JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road • Laurel, Maryland 20723-6099

AOS-17-0841
September 2017

# Identity, Credential, and Access Management (ICAM) Use Cases

## Version 1.0

Prepared by: Thomas Smith, The Johns Hopkins University Applied Physics Laboratory

Prepared for:
Department of Homeland Security Federal Emergency Management Agency
Washington, DC

This document was prepared under funding provided by the U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) (Contract Number N00024-13-D-6400; Task Order 0838, Task Number S8921, FEMA Identity, Credential and Access Management (ICAM) Modernization and State, Local, Tribal, Territorial (SLTT) Pilot Implementation). Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security or the Federal Emergency Management Agency.

The Johns Hopkins University Applied Physics Laboratory (JHU/APL) assumes no liability for this document's content or use thereof. This document does not constitute a standard, specification, or regulation. Additionally, JHU/APL does not endorse particular products or manufacturers. Trade and manufacturer's names may appear in this report only because they are considered essential to the objective of this document.

Principal Author: Thomas C. Smith
Contributing Authors: Dallas L. Pearson III (JHU/APL), Lauren B. Davis (JHU/APL)

The author would like to express his appreciation to the sponsor Mr. Craig Wilson.

*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.*

Please send comments to:

Mr. John Contestabile
Program Manager
JHU/APL
11100 Johns Hopkins Road
Laurel, MD  20723-6099
Phone: 443-220-8090
E-mail: John.Contestabile@jhuapl.edu

*This page intentionally left blank.*

# CONTENTS

*This page intentionally left blank.*

## FIGURES

Page

*This page intentionally left blank.*

# TABLES

## EXECUTIVE SUMMARY

This report describes twenty-two Identity, Credential, and Access Management (ICAM) use cases for Person (PE) and Non-Person Entities (NPEs). The Johns Hopkins University Applied Physics Laboratory (JHU/APL) identified and developed these use cases to provide details and customizations specifically tailored to address operational ICAM needs. This collection of process flows characterizes an ICAM focused subset of cybersecurity use cases, but they do not address the much larger and broader collection of security concerns including conformance, risk management, key management, enterprise governance, redress and recovery. As such they support any government or private sector organization (ORG) that is addressing ICAM as a critical aspect of its cybersecurity enhancement plan. This managing organization is referred to throughout this document using the ORG identifier.

The eighteen PE and NPE ICAM use cases covered in this document are based on the services framework and use cases defined by the Federal ICAM (FICAM) community (References 1, 2). The four Digital Policy Management (DPM) use cases presented are based on the DPM framework and use cases described in Reference 3. This combination of references provides substantial treatment of physical and logical access use cases for PEs but the coverage of NPEs is incomplete. This document addresses this gap by defining six new NPE use cases.

PEs are human credentialed cyberspace actors with a digital identity. PEs have numerous affiliations with organizations but this report identifies three discriminating categories: ***employee*** – works for and compensated by ORG, ***contractor*** – works for ORG under contract, and ***partner*** (PTR) – shares resources with ORG.

NPEs are non-human credentialed cyberspace actors with a digital identity. This report divides the NPE classification into Endpoint Devices (EPDs) and Authoritative Resources (ARs). NPEs join with Managed Zones (MZs) to define Protected Resources (PRs). This document identifies and describes the ICAM management, enforcement, and support service use cases for all of these NPEs and includes details that are critical to characterizing the enterprise and federated cybersecurity approaches, architectures, and technologies.

MZ are physically controlled structures such as sites, buildings, rooms, etc.; and logically controlled structures such as networks, subnets, etc. Text and binary information objects are termed artifacts, and like MZs they are PRs with metadata that characterize their identity, however they are not credentialed. The Logical Entity (LE) that controls the MZ or artifact provides the digital trust, confidentially, integrity and authenticity.

LEs are authoritative concepts like businesses, agencies, jurisdictions, and other organizations. Their credentials are typically use to provide trust, confidentially, integrity and authenticity.

This report also characterizes the supporting roles of PE system and process administrators and the PEs managing NPEs (i.e., the NPE Administrator), the PE or organization that purchased the NPE (i.e., the NPE Owner), the PE that is delegated responsibility by the owner for the NPE (i.e., the NPE Assignee), and the PE that simply uses the NPE (i.e., the NPE User). These supporting actors include employees and contractors of ORG and PTR organizations.

The premise of this report is that the ORG business model exposes its intellectual property and resource investments to personnel and devices that belong to both ORG and PTRs. The infrastructure and entity space (PE and NPE) that characterize these physical and cyber security concerns is fluid and this drives the ORG business use cases. The rapidly emerging mobility, virtualization and flexible working environment drivers have a significant impact on the ORG technical approaches and solutions. In contrast, the conceptual ICAM concerns and supporting use cases are inherently stable and provide a reasonable ICAM framework.

JHU/APL has developed an ICAM information model that spans and aligns PE and NPE use cases over enterprise, federated and hybrid architectures plus nine conceptual ICAM processes that describe both PE and NPE ICAM use cases in conjunction with four Digital Policy Management (DPM) use cases. These twenty-two ORG ICAM use cases are:

- ORG-01-PE: Establish, Maintain, and Control PE Digital Identity Record
- ORG-01-NPE: Establish, Maintain, and Control NPE Digital Identity Record
- ORG-02-PE: Establish, Maintain, and Control PE Credential
- ORG-02-NPE: Establish, Maintain, and Control NPE Credential
- ORG-03-PE: Provision and Deprovision PE Privileges
- ORG-03-NPE: Provision and Deprovision NPE Privileges
- ORG-04-PE: Provision and Deprovision PE Resource Access
- ORG-04-NPE: Provision and Deprovision NPE Resource Access
- ORG-05-PE: Authenticate PE for Access
- ORG-05-NPE: Authenticate NPE for Access
- ORG-06-PE: Authorize PE Access
- ORG-06-NPE: Authorize NPE Access
- ORG-07-PE: Secure PE Communication Channel with Public Key Infrastructure (PKI)
- ORG-07-NPE: Secure NPE Communication Channel with PKI
- ORG-08-PE: Secure PE Artifact with PKI
- ORG-08-NPE: Secure NPE Artifact with PKI
- ORG-09-PE: PE Monitoring and Reporting
- ORG-09-NPE: NPE Monitoring and Reporting

- ORG-01-DPM: Create and Maintain Digital Policy (DP) Content
- ORG-02-DPM: Manage Activated DPs
- ORG-03-DPM: Provide DPs for Access
- ORG-04-DPM: Import and Export Policies

These use cases address:

- management services – digital identity, credentialing and privilege management;
- enforcement services – authentication, authorization and access control; and
- support services – cryptography and governance.

*This page intentionally left blank.*

# 1. INTRODUCTION

## 1.1 Purpose

This report defines a set of Identity, Credential, and Access Management (ICAM) use cases that:

- Are based on published ICAM community use cases,
- Align with the Federal Identity, Credential, and Access Management (FICAM) services framework[1],
- Provide complete coverage of ICAM Person Entity (PE), Non-Person Entity (NPE) and Digital Policy Management (DPM) concerns,
- Identify a conceptual set of ICAM processes that span entities, and
- Incorporate many of the emerging ICAM concepts and developments.

This report also clarifies PE and NPE classifications with respect to ICAM processes and entity relationships and develops an ICAM information model that spans and aligns PE and NPE use cases over enterprise, federated and hybrid architectures.

## 1.2 Scope

These use cases support any government or private sector organization (ORG)[2] that is addressing or planning to address ICAM as a critical aspect of its cybersecurity enhancement plan. It is very important to note however, that these represent an ICAM focused subset of use cases that do not include the much larger and broader collection of cybersecurity concerns that cover conformance, risk management, key management, enterprise governance, redress and recovery.

The premise of this report is that the ORG business model exposes its intellectual property and resource investments to personnel and devices that belong to both ORG and business partners (PTRs). The infrastructure and entity space (PE and NPE) that characterize these physical and cyber security concerns is fluid and this drives the ORG business use cases. The rapidly emerging mobility, virtualization and flexible working environment drivers have a significant impact on the ORG technical approaches and solutions. In contrast, the conceptual ICAM concerns and supporting use cases are inherently stable and provide a reasonable ICAM framework.

JHU/APL has developed an ICAM information model that spans and aligns PE and NPE use cases over enterprise, federated and hybrid architectures, plus nine conceptual ICAM processes that describe both PE and NPE ICAM use cases in conjunction with four DPM use cases.

[1] References 1 and 2.

[2] The ORG identifier is used throughout this document to refer to this generic organizational context.

*This page intentionally left blank.*

# 2. APPROACH

- Research ICAM functions, services, and use cases that have been documented by the ICAM community.
- Assess the coverage of the documented use cases across all entity types. This includes looking at overlaps and gaps in coverage.
- Synthesize a single list of use cases that provides complete PE and NPE coverage.
- Where possible, derive use case details from the documented use cases.
- Create new use case details where there were gaps in coverage for the previously documented use cases.
- Provide a set of organizing principles for those use case details, including:
  - Mapping to the FICAM Services Framework
  - An ICAM Data Concept Model
  - A use case actor (i.e., entity) hierarchy
  - A common use case presentation format

*This page intentionally left blank.*

# 3. BACKGROUND

This section: characterizes entities, their relationships and discusses the complexities of incorporating entities in an enterprise; describes the types of authenticators and the various assurance level schemes; provides the context for understanding the diversity of PTR organizations and the FICAM services framework.

## 3.1 Entities

### 3.1.1 Person Entity

A PE is a credentialed human cyberspace actor with a digital identity. A comparison of this PE classification with NPE classifications is provided in Table 3-1.

PEs have numerous affiliations but this report identifies three major categories:

- **Employee** – this is an affiliation with their primary organization, that is the organization that provides compensation e.g., paycheck, health insurance, etc., like full time, part time, temporary, volunteer. From an ICAM perspective, retired and family affiliates can be included in this category. In this report your ORG is the primary organization.

- **Contractor** – this is an affiliation with ORG where PEs are employees of a PTR organization, but working for ORG via a contract with this PTR.

- **Partner** – this is an affiliation with ORG where ORG and the PTR organization have established a mutually beneficial working relationship allowing the PE to provide information and services during the course of doing business with ORG and similarly for ORG to provide information and services to the PTR.

### 3.1.2 Non-Person Entity

An NPE is a credentialed non-human cyberspace actor with a digital identity. Text and binary information objects are referred to as artifacts in this report.

From a basic cyber information-sharing perspective, as depicted in Figure 3-1, NPEs actively act in source, custodian, consumer, and connector roles during the dissemination of text-based and binary-based information artifacts.

- The ***source*** creates and authorizes the artifact.
- The ***custodian*** markets the artifact.
- The ***consumer*** employs the artifact.
- The ***connector*** transports the artifact.

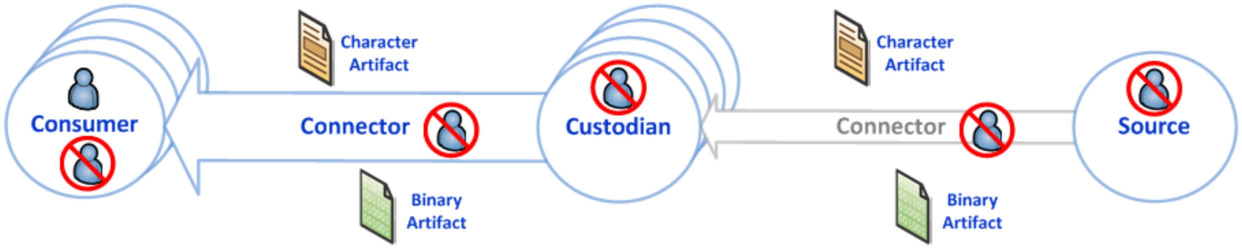


**Figure 3-1 Cyber Information Sharing Concept**

It is important to note the following roles and relationships:

- NPEs can exhibit connector, consumer, custodian, and source roles.
- An NPE can be both the source as well as the custodian of an artifact.
- An artifact always has a single source and it can have multiple custodians and multiple consumers.
- The artifact flow between the source and the custodian is limited in frequency and volume, providing the initial artifact and updates.
- The artifact flow direction is fixed, and the NPE consumer, custodian, and source roles are contextually dynamic (e.g., a custodian can be a consumer of another custodian).
- The flow is one-to-many. A source can support multiple custodians and a custodian can support multiple consumers.
- Custodians and sources are both artifact providers.

### 3.1.3 PE and NPE Characterizations

Entities are classified as PE or NPE. They include concrete (i.e., physically touchable) entities that require both physical and logical access control, and virtual (i.e., not physically touchable) entities that only require logical access control. All entities require a digital presence to perform in cyberspace that includes a unique digital representation and some assessment of the unique coupling of that representation to the attributing concrete or virtual entity.

- Identity management establishes the authoritative validity of the digital representation,
- Credential management establishes an entity’s digital proxy and the entity/proxy coupling and assessment mechanisms, and
- Access management exercises these elements to establish and enforce the access control policies.

Table 3-1 summarizes the taxonomy and characterization of the PE and NPE groupings used in this report.

### Table 3-1 PE and NPE Characterizations and Relationships

| ID | PE | PR | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | MZ | | NPE | | | | |
| | | | | EPD | AR | | | |
| | | | | | MP | | | LE |
| | | | | | MSP | MND | MSS | |
| **Access Control** | Physical and logical | Physical | Logical | Physical and logical | Physical and logical | Physical and logical | Logical | Logical |
| **Role** | Personnel | Structure | Structure | Access | Content | Infrastructure | Service | Authority |
| **Actors** | Users, privileged users, etc. | Sites, buildings, controlled areas, etc. | networks, subnets, etc. | Desktops, laptops, thin clients, tablets, smartphones, etc. | File, database, mail, chat, IM, audio, video, etc. servers, | Gateways, routers, switches, bridges, hubs, repeaters, modems, domain controllers, etc. | Web servers, web apps and applications including mail, chat, IM, video, etc. | Organizations including business, agencies, jurisdictions, groups, etc. |

AR – Authoritative Resource
EPD – EndPoint Device
ID – Identifier
IM – Instant Messaging
LE – Logical Entity
MND – Managed Network Device
MP – Managed Provider
MSP – Managed Service Provider
MSS – Managed Shared Service
MZ – Managed Zone
PR – Protected Resource

PEs represent themselves using their chosen identity and authenticate their claim to this identity using a credential. The authenticated PE is then authorized for physical or logical access by the appropriate PR access control policies within the authorizing resource's scope of control.

NPEs are non-human credentialed cyberspace actors with a digital identity. In this report NPEs are classified as Endpoint Devices (EPDs) and Authoritative Resources (ARs). Protected Resources (PRs) include NPEs and Managed Zones (MZs) as shown in Table 3-1.

An EPD is an internet-capable computing device on a Transmission Control Protocol/Internet Protocol (TCP/IP) network that is used by a PE to gain logical access to PRs within the ORG enterprise. The network connection for the EPD can be wired or wireless and the EPD logical access to the ORG enterprise can be local or remote to the physical location. EPDs include mobile devices, laptops, desktops, and other non-mobile devices that are used by persons to gain logical access to PRs. An EPD is concrete or virtual and acts as the access point that enables a PE to interact with a networked computing environment like the internet. Desktops, laptops, thin clients, tablets, smartphones, and wearable devices are examples of EPDs. EPDs include any object with internet access that collects and exchanges data with a PE, as an instance in the Internet of Things (IoT).

An AR is an NPE that provides authoritative services and information. ARs are subdivided into MPs and Logical Entities (LEs) and include organizations, devices, applications, and information objects that establish the network infrastructure, host operational capabilities, and provide internal and external access to and the representation of digital information.

A PR is a MZ or NPE that should be protected with Access Manager (AM) capabilities that are required to assess and enforce physical and logical access control security policies. This includes EPDs, Managed Providers (MPs) and LEs. MPs are classified in Table 3-1 as Managed Service Providers (MSPs), Managed Network Devices (MNDs), and Managed Shared Services (MSSs).

- An MSP is either concrete or virtual. It acts as a content provider for data repositories like files, databases, mail, chat, audio, video, and instant messages within the enterprise.

- An MND is either concrete or virtual. It is an infrastructure provider for networking capabilities that act as gateways, routers, switches, bridges, hubs, repeaters, modems, domain-naming systems, and domain controllers within the enterprise.

- MSSs are virtual. They provide web and application desktop, collaboration, information management, collection, and assessment services within the enterprise.

MZs are physically controlled structures like sites, buildings, rooms, etc., and logically controlled structures like networks, subnets etc. Text and binary information objects are artifacts and like MZs they are PRs with metadata that characterize their identity, however they are not credentialed. The LE that controls the MZ or artifact provides the digital trust, confidentially, integrity and authenticity.

LEs are virtual and represent logical authoritative concepts like businesses, agencies, jurisdictions, and other organizations. They typically use their credentials to provide trust, confidentially, integrity and authenticity.

NPEs typically authenticate with a Public Key Infrastructure (PKI) digital certificate over point-to-point connections using secure protocols within various Open Systems Interconnection (OSI) layers; for example using Transport Layer Security (TLS) and Virtual Private Network (VPN) protocols. The consumer access is regulated to the level and scope of the privileges authorized by the provider policies.

This document identifies and describes the ICAM management, enforcement, and support service use cases for all of these NPEs and includes the details that are critical to characterizing the enterprise and federated cybersecurity approaches, architectures, and technologies.

### 3.1.4 PE Relationships to NPEs

There are two controlling roles that either a PE or LE can have with respect to an NPE:

- **NPE Owner** – The person or organization that purchased the NPE and is legally responsible for paying the bill. The person can be an employee or contractor of ORG or PTR, and the organization can be ORG or a PTR.

- **NPE Assignee** – The person or organization that the NPE Owner delegates as the party responsible for the NPE. The person can be an employee or contractor of ORG or PTR, and the organization can be either ORG or a PTR.

There are two access roles that a PE can have with an NPE:

- **NPE Administrator** (or privileged user) – The person who has privileged access to configure and manage the NPE. This can only be an employee or contractor of ORG or PTR organization or agency that has been granted privileged access by ORG and agreed to by the NPE Owner or NPE Assignee.

- **NPE User** – The person who engages the operational capabilities of the NPE. This can only be an employee or contractor of ORG or PTR that has been granted usage by the NPE Owner or NPE Assignee.

## 3.2 Authenticators[3]

An authenticator authoritatively binds a digital identity to a PE or NPE. It is then used by that entity to authenticate their identity claim to a third party by demonstrating possession and control of the bound authenticator. During the authentication process, this entity-to-authenticator binding is established when the entity successfully applies one or more factors. Increasing the number of factors required by the authentication process improves the resulting confidence in the entity’s identity claim.

[3] Reference 3.

There are three authentication factors:

- *Something you know* – secret
- *Something you have* – concrete
- *Something you are* – biometric

The binding strength of multiple authentication factors is predicated on the uniqueness of their binding relationship and the ability of the individual to demonstrate exclusive possession and control of the authenticator to a verifier. Authenticators are physical models providing capabilities that incorporate these conceptual factors with specific binding mechanisms. Some authenticators are single factor while others support multiple factors. Simply employing different authenticators does not necessarily achieve multi-factor authentication. For example combining Look-up Secret and Out of Band authenticators provides single factor authentication – a more complex *something you have*; while combining Memorized Secret and Look-up Secret yields two-factor authentication – *something you know* and *something you have*.

The verifier is the entity that confirms the individual's identity by validating possession and control of one or two authenticators using an authentication protocol.

The types of authenticators are listed here with the factors that each supports:

- **Memorized Secret** – a memorized value that is chosen by the user. It should be sufficiently complex so it's impractical for an attacker to guess and methodically controlled so that it is not discovered. Providing the secret is a factor.
  ***Factor:*** *something you know*
- **Look-up Secret** – a table of multiple identifier/secret pairs that is possessed by the user and the verifier. The verifier prompts the user with the identifier(s) and the user responds with the secret(s). The table can be a physical card or an electronic record stored on a device. The table must be methodically controlled to protect the contents from discovery. Possessing the table is a factor.
  ***Factor:*** *something you have*
- **Out of Band (OOB)** – a physical device held by the user that is uniquely addressable and communicates securely with the verifier over a distinct secondary communications channel. The verifier prompts the user on the primary channel, the device displays a secret over the secondary channel and the user manually echoes that secret back to the verifier demonstrating passion and control of the device. Possessing the device is a factor.
  ***Factor:*** *something you have*

- **One Time Password (OTP)** – a physical device held by the user. Secrets are cryptographically and independently generated by the device and verifier and then compared by the verifier demonstrating that the user has possession and control of the device. The device and the verifier use a common symmetric cryptographic key and nonce to generate the shared secret. Possessing the device is a factor.
  ***Factor***: *something you have*

  When the device has a keypad it can also prompt the user for a Memorized Secret. Providing the secret is an additional factor.
  ***Factor:*** *something you know*
- **Cryptographic (Crypto)** – a symmetric or asymmetric cryptographic key stored in a device (CryptoD) and used in an authentication protocol to demonstrate possession and control of the authenticator (e.g., sign and return a verifier message). The cryptographic key may be embedded in secure software (CryptoSS) or hardware (CryptoSH) container within the device. Possessing the device is a factor.
  ***Type:*** CryptoD
  ***Factor:*** *something you have*

  When the cryptographic device is in a tablet, smartphone or smartcard with secure Crypto (CryptoSS, CryptoSH) that must be unlocked with a Memorized Secret to access the cryptographic key. Unlocking the secure Crypto with a secret is an additional factor.
  ***Factor*****:** *something you know*

  When the cryptographic device is in a tablet, smartphone or smartcard with secure Crypto (CryptoSS, CryptoSH) that must be unlocked with a biometric to access to the cryptographic key. Unlocking the secure Crypto with a biometric is an additional factor.
  ***Factor*****:** *something you are*

## 3.3 Assurance Levels

### 3.3.1 Office of Management and Budget (OMB) M-04-04

The M-04-04 2003 Office of Management and Budget (OMB) memorandum[4] established four PE authentication Levels of Assurance (LOAs) that apply to Federal systems. The general criteria for the LOA steps are summarized in Table 3-2.

**Table 3-2 M-04-04 Levels Of Assurance (LOA)**

| Requirement | LOA1 | LOA2 | LOA3 | LOA4 |
|---|---|---|---|---|
| **Binding Confidence** | None | Some | High | Very High |
| **Identity Proofing** | Self-asserted | Consistent | Verified | In-Person<br>Verified<br>Collect Biometric |
| **Authenticator Protection** | Policy | Policy | Cryptographic | Hardware Cryptographic |
| **Authentication Protocol** | Not Required | Secure | Cryptographic | Cryptographic |
| **Factors** | Single | Single | Multi | Multi |
| **Man-in-the-Middle Resistant** | Not Required | Not Required | Required | Required |
| **Verifier Impersonation Resistant** | Not Required | Not Required | Required | Required |
| **Verifier Compromise Resistant** | Not Required | Not Required | Required | Required |
| **Replay Resistant** | Not Required | Required | Required | Required |

[4] Reference 5.

### 3.3.2 National Institute of Standards and Technology Digital Identity Guidelines

The National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines for Federal systems. This 2017 special publication (SP-800-63-3[5]) provides technical requirements for Federal agencies implementing digital identity services with guidelines that cover remote authentication for users interacting with government IT systems over open networks.

The updated electronic authentication guidelines address the concern that the LOA approach does not provide implementers with adequate flexibility to achieve a mission-sensitive solution. The new publication provides a risk-based approach that identifies three assurance level components that can be used independently and combined in any fashion to meet mission needs.

#### *3.3.2.1 Identity Assurance Level*

Identity Assurance Level (IAL) covers the identity proofing process and the binding between an authenticator and the identity record for a specific PE.

**Table 3-3 Identity Assurance Levels (IALs)[6]**

| Requirement | IAL1 | IAL2 | IAL3 |
|---|---|---|---|
| **Presence** | Not Required | Remote<br>or<br>In-Person | In-Person |
| **Resolve to Real Identity** | Not Required | Required | Required |
| **Collect Evidence** | Not Required | 2-STRONG<br>or<br>1-STRONG +<br>1-FAIR+1-WEAK | 2-SUPERIOR<br>or<br>1-SUPERIOR+2-STRONG<br>or<br>2-STRONG+1-FAIR |
| **Validate Evidence** | Not Required | Each piece at evidence strength with 1 third party validation | Each piece at evidence strength with 1 third party validation |
| **Verify Claim** | Not Required | STRONG | SUPERIOR |
| **Address of Record** | Not Required | Verified by Enrollment Code | Verified by Enrollment Code |
| **Collect Biometric** | Not Required | Optional | Required |
| **Security Controls [SP800-53 or equivalent]** | Not Required | Moderate Baseline | High Baseline |

[5] Reference 6.

[6] Reference 7, UNACCEPTABLE, WEAK, FAIR, STRONG and SEPERIOR strength criteria are described in detail in this reference.

### *3.3.2.2 Authenticator Assurance Level*

Authenticator Assurance Level (AAL) covers the PE authentication process.

**Table 3-4 Authenticator Assurance Levels (AALs)**[7]

| Requirement | AAL1 | AAL2 | AAL3 |
|---|---|---|---|
| **Authenticator** | any | 2-factor | 2-factor Cryptographic Device |
| **Verification [FIPS 140]** | *verifiers* - Level 1 | *authenticators* - Level 1<br>*verifiers* - Level 1 | *authenticators* - Level 2 multi-factor with Level 3 physical security<br>*verifiers* - Level 1 software crypto device |
| **Reauthentication** | 30 days | 12 hours or<br>30 min of inactivity<br>1-factor | 12 hours or<br>15 min of inactivity<br>2-factor |
| **Security Controls [SP800-53 or equivalent]** | Low Baseline | Moderate Baseline | High Baseline |
| **Man-in-the-Middle Resistant** | Required | Required | Required |
| **Verifier Impersonation Resistant** | Not Required | Not Required | Required |
| **Verifier Compromise Resistant** | Not Required | Not Required | Required |
| **Replay Resistant** | Not Required | Required | Required |
| **Authentication Intent** | Not Required | Recommend | Required |

[7] Reference 3.

#### *3.3.2.3 Federation Assurance Level*

Federation Assurance Level (FAL) covers the assertion protocol utilized in a federated environment to communicate PE authentication and attribute information between ORG and PTRs.

- Consumer – sends an entity identity request, then receives and processes the assertion about the entity.

- Provider – manages entity identities and responds to identity authentication and attribute request.

**Table 3-5 Federation Assurance Levels (FALs)[8]**

| Requirement | FAL1 | FAL2 | FAL2 |
|---|---|---|---|
| **Assertion Type** | Bearer | Bearer | Holder of Key |
| **Signed By** | Provider | Provider | Provider |
| **Encrypted For** | Not Required | Consumer | Consumer |

### 3.3.3 OMB LOA Alignment with NIST Assertion Levels

The NIST assertion levels[9] update the electronic authentication guidelines to provide implementers with adequate flexibility to achieve a risk-based mission-sensitive solution. It also provides a mapping of these three new assurance level components xAL (i.e., IAL, AAL and FAL) to the standard OMB LOA. This alignment facilitates the balancing of LOA system requirements with the xAL criteria tailored for operational needs and legacy investments. This alignment is shown in Table 3-6.

**Table 3-6 LOA Alignment with Assertion Levels**

| OMB M-04-04 | IAL | AAL | FAL |
|---|---|---|---|
| **LOA1** | 1 | 1, 2 or 3 | 1, 2 or 3 |
| **LOA2** | 1 or 2 | 2 or 3 | 2 or 3 |
| **LOA3** | 1 or 2 | 2 or 3 | 2 or 3 |
| **LOA4** | 1, 2 or 3 | 3 | 3 |

## 3.4 Partners

PTRs have established a mutually beneficial working relationship with ORG that enables the controlled exchange of information and services during the course of doing business. The following PTR communities can be included:

- **Federal Government** that includes Federal departments and agencies.

[8] Reference 4.

[9] References 6, 7, 3, and 4

- **State, Local, Tribal and Territorial (SLTT) Governments,** including all 50 states and the District of Columbia, the Regional Consortium Coordinating Council, recognized local jurisdictions within the Unites States, and the governing entities for the many recognized tribal governments and communities across the United States.

- **Foreign Partners** that belong to one or more cross-border sharing communities or consortia teams.

- **Private Sector** including academic and commercial.

## 3.5 Endpoint Device

An EPD is an internet-capable computing device on a TCP/IP network that is used by a person to gain logical access to protected resources within the ORG enterprise. The network connection for the EPD can be wired or wireless and the EPD logical access to the ORG enterprise can be local or remote to the physical location. The EPD classification includes mobile devices, laptops, desktops, and other non-mobile devices that are used by persons to gain logical access to protected resources.

### 3.5.1 Person and Organization Relationships to EPDs

As shown in Table 3-7, the four NPE roles with respect to EPDs can be filled by six combinations of persons and organizations, where the organizations are characterized as either ORG or PTRs, and the persons are the personnel (employees, contractors, etc.) of these organizations. The group concept is a logical aggregation of personnel that is formed by the owner for the explicit purpose of sharing an EPD among multiple users, i.e., the members of the group. In Table 3-7**,** the group assignee indicates that both the use and responsibility of the EPD are shared, while only one PE can use it at a time.

**Table 3-7 Variations of EPD Affiliation Roles**

| Variation | NPE Owner | NPE Assignee | NPE Admin | NPE User |
|---|---|---|---|---|
| ORG User | ORG | PE | PE | PE |
| ORG Group | ORG | Group | PE | PE |
| ORG Personal | PE | PE | PE | PE |
| PTR User | PTR | PE | PE | PE |
| PTR Group | PTR | Group | PE | PE |
| PTR Personal | PE | PE | PE | PE |

- **ORG User:** ORG decides to enable logical access to ORG protected resources by purchasing an EPD and assigning it directly to an employee or contractor that needs access. In this case, ORG is the NPE Owner, and the employee or contractor is both the NPE Assignee and User.

- **ORG Group:** ORG decides to enable logical access to ORG protected resources by purchasing an EPD and assigning it to a sub-organization that shares the EPD with its members as a multi-user device. In this case ORG is the NPE Owner, the sub-organization is the NPE Assignee, and the employee or contractor that is currently operating the EPD is the User.

- **ORG Personal:** ORG decides to enable logical access to ORG protected resources by allowing employees and contractors to use their personal EPD. In this case the employee or contractor is the NPE Owner, Assignee, and User.

- **PTR User:** ORG decides to enable logical access to ORG protected resources by accepting PTR Owned and Assigned EPDs that are currently being used by a PTR employee or contractor. In this case the PTR organization is the NPE Owner; the Assignee and User are the PTR employee or contractor that is currently operating the EPD.

- **PTR Group:** ORG decides to enable logical access to ORG protected resources by accepting PTR Owned EPDs that are assigned to PTR sub-organizations as a multi-user device and currently being used by a PTR employee or contractor of that sub-organization. In this case the PTR organization is the NPE Owner, the PTR sub-organization is the NPE Assignee, and the employee or contractor of that sub-organization that is currently operating the EPD is the User.

- **PTR Personal:** ORG decides to enable logical access to ORG protected resources by allowing PTR employees and contractors to use their personal EPD. In this case the PTR employee or contractor is the NPE Owner, Assignee, and User.

### 3.5.2 Business and Personal Enablement Models

The software and hardware components of the EPD can be activated or deactivated to protect the device and the resources it contains. The criteria for these EPD protections and capabilities are established by the NPE Owner and delegated assignee or group of assignees. The assignee is responsible for the control and enablement, and can delegate portions of that concern to the users.

ORG is solely responsible for the management and control of EPD access to the ORG enterprise PRs and the enforcement of security controls for the ORG information in transit with the EPD and at rest on the EPD.

As shown in Figure 3-2, an EPD can be owned by ORG, a PTR organization, or a person. Within the context of these ownership/enablement models, ORG is the EPD corporate owner and all non-ORG owners (PTR, private and person) are grouped as personal. In Figure 3-2, blue represents ORG enablement and yellow represents personal and PTR organization enablement.

The Corporate-Owned, Business Only (COBO); Corporate-Owned, Personally Enabled (COPE); and Bring Your Own Device (BYOD) concepts are presented elsewhere (Reference 9) and (Reference 10). The concept of Personally Owned, Business Applied (POBA) is introduced to balance the COBO business enablement. In COBO, the corporate-owned EPD has full business enablement whereas in POBA the personally owned EPD has no business enablement. Figure 3-2 shows business and personal ownership as poles with non-owner enablement granted by the owner. COBO is shown as a corporate-only blue dot and POBA as a personal-only yellow dot with COPE supporting corporate-granted personal enablement and BYOD supporting personally granted corporate enablement.

- **COBO** (Corporate-Owned, Business Only) – ORG owns and controls the EPD, applications and access to business resources, services and information; employee and contractor usage is restricted to clearly defined business purposes, and the user is not authorized to customize the EPD in any way for personal use. This applies to ORG-owned devices.

- **COPE** (Corporate-Owned, Personally Enabled) – ORG owns and controls the EPD, applications and access to business resources, services, and information but allows the employees and contractors to use the device for non-business purposes, and the user may be authorized to customize the EPD personal use. This applies to ORG-owned devices.

- **POBA** (Personally Owned, Business Applied) – the ORG or PTR employee or contractor owns and controls the device, applications, and information availability; ORG controls access to their business resources, services, and information. This applies to both personal (ORG and PTR) and PTR-organization-owned devices.

- **BYOD** (Bring Your Own Device) – the person (ORG and PTR) or PTR organization owns and controls the device, applications, and information availability and chooses to install one or more business applications; ORG controls access to their business resources, services, and information. This applies to both personal (ORG and PTR) and PTR-organization-owned devices.

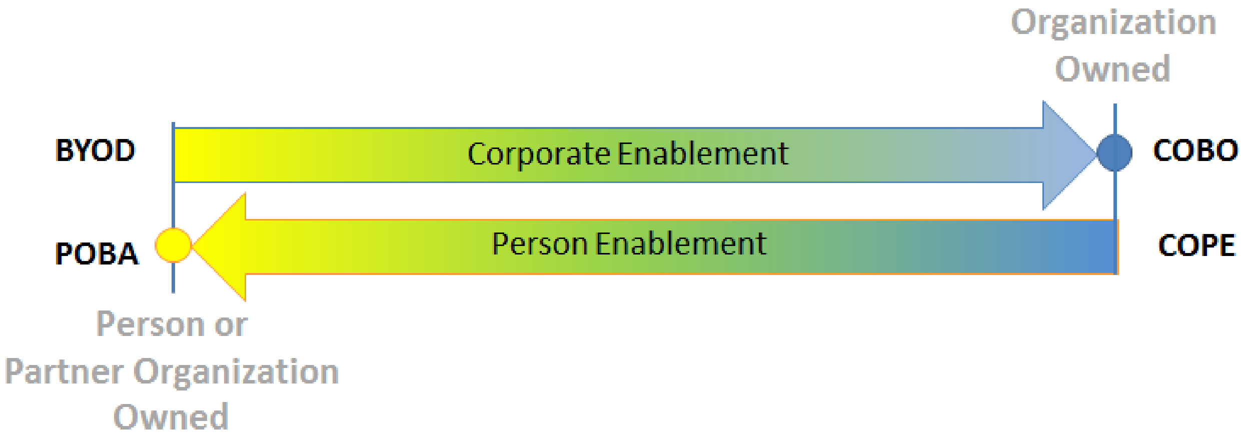


**Figure 3-2 Corporate and Personal Enablement of ORG-, PTR-and PE-owned EPDs**

### 3.5.3 Security

NIST identifies six mobile EPD security characteristics and provides alignment with the controls from the NIST Cybersecurity Framework (Reference 11), the NIST Security and Privacy

Controls for Federal Information Systems and Organizations (Reference 12), the ISO and International Electrotechnical Commission (IEC) Information Technology – Security Techniques – Code of Practice for Information Security Management (Reference 13), and the Center for Internet Security's Critical Security Controls for Effective Cyber Defense (Reference 14). These also align with the Federal Chief Information Officer (CIO) Council (Reference 9) security concerns. The EPD security characteristics that NIST identifies are:

**Data Protection**

- Protected Storage: device encryption, secure containers, trusted key storage, hardware security modules, remote wipe
- Protected Communications: VPN including per-App VPN, encrypted/signed email (e.g., Secure/Multipurpose Internet Mail Extensions [S/MIME]), Short Message Service (SMS)
- Data Protection in Process: encrypted memory, protected execution environments

**Data Isolation**

- Virtualization, sandboxing, memory isolation, trusted execution, device resource management, data flow control, data tagging, baseband isolation
- Device integrity
- Baseband integrity checks, application black/whitelisting
- Device integrity checks: boot validation, application verification, verified application and operating system (OS) updates, trusted integrity reports, policy integrity verification

**Monitoring**

- Canned reports and ad hoc queries, auditing and logging, anomalous behavior detection, compliance checks, asset management, root and jailbreak detection, geo-fencing

**Identity and Authorization**

- PE: local user authentication to applications, local user authentication to device, remote user authentication, user provisioning and enrollment, implementation of user roles for authorization, user credential and authenticator storage and use
- EPD: remote device authentication, implementation of device roles for authorization, device credential and authenticator storage and use, device provisioning and enrollment

**Privacy Protection**

- User informed consent, user privacy notification, data monitoring minimization

The ICAM EPD use cases that are presented in this document align with the NIST Identity and Authorization EPD characterization and the Monitoring Auditing and Logging characterizations listed above in this section. The remainder of the security characterizations that NIST identifies are out of scope.

### 3.5.4 Enterprise Mobility Management

Gartner (Reference 15) introduced the Enterprise Mobility Management (EMM) concept in response to the focus shift in the market from managing devices to managing apps, data, and connectivity. EMM is a consolidation of EPD management, EPD application management, EPD content management, EPD security management, EPD identity management, and capabilities that facilitate the integration of an EPD with an existing enterprise infrastructure. These are also identified as critical management concerns by the Federal CIO Council (Reference 9) and NIST (Reference 16). These EMM capabilities support corporate management of remote access, workplace isolation, enterprise app stores, policy enforcement, and other security needs (Reference 17). EMM is emerging as a unifying approach for managing mobile and traditional EPDs (Reference 15). This is driven by device ownership and availability, the coexistence of personal and business activities, web availability, the need for access to remote and multiple sites, and the rise in thin client/server side applications. EMM also presents a more efficient workflow than client management tool imaging techniques and is predicted to be the prevalent management tool within the next two years (Reference 15). EMM is transforming into a unified endpoint management (UEM) approach that provides a single policy definition point for all EPDs (Reference 18).

### 3.5.5 Platforms

Vendors have also designed ICAM and security capabilities into the core OS and hardware. This support is vendor dependent but includes biometrics, OS security updates, integrity protection, kernel security, app privilege and data isolation, encryption and access control, app updates, and secure browsing (Reference 17).

A notional representation of an EPD is shown in Figure 3-3. It offers an EPD containing foundational hardware and firmware; an OS; a general set of component hardware and drivers; vendor supplied software; and a set of capabilities that addresses the basic operational concern of providing a unified workspace (Reference 19) containing Management, Virtual Desktop, File Sharing and Synchronization and Support. This EPD is an active participant in establishing and maintaining a coherent PE and NPE ICAM context within the enterprise.

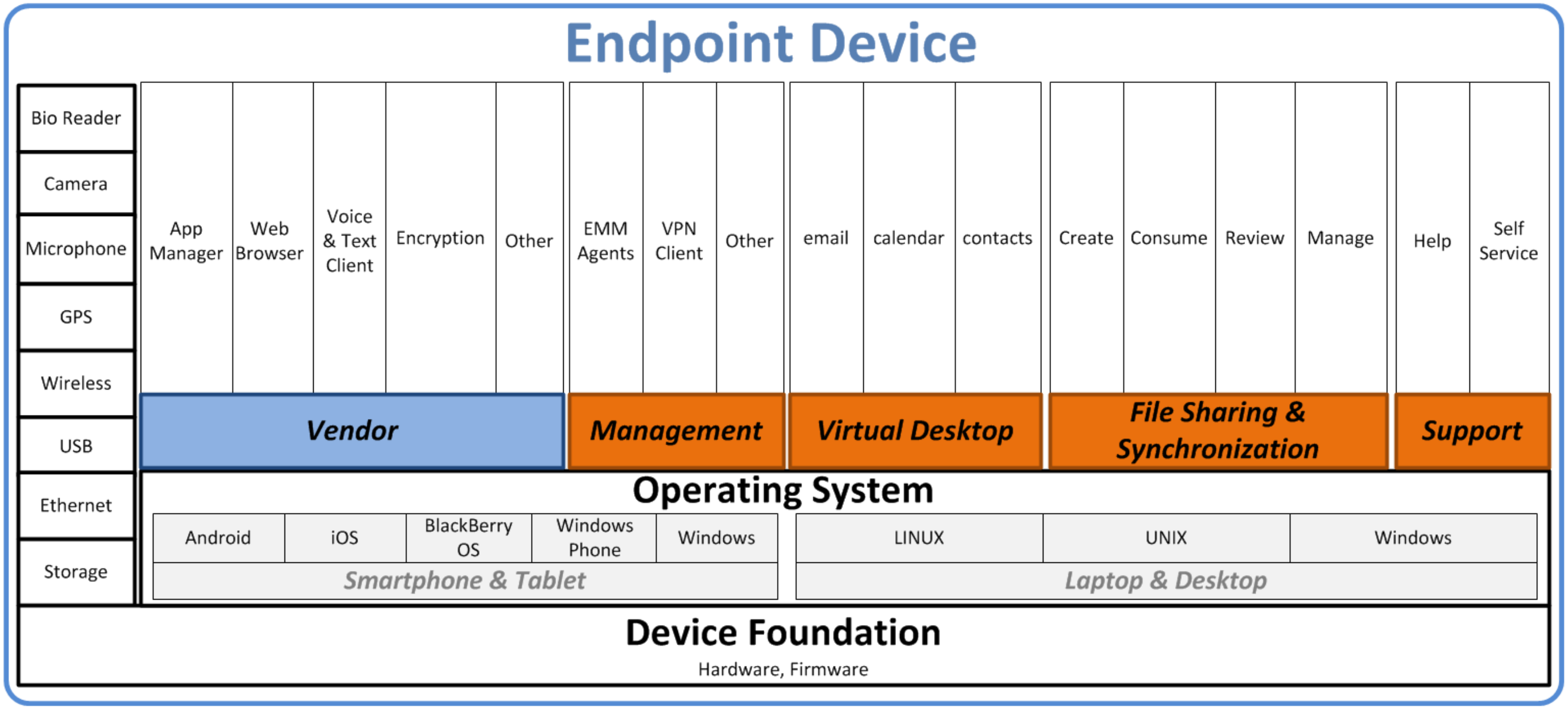


**Figure 3-3 Notional Endpoint Device**

### 3.5.6 EMM and Federation

Organizations (e.g., ORG) typically handle ICAM for enterprise EPDs using an EMM solution as recommended by NIST (Reference 16). This approach enrolls all EPDs into the centralized EMM and is applied to all corporate, PTR, and personally owned EPDs that require enterprise access. The ICAM activities in the enrollment action are issuing the EPD with a trusted digital credential, gathering EPD identity attributes and establishing the Identity Record, Credential Profile and Account Profile (see Figure 4-2) for each enrolled EPD. PTRs have already done this with the EPDs that they own and manage in their enterprise. Federated identity allows an organization to leverage these remote PTR ICAM capabilities but requires that each PTR have Identity Provider (IdP) authentication and attribute retrieval services. It also requires that ORG establish a mutual trust agreement with all participating PTR IdPs and Service Providers (SPs).

## 3.6 ICAM Functions

The ICAM capabilities of an organization are implemented with people, processes, and technologies and are comprised of the functions identified in References 1 and 2. These functions are listed in Figure 3-4 and described in Appendix A. The allocation of each function to the ORG enterprise and ORG federation support for PTRs is indicated by color. Use cases for the Enterprise Governance, Redress, Recovery and Key Management support functions are not provided.

`

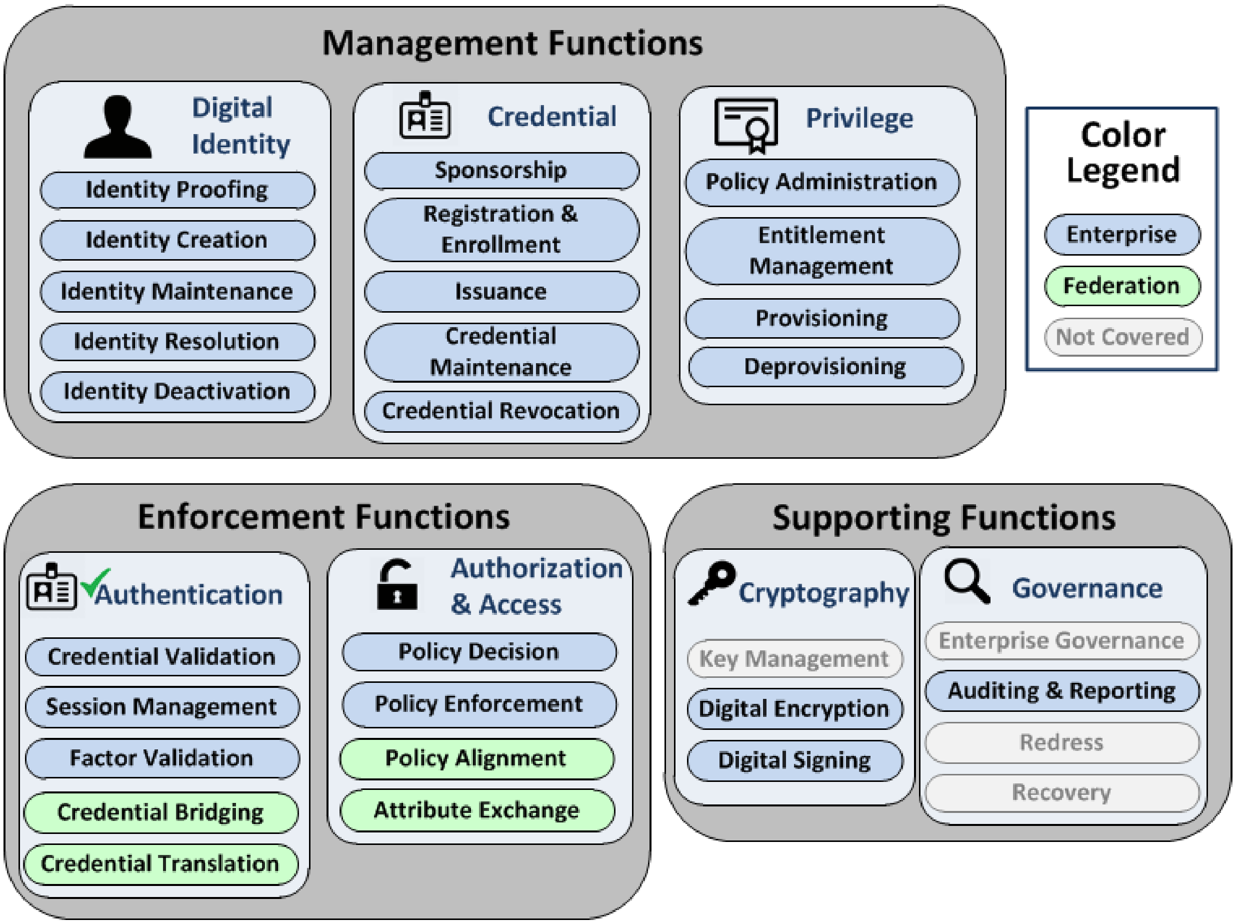


**Figure 3-4 ICAM Functions Allocated to ORG and PTR Systems**[10]

[10] Derived from References 1 and 2.

## 3.7 Logical Access Control Models[11]

The object oriented computer programming paradigm defines early and late binding mechanisms to differentiate when an identifier's object type is determined.

- In early or ***static binding*** identifier types are fixed at implementation time providing monomorphic execution.

- In late or ***dynamic binding*** identifier types are determined at runtime providing polymorphic execution.

Similarly, the early and late application of access control policies at decision (execution) time can be monomorphic or polymorphic depending on the implemented access control approach.

There are three prevailing approaches for controlling access in accordance with a policy:

- Identity-Based Access Control (IBAC),
- Role-Based Access Control (RBAC), and
- Attribute-Based Access Control (ABAC).

IBAC provides static (monomorphic) PR access control by entity identity. It captures the SP access control policies for each Account as Account Policy declared lists of permit or deny Resource Privileges. This Access Control List (ACL) is created, maintained, and controlled by the SP administrator. The SP administrator interprets and applies the appropriate access control policies to each account based on the identity and Access Profile of the Account owner. When a PE successfully authenticates to access his Account, the declared Resource Privileges for that account apply.

RBAC provides static (monomorphic) PR access by entity category. It captures the SP access control policies as Privilege Policy declared definitions that identify the business or application role and enumerate the permit or deny Resource Privileges for that role. These roles are created, maintained, and controlled by the SP administrator. The SP administrator establishes the role semantics, IDs, and interprets the access control policies to assign the appropriate Resource Privileges to that role. This establishes each role as a proxy for a logical aggregation of Resource Privileges. The IdP then assigns one or more of these roles to the Authorization Profile of each entity. When an entity successfully authenticates to access their Account, the Account Policy compares the Authentication Profile roles to the identified Privilege Policy roles and applies to the Account the declared Resource Privileges of each role that aligns.

ABAC provides dynamic (polymorphic) PR access by Digital Policy (DP) evaluation of entity, authentication, resource, and environment attributes. It captures the SP access control policies as Privilege Policies that are declared policy definitions designed to dynamically establish the set of applicable policies and ultimately the permit or deny Resource Privileges for the Account. These DPs are created, maintained, and controlled by the SP administrator. When an entity successfully

[11] These descriptions are in terms defined in Section 4-4 ICAM Data Concept Model.

authenticates to access their Account, the Account Policy interprets the identified entity authentication, Authorization Profiles, Resource Profile, and Environment attribute states and applies the derived Resource Privileges to that account.

# 4. ICAM USE CASES

This section identifies and describes the twenty-two ICAM use cases that:

- Are based on published ICAM community use cases,
- Align with the FICAM services framework and provide complete coverage of ICAM PE, NPE and DPM concerns,
- Identify a conceptual set of ICAM process flows that span entities, and
- Incorporate many of the emerging ICAM concepts and developments.

The eighteen use cases that are specific to either PEs (nine use cases) or NPEs (nine use cases) are based on the services framework and use cases defined by the FICAM community (Reference 1, 2). The four DPM use cases are based on the DPM framework and use cases described in Reference 3. This combination of references provides substantial treatment of physical and logical access use cases for PEs but the coverage of NPEs is incomplete. This document addresses this gap by defining six new NPE use cases.

This collection of process flows characterize an ICAM focused subset of cybersecurity use cases, but they do not address the much larger and broader collection of security concerns including conformance, risk management, key management, enterprise governance, redress and recovery. As such they support any government or private sector organization that is addressing ICAM as a critical aspect of their cybersecurity enhancement plan. This managing organization is referred to throughout this document using the ORG identifier.

This section also presents an ICAM information model that spans and aligns PE and NPE use cases over enterprise, federated and hybrid architectures.

## 4.1 ICAM Use Cases from References

Thirty-eight use cases were identified in three reference documents. The FICAM Roadmap (Reference 1) includes eleven ICAM use cases. The General Services Administration (GSA) FICAM Enterprise Architecture Use Cases (Reference 2) includes twenty. The Digital Policy Management Framework (DPMF) for Attribute-Based Access Control (ABAC) report (Reference 3) includes seven DPM use cases.

The use cases from the three references are listed in the following subsections. JHU/APL added ID numbers that were not in the original documents so each ORG ICAM use case could be mapped to the sources.

This report consolidates the thirty-eight referenced ICAM use case into twenty-two: nine PE, nine NPE and four DPM. Six of the nine NPE use cases that are developed in this report are not covered by these three references.

### 4.1.1 FICAM Use Cases

The FICAM Roadmap (Reference 1) describes a total of eleven ICAM use cases, which are listed below.

- FICAM-UC-01: Create and Maintain Digital Identity Record for Internal User
- FICAM-UC-02: Create and Maintain Digital Identity Record for External User
- FICAM-UC-03: Perform Background Investigation for Federal Applicant
- FICAM-UC-04: Create, Issue, and Maintain Personal Identity Verification (PIV) Card
- FICAM-UC-05: Create, Issue, and Maintain PKI Credential
- FICAM-UC-06: Create, Issue, and Maintain Password Token
- FICAM-UC-07: Provision and Deprovision PE Account for an Application
- FICAM-UC-08: Grant Physical Access to Employee or Contractor
- FICAM-UC-09: Grant Visitor or Local Access to Federally-Controlled Facility or Site
- FICAM-UC-10: Grant Logical Access
- FICAM-UC-11: Secure Document or Communication with PKI

GSA describes a total of twenty additional ICAM use cases for FICAM (Reference 20), which are listed below.

- GSA-UC-01: Create and Maintain an Identity
- GSA-UC-02: Proof an Identity at LOA 2
- GSA-UC-03: Proof an Identity at LOA 3
- GSA-UC-04: Proof an Identity at LOA 4
- GSA-UC-05: Resolve an Identity Internal to an Agency
- GSA-UC-06: Create and Issue LOA 2 Credential
- GSA-UC-07: Create and Issue LOA 3 Credential
- GSA-UC-08: Create and Issue LOA 4 Credential
- GSA-UC-09: Create and Issue a Derived PIV

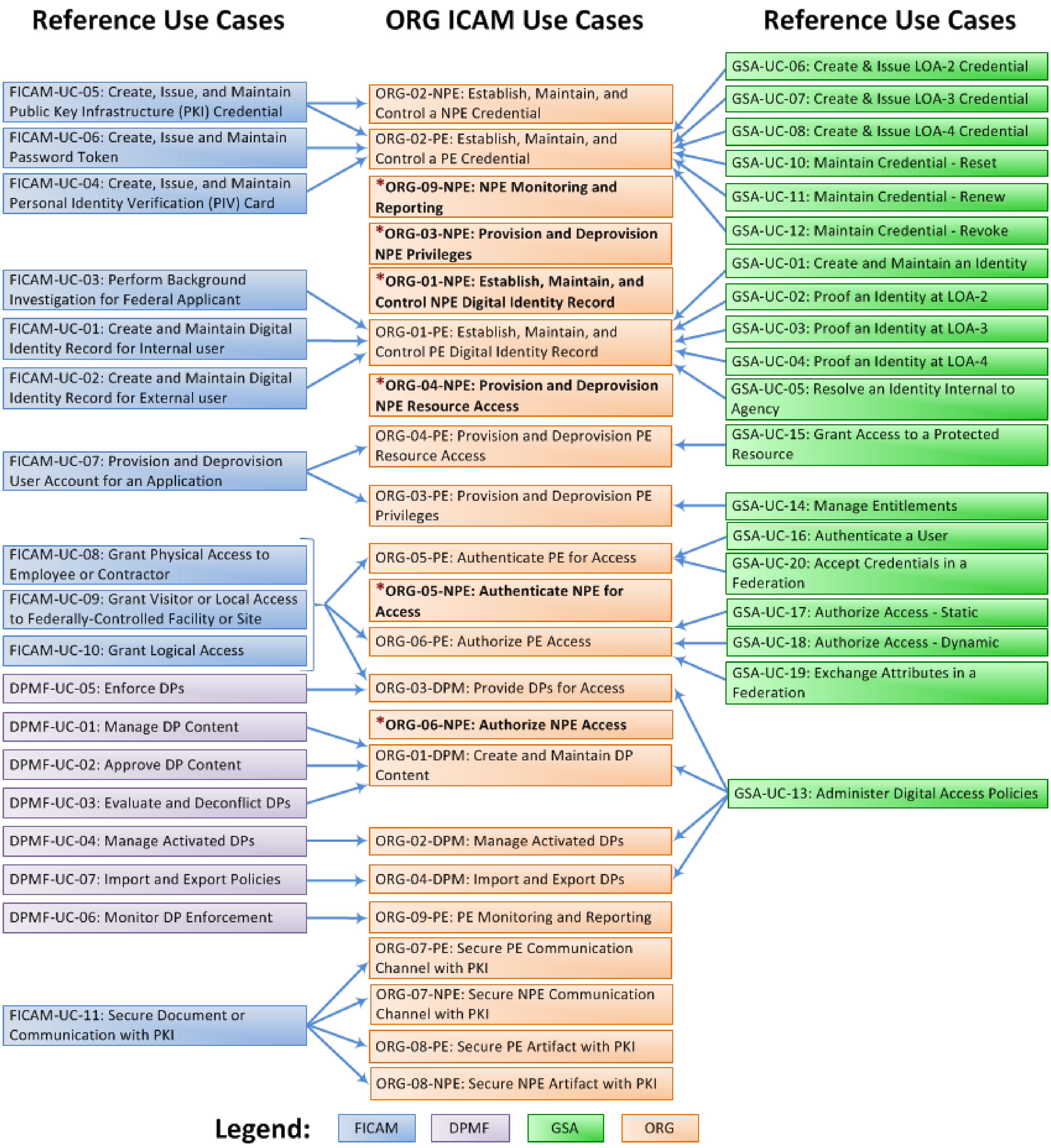
- GSA-UC-10: Maintain Credential – Reset
- GSA-UC-11: Maintain Credential – Renew
- GSA-UC-12: Maintain Credential – Revoke
- GSA-UC-13: Administer Digital Access Policies
- GSA-UC-14: Manage Entitlements
- GSA-UC-15: Grant Access to a Protected Resource
- GSA-UC-16: Authenticate a User
- GSA-UC-17: Authorize Access – Static
- GSA-UC-18: Authorize Access – Dynamic
- GSA-UC-19: Exchange Attributes in a Federation
- GSA-UC-20: Accept Credentials in a Federation

### 4.1.2 DPMF Use Cases

The ABAC DPMF report (Reference 3) describes a total of seven DPM use cases, which are listed below. All seven use cases are applicable to ORG ICAM solutions that implement an ABAC approach.

- DPMF-UC-01: Manage DP Content
- DPMF-UC-02: Approve DP Content
- DPMF-UC-03: Evaluate and Deconflict DPs
- DPMF-UC-04: Manage Activated DPs
- DPMF-UC-05: Enforce DPs
- DPMF-UC-06: Monitor DP Enforcement
- DPMF-UC-07: Import and Export Policies

Figure 4-1 maps the ORG ICAM use cases to the applicable FICAM, GSA and DPMF use cases. It is apparent that the ORG ICAM use cases consolidate the referenced use cases into nine PE, nine NPE and four DPM focused activities. Section 4.1 provides details on how many of these use cases are supported by multiple flows.


Reference Use Cases
ORG ICAM Use Cases
Reference Use Cases
FICAM-UC-05: Create, Issue, and Maintain Public Key Infrastructure (PKI) Credential
FICAM-UC-06: Create, Issue and Maintain Password Token
FICAM-UC-04: Create, Issue, and Maintain Personal Identity Verification (PIV) Card
FICAM-UC-03: Perform Background Investigation for Federal Applicant
FICAM-UC-01: Create and Maintain Digital Identity Record for Internal user
FICAM-UC-02: Create and Maintain Digital Identity Record for External user
FICAM-UC-07: Provision and Deprovision User Account for an Application
FICAM-UC-08: Grant Physical Access to Employee or Contractor
FICAM-UC-09: Grant Visitor or Local Access to Federally-Controlled Facility or Site
FICAM-UC-10: Grant Logical Access
DPMF-UC-05: Enforce DPs
DPMF-UC-01: Manage DP Content
DPMF-UC-02: Approve DP Content
DPMF-UC-03: Evaluate and Deconflict DPs
DPMF-UC-04: Manage Activated DPs
DPMF-UC-07: Import and Export Policies
DPMF-UC-06: Monitor DP Enforcement
FICAM-UC-11: Secure Document or Communication with PKI
ORG-02-NPE: Establish, Maintain, and Control a NPE Credential
ORG-02-PE: Establish, Maintain, and Control a PE Credential
*ORG-09-NPE: NPE Monitoring and Reporting
*ORG-03-NPE: Provision and Deprovision NPE Privileges
*ORG-01-NPE: Establish, Maintain, and Control NPE Digital Identity Record
ORG-01-PE: Establish, Maintain, and Control PE Digital Identity Record
*ORG-04-NPE: Provision and Deprovision NPE Resource Access
ORG-04-PE: Provision and Deprovision PE Resource Access
ORG-03-PE: Provision and Deprovision PE Privileges
ORG-05-PE: Authenticate PE for Access
*ORG-05-NPE: Authenticate NPE for Access
ORG-06-PE: Authorize PE Access
ORG-03-DPM: Provide DPs for Access
*ORG-06-NPE: Authorize NPE Access
ORG-01-DPM: Create and Maintain DP Content
ORG-02-DPM: Manage Activated DPs
ORG-04-DPM: Import and Export DPs
ORG-09-PE: PE Monitoring and Reporting
ORG-07-PE: Secure PE Communication Channel with PKI
ORG-07-NPE: Secure NPE Communication Channel with PKI
ORG-08-PE: Secure PE Artifact with PKI
ORG-08-NPE: Secure NPE Artifact with PKI
GSA-UC-06: Create & Issue LOA-2 Credential
GSA-UC-07: Create & Issue LOA-3 Credential
GSA-UC-08: Create & Issue LOA-4 Credential
GSA-UC-10: Maintain Credential - Reset
GSA-UC-11: Maintain Credential - Renew
GSA-UC-12: Maintain Credential - Revoke
GSA-UC-01: Create and Maintain an Identity
GSA-UC-02: Proof an Identity at LOA-2
GSA-UC-03: Proof an Identity at LOA-3
GSA-UC-04: Proof an Identity at LOA-4
GSA-UC-05: Resolve an Identity Internal to Agency
GSA-UC-15: Grant Access to a Protected Resource
GSA-UC-14: Manage Entitlements
GSA-UC-16: Authenticate a User
GSA-UC-20: Accept Credentials in a Federation
GSA-UC-17: Authorize Access - Static
GSA-UC-18: Authorize Access - Dynamic
GSA-UC-19: Exchange Attributes in a Federation
GSA-UC-13: Administer Digital Access Policies
Legend:
FICAM
DPMF
GSA
ORG

The arrows indicate the referenced use cases that support each ORG use case

* indicates that this ORG use case has no references

**Figure 4-1 Mapping Reference ICAM Use Cases to ORG ICAM Use Cases**

## 4.2 ICAM Data Concept Model

Figure 4-2 presents a concept model of the data elements involved in ICAM data exchanges within an ORG when PEs, NPEs and PEs using an EPD (PE/EPD) require PR access control. These data concepts and their relationships establish a common context throughout the use cases.

The data elements in the model are colored to emphasize the component (IdP, SP) they characterize. The IdP component establishes, maintains and controls digital identities that it shares through an IdP service. The SP component establishes, maintains and controls PR data and service sharing. There is also an Authenticator Provider (AP) that establishes, maintains and controls authenticators. As described in Section 3.2, authenticators establish a risk-based binding of an entity's claim to a digital identity. Authenticators do not share data and therefore they are not a component in this data concept model.

Within an enterprise, it is likely that a single organization manages the IdP and SP services and controls the data sharing. In contrast, within a federation, the IdP and SP are controlled by separate managing organizations, and the data are shared across their jurisdictional boundaries. In either case the authenticator must be trusted by the participating jurisdiction(s). The IdP elements identify and characterize the entity from a business perspective, whereas the SP elements characterize the shared PR services and their access controls.

The concept model identifies the following elements and relationships:

- **Identity Record** contains the core attributes that establish a digital proxy of the data that uniquely characterize the PE's or NPE's identity. There is one Identity Record instance per entity.

- **Credential Profile** is a representation of the PE or NPE credential. It contains the credential unique ID and may include other characteristics of the credential. The Credential Profile uniquely identifies the entity.

- **Account Profile** contains the PR ID and the alphanumeric Account ID that is generated by the SP to uniquely identify the Account assigned to the PE or NPE. An entity may have multiple Account Profiles associated with its Identity Record, but there is always one Account Profile instance per Account instance.

- **Access Control Profile** contains the business-focused attributes that support access control decisions and characterizes the business demographics of the PE or EPD as maintained by the IdP. These business demographics may include entity type, current location, owner and affiliated country, assignee and affiliated country, hardware and software configuration and status, EMM controls and status, boot up integrity checks, and any other aspects of the entity that are required by the applicable Account Policies. There is one Access Control Profile instance per Identity Record instance.

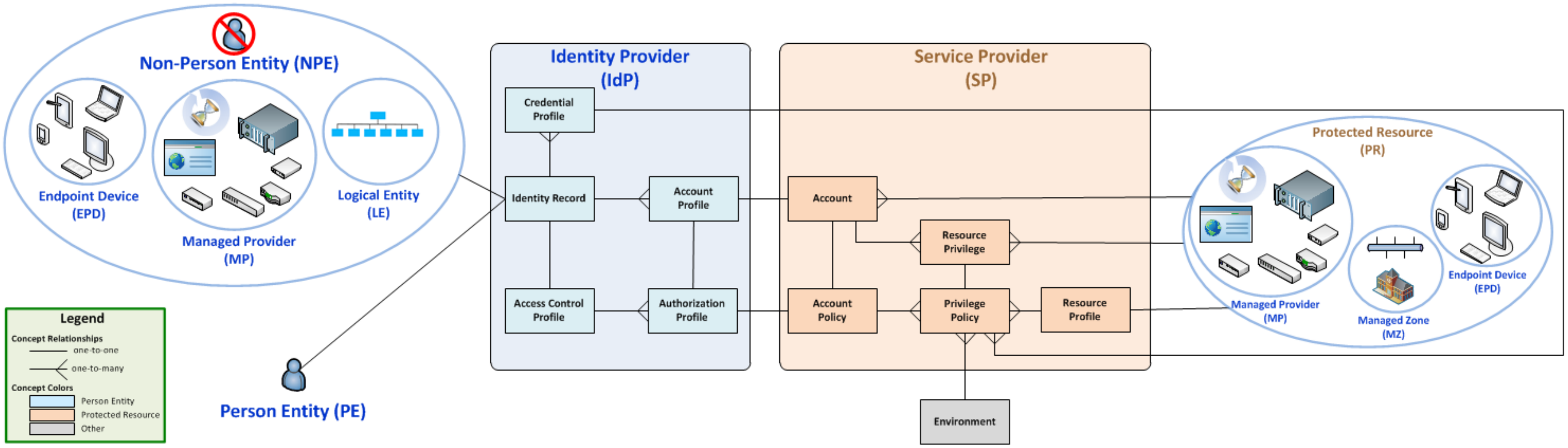


**Figure 4-2 Conceptual ICAM Data Elements**

- **Authorization Profile** is associated with the Account Profile that identifies the PE or NPE Account, and thus the Account Policy and Privilege Policies that support the access decisions for that Account. The Authorization Profile instance incorporates the appropriate Access Control Profile business-focused data plus any additional entity attributes that are needed to parameterize the Account Policy decision processing of the Privilege Policies for the entity. The Authorization Profile supplies entity attributes to the multiple Privilege Policies that comprise the Account Policy.

- **Account** contains the unique ID for the PR-specific context that is assigned to the PE or NPE by the SP. Account creation takes place either as an out-of-band process that occurs before the entity visits the PR or as a just-in-time process that takes place when the entity first visits the resource. In either case, the account data is persisted by the PR to provide and manage individualized continuity across entity sessions. The associated Account Policy regulates the PRs that are assigned to the Account

- **Resource Privilege** is a privileged action, operation, or application role that is conditionally dispensed to a PE or NPE Account by the Account Policy.

- **Resource Profile** contains attributes that characterize the elements of the PR that influence the Privilege Policies, especially dynamic data.

- **Account Policy** is the set of Privilege Policies that collectively determine the access control decision for an Account.

- **Privilege Policy** is an access control element that uses the Credential Profile, Authorization Profile, Resource Profile, and Environment attribute data to parameterize the Account Policy and conditionally regulate the Resource Privileges assigned to PE and NPE Accounts.

- **Environment** contains data that influence the Privilege Policies decision processing but are managed outside the scope of the IdP and SP. These include threat level, time of day, etc.

## 4.3 PE Use Cases

### 4.3.1 ORG-01-PE: Establish, Maintain, and Control PE Digital Identity Record

This use case focuses on the high-level steps required to establish, maintain, and control the Identity Record life cycle for each PE that is affiliated with ORG.

- Establish PE Identity Record – This flow provides the high-level process steps for ORG to establish an Identity Record and the associated Access Control Profile for a PE that will be accessing ORG services.

- Maintain PE Identity Record – This flow provides the high-level process steps for ORG to change or update the attributes of a PE Identity Record and the associated Access Control Profile.

- Control PE Identity Record – This flow provides the high-level process steps for ORG to deactivate and reactivate a PE Identity Record or the associated Access Control Profile.

### 4.3.2 ORG-02-PE: Establish, Maintain, and Control PE Credential

This use case focuses on the high-level steps required for ORG to establish (enroll and issue), maintain (life cycle management and self-service needs), and control (deactivate and reactivate) a PE credential.

- Establish PE Credential – This flow provides the high-level steps needed for ORG to enroll and issue a PE credential.

- Maintain PE Authenticator – This flow provides the high-level steps needed for ORG to renew, reissue, update, change, or reset a PE authenticator.

- Control PE Credential – This flow provides the high-level steps needed for ORG to deactivate (suspend, revoke, or block) or reactivate (reinstate and unblock) a PE credential.

- Maintain PE Authenticator Profile – This flow provides the high-level steps for ORG to allow a PE to update or change the OOB channels and/or knowledge authenticators in his authenticator profile.

### 4.3.3 ORG-03-PE: Provision and Deprovision PE Privileges

This use case describes the high-level life cycle steps required for ORG to assign, suspend, restore, and remove Resource Privileges for a PE within the scope of applicable business activities and environments.

- Establish PE Authorization Profile – This flow provides the high-level steps needed for ORG to establish (create, restore) an Authorization Profile for a PE.

- Establish PE PR Privilege – This flow provides the high-level steps needed for ORG to establish (assign, restore) a PR privilege to a PE.

- Control PE PR Privilege – This flow provides the high-level steps needed for ORG to control (unassign, suspend, deactivate) a PR privilege for a PE.

- Control PE Authorization Profile – This flow provides the high-level steps needed for ORG to control (suspend, deactivate) an Authorization Profile for a PE.

### 4.3.4 ORG-04-PE: Provision and Deprovision PE Resource Access

This use cases focuses on the high-level life cycle steps required for ORG to capture, provision, modify, and deprovision the privileged set of actions, operations, and application roles that are available to a PE for a PR within the scope of applicable business activities and environments.

- Capture Resource Privileges – This flow provides the high-level steps needed for ORG to create and maintain a complete list of the accesses, actions, operations, and application roles that are available to a PE for a PR

- Provision PE for PR Access – This flow provides the high-level steps needed for ORG to establish a PE Account with the authorized PR access permissions.

- Modify PE Permissions for PR – This flow provides the high-level steps needed for ORG to maintain and control a PE Account with the authorized PR access permissions.

- Deprovision PE from PR – This flow provides the high-level steps needed for ORG to deprovision a PE SP Account and deactivate the authorized PR access permissions.

### 4.3.5 ORG-05-PE: Authenticate PE for Access

This use case focuses on the high-level steps required for ORG to authenticate PEs when they request access to a PR.

- PE Facility Authentication – This use case flow provides the high-level steps needed for ORG to authenticate and log the entry and exit of a PE within ORG facilities.

- PE Enterprise Authentication – This flow provides the high-level steps needed for ORG to authenticate an ORG PE that is requesting access to an ORG PR.

- PE Federated Authentication – This flow provides the high-level steps needed for ORG to authenticate an ORG PE that is requesting access to a PTR SP.

### 4.3.6 ORG-06-PE: Authorize PE Access

This use case focuses on the high-level steps required for ORG to authorize logical and physical access for a PE User and their EPD. User and EPD access to the facility are determined separately.

- Authenticated PE Authorization – This flow provides the high-level steps needed for ORG to authorize an authenticated PE that is requesting access to an ORG PR or SP.

- PE Facility Access – This flow provides the high-level steps needed for ORG to manage the entry and exit of an authenticated PE within ORG facilities.

### 4.3.7 ORG-07-PE: Secure PE Communications Channel with PKI

This use case focuses on the high-level steps required for ORG to protect the confidentiality of the network TCP/IP layer messages that are employed to provide ICAM services.

- PE Confidential Communications with Trusted PR – This flow provides the high-level steps needed for a PE to establish a trusted and confidential channel with a PR.

### 4.3.8 ORG-08-PE: Secure PE Artifact with PKI

This use case focuses on the high-level steps required for ORG to protect the integrity and confidentiality of text and binary artifacts.

- Secure Artifact for Confidential Transaction – This flow provides the high-level steps needed for a PE and a PR or LE to share an artifact in a trusted and confidential manner.

- Secure Artifact Integrity for Transaction – This flow provides the high-level steps needed for a PE and a PR or LE to share an artifact in a trusted, non-reputable and untampered manner.

### 4.3.9 ORG-09-PE: PE Monitoring and Reporting

This use case focuses on the high-level steps required for an SP organization to manage, review and examine records and activities that assess the adequacy of system controls and the presentation of logged data in a meaningful context.

- Monitor PE Access – This flow provides the high-level steps needed to log PE monitored events on Monitored Systems (MSs) and PRs.

- Generate PE Activity Report – This flow provides the high-level steps needed to report the configuration, status and activity log of an MS or PR.

- Register PE Activity Monitors – This flow provides the high-level steps needed to register the PE event on MS and PR and the Event Tracking System (ETS).

## 4.4 NPE Use Cases

### 4.4.1 ORG-01-NPE: Establish, Maintain, and Control NPE Digital Identity Record

This use case focuses on the high-level steps required to establish, maintain, and control the Identity Record life cycle for each NPE affiliated with ORG.

- Establish NPE Identity Record – This flow provides the high-level process steps for ORG to establish an Identity Record and the associated Access Control Profile for an NPE.

- Maintain NPE Identity Record – This flow provides the high-level process steps for ORG to change or update the attributes of an NPE Identity Record and the associated Access Control Profile.

- Control NPE Identity Record – This flow provides the high-level process steps for ORG to deactivate and reactivate an NPE Identity Record or the associated Access Control Profile.

### 4.4.2 ORG-02-NPE: Establish, Maintain, and Control NPE Credential

This use case focuses on the high-level steps required for ORG to establish (enroll and issue), maintain (life cycle management and self-service needs), and control (deactivate and reactivate) an NPE credential.

- Establish NPE Credential – This flow provides the high-level steps needed for ORG to enroll and issue a credential for an NPE.

- Maintain NPE Credential – This flow provides the high-level steps needed for ORG to renew, reissue, update, change, or reset an NPE credential.

- Control NPE Credential – This flow provides the high-level steps needed for ORG to deactivate (suspend, revoke, or block) or reactivate (reinstate and unblock) an NPE credential.

### 4.4.3 ORG-03-NPE: Provision and Deprovision NPE Privileges

This use case focuses on the high-level life cycle steps required for ORG to assign, suspend, restore, and remove Resource Privileges for an NPE within the scope of applicable business activities and environments.

- Establish NPE Authorization Profile – This flow provides the high-level steps needed for ORG to establish (create, restore) an Authorization Profile for an NPE.

- Control NPE Authorization Profile – This flow provides the high-level steps needed for ORG to control (suspend, deactivate) an Authorization Profile for an NPE.

- Establish NPE PR Privilege – This flow provides the high-level steps needed for ORG to establish (assign, restore) a PR privilege to an NPE.

- Control NPE PR Privilege – This flow provides the high-level steps needed for ORG to control (unassign, suspend, deactivate) a PR privilege for an NPE.

### 4.4.4 ORG-04-NPE: Provision and Deprovision NPE Resource Access

This use cases focuses on the high-level life cycle steps required for ORG to capture, provision, modify, and deprovision the privileged set of actions, operations, and application roles that are available to an NPE for a PR within the scope of applicable business activities and environments.

- Capture Resource Privileges – This flow provides the high-level steps needed for ORG to create and maintain a complete list of the accesses, actions, operations, and application roles that are available to an NPE for a PR.

- Provision NPE for PR Access – This flow provides the high-level steps needed for ORG to establish an NPE SP Account with the authorized PR access permissions.

- Modify NPE Permissions for PR – This flow provides the high-level steps needed for ORG to maintain and control an NPE SP Account with the authorized PR access permissions.

- Deprovision NPE from PR – This flow provides the high-level steps needed for ORG to deprovision an NPE SP Account and deactivate the authorized PR access permissions.

### 4.4.5 ORG-05-NPE: Authenticate NPE for Access

This use case focuses on the high-level steps required for ORG to authenticate NPEs when they request access to a PR.

- NPE Facility Authentication – This flow provides the high-level steps needed for ORG to authenticate and log the NPE information and the transfer paperwork validity and authority.

- NPE Enterprise Authentication – This flow provides the high-level steps needed for ORG to authenticate an NPE that is requesting access to an ORG PR and to provide the ORG PR credential to the NPE when requesting mutual authentication.

- NPE Federated Authentication – This flow provides the high-level steps needed for ORG to authenticate an ORG NPE that is requesting access to a PTR SP and to authenticate the PTR SP.

### 4.4.6 ORG-06-NPE: Authorize NPE Access

This use case focuses on the high-level steps required for ORG to authorize logical and physical access for as NPE or a PE User and their EPD. User and EPD access to the facility are determined separately.

- Authenticated NPE Authorization – This flow provides the high-level steps needed for ORG to authorize an authenticated NPE that is requesting access to an ORG SP.

- Authenticated User/EPD Authorization – This flow provides the high-level steps needed for ORG to authorize an authenticated User/EPD entity pair that is requesting access to a ORG SP

- NPE Facility Access – This flow provides the high-level steps needed for ORG to manage the entry and exit of an authenticated NPE within ORG facilities.

### 4.4.7 ORG-07-NPE: Secure NPE Communication Channel with PKI

This use case focuses on the high-level steps required for ORG to protect the confidentiality of the network TCP/IP layer messages that are employed to provide ICAM services.

- NPE Confidential Communications with Trusted PR – This flow provides the high-level steps needed for an NPE to establish a trusted and confidential channel with a PR.

- NPE Confidential Communications with Mutually Trusted PR – This flow provides the high-level steps needed for an NPE to establish a mutually trusted and confidential channel with a PR.

### 4.4.8 ORG-08-NPE: Secure NPE Artifact with PKI

This use case focuses on the high-level steps required for ORG to protect the integrity and confidentiality of text and binary artifacts.

- Secure Artifact for Confidential Transaction – This flow provides the high-level steps needed for an NPE and a MP or LE to share an artifact in a trusted and untampered manner. This also enables provider non-repudiation.

- Secure Artifact Integrity for Transaction – This flow provides the high-level steps needed for an NPE and a MP or LE to share an artifact in a trusted and confidential manner.

### 4.4.9 ORG-09-NPE: NPE Monitoring and Reporting

This use case focuses on the high-level steps required for an SP organization to manage, review, and examine records and activities that assess the adequacy of system controls and the presentation of logged data in a meaningful context.

- Monitor NPE – This flow provides the high-level steps needed to log the configuration and status of an NPE.

- Monitor NPE Access – This flow provides the high-level steps needed to log NPE monitored events on MSs and PRs.

- Generate NPE Activity Report – This flow provides the high-level steps needed to report the configuration, status, and activity log of an NPE.

- Register NPE Activity Monitors – This flow provides the high-level steps needed to register an NPE event on an MS and protect the ETS.

## 4.5 DPM Use Cases

### 4.5.1 ORG-01-DPM: Create and Maintain DP Content

This use case focuses on the high-level steps required for ORG to manage the life cycle of the DPs that control access to their PR services.

- Create and Maintain DP Content – This flow describes how the ORG Digital Policy Administrator (DPA) interacts with the Digital Policy Management System (DPMS) to create, update, and verify DP content.

### 4.5.2 ORG-02-DPM: Manage Activated DPs

This use case focuses on the high-level steps required for ORG to verify DP functionality and that the execution conforms to the intent.

- Activate New Verified DP – This flow describes how the ORG DPA interacts with the DPMS to activate a new verified DP in the Access Manager (AM).
- Supersede, Revoke, or Retire DP – This flow describes how DPA interacts with the DPMS to ensure that the superseded, expired, or revoked DPs are not available to AM.
- Manage AM Subscriptions – This flow describes how the ORG DPA interacts with the DPMS to manage the dissemination of active DPs including DP and attributes retrieval ordering precedence to the AM for enforcement.
- Bind DP to Objects – This flow describes how the ORG DPA interacts with the DPMS to bind DPs to the applicable PR when the AM retrieves DPs with PR Resource Profile attributes, rather than through a separate DP discovery mechanism.

### 4.5.3 ORG-03-DPM: Provide DPs for Access

This use case focuses on the high-level steps required for ORG to activate DP enforcement.

- Provide DPs for Access – This flow describes how the ORG DPMS provides Activated DPs to subscribed AMs for use in ABAC policy enforcement.

### 4.5.4 ORG-04-DPM: Import and Export DPs

This use case focuses on the high-level steps required for ORG to share DPs with other enterprise and federation PTRs.

- Import and Export DPs – This flow describes how the ORG DPA interacts with the DPMS to send and revive DPs (i.e., Approved Human-Readable Structured Language Policies [HRSLPs], Approved DPs, or Activated DPs) with PTR domains.

As previously described and illustrated in Figure 3-4, the PE and NPE use cases address the following:

- Management services – digital identity, credentialing and privilege management
- Enforcement services – authentication, authorization and access control
- Support services – cryptography and governance

Although the use cases provide details on these important ORG ICAM concerns, they do not address security, conformance and risk management.

## 4.6 FICAM Services Framework Alignment

The ORG ICAM Use Cases align with the FICAM Services Framework as follows:

**Digital Identity** – The processes required to capture and validate information that uniquely identifies an entity, determines the suitability of that entity, and creates and manages the identity life cycle for that entity.

- ORG-01-PE: Establish, Maintain, and Control PE Digital Identity Record
- ORG-01-NPE: Establish, Maintain, and Control NPE Digital Identity Record

**Credentialing** – The processes for binding an identity to a physical or electronic credential so that it can be used as a proxy for proving an identity claim.

- ORG-02-PE: Establish, Maintain, and Control PE Credential
- ORG-02-NPE: Establish, Maintain, and Control NPE Credential

**Privilege Management** – The processes for establishing and maintaining the privilege attributes that comprise an entity’s access profile. These attributes are features of the entity that can be used as the basis for making policy-based access decisions.

- ORG-03-PE: Provision and Deprovision PE Privileges
- ORG-04-PE: Provision and Deprovision PE Resource Access
- ORG-03-NPE: Provision and Deprovision NPE Privileges
- ORG-04-NPE: Provision and Deprovision NPE Resource Access

**Authentication** – The processes for verifying that an identity claim is genuine and proven with a valid credential.

- ORG-05-PE: Authenticate PE for Access
- ORG-05-NPE: Authenticate NPE for Access

**Authorization and Access** – The processes required for granting or denying specific requests to obtain access to PRs.

- ORG-06-NPE: Authorize NPE Access

**Cryptography** – The processes to use and manage ciphers and ensure the authenticity, confidentiality, and integrity of shared data.

- ORG-07-PE: Secure PE Communication Channel with PKI

- ORG-08-PE: Secure PE Artifact with PKI
- ORG-07-NPE: Secure NPE Communication Channel with PKI
- ORG-08-NPE: Secure NPE Artifact with PKI

**Auditing and Reporting** – The processes to capture and review records and activities for assessing the adequacy of system controls.

- ORG-09-PE: PE Monitoring and Reporting
- ORG-09-NPE: NPE Monitoring and Reporting

**DPM** – The processes to dynamically create, disseminate, and maintain hierarchical rule sets and control digital resource management, utilization, and protection.

- ORG-01-DPM: Create and Maintain DP Content
- ORG-02-DPM: Manage Activated DPs
- ORG-03-DPM: Provide DPs for Access
- ORG-04-DPM: Import and Export DPs

## 4.7 Use Case Overview

The use case actors represent the user roles, services, groupings, and components that interact with ORG ICAM functions during use case execution. This section describes the PE and NPE actors, which are shown hierarchically in Figure 4-3.

The PE actors are as follows:

- **AAA** – The Authorized Authority Administrator or his/her designated subordinate who manages the specific authoritative business-focused data in his/her assigned system and helps establish the NPE Access Control Profile
- **AMSA** – The Account Management System Administrator or authorized subordinate
- **CMSA** – The Credential Management System Administrator or authorized subordinate
- **DPA** – The Digital Policy Administrator or authorized subordinate
- **EAR** – The PE who is the Event Auditor and Reporter
- **Entity** – Both PE and NPE
- **FAM** – The Facility Access Manager who monitors and controls physical access to ORG facilities

- **IRA** – The Identity Record Administrator or authorized subordinate
- **NPE Administrator** (or privileged user) – The person who has privileged access to configure and manage the NPE. This can only be an employee or contractor of ORG or PTR organization that has been granted privileged access by ORG and agreed to by the NPE Owner or Assignee.
- **NPE Assignee** – The PE or organization that the Owner delegates as the party responsible for the NPE. The PE can be an employee or contractor of ORG or a PTR, and the organization can be either ORG or a PTR.
- **NPE Owner** – The person or organization that purchased the NPE. The person (PE) can be an employee or contractor of ORG or an ORG PTR, and the organization can be ORG or a PTR.
- **NPE User** – The PE who is currently operating the NPE. This can only be a PE employee or contractor of ORG or a PTR organization that has been granted usage by the NPE Assignee.
- **PE** – A Person Entity
- **PMSA** – The Privilege Management System Administrator or authorized subordinate
- **PTR PE** – A PE with a PTR primary affiliation
- **SRAA** – The Service Request Application Administrator or designated subordinate

The NPE actors are as follows:

- **AAES** – The Authoritative Attribute Exchange Service that consolidates each Identity Record and Access Control Profile from the distributed authoritative business data
- **AM** – The Access Manager component of the Logical Access Control System (LACS)
- **AMS** – The Account Management System
- **AR** – An Authoritative Resource
- **CA** – The Certificate Authority that issues the PKI certificates
- **CMS** – The Credential Management System
- **CMSW** – The Credential Management System Wizard
- **DPMS** – The Digital Policy Management System
- **EPD** – The Endpoint Device

- **EMM** – The Enterprise Mobility Management
- **ETS** – The Event Tracking System
- **IdP** – The Identity Provider
- **LE** – A Logical Entity
- **MND** – A Managed Network Device
- **MP** – A Managed Provider
- **MS** – A Monitored System is a subset of the MPs
- **MSP** – A Managed Server Platform
- **MSS** – A Managed Shared Service
- **NPE** – The Non-Person Entity
- **ORG**[12] – The organization that is performing the use case processing
- **PMS** – The Privilege Management System
- **PR** – The Protected Resource including network, domain, application, and service
- **PTR**[13] – An organization or agency that has a partnership relationship with ORG
- **SP** – The Service Provider

[12] While this never appears directly as an actor, it is implied in every use case and it is an LE covering all the actors identified above.

[13] While this never appears directly as an actor, it is an LE covering all the actors identified above

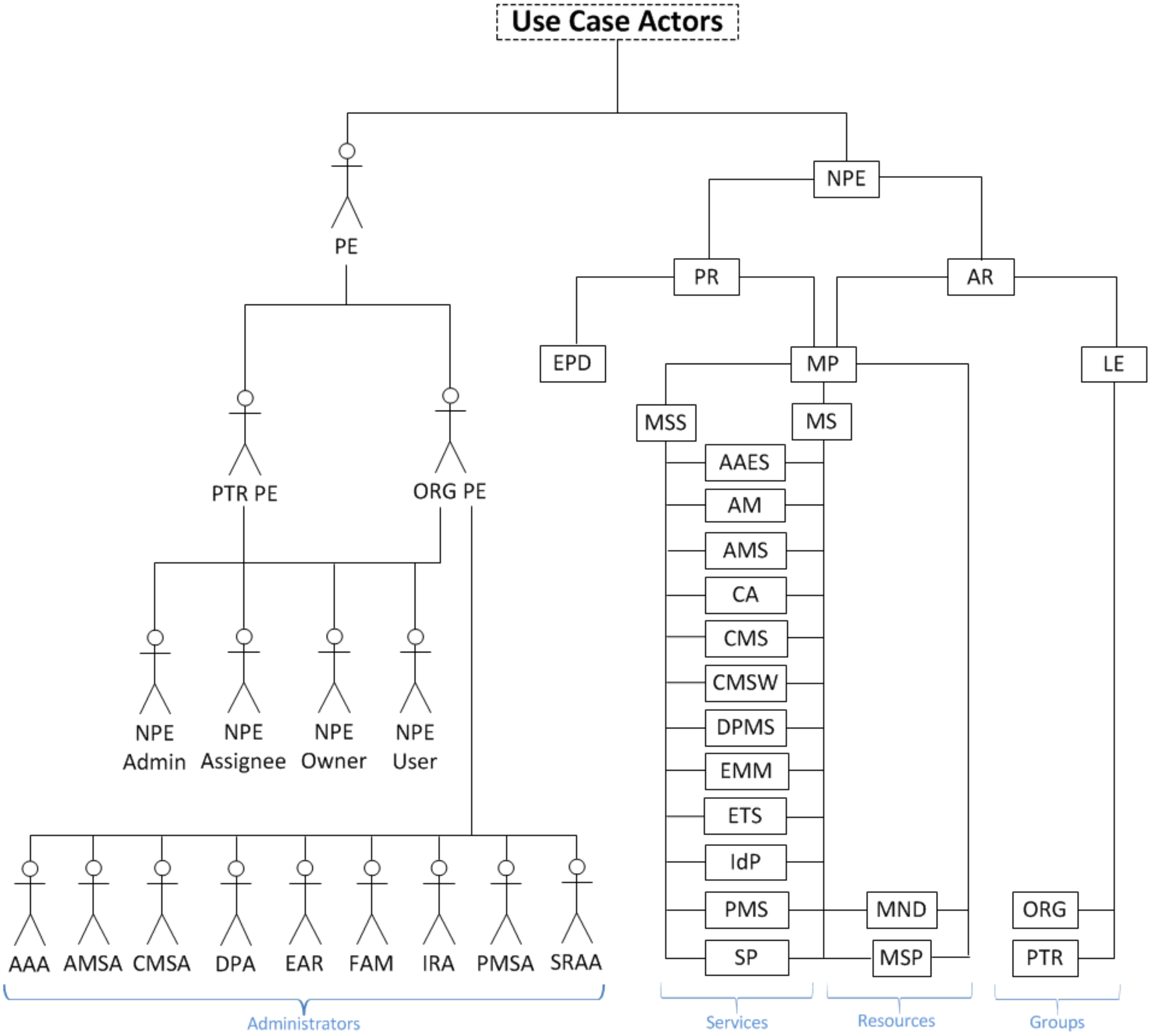


**Figure 4-3 ORG Use Case Actor Hierarchy**

In addition to the use case actors, the use cases describe artifacts that are acted upon. The artifacts include the ICAM Data Concept Model elements (Section 4.1) and the following:

- **ACR** – The Authorized Credential Request provides create, maintain, and control servicing data and authorizations.

- **AMR** – The Activity Monitoring Request provides create, activate, or deactivate NPE activity monitoring events and logging.

- **AND** – The Authentication Data and Results including the credential unique ID.

- **APAR** – The Authorized Privilege and Account Request provides capture, provision, modify, and deprovision servicing data and authorizations for PR privileges and Accounts.

- **APPR** – The Authorized Privilege and Profile Request provides establish (assign, restore) and control (unassign, suspend, deactivate) servicing data and authorizations for PR privileges and Authorization Profiles.

- **Paperwork** – Documented and authoritative permission to physically transport equipment into or out of an ORG facility.

- **Payload** – Any item (text or binary) that can be signed, encrypted or both, e.g., a file, email, message, etc.

- **Credential** – CryptoSH [including PIV, Personal Identity Verification – Interoperable (PIV-I), Common Access Card (CAC), Derived PIV/PIV-I Credential (DPC)], Memorized Secret, Look-up Secret, OOB, OTP, CryptoD and CryptoSS

- **DP** – Digital Policy

- **MAR** – The Monitored Activity Report on NPE configuration, status, and monitored activities.

- **SRA** – The Service Request Application part of the on boarding package and provides new, change, update, deactivate and reactivate servicing data and authorizations.

Figure 4-4 provides context for the NPE use cases, indicating which use case actors interact during each use case.

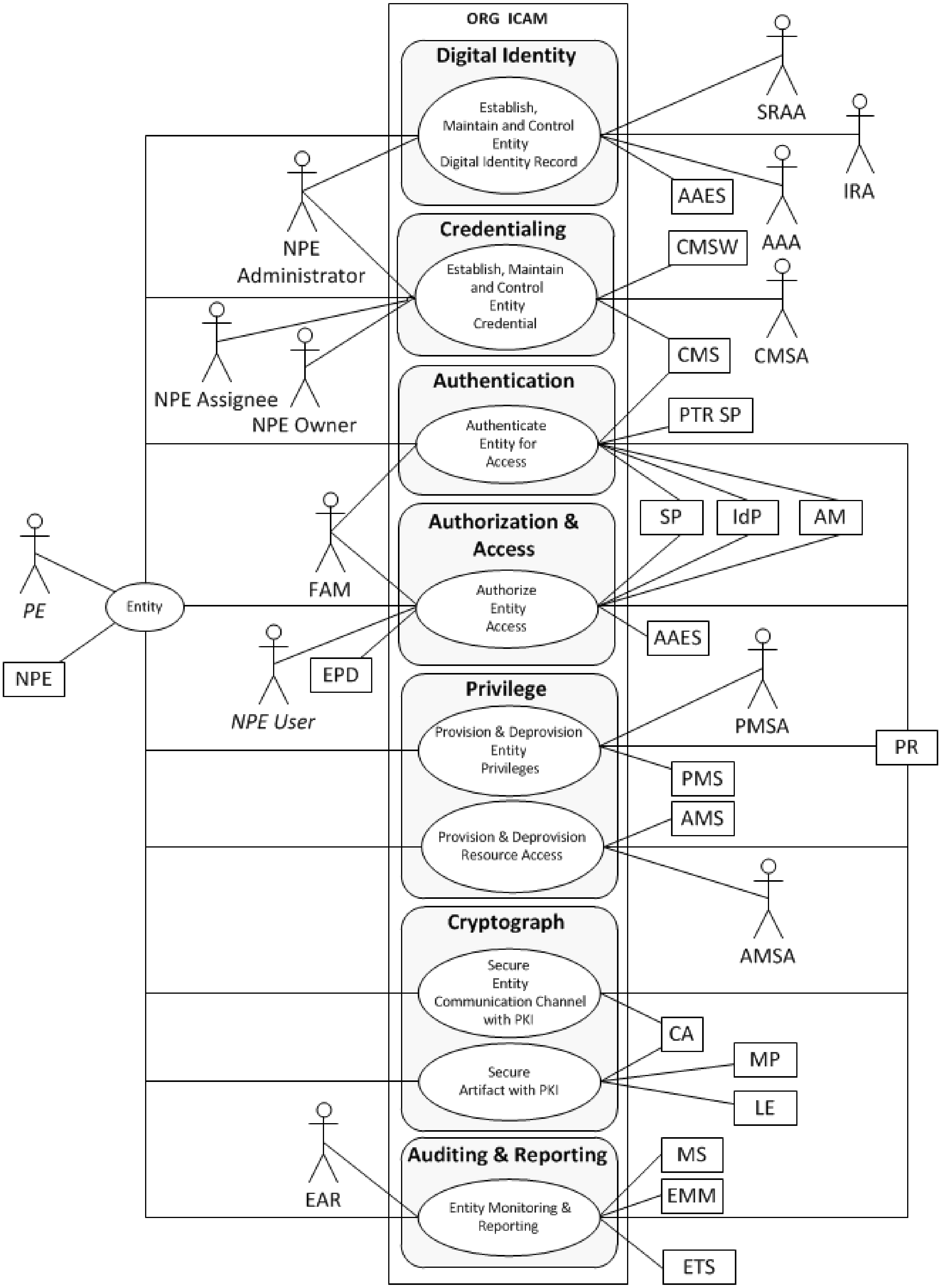


**Figure 4-4 ORG Use Case Context**

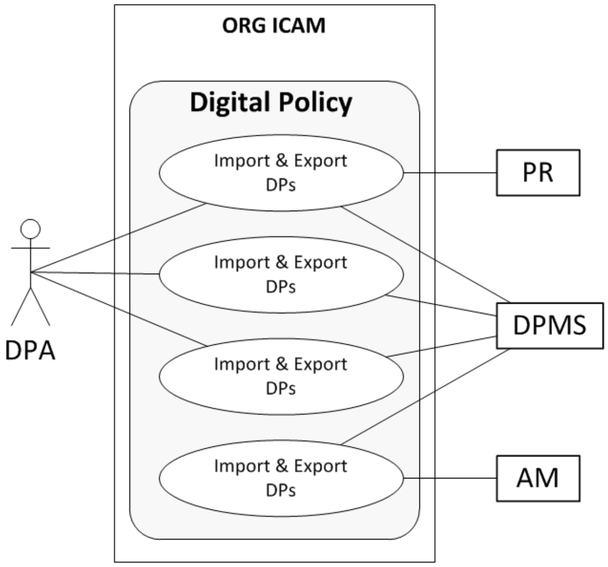


**Figure 4-5 ORG DPM Use Case Context**

## 4.8 PE and NPE Use Case Alignment

The FICAM Services Alignment is summarized in the NPE column of Table 4-1. This side-by-side comparison shows how the ICAM aspects of these entity types are conceptually related and aligned with the FICAM services. Several of the ORG ICAM PE use cases apply without modification to the NPE, and they are shown in the table spanning the columns. These are the four DPM use cases that detail the life cycle specifics of controlling entity access with digital policies and therefore apply to both PEs and NPEs.

**Table 4-1 FICAM Services Alignment of PE and NPE Use Cases**

| ID | PE | PR | | | | | |
|---|---|---|---|---|---|---|---|
| | | MZ | NPE | | | | |
| | | | EPD | AR | | | |
| | | | | MP | | | LE |
| | | | | MSP | MND | MSS | |
| **Digital Identity** | ORG-01-PE: Establish, Maintain, and Control PE Digital Identity Record | ORG-01-NPE: Establish, Maintain, and Control NPE Digital Identity Record | | | | | |
| **Credentialing** | ORG-02-PE: Establish, Maintain, and Control a PE Credential | ORG-02-NPE: Establish, Maintain, and Control NPE Credential | | | | | |
| **Privilege Management** | ORG-03-PE: Provision and Deprovision PE Privileges | ORG-03-NPE: Provision and Deprovision NPE Privileges | | | | | |
| | ORG-04-PE: Provision and Deprovision PE Resource Access | ORG-04-NPE: Provision and Deprovision NPE Resource Access | | | | | |
| **Authentication** | ORG-05-PE: Authenticate PE for Access | ORG-05-NPE: Authenticate NPE for Access | | | | | |
| **Authorization and Access** | ORG-06-PE: Authorize PE Access | ORG-06-NPE: Authorize NPE Access | | | | | |
| **Cryptography** | ORG-07-PE: Secure PE Communication Channel with PKI | ORG-07-NPE: Secure NPE Communication Channel with PKI | | | | | |
| | ORG-08-PE: Secure PE Artifact with PKI | ORG-08-NPE: Secure NPE Artifact with PKI | | | | | |
| **Auditing and Reporting** | ORG-09-PE: PE Monitoring and Reporting | ORG-09-NPE: NPE Monitoring and Reporting | | | | | |
| **DPM** | ORG-01-DPM: Create and Maintain DP Content | | | | | | |
| | ORG-02-DPM: Manage Activated DPs | | | | | | |
| | ORG-03-DPM: Provide DPs for Access | | | | | | |
| | ORG-04-DPM: Import and Export DPs | | | | | | |

## 4.9 Use Case Presentation Format

Each ORG ICAM use case is described using one or more tables in the format shown in Table 4-2. Separate tables are used when the Trigger, Pre-conditions, or Post-conditions differ from the previous flows within a use case.

**Table 4-2 Use Case Description Format**

| **Identifier** | **Use Case Flow Identifier** |
|---|---|
| Description | Overview description of the use case flow. |
| Actor(s) | One or more actors that interact with the system during execution of the use case flow. There are person and non-person actors as described in Section 4.7, and they are labeled as such in this area for emphasis. |
| Artifact(s) | Containers and other artifacts that are acted upon during the use case. |
| Trigger | The event that triggers the start of the use case flow. |
| Pre-conditions | A description of the conditions that must be true before the use case flow begins. |
| Post-conditions | A description of the conditions that are changed by the execution of the use case flow. |
| Main Flow | A list of steps that are executed in the Main use case flow. Every use case has one Main Flow. The description of these steps is architecturally agnostic. The normal flow is sequential with conditional execution. The flow may jump to another step in the same flow or any of the other flows defined in the same use case. These flow jumps are noted in the appropriate step. |
| Alternate Flow | A list of steps that are executed in the Alternate use case flows. A use case can have any number of Alternate Flows. The description of these steps is architecturally agnostic. The normal flow is sequential with conditional execution. The flow may jump to another step in the same flow or any of the other flows defined in the same use case. These flow jumps are noted in the appropriate step. |
| Shared Flow | A list of steps that are executed by two or more flows. A use case can have any number of Shared Flows. |

*The Use Case Flow Identifier is the use case ID with a letter appended sequentially starting with “A.”

The use case descriptions and a use case diagram (a type of context diagram) are also provided for each FICAM functional area.[14]

[14] For further information on use cases and use case diagrams, see the list of resources at http://www.uml.org.

## 4.10 Digital Identity Use Case

This use case describes the processes required to capture and validate information that uniquely identifies an entity, determines the suitability of that entity, and creates and manages the identity life cycle for that entity.

### 4.10.1 Actors and Artifacts

The Digital Identity Use Case Context is shown in Figure 4-6, and the identified actors are characterized in this subsection.

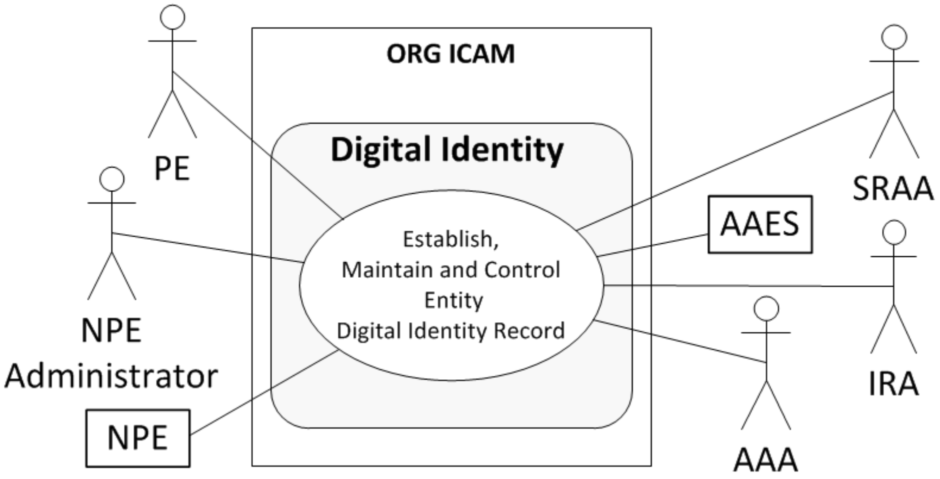


**Figure 4-6 Digital Identity Use Case**

The PE actors for the Digital Identity use case are:

- **AAA** – The Authorized Authority Administrator or designated subordinate
- **IRA** – The Identity Record Administrator or authorized subordinate
- **NPE Administrator** (or privileged user)
- **PE** – The Person Entity that is the focus of the PE use case
- **SRAA** – The Service Request Application Administrator or designated subordinate

The NPE actors for the Digital Identity use case are:

- **AAES** – The Authoritative Attribute Exchange Services
- **NPE** – The Non-Person Entity that is the focus of the NPE use case

The artifacts for the Digital Identity use case are:

- **SRA** – The Service Request Application

- **Identity Record**
- **Access Control Profile**

### 4.10.2 PE Description

The following use cases are covered in this section:

- ORG-01-PE: Establish, Maintain and Control PE Digital Identity Record

This use case focuses on the high-level steps required to establish, manage, and control the Identity Record life cycle for each ORG PE and PTR PE that is affiliated with ORG. A PE is considered internal to ORG when the affiliation establishes ORG as his primary IdP. A PE is identified as a PTR when their primary affiliation is with a PTR organization or agency and the PE provides information to ORG during the course of doing business.

When ORG hires employees and contractors, they go through an on-boarding process that establishes their internal affiliation and generates a managed digital identity that enables that person to perform business activities for that agency. This on-boarding process captures and vets the identity information provided by the PE and creates a standardized on-boarding package including a SRA that identifies the required Identity Record and Access Control Profile data for that PE. The PE’s primary organization normally duplicates the Identity Record data across the multiple systems that capture the Access Control Profile data including human resources, contractor management, security, payroll, and various information systems. This enables the enrichment of the identity with essential business-focused data that are easily controlled by the appropriate AAA. The management, synchronization, authority, alignment, and access of the PE’s common Identity Record and the distributed Access Control Profile data are centralized in an AAES. The IRA uses the AAES to establish, manage, and control the Identity Record life cycle and the associated Access Control Profile of each ORG PE.

When ORG allows PTR PEs to establish an external affiliation with them, then ORG generates a managed digital identity that enables that person to perform business activities for that PTR using ORG services. The IRA uses the AAES to establish, manage, and control the Identity Record life cycle of each PTR PE. The PTR or its requesting PE provides an SRA that is processed by the ORG SRA Administrator or his designated subordinate (SRAA) that manages and authorizes the requested ORG service or application access. Establishing an Identity Record for a PTR PE is the first step in providing that PE access to an ORG service or application (i.e., an ORG service or application). ORG-02-PE must be executed to create a trusted credential if the PTR or the SRA does not identify one. ORG-03-PE and ORG-04-PE are also required to activate the appropriate PTR PE privileges.

### 4.10.3 ORG-01-PE: Establish, Maintain and Control PE Digital Identity Record

The details of this use case are covered in:

A. Establish PE Identity Record (Table 4-3)

B. Maintain PE Identity Record (Table 4-4)

C. Control PE Identity Record (Table 4-5)

### Table 4-3 Establish PE Identity Record

| **Identifier** | **ORG-01-PE-A: Establish PE Identity Record** |
|---|---|
| Description | This use case flow provides the high-level process steps for ORG to establish an Identity Record and the associated Access Control Profile for a PE that will be accessing ORG services. |
| Actor(s) | Person:<br>• Authorized Authority Administrator (AAA)<br>• Identity Record Administrator (IRA)<br>• Service Request Application Administrator (SRAA)<br>• Person Entity (PE)<br>Non-person:<br>• Authoritative Attribute Exchange Services (AAES) |
| Artifact(s) | • Service Request Application (SRA) – new PE<br>• Identity Record<br>• Access Control Profile |
| Trigger | An SRA is provided electronically to the SRAA |
| Pre-conditions | An SRA is created in one of the following ways:<br>1. ORG is on-boarding a new employee or contractor.<br>2. A PTR has submitted in person or remotely an SRA for a new PTR PE and the ORG sponsor accepts sponsorship<br>3. The SRA is automatically generated based on workflows established within the agency, e.g., just-in-time provisioning. |
| Post-conditions | The PE Identity Record and Access Control Profile containing the SRA data are available via the AAES. |

| Identifier | ORG-01-PE-A: Establish PE Identity Record |
|---|---|
| Main Flow | 1. SRAA proofs the identity in one of the following ways:[15]<br>a. Identity Assurance Level 1 (IAL-1)<br>• Remote or in-person the entity may self-assert an identity.<br>b. IAL-2<br>• Remote or in-person the entity provides identity evidence that resolves to a real unique identity.<br>• The SRAA validates the identity evidence with STRONG[5] verification.<br>• The SRAA confirms the address with enrollment code.<br>c. IAL-3<br>• In-person the entity completes IAL-2 steps with SUPERIOR[5] verification.<br>• A biometric is collected.<br>2. The SRAA approves and SRA and passes it to the IRA.<br>3. The IRA creates an Identity Record in the AAES for the PE that includes the appropriate SRA data elements.<br>4. The IRA updates the Identity Record data elements with the current data from the PE.<br>5. Based on the agency’s architecture, on-boarding and PTR PE processing policies:<br>a. AAAs of one or more additional business specific systems are notified of the new PE Identity Record and the SRA is provided electronically.<br>b. Each AAA retrieves the PE Identity Record from the AAES, creates a new record in its system containing that data, and adds the business-focused data that are identified in the SRA and managed by its system |

[15] Reference 7 and Section 3.3.2.

### Table 4-4 Maintain PE Identity Record

| **Identifier** | **ORG-01-PE-B: Maintain PE Identity Record** |
|---|---|
| Description | This use case flow provides the high-level process steps for ORG to change or update the attributes of a PE Identity Record and the associated Access Control Profile. |
| Actor(s) | Person:<br>• Authorized Authority Administrator (AAA)<br>• Identity Record Administrator (IRA)<br>• Service Request Application Administrator (SRAA)<br>• Person Entity (PE)<br>Non-person:<br>• Authoritative Attribute Exchange Services (AAES) |
| Artifact(s) | • Service Request Application (SRA) – change, update EPD<br>• Identity Record<br>• Access Control Profile |
| Trigger | An SRA is initiated to a change in a PE's attributes. |
| Pre-conditions | The PE has an active Identity Record and Access Control Profile in the AAES. |
| Post-conditions | The completed PE attribute change or update is available via the AAES. |
| Main Flow | 1. An SRA to change or update a PE's Identity Record or associated Access Control Profile is made using one of the following methods:<br>a. The SRAA, IRA or AAA receives an electronic notification or SRA request to change or update a PE's attributes. The IRA or AAA verifies the attribute change per agency policy and changes or updates the PE attributes in the appropriate system.<br>b. The PE uses a self-service system to change or update its attributes in the affected system.<br>c. The attribute change is triggered and completed automatically based on workflows established within the agency.<br>2. The updated or changed attributes are made available via AAES.<br>3. The old PE attribute data is maintained for the required time period and deactivated or otherwise flagged. |

Table 4-5 Control PE Identity Record

| Identifier | ORG-01-PE-C: Control PE Identity Record |
|---|---|
| Description | This use case flow provides the high-level process steps for ORG to deactivate and reactivate a PE Identity Record or the associated Access Control Profile. |
| Actor(s) | Person:<br>• Authorized Authority Administrator (AAA)<br>• Identity Record Administrator (IRA)<br>• External Person Entity (PE)<br>• Service Request Application Administrator (SRAA)<br>Non-person:<br>• Authoritative Attribute Exchange Service (AAES) |
| Artifact(s) | • Service Request Application (SRA) – deactivate/ reactivate PE<br>• Identity Record<br>• Access Control Profile |
| Trigger | An authorized request is initiated to a change in a PE attributes. |
| Pre-conditions | • The PE has an active Identity Record and Access Control Profile in the AAES and the SRA is deactivate, or<br>• The PE has an inactive Identity Record and Access Control Profile in the AAES and the SRA is reactivate. |
| Post-conditions | The completed PE status change has been applied. |
| Main Flow | 1. An SRA to change the PE status is made using one of the following methods:<br>a. The SRAA, IRA or AAA receives an electronic notification or request to deactivate/reactivate a PE. The IRA or AAA verifies the request per agency policy and updates the PE status in the appropriate system(s).<br>b. The PE Administrator uses a self-service system to deactivate/activate the PE status in the affected system(s).<br>c. The PE status change is triggered and completed automatically based on workflows established within the agency.<br>2. The deactivated PE is no longer available via AAES or the reactivated PE is available via AAES. |

### 4.10.4 NPE Description

The following use case is covered in this subsection:

- ORG-01-NPE: Establish, Maintain, and Control NPE Digital Identity Record

This use case focuses on the high-level steps required to establish, maintain, and control the Identity Record life cycle for each NPE that is affiliated with and managed by ORG. This affiliation is established between the NPE Owner and ORG by mutual agreement. An NPE is considered managed to ORG when the NPE Owner establishes ORG as the IdP of that NPE. The NPE Owner can be ORG or a PTR that shares information with ORG during the course of doing business.

As part of ORG Authority To Operate (ATO) processing for deploying an NPE in the ORG enterprise, the NPE goes through a provisioning process that establishes a managed digital identity. This process captures and vets the identity information for the NPE and creates a standardized Provisioning Package that includes an SRA for each NPE. The SRA identifies the required Identity Record and Access Control Profile data for the NPE. The SRA is processed by the ORG SRAA or designated subordinate who manages and authorizes the requested access privileges.

The management, synchronization, authority, alignment, and access of the NPE Identity Record and the distributed Access Control Profile data are centralized in an AAES. The IRA or authorized subordinate uses the AAES to establish, manage, and control the Identity Record life cycle and the associated Access Control Profile of each NPE.

### 4.10.5 ORG-01-NPE: Establish, Maintain, and Control NPE Digital Identity Record

The details of this use case are provided in three sub-cases:

A. Establish NPE Identity Record (Table 4-6)

B. Maintain NPE Identity Record (Table 4-7)

C. Control NPE Identity Record (Table 4-8)

Table 4-6 Establish NPE Identity Record

| Identifier | ORG-01-NPE-A: Establish NPE Identity Record |
|---|---|
| Description | This use case flow provides the high-level process steps for ORG to establish an Identity Record and the associated Access Control Profile for an NPE that will be used to access ORG PRs. |
| Actor(s) | Person:<br>• Authorized Authority Administrator (AAA)<br>• Identity Record Administrator (IRA)<br>• Service Request Application Administrator (SRAA)<br>• NPE Administrator<br>Non-person:<br>• Non-Person Entity (NPE)<br>• Authoritative Attribute Exchange Services (AAES) |
| Artifact(s) | • Service Request Application (SRA) – new NPE<br>• Identity Record<br>• Access Control Profile |
| Trigger | An SRA is provided electronically to the SRAA. |
| Pre-conditions | An SRA is created in one of the following ways:<br>• ORG submits an SRA for a new authorized ORG or PTR NPE.<br>• An SRA is automatically generated based on workflows established within the agency, e.g., just-in-time provisioning. |
| Post-conditions | The NPE Identity Record and Access Control Profile containing the SRA data are available via the AAES. |
| Main Flow | 1. The SRAA approves an SRA and passes it to the IRA.<br>2. The IRA creates an Identity Record in the AAES for the NPE that includes the appropriate SRA data elements.<br>3. The IRA updates the Identity Record data elements with the current data from the NPE.<br>4. Based on the agency's architecture, the AAAs of one or more additional business-specific systems are notified of the new NPE Identity Record and the SRA is provided electronically.<br>5. Each AAA retrieves the NPE Identity Record from the AAES, creates a new record in its system containing that data, and adds the business-focused data that are identified in the SRA and managed by its system. |

### Table 4-7 Maintain NPE Identity Record

| **Identifier** | **ORG-01-NPE-B: Maintain NPE Identity Record** |
|---|---|
| Description | This use case flow provides the high-level process steps for ORG to change or update the attributes of an NPE Identity Record and the associated Access Control Profile. |
| Actor(s) | Person:<br>• Authorized Authority Administrator (AAA)<br>• Identity Record Administrator (IRA)<br>• Service Request Application Administrator (SRAA)<br>• NPE Administrator<br>Non-person:<br>• Non-Person Entity (NPE)<br>• Authoritative Attribute Exchange Services (AAES) |
| Artifact(s) | • Service Request Application (SRA) – change, update NPE<br>• Identity Record<br>• Access Control Profile |
| Trigger | An authorized request is initiated to change NPE attributes. |
| Pre-conditions | The NPE has an active Identity Record and Access Control Profile in the AAES. |
| Post-conditions | The completed PE attribute change is available via the AAES. |
| Main Flow | 1. An SRA to change an NPE Identity Record or associated Access Control Profile is made.<br>a. The SRAA, IRA, or AAA receives an electronic notification or SRA request to update the NPE attributes. The IRA or AAA verifies the attribute change per agency policy and updates the NPE attributes in the appropriate system.<br>b. The NPE Administrator uses a self-service system to change the NPE attributes in the affected system.<br>c. The attribute change is triggered and completed automatically based on workflows established within the agency.<br>2. The updated attributes are made available via AAES. |

### Table 4-8 Control NPE Identity Record

| **Identifier** | **ORG-01-NPE-C: Control NPE Identity Record** |
|---|---|
| Description | This use case flow provides the high-level process steps for ORG to deactivate and reactivate an NPE Identity Record or the associated Access Control Profile. |
| Actor(s) | Person:<br>• Authorized Authority Administrator (AAA)<br>• Identity Record Administrator (IRA)<br>• Service Request Application Administrator (SRAA)<br>• NPE Administrator<br>Non-person:<br>• Non-Person Entity (NPE)<br>• Authoritative Attribute Exchange Services (AAES) |
| Artifact(s) | • Service Request Application (SRA) – deactivate/ reactivate EPD<br>• Identity Record<br>• Access Control Profile |
| Trigger | An authorized request is initiated to deactivate/ reactivate an NPE |
| Pre-conditions | • The NPE has an active Identity Record and Access Control Profile in the AAES and the SRA is deactivate<br>• The NPE has an inactive Identity Record and Access Control Profile in the AAES and SRA is reactivate |
| Post-conditions | The completed NPE status change has been applied. |
| Main Flow | 1. An authorized change to the NPE status is made using one of the following methods:<br>a. The SRAA, IRA or AAA receives an electronic notification or request to deactivate/reactivate an NPE. The IRA or AAA verifies the request per agency policy and updates the NPE status in the appropriate system(s).<br>b. The NPE Administrator uses a self-service system to deactivate/activate the NPE status in the affected system(s).<br>c. The NPE status change is triggered and completed automatically based on workflows established within the agency.<br>2. The deactivated NPE is no longer available via AAES or the reactivated NPE is available via AAES. |

## 4.11 Credentialing Use Case

This use case describes the processes for binding an identity to a physical or electronic credential so that it can be used as a proxy for proving an identity claim.

### 4.11.1 Actors and Artifacts

The Credentialing Use Case Context is shown in Figure 4-7, and the identified actors are characterized in this subsection.

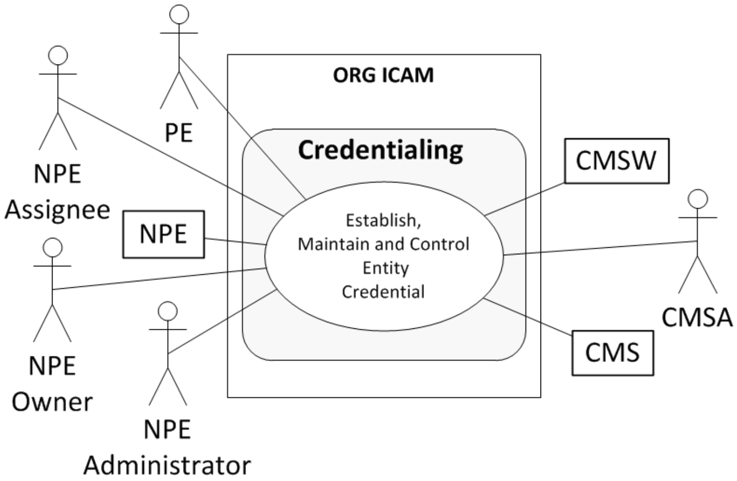


**Figure 4-7 Credentialing Use Case Context**

Person actors for the Credentialing use case are:

- **CMSA** – The CMS Administrator or authorized subordinate
- **NPE Administrator** (or privileged user)
- **NPE Assignee**
- **NPE Owner**
- **PE** – The Person Entity that is the focus of the PE use case

Non-person actors for the Credentialing use case are:

- **CMS** – The Credential Management System
- **CMSW** – The CMS Wizard
- **NPE** – The Non-Person Entity that is the focus of the NPE use case

Artifacts for the Credentialing use case are:

- **ACR** – The Authorized Credential Request
- **Credential Profile**
- **Credential** – CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, CryptoD and CryptoSS

### 4.11.2 PE Description

The following use case is covered in this section:

- ORG-02-PE: Establish, Maintain and Control PE Credential

This use case focuses on the high-level steps required to establish (enroll and issue), maintain (life-cycle management and self-service needs), and control (deactivate and reactivate) a PE authenticator credential. The authentication process binds the PE's digital identity account record to a specific resource using the credential identity attributes. Depending on the establishment process, authenticator credentials can be LOA1 or LOA2.

The Credential Profile information collected and generated by these services is persisted in a CMS that is controlled by a CMSA. The CMS exposes a CMSW to support PE authenticator life-cycle management and self-service needs.

### 4.11.3 ORG-02-PE: Establish, Maintain, and Control a PE Credential

The details of this use case are covered in:

A. Establish PE Credential (Table 4-9)

B. Maintain PE Authenticator (Table 4-10)

C. Control PE Credential (Table 4-11)

D. Maintain PE Credential Profile (Table 4-12)

**Table 4-9 Establish PE Credential**

| **Identifier** | **ORG-02-PE-A: Establish PE Credential** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to enroll and issue a PE credential. |
| Actor(s) | Person:<br>• Credential Management System Administrator (CMSA)<br>• Person Entity (PE)<br>Non-person:<br>• Credential Management System (CMS) |
| Artifact(s) | • Authorized Credential Request (ACR) – create<br>• Credential Profile<br>• Credential - CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, CryptoD and CryptoSS |
| Trigger | The CMSA receives an ACR sponsored request to establish a password authenticator credential for a PE. |
| Pre-conditions | • Sponsoring has occurred.<br>• An ACR has been generated and given to the CMSA.<br>• PE digital identity establishment is complete and the Enrollment Code has not expired. |
| Post-conditions | The PE authenticator credential is established. |
| Main Flow | 1. The CMSA authenticates and verifies the ACR.<br>2. The Enrollment Code provided by identity proofing is used to authenticate the PE.<br>3. The CMSA creates or captures the unique credential identifier record key and creates a corresponding CMS Credential Profile. The OOB channels are added to that record.<br>4. The CMSA may request knowledge-based questions. These registered knowledge authenticators are added to the CMS Credential Profile.<br>5. The CMSA creates the appropriate AAL authenticator for the credential. If the credential includes a Memorized Secret, the PE may be asked to immediately change or update the authenticator upon initial login. The new Memorized Secret is added to the CMS Credential Profile.<br>6. The CMSA verifies that the PE credential authenticates and provides the correct access control.<br>7. The CMSA provides the credential to the PE As stipulated by the applicable AAL requirements:<br>a. in person or<br>b. using one of the established OOB communication channels. |

### Table 4-10 Maintain PE Authenticator

| **Identifier** | **ORG-02-PE-B: Maintain PE Authenticator** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to renew, reissue, update, change, or reset a PE authenticator. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>• Credential Management System Administrator (CMSA)<br>Non-person:<br>• Credential Management System (CMS)<br>• CMS Wizard (CMSW) |
| Artifact(s) | • Authorized Credential Request (ACR) – maintain<br>• Credential Profile<br>• Credential - CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, CryptoD and CryptoSS |
| Trigger | An ACR to renew, reissue, update, change, or reset a credential authenticator is generated. |
| Pre-conditions | • The authenticator credential is established in the CMS.<br>• ACR  to renew, reissue, update, change, or reset his authenticator is created in one of the following ways:<br>a. The PE uses the CMSW to request the ACR and the CMSW creates it.<br>b. The PE requests the ACR and the CMSA creates it.<br>c. An automated business process creates the ARC |
| Post-conditions | The PE’s authenticator is renewed, reissued, updated, changed, or reset and the Credential Profile is updated |
| Main Flow (Memorized Secret Authenticator) | 1. The CMSW or CMSA validates the credential claim by having the PE use the current authenticator to log in to the CMSW.<br>2. The CMSW prompts the PE for a new authenticator, and the PE enters a new secret.<br>3. The CMSW prompts the PE to re-enter the new secret, and the PE re-enters a new secret.<br>4. The CMSW verifies that the two PE responses are identical.<br>5. The CMSW confirms that the new authenticator satisfies the CMS Memorized Secret policies.<br>6. The CMSW updates the CMS unique credential identifier in the Credential Profile with the new authenticator. |
| Alternate Flow (Memorized Secret Authenticator – OOB OTP valuation) | 1. The CMSW requests the unique credential identifier, and the PE provides a valid response.<br>2. The CMSW sends an OTP to the PE using one of the OOB channels established for the unique credential identifier, typically cellphone, or telephone.<br>3. The CMSW prompts the PE for the OTP, and the PE provides the correct response.<br>4. Proceed to Main Flow step 2 and continue to the end of the Main Flow. |

| **Identifier** | **ORG-02-PE-B: Maintain PE Authenticator** |
|---|---|
| Alternate Flow (Device Authenticator) | 1. The PE meets in-person with the CMSA.<br>2. The CMSA takes the device from the PE and validates the credential claim by having the PE authenticate using all of the current and supported multi-factor authenticators for the device.<br>3. The CMSA executes the ARC renewed, reissued, updated, changed, or reset action<br>4. The CMSA confirms that the updated authenticator(s) are active and that the device authenticates properly.<br>5. The CMSA updates the Credential Profile.<br>6. The CMSA returns the device to the PE. |

### Table 4-11 Control PE Credential

| **Identifier** | **ORG-02-PE-C: Control PE Credential** |
|---|---|
| Description | This flow provides the high-level steps needed for ORG to deactivate (suspend, revoke, or block) or reactivate (reinstate and unblock) a PE credential. |
| Actor(s) | Person:<br>• Credential Management System Administrator (CMSA)<br>• Person Entity (PE)<br>Non-person:<br>• Credential Management System (CMS) |
| Artifact(s) | • Authorized Credential Request (ACR) – control<br>• Credential Profile<br>• Credential - CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, Crypto and CryptoSS |
| Trigger | The CMSA receives an ACR to suspend, revoke, block, reinstate, or unblock a PE credential. |
| Pre-conditions | • The credential is established in the CMS.<br>• An ACR to suspend, revoke, block, reinstate, or unblock a PE credential is passed to the CMSA. |
| Post-conditions | The PE’s credential is deactivated (suspend, revoke, or block) or reactivated (reinstate or unblock). |
| Main Flow (Reactivate, Reinstate, or Unblock) | 1. The CMSA authenticates and verifies the ACR.<br>2. The CMSA activates the CMS Credential Profile identified by the unique credential identifier.<br>3. The CMSA notifies the PE of this change.<br>4. The CMSA provides the credential to the PE as stipulated by the applicable AAL requirements:<br>a. in person or<br>b. using one of the established OOB communication channels. |
| Alternate Flow (Deactivate, Suspend, Revoke, or Block) | 1. The CMSA authenticates and verifies the ACR.<br>2. The CMSA deactivates the CMS Credential Profile identified by the unique credential identifier.<br>3. The CMSA notifies the PE of this change.<br>4. The CMSA collects the credential from the PE as stipulated by the applicable AAL requirements. |

**Table 4-12 Maintain PE Credential Profile**

| **Identifier** | **ORG-02-PE-D: Maintain PE Credential Profile** |
|---|---|
| Description | This flow provides the high-level steps for ORG to allow a PE to update or change the OOB channels and/or knowledge authenticators in his authenticator profile. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>Non-person:<br>• Credential Management System (CMS)<br>• CMS Maintain Password Authenticator Wizard (CMSW) |
| Artifact(s) | • Authorized Credential Request (ACR) – maintain<br>• Credential Profile<br>• Credential - CryptoSH [PIV, PIV-I, CAC, DPC], Memorized Secret, Look-up Secret, OOB, OTP, CryptoD and CryptoSS |
| Trigger | The PE browses to the CMSW to update or change the OOB channels and/or knowledge authenticators. |
| Pre-conditions | • The authenticator credential is established in the CMS.<br>• The PE accesses the CMSW and makes an ACR to update or change the OOB channels or knowledge authenticators. |
| Post-conditions | The PE's OOB channels and/or knowledge authenticators have been updated in the Credential Profile. |
| Main Flow (Knowledge Authenticators and/or OOB Channels) | 1. The CMSW validates the credential claim by having the PE use the authenticator to log in.<br>2. The CMSW prompts the PE with the existing knowledge authenticators and OOB channels.<br>3. The PE uses the CMSW editing capability to add, delete, and modify the presented information (i.e., knowledge authenticators and OOB channel information).<br>4. The CMSW updates the authenticator in the CMS Credential Profile for the PE. |

### 4.11.4 NPE Description

The following use case is covered in this subsection:

- ORG-02-NPE: Establish, Maintain, and Control NPE Credential

This use case focuses on the high-level steps required for ORG to establish (enroll and issue), maintain (life cycle management and self-service needs), and control (deactivate and reactivate) an NPE credential. A credential is critical to the NPE authentication process and contains an authenticator and an NPE Digital Identity Record ID. This ID is used to bind the NPE to the Digital Identity Record once the credential authenticator has been verified and validated. The authenticator verification and validation processing provides confidence that this credential is a proxy for the NPE and therefore asserting a valid claim to its Digital Identity Record. This entity coupling to a credential is known as the binding. The confidence in this binding is called the binding strength and it is used to quantify the LOA. The NPE demonstrates the binding with the following factors: knowing a shared secret (something known), having unique control (something possessed), or having a unique characterization (something distinctive). For devices like the NPE, symmetric PKI certificates are an example of something known, asymmetric PKI certificates are an example of something possessed, and device fingerprinting is an example of something distinctive. The factors that are applied during the authentication process determine the binding strength—the confidence in an entity's claim to an identity.

The Credential Profile information collected and generated by these services is persisted in a CMS that is controlled by a CMSA. The CMS also supports just-in-time transactions and self-service needs.

### 4.11.5 ORG-02-NPE: Establish, Maintain, and Control NPE Credential

The details of this use case are provided in three sub-cases:

A. Establish NPE Credential (Table 4-13)

B. Maintain NPE Credential (Table 4-14)

C. Control NPE Credential (Table 4-15)

### Table 4-13 Establish NPE Credential

| **Identifier** | **ORG-02-NPE-A: Establish NPE Credential** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to enroll and issue a credential for an NPE. |
| Actor(s) | <u>Person</u>:<br>• Credential Management System Administrator (CMSA)<br>• NPE Assignee<br>• NPE Owner<br>• NPE Administrator<br><u>Non-person</u>:<br>• Credential Management System (CMS)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Credential Request (ACR) – create<br>• Credential Profile<br>• Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | The CMSA receives an ACR to establish a credential for an NPE. |
| Pre-conditions | • If the NPE is owned by a PTR, then ORG sponsoring has occurred.<br>• An ACR has been generated and given to the CMSA. |
| Post-conditions | The NPE is enrolled and a credential is established. |
| Main Flow | 1. The CMSA authenticates and verifies the ACR.<br>2. Identity proofing is completed in one of the following ways:<br>a. In-person identity proofing: The NPE Assignee delivers in-person the NPE Ownership and Assignee documentation that is required by ORG in-person NPE policy for CMSA inspection and verification.<br>b. Remote identity proofing: The NPE Assignee delivers electronically the NPE Ownership and Assignee documentation in the form and manner that is required by ORG remote NPE policy for CMSA inspection and verification.<br>3. The CMSA creates a unique credential ID record key and a corresponding CMS Credential Profile that includes the NPE Owner, NPE Assignee, and NPE Administrator.<br>4. The CMSA uses the CMS to create a credential and add to the CMS Credential Profile.<br>5. The NPE Administrator installs and activates the credential in the NPE.<br>6. The CMSA verifies that the NPE credential provides the correct access control.<br>7. The CMSA notifies the NPE Administrator, NPE Assignee, and NPE Owner that this change has occurred. |

### Table 4-14 Maintain NPE Credential

| **Identifier** | **ORG-02-NPE-B: Maintain NPE Credential** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to renew, reissue, update, change, or reset an NPE credential. |
| Actor(s) | Person:<br>• Credential Management System Administrator (CMSA)<br>• NPE Administrator<br>• NPE Assignee<br>• NPE Owner<br>Non-person:<br>• Credential Management System (CMS)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Credential Request (ACR) – maintain<br>• Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | The CMSA receives an ACR to renew, reissue, update, change, or reset a credential for an NPE. |
| Pre-conditions | • The NPE credential is established in the CMS.<br>• An ACR to renew, reissue, update, change, or reset an NPE credential exists. |
| Post-conditions | The NPE credential is renewed, reissued, updated, changed, or reset. |
| Main Flow | 1. When possible, the CMSA verifies the current NPE credential authenticator status in the CMS with the current NPE credential authenticator and its consistency with the requested maintenance.<br>2. The CMSA creates a new credential or authenticator, deactivates the old credential or authenticator, and adds the new credential or authenticator to the existing CMS Credential Profile.<br>3. The NPE Administrator installs and activates the new credential or authenticator in the NPE.<br>4. The CMSA verifies that the NPE credential provides the correct access control.<br>5. The CMSA notifies the NPE Administrator, NPE Assignee, and NPE Owner that this change has occurred. |

### Table 4-15 Control NPE Credential

| **Identifier** | **ORG-02-NPE-C: Control NPE Credential** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to deactivate (suspend, revoke, or block) or reactivate (reinstate and unblock) an NPE credential. |
| Actor(s) | Person:<br>• Credential Management System Administrator (CMSA)<br>• NPE Administrator<br>• NPE Assignee<br>• NPE Owner<br>Non-person:<br>• Credential Management System (CMS)<br>• Non-Person Entity (NPE) Credential |
| Artifact(s) | • Authorized Credential Request (ACR) – control<br>• Credential Profile<br>• Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | The CMSA receives an authorized ACR to suspend, revoke, block, reinstate, or unblock an NPE credential. |
| Pre-conditions | • The credential is established in the CMS.<br>• An authorized ACR to suspend, revoke, block, reinstate, or unblock the NPE credential is passed to the CMSA. |
| Post-conditions | The NPE credential is deactivated (suspend, revoke, or block) or reactivated (reinstate or unblock). |
| Main Flow (Reactivate, Reinstate, or Unblock) | 1. The CMSA activates the CMS Credential Profile identified by the unique credential ID.<br>2. The CMSA notifies the NPE Administrator, NPE Assignee, and NPE Owner that this change has occurred. |
| Alternate Flow (Deactivate, Suspend, Revoke, or Block) | 1. The CMSA deactivates the CMS Credential Profile identified by the unique credential ID.<br>2. The CMSA notifies the NPE Administrator, NPE Assignee, and NPE Owner that this change has occurred. |

## 4.12 Privilege Management Use Cases

These use cases describe the processes for establishing and maintaining the privilege attributes that comprise an individual's access profile. These attributes are features of an individual that can be used as the basis for making policy-based access decisions.

### 4.12.1 Actors and Artifacts

The Privilege Management Use Case Context is shown in Figure 4-8, and the identified actors are characterized in this subsection.

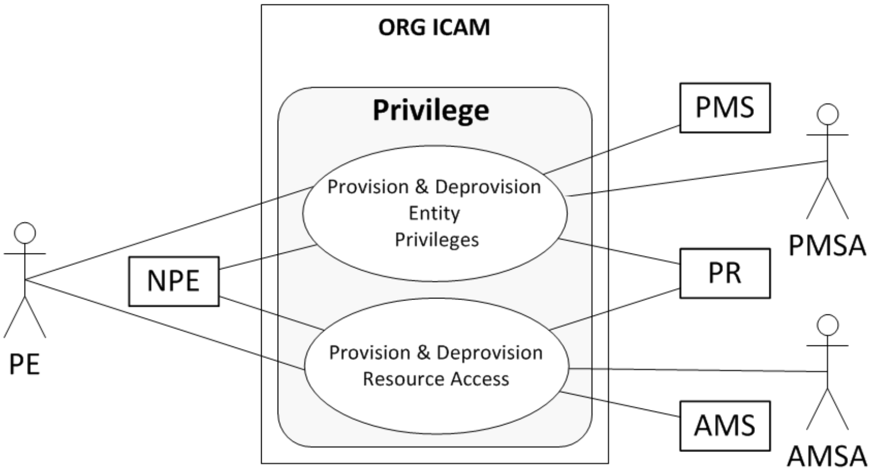

ORG ICAM
Privilege
Provision & Deprovision Entity Privileges
Provision & Deprovision Resource Access
PE
NPE
PMS
PMSA
PR
AMSA
AMS

**Figure 4-8 Privilege Management Use Case Context**

Person actors for the Privilege Management use cases are:

- **AMSA** – The AMS Administrator or authorized subordinate
- **PE** – The Person Entity that is the focus of the PE use case
- **PMSA** – The PMS Administrator or authorized subordinate

Non-person actors for the Privilege Management use cases are:

- **AMS** – The Account Management System
- **NPE** – The Non-Person Entity that is the focus of the NPE use case
- **PMS** – The Privilege Management System
- **PR** – The Protected Resource including MSS, MND and MSP

Artifacts for the Privilege Management use cases are:

- **APAR** – The Authorized Privilege and Account Request

- **APPR** – The Authorized Privilege and Profile Request
- **Identity Record**
- **Authorization Profile**
- **Credential Profile**
- **Resource Privilege**
- **Account**

### 4.12.2 PE Description

The following use cases are covered in this section:

- ORG-03-PE: Provision and Deprovision PE Privileges
- ORG-04-PE: Provision and Deprovision PE Resource Access

These use cases describe the high-level life-cycle steps required for ORG to assign, suspend, restore, and remove Resource Privileges for a PE within the scope of applicable business activities and environments. Resource Privileges enumerate the accesses, actions, operations, and application roles that are supported by each PR and are assigned as PE privileged rights that satisfy the specific access control policies that are required for a PE by each PR. A resource specific Authorization Profile captures these business characteristics and maintains them for each PE. PRs create Accounts to maintain the PE specific preferences and assigned PE privileges. The Account Policy influences the transformation of PE Authorization Profile data to PE privileges in the Account through the execution of the Account Policy of that PR.

### 4.12.3 ORG-03-PE: Provision and Deprovision PE Privileges

The details of this use case are covered in:

A. Establish PE Authorization Profile (Table 4-16)

B. Establish PE PR Privilege (Table 4-17)

C. Control PE PR Privilege (Table 4-18)

D. Control PE Authorization Profile (Table 4-19)

### Table 4-16 Establish PE Authorization Profile

| Identifier | ORG-03-PE-A: Establish PE Authorization Profile |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to establish (create, restore) an Authorization Profile for a PE. ORG-04-PE must be completed (before, after, or concurrently) before the PE has the authorized PR access. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS)<br>• Protected Resource (PR) |
| Artifact(s) | • Authorized Privilege and Profile Request (APPR) – establish<br>• Identity Record<br>• Authorization Profile<br>• Credential Profile |
| Trigger | The PMSA receives an APPR to assign a PE privilege or restore an Authorization Profile for a PE. |
| Pre-conditions | The PE does not have an active Authorization Profile in the PMS. |
| Post-conditions | The PE has an active Authorization Profile. |
| Main Flow<br>(Create) | 1. The PMSA adds the PE Authorization Profile to the PMS.<br>2. The PMSA confirms that the Identity Record identifies the correct PE, that the associated Credential Profiles contain the correct credential identity attributes for the appropriate PR, and that the Identity Record is also associated with the PR Authorization Profile.<br>3. The PMSA activates the PE Authorization Profile. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow<br>(Restore) | 1. The PMSA confirms that the Identity Record identifies the correct PE, that the associated Credential Profiles contain the correct credential identity attributes for the appropriate PR, and that the Identity Record is also associated with the PR Authorization Profile.<br>2. The PMSA activates the PE Authorization Profile. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-17 Establish PE PR Privilege

| Identifier | ORG-03-PE-B: Establish PE PR Privilege |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to establish (assign, restore) a PE PR privilege. ORG-04-PE must be completed (before, after, or concurrently) before the PE has the authorized PR access. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS) |
| Artifact(s) | • Authorized Privilege and Profile Request (APPR) – establish<br>• Authorization Profile |
| Trigger | The PMSA receives an APPR to restore or assign a PE PR privilege. |
| Pre-conditions | The PE has an active Authorization Profile in the PMS. |
| Post-conditions | The PE’s Authorization Profile contains the requested PE PR privilege, and it is active. |
| Main Flow (Restore) | 1. The PMSA confirms that the requested PE PR privilege attributes are in the PE’s Authorization Profile.<br>2. The PMSA activates the requested PE PR privilege in the PE’s Authorization Profile. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow (Assign) | 1. The PMSA confirms that the requested PE PR privilege attributes are not in the PE’s Authorization Profile.<br>2. The PMSA adds the requested PE PR privilege to the PE’s Authorization Profile by adding the attributes and updating the appropriate attribute values.<br>3. The PMSA activates the requested PE PR privilege in the PE’s Authorization Profile. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

**Table 4-18 Control PE PR Privilege**

| **Identifier** | **ORG-03-PE-C: Control PE PR Privilege** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to control (suspend, deactivate, unassign) a PE PR privilege. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS) |
| Artifact(s) | • Authorized Privilege<br>• and Profile Request (APPR) – control<br>• Authorization Profile |
| Trigger | The PMSA receives an authorized request to suspend or deactivate a PE PR privilege. |
| Pre-conditions | The PE has an active Authorization Profile in the PMS. |
| Post-conditions | The requested PE PR privilege is no longer active in the PE Authorization Profile. |
| Main Flow<br>(Suspend, Deactivate) | 1. The PMSA confirms that the requested PE PR privilege attributes are in the PE's Authorization Profile.<br>2. The PMSA deactivates the requested PE PR privilege. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow<br>(Unassign) | 1. The PMSA confirms that the requested PE PR privilege attributes are in the PE's Authorization Profile.<br>2. The PMSA removes the requested PE PR privilege from the PE's Authorization Profile by updating the appropriate attribute values. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

## Table 4-19 Control PE Authorization Profile

| **Identifier** | **ORG-03-PE-D: Control PE Authorization Profile** |
|---|---|
| Description | The high-level steps needed for ORG to control (suspend, deactivate) an Authorization Profile for a PE. ORG-04-PE must be completed (before, after, or concurrently) before the PE has the authorized PR access. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS) |
| Artifact(s) | • Authorized Privilege and Profile Request (APPR) – control<br>• Authorization Profile |
| Trigger | The PMSA receives an APPR to suspend or deactivate an Authorization Profile for a PE. |
| Pre-conditions | The PE has an active Authorization Profile in the PMS. |
| Post-conditions | The requested PE Authorization Profile is no longer active. |
| Main Flow (Control, Suspend, Deactivate) | 1. The PMSA suspends or deactivates each PE privilege in the PE's Authorization Profile.<br>2. The PMSA suspends or deactivates the requested Authorization Profile. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

### 4.12.4 ORG-04-PE: Provision and Deprovision PE Resource Access

This use cases focuses on the high-level life cycle steps required for ORG to capture, provision, modify, and deprovision the privileged set of actions, operations, and application roles that are available to a PE for a PR within the scope of applicable business activities and environments.

The details of this use case are covered in:

A. Capture Resource Privileges (Table 4-20)

B. Provision PE for PR Access (Table 4-21)

C. Modify PE Permissions for PR (Table 4-22)

D. Deprovision PE from PR (Table 4-23)

**Table 4-20 Capture Resource Privileges**

| **Identifier** | **ORG-04-PE-A: Capture Resource Privileges** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to create and maintain a complete list of the accesses, actions, operations, and application roles that are available to a PE for a PR. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>• Person Entity (PE)<br>Non-person:<br>• Account Management System (AMS)<br>• Protected Resource (PR) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – capture<br>• Resource Privilege |
| Trigger | A PR is added, updated or removed from ORG and the AMSA revives an APAR containing a new authorized list of actions, operations, and application roles that are available as Resource Privileges for the PR. |
| Pre-conditions | None |
| Post-conditions | The AMS contains the Resource Privileges for a PR. |
| Main Flow<br>(Create) | 1. The AMSA confirms that the PR is not currently managed in the AMS.<br>2. The AMSA creates an entry in the AMS for the identified PR.<br>3. The AMSA updates the Resource Privileges to coincide with the APAR. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow<br>(Maintain) | 1. The AMSA confirms that the PR is managed in the AMS.<br>2. The AMSA updates the Resource Privileges to coincide with the APAR. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-21 Provision PE for PR Access

| **Identifier** | **ORG-04-PE-B: Provision PE for PR Access** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to establish a PE Account with the authorized PR access permissions. ORG-03-PE must be completed (before, after, or concurrently) before the PE has the authorized PR access. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>• Person Entity (PE)<br>Non-person:<br>• Account Management System (AMS)<br>• Protected Resource (PR) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – provision<br>• Account |
| Trigger | The PE requires PR access and a provisioning APAR for the EPD is generated. |
| Pre-conditions | The PE does not have an Account in the AMS. |
| Post-conditions | The PE has an Account with the appropriate PR Access in the AMS. |
| Main Flow<br>(Manual) | 1. The AMSA receives the provisioning APAR.<br>2. The AMSA validates that there is no Account and that the PE needs access to the PR. The AMSA provides electronic approval.<br>3. The AMSA creates an Account for the PE with the appropriate access permissions in the AMS. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow<br>(Just-in-time) | 1. A predefined trigger (e.g., PR access attempt with no account) initiates the provisioning process without intervention.<br>2. An account for the PE is created with privileges defined by ORG policy. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-22 Modify PE Permissions for PR

| **Identifier** | **ORG-04-PE-C: Modify PE Permissions for PR** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to maintain and control a PE Account with the authorized PR access permissions. ORG-03-PE must be completed (before, after, or concurrently) before the PE has the authorized PR access. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>• Person Entity (PE)<br>Non-person:<br>• Account Management System (AMS)<br>• Protected Resource (PR) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – modify<br>• Account |
| Trigger | The PE requires a change in PR access permissions. |
| Pre-conditions | The PE has an Account for the PR in the AMS. |
| Post-conditions | The PE has appropriate Account access permissions for the PR in the AMS. |
| Main Flow<br>(Manual) | 1. The AMSA receives the modify APAR.<br>2. The AMSA validates that there is an Account and that the PE needs these access permissions to the PR. The AMSA provides electronic approval.<br>3. The AMSA modifies the Account for the PE with the appropriate access permissions in the AMS. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow<br>(Just-in-time) | 1. A predefined trigger (e.g., an assignment change) initiates the modify process without intervention.<br>2. The account permissions for the PE are modified with privileges defined by ORG policy. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

**Table 4-23 Deprovision PE from PR**

| **Identifier** | **ORG-04-PE-D: Deprovision PE from PR** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to deprovision a PE Account and deactivate the authorized PR access permissions. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>• Person Entity (PE)<br>Non-person:<br>• Account Management System (AMS)<br>• Protected Resource (PR) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – deprovision<br>• Account |
| Trigger | The PE no longer requires access to the PR. |
| Pre-conditions | The PE has an active Account with access permissions for the PR in the AMS. |
| Post-conditions | The PE no longer has an active Account for the PR in the AMS. |
| Main Flow<br>(Manual) | 1. The AMSA receives the deprovision APAR.<br>2. The AMSA validates that there is an Account and that the PE no longer needs access to the PR. The AMSA provides electronic approval.<br>3. The AMSA deprovisions the Account for the PE in the AMS. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow<br>(Just-in-time) | 1. A predefined trigger (e.g., an assignment change) initiates the deprovision process without intervention.<br>2. The account for the PE is deprovisioned. Sufficient records are maintained about the PE account and activities such that complete auditing functions can be performed for a specified period of time. |

### 4.12.5 NPE Description

The following use cases are covered in this subsection:

- ORG-03-NPE: Provision and Deprovision NPE Privileges
- ORG-04-NPE: Provision and Deprovision NPE Resource Access

These use cases describe the high-level life cycle steps required for ORG to assign, suspend, restore, and remove Resource Privileges for an NPE within the scope of applicable business activities and environments. Resource Privileges enumerate the actions, operations, and application roles that are supported by each PR and are assigned as NPE privileged rights that satisfy the specific access control policies that are required for an NPE by each PR. The IdPs maintain resource specific Authorization Profile that capture these business characteristics and maintains them for each NPE. The SPs create Accounts to maintain the NPE User specific preferences and assigned privileges for the specific NPE. The NPE Account Policy influences the transformation of NPE Authorization Profile data to Account privileges through the execution of the Account Policy of that PR.

### 4.12.6 ORG-03-NPE: Provision and Deprovision NPE Privileges

The details of this use case are provided in four sub-cases:

A. Establish NPE Authorization Profile (Table 4-24)

B. Establish NPE PR Privilege (Table 4-25)

C. Control NPE PR Privilege (Table 4-26)

D. Control NPE Authorization Profile (Table 4-27)

**Table 4-24 Establish NPE Authorization Profile**

| **Identifier** | **ORG-03-NPE-A: Establish NPE Authorization Profile** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to establish (create, restore) an Authorization Profile for an NPE. |
| Actor(s) | Person:<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS)<br>• Protected Resource (PR)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Profile Request (APPR) – establish<br>• Identity Record<br>• Authorization Profile<br>• Credential Profile |
| Trigger | The PMSA receives an APPR to assign an NPE privilege or restore an Authorization Profile for an NPE. |
| Pre-conditions | The NPE does not have an active Authorization Profile in the PMS. |
| Post-conditions | The NPE has an active Authorization Profile. |
| Main Flow (create) | 1. The PMSA adds the NPE Authorization Profile to the PMS.<br>2. The PMSA confirms that the Identity Record identifies the correct NPE, that the associated Credential Profiles contain the correct credential identity attributes for the appropriate PR, and that the Identity Record is also associated with the PR Authorization Profile.<br>3. The PMSA activates the NPE Authorization Profile. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow (restore) | 1. The PMSA confirms that the Identity Record identifies the correct NPE, that the associated Credential Profiles contain the correct credential identity attributes for the appropriate PR, and that the Identity Record is also associated with the PR Authorization Profile.<br>2. The PMSA activates the NPE Authorization Profile. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-25 Establish NPE PR Privilege

| **Identifier** | **ORG-03-NPE-B: Establish NPE PR Privilege** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to establish (assign, restore) a PR privilege to an NPE. |
| Actor(s) | Person:<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS)<br>• Protected Resource (PR)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Profile Request (APPR) – establish<br>• Authorization Profile |
| Trigger | The PMSA receives an APPR to restore or assign a PR privilege to an NPE. |
| Pre-conditions | The NPE has an active Authorization Profile in the PMS. |
| Post-conditions | The NPE Authorization Profile contains the requested PR privilege, and it is active. |
| Main Flow (assign) | 1. The PMSA confirms that the requested PR privilege attributes are not in the NPE Authorization Profile.<br>2. The PMSA adds the requested PR privilege to the NPE Authorization Profile by adding the attributes and updating the appropriate attribute values.<br>3. The PMSA activates the requested PR privilege in the NPE Authorization Profile. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow (restore) | 1. The PMSA confirms that the requested PR privilege attributes are in the NPE Authorization Profile.<br>2. The PMSA activates the requested PR privilege in the NPE Authorization Profile. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-26 Control NPE PR Privilege

| **Identifier** | **ORG-03-NPE-C: Control NPE PR Privilege** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to control (suspend, deactivate, unassign) a PR privilege for an NPE. |
| Actor(s) | Person:<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS)<br>• Protected Resource (PR)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Profile Request (APPR) – control<br>• Authorization Profile |
| Trigger | The PMSA receives an APPR to suspend or deactivate a PR privilege for an NPE. |
| Pre-conditions | The NPE has an active Authorization Profile in the PMS. |
| Post-conditions | The requested PR privilege is no longer active in the NPE Authorization Profile. |
| Main Flow (suspend, deactivate) | 1. The PMSA confirms that the requested PR privilege attributes are in the NPE Authorization Profile.<br>2. The PMSA deactivates the requested PR privilege. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow (unassign) | 1. The PMSA confirms that the requested PR privilege attributes are in the NPE Authorization Profile.<br>2. The PMSA removes the requested PR privilege from the NPE Authorization Profile by updating the appropriate attribute values. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-27 Control NPE Authorization Profile

| **Identifier** | **ORG-03-NPE-D: Control NPE Authorization Profile** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to control (suspend, deactivate) an Authorization Profile for an NPE. |
| Actor(s) | Person:<br>• Privilege Management System Administrator (PMSA)<br>Non-person:<br>• Privilege Management System (PMS)<br>• Protected Resource (PR)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Profile Request (APPR) – control<br>• Authorization Profile |
| Trigger | The PMSA receives an APPR to suspend or deactivate an Authorization Profile for an NPE. |
| Pre-conditions | The NPE has an active Authorization Profile in the PMS. |
| Post-conditions | The requested NPE Authorization Profile is no longer active. |
| Main Flow | 1. The PMSA suspends or deactivates each PR privilege in the NPE Authorization Profile.<br>2. The PMSA suspends or deactivates the requested Authorization Profile. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

### 4.12.7 ORG-04-NPE: Provision and Deprovision NPE Resource Access

The details of this use case are provided in four sub-cases:

A. Capture Resource Privileges (Table 4-28)

B. Provision NPE for PR Access (Table 4-29)

C. Modify NPE Permissions for PR (Table 4-30)

D. Deprovision NPE from PR (Table 4-31)

**Table 4-28 Capture Resource Privileges**

| **Identifier** | **ORG-04-NPE-A: Capture Resource Privileges** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to create and maintain a complete list of the accesses, actions, operations, and application roles that are available to a NPE for a PR. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>Non-person:<br>• Protected Resource (PR)<br>• Account Management System (AMS)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – capture<br>• Resource Privilege |
| Trigger | A PR is added, updated or removed from ORG and the AMSA receives an APAR containing a new authorized list of actions, operations, and application roles that are available as Resource Privileges for the PR. |
| Pre-conditions | None |
| Post-conditions | The AMS contains the Resource Privileges for a PR. |
| Alternate Flow (create) | 1. The AMSA confirms that the PR is not currently managed in the AMS.<br>2. The AMSA creates an entry in the AMS for the identified PR.<br>3. The AMSA updates the Resource Privileges to coincide with the APAR. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Main Flow (maintain) | 1. The AMSA confirms that the PR is managed in the AMS.<br>2. The AMSA updates the Resource Privileges to coincide with the APAR. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-29 Provision NPE for PR Access

| **Identifier** | **ORG-04-NPE-B: Provision NPE for PR Access** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to establish an NPE Account with the authorized PR access permissions. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>Non-person:<br>• Protected Resource (PR)<br>• Account Management System (AMS)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – provision<br>• Account |
| Trigger | An NPE requires PR access and a provisioning APAR for the NPE is generated. |
| Pre-conditions | The NPE does not have an Account in the AMS. |
| Post-conditions | The NPE has an Account with the appropriate PR Access in the AMS. |
| Main Flow (manual) | 1. The AMSA receives the provisioning APAR.<br>2. The AMSA validates that there is no Account and that the NPE needs access to the PR. The AMSA provides electronic approval.<br>3. The AMSA creates an Account for the NPE with the appropriate access permissions in the AMS. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |
| Alternate Flow (just-in-time) | 1. A predefined trigger (e.g., PR access attempt with no account) initiates the provisioning process without intervention.<br>2. An account for the NPE is created with privileges defined by ORG policy. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-30 Modify NPE Permissions for PR

| Identifier | ORG-04-NPE-C: Modify NPE Permissions for PR |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to maintain and control a PE User Account with the authorized PR access permissions. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>Non-person:<br>• Protected Resource (PR)<br>• Account Management System (AMS)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – modify<br>• Account |
| Trigger | An NPE requires PR access updates and a modification APAR for the NPE is generated. |
| Pre-conditions | The NPE has an Account for the PR in the AMS. |
| Post-conditions | The NPE has appropriate Account access permissions for the PR in the AMS. |
| Main Flow | 1. AMSA receives the modification APAR<br>2. The AMSA validates that there is an Account and that the NPE needs these access permissions. The AMSA provides electronic approval.<br>3. The AMSA updates the Account for the NPE with the APAR access permissions in the AMS. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

### Table 4-31 Deprovision NPE from PR

| Identifier | ORG-04-NPE-D: Deprovision NPE from PR |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to deprovision a NPE Account and deactivate the authorized PR access permissions. |
| Actor(s) | Person:<br>• Account Management System Administrator (AMSA)<br>Non-person:<br>• Protected Resource (PR)<br>• Account Management System (AMS)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authorized Privilege and Account Request (APAR) – deprovision<br>• Account |
| Trigger | An NPE no longer requires access to the PR and a deprovision APAR for the NPE is generated. |
| Pre-conditions | The NPE has an active Account with access permissions for the PR in the AMS. |
| Post-conditions | The NPE no longer has an active Account for the PR in the AMS. |
| Main Flow | 1. AMSA receives the deprovision APAR.<br>2. The AMSA validates that there is an Account and that the NPE no longer needs these access permissions. The AMSA provides electronic approval.<br>3. The AMSA removes the Account for the NPE from the AMS. Sufficient records are maintained about the NPE account and activities such that complete auditing functions can be performed for a specified period of time. |

## 4.13 Authentication Use Case

This use case describes the processes for verifying that an identity claim is genuine and proven with a valid credential.

### 4.13.1 Actors and Artifacts

The Authentication Use Case Context is shown in Figure 4-9, and the identified actors are characterized in this subsection.

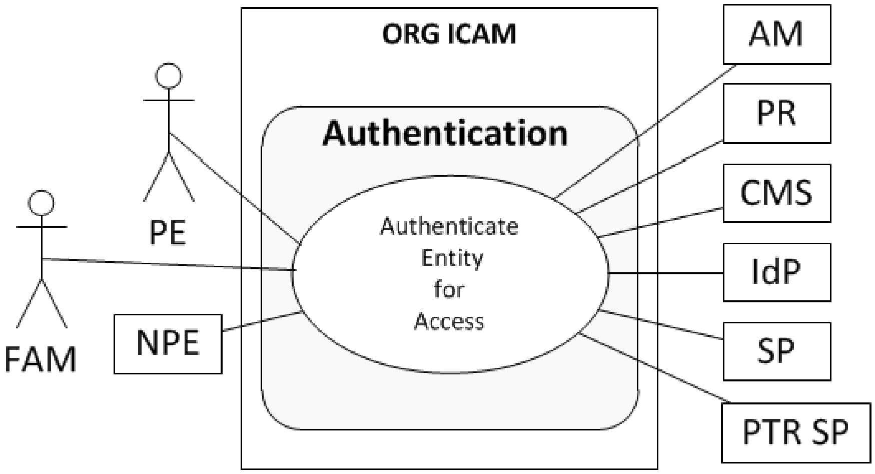


**Figure 4-9 Authentication Use Case Context**

Person actors for the Authentication use case are:

- **FAM** – The ORG Facility Access Manager
- **PE** – The Person Entity that is the focus of the PE use case

Non-person actors for the Authentication use case are:

- **AM** – The ORG Access Manager component of the Physical Access Control System (PACS) or LACS
- **CMS** – The ORG Credential Management System
- **IdP** – The ORG Identity Provider
- **NPE** – The Non-Person Entity that is the focus of the NPE use case
- **PR** – The ORG Protected Resource
- **PTR SP** – The Partner Service Provider
- **SP** – The ORG Service Provider

Artifacts for the Authentication use care are:

- **AND** – The Authentication Data and Results
- **Credential Profile**
- **Credential** – CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, Crypto and CryptoSS
- **Paperwork** – Documented and authoritative permission to physically transport equipment into or out of an ORG facility

### 4.13.2 PE Description

The following use case is covered in this section:

- ORG-05-PE: Authenticate PE for Access

This use case focuses on the high-level steps required for ORG to authenticate ORG and PTR PEs when they request access to a PR. A PE is considered internal to the organization when his affiliation establishes that organization is his primary IdP. A PE is identified as external when his primary affiliation is with a PTR and the PE provides information to organization during the course of doing business. A PACS AM is deployed by ORG to manage PE physical ingress and egress. A LACS AM is deployed by ORG to manage enterprise and federated PE access to applications. The AM is responsible for orchestrating the authentication and authorization of PE access to PRs. The IdP conceptual data elements shown in Figure 4-2 are PE focused and support authentication processing, whereas the SP conceptual data elements are PR focused and support authorization processing. This is an authentication use case and therefore the organization is the IdP.

When a PE attempts to gain access to an ORG site, facility or controlled area, the AM challenges the ORG or PTR PE to authenticate with an approved credential as part of the ORG PACS. The ORG PACS authorizes and enforces access. When the PE does not have a credential that is provisioned in the PACS, the FAM applies the ORG physical access control security policies to authenticate the PE. The FAM authorizes and enforces access.

When a PE attempts to use an EPD, the AM domain controller challenges the PE to authenticate with an approved credential as part of the network LACS. Each time an ORG or PTR PE attempts to again access to a PR, the AM challenges the requesting PE to authenticate with a credential type that is accepted by that PR. Organizations may deploy Single Sign-On (SSO) approaches that improve the user experience by hiding additional authentication challenges. SSO is designed as a transparent authentication capability and provided as a service extension of the IdP.

The authentication process validates the integrity and trust of the presented credential and challenges the PE to prove his right to claim the identity that is bound to the identity by providing the correct responses to one or more factors – something you have, know, are, and do.

The AM collects the authentication data and results, bundles it with the credential unique identifier, and delivers it to the SP for authorization processing.

ORG and PTR enterprises issue trusted digital credentials, gather identity attributes and establish and manage Identity Records, Credential Profiles and Account Profiles for each enrolled PE. Federation allows ORG to leverage these remote PTR capabilities but requires that each PTR exposes IdP authentication and attribute retrieval services. It also requires that ORG establish a mutual trust agreement with all participating PTR IdPs and SPs.

### 4.13.3 ORG-05-PE: Authenticate PE for Access

The details of this use case are covered in:

A. PE Facility Authentication (Table 4-32)

B. PE Enterprise Authentication (Table 4-33)

C. PE Federated Authentication (Table 4-34)

**Table 4-32 PE Facility Authentication**

| **Identifier** | **ORG-05-PE-A: PE Facility Authentication** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authenticate and log the entry and exit of a PE within ORG facilities. |
| Actor(s) | Person:<br>• Facility Access Manager (FAM)<br>• Person Entity (PE)<br>Non-person:<br>• Access Manager (AM) – PACS |
| Artifact(s) | None |
| Trigger | A PE is entering or exiting an ORG facility. |
| Pre-conditions | None |
| Post-conditions | The PE facility access is permitted or denied and the entry or exit of the PE is logged. |
| Main Flow<br>(Enter – credentialed) | 1. The FAM examines the PE credential.<br>2. The PE presents his credential to the AM.<br>3. The AM permits or denies PE access.<br>4. The AM logs the time, PE information and the access decision. |
| Alternate Flow<br>(Enter – not credentialed) | 1. The FAM examines ORG required identity documents and the access reason provided by PE.<br>2. The PE is searched.<br>3. The FAM approves or disapproves PE and possessions access to the facility and logs the time, PE information and access decision.<br>4. The FAM issues a temporary credential.<br>5. The FAM provides an escort when required.<br>6. The PE enters. |
| Alternate Flow<br>(Exit – credentialed) | 1. The PE presents his credential to the AM.<br>2. The AM logs the time, PE information and the exit.<br>3. The PE exits. |
| Alternate Flow<br>(Exit – not credentialed) | 1. FAM collects temporary credential and returns any possessions.<br>2. The FAM logs the time, PE information and the exit.<br>3. The PE exits. |

### Table 4-33 PE Enterprise Authentication

| **Identifier** | **ORG-05-PE-B: PE Enterprise Authentication** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authenticate an ORG PE that is requesting access to an ORG PR or SP. |
| Actor(s) | Person:<br>• ORG Person Entity (PE)<br>Non-person:<br>• Access Manager (AM) – LACS<br>• Credential Management System (CMS)<br>• ORG Protected Resource (PR)<br>• ORG Service Provider (SP) |
| Artifact(s) | • Authentication Data and Results (AND)<br>• Credential - CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, Crypto and CryptoSS<br>• Credential Profile |
| Trigger | An ORG PE attempts to access a PR or SP. |
| Pre-conditions | The ORG PE has a valid credential for the PR or SP. |
| Post-conditions | PE Authentication is complete |
| Main Flow | 1. The AM challenges the PE to select a credential type.<br>2. The PE selects either:<br>a. The smartcard option and presents the card to the local terminal reader (first factor – something you have).<br>Go to step 1 of Shared Flow (PIV, PIV-I, CAC) and continue.<br>b. The smartphone or tablet with DPC option<br>Go to step 1 of Shared Flow (DPC) and continue<br>c. The Memorized Secret option.<br>Go to step 1 of Shared Flow (Memorized Secret) and continue.<br>d. The OTP device option.<br>Go to step 1 of Shared Flow (OTP device) and continue.<br>e. The CryptoD option.<br>Go to step 1 of Shared Flow (CryptoD) and continue.<br>3. The AM transforms the AND into an assertion form that is accepted by the PR or SP.<br>4. The AM passes the authentication assertion to the PR or SP. |
| Alternate Flow (SSO) | 1. An ORG PE has successfully authenticated and attempts accessing a different PR or SP in the same session.<br>2. The PR or SP requests an SSO authentication assertion from the AM.<br>3. The AM provides an SSO authentication assertion to the PR or SP. |

| Identifier | ORG-05-PE-B: PE Enterprise Authentication |
|---|---|
| Shared Flow<br>(PIV, PIV-I, CAC) | 1. The local terminal accesses the smartcard, validates the smartcard integrity and expiration, and validates the public Card Authentication Key (CAK) and the subject Authentication Certificate (AuthN Cert) trust, expiration, revocation, and policy Object Identifiers (OIDs) using standards-compliant PKI path validation [Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP), Server-based Certificate Validation Protocol (SCVP), etc.].<br>2. The local terminal challenges the PE for the smartcard Personal Identification Number (PIN) (second factor – something you know).<br>3. The PE provides the correct PIN, and the local terminal verifies that the smartcard is unlocked.<br>4. The local terminal verifies that the AuthN Cert key pair is valid.<br>5. When the local terminal has a fingerprint reader (third factor – something you are) else go to step 6:<br>a. The local terminal challenges the PE to provide his fingerprint.<br>b. The local terminal verifies that the PE fingerprint matches the one on the smartcard.<br>6. The AM passes the public AuthN Cert, or unique attributes from it, to the local CMS for Credential Profile verification.<br>7. The AM extracts the credential unique identifier from the AuthN Cert and aggregates it with the credential type, factor types, verified public AuthN Cert, and the collected verification data into an AND.<br>8. Proceed to Main Flow step 3 |
| Shared Flow<br>(DPC) | 1. The smartphone or tablet challenges the PE for the DPC PIN (second factor – something you know).<br>2. The PE provides the correct PIN, and the smartphone or tablet verifies that the CryptoSS or CryptoSH container is unlocked.<br>3. The smartphone or tablet passes the public AuthN Cert, or unique attributes from it, to the local CMS for Credential Profile verification.<br>4. The smartphone or tablet extracts the credential unique identifier from the AuthN Cert and aggregates it with the credential type, factor types, verified public AuthN Cert, and the collected verification data into an AND.<br>5. The smartphone or tablet transforms the AND into an assertion form that is accepted by the PR or SP.<br>6. The smartphone or tablet passes the authentication assertion to the PR or SP |

| Identifier | ORG-05-PE-B: PE Enterprise Authentication |
|---|---|
| Shared Flow<br>(Memorized Secret) | 1. The AM challenges the PE to provide the Memorized Secret credential data (first factor – something you know).<br>2. The PE provides the correct Memorized Secret credential data.<br>3. The AM passes the PE response to the local CMS for Credential Profile verification.<br>4. The CMS verified response may be combined with an OOB channel from the Credential Profile (second factor – something you have). When an OOB is provided, the AM either:<br>a. Sends an OTP to the PE using the OOB channel, prompts the PE for the OTP, and then the PE provides the correct response.<br>b. Sends a message to the PE using the OOB channel and waits a prescribed time for the PE to acknowledge receipt<br>5. The CMS verified response may be combined with a Look-up Secret (second factor – something you have) where the AM verifier prompts the user with the identifier(s) and the user responds with the secret(s)<br>6. The AM aggregates the credential, factor types, credential unique identifier (username), and the collected verification data into an AND.<br>7. Proceed to Main Flow step 3. |
| Shared Flow<br>(OTP Device) | 1. The AM challenges the PE to provide the OTP device displayed PIN (first factor – something you have).<br>2. The PE provides the correct PIN<br>3. The AM challenges the PE to use the OTP device keypad to provide a Memorized Secret (second factor – something you know)<br>4. The PE provides the correct secret<br>5. The AM aggregates the credential, factor types, credential unique identifier, and the collected verification data into an AND.<br>6. Proceed to Main Flow step 3. |
| Shared Flow<br>(CryptoD) | 1. The AM challenges the PE to select the stored PKI key pair (first factor – something you have).<br>2. The PE selects a PKI key pair<br>3. The AM validates the PKI key trust, expiration, revocation, and policy OIDs using standards-compliant PKI path validation CRL, OCSP, SCVP, etc.).<br>4. The AM uses an authentication protocol to insure that the PE possesses and controls the PKI private key<br>5. The AM aggregates the credential, factor types, credential unique identifier, and the collected verification data into an AND.<br>6. Proceed to Main Flow step 3. |

### Table 4-34 PE Federated Authentication

| **Identifier** | **ORG-05-PE-C: PE Federated Authentication** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authenticate an ORG PE that is requesting access to a PTR SP |
| Actor(s) | Person:<br>• ORG Internal Person Entity (PE)<br>Non-person:<br>• Credential Management System (CMS) supporting the IdP<br>• Identity Provider service provided by ORG (IdP)<br>• Partner organization Protected Resource Service Provider (PTR SP) |
| Artifact(s) | • Authentication Data and Results (AND)<br>• Credential - CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, CryptoD and CryptoSS |
| Trigger | An ORG PE needs to access a PTR SP. |
| Pre-conditions | PE has a credential that is accepted by the PTR SP. |
| Post-conditions | PE authentication is complete, and the PTR SP is ready for ORG-06-PE authorization processing. |
| Main Flow<br>(SP Initiated) | 1. An ORG PE attempts accessing a PTR SP.<br>2. The PTR SP presents a list of IdPs that generate authentication assertions that are acceptable to the PTR SP.<br>3. The PE selects an IdP.<br>4. The PTR SP redirects the PE session to the selected IdP.<br>5. Go to Alternate Flow (Credential Processing) step 1 and continue to the end; then return here at step 5.<br>6. The IdP transforms the AND into an assertion form that is accepted by the PTR SP.<br>7. The IdP redirects the PE session and provides the authentication assertion to the PTR SP. |
| Alternate Flow<br>(IdP Initiated) | 1. An ORG PE attempts accessing the ORG IdP.<br>Go to Alternate Flow (Credential Processing) step 1 and continue to the end; then return here at step 2.<br>2. The IdP presents a list of PTR SPs that accepts its authentication assertions.<br>3. The PE selects a PTR SP.<br>4. The IdP transforms the AND into an assertion form that is accepted by the PTR SP.<br>5. The IdP redirects the PE session and provides the authentication assertion to the selected PTR SP. |
| Alternate Flow<br>(SSO) | 1. An ORG PE has successfully authenticated using the ORG IdP and attempts accessing a different PTR SP in the same session.<br>2. The PTR SP identifies the ORG IdP and requests an SSO authentication assertion.<br>3. The ORG IdP SSO service provides the SSO authentication assertion to the PTR SP. |

| **Identifier** | **ORG-05-PE-C: PE Federated Authentication** |
|---|---|
| Shared Flow<br>(Credential Processing) | 1. The IdP challenges the PE to select a credential type.<br>2. The PE selects either:<br>a. The smartcard option and presents the card to the local terminal reader (first factor – something you have)<br>Go to step 1 of Shared Flow (PIV, PIV-I, CAC) and continue<br>b. The smartphone or tablet with DPC option<br>Go to step 1 of Shared Flow (DPC) and continue<br>c. The Memorized Secret option<br>Go to step 1 of Shared Flow (Memorized Secret) and continue.<br>d. The OTP device option.<br>Go to step 1 of Shared Flow (OTP device) and continue.<br>e. The CryptoD option.<br>Go to step 1 of Shared Flow (CryptoD) and continue.<br>3. Return to either Main Flow (SP Initiated) step 5 or Alternate Flow (IdP Initiated) step 2. |
| Shared Flow<br>(PIV, PIV-I, CAC) | 1. The local terminal accesses the smartcard, validates the smartcard integrity and expiration, and validates the public CAK and the subject AuthN Cert trust, expiration, revocation, and policy OIDs using standards-compliant PKI path validation (CRL, OCSP, SCVP, etc.).<br>2. The local terminal challenges the PE for the smartcard PIN (second factor – something you know).<br>3. The PE provides the correct PIN, and the local terminal verifies that the smartcard is unlocked.<br>4. The local terminal verifies that the AuthN Cert key pair is valid.<br>5. When the local terminal has a fingerprint reader (third factor – something you are):<br>a. The local terminal challenges the PE to provide his fingerprint.<br>b. The local terminal verifies that the PE fingerprint matches the one on the smartcard.<br>6. The IdP passes the public AuthN Cert, or unique attributes from it, to the local CMS for Credential Profile verification.<br>7. The IdP extracts the credential unique identifier from the AuthN Cert and aggregates it with the credential type, factor types, verified public AuthN Cert, and the collected verification data into an AND.<br>8. Proceed to Shared Flow (Credential Processing) step 3. |
| Shared Flow<br>(DPC) | 1. The smartphone or tablet challenges the PE for the DPC PIN (second factor – something you know).<br>2. The PE provides the correct PIN, and the smartphone or tablet verifies that the CryptoSS or CryptoSH container is unlocked.<br>3. The smartphone or tablet passes the public AuthN Cert, or unique attributes from it, to the local CMS for Credential Profile verification.<br>4. The smartphone or tablet extracts the credential unique identifier from the AuthN Cert and aggregates it with the credential type, factor types, verified public AuthN Cert, and the collected verification data into an AND.<br>5. The smartphone or tablet transforms the AND into an assertion form that is accepted by the PR or SP.<br>6. The smartphone or tablet passes the authentication assertion to the PR or SP.<br>7. Proceed to Shared Flow (Credential Processing) step 3. |

| **Identifier** | **ORG-05-PE-C: PE Federated Authentication** |
|---|---|
| Shared Flow<br>(Memorized Secret) | 1. The IdP challenges the PE to provide the Memorized Secret credential data (first factor – something you know).<br>2. The PE provides the correct Memorized Secret credential data.<br>3. The IdP passes the PE response to the local CMS for Credential Profile verification.<br>4. The CMS verified response may include an OOB channel from the Credential Profile (second factor – something you have). When an OOB is provided the IdP either:<br>a. Sends an OTP to the PE using the OOB channel, prompts the PE for the OTP, and then the PE provides the correct response.<br>b. Sends a message to the PE using the OOB channel and waits a prescribed time for the PE to acknowledge receipt.<br>5. The IdP aggregates the credential, factor types, credential unique identifier (username), and the collected verification data into an AND.<br>6. Proceed to Shared Flow (Credential Processing) step 3. |
| Shared Flow<br>(OTP Device) | 1. The AM challenges the PE to provide the OTP device displayed PIN (first factor – something you have).<br>2. The PE provides the correct PIN<br>3. The AM challenges the PE to use the OTP device keypad to provide a Memorized Secret (second factor – something you know)<br>4. The PE provides the correct secret<br>5. The AM aggregates the credential, factor types, credential unique identifier, and the collected verification data into an AND.<br>6. Proceed to Shared Flow (Credential Processing) step 3. |
| Shared Flow<br>(CryptoD) | 1. The AM challenges the PE to select the stored PKI key pair (first factor – something you have).<br>2. The PE selects a PKI key pair<br>3. The AM validates the PKI key trust, expiration, revocation, and policy OIDs using standards-compliant PKI path validation CRL, OCSP, SCVP, etc.).<br>4. The AM uses an authentication protocol to insure that the PE possesses and controls the PKI private key<br>5. The AM aggregates the credential, factor types, credential unique identifier, and the collected verification data into an AND.<br>6. Proceed to Shared Flow (Credential Processing) step 3. |

### 4.13.4 NPE Description

The following use case is covered in this subsection:

- ORG-05-NPE: Authenticate NPE for Access

This use case focuses on the high-level steps required for ORG to authenticate NPEs requesting access to a PR. The physical access control of NPEs focuses on the visual verification of equipment, ownership and property passes while the logical access control is inherently automated. A PACS AM is deployed by ORG to manage NPE physical ingress and egress. A LACS AM is deployed by ORG to manage enterprise and federated PE access to applications. The AM is responsible for orchestrating the authentication and authorization of NPE access to PRs. The IdP conceptual data elements shown in Figure 4-2 are entity focused and support authentication processing, whereas the SP conceptual data elements are PR focused and support authorization processing.

When an authenticated ORG or PTR PE attempts to enter or exit an ORG site, facility or controlled area with NPE equipment, the FAM challenges the PE to produce paperwork that authenticates ownership and authority to transport the NPE. The FAM then evaluates and enforces the ORG access control security policies.

When an NPE attempts to gain logical access to a PR, the AM domain controller challenges the NPE to authenticate with an approved credential as part of the network LACS. Each time an NPE attempts to gain access to a PR, the AM challenges the requesting NPE to authenticate with its provisioned credential.

When a PE attempts to use an EPD for logical access, the AM domain controller challenges the EPD and the PE User to authenticate with an approved credential as part of the network LACS. Each time a PE/EPD attempts to gain access to a PR or its SP, the AM challenges the requesting EPD and PE to authenticate with their provisioned credentials.

The authentication process validates the integrity and binding strength of the presented credential authenticator. The AM collects the authentication data and results, bundles it with the credential unique ID into an AND, and delivers it to the SP for authorization processing.

As discussed in Sections 4.10 and 4.11, enterprises issue trusted digital credentials, gather identity attributes, and establish and manage Identity Records, Credential Profiles, and Account Profiles for each enrolled NPE. Federation allows ORG to leverage these remote PTR capabilities but requires that each PTR exposes IdP authentication and attribute retrieval services. It also requires that ORG establish a mutual trust agreement with all participating PTR IdPs and SPs.

### 4.13.5 ORG-05-NPE: Authenticate NPE for Access

The details of this use case are provided in two sub-cases:

A. NPE Facility Authentication (Table 4-35)

B. NPE Enterprise Authentication (Table 4-36)

C. NPE Federated Authentication (Table 4-37)

**Table 4-35 NPE Facility Authentication**

| **Identifier** | **ORG-05-NPE-A: NPE Facility Authentication** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authenticate and log the NPE information and the transfer paperwork validity and authority. |
| Actor(s) | Person:<br>• Facility Access Manager (FAM)<br>Non-person:<br>• Non-Person Entity (NPE) |
| Artifact(s) | Paperwork |
| Trigger | A PE is entering or exiting an ORG facility. |
| Pre-conditions | None |
| Post-conditions | The NPE facility access is accepted or rejected and logged. |
| Main Flow<br>(Enter) | 1. The FAM examines the validity of NPE paperwork.<br>2. The FAM accepts or rejects the NPE paperwork.<br>3. The AM logs the time, NPE information and the paperwork authority. |
| Alternate Flow<br>(Exit) | 1. The FAM examines the NPE paperwork.<br>2. The FAM accepts or rejects the NPE paperwork.<br>3. The FAM logs the time, NPE information and the paperwork authority. |

### Table 4-36 NPE Enterprise Authentication

| **Identifier** | **ORG-05-NPE-B: NPE Enterprise Authentication** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authenticate an NPE that is requesting access to an ORG PR. |
| Actor(s) | Non-person:<br>• Access Manager (AM)<br>• Credential Management System (CMS)<br>• ORG Protected Resource (PR)<br>• ORG Service Provider (SP)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authentication Data and Results (AND)<br>• Credential Profile<br>• Credential – CryptoD, CryptoSS or CryptoSH |
| Trigger | An NPE attempts to access an ORG PR or SP. |
| Pre-conditions | The NPE has a valid credential for the ORG PR or SP. |
| Post-conditions | The NPE Authentication is complete, and the ORG PR or SP is ready for authorization processing. |
| Main Flow | 1. The AM challenges the NPE for its credential authenticator and the NPE provides it.<br>2. The AM verifies the integrity and validity of the credential authenticator with the CMS and calculates the NPE and credential binding strength.<br>3. The AM compiles the NPE authentication data into an AND.<br>4. The AM passes the AND to the PR or SP. |
| Alternate Flow (Authentication Failed) | 1. The AM challenges the NPE for its credential authenticator and the NPE responds in one of the following ways:<br>a. With no credential authenticator<br>b. With an invalid credential authenticator<br>2. The AM compiles a failed AND that includes the authenticator error condition.<br>3. The AM passes the AND to the PR or SP. |

### Table 4-37 NPE Federated Authentication

| **Identifier** | **ORG-05-NPE-C: NPE Federated Authentication** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authenticate an ORG managed NPE that is requesting access to a PTR SP. This request can be initiated by either the SP or the IdP. |
| Actor(s) | Non-person:<br>• ORG Access Manager (AM)<br>• ORG Credential Management System (CMS) supporting the IdP<br>• PTR Service Provider (SP)<br>• ORG Identity Provider (IdP)<br>• ORG Non-Person Entity (NPE) |
| Artifact(s) | • Authentication Data and Results (AND)<br>• Credential – CryptoD, CryptoSS or CryptoSH |
| Trigger | An NPE requests to access a PTR SP. |
| Pre-conditions | • NPE is managed by the IdP.<br>• IdP is trusted by the PTR SP. |
| Post-conditions | NPE authentication is complete, and the PTR SP is ready for authorization processing. |
| Main Flow<br>(SP Initiated) | 1. An NPE attempts accessing a PTR SP.<br>2. The PTR SP redirects the NPE session to the IdP for authentication.<br>3. Proceed to Shared Flow (credential processing) step 1 and continue to the end; then return here at step 4.<br>4. The IdP transforms the authentication bundle into an AND form that is that is at the appropriate FAL and accepted by the PTR SP.<br>5. The IdP redirects the NPE session and provides the AND to the PTR SP. |
| Alternate Flow<br>(IdP Initiated) | 1. An NPE attempts accessing the IdP.<br>2. Proceed to Shared Flow (credential processing) step 1 and continue to the end; then return here at step 3.<br>3. The NPE selects a PTR SP.<br>4. The IdP transforms the authentication bundle into an AND form that is at the appropriate FAL and accepted by the PTR SP.<br>5. The IdP redirects the NPE session and provides the AND to the selected PTR SP. |
| Shared Flow<br>(Credential Processing)* | 1. The ORG AM challenges the ORG NPE for its credential authenticator and one of the following happens:<br>a. ORG NPE provides an authenticator.<br>b. ORG NPE does not provide an authenticator. The AM compiles a failed authentication status that includes the “authenticator not provided” condition, go to step 3.<br>2. The ORG AM verifies the integrity and validity of the credential authenticator with the ORG CMS and one of the following happens:<br>a. The authenticator passes and the AM calculates the NPE and credential binding strength.<br>b. The authenticator fails and the AM compiles a failed authentication status that includes the authenticator error condition.<br>3. The ORG AM creates an AND for the ORG NPE. |

*This credential processing flow is common to the SP and IdP initiated flows.

## 4.14 Authorization and Access Use Case

This use case describes the processes required for granting or denying specific requests to obtain access to PRs.

### 4.14.1 Actors and Artifacts

The Authorization and Access Use Case Context is shown in Figure 4-10, and the identified actors are characterized in this subsection.

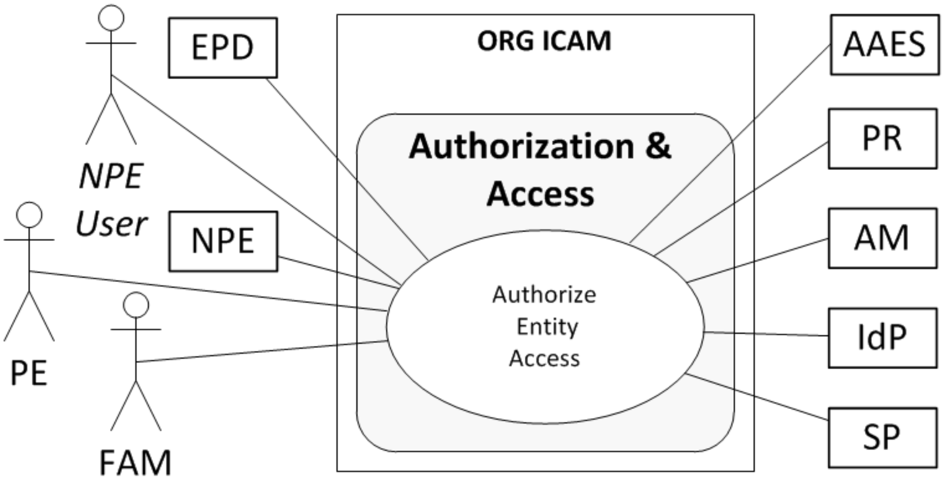


**Figure 4-10 Authorization and Access Use Case Context**

Person actors for the Authorization and Access use case are:

- **FAM** – The ORG Facility Access Manager
- **NPE User** – The PE who is currently operating the EPD

Non-person actors for the Authorization and Access use case are:

- **AAES** – The Authoritative Attribute Exchange Service
- **AM** – The Access Manager component of the PACS or LACS
- **EPD** – The Endpoint Device that used by the NPE User
- **IdP** – The Identity Provider
- **NPE** – The Non-Person Entity that is the focus of the use case
- **PR** – The Protected Resource
- **SP** – The Service Provider

Artifacts for the Authorization and Access use case are:

- **AND** – The Authentication Data and Results
- **Account**
- **Account Policy**
- **Credential** – CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, Crypto and CryptoSS

### 4.14.2 PE Description

The following use case is covered in this section:

- ORG-06-PE: Authorize PE Access

This use case focuses on the high-level steps required for ORG to authorize logical and physical access to a PR for ORG and PTR PEs. A PE is considered internal to ORG when his affiliation establishes that ORG is his primary IdP. A PE is identified as external when his primary affiliation is with a PTR, and the PE provides information to ORG during the course of doing business. The physical access control of the PE is handled by the FAM and the PACS AM. The logical access is handled by the LACS AM that is deployed by ORG to manage enterprise and federated PE application access. The PACS and LACS AMs are responsible for orchestrating the authentication and authorization of PE access to PRs. The IdP conceptual data elements shown in Figure 4-2 are PE focused and support authentication processing, whereas the SP conceptual data elements are PR focused and support authorization processing. This is an authorization use case and therefore ORG is the SP. Details on how these concepts relate to the IBAC, RBAC, and ABAC access control models are provided in Section 3.7 and not addressed in these conceptual uses case.

When a PE attempts to gain access to an ORG site, facility or controlled area, the AM challenges the ORG or PTR PE to authenticate with an approved credential as part of the ORG PACS. The ORG PACS authorizes and enforces access. When the PE does not have a credential that is provisioned in the PACS, the FAM applies the ORG physical access control security policies to authenticate the PE. The FAM authorizes and enforces access.

When a PE attempts to use an EPD to access an ORG PR, the AM domain controller challenges the PE to authenticate with an approved credential as part of the network LACS. Each time an ORG or PTR PE attempts to again access to a PR, the AM challenges the requesting PE to authenticate with a credential type that is accepted by that PR. The AM applies the PR access control security policies to authorize and enforce access.

The SP establishes PE specific Accounts to maintain individualized continuity across sessions. Each Account defines the initial session settings and privileges for the authorized PE. The AM authorization process combines the PE authentication assertion that is provided by the IdP (ORG-05-NPE: Authenticate NPE for Access) with the Account Policy to determine PE access and establish the Account privileges. The Account Policy is a set of Privilege Policies that collectively define the Resource Privileges for an Account. Each Privilege Policy integrates PE Credential and Authorization Profile data with Environmental conditions to assign a Resource Privilege to the Account.

### 4.14.3 ORG-06-PE: Authorize PE Access

The details of this use case are covered in:

A. Authenticated PE Authorization (Table 4-38)

B. PE Facility Access (Table 4-39)

### Table 4-38 Authenticated PE Authorization

| **Identifier** | **ORG-06-PE-A: Authenticated PE Authorization** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authorize an authenticated PE that is requesting access to an ORG PR or SP. |
| Actor(s) | Person:<br>• ORG or PTR Person Entity (PE)<br>Non-person:<br>• Authoritative Attribute Exchange Service (AAES)<br>• Access Manager (AM) component of ORG LACS<br>• ORG Service Provider (SP)<br>• Identity Provider (IdP) for ORG or a PTR<br>• Protected Resource controlled by ORG (PR) |
| Artifact(s) | • Account<br>• Account Policy<br>• Authentication Data and Results (AND)<br>• Credential - CryptoSH [including PIV, PIV-I, CAC and DPC], Memorized Secret, Look-up Secret, OOB, OTP, Crypto and CryptoSS |
| Trigger | PE AND is received from an ORG or trusted IdP. |
| Pre-conditions | PE is authenticated |
| Post-conditions | PE access to PR or SP is authorized and enforced. |
| Main Flow | 1. The AM processes the PE AND authentication assertion that:<br>a. Affirms the appropriate trust with the IdP.<br>b. Establishes the AAL of the identified credential.<br>c. Verifies that the credential and AAL are appropriate for the PR or SP.<br>2. The AM uses the credential unique identifier to either:<br>a. Find the Account for the authenticated PE.<br>b. Create a new Account for the authenticated PE and establish the Account Policy that is appropriate for controlling PTR PE access to the PR or SP.<br>3. The AM resolves the PE AND attributes with the Account Policy parameters and determines that no additional PR or SP attributes are required or uses the PE AND credential unique ID to either:<br>a. Retrieve additional PE attribute data from the ORG AAES or IdP.<br>b. Retrieve additional PE attribute data from the PTR IdP.<br>4. The AM combines the PE AND authentication assertion, attribute data and LOA with the Account Policy to:<br>a. Determine PE access.<br>b. Establish Account privileges.<br>5. The AM enforces the PE access decision.<br>6. The AM logs the access event. |

Table 4-39 PE Facility Access

| **Identifier** | **ORG-06-PE-B: PE Facility Access** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to manage the entry and exit of an authenticated PE within ORG facilities. |
| Actor(s) | Person:<br>• Facility Access Manager (FAM)<br>• Person Entity (PE) |
| Artifact(s) | None |
| Trigger | A PE is entering or exiting an ORG facility. |
| Pre-conditions | The PE is authenticated |
| Post-conditions | The PE facility access is permitted or denied and the entry or exit of the PE is logged. |
| Main Flow<br>(Enter) | 1. The FAM examines the PE authentication and collects the information required by the ORG Physical Access Control policy.<br>2. The FAM permits or denies PE access to the facility.<br>3. The FAM logs the time, PE information and the access decision. |
| Alternate Flow<br>(Exit) | 1. The FAM examines the PE authentication and collects the information required by the ORG Physical Access Control policy.<br>2. The FAM permits the PE to exit the facility.<br>3. The FAM logs the time, PE information and the exit. |

### 4.14.4 NPE Description

The following use case is covered in this subsection:

- ORG-06-NPE: Authorize NPE Access

This use case focuses on the high-level steps required for ORG to authorize logical and physical access for a NPE or a PE User and their EPD. User access to the facility is determined separately and the NPE logical access to a PR is controlled within the facility.

The logical access control of an NPE is handled by the LACS AM that is deployed by ORG to manage enterprise and federated access. The AM is responsible for orchestrating the authentication and authorization of each NPE and each user PE/EPD entity pair that is requesting logical access to a PR. The IdP conceptual data elements that are shown in Figure 4-2 are entity focused and support authentication processing, whereas the SP conceptual data elements are PR focused and support authorization processing. This is an authorization use case where ORG is the SP and controlling access to one of its PR for an authenticated NPE. The SP establishes NPE specific Accounts to maintain individualized continuity across sessions. Each Account defines the initial session settings and privileges for the authorized NPE. The AM authorization process takes the NPE ANDs that are provided by the IdP with the Account Policy to determine NPE access decision and establish the Account privileges for this session. The Account Policy is a set of Privilege Policies that collectively define the Resource Privileges for an Account. Each Privilege Policy integrates NPE entity Credential Profile and Authorization Profile data with Environmental conditions to assign one or more Resource Privileges to the session for this Account.

The physical access control of NPE MP equipment is handled by the FAM.

### 4.14.5 ORG-06-NPE: Authorize NPE Access

The details of this use case are provided in two sub-cases:

A. Authenticated NPE Authorization (Table 4-40)

B. Authenticated User/EPD Authorization (Table 4-41)

C. NPE Facility Access (Table 4-42)

**Table 4-40 Authenticated NPE Authorization**

| Identifier | ORG-06-NPE-A: Authenticated NPE Authorization |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authorize an authenticated NPE that is requesting access to a ORG SP. |
| Actor(s) | Non-person:<br>• Authoritative Attribute Exchange Service (AAES)<br>• Access Manager (AM) component of ORG LACS<br>• Identity Provider (IdP) for ORG or a PTR<br>• Protected Resource controlled by ORG (PR)<br>• ORG Service Provider (SP)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Authentication Data and Results (AND)<br>• Account<br>• Account Policy<br>• Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | NPE AND is received from an ORG or trusted IdP. |
| Pre-conditions | The NPE is authenticated and the AM has the AND. |
| Post-conditions | NPE access to ORG PR is authorized and enforced. |
| Main Flow | 1. The AM processes the NPE AND that:<br>a. Affirms the appropriate trust with the IdP.<br>b. Establishes the LOA of the identified credential.<br>c. Verifies that the credential and LOA are appropriate for the PR.<br>2. The AM uses the NPE credential unique ID to either:<br>a. Find the SP Account for the authenticated NPE.<br>b. Create a new SP Account for the authenticated NPE and establish the Account Policy that is appropriate for controlling access to the SP.<br>3. The AM resolves the AND attributes with the Account Policy parameters and determines that no additional NPE attributes are required or uses the AND credential unique ID to either:<br>a. Retrieve additional NPE attribute data from the ORG AAES.<br>b. Retrieve additional NPE attribute data from the PTR IdP.<br>4. The AM applies the Account Policy to the NPE AND and supplemental NPE attribute data to:<br>a. Determine NPE access.<br>b. Establish Account privileges for the requested session.<br>5. The AM enforces the NPE access decision for the SP.<br>6. The AM logs the NPE access event to the SP PR. |

**Table 4-41 Authenticated User/EPD Authorization**

| **Identifier** | **ORG-06-EPD-B: Authenticated User/EPD Authorization** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to authorize an authenticated User/EPD entity pair that is requesting access to a ORG SP |
| Actor(s) | Person:<br>• Endpoint Device User (NPE User)<br>Non-person:<br>• Authoritative Attribute Exchange Service (AAES)<br>• Identity Provider (IdP)<br>• Access Manager (AM) component of ORG LACS<br>• Protected Resource controlled by ORG (PR)<br>• ORG PR Service Provider (SP)<br>• Endpoint Device (EPD) |
| Artifact(s) | • Authentication Data and Results (AND)<br>• Credential – CryptoSH, CryptoD and CryptoSS<br>• Account<br>• Account Policy |
| Trigger | NPE User and EPD ANDs are received from trusted IdPs. |
| Pre-conditions | Both the NPE User and the EPD are authenticated and the AM has their ANDs |
| Post-conditions | User/EPD access to PR or SP is authorized and enforced. |
| Main Flow | 1. The AM processes the EPD AND that:<br>a. Affirms the appropriate trust with the IdP.<br>b. Establishes the LOA of the identified credential.<br>c. Verifies that the credential and LOA are appropriate for the PR or SP.<br>2. The AM processes the NPE User AND that:<br>a. Affirms the appropriate trust with the IdP.<br>b. Establishes the LOA of the identified credential.<br>c. Verifies that the credential and LOA are appropriate for the PR or SP.<br>3. The AM uses the NPE User credential unique identifier to either:<br>a. Find the User Account for the authenticated NPE User.<br>b. Create a new User Account for the authenticated NPE User and establish the Account Policy that is appropriate for controlling access to the PR or SP.<br>4. The AM resolves the NPE User and EPD AND attributes with the Account Policy parameters and determines that no additional PR or SP attributes are required or uses the NPE User AND credential unique ID to either:<br>a. Retrieve additional NPE User attribute data from the ORG AAES.<br>b. Retrieve additional NPE User attribute data from the IdP.<br>5. The AM applies the Account Policy to the NPE User AND data, EPD AND data and environment data to:<br>a. Determine NPE User access.<br>b. Establish User Account privileges for the requested session.<br>6. The AM enforces the access decision for the PR or SP.<br>7. The AM logs the access event. |

## Table 4-42 NPE Facility Access

| **Identifier** | **ORG-06-NPE-C: NPE Facility Access** |
|---|---|
| Description | This use case flow provides the high-level steps needed for ORG to manage the entry and exit of an authenticated NPE within ORG facilities. |
| Actor(s) | Person:<br>• Facility Access Manager (FAM)<br>Non-person:<br>• Non-Person Entity (NPE) – equipment |
| Artifact(s) | None |
| Trigger | MP system or component equipment is entering or exiting an ORG facility. |
| Pre-conditions | The NPE is authenticated |
| Post-conditions | The NPE equipment facility access is permitted or denied and the entry or exit of the NPE equipment is logged. |
| Main Flow<br>(Enter) | 1. The FAM examines the NPE equipment paperwork authentication and collects the information required by the ORG physical access control security policy.<br>2. The FAM permits or denies NPE equipment access to the facility as mandated by the ORG Physical Access Control policy.<br>3. The FAM logs the time, NPE equipment information and the access decision. |
| Alternate Flow<br>(Exit) | 1. The FAM examines the NPE equipment paperwork authentication and collects the information required by the ORG physical access control security policy.<br>2. The FAM permits or denies the removal of the NPE equipment from the facility as mandated by the ORG physical access control security policy.<br>3. The FAM logs the time, NPE equipment information and the exit decision. |

## 4.15 Cryptography Use Cases

These use cases describe the processes required to use and manage ciphers and ensure the authenticity, confidentiality, and integrity of shared data.

### 4.15.1 Actors and Artifacts

The Cryptography Use Case Context is shown in Figure 4-11, and the identified actors are characterized in this subsection.

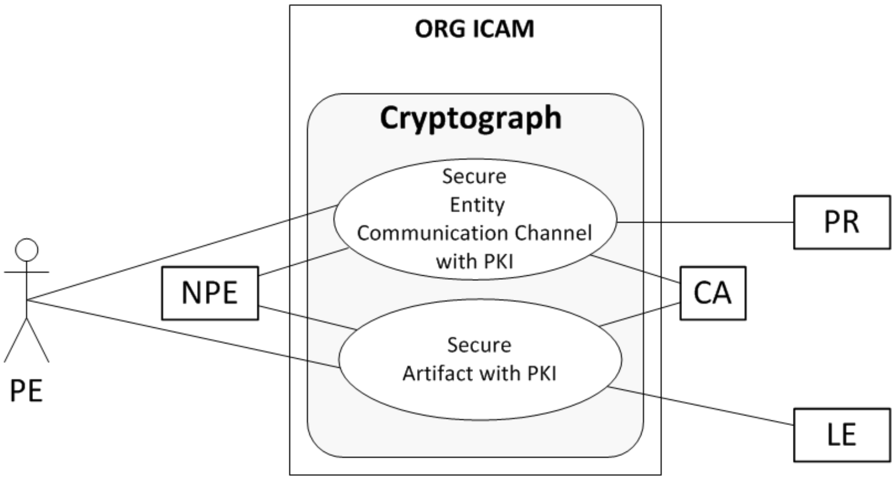


**Figure 4-11 Cryptography Use Case Context**

Person actors for the Cryptography use cases are:

- **PE –** The Person Entity that is the focus of the PE use case

Non-person actors for the Cryptography use cases are:

- **CA** – The Certificate Authority
- **LE** – The Logical Entity
- **NPE** – The Non-Person Entity that is the focus of the NPE use case
- **PR** – The Protected Resource

Artifacts for the Cryptography use cases are:

- **Credential** – CryptoD, CryptoSS, CryptoSH [including PIV, PIV-I, CAC and DPC]
- **Payload**

### 4.15.2 PE Description

The following use cases are covered in this section:

- ORG-07-PE: Secure PE Communication Channel with PKI
- ORG-08-PE: Secure PE Artifact with PKI

These use cases focus on the high-level steps required for ORG to protect the confidentiality of the network TCP/IP layer messages that are employed to provide ICAM services.

Digital encryption is used to provide electronic data confidentiality. It is the process of transforming data from a readable form into a non-readable form that requires a cryptographic key and decryption processing to reconstitute the readable form.

Digital signatures provide origin authentication, data integrity, and signatory non-repudiation. It is a cryptographic transformation process to create an electronic signature token that uniquely binds the signer to the exact data. The data receiver can then validate the signature token with the signer's cryptographic key to authenticate the signer and verify the integrity of the received data.

PKI is a formal set of roles, policies, and procedures for managing and distributing digital certificates. The CA creates, stores, issues, and signs the digital certificates. The certificate signing establishes digital trust (origin authentication and data integrity) and enables a hierarchical chain of subordinate CAs with digitally verifiable trust back to the root CA. The CA also manages the revocation of the certificates it issues and makes that information available upon request.

Asymmetric key algorithms create key pairs that are mathematically unique but that functionally complement each other. Thus, whatever either key encrypts, the paired key can decrypt. This functional coupling allows a single private key to be bound to a PE and any number of widely distributed public keys. PIV, PIV-I, and CAC smartcards are ideal for providing the PE cryptographic keys because they already create, manage, and control asymmetric PKI certificates for PE authentication and document encryption and signing. These smartcards also provide a secure key container and an issuance process that restricts the private keys to that container.

Symmetric-key algorithms create key pairs that share a secret so that they can mutually encrypt and decrypt.

### 4.15.3 ORG-07-PE: Secure PE Communication Channel with PKI

The details of this use case are covered in two sub-cases:

A. PE Confidential Communications with Trusted PR (Table 4-43)

### Table 4-43 PE Confidential Communications with a Trusted PR

| **Identifier** | **ORG-07-PE-A: PE Confidential Communications with a Trusted PR** |
|---|---|
| Description | This use case flow provides the high-level steps needed for a PE to establish a trusted and confidential channel with a PR. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>Non-person:<br>• Certificate Authority (CA)<br>• Protected Resource (PR) |
| Artifact(s) | • Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | The PE attempts a connection with the PR. |
| Pre-conditions | A CA has issued an asymmetric key pair to the PR. |
| Post-conditions | The PE's browser has a trusted confidential transport layer channel with the PR. |
| Main Flow<br>(PR is Trusted) | 1. The PE's browser checks the trust chain of the PR public key and that the PR possesses the paired private key.<br>2. The credential validated.<br>3. A trusted, confidential channel is established. |
| Alternate Flow<br>(PR is Not Trusted) | 1. The PE's browser checks the trust chain of the PR public key and that the PR possesses the paired private key.<br>2. The credential is not validated.<br>3. The PE's browser prompts the PE to trust or not trust the PR.<br>4. The PE accepts the trust, and the confidential channel is established or the PE rejects the trust and the connection is terminated. |

### 4.15.4 ORG-08-PE: Secure PE Artifact with PKI

The details of this use case are covered in:

A. Secure Artifact for Confidential Transaction (Table 4-44)

B. Secure Artifact Authenticity and Integrity for Transaction (Table 4-45)

**Table 4-44 Secure Artifact for Confidential Transaction**

| **Identifier** | **ORG-08-PE-A: Secure Artifact for Confidential Transaction** |
|---|---|
| Description | This use case flow provides the high-level steps needed for a PE and a PR or LE to share an artifact in a trusted and confidential manner. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>Non-person:<br>• Certificate Authority (CA)<br>• Logical Entity (LE)<br>• Protected Resource (PR) |
| Artifact(s) | • Credential – CryptoD, CryptoSS, CryptoSH [including PIV, PIV-I, CAC and DPC]<br>• Payload |
| Trigger | A payload needs to be shared in confidence between a PE and a PR or LE. |
| Pre-conditions | • The PE has a Federal Information Processing Standard (FIPS)-201 compliant smartcard (PIV, PIV-I or CAC) or DPC, or CryptoD, CryptoSS, CryptoSH<br>• A trusted CA has issued asymmetric encryption key pairs to the PR or LE. |
| Post-conditions | The payload was shared in confidence. |
| Main Flow<br>(PE Provides Payload) | 1. The PE elects to encrypt the payload before sharing.<br>2. The PE retrieves the PR or LE public encryption key and encrypts the payload.<br>3. The PE sends the encrypted payload.<br>4. The PR or LE uses their private encryption key to decrypt the payload. |
| Alternate Flow<br>(PR or LE Provides Payload) | 1. The PR or LE elects to encrypt the payload before sharing.<br>2. The PR or LE retrieves the PE public encryption key and encrypts the payload.<br>3. The PR or LE sends the encrypted payload.<br>4. The PE unlocks his smartcard and uses the private encryption key to decrypt the payload. |

**Table 4-45: Secure Artifact Authenticity and Integrity for Transaction**

| **Identifier** | **ORG-08-PE-B: Secure Artifact Authenticity and Integrity for Transaction** |
|---|---|
| Description | This use case flow provides the high-level steps needed for a PE and a PR or LE to share a payload in a trusted, non-reputable and untampered manner. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>Non-person:<br>• Certificate Authority (CA)<br>• Logical Entity (LE)<br>• Protected Resource (PR) |
| Artifact(s) | • Credential – CryptoD, CryptoSS, CryptoSH [including PIV, PIV-I, CAC and DPC]<br>• Payload |
| Trigger | A payload needs to be shared between a PE and a PR or LE in a trusted, non-reputable and untampered manner. |
| Pre-conditions | • The PE has a FIPS-201 compliant smartcard (PIV, PIV-I or CAC) or DPC or CryptoD, CryptoSS, CryptoSH<br>• A trusted CA has issued asymmetric encryption key pairs to the PR or LE. |
| Post-conditions | The payload was shared in a trusted, non-reputable and untampered manner. |
| Main Flow<br>(PE provides payload) | 1. The PE elects to sign the payload before sharing.<br>2. The PE unlocks his smartcard and uses the private signing key to sign the payload.<br>3. The PE sends the signed payload.<br>4. The PR or LE retrieves the PE public signing key and uses it to verify the integrity of the payload and the validity of the signer. |
| Alternate Flow<br>(PR or LE provides payload) | 1. The PR or LE elects to sign the payload before sharing.<br>2. The PR or LE uses his private signing key to sign the payload.<br>3. The PR or LE sends the signed payload.<br>4. The PE retrieves the PR or LE public signing key and uses it to verify the integrity of the payload and the validity of the signer. |

### 4.15.5 NPE Description

The following use cases are covered in this subsection:

- ORG-07-NPE: Secure NPE Communication Channel with PKI
- ORG-08-NPE: Secure NPE Artifact with PKI

These use cases focus on the high-level steps required for ORG to protect the confidentiality and integrity of artifacts transferred in messages that are employed to provide ICAM services.

Digital encryption is used to provide electronic data confidentiality. It is the process of transforming data from a readable form into a non-readable form that requires a cryptographic key and decryption processing to reconstitute the readable form.

Digital signatures provide origin authentication, data integrity, and signatory non-repudiation. It is a cryptographic transformation process to create an electronic signature token that uniquely binds the signer to the exact data. The data receiver can then validate the signature token with the signer's cryptographic key to authenticate the signer and verify the integrity of the received data.

PKI is a formal set of roles, policies, and procedures for managing and distributing digital certificates. The CA creates, stores, issues, and signs the digital certificates. The certificate signing establishes digital trust (origin authentication and data integrity) and enables a hierarchical chain of subordinate CAs with digitally verifiable trust back to the root CA. The CA also manages the revocation of the certificates it issues and makes that information available upon request.

Asymmetric-key algorithms create key pairs that are mathematically unique yet functionally complement each other. Thus, whatever either key encrypts, the paired key can decrypt. This functional coupling allows a single private key to be bound to an entity and any number of widely distributed public keys.

Symmetric-key algorithms create key pairs that share a secret so that they can mutually encrypt and decrypt.

### 4.15.6 ORG-07-NPE: Secure NPE Communication Channel with PKI

The details of this use case are provided in two sub-cases:

A. NPE Confidential Communications with Trusted PR (Table 4-46)

B. NPE Confidential Communications with Mutually Trusted PR (Table 4-47)

**Table 4-46 NPE Confidential Communications with a Trusted PR**

| **Identifier** | **ORG-07-NPE-A: NPE Confidential Communications with Trusted PR** |
|---|---|
| Description | This use case flow provides the high-level steps needed for an NPE to establish a trusted and confidential channel with a PR. |
| Actor(s) | Non-person:<br>• Protected Resource (PR)<br>• Certificate Authority (CA)<br>• Non-Person Entity (NPE) |
| Artifact(s) | Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | The NPE attempts a confidential connection with the PR. |
| Pre-conditions | • A CA has issued an asymmetric key pair to the PR.<br>• The NPE has the CA certificate trust chain.<br>• The NPE has the public asymmetric key for the PR. |
| Post-conditions | The NPE has a trusted confidential transport layer channel with the PR. |
| Main Flow | 1. The NPE and PR negotiate a cipher.<br>2. The NPE verifies the trust chain and revocation of the PR public key.<br>3. The NPE verifies that the PR possesses the paired private key.<br>4. The trusted, confidential channel is established. |

Table 4-47 NPE Confidential Communications with Mutually Trusted PR

| Identifier | ORG-07-NPE-B: NPE Confidential Communications with Mutually Trusted PR |
|---|---|
| Description | This use case flow provides the high-level steps needed for an NPE to establish a mutually trusted and confidential channel with a PR. |
| Actor(s) | Non-person:<br>• Protected Resource (PR)<br>• Certificate Authority (CA)<br>• Non-Person Entity (NPE) |
| Artifact(s) | Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | The NPE attempts a confidential connection with the PR. |
| Pre-conditions | • A CA has issued asymmetric key pairs to the PR and NPE.<br>• The NPE and PR have the CA certificate trust chain.<br>• The NPE has the public asymmetric key for the PR.<br>• The PR has the public asymmetric key for the NPE. |
| Post-conditions | The NPE has a mutually trusted confidential channel with the PR. |
| Main Flow | 1. The NPE and PR negotiate a cipher.<br>2. The NPE verifies the trust chain and revocation of the PR public key.<br>3. The NPE verifies that the PR possesses the paired private key.<br>4. The PR verifies the trust chain and revocation of the NPE public key.<br>5. The PR verifies that the NPE possesses the paired private key.<br>6. The mutually trusted, confidential channel is established. |

### 4.15.7 ORG-08-NPE: Secure NPE Artifact with PKI

The details of this use case are provided in two sub-cases:

A. Secure Artifact Integrity for Transaction (Table 4-48)

B. Secure Artifact for Confidential Transaction (Table 4-49)

### Table 4-48 Secure Artifact Authenticity and Integrity for Transaction

| **Identifier** | **ORG-08-NPE-A: Secure Artifact Authenticity and Integrity for Transaction** |
|---|---|
| Description | This use case flow provides the high-level steps needed for an NPE and a PR or LE to share an artifact in a trusted, non-reputable and untampered manner. This also enables provider non-repudiation. |
| Actor(s) | Non-person:<br>• Protected Resource (PR)<br>• Certificate Authority (CA)<br>• Logical Entity (LE)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Payload - text or binary<br>• Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | The NPE attempts sharing a confidential payload with a PR or LE. |
| Pre-conditions | • A CA has issued asymmetric encryption key pairs to the NPE and PR or LE.<br>• The NPE and PR or LE have the CA certificate trust chain.<br>• The NPE has the public asymmetric key for the PR or LE and the PR or LE has the public asymmetric key for the NPE.<br>• The NPE and PR or LE have negotiated a cipher.<br>• The NPE and PR or LE have an established communication channel and protocol. |
| Post-conditions | The payload was shared in a trusted, non-reputable and untampered manner. |
| Main Flow (NPE Provides Payload) | 1. The NPE uses their private signing key to sign the payload.<br>2. The NPE sends the signed payload to the PR or LE.<br>3. The PR or LE verifies the NPE public signing key by checking trust chain and revocation.<br>4. The PR or LE uses the NPE public signing key to verify the integrity of the payload and the validity of the signer |
| Alternate Flow (PR or LE Provides Payload) | 1. The PR or LE uses their private signing key to sign the payload.<br>2. The PR or LE sends the signed payload to the NPE.<br>3. The NPE verifies the PR or LE public signing key by checking trust chain and revocation.<br>4. The NPE uses the PR or LE public signing key to verify the integrity of the payload and the validity of the signer |

### Table 4-49 Secure Artifact for Confidential Transaction

| **Identifier** | **ORG-08-NPE-B: Secure Artifact for Confidential Transaction** |
|---|---|
| Description | This use case flow provides the high-level steps needed for an NPE and a PR or LE to share a payload in a trusted and confidential manner. |
| Actor(s) | Non-person:<br>• Protected Resource (PR)<br>• Certificate Authority (CA)<br>• Logical Entity (LE)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Payload - text or binary<br>• Credential – CryptoD, CryptoSS, CryptoSH |
| Trigger | A payload needs to be shared in confidence between an NPE and an NPE. |
| Pre-conditions | • A CA has issued asymmetric encryption key pairs to the NPE and PR or LE.<br>• The NPE and PR or LE have the CA certificate trust chain.<br>• The NPE has the public asymmetric key for the PR or LE and the PR or LE has the public asymmetric key for the NPE.<br>• The NPE and PR or LE have negotiated a cipher.<br>• The NPE and PR or LE have an established communication channel and protocol. |
| Post-conditions | The payload was shared in confidence. |
| Main Flow<br>(NPE Provides Payload) | 1. The NPE verifies the PR or LE public encryption key by checking trust chain and revocation.<br>2. The NPE uses the PR or LE public encryption key to encrypt the payload.<br>3. The NPE sends the encrypted payload.<br>4. The PR or LE uses their private encryption key to decrypt the payload. |
| Alternate Flow<br>(PR or LE Provides Payload) | 1. The PR or LE verifies the NPE public encryption key by checking trust chain and revocation.<br>2. The PR or LE uses the NPE public encryption key to encrypt the payload.<br>3. The PR or LE sends the encrypted payload.<br>4. The NPE uses their private encryption key to decrypt the payload. |

## 4.16 Auditing and Reporting Use Case

This use case describes the processes required to capture and review records and activities for assessing the adequacy of system controls.

### 4.16.1 Actors and Artifacts

The Auditing and Reporting Use Case Context is shown in Figure 4-12, and the identified actors are characterized in this subsection.

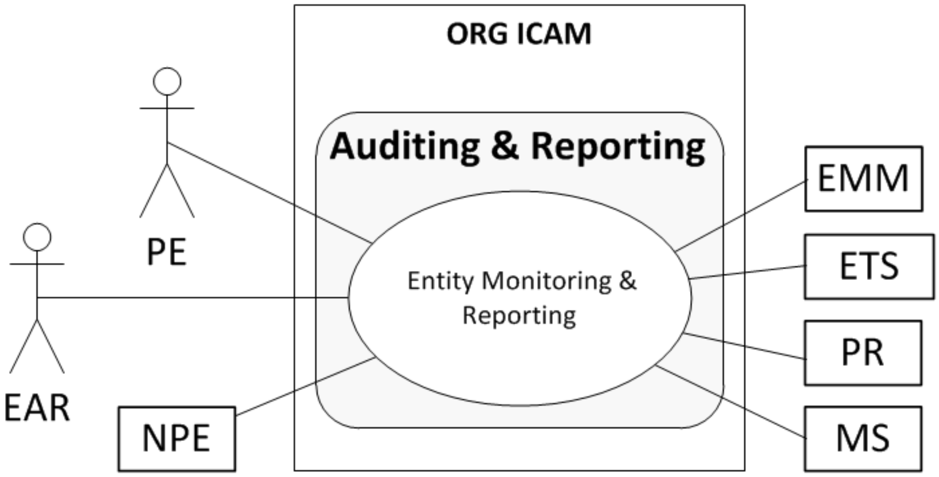


**Figure 4-12 Auditing and Reporting Use Case Context**

Person actors for the Auditing and Reporting use case are:

- **EAR** – The Event Auditor and Reporter
- **PE** – The Person Entity that is the focus of the PE use case

Non-person actors for the Auditing and Reporting use case are:

- **EMM** – The Enterprise Mobility Management
- **ETS** – The Event Tracking System
- **MS** – The Monitored System
- **NPE** – The Non-Person Entity that is the focus of the NPE use case
- **PR** – The Protected Resource

Artifacts for the Auditing and Reporting use case are:

- **AMR** – The Activity Monitoring Request

- **MAR** – The Monitored Activity Report

### 4.16.2 PE Description

The following use case is covered in this subsection:

- ORG-09-PE: PE Monitoring and Reporting

This use case focuses on the high-level steps required for an SP organization to manage the review and examine records and activities that assess the adequacy of system controls and the presentation of logged data in a meaningful context. It includes PE successful and unsuccessful PR access attempts and other event logs that enable administrators to determine if PEs are exhibiting concerning behaviors.

### 4.16.3 ORG-09-PE: PE Monitoring and Reporting

The details of this use case are covered in:

A. Monitor PE Access (Table 4-50)

B. Generate PE Activity Report (Table 4-51)

C. Register PE Activity Monitors (Table 4-52)

**Table 4-50 Monitor PE Access**

| **Identifier** | **ORG-09-PE-A: Monitor PE Access** |
|---|---|
| Description | This use case flow provides the high-level steps needed to log PE monitored events on MSs and PRs. |
| Actor(s) | Person:<br>• Person Entity (PE)<br>Non-person:<br>• Event Tracking System (ETS)<br>• Monitored System (MS)<br>• Protected Resource (PR) |
| Artifact(s) | None |
| Trigger | A PE monitored activity occurs and triggers ETS logging. |
| Pre-conditions | • PE activity monitors are registered in the PR, MS, and ETS.<br>• The PE attempts to execute a monitored activity. |
| Post-conditions | PE activities are logged in the ETS. |
| Main Flow | 1. The PR or MS detect a PE monitored activity.<br>2. The PR or MS collect the PE activity data.<br>3. The PR or MS log the PE activity data in the ETS. |

### Table 4-51 Generate PE Activity Report

| **Identifier** | **ORG-09-PE-B: Generate PE Activity Report** |
|---|---|
| Description | This use case flow provides the high-level steps needed to report the configuration, status and activity log of an MS or AR. |
| Actor(s) | Person:<br>• Event Auditor and Reporter (EAR)<br>• Person Entity (PE)<br>Non-person:<br>• Event Tracking System (ETS)<br>• Monitored System (MS)<br>• Protected Resource (PR) |
| Artifact(s) | • Monitored Activity Report (MAR) |
| Trigger | PE monitoring is requested. |
| Pre-conditions | PE activity monitors are registered in the PR, MS, and ETS. |
| Post-conditions | A PE MAR is generated and available for Auditing. |
| Main Flow | 1. The EAR accesses the ETS.<br>2. The EAR identifies the monitored PE, MS, or PR and desired activities.<br>3. The EAR generates the PE MAR. |

**Table 4-52 Register PE Activity Monitors**

| **Identifier** | **ORG-09-PE-C: Register PE Activity Monitors** |
|---|---|
| Description | This use case flow provides the high-level steps needed to register the PE event on an MS or PR and the ETS. |
| Actor(s) | Person:<br>• Event Auditor and Reporter (EAR)<br>• Person Entity (PE)<br>Non-person:<br>• Event Tracking System (ETS)<br>• Monitored System (MS)<br>• Protected Resource (PR) |
| Artifact(s) | • Activity Monitoring Request (AMR) |
| Trigger | The EAR receives an authorized PE activity monitoring request for an MS or PR. |
| Pre-conditions | A PE AMR for a PR or MS has been authorized. |
| Post-conditions | PE activity monitoring events are registered in the MS or PR and the ETS. |
| Main Flow<br>(Create) | 1. The EAR receives a create AMR for a PE.<br>2. The EAR accesses the ETS.<br>3. The EAR defines PE action events and ETS logging response for the MS or PR.<br>4. The EAR enables and activates the logging responses in the MS or PR.<br>5. The EAR registers and activates the action event and logging response monitors in the ETS. |
| Alternate Flow<br>(Activate, Deactivate) | 1. The EAR receives an activate or deactivate AMR for a PE.<br>2. The EAR accesses the ETS.<br>3. The EAR activates or deactivates the logging responses in the MS or PR for the PE as requested in the AMR.<br>4. The EAR activates or deactivates the action event and logging response monitors in the ETS as requested in the AMR. |

### 4.16.4 NPE Description

The following use case is covered in this subsection:

- ORG-09-NPE: NPE Monitoring and Reporting

This use case focuses on the high-level steps required for an SP organization to manage the review and examination of records and activities that assess the adequacy of system controls and the presentation of logged data in a meaningful context. It includes successful and unsuccessful PR access attempts and other event logs that enable administrators to determine whether entities are exhibiting concerning behaviors.

### 4.16.5 ORG-09-NPE: NPE Monitoring and Reporting

The details of this use case are provided in four sub-cases:

A. Monitor NPE (Table 4-53)

B. Monitor NPE Access (Table 4-54)

C. Generate NPE Activity Report (Table 4-55)

D. Register NPE Activity Monitors (Table 4-56)

**Table 4-53 Monitor NPE**

| **Identifier** | **ORG-09-NPE-A: Monitor NPE** |
|---|---|
| Description | This use case flow provides the high-level steps needed to log the configuration and status of an NPE. |
| Actor(s) | Non-person:<br>• Event Tracking System (ETS)<br>• Non-Person Entity (NPE)<br>• Enterprise Mobility Management (EMM) |
| Artifact(s) | None |
| Trigger | Authorized NPE monitoring is requested. |
| Pre-conditions | • The NPE is network accessible.<br>• The NPE is registered in the ORG EMM system. |
| Post-conditions | The NPE configuration and status is logged in the ETS. |
| Main Flow | 1. One of the following happens:<br>a. An authorized user accesses the ORG EMM system and ETS.<br>b. An automated ETS process accesses the ORG EMM system.<br>2. Logical access to the NPE is established.<br>3. The NPE configuration and status is retrieved a logged in the ETS.<br>4. Access to the NPE, ETS, and ORG EMM system is terminated. |

**Table 4-54 Monitor NPE Access**

| **Identifier** | **ORG-09-NPE-B: Monitor NPE Access** |
|---|---|
| Description | This use case flow provides the high-level steps needed to log NPE monitored events on MSs and PRs. |
| Actor(s) | Non-person:<br>• Event Tracking System (ETS)<br>• Monitored System (MS)<br>• Protected Resource (PR)<br>• Non-Person Entity (NPE) |
| Artifact(s) | None |
| Trigger | An NPE monitored activity occurs and triggers ETS logging. |
| Pre-conditions | • NPE activity monitors are registered in the PR, MS, and ETS.<br>• The NPE attempts to execute a monitored activity. |
| Post-conditions | NPE activities are logged in the ETS. |
| Main Flow | 1. The PR or MS detect an NPE monitored activity.<br>2. The PR or MS collect the NPE activity data.<br>3. The PR or MS log the NPE activity data in the ETS. |

### Table 4-55 Generate NPE Activity Report

| **Identifier** | **ORG-09-NPE-C: Generate NPE Activity Report** |
|---|---|
| Description | This use case flow provides the high-level steps needed to report the configuration, status and activity log of an NPE. |
| Actor(s) | Person:<br>• Event Auditor and Reporter (EAR)<br>Non-person:<br>• Event Tracking System (ETS)<br>• Monitored System (MS)<br>• Protected Resource (PR)<br>• Non-Person Entity (NPE) |
| Artifact(s) | Monitored Activity Report (MAR) |
| Trigger | NPE monitoring is requested. |
| Pre-conditions | NPE activity monitors are registered in the PR, MS, and ETS. |
| Post-conditions | An NPE MAR is generated and available for Auditing. |
| Main Flow | 1. The EAR accesses the ETS.<br>2. The EAR identifies the monitored NPE and desired activities.<br>3. The EAR generates the NPE MAR. |

### Table 4-56 Register NPE Activity Monitors

| **Identifier** | **ORG-09-NPE-D: Register NPE Activity Monitors** |
|---|---|
| Description | This use case flow provides the high-level steps needed to register the NPE event on MS and PR and the ETS. |
| Actor(s) | Person:<br>• Event Auditor and Reporter (EAR)<br>Non-person:<br>• Event Tracking System (ETS)<br>• Monitored System (MS)<br>• Protected Resource (PR)<br>• Non-Person Entity (NPE) |
| Artifact(s) | • Activity Monitoring Request (AMR) |
| Trigger | The EAR receives an authorized NPE activity monitoring request for an MS or PR. |
| Pre-conditions | An NPE AMR for a PR or MS has been authorized. |
| Post-conditions | NPE activity monitoring events are registered in the MS or PR and the ETS. |
| Main Flow<br>(Create) | 1. The EAR receives a create AMR for an NPE.<br>2. The EAR accesses the ETS.<br>3. The EAR defines NPE action events and ETS logging response for the MS or PR.<br>4. The EAR enables and activates the logging responses in the MS or PR.<br>5. The EAR registers and activates the action event and logging response monitors in the ETS. |
| Alternate Flow<br>(Activate, Deactivate) | 1. The EAR receives an activate or deactivate AMR for an NPE.<br>2. The EAR accesses the ETS.<br>3. The EAR activates or deactivates the logging responses in the MS or PR for the NPE as requested in the AMR.<br>4. The EAR activates or deactivates the action event and logging response monitors in the ETS as requested in the AMR. |

## 4.17 DPM Use Cases

These use cases describe the process required to dynamically create, disseminate, and maintain hierarchical rule sets and control digital resource management, utilization, and protection.

### 4.17.1 Actors and Artifacts

The DPM Use Case Context is shown in Figure 4-13, and the identified actors are characterized in this section.

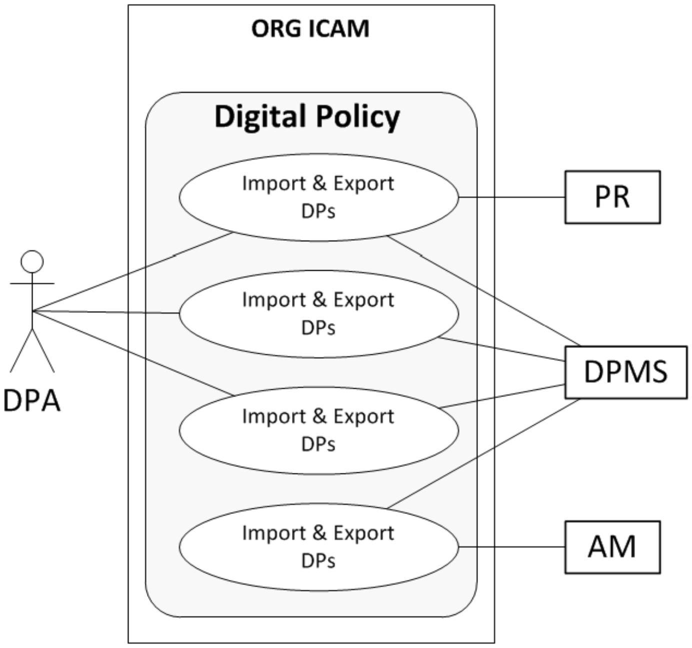


**Figure 4-13 DPM Use Case Context**

Person actors for the DPM use cases are:

- **DPA** – The Digital Policy Administrator or designated subordinate

Non-person actors for the DPM use cases are:

- **AM** – The Access Manager component of the LACS
- **DPMS** – The Digital Policy Management System
- **PTR** – An organization or agency that has a partnership relationship with ORG

Artifacts for the DPM use cases are:

- **Authorization Profile**
- **Credential Profile**

- **DP** – Digital Policy
- **Environment**
- **Resource Profile**

### 4.17.2 DPM Description

Section 3-17 describes several Logical Access Control Models that implement organizational policies using different schemes. The digital policies that apply to an Account are represented in the set of Privilege Policies that define the Account Policy. It is important to note that externalizing digital access control policies from the PE, PR, authentication, and environmental attribute data, and the AM implementation is one of the discriminating factors of ABAC over IBAC and RBAC. This clear separation of concerns significantly simplifies the operation and maintenance by providing direct and independent refinement of ORG access control policies. ABAC is therefore the Logical Access Control Model that is addressed by DPM.

This use case focuses on the high-level steps required for an SP organization to manage the life cycle of the DPs that control PE and NPE access to each of their PR services. These policies are composed and managed by the organization policy makers in their Natural Language Policy (NLP) form and then transformed into DPs to support LACS AM. The DP life cycle is managed by the DPA and proceeds as follows:

1. The DPA either creates a draft DP from an NLP or comparable representation, or obtains an existing DP from some reasonable source. The DPA then creates test cases and test data that will verify that the Draft DP satisfies the intent of the NLP. The DPA gets approval that the Draft DP satisfies the intent of the NLP and transitions the Draft DP to Approved DP.
    - Use Cases: Import and Export DPs, Create and Maintain DP Content
2. The DPA then evaluates, deconflicts, and updates the Approved DP iteratively until it is verified to pass the test case evaluation (go to step 3), or it is determined that this approach will not work (go to step 1). Conflicting DPs become part of the update process, or they are identified for retirement. The Approved DP is transitioned to Verified DP.
    - Use Case: Create and Maintain DP Content
3. The DPA then activates and deploys the Verified DP and deactivates and retires the identified DPs.
    - Use Cases: Provide DPs for Access, Manage Activated DPs
4. The DPA monitors the active DP enforcement. When an issue occurs, the DPA defines new test cases and test data and provides them with the active DP as a candidate to step 2.
    - Use Case: Monitor DP Enforcement

5. The DPA can export and share DPs.

   - Use Case: Import and Export DPs

### 4.17.3 ORG-01-DPM: Create and Maintain DP Content

The details of this use case are covered in:

A. Create and Maintain DP Content (Table 4-57)

There are no alternate flows, but exception flows are noted inline.

### Table 4-57 Create and Maintain DP Content

| Identifier | ORG-01-DPM-A: Create and Maintain DP Content |
|---|---|
| Description | This use case describes how the ORG DPA interacts with the DPMS to create, update, and verify DP content. |
| Actor(s) | Person:<br>• Digital Policy Administrator (DPA)<br>Non-person:<br>• Digital Policy Management System (DPMS) |
| Artifact(s) | • Authorization Profile<br>• Credential Profile<br>• Digital Policy (DP)<br>• Environment<br>• Resource Profile |
| Trigger | The DPA receives instructions for creating or modifying DP content to correct a difference between the organization’s policy intent and the actual ABAC DPs in the DPM. These instructions define the policy intent for controlling access using the attributes of the Authorization Profile and assertion, Credential Profile, Resource Profile, and Environment including policy exception handling and policy obligations. |
| Pre-conditions | The DPA has identified a difference between the organization’s policy intent and the actual ABAC DPs being enforced. |
| Post-conditions | New or revised DP content has been proposed for use in the ABAC enforcement and advanced from Draft DP to Approved DP, and then to Verified DP. |
| Main Flow<br>(exception flows are noted in-line) | 1. The DPA receives instructions in the DPMS for creation or modification of DP content.<br>Note: These instructions may include NLP and/or previously Approved DP or Activated DP that needs to be revised. The instructions must include the reason/intent for the new or revised policy.<br>2. The DPA identifies attribute types needed for DP and uses the DPMS to verify the presence of attribute types in the Authorization Profile and assertion, Credential Profile, Resource Profile, and Environment attributes.<br>Note: If some attributes that are needed are not available, ORG-04-PE and/or ORG-03-PE would be initiated to make the needed attributes available before proceeding.<br>3. The DPA creates Draft DP in the DPMS that meets the intent of the instructions.<br>Note: Policy conversion can be a multi-step process and requires some form of semantic analysis or even interpretation of the written policy along with capturing the authority, applicability of the policy, rule sets, and time horizon of the policy. |

| Identifier | ORG-01-DPM-A: Create and Maintain DP Content |
|---|---|
| | 4. The DPA generates evidence with test cases and test data to demonstrate that the Draft DP corresponds to the intent of the policy.<br>Note: This may include formal proof of correspondence between policies expressed in NLP, HRSLP, and/or DP formats. If HRSLP is not provided in step 1, it may be produced in this step by translation from DP as supporting evidence.<br>5. The DPA uses the DPMS to approve the draft DP and evidence.<br>6. The DPA uses the DPMS to evaluate the draft DP and evidence.<br>Note: ORG-07-PE is used to bind the Approved DP content to the attributes defining its effective and expiration dates and its “Approved” status using the digital signature of the Policy Steward. Disapproval may result in returning to step 3 for more evidence or to step 2 for revision of the DP. When the evidence includes HRSLP, this step may also result in Approved HRSLP being returned.<br>7. DPA uses the DPMS to identify other DPs with overlapping policy attribute triggers, analyzes the Approved DP for potential unresolved conflicts with the other DPs, and resolves any conflicts that are identified.<br>Note: Resolution of conflicts may include rejection of the Approved DP, returning to an earlier step in this use case, or modification of the policy combining rules.<br>8. The DPA uses the DPMS to perform quality and consistency checks on the outcome of triggered DPs to validate that they will execute as intended and resolves any unintended results.<br>Note: Resolution of unintended results may include rejection of the Approved DP, returning to an earlier step in this use case, or modification of the policy combining rules.<br>9. The DPA uses the DPMS to transition the Approved DP to the Verified DP state. |

### 4.17.4 ORG-02-DPM: Manage Activated DPs

The details of this use case are covered in:

A. Activate New Verified DP (Table 4-58)

B. Supersede, Revoke, or Retire DP (Table 4-59)

C. Manage AM Subscriptions (Table 4-60)

D. Bind DP to Objects (Table 4-61)

**Table 4-58 Activate New Verified DP**

| **Identifier** | **ORG-02-DPM-A: Activate New Verified DP** |
|---|---|
| Description | This use case describes how the ORG DPA interacts with the DPMS to activate a new verified DP in the AM. |
| Actor(s) | Person:<br>• Digital Policy Administrator (DPA)<br>Non-person:<br>• Access Manager (AM)<br>• Digital Policy Management System (DPMS) |
| Artifact(s) | • Digital Policy (DP) |
| Trigger | New Verified DP is available. |
| Pre-conditions | Information is available to the AM that allows a determination of the appropriate state and revocation status of the DPs and the subscription status of the AM. |
| Post-conditions | Activated DPs are available for discovery and retrieval by the AM. |
| Main Flow | 1. DPA retrieves new Verified DP in the DPMS.<br>2. DPA uses the DPMS to reformat DP for use by AM. This may include transformation to stay within the constraints of multiple AM types.<br>3. DPA uses the DPMS to transition the reformatted DP(s) to the Activated DP state and makes each Activated DP available for discovery and retrieval by AM. Only Activated DPs where the current date/time is between the effective and expiration date/time values are available for discovery and retrieval by the AM. |

Table 4-59 Supersede, Revoke, or Retire DP

| **Identifier** | **ORG-02-DPM-B: Supersede, Revoke, or Retire DP** |
|---|---|
| Description | This use case describes how the ORG DPA interacts with the DPMS to ensure that the superseded, expired, or revoked DPs are not available to AM. |
| Actor(s) | Person:<br>• Digital Policy Administrator (DPA)<br>Non-person:<br>• Access Manager (AM)<br>• Digital Policy Management System (DPMS) |
| Artifact(s) | • Digital Policy (DP) |
| Trigger | Activated DP is identified for supersession, revocation, and/or retirement. |
| Pre-conditions | Information is available to the DPA that allows a determination of the appropriate state and revocation status of the DPs. |
| Post-conditions | Retired, expired, and revoked DPs are not used by the AM. Retired DPs are retained for use in audit analysis. |
| Main Flow | 1. The DPA uses the DPMS to identify one or more DPs that should not be used for policy enforcement.<br>Note: When a new Verified DP supersedes existing Activated DPs, this Alternate Flow is invoked along with the Main Flow. When Activated DPs are expired or revoked, this Alternate Flow is invoked without the Main Flow.<br>2. The DPA uses the DPMS to ensure that the DPs are not available to the AM by adding them to a Digital Policy Revocation List (DPRL) and transitioning them to the Retired DP state. A DPRL is similar to a CRL in a PKI where the list is checked to determine whether the certificate (or in this case the DP) has been revoked prior to using it. Retired DPs may be physically removed from the stores that are accessible to the AM, but they should be retained for use in audit analysis in the Monitor DP Enforcement use case. |

### Table 4-60 Manage AM Subscriptions

| **Identifier** | **ORG-02-DPM-C: Manage AM Subscriptions** |
|---|---|
| Description | This use case describes how the ORG DPA interacts with the DPMS to manage the dissemination of active DPs including DP and attributes retrieval ordering precedence to the AM for enforcement. |
| Actor(s) | Person:<br>• Digital Policy Administrator (DPA)<br>Non-person:<br>• Access Manager (AM)<br>• Digital Policy Management System (DPMS) |
| Artifact(s) | • Digital Policy (DP) |
| Trigger | AM subscriptions to Activated DPs including DP and attribute retrieval ordering precedence. |
| Pre-conditions | Information is available to the Policy Dissemination Administrator that allows a determination of the subscription status of the AM. |
| Post-conditions | AM subscriptions are up to date. |
| Main Flow | 1. The DPA uses the DPMS to identify an AM that should have its Activated DP subscription updated.<br>2. The DPA uses the DPMS to update the AM subscription.<br>3. The DPA uses the DPMS to provide DP and attribute retrieval ordering precedence rules to the AM. |

### Table 4-61 Bind DP to Objects

| **Identifier** | **ORG-02-DPM-D: Bind DP to Objects** |
|---|---|
| Description | This use case describes how the ORG DPA interacts with the DPMS to bind DPs to the applicable PR when the AM retrieves DPs with PR Resource Profile attributes, rather than through a separate DP discovery mechanism. |
| Actor(s) | Person:<br>• Digital Policy Administrator (DPA)<br>Non-person:<br>• Access Manager (AM)<br>• Digital Policy Management System (DPMS) |
| Artifact(s) | • Digital Policy (DP)<br>• Resource Profile |
| Trigger | This alternate flow is invoked along with the main flow (ORG-02-DPM-A) when the AM retrieves the DPs with PR Resource Profile attributes. |
| Pre-conditions | The AM is configured to retrieve DPs with PR Resource Profile attributes. |
| Post-conditions | Activated DPs are available for discovery and retrieval by AMs via attribute discovery and retrieval services. |
| Main Flow | 1. The DPA uses the DPMS to bind applicable Activated DPs to the PR and removes superseded, expired, or revoked DPs.<br>2. The DPA uses the DPMS to update PR Resource Profile attributes with the applicable DP binding.<br>Note: This step assumes that the AM can be used to post updates for PR Resource Profile attributes. |

### 4.17.5 ORG-03-DPM: Provide DPs for Access

The details of this use case are covered in:

A. Provide DPs for Access (Table 4-62)

**Table 4-62 Provide DPs for Access**

| **Identifier** | **ORG-03-DPM-A: Provide DPs for Access** |
|---|---|
| Description | This use case describes how the ORG DPMS provides Activated DPs to subscribed AMs for use in ABAC policy enforcement. |
| Actor(s) | Non-person:<br>• Access Manager (AM)<br>• Digital Policy Management System (DPMS) |
| Artifact(s) | • Digital Policy (DP) |
| Trigger | AM requests the DPs that are applicable to a subject request for access to a PR under the current environmental conditions. |
| Pre-conditions | The AM is subscribed to the published DPs and configured with rules that govern the content and format of requests and the processing of responses. |
| Post-conditions | The AM has the Activated DPs that are needed to render an access control decision, enforce that decision, and satisfy policy obligations. |
| Main Flow | 1. The AM uses the DPMS to request the DPs that are applicable to a PE request for access to a PR under the current environmental conditions.<br>2. Applicable Activated DPs that are not expired, superseded, or revoked are returned by the DPMS to the AM. |

### 4.17.6 ORG-04-DPM: Import and Export DPs

The details of this use case are covered in:

A. Import and Export DPs (Table 4-63)

Similar use case flows could be executed to import and export non-digital (i.e., NLP) policies.

**Table 4-63 Import and Export DPs**

| **Identifier** | **ORG-04-DPM-A: Import and Export DPs** |
|---|---|
| Description | This use case describes how the ORG DPA interacts with the DPMS to send and receive DPs (i.e., Approved HRSLPs, Approved DPs, or Activated DPs) with PTR domains. |
| Actor(s) | Person:<br>• Digital Policy Administrator (DPA)<br>Non-person:<br>• Digital Policy Management System (DPMS)<br>• Partner (PTR) |
| Artifact(s) | • Digital Policy (DP) |
| Trigger | The DPA identifies DPs to be shared in a hierarchical relationship or under peer-to-peer information sharing agreements. |
| Pre-conditions | The policy aspects of the hierarchical relationships and peer-to-peer information sharing agreements are known to the DPAs in both domains. |
| Post-conditions | Applicable DPs are shared across the PTR DPM domains. |
| Main Flow<br>(Export DPs) | 1. DPA uses the DPMS to identify DPs to be shared with the other PTR DPM Domain.<br>2. DPA sends identified DPs to another PTR DPM domain. ORG procedures established for DP sharing with other PTR DPM domains control this process. |
| Alternate Flow<br>(Import DPs) | 1. DPs are received from another PTR DPM domain.<br>2. The DPA uses the DPMS to process the received DPs. This processing includes execution of ICAM use cases involving the sending and receiving domains to ensure the DPs accurately reflect the policy intent; procedures established in the receiving PTR DPM domain processing and whether the state of the DP in the sending domain is retained by the receiving domain. For example, Activated DP from another domain might be considered Approved DP in the receiving domain and require execution of steps 7-9 of ORG-01-DPM followed by ORG-02-DPM before it is considered Activated DP in the receiving domain. The procedures of the receiving domain should be consistent with the hierarchical relationships or peer-to-peer information sharing agreements that govern the policy sharing. |

# 5. NEXT STEPS

As summarized in Figure 3-4, the twenty-two use cases defined by this report cover all 14 management functions, all 9 enforcement functions and 3 of the 6 supporting functions identified by the FICAM services framework. However, these ICAM use cases do not address the broader set of use cases covering security, conformance and risk management or the ICAM support functions of key management, enterprise governance, redress and recovery. The following follow-on efforts are suggested to help close this gap between the ORG cybersecurity concerns and the ICAM use cases defined by this report:

1. Develop cybersecurity use cases that cover security management, content management, application management, infrastructure management, key management, ICAM conformance, enterprise governance, redress, recovery and ICAM risk management.

2. Develop operational use cases, identity the ICAM use cases that apply and formulate ICAM requirements that can be used to evaluate proposed approaches, architectures, and technologies for implementing ICAM in government and private sector organizations.

*This page intentionally left blank.*

# 6. REFERENCES

1. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 2.0, 8 December 2011. Retrieved from http://www.idmanagement.gov/documents/ficam-roadmap-and-implementation-guidance

2. U.S. General Services Administration (GSA) in-progress Federal ICAM Enterprise Architecture Services Framework, beta site http://gsa.github.io/ficam-arch/services/.

3. NIST Special Publication 800-63-3B DRAFT, National Institute of Standards and Technology, *Digital Identity Guidelines: Authentication and Lifecycle Management*, February 2017.

4. NIST Special Publication 800-63-3C DRAFT, National Institute of Standards and Technology, *Digital Identity Guidelines: Federation and Assertions*, February 2017.

5. E-Authentication Guidance for Federal Agencies, Office of Management and Budget, December 16, 2003.

6. NIST Special Publication 800-63-3 DRAFT, National Institute of Standards and Technology, *Digital Identity Guidelines*, February 2017.

7. NIST Special Publication 800-63-3A DRAFT, National Institute of Standards and Technology, *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*, February 2017.

8. *Digital Policy Management Framework (DPMF) for Attribute-Based Access Control (ABAC)*, 19 December 2014. Retrieved from https://www.ise.gov/resources/document-library/digital-policy-management-framework-attribute-based-access-control.

9. *Government Mobile and Wireless Security Baseline*, Federal CIO Council, 23 May 2013.

10. Mobile Security Reference Architecture, Federal CIO Council and U.S. Department of Homeland Security National Protection and Programs Directorate (NPPD), 23 May 2013.

11. Framework for Improving Critical Infrastructure Security, Version 1.0, National Institute of Standards and Technology, February 2014.

12. NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* Revision 4, National Institute of Standards and Technology, April 2013.

13. *Information Technology – Security techniques – Code of practice for information security management*, ISO/IEC 27002, International Organization for Standardization/International Electrotechnical Commission, 2013.

14. *Critical Security Controls for Effective Cyber Defense, Version 6.0,* Center for Internet Security, October 2015.

15. A. Garver, *Make Enterprise Mobility Management a Use-Case Decision for Managing Windows 10 and Mac OS X*, Gartner, Inc., G00293667, 21 March 2016.

16. NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, National Institute of Standards and Technology, June 2013.

17. *Mobile Device Security: A Comparison of Platforms*, Patrick Hevesi, Gartner, Inc., G00292802, 6 April 2016.

18. M. Disabato, *Moving Beyond EMM to Unified Workspaces and the Contextual Fabric*, Gartner, Inc., G00303880, 6 February 2017.

19. *Unified Workspaces: The Convergence of the Mobile and End-User Computing Journey*, A. Garver, Gartner, Inc., G00293326, 29 January 2016.

20. U.S. General Services Administration (GSA) in-progress Federal ICAM Enterprise Architecture Use Cases, beta site http://gsa.github.io/ficam-arch/usecases/.

21. E-Authentication Guidance for Federal Agencies, Office of Management and Budget, December 16, 2003.

# APPENDIX A. DESCRIPTIONS OF ICAM FUNCTIONS

**Table A-1 ICAM Function Descriptions**[16]

| ICAM Functions | Descriptions |
|---|---|
| Account Management | Processes of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions. |
| Adjudication | Process of evaluating pertinent data in a background investigation, as well as any other available information that is relevant and reliable to determine whether a covered individual is suitable for government employment and/or eligible for particular privileges. |
| Attribute Exchange | Discovering and sharing identity attributes between different systems to promote interoperability and simplify the process for establishing an identity.<br>*Keywords*: Attribute Definition, Attribute Retrieval Service |
| Audit Analysis | Capability to collect detailed information about system entities, usage activity, and identity audit events and present it in a meaningful way. |
| Audit Record Generation | Capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. |
| Auditing & Reporting | Monitoring, reviewing, and reporting on an ICAM program’s conformance with rules, policies, and requirements.<br>*Keywords*: Data collection, Monitoring, Analysis, Data Certification |
| Authoritative Attribute Exchange | Capability that performs discovery and mapping of attributes from authoritative source repositories and enables sharing of these attributes. |
| Backend Attribute Retrieval | Capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision. |
| Bind/Unbind | Process of building or removing a relationship between an entity’s identity and further attribute information on the entity (e.g., privileges, properties, status, credentials, etc.). |
| Biometric Validation | Capability to support capturing, extracting, comparing, and matching a measurable, physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an entity. Biometrics modalities include face, fingerprint, and iris recognition and can be matched on card, on reader, or on server. |

[16] Descriptions in the table are from References 1 and 2.

**Table A-1 ICAM Function Descriptions (Continued)**

| ICAM Functions | Descriptions |
|---|---|
| Credential Bridging | Establishing a cross-certified, affiliated relationship to trust credentials at a level of assurance asserted by those credentials.<br>*Keywords*: Federal PKI Bridge |
| Credential Life-Cycle Management/ Maintenance | Process of maintaining a credential and associated support over the life cycle; common processes include renewal, reissuance, suspension, blocking and unblocking, revocation, etc. Life-cycle support activities vary depending on the credential type and may include a Self-Service component. |
| Credential Maintenance | Maintaining a credential over its life cycle.<br>*Keywords*: Renewal, Reset, Suspension, Blocking, Reissuance |
| Credential Revocation | Withdrawing a credential from a person or entity.<br>*Keywords*: Termination |
| Credential Translation | Transforming a token or credential into an alternative format, potentially containing claims about the client, for acceptance at a relying party.<br>*Keywords*: Secure Token Service, Assertion Service |
| Credential Validation | Process that establishes the validity of the identity credential presented as part of the authentication transaction; PKI certificates are validated using techniques such as revocation status checking and certificate path validation. Validation of other credentials can include security object check, Cardholder Unique Identifier validation, mutual Secure Socket Layer/Transport Layer Security, the validation of digital signatures, or other non-biometric and non-cryptographic mechanisms. |
| Digital Identity Life-Cycle Management | Process of establishing and maintaining the attributes that comprise an individual’s digital identity; supports general updates to an identity such as a name change or biometric update. |
| Deprovisioning | Removing an entity’s access privileges from a protected resource. |
| Digital Signature | Capability of an asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection. |
| Encryption/Decryption | Encryption is the process of transforming information using a cipher algorithm to make it unreadable to any entity except those possessing special knowledge, usually referred to as a key. Decryption is the process of making encrypted information readable again. |
| Enrollment/Registration | Process of collecting and storing identity information of an entity in a registry/repository; associates the entity with minimal information representing the entity within a specific context and allows the entity to be distinguished from any other entity in the context. |
| Enterprise Governance | Developing and implementing the policies, rules, and procedures to manage and improve an ICAM program. |

**Table A-1 ICAM Function Descriptions (Continued)**

| **ICAM Functions** | **Descriptions** |
|---|---|
| Entitlement Management | Establishing and maintaining the authoritative access permissions for a person or non-person entity.<br>*Keywords*: Privilege, Right, Access Recertification, Account Management |
| Factor Validation | Validating the credential factors: something you know, something you have and something you are. |
| Federation | Capability to support a trust relationship between discrete digital Identity Providers that enable a relying party to accept credentials from an external Identity Provider in order to make access control decisions; provides path discovery and secure access to the credentials needed for authentication; and federated services typically perform security operations at run time using valid NPE credentials. |
| Identity Creation | Establishing a digital identity composed of attributes that define a person or entity.<br>*Keywords*: Identity Lifecycle Management, Identity Record, Authoritative Source |
| Identity Deactivation | Deactivating or removing an identity record.<br>*Keywords*: Identity Lifecycle Management, Suspension, Archiving, Deletion |
| Identity Maintenance | Maintaining accurate and current attributes within an identity record over its life cycle.<br>*Keywords*: Identity Lifecycle Management, Updating, Attribute Management |
| Identity Proofing | Process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity; initiates chain of trust in establishing a digital identity and binding it to an individual. |
| Identity Resolution | Finding and connecting disparate identity records for the same person or non-person entity.<br>*Keywords*: Identity Reconciliation, Account Linking |
| Issuance | Process by which possession of a credential is passed to an entity. Service characteristics vary by credential type.<br>*Keywords*: Activation, Token |
| Key Management | Processes involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. |
| Linking/Association | Process of linking one Identity Record with another across multiple systems; activation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications in response to an automated or interactive process; used in conjunction with Authoritative Attribute Exchange. |

**Table A-1 ICAM Function Descriptions (Continued)**

| **ICAM Functions** | **Descriptions** |
|---|---|
| Policy Administration | Process of creating, disseminating, modifying, managing, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection in a standard policy exchange format. |
| Policy Alignment | Establishing a mutual relationship between parties by deliberately establishing common standards and principles.<br>*Keywords*: Trust Relationship |
| Policy Decision | Capability that serves as an access control authorization authority for evaluating access control policies based on a variety of inputs. |
| Policy Enforcement | Capability that restricts access to specific systems or content in accordance with policy decisions that are made. |
| Privilege Administration | Process for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile; supports updates to privileges over time as an individual's access needs change. |
| Provisioning | Capability of creating entity access accounts and assigning privileges within the scope of a defined process or interaction; provide entities with access rights to applications and other resources that may be available in an environment; may include the creation, modification, deletion, suspension, or restoration of a defined set of privileges. Linking and unlinking access permissions for an entity to a protected resource.<br>*Keywords*: Workflow, Deprovisioning |
| Registration | Collecting the information needed to issue a credential to a person or non-person entity.<br>*Keywords*: Enrollment |
| Recovery | Preparing the procedures and assets that would be needed to recover from a security or privacy breach and ensure continuity of service.<br>*Keywords*: Mitigation |
| Redress | Fixing problems and vulnerabilities that occur during standard operation of an ICAM program.<br>*Keywords*: Remediation |
| Resource Attribute/Metadata Management | Process for establishing and maintaining data (such as rules for access, credential requirements, etc.) for a resource/asset being provisioned to define the access, protection, and handling controls. Specific data tags are used that explicitly state how data or a service is accessed, stored, transmitted, or even if it can be made discoverable. |
| Self-Service | Capability to request access to network and physical resources based on established credentials, reset forgotten passwords, update identity and credential status information, and view corporate and organizational identity information using electronic interfaces and without supervisory intervention. |

**Table A-1 ICAM Function Descriptions (Continued)**

| **ICAM Functions** | **Descriptions** |
|---|---|
| Session Management | Capability that allows for the sharing of data among multiple relying parties as part of an authenticated user session; includes protocol translation services for access to systems needing different authentication protocols; manages automatic timeouts and requests for re-authentication. |
| Sponsorship | Process for establishing the need for a card/credential by an authorized official; this step is critical for NPE credential request and issuance. Formally establishing that a person or entity requires a credential.<br>*Keywords*: Sponsor, Authorizing Official, Affiliation, Request |
| Vetting | Process of examination and evaluation, including background check activities, results in establishing verified credentials and attributes. |

# APPENDIX B. LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AAA | Authorized Authority Administrator |
| AAES | Authoritative Attribute Exchange Service |
| AAL | Authenticator Assurance Levels |
| ABAC | Attribute-Based Access Control |
| ACL | Access Control List |
| ACR | Authorized Credential Request |
| AM | Access Manager |
| AMR | Activity Monitoring Request |
| AMS | Account Management System |
| AMSA | Account Management System Administrator |
| AND | Authentication Data and Results |
| AP | Authenticator Provider |
| APAR | Authorized Privilege and Account Request |
| APPR | Authorized Privilege and Profile Request |
| AR | Authoritative Resource including MPs and LEs |
| ATO | Authority to Operate |
| AuthN | Authentication |
| AuthN Cert | Authentication Certificate |
| BYOD | Bring Your Own Device |
| CA | Certificate Authority |
| CAC | Common Access Card |
| CAK | Card Authentication Key |
| CIO | Chief Information Officer |
| CMS | Credential Management System |

| | |
|---|---|
| CMSA | Credential Management System Administrator |
| CMSW | Credential Management System Wizard |
| COBO | Corporate-Owned, Business Only |
| COPE | Corporate-Owned, Personally Enabled |
| CRL | Certificate Revocation List |
| Crypto | Cryptographic key |
| CryptoD | Cryptographic device with basic authenticator storage |
| CryptoSH | Cryptographic device with FIPS-140 secure authenticator hardware storage |
| CryptoSS | Cryptographic device with FIPS-140 secure authenticator software storage |
| DP | Digital Policy |
| DPA | Digital Policy Administrator |
| DPC | Derived PIV/PIV-I Credential |
| DPM | Digital Policy Management |
| DPMF | Digital Policy Management Framework |
| DPMS | Digital Policy Management System |
| DPRL | Digital Policy Revocation List |
| EAR | Event Auditor and Reporter |
| EMM | Enterprise Mobility Management |
| EPD | Endpoint Device |
| ETS | Event Tracking System |
| FAL | Federation Assurance Levels |
| FAM | Facility Access Manager |
| FICAM | Federal Identity, Credential, and Access Management |
| FIPS | Federal Information Processing Standard |
| GPS | Global Positioning System |

| | |
|---|---|
| GSA | U.S. General Services Administration |
| HRSLP | Human-Readable Structured Language Policy |
| IAL | Identity Assurance Levels |
| IBAC | Identity-Based Access Control |
| ICAM | Identity, Credential, and Access Management |
| ID | Identifier |
| IdP | Identity Provider |
| IEC | International Electrotechnical Commission |
| IM | Instant Messaging |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IRA | Identity Record Administrator |
| ISO | International Organization for Standardization |
| JHU/APL | The Johns Hopkins University Applied Physics Laboratory |
| LACS | Logical Access Control System |
| LE | Logical Entity |
| LOA | OMB M-04-04 Level of Assurance, classifications are 1-4 |
| MAR | Monitored Activity Report |
| MND | Managed Network Device |
| MP | Managed Provider including MSPs, MNDs and MSSs |
| MS | Monitored System |
| MSP | Managed Server Platform |
| MSS | Managed Shared Service |
| MSSP | Managed Security Service Provider |
| MZ | Managed Zone |

| | |
|---|---|
| NIST | National Institute of Standards and Technology |
| NLP | Natural Language Policy |
| NPE | Non-Person Entity |
| OCPS | Online Certificate Status Protocol |
| OID | Object Identifier |
| OMB | Office of Management and Budget |
| OOB | Out of Band authenticator |
| ORG | Organization |
| OS | Operating System |
| OSI | Open Systems Interconnection |
| OTP | One Time Password authenticator |
| PE | Person Entity |
| PIN | Personal Identification Number |
| PIV | Personal Identify Verification |
| PIV-I | Personal Identity Verification-Interoperable |
| PKI | Public Key Infrastructure |
| PMS | Privilege Management System |
| PMSA | Privilege Management System Administrator |
| POBA | Personally Owned, Business Applied |
| PR | Protected Resource |
| PTR | Organization or agency that has a partnership relationship with ORG |
| RBAC | Role-Based Access Control |
| S/MIME | Secure/Multipurpose Internal Mail Extension |
| SCVP | Server-based Certificate Validation Protocol |
| SLTT | State, Local, Tribal, and Territorial |

| | |
|---|---|
| SMS | Short Message Service |
| SP | Service Provider |
| SRA | Service Request Application |
| SRAA | Service Request Application Administrator |
| SSO | Single Sign-On |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UC | Use Case |
| UEM | Unified Endpoint Management |
| VPN | Virtual Private Network |
| xAL | NIST IAL, AAL or FAL assurance level |