# INFORMATION SHARING ENVIRONMENT GUIDANCE (ISE-G)

# IDENTITY AND ACCESS MANAGEMENT FRAMEWORK FOR THE ISE

# VERSION 1.0

1. Authority. The National Security Act of 1947, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated 10 April 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated 16 December 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); Director of National Intelligence (DNI) memorandum dated 2 May 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law.

2. Purpose. This issuance serves as implementation guidance on the Information Sharing Environment (ISE) Identity and Access Management (IdAM) Framework under the Common Terrorism Information Sharing Standards (CTISS) program. It implements information technology capabilities in the ISE to facilitate terrorism and/or homeland security information sharing, access, and collaboration. The ISE IdAM Framework provides common definitions and requirements to guide ISE participants on leveraging and integrating existing efforts toward a common identity and access management solution for the ISE. This Framework identifies and organizes those current IdAM standards, technologies, and operational principles that ISE participants are implementing or will implement to support both discovery and access to terrorism and/or homeland security information.

3. Applicability. This ISE IdAM Framework applies to all departments or agencies that possess or use terrorism and/or homeland security information, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, consistent with Section 1016(i) of the IRTPA.

4. References. *National Strategy for Information Sharing*, October 2007; 28 Code of Federal Regulations (CFR) Part 23; *Presidential Memorandum to Executive Departments and Agencies*, 9 May 2008, (Designation and Sharing of Controlled Unclassified Information); National Information Exchange Model, *Concept of Operations*, Version 0.5, 9 January 2007; *ISE Implementation Plan*, November 2006; *ISE-AM-300: Common Terrorism Information Sharing Standards Program*, 31 October 2007; *Common Terrorism Information Sharing Standards Program Manual*, Version 1.0, October 2007; *ISE Profile and Architecture Implementation Strategy*, Version 1.0, May 2008; *ISE Enterprise Architecture Framework (EAF)*, Version 2.0, September 2008.

5. Definitions.

a. Attribute Based Authorization: A structured process that determines when a user is authorized to access information, systems, or services based on attributes of the user and of the information, system, or service.

b. Attribute Provider: An entity that provides a service for establishing and vetting access control attributes for ISE participants. This service is performed by an ISE Implementation Agent.

c. Credential Services Issuer/Provider (CSP): The entity that performs identity proofing prior to issuing a credential. The issuance of the credential and the processes of identity proofing used is documented (in a Trust Model) and submitted to the Identity Provider (IDP). The Trust Model documentation describes how these credentials are issued, protected, and managed to provide the assurance of the established E-Authentication Assurance Level (EAAL). The documentation also describes the method used to securely provide the ISE participant credentialing and any required authentication tokens. This function can be performed by the IDP.

d. ISE Core: Basic infrastructure in the ISE that will facilitate and/or support the ISE environment at large; contains the core transport components and other services that will be used to interconnect the ISE Shared Spaces of each ISE participant and allow exchange of information.

e. ISE Implementation Agent (IIA): An ISE Implementation Agent refers to an organization responsible for providing infrastructure and services in the ISE Core. In the context of this Framework, the term IIA refers to an organization responsible for providing additional infrastructure and services supporting an integrated identity and access management process in the ISE.

f. ISE Participant: Any Federal, State, local, or tribal government (SLT) organization, to include employees, that participates in the ISE (ISE Implementation Plan, November 2006).

g. Identity and Access Management: An overarching term often used to refer to the processes of authentication, authorization, assignment of attributes and privileges, access management, credential issuance, and the identification of a digital identity and the binding of that digital identity to an individual.

h. Identity Proofing: The process of validating sufficient information/evidence to uniquely identify persons as having the identity they claim.

i. Identity Provider (IDP): The entity in the ISE that provides identity proofing/vetting, credentialing, access-attributes services, and local authentication services. It may also provide the identity and access control attribute exchange service.

j. Interoperability: The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

k. Service Provider (SVP): In the context of this Framework, Service Provider refers to an entity in the ISE that provides access to its terrorism and/or homeland security information, services, and applications based on a set of attributes.

l. Service Requestor: In the context of this Framework, Service Requestor refers to the entity in the ISE that is requesting the service with a set of attributes defined by the SVP and identity assertions provided by the IDP.

6. Guidance. This ISE IdAM Framework is hereby established for implementing information technology capabilities in the ISE for IdAM services. It incorporates voluntary consensus standards[1] for information technology resources used by Federal and SLT government organizations, the private sector, and foreign partners, as appropriate.

7. Responsibilities.

a. The Program Manager, Information Sharing Environment (PM-ISE), in consultation with the Information Sharing Council (ISC), shall:

(1) Work with ISE participants, through the CTISS Committee, to publish, maintain, administer, and manage the ISE IdAM Framework and develop a new framework or modify this ISE IdAM Framework as required;

(2) Assist with the development of the ISE IdAM Framework implementation guidance, consistent with existing governance structures and, as appropriate, address privacy, policy, architecture, and legal issues;

(3) Publish this ISE IdAM Framework in coordination with the White House Office of Science and Technology Policy, the National Institute of Standards and Technology (NIST), General Service Administration (GSA), Office of Management and Budget (OMB), and the Federal Chief Information Officer (CIO) Council, as appropriate, for broader publication of this ISE IdAM Framework; and

(4) Monitor the implementation and use of this ISE IdAM Framework.

(a) Propose periodic compliance audits

(b) Provide operational guidance to ISE participants.

[1] "Voluntary Consensus Standards: Standards developed or adopted by voluntary consensus standards bodies, both domestic and international (OMB Circular A-119).

b. Each ISE participant shall:

(1) Propose ISE IdAM Framework updates to the PM-ISE;

(2) Incorporate this ISE IdAM Framework, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g., operations and maintenance {O&M} or enhancements);

(3) Incorporate this ISE IdAM Framework, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission-specific programs, systems, or initiatives (e.g., development, modernization, or enhancement {DME}); and

(4) Abide by privacy and civil liberty laws, Executive Orders, regulations, policies, and other authority, while implementing the ISE IdAM Framework.

8. Effective Date and Expiration. This ISE-G is effective immediately and will remain in effect as the Framework for ISE IdAM services until updated, superseded, or cancelled.

Thomas E McNamara

Thomas E. McNamara
Program Manager for the
Information Sharing Environment

Date: December 19, 2008

Attachment:
Part A – ISE Guidance – Identity and Access Management (IdAM)

# PART A – ISE GUIDANCE – IDENTITY AND ACCESS MANAGEMENT (IdAM)

## SECTION I – INTRODUCTION

Common IdAM practices and processes are required for the ISE to effectively share terrorism and/or homeland security information in a trusted manner. The goal of this Framework is to assist ISE participants in leveraging their IdAM activities, including but not limited to investments and technology, to facilitate common sharing. This Framework also recognizes national level activities and responsibilities currently underway to establish guidance to align IdAM efforts. As shown in Figure 1, this Framework presents a coordinated, federation concept that helps align individual and disparate ISE participant IdAM efforts. Implementation of common policies, standards, and operational principles through this Framework provide each ISE participant the capability and trust to securely access data or systems in other ISE participant networks and enclaves.

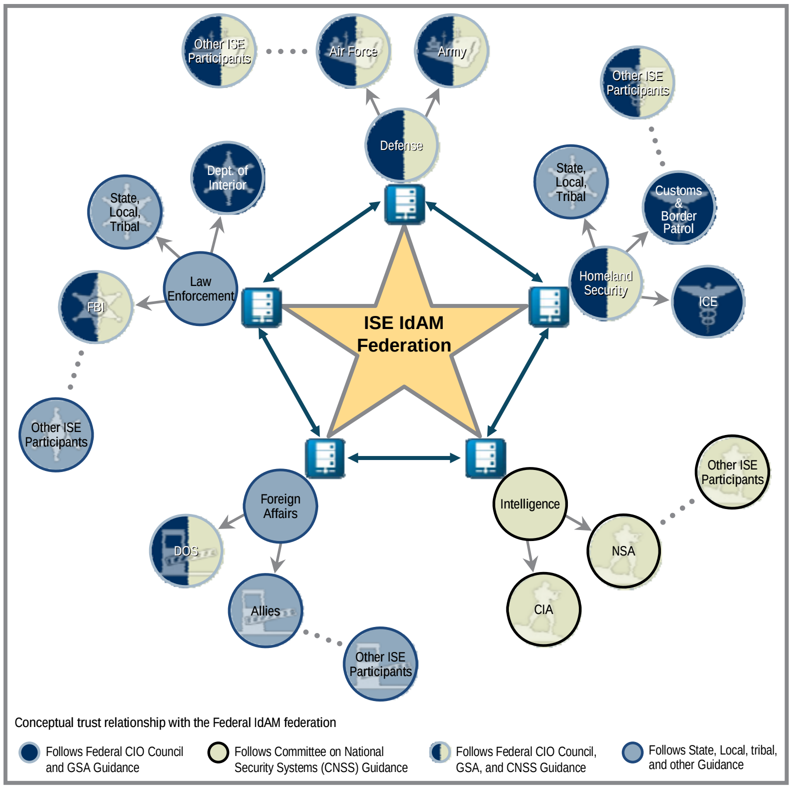
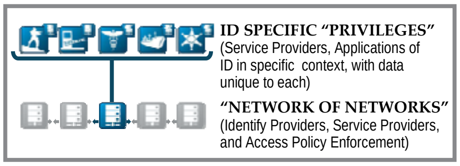


***Figure 1: The ISE IdAM Federation Concept and Challenge*** *depicts the magnitude and complexity inherent in coordinating the ISE IdAM efforts within the context of the broader Federal Government IdAM initiative, and shows alignment with the National Science and Technology Council (NSTC) vision expressed in their "Identity Management Task Force Report 2008". Users with local access credentials connect to the ISE through their local IDP. This allows them access to and request of shared terrorism and/or homeland security information from an ISE SVP in the "Network of Networks" core. When user access is requested, the identity information is supplied by the user's home-network to the SVP. The SVP passes it to the user's IDP through the core to be matched with that user's Digital ID Credential. The IDP then validates the request back to the SVP through the same core.*

*The legend below describes the connection in the figure between the community's identities and the core services.*


ID SPECIFIC "PRIVILEGES"
(Service Providers, Applications of ID in specific context, with data unique to each)
"NETWORK OF NETWORKS"
(Identify Providers, Service Providers, and Access Policy Enforcement)

## 1. Document Organization

To support the ISE, several key concepts have been agreed to by the CTISS Committee and are introduced in this document: ISE IdAM Federation Concept (Section II); ISE Implementation Agents for IdAM (Section III); IdAM Processes (Section IV); and tables of accepted ISE participant IdAM-related documentation and standards used for providing a common lexicon and coordination of ISE IdAM activities (Section V).

# SECTION II – ISE IdAM FEDERATION CONCEPT

## 1. Framework

The basis of the ISE IdAM Framework is an identity management federation concept that provides ISE participants the opportunity to contribute to the collection, development, and implementation of the policies, standards, and operational principles on which this Framework is developed. This Framework requires a commitment from each ISE participant to abide by the established technical and functional standards, policies, business rules, and agreements acknowledged, developed, and implemented for the ISE IdAM federation.

This Framework supports the coexistence of multiple federated identity schemes and promotes both Direct and Brokered Trust models (discussed in Section IV). The trust relationships between ISE participants are not universal but rather paired, with brokered trust being the basis of exchange between ISE participants that do not have an established direct trust relationship. As the number and diversity of ISE participants implementing this Framework in the chain between the Service Requestor and Service Provider (SVP) becomes larger (defined in Section III), brokered trust becomes critical to information sharing. The success of this Framework is dependent on all ISE participants working together in concert to ensure enhanced sharing of terrorism and/or homeland security information while maintaining the security of that information and the systems that process it.

This Framework defines the following required entities and functions for sharing terrorism and/or homeland security information within the ISE:

A. ISE Implementation Agents (IIA):

(1) Identity Providers (IDP) – provide ISE participants identity vetting, proofing, credentialing, access attribute services, and local authentication services.

(2) Service Providers (SVP) – provide access to services and applications that facilitate the sharing of terrorism and/or homeland security information to all ISE participants.

B. IdAM Processes:

(1) E-Authentication Assurance Level (EAAL) Certification Process – provides guidance on how an IDP or SVP is certified at an EAAL.

This Framework has a number of ISE IdAM related processes that will be developed by the ISC in conjunction with ISE participants. These processes include the following: the Brokered Identity Enforcement Process that will be used to provide guidance and polices for establishing the brokered trust relationships in the ISE; the Attribute-Based Access Policy Enforcement Process that will be used to provide guidance and policies for establishing an attribute-based access control policy for the ISE; and the Program Management Process, which through the CTISS Committee, will oversee the development and implementation of the technical, policy, and business interoperability standards, agreements, and subsequent versions of this Framework.

## 2. E-Authentication Assurance Levels used by the ISE IdAM Framework

Applying authentication and authorization EAALs for accessing terrorism and/or homeland security information in the ISE is a key concept of IdAM. Using commonly defined EAAL standards contributes to interoperability and trust within the ISE. This Framework follows the NIST Electronic Authentication Guideline[2] as the E-Authentication Assurance Level standard. All four E-Authentication Assurance Levels are shown for consistency with the NIST standard; however, the understanding is that EAAL 3 and 4 provide the highest protection that will most likely be used in the ISE.

The Controlled Unclassified Information (CUI) Framework[3] will play a significant role in defining authentication and access protection requirements for CUI terrorism and/or homeland security information, and thus the appropriate EAAL. Consistent with existing Federal policy, as CUI data protection requirements are developed by the CUI Executive Agent [the National Archives and Records Administration (NARA)] and the interagency CUI Council, they will be incorporated into this Framework. Until the CUI guidelines are established, it is possible that EAALs 1 or 2 may also be used.

For brevity, the EAAL definitions presented are taken from OMB M-04-04[4], which are consistent with the NIST standards. Each EAAL describes the IDP's degree of certainty that the ISE participant has presented evidence (credential(s) in this context) confirming claimed identity; the four EAALs to be used in the ISE are:

**Level 4 –** Very High confidence in the asserted identity's validity;

**Level 3 –** High confidence in the asserted identity's validity;

**Level 2 –** Some confidence in the asserted identity's validity; and

**Level 1 –** Little or no confidence in the asserted identity's validity.

## 3. Credential Adjudication Mechanisms

Credential adjudication mechanisms are required in the ISE in order to negotiate the various identity credentials presented by ISE participants for access to services. In turn, the SVPs present these same credentials to the adjudication mechanism for identity assurance validation. These mechanisms will be based on a Brokered Trust model that transcends the various ISE participants. Without this brokered trust, ISE-wide terrorism and/or homeland security information sharing cannot take place.

Credentialing technologies, defined by HSPD-12 and Federal Information Processing Standard (FIPS) 201-1, are among those used by ISE participants. These technologies are recommended as acceptable standards for the ISE IdAM Framework, recognizing that Federal agency ISE

[2] NIST Special Publication 800-63 V1.0.2 "Electronic Authentication Guideline" released in April 2006.

[3] The CUI Framework refers to the White House memorandum "Designation and Sharing of Controlled Unclassified Information (CUI)" located at http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html.

[4] Office of Management and Budget (OMB) "E-Authentication Guidance for Federal Agencies" is listed in Section V table 3 and can be found at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.

participants are required to follow HSPD-12 and FIPS 201-1. Other ISE participants are encouraged to follow these standards for interoperability with Federal agency ISE participants. Therefore, since all ISE participants are not required but encouraged to use the same standard, the Brokered Trust model must allow for, accept, and adjudicate the various ISE participant credentials presented for access to SVP services in order to provide identity assurance for the SVP.

## 4. Attribute-based Authorization Mechanisms

Critical to the ISE is access control – determining when a user is authorized to access information, systems, or services. Not every user, even trusted users that are properly identified and authenticated, are authorized access to everything. Attribute-based authorization allows decisions concerning access to be based on the attributes of the user and the attributes of the information, system, or service. Attribute-based[5] authorization technology will be required in the ISE. In order for shared terrorism and/or homeland security information to be accessed by the appropriate ISE participants, attributes assigned to them in conjunction with their identity credentials will facilitate the access.

As an example, a set of attributes may include:

A. Name: [First, Middle, Last]

B. Unique Identification Number: [a hash taken from this set of minimum attributes + Random Number]

C. Basic Role: [Law Enforcement, Defense, Homeland Security, Intelligence, Foreign Affairs]

An ISE participant may have more than one basic role assigned. Other required attributes will come from the guidance provided by the various ISE participant organizations defining attribute definitions, such as the IC/DoD Authorization and Attribute Services Tiger Team (AATT) and the Global Federated Identity and Privilege Management (GFIPM) working groups.

## 5. Biometrics

The National Science and Technology Council and NIST publish biometric standards. These standards are incorporated into this Framework as a basis for potentially using biometrics for assuring personnel identity and physical presence while ISE participants are accessing shared terrorism and/or homeland security information.

## 6. Governance

The ISE IdAM federation concept is a common identity management approach for the ISE and is under the Information Sharing Council (ISC) governance process as outlined in the ISE Implementation Plan. Figure 2 depicts this relationship with regards to the ISE IdAM activity.

[5] Attributes within the context of this Framework shall be developed by the various community representative organizations such as the Authorization and Attribute Services Tiger Team (AATT) in the defense and intelligence communities, and the Global Security Working Group that has developed an attribute standard with a focus on law enforcement and public safety for Global Federated Identity and Privilege Management (GFIPM).

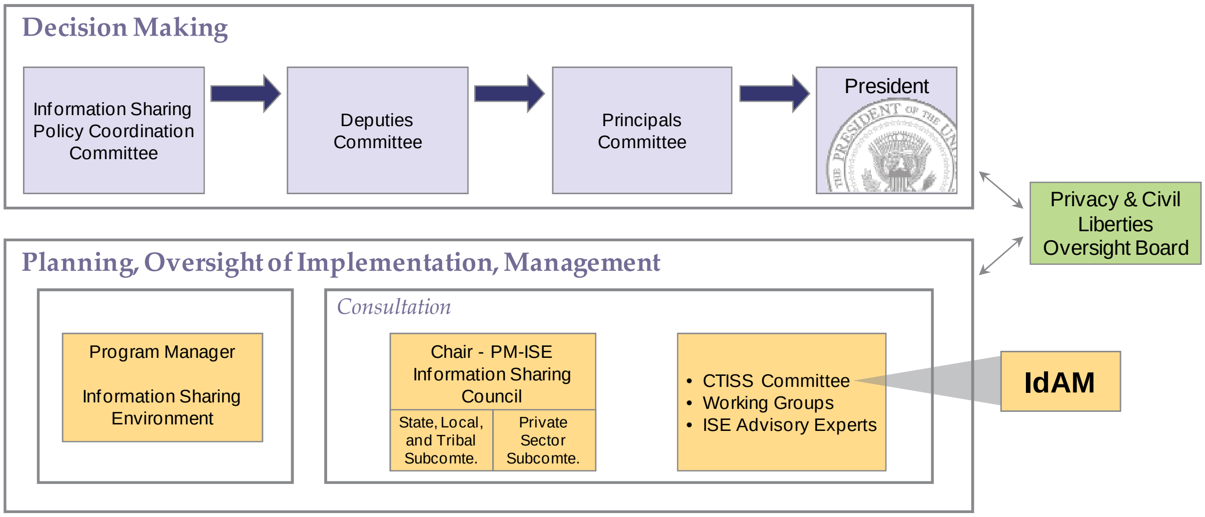

Decision Making
Information Sharing Policy Coordination Committee
Deputies Committee
Principals Committee
President
Privacy & Civil Liberties Oversight Board
Planning, Oversight of Implementation, Management
Program Manager
Information Sharing Environment
Consultation
Chair - PM-ISE Information Sharing Council
State, Local, and Tribal Subcomte.
Private Sector Subcomte.
• CTISS Committee
• Working Groups
• ISE Advisory Experts
IdAM

*Figure 2: The ISE IdAM Governance*

The ISC includes member organizations that serve on the Federal CIO Council. The Federal CIO Council is responsible for addressing the continuing critical need for improvement and coordination for a secure, well protected national cyber infrastructure as well as stringent standards for identity management across all sectors. The ISE IdAM Framework will be aligned with the Government-wide standards, policies, and processes to which Federal agencies are required to adhere when implementing identity and access management solutions. The intent is to leverage existing capabilities such as NIST FIPS 201-1[6] and the Federal Public Key Infrastructure to improve sharing within Federal and SLT agencies, the private sector, and foreign partners. Additionally, with respect to Federal agencies participating in the ISE and their interfaces to SLT partners, OMB M-04-04 "E-Authentication Guidance for Federal Agencies," will be leveraged as appropriate. Federal efforts include the E-Government sectors of Government-to-Citizen, Government-to-Business, and Government-to-Government.[7]

[6] Federal Information Processing Standards Publication (FIPS PUB) 201-1 "Personal Identity Verification (PIV) of Federal Employees and Contractors" is located at http://www.csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

[7] In the context of this Framework, Government-to-Government pertains to any Government organization required by IRTPA to share terrorism and/or homeland security information.

# SECTION III – ISE IMPLEMENTATION AGENTS FOR IdAM

## 1. Introduction

The IDP and SVP functions discussed in this Framework will be implemented through the various ISE Implementation Agents (IIAs) identified to provide these functions. A key concept is that a federation of multiple IIAs will be most effective and efficient at managing ISE participants' identities, services, and terrorism and/or homeland security information. There will be multiple ISE IDPs and SVPs with the IDP logically located close to the ISE participant. IIAs provide functionality for their own organization or as a provider to other ISE participant organizations. These functions (IDP and SVP) exist in the ISE participant organizations today and are leveraged with the application of this Framework. In order to align this Framework with ongoing Federal efforts, guidance from NIST, GSA, and other Federal efforts must be leveraged by the IIAs.

## 2. Identity Providers (IDP)

The IDP is defined as the entity that provides vetting, credentialing, access attributes, and local authentication services for federated ISE participants. Federal agency ISE participants providing IDP services are required to use the Homeland Security Presidential Directive (HSPD-12)[8] and FIPS 201-1 standards for the identity proofing and credential requirements of this service. Intelligence Community agencies and SLT governments not required to use HSPD-12 and FIPS 201-1 standards are encouraged to do so for interoperability with Federal agency ISE participants. Based on the success of the IDP process, identity and access assertions of an ISE participant's identity are provided to a SVP, which is consumed by the SVP as part of the validation of the service request. For the purpose of this Framework, the ISE IDP includes the Credential Issuer as a single entity. Although an ISE participant may have a separate IDP and Credential Provider in their organization, the ISE IdAM Framework addresses both as a single entity, labeled the IDP. Within the ISE IdAM Framework, this definition is expanded to include third party assertions acting on behalf of the requestor. This service can occur through brokered trust between the requestor's IDP and the third party's IDP. The third party IDP could then have a brokered trust relationship with the eventual SVP or another third party. The result is a sequence, or chain-of-trust, of identity and access assertions, from the origin of the service request to the SVP.

The IDP provides a certain level of identity proofing as well as a mechanism for providing secure assertions of the claimant's identity and access attributes. Within the Federal Government and stated in the NIST Electronic Authentication Guideline, the level of trust in the identity assertions provided by an IDP is defined as the EAAL.

### A. IDP Requirements

Identity establishment as well as credential and attribute management are critical to implementing a trust model capable of providing the trusted information sharing required by the ISE. Examples of implementation guidance are presented in both HSPD-12 and the NIST

[8] Homeland Security Presidential Directive/HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" is located at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

Electronic Authentication Guideline. In order to ensure integrity, compatibility, privacy, and civil liberties, IDPs shall address the following requirements:

(1) IDPs shall follow a prescribed ISE participant vetting and credentialing trust model based on the EAALs 1-4. The model ensures all credentials authenticated by these providers have been issued, protected, and managed to provide the assurance of the established EAAL for the IDP.

(2) IDPs shall develop or follow a process by which users provide the evidence, required by that IDP's EAAL, to the Credential Issuer, who independently verifies the user's identity credentials.

(3) IDPs shall develop or follow a process by which access attributes associated with users are verified.

(4) IDPs shall develop or follow a process by which they securely provide users their credential and any required authentication tokens.

(5) IDPs shall develop or follow a process to periodically re-evaluate the status of the users and the validity of their associated credentials.

(6) IDPs shall develop or follow a process for revocation checking to ensure the cancellation of credentials if a user's access is no longer authorized.

(7) IDPs shall develop or follow a process for auditing the credential issuing process, including registration activities, to ensure credentials are issued in accordance with the process specified by the Trust Model. Auditing must be conducted in a manner that identifies any irregularities or security breaches.

(8) IDPs shall provide a process to assist users who have either lost or forgotten their credential or associated tokens.

(9) IDPs, in accordance with their local organizations' information system certification and accreditation policies and procedures, shall perform information system security certification and accreditation on those portions of the ISE Core they oversee and manage. The associated documents will be required to obtain the EAAL Certification.

(10) IDPs shall follow any additional requirements as established by the Federal CIO Council, GSA, and CNSS.

## 3. Service Providers (SVP)

At the most basic level, a service is a mechanism to enable access to one or more capabilities, and an ISE SVP is an entity that provides a service. This service can be internal to an ISE participant or available to other ISE participants, based on the interface constraints and policies associated with the service description. Most often services provide data to the requestor based on a set of attributes submitted by the requestor as part of the service request.

In a Brokered Trust model of multiple ISE participants, a SVP can also refer to a second party ISE participant that acts on behalf of the first ISE participant requestor to a third ISE participant SVP. In most cases the identity assertions provided by the second ISE participant to the third ISE participant are those of the second ISE participant, rather than the identity assertions associated with the original ISE participant requestor. Any access limitations of the original requestor must be incorporated into the relationship between the second party process and the actual SVP, based on attributes[9] the original requestor has been assigned.

Within the flow among service requestors, IDPs, and SVPs, the SVP acts as a consumer of identity and attribute assertions created by the IDP and submitted as part of the service request by the service requestor. In the ISE IdAM Framework environment, it cannot be guaranteed that the requestor or intermediary parties will be certified at the same or higher level as required by the SVP. Therefore, the SVP must establish a requestor EAAL policy that specifies the SVP's reaction to a request in which the requestor or intermediary proxies have an EAAL less than that required by the SVP.

## A. SVP Requirements

These SVP requirements are established in order to implement a trust model capable of providing the trusted information sharing required by the ISE. In order to ensure integrity, compatibility, privacy, and civil liberties, SVPs shall address the following requirements:

(1) SVPs shall have the capability to validate identity assertions that are submitted as part of a service request.

(2) SVPs shall have the capability to define a requestor EAAL policy.

(3) A SVP's requestor EAAL policy shall define the services available to a requestor based on the requestor and intermediate proxy EAALs.

(4) SVPs shall have the capability to limit service support based on the attribute assertions provided by the IDP of the original requestor, and they may accept brokered trust third party access assertions.

(5) SVPs shall have the capability to react to receipt of requestor assertions of various EAALs based on the established policy.

(6) SVPs acting as proxies shall have the capability to validate identity assertions that are submitted as part of the service request.

(7) SVPs acting as a third party shall have the ability to associate their own identity assertions in a service request that is being transmitted to a subsequent SVP.

[9] Attributes within the context of this Framework shall be developed by the various community representative organizations such as the Authorization and Attribute Services Tiger Team (AATT) in the defense and intelligence communities, and the Global Security Working Group that has developed an attribute standard with a focus on law enforcement and public safety for Global Federated Identity and Privilege Management (GFIPM).

(8) SVPs, in accordance with their local organizations' information system certification and accreditation policies and procedures, shall perform information system security certification and accreditation on those portions of the ISE Core they oversee and manage. The associated documents will be required to obtain the EAAL Certification.

(9) SVPs shall have the capability to limit service support based on the attribute assertions provided by the Attribute Provider holding access attributes of the original requestor, and they may accept brokered trust third party access assertions.

(10) SVPs shall have the capability to limit service support based on the attribute assertions provided by the Attribute Provider holding access attributes of the requested resource and/or application, and they may accept brokered trust third party access assertions.

(11) SVPs shall protect the shared terrorism and/or homeland security information as required by laws/regulations/rules.

## SECTION IV – IdAM PROCESSES

### 1. Introduction of Relationships and Models

The processes discussed in this Framework are implemented through the various IIAs identified to perform these processes. IIAs will perform these processes for their own organization and/or as a provider to other ISE participant organizations.

This Framework supports and facilitates both Direct and Brokered Trust relationship models between IDPs and SVPs. Section V lists a set of defined technical standards, including attribute metadata standards, that facilitate interoperability of both identity and access information between ISE participants for both models. Furthermore, this Framework will support attribute translation and third-party trust brokering (Brokered Trust Model) services between ISE participants. For the remainder of this section, ISE participant “A,” “B,” or “C” will be referred to as “A,” “B,” or “C.” Figure 3 depicts one of the more common direct trust requests between a Service Requestor and a SVP.

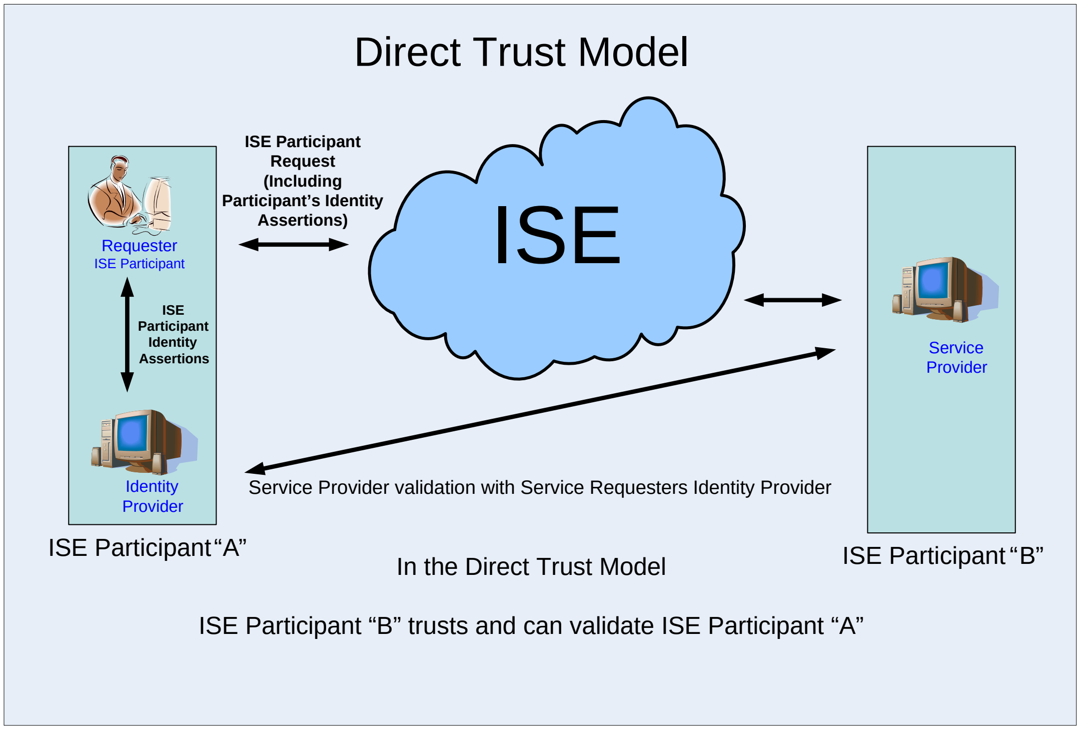

Direct Trust Model
ISE Participant Request (Including Participant’s Identity Assertions)
ISE
Requester
ISE Participant
ISE Participant Identity Assertions
Identity Provider
Service Provider
Service Provider validation with Service Requesters Identity Provider
ISE Participant“A”
In the Direct Trust Model
ISE Participant“B”
ISE Participant “B” trusts and can validate ISE Participant “A”

*Figure 3: Represents a Direct Trust Model between ISE participants*

In the Brokered Trust Model, the trust relationships between ISE participants are not universal but rather paired, with brokered trust being the basis of exchange between ISE participants that do not have a trust relationship. Figure 4 depicts one of the more common brokered trust request chains between an original requestor and a SVP.

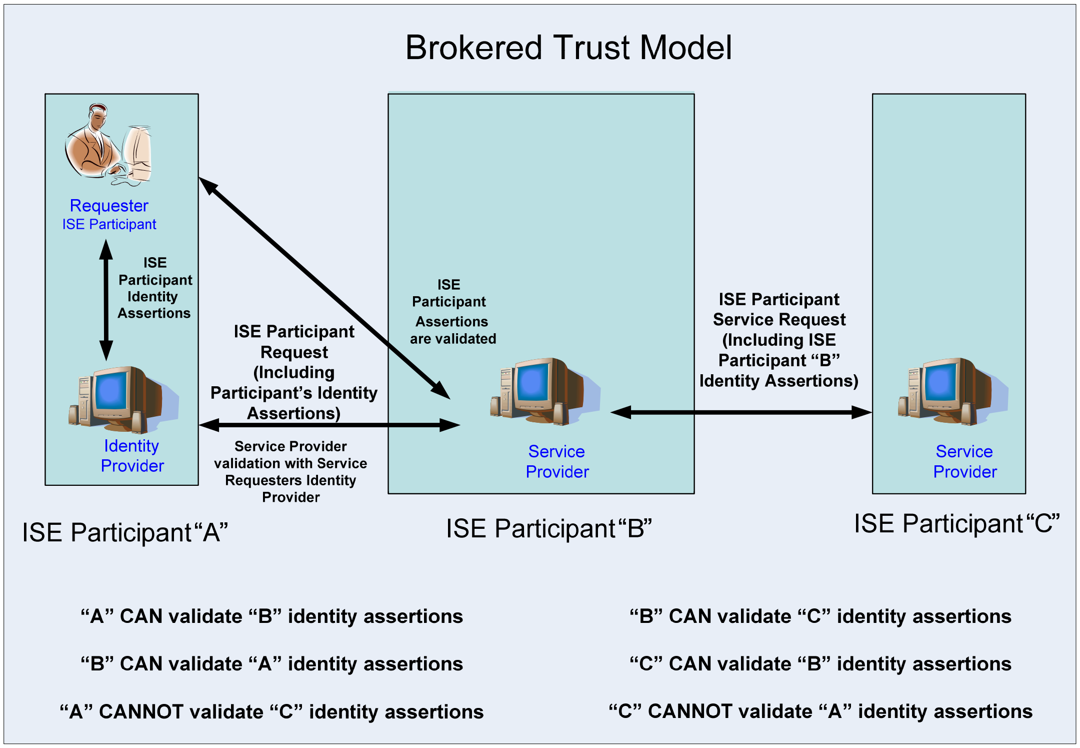

Brokered Trust Model
Requester
ISE Participant
ISE Participant Identity Assertions
Identity Provider
ISE Participant Request (Including Participant's Identity Assertions)
Service Provider validation with Service Requesters Identity Provider
ISE Participant Assertions are validated
Service Provider
ISE Participant Service Request (Including ISE Participant "B" Identity Assertions)
Service Provider
ISE Participant "A"
ISE Participant "B"
ISE Participant "C"
"A" CAN validate "B" identity assertions
"B" CAN validate "A" identity assertions
"A" CANNOT validate "C" identity assertions
"B" CAN validate "C" identity assertions
"C" CAN validate "B" identity assertions
"C" CANNOT validate "A" identity assertions

***Figure 4: Represents a Brokered Trust Model between ISE participants***

The example in Figure 4 would be a situation in which “A” has a trust relationship with “B,” but not with “C.” “B” has a trust relationship with both “A” and “C.” “C” has a trust relationship with “B,” but not with “A.” In most cases this lack of a trust relationship is based on the following facts:

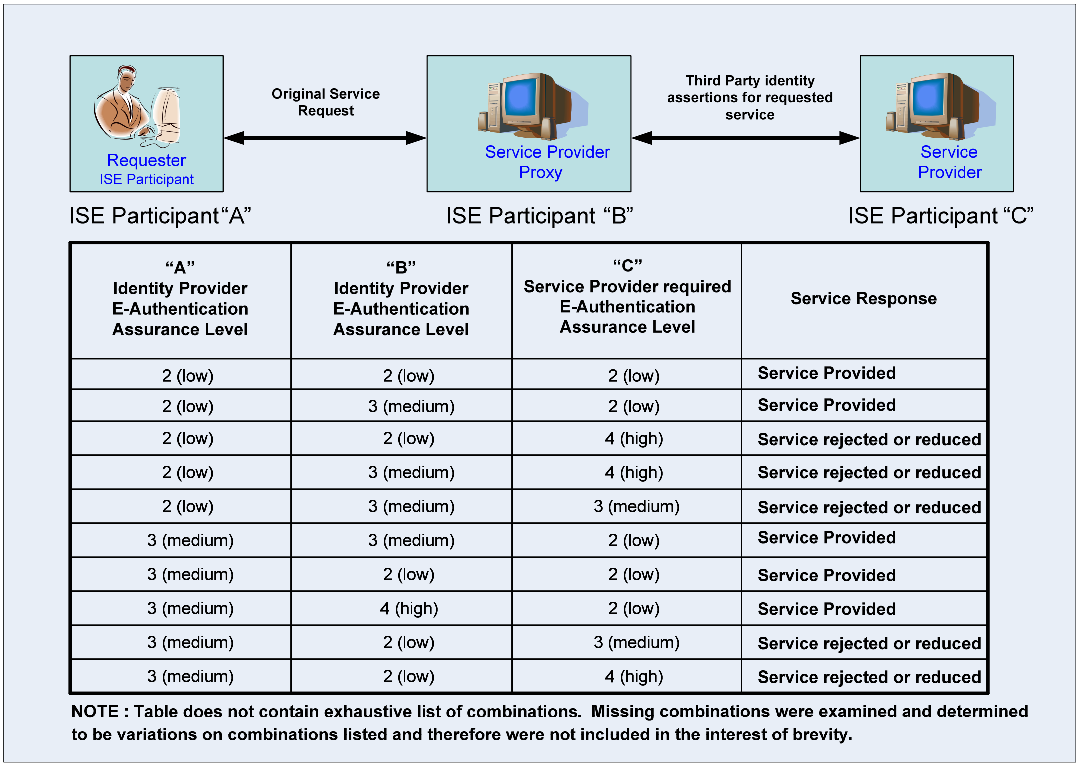
- “A” SVPs can securely validate[10] identity assertions provided by “B” IDPs but not those provided by “C” IDPs;
- “B” SVPs can securely validate identity assertions provided by both “A” and “C” IDPs; and
- “C” SVPs can securely validate identity assertions provided by “B” IDPs but not those provided by “A” IDPs.

If a requestor in “A” needs to make a request of service in “C,” the “C” SVP must receive securely validated evidence that the service request originated from an authorized requestor through a brokered trust mechanism and/or an attribute based policy service.[11] Therefore, some form of brokered trust must be established to secure the process chain between the originator of a

[10] Validate identity assertions through the Brokered Trust Model discussed in Section II-3 “Credential Adjudication Mechanisms”.
[11] This may be provided by the IDP or SVP.

service request and the SVP of the requested service. While this concept can be applied to direct trust between IDPs for a single ISE participant, it is more commonly used to refer to passing trust to one ISE participant acting on behalf of a request from another ISE participant based on credentials from a third ISE participant. For example, a user in “A” makes a request to “B,” where the “B” SVP acts as a third party intermediary for the “A” service request. What this means is that “B” authenticates the user’s identity via the identity assertions provided by “A” and then provides the identity validation for the service request to the “C” SVP. However, instead of passing the “A” requestor’s identity assertions to “C,” the “B” third party service presents its own identity assertions provided by the “B” IDP to the “C” SVP. The “C” SVP can authenticate the “B” provided identity assertions and, through brokered trust, accepts that “B” has validated the originator of the request via the “A” IDP.

Within the ISE IdAM Framework, brokered trust becomes critical to information sharing as the chain of ISE participants between requestor and SVP becomes longer because of the dramatically increased number of ISE participants that are involved in the Framework. With the wide diversity of ISE participants involved, a variety of identity proofing standards, processes, and methods are used to secure identity assertions. As a result, a request can originate with one ISE participant and transition multiple ISE participants before reaching the SVP. Each of the ISE participants involved in the request-to-service chain may have differing EAALs, which lead to the issue of handling situations in which the EAAL of the third party provider is less than or more than the level of the requestor’s originating identity service or that of the SVP. Figure 5 describes the set of possible conditions and the expected response of the requested service under each of these conditions.



| “A”<br>Identity Provider<br>E-Authentication<br>Assurance Level | “B”<br>Identity Provider<br>E-Authentication<br>Assurance Level | “C”<br>Service Provider required<br>E-Authentication<br>Assurance Level | Service Response |
|---|---|---|---|
| 2 (low) | 2 (low) | 2 (low) | Service Provided |
| 2 (low) | 3 (medium) | 2 (low) | Service Provided |
| 2 (low) | 2 (low) | 4 (high) | Service rejected or reduced |
| 2 (low) | 3 (medium) | 4 (high) | Service rejected or reduced |
| 2 (low) | 3 (medium) | 3 (medium) | Service rejected or reduced |
| 3 (medium) | 3 (medium) | 2 (low) | Service Provided |
| 3 (medium) | 2 (low) | 2 (low) | Service Provided |
| 3 (medium) | 4 (high) | 2 (low) | Service Provided |
| 3 (medium) | 2 (low) | 3 (medium) | Service rejected or reduced |
| 3 (medium) | 2 (low) | 4 (high) | Service rejected or reduced |

NOTE : Table does not contain exhaustive list of combinations. Missing combinations were examined and determined to be variations on combinations listed and therefore were not included in the interest of brevity.

*Figure 5: Combinations of E-Authentication Assurance Levels*

## 2. E-Authentication Assurance Level Certification Process

Establishing the E-Authentication Assurance Level (EAAL) of the IDPs and SVPs of the ISE are the two primary purposes for the ISE EAAL Certification process. This process shall be established for adding new IDP and/or SVP networks to the ISE. NIST has established standards defining the E-Authentication Assurance Levels to which IDPs can be assigned. Section II, sub-section 2 of this Framework describes how the EAALs assigned to both the requestor's IDP as well as the EAAL required by the SVP will affect the ability of a requestor to successfully request a service.

To ensure that the EAAL that is assigned to either an IDP or associated as a requirement for a SVP is appropriate, the EAAL Certification shall be performed by a third party certification agent.[12]

IDP EAALs – The ISE EAAL Certification Process for IDPs identifies the steps that are performed to validate the EAAL established by an IDP based on the EAAL descriptions found in NIST Electronic Authentication Guidance, OMB M-04-04 and OMB M05-24.

SVP EAALs – The ISE EAAL Certification Process for SVPs identifies the steps that are performed to validate the EAAL established by a SVP. The categorization of the SVP's EAAL is based on the level descriptions in NIST Electronic Authentication Guidance and the established CUI terrorism and/or homeland security information protection guidelines for ISE shared terrorism and/or homeland security information. For the situation in which a SVP's information is at a higher level than that of the requestor, the SVP has the option to reduce the required EAAL for access to that information, and/or the IDP's EAAL certification can be raised after a re-certification process to a higher EAAL is successfully completed.

### A. E-Authentication Assurance Level Certification Requirements

These requirements are established in order to implement a common trust model capable of providing the trusted information sharing required by the ISE. These certification requirements refer to the application of the EAAL certification process to IDPs and SVPs interfacing with the ISE. In order to ensure integrity, compatibility, privacy, and civil liberties, IIAs implementing the EAAL Certification Processes shall address the following requirements.

(1) All ISE participants being added to the ISE Core shall have their IDP or SVP certified to the EAAL at which it operates.

(2) All ISE participants connected to the ISE Core shall have their IDP's or SVP's EAAL re-certified either on an established periodic rate or on a continual basis based on changes to the ISE environment in which the IDP or SVP resides. The recertification periods will be based on guidance provided by ISE-identified standards bodies.

[12] The Certification Agent refers to an ISE Implementation Agent performing the EAAL Certification process for all other organizations except their own. Each organization must be certified by a third party in keeping with the security principle of separation of duties, consistent with statutory and other policy guidelines. Self certification is not acceptable.

(3) An ISE participant connected to the ISE Core shall have its IDP or SVP re-certified whenever the security support structure of the IDP or SVP for that ISE participant is changed.

(4) The ISE Core shall provide protective measures to control access by requests from ISE participants with IDPs or SVPs with an EAAL less than that of the ISE Core.

(5) The ISE Core shall provide information to SVPs regarding the lowest EAAL in the path of a service request from the original requestor to the SVP.

(6) All SVPs shall provide the ISE Core with instructions for handling requests with a lowest path EAAL below the requirements of the SVP.

(7) ISE participants, IDPs, SVPs, and IIAs shall follow any additional requirements as established by the Federal CIO Council, GSA, and the Committee on National Security Systems (CNSS).

## SECTION V – IDENTITY AND ACCESS MANAGEMENT-RELATED DOCUMENTATION AND STANDARDS

The following tables constitute voluntary consensus IdAM Policy and Procedural Reference Documents and Directives, Standards, and Related Guidance Publications leveraged in this Framework. These policies, standards, and guidance documents are to be used or referenced by IIAs in planning, implementing, and providing IdAM services to the ISE. ISE participants shall also ensure alignment with existing information technology standards for interfacing their ISE Shared Space[13] to the ISE Core. The foregoing make up the majority of allowed policies, standards, and guidance, but leave room to add existing, create new, and/or edit/combine standards for the purposes of ISE IdAM. As the listed IdAM polices, standards, or guidance documents are updated by the owning organization or standards body, the updated versions will supersede the versions listed in this Framework.

Table 1 provides ISE participants' policy and procedural reference documents and directives for their IdAM activities performed within the ISE. The document, responsible organization, and a brief description of the documents are listed for each.

***Table 1 – IdAM Policy and Procedural Reference Documents and Directives***

| Reference Document | Responsible Organization | Document Description |
|---|---|---|
| Defense Biometrics | Defense Science Board | Defense Science Board, "Report of the Defense Science Board Task Force on Defense Biometrics," March 2007 |
| Department of Defense and Intelligence Community Unified Authorization and Attribute Service; Authorization Attribute Set, Version 1.0, 1 November 2008 | OSD/NII<br>DoD/CIO | Defines a set of subject attributes used to support Attribute Based Access Control decisions across the DoD and IC<br>https://www.intelink.gov/wiki/Attribute_Interface#Attribute_Information |
| GFIPM Interface Control Document | DOJ's Global Justice Information Sharing Initiative | This document defines the normative technical requirements to achieve interoperability with GFIPM in a browser to Web server environment.<br>See section 3 for document references and URLs for other applicable base standards, such as SAML |
| HSPD 12 credentialing | GSA | GSA-General Services Administration: Federal Identity Credentialing Office of Government-wide Policy, "HSPD-12: The Role of Federal PKI" |
| HSPD-24/NSPD-59 | White House | Biometrics for Identification and Screening to Enhance National Security |
| NSTC Subcommittee on Biometrics and Identity Management (IdM) Task Force Report | National Science and Technology Council (NSTC) | NSTC, "Subcommittee on Biometrics and IdM Task Force Report" |
| SP 800-73 Interfaces for Personal Identity Verification | NIST | NIST Special Publication 800-73, March 2006 – specifies interface requirements for retrieving and using identity credentials from the PIV Card and is a companion document to FIPS 201-1 |

[13] The *ISE Enterprise Architecture Framework, Version 2.0*, describes "ISE Shared Spaces" as networked data and information repositories used to make standardized terrorism-related information through the Common Terrorism Information Sharing Standards (CTISS), applications and services accessible to other ISE Participants.

| Reference Document | Responsible Organization | Document Description |
|---|---|---|
| Office of Management and Budget (OMB) Memorandum 04-04 | OMB | OMB-Executive Office of the President: Memorandum to the Heads of all Departments and Agencies: "E-Authentication Guidance for Federal Agencies," 16 December 2003 |
| Global Justice Reference Architecture | DOJ's Global Justice Information Sharing Initiative | The Global Justice Reference Architecture (JRA) Specification version 1.6 and Web Services Interaction Profile version 1.1, available at http://www.it.ojp.gov/topic.jsp?topic_id=242 |
| National Information Exchange Model (NIEM) 2.0 | DHS, DOJ, interagency participants | "National Information Exchange Model (NIEM) 2.0" http://www.niem.gov/niem-2/niem/index.html |
| OMB Memorandum 05-24 | OMB | OMB-Executive Office of the President: Memorandum to the Heads of all Departments and Agencies: "Implementation of Homeland Security Presidential Directive (HSPD) 12 – "Policy for a Common Identification Standard for Federal Employees and Contractors" 5 August 2005 |
| OMB Memorandum 06-16 | OMB | OMB-Executive Office of the President: Memorandum to the Heads of all Departments and Agencies: "Protection of Sensitive Agency Information," 23 June 2006 |
| OMB M-07-16 | OMB | Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 2007 |

Table 2 provides standards (Standard) and policies to be used within the ISE, the implementing authoritative organization (Standards Body or Responsible Organization), and a brief description of the standard, the version and date of the latest release of the standard (Standards Description/Version/Date).

***Table 2 – IdAM Related Standards***

| Standard | Standards Body or Responsible Organization | Related Standards Description / Version / Date |
|---|---|---|
| E-Authentication Federation Operational Standards | General Services Administration (GSA) | GSA, "E-Authentication Federation Operational Standards" Version 1.0.0, 26 December 2006 |
| Global Federal Identity and Privilege Management (GFIPM) | Department of Justice's (DOJ) Global Justice Information Sharing Initiative | GFIPM Delivery Team, "Information Sharing Environment (PM-ISE) Inter-Federation Pilot Project: Global Federated Identity and Privilege Management (GFIPM)" White Paper, 15 April 2008 |
| GFIPM Metadata 1.0 Federation Standard | DOJ's Global Justice Information Sharing Initiative | "Global Federated Identity and Privilege Management (GFIPM) Metadata 1.0" GFIPM Federation Standard, 15 February 2008 http://it.ojp.gov/topic.jsp?topic_id=248 |
| GFIPM Metadata 1.0 Encoding Rules for Transport VIA Security Assertions Markup Language (SAML) 2.0 | DOJ's Global Justice Information Sharing Initiative | "Global Federated Identity and Privilege Management (GFIPM) Metadata 1.0 Encoding Rules for Transport via SAML 2.0" GFIPM Federation Standard, 15 February 2008 http://gfipm.net/standards/SAML%202.0%20Encoding%20Rules.pdf |
| ITU-T Recommendation X.1250 | International Telecommunications Union | "Requirements for Global Identity Management trust and interoperability" |

| Standard | Standards Body or Responsible Organization | Related Standards Description / Version / Date |
|---|---|---|
| PKIKMITKNPP | NIST – National Institute of Standards and Technology (NIST) | Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP |
| PP_FWPP-MR | National Security Agency (NSA) | U.S. Government Firewall Protection Profile for Medium Robustness Environments |
| SLOSPP | NSA | Protection Profile for Single-level Operating Systems in Environments Requiring Medium Robustness |
| Web Services Security | Organization for the Advancement of Structured Information Standards (OASIS) | Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). OASIS Standard Specification, 1 February 2006. Available at http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf |
| Web Services Security SAML Token Profile 1.1 | OASIS | Web Services Security: SAML Token Profile 1.1. OASIS Standard Specification, 1 February 2006. Available at http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SAMLTokenProfile.pdf |

Table 3 provides ISE participants a list of related guidance publications on IdAM activities performed within the ISE. The publication, responsible organization, and a brief description and the version and date of latest release of the publication are listed for each.

***Table 3 – IdAM Related Guidance Publications***

| Publication | Responsible Organization | Publication Description / Version / Date |
|---|---|---|
| SP 800-63 Electronic Authentication Guideline | NIST | NIST Special Publication 800-63 Version 1.0.2, April 2006 – provides recommended guidance for Electronic Authentication methods used by Federal Government agencies |
| SP 800-73 Interfaces for Personal Identity Verification | NIST | NIST Special Publication 800-73, March 2006 – specifies interface requirements for retrieving and using identity credentials from the PIV Card and is a companion document to FIPS 201-1 |
| SP 800-79 Guidelines for the Accreditation of Personal Identity Verification Card Issuers | NIST | NIST Special Publication 800-79, June 2008 – provides appropriate and useful guidelines for accrediting the reliability of issuers of Personal Identity Verification cards that are established to collect, store, and disseminate personal identity credentials and issue smart cards, based on the standards published in response to HSPD-12 |
| SP 800-76  Biometric Data Specification for Personal Identity Verification | NIST | NIST Special Publication 800-76, January 2007 – describes technical acquisition and formatting specifications for the biometric credentials of the PIV system, including the PIV Card itself |
| SP 800-96 PIV Card to Reader Interoperability Guidelines | NIST | NIST Special Publication 800-96, September 2006 – presents recommendations for PIV card readers in the area of performance and communications characteristics to foster interoperability |

| Publication | Responsible Organization | Publication Description / Version / Date |
|---|---|---|
| SP 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) | NIST | NIST Special Publication 800-16, March 2008 – This Special Publication 800-series reports on the Information Technology Laboratory's (ITL) research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, Government, and academic organizations |
| Federal Information Processing Standards Publication (FIPS Pub) 140-2 | NIST | Security Requirements for Cryptographic Modules, August 2002 |
| FIPS Pub 180-2 w/ CN 1 | NIST | Secure Hash Standard, 1 August 2002, with Change Notice 1 to include SHA-224, 25 February 2004 |
| FIPS Pub 196 | NIST | Entity Authentication using Public Key Cryptography, February 1997 |
| FIPS Pub 197 | NIST | Advanced Encryption Standard, November 2001 |
| FIPS Pub 200-1 | NIST | Minimum Security Requirements for Federal Information and Information Systems, March 2006 |
| FIPS Pub 201-1 | NIST | Personal Identity Verification of Federal Employees and Contractors, March 2006 |