Approved PACS Topology Mapping Form (PACS 13.02)
VERSION 1.3.0

FIPS 201 EVALUATION PROGRAM

March 2, 2015
FINAL

Office of Government-wide Policy
Office of Technology Strategy
Identity Management Division
Washington, DC 20405
Document History

<table>
<thead>
<tr>
<th>Status</th>
<th>Version</th>
<th>Date</th>
<th>Comment</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>First draft</td>
<td>0.0.1</td>
<td>2/6/2014</td>
<td>Mapping for PACS 13.02</td>
<td>Limited</td>
</tr>
<tr>
<td>Draft</td>
<td>0.0.2</td>
<td>2/14/2014</td>
<td>Initial edit</td>
<td>Limited</td>
</tr>
<tr>
<td>Draft</td>
<td>0.0.3</td>
<td>2/18/2014</td>
<td>Updated definitions, diagrams</td>
<td>Limited</td>
</tr>
<tr>
<td>Draft</td>
<td>0.0.4</td>
<td>2/19/2014</td>
<td>Team edits</td>
<td>Limited</td>
</tr>
<tr>
<td>Draft</td>
<td>0.0.5</td>
<td>2/20/2014</td>
<td>Team edits</td>
<td>Limited</td>
</tr>
<tr>
<td>Draft</td>
<td>0.0.6</td>
<td>2/22/2014</td>
<td>Cleaned up table inconsistencies</td>
<td>Limited</td>
</tr>
<tr>
<td>Draft</td>
<td>0.1.0</td>
<td>5/16/2014</td>
<td>Cleaned up grammatical errors.</td>
<td>Public</td>
</tr>
<tr>
<td>Draft</td>
<td>0.1.1</td>
<td>7/8/2014</td>
<td>Revised category descriptions and Topology illustration to make it clearer that the configurations are examples, and that other approaches are acceptable. Changed Program name back to FIPS 201 Evaluation Program.</td>
<td>Public</td>
</tr>
<tr>
<td>Final</td>
<td>1.3.0</td>
<td>3/2/2015</td>
<td>Revised to be in sync with FRCT v1.3.0</td>
<td>Public</td>
</tr>
</tbody>
</table>
Table of Contents

1 Background ................................................................................................................. 1
2 Objectives..................................................................................................................... 1
3 Normative References ..................................................................................................... 1
4 FIPS 201 Evaluation Program Defined Categories .................................................. 2
   4.1 PACS and Validation Infrastructure (PVI) Category .............................................. 3
       4.1.1 PACS Functionality ................................................................................................. 3
       4.1.2 Validation Functionality .......................................................................................... 4
   4.2 PIV Reader Category ............................................................................................. 4
   4.3 Implementation & FISMA ....................................................................................... 5
   4.4 Topology Diagrams ............................................................................................... 6
5 Mapping ....................................................................................................................... 9
1  Background

The General Services Administration (GSA) is responsible for supporting the adoption of interoperable and standards-based Identity, Credential, and Access Management (ICAM) technologies throughout the Federal Government. As part of that responsibility, GSA operates and maintains the Federal Information Processing Standard (FIPS) 201 Evaluation Program and its associated Approved Products List (APL), as well as services for Federal ICAM (FICAM) conformance and compliance.

2  Objectives

The FIPS 201 Evaluation Program's PACS evaluation process is designed to be agnostic to architecture, and focuses solely on functional testing using an end-to-end testing methodology. This document facilitates applicant mapping of the functional requirements identified in *Functional Requirements and Test Cases* [FRTC] to the categories identified in the FIPS 201 Evaluation Program's PACS 13.02 topology.

3  Normative References


4 FIPS 201 Evaluation Program Defined Categories

The PACS 13.02 Topology defines one new category and re-uses a category from the PACS 13.01 Topology (4.1 – 4.2 below). Each of these categories is defined as part of a whole PACS solution that can be tested end-to-end using the [FRTC]. Note that a
category is not defined as a single object that is procured as a single SKU. The following definitions define the objects that make up a functional element called a category:

1. **Compatible** components are proved to work with each other.
2. **Interoperable** components are tested to determine the set of like and related components with which it can reliably be operated in combinations. Interoperable components must use an industry standard (e.g., ISO, ANSI, IETF RFC) to enable standardized interfaces between components.
3. A **subsystem** is assembled of compatible components. Hence a subsystem would be tested and acquired as a unit or “configuration item”. A subsystem may leverage an interoperable component external to the subsystem.
4. A **category** is made up of subsystems, compatible and/or interoperable components that meet functional requirements defined in [FRTC].

The two categories defined by this topology are **PACS and Validation Infrastructure**, and **PIV Reader**. They are further described in the following sections.

### 4.1 PACS and Validation Infrastructure (PVI) Category

The PACS and Validation Infrastructure is made up of a single product that has unified the PACS Infrastructure and Validation System functionality from topology 13.01 into a single infrastructure product. The resulting application becomes a unified infrastructure providing both capabilities with a single part number with many compatible components. This section will provide a definition for the compatible components that constitute a PACS and Validation Infrastructure. They are as follows:

1. PACS and Validation Application (PVA) and its server (also called the head-end);
2. Database and its server (often an integral part of the PVA, and on the same server);
3. Controllers (also called bridges, field panels, controllers, or secure controllers);
4. SCVP servers;
5. OCSP responders;
6. Full path discovery and validation software; and
7. Workstations (e.g., for administration, registration of individuals, help desk).

Other approaches that meet the functional requirements are also valid.

#### 4.1.1 PACS Functionality

The PVI’s functionality is made up of both PVA functions associated with physical access control and controllers. The PVA software runs on a server (be it physical, virtual image or cloud) and performs traditional PACS functionality as well as full support for FICAM Approved authentication methods leveraging PKI. The PVA communicates with controllers that are connected to PIV Readers. The controller is commonly installed locally to ensure performance and local security. Historically, this has included storing a local database within the controller for increased performance, for making access decisions and event logging should communications be lost with the host. The PVI controller’s functionality may include:
1. Communications between the PIV Reader and the PVA;
2. Access control status and logging;
3. I/O controllers;
4. Alarm controllers; and
5. Door controllers for the lockset, door position switch and request to exit.

Some vendors might want to consolidate these controller functions into a single component to increase performance or reduce the overall deployed footprint, thereby lowering costs.

A PACS and Validation Infrastructure is a diverse environment that interoperates with many different subsystems outside the scope of the current FIPS 201 Evaluation Program. These often include:

1. Intrusion Detection Systems (IDS);
2. Video Management Systems (VMS);
3. Visitor Management Systems (also called VMS);
4. Enterprise Identity Management Systems (E-IdM); and
5. Physical Security Information Management systems (PSIM).

These additional subsystems comprising a total physical security program may become categories in a future FIPS 201 Evaluation Program spiral.

4.1.2 Validation Functionality
Validation functions of the PVI provide the necessary capabilities to perform identification and authentication of the credential and the bearer of a credential according to various approved FICAM Authentication Methods. These methods and the controls necessary to implement them, are defined fully in [E-PACS] and tested as an end-to-end system according to [FRTC]. Validation functions, as defined by the FIPS 201 Evaluation Program, have a direct impact on PACS behaviors as well as the PIV Reader. The interoperable components that may constitute or support the PVA’s validation functionality include:

1. SCVP Servers/Clients;
2. OCSP responders; and
3. Full path discovery and validation software.

PKI validation functions are in integral part of the PVA. For convenience, an SCVP Client (and potentially server) may be part of the solution that generally resides in the same footprint as the PVA.

Other approaches that meet the functional requirements are also valid.

4.2 PIV Reader Category
A PIV Reader is a shared category with the 13.01 topology. It is an accepting device as defined in [E-PACS] that provides the human interface, the card interface, and the
communications\textsuperscript{1} to and from the PACS and Validation Infrastructure. It is installed at a door, portal, or gateway. As an accepting device, a PIV Reader may be a wholly-integrated unit, or it may be an assembly of components including:

1. Contact smart card reader;
2. Contactless smart card reader;
3. LCD display;
4. LED lights;
5. Audio announcers;
6. PIN pad;
7. Fingerprint sensor;
8. Other biometric modalities (e.g., iris); and
9. Communications to a PACS and Validation Infrastructure (e.g., Wiegand, RS-485, secure wireless, Ethernet).

The PIV Reader is a device that is installed at the door and performs functions to interact with the bearer of the credential, the credential itself. This configuration can vary. The PIV Reader must support a minimum of one FICAM authentication mode as defined in [E-PACS], but may support multi-factor authentication.

Other approaches that meet the functional requirements are also valid.

\textbf{4.3 Implementation & FISMA}

The Government recognized the importance of information security to the economic and national security interests of the United States, and to address these concerns the President in December 2002 signed into law the E-Government ACT (Public Law 107-347). Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), which requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and information systems that support operations and assets of an agency.

Since all PACS and Validation Infrastructure requires access to private or public network domains at a minimum for PKI validation services, FISMA requirements for securing access to the systems hosting these applications and communications to their infrastructures come into play.

The specific requirements needed to comply with FISMA vary upon the security policies and procedures based on the individual agency’s risk assessment.

Also impacting requirements is the manner by which the 13.02 topology is deployed. The deployment options for 13.02 and definitions may include the following:

\textsuperscript{1} Vendors have the flexibility on how the communication works (i.e., whether communication is direct at run time or other mechanisms are used).
1. **Standalone Server** - A built-for-purpose server that may or may not belong to a domain or workgroup but hosts the PVA, typically hosted locally in a secure LAN room or NOC and accessible through the locally configured network or enterprise.

2. **Server Cluster** - A built for purpose cluster used to host the PVA and provide high performance computing, with high availability characteristics, typically hosted locally in a secure LAN room or NOC and accessible through the locally configured network or enterprise.

3. **Virtual Server** - Uses a method of hosting virtual machines within a physical server environment, and is typically hosted locally in a secure LAN room or NOC and accessible through the locally configured network or enterprise.

4. **Cloud Software as a Service (SaaS)** - When implementing cloud based services, communications between endpoints (i.e., controllers and the PVA SaaS) is generally protected by secure VPN connections or other FICAM-approved cryptographic protocol.

   a. **Private** - A private cloud solution is typically a vendor-hosted, dedicated computing resource allocated within the scope of the privately-controlled network infrastructure. This model provides a level of isolation from Public network access, while enabling SaaS capability. This allows enterprise security applications to be shared among organizations or facilities within the private network domain.

   b. **Public** - A public cloud solution could provide PVA functionality in the SaaS model hosted by the vendor. This type of implementation generally travels outside the locally configured network to outside hosted networks.

Depending on the deployment options, additional functional requirements may vary to reflect FISMA guidelines, as it relates to protection of information and assets

### 4.4 Topology Diagrams

The Applicant must submit a topology diagram to the FIPS 201 Evaluation Program. The diagram must show the architectural linkage between the PVI and the interoperable components that make up an end-to-end system. It must show which components belong to a given category. The diagram facilitates an understanding of how a system is linked together and how it performs the functions required by [FRTC]. In other words, the diagram is a communications tool to enable the FIPS 201 Evaluation Program to understand how a given solution is put together to support end-to-end operational testing. Figure 1 portrays possible locally-hosted approach. Figure 2 portrays a possible cloud-hosted approach. Other approaches that meet the functional requirements are also valid.
A complete topology diagram identifies every component that makes up an applicant's solution for the FIPS 201 Evaluation Program categories and provides the specific linkages (communications, internal messaging) that makes up the solution. As new topologies are adopted per the FIPS 201 Evaluation Program's *Topology Adoption*
Process [TAP], applicants must map their solution and its components into these new topologies.