



California  
DEPARTMENT OF TECHNOLOGY

# California Enterprise Architecture Framework

## Identity and Access Management (IdAM) Reference Architecture (RA)

---

Version 1.0 Final  
January 2, 2014



*This Page is Intentionally Left Blank*



# TABLE OF CONTENTS

1	Introduction.....	1
1.1	Purpose .....	1
1.2	Limitations.....	2
1.3	Intended Users.....	2
1.4	Document Organization .....	2
1.5	Future Directions .....	2
2	Identity and Access Management Overview .....	3
2.1	Definitions.....	3
2.2	Challenges for IdAM in Government Context.....	4
2.3	IdAM Business Benefits.....	5
2.4	Main IdAM Usage Scenarios .....	6
2.5	Key Capabilities of IdAM Solution .....	6
2.6	Components of IdAM Solution.....	7
2.6.1	<i>Authentication and Authorization Services.....</i>	<i>8</i>
2.6.2	<i>Identity and Policy Repositories .....</i>	<i>9</i>
2.6.3	<i>Identity Management Components .....</i>	<i>9</i>
2.6.4	<i>Policy and Privilege Management Components .....</i>	<i>10</i>
2.6.5	<i>Protected Resources and IdAM Integration Components.....</i>	<i>11</i>
2.6.6	<i>Auditing and Reporting Components.....</i>	<i>12</i>
2.6.7	<i>Cryptography Components .....</i>	<i>13</i>
2.7	Federated Identity Management (FIM) .....	13
2.7.1	<i>FIM Roles and Scenarios .....</i>	<i>13</i>
2.7.2	<i>Types of FIM Solutions .....</i>	<i>18</i>
2.7.3	<i>FIM-Related Standards .....</i>	<i>18</i>
3	IdAM Reference Architecture Description .....	19
3.1	IdAM RA Conceptual View .....	19
3.2	IdAM RA Logical View .....	21
3.2.1	<i>High-Level Interactions .....</i>	<i>21</i>
3.2.2	<i>Accessing Protected Resources .....</i>	<i>23</i>
3.2.3	<i>Creating and Maintaining Digital Identities, Accounts and Policies.....</i>	<i>26</i>
3.3	IdAM RA Deployment View.....	29



4	Glossary .....	30
5	References .....	31
6	Document History .....	32



## LIST OF FIGURES

<i>Figure 2-1 Overview of IdAM Components</i> .....	7
<i>Figure 2-2 Components in Authentication and Authorization Services</i> .....	8
<i>Figure 2-3 Identity and Policy Repository Components</i> .....	9
<i>Figure 2-4 IdAM Identity Administration Components</i> .....	10
<i>Figure 2-5 IdAM Policy and Privilege Management Components</i> .....	10
<i>Figure 2-6 Protected Resources and IdAM Integration Components</i> .....	11
<i>Figure 2-7 Auditing and Reporting Components in IdAM</i> .....	12
<i>Figure 2-8 IdAM Cryptography Components</i> .....	13
<i>Figure 2-9 FIM Federated SSO Scenario</i> .....	14
<i>Figure 2-10 FIM Federated SSO Scenario</i> .....	16
<i>Figure 2-11 FIM Web Services Scenario</i> .....	17
<i>Figure 3-1 Identity and Access Management Reference Architecture – Conceptual View</i> .....	20
<i>Figure 3-2 IdAM Component Interactions</i> .....	21
<i>Figure 3-3 Accessing Protected Resources</i> .....	24
<i>Figure 3-4 Creating and Maintaining Digital Identities, Accounts and Policies</i> .....	27



## LIST OF TABLES

<i>Table 3-1 High-level interactions among IdAM components.....</i>	<i>22</i>
<i>Table 3-2 Accessing protected resources - IdAM component interactions .....</i>	<i>25</i>
<i>Table 3-3 Creating and maintaining digital identities, accounts and policies - IdAM component interactions .....</i>	<i>28</i>
<i>Table 6-1 Document History .....</i>	<i>32</i>



*This Page is Intentionally Left Blank*

# 1 Introduction

Identity and Access Management (further abbreviated as IdAM) is a key infrastructure element in enterprise today. IdAM serves as the cornerstone of any valid security solution in IT. However, the IdAM problem domain is not considered simple in the first place. IT Security in itself is hard and IdAM in today's enterprise is far from simple.

The emerging SOA/Cloud combination helps organizations become more agile, but also creates new challenges for Enterprise Architecture practitioners, not only at the conceptual level, but also in practice of dealing with IdAM patterns and their implementations.

The rising adoption of SOA makes traditional approaches to IdAM insufficient as the traditional perimeter-based security cannot adequately protect exposed services. Also, the move towards Cloud-based deployments adds new issues to the mix. Last but not least, in the government space there is a special combination of requirements (including the target scale, variation in user skills, existing infrastructure and applications). All of those factors make IdAM a crucial area for CEAF 2.0.

## 1.1 Purpose

The *State Identity, Credential, and Access Management (SICAM) Roadmap and Implementation Guidance, Version 2.0* (further abbreviated as *SICAM 2.0*), described the concepts, processes, standards, and implementation approach for SICAM and introduced the conceptual level SICAM architecture framework. As stated in SICAM 2.0, effective implementation of SICAM requires state agencies to apply that conceptual architecture framework to build their portion of IdAM capabilities depending on their role in the federated government framework (e.g., service consumer, service provider and identity provider), and the security requirements of their existing applications and/or application components (e.g., services) which need to be accessible in a federated environment.

To assist state agencies apply the SICAM conceptual architecture framework effectively, additional guidance is provided through this Reference Architecture, referred to as Identity and Access Management Reference Architecture (IdAM RA).

The IdAM RA document provides further guidelines and options for making architectural decisions when implementing IdAM solutions in accordance with SICAM 2.0.

The objectives for this document include the following:

- To introduce key terms and distinctions relevant for the topic
- To provide inputs for creating or evaluating architectures for IdAM from enterprise perspective
- To identify building blocks (architectural layers, services, components) for integrating elements of an IdAM solution
- To communicate the key architectural decisions relevant for creating or evaluating IdAM solutions
- To communicate opportunities for solution and/or platform sharing at agency, cross-agency and/or state levels

## 1.2 Limitations

The document focuses on IdAM and related concepts at the enterprise architectural level in the context of CEAF 2.0 and SICAM 2.0. It is not intended to serve as the IdAM-related product guide, or a guide for *organizational* aspects of IdAM solutions. It is also not intended as an endorsement of any product. Its overall perspective remains CEAF- and SICAM-centric.

## 1.3 Intended Users

The primary intended users of this document are Enterprise Architecture practitioners and other architects that contribute to enterprise architecture. This broad group includes architects from other domains/disciplines such as Security, Application, Information, Business, Technology, Infrastructure, and Solution Architects. It is also beneficial to Managers, at senior or operational levels, who are involved with IdAM or related areas, such as broader Security domains, Enterprise Application Integration, Cloud Computing, SOA, and similar areas.

## 1.4 Document Organization

The IdAM Reference Architecture documentation is organized as follows:

- Section “IdAM Overview” provides background for the IdAM RA by introducing descriptions and definitions of IdAM, discusses the main usage scenario types found in IdAM implementations, and identifies architectural components for respective usage scenarios
- The section “IdAM Reference Architecture Description” elaborates RA for IdAM using the following architectural views:
  - The Conceptual View (in the subsection “IdAM RA Conceptual View”) introduces the necessary capabilities for an IdAM architecture and how they are supported by Architectural Building Blocks (ABBs)
  - The Logical View (in the subsection “IdAM RA Logical View”) describes key interactions among Layers and/or ABBs to realize functionality specific to IdAM systems
  - The Deployment View (in the subsection “IdAM RA Deployment View”) focuses on system topologies and deployment facets of IdDM in the state
- The section “Glossary” provides description of the terms and abbreviations used in the document
- The section “References” lists publications used for preparation of the document

## 1.5 Future Directions

Future evolution of the document includes the following steps:

- Addition of existing best-practice-based realizations of the IdAM RA
- Identification and elaboration of solution sharing opportunities
- Formulation of implementation guidelines for IdAM RA

## 2 Identity and Access Management Overview

This section provides a description of IdAM, including clarification of key terms and concepts. It identifies IdAM's intended business benefits and summarizes its main usage scenarios. A set of key capabilities of IdAM solutions are identified in this section and key components of the solution are described at a high level.

### 2.1 Definitions

For the purpose of the IdAM RA, as a part of CEAF 2.0, we adopt the following definition of Identity and Access Management (IdAM):

*IdAM is the set of business processes, technologies and policies for the creation, maintenance, termination, and use of digital identities for people, systems, and services and for controlling how these digital identities are used to access resources (information, applications or systems).*

IdAM has two parts, one focusing on Identity Management, and the other concerned with Access Management. Given that Access Management requires Identity Management for its operation, it makes sense to treat them jointly at the architectural level. Both elements of IdAM belong to a larger domain of enterprise security and they are core components of any enterprise security solution. IdAM addresses some of the fundamental security requirements, including the following:

- Requirement to determine who the users of the system or systems are, and how to validate that they are who they claim to be
- Requirement to ensure that a given user is required to go through an authentication procedure only once even when accessing multiple systems, services or resources
- Requirement to determine which resources (information, applications, services, etc.) they have access to and on what basis as well as supporting fine-grained authorization enforcement
- Requirement to identify the roles with responsibility for authorizing access to specific resources
- Requirement to monitor, capture, and audit identity- and access-related events in the organization
- Requirement to streamline and reduce the total cost of ownership of maintaining digital identities through automation and/or through trust relationships with other organizations

The above list is not exhaustive – nevertheless it is representative of the scope of IdAM, its challenges and difficulties in an environment that contains many interconnected systems and services, which are accessed by disparate groups of users (internal or external, human or systems), to whom different regulations and rules may apply.

Stated succinctly, the goal of IdAM is *to enable the right individuals to access the right resources at the right times from the right environment for the right reasons*. IdAM should be viewed as an enterprise-wide shared middleware layer capable of supporting a number of disparate applications, regardless of whether they are legacy applications or not, whether they fit the SOA approach or not, or whether they make use of Cloud Computing or not.

The area of IdAM uses a number of key terms, which are briefly introduced here:

- **Entity** refers to an individual or an organization

- **Attribute** is a characteristic of an entity (e.g., names, DOB, etc.)
- **Identity** is an abstract representation of entity in a given context
- **Partial Identity** is a subset of attributes of an identity
- **Context** is scope in which particular (partial) identity is defined and has meaning

The extent of the context varies from a narrow and constrained (e.g., within boundaries of a single application or system) scope, to wider departmental or organizational scopes (local or distributed), and up to global or universal scope. This is an important factor when considering enterprise-level IdAM solutions, because pre-existing IdAM approaches that may be sufficient in a narrow scope are not necessarily acceptable in larger scopes.

## 2.2 Challenges for IdAM in Government Context

There are a number of challenges when creating an enterprise-level IdAM solution and when driving adoption of the solution, both internally in an organization, and externally, for external users and service consumers. Some of those challenges are *common* to most IdAM solutions, regardless of whether they are deployed in public or in private sector, or whether they use SOA or not. The fundamental challenge is the lack of universal or standardized approaches to design and development of identity management systems, even though initiatives to produce such approaches do exist (e.g., the Liberty Alliance). More specific challenges include the following:

- Providing for Authentication and Authorization functions as required by the business
- Avoiding “password fatigue” by supporting Single Sign-On
- Efficiently provisioning and de-provisioning users and services
- Detecting threats and fraud
- Detecting compromised identities
- Monitoring and auditing accesses to protected resources
- Interoperability problems with disparate IdAM implementations

Adopting SOA introduces another set of challenges, including the following:

- Transport-level security and perimeter-based security for services is no longer sufficient because using services entails many potential points of entry. This makes unavoidable the introduction of access control at mediation points (such as routing in the ESB, XML gateways) and at the end point (the target service)
- Loose coupling and mediation between components in the SOA world exposes more vulnerabilities, and adds complexity to interactions between components as far as establishing the trust and monitoring are concerned
- The mechanisms for Authentication or Authorization cannot be assumed to be homogeneous, internally provided or under organization’s full control. Rather, these mechanisms become increasingly heterogeneous, possibly provided externally to an organization or even the enterprise, and with limited to no control over its internal functioning
- Ensuring that an identity is authoritative and unique in a given context/security domain, given that heterogeneous systems introduce multiple digital identities from disparate sources
- Matching and relating identities (identity resolution) and mapping multiple digital identities to a single user or entity
- Identifying ramifications of the changing ratio between human users and other systems/applications when importance of non-human users grows considerably

- Developing security policies for identity management that can be effective in SOA and address the shift from application-centric approaches to organization- and user-centric approaches

Public sector, moreover, is characterized by a combination of challenges for IdAM that are not as visible or important elsewhere. These government-specific challenges can influence how IdAM solutions should be approached in state organizations; they include the following:

- Targeting very broad demographic *groups* of users, with considerable differences in age, technical skills, and their physical and cognitive abilities
- Involving large or very large number of users. Especially in the case of publicly accessible systems, the number of serviced users can reach tens of millions. This is not so common in other contexts, and which – together with inherent strong differentiation in the roles and privileges of the users – may create rather unique combination, not only from a technical perspective, but also with respect to the cost of potential licensing, standards and regulatory issues
- Dealing with a number of incompatible IdAM solutions (ranging from legacy systems with their own internal proprietary solutions to various standard-based solutions) as the requirement to service a large and varied user base means the need to integrate disparate systems – this can have an impact on long term evolution of IdAM solutions in the government space
- Meeting users expectations with respect to protecting their privacy (including identity theft), and providing high level of transparency in handling of security and privacy by government organizations
- Addressing requirements of law enforcement and national security, which can affect security in government-provided on-line services to a higher degree than elsewhere

The above factors can affect specific organization's IdAM-related goals and policies, satisfaction of which could be challenging using a single, one-fits-all IdAM solution. Although the presented IdAM Reference Architecture attempts to provide a common starting point for IdAM solutions in the government context, it should be kept in mind that some of the possible requirements, e.g. those related to law enforcement, may be best addressed by careful analysis of specific cases and their detailed requirements.

## 2.3 IdAM Business Benefits

Although introducing an IdAM solution is not simple for IT, it has – when successful - the following benefits for the business:

- Allowing for reliable identification of participants in electronic interactions (including, but not limited to, e- business transactions). In more general terms, IdAM solution allows enforcement of business policies that involve identity and access to resources, with a view to enable on-line interactions in the first place
- Increasing reliability and efficiency in managing internal (within the organization) and external users by adopting proven and consistent solutions; the efficiency of this managing has an impact on the level of organizational agility, in terms of the organization's ability to accommodate changing applicable regulations or laws, changes in user base, or simply making new functions or services available quickly and reliably
- Improving resilience to identity-based security attacks and improving ability to detect such attacks

- Simplifying security aspects of integration of business applications, and consequently increasing flexibility in creating new or modifying existing business processes by providing enterprise-wide IdAM shared middleware layer
- Supporting future evolution of security aspects of internal applications and of integration with external service providers by adopting open standards and standardized APIs
- Enhancing usability for users of complex applications by supporting Single Sign-On (SSO) and Cross-Domain Single Sign-On (CDSO), Single Logoff, and Federated Identity Management (FIM)

## 2.4 Main IdAM Usage Scenarios

Use cases and usage scenarios representative for IdAM solutions can be grouped in a number of different ways. The grouping adopted in this document is based on distinguishing the main actors who participate in the usage scenarios. The resulting grouping is as follows:

- End-User scenarios, which involve internal or external service consumers (people or systems), and which take place at runtime, when services are actually consumed or resources accessed
- Administrative scenarios, which typically involve Security Administrators, and take place at IdAM configuration time
- Compliance enforcement and Audit scenarios, which involve Auditors and Compliance Officers, and which utilize Audit Trails produced during execution of IdAM functions.

For discussion of the above groups of scenarios and the IdAM components involved in their execution, please refer to the section “IdAM RA Logical View”

## 2.5 Key Capabilities of IdAM Solution

The core capabilities of IdAM are as follows:

- *Centralized life cycle management* of a user's digital identity and attributes, which involves the following:
  - User and Group administration
  - Delegated administration and self service
  - Credentialing
- *Centralized administration* of the following:
  - User groups, user entitlements/permissions
  - Access policies
  - Provisioning of security for existing applications
- Providing Authentication Service, including support for multi-factor authentication when needed
- Brokering authentication over multiple systems
  - Single Sign-On
  - Session Management (potentially including Single Logoff)
- Propagation of authenticated identities
  - Federation of Identity Providers and Service Providers
  - Federated Single Sign-On, Single Logoff (including Session Management)

- Account Mapping/Linking across organizations or security domains
- Security Mediation, when IdAM functions and services are provided on behalf of another system
- Real-time access policy decisions and enforcement based on identities, attributes, roles, policy rules and environment data
- Auditing capabilities, involving the following:
  - Recording security events (e.g., identity life cycle management events, authentication and authorization events, attribute retrieval events, account mapping events, security token generation and mediation events)
  - Gathering and analyzing data about accesses to applications, data and other IT services
  - Delivering centralized reporting and security business intelligence on how identities are created, managed and used for access
- Compliance with applicable laws, regulations, policies and standards

## 2.6 Components of IdAM Solution

The following figure provides an overview of main groups of components in an IdAM solution:

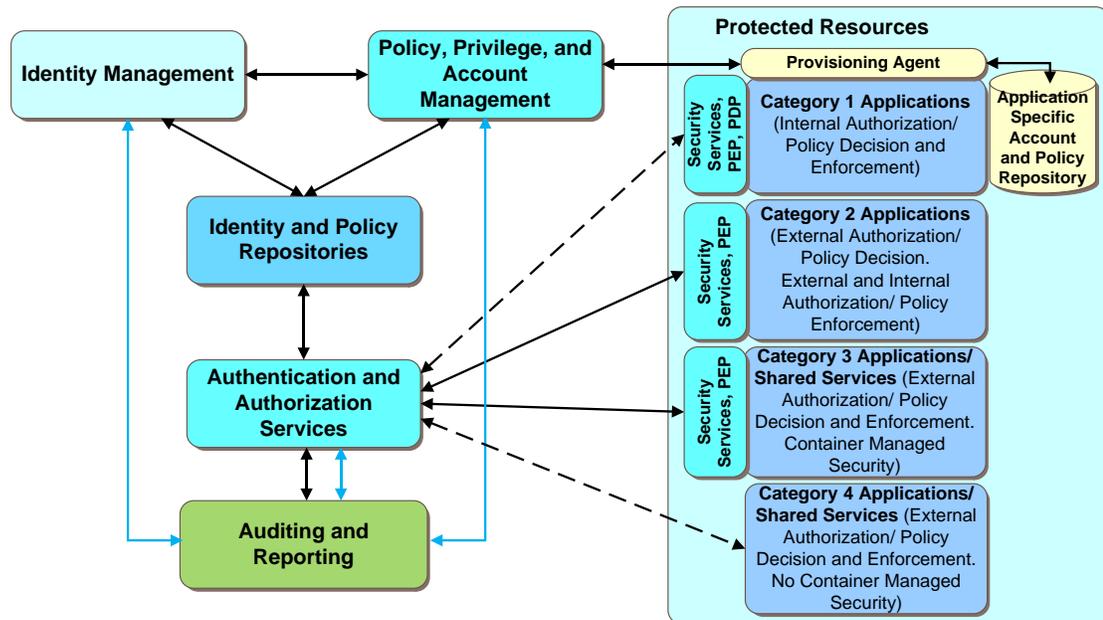


Figure 2-1 Overview of IdAM Components

The above figure shows the following components:

- **Authentication and Authorization Services** - responsible for authenticating users and enforcing policy- and attribute-based authorization and/or providing such authorization decisions for protected resources. These services also provide Single Sign-On (SSO), Federated Single Sign-On (FSSO), identity attribute retrieval, account mapping/linking, and secure token services
- **Identity and Policy Repositories** - various directories and meta-directories or virtual directories and databases used to store IdAM-related information

- **Identity Management Components** - responsible for managing the Identity Lifecycle. This lifecycle covers validating, creating, storing, maintaining and eventually disposing of identities and their attributes
- **Policy, Privilege, and Account Management Components** - responsible for managing access policies for protected resources, and user entitlements including user groups and other attributes used for policy enforcement. This also includes centralized provisioning of user accounts to preserves the security for existing applications
- **Protected Resources and IdAM Integration Components** - consist of provisioning agents which are responsible for provisioning application specific user accounts and policy enforcement/decision agents for runtime policy enforcement
- **Auditing and Reporting Components** - responsible for collecting identity and access management events, analyzing those events, and providing compliance and other identity and access management reports

The above components are described in subsections that follow.

### 2.6.1 Authentication and Authorization Services

The following diagram shows main components of Authentication and Authorization Services:

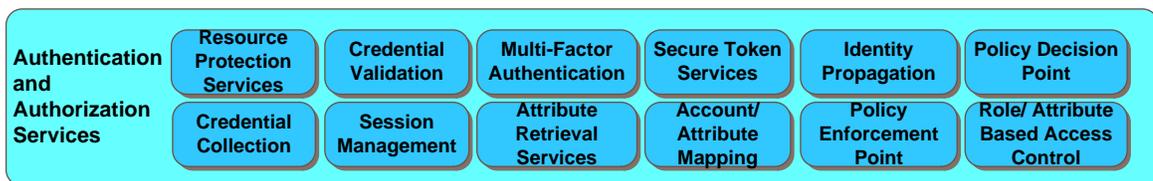


Figure 2-2 Components in Authentication and Authorization Services

Authentication Services have the following responsibilities:

- Credential Validation
- Multi-Factor Authentication (when needed)
- Supporting Single Sign-On (SSO) and Federated SSO
- Supporting Session Management and Single Signoff

Authentication Services are not self-sufficient - they make use of the following other components:

- Attribute Services
- Account/Attribute Mapping services
- Attribute Retrieval Services
- Secure Token Services

Responsibilities of Authorization Services include the following:

- Support Policy-Driven Security
- Support Role-Based Access Control
- Support Attribute-Based Access Control
- Providing Policy Enforcement Points (“PEP”) for protected resources
- Providing Policy Decision Points (“PDP”)
- Supporting Policy Repository or Repositories ( containing Policy/ Rules, Initiator Data, Target Data, and Environment Data)

## 2.6.2 Identity and Policy Repositories

Identity and Policy Repository components provide infrastructure for storing digital identities, their entitlements and other access control policies. The following diagram shows the Identity and Policy Repositories group components:

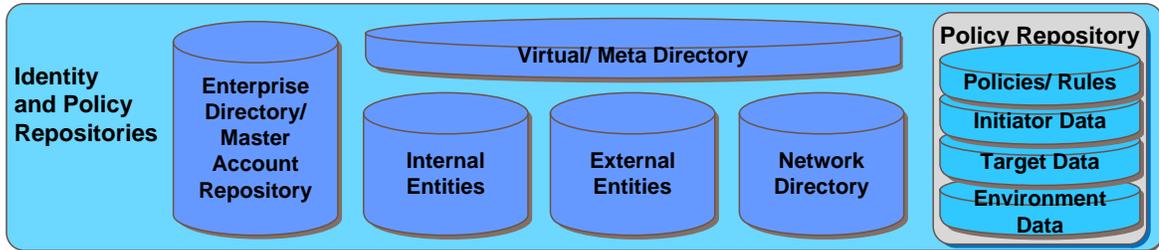


Figure 2-3 Identity and Policy Repository Components

It should be noted that the above diagram represents the Identity and Policy Repository components in a large scale enterprise IdAM environment. Not all the repositories shown in the above figure are necessary in a small-scale environment or in a more homogeneous application environment.

A brief description of the components shown in the above diagram is provided below:

- General-purpose directory services that are responsible for the following:
  - Meeting the general needs of applications and systems in the scope of security services, and - at the same time - minimizing the need for special purpose identity stores
  - Directory for *Internal Entities* (e.g., employees)
  - Directory for *External Entities* (e.g., federated identities)
- *Enterprise Directory and/or Master Account Repository*, which is typically used by the Identity Administration system to maintain a single authoritative source of digital identities and the account bound to them. This may be a relational database or an LDAP. Such a directory is not required in a small-scale environment or in a single directory environment. For example, an Active Directory may be used as an Enterprise Directory and/or Master Account Repository in such an environment
- Special-purpose directory services (such as *Network Directory* or Active Directory or mainframe RACF)
- *Meta/Virtual Directory* provides federation capabilities for disparate directory services. They provide an abstraction layer between directories and the applications that use them. Meta/Virtual Directory may not be required in a single directory environment or in an environment where applications are separated in such a way that a given application is authorized only for users digitally represented in a single directory
- Policy Repository, which stores policies and rules, and related applicable data. This includes data about the target protected resource including the protected operations, the data about the user/application that initiates a request to access a protected resource, and the data about the environment from which the request for access originates.

## 2.6.3 Identity Management Components

Identity Management components are responsible for creation and lifecycle management of Digital Identity. The following diagram shows these components:

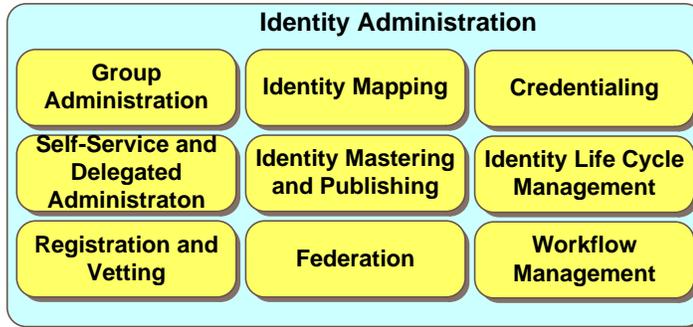


Figure 2-4 IdAM Identity Administration Components

Key Identity Management components are responsible for the following areas:

- Group Administration, capable of processing external data feeds (e.g., HR Feeds, Master Data Management Feeds)
- Self-Service (e.g., Registration, Password Resets)
- Delegated Administration
- Attribute Change, Identity Termination
- Event/Trigger Handling (such as events originating from HR systems)
- Attribute Discovery and Identity Mapping (where MDM, Identity Analytics are leveraged)

The approach to identity management reflected in the above components and their responsibilities reflects the shift from the traditional, application-centric identity management, to **user-centric** identity management, which – in contrast to the former – allows for managing identity across many applications or systems.

For discussion of Federated Identity Management (FIM) please see the section “Federated Identity Management (FIM)”.

#### 2.6.4 Policy and Privilege Management Components

The following diagram shows Policy and Management components:

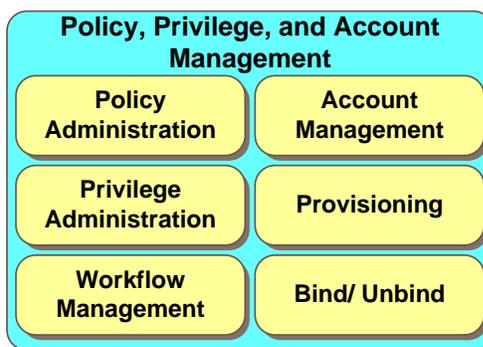


Figure 2-5 IdAM Policy and Privilege Management Components

Policy and Privilege management Components are as follows:

- Policy Administration
- Privilege Administration
- Account Management
- Bind/Unbind

- Provisioning
- Workflow Management

These components provide centralized provisioning of user accounts for existing applications:

- Existing applications may combine security services, policy enforcement and policy decision in a proprietary way
- Interoperability is best achieved by passing them the security information they need
  - J2EE applications – User Name Token
  - Mainframe Applications – RACF pass ticket
- This requires both provisioning these applications and identity mediation
- Identity mediation is preferable to be done through the EAI hub/bus

## 2.6.5 Protected Resources and IdAM Integration Components

Resources protected with enterprise IdAM are the applications and services that are designated as requiring access protection by the overall organization's security policies. For the purposes of the IdAM RA, these applications are classified into four categories as shown in Figure 2-6 below. Also shown in Figure 2-6 are the IdAM-related components necessary to integrate these applications and services with the IdAM's authentication and authorization services in order to preserve their existing security mechanisms while enhancing overall security (through externally enforced policies and authorization rules).

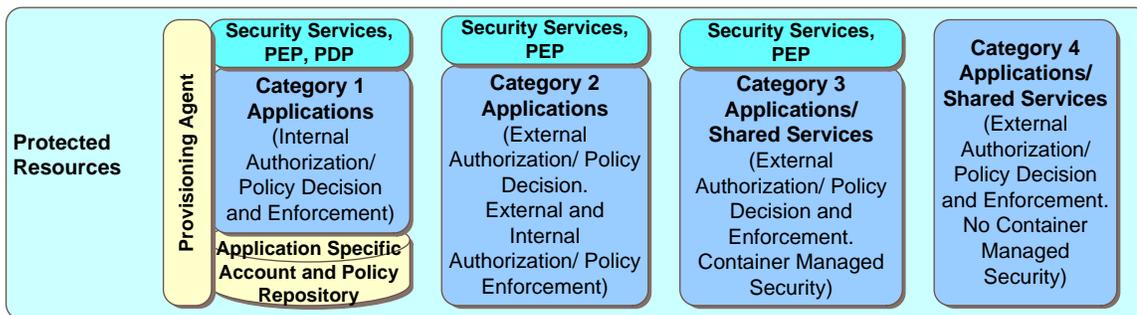


Figure 2-6 Protected Resources and IdAM Integration Components

The components shown in Figure 2-6 are briefly described below:

- *Category 1 Applications* contain internal mechanisms to determine and enforce authorization and policy rules. They contain embedded or platform-specific *Security Services*, *Policy Enforcement Point* (the *code* that actually enforces authorization rules), and *Policy Decision Point* (the *code* that determines whether access should be allowed or denied). The Security Services, PEP, and PDP may not be discrete components, but may be intermingled with the application code. These applications typically use a local application-specific or platform-specific user account and authorization rule/policy repositories. To integrate them with the enterprise IdAM system, it is necessary to provision a user account with the required attributes in the local repository. During execution time, the IdAM system provides security mediation and generates a security token accepted by the application or the platform. Therefore, a *Provisioning Agent* is typically necessary to integrate the security of this category of applications with enterprise IdAM.

- *Category 2 Applications* do not contain their own user account and authorization rule/policy repositories. They use an external repository such as an LDAP. They also typically run inside a container such as a Java EE Application Server. Coarse-grained authorization rules (e.g., based on URLs) for these applications are enforced externally by the IdAM system. Additionally, the container may enforce authorization rules (e.g., to a specific resource or to a specific operation). Fine-grained or contextual authorization rules and policies are typically enforced by the application itself. In this situation, the application and/or the container obtains authorization decisions, by communicating with the PDP through the container provided API. The PDP is external to these applications.
- *Category 3 Applications/Shared Services* also do not contain their own user account and authorization rule/policy repositories. IdAM Authentication and Authorization Services enforce externally defined authorization rules and policies. Additionally, the Security Services provided by the container of the Application/Shared Service that are safeguarding the Application/Shared Service interact with the Authentication and Authorization Services. This interaction is through the Policy Enforcement Point which interacts with the Policy Decision Point to obtain authorization and policy decisions for the application container enforced authorizations.
- *Category 4 Applications/Shared Services* do not contain their own security mechanisms. IdAM Authentication and Authorization Services enforce externally defined authorization rules and policies by intercepting all access to these protected resources

For additional information pertaining to the above components and how IdAM components interact to protect these resources, please refer to the section “High-Level Interactions”.

### 2.6.6 Auditing and Reporting Components

The following diagram shows main Auditing and Reporting components in an IdAM solution:



Figure 2-7 Auditing and Reporting Components in IdAM

Auditing and Reporting components are responsible for the following:

- Handling of all security events, including Authentication, Authorization, Federation, Token Generation, Account Mapping, Attribute Retrieval, and Policy decision events - this is performed by Security Event Handler
- Persisting the record of relevant events in the Audit Trail
- Support auditing of the Trail using a mix of mechanized and manual processes, by using Audit Analysis Rules (and potential support from a Business Rule Engine) and dedicated Audit Tools
- Allowing for creation of reports targeting specific class of events and/or specific types of issues or transgressions, using Report Templates and a Reporting Engine for creation of physical reports in desired delivery formats

## 2.6.7 Cryptography Components

The following diagram shows typical Cryptography components in an IdAM solution:

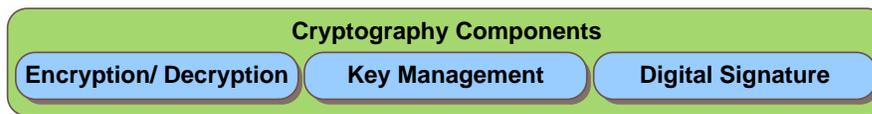


Figure 2-8 IdAM Cryptography Components

Responsibilities of IdAM cryptography components include the following:

- Encrypting clear text data and decrypting secured data using standard cryptography algorithms and techniques (e.g., asymmetric key algorithms, public key cryptography)
- Managing keys used in cryptography (encryption and decryption), which includes generating, exchanging, storing, using, and replacing the keys in a controlled manner
- Accessing and applying Digital Signatures, which are used to protect the content, to support non-repudiation and as a measure to detect data tampering

## 2.7 Federated Identity Management (FIM)

Federating separate and stand-alone Identity Management systems makes it possible for users to use the same identity and credentials, in a transparent manner, across all federation participants – be it various business units of the same organization, or multiple organizations. FIM involves building *trust relationships* between federation participants and creation of *circles of trust*, based on adoption of common standards and policies. In practice, FIM is capable of spanning multiple systems and large number of users<sup>1</sup>.

FIM offers a number of benefits:

- Economic benefits, e.g. by streamlining administration of identity in federated organizations
- Usability enhancements, e.g., by simplifying access with Single Sign-On and by offering access from multiple locations and by increasing mobility
- Strengthening security and safety, by separating processing of identity from providing a service or access to a resource, and by containing identity management to the home security domain rather than replicating it in many domains or applications
- Enhancing privacy, by sharing in the federation only the minimal information (minimal set of identity attributes)

From an IT perspective, FIM marks a shift away from the traditional focus on entities that house resources of interest to more user- and service-centric focus. This shift makes it easier to move applications and services to the cloud.

The main interest of FIM is that it allows simplifying management of identity and access across multiple applications or systems, in multiple organizations. The following subsections discuss roles, scenarios and standards relevant for implementation of FIM in enterprise.

### 2.7.1 FIM Roles and Scenarios

The following main roles appear in FIM:

<sup>1</sup> For example, InCommon Federation (<http://www.incommon.org/>) has more than 400 participating organizations (mostly research and educational institutions) and services ca. 6 million end-users.

- *Principal* (“User” or “Subject”) is the identified entity, the subject of claims about their identity
- *Identity Provider* (“IdP”) is the system providing identity of the Subject, which typically maintains identity information about the Subject
- *Service Provider* (“SP”) is the system providing the actual service or access to the target resource that consumes the information from the IdP (identity assertions) to make an authorization decision

Using the concepts of Identity Provider and Service Provider, Federation is defined as “an association comprising any number of service providers and identity providers.”

In order for the federation to function, all of its participants must agree on the same identity policies and procedures related to managing identity and passing of the identity-related attributes and assertions between the IdP and the SP.

In its practical implementation, FIM does not require replication of identity information across federation members, nor does it require unification of identity management policies. FIM solutions clearly separate establishment of identity from access control – the identity of the subject is processed by the IdP, and access control is performed in the target domain containing requested resources – by the SP.

Let us consider three illustrative scenarios for FIM:

- ***IDP-initiated Federated SSO scenario***, in which a request (e.g., usually resulting from an IDP Portal link) is redirected to a Service Provider’s portal, application, or a cloud SaaS application, as shown in the diagram below:

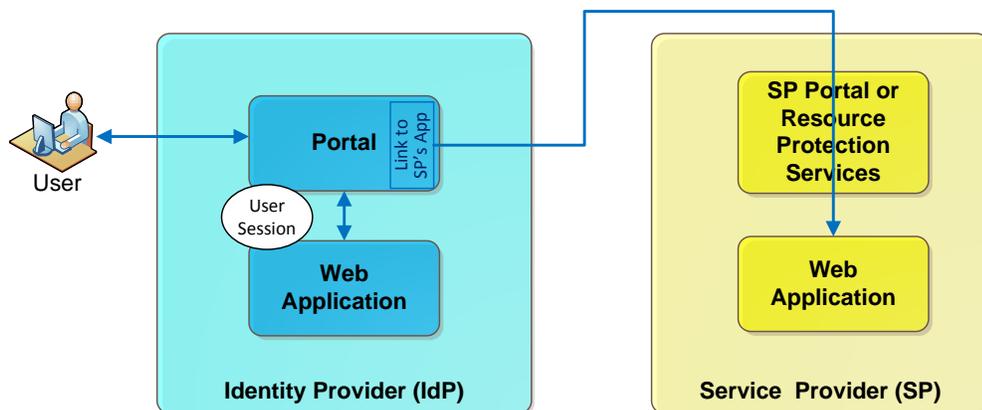


Figure 2-9 FIM Federated SSO Scenario

In this scenario, user has already authenticated at IDP and IDP has an active session for the user. The split of responsibilities between the IdP and SP and the IdAM components necessary to support this scenario are listed below.

The IDP is responsible for the following:

- Maintaining User identity and attributes
- Authenticating User

- Recognizing when User attempts to access a Service Provider's application (or other protected resource)
- Generating a standards-based Identity Token with necessary identity attributes based on trust agreement with the SP
- Creating, encrypting and signing a standards-based message to the SP based on trust agreement with the SP

To fulfill the above responsibilities, IDP's IdAM solution will need the following federation-related key components:

- Attribute Retrieval Service
- Account Mapping Component including the configuration and/or metadata to support account mapping
- Secure Token Service Component

The SP is responsible for the following:

- Maintaining local user account with minimal attributes that are needed by the SP application(s) and comply with the federation trust agreements
- Recognizing the Identity Token associated with the request
- Verifying that the Identity Token was generated by a trusted IDP by verifying message signature
- Extracting attributes from the Identity Token
- Mapping the identity provided by the IDP to a local account recognized by the target application(s)
- Extracting additional local identity attributes, if necessary
- Creating an Identity/SSO token recognized by SP application(s)
- Creating a user session
- Allowing access to the SP application based on authorization rules

To fulfill the above responsibilities, SP's IdAM solution will need the following federation-related key components:

- Attribute Retrieval Service
- Account Mapping Component including the configuration and/or metadata to support account mapping
- Secure Token Service Component

- ***SP-initiated Federated SSO scenario***, in which a request (e.g., usually resulting from User's attempt to directly access an SP Portal, application or other protected resource) is redirected to an IDP for authentication, as shown in the diagram below:

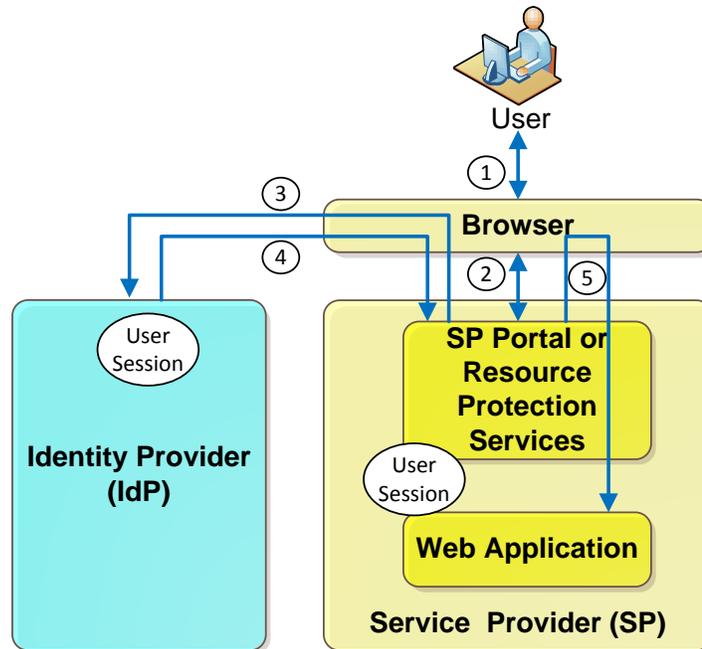


Figure 2-10 FIM Federated SSO Scenario

In this scenario, user has not yet authenticated at the IDP and the IDP does not have an active session for the user. The split of responsibilities between the IDP and SP and the IdAM components necessary to support this scenario are listed below.

The IDP is responsible for the following:

- Maintaining User identity and attributes
- Recognizing the SP-redirected request for user authentication
- Presenting a “user interface” to the user and collecting user credentials
- Authenticating user, including strong and multi-factor authentication when required and configured
- Creating a user session
- Generating a standards-based Identity Token with necessary identity attributes based on trust agreement with the SP
- Generating a re-direction back to SP’s application with an encrypted Identity Token included in the re-direct request

To fulfill the above responsibilities, IDP’s IdAM solution will need the following key components:

- Credential collection components
- Attribute Retrieval Service
- Account Mapping Component including the configuration and/or metadata to support account mapping
- Secure Token Service Component

The SP is responsible for the following:

- Maintaining local user account with minimal attributes that are needed by the SP application(s) and comply with the federation trust agreements
- Recognizing the federation user and identifying the IDP for the user

- Redirecting the user to the IDP
- Recognizing the Identity Token passed back by the IDP
- Verifying that the Identity Token was generated by the IDP
- Extracting attributes from the Identity Token
- Mapping the identity provided by the IDP to a local account recognized by the target application(s)
- Extracting additional local identity attributes, if necessary
- Creating an Identity/SSO token recognized by SP application(s)
- Creating a user session
- Allowing access to the SP application based on authorization rules

To fulfill the above responsibilities, SP's IdAM solution will need the following key components:

- Components to distinguish local and remote users
  - Redirection components
  - Attribute Retrieval Service
  - Account Mapping Component including the configuration and/or metadata to support account mapping
  - Secure Token Service Component
- **Web Services Security Management scenario**, in which either the IDP application or SP application consumes another SP's Service or a cloud service

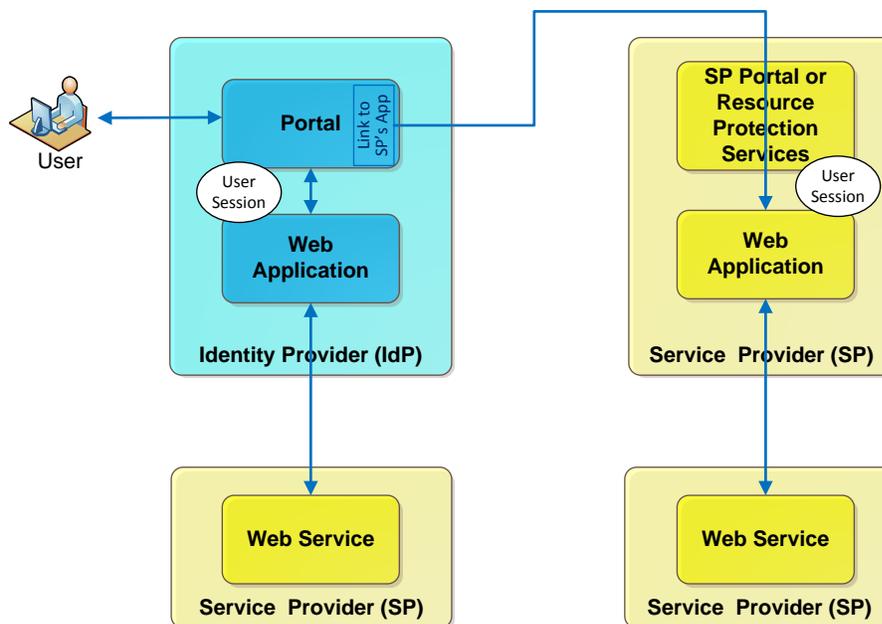


Figure 2-11 FIM Web Services Scenario

In this scenario, user has an active session at IDP and/or at SP. The invoker of the service (IDP application or SP application) has the responsibility to provide Identity Token as part of accessing the service. In this case, the invoker of the service will need the following components to support the generation and transmission of the Identity Token:

- Attribute Retrieval Service
- Account Mapping Component including the configuration and/or metadata to support account mapping
- Secure Token Service Component

## 2.7.2 Types of FIM Solutions

Federated Identity Management solutions can be classified into the following types:

- Federation Solutions
  - Transient Federation
  - Account Mapping
  - Account Linking
- System-based and User-based federation
- Federation Protocols and Standards
- Federated Single Sign-On

## 2.7.3 FIM-Related Standards

There are a number of approaches and patterns for implementing FIM solutions, and a number of applicable standards.

The standards relevant for IdAM RA include the following:

- **SAML** (Security Assertion Markup Language) - an open, XML-based standard specifying how authentication and authorization information is exchanged between parties. SAML distinguishes between the Principal, Identity Provider, and Service Provider roles. The standard has been developed and supported by OASIS (Organization for the Advancement of Structured Information Standards).
- **WS-Federation** is an open standard intended to provide, in conjunction with WS-Security, WS-Trust and WS-SecurityPolicy standards, a flexible federated identity architecture with clean separation between trust mechanisms, security token formats, and the protocol for obtaining tokens. The primary focus of the standard is Web Services. The standard is supported by a number of major vendors.
- **OpenID** is an open standard for supporting decentralized federation of IdPs to support SSO, popular in major Internet websites. The standard is supported by the OpenID Foundation (<https://openid.net/foundation/>) and is being evaluated by the State.
- **Liberty Identity Federation** (ID-FF) defines a set of protocols, bindings, and profiles that provides a solution for identity federation, cross-domain authentication, and session management. This framework can be used to create a new identity management system or to develop one in conjunction with legacy systems.

Of the above standards, SAML is the most popular and Gartner's declaration of SAML 2.0 as a *de facto* standard across industries reflects that. SAML is the currently specified standard for the State and CEAF. WS-Federation and OpenID are being evaluated for potential adoption in future.

### 3 IdAM Reference Architecture Description

This section provides a focused description of IdAM Reference Architecture (RA), using three views:

- Conceptual View, which provides a summary of logical-level building blocks for IdAM as presented in the Section 2 above
- Logical View, which provides an overview of relationships and interactions between components in an IdAM solution for specific usage scenarios
- Deployment View, which illustrates the distribution of processing and components across nodes in the system

Each of the above views is presented in the subsections that follow.

#### 3.1 IdAM RA Conceptual View

The figure below shows the IdAM Conceptual View which brings together all major components of an IdAM solution that have been already described in the section “Components of IdAM Solution”. The diagram shows subsequent horizontal layers of components involved in protecting access to resources and in establishing and managing identity, policy and privileges, etc. The vertically placed layers represent auxiliary components that can be used in a number of horizontal layers (such as e.g. cryptography components) or audit-related components, which process security events produced by a number of components.

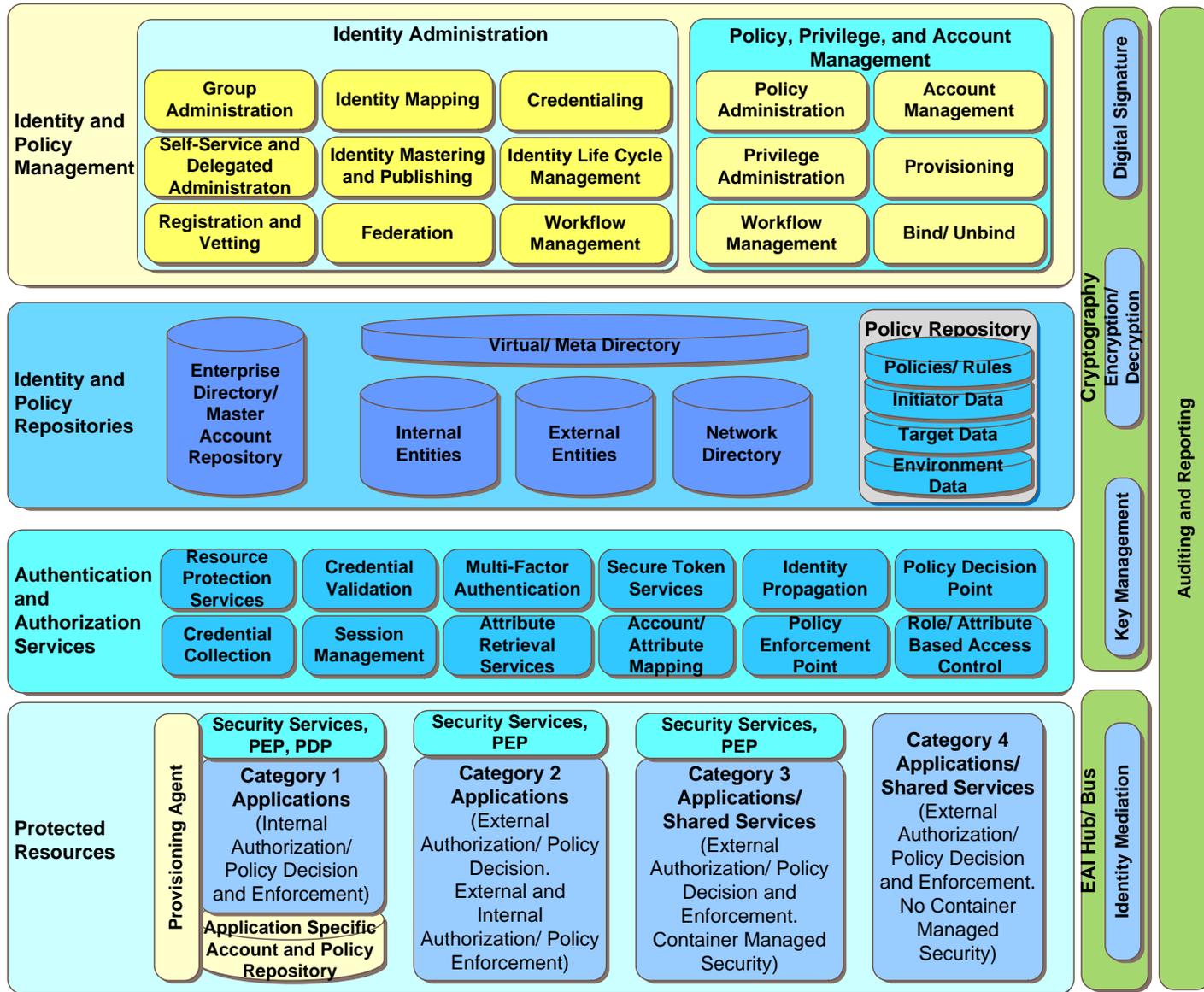


Figure 3-1 Identity and Access Management Reference Architecture – Conceptual View

### 3.2 IdAM RA Logical View

This section shows relationships and main interactions between components of IdAM. First, high-level interactions are presented. They are followed by specific IdAM scenarios to illustrate logical interactions among the various IdAM components to realize a specific scenario.

It should be noted that the interactions shown in this section are logical abstractions representing typical interactions. In practice, however, due to the physical packaging of IdAM logical components and services in the *specific system software products* selected, the component interactions (and also the names of components and services) may change. Therefore, this section is intended to enable the reader understand how IdAM components logically realize a given scenario or use case, and use that knowledge to evaluate specific technology choices to provide desired capabilities.

#### 3.2.1 High-Level Interactions

The following diagram shows high-level typical interactions among components of an IdAM solution:

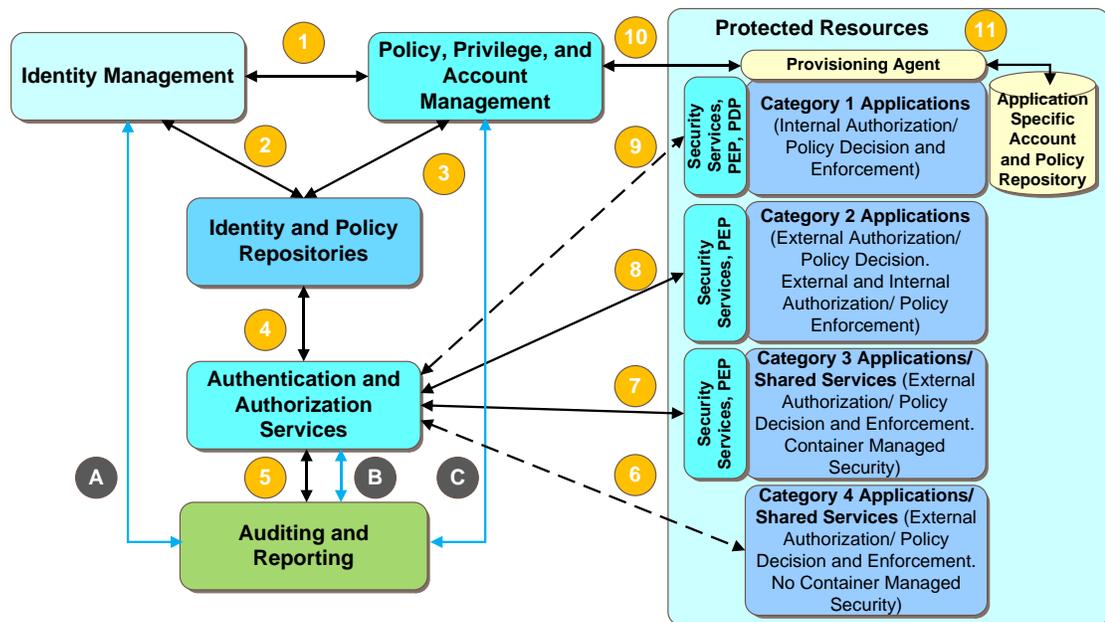


Figure 3-2 IdAM Component Interactions

In the above diagram, the conventions adopted to show relationship types are as follows:

- Continuous lines show direct interactions, whereas dashed lines indicate indirect relationship
- Black lines indicate primary IdAM interactions, while blue lines point out propagation of security events and audit data

The following table summarizes interactions portrayed in the above diagram.

Table 3-1 High-level interactions among IdAM components

Label	Description
(1)	Identity Management interacts with Policy and Privilege Management.
(2)	Interaction between Identity Management component and the Identity Repositories representing create, read, update, delete, and search operations, using repository-specific API.
(3)	Interaction between Policy and Privilege Management component and Identity and Policy Repositories representing create, read, update, delete, and search operations, using repository-specific API.
(4)	Authentication and Authorization Services access Repositories for identity information (in case of authentication and attribute- or role-based authorization) and for access policies (in case of policy-based and/or fine-grained authorization).
(5)	Authentication and Authorization Services access directly Audit components in scenarios requiring access to past data, e.g. to check repeated failed authentication attempts, or in order to directly trigger audit alarms.
(6)	Authentication and Authorization Services enforce externally defined authorization rules and policies by intercepting <i>all access</i> to the protected resource (application or shared service). The protected resource does not have a policy enforcement point as all authorization rules and policies are enforced externally by the Authentication and Authorization Services. This interaction is depicted as <i>indirect interaction</i> because there is no direct communication between the protected resource and the Authentication and Authorization Services.
(7)	Authentication and Authorization Services enforce externally defined authorization rules and policies as described in (6) above. Additionally, the Security Services provided by the container of the Application/Shared Service that are safeguarding the Application/Shared Service interact with the Authentication and Authorization Services. This interaction is through the Policy Enforcement Point which interacts with the Policy Decision Point to obtain authorization and policy decisions for the application container enforced authorizations. In this case, Subject's identity information is used to produce access decision by the PDP at the request of the PEP.
(8)	This interaction is similar to (7) described above with one difference. In addition to the externally enforced authorizations and container enforced authorizations, the protected application enforces fine-grained authorizations. To obtain these authorization decisions, the application communicates with the PDP through the container provided API.
(9)	Similar to (6), Authentication and Authorization Services enforce externally

	<p>defined authorization rules and policies by intercepting <i>all access</i> to the protected resource (application or shared service). Additionally, the protected resource enforces its own authentication and authorization rules. To do this, the protected resource uses a local Application Specific Account and Policy Repository. This category of protected applications (usually legacy or packed applications) typically pre-date enterprise IdAM solutions and standards. The only mechanism to protect them through enterprise IdAM solution while providing SSO, without modifying the application, is to provide the application <i>what it needs</i> so that its security enforcement is preserved. This is accomplished by provisioning the user account and attributes (populate the local Application Specific Account and Policy Repository) and by providing a security token that the application or its container can understand (through secure token services and account/attribute mapping services).</p>
(10)	<p>Policy and Privilege Management component accesses the local application-specific Provisioning Agent to populate Application Specific Account and Policy Repository.</p>
(11)	<p>The Provisioning Agent provides for standardized accessing of application's internal identity and policy information. The Agent is used by the Policy and Privilege Management component to populate local account and attributes.</p>
(A), (B), (C)	<p>These interactions represent the flow of security events that get recorded in the Audit Trail and subsequently analyzed for suspect activity, compliance conformance, performance data, and similar. The Audit component may raise alarms which can be consumed and processed by other IdAM components, in order e.g., to block a security violation in progress.</p>

### 3.2.2 Accessing Protected Resources

The following diagram shows components and their interactions when a user is attempting to access a resource (application or shared service) protected by enterprise IdAM. Descriptions of the interactions shown in the diagram are provided in the table below.

Identity and Access Management (IdAM) Reference Architecture (RA)

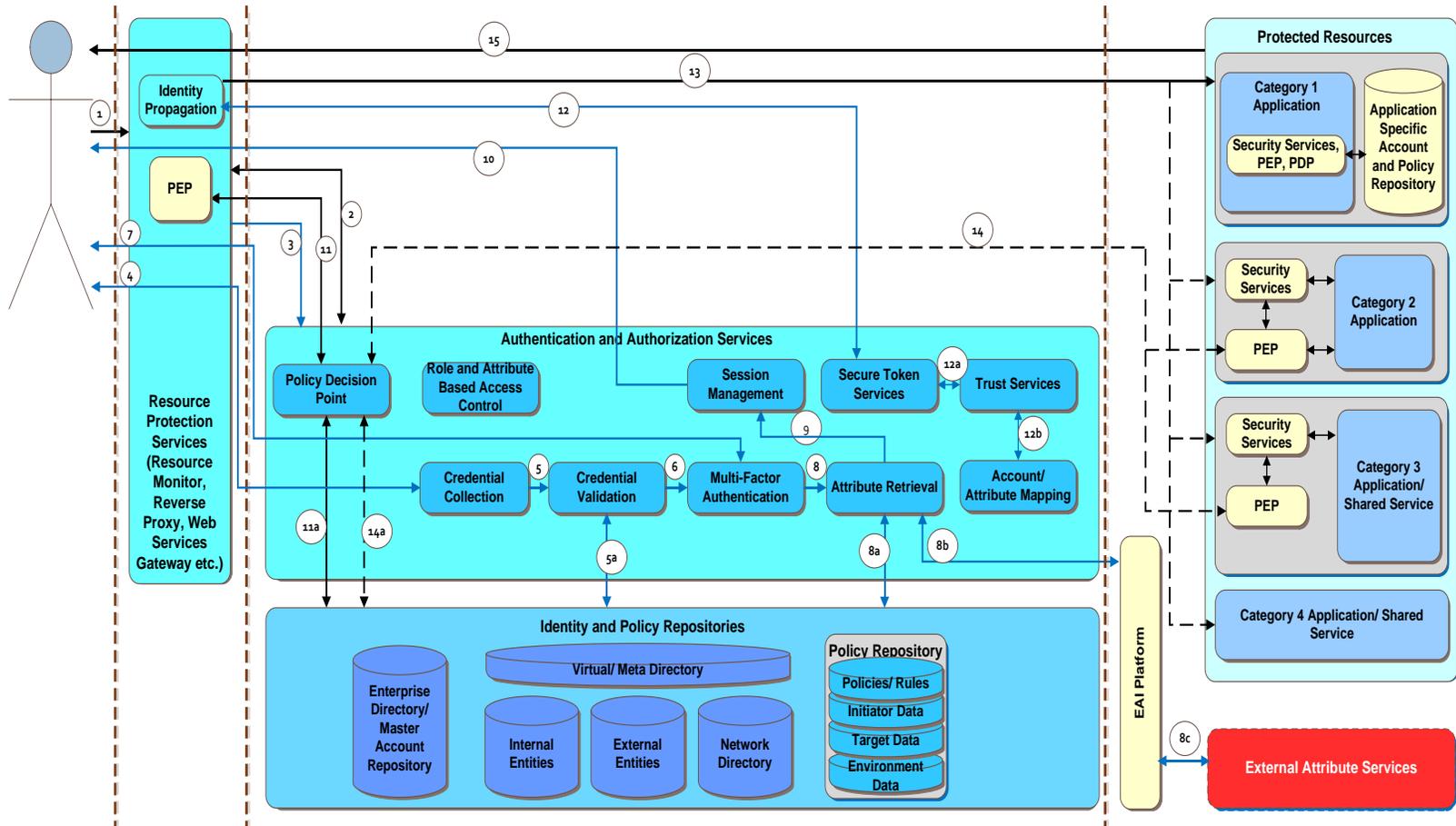


Figure 3-3 Accessing Protected Resources

Table 3-2 Accessing protected resources - IdAM component interactions

Label	Description
(1)	User attempts to access a <i>Protected Resource</i> (application or shared service).
(2)	<i>Resource Protection Services</i> component of the <i>Authentication and Authorization Services</i> intercepts the user access request and verifies if the user has already authenticated and has an active session. If the user has an active session, interaction (11) is initiated. If the user does not have an active session, then interaction (3) is initiated.
(3)	The <i>Resource Protection Services</i> invoke the <i>Authentication Services</i> to authenticate the user. <i>Authentication Services</i> determine the authentication mechanism and Identity Provider based on the target <i>Protected Resource</i> and the <i>Environment Data</i> of the user. To do this determination, <i>Authentication Services</i> may interact with the user to allow the user to select an Identity provider (this interaction is not shown in the diagram). If the user's Identity Provider is external (e.g., in case of a <i>Service Provider</i> ), the <i>Authentication Services</i> redirect the user to the external Identity Provider (this scenario is not shown in the diagram). Otherwise, the <i>Authentication Services</i> trigger the <i>Credential Collection</i> .
(4)	This <i>Credential Collection</i> component interacts with the user and collects user credentials (typically a user Id and password).
(5), (5a)	<i>Credential Validation</i> component validates the user supplied credentials with the <i>Identity Repository</i> .
(6)	<i>Multi-Factor Authentication</i> (or <i>Strong Authentication</i> ) is triggered based on the authentication mechanism determined in (3).
(7)	<i>Multi-Factor Authentication</i> interacts with the user to collect other forms of identification information. After multi-factor authentication is successfully done, <i>Attribute retrieval</i> component is triggered to retrieve additional user-related attributes depending on the target <i>Protected Resource</i> .
(8), (8a), (8b), (8c)	<i>Attribute Retrieval Services</i> retrieves additional user attributes from the <i>Identity and Policy Repositories</i> or through <i>External Attribute Services</i> (through the <i>EAI platform</i> ).
(9)	An authenticated user session is created.
(10)	User is directed to the original protected resource user was trying to access.
(11), (11a)	The <i>Resource Protection Services</i> checks user's authorization to access the protected resource. This check is performed by invoking the <i>PDP</i> through the <i>PEP</i> to determine authorization decision. <i>PDP</i> provides the authorization decision based on the defined policies.

(12), (12a), (12b)	If user is authorized, the <i>Resource Protection Services</i> determines how the authenticated user information need to be communicated to the Protected Resource (e.g., SAML token, HTTP headers, User name token, RACF pass ticket) and invokes the Secure Token Services component if necessary. The Secure Token Services component creates the requested token from the authenticated user information. During this process, the user information is mapped to account and attribute information the Protected Resource recognizes based on configured trust services/policies.
(13)	The user request is now sent to the Protected Resource.
(14), (14a)	Depending on the category of the Protected Resource, the application or the application container enforces fine-grained authorizations. To do this, the container or the application invokes the PDP through the PEP for authorization decisions. Please see Section 3.2.1 for more information.
(15)	The Protected Resource responds to the user request.

### 3.2.3 Creating and Maintaining Digital Identities, Accounts and Policies

The following diagram shows components and their interactions when a Digital Identity, Account or Policy is being created, including the provisioning of accounts and administration of privileges. It should be noted that while each of these functions can be treated as separate use cases, they are represented in one diagram to illustrate and briefly describe all related logical integrations.

Descriptions of the interactions shown in the diagram are provided in the table below.

Identity and Access Management (IdAM) Reference Architecture (RA)

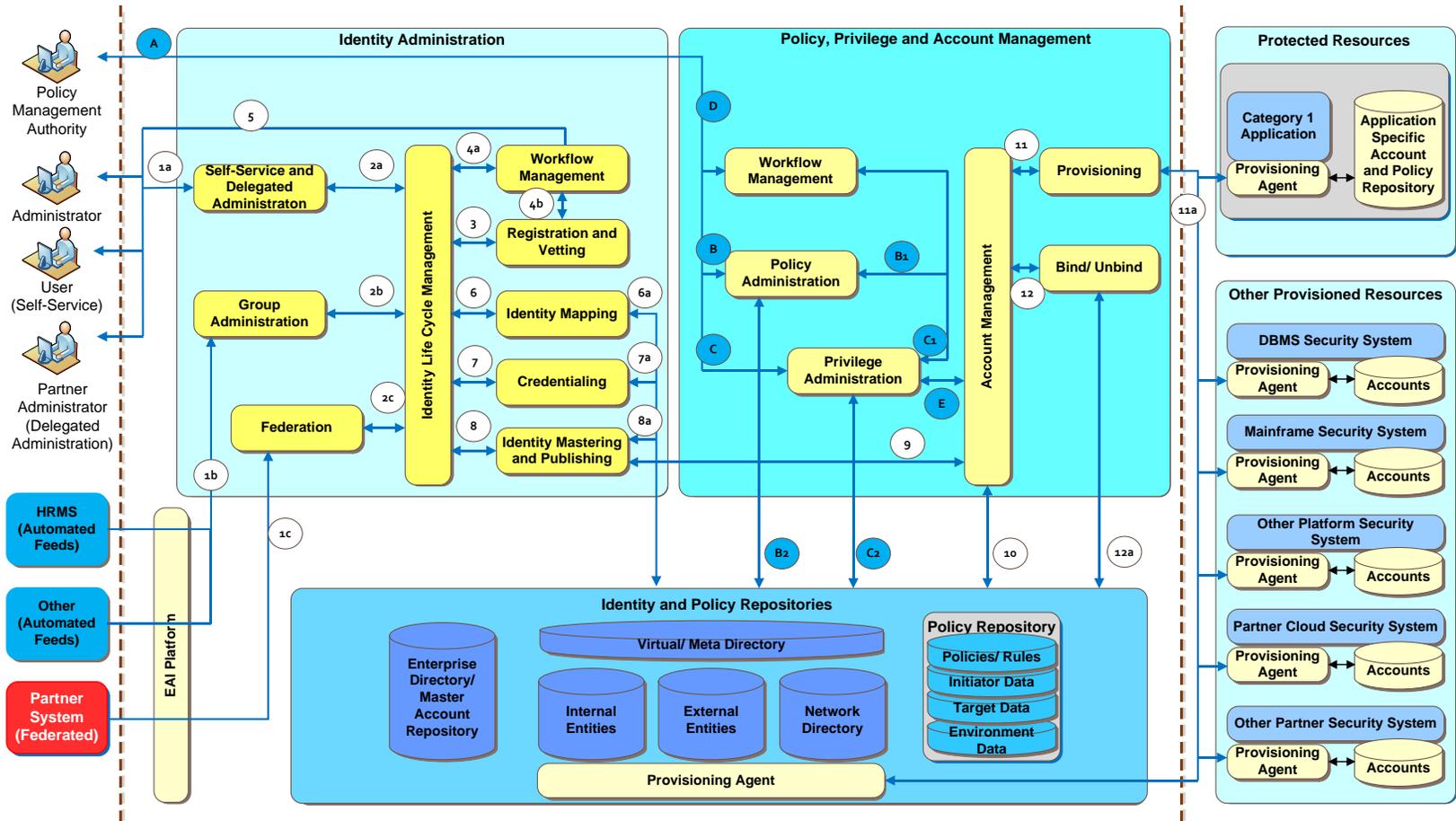


Figure 3-4 Creating and Maintaining Digital Identities, Accounts and Policies

Table 3-3 Creating and maintaining digital identities, accounts and policies - IdAM component interactions

Label	Description
(1a)	This represents user or administrator initiated request for the creation or maintenance of an identity, credentials, or a user account. It also includes delegated administrators at the partner/affiliate enterprise site. These requests are initiated through the <i>User Interface</i> provided by the Identity Administration component. It should be noted that the Identity Administration component may also be protected by the enterprise IDAM and hence the interactions described in Section 3.2.2 are applicable for accessing this application. For simplicity these interactions are omitted from Figure 3-4.
(1b)	This represents automated feeds from other systems, including the Human Resources Management System (HRMS) which is crucial to automating the creation of identities for internal users. These requests are ideally received through the EAI platform.
(1c)	Represents external requests for identity or account creation may come from the federated or non-federated partner sites. These requests are also ideally received through the EAI platform.
(2a), (2b), (2c)	Identity Life Cycle Management Services are triggered to orchestrate the identity creation and maintenance flow.
(3)	<i>Registration and Vetting Services</i> are triggered by the Identity Life Cycle Management Services to validate the request and enforce other organization policies associated with the creation and maintenance of digital identities. In some cases, such as identity requests for internal employees originated from the HRMS or Physical Access Security System, Vetting may be bypassed.
(4a), (4b)	<i>Identity Lifecycle Workflow Management</i> is triggered to orchestrate the flow of activities in the creation and maintenance of identities.
(5)	Represents human tasks (such as administrator approvals) of the Workflow Management.
(6), (6a)	Identity Mapping services will be triggered to map the information from the request to the identity and/or account information in the repositories or in federation case, to perform SAML identity mapping. During these interactions a digital identity is created.
(7), (7a)	Represents the creation and notification of credentials.
(8), (8a)	Represents the publishing of the identity or changes to attributes to the provisioned systems and other subscribing systems

(A)	This represents a request to create or maintain policies and/or privileges from an authorized administrator or the policy management authority.
(B)	<i>Policy Administration</i> component is triggered to create or maintain policies.
(C)	<i>Privilege Administration</i> component is triggered to create or maintain enterprise roles and privileges.
(B1), (C1)	<i>Policy or Privilege Management Workflow</i> is triggered to orchestrate the flow of activities in the creation and maintenance of policies and privileges.
(D)	Represents human tasks (such as administrator approvals) of the Policy or Privilege Management Workflow.
(B2), (C2)	Policy or Privilege Management components update the repositories.
(9), (E)	<i>Account Management</i> component is triggered to create or maintain user accounts, privileges and policies in the provisioned systems. This may be triggered during identity administration or policy and privilege management.
(10)	Account Management component retrieves the information about the existing accounts corresponding to the master account/identity from the repositories.
(11)	<i>Provisioning Services</i> is triggered to create user accounts for <i>Category 1 Protected Resources</i> and other <i>Provisioned Security Systems</i> . This includes database management systems, mainframe and other platform security systems, partner security systems including partner cloud security systems and other directories such as network directory.
(11a)	Provisioning Services uses <i>Provisioning Agents</i> to create and maintain user accounts for the various resource systems referred in (11). It should be noted that <i>not all</i> end systems (Provisioned Security Systems) require agents. Additionally, the communication between the Provisioning Services and Provisioning Agents may go through the EAI platform.
(12), (12a)	The Bind/Unbind component binds (or unbinds) the provisioned (or de-provisioned) user accounts to the master account/identity so that the runtime Secure Token Services and Account Mapping Services can generate valid tokens. This also allows a complete view of an identity and its associated accounts in the enterprise which facilitates improved security and auditability.

### 3.3 IdAM RA Deployment View

This subsection is to be completed in a future release. It is intended to show best-practice-based system topologies and implementation patterns of IdAM, based on existing realizations of the IdAM RA in the state.

## 4 Glossary

**Access Control** ensures that resources are only granted to those users who are entitled to them.

**Access Control List (“ACL”)** is a mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

**Access Control Service** is a security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

**Authentication** is the process of confirming the correctness of the claimed identity.

**Authorization** is the approval, permission, or empowerment for someone or something to do something.

**Digital Signature** is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

**Identity and Access Management** – See the section “Identity and Access Management Definition”.

**Identity Provider (“IdP”)** is a kind of provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.

**Federated Identity Management (“FIM”)** – see the section “Federated Identity Management (FIM)”.

**Federation** is an association comprising any number of service providers and identity providers.

**Reference Architecture** models the abstract architectural elements in the domain independent of the technologies, protocols, and products that are used to implement the domain.

**Service Component** is an actual application, program, or a subsystem providing implementation of a Service treated as a contract and performing specific responsibilities.

**Service Provider (“SP”)** – in context of IdAM, this is the home system for the requested service, application or resource. In context of FIM, SP has specific responsibilities for access control - see the section “Federated Identity Management (FIM)”.

## 5 References

### State and Federal Documents

- A. State of California, California State Information Technology Strategic Plan, 2013 Update
- B. State of California, California Enterprise Architecture Framework, Version 2.0
- C. State of California, State Identity, Credential, and Access Management (SICAM) Roadmap and Implementation Guidance, Version 2.0
- D. National Strategy For Trusted Identities in Cyberspace,  
[http://www.whitehouse.gov/sites/default/files/rss\\_viewer/NSTICstrategy\\_041511.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf)
- E. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0 -  
[http://www.idmanagement.gov/documents/FICAM\\_Roadmap\\_and\\_Implementation\\_Guidance\\_v2%200\\_20111202.pdf](http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf)
- F. Introduction to the National Information Exchange Model (NIEM) –  
[https://www.niem.gov/files/NIEM\\_Introduction.pdf](https://www.niem.gov/files/NIEM_Introduction.pdf)

### Books and Papers

- 1. Open Enterprise Security Architecture (O-ESA), The Open Group, Van Haren Publishing

### Web Sites

- a. Gartner IT Glossary, <http://www.gartner.com/it-glossary>
- b. InCommon Federated Identity Management, <http://www.incommon.org/>



## 6 Document History

*Table 6-1 Document History*

Release	Description	Date
Version 1.0 Draft	Initial creation	05/03/2013
Version 1.0 Second Draft	Revised based on internal review comments	06/21/2013
Version 1.0 Final Draft	Addressed EAC review comments	10/21/2013
Version 1.0 Final	Final version	01/02/2014