PACS Assessment Toolkit

DRAFT VERSION 1.0.0

FIPS 201 EVALUATION PROGRAM

September 16, 2021

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

Introduction

Although there are several guidelines such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116 that pertain to electronic Physical Access Control Systems (ePACS), no formalized ePACS operational assessment standard or methodology has been developed to help implementers identify operational gaps.

Purpose and Scope

This form gives PACS implementers a mechanism to determine whether their systems have been configured in a fashion that meets the intent of Federal Identity, Credential, and Access Management (FICAM) and NIST guidelines for the use of Personal Identity Verification (PIV) credentials in facility access controls. These guidelines provide an end state for PACS that encompass secure, auditable, and interoperable physical access controls based on authentication mechanisms available via the PIV, including the following:

- One-factor readers: PKI authentication using the Card Authentication Certificate (PKI-CAK)
- Two-factor readers: PKI authentication using the PIV Authentication Certificate (PKI-Auth)
- Three-factor readers: PKI-Auth + attended or unattended Biometric verification (PKI-Auth+BIO(-A) or PKI-CAK+BIO(-A))

Once completed, the form's outputs are intended to provide recommended changes to a physical access control policy or PACS configuration that meets the intended FICAM end state.

This form is meant to be used on a voluntary basis as part of a self-assessment and is not part of any official reporting mechanism at the time of initial publication. It may contain information that is redundant to, or useful in, other required documentation such as a System Security Plan (SSP).

In Scope

This form can be used to assess ePACS at essentially any level of organization (local or enterprise), provided there is an ePACS infrastructure installed that is meant to use NIST-recommended PIV authentication mechanisms. This assessment toolkit includes the following topics:

- PACS governance and acquisition information:
    - General system information
    - Physical access control policy alignment to relevant standards and guidelines
    - FIPS 201 Evaluation Program PACS Approved Product List alignment
- System configuration and usage:
    - Alignment agency to policy and procedures
    - Hardware configurations, including card readers
    - ePACS software administrator management
    - ePACS software PKI configurations
    - Logging and auditing capabilities and configurations
    - Authorization processes, including card or user registration
    - Time of access processes such as card or user authentication (using various approved methods) and identification

Out of Scope

Although several other categories of considerations would be required to facilitate an Authority to Operate (ATO) for ePACS, several of these are considered out of scope because they do not support the more specific intent of FICAM and SP 800-116 alignment. Some of these additional considerations considered out of scope include the following:

- Life safety requirements
- Risk assessment processes and outputs
- Non-FIPS 201 related visitor management processes/mechanisms
- Self-contained/disconnected ePACS supporting classified areas/SCIFs (unless they require FIPS 201 and PIV conformance)
- External privileged access solutions or integrations
- Developing or future authentication capabilities such as support for On-Card Biometric Comparison (OCC), Secure messaging (SM), and Virtual Contact Interface (VCI)

Intended Audience

This form is intended for ePACS implementers throughout the federal government who own or operate ePACS that are designed to be FIPS 201 compliant.

Assumptions and Prerequisites

It is assumed that organizations leveraging this toolkit have done the following:

- Acquired and installed an ePACS to facilitate controlled access to a campus, building/facility, secure areas, or some combination thereof
- Conducted a risk assessment of the associated controlled areas and have established a facility security plan, physical access control policy, or similar document guiding the design and implementation of the system
- Established collaboration with appropriate IT resources to ensure baseline system functionality (e.g., networking, domain management, connectivity to external systems, etc.)

Toolkit Organization and Usage

This toolkit contains five primary sections, each with a slightly different purpose:

- General Information Worksheet: Consolidates generic information on the ePACS itself to include a high-level inventory of components
- Policy Analysis Worksheet: Presents several driving questions that relate to elements in a comprehensive physical access control policy which also drive critical ePACS configurations
- Operational Functionality Worksheet: Consolidates information regarding several key configurations of ePACS to gauge the security and interoperability of the ePACS
- Test Cases Worksheet: Provides both positive and negative test cases to ensure proper configuration of both reader and supporting PACS infrastructure to support the ePACS functionality
- Additional Considerations Worksheet: Includes considerations that are not formally part of this toolkit but may be helpful in ensuring operational redundancy and supporting an SSP and ATO

General Information Worksheet

Worksheet directions: Select checkboxes for items or options that pertain to your organization. Enter information in provided fields accordingly.

ePACS Scope

Enterprise ePACS	○
Local ePACS	○

System Point of Contact

	Name	Title	E-mail	Phone
System owner				
Authorizing official				
Vendor support				
System or Business Administrator				

System Server Location(s)

Facility Designation and/or FRPPMS Identifier	Physical Address	Room Designator	Responsible Party	Main POC

ePACS Site Specifics

Facility Designation and/or FRPPMS Identifier	Physical Address	Location of PACS Server (local/enterprise)	Responsible Party	Main POC	Number of Internal Access Points	Number of External Access Points

ePACS Inventory Information

Note: Common Name, Manufacturer, and Version information entered in this table will automatically populate the Common Name, Manufacturer, and Version columns in the first six rows of the Operational Functionality Worksheet/PACS Software and Hardware Configuration section.

	Common Name	**Manufacturer**	**Version**	**APL #**	**No APL #**	**Perimeter #**	**Internal #**
Access control system software					□	▨	▨
Validation system					□	▨	▨
ePACS components					□		
One-factor readers: PKI authentication using the Card Authentication Certificate (PKI-CAK)					□		
Two-factor readers: PKI authentication using the PIV Authentication Certificate (PKI-Auth)					□		
Three-factor readers: PKI-Auth + attended or unattended Biometric verification (PKI-Auth+BIO(-A) or PKI-CAK+BIO(-A))					□		

ePACS FISMA ID/ATO Status

Note: If ATO has been completed and the system conforms with IP policy, there is no need to fill in the Operational Functionality Worksheet/IP Conformance section.

Has the system received an ATO?

Yes	○
No	○

System FISMA ID	

Policy Analysis Worksheet

Worksheet directions: Select checkboxes for items or options that pertain to your organization. Enter information in provided fields accordingly.

ePACS Governance

Do you have a Physical Access Policy or similar guiding document (e.g., standard operating procedure, enterprise guidance, or other guide)?

Yes	○
No	○

Do you have a change control process defined for your ePACS?

Yes	○
No	○

List stakeholders	
List approvers	
Describe the process	
Describe any testing or verification	

Risk Assessment

What risk framework is used for your ePACS categorization and planning?

NIST RMF	□
ISC RMP	□
Other/local	□
Framework name	
None	□

SP 800-116 R1	FSL	Agency Internal Risk Rating(s)	Number of Facilities	Number of Areas	Total
Custom	I				
	II				
Limited	III				
Controlled	IV				
Exclusion	V				

Does the policy address which areas require human guards?

Yes	○
No	○

If manned guard posts are not used 24 hours each day, are additional authentications factors or other security devices used?

N/A	○
Yes	○
Describe additional factors	
No	○

Are records maintained to document reader mode (i.e., time-based access) decisions and are procedures outlined in the policy for space owners to record changes?

Yes	○
No	○
No, inherited, ePACS active 24/7	○

Does the policy indicate additional access controls based on environmental factors?

None	□
Force Protection Condition (FPCON)	□
National Terrorism Advisory System (NTAS)	□
Other	□
List other	

Does the policy or procedure define how access control systems should operate in a disaster or emergency?

Fail-safe (Fail-open)	○
Fail-secure (Fail-closed)	○
Hybrid based on ratings	○
Not documented	○

General: Access Requirements and Authentication

General: Authentication

Note: Items selected in the table below affect available options in the Operational Functionality Worksheet/Trust Store Configuration section.

Does the policy list acceptable authenticators/credentials?

Internal PIV/CAC	□		
External PIV/CAC	□		
Derived PIV	□		
PIV-I	□		
Local badge or alternative authenticator	□	IAL	AAL
Other	□	IAL	AAL
None	□		

Does the policy allow for temporary credentials if primary credentials are lost or stolen?

Yes	○
List credential/solution	
No	○

General: Authorization

Does the policy indicate physical access authorization for specific user populations, either generally or by area categorization?

Internal or standard users (employees)	□
Contractors	□
Partner organization employees or contractors	□
Detailed personnel	□
Volunteer personnel	□
Other role-based authorization	□
List roles	
None	□

Does the policy state minimum requirements for standard/baseline physical access authorization (e.g., facilities)?

None	□
NACI/Suitability determination	□
Role-based authorization (part of a team)	□
Validation of need	□
Other	□
List other authorization factors	

Does the policy define authorization requirements or each category of secure area?

Yes	○
No	○

Does the policy state when users should be removed from physical access?

Yes	○
No	○

Examples	Deprovisioning Method	Applicability
Employment terminated		□
Transfer		□
Temporary flag		□
Other (List other conditions):		□

Does the policy specify a maximum time of unused access before removing accesses?

Yes	○
What time frame?	
No	○

Privileged or Administrator Access

Does the policy list minimum administrative user qualifications?

No	□
Suitability determination	□
Security clearance	□
Professional certification	□
Other	□
List other	

Are privileged accounts monitored or do administrative activities result in notifications?

Yes	○
Describe details (e.g., audit log analysis, etc.)	
No	○

Is remote administration of the PACS, validation engine, or readers allowed?

Yes	○
Describe additional security controls (e.g., VPN, etc.)	
No	○

Visitor Management

Does the policy define common categories of visitors and are they aligned to types of acceptable credentials?

No	□
Public visitor	□
Foreign national visitor	□
Other federal visitor	□
Other government visitor	□

Does the policy delineate short- and long-term visitors and the associated credential?

Yes	○
No	○

Does the policy specify what vetting is used to determine authorization of visitors?

No □		
Vetting	**Applicability**	**Visitor Access Level**
NACI/Suitability determination	□	
Role-based authorization (part of a team)	□	
Validation of need	□	
Other	□	

Does the policy specify or reference detection of and actions on unauthorized access?

Yes	○
No	○

Audit/Logging Requirements

Does the policy stipulate what information is to be collected in audit logs?

Yes	○
No	○

Does the policy state who can view or modify audit logs?

Yes	○
Describe roles	
No	○

Does the policy state how long audit logs are to be retained or archived?

Yes	○
Describe log retention lifecycle	
No	○

Does the policy stipulate how physical access is granted or denied in the event of an auditing system failure?

Yes	○
No	○

Operational Functionality Worksheet

Worksheet directions: Select checkboxes for items or options that pertain to your organization. Enter information in provided fields accordingly.

PACS Software and Hardware Configuration

This section is intended to verify the system configuration and operation aligned with agency policies. PACS system and components are installed and versions that have been APL approved, readers are configured to operate in a mode consistent with FICAM authentication modes, and users are identified using unique identifiers. It is assumed that ePACS readers will always have a one-factor minimum configuration.

Note: Information entered in the Common Name, Manufacturer, and Version columns in the General Information Worksheet/ePACS Inventory Information section will automatically populate the Common Name, Manufacturer, and Version columns in the first six rows of the table below.

	Common Name	**Manufacturer**	**Version**	**Version APL Listed**	**Authentication Mechanism Enabled**
PACS software					▨
Validation system					▨
PACS components					▨
One-factor readers					
Two-factor readers					
Three-factor readers					
Unique user identification					

Time Synchronization

Components that have the capability of using a time sync server should be using agency-approved time sync servers. In PKI processing, it is essential that time is correct for components.

	Common Time Source(s)	**Specific Time Server**	**Other Sources**	**Time Zone**
Server setting				
Client workstation setting (e.g., administrator, guard, registration stations, etc.)				
PACS components				

Trust Store Configuration

This section is intended to verify that the PACS system is operating using the allowable trust authorities as defined by the agency.

Note: The availability of credentials in the table below is limited by the selection of applicable authenticators/credentials in the Policy Analysis Worksheet/General Authentication section.

			PIV/CAC or Federally Issued PIV-I		**Commonly Applicable PKIs**	
	Treasury SSP	**Entrust SSP**	**Verizon SSP**	**DoD PKI**	**DoS PKI**	**GPO**
Internal PIV/CAC CA	□	□	□	□	□	□
External PIV/CAC CA	□	□	□	□	□	□
Derived PIV		□			□	
PIV-I CA						

Local badge or alternative PKI authenticator	List CAs
Other CA (e.g., TWIC, ECA, etc.)	List CAs

PKI Revocation Configuration

Use this section to document the revocation solution the agency is leveraging and ensure the update frequency aligns with best practices.

Revocation Solutions (SCVP, OCSP, CRL, etc.)	**Product Name**	**Update Frequency**	**Has a Secondary?**

Audit Logging

Audit logs should meet the details required per agency policy (e.g., SP 800-53) and FICAM requirements.

Audit Log	**Log Location (Directory)**	**Timestamp Enabled?**	**Level of Detail Sufficient to Comply with Agency Requirements?**
PKI path validation log			
Physical access log			

IP Configuration

Note: If ATO has been completed, there is no need to fill in the Operational Functionality Worksheet/IP Conformance section.

All PACS components that require an IP address need to conform with the agency's IT policy on IP addresses.

	IPv4 or IPv6?	**Conforms with Agency's IT Policy?**
Server IP configuration		
Client IP configuration		
PACS component configuration		

PACS Hardware Locations

Use this section to verify alignment with agency policy and deployed reader configurations.

	Does the Inventory from General Information (Planned) Match the Reader Inventory (Deployed)?	**Meets Policy Requirements**	**Note Any Exceptions**	**Note Any Mitigations**
One-factor readers/Controlled areas	□			
Two-factor readers/Limited areas	□			
Three-factor readers/Exclusion areas	□			

Failure Mode Operations

How does the system behave when the revocation information source is offline?	
How does the PACS software (workstations) respond if the PACS server is offline or unavailable?	
How do the PACS components react if the server is offline or unavailable?	

Test Cases Worksheet

Worksheet directions: Enter information in the Notes fields as necessary.

Positive Test Cases

Test Case	**Test Card** Valid card	**Step #**	**Test Procedure** Purpose: Ability for ePACS to properly process valid credentials; may need to be repeated for every allowable credential type and issuing CA	**Notes**
PTC-1		1	Perform enrollment on every card type allowable by policy.	
PTC-1		1a	Verify PKI validation for each card enrolled by audit log inspection.	
PTC-1		1a1	Does the audit log trace the path to the Root CA?	
PTC-1		1a2	Does the audit log show the intermediate CA validation?	
PTC-1		2	Does the system capture unique identifiers as defined in policy?	
PTC-1		3	Assign access rights to enrolled card.	
PTC-1		4	Read card at PACS card reader.	
PTC-1		4a	Read card at single-factor reader.	
PTC-1		4b	Read card at two-factor reader.	
PTC-1		4c	Read card at three-factor reader.	
PTC-1		5	Was access granted as expected at each card reader?	
PTC-1		6	Did the ePACS log show access granted at each card reader?	
PTC-1		7	Do the timestamps of the card read align with the ePACS logs?	
PTC-1		8	Did the system perform real time certificate process at time of card read?	
PTC-1		8a	If yes, did the logs show processing of the appropriate certificate?	
PTC-1		8b	If no, ensure negative test cases are performed.	

Negative Test Cases

Test Case	**Test Card** Card contains a revoked content signer certificate	**Step #**	**Test Procedure** Purpose: Ability for ePACS to deny access of a card with a revoked content signer certificate	**Notes**
NTC-1		1	Enroll card with revoked content signer certificate.	
NTC-1		1a	System should not allow card to be enrolled.	
NTC-1		2	Enroll good version of card in system.	
NTC-1		3	Assign access rights to enrolled card.	
NTC-1		4	Read faulted card at single-factor reader.	
NTC-1		4a	System should not allow access.	
NTC-1		5	Do the timestamps of the card read align with the ePACS logs?	
NTC-1		6	Did the system perform real time certificate process at time of card read?	
NTC-1		6a	If yes, did the logs show processing of the appropriate certificate?	
NTC-1		6b	If no, notate the denial message from the ePACS logs.	
NTC-1		7	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	

Test Case	**Test Card** End entity certificates have expired (e.g., PIV Authentication, Card Authentication)	**Step #**	**Test Procedure** Purpose: ePACS recognizes when a card is expired and denies access	**Notes**
NTC-2		1	Enroll card in ePACS system.	
NTC-2		1a	System should not allow card to be enrolled.	
NTC-2		1b	If unable to enroll card prior to certificate expiration, PKI processing may need to be relaxed for this step.	
NTC-2		2	Assign access rights to enrolled card.	
NTC-2		3	If PKI processing was relaxed, ensure PKI processing is restored to baseline configuration.	
NTC-2		4	Read expired card at single-factor reader.	
NTC-2		4a	System should not allow access.	
NTC-2		5	Do the timestamps of the card read align with the ePACS logs?	
NTC-2		6	Did the system perform real time certificate process at time of card read?	
NTC-2		6a	If yes, did the logs show processing of the appropriate certificate?	
NTC-2		6b	If no, notate the denial message from the ePACS logs.	
NTC-2		7	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	
NTC-2		8	Repeat steps 4 through 7 for two- and three-factor readers.	

Test Case	**Test Card** Certificates have been revoked	**Step #**	**Test Procedure** Purpose: ePACS denies access to a revoked card	**Notes**
NTC-3		1	Enroll card in ePACS system.	
NTC-3		1a	System should not allow card to be enrolled.	
NTC-3		1b	If unable to enroll card prior to card revocation, PKI processing may need to be relaxed for this step.	
NTC-3		2	Assign access rights to enrolled card.	
NTC-3		3	If PKI processing was relaxed, ensure PKI processing is restored to baseline configuration.	
NTC-3		4	Read faulted card at single-factor reader.	
NTC-3		4a	System should not allow access.	
NTC-3		5	Do the timestamps of the card read align with the ePACS logs?	
NTC-3		6	Did the system perform real time certificate process at time of card read?	
NTC-3		6a	If yes, did the logs show processing of the appropriate certificate?	
NTC-3		6b	If no, notate the denial message from the ePACS logs.	
NTC-3		7	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	
NTC-3		8	Repeat steps 4 through 7 for two- and three-factor readers.	

Test Case	**Test Card** Card from unknown issuing CA	**Step #**	**Test Procedure** Purpose: ePACS only trusts card issued from known issuers	**Notes**
NTC-4		1	Enroll card in ePACS system.	
NTC-4		1a	System should not allow card to enroll from unknown issuer.	
NTC-4		2	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	

Test Case	**Test Card** Valid card	**Step #**	**Test Procedure** Purpose: Verify ePACS interaction with card PIN	**Notes**
NTC-5		1	Enroll card in ePACS system.	
NTC-5		2	Assign access rights to enrolled card.	
NTC-5		3	Insert card at two-factor reader.	
NTC-5		4	Enter incorrect PIN at card reader.	
NTC-5		4a	System should deny access.	
NTC-5		5	Insert card at two-factor reader.	
NTC-5		6	Enter correct PIN at card reader.	
NTC-5		6a	System should grant access.	
NTC-5		7	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	
NTC-5		8	Repeat steps 3 through 7 for three-factor reader.	

Test Case	**Test Card** Valid card	**Step #**	**Test Procedure** Purpose: ePACS recognizes when an intermediate CA or issuing CA is invalid	**Notes**
NTC-6		1	Load intentionally faulted Intermediate CA or Issuing CA path into the system.	
NTC-6		2	Enroll card in ePACS system.	
NTC-6		2a	System should not allow card to be enrolled	
NTC-6		3	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	

Test Case	**Test Card** Valid card	**Step #**	**Test Procedure** Purpose: ePACS is able to deny access on bad/incorrect fingerprint at reader	**Notes**
NTC-7		1	Enroll card in ePACS system.	
NTC-7		2	Assign access rights to enrolled card.	
NTC-7		3	Insert card at three-factor reader	
NTC-7		4	Enter correct PIN at card reader.	
NTC-7		5	Present non-enrolled finger (typically index finger is enrolled or can use another person's finger for this test).	
NTC-7		5a	System should deny access.	
NTC-7		6	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	

Test Case	**Test Card** Card with tampered biometric	**Step #**	**Test Procedure** Purpose: ePACS is able to recognize a card in which a biometric has been tampered or not signed with the appropriate certificate	**Notes**
NTC-8		1	Enroll card in ePACS system.	
NTC-8		2	Assign access rights to enrolled card.	
NTC-8		3	Insert card at three-factor reader.	
NTC-8		4	Enter correct PIN at card reader.	
NTC-8		5	Present fingerprint to reader.	
NTC-8		6	System should deny access.	
NTC-8		7	Verify all audit logs for ePACS and PKI processing to ensure level of detail meets agency requirements for all steps above.	

Validate

Click button to validate form

Recommendations

Recommendations

Recommendations

Recommendations

Additional Considerations Worksheet

Although these considerations are not formally part of this ePACS assessment, they can be helpful in ensuring operational redundancy and supporting an SSP and ATO.

Worksheet directions: Select checkboxes for items or options that pertain to your organization. Enter information in the provided field accordingly.

Does the policy or procedure outline what mitigation, countermeasures, or notifications/alarms are used for unauthorized access to physical spaces or ePACS software?	□
Are there any system interconnections with your ePACS, and if there are, how are those interconnections secured?	□
Is the ePACS configured to allow PIN to ePACS?	□
Does the ePACS utilize alternative biometrics not stored on the PIV card?	□
Does the audit log retention and archival plan align with the agency's records retention policy?	□
Are there additional systems connected to the ePACS (e.g., cameras, intrusion detection)?	□
Do those additional systems use the same time synchronization source?	□
Is the ePACS included in the agency's disaster recovery and continuity of operations plans?	□
Does the ePACS have sufficient backup power for all critical components?	□
Is the ePACS included in any preventive maintenance plans?	□
Does the agency have any policy or plans around authorization to the ePACS software and management of roles within?	□
Are there any training materials available to ePACS software users?	□
Is there an operation plan for system security escalation?	□
If ePACS or any system components are IPv4, is there a roadmap to migrate to IPv6 per M-21-07 and M-20-17?	□