Smart Card Alliance

FIPS 201 PIV II Card Use with Physical Access Control Systems: Recommendations to Optimize Transaction Time and User Experience

May 2007

Developed by:
Smart Card Alliance Physical Access Council

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.

The Physical Access Council is focused on accelerating the widespread acceptance, usage, and application of smart card technology for physical 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 physical access industry and that will address key issues that end user organizations have in deploying new physical access system technology.

The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software and reader vendors; physical access control systems vendors; and integration service providers. Physical Access Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

Additional information about the use of smart cards for secure identity applications can be found at http://www.smartcardalliance.org.

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.

FIPS 201 PIV II Card Use with Physical Access Control Systems: Recommendations to Optimize Transaction Time and User Experience

FIPS 201-1 PIV II end-point smart cards provide enhanced interoperability and unify identity verification for use in both logical and physical access control. Users need to understand why there is a difference in the system behavior when using PIV smart card technology vs. the typical proximity cards and readers in wide use today. It is important for government agencies to obtain the best possible user experience from the new PIV II card-enabled physical access control systems (PACS). Listed below are a number of factors that impact transaction performance in PACS applications.

First, some operational differences between the two technologies can impact the user experience. For example, the new PIV smart card is a departure from the low frequency proximity cards in use today. Agencies and installers must be aware of, and prepare for, operational differences between these technologies. The PIV card contains an order of magnitude more information than the proximity card and there are cryptographic processing requirements. This translates into an increase in the time that the card must remain near the reader. The transaction time between presenting a proximity card to actually unlocking the door is typically around one second. The best-case scenario for a PIV card is about two seconds, with some observed at four seconds. Clearly this will impact throughput at agency portals. Furthermore, those used to the “wave and go” nature of a proximity card will need to be trained to “touch and hold” the PIV card due to the shorter read range and increased processing times. All of the above factors should be considered during installation and be a part of the end user training when implementing a PIV card-enabled PACS. User training is discussed in detail in Appendix A.

Second, transaction performance in PACS applications is related to variances in the production of the PIV card and readers, such as data encoding, manufacturing, and architecture. For example, testing by some Smart Card Alliance members has shown that the order in which the data is encoded on the PIV card can have a significant effect on the transaction time for a PACS reader to obtain and process the information from a PIV card. If the personalization systems used to encode the PIV cards use the methods detailed in Appendix B, this transaction time could be significantly enhanced at no additional cost.

A third factor is that cards may not all comply with the international standard required by the PIV specification for contactless smart card antenna frequency tuning. Antenna tuning is not part of the current test suite being performed by either GSA or NIST. This yields reduced read range. The result is that users may need to make a number of card presentations to the reader before they learn the optimal way of presenting the card. End user training (as described in Appendix A) should include instruction in the proper way to present the PIV card to a reader.

Finally, the RF field emitted from the reader to power and communicate with the card is different between models of readers. Readers must be built to fit different locations like doorframes or hardened enclosures for exterior uses. Different mounting surfaces affect the read range by absorbing or reflecting the RF energy from the reader in different and unpredictable ways. Agencies need to be aware of this when installing PACS readers and train end users in the proper use of the PIV card. Appendix C provides guidance on installation best practices.

Any of these factors can affect the transaction time and user experience when using the new PIV II cards in a PACS. As described in this document, many of these factors can be mitigated through minor changes at little or no cost, and with no impact on the NIST standards. In addition, user training can help to set user expectations for the performance of the new PIV II cards when used in PACS.

This white paper was developed by the Smart Card Alliance Physical Access Council to assist government agencies with the use of FIPS 201 PIV II end point smart cards in physical access control systems. The Physical Access Council plans to develop on-going updates to these implementation recommendations to address other issues that affect the performance of PIV II cards in PACS implementations.

Appendix A: PIV Card User Briefing – PACS Usage

Background

During the past few months, PIV cards have been issued to employees of numerous Federal agencies. In instances where the PIV card is registered and used with a physical access control system (PACS) as an access credential, the user experience is different from that of previous generation access credentials.

Card-to-reader transactions using legacy cards were very basic. The reader simply read an encoded number from the presented card and sent the number to the PACS controller. The encoded number usually represents a small amount of data and requires no, or minimal, processing before the reader transmits the captured data to the controller for authorization.

For decades, PACS card and reader manufacturers have cooperated to increase the efficiency of the card-to-reader data capture as well as the reader transmit processes. Today, regardless of card technology, physical access transactions, measured in less than one second, are almost negligible to the everyday user.

With the introduction of the PIV card, the processing required to read and capture required data and format and transmit a GSA-compliant message to the PACS controller is significantly more complex and takes more time. Transaction times vary between cards, readers and reader-card combinations, but generally are in the two to four second range. This change in reader behavior is significant enough to give an uninformed user an impression that something is wrong and frequently results in frustration and a conclusion that "the card does not work."

This simply illustrates the necessity to manage cardholder expectations. The best approach to avoid this frustration is to inform the card recipient to expect a performance difference when using the new PIV card.

What Are the Differences?

Different card technologies have different operational processes. Since the most common type of PIV application is likely to be contactless data transfer and, according to the Security Industry Association (SIA), the most common legacy technology is the 125KHz proximity card and reader, this document focuses on contactless technology.

For the purpose of this topic, there are four differences which combine to result in a longer wait before the system receives a message from the PIV reader. Differences can be segmented into four areas:

1. Read range. Both the 125 KHz proximity and the PIV contactless cards transmit data only when they are close to the reader and "energized" by the reader's RF field. Read range is one important factor to the perception of card and reader performance.

   - 125 KHz: The 125 KHz reader starts receiving card data earlier (i.e., from a longer distance), even before the user has stopped moving the card toward the reader. This gives the impression of a quicker read than what is actually the case.
   - PIV card: A PIV reader has, for privacy reasons, a very short read range. The card is not "energized" until very close to the reader surface. This gives the impression of a slow read process.

     The short read range for the PIV card also makes orientation and position relative to the reader face critical. Holding the PIV card the "wrong" way, or in the "wrong area," greatly affects read performance. A cardholder can significantly improve the read time by learning how to properly present the card to the reader.

2. Card data access.

   - 125 KHz: The 125 KHz card contains only one, short dataset, which is very quick for the reader to access and capture.

- PIV card: The PIV card contains a large number of datasets. The reader must search, identify and select the correct set. The result is a longer read time.

3. Card data format

   - 125 KHz: No formatting is required. The reader sends data as read from card.
   - PIV card: The reader must format the message using data read from PIV card. The result is a longer processing time.

4. Transmission

   - 125 KHz: 125 KHz cards use a short 4-byte message. The message is very quick to send.
   - PIV card: The PIV GSA-formatted data stream is over 3000 bytes. The result is a longer send time.

Recommendations

A short training session conducted by PACS operators will reduce the confusion of a new cardholder when using the new PIV card at an access control point. The instruction should ideally be conducted as the PIV cards are having physical access privileges registered in the local PACS. The instruction can be a two-part program -- verbal and practical. For practical instruction, user practice requires the installation of a PIV reader in the PACS enrollment office. The reader should be within easy reach of both the PACS enrollment operator and the cardholder. As physical access privileges are registered for the card, the cardholder can be guided by the enrollment officer in the proper card presentation procedure. The cardholder can also be briefed on the system responses.

Verbal Training

- A brief explanation of the above four points
- A brief explanation of system responses (e.g., light indicator, audible signals)

Practical Demonstration

- The PACS enrollment officer demonstrates how to properly present the PIV card to the reader. The officer points out the read and processing time before access grant responses appear.
- The cardholder repeats the process. When needed, the enrollment officer provides guidance.
- Improper procedures (e.g., card orientation, location) can and should be practiced as well. This provides the cardholder with some experience with the lack of system response due to incorrect card presentation.

These simple steps will add a few minutes to the PACS registration procedure. However, agency and department PIV cardholders are more likely to be positive and accept the new cards and readers if they understand why and how the user experience is changing.

Appendix B: Data Encoding

The response time for an ISO/IEC 14443 smart card reader to read a secure smart card is very quick -- typically less than ¼ second (250 ms). The response time for a FIPS 201 GSA-certified smart card reader to read a PIV II end-point card could be more than four times (4X) that amount. The additional time required to read a PIV II card is due to the additional encryption and security protocols defined in FIPS 140-2 and mandated in FIPS 201 for PIV II end-point cards, as well as to the way the data are encoded. This appendix recommends certain changes to data encoding that will improve the performance of the PIV card with the PACS.

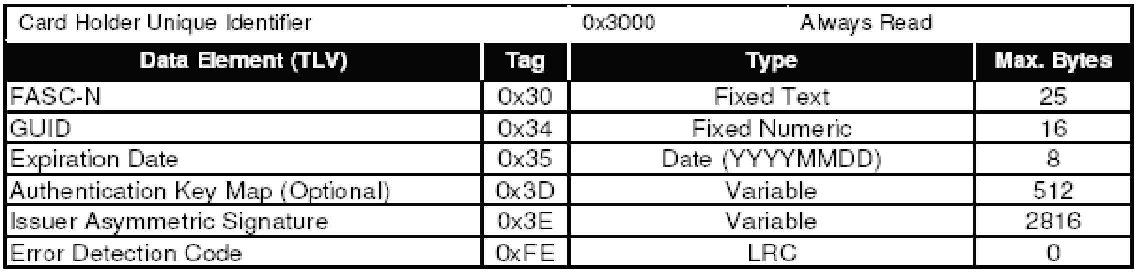
1. Data Access

An important gating factor in the PIV card PACS transaction time is the time it takes to retrieve the data needed to uniquely identity a cardholder. Based on the GSA recommendation, the CHUID container (ID 0x3000) must be read and the FASC-N (TAG 0x30 – 25 bytes) and the Expiration Date (TAG 0x35 – 8 bytes) must be retrieved. (It should be noted that PIV end-state cards do not use container IDs but only the TAGs (5FC102 for the CHUID).)

There are two ways to optimize this time.

- The first method consists of leveraging ISO/IEC 7816-4 and makes use of parameter 5C of the Get Data function that allows the direct accessing of a specific TAG. Unfortunately, there is no provision in SP 800-73-1 to support this option and it will require a special publication change. Moreover, it could create backward compatibility issues in the field if it gets added at a later stage.
- The second option, which is more straightforward and doesn't require a special publication change, consists of sorting the TAGs in an ascending order within the CHUID container. This operation typically takes place at the point of issuance and is managed by the card middleware.

  As an example, if the TAGs are arranged in a descending order, the reader will have to read all other TAGs (up to 3328 bytes[1]) before getting to the useful information. Assuming a transmission speed of 106 Kbps, the transaction time alone (without the overhead of command processing and other functions) will be about 250 ms. However, if the TAGs are arranged in ascending order, the reader will only need to read the first 49 bytes[2] (roughly 3 ms).



Card Holder Unique Identifier		0x3000	Always Read
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
FASC-N	0x30	Fixed Text	25
GUID	0x34	Fixed Numeric	16
Expiration Date	0x35	Date (YYYYMMDD)	8
Authentication Key Map (Optional)	0x3D	Variable	512
Issuer Asymmetric Signature	0x3E	Variable	2816
Error Detection Code	0xFE	LRC	0

[1] TAG 0x3E + TAG 0x3D = 2816 + 512 = 3328

[2] TAG 0x30 + TAG 0x34 + TAG 0x35 = 25 + 16 + 8 = 49

2. **Anti-collision and Select Sequence**

   The anti-collision and select sequence slows transaction time. By having a default application automatically selected at power-up, transaction time can be significantly reduced. This is supported in the SP 800-73 documentation (see excerpt below).

   > ***3.4.2 Default Selected Card Application***
   >
   > *The card platform shall support a default selected card application. In other words, there shall be a currently selected application immediately after a cold or warm reset. This card application is the default selected card application.*

3. **Processor Start-up Routine**

   Initial ISO communications with the credential are handled by the operating system without a full processor power-up; however, the transmission of the Get Data command initiates the full processor power-up sequence. The power-up time to respond to the request has been measured on the currently available test cards at <500 ms. (During this period, multiple frame waiting time (FWT) commands are sent by the credential and must be acknowledged by the reader. Each FWT has a possible maximum value of approximately 5 seconds. If the credential needs additional time after each FWT, then a waiting time extension (WTX) is sent and processed.) A processor quick start-up routine for contactless communications would eliminate this delay. The maximum allowable delay is documented in ISO/IEC 14443-4.

4. **Encryption and Security**

   FIPS 140-2 adds very stringent security requirements that slow down the initialization phase of the PIV smart card after power-on. This initialization can take more than several hundred milliseconds (for initialization of all cryptographic functions). The CHUID container (free read) is the only information accessible through the contactless interface of a FIPS 201 PIV card. Since reading the CHUID doesn’t involve cryptography, it would be wise to modify the standard and remove the requirement for FIPS 140-2 cryptographic initialization in the contactless mode.

In summary, this document lists several factors that could slow transaction time using a PIV card with a PACS. It also makes recommendations as to how to address each factor to optimize performance. It is important to remember that for legacy PACS, the access decision remains in the panel. Any additional manipulation of the received credential data, database lookup, and access rights comparison that take place within the PACS will cause some delay before a door release is granted. It can be difficult for the agency user to define where the delay is occurring, at the reader or at the panel.

Appendix C: Reader Installation Impact on Performance

Readers are installed at access control points and are subjected to a wide range of environments. Card read range and performance are significantly impacted by the environment; transaction time may vary from one to several seconds. It is safe to say that each control point has unique operational parameters. It is difficult, if not impossible, for reader manufacturers to predict and anticipate these parameters.

As an example, the same 13.56 MHz contactless reader will behave differently when installed on a hallway drywall than when moved to a metallic door frame, near a metal conduit, near a metallic wall stud inside the wall, near an exit reader located on the opposite side of the wall, or on a metal post at an exterior entry control point. The varied density of these materials affects the RF fields and wave pattern (backscatter) at the reader itself. Each of these few examples represents a unique RF environment, which in turn affects reader performance and, ultimately, the user's experience with this new technology.

Manufacturers and installers can take a few steps to minimize (but not eliminate) these unpredictable variables. One step is to increase control of the reader RF environment. This can be achieved with a few additional steps:

- Providing specifically-designed reader mounting hardware that minimizes the effect of such interference (such as spacers).
- Providing additional installer training and following without deviation, manufacturers' installation instructions.
- Using only mounting hardware supplied by the reader manufacturer.
- Using only cables specified by the reader manufacturer.
- When mounting the reader on metal, drilling the cable access hole just slightly larger then the cable diameter. Big holes drilled in the metal mounting surface can act as closed loops and absorb the RF energy, thus reducing the reading distance.
- Protecting the cable from sharp edges and any damage from chafing
- Preparing the end of the cable by cutting it back to expose the wires, with each end twisted to eliminate any loose or frayed wires. After connecting to the reader, twist the cable conductors a few times to twine the wire ends to avoid differential mode interference on the data lines.
- Keeping wires at the reader connector as short as possible: long, unshielded connections will reduce the sensitivity of the reader.
- Making available an installation test card. This will allow the installer to simply move the reader to the most favorable wall location before permanently mounting it on the wall.

PACS owners and managers can also take steps to improve the user experience for PIV cardholders. Since PIV readers may not react as quickly or in the same way as proximity card readers, user training and education are very important. Simply waving the card past a reader may need to change to touching the reader and holding the card still for the access grant. Appendix A includes additional detail about recommended user training.

Although not complete, these simple steps will greatly reduce the variables and improve the consistency of reader performance.

Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council to assist government agencies with the use of FIPS 201 PIV II end point smart cards in physical access control systems. 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 wishes to thank the Physical Access Council members for their contributions. Special thanks go to the individuals who participated in the project to write, review and edit this paper and to Dwayne Pfeiffer who managed this project.

John Attala, Infogard
Tim Baldridge, NASA
Consuelo Bangs, Sagem/Morpho
Nathan Cummings, HID Corporation
Sal D'Agostino, CoreStreet
Tony Damalas, Diebold Actcom
Dave Engberg, CoreStreet
Bob Fee, LEGIC Identsystems
Bob Gilson, Dept. of Defense/DMDC
Christophe Goyet, Oberthur Card Systems
Walter Hamilton, IDTP
Steve Hopper, Infogard
Steve Howard, Thales e-Security
Michael Kelley, BearingPoint
Lolie Kull, EDS
Gilles Lisimaque, IDTP
Don Malloy, Innovative Card Technologies
Cathy Medich, Smart Card Alliance
Bob Merkert, SCM Microsystems
Dwayne Pfeiffer, Northrop Grumman
Corey Ramey, Tennessee Valley Authority
J.C. Raynon, SCM Microsystems
Roger Roehr, Tyco Fire & Security
Steve Rogers, Integrated Engineering
Paul Russell, Lenel
John Santisteban, Fargo Electronics
Adam Shane, AMAG Technology
John Spongr, BQT Solutions
Jim St. Pierre, MDI
Mike Sulak, Dept. of State
Lars Suneborn, Hirsch Electronics
Beth Thomas, Honeywell
Mark Visbal, Security Industry Association
Steve Weymann, Infogard
Eric Widlitz, HID Corporation
Rob Zivney, Hirsch Electronics