State Identity Credential and Access Management (SICAM) Guidance and Roadmap

EXECUTIVE SUMMARY

The State Identity and Credential Access Management (SICAM) Guidance and Roadmap outline a strategic vision for state-based identity, credential, and access management efforts, and emphasizes the importance of implementing the SICAM architecture and services in support of the challenges associated with trust, interoperability, security, and process improvement.

States can, and should, provide a secure, auditable environment for the processing and exchange of information across the entire spectrum of state business. SICAM is comprised of the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and/or Non-Person Entities (NPE). This guidance promotes a federated approach where the identification of the information requester and supplier are guaranteed. This is of vital importance in an environment where phishing, scamming, and identity theft are rampant. It is essential that state governments take the initiative to ensure the integrity of the data entrusted to them and provide a high level of security and privacy to citizens, customers, and partners.

The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries. This will significantly reduce administrative and technological overhead caused by siloed, incompatible, and un-auditable identity management systems, lead to improved business processes and efficiencies, and reduce cyber security risk.

There are multiple initiatives underway to address these challenges – Personal Identity Verification (PIV) cards are being issued in increasing numbers, the Public Key Infrastructure (PKI) has connected government and commercial PKIs via a trust framework, working groups are tackling relevant process, technology and operational questions for mission-specific functions, and many others are leveraging digital identities to enable trusted government to citizen (G2C), government to business (G2B), and government to government (G2G) transactions.

The primary audience for the document is the state Chief Information Officer (CIO), state Chief Information Security Officer (CISO), state Enterprise Architect (EA) and other state ICAM implementers at all stages of program planning, design, and implementation; however, the document may also be used as a resource for systems integrators, end users, other entities, and commercial business partners seeking interoperability or compatibility through state programs. While this document serves to outline a common framework for SICAM in the state government, it is understood that agencies are at different stages in the implementation of their SICAM architectures and programs. As a result, they will need to approach alignment with SICAM from varying perspectives. The SICAM Guidance and Roadmap will also serve as an important tool for providing awareness to external mission partners and drive the development and implementation of interoperable solutions.

This SICAM Guidance and Roadmap is being released as Version 1.0 and may include revised content in future iterations. The document should be used for research purposes only and it has been acknowledged by the authors that use of content from other documents has been indicated in the bibliography.

Document Overview

The SICAM Guidance and Roadmap provides architectural direction for a statewide identity management framework and is organized into the following sections:

Section 1 - Introduction: The introduction gives background information, provides the value proposition for the SICAM, and defines the document scope.

Section 2 – Goals and Objectives: The goals and objectives primarily focus on the role of the state government in achieving the SICAM end-state. Other key stakeholders have a crucial role in enabling interoperability and trust across the SICAM landscape to accomplish secure information sharing outside of state government boundaries. Stakeholders, mentioned throughout this document, include citizens, external businesses and commercial entities wishing to conduct business with state governments; the health IT community as it increases its reliance on SICAM activities in order to facilitate the use of e-health records; Federal/Emergency Response Official (F/ERO) – emergency preparedness; and federal, local, and tribal governments that require information exchanges to meet mission needs.

Section 3 – Assurance Levels: The State Identity, Credential and Access Management Assurance Level Model is a tool for objectively assessing the ability of government to perform a project over the lifecycle of SICAM presence across the enterprise. The assurance model represents a flexible and adaptive approach toward identification of the current ICAM presence and the next steps to be considered for establishing assurance levels for the SICAM architecture solution.

Section 4 – SICAM Principles, Processes and Concepts: This section introduces key principles and components that characterize SICAM architecture, but are not an exhaustive set of all the complexities that exist.

Section 5 – SICAM Architecture Framework: Development of the SICAM Architecture Framework provides the rules and definitions necessary for the integration of information and services at the conceptual level. The framework combines business and environment processes and represents the blueprint for the implementation of the SICAM solution. The blueprint contains the details that are essential for allowing data to flow from agency to agency.

Section 6 – Approach to Implementation: This section outlines key strategies for meeting the targeted framework for SICAM. This section will also outline how interoperability will occur to share identity attributes across department and agency boundaries, By breaking down boundaries, states can reduce the total cost of ownership for department an agency identity systems.

Section 7 – Summary: There are many steps along the way and an organization may find that not all of the areas fit neatly within the lines. Maturity within the architecture framework will vary across the business architecture processes and technology architecture, as well as the architecture blueprint. This is an evolving process for states and leads to an efficient, effective, and responsive development for identity and access management solutions.

Appendix A-K: Includes additions to the document that can be used as reference material on topics found within SICAM.

Contents

Acknowledgements

NASCIO would like to express its thanks and gratitude to the members of the 2012 State Digital Identity Working Group for lending their time and expertise to help guide this publication's development. NASCIO would also like to extend a special thank you to former members of the State Digital Identity Working Group who made it possible for this group to continue down the path towards developing the first version of the State Identity Credential and Access Management Guidance and Roadmap.

Finally, NASCIO extends a special thanks to those state CIOs and their staff who contributed in the development and revision of this product.

Please direct any updates, questions or comments about this publication or any of NASCIO's State Digital Identity Working Group research products to Chad Grant at cgrant@amrms.com or call (859) 514.9153.

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers and information technology executives from the states, territories, and the District of Columbia.The primary state government members are senior officials who have executive level and statewide responsibility for information technology leadership. State officials who are involved in agency level information technology management may participate as associate members. Representatives from other public sector and non-profit organizations may also participate as associate members. Private sector firms may join as corporate members and participate in the Corporate Leadership Council. AMR Management Services provides NASCIO's executive staff.

1. INTRODUCTION

1.1 Background

The Federal Government has made progress regarding ICAM in recent years. The Homeland Security Presidential Directive 12 (HSPD-12) initiative provides a common, standardized identity credential that enables common physical access credentials and secure, interoperable online transactions. Additional federal initiatives have resulted in the development of the following standards and guidelines that support ICAM strategies:

- Smart Access Common ID Card: GSA, NIST (1998)
- Federal PKI Policy Authority (2002)
- OMB directive on smart ID cards: HSPD-12 (2004)
- Personal Identity Verification (PIV) of Federal Employees and Contractors:
  - FIPS-201-1 (2006)
  - FIPS-201-2 (2011)
- First Responder Authentication Credential (FRAC) (2006)
- Federal Identity, Credentialing and Access Management (FICAM) (2009)
- Cyberspace Policy Review (2009)
- Personal Identity Verification Interoperability for Non-Federal Issuers (PIV-I) (2009)

Nationally, in recognition of the rising cybersecurity risks as online transactions increase, the White House published the draft National Strategy for Trusted Identities in Cyberspace, Enhancing Online Choice, Efficiency, Security, and Privacy (NSTIC) in April 2011. This strategy aims to reduce online fraud and identity theft by increasing the level of trust associated with identities in cyberspace. NSTIC outlines the needs of parties involved in electronic transactions (e.g., online banking, accessing electronic health records, accessing state benefits) to have a high degree of trust that they are interacting with known entities. The strategy presents a framework for raising the level of trust associated with the defined identities of individuals, organizations, services, and devices involved in certain types of online transactions. The broad vision of the strategy is "individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation." In addition, NSTIC recognizes the importance of the private sector and puts a great deal of emphasis on this being an industry led initiative. This vision is directly applicable to state goals as more services are provided online. The strategy also seeks to meet the privacy and security concerns of citizens by making participation voluntary.

In order for states to participate in the federal ecosystem, they must be able to adhere to their guidelines. The FICAM documents refer to federal and state governments as G2G relationships. However, gaps still remain across ICAM programs in the federal government, and there is much work that is in progress or yet to be done. In addition to key factors such as interoperability and trust, limitations on how federal standards and guidelines address state needs led to the development of this document, the State Identity, Credentialing and Access Management (SICAM) Guidance and Roadmap.

Proactive delivery of citizen services is also critical. States want to respond quickly to a change in a citizen's employment, legal or health status, and automatically deliver the services for which the citizen is eligible. This improves the well-being of the population and can help reduce the billions of dollars in services fraud the states experience today.

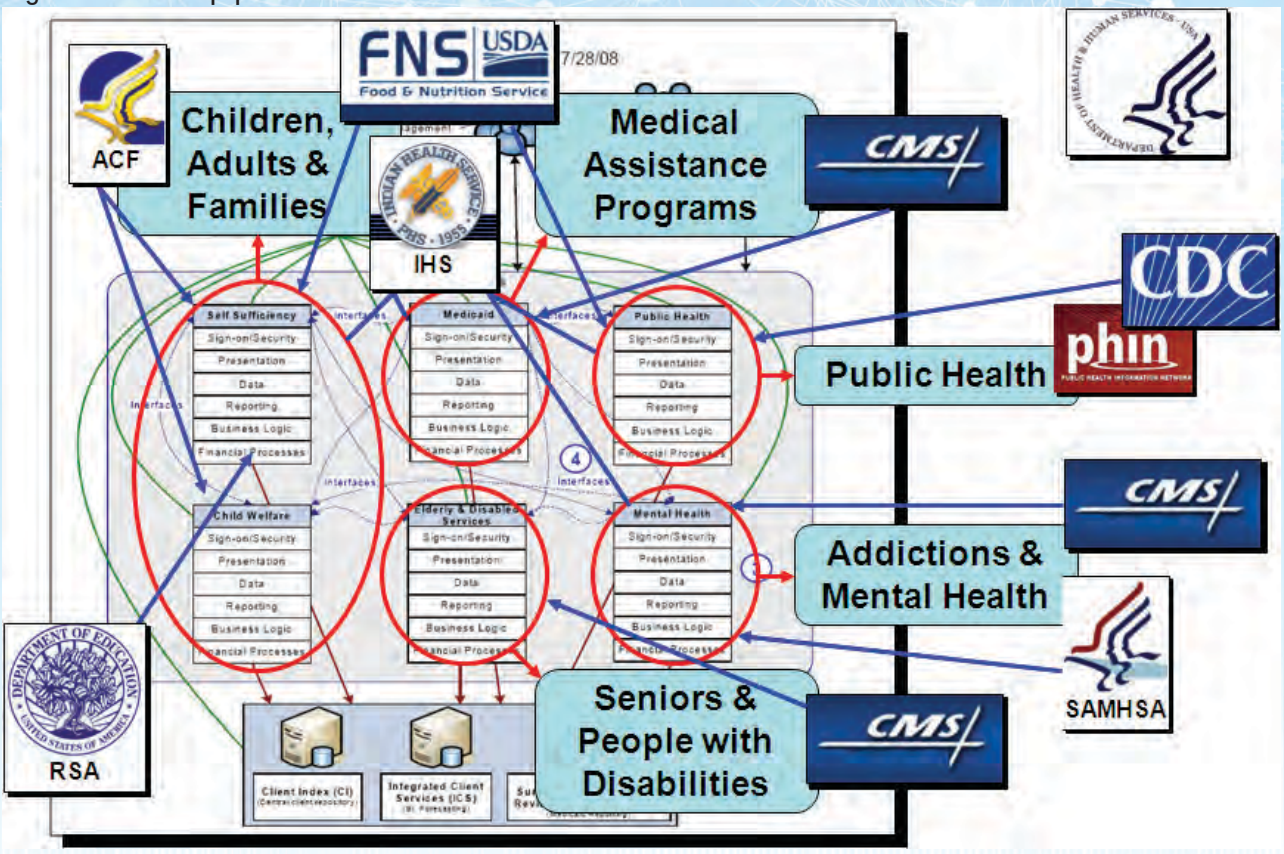
Critical to thwarting out vulnerabilities is a state's ability to coordinate a combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguard personal identity information – better known as Identity Management (IdM). By having these types of access controls in place, states can leverage the process of determining whether a subject is allowed to have access to particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized for access.

In recent years, increasing emphasis has also been placed on improving the complex cyber and physical security of the hundreds of thousands of facilities operated by government. States need to appropriately leverage existing and planned ICAM solutions in a federated manner. As a result, stronger more reliable ICAM capabilities will need to be developed and this will be critical to the success of all governments' missions.

As part of the nationwide movement toward proactive citizen service delivery, transparency, and accountability, states are increasing sharing and utilizing data between departments, agencies, counties, and the federal government. Programs like the US Department of Education's State Longitudinal Data Systems (SLDS), require the ability to measure a student's performance and the specific factors (e.g., educational programs, teachers, schools) that influenced outcomes from Preschool to age 20 (P-20). To meet the SLDS requirement, student and teacher data must be analyzed from the multiple state departments that deliver educational services, including Human Services, K-12 Education, Workforce Development, Corrections, and Higher Education. Similarly, states are being asked to measure and report the outcomes of other federally funded programs such as health, job creation, voting, welfare, and nutrition. In order to link the SLDS data from multiple departments and determine a correlation, there must be a common unique identity for a student between these systems. Many questions still exist in states and concepts of opt-in, opt-out, and mandatory vs. non-mandatory will need to be discussed amongst stakeholders, but those policy considerations are out of the scope of this document.

Similarly in the case of providing access to, delivering, or updating citizen services, states must manage eligibility and authorizations and communicate basic identity information (e.g., name, address, and dependent) amongst themselves so that if one department receives new information about a citizen, other departments will be updated as well. When looking across the large federally funded, state administered benefit programs, there are common basic architectural needs for identity, access, security, and data management. As Figure 1 depicts, managing these architectural requirements in silos leads to risk, errors and redundant efforts.

Figure 1: Stove-piped Architecture



There is a need to standardize and federate within and across state boundaries. Towards this end, and for the purposes of federating identity and access management across states and their business partners, new approaches to state identity systems are required. This SICAM approach leverages concepts of a Federated Trust Model (FTM) which will allow existing and new resources to be rapidly integrated and securely accessed across boundaries. Electronic authentication of individuals can provide the base elements to allow for secure electronic transactions at varying assurance levels and establishing trust for multiple purposes and multi-layered security.

While programs specific to a particular state departments or agencies are not discussed within this document, it is envisioned that all state department and agency ICAM programs within government will align with a central SICAM framework and the central infrastructure that will integrate resources and identity mechanisms across department and agencies boundaries.

The primary audience for the document is the state Chief Information Officer, state Chief Information Security Officer, state Enterprise Architect and other state ICAM implementers at all stages of program planning, design, and implementation; however, the document may also be used as a resource for systems integrators, end users, and other entities such as, commercial business partners seeking interoperability or compatibility through a FTM with state programs. While the document serves to outline a common framework for ICAM in the state government, it is understood that agencies are at different stages in the implementation of their ICAM architectures and programs. As a result, they will need to approach alignment with the SICAM Guidance and Roadmap from varying perspectives.

1.2 Value Proposition

The purpose of this guidance is to outline a common framework for ICAM within state government and to provide supporting implementation guidance for program managers, leadership, and stakeholders as they plan and execute a common architecture for ICAM management programs.

This document will help states leverage digital infrastructure to securely conduct business electronically within and between other states, their business and coalition partners, and with the public, by promoting the use of digital ids, authentication, digital signature, and encryption technologies. Guidance is provided for both legacy system integration and new application development. This document provides guidance to gain significant benefits around security, cost, and interoperability thus providing positive impacts beyond an individual agency in improving delivery of services to the citizens of a state. It also seeks to support the enablement of systems, policies, and processes to facilitate business between the government and its business partners and constituents. An example of an existing trust framework is the Federal Public Key Infrastructure (FPKI) Policy Authority. FPKI is an interagency body set up under the CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.

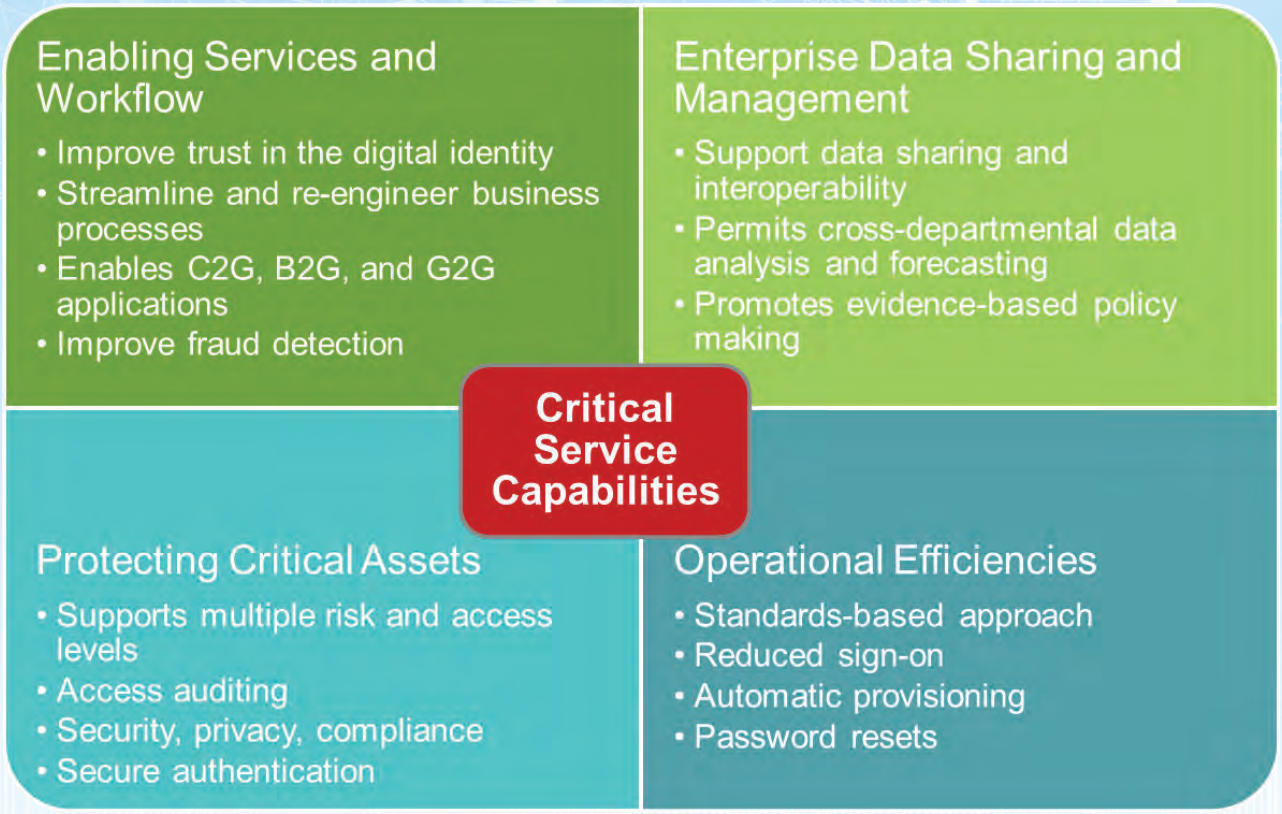
The architecture, milestones and implementation approaches outlined here will be leveraged by states as they attain greater interoperability and increased security. In support of the overall purpose, the roadmap was written to accomplish the following objectives:

- Provide background information on ICAM and educate the reader about key programs in each area and how they are interrelated;
- Give guidance on how to incorporate a segment architecture for ICAM programs;
- Provide a high-level vision for the target of a Federated Trust Model (FTM) to be used by states and management of ICAM systems, technologies, data, and services;
- Enumerate and provide references to technical standards that are applicable to identity, credential, and access management programs;
- Increase the pursuit of technological interoperability and reuse across the government

A key aspect of access management is the ability to leverage an enterprise identity for entitlements, privileges, multi-factor authentication, roles, attributes and different levels of trust. Logical access and physical access are often viewed as the most significant parts of ICAM from a return on investment perspective. To maximize that return, a successful access management solution is dependent on identity, credentials, and attributes for making informed access control decisions, preferably through automated mechanisms.

The level of investments made must allow for the construction and development of all the foundational elements from which return on investment (ROI) is derived. Lack of this proper foundation will risk the resulting trust models, security services, and envisioned value and need intended for the SICAM initiative.

Figure 2: Critical Service Capabilities



Identity and access management technologies are enabling, foundational tools that support multiple business facets, both internal and external. The benefits associated with a centralized and federated implementation of SICAM are highlighted in Figure 2 and summarized below:

- **Increased security**, which correlates directly to reduction in identity theft, data breaches, and trust violations. Specifically, SICAM closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing.
- **Compliance with laws**, regulations, standards and state policies.
- **Improved interoperability**, specifically between agencies using credentials along with other third party credentials that meet the requirements of the federated trust framework.
- **Enhanced customer service**, facilitating secure, unified, and user-friendly transactions – including information sharing – translates directly into improved customer service scores, lower help desk costs, and increased consumer confidence in agency services.
- **Elimination of redundancy**, both through agency consolidation of processes and workflow and the provision of government-wide services to support SICAM processes. This results in extensibility of the IT enterprise and reduction in the overall cost of security infrastructure.
- **Increase in protection of personally identifiable information (PII)** by consolidating and securing identity data through the use of encryption, improving access controls, and automating provisioning processes.
- **Enhanced Privacy**, transparent process and notice regarding the collection, use, dissemination and maintenance of information.
- **Voluntary**, self-determining participation within and identity and access management

system.

A state's ability to improve their cybersecurity posture can be accomplished through standardized controls around identity and access management. Initiatives such as the National Strategy for Trusted Identities in Cyberspace (NSTIC), provides a framework for identity ecosystems. Much like NSTIC, the SICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. This guidance and roadmap presents a common framework needed to plan and execute SICAM programs.

1.3 Scope

This guidance applies to all such transactions for which authentication and authorization is required, regardless of the constituency (e.g. individual user, business, or government entity).

- This guidance focuses on the actions permitted of an identity after authentication has taken place. Decisions concerning authorization are and should remain the purview of the business process owner.
- This guidance applies to authentication and authorization of human users of state agency IT systems for the purposes of conducting government business electronically (or e-government). Though authentication and authorization typically involves a computer or another electronic device, this guidance does not apply to the authentication of servers, or other machines and network components.
- This guidance is intended to help states identify and analyze the risks associated with many of the steps for the authentication and authorization process. The process includes (but is not limited to) identity proofing, credentialing, technical and administrative management, record keeping, auditing, and use of the credentials. Each step of the process influences the technology's overall conformance to the desired assurance level.
- This guidance does not address issues associated with "intent to sign," or state use of authentication credentials as electronic signatures. The Uniform Electronic Transactions Act (UETA) was developed by the National Conference of Commissioners on Uniform State Laws to provide a legal framework for the use of electronic signatures and records in government or business transactions. UETA makes electronic records and signatures as legal as paper and manually signed signatures. Forty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands have adopted the Uniform Electronic Transactions Act (UETA) promulgated by the Uniform Law Commission and details can be found at the National Conference of State Legislatures (NCSL) website at http://www.ncsl.org/issues-research/telecom/uniform-electronic-transactions-acts.aspx.

Types of authentication that are applicable to this guidance:

a) Identity authentication—confirming a person's unique identity.
b) Attribute verification—confirming that the person belongs to a particular group (such as military veterans or U.S. citizens).

Attribute authentication is the process of establishing an understood level of confidence that an individual possesses a specific attribute. If the attribute does not provide ties to the user's identity, it would be considered an anonymous credential. Attribute authentication is not specifically addressed in this document; however agencies may accept "anonymous credentials" in certain contexts wen verification is not needed.

1.4 ICAM Definitions

ICAM comprises the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and/or Non-Person Entities (NPE). NPE have been defined by the NSTIC as an entity with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts. The binding of those identities to credentials may serve as a proxy for the individual or NPE in electronic transactions, and leveraging the credentials to provide authorized access to an agency's resources. ICAM systems have generally supported different offices, programs, and systems within different agencies and typically are directed and managed separately as individual stove-pipes in the past.

The historical reality of IT decentralization across state agencies has led to a patchwork of siloed system tools, technologies and processes not based on standards and not able to support the agile needs of 21st century state governments. These siloed approaches are increasingly expensive to maintain and too inflexible to respond to any demands set forth by new federal or state laws, regulations, or budgetary pressures. A few states have implemented federated ID frameworks and a few are actively engaged in the process but to our knowledge, many states are either creating independent frameworks or are not addressing the issue. A common architectural approach, supported by standard definitions will help to reduce costs, avoid siloed solutions, and increase cross-state collaboration and interoperability.

1.4.1 Identities and Credentials

The identity and credentialing aspects of the SICAM Guidance and Roadmap address core identity issuance processes. Included in the issuance process are several steps and key concepts that build upon each other to form a trust framework. Below you will find a few of the key terms for identity management. There are a variety of definitions used in the issuance process and for further definitions consult the original version of NIST SP 800-63.

- **Digital identity** is the representation of identity in a digital environment.
- **Identity providers** are entities that manage identity information on behalf of parties and provide assertions of authentication to other providers.
- **Issuers** are the entities responsible and trusted to issue identities to individuals, organizations and/or systems.
- A **credential** is an object that authoritatively binds an identity to a token possessed and controlled by a person.
- An **attribute** is a distinct characteristic of an object. An object's attributes are often used to describe traits, such as size, shape, weight, color, etc.
- **Authentication** is the process of establishing confidence in the identity of users or information systems.
- **Authorization** is the process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Once a subject is authenticated, it may be authorized to perform different types of access.
- A **Relying party** is a system entity that decides to take an action based on information from another system entity.
- **Trust** is the extent to which a party is willing to depend on something or someone in a given situation with a relative feeling of security.

1.4.1.1 Identity Management

The formal identification process may consist of collecting information about a person and validating that information to provide some level of assurance that the person is who they claim to be. The identification process could then result in the issuance of both physical and electronic credentials dependent on future requirements. An issued credential is something that the user would then provide to validate a claim of their identity.

- A physical credential (e.g., drivers' license, passport, etc.) can be issued by various authorities (e.g., DMV, State Department, etc.).
- An electronic credential (e.g. user name and password) may be issued during an online registration process or other process where the validity of the requestor is checked against information currently stored in data repositories and is consistent with the same information for obtaining the physical credentials. Obtaining access to a controlled state asset or service will require the user to assert their identity by providing a pre-issued credential as proof of that identity.

However, not all credentials are equal. The level of assurance provided by a credential depends directly on the process that was used to issue a credential. Once issued, the credential must be validated as part of the authentication process. The individual must also have authorization to access the resource or service, regardless of the validity of the identity.

Before receiving credentials, an applicant must demonstrate that the identity claimed is real and that they are verified to use that identity. This process is referred to as identity proofing.

State agencies are governed by specific laws, regulations, and policies that include processes for identity-proofing before issuance of identity credentials. Agencies can, if they so choose, issue photo badges or ID's, a digital signature, and/or username/password pairs as credentials. Credential issuance generally involves the following steps:

- Identity-proofing is where the claimed identity of the person is validated. In most states, this requires background checks and other means of verification processes which may include, at times, criminal history database checks, and other information provided by the claimant. Security managers will verify identity using an ID card(s) issued through an appropriately rigorous process prior to issuing local credentials. Where multiple proofs of identity are required, care should be taken to require use of ID cards which are issued using different identity proofing processes.
- Registration and naming, where the identity is assigned an identifier
- Generation of an authentication credential. Depending on the business requirements and technology used, may involve selection or generation of PINs, PKI certificates, photograph, and/or biometric reference samples.
- Binding the intended authentication method to the identity.

The reason for federating state identity systems is that they can work harmoniously together to improve the security assurance levels of identities. This involves not only technology standards, but a trust framework of processes, policies, and procedures that issuing and relying parties can agree to.

1. State employees or their business partners commonly need access to multiple resources that span agency domains. A federated identity system can be the foundation for new sys-

tem designs that allow employees to seamlessly access resources that span other agency domains.

2. When a citizen uses an online process to obtain services with the state, the more identifying information the person knows, the higher the level of assurance will be to the state that that person is who they say they are, which in turn allows them to obtain a specific level of services.

Authentication

Credentials are authenticated using one of three personal authentication factors or techniques. The three categories of authentication factors are:

1. something you know (e.g., a password)
2. something you have (e.g., a certificate with associated private key, smart card, or cookie)
3. something you are (e.g., a biometric attribute such as fingerprint or facial)

In addition, there are also emerging authentication factors such as:

4. somewhere you are (e.g., location identification, such as phone triangulation, GPS, IP address, DNS routing, etc)

Single-factor authentication is defined as the use of any one of these categories or authentication factors. If two factors are employed, this is considered two-factor authentication. Note that the factors must be different and multiple passwords would not be considered two-factor authentication. If three factors are required then this constitutes use of three-factor authentication. Finally, a fourth factor could possibly be used via cell phones that operate as something you have by returning a personal identification number (PIN) response and also as somewhere you are based on cell phone triangulation. Individual authentication assurance increases when you combine authentication technologies and techniques, especially when combining differing authentication factors.

Access

Access is when ordained resources are granted. The purpose of access is closely tied to access management and is intended to ensure that the proper identity verification is made when an individual attempts to access security sensitive buildings, computer systems, or data. It has two areas of operations: logical and physical access. Logical access is the access to an IT network, system, service, or application. Physical access is the access to a physical location such as a building, parking lot, garage, or office. Access management leverages identities, credentials, and privileges to determine access to resources by authenticating credentials. After authentication, a decision as to whether he/she is authorized to access the resource can be made. These processes allow agencies to obtain a level of assurance about the identity of the individual attempting to access a resource.

In addition, access control sets the stage for additional activities outside of the traditional access control paradigm. One corollary to access management is the ability to ensure that all individuals attempting access have a genuine need. This is tied to authentication and authorization, but also to the business rules surrounding the data itself. Privacy is provided by properly ensuring confidentiality and by refraining from collecting more information than that which is necessary. Today, agencies create a digital representation of an identity in order to enable unique application-specific processes, such as provisioning access privileges. As a result, maintenance and pro-

tection of the identity itself is treated as secondary to the mission associated with the application itself. This document offers an approach to "identity management" (IdM), wherein creation and management of digital identity records are shifted from stove-piped applications to an authoritative enterprise view of identity that enables cross-agency application or mission-specific uses without creating redundant, distributed sources that are harder to protect and keep current.

Digital Identity

Unlike accounts to logon to networks, systems or applications, enterprise identity records are not tied to job title, job duties, location, or whether access is needed to a specific system. Those things may become attributes tied to an enterprise identity record, and could also become part of what uniquely identifies an individual in a specific application. Access control decisions will be based on the context and relevant attributes of a user—not solely their identity. The concept of an enterprise identity is that individuals will have a digital representation of themselves which can be leveraged across agency boundaries for multiple purposes, including access control.
Establishment of a digital identity typically begins with collecting identity data as part of an on-boarding process. A digital identity typically consists of a set of attributes that when combined uniquely identify a user within a system or enterprise. In order to establish trust in the individual represented by a digital identity, especially for state government use or business partner access, an agency may also conduct a background investigation. Attributes for an individual may be stored in various authoritative data sources within different agencies and linked to form an enterprise view of the digital identity.

This digital identity may then be provisioned into applications in order to support physical and logical access. They may then be de-provisioned when access is no longer required. While the background investigation and on-boarding process are internal to the state government, similar processes may also be applied to external users and entities for which an agency manages identity data, although they are typically less stringent and vary depending on the usage scenario.

With the establishment of an enterprise identity, it is important that policies and processes are developed to manage the lifecycle of each identity and, when appropriate, ensure that privacy is maintained. Management of an identity includes:

- The trust framework and schema for establishing a unique digital identity,
- The ways in which identity data will be used,
- The protection, (proper access and encryption), of Personally Identifiable Information (PII),
- Controlling access to identity data,
- The policies and processes for management of identity data,
- Developing a process for remediation; solving issues or defects,
- The capability to share authoritative identity data with applications that leverage it,
- The revocation of an enterprise identity, and
- The system that provides the services and capabilities to manage identity.

As part of the framework for establishing a digital identity, due diligence should be employed to limit data stored to the minimum set of attributes required to define the unique digital identity and still meet the requirements of how agency systems integrate at the state level. A balance is needed between information stored in independent agency systems, and information made available to internal and external systems and the privacy of individuals. States must consider what

happens if there is break in the trust framework and citizens, information is unwillingly released. Concerns around liability may need to be vetted with the stakeholders within your state.

1.4.1.2 Credential Management

According to National Institute of Standards and Technology Special Publication 800-63 (NIST SP 800-63), a credential is an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. Credential management supports the lifecycle of the credential itself.

In state government, examples of credentials are passwords, user ids, smart cards, private/public cryptographic keys, and digital certificates. The policies around credential management, from identity proofing to issuance to revocation, are fairly mature compared to the other parts of ICAM. The PIV standards [Federal Information Processing Standards 201 (FIPS 201), SP 800-73, etc.] and Federal PKI Common Policy are examples of documents which have been in place and are foundational to state agency-specific credential implementations.
Credentialing generally involves four major components:

1. An authorized individual sponsors an entity, employee, or citizen to establish the need for a credential.
2. An individual enrolls for the credential, a process which typically consists of identity proofing and the capture of necessary data such as birth certificate, passport, biographic and biometric data. The data types required depend on the credential type and usage scenario. Additionally, step two may be automatically fed additional authoritative attribute data collected and maintained through identity management processes and systems, since enrollment for a credential requires much of the same data collection that is required as part of Identity Management.
3. A credential must then be produced and issued to an individual. As in the case of enrollment, issuance processes will vary based upon the credential being issued. Identity proofing, production, and issuance requirements for other credential types typically include process subsets or technologies with the same general principles.
4. Finally, a credential must be maintained over its lifecycle, which might include revocation, reissuance/replacement, re-enrollment, expiration, PIN reset, suspension, or re-instatement.

A key distinction in the lifecycle management of credentials versus identities is that credentials eventually expire. The attributes which form your digital identity may change or evolve over time, but your identity does not become invalid or terminated from a system perspective. Credentials however are usually valid for a pre-defined period of time based on policy. An example would be digital certificates which are issued to an individual or entity and expire based on the Issuer's PKI Common Policy. While the identity of an individual or entity does not change, the certificates associated with that individual or entity can be revoked and new ones issued. This does not have a bearing on the identity or entity as credentials are a tool for authentication that provide varying levels of assurance about the authentication of the individual or entity.

1.4.2 Access Management

Access management is the management and control of the ways in which entities rely on identities and credentials to granted access to resources. Entities provided access based on these identities / credentials are considered relying parties.

The purpose of access management is to ensure that the proper identity verification is made when an individual attempts to access security sensitive buildings, computer systems, or data. This covers two areas of operations: logical and physical access. Logical access is the access to an IT network, system, service, or application that inevitably gains access to data. Physical access is the access to a physical location such as a building, parking lot, garage, or office. Access management leverages identities, credentials, and privileges to determine access to resources by authenticating credentials.

After authentication, the system determines what resources are authorized to be accessed. These processes allow agencies to obtain a level of assurance for the identity of the individual attempting access to meet the following:

1. **Authentication** - Ensuring that all access is properly validated.
2. **Confidentiality** - Ensuring that all access to information is authorized in terms of disclosure and non-disclosure.
3. **Integrity** - Ensuring that all information is protected from unauthorized creation, modification, or deletion.
4. **Availability** - Ensuring that authorized parties are able to access needed information.
5. **Non-repudiation** - Ensuring the accountability of parties gaining access and performing actions.

In addition to the access controls listed above, the system can also ensure that all individuals attempting access have a genuine need. This is tied to authentication and authorization, but also to the business rules surrounding the data itself. Privacy is provided by properly ensuring confidentiality and by preventing the collection of more information than necessary.

The four core support areas that enable successful access management for both physical and logical access are:

- **Master Data Management (MDM)** - comprises a set of processes and tools that consistently defines and manages the master data (i.e. non-transactional data entities) of an organization (which may include reference data). MDM has the objective of providing processes for collecting, aggregating, matching, consolidating, quality-assuring, persisting and distributing such data throughout an organization to ensure consistency and control in the ongoing maintenance and application use of this information. As part of attribute verification, states can leverage tools and follow a clearly defined set of processes that have been created for MDM.
- **Resource Management** - Processes for establishing and maintaining data (such as rules for access, credential requirements, etc.) for a resource/asset that may be accessed. This provides rules for the object of an access transaction.
- **Privilege Management** - Processes for establishing and maintaining the entitlement or privilege attributes that exist within an individual's access profile. This provides rules for the subject of an access transaction. Privileges are considered attributes that can be linked to a digital identity.
- **Policy Management** – Processes for establishing and maintaining policies that incorporate business rules and logic, usually based on attributes or roles. This governs what is allowable or unallowable in an access transaction.

2. GOALS AND OBJECTIVES

Though goals and objectives primarily focus on the role of the state government in achieving the SICAM end-state, other key stakeholders have a crucial role in enabling interoperability and trust across the SICAM landscape to accomplish secure information sharing outside of state government boundaries. Stakeholders, mentioned throughout this document, include external business and commercial entities wishing to conduct business with state government, such as the health IT community as it increases its reliance on SICAM activities in order to facilitate the use of e-health records and Federal/Emergency Response Official (F/ERO) – emergency preparedness; and federal, local, and tribal governments that require information exchanges to meet mission needs. At this point it is also important to emphasize the importance of increasing education and developing cross-agency communication.

Figure 3: Primary SICAM Goals and Objectives

Goal 1: Trust	Goal 2: Interoperability	Goal 3: Security	Goal 4: Process Improvement
❑ Establish trusted identity	❑ Facilitate access to intrastate agency services	❑ Enable multi-factor authentication	❑ Improve citizen facing services
❑ Align with State, Federal & industry credentialing policies and standards	❑ Provision centrally, reduce credentialing efforts	❑ Expand secure access to data and systems	❑ Facilitate secure online transactions
❑ Align State business processes with ICAM processes	❑ Integrate with State agency registration systems	❑ Support broad cybersecurity programs	❑ Offer non-repudiation through digital signatures
❑ Establish trusted relationship with Federal, State, Local and Open Solution credential providers	❑ Align interoperability goals with intrastate, other States and Federal agencies	❑ Integrate electronic verification with physical security	❑ Reduce manual processing and data entry
❑ Ensure only qualified customers, employees and contractors access services	❑ Interoperate with FEMA and other emerging attribute standards	❑ Enable risk-based access control frameworks	❑ Provide tools for broad process improvement
		❑ Improve electronic audits	

2.1 Goal 1: Trust

States have traditionally played an active role in establishing and maintaining the identity of their constituents. The issuance of birth certificates, public school identification cards and driver's licenses are examples of instances where identities are established and credentials are issued at the state and local level. The challenge across states is that there are wide variances in the policies, practices and standards followed to establish identities. It is because of this variance that universal trust of identities and credentials across states and municipalities has not occurred.

State government stands to gain great value and enhanced service delivery by developing a foun-

dation of inter-organizational trust and interoperability across the state enterprise. Strong interoperable state identity credentials are the key to streamlining and automating building access, temporary access requests, and other access and authorization for government purposes. State government must tackle the governance and technical challenges posed by the abundance, variety, and complexity of ICAM-related programs in order to promote trust and interoperability and enable service delivery and information sharing across all partners.

Goal 1 is focused on establishing common standards, policies and practices for identity verification and vetting and credential issuance. With common, auditable identity and credentialing standards, all states will eventually be able to trust the identity of individuals presenting another states credential.

Objective 1.1: Align with State, Federal and Industry Credentialing Standards, Policies and Processes.

For the past several years there have been many inter-related but distinct state/federal government and industry initiatives to establish standard frameworks for identity, credentialing and access management. In addition, programs within other communities of interest have begun identifying their own identity, credential, and access management requirements, needs and procedures. States should leverage the existing knowledge bases, guidance and best practices which include:

- Industry bridges such as SAFE BioPharma[1] and Certipath Bridge[2]
- Federal Guidelines including Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance[3], Homeland Security Presidential Directive 12 (HSPD-12)[4] and Federal Information Processing Standard 201 (FIPS 201)[5] and associated Special Publications[6]
- Guidelines being developed by the U.S. Department of Health and Human Services (HHS) and being driven by Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted to promote the adoption and meaningful use of health information technology.

Objective 1.2: Establish Trusted Relationships with State, Federal, Local and Standards-Based Open Credential Providers.

By establishing trusted relationships with other state, federal and open credential providers, states can avoid the requirement to independently credential all its citizens. It can instead become a relying party of other identity credentials by establishing policies to accept credentials it deems trustworthy. Trusted physical and logical credentials and standards include, but are not limited to;

- Federal Personal Identity and Verification (PIV), PIV Interoperable (PIV-I) and First Responder Authentication Credentials (FRAC)
- Kantara Initiative[7], Transglobal Secure Collaboration Program (TSCP)[8] and InCommon

---

1 http://www.safe-biopharma.org/
2 http://www.certipath.com/
3 http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf
4 http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm
5 http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
6 NIST Special Publications 800-37, 800-53, 800-63, 800-73, 800-76, 800-78 – http://csrc.nist.gov/publications/PubsFIPS.html
7 http://kantarainitiative.org/
8 http://www.tscp.org/
9 http://www.incommonfederation.org/

Federation[9] digital identity standards

Objective 1.3: Comply with State Laws, Regulations, Standards, and ICAM Governance.
This objective includes aligning and coordinating operations and policies to meet the laws, regulations, standards, and other guidance in forming ICAM systems; aligning state with common ICAM practices; and where necessary, reviewing and aligning policies to ensure consistency.

Objective 1.4: Establish and Enforce Accountability for ICAM Implementation to Governance Bodies.
Necessary authority must be given to and exercised by the SICAM governance authorities to ensure accountability across state government in meeting its SICAM vision. In addition to developing comprehensive guidance and standards in support of the SICAM segment architecture, the governance bodies must establish and track specific performance metrics. Each state shares the responsibility for establishing the trust and interoperability processes necessary to achieve the SICAM vision. The state may be asked to report status against performance metrics periodically to a governing body.

Objective 1.5: Promote Public Confidence through Transparent SICAM Practices.
Public confidence in the security of the state government's electronic information and information technology is essential to adoption and use of E-Government services. State government must build a robust framework of policies and procedures committed to respecting and protecting the privacy of users in order to enable the trust required to move state government transactions online.

Objective 1.6: Establish and Maintain Secure Trust Relationships.
Establishing compatible identity, credential and access management framework policies can lead to a stronger baseline for evaluating partners against these pre-determined policies. This is a critical component for measuring success factors and building trust relationships across enterprises. State will identify and leverage existing trust relationships and continue working to build new trust relationships between the government and its partners (other governments, businesses, the health care community, and the State public) in order to move transactions online.

2.2 Goal 2: Interoperability

States and local governments have traditionally issued a multitude of single-use credentials to their constituents. Credentials and licenses used to gain access services such a library, recreation center, Medicaid, Medicare, drivers, fishing licenses, and employee IDs have served their purpose to provide authorization to use a particular facility or service. They redundantly attempt to establish identities at varying levels of trust, and this includes various forms of tamper proof features. The goal of interoperability is to establish common credentials – both physical and logical – that can be used to uniformly establish identity and that can be used to provide authorizations across facilities and services.

A key objective of the SICAM architecture is to implement a holistic approach for state government-wide identity, credential, and access management initiatives that support access to state IT systems and facilities. The intention is that state agencies will use this guidance to implement and/or provide a coordinated approach to SICAM across E-Government interactions [Government-to-Government, Government-to-Business, Government-to-Citizen, and Internal Effectiveness and Efficiency (IEE)] at all levels of.

The SICAM segment architecture also provides a framework that may be leveraged by other identity management architectural activities within specific communities of interest. The targeted outcome is a standards-based approach for all state government-wide identity, credential and access management to ensure alignment, clarity, and interoperability.

Objective 2.1: Support Information Sharing Environment (ISE) Communities of Interest.
State government operations rely on collaboration and knowledge sharing with other communities (including health IT, federal/local/tribal governments, industry, and foreign governments) in order to conduct business. This information sharing demands trust among the various players and an ICAM capability which supports this scope of interoperation. Future federal solutions must acknowledge and account for the need to support interoperable access to systems and data to support information sharing while maintaining control of the allowed access and appropriate information protections. The SICAM segment architecture addresses the concept of federated information flow, which requires two or more federated enterprises to support transactions across common interfaces.

Objective 2.2: Align Processes with External Partners.
The SICAM segment architecture supports a consistent approach for all government-wide identity, credential and access management processes to ensure alignment, transparency, and interoperability. This allows state government a means to do business with organizations such as banks and health organizations, and support G2B transactions by enabling common standards and leveraging an existing federated infrastructure. State government will respect the different requirements of state agency partners as to risk, assurance, and mission, and provide solutions that meet those needs and maintain inter-agency and inter-organizational interoperability.

Objective 2.3: Leverage Standards and Commercial Off-the-Shelf Technologies for SICAM.
State government should use commercial off the shelf (COTS) products and services, whenever possible, in order to enhance interoperability with the use of open standards and protocols and technological innovation and promote availability of SICAM systems and components.

Objective 2.4: Increase Interoperability and Reuse of ICAM Programs and Systems.
Implementation of the SICAM segment architecture is intended to unify existing ICAM programs and initiatives, as well as agency-specific ICAM activities, under a common governance framework, recognizing the unique role of each program in the overall structure while eliminating redundancies and increasing interoperability between solutions.

2.3 Goal 3: Security (Improve Security Posture across the State Enterprise)

ICAM capabilities play a key role in enhancing the ability to prevent unauthorized access to state government systems, resources, information, and facilities. As a function of logical security, ICAM can help protect information's confidentiality, assure that the information is not altered in an unauthorized way, and ensure information is released only to those entities authorized to receive it. ICAM will support and augment existing security controls as specified by the Federal Information Security Management Act (FISMA) and supporting NIST Special Publications 800-53 and 800-37, by promoting the use of strong identity solutions appropriate to the environment. A focus on SICAM outcomes can help improve the state's security posture beyond what controls are in place to meet mandates, but who has access to data and resources and what information is collected is also a very important for states to consider.

Objective 3.1: Enable Cyber Security Programs.
SICAM is a critical piece in protecting information and achieving cyber security goals. As a rising priority, cyber security will continue to grow and change within state government.

Objective 3.2: Integrate Electronic Verification Procedures with Physical Security Systems.
Once ICAM systems are in place and well established, the next step is for agencies to establish the need for electronic physical security systems and adopt and implement the appropriate policies and technologies to support physical access control leveraging electronic authentication.

Objective 3.3: Drive the Use of a Common Risk Management Framework for Access Control Mechanisms.
Existing authentication guidance and best practices for both logical and physical access dictate the use of a common risk management approach in determining the appropriate credential types and access control mechanisms. Driving the adoption and use of these approaches to ensure access controls are compliant with security requirements and risk-based analyses are imperative.

Objective 3.4: Improve Electronic Audit Capabilities.
Solutions adopted as part of SICAM initiatives will provide robust auditing capabilities to support accountability, provide discrete non-repudiation, and enhance transparency in security effectiveness.

2.4 Goal 4: Process Improvement (Facilitate E-Government by Streamlining Access to Services)

Strong and reliable identity, credential, and access management is a key component of successful E-Government implementation. When enabling electronic government, programs share sensitive information within government, between the government and private industry or individuals, and among governments using network resources and the World Wide Web. Further, this move towards enabling E-Government must be achieved in a flexible, cost-effective manner through collaboration among the public, industry, academia, and the government; and a corresponding policy and management structure must support the implementation of the solution.

Another goal of this effort is to allow agencies to create (and maintain) information systems that deliver more convenience, appropriate security, and privacy protection more effectively and at a lower cost. Establishing a clear vision is the first step in supporting these goals. Below are some specific benefits that may be realized from implementing this vision.

Objective 4.1: Expand Secure Electronic Access to Government Data and Systems.
To align with the SICAM segment architecture, state agencies should design, build, and deploy ICAM solutions to support a broad range of electronic government use cases which will support their mission areas across Government-to-Government (G2G), Government-to-Business (G2B), and Government-to-Citizen (G2C) interactions. State agencies must cooperate across agency boundaries in service delivery to give citizens, businesses, and other governments increased electronic accessibility to state government services through a wide choice of access mechanisms. The implementation of SICAM initiatives will facilitate the creation of government services that are more accessible, efficient, and easy to use.

Objective 4.2: Reduce Administrative Burden Associated with Performing ICAM Tasks.
Current ICAM efforts still rely on numerous manual, paper-based processes. Through automation

and streamlining processes, state government stands to significantly reduce the administrative burden and cost associated with the various ICAM tasks. For instance, the legacy practice of manually administering user accounts/privileges on a system-by-system, user-by-user basis creates a great administrative burden.

Objective 4.3: Align Existing and Reduce Redundant ICAM Programs.
A key objective of the SICAM segment architecture is to reduce or eliminate duplicative efforts and stove-piped programs and systems related to identity vetting, credentialing, and access control. Future ICAM solutions will leverage the existing investments of the central SICAM system and provide a more efficient use of tax dollars when designing, deploying and operating ICAM systems.

2.5 How the Goals and Objectives Should Be Used

In order to provide a federated ICAM solution, states will need to align goals with objectives to identify the concepts that need to be addressed. The objectives serve as a roadmap for businesses to analyze what needs to be done to meet the value propositions of providing a federated ICAM framework.

3. ASSURANCE LEVELS AND THE SICAM ASSURANCE LEVEL MODEL

Applying the Assurance Level Model requires a basic understanding of the 4 levels of assurance. The guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The levels of assurance as defined in the NIST Special Publication 800-63 are provided below:

Assurance Levels

3.1 Level 1

Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

3.2 Level 2

Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

3.3 Level 3

Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. While tokens may evolve, there are currently three kinds of tokens that may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

3.4 Level 4

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are required, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

3.5 Assurance Level Model

The Identity, Credential and Access Management Assurance Level Model envisions a continuous open architecture that can meet the goals and objectives over the lifecycle of an ICAM presence across the enterprise. The maturity model represents a flexible and adaptive approach toward identification of the current ICAM level of sophistication and the next steps to be considered in advancing the maturity level of the ICAM solution.

The SICAM Assurance Level Model provides a path for architecture and procedural improvements within an organization. As the architecture matures, predictability, process controls and effectiveness also increase.

Whatever the current stage of the state's ICAM program, each activity undertaken also has its own lifecycle. Without continuous monitoring of the driving business and technology factors, any ICAM Framework Architecture can soon become obsolete. Just as individual product and compliance components need to go through the cyclic process of documentation, review, compliance, communication, and vitality, the high-level ICAM Architecture Framework and procedures must be reviewed and updated to properly reflect environmental changes.

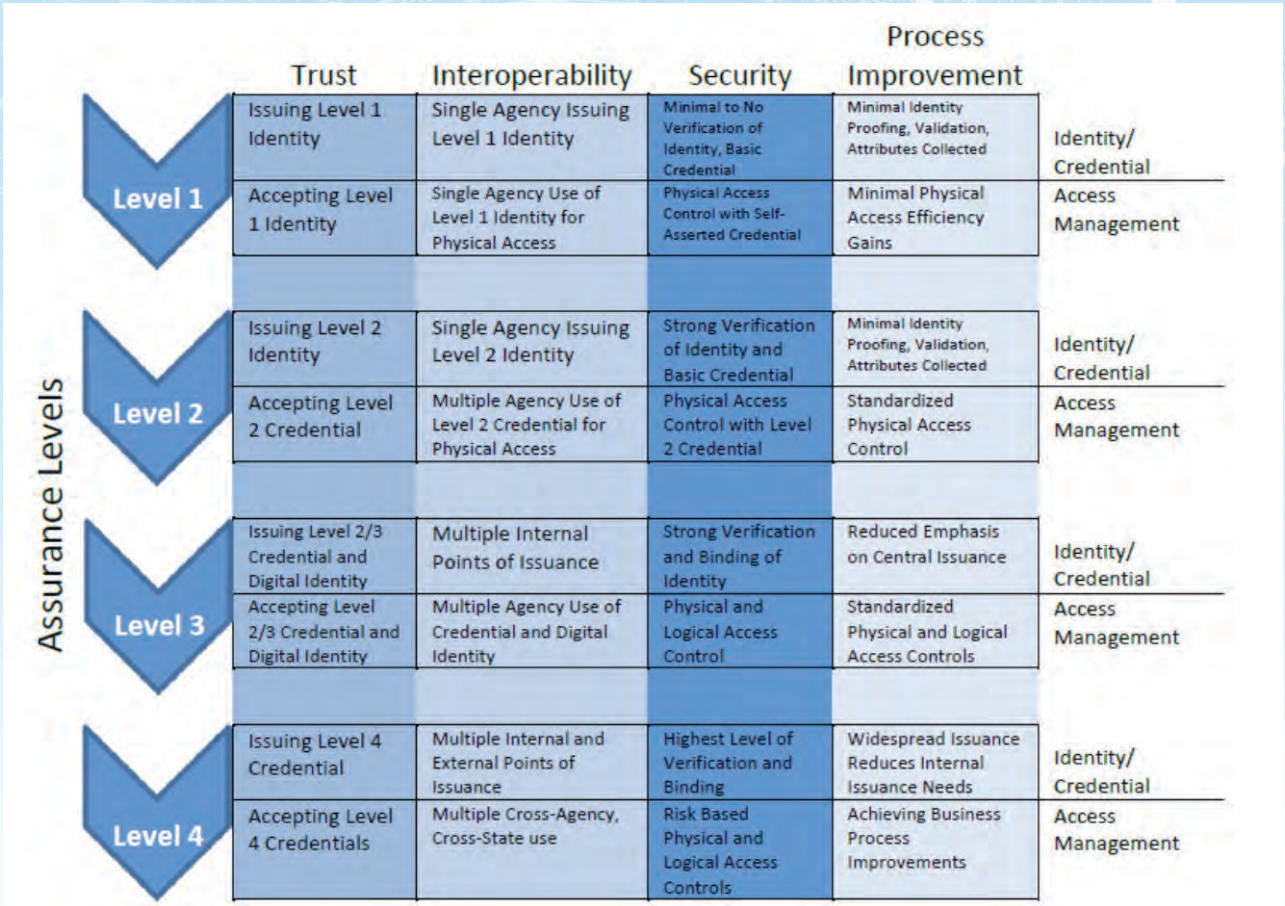
The Identity, Credential and Access Management Assurance Level Model envision a continuous improvement process, migrating from Level 1 through Level 4. The diagram in Figure 4 summarizes the ICAM assurance levels across the 4 main SICAM goals.

Inherently, the further you go down the stack in levels of assurance levels the more trusted your total solution for ICAM becomes. Trust, Interoperability, Security, and Process Improvement goals become realized as we move from Level 1 through 4.

3.6 How to use the SICAM Assurance Level Model

The SICAM Assurance Level Model can best be used to serve as a starting point for organizations who wish to participate either as a service provider (node) or an organization who wishes to incrementally improve their ICAM posture by participating in an enterprise solution. In order to do this an organization would use the SICAM Assurance Level Model as a guideline in assessing their current status and define where they need to be. Some organizations will require only a level one maturity while others may even need to extend the assurance level for specific needs. By reviewing the business needs and aligning process improvements states will be able to increase the business value and potentially increase the return on investment.

Figure 4: Assurance Level Model



Assurance Levels	Trust	Interoperability	Security	Process Improvement	
Level 1	Issuing Level 1 Identity	Single Agency Issuing Level 1 Identity	Minimal to No Verification of Identity, Basic Credential	Minimal Identity Proofing, Validation, Attributes Collected	Identity/ Credential
	Accepting Level 1 Identity	Single Agency Use of Level 1 Identity for Physical Access	Physical Access Control with Self-Asserted Credential	Minimal Physical Access Efficiency Gains	Access Management
Level 2	Issuing Level 2 Identity	Single Agency Issuing Level 2 Identity	Strong Verification of Identity and Basic Credential	Minimal Identity Proofing, Validation, Attributes Collected	Identity/ Credential
	Accepting Level 2 Credential	Multiple Agency Use of Level 2 Credential for Physical Access	Physical Access Control with Level 2 Credential	Standardized Physical Access Control	Access Management
Level 3	Issuing Level 2/3 Credential and Digital Identity	Multiple Internal Points of Issuance	Strong Verification and Binding of Identity	Reduced Emphasis on Central Issuance	Identity/ Credential
	Accepting Level 2/3 Credential and Digital Identity	Multiple Agency Use of Credential and Digital Identity	Physical and Logical Access Control	Standardized Physical and Logical Access Controls	Access Management
Level 4	Issuing Level 4 Credential	Multiple Internal and External Points of Issuance	Highest Level of Verification and Binding	Widespread Issuance Reduces Internal Issuance Needs	Identity/ Credential
	Accepting Level 4 Credentials	Multiple Cross-Agency, Cross-State use	Risk Based Physical and Logical Access Controls	Achieving Business Process Improvements	Access Management

4. SICAM PRINCIPLES, PROCESSES AND CONCEPTS

This section introduces key principles, processes and concepts that characterize SICAM architecture and is not an exhaustive set of all the complexities that exist. Later sections of this document will discuss how these principles and concepts are applied within the architecture framework.

4.1 Implied Architectural Principles

1. **Federated Approach**: At its most fundamental level the SICAM architecture describes a federation service based on a collection of data sources (or nodes) networked together and used for identification purposes. Networks may be modeled as graphs of nodes and the links between them. In the context of SICAM, a node is an entity that participates with other nodes in a federated system that orchestrates the exchange of information for purposes of providing a level of assurance that the identity is authenticated and has the attributes to perform some transaction. Regardless of its internal structure, the implementation of a federated architecture enables each node to maintain autonomy inside their domain, while adhering to SICAM specification for inter-node communication.
2. **Centralization**: The SICAM architecture allows decentralized nodes to participate as the single entry point for authentication.

3. **Separation of Authentication from Authorization**: A founding principle is to separate authentication functionality from authorization functionality. SICAM scope shall not include authorization concepts, rules, governance, and/or policies determining a set of permissions that are granted to a specific trusted identity. It is worth noting that when states determine the return on investment for identity management in a federated enterprise that authorization is included when factoring comprehensive savings.
4. **Local Autonomy and Creating a Trust Framework**: The Framework acknowledges that the participation of nodes in a trust community is a local decision, governed by federal and state regulations and local policies and permissions. Given this principle, participants in a trust community must meet eligibility requirements and agree to abide by the community operating rules established by the community's governance group. SICAM transactions must include enough information about the originating and receiving nodes (requestor/sender depending on whether it is a push or pull transaction) to ensure the appropriate authentication of the participating SICAM nodes as legitimate members of the trust community eligible to participate in information or transactional exchanges.
5. **Local Accountability**: Each SICAM node is accountable for the accuracy and truth of the information it provides to assist the decision making process, as embodied by the local autonomy principle.
6. **Adherence to Standards**: The SICAM Roadmap encourages implementing standards established by voluntary consensus standards bodies to accomplish the exchange of identity and attribute information among all such entities and networks.

4.2 Process Areas for Identity Management

1. Key Process Areas: There must be an existing system or group of systems, rules and procedures that need to be followed to provide identity management capabilities.

- Enrollment: Initiates the chain of trust for identity proofing and provides trusted services to confirm sponsorship, bind an applicant to attributes, and validate identity documentation.
- Issuance: Process of granting a credential to the applicant after all identity proofing, background checks and related approvals have been completed.
- Usage: Using the credential to access logical and/or physical resources based on authentication of the identity, credential, and authorization to access the resource.
- Provisioning and de-provisioning: Automatically providing an identity with access to a role, resource or service, or automatically changing or removing that access, based on the life cycle of events or work requests or changed attributes. For example; the first-day, second-day, on-going provisioning and last-day de-provisioning of the access rights of an employee.
- Relying party: A system entity that decides to take an action based on information from another system entity. A relying party will either grant or deny access.
- Security token life-cycle management: Managing a collection of security related hardware based devices. This includs the manufacturing, issuance and revocation of the token.

- Authentication: To confirm system or individual entities asserted principal identity with a specified, or understood, level of confidence.
- Assertions: Producing data as an act of authentication performed on a subject with respect to a specified source for attribute information.
- Administrating a domain: A combination of one or more administrative policies, internet domain name registrations, civil legal entities, collection(s) of hosts, network devices and the interconnecting networks, and possibly other traits. Administrative domains may interact and enter into agreements for providing and/or consuming services across administrative domain boundaries.

4.3 Technical Concepts for Consideration

1. **Service-Oriented, Layered Architecture:** Many states are still using legacy systems and may need to consider how emerging technologies can be applied to the existing enterprise. The use of layered architecture is a common messaging, security and privacy foundation which supports the SICAM identity information exchange services. Benefits include:
   - **Cross-platform integration:** Messages are the "universal translators" between different platforms and languages and permit each system to work with their native data types.
   - **Reliable communication:** Messages can use a "store-and-forward" style for delivery.
   - **End-to-end security:** Messages can transfer the complete end-to-end security of payload data using a combination of vendor neutral standards. Conforming to the standards profile will likely increase the ability to control the authentication of the personal identity.
2. **Utilize Web Services:** Web Services provide the basis for transport, discovery and exchange capabilities. Benefits to utilization of web services include:
   - **Standard protocol:** Functionality is exposed via web services interfaces.
   - **Web service description:** This description is provided via an XML document called a Web Services Definition Language (WSDL) document.
3. **Finding Web Services:** The discovery capabilities are provided by a listing of web services implemented via a Web Services Registry.
   - **Digital identity:** The representation of identity in a digital environment.
   - **Credentialing:** The process that authoritatively binds an identity (ad optionally, additional attributes) to a token possessed and controlled by a person.
   - **Privilege management:** The process of managing user authorization.
   - **Authentication:** To confirm or assert system identity with a specified, or understood, level of confidence.
   - **Authorization:** The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access.
   - **Access:** Provides the authorization, control and enforcement services that enable users to access resources.
   - **Cryptography:** The mathematical methods of protecting and keeping private or shared secrets, usually in a message. The Computer Security Division's (CSD) Security Technol-

ogy Group (STG) at NIST is involved in the development, maintenance, and promotion of a number of standards and guidance that cover a wide range of cryptographic technology. As it develops new standards, recommendations, and guidance, STG is aiming to develop a comprehensive Cryptographic Toolkit that will enable U.S. Government agencies and others to select cryptographic security components and functionality for protecting their data, communications, and operations. The toolkit currently includes a wide variety of cryptographic algorithms and techniques, and more will be added in the future. For information on NIST's "umbrella" crypto standard, FIPS 140-2, Security Requirements for Cryptographic Modules, please visit the Cryptographic Module Validation Program's (CMVP) home page.

- **Auditable services:** Consist of those subjects, units, or systems which are capable of being defined and evaluated.
- **Attribute management:** A distinct characteristic of an object. Attributes can be categorized as either human or object attributes. Human attributes are often specified in terms of physical traits, such as size, shape, weight and color, etc., or for roles that they may serve. Objects may have attributes describing size, type of encoding, network address and so on.
- **Registries:** Those who provide the process for (re)establishing an identity with a service provider.

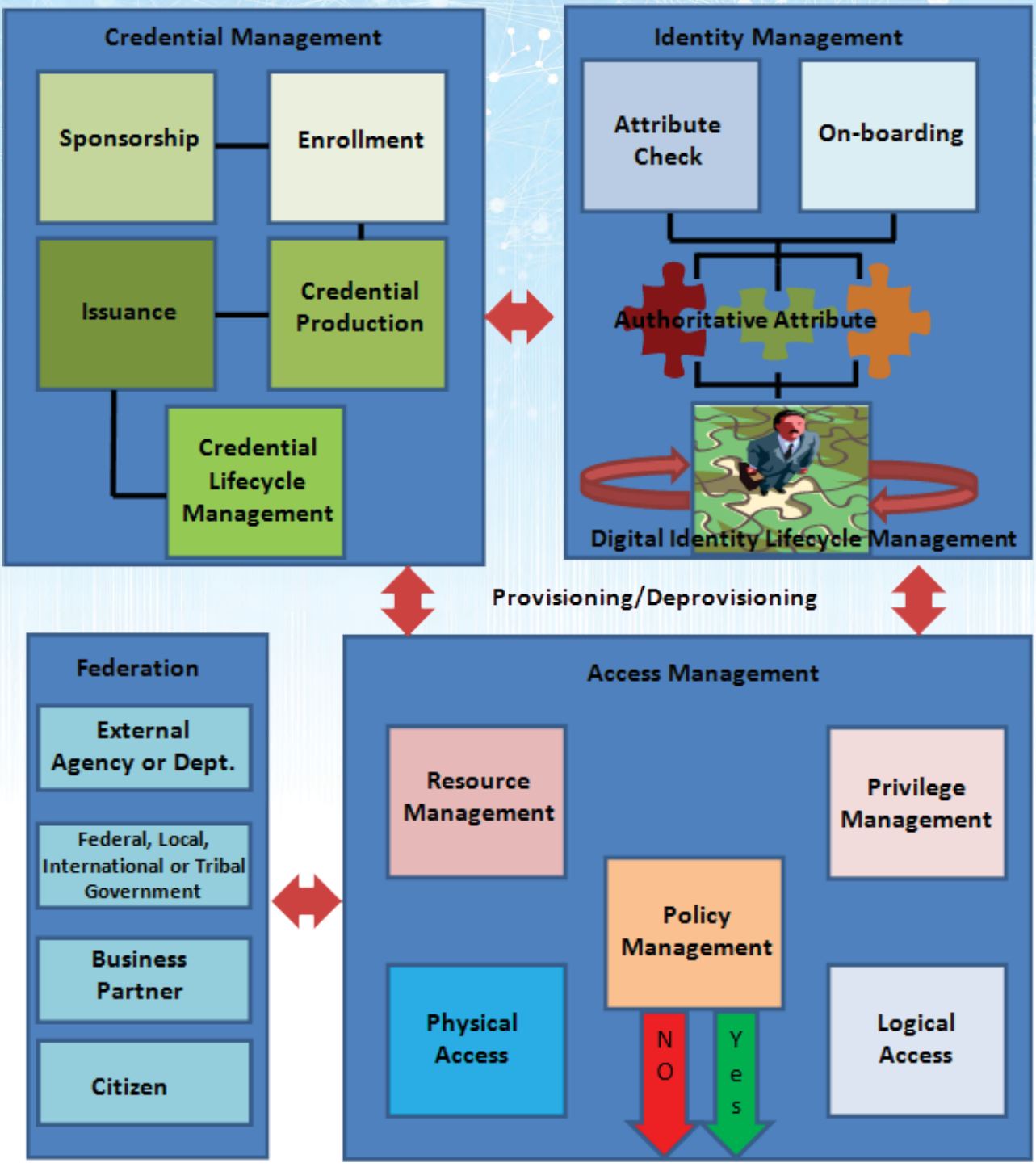
5. SICAM ARCHITECTURE FRAMEWORK

Development of the SICAM Architecture Framework provides the rules and definitions necessary for the integration of information and services at the conceptual design level. The framework combines business and environment processes and represents the roadmap for the implementation of the SICAM solution.

For agencies to become integrated as part of a federated framework, systems will need to address architectural elements to adapt and fit within the architectural framework of SICAM. Standards-based deployment is critical and a key to success. After business issues are addressed, agencies must ensure that the technology being deployed is non-proprietary and standards-compliant. The predominant standard for identity federation is the Security Assertion Markup Language (SAML), and the current version being 2.0. This protocol was developed through the input and extensive real-world experience of hundreds of major deployments and dozens of the leading vendors in the industry. SAML is an XML-based open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). It should be noted that there are other standards for communication being used such as SOAP.

The SICAM Architecture Framework focus for identity federation fits within a larger framework of a shared services model. In the context of identity federation, states can offer a service that validates identity information. The DMV for instance can validate citizen identity information or the state could validate business entity information which may include employee information. Figure 5 illustrates this framework for states, but note that there would also be an auditing and reporting function for each process.

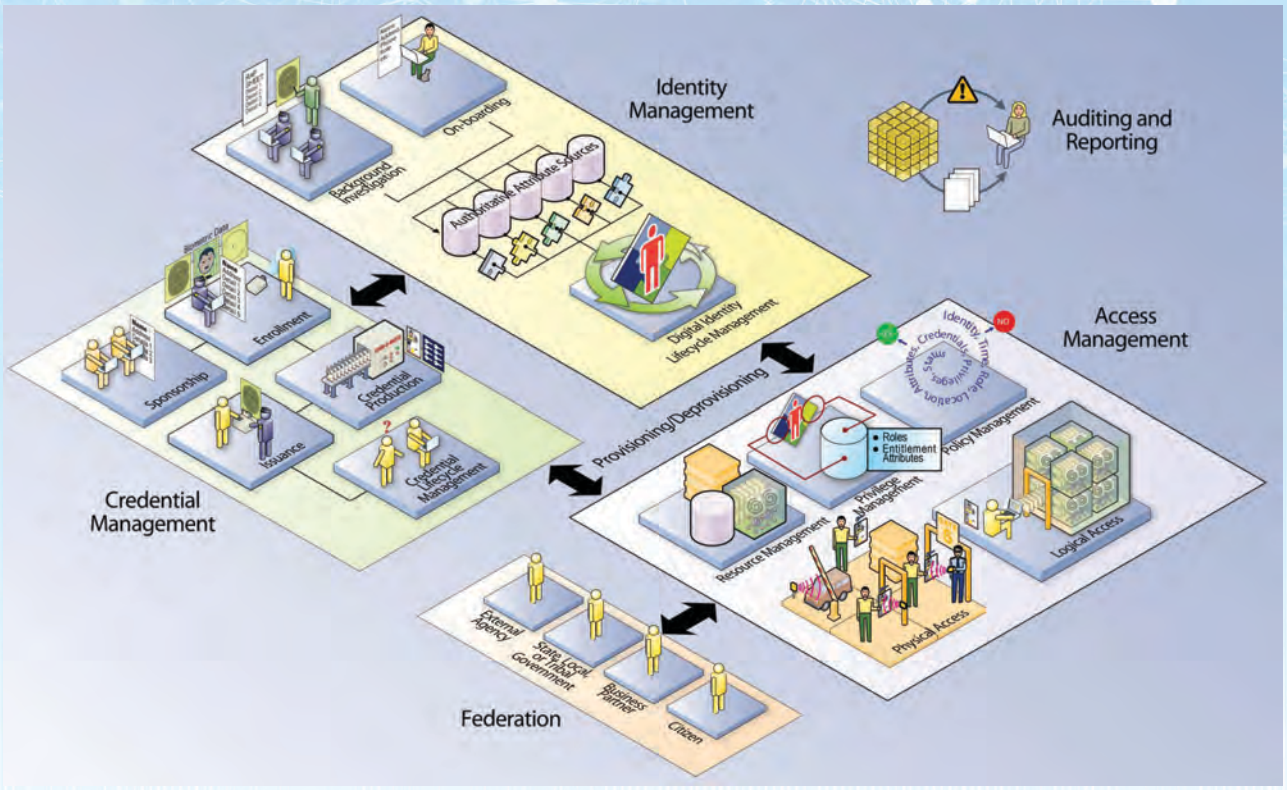
Figure 5: Targeted SICAM Architecture Framework



5.1 ICAM Architecture Framework Target

The architectural overview in Figure 6, which is part of the FICAM Roadmap and Implementation Guidance, illustrates a federated government framework that provides centralized services to citizens, business, employees, and other government entities that span state, local and federal jurisdictions. It illustrates how government entities can share services across independent information technology domains and federation with states.

Figure 6: Example of the Targeted Architecture from the FICAM Roadmap



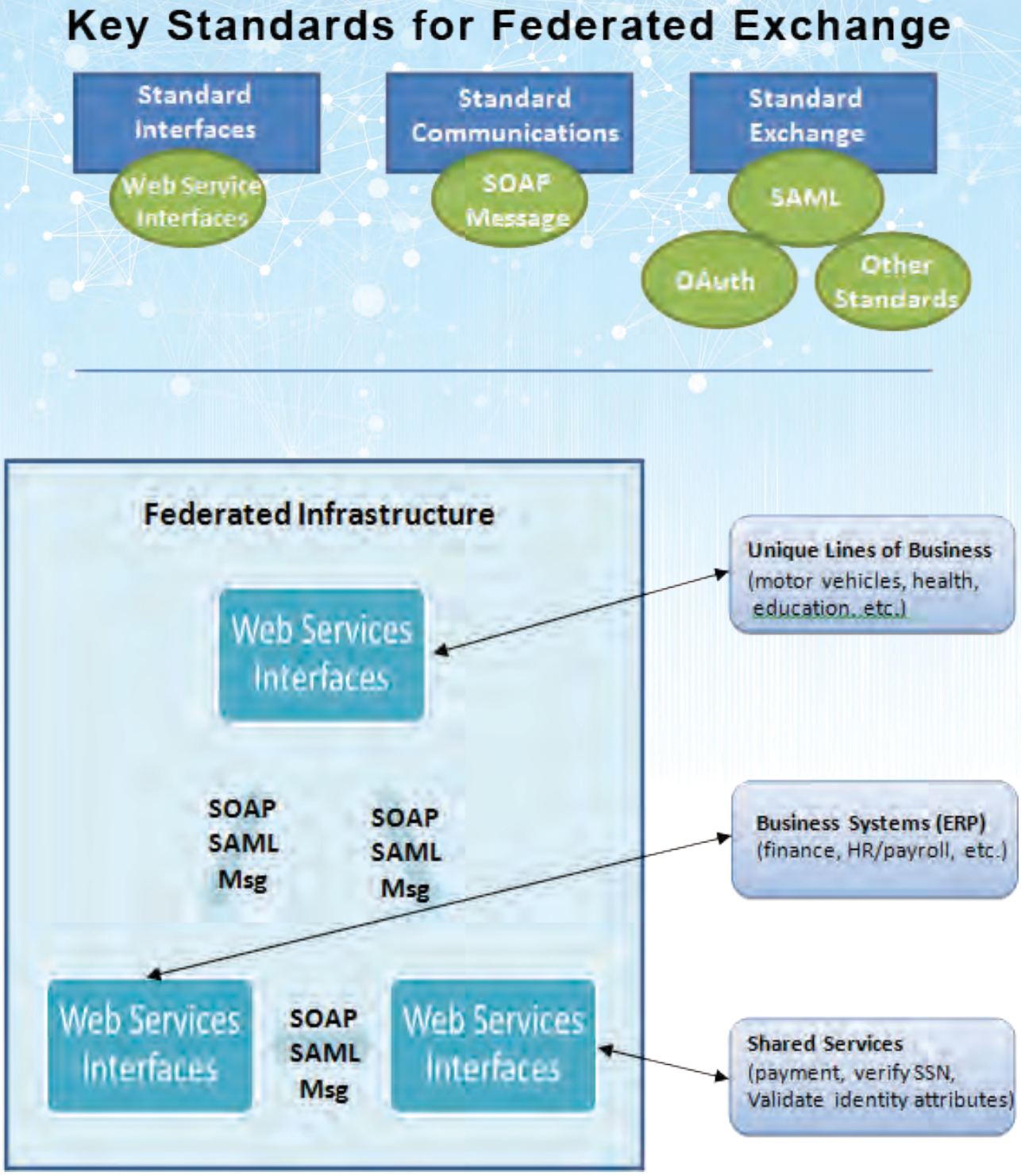
Stakeholders would have an opportunity to connect through portal web pages or interact through shared federated government services. Here is one scenario for end state use:

> A citizen could connect through a state portal to obtain access to resources or benefits from a government entity. During this process (enrollment), the citizen would be asked a series of questions to identify who they are (proofing). The questions may be based on credentials that the citizen holds that were issued to them from a government entity. The federated system would be used during this process to interact with other departments within the federated system (vetting). In this scenario, the federated system would provide identity validation before the citizen was granted access to the resources or benefits.

5.2 Key Standards for Federated Exchange

In a federated exchange there is a need to be able to exchange data across disparate systems using common language. Figure 7 illustrates the key standards and how they interact in a federated services environment.

Figure 7: Key Standards for Federated Exchange

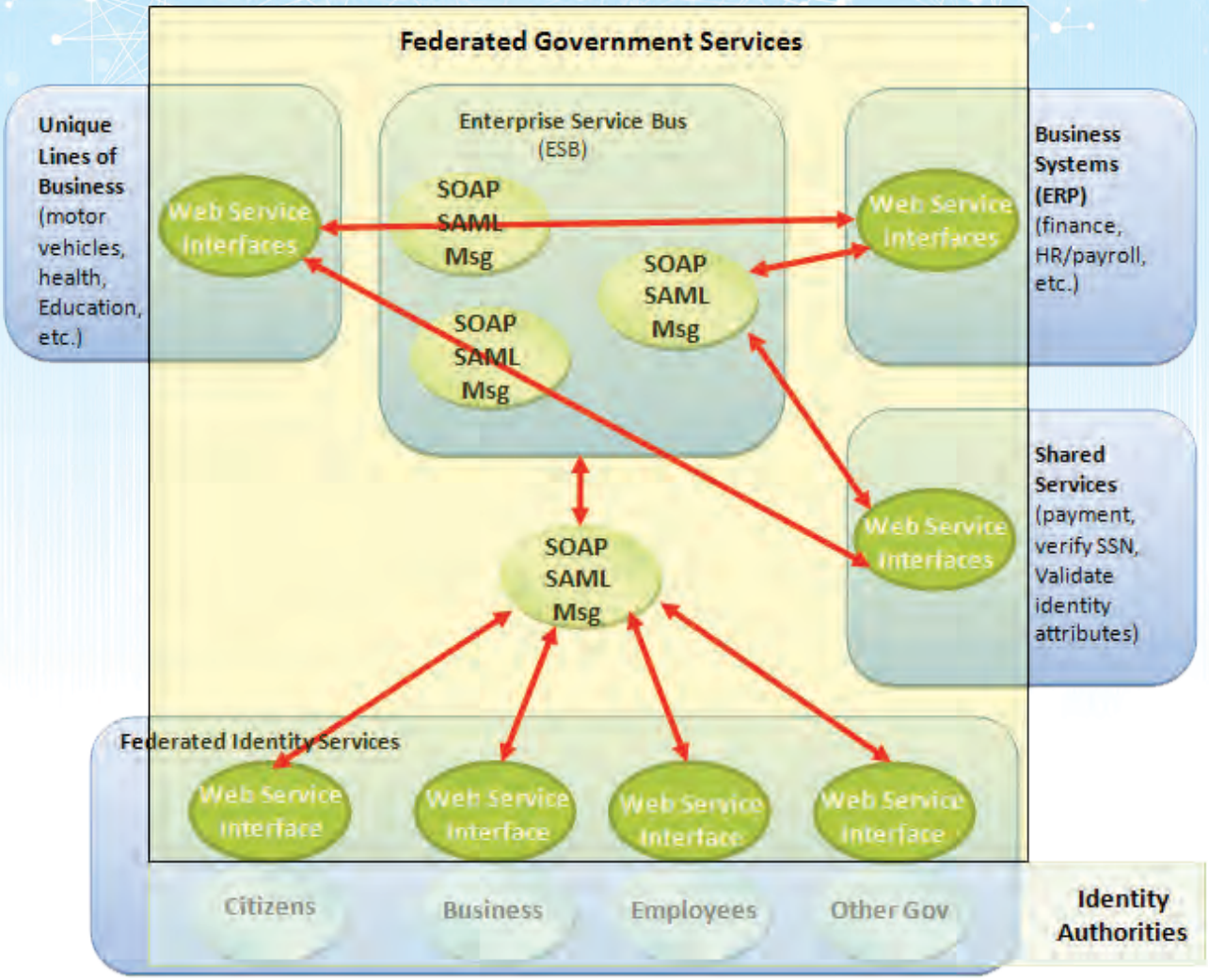


Standards such as Web Service for service interaction, the Simple Object Access Protocol (SOAP) for message format, and the Security Assertion Markup Language (SAML) for security exchange are established as the state standards for identity federation. This is critical for ensuring the proliferation of interoperable technologies and seamless integration for the federated organization.

5.3 Message and Identity Management

The primary focus and direction of the state is to leverage approved open standards for messaging and identity within the federated system. Since there will likely be a variety of disparate government systems interacting within the federated organization, this places even more importance on establishing acceptable use of open standards for messaging and identity.

Figure 8: Message & Identity Management

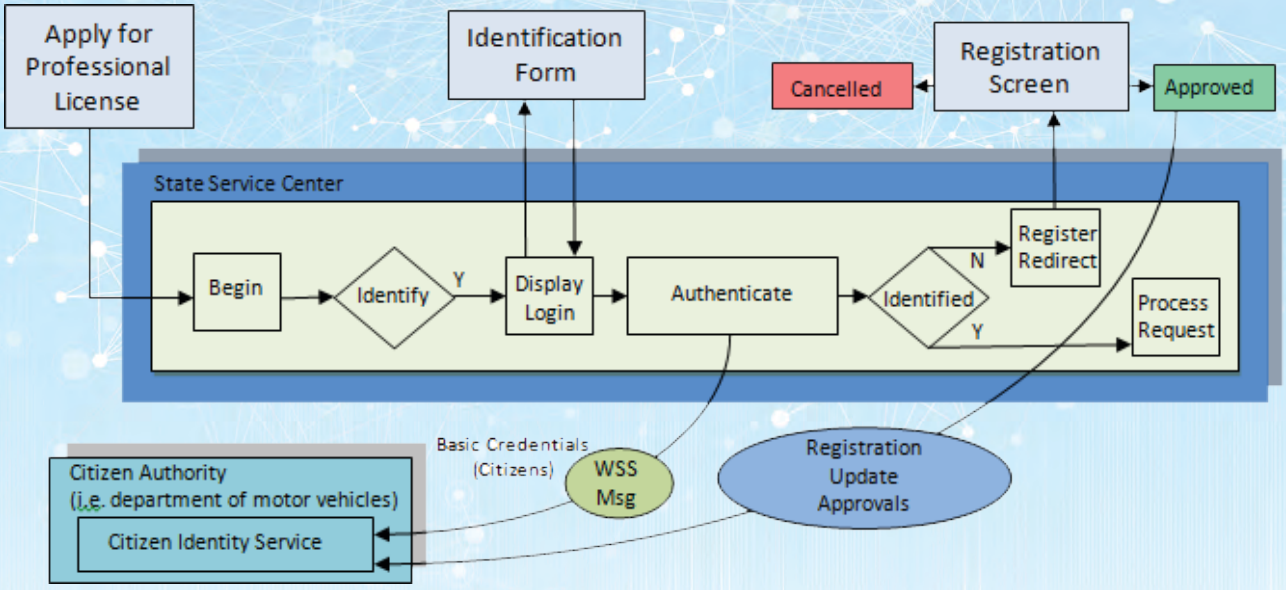


The combination of service, message, and identity standards provides the opportunity to federate multiple governmental services. Infrastructure to support these standards will align with the size and cultural autonomy of the organization.

5.4 Authentication (Citizen Application for a License)

Figure 9 illustrates specifics regarding the interaction between government services, messaging and identity authentication.

Figure 9: Authentication Model

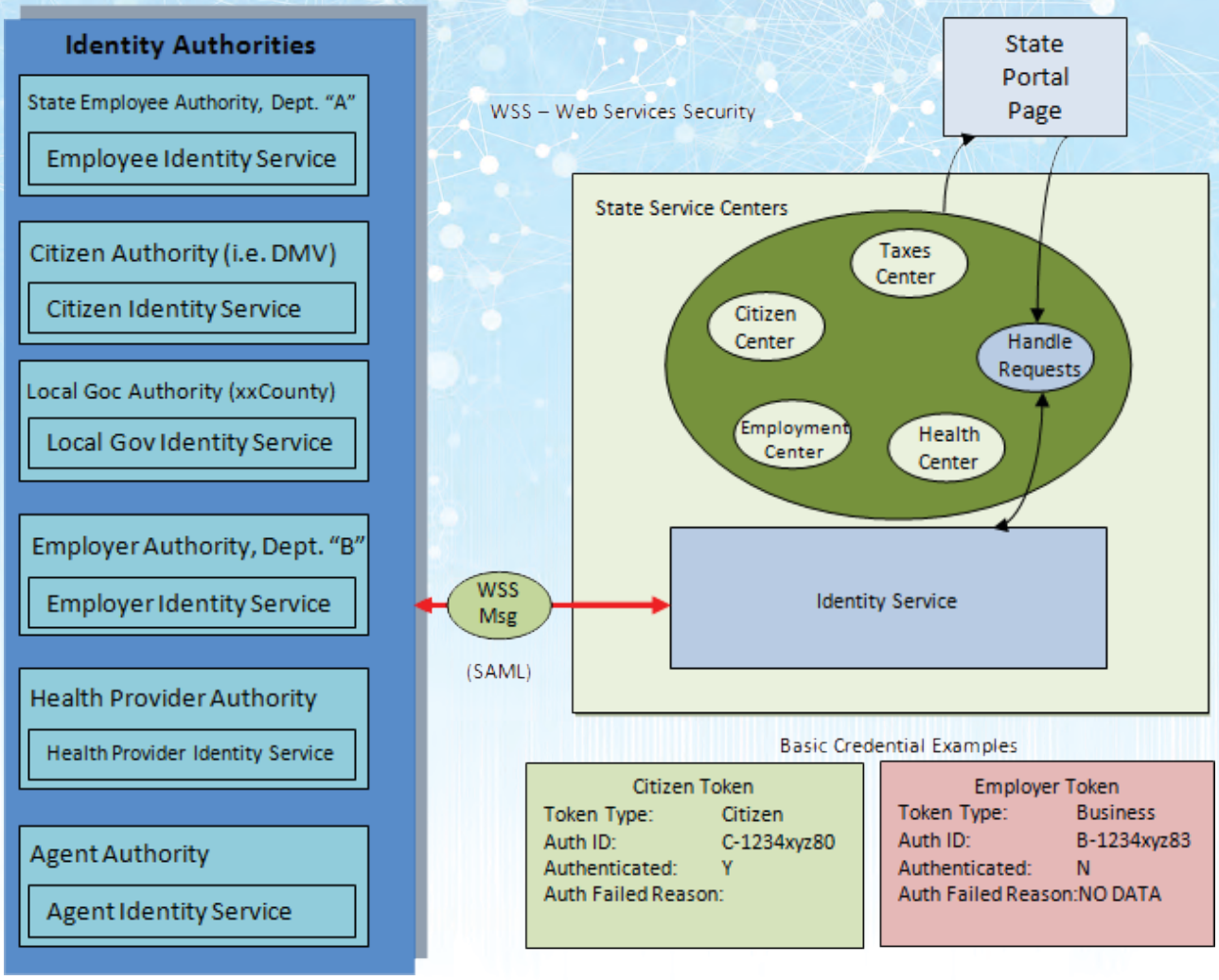


As shown above, the citizen is applying for a professional license through a state web portal. This is where the message flow behind the online screen begins and the identity of the citizen is authenticated through a citizen identity service. If there is a confirmed identity, the process flow continues which leads to the processing of the license. If an identity match does not occur, then a registration process is initiated that allows the citizen to validate and store their identity attributes in the citizen identity service.

5.5 Identity Attributes

In a federated environment, a single entity or individual can have multiple attributes. Attribute based security concepts support this fact. In Figure 10, a state shared service center federates across multiple governmental services. In doing so, it must establish the attributes of the identity requesting actions from the services center.

Figure 10: Identity Attributes



The figure above shows how the citizen token contains different attributes than an employer token even though it could be the same individual. The identity service has the ability to establish identity and attributes on an inbound request. This makes for an authorized and secure message being sent to the federated service providers. The service provider would also validate identity and attributes within their domain and may even prompt for more attributes if needed.

6. APPROACH TO IMPLEMENTATION

In this section, we will outline a few key strategies for meeting the targeted framework for SICAM. This section will also outline how interoperability will occur to share identity attributes across agency boundaries in an effort to reduce the total cost of ownership for agency identity systems and to improve the identity assurance levels for agencies that leverage these services.

States, as the holders of great amounts of personal information about its citizens, employees, and businesses, are responsible for protecting the privacy of that information. The following Fair Information Practice Principles should be adopted to enhance privacy throughout the SICAM infrastructure:

- **Transparency:** Organizations should be transparent and provide notice to the individual regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation:** Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification:** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation:** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity:** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security:** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

6.1 Risk-Based Approach

Participants are governed by the agreed upon federation rules but granted the flexibility to establish additional layered agreements with other participants and within communities of interest. Rather than requiring all participants to adopt a high-security model, this approach allows the various participants to make a risk-based decision to determine with whom they want to interact.

6.1.1 Risk Assessment

Improper authentication of users can result in direct and dire consequences to an application, system, and organization. This approach emphasizes the development of authentication requirements based on risk. It is designed to approach the task from a business process owner perspective, identify organization risk, and then match those risks to the appropriate technical solution. This is accomplished through a risk assessment for each transaction. The assessment identifies:

- Risks
- Likelihood of Occurrence

Appendix G outlines the steps agencies should take to conduct a risk assessment of the e-government system and includes the following:

1. Analyze Data Security Classification
2. Assess Impact
3. Assess Likelihood
4. Calculate Risk Rating
5. Determine Security Level

From the risk assessment, agencies can then determine the appropriate assurance level for the data or transaction in question, as well as appropriate levels of identity proofing and related authentication technologies.

To determine the appropriate level of assurance in the user's asserted identity agencies must assess the potential risks and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

1. Potential Harm or Impact
2. The Likelihood of Such Harm or Impact

6.2 Determine Assurance Level

Transactions, processes, and/or information will be classified by the information owner based on its value, sensitivity, consequences of loss or compromise, and/or legal and retention requirements. An appropriate assurance – or trust - level for user credential and authentication must be assigned and implemented to protect the integrity and confidentiality of the information and validity of transactions.

Assurance Levels	
Level	Description
1	Little or no confidence in the asserted identity's validity
2	Confidence exists that the asserted identity is accurate
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

The four trust levels are:

Compare the impact profile (security level) from the security level assessment to the impact profiles associated with each assurance level, as shown in the table on the following page. Map the potential impacts defined in the security level assessment to the four trust levels (1, 2, 3, 4). This will identify the level (1-4) of trust required. For example, the "financial loss or agency liability" category has a security level rating of "high". This translates to a Level 4 Assurance.

Appendix A -	Appendix B - Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Additional security controls (audit logging, access right, data validation and verification controls, etc.) should also be implemented for higher trust levels. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment.

6.2.1 Assurance Level Guidelines

In analyzing potential risks, the agency must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms-to-agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.

Associated authentication requirements will be based on the information classification along with any other requirements of the information or transaction being processed. Authentication technologies are determined – and credentials are assigned to users – based on the level of assurance/trust required by the sensitivity of the information and the nature of the transaction.

6.3 Determine Identity Proofing Requirements

The registration and identity proofing process is designed, to a greater or lesser degree depending on the assurance level, to ensure that the state and/or credential provider knows the true identity of the applicant. Specifically, the requirements include measures to ensure that:

1. A person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
2. The applicant whose token is registered is in fact the person who is entitled to the identity;
3. The applicant cannot later repudiate the registration; therefore, if there is a dispute about a later authentication using the subscriber's token, the subscriber cannot successfully deny he or she registered that token.

The following text establishes registration requirements specific to each level. There are no level-specific requirements at Level 1. Both in-person and remote registration are required for Levels 2 and 3. Explicit requirements are specified for each scenario in Levels 2 and 3. Only in-person registration is permitted at Level 4. Detailed level-by-level identity proofing requirements are stated in Appendix H: Identity Proofing Requirements by Assurance Level.

A credential is evidence attesting to one's right to a privilege or authorization. Credentials can take multiple forms, depending on the transaction, business process, and method of access (remote or in-person). Applicants are to be vetted to the minimum requirements before the appropriate assurance level is assigned and the corresponding credential issued.

State may impose additional vetting requirements such as conducting national background checks, checking criminal history records, terrorist watch lists, legal immigration status, and credit history. While these additional checks may be needed to meet specific state requirements, they have no additional bearing on the assigned proofing level or designated assurance level. Additionally, in some contexts, states may choose to use additional knowledge-based authentication methods to increase their confidence in the registration process.

Once an entity has gone through registration, vetting, proofing and issuance, the assurance level is stored as a user attribute in the state system. Any additional checks required by the state will also be maintained in the agency system. The personal information used to vet the identity is to conform to all appropriate legislation governing the storage of personal data.

The sensitive data collected during the registration and identity proofing stage must be protected at all times (e.g., transmission and storage) to ensure its security and privacy. Additionally, the results of the identity proofing step (which may include background investigations of the applicant) have to be protected to ensure source authentication, confidentiality and integrity.

Further reference material from NIST:
• NIST 800-63 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

6.3.1 Use of Anonymous Credentials

Unlike identity authentication, anonymous credentials may be appropriate to use to evaluate an attribute when authentication need not be associated with a known personal identity. To protect privacy, it is important to balance the need to know who is communicating with the Government against the user's right to privacy. This includes using information only in the manner in which individuals have been assured it will be used. It may be desirable to preserve anonymity in some cases, and it may be sufficient to authenticate that:

- The user is a member of a group; and/or
- The user is the same person who supplied or created information in the first place; and/or
- A user is entitled to use a particular pseudonym.

These anonymous credentials have limited application and are to be implemented on a case-by-case basis. Some people may have anonymous and secure identity credentials. Anonymous credentials are appropriate for Levels 1 and 2 only. The National Strategy for Trusted Identities in Cyberspace (NSTIC), released by the White House in April of 2011, focuses on voluntary participation with minimal disclosure for those who would like to remain anonymous.

Further reference material on the NSTIC can be found at:

- Full NSTIC Strategy Document http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
- NSTIC Program Management Office http://www.nist.gov/nstic/npo.html

6.4 Authentication Technology Selection

All State systems will authenticate the identity of any user prior to allowing any access. All users will be identified to the system by a credential, comprising of the following classification steps:

- Unique user-ID; and
- Method of authentication.

The level of authentication will be commensurate with the sensitivity of the information being accessed. It is not in this document's scope to specify which types of authentication technologies to use, but instead, to provide recommendations and guidelines to assist agencies in determining how to choose the right technology(ies) for their application(s).

This section starts with an overview of the Federal E-Authentication model and the process of authentication, then provides an overview of various types of tokens and the appropriate token type to use based upon the assurance level determined in the risk assessment. Authentication rules must be automatically enforced by the system being accessed.

6.4.1 E-Authentication Model

In accordance with [OMB 04-04], e-authentication is the process of establishing confidence in user identities electronically presented to an information system. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. In most cases, the authentication and transaction take place across an open network such as the Internet; however, in some cases access to the network may be limited and access control decisions may take this into account.

E-authentication begins with registration. An applicant applies to a Registration Authority (RA) to become a Subscriber of a Credential Service Provider (CSP) and, as a subscriber, is issued or registers a secret, called a token, and a credential that binds the token to a name and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events.

The subscriber's name may either be a verified name or a pseudonym. A verified name is associated with the identity of a real person and before an applicant can receive credentials or register a token associated with a verified name, he or she must demonstrate that the identity is a real identity, and that he or she is the person who is entitled to use that identity. This process is called identity and is performed by an RA that registers subscribers with the CSP. At level 1, since names are not verified, names are always assumed to be pseudonyms. Level 2 credentials and assertions must specify whether the name is a verified name or a pseudonym. This information assists relying parties, that is, parties who rely on the name or other authenticated attributes, in making access control or authorization decisions. Only verified names are allowed at levels 3 and 4.

In this document, the party to be authenticated is called a claimant and the party verifying that identity is called a verifier. When a claimant successfully demonstrates possession and control of

a token in an on-line authentication to a verifier through an authentication protocol, the verifier can verify that the claimant is the subscriber. The verifier passes on an assertion about the identity of the subscriber to the relying party. That assertion includes identity information about a subscriber, such as the subscriber name, an identifier assigned at registration, or other subscriber attributes that were verified in the registration process (subject to the policies of the CSP and the needs of the application). Where the verifier is also the relying party, the assertion may be implicit. In addition, the subscriber's identifying information may be incorporated in credentials (public key certificates) made available by the claimant. The relying party can use the authenticated information provided by the verifier/CSP to make access control or authorization decisions.

Authentication simply establishes identity, or in some cases verified personal attributes (for example the subscriber is a U.S. citizen, is a first responder, or is assigned a particular number or code by an agency or organization), not what that identity is authorized to do or what access privileges he or she has; this is a separate decision.

Relying parties, typically government agencies, will use a subscriber's authenticated identity and other factors to make access control or authorization decisions. In many cases, the authentication process and services will be shared by many applications and agencies, but the individual agency or application is the relying party that must make the decision to grant access or process a transaction based on the specific application requirements. These guidelines provide technical recommendations for the process of authentication, not authorization.

Further reference material:

- OMB M-04-04 http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

6.4.2 Federated Identity Management & Authentication

Federated identity management is the use of trust relationships, or frameworks, between separate security domains (organizations) to provide appropriate and secure, seamless authentication for users. This enables organizations to be more agile and efficient while improving user productivity and reducing overhead. It is a long-term goal of the state to implement a federated identity management approach and trust model to enable assurance and authentication of external entities in order to:

- mitigate security and privacy risks by developing trust relationships with communities of interest;
- control costs and risks by eliminating the need for each agency to create and maintain a separate credentialing system for each online application;
- facilitate e-Government services in a meaningful way.

6.4.3 Authentication Systems

Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a voice print or other biometric data)

Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors. The system may be implemented so that multiple factors are presented to the Verifier, or some factors may be used to protect a secret that will be presented to the Verifier. For example, consider a hardware device that holds a cryptographic key. The key might be activated by a password or the hardware device might include a biometric capture device and uses a biometric to activate the key. Such a device is considered to effectively provide two-factor authentication, although the actual authentication protocol between the Verifier and the Claimant simply proves possession of the key.

Tokens are characterized by the number and types of authentication factors that they use. For example, a password is a token that is something you know, a biometric is something you are, and a cryptographic identification device is something you have. Tokens may be single or multi-factor tokens as described below:

- Single-factor token – a token that uses one of the three factors to achieve authentication. For example, a password is something you know, and can be used to authenticate the holder to a remote system.
- Multi-factor token – a token that uses two or more factors to achieve authentication. For example, a private key on a smart card that is activated via PIN is a multi-factor token. The PIN is something you know and the smart card is something you have.

6.5 Attribute Management

An identity attributes service plays an important role in statewide identity services federation. User attributes can carry authorization information for states to use within their applications. Attribute exchange and validation across state systems to define their security policies and application entitlement services. Even though an authorization service must be managed inside each state's security domain, cross-domain federation amongst states through centralized statewide identity management system provides a certain level of attributes exchange and attributes validation which is the key capability of the attribute service. Security policies must be provided to protect the attributes which contains sensitive or privacy information. State privacy policy or FIPPS must be followed in any attribute exchange and validation practice. End-to-end security solutions must be provided to the attribute service to meet the security and privacy requirement of states.

6.5.1 User Attribute Service at Department and Agency Level

While the SICAM Guidance and Roadmap encourages an enterprise approach to IdM, if a department or agency maintains its own identity service it should include a user attribute management service. The department or agency specific authoritative user attributes can only be retrieved or validated from the department or agency based on the trust model and security measures. The department or agency attribute service must provide a standard based attribute retrieval and validation service to other departments or agencies based upon the configured trust agreements established with other departments or agencies.

The department or agency user attribute management process must be fully integrated with department or agency identity management solution which provides an identity life cycle management solution that effectively manages the user attribute creation, change, and deletion. The department or agency IDM solution must enforce the authenticity of the attributes through its business process in order to provide an authoritative attribute service to other departments or agencies.

6.5.2 User Attribute Service at State Level

The centralized statewide identity service is responsible for ID validation and rationalization across the state and also issuing statewide unique identifiers for individuals. The centralized statewide identity services provide registration service to employees and password token registration service for citizens. The state maintains a centrally correlated user registry. Certain user attributes are maintained in this registry, for example, the unique identifier, and stateissued unique ID's, basic information about the user, and biometric information about the individual. When needed, the centralized statewide identity services must be able to provide user attributes or validate user attributes from the central user registry in a trusted and secure manner. States must ensure, through a secure manner, that privacy is also adhered to and the personally identifiable information of citizens is not breached or used for unintended purposes.

6.5.3 Establish mechanisms and infrastructure for attribute retrieval / exchange

Attributes can be retrieved and exchanged through different mechanisms based on the protocols that the state centralized identity system have leveraged.

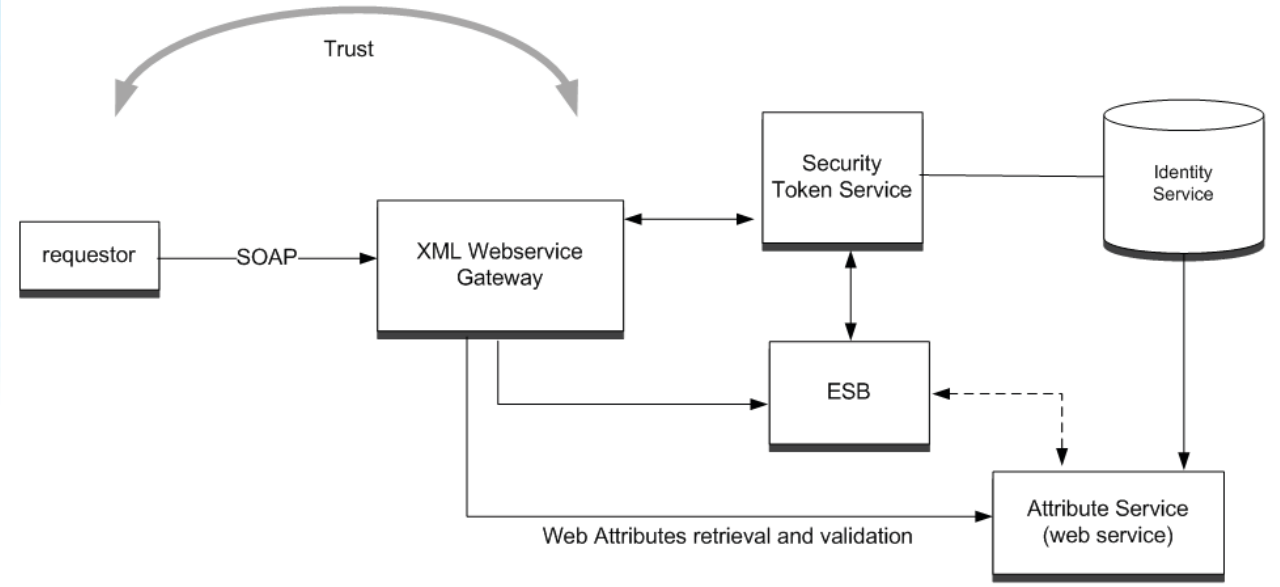


Figure 11: Attribute Service Architecture

6.5.4 Via Backend Attribute Exchange (BAE) SAML profile (through web service)

States should consider a standard mechanism for relying parties to obtain information (backend attributes) directly from the authoritative source (attribute authority). The authoritative source is the state centralized identity service provider. Access to backend attributes is either in real-time, when immediately needed (e.g., guard suspects token tampering), or in advance under certain circumstances. In addition to those with credentials, individuals who only have a password token to access a state resources that may require further information or information validation from an authoritative source. This is typically the state that manages the individual's profile. The standard approach to retrieve or validate the attributes needs to be established within state sites as well.

BAE is a general concept pertaining to exchange of information in a secure and trusted environment between an attribute authority and a SAML 2.0 service provider. The Security Assertion Markup Language (SAML) based exchange of backend attributes for one credential per request/response pair. The same attribute exchange mechanism should apply to generic individuals who have other form of credentials. The attributes supported in the states central identity system and departments or agencies must be defined to support the existing credential attributes. The unified attribute service with standard interface provides the following functions to all trusted parties in states:

1. Attribute Service is a web service component with a published WSDL. It can be optionally integrated with state ESB and has to comply with the state web service security policy.
2. The requestor must have a trust relationship with the attribute service based on the trust model defined in SICAM. All attribute service invocations must be validated, audited before the service is provided.
3. Attribute service must comply with SAMLV2.0 Request/Response Protocol [SAML2Core] for attribute retrieval.
4. Attribute service must comply with The SAML2.0 profile of XACMLv2.0 [XAC-SAML] for attribute validation. It is highly desired that a state has the capability to provide attribute validation, instead of attribute retrieval due to privacy issue.

For more information on SAML please visit: http://www.oasis-open.org/committees/security

6.5.5 Establish State Level Attribute Classification

The attributes which are collected, maintained, and exposed as part of a user lifecycle management process are specific to the business requirements of the state. This section describes several examples of user types and attributes classification on those users which dictate the storage and sharing of user attribute information within the statewide identity services trust framework. User attribute information is comprised of both publically available as well as sensitive PII information. There are three types of attributes which should be considered when defining the attribute classification for user information. These types are listed below.

1. Basic – The attributes reflects the basic information about the user. These attributes can be shared amongst states and can be used for identity data correlation. These attributes can be retrieved through trusted attribute service
2. Intermediate – The attributes are unique to the business of states and can be shared among certain states based on business agreement and trust model. In most cases, these attributes can only be validated through attribute service. However, in some business transactions, they can be retrieved from the state through trust attribute service.
3. Advanced – These are highly private attributes which are stored in state identity registry. These attributes are only used in state and should never be shared with other states without user's consent.

There are several different types of users which are maintained by the state. This includes employees, first responders, and citizens as well as many other types of users.

6.6 Governance

Governance is crucial for promoting interoperability, federation and emphasizing the benefit of identity management. The governance section identifies key details and considerations in establishing a state governance framework for SICAM. Additionally, this section highlights legislative and policy directives that give rise to the need for development and support of SICAM infrastructure and processes to support the state's missions.

The SICAM roadmap should evolve as states incorporate it within their specific EA. Any changes to the plans, projects, and/or reference agency's architecture should be captured in an appropriate documentation trail, and should be justified on the basis of costs, benefits, and risks. Changes should be processed through established change control processes and board authority. The change documentation should characterize the problem, solution, and alternatives chosen and rejected in light of established priorities. The federated identity management model is based on a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.

Furthermore, it is an architectural style for a community of providers and consumers of services to achieve mutual value, that:

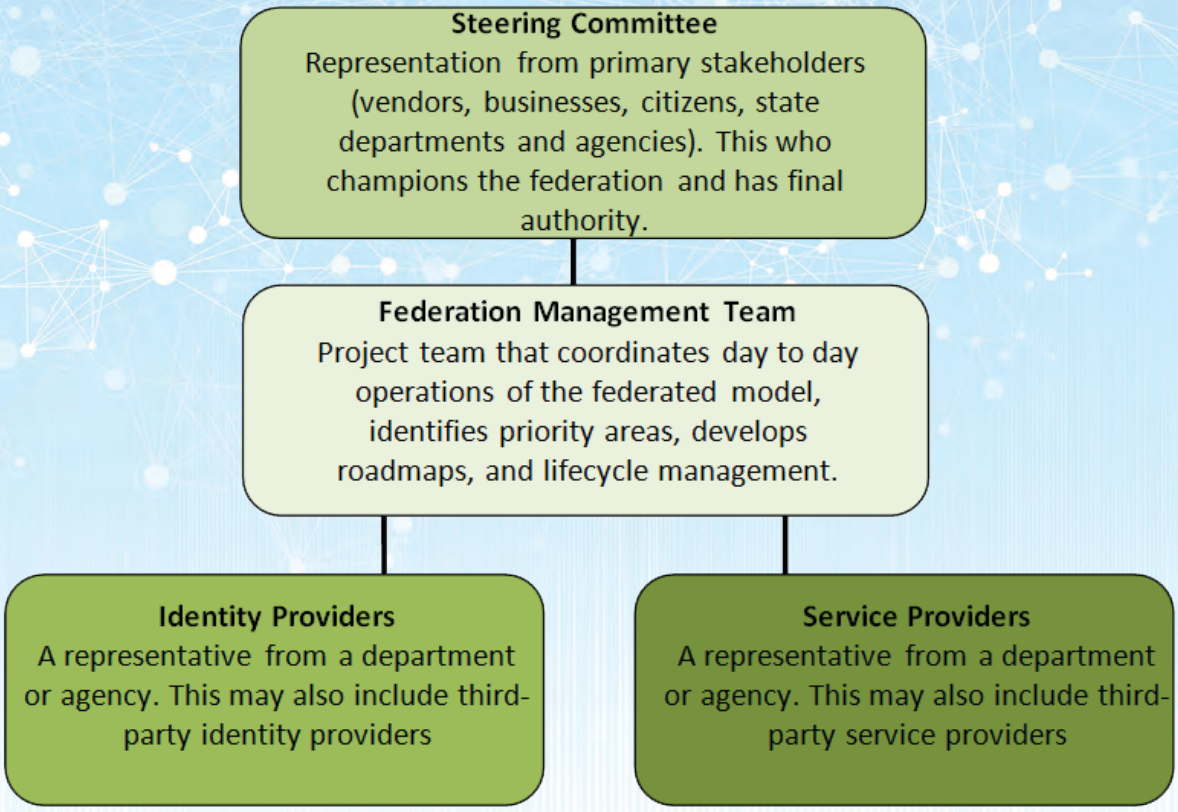
1. Allows participants in the trust ecosystem to work together within a common process framework, but also in a technology independent environment
2. Specifies the areas of agreement to which organizations, people and technologies must adhere in order to participate in the trust ecosystem
3. Provides for business value and business processes to be realized by the community
4. Allows for a variety of technologies to be used to facilitate interactions within the community
5. Outlines policies and procedures for non-compliance by any participating entity

Effective operations of such a model for the state would require a high level of coordination between various states systems under a governance model compatible with objectives and design of SICAM.

6.6.1 Establish Governance Authority

On the following page is a high-level organizational structure example for establishing a federated identity governance authority. This example is based on the GIFPM governance model, but adjustments have been made to reflect specific state organizational designs – this gives an example of how there might only be a handful of identity providers and other entities will act as service providers.

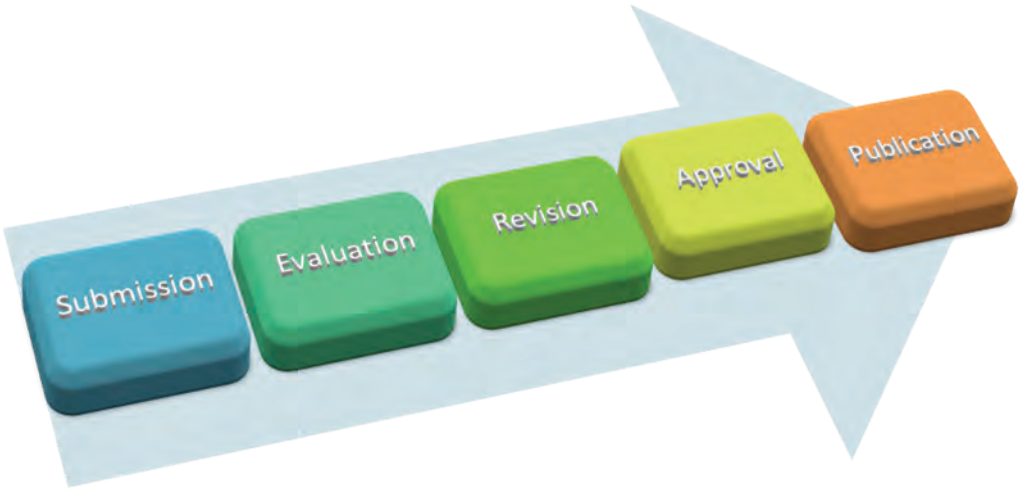
Figure 12: High Level Perspective on Establishing Federated Identity Governance



6.6.2 Manage Lifecycle of Common Specifications and Standards

The management of common specifications and standards consists of five high level processes represented in Figure 13 below.

Figure 13: Lifecycle Maintenance Process



- Submission – states submit revisions/modifications to the reference model(s) to the Federation Management Office (FMO) for consideration.
- Evaluation – The FMO collects, reviews, and screens the submissions based on standardized evaluation criteria.
- Revision – The FMO forms a team to perform analysis and develop the revised model.
- Approval – The Steering Committee reviews the final version for publication.
- Publication – The FMO publishes the revision.

Governance Entity	Role
Steering Committee	▪ Charter the Enterprise Architecture and Standards Committee ▪ Ensure alignment with the information technology strategic plan
Federation Management Office (FMO)	▪ Review and approve reference model revisions ▪ Collaborate with other committees to ensure alignment and consistency with the Enterprise Architecture policy, review, and evaluate the submissions based on standardized evaluation criteria ▪ Form team(s) to perform analysis and develop the revised SICAM Model ▪ Review and revise the SICAM ▪ Publish the revision(s)
Department or Agency– Identity Provider / Service Provider	▪ Serve as submitters of potential modifications to the reference models ▪ Supply subject matter experts ▪ Provide feedback on reference model revision(s)

Management of attributes on the local domain level (within each state department or agency) and cross-domain level (under the SICAM governance model) requires a governance process. Management of these attributes and artifacts associated with them is one of the key elements of the federated identity governance model.

6.6.3 Establish Identity Provider and Security and Privacy Certification, On-boarding and Membership Process

Part of the SICAM framework is to identify a process for a state's to apply for identity provider certification. A state that manages a specific population of identities should be able to apply and be considered an authority for these identities. Part of the process of establishing the new identity provider is to identify the business reason and validate the value of contribution to these identities from the service provider perspective. In other words, a state that can provide or validate certain attributes associated with identities should be allowed to become an identity provider only if a specific business case exists and there is a demand from the service provider community to consume these identities.

This process can be formalized by a Federation Management Office and evaluation criteria will need to be established by the steering committee to evaluate prospective identity providers. A typical process for partaking in the federated identity management consists of the following steps:

1. Request-to-Join Process
2. Application Process
3. On-boarding Process
4. Ongoing Membership

For example, the GIFPM framework describes the following content of application to join packaged required to be completed by each identity provider candidate.

The identity provider application package consists of the following contents:

a) **Completed Application Form** – a standard form on which an organization provides basic organization information about itself, e.g. name, address, names, and titles of its organizational officers, etc.

b) **Signed IDP Agreement** – an agreement signed by an IDP to indicate its intent and willingness to abide by the governance and rules of the Federation

c) **Authority-to-Operate Document** – a document attesting to the organization's authority to operate as an identity provider for users under a specific legal jurisdiction

d) **Local Security Policy Document** – a document describing the security policy that is currently in place within the organization

e) **Local User Agreement Document** – a document describing the terms and conditions to which users must agree as a prerequisite for using a digital identity issued by the organization

f) **Local User Vetting Policies & Procedures Document** – a document describing the user vetting policies and procedures that are currently in place within the organization

g) **Completed Local Attribute Mapping Form** – a document describing how the organization plans to map its local policies and locally stored user attributes into attributes conforming to interoperable standards.

h) **Completed Security Practices Checklist Form** – a checklist that summarizes the organization's local security policy. The checklist is for informational purposes only and applicants are not required to be compliant with all items on the checklist.

Similar to the certification to operate as an identity provider within the SICAM framework, various states should be able to apply for service provider certification. The process of justifying why a states should act as service provider can be simplified (ability to handle more service providers) when compared to vetting of identity providers.

A standard process of joining as a service provider in the GIFPM governance framework consists of the following steps:

a. **Completed Application Form** – a standard form on which an organization provides basic organization information about itself, e.g. name, address, names, and titles of its organizational officers, etc.

b. **Signed SP Agreement** – an agreement signed by an SP to indicate its intent and willingness to abide by the governance and rules of the Federation

c. **Authority-to-Operate Document(s)** – a set of documents attesting to the organization's authority to operate as a service provider and make available electronic resources belonging to, or under the legal control of, a specific legal jurisdiction

d. **Local Security Policy Document** – a document describing the security policy that is currently in place within the organization

e. **Completed Local Access Policy Mapping Form** – a document describing how the organization plans to map its local access control policies into rules that can be expressed using attributes from the GFIPM Metadata standard

f. **Completed Security Practices Checklist Form (based on FIPS 200)** – a checklist that summarizes the organization's local security policy. The checklist is optional –applicants are not required to be compliant with all items on the checklist.

6.6.4 Token Acceptance Policy

After a state has performed a risk analysis, it can then choose technologies to support the appropriate security and risk level. States should determine technology based on the risk analysis, cost, and balancing this delicate equation in a way that will not fiscally burden the state.

6.6.5 Trust Policies

Trust policies need to be implemented to enable trust in an ecosystem of numerous identity providers, service providers, and relying parties. State policies will need to be developed for:

- Governance for establishing a digital identity.
- Who can provide identity proofing?
- What levels of assurance are needed and how can the risk analysis benefit setting standards and policy functions?
- Establishing roles in an enterprise that equate to types of information that can be accessed, which helps inform the types of technology tokens and security controls that need to be implemented.
- What are the attributes needed for transition types by relying parties in order to trust the identity? With this concept, we recognize that a person only has one identity, but can have multiple attributes and privileges (e.g., driver, voter, receiver of benefits, employee, first responder, patient) assigned to her or him. The assigning of attributes assigned will remain with the state programs that are serving individuals.
- Use of a policy engine to electronically enforce all necessary federal and state statutes.

6.7 Maintenance

The SICAM roadmap should evolve as states incorporate it within their specific EA. Any changes to the plans, projects, and/or reference agency's architecture should be captured in an appropriate documentation trail, and should be justified on the basis of costs, benefits, and risks.

Changes should be processed through established change control processes and board authority. The change documentation should characterize the problem, solution, and alternatives chosen and rejected in light of established priorities.

The preferred method by which the registration authority will evolve and mature for use throughout reference agencies is Communities of Practice (CoP). These CoP's provide an environment where the community or users of the architecture are empowered or own the maturity of the model. These CoP's may decide to meet face to face, via internet, or other collaborative means. The use of a wiki provides the single source owner and approval processes by evaluating community input and real life experiences. This tool can be used in the evolution and adaptation as constant change is addressed. With each community (reference agencies) providing input and feedback to their best practices, the overall model of identity management can be assessed on a regular basis (at least annually) and grow into the appropriate and expected target architecture. Much like the reference models, the reference architecture will mature with changes as feedback and lessons learned are provided.

Individual organizations, on the other hand, will maintain their architecture within the enforcement structure and configuration control mechanisms as with any EA. Using a system of oversight processes and independent verification, the reference agency architecture team will periodically assesses and align their specific identity management architecture to the ever-changing business practices, funding profiles, and technology insertions.

The successful maturity of each agency's identity management enterprise architecture should continuously reflect the current state (baseline architecture), the desired state (target architecture), and the long-and short-term strategies for managing the change (the sequencing plan). At no time will specific target architectures ever be achieved with each iterative update of the EA, all three components shown in the figure and the timeline are recast. The target architecture is a vision of the future that evolves in advance of it being achieved.

6.8 Communication Strategy

Like any complex project, program, activity or task, there must be solid communications. This is accomplished through a communications plan. This plan will (1) keep senior executives and business leaders continually informed, and (2) disseminate EA information to management teams as appropriate. The CIO staff, in cooperation with the Chief Architect and support staff, defines a communications plan consisting of (a) constituencies, (b) level of detail, (c) means of communication, (d) participant feedback, (e) schedule for marketing efforts, (f) working groups, and (g) method of evaluating progress and buy-in. It is the CIOs role to interpret the state vision and to recognize innovative ideas (e.g., the creation of a digital government) that can become key drivers within the EA strategy and plan. If resources permit, the Chief Architect should use one or all of the following tools to communicate with the community of interest: seminars and forums, web pages, electronic surveys, and e-mail list servers.

To meet these general information needs, the Identity Management Reference Architecture Program will implement the following communications tools.

1. The Program will develop a set of basic information materials describing the scope of the statewide Enterprise Architecture. This set of materials will describe the value, benefits, and importance of Enterprise Architecture. The materials will be brief and concise, and may consist of one of the following: one-page briefing or brochure, key concept map,

Frequently-Asked Questions (FAQ) document, and PowerPoint presentation.

2. In all status reporting, Committee and Program achievements will be explicitly linked to government-wide business objectives.
3. The basic EA scope and value materials, as well as some high-level business-oriented status information, will be available (and prominently displayed) on an EA website, be it SharePoint, Wiki, or other collaboration tool. These materials should be suitable for use/delivery by EA Committee members as well as program staff.
4. Other means used will be used, such as, phone conferences, online collaboration meeting tools, wiki engines, and the internet, to name a few.

The communications plan will also identify stakeholders of the reference agency, the information needs of those stakeholders, and the communication strategy to be followed by the reference EA program in meeting those needs. The enterprise architecture and the operations of the program charged with evolving that architecture are important topics of communication that must be addressed by the program if the enterprise architecture initiative is to succeed.

6.9 Architecture Compliance Process

The architecture compliance function will be implemented according to state EA Policy and standards. The annual evaluations should cover:

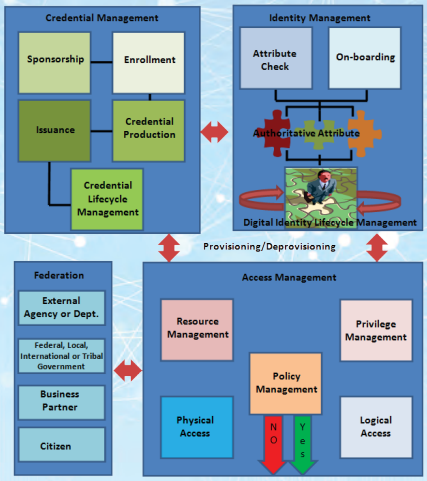
1. Business Performance, as per SICAM maturity model measurement areas
2. Technical Alignment with Enterprise and Agency-level Standards
3. Architecture Alignment

The data collected within the business performance area will be used for reporting to state CIOs. The remaining portions of the evaluation will be used by internal staff. The compliance function will empower the governing body to lead the state EA program to drive momentum towards the agreed upon goals.

States that do not make progress or remain compliant may have funds frozen or may be asked to outsource their identity management capability. In most cases, however, the assessment should be used to align investments with SICAM needs and to update the EA models.

7. CONCLUSION

The SICAM Guidance and Roadmap is a development framework, illustrating basic enterprise architecture methodologies and approaches for implementing an enterprise ICAM solution. It contains templates to be used in the process and samples of real cases, which were compiled from the input of several state and local representatives.



There are many steps along the way and an organization may find that not all of the areas fit neatly within the lines of this document. Maturity within the architecture framework will vary across the business architecture processes, technology architecture, as well as the architecture blueprint. This is an evolving process for states and will lead to an efficient, effective responsive development and support organization for identity and access management solutions.

It is through the architecture frameworks and framework elements that the SICAM provides state and local governments the means to apply adaptive enterprise architecture, which aids in a structured and consistent delivery of services and information. Enterprise Architecture is a key success factor to an organizations ability to plan and react to the many mandates and challenges presented to states. We encourage you to use all the tools developed under NASCIO's guidance and can access publication at the following link http://www.nascio.org/publications/.

APPENDIX A - ACRONYMS

Acronym	Description
AAES	Authoritative Attribute Exchange Service
ADS	Authoritative Data Source
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BAE	Backend Attribute Exchange
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CIO	Chief Information Officer
CRL	Certificate Revocation List
CSP	Credential Service Provider
CVS	Clearance Verification System
DA	Data Administrator
DBMS	Database Management System
DOB	Date of Birth
EA	Enterprise Architecture
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
GUI	Global Unique Identifier
HR	Human Resources
IAFIS	Integrated Automated Fingerprint Identification System
IAM	Identity Access Management
ICAM	Identity, Credential & Access Management
ID	Identification
IDMS	Identity Management System
IDP	Identity Provider
ISE	Information Sharing Environment
LACS	Logical Access Control Systems
LRA	Local Registration Agent
NCES	Net-Centric Enterprise Services
NIEM	National Information Exchange Model
NIST SP	National Institute of Standards and Technology Special Publication

APPENDIX A - ACRONYMS (CONT.)

Acronym	Description
NPE	Non-Person Entity
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
RP	Relying Party
SP	Service Provider

APPENDIX B - GLOSSARY

Many of the technical definitions below are abstracted from the OASIS Glossary of terms at:
https://www.oasis-open.org/glossary/index.php
The Liberty Alliance Project's Liberty Technical Glossary Version: v2.0 is available at:
http://projectliberty.org/liberty/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files/liberty_glossary_v2_0/

Term	Definition
(AAA)	Three system functions that are the underpinning of a security service: authentication recognizes the user; authorization enforces access controls and delivers services; accounting tracks users' usage of system resources.
Adjudication	Evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: ▪ suitable for State Government employment; ▪ eligible for logical and physical access; ▪ eligible for access to classified information; ▪ eligible to hold a sensitive position; or ▪ fit to perform work for or on behalf of the State Government as a contractor employee.
Adjudicator	Provides adjudication of background check information to determine eligibility of the applicant to receive a credential, access rights, or be able to work for the State Government as an employee or contractor.
Administrative Domain	An environment or context that is defined by some combination of one or more administrative policies, Internet Domain Name registrations, civil legal entities (for example, individuals, corporations or other formally organized entities), plus a collection of hosts, network devices and the interconnecting networks (and possibly other traits), plus (often various) network services and applications running upon them. An administrative domain may contain or define one or more security domains. An administrative domain may encompass a single site or multiple sites. The traits defining an administrative domain may and, in many cases will, evolve over time. Administrative domains may interact

Term	Definition
	and enter into agreements for providing and/or consuming services across administrative domain boundaries.
Administrative Domain	An environment or context that is defined by some combination of one or more administrative policies, Internet Domain Name registrations, civil legal entities (for example, individuals, corporations or other formally organized entities), plus a collection of hosts, network devices and the interconnecting networks (and possibly other traits), plus (often various) network services and applications running upon them. An administrative domain may contain or define one or more security domains. An administrative domain may encompass a single site or multiple sites. The traits defining an administrative domain may and, in many cases will, evolve over time. Administrative domains may interact and enter into agreements for providing and/or consuming services across administrative domain boundaries.
Affiliation	In Liberty, an affiliation is a set of one or more entities, described by provider ID's, who may perform Liberty interactions as a member of the set. An affiliation is referenced by exactly one affiliation ID and is administered by exactly one entity identified by their provider ID. Members of an affiliation may invoke services either as a member of the affiliation (using affiliationID) or individually (using their provider ID). Affiliation and affiliation group are equivalent terms.
Affiliation ID	In Liberty, an Affiliation ID identifies an affiliation. It is schematically represented by the affiliation ID attribute of the <AffiliationDescriptor> metadata element.
Applicant	Individuals that request issuance of a credential or access to an application. An applicant becomes a credential holder after issuance and a user after being granted access to an application.
Application Administrator	The party responsible for the maintenance and implementation of access control rights. Application Administrators should not be the approvers due to separation of duties.
Asserting Party	Formally, the administrative domain that hosts one or more

Term	Definition
Assertion	A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject or authorization permissions applying to the subject with respect to a specified resource. As used in Liberty, assertions typically concern things such as: an act of authentication performed by a Principal, attribute information about a Principal or authorization permissions applying to a Principal with respect to a specified resource.
Attribute	A distinct characteristic of an object (in SAML, of a subject). An object's attributes are said to describe it. Attributes are often specified in terms of physical traits, such as size, shape, weight and color, etc., for real world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address and so on. Which attributes of an object are salient is decided by the beholder. See also XML attribute.
Attribute Assertion	An assertion that conveys information about attributes of a subject.
Attribute Authorities	An entity recognized as having the authority to verify the association of attributes to an identity.
Attribute Authority	A system entity that produces attribute assertions.
Authentication	To confirm system entities asserted principal identity with a specified, or understood, level of confidence.
Authentication Assertion	An assertion that conveys information about a successful act of authentication that took place for a subject. In the Liberty specification suite, an authentication assertion contains a <lib:AuthenticationStatement>. Note that the foregoing element is defined in a Liberty namespace. Also known as Liberty authentication assertion and IDFF authentication assertion. Liberty authentication assertions are formal XML extensions of SAML assertions.
Authentication Authority	A system entity that produces authentication assertions. In the Liberty architecture, it is typically an identity provider (synonymous with authenticating identity provider or authenticating IdP). An identity provider that authenticated a Principal Authentication, Authorization and Accounting Services
Authentication Credential	A type of authenticator possessed by a user that provides a strong mechanism used to prove the credential holder's identity. Examples include a PKI certificate or a PIV card.

Term	Definition
Authenticator	A memory, possession, or quality held by a person that can serve as proof of identity when presented to a verifier.
Authoritative Attribute Exchange Service (AAES)	Service that performs discovery and mapping of attributes from authoritative source repositories.
Authoritative Data Source	The repository or system that contains the data and attributes about an individual that are considered to be the primary source for this information. If two systems with an individual's data have mismatched information, the authoritative data source is used as the most correct.
Authorization	The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access.
Authorization Decision	The result of an act of authorization. The result may be negative: that is, it may indicate that the subject is not allowed any access to the resource.
Authorization Decision Assertion	An assertion that conveys information about an authorization decision.
Authorizer	Approves or denies access to applications or facilities based on business rules.
Bearer token	In Liberty, a bearer token is a form of security token that connotes some attribute(s) to its holder. Typically bearer tokens connote identity and they consist essentially of credentials of some form, e.g. SAML assertions.
Binding, Protocol Binding	An instance of mapping SAML requestresponse message exchanges into a specific protocol. Each binding is given a name in the pattern "SAML xxx binding".
Biometrics	A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
Board of Directors	This is the executive level body with representation from primary stakeholders that guides the federation and is the final authoritative body to make decisions for the federation.
Card Management System	An application that manages the issuance and administration of multi-function enterprise access smart cards. The CMS manages cards, as well as data, applets and digital credentials, including PKI certificates related to the cards throughout their lifecycle.

Term	Definition
Cardholder/Credential Holder	An individual possessing an issued token, PKI certificate, PIV Card or other authentication device.
Certificate Revocation List (CRL)	A composite list of all expired and revoked certificates issued from a CA that can be used to verify the current status of a PKI certificate.
Certificate Status Servers	The counterpart to the Certification Authority that passes revocation and expiration status to relying parties in real time.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
Circle of Trust (CoT)	A federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment. Also known as a Trust Circle.
Citizen	A citizen for purposes of this document, is strictly used to describe a human inhabitant within the State, whether or not they are considered a legal citizen and/or entitled to rights or services provided by the State.
Clearance Verification System (CVS)	A State repository for authorized personnel to determine whether an appropriate background investigation has been performed.
Core Identity Attributes	Attributes that are specific to an individual and, when aggregated, uniquely identify a user within and across agency systems. Core Identity Attributes are also the list of attributes that agencies must make available to one another to enable federation of identity records.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Credentialing Determination	Determination of whether or an individual is eligible to receive a PIV credential as either a State employee or contractor.
Data Administrator (DA)	An individual responsible for maintaining an organization's data and establishing relationship between authoritative data repositories. The individual may also be an application administrator responsible for managing local data.
Digital Identity	The representation of Identity in a digital environment.

Term	Definition
Discoverable	A discoverable "in principle" service is one having a service type URI assigned (this is typically in done in the specification defining the service). A discoverable "in practice" service is one that is registered in some discovery service instance. IDWSF services are by definition discoverable "in principle" because such services are assigned a service type URI facilitating their registration in Discovery Service instances.
Discovery Service (DS)	An IDWSF service facilitating the registration, and subsequent discovery of, IDWSF service instances. See also discoverable.
Domain Controller	The server(s) that manages passwords and authentication requests for a set of applications.
E-Authentication Assurance Level (EAAL)	Evaluation categories by which authentication mechanisms are measured based on NIST SP 800-63. The lowest level assurance is 1; the highest level assurance is 4.
Enrollment Officer	The individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind an Applicant to his/her biometric, and validate identity documentation. The Enrollment Officer delivers a secured enrollment package to the IDMS for adjudication.
External Identity Provider (IDP)	A service or system that establishes an individual's identity and links the identity to a physical or electronic credential or token. IDP's validate the identity of the individual using the credential or token issued and pass along verification of the individual's identity to a relying party, usually through a SAML assertion. Within this Use Case, External IDPs are agency systems, other than the agency performing the validation. External IDP's are those systems or services that are not directly controlled or managed by the agency.
External System or Third Party Application	Resources maintained and operated by a separate state agency, the private sector, or another third party outside of the agency.
External User	Any individual attempting or requesting access to agency facilities or systems that is not an employee, contractor, or primary affiliate of the agency. External users may be PIV holders from another agency, business partners, or private citizens.
Federation	A trust model formed among a collection of Identity Providers and Service Providers spanning multiple department organizational boundaries.

Term	Definition
Federation Management	This is the body that manages the day-to-day operations of the Federation, including developing and maintaining standards, membership coordination and providing executive secretariat services to the Board of Directors.
Federation to Federation	The establishment of an inter-federation trust model between like and unlike federations.
Global Federated Identity and Privilege Management (GFIPM) framework	An initiative that provides the justice community and partner organizations with a standards-based approach for implementing federated identity management using the concept of globally understood metadata. GFIPM utilizes direct trust across participating agencies.
Government-to-Business (G2B)	G2B is the online non-commercial interaction between local and central government and the commercial business sector, rather than private individuals.
Government-to-Citizen (G2C)	G2C is the electronic interaction between citizens, or private individuals and government resources
Government-to-Government (G2G)	G2G is the electronic interaction between Federal, State, City, County, and tribal Government agencies.
ID*	A shorthand designator referring to the Liberty IDWSF, IDFF and IDSIS specification sets. For example, one might say that the former specification sets are all part of the Liberty ID* specification suite. ID* fault message – A SOAP <S:Fault> element containing a <Status> element, with the attributes – and attribute values of both elements configured as specified herein or as specified in other specification(s) in the IDWSF or IDSIS specification sets.
ID* message	Equivalent to ordinary ID* message.
Identifier	A representation (for example, a string) mapped to a system entity that uniquely refers to it.
Identity	The essence of an entity. One's identity is often described by one's characteristics, among which may be any number of identifiers.
Identity	The unique biological person defined by DNA; the physical being.
Identity Management (IdM)	The combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguard of personal identity information.

Term	Definition
Identity Management System (IDMS)	An automated system of hardware (servers) and software (programs) that provides the workflow management (services) of identity functions, as normatively described in FIPS 201. An IDMS is separately layered and/or compartmentalized within one system and/or a modular component of an agency's centralized system/enterprise. The IDMS will be encapsulated in an environment that is secure, auditable and protect the privacy of personal information. The IDMS establishes the centralized Chain-of Trust that is then integrated into the components of a FIPS 201 compliant enterprise.
Identity provider (IdP)	A Liberty enabled system entity that manages identity information on behalf of Principals and provides assertions of Principal authentication to other providers.
Identity Providers	An entity that vets individuals, collects attributes about these individuals, maintains these attributes in an accurate and timely manner. The IDP performs user authentication each time an individual presents themselves to the federation and assigns the current attributes about the individual for a given information technology session. These attributes are presented to Service Providers in the Federation or on a federation to federation basis.
Identity service	In Liberty, an abstract notion of a web service whose operations are indexed by identity.
IDFF	The Identity Federation Framework (IDFF) is the title for a subset of the Liberty specification suite which defines largely HTTP based protocols for web single signon and identity federation.
IDPP	The "ID Personal Profile" is an IDSIS – based service which can provide profile information regarding Principals, typically subject to policy established by those Principals.
IDSIS	Liberty Identity Service Interface specification set. IDSIS based services are identity services typically built on IDWSF.
IDWSF	Liberty Identity Web Services Framework specification set. An IDWSF based service is an identity service that is at least discoverable in principle and is based on the Liberty specifications for SOAP bindings and security mechanisms.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Term	Definition
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information use by an agency. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources provided by the agency, or outside service providers on behalf of the agency.
Integrated Automated Fingerprint Information System (IAFIS)	A national fingerprint and criminal history system maintained by the FBI, Criminal Justice Information Services (CJIS) Division that provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.
Internal Actors	Individuals (users, applicants, credential holders, etc.) that primarily consist of employees and contractors of an agency, but also include any fellows, interns, researchers or other individuals tightly affiliated with an agency. These are users who have a primary affiliation to the agency, and for whom the agency typically collects digital identity records and provides credentials for access to agency IT resources or buildings.
Internal/Agency/Local Application or System	A logical system, software or other application in which access is controlled by a particular agency. Internal systems are those hosted, managed, or otherwise controlled by the agency. These systems may only be available within the agency networks and behind agency firewalls.
Investigative Service Provider (ISP)	An entity responsible for collecting and processing personal investigative data, performing various checks, and providing investigative results to the requesting agency.
Investigator	An authorized individual who performs background investigations on behalf of an Investigative Service Provider.
Issuer	The entity that issues a credential to the Applicant after all identity proofing, background checks, and related approvals have been completed, especially for, but not limited to, PIV and PKI credentials.

Term	Definition
Markup Language	A set of XML elements and XML attributes to be applied to the structure of an XML document for a specific purpose. A markup language is typically defined by means of a set of XML schemas and accompanying documentation. For example, the Security Assertion Markup Language (SAML) is defined by two schemas and a set of normative SAML specification text.
Ordinary ID* message	A Liberty Identity Web Services Framework (IDWSF) or Service Interface Specification (IDSIS) message. It is designed to be conveyed by essentially any transport or transfer protocol, notably SOAP. It is also known among the ID* specifications as a service request or an IDWSF (service) request or an IDSIS (service) request.
Policy Decision Point (PDP)	A system entity that makes authorization decisions for itself or for other system entities that request such decisions. For example, a SAML PDP consumes authorization decision requests and produces authorization decision assertions in response. A PDP is an "authorization decision authority".
Policy Enforcement Point (PEP)	A system entity that requests and subsequently enforces authorization decisions. For example, a SAML PEP sends authorization decision requests to a PDP and consumes the authorization decision assertions sent in response.
Principal	A system entity whose identity can be authenticated. In Liberty usage, Principal is usually synonymous with a "natural person". A Principal's identity may be federated. Examples of Principals include individual users, groups of individuals, organizational entities, e.g., corporations, or a component of the Liberty architecture.
Principal Identity	A representation of a principal's identity, typically an identifier.
Privacy	In Liberty, proper handling of personal information throughout its life cycle, consistent with the preferences of the subject.
Profile	In SAML, a set of rules describing how to embed assertions into and extract them from a framework or protocol. Each profile is given a name in the pattern "xxx profile of SAML". In Liberty, a profile is data comprising attributes that may be maintained on behalf of a system entity (usually a Principal), over and beyond its various identifiers. At least some of this information (for example, addresses, preferences, card numbers) is typically provided by the Principal.

Term	Definition
Provider	A entity that performs one or more of the provider roles in the Liberty architecture – for example service provider or identity provider.
Relying Party	A system entity that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving assertions from an asserting party (a SAML authority) about a subject.
Requester, SAML Requester	A system entity that utilizes the SAML protocol to request services from another system entity (a SAML authority, a responder). The term "client" for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML requester is architecturally distinct from the initial SOAP sender.
Resource	a) Data contained in an information system (for example, in the form of files, information in memory, etc). b) A service provided by a system. SAML refers to resources by means of URI references.
Responder, SAML Responder	A system entity (a SAML authority) that utilizes the SAML protocol to respond to a request for services from another system entity (a requester). The term "server" for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML responder is architecturally distinct from the ultimate SOAP receiver.
Rights Expression Language (REL)	In Liberty, a Rights Expression Language facilitates the expression of who are the "rights holders" for a resource, who is authorized to use a resource and their applicable permissions, and any constraints or conditions imposed on such permissions. They also may express "rights entities" and "rights transactions".
SAML Authority	An abstract system entity in the SAML domain model that issues assertions. See also attribute authority, authentication authority, and policy decision point (PDP).
Security	A collection of safeguards that ensure the confidentiality of information, protect the systems or networks used to process it and control access to them. Security typically encompasses the concepts of secrecy, confidentiality, integrity and availability. It is intended to ensure that a system resists potentially correlated attacks.

Term	Definition
Security Architecture	A plan and set of principles for an administrative domain and its security domains that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services and the performance levels required in the elements to deal with the threat environment. A complete security architecture for a system addresses administrative security, communication security, computer security, emanations security, personnel security and physical security, and prescribes security policies for each. A complete security architecture needs to deal with both intentional, intelligent threats and accidental threats. A security architecture should explicitly evolve over time as an integral part of its administrative domain's evolution.
Security Assertion	An assertion that is scrutinized in the context of a security architecture.
Security Assertion Markup Language, SAML	The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP).
Security Domain	An environment or context that is defined by security models and security architecture, including a set of resources and set of system entities that are authorized to access the resources. One or more security domains may reside in a single administrative domain. The traits defining a given security domain typically evolve over time.
Security Policy	A set of rules and practices that specify or regulate how a system or organization provides security services to protect resources. Security policies are components of security architectures. Significant portions of security policies are implemented via security services, using security policy expressions.
Security Policy Expression	A mapping of principal identities and/or attributes thereof with allowable actions. Security policy expressions are often essentially access control lists.

Term	Definition
Security Service	A processing or communication service that is provided by a system to give a specific kind of protection to resources, where said resources may reside with said system or reside with other systems, for example, an authentication service or a PKIbased document attribution and authentication service. A security service is a superset of authentication, authorization and accounting (AAA) services. Security services typically implement portions of security policies and are implemented via security mechanisms.
Security Token	In Liberty, a security token is a collection of security related information that is used to represent and substantiate a claim. Outside of Liberty, the term "security token" often refers to hardware based devices, e.g. so called "token cards". One should not confuse the latter and the former definitions. However, it is possible for some given authentication mechanism to employ token cards in the process of authentication.
Service Providers	A federation member organization that provides one or more electronic information service(s) to the Federation. Service providers' services evaluate the set of Identity Provider attributes presented to the SP in a form that is consistent with the SICAM Interface Control Document (e.g. SAML assertion) to determine what access to provide or deny to each end user.
Session	A lasting interaction between system entities, often involving a user, typified by the maintenance of some state of the interaction for the duration of the interaction.
Simple Authentication and Security Layer (SASL)	An approach to modularizing protocol design such that the security design components, e.g. authentication and security layer mechanisms, are reduced to a uniform abstract interface. This facilitates a protocol's use of an open-ended set of security mechanisms, as well as a so called "late binding" between implementations of the protocol and the security mechanisms' implementations. This late binding can occur at implementation and/or deployment time. The SASL specification also defines how one packages authentication and security layer mechanisms to fit into the SASL framework, where they are known as SASL mechanisms, as well as register them with the Internet Assigned Numbers Authority for reuse.

Term	Definition
Site	An informal term for an administrative domain in geographical or DNS name sense. It may refer to a particular geographical or topological portion of an administrative domain or it may encompass multiple administrative domains, as may be the case at an ASP site.
SSO Assertion, Single Signon Assertion	An assertion with conditions embedded that explicitly define its lifetime and include one or more statements about the authentication of a subject. Additional information about the subject, such as attributes, may also be included in the assertion.
Subject	A principal in the context of a security domain. SAML assertions make declarations about subjects.
System Entity	An active element of a computer/network system. For example, an automated process or set of processes, a subsystem, a person or group of persons that incorporates a distinct set of functionality.
Transport Layer Security Protocol (TLS)	An evolution of the SSL protocol. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery.
Trusted Authority	In Liberty, a Trusted Third Party (TTP) which issues and vouches for assertions, otherwise known as an identity provider.
Trusted Third Party	In general, a security authority or its agent, trusted by other entities with respect to security related activities. In the context of Liberty, these other entities are, for example, Principals and service providers and the trusted third party is typically the identity provider(s) involved in the particular interaction of interest
Ultimate SOAP Receiver	The SOAP receiver that is a final destination of a SOAP message. It is responsible for processing the contents of the SOAP body and any SOAP header blocks targeted at it. In some circumstances, a SOAP message might not reach an ultimate SOAP receiver, for example because of a problem at a SOAP intermediary. An ultimate SOAP receiver cannot also be a SOAP intermediary for the same SOAP message.

Term	Definition
Uniform Resource Identifier (URI)	A compact string of characters for identifying an abstract or physical resource. URIs are the universal addressing mechanism for resources on the World Wide Web. Uniform Resource Locators (URLs) are a subset of URIs that use an addressing scheme tied to the resource's primary access mechanism, for example, their network "location".
URI Reference	A URI that is allowed to have an appended number sign (#) and fragment identifier. Fragment identifiers address particular locations or regions within the identified resource.
User	A natural person who makes use of a system and its resources for any purpose.
XML	Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.
XML Attribute	An XML data structure that is embedded in the starttag of an XML element and that has a name and a value. For example, the italicized portion below is an instance of an XML attribute: <Address AddressID="A12345">...</Address>. See also attribute.
XML Element	An XML data structure that is hierarchically arranged among other such structures in an XML document and is indicated by either a starttag and endtag or an empty tag. For example: <Address AddressID="A12345"> <Street>105 Main Street</Street> <City>Springfield</City> <State Or Province> <Full>Massachusetts</Full> <Abbrev>MA</Abbrev> </State Or Province> <Post Code="567890"/> </Address>
XML Namespace	A collection of names, identified by a URI reference, which are used in XML documents as element types and attribute names. An XML namespace is often associated with an XML schema. For example, SAML defines two schemas and each has a unique XML namespace.

Term	Definition
XML Schema	The format developed by the World Wide Web Consortium (W3C) for describing rules for a markup language to be used in a set of XML documents. In the lowercase, a "schema" or "XML schema" is an individual instance of this format. For example, SAML defines two schemas, one containing the rules for XML documents that encode security assertions, and one containing the rules for XML documents that encode request/response protocol messages. Schemas define not only XML elements and XML attributes, but also data types that apply to these constructs.

APPENDIX C - GOVERNANCE ROLES AND RESPONSIBILITIES

	Steering Committee	Federation Management Team	Identity Provider	Service Provider
Who / why?	This is the executive level body with representation from primary stakeholders that guides the federation and is the final authoritative body to make decisions for the federation	This is the body that manages the day-to-day operations of the Federation, including developing and maintaining standards, membership coordination and providing executive secretariat services to the Steering Committee.	An entity that vets individuals, collects attributes about these individuals, maintains these attributes in an accurate and timely manner. The IDP performs user authentication each time an individual presents themselves to the federation and assigns the current attributes about the individual for a given information technology session. These attributes are presented to Service Providers in the Federation or on a federation-to-federation basis	A federation member organization that provides one or more electronic information service(s) to the Federation. Service providers' services evaluate the set of Identity Provider attributes presented to the SP in a form that is consistent with the SICAM Interface Control Document (e.g. SAML assertion) to determine what access to provide or deny to each end user.
Activities/ Responsibilities		▪ Developing policies and guidelines pertaining to the definition and usage of the SICAM Metadata Specification standard for end-user attributes ▪ Implementing	▪ Identity Provider shall provide a trust model that ensures that an individual is linked to identities which have been issued, protected, and managed to	▪ Service providers shall have the capability to validate identity assertions that are submitted by the

	Steering Committee	Federation Management Team	Identity Provider	Service Provider
		approved processes for determining the membership of any new party in the SICAM ▪ Developing technical architecture and providing documents, including Interface Specifications, for technical interoperability within the SICAM ▪ Conducting day-to-day operational services, i.e., audits ▪ Defining Change Management processes for the SICAM ▪ Conducting interoperability testing of candidate commercial products, schemes or protocols ▪ Reviewing the conformance of the applicants to membership standards, including IDPs' mapping of their local policies and user attributes into SICAM standard attributes and SPs' mapping of their local access control	provide the accuracy of asserted attributes. ▪ Identity Provider shall develop and provide an authentication process by which the user provides evidence to the identity provider, who independently verifies that the user is who he or she claims to be. ▪ Identity Provider shall develop a process to periodically reevaluate the status of the user and the validity of his or her associated identity. ▪ Identity Provider shall develop a process for attribute management to ensure the timely cancellation or modification of attributes should the user's status change. ▪ Identity Provider shall develop a process for	Federation Identity Providers (IDP) as part of a service request ▪ Service providers shall have the ability to define attributes that IDPs must present for access to the service. ▪ Service providers shall have the capability to react to receipt of various requestor assertions based on the established policy. ▪ Service providers shall provide audit services and make them available upon request to the federation. ▪

	Steering Committee	Federation Management Team	Identity Provider	Service Provider
		policies into Boolean logic based on SICAM standard attributes ▪ Management and implementation of accepted SICAM standards and protocols operating within the SICAM ▪ Accountability authority and ensuring validity of the documents of the SICAM ▪ Facilitating the roles, relationships and mutual obligations of all parties operating in the SICAM ▪ Coordinate help desk efforts and provide engineering support ▪ Provide administrative support for the Board of Directors	auditing the attribute identification process, including registration activities, to ensure attributes are maintained in accordance with the process specified by that Identity Provider. Auditing must be conducted in a manner to identify any irregularities or security breaches. Audit information must be made available to the federation upon request. ▪ Identity Provider shall provide a process to assist users who have either lost or forgotten their means of authentication. ▪ Identity Provider shall adhere to the problem resolution process in SICAM Policies and Procedures Guidelines.	

APPENDIX D - SERVICE PROVIDER TRUST AGREEMENT

The GIFPM framework provides the following examples of trust agreements. They are included in GIFPM Governance Guidelines Working Draft v0.95

Source: http://it.ojp.gov/docdownloader.aspx?ddid=1079

Service Provider Agreement

In order to allow for the connection of multiple parties in an electronic information sharing trust environment, The _____ (insert federation name) Federation (—the Federation), allows for the interconnection of separately-provided identities, associated with end users, and services for those users

Therefore,
This Service Provider Agreement (the —SP Agreement) is being entered into by the Federation Management and _____ (insert authorized organization name), the Service Provider. The purpose of the SP Agreement is to memorialize the intent of the Service Provider to provide services to the Federation and for the Federation Management to allow the Service Provider access to the Federation infrastructure to unite Identity Provider end-users and the Service Provider's services.

Service Provider Role

The Service Provider agrees to provision its services in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines. These services will be accessible to Identity Provider end-users who meet the requirements of an established and documented access policy that the Service Provider has defined. Unless the Service Provider has specifically identified certain or all of the Service Provider's services as not public, the Federation may publicize the services which the Service Provider has made available to the Federation.
However, Service Providers who need to keep confidential the availability of their service(s), may specify the set of required attributes for discovery of their Services in the Federation directory of services. At all times that the Service Provider is a party to this agreement it agrees to abide by Specifically the Service Provider agrees to meet minimum security and availability standards. The Service Provider agrees to comply with any decisions made through the governance process, in accordance with the Global Federated Identity and Privilege Management Governance Guidelines

1. Service providers shall have the capability to validate identity assertions that are submitted by the Federation Identity Providers (IDP) as part of a service request.
2. Service providers shall have the ability to define attributes that IDPs must present for access to the service.
3. Service providers shall have the capability to react to receipt of various requestor assertions based on the established policy.
4. Service providers shall provide audit services and make them available upon request to the federation.

All service providers must certify that they are only providing information or services that they have legal rights to provide. Consumers of a federation service are obligated to comply with the specific service-level policies governing the appropriate use, handling, dissemination and/or destruction of the information accessed. The user obligations specified by a specific service policy is not in the scope of the Federation governance.

Federation Role
The Federation Management agrees that it will provide the Service Provider with the operational support to enable the Identity Providers' end-users and the Service Provider's services to interact. The Federation Management agrees that it will abide by the Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP] and that it will make governance decisions in accordance with GFIPM Governance Guidelines [GFIPM GOV].

Personally Identifiable Information
All Service Providers must manage their information service privacy data in accordance with their service specific privacy policies. All identity attributes received by the service provider from Identity Providers can only be used to make authorization decisions, dynamically provision accounts, and perform audit logging.

Termination
Termination of this agreement may occur for cause or for no cause. Either party may terminate this agreement, in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP], upon the occurrence of any material default of this agreement by the other party or upon 60 days notice to the other party.

Modification of Agreement
A modification of this agreement proposed by the Federation Management or by the Service Provider will not be final unless it has been agreed to by both parties and approved by the Board of Directors in writing.

Waiver
A waiver of any provision of this agreement shall not be considered a permanent waiver of such provision unless agreed to in writing by the Federation Management and the Board of Directors.

Assignment
This agreement may not be assigned, in whole or in part, by the Service Provider without the prior written consent of the Federation Management and the Board of Directors.

Severability
If any provision of this Agreement is vague or contradicts another provision in this agreement or any Federation Document, the remaining provisions of this Agreement nevertheless will continue in full force and effect without being impaired or invalidated in any way. The vague or contradictory provision will be reviewed and then clarified or corrected by the Board of Directors.

Entire Agreement
This Agreement is the entire Agreement between the parties and supersedes any and all prior oral and written agreements, commitments, understandings or communications with respect to the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by a duly authorized representative of each party.

Federation Documents
The operation of the Federation is governed by the following documents, which are incorporated into this agreement by reference:

- The Global Federated Identity and Privilege Management Governance Guidelines [GFIPM GOV] – this document defines the roles and responsibilities of the Federation, the Federation Management, the Board of Directors, Service Providers, and Identity Providers.
- The Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP] – this document details the way in which the Federation policies will be carried out.
- GFIPM Interface Control Document [GFIPM ICD] – this document details the technical interfaces required to be part of the federation.
- GFIPM Metadata Specification Package [GFIPM METADATA] – this specification package details the metadata requirements that must be used as part of the federation.

Notices

All notices, certificates, acknowledgments or other written communications required to be given under this Agreement shall be in writing and shall be deemed to have been given and properly delivered if duly mailed by certified or registered mail to the other Party at its address as follows, or to such other address as either Party may, by written notice, designate to the other.

Notice to the Federation Management shall be delivered as follows:

(insert address)_____

Notice to the Service Provider shall be delivered as follows:

(insert address)_____

The following material, which has been submitted with this agreement, is incorporated in the agreement by reference: (insert list documents)

APPENDIX E - IDENTITY PROVIDER TRUST AGREEMENT

The GIFPM framework provides the following examples of trust agreements. They are included in GIFPM Governance Guidelines Working Draft v0.95

Source: http://it.ojp.gov/docdownloader.aspx?ddid=1079

Identity Provider Agreement

In order to allow for the connection of multiple parties in an electronic information sharing trust environment, The _____ (insert federation name) Federation —the Federation□) allows for the interconnection of separately provided identities, associated with end users, and services for those users.

Preamble
This Identity Provider Agreement (the —IDP Agreement) is being entered into by the Federation Management and _____ (insert authorized organization name), the Identity Provider. The purpose of the IDP Agreement is to memorialize the intent of the Federation Management to provide access to the federation systems to Identity Provider and Identity Provider end users, and for the Identity Provider to create, maintain, and manage identities of their respective end users.

Identity Provider Role
The role of the Identity Provider is to create, maintain, secure and manage the identities of their end users; and accurately assert those identities, and attributes about those identities, only to authorized Federation Service Providers (SP) in accordance with federation technical documents. In accomplishing this role, the Identity Provider agrees that it will adhere to a documented process for the initial vetting of their end users identity, for any changes, for the removal of end users, and for the ongoing management of users attributes. At all times that the Identity Provider is a party to this agreement it agrees to abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP]. Specifically the Identity Provider agrees to meet minimum security and availability standards and at a minimum should do the following:

1. Identity Provider shall provide a trust model that ensures that an individual is linked to identities which have been issued, protected, and managed to provide the accuracy of asserted attributes.
2. Identity Provider shall develop and provide an authentication process by which the user provides evidence to the identity provider, who independently verifies that the user is who he or she claims to be.
3. Identity Provider shall develop a process to periodically reevaluate the status of the user and the validity of his or her associated identity.
4. Identity Provider shall develop a process for attribute management to ensure the timely cancellation or modification of attributes should the user's status change.
5. Identity Provider shall develop a process for auditing the attribute identification process, including registration activities, to ensure attributes are maintained in accordance with the process specified by that Identity Provider. Auditing must be conducted in a manner to

identify any irregularities or security breaches. Audit information must be made available to the federation upon request.

6. Identity Provider shall provide a process to assist users who have either lost or forgotten their means of authentication.
7. Identity Provider shall adhere to the problem resolution process in Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP].

Federation Role
The Federation Management agrees that it will provide the Identity Provider and their end users access to the federation systems. The Federation Management agrees that it will abide by the Global Federated Identity and Privilege Management Operational Policies and Procedures Guidelines [GFIPM OPP] and that it will make governance decisions in accordance with the Federated Identity and Privilege Management Governance Guidelines [GFIPM OPP].

Personally Identifiable Information (PII)
Identity Providers assert identity attribute data, including PII attributes, as necessary to meet the authorization requirements of Service Providers, for audit logs and for supporting dynamic account provisioning. IDP attributes, including PII attributes, shall 740 not be used for any other business purposes.

Termination
Termination of this agreement may occur for cause or for no cause. Either party may terminate this agreement, in accordance with the Global Federated Identity and Privilege Management Operational Policies and Procedures [GFIPM OPP], upon the occurrence of any material default of this agreement by the other party or upon 60 days notice to the other party.

Modification of Agreement
A modification of this agreement proposed by the Federation Management or by the Identity Provider will not be final unless it has been agreed to by both parties and approved by the Board of Directors in writing

Waiver
A waiver of any provision of this agreement shall not be considered a permanent waiver of such provision unless agreed to in writing by the Federation Management and the Board of Directors.
Assignment
This agreement may not be assigned, in whole or in part, by the Identity Provider without the prior written consent of the Federation Management and the Board of Directors.

Severability
If any provision of this Agreement is vague or contradicts another provision in this agreement or any Federation Document, the remaining provisions of this Agreement nevertheless will continue in full force and effect without being impaired or invalidated in any way. The vague or contradictory provision will be reviewed and then clarified or corrected by the Board of Directors.

Entire Agreement
This Agreement is the entire Agreement between the parties and supersedes any and all prior oral and written agreements, commitments, understandings or communications with respect to

the subject matter of this Agreement. This Agreement may not be modified except in writing and signed by a duly authorized representative of each party.

Federation Documents
The operation of this Federation is governed by the following documents, which are incorporated into this agreement by reference: The Global Federated Identity and Privilege Management Governance Guidelines [GFIPM GOV] – this document defines the roles and responsibilities of the Federation, the Federation Management, the Board of Directors, Service Providers, and Identity Providers. Global Federated Identity and Privilege Management Operational Standards Policies and Procedures Guidelines [GFIPM OPP] – this document details the way in which the federation policies will be carried out. Global Federated Identity and Privilege Management Interface Control Document [GFIPM ICD] – this document details the technical interfaces required to be part of the federation. Global Federated Identity and Privilege Management Metadata Specification [GFIPM METADATA] – this document details the metadata requirements that must be used as part of the federation.

Notices
All notices, certificates, acknowledgments or other written communications required to be given under this Agreement shall be in writing and shall be deemed to have been given and properly delivered if duly mailed by certified or registered mail to the other Party at its address as follows, or to such other address as either Party may, by written notice, designate to the other.

Notice to the Federation Management shall be delivered as follows:

(Insert address)_____

Notice to the Identity Provider shall be delivered as follows:

(Insert address)_____

The following material, which has been submitted with this agreement, is incorporated in the agreement by reference:
(List documents)

Signatures
By signing below _____ (authorized organization name), the Identity Provider, certifies that they have read this document, that it is accurate and agrees to abide by this agreement and all Federation documents referenced herein.

_____ (authorized organization name),
the Identity Provider By:
_____ (authorized representative)
_____ (title)Signature

By signing below _____ (insert authorized organization name) , the Service Provider, certifies that they have read this document, that it is accurate and agrees to abide by this agreement and all Federation documents referenced herein.

_____ (insert authorized organization name),
the Service Provider By:
_____ (signature of authorized representative) _____ (insert title)

APPENDIX F - ASSURANCE LEVEL DEFINITIONS AND EXAMPLES

Assurance Level Classifications		
Level	Description	Examples
1	Little or no confidence in the asserted identity's validity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.	A. the submission of forms by individuals in an electronic transaction will be a Level 1 transaction: (i) when all information is flowing to the organization from the individual, (ii) there is no release of information in return, and (iii) the criteria for higher assurance levels are not triggered. For example, if an individual applies to an agency for an annual park visitor's permit (and the financial aspects of the transaction are handled by a separate contractor and thus analyzed as a separate transaction, the transaction with the Federal agency would otherwise present minimal risks and could be treated as Level 1. B. A user presents a self-registered user ID or password to the U.S. Department of Education web page, which allows the user to create a customized "My.ED.gov" page. A third party gaining unauthorized access to the ID or password might infer personal or business information about the individual based upon the customization, but absent a high degree of customization however, these risks are probably very minimal. C. A user participates in an online discussion on the state.gov website, which does not request identifying information beyond name and location. Assuming the forum does not address sensitive or private information, there are no obvious inherent risks.
2 Federal Bridge Certification Authority (FBCA) Basic Level	Some confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to	A. A user subscribes to the Gov Online Learning Center (www.golearn.gov). The site's training service must authenticate the person to present the appropriate course material, assign grades, or demonstrate that the user has satisfied compensation-or promotion-related training requirements. The only risk associated with this transaction is a third party gaining access to grading information, thereby harming the student's privacy or reputation. If the agency determines that such harm is minor, the transaction is Level 2.

	any state action)	B. A beneficiary changes her address of record through the Department of Human Services web site. The site needs authentication to ensure that the entitled person's address is changed. This transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the beneficiary's address of record, it entails moderate risk of unauthorized release of personally sensitive data. The agency determines that the risk of unauthorized release merits Assurance Level 2 authentication. C. An agency program client updates bank account, program eligibility, or payment information. Loss or delay would significantly impact him or her. Errors of this sort might delay payment to the user, but would not normally result in permanent loss. The potential individual financial impact to the agency is low, but the possible aggregate is moderate. D. An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create moderate potential impact for unauthorized release, but the system's security measures reduce the overall risk to low. E. A first responder accesses a disaster management reporting web site to report an incident, share operational information, and coordinate response activities. Department of Homeland Security has established that the default assurance level for first responders be at Level 2 or higher.

3 FBCA Medium Level	A high degree of confidence in the asserted identity's validity. This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving private information where access by individuals with malicious intent would result in significant harm.	A. A team electronically submits a bidder's confidential information to the State AG Office for review. Improper disclosure would give competitors a competitive advantage. B. A supplier maintains an account with the Department of Personnel & Administration's Contracting Officer for a large state procurement. The potential financial loss is significant, but not severe or catastrophic, so Level 4 is not appropriate. C. An agency employee or contractor uses a remote system giving him access to potentially sensitive personal client information. Her access to PII creates moderate potential impact for unauthorized release. If technical controls (such as a virtual private network) are in place to limit system access to the agency premises, this could be level 2. The sensitive personal information available to him creates a moderate potential impact for unauthorized release.
4 FBCA Medium (Hardware) or High Level	A very high degree of confidence in the asserted identity's validity. Users may present Level 4 credentials to assert identity and gain access to highly restricted system or physical resources, without the need for further identity assertion controls. This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are severe. This may include very high value transactions or high levels of fraud risk.	A. State Patrol official accesses a law enforcement database containing criminal records. Unauthorized access could raise privacy issues and/or compromise investigations. B. A Department of Corrections pharmacist dispenses a controlled drug. The Department would need full assurance that a qualified doctor prescribed it. The Department is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount. C. Agency investigators use a remote system giving them access to potentially sensitive personal client information. Using their laptop at client worksites, personal residences, and businesses, they accesses information over the Internet via various connections. Federal statutes require "securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them."

APPENDIX G – CALCULATING A RISK ASSESSMENT FOR E-GOVERNMENT

Step 1 - Data Security Classification Analysis

At the outset, Agencies must baseline the data that they are responsible for by performing a data security classification analysis of internal data and systems. A formal data governance process should be implemented to ensure that a common framework is employed for data lifecycle management. The framework is intended to enable consistent processes and methods for determining and implementing data standards, care, security, ownership, sharing, and lifecycle management.

Out of the data governance analysis, agency stakeholders should fully understand the confidentiality of the data that they are stewards of, as well as the need to protect the integrity of the data while ensuring appropriate access to the data.

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in NIST Special Publication 800-37. The three potential impact values are:

- Low Impact
- Moderate Impact
- High Impact

Step 2 - Impact Assessment

To determine the appropriate level of criticality and sensitivity, the information owner must first assess the potential impact an authentication error would have.

Category	Potential Impact Level		
	Low/1	Moderate/2	High/3
Inconvenience or distress	At worst, limited, short-term inconvenience or distress to any party.	At worst, serious short-term or limited long-term inconvenience or distress to any party.	Sever or serious long-term inconvenience or distress to any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).
Financial loss	At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an	At worst, a serious unrecoverable financial loss to any party, or a serious agency liability.	Sever or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

Category	Potential Impact Level		
	Low/1	Moderate/2	High/3
	insignificant or inconsequential agency liability.		
Harm to agency programs or public interests	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness, or (ii) significant damage to organizational assets or public interests.	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) severe mission capability degradation to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
Unauthorized release of information Confidentiality	The unauthorized access or disclosure of information would have minimal or no impact to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized access or disclosure of information could have only limited impact to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized access or disclosure of information could severely impact to the organization, its critical functions, employees, third party business partners and/or its customers.

Category	Potential Impact Level		
	Low/1	Moderate/2	High/3
Integrity	The unauthorized modification or destruction of information would have minimal or no impact to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized modification or destruction of information would have only limited impact to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized modification or destruction of information could severely impact the organization, its critical functions, employees, third party business partners and/or its customers.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Personal safety	At worst, minor injury not requiring medical treatment.	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.	A risk of serious injury or death.
Civil or criminal violations	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

A risk analysis is to some extent a subjective process, in which the information owner must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. The information owner should consider a wide range of possible scenarios in seeking to determine what potential harms are associated with their business process. The table below provides a sample assessment example.

Security Level Assessment for Authentication				
Categories of Harm	Impact (Step 1)	Likelihood (Step 2)	Risk Rating (Step 3)	Security Level (Step 4)
Inconvenience, Distress, or Damage to Standing/Reputation	3			
Financial Loss or Agency Liability	3			
Harm to Agency Programs or Public Interests	2			
Unauthorized Release of Information	2			
Personal Safety	N/A			
Civil or Criminal Violations	2			

N/A = No Impact; 1 = Low Impact; 2 = Moderate Impact; 3 = High Impact

Step 3 - Likelihood Assessment

The second step determines the likelihood that an asset would be misused if not properly secured. The information owner must also determine the likelihood that a risk will materialize and that the impact occurs.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-Source Motivation and Capability
- Nature of the Vulnerability
- Existence and Effectiveness of Current Controls
- Past History

Likelihood should be defined in concrete terms such as impacts are likely to occur daily, weekly, yearly, every decade, or "once in a career". The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as low, medium, or high. Table 3 below describes these three likelihood levels.

Step 4 - Calculate Risk Rating

The next step is to combine impact and likelihood to establish an overall risk rating. This can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example:

- The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low.
- The value assigned for each impact level is 3 for High, 2 for Medium, and 1 for Low.

Likelihood	Impact		
	Low (1)	Medium (2)	High (3)
Low (0.1)	1 x .1 = .1	2 x .1 = .2	3 x .1 = .3
Medium (0.5)	1 x .5 = .5	2 x .5 = 1	3 x .5 = 1.5
High (1.0)	1 x 1 = 1	2 x 1 = 2	3 x 1 = 3

Therefore, to understand in numerical terms the risk rating for each factor, the following calculation is used: impact x likelihood = risk rating, where the value for the probability factor (0.1, 0.5, 1.0) is substituted for the likelihood numerical 1-3 ranking done in Step 3. Taking the "Inconvenience, Distress, or Damage" category, this formula becomes 3 (for High) x .5 (for 2/Med) = 1.5. See example risk rating assessment below.

Security Level Assessment for Authentication				
Categories of Harm	Impact (Step 1)	Likelihood (Step 2)	Risk Rating (Step 3)	Security Level (Step 4)
Inconvenience, Distress, or Damage to Standing/Reputation	3	2	1.5	
Financial Loss or Agency Liability	3	3	3	
Harm to Agency Programs or Public Interests	2	2	1	
Unauthorized Release of Information	2	1	.2	
Personal Safety	N/A	N/A	N/A	
Civil or Criminal Violations	2	2	1	

Step 5 - Determine Security Level

The Security Level defines the results of the Security Level Impact Assessment table's Risk Rating to identify the appropriate Security Level for each Category of Harm.

Security Level	
Risk Scale	Level of Security
Up to .3	Low
>.3 to 1.5	Medium
>1.5 to 3	High

The table below shows a sample completed Security Level Assessment for Authentication.

Security Level Assessment for Authentication				
Categories of Harm	Impact (Step 1)	Likelihood (Step 2)	Risk Rating (Step 3)	Security Level (Step 4)
Inconvenience, Distress, or Damage to Standing/Reputation	3	2	1.5	High
Financial Loss or Agency Liability	3	3	3	High
Harm to Agency Programs or Public Interests	2	2	1	Medium
Unauthorized Release of Information	2	1	.2	Low
Personal Safety	N/A	N/A	N/A	N/A
Civil or Criminal Violations	2	2	1	Medium

Now that the risks have been identified and their potential impact quantified, this information can be tied to assurance levels and authentication technologies. Agencies should assess their potential impact category outcomes relative to the authentication level, and choose the lowest level of authentication that will cover all of potential impacts identified.

APPENDIX H - IDENTITY PROOFING REQUIREMENTS BY ASSURANCE LEVEL

	In-Person	Remote
Level 1	Minimum Requirements	
	There are no level-specific requirements at Level 1	
Level 2	Minimum Requirements	
	Possession of a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport). Enrolling official: ▪ Inspects photo-ID, compare picture to applicant, record ID number, address and DOB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number. Enrolling official: ▪ Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DOB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. ▪ Initiate address confirmation and notification: a) Send notice to the address of record confirmed by the records check; or b) Issue credentials in a manner that confirms the address of record supplied by the applicant; or ▪ Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications or email at the number or email address indicated by the applicant's records.

	In-Person	Remote
Level 3	Minimum Requirements	
	Possession of a verified current primary government photo ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport). Enrolling official: ▪ Inspect Photo ID and verify via the issuing organization or through credit bureaus or similar databases. Confirm that name, DOB, address, and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and DOB. If ID is valid and photo matches applicant then: a) if ID confirms address of record, authorize or issue credentials and send notice to address of record; b) if ID does not confirm address of record, issue credentials in a manner that confirms address of record.	Possession of a valid government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number. Enrolling official: ▪ Verify information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar data bases, and confirm that: name, DOB, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. ▪ Address confirmation: a) Issue credentials in a manner that confirms or independently verifies the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records while recording the applicant's voice.
		that confirms the ability of the applicant to receive telephone communications or email at the number or email address indicated by the applicant's records.

	In-Person	Remote
Level 4	Minimum Requirements	
	Possession of a verified current primary In-person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person), one of which must be current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application Enrollment Official: ▪ Primary Photo ID: Inspect photo ID and verify via the issuing government agency, compare picture to applicant, record ID number, address, and DOB. ▪ Secondary Government ID or Financial Account: a) Inspect photo ID and if apparently valid, compare picture to applicant, record ID number, address, and DOB; or b) Verify financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirm that; name, DOB, address, and other personal information in records are for the most part, consistent with the application and sufficient to identify a unique individual. ▪ Record Current Biometric: record a current biometric (e.g., photo, fingerprint, or other) to ensure that applicant cannot repudiate application. ▪ Confirm Address: issue credentials in a manner that confirms address of record. ▪ Conduct appropriate background check if required.	Possession of a valid government ID Not Applicable

APPENDIX I - GENERIC USAGE PATTERNS

This appendix described the user interaction during federated identity interactions. The examples listed here are examples of identity federations involving several trusted partners. Other examples and more complex examples will emerge during the deployment of a SICAM architecture.

SICAM Basic Usage Pattern

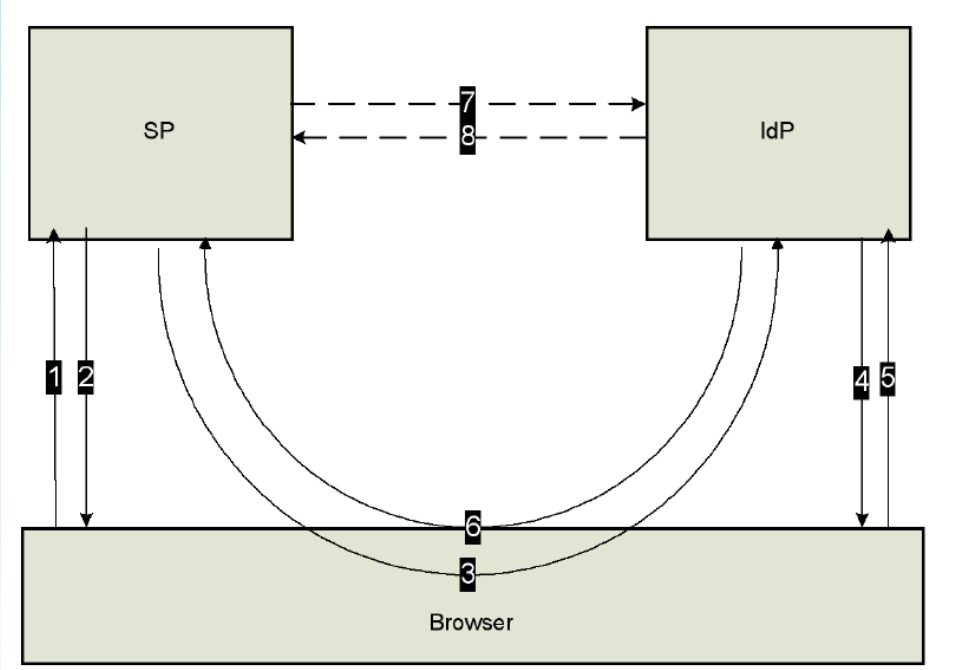


Figure 1 - SICAM Generic Usage Pattern

The summarized communication flow for the generic usage pattern is:

1. The service user attempts to access a resource at an SP website.
2. The SP may place a session cookie or similar object on the service user's browser to establish the local authentication session
3. The SP service user is redirected via their web browser to a logon page.
4. The IdP presents the web user with a logon page.
5. SP service user submits logon information on the logon page.

The IdP will respond to the SP department with a message via the service user's browser. The message contains either an assertion or an artifact, depending on the SAML binding used. Where the message contains an assertion (i.e. POST binding), the SP uses the assertion to authenticate the service user using its own internal processes and the pattern is complete. Where the message contains an artifact (i.e. Artifact binding), the SP dereferences the artifact to determine the IdP and continues with Step 7.

1. Where the message contains an artifact, the SP includes the artifact in a request (such as

an application-to-application digitally-signed SOAP message based Web Services call) to the IdP via a 'back channel' (such as an appropriately secured SSL/TLS leased data connection or Virtual Private Network) to receive the assertion.

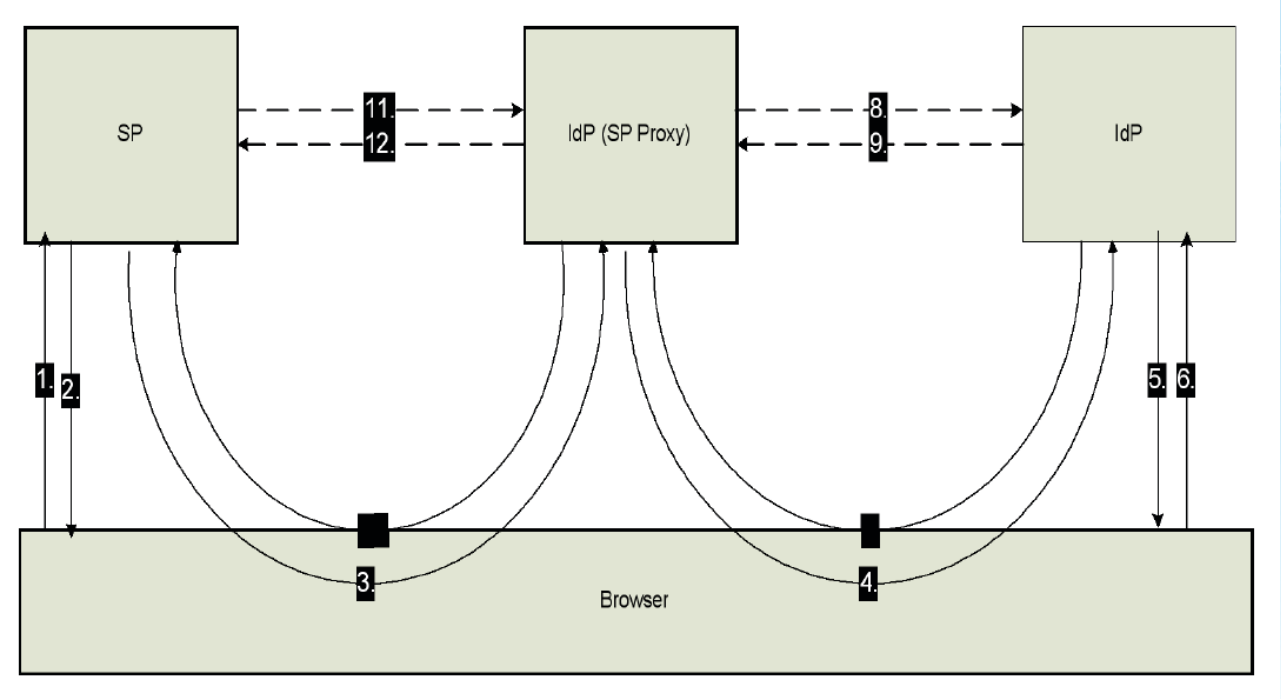
2. The IdP resolves the request by sending a message with the assertion reserved for the artifact via the mechanism described in (7) above.

In SICAM model the following design and business principles should apply:

- No reliance on the security of the service user's personal computer – Due to the difficulty in securing every personal computer (PC) on the Internet, no reliance can be placed upon the service user's PC for the transport of authentication-related messages and for installing client-side authentication software (with the exception of multi-factor authentication software applications).
- Federated identifier – Service users who logon at the authentication provider website must be given something (a unique federated identifier) that they can present to service provider websites as confirmation that they have been successfully authenticated.
- State persistence – If the service user goes to the SP website and encounters a step(s) in a service that requires the service user to be authenticated, the service user must be redirected to the authentication provider website. The redirection process and application logic must be implemented in such a way that the authentication provider website will redirect the service user back to the service provider website once they have authenticated, bearing their authentication credential, 'handle' and session ID. The service provider website must then be able to seamlessly resume the interrupted service step.
- Verified federated identifier – The effort to compromise the security of the authentication credential must be prohibitive. The service provider website must be able to verify that the credential was issued by some party that the service provider website trusts. Typically this is achieved using digital certificates for the servers involved in the exchange.

- **Verified messages** – The effort to compromise the security of any messages, or fragments of messages, that support the above requirements must be prohibitive. The service provider website and authentication provider website must be able to verify that the messages were issued by a party within the federation of websites. Typically this is achieved by signing and/or encrypting the message parts.
- **Universal services** – Any service provider with an online presence and seeking to authenticate their service users on the Internet must be able to participate in the federation.
- **Audit Trail** – Security assertion sessions must have an accompanying audit trail.
- **Archive management** – Establish practices for managing archives containing signed or en crypted data. Examples of potential issues are:
  - Logs that contain information that was signed with certificates that have since expired may be difficult to validate. Without trusted timestamps it would be unclear whether the signed object was created before the certificate was revoked or expired.
  - Encrypted elements in the logs will likely require the private key of the recipient to decrypt. If those keys have not been archived it may be impossible to read the old logs.

Figure 2 – SICAM IdP Proxy Usage Pattern



The profile depicted in Figure 2 is a variation on the generic SAML v2.0 Web Browser SSO profile . It describes how an IdP contacted by an SP acts in the role of an SP (i.e. proxies) to a different (endpoint) IdP where the service user ultimately authenticates. The endpoint IdP returns an assertion that is used by the proxying IdP to build a new assertion for the originating SP to use.

The use pattern reflecting this profile emerged from a number of agencies that expect to use the GLS (the endpoint IdP) for the act of authenticating, while managing all other aspects of the service user's session – SSO, authorization and provisioning, identity attributes etc.

APPENDIX J - EXAMPLE OF IDENTITY ATTRIBUTES

	Individual	Employee	First Responder
Attribute Name	Classification	Classification	Classification
Given Name	1	1	1
Middle Name	1	1	1
Sur Name	1	1	1
NameSuffix Text	1	1	1
Sex Code	1	1	1
Organization Association Category		1	1
Organizational Affiliation		1	1
Photo	1	1	1
Card Expiration Date			1
Card Issue Date			1
Employee Rank Text			1
Cardholder Unique Identifier		1	
Fingerprint Image	1	1	1
Digital Signature Certificate			1
Key Management Certificate			1
Card Authentication Certificate			1
Card Holder ID Status			1
Card Holder ID Status Date			1
Telephone Number	2	2	2
Birth Date	2	2	2
Citizenship FIPS10-4 Code	2	2	2
US Citizenship	2	2	2
Security Clearance Code		2	2
Clearance Date		2	2
Clearing Agency		2	2
Card Status			1
Card Status Date			1
Designated Role		2	2

	Individual	Employee	First Responder
Attribute Name	Classification	Classification	Classification
Certification Type			2
Certification Name			2
Certification Date			2
Certifying Authority			1
Emergency Contact Person GivenName			3
Emergency Contact Person SurName			3
Emergency Contact Telephone Number			3
Emergency Contact Email			3
Driver License Number	2	2	2
DL Expiration Date	2	2	2
Social Security Number	3	3	3
Mailing Address	3	3	3
Mailing Address City	2	2	2
State	2	2	2
Zip Code	2	2	2
Residence Address (if different than mailing address)	3	3	3
City	2		
State	2		
Zip Code	2		
Hair Color	3		
Eye Color	3		
Height	3		
Weight	3		
License Class	2		
Also Known As (AKA) Names	1		

APPENDIX K - BIBLIOGRAPHY

Several sources of publically available information were used in the creation of this document. The following list includes many of the valuable resources, but may not be inclusive of all information used in the creation of this document.

U.S. Department of Justice's, Global Federated Identity and Privilege Management (GFIPM), Governance Guidelines -- Working Draft Version 0.95 -
http://it.ojp.gov/docdownloader.aspx?ddid=1079

U.S. Department of Justice's, Global Federated Identity and Privilege Management (GFIPM), Operational Policies and Procedures -- Working Draft Version 0.95 -
http://it.ojp.gov/docdownloader.aspx?ddid=1080

Global Federated Identity and Privilege Management (GFIPM) Metadata Specification Version 1.0 –
http://www.it.ojp.gov/documents/GFIPM-Metadata-1.0.zip

Global Federated Identity and Privilege Management (GFIPM) Executive Summary -
http://www.it.ojp.gov/documents/GFIPM_flyer.pdf

Global Federated Identity and Privilege Management (GFIPM) Security Interoperability Demonstration Project Report
http://www.it.ojp.gov/documents/GFIPM_Security_Interoperability_Demonstration_Project_Report_2007-08-30.pdf

National Strategy for Trusted Identities in Cyberspace -
http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance -
http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

"NIST Special Publication 800-63 - Electronic Authentication Guideline" -
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

"NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems" –
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

M-04-04:E-Authentication Guidance for Federal Agencies, OMB M-04-04 E-Authentication Guidance established 4 authentication levels. -
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

NIST SP 800-116 defines PIV credentials based Identity assurance levels for Uncontrolled/Controlled/Limited/Exclusion areas. -
http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf

"ACCESS CONTROL IN SUPPORT OF INFORMATION SYSTEMS SECURITY TECHNICAL IMPLEMENTATION GUIDE Version 2, Release 2" - 26 DECEMBER 2008 -
http://iase.disa.mil/stigs/stig/access_control_stig_v2r2_final_26_dec_2008.pdf

"Introduction to the National Information Exchange Model (NIEM)" -
http://www.niem.gov/files/NIEM_Introduction.pdf

"FIPS PUB 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors" -
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

FIPS PUB 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES -
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

"Federal Public Key Infrastructure (FPKI) Architecture Technical Overview" -
http://www.idmanagement.gov/fpkia/documents/FPKIAtechnicalOverview.pdf

"Personal Identity Verification Interoperability For Non-Federal Issuers" -
http://www.idmanagement.