# Enabling Strong Authentication with Personal Identification Verification Cards: Public Key Infrastructure (PKI) in Enterprise Physical Access Control Systems (E-PACS) Recommended Procurement Language for RFPs

VERSION 1.1.0


## FIPS 201 EVALUATION PROGRAM

**February 24, 2015**

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

# Document History

| Status | Version | Date | Comment | Audience |
|---|---|---|---|---|
| Draft | 1.06 | 08/20/2013 | Added new content to section 4.1.2:<br>- Section 6. Performance Criteria<br>- Section 7. Severity Notification<br>- Section 8. Removed Products List<br>Added new content to section 4.1.3:<br>- Content on requirements for PACS Integrator/Installer training and certification requirements | Limited |
| Final | 1.1.0 | 02/24/2015 | Updates to Guidance | Public |

# Table of Contents

# 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 201 Evaluation Program (Program) and its Approved Products List (APL), as well as services for Federal Identity, Credentialing and Access Management (FICAM) segment architecture conformance and compliance.

The Program[1] provides testing of Enterprise Physical Access Control Systems (E-PACS) for listing on the APL that fully support both Personal Identity Verification (PIV) and PIV Interoperable (PIV-I) credentials. Performance-based requirements for the use of PIV and PIV-I in E-PACS are detailed in the *FIPS 201 Evaluation Program Functional Requirements and Test Cases* [FRTC] document. Office of Management and Budget (OMB) established the authority for these activities in the following memoranda:

- **OMB Memorandum M-05-24 [M-05-24],** Question 5.

  *"A. **Requirement to use federally approved products and services** – To ensure government-wide interoperability, all departments and agencies **must** acquire products and services that are approved to be compliant with the Standard and included on the approved products list.*

  *B. **Use of GSA Acquisition Services** - Third paragraph states:*

  *Departments and agencies are encouraged to use the acquisition services provided by GSA. Any agency making procurements outside of GSA vehicles for approved products **must certify the products and services procured meet all applicable federal standards and requirements, ensure interoperability and conformance to applicable federal standards for the lifecycle of the components, and maintain a written plan for ensuring ongoing conformance to applicable federal standards for the lifecycle of the components.**"*

This provides GSA with the authority to act as executive agent for OMB to ensure that the Program serves the needs of the federal enterprise in an inclusive manner to the various standards, requirements, interoperability and conformance as applied within the execution of HSPD-12.

- **OMB Memorandum M-06-18 [M-06-18],** Pages 3 and 4:

  *"Agencies that proceed with the acquisition of products and services for the implementation of HSPD-12 through acquisition vehicles other than GSA IT Schedule 70 must*

[1] The FIPS 201 Evaluation Program website is located at http://idmanagement.gov/ficam-testing-program

> *ensure that* ***only approved products/services from the Approved Product List are acquired and incorporated into system solutions*** *and ensure compliance with other federal standards and requirements for systems used to implement HSPD-12. In order to ensure government-wide interoperability, this applies for the lifecycle of the products, services, and/or systems being acquired."*

In addition, OMB Memorandum M-11-11 [M-11-11] requires that all acquisitions be compliant with the *FICAM Roadmap and Implementation Guidance* [Roadmap] and that all E-PACS acquisitions be compliant with *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116* [SP 800-116]. Specifically:

> *"To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the agency's policy needs to include the following requirements:*
>
> - *Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.*
> - *Effective the beginning of FY2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.*
> - *Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation. In order to ensure government-wide interoperability, OMB Memorandum 06-18, "Acquisition of Products and Services for Implementation of HSPD-12" requires agencies to acquire products and services that are approved as compliant with Federal policy, standards and supporting technical specifications.*
> - *Agency processes must accept and electronically verify PIV credentials issued by other federal agencies.*
> - *The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's "Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance" (available at www.idmanagement.gov)."*

The Program is not the only place that is focused on improvements to E-PACS as a FICAM-conformant solution. The latest Federal Information Security Management Act (FISMA) guidance in *NIST SP 800-53-4*, dated April 2013 [SP800-53-4] adds new focus

to FICAM conformance and security. It now includes E-PACS and provides focus on its importance as a Cyber Security initiative of the Federal enterprise. One of the core controls guiding FICAM conformance in using PIV and PIV-I is:

> *"**IA-5(2)** AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*
> *The information system, for PKI-based authentication:*
>
> *(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;*
>
> *(b) Enforces authorized access to the corresponding private key;*
>
> *(c) Maps the authenticated identity to the account of the individual or group; and*
>
> *(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network".*

There are a minimum of five additional controls referencing E-PACS, with one clearly citing [E-PACS] as a source of requirements for FICAM conformance.

It is recognized that security professionals supporting E-PACS within agencies work very closely with the vendor community to ensure a solution that is fit for purpose in their unique environment. Accordingly, an agency may use a vendor PACS solution that meets the agency's needs but is not yet on the APL - but only for a specified period of time. The agency must include procurement language that requires the vendor to apply to the FIPS 201 Evaluation Program for evaluation and become listed on the APL within six months of contract award or replace all unapproved components with APL components at contractor expense[2] In addition, procurement language must include the following process and time line to be listed on the APL:

- Within 30 days of contract award, the vendor must apply to the FIPS 201 Evaluation Program.
- Within 60 days of contract award, the vendor must receive approval of its application.
- Within 90 days of award, the vendor must be in an approved FIPS 201 Evaluation Program Lab for testing.
- Within 6 months of contract award, the vendor's solution must be listed on the FIPS 201 Evaluation Program APL.
- If after 6 months from contract award, the vendor's solution is not on the APL, then within 1 year of contract award, the vendor must replace the solution with one that is listed on the APL.

[2] The application for FIPS 201 Evaluation Program certification to be listed on the APL can be found at https://www.idmanagement.gov/sites/default/files/documents/PACS%20Application%20Package.zip

The above process and specified timeframe will strengthen solutions acquired by agencies and ensure those solutions are FICAM conformant.

Per [M-05-24] Question 5.B paragraph 3, Departments and agencies are strongly encouraged to use the [APL].

> *"Any agency making procurements outside of GSA vehicles for approved products must certify the products and services procured meet all applicable federal standards and requirements, ensure interoperability and conformance to applicable federal standards for the lifecycle of the components, and maintain a written plan for ensuring ongoing conformance to applicable federal standards for the lifecycle of the components."*

The Program's [FRTC] meets this requirement for E-PACS solutions. It is recommended [FRTC] be used as the baseline for any agency's testing program should the agency seek to certify E-PACS products and services independently of the APL.

# 2 Intended Audience

This document is intended for use by procurement officials in developing a Request for Proposal (RFP), Statement of Work (SOW), or Performance Work Statement (PWS) for the acquisition of HSPD-12, FIPS 201, and FICAM-conformant E-PACS solutions for use in federal facilities. Individuals involved in developing procurements may include Contract Officers, Contracting Officer Technical Representatives, Facility Security Professionals and System Architects.

# 3 Objectives

This document provides language for E-PACS related procurements to ensure compliance with applicable policies noted above. This language is intended to be added to the requirements section of an SOW, PWS or RFP. The language fully leverages approved Public Key Infrastructure (PKI) authentication methods for E-PACS listed on the APL. The language is fully conformant with the mandates within [M-11-11] to stay aligned with [Roadmap] and [SP 800-116].

The procurement language provided is tightly focused on requiring all E-PACS solutions to be capable of supporting approved PKI authentication methods. This language does not provide architectural guidance, implementation detail or limitations on use of additional authentication methods. Program Managers and System Architects writing RFP/SOW language may find useful guidance in *FICAM PIV in E-PACS Guidance Draft Version 2.1, January 31, 2013* [E-PACS].

# 4 Recommended Language for E-PACS RFPs and SOWs

All RFPs, PWSs and SOWs for new or upgraded E-PACS should include the language for integrating the mandatory authentication mechanisms of [FIPS 201] into E-PACS provided in both *Section 4.1* and *Section 4.1.3*. The section headers and language are designed to be directly cut and pasted into procurements. Please note that the normative references in *Section 4.1.3* support the language in *Section 4.1* and may be in addition to any other normative references required by the procurement.

## *4.1 Requirements for PKI in E-PACS*

*Office of Management and Budget (OMB) Memorandum M-05-24* [M-05-24] provides GSA with the authority to act as executive agent for OMB to ensure that the GSA program serves the needs of the federal enterprise in an inclusive manner to the various standards, requirements, interoperability and conformance as applied within the execution of HSPD-12.

*OMB Memorandum M-06-18* [M-06-18] requires all agencies to use the General Services Administration (GSA) Approved Products List [APL] in all procurements for *Homeland Security Presidential Directive 12* [HSPD-12] and *Federal Information Processing Standard 201* [FIPS 201] compliant systems. The GSA FIPS 201 Evaluation Program lists compliant Enterprise Physical Access Control Systems (E-PACS) solutions on the [APL] for procurements.

*OMB Memorandum M-11-11* [M-11-11] requires all E-PACS systems at federally owned or leased buildings "be enabled to use PIV credentials" and that "agency processes must accept and electronically verify PIV credentials issued by other federal agencies." [M-11-11] further requires compliance with *FICAM Roadmap and Implementation Guidance* [Roadmap], which expands the use of Personal Identity Verification (PIV) to include PIV Interoperable (PIV-I) credentials in FICAM compliant solutions. Both PIV and PIV-I credentials contain PKI digital certificates, fingerprint minutia templates, and a secure Personal Identification Number (PIN).

### *4.1.1 Definition of "Electronically verify"*

"Electronically verify" means that the E-PACS at federally owned or leased facilities must be capable of performing ***PKI strong authentication methods*** to establish a high degree of confidence in the credential, and as required by the facility, the binding between the credential and the bearer. Before granting physical access to a Government employee or contractor, electronic verification of a PIV or PIV-I credential by the E-PACS shall evaluate the credential to determine:

1. The digital certificate is valid at time of use (specifically, the issuing certificate authority has not placed the certificate on its certificate revocation list (CRL) within the previous 6 hours),
2. A successful challenge/response was issued utilizing the private key, and
3. A positive confirmation that the certificate's public key is identical to the public key registered to and authorized for access to the facility.

Depending on the local security level, E-PACS shall support a minimum of one FICAM approved PIV PKI authentication method, specifically PKI-CAK, PKI-AUTH, and PKI-AUTH + BIO(-A), as defined in [SP 800-116] in accordance with ICAM Sub Committee (ICAMSC) Guidance. The E-PACS solution shall be comprised of products that are listed on the [APL]. As required by FIPS 201, E-PACS must validate that PIV Credentials were issued under [Common], and have not been placed on CRL by the issuing certificate authority within the previous 6 hours before the time of access.

1. Contractor shall ensure that proposed solutions align with these goals and fully describe related capabilities, assumptions, limitations, and non-conformance.
2. Any non-conformance to this requirement must be justified in a separate technical appendix. This appendix may be shared with the ICAMSC and the FIPS 201 Evaluation Program.

### *4.1.2 Required E-PACS Capabilities*

The E-PACS shall be capable of evaluating the validity of a PIV/PIV-I credential and the binding of the credential to the bearer at time of registration and at time of access in accordance with the following requirements:

1. The E-PACS shall confirm the validity of the PIV/PIV-I credential presented by performing the following functions:
   a. Active Authentication
      i. A challenge/response protocol using PKI certificates on the PIV/PIV-I card.
      ii. *Note:* at time of access, the E-PACS shall confirm the public key used in item 1.a.i is identical to the public key that was initially registered and authorized for access.
   b. Validation of Trusted Origin
      i. Certificate status checking (i.e. confirming expiration, revocation, signature validation).
      ii. Path discovery and validation (i.e. evaluating the full trust chain to a trust anchor for policies, constraints, expiration, revocation status and signature verification).
      iii. The certificate policy presented by the credential shall chain back to [Common] for PIV, or to [FBCA] for PIV-I.
   c. Bearer Confirmation
      i. Use PKI-CAK if no bearer confirmation is required.
      ii. Use PKI-AUTH for challenge/response, and confirmation of the bearer's presented PIN.
      iii. Use PKI-AUTH + BIO(-A) for challenge/response and confirmation of the bearer's presented PIN and fingerprint.

   Only when the results of these three operations (1.a, 1.b and 1.c) are confirmed as positive should a credential either be registered to the E-PACS for authorization, or granted access based on the authorization profile for that credential.
2. The E-PACS shall use an [APL] approved Validation System to perform item 1.b "Validation of Trusted Origin". Validation Systems may use one or a combination of:

a. Certificate Revocation Lists (CRLs),
b. Online Certificate Status Protocol (OCSP), or
c. Server-based Certificate Validation Protocol (SCVP).

3. The E-PACS may use cached information for item 1.b "Validation of Trusted Origin" using the technologies identified in 2. In all cases, credentials must be valid at time of registration or access such that:
   a. The PIV credential's certificates have not been placed on CRL by the issuing certificate authority within the previous 6 hours.
   b. Full path discovery and validation information is not more than 18 hours old.
4. At time of in-person registration, the E-PACS shall:
   a. Capture the Content-Signer certificate, the PKI-AUTH certificate, and the PKI-CAK certificate for purposes of periodic Validation of Trusted Origin (items 1.b, 2 and 3).
   b. At a minimum, use PKI-AUTH for challenge/response, and confirmation of the bearer's presented PIN.
   c. Check the expiration date of all data objects and signers on the credential and perform a private key challenge/response for each certificate being registered.
   d. Perform Validation of Trusted Origin (items 1.b, 2 and 3) of the user's credential and its signers.
5. An organization may have an Enterprise Identity Management (E-IdM) system in place. In this environment, the E-PACS may have direct provisioning and de-provisioning of access records from the E-IdM that are tightly bound to Human Resources processes. This method shall be in addition to "Validation of Trusted Origin" as described in items 1.b, 2 and 3.
   a. At a minimum, the E-IdM shall provide the CHUID, the Content-Signer certificate, the PKI-AUTH certificate, and the PKI-CAK certificate for purposes of:
      i. Periodic "Validation of Trusted Origin" (items 1.b, 2 and 3)
      ii. Verification of the public key as registered to the E-PACS (item 1.a.ii)
6. Performance Criteria at time of access
   a. PKI-CAK
      i. Performance Time is measured from detection of the card by the PIV reader (contact or contactless) to the access grant or access denied response at the door. Included as a part of this process is the PKI challenge and response to include certificate validation (items 1.b, 2 and 3).
      ii. Performance Time shall be 2.5 seconds or less.
   b. PKI-AUTH
      i. Performance Time is measured from completion of entering the PIN to the access grant or access denied response at the door. Included as a part of this process is the PKI challenge and response to include certificate validation (items 1.b, 2 and 3).
      ii. Performance Time shall be 2.5 seconds or less.
   c. PKI-AUTH + BIO(-A)
      i. Performance Time is measured from completion of entering the PIN and successful presentation of a fingerprint to the access grant or access denied

response at the door. Included as a part of this process is match-to-card fingerprint validation, and the PKI challenge and response to include certificate validation (items 1.b, 2 and 3).

ii. No Performance Criteria are established at this time.

7. Severity Notification
   a. Background: The FIPS 201 Evaluation Program / Approved Product List (APL) updates the technical criteria for approved product / service listings on a periodic, and as needed, basis. When these updates are made, listed/approved products are re-assessed according to the updated criteria (this generally occurs due to identification of new threats, updated standards / policies, etc.). Noncompliant products / services will be assessed a "Severity" finding. When this is the case, the Severity classification may be either a 1 (most severe), 2 (moderate), or 3 (low severity). Each severity finding has an allowable period of time for the vendor to correct and update their product / service.
   b. Requirements: Severity 1 findings require the most urgent attention by the vendor to correct the noted product / service issue.
      i. It is the responsibility of the product/service vendor to promptly notify the Integrator / Installer of any Severity 1 findings, and provide a brief action plan to address timely resolution of the noted issue. Resolution of noted issue shall include provision of a "patch", approved by the FIPS 201 Evaluation Program, free of charge to the Integrator / Installer. Additionally, the product / service vendor shall notify the Integrator / Installer when the issue has been resolved and confirm acknowledgement.
      ii. It is the responsibility of the Integrator / Installer to promptly notify the Contracting Officer (CO) and / or Contracting Officer Technical Representative (COTR) of any Severity 1 findings, and provide a brief action plan to address timely resolution of the noted issue. Resolution of noted issue shall include provision of a "patch", approved by the FIPS 201 Evaluation Program, free of charge to the government. Additionally, the Integrator / Installer shall notify the CO/COTR when the issue has been resolved and confirm acknowledgement.
8. Products / Services Transitioned to the Removed Products List (RPL)
   a. Background: The FIPS 201 Evaluation Program / Approved Product List (APL) updates the technical criteria for listing on a periodic, and as needed, basis. When these updates are made, listed/approved products are re-assessed according to the updated criteria (typically due to identification of new threats, updated standards / policies, etc.). When this occurs, products or services may be transitioned to the Removed Products List. In general, this is done when technology becomes obsolete or is no longer suitable for government use (due to vulnerability, etc.).
   b. Requirements: The Integrator / Installer of APL approved Products / Services vendor must stipulate that their product / service, when provided to the government, shall, from time of procurement, remain active on the APL (not transitioned to the RPL) for a minimum period of one year.

### *4.1.3 Requirements of Vendors and Integrators / Installers*

#### 4.1.3.1 Vendors

As previously stated it is recognized that security professionals supporting E-PACS within agencies work very closely with the vendor community to ensure a solution that is fit for purpose in their unique environment. Accordingly, an agency may use a vendor PACS solution that meets the agency's needs but is not yet on the APL - but only for a specified period of time. The agency must include procurement language that requires the vendor to apply to the FIPS 201 Evaluation Program for evaluation and become listed on the APL within six months of contract award or replace all unapproved components with APL components at contractor expense[3] In addition, procurement language must include the following process and time line to be listed on the APL:

a. Within 30 days of contract award, the vendor must apply to the FIPS 201 Evaluation Program.
d. Within 60 days of contract award, the vendor must receive approval of its application.
e. Within 90 days of award, the vendor must be in an approved FIPS 201 Evaluation Program Lab for testing.
f. Within 6 months of contract award, the vendor's solution must be listed on the FIPS 201 Evaluation Program APL
g. If after 6 months from contract award, the vendor's solution is not on the APL, then within 1 year of contract award, the vendor must replace the solution with one that is listed on the APL.

#### 4.1.3.2 Integrators / Installers

With regard to PACS Integrators (or Installers), PACS configuration work performed under the awarded task must be performed by personnel that are listed on IDManagement.gov as a Certified System Engineer ICAM PACS. The certification must be current. (Note: This certification program will provide necessary training and a minimum assurance of ability to efficiently and effectively implement PKI and federal ICAM architectures for E-PACS and meet federal requirements.)

[3] The application for FIPS 201 Evaluation Program certification to be listed on the APL can be found at https://www.idmanagement.gov/sites/default/files/documents/PACS%20Application%20Package.zip

## 4.2 Normative References


**[HSPD-12]** Homeland Security Presidential Directive 12, August 27, 2004
https://www.dhs.gov/homeland-security-presidential-directive-12

**[FIPS 201]** Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
http://csrc.nist.gov/publications/PubsFIPS.html

**[Common]** FPKIPA X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.21, December 18, 2012
http://idmanagement.gov/fpki-certificate-policies-cps

**[FBCA]** X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.26, April 26, 2012
http://idmanagement.gov/fpki-certificate-policies-cps

**[APL]** GSA Approved Products List
http://idmanagement.gov/approved-products-list-apl

**[E-PACS]** FICAM Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS), DRAFT Version 2.0.2, May 24, 2012
http://idmanagement.gov/ficam-testing-program

**[FRTC]** FIPS 201 Evaluation Program Functional Requirements and Test Cases
http://idmanagement.gov/ficam-testing-program

**[M-05-24]** Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf

**[M-06-18]** Office of Management and Budget (OMB) Memorandum M-06-18, June 30, 2006
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-18.pdf

**[M-11-11]** OMB Memorandum M-11-11, February 3, 2011
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

**[Roadmap]** FICAM Roadmap and Implementation Guidance, Version 2.0, December 2, 2011
http://idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance

**[SP800-53-4]** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53-4, April 2013
http://csrc.nist.gov/publications/PubsSPs.html

**[SP800-116]** National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, November 2008
http://csrc.nist.gov/publications/PubsSPs.html