

Guide for Assessing Personal Identity Verification Card Systems

Edward W. Busch

Craven Community College

SEC 170

Dr. Bruce Waugh

April 2012

Overview

This paper serves as a primer for anyone preparing to perform a security/reliability assessment of a Personal Identity Verification (PIV) Card Issuer (PCI) Facility. First, a summary of Homeland Security Presidential Directive 12 (HSPD 12) provides the objectives behind the implementation of PCI Facilities throughout Government Agencies. This is followed by a brief review of the document that establishes the architectural and technical standards for PCI Facilities. Then, the publication that provides the detailed guidelines for performing an assessment is reviewed. I will follow up by providing information learned during the preparation and performance of actual assessments to show the reader what to expect and how to become more efficient in the process of gathering assessment data.

Homeland Security Presidential Directive 12

President George W. Bush signed Homeland Security Presidential Directive 12 (HSPD 12) on August 27, 2004. HSPD 12 (*Policy for a Common Identification Standard for Federal Employees and Contractors*) was the culmination of efforts, following the terrorist attack of September 11, 2001, to develop a common identification (credential) standard that ensures that people are who they say they are, so government facilities and sensitive information stored in federal networks can be protected. HSPD-12 requires federal agencies to issue “smart card” credentials to their employees and contractors. These credentials are commonly known as Personal Identity Verification (PIV) cards. PIV Card Issuers (PCIs) are the entities that issue these cards. Paragraph 3 of HSPD 12 stipulates four basic objectives to assure “secure and reliable identification of an individual.” These objectives, when met, provide a form of identity

that “(a) is issued based on sound criteria for verifying an individual employee’s identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued by providers whose reliability has been established by an official accreditation process.” Providers, in this paper, are referred to as PCIs (PIV Card Issuers) or PCI Facilities.

In addition, HSPD 12 stipulates that its requirements, “...be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.” The Privacy Act, in summary, protects the Personally Identifiable Information (PII) of all Americans. NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* is a good source for learning how to identify and protect PII. PII, in short, is any collection of information that traces back to one specific individual. A good example of PII is the combination of a person’s name, date of birth, address and Social Security Number. Since collection of this type of information (and more) is a major ingredient in the issuance of a PIV card, it is easy to understand why the security and reliability of PCI Facilities must be highly scrutinized.

HSPD 12 and NIST

HSPD 12 directed the Department of Commerce to develop a, “Federal standard for secure and reliable forms of identification.” In response, and as directed by the Secretary of Commerce, the National Institute of Standards and Technology (NIST) Computer Security Division initiated a new program for improving the identification and authentication of federal employees and contractors for access to federal facilities and information systems by developing two new documents. The first is the Federal Information Processing Standard (FIPS) 201-1, entitled

Guide for Assessing Personal Identity Verification Card Systems 4

Personal Identity Verification (PIV) of Federal Employees and Contractors. This standard defines the architectural and technical requirements to produce a common identity credential that meets the first three objectives of HSPD 12, described above.

FIPS 201-1, Appendix B, specifies that NIST “...establish a government-wide program to accredit official issuers of PIV Cards...” This addresses the fourth basic objective of HSPD 12 – that a credential, “is issued only by providers whose reliability has been established by an official accreditation process.” To satisfy this requirement, NIST developed SP 800-79-1, entitled *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*. This publication established, “...detailed criteria that PIV Card Issuers must meet for accreditation,” and a “...government-wide program to accredit official issuers of PIV Cards against these accreditation criteria.”

So briefly, FIPS 201-1 sets up the standards for building and implementing the PCI systems and SP 800-79-1 provides the guidelines for assessing the various controls that ensure conformance to the system standards set forth in FIPS 201-1. Accreditation of PCIs, through this common process, establishes the *reliability* of agency PCIs. Reliability must be unquestioned to establish trust in the issued credentials. Trust is pivotal in meeting the HSPD 12 objective of using PIV cards across agencies throughout the federal government. Trust between federal agencies may exist only if participating agencies use the same, repeatable assessment methodology provided by SP 800-79-1.

Many other NIST documents support FIPS 201-1 and SP 800-79-1. These documents are identified, as required, during the discussion.

Federal Information Processing Standard (FIPS) 201-1

The assessor must become thoroughly familiar with FIPS 201-1 before developing and/or executing a PCI Facility assessment plan. Without knowing the standards involved, an objective and accurate assessment is not possible. A good approach involves first reading and understanding FIPS 201-1 - then moving on to SP 800-79-1. These documents (as are most documents referenced in this paper) are available at NIST's website - <http://csrc.nist.gov/publications/PubsSPs.html>. FIPS 201-1 is divided into two parts, Part 1 (PIV-I) and Part 2 (PIV-II).

Part 1 contains the controls and processes necessary to assure that the information contained on a PIV card reflects that the cardholder's identity has been thoroughly verified and that the required clearance(s) has/have been obtained or initiated prior to releasing the card to an individual. This "identity proofing" process ensures that each PIV card applicant is who they say they are. Additionally, Part I details the PIV privacy standards which address the requirement of HSPD 12 to protect personal privacy. There is a wealth of Personally Identifiable Information contained within the electronic chip on every PIV card issued. Agencies are bound by many laws, directives, policies and regulations to protect this information during its collection, handling and storage.

Part 2 deals with technical specifications of the PIV system's components and processes. These standards are required to ensure interoperability and uniformity of PIV card credentials that are issued and used across Federal government agencies as a common form of identification.

A thorough knowledge of FIPS 201-1 makes the controls and processes used during the PCI assessment much easier to understand.

Special Publication 800-79-1

SP 800-79-1 contains the suggested assessment and accreditation methodology for verifying that issuers of PIV credentials and cards (PCI Facilities) conform to the standards and implementation directives (most notably, FIPS 201-1) developed under HSPD-12. In Appendix G, it details the controls derived from the FIPS 201-1 standard (and other relevant documents) and the procedures used for assuring the controls are in place.

Although not covered in this paper, SP 800-79-1 also provides post-assessment guidance for evaluating the results (findings) of an assessment and for making a decision on whether or not to accredit the PCI. The Designated Accreditation Authority (DAA) makes the accreditation decision. The DAA is an appointed official of an organization that has the ultimate responsibility of implementing system security. The DAA can take one of three actions following an assessment evaluation:

- Issue an Authority to Operate (ATO) – Allows the PCI to operate for a period of three years before a re-accreditation is required (earlier if there is a significant change in personnel, systems and/or operating procedures at the PCI).
- Issue an Interim Authority to Operate (IATO) – Allows the PCI to operate for a maximum period of three months. This is normally done when the deficiencies can be corrected in a reasonable period and there are no major risks involved. The DAA may place limitations on the operation of the PCI Facility and a Plan of Action & Milestones

Guide for Assessing Personal Identity Verification Card Systems 7

(POA&M) must be developed to identify and remediate the deficiencies. The IATO is replaced with an ATO when the deficiencies are corrected.

- Issue a Denial of Authorization to Operate (DATO) – This action requires that the PCI be shut down if is currently in operation. If not in operation, it may not start. As with the IATO, a POA&M is developed to identify and remediate the deficiencies. The DAA will repeat the assessment evaluation after the deficiencies are corrected.

PCI Controls

PCI controls are the safeguards used to avoid, counteract or minimize the security and reliability risks associated with the PIV card issuance process. In Appendix G, the PCI controls are organized into four *PCI Accreditation Topics* (PATs). These are:

- **Organizational Preparedness:** Controls that cover the physical environment of the PCI Facility and how it will be managed and operated.
- **Security Management & Data Protection:** Operational and technical controls that are in place to protect the Personally Identifiable Information of PIV cardholders, from the PIV card request, through issuance of the credential.
- **Infrastructure Elements:** Controls that span the activities required to procure, deploy, and maintain the PCI system components (PIV Card Stock, PIV Card Printers, etc.).

Guide for Assessing Personal Identity Verification Card Systems 8

- Processes:** These controls examine the processes and functions involved in issuing a PIV card, starting with the PIV card request, through the issuance and maintenance of the credential.

Each PAT is further broken down into two or more *Accreditation Focus Areas*. Each Focus Area contains a set of *related* controls that will be checked during the assessment process. An example of a Focus Area is Card Activation & Issuance (AI). The AI controls address all of the procedures used to print and issue PIV cards to the cardholders and to verify that the cards meet FIPS 201-1 technical standards. Table 1 shows the four PATs and their respective Focus Areas. SP 800-79-1, Appendix G provides additional information on each of the Focus Areas.

PCI Accreditation Topic	Accreditation Focus Area
Organizational Preparedness	Preparation & Maintenance of Documentation (DO)
	Assignment of Roles & Responsibilities (RR)
	Facility & Personnel Readiness (FP)
Security Management & Data Protection	Protection of Stored & Transmitted Data (ST)
	Enforcement of Applicable Privacy Requirements (PR)
Infrastructure Elements	Deployed Products & Information Systems (DP)
	Implementation of Credential Infrastructures (CI)
Processes	Sponsorship Process (SP)
	Enrollment/Identity-Proofing Process (EI)
	Adjudication Process (AP)
	Card Production Process (CP)
	Card Activation & Issuance Process (AI)
	Maintenance Process (MP)

Table 1 – PCI Accreditation Topics and Focus Areas

Guide for Assessing Personal Identity Verification Card Systems 9

Each Accreditation Focus Area contains one or more related controls that must be satisfied in order for that area, within the PCI Facility, to be considered reliable. Table 2 shows the present number of controls per Focus Area. SP 800-79-1, Appendix G, details all of the controls and identifies the source document(s) necessitating each control.

PCI Accreditation Topic	Focus Area	# of Controls
Organizational Preparedness	DO	7
	RR	6
	FP	9
Security Management & Data Protection	ST	2
	PR	6
Infrastructure Elements	DP	3
	CI	6
Processes	SP	2
	EI	12
	AP	2
	CP	4
	AI	13
	MP	7

Table 2 – Focus Area Control Distribution

As indicated in the table, there are currently 79 controls that must be satisfied in order for the PCI Facility to be accredited as a secure and reliable system. Each control is examined in one or more ways to determine full compliance. Normally, there is a requirement that the control is documented in the facility’s SOPs, User Manuals, etc. Then, there is another requirement that the documented control is implemented and functioning as intended.

For example, look at control number EI-2 (SP 800-79-1, Appendix G) in the Enrollment/Identity Proofing Process Focus Area. There are determining statements for the control that must each be satisfied. The control states, “The PCI Facility requires the applicant to appear in-person at least once before the issuance of a PIV Card.” The assessment guidance provided for the control

Guide for Assessing Personal Identity Verification Card Systems 10

requires it be determined that (1) *“the requirement that an applicant appear in-person at least once before the issuance of a PIV Card is documented”* and (2) *“the applicant appears in-person at least once before the issuance of a PIV Card.”* Both of these statements must be satisfied for the control to be fully compliant. To look at this another way, if each statement is converted into a question (e.g., *“Is the requirement that an applicant.....”* and *“Does the applicant.....”*), then the answer must be “yes” in response to both questions for control EI-2 to be fully compliant.

Using the determination statements provided in the control, the assessor first ensures that this control exists in the site’s DAA approved documentation. Then, during the PIV card Enrollment/Issuance process, the assessor must observe that an applicant does appear, in person, at least once.

The above example uses a common methodology used throughout the assessment process. That is, documentation must be in place to support the control and then, through interview, observation or testing actions, it is determined if the control is implemented as documented.

Appendix G of SP 800-79-1 contains all of the Focus Areas (partitioned by PAT) and their respective controls and assessment guidance for each. That is, each control is listed along with the criteria (determination statements) used to establish that the control has been satisfactorily implemented. There are 159 statements involved in assuring that all 79 controls are implemented and operating as intended. When developing your own PCI Facility assessment plan, with Appendix G as a guide, you may choose to combine determination statements or add granularity to them, thereby changing the total number of questions used for the assessment. However, you cannot *omit* statements, because such actions undermine the strength of the controls or cause

non-conformity to the standards set forth in FIPS 201-1. There are no restrictions on adding determination statements to *strengthen* a control. Additionally, a PCI Facility can add controls that strengthen system reliability or security. However, all of the seventy-nine controls currently contained in Appendix G *must* be implemented (and therefore be contained in the assessment plan).

This paper does not address the development of the plan used to perform a PCI Facility assessment. Probably the simplest method is to build a Microsoft Excel™ spreadsheet containing each of the controls broken down under their respective PCI Accreditation Topics and Accreditation Focus Areas. Under each AFA, add the determination statements (from SP 800-79-1, Appendix G) in the form of a question (an example is provided earlier in this paper). Provide a simple Yes/No or Satisfied/Not Satisfied column. Then, either print a hardcopy from which you can ask questions and make the appropriate entries – or use a laptop to enter the data directly as the assessment is performed. The latter method is preferred because using the sort feature you can look at the assessment data in a variety of ways when building your final report. Sections 3 and 4 of SP 800-79-1 provide detailed information to help one build a sound assessment plan.

Performing the PCI Facility Assessment

First Things First

Prior to performing an assessment of a PCI Facility, the external information systems (agency data centers, portals, etc.) used to process and store PIV card data collected by the facility must be secured. As stated in SP 800-79-1, “...before the organization official accredits the PCI and its facilities, all PCI information systems used must be accredited.” Assessment of the systems

external to the PCI Facility is covered under NIST Special Publications 800-37 (*Guide for Applying the Risk Management Framework to Federal Information Systems*), 800-53 (*Recommended Security Controls for Federal Information Systems and Organizations*) and 800-53A (*Guide for Assessing the Security Controls in Federal Information Systems and Organizations*). These documents address the security of the information and systems (in terms of confidentiality, integrity and availability) used to collect, process and store PIV card data. It is important to repeat that these (external) systems must be accredited (have an Authority to Operate) *before* accreditation of the PCI Facility can be granted. PCI Facilities are not permitted to operate without accreditation of the supporting IT infrastructure.

This means that no matter how reliable and secure the PCI Facility is, it cannot be made operational until the security (confidentiality, integrity and availability) of the supporting information systems have been accredited by the proper authority.

What is involved

As stated in SP 800-79-1, “An Assessor must– (i) compile evidence that the PCI controls employed in the PCI are implemented correctly, operating as intended, and producing the desired results; and (ii) present this evidence in a manner such that the DAA can make a credible, risk-based decision about the operation of the PCI.” Therefore, all of the controls for the PCI Facility will be evaluated and a report will be generated and submitted to the DAA. The DAA will use the information to make a decision on whether or not to grant accreditation. Note that the assessor just collects data and reports it – he or she is not directly involved in the accreditation decision. Read Section 4 of SP 800-79-1 (again) before your first site assessment.

Preparation

There is preliminary work you must accomplish to help the actual assessment process run more smoothly and to let the PCI Facility staff know that you are not the enemy. Building a rapport with site personnel before your arrival will pay huge dividends during your visit.

Initially, contact the PCI Manager and provide a brief overview of the assessment process and any preliminary work the site can accomplish to help the visit run more efficiently. Provide a copy of the assessment form(s) and any other helpful information to the manager as far in advance of the site visit as possible. Advise the manager that the assessment is based on the controls listed in NIST SP 800-79-1, Appendix G. Also, advise him or her that Appendix C (PCI Readiness Review Checklist), in the same publication, is an excellent tool to determine the readiness of the facility for the assessment. This allows the site to perform its own “self-assessment” prior to your arrival. Discuss additional information that includes the “who, what, where and when” aspects of the assessment. One last important note: Ask the PCI Manager to reserve a room large enough to accommodate all personnel taking part in the assessment.

Impress upon the manager that the availability of all essential documentation as well as access to key personnel in all PCI functional rolls are essential ingredients for a smooth-running, successful assessment. The most important personnel required for participation and a brief description of their roles are:

- **PCI Facility Manager** – This person is responsible for the overall operations of the PCI Facility. The Manager ensures that the PCI Facility is in conformance with the provisions contained in FIPS 201-1, SP 800-79-1 and all related documents.

- **Sponsor** – This person is the liaison between supervisors/managers and the PIV card applicant. The Sponsor ensures the applicant requires a PIV card and initiates the issuance process.
- **Registrar** – this person performs identity proofing of PIV card applicants, initiates the required background investigation, and records the results. The Registrar provides final approval for PIV card issuance to the Issuer.
- **Issuer** – This person performs the PIV card “build” operations and issues the card to the applicant. The Issuer also maintains records and controls for the PIV card stock used to issue the credentials.

On-Site Assessment Activities

The four basic activities used to perform the assessment are interviewing, reviewing, testing and observing. During the assessment process, at least one activity, up to a combination of all four, is required to assess the effectiveness of each PCI control.

Interviews and Documentation

The most efficient way to perform an assessment divides the effort into two halves. The first half takes place in a conference room/work area with a representative from each of the functional roles (Sponsor, Registrar and Issuer) and the PCI Facility Manager present. In addition, the site/agency Privacy Officer should be readily available. Approximately 30% of the questions asked to validate PCI controls involve interviews of PCI Facility personnel who play an active role the day-to-day management and operation of the facility.

All documents relating to the assessed controls should also be available in the conference room, along with the person(s) most familiar with the contents of each. Nearly 40% of the controls are document related. Standard Operating Procedures (SOPs), User Manuals/Guides, etc., play a major role in the operation of a PCI Facility and are required by SP 800-79-1. Provide a list of the required documents to the PCI Manager as part of the assessment preparation activities.

More than 70% of the assessment can be completed inside a conference room without ever having seen the PCI systems in operation. This includes looking at a representative PIV card issued by the agency. However, to accomplish this, *all of the appropriate personnel and documentation must be at the assessor's disposal.*

Testing and Observation

During the assessment process, it is important to ensure that the PCI Facility issue or reissue a PIV card, starting with the initial request, until actual issuance of the card to an individual takes place. Observe each step of the process to ensure that the controls required by SP 800-79-1 are satisfied. It is not enough to document that a 1:1 biometric match (e.g., fingerprint scan) be performed before releasing the card to the new cardholder - it must be verified through observation during the actual card issuance process. Approximately 30% of the controls being tested required testing and/or observation of the processes involved.

By observing the entire process, the assessor will be able to determine controls that, while documented, are not properly implemented. In addition, many of the controls, such as Physical Security, Emergency Lighting, etc., can only be accurately evaluated as the assessor completes the walk-through, from start to finish. Remember, all components of the PCI Facility must have the required controls implemented. For instance, the Registrar, Sponsor and Issuer workstations

Guide for Assessing Personal Identity Verification Card Systems 16

may be in different locations within the facility – but they must all have the Physical Security controls required by SP 800-79-1 in place.

The protection of Personally Identifiable Information (PII) is of critical importance in the PIV card issuance process. A substantial amount of PII is collected during the process, from the initial request, until the cardholder takes physical possession of the credential. Consider the type of personal information collected (name, DOB, SSN, etc.). It is paramount that PCI Facility personnel take every precaution in thoroughly protecting PII. Areas used during the process should assure privacy so that PII collected from the registrant and entered into the system(s) is not compromised. Privacy screens are a good idea in areas where staff or other persons may pass by and view the PC screen during an issuance process. These are the thoughts that should be on your mind as you perform the walk-through.

Assessment Review

Once the data collection phase of the assessment is complete, it is a good idea to have a final meeting with as many of the PCI Facility personnel as possible. Here, discuss, in general, the results of the assessment. If there are any control items for which you require further information or clarification, this is a good time to ask your questions. Advise those in the meeting that the results still have to be reviewed and analyzed before the final report is sent forward to the DAA. Remind them that you are only in “collection mode.” The DAA is responsible for providing the site with the assessment results and the accreditation decision. In addition, the DAA is responsible for providing the remediation actions required for controls that have not been fully satisfied. Of course, if you can provide any information that may be of help in clearing noted discrepancies, you may do so. This will allow the PCI Facility staff to rectify problem areas in a timely manner.

Conclusion

A successful assessment of a PCI Facility can be accomplished by following some basic guidelines. Become intimately familiar with FIPS 201-1 and SP 800-79-1. Use these and other available NIST documents to develop and execute the PCI assessment plan – that is why NIST developed them. Develop a good relationship with PCI Facility personnel before and during the assessment visit. Structure the assessment so that all documentation and personnel interview questions are addressed first. Then, perform a complete walk-through of the facility during the PIV card issuance process, assessing the remaining controls that require test and observation. As you follow the staff during an actual card issuance process, imagine yourself in the role of the PIV card applicant. As an assessor, you will find that assessing adequate implementation of the controls is easier if you measure them from a personal perspective. The two basic objectives the PCI Facility must meet are (1) Issuance of trusted and accurate credentials and (2) Protection of Personally Identifiable Information. When the data collection phase of the assessment is complete, meet with the PCI Facility staff to deal with any unanswered questions and to provide information on what actions will follow leading to the decision by the DAA to accredit the system.

References

[SP800-79-1] NIST Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, NIST, June 2008.

(Available at <http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf>)

[SP800-37] NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST Aug 2009.

(Available at <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>)

[SP800-53] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Aug 2009.

(Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf)

[SP800-53A] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, NIST, June 2010.

(Available at <http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>)

[SP-800-122] NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST, April 2010.

(Available at <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>)

[FIPS 201-1] NIST Federal Information Processing Standard 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, March 2006.

(Available at <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>)

Executive Office of the President, Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

(Available at http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm)