PIV Card/Reader Challenges with Physical Access Control Systems: A Field Troubleshooting Guide

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

A Smart Card Alliance Access Control Council and Identity Council White Paper

Publication Date: October 2012

Publication Number: ACC - 12001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Copyright © 2012 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

Smart Card Alliance © 2012

PIV Card/Reader Challenges: Compilation of End User Observations, Potential Causes, and Corrective Actions

The Smart Card Alliance Access Control and Identity Councils have assembled and documented reported usage difficulties and symptoms of Personal Identity Verification (PIV) card and contactless reader failures with physical access control systems (PACS) from field installations. This 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 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 are submitted by manufacturers of cards, readers, and PACS; system integrators; installation companies; and credential issuers. The Smart Card Alliance appreciates the honest and open communication from individuals and organizations who volunteered and supported the inclusion of sensitive product performance information. This white paper is indeed 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 Testing Recommendations

When deploying a PACS that is composed of many components listed on the General Services Administration (GSA) Approved Products List (APL)[1] and that were likely obtained from several vendors and installed by contractors, it is important to understand that being on the APL does not necessarily guarantee component interoperability with other components on the list. Therefore, the implementer must 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 of the acquired components operate together at the same level of functionality in accordance with currently published 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 PIV cards, or PIV card profile changes, 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 agencies may introduce compatibility issues outside of the implementer's control.

Even though components are tested prior to listing on the GSA APL, it is not a given that the listed products will interoperate due to changing specifications and functionality over time; their listings will be associated with a specific set of test procedures and vendor attestations current at the time of their testing.

Interoperability 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, specifications in FIPS 201 and associated special publications as well as locally required PIV card profiles may change. The organization should consider replicating existing products (e.g., PIV-compliant and non-PIV) that are currently in the field in the lab environment. Components that support new functionality 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.

[1] http://fips201ep.cio.gov/apl.php

Figure 1 shows an example of a basic agency test lab configuration.

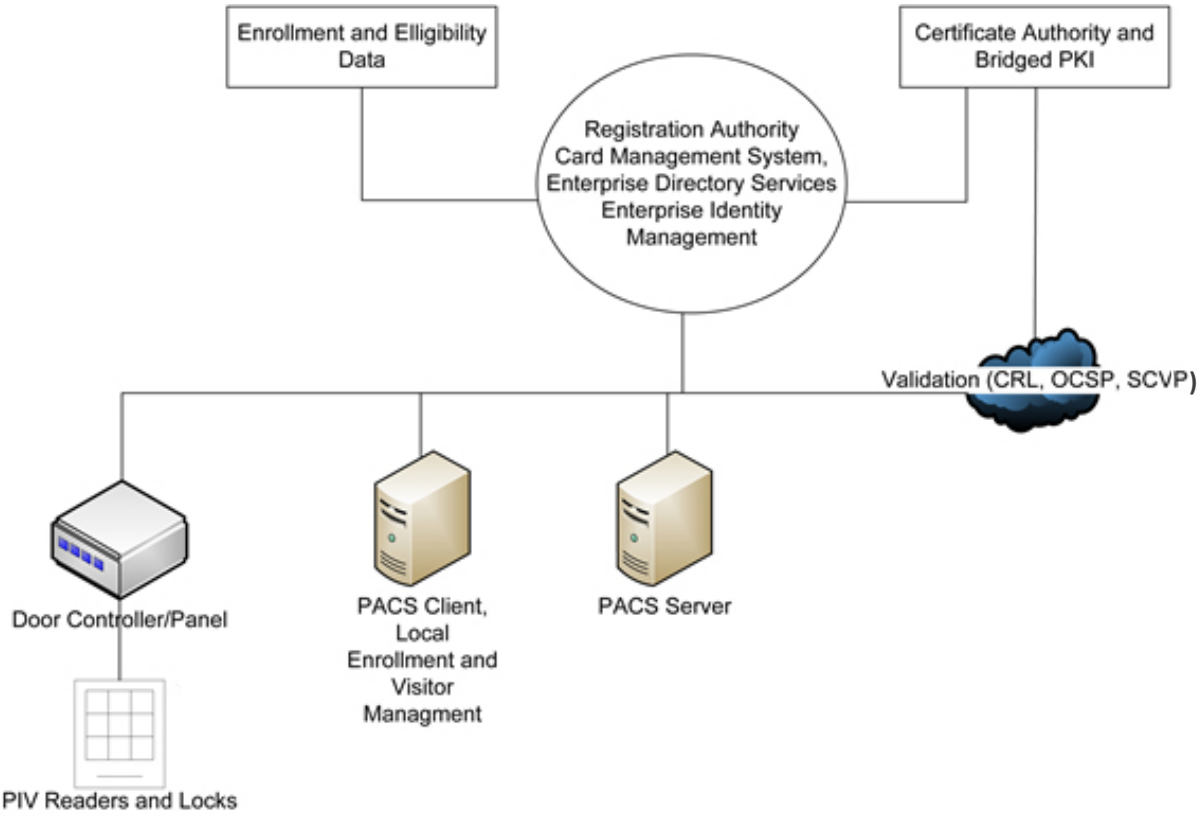

Figure 1. Example of Basic Agency Test Lab Configuration

It should be noted that many different cards from different manufacturers and issuing agencies are used within the Federal government, including the PIV card, PIV-interoperable (PIV-I) card, Common Access Card (CAC), and Transportation Worker Identification Credential (TWIC). The guidance in this white paper is provided for agencies that use FIPS 201-compliant cards and is primarily focused on the use of PIV cards; the guidance is also applicable to CACs that have the PIV container.

For the purpose of this document, TWIC and PIV-I cards are out of scope.[2]

Reported Field Issues

The reported usage difficulties with PIV cards and contactless readers that are covered in this white paper include:

- Intermittent operation, such as the reader not reading the PIV 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

[2] The revised FIPS 201-2 specification is anticipated to include changes relevant to interoperability.

1. 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 1.1 – 1.2 below. The main sources for these symptoms are related to card presentation, reader-card incompatibility, and card-related issues.

1.1. Card Presentation Issues

1.1.1. PIV card and reader field

The PIV card may not be held within the card reader field long enough for the reader to properly read and process the card data.

The longer card-to-reader initialization time needed for PIV cards sometimes causes a user to remove the card from the reader too soon. The early removal of the card interrupts the initialization process and 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 card user's patience may also vary during the day, thereby contributing to the perception of intermittent operation.

Corrective Actions: End user practice and training of both proper and improper card presentation should be provided when the card is issued. Observe the behavior of the visual or audio prompts.[3]

Be sure that end users understand that they must remove the PIV card from the electronically opaque sleeve.

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

1.1.2. PIV card read range

PIV card is not held within the correct read range.

PIV cards have a short read range and typically must be held less than one inch from the reader or must nearly touch the reader itself in order for the initialization process to be completed. See Appendix B for information about why the card must be held close to the card reader.

Corrective Action: 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 PIV card than it did to read a 125 KHz proximity card.

1.2. Card Reader Issues

1.2.1. Insufficient power source to card reader

Various PIV card readers often have different power requirements than legacy proximity or magnetic stripe card readers. Because the PIV card readers have increased processing capabilities, there is a greater demand for power.

Corrective Action: Contact the reader supplier and verify the card reader voltage and maximum amperage requirement. The reader interface module supplier will need to verify if the module supports those power consumption requirements.

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

[3] See Level One Troubleshooting, Basic Test 1-1, for additional information.

1.2.2. Incompatible card reader model/versions

A non-PIV compatible card reader may have been mistakenly installed, or the reader may have been current 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. Replace or update 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.

1.2.3. Reader configuration and CHUID

The reader may be configured to read and send partial data from the CHUID container.

This situation may result from PACS limitations. Some PACS cannot process the minimum PIV data required by Special Publication (SP) 800-73-3.[4] This configuration issue presents an opportunity for installation errors that may be relatively easy to correct without component replacement. 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 differences in configuration. Change as required to achieve normal operation. See Appendix A, Level Two Troubleshooting, for additional details.

1.2.4. Improper reader assembly configuration

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

The reader assembly may not be properly configured for the PIV data model, read sequence, or GSA APL specified data output.

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 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 differences in configuration. Change as required to achieve normal operation. See Appendix A, Level Two Troubleshooting, for additional details.

1.2.5. 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

[4] http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf

implemented, some PACS may be configured to lockout the credential instead of, 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 only one attempt. Correct as required.

1.2.6. Reader-related interoperability.

Readers should be tested for ISO/IEC 14443 compliance. ISO/IEC 14443-4, paragraph 7.2, provides an optional provision of the ISO/IEC standard that covers the wait time between sent and received data packets. Non-compliance may prevent a reader from establishing communication with the card.

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

1.2.7. 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 PIV card 13.56 MHz 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. Reader antennae may need to be tuned for the environment, which can include the standard or installer-supplied mounting box, even when not otherwise mounted on metal.

Corrective Actions

- The statement of work (SOW) for new installations and upgrades must include clearly defined card reader requirements that are aligned with functional needs for the agency. These should include reader model, firmware version, 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 PIV implementations should be verified before they begin installation.
- Local 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 PIV test cards to validate new card reader installations and reader upgrades. Test cards are available from NIST[5] and card manufacturers.

2. 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

2.1. 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 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, pressure from read heads in a contact interface reader, or continuously removing and re-inserting the card from the electronically opaque card sleeve or card holder.

Corrective Action: See Appendix A for level one troubleshooting assistance. Contact the card manufacturer for warranty replacement information. Cards are issued by a different organization than the PACS or reader manufacturer and will have a different procedure to remedy any issues.

2.2. Incorrect protocol encoding

Cards and/or card readers may not have a complete implementation of ASN.1 parsing. The encoding differences between the cards and readers may prevent a card and a card reader from establishing proper communication. Card should be tested for ISO/IEC 14443 compliance. ISO/IEC 14443-4, paragraph 7.2, includes an optional provision of the ISO/IEC standard that covers wait time between sent and received data packets. If cards/readers don't implement this option, it may cause a time-out issue and prevent the card from establishing communication with the reader.

Corrective Action: See Appendix A for second level troubleshooting assistance. Contact the system supplier and provide diagnostic details for factory assistance and possible availability of updates. The card may need further analysis by the card issuer.

2.3. FIPS 201 optional data objects

Readers or other relying party system components may not recognize the data model from the presented card because optional data objects are present or because they are not present. This may be caused by variations in the number of optional data objects selected and used by different issuers. A recent example of this was discovered in the PIV Printed Information container (0x3001) for the tag 03 "Employee Affiliation." In this optional data object, the data element, tag 03, was missing from some cards while two optional data elements, Organizational

[5] Information on test cards available from NIST is available at http://www.nist.gov/srd/nistsd33.cfm.

Affiliation (line one) and Organizational Affiliation (line two), were added. This caused some readers and systems to reject the card as non-conforming.

Use or non-use of optional data objects and data elements may impact interoperability. This situation is more likely to be encountered when a card from another agency or issuer is presented since different policies for optional features, or different interpretations for implementing optional (or even standard) features can exist.

Corrective Action: See Appendix A 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 may 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 of 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 PIV 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 PIV identifier. Reconfigure or update as required.

Some PACS control panels may need to remain configured as “card only” readers even when a PIV card and PIN reader is installed in the field. This is because the PIV card PIN is match-to-card, not match-to-host.

See Appendix A 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 have the current configuration and firmware version. The card works at some access control points, but not all.

In this case, all PACS control panels may not be the same configuration or have 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 PIV identifier. Update as required.

See Appendix A 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 PIV identifier (FASC-N)

PACS controllers may be unable to process the PIV identifier (Federal Agency Smart Card Number (FASC-N)). Using abbreviated identifiers may lead to collisions (i.e., duplicate numbers) in the PACS user database. This can be the result of the reader configuration, the PACS configuration, or both.

Corrective Action: Review SP 800-116[6] for guidance regarding options for bit length and format of the unique identifier. 48 bits is sufficient to support the first three fields of the FASC-N in accordance with SP 800-73. Some PACS cannot handle this bit length. If planning for the future, consideration should be given to the Universally Unique Identifier (UUID) in the Global Unique ID (GUID) field which is 128 bits. Contact manufacturer to discuss possible solution.

4. PACS Card Registration Issues

Symptom: The PIV card cannot be registered 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 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 may have encoded the credential number incorrectly which would then prevent PACS registration. PACS registration may include reading and matching biometrics and storing certificates. Encoding issues are not limited to just the unique identifier associated with the card or cardholder.

Corrective Action: See Appendix A 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 PIV identifier (FASC-N)

The PACS may be unable to process the PIV 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.

[6] http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

Publication Acknowledgements

This guidance document was developed by the Smart Card Alliance Access Control Council and Identity Council to help users diagnose the cause of the PIV card/reader issues with physical access control systems and provide troubleshooting guidance to quickly identify corrective actions.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks the Council members for their contributions. Participants involved in the development of this 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; Identive; IDmachines; IQ Devices; NASA; NXP Semiconductors; Oberthur Technologies; Quantum Secure Inc.; RM Industries; Roehr Consulting; SafeNet, Inc.; SAIC; 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**, Identive, who managed the project, recruited participation and contributed content.

The Smart Card Alliance thanks the following Council members who contributed to writing and/or reviewing this guidance document:

- **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
- **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
- **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**, Datacard Group
- **Mike Kelley**, Secure Mission Systems
- **Russ Kent**, HP Enterprise Services
- **Harold Kocken**, Deloitte & Touche LLP
- **Kevin Kozlowski**, XTec, Inc.
- **Lolie Kull**, HP Enterprise Services
- **LaChelle LeVan**, Independent
- **Michael Lewis**, Dept. of Defense
- **Gilles Lisimaque**, ID Technology Partners
- **Diana Loughner**, IDenticard
- **Stafford Mahfouz**, Tyco Software House
- **Brad McGoran**, Exponent
- **Cathy Medich**, Smart Card Alliance
- **Bob Merkert**, RM Industries
- **Mike Mostow**, AMAG Technology
- **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
- **Gurpreet Manes**, SafeNet
- **Dan Schleifer**, IDmachines
- **Adam Shane**, AMAG Technology
- **Mark Steffler**, Quantum Secure
- **Mike Sulak**, Dept. of State
- **Lars Suneborn**, Identive
- **Rick Uhrig**, XTec, Inc.
- **Chris Williams**, SAIC
- **William Windsor**, GSA
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, ID Technology Partners

About the Smart Card Alliance Access Control Council

The Smart Card Alliance Access Control Council is focused on accelerating the widespread acceptance, use, and application of smart card technology for physical and logical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the access control community and that will help expand smart card technology adoption in this important market.

About the Smart Card Alliance Identity Council

The Identity Council is focused on promoting best policies and practices concerning person and machine identity, including strong authentication and the appropriate authorization across different use cases. Through its activities the Council encourages the use of digital identities that provide strong authentication across assurance environments through smart credentials – e.g., smart ID cards, mobile devices, enhanced driver's licenses, and other tokens. The Council furthermore encourages the use of smart credentials, secure network protocols and cryptographic standards in support of digital identities and strong authentication on the Internet.

The Council addresses the challenges of securing identity and develops guidance for organizations so that they can realize the benefits that secure identity delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

Additional information on the use of smart card technology for identity and access control applications can be found on the Smart Card Alliance web site at http://www.smartcardalliance.org.

Appendix A: Basic Troubleshooting

Level One Troubleshooting

No additional 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 known good transparent contactless interface reader 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" refers to a PIV card that has previously been authenticated (using the GENERAL AUTHENTICATE APDU), whose PIV authentication certificate is not revoked by the PIV card issuer, and that has been 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 PIV card from the electronically opaque sleeve 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?

This test is applicable to PIV cards and readers that do not incorporate other RF technologies. 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 if the card has both a 125 KHz chip and a 13.56 MHz smart card interface. In the case of a dual-frequency card tested on a dual-frequency reader, the diagnostic method described in level two troubleshooting below should be used.

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

Present a card to the reader and observe the reader indicator light. 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, the reader detects the presence of the card. This indicates that the card transmits data to the reader.

Does the reader visual or audible indicator change?

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 thumb. Move the card to the surface of the reader and put light pressure on the ICC. This is one way to test for a broken antenna bond, as the pressure may reestablish a connection temporarily.

Does the reader visual or audible indicator change?

Answer: Yes. This indicates that the card is defective. Replace the card..

Answer: No. 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.** 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. Contact the card issuer immediately as problems often occur in batches and the problem may already be known.
>
> **Answer: No.** The tests produce correct results. 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.

Level Two Troubleshooting: Card and Reader Data Operation

Level two tests require some basic skills and the ability to use simple diagnostic tools. Diagnostic tools are now commercially available. Contact the PACS manufacturer, card manufacturer, or systems integrator/installer 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 the card version, expiration date, and other data objects.[7] Figure 2 shows a generic example of a diagnostic viewer displaying a successful card read.

Figure 2. Successful Read of PIV Card

Figure 3 shows a generic example of an unsuccessful attempt to read the card.

[7] The TWIC program implemented the PIV applet and all of its optional features and performed a thorough pilot. The diagnostic tools produced by participants of the TWIC reader pilot are able to test all of the containers in the PIV data model, including those that are optional. This is in part because the TWIC pilot test required comprehensive error or diagnostic codes to be available.

Figure 3. Unsuccessful Attempt to Read the PIV Card - AID Error

Diagnostic tools may require a known good card, a contact and contactless reader, a method to display the transmitted data, and an extra reader of the same brand and type as those installed on-site. In addition, it is advantageous to have several known good cards of different versions and from different manufacturers and an additional reader of the latest version and firmware (if the installed readers are of an earlier vintage).

The diagnostic tool display may be a diagnostic feature in a PACS application or an application provided by a card manufacturer or other provider.

This section outlines several general tests that can be performed with the diagnostic tools described above. 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. 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 1.2.4). 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.

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. 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 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.

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 PIV 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.[8]

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.

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?

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

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.

Level Two Troubleshooting: PACS Registration Issues

This test is intended to troubleshoot a problem when the PACS will not register the PIV 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) 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 PIV 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.

Escalation

It is important to contact the organizations that provide maintenance and support for the PIV card or for the PACS. This organization will have an escalation procedure for contacting suppliers or integrators to resolve issues. An escalation procedure will likely be required when one or more of the predefined FIPS 201 or other options are introduced as these options often cause interoperability issues. 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 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.

Appendix B: Technical Details

For card presentation to be successful, it is essential to ensure that the RF 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 technology cards. Although a PIV card should comply with the ISO/IEC 14443 standard, NIST FIPS 140-2 validation imposes 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. The card also stays powered in the smart card reader throughout the day.

However, when cards are used in a PACS, this NIST requirement has a major impact on timing and on power consumption.

Timing Impact

Because all supported cryptographic algorithms must be tested, regardless of whether they are going to be used in the current session, a PIV card must run tests on numerous algorithms (e.g., 3DES, AES, RSA, ECC, SHA1, SHA2, 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 PACS authentication 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.

Appendix C: Acquisition of Approved Products and Services for Implementation of HSPD-12 (OMB 06-18)

HSPD-12 requires that Federal identity management, credentialing systems and tokens be interoperable across all departments and agencies for logical and physical access controls. The General Services Administration (GSA), a Federal acquisition vehicle, management and policy service provider, was designated by OMB as the "executive agency for Government-wide acquisitions of information technology for HSPD-12."

With the OMB authority, GSA established the FIPS 201 and HSPD-12 Evaluation Programs to approve vendor products and services. GSA's Office of Government-wide Policy (OGP) created and maintains the FIPS 201 Evaluation Program Approved Products List (APL), while the Federal Acquisition Service (FAS) created and maintains the HSPD-12 vendor qualifications for service and product integration.

GSA makes approved products and services available through acquisition vehicles that are available to all agencies.

GSA has established Special Item Number (SIN) 132-62 on information technology (IT) schedule 70 for the acquisition of approved HSPD-12 implementation products and services. Below is a list of categories of services and products as established for SIN 132-62.. For the purpose of this document, item 5, PIV integration services and products; item 6, logical access control and physical access control services and products; and item 7, approved FIPS 201 services and products are relevant.

1. PIV enrollment and registration services and products
2. PIV system infrastructure services and products
3. PIV card production services and products
4. PIV card activation and finalization services and products
5. PIV integration services and products
6. Logical access control and physical access control services and products
7. Approved FIPS 201 services and products
8. Other professional services

All products and services offered on SIN 132-62 have been evaluated and qualified to be in compliance with government-wide requirements. Agencies may acquire individual product items, deployment services, or complete contractor-managed services for any of the HSPD-12 categories or may acquire bundled, integrated solutions.

A list of HSPD-12 qualified system providers is available at: http://www.idmanagement.gov/pages.cfm/page/IDManagement-qualified-HSPD12-service-providers. Note: a qualified vendor may have a SIN 132-62 certification without providing products on GSA schedules.

In addition, HSPD-12 products and services are offered for agency acquisition via the GSA Schedule 70 and Schedule 84 contracts. Schedule 70 is a general purpose contract for information technology equipment, software and services. In addition, integrated electronic physical access control systems, including planning, design, installation, monitoring and service, as well as products, are found on Schedule 84.

Schedule 84 is GSA's contract for law enforcement, security, facilities management, fire, rescue, clothing, marine craft and emergency/disaster response. The follow is a partial list of Schedule 84 products and services:

- Security systems integration and design services
- Security management and support services
- Security system life cycle support
- Alarm and signal systems, facility management systems, professional security/facility management services and guard services
- Fire alarm systems (excludes fire suppression devices)
- Access control systems, door entry control by card access, magnetic proximity – including but not limited to biometric
- Access control systems, door entry control by touch access, dial, digital, keyboard, keypad – including but not limited to biometric, voice, fingerprint, iris, hand geometry, weight
- Access control systems, parking access control – including but not limited to biometric
- Access control systems, emergency exit door access/alarm systems for security and/or fire safety – including but not limited to biometric
- Access control systems – vehicle arrest/security barrier/barricade/bollard systems, decorative barrier planters
- Other access control systems – including but not limited to biometric access control – e.g., facial, voice, fingerprint, iris recognition
- Intrusion alarms and signal systems – including audible and visible warning devices (no personal alarms)
- Perimeter security/detection systems – including but not limited to fencing, sensors

Schedule 70 is GSA's contract for general purpose commercial information technology equipment, software and services. The follow is a partial list of Schedule 70 products and services:

- Introduction of new information technology services and/or products
- Electronic credentials, not identity proofed (Assurance Level 1, OMB M-04-04[9])
- Identity proofed (Assurance Level 2, OMB M-04-04)
- Digital certificates, including ACES (Assurance Level 3 and 4, OMB M-04-04)
- E-authentication hardware tokens
- Remote identity and access managed service offering

[9] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf