above, both at the suspect reader and at a reader that is performing with no problems.

Does the diagnostic display show the expected data received from the known good card?

Answer: Yes. Card and reader are now compatible and operational. End test for this reader.

Answer: No. Remove the reader, and if present, the reader interface module, to check and document reader vintage, version, and serial number. Contact system integrator for verification of reader compatibility; update reader or PACS configuration if necessary.

Basic Test 2-4

This test is intended to verify that a known good reader is operational at the specific location.

- Replace the suspect reader with a known good reader. Repeat Basic Test 2-3.

Does the diagnostic display now show the expected data received from the known good card?

Answer: Yes. The card and reader are now compatible and operational. Arrange for reader update or replacement as required for the remaining readers onsite. End test for this reader.

Answer: No. Contact the system integrator for verification of reader compatibility and correct reader wiring; update reader configuration or repair if necessary.

6.3 Level Two Troubleshooting: Power Issues

A good reader might perform poorly in the field due to power issues. Readers are designed to operate over a specific range of available voltages (such as 5-16 VDC) and current. A reader that is powered by a PACS at the lower limit (e.g., 5 VDC) may be susceptible to voltage drop in the wiring between the PACS power source and the reader. Performance issues can include reduced read range, intermittent operation, and non-operation.

This test is intended to verify that the power is adequate for the card reader, reader interface module and other intermediate components, if present. When the reader has inadequate power during the card transaction, it is likely that a read failure will occur.

1) Consult with the manufacturer's documentation to verify that the power source is sufficient for the reader(s).
2) If more than one reader is connected to a power source, verify that the power source is sufficient to power all connected readers during simultaneous card read transactions.[11]
3) Determine that the voltage at the reader consistently meets manufacturers recommendations with all other connected devices powered up.

Basic Test 2-5

Does the reader have peak power requirements that are greater than the maximum available power?

Answer: Yes. Conclusion: The power source needs to be properly sized to support the number of readers connected. Consult with the system integrator for the proper method of supplying the reader power to comply with manufacturer requirements.

Answer: No. Conclusion: The power requirements are being met by the reader power source. Proceed to Basic Test 2-6.

Basic Test 2-6

Is the reader and interface board properly grounded in accordance with manufacturer's documentation?

Answer: Yes. Conclusion: The reader and interface board are installed in accordance with the manufacturer's documentation.

Answer: No. Connect the ground wires in accordance with the manufacturer documentation. Improper grounding can cause noise and other difficulties with the reader.

[11] This issue may be more apparent during high throughput periods.

Basic Test 2-7

This test is intended to verify PACS panel-to-reader location cabling, power issues and local access control point issues which may affect card-reader operation. Remove the suspect reader from the access control location and connect the reader directly to the PACS control panel.

Repeat Basic Test 2-2.

Does the diagnostic display show the expected data received from the known good card?

Answer: Yes. Conclusion: The reader is operational and compatible with the known good cards. Check cabling between the PACS control panel and access control point for proper cable type, voltage and terminations. End test for this reader.

Answer: No. Reader is likely defective. Contact PACS service provider to arrange further troubleshooting assistance and possible replacement reader. Provide test process and result details.

6.4 Level Two Troubleshooting: PACS Registration Issues

This test is intended to troubleshoot a problem when the PACS will not register the TWIC card. The procedure requires diagnostic tools similar to those described in the level two basic troubleshooting tests above.

1) Connect the contact and contactless reader to the diagnostic tool.
2) Insert a known, good card into the contact smart card reader.
3) If required by the registration system, enter the PIN to release the card's PIN-protected data.
4) Observe the display and document the relevant data.
5) Remove the card from the contact interface reader and present the card to the contactless reader.
6) Read the card and observe the display.

The display may show several errors that affect PACS registration, including an unknown application ID (AID), issues with application selection, and issues with reading the print buffer. These errors indicate that the relying system (in this case the PACS registration server) and the TWIC card are incompatible.

Contact the system supplier and provide the error information from the diagnostic tool for additional support. These details may help the system manufacturer create an update that supports the AID and profile of the presented card. Alternatively, the details might indicate a card failure and a need to contact the card issuer.

Other possible card rejection errors which should normally be detected/provided by the PACS registration module:

- Card has reached is expiration date.
- Card is on the Cancelled Card List.
- Card certificate is invalid, or data object signature is incorrect.
- Card is not a TWIC card.
- Version of the presented TWIC card is not supported by the PACS.

6.5 Escalation

It is important to contact the organizations that provide maintenance and support for the TWIC card (Universal Enrollment System (UES) activation centers or TSA) or for the PACS when the reason of the failure is not understood/diagnosed. This organization will have an escalation procedure for contacting suppliers or integrators to resolve issues. An escalation procedure will likely be required when a new version of the TWIC card or new features in the card are introduced as these options may cause interoperability issues with fielded equipment. Some optional implementations may not be able to be diagnosed in the field and are beyond the objectives and scope of this basic troubleshooting guide and should be addressed between the customer and component providers. Final resolution may be policy related and any policy issues should be resolved prior to technical modifications being implemented to support any options.

7 Appendix B: Technical Details

For card presentation to be successful, it is essential to ensure that the radio frequency energy supplied by the reader is sufficient to initiate the card power-up sequence for its self-test. This process may take more time than users are accustomed to with older or other technology cards. Although a TWIC card should comply with the ISO/IEC 14443 standard for contactless cards, some security requirements imposed by the Federal government, such as NIST FIPS 140-2 validation, impose additional requirements (such as the Cryptographic Module Validation Program [CMVP]) that significantly affect the amount of time required to complete all card-to-reader interactions.

FIPS 140-2 requires a crypto module to perform a self-test on all of its cryptographic algorithms during the power-on sequence. For smart cards that are used to log onto a personal computer every morning, this test sequence is hidden by other processes that are executed simultaneously in the background, such as PIN capture, subsequent authentication, and electronic signatures. However, when cards are used in a PACS, this NIST requirement has a major impact on timing and on power consumption.

Traditional 125KHz Proximity cards and readers are much simpler (and less secure) than TWIC cards and readers. They typically can operate at greater distances, have faster reads, are less orientation sensitive, and have a shorter learning curve. This is mainly due to the fact that the chip only transmits a single number, with no cryptography implemented or power-up self-test.

Some sites might implement readers with separate antennae to support both TWIC and 125Khz technologies. These sites will need to address the additional training and operational challenges associated with the different behavior characteristics of these two different RF and encryption technologies.

7.1 Timing Impact

Because all supported cryptographic algorithms must be tested, regardless of whether they are going to be used in the current session, a TWIC card must run tests on numerous algorithms today (e.g., 3DES, AES, RSA, ECC, SHA1, SHA2, and the random number generator) which can take, depending on the card, up to 500 msec. This amount of time is significant when compared to the average transaction time expected for PACS. For contactless readers, the card must be kept within the RF field for approximately 1 sec to allow both the self-tests and the communications to complete. Visual and audio feedback may be given to let the user know when it is safe to remove the card. User training could help minimize the impact of the longer time.

Note: It is expected that in some near future, in more modern cards, the verification self-tests will be optimized and require less time. This may require firmware updates to card readers.

8 Appendix C: Qualified TWIC Readers

The TWIC Qualified Technology List (QTL) Reader Testing Program was originally established in anticipation of U.S. Coast Guard (USCG) rulemaking that would require the use of qualified TWIC readers for access control by owners and operators of various regulated maritime facilities and vessels (TWIC Reader Rule). While established prior to the final TWIC Reader Rule, numerous TWIC reader vendors undertook the considerable expense to submit their TWIC reader products for formal QTL testing in the expectation that such testing would be required by the anticipated TWIC Reader Rule and would establish a significant market for TWIC QTL listed readers.

The TWIC Reader Requirements – Final Rule was issued by the USCG on August 23, 2016 (Docket No. USCG–2007–28915). This Rule requires certain high-risk vessels and facilities to perform electronic TWIC inspections. However, there is no requirement to use readers from the QTL. The required compliance date set by the Rule is August 23, 2018. Other non-high-risk maritime operators are free and encouraged to deploy TWIC reader devices on a voluntary basis.

Independently of the reader itself, there is no TWIC program available to operators or PACS vendors to verify the functionality/conformity of the PACS in its entirety. Nevertheless, it is possible for a PACS operator to ask the Coast Guard to use the set of TWIC test cards they have in their possession to test the functionality of the PACS as a whole. This card set is composed of nine different TWIC cards, providing the ability to verify the system is working correctly with a good card, and if it detects cards which have been cancelled (on the CCL), which have expired, or which have bad data or bad digital signatures.