INFORMATION SERVICES BOARD

Primary Contributors:

Paul Warren Douglas
Department of Information Services

Laura Parma
Department of Information Services

Agnes Kirk
Department of Information Services

Enterprise Architecture Committee
Documenter Team
21 Agencies
72 Individuals

Identity Management
User Authentication Standards

ISB Standards

Version 2.0

July 10, 2008

Information Services Board
Enterprise Architecture Committee

Bill Kehoe, *Department of Licensing*
Frank Westrum, *Department of Health*
Co-Chairs

Laura Parma, Initiative Steward
Department of Information Services

Paul Warren Douglas, *Initiative*
Enterprise Architect

Table of Contents

1. Document History

Date	Version	Editor	Change
June 10, 2008	1.0	Paul Warren Douglas	Initial Draft
June 11, 2008	1.1	Paul Warren Douglas	EA Committee final revisions and Endorsement
July 10, 2008	2.0	Paul Warren Douglas	Adopted by the Information Services Board

2. Document Context

This document was adopted as Standards by a vote of the Information Services Board (ISB) on July 10, 2008.

- The ISB Enterprise Architecture Standards and Guidelines are at: http://isb.wa.gov/policies/eaprogram.aspx

Initiative Steward

- Laura Parma, Department of Information Services

Initiative Enterprise Architect

- Paul Warren Douglas, Department of Information Services

Documenter Team

- The 71 members from 21 agencies are listed in Appendix A

Enterprise Architecture Committee

- Information about the ISB Enterprise Architecture Committee is at: http://isb.wa.gov/committees/enterprise/comartifacts/index.aspx

3. Introduction

These standards designate the state's Enterprise Active Directory (EAD), SecureAccess Washington® (SAW), and Transact Washington™ (TAW) as common user authentication solutions for state government to leverage available statewide investments, provide an integrated end-user experience, and enable single/reduced sign-on.

Federated Identity Management (FID) is designated as an architectural strategy via extended SAW functionality, policies, practices, and technologies to enable single/reduced sign-on across organizational boundaries.

3.1. Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the Information Services Board (ISB), including the authority to develop statewide or interagency information services and technical policies, standards, and procedures.

3.2. Scope

These standards apply to all Washington State executive branch agencies and agencies headed by separately elected officials (referred to as "agency or agencies" throughout this document).

Exemption requests must be submitted to the Department of Information Services (DIS) Management and Oversight of Strategic Technologies Division and will be forwarded to the ISB for decision. A state agency must make a clear business case to develop or procure a custom user authentication solution.

Starting July 10, 2008, the Identity Management User Authentication Standards will govern the planning and construction of all agency applications that require user authentication as follows:

3.2.1.1. Agency to Agency – Internal to Internal

By December 31, 2010 all agencies shall develop a migration strategy in coordination with DIS to join the state's Enterprise Active Directory. EAD is defined in Section 4.1.1 and excludes the legislative and judicial branches of government, and higher education.

3.2.1.2. Individuals and Businesses to Agencies – External to Internal

Agency applications existing or under construction as of July 10, 2008 are not immediately required to incorporate SecureAccess Washington or Transact Washington as described in Section 4.2 unless there is a significant upgrade or when subject to other over-arching polices.

By December 31, 2010 all agencies shall develop a migration strategy in coordination with DIS to comply or when applications are significantly upgraded, redesigned, or replaced.

3.2.1.3. Government to Government – Internal to other Internal

Other government entities including: legislative and judicial government, higher education, local governments, and federal government users will authenticate using Federated Identity Management (FID) via extended SAW functionality as described in section 4.3.

3.3. Related Policies, Standards, and Strategic Plans

Related ISB polices include, but are not limited to: ISB **[Investment Standards];** ISB EA **[Networking Standards]**; and ISB **[Security Standards].**

These recommendations are in accordance with the IdM Initiative Charter objectives (see Appendix C) adopted on March 8, 2007 by ISB, the 2008-2014 State Strategic Information Technology Plan Goals (see Appendix D), and the state's over-arching enterprise architecture (EA) principles at: http://isb.wa.gov/committees/enterprise/architecture/index.aspx.

4. Standards

These standards are designed to reduce the number of user credentials (e.g. IDs and passwords) and authentications (e.g. log-in prompts) required to access state agency and educational resources and services.

4.1. Agency to Agency – Internal to Internal

4.1.1. Enterprise Active Directory (EAD)

EAD is the standard user authentication solution for state agencies to provide single sign-on for employee access to applications and IT assets within the State Government Network (SGN.)

The Enterprise Active Directory is defined as the state's Active Directory implementation in the SGN that serves the SGN executive branch agencies. It provides the directory structure used for authentication inside of the SGN. It excludes the separate branches of government (Legislative Branch and Judicial Branch) and higher education.

4.1.1.1. Assumptions

- Agencies are responsible for creating processes that support user access. Passwords should be managed by the individual user.
- Agencies and Application Owners should be responsible for identity proofing new users to ensure authorized access for SGN employees.

4.2. Individuals and Businesses to Agencies – External to Internal

4.2.1. SecureAccess Washington (SAW)

SAW is the standard user authentication solution to be used by state agencies to allow users to access resources/online applications in a secure manner.

SAW provides single/reduced sign-on for non-SGN users, businesses, and the public to access applications that require user authentication via a user ID and password.

- Agencies determine the role of a user and the authorization to conduct certain activities. Agencies are responsible for which user is placed in a particular role to ensure authorized access.
- Application Owners are responsible for identity proofing new users requesting access to their applications via the User ID authentication gateway. Application Owners have the ability to remove access to a backend application if a user no longer has a business need to access the application, or if it is believed a user account has been compromised.

4.2.1.1. Assumptions

- Future security allows for gradation of authentication levels based on common risk assessment
- The state's IdM solutions will evolve to meet changing business needs and technical solutions.

4.2.2. Transact Washington (TAW)

TAW is the standard authentication solution for applications that require the strongest level of user authentication.

- TAW provides single sign-on via public key infrastructure (PKI) and digital certificate technology for applications that require the strongest level of user authentication.
- Identity proofing for users of x.509 digital certificates is conducted by the issuer of the digital certificates.

4.2.2.1. Assumptions

- Future statewide risk assessment model provides agencies with additional decision criteria to determine the level of risk necessary for PKI.
- The state's IdM solutions will evolve to meet changing business needs and technical solutions.

4.3. Government to Government – Internal to other Internal

4.3.1. Federated Identity Management (FID)

FID is an architectural strategy via extended SAW functionality for Government to Government interaction, and future Businesses to Government interaction.

FID IdM solution enables single/reduced sign-on across organizational boundaries. Employees access other government applications without re-authenticating to each application.

- FID architecture extends SAW and provides the architecture to extend and "federate" authentication to other government entities including: the Legislative Branch, Judicial Branch, higher education, local governments, and federal government users.
- Requires trust models and cross-organizational relationships through policy, contracts and data sharing agreements, and technologies.
- Non-SGN connected Government users access an agency application via a Single Sign-On Gateway. The Gateway authenticates the user via a federated identity management (FID) solution that communicates with non-agency user directories.
- Authentication across organizational boundaries is determined through risk assessment and contractually agreed upon identity proofing methods appropriate to the information being transmitted or data accessed.
- Identity proofing is the responsibility of the employee's agency.

4.3.1.1. Assumptions

- FID requires a combination of business and architectural components including:
  - *Trust relationships between the cross-organizational partners*: The architecture should identify one or more industry standard trust models.
  - *Agreements built on policies, contracts, and principles.* The trust relationship is established and built on a contractual framework for user authentication, confidentiality, data integrity, and accountability.
  - *Agreed upon assurance levels and risk assessment models*: The architecture will include an agreed upon risk assessment model aligned with industry standards.
  - *Technologies for interoperability:* Technologies may include any one or more industry standard.
- The architecture supports future individual and business user authentication via a federated identity management solution to access an agency application.

5. Rationale

5.1.1.1. Leverage Existing Investments

Baseline architecture findings indicated Washington State's current IdM Solution Sets are relatively mature when compared with other state's and educational solutions (**NASCIO, GARTNER**).

- The state's common enterprise IdM security infrastructure includes Secure Access Washington, Transact Washington, and Enterprise Active Directory.

5.1.1.2. Integrated End-User Experience

Ensures citizens and businesses can interact seamlessly with multiple federal, state, and local agencies.

- Single/Reduced Credentials and Sign-on reduce the number of user credentials (e.g. IDs and passwords) and authentications (e.g. log-in prompts) required to access state agency and educational resources and services.

5.1.1.3. Efficiency and cost-effectiveness

Common user authentication promotes efficiency and cost-effectiveness of the state's user authentication investments.

- More efficient and cost-effective than alternatives provisioned separately by individual agencies.
- Consolidating user authentication frees state agencies to devote more resources to their core business missions and to direct technology support for their customers.

5.1.1.4. Security

Common security system infrastructure protects agencies from unauthorized external access to or broadcast on the Internet of the agencies' intellectual property, proprietary and confidential data.

- The IdM solutions are housed in a secure Data Center that allows physical access only to authorized personnel.
- The perimeter firewalls, gateways, and security policies implement a baseline level of network security that satisfies enterprise-wide security requirements
- The IdM solutions ensure the appropriate level of protection of state resources through security best practices.
- The architecture solutions ensure compliance with the ISB IT Security Standards and industry best practices.

5.1.1.5. Scalability

- Network infrastructure, hardware and software component architecture are highly available, and fully redundant to allow for the addition of resources without system downtime. The system should be scalable to include all state employees.

- The solutions are designed to be scalable to handle hundreds of thousands of registered users and be able to grow as needed to support concurrent usage.

5.1.2. Implications

The designation of the IdM User Authentication Standards as common, shared solutions has potential implications including:

5.1.2.1. Migration Strategies

- Agencies not currently part of the EAD may need to invest in future infrastructure. Each agency will build a migration and risk mitigation strategy (see Section 3.2 Scope.)

5.1.2.2. Regulatory Compliance

Agencies are encouraged to contact their legal and policy offices, including the agency's appointed Attorney General, for relevant laws and regulations applicable to the business of the agency.

There are a number of federal and state laws, policies, and regulations related to regulatory compliance. Privacy is growing concern and legal issues continue to evolve due to the ubiquitous nature of the Internet and virtual physical location of information of data. States now have a responsibility to protect a resident's private/sensitive information regardless of location.

6. Glossary

The Conceptual Technical Reference Architecture contains the ‘Global Glossary.’ Some terms are included within this document’s Glossary for readability.

AUTHENTICATION

Validation of identification credentials. This is a process where a person, device or a computer program proves their identity in order to access environments, systems, resources and information. The person’s identity is a simple assertion, the login ID for a particular computer application, for example. Proof is the most important part of the concept and that proof is generally something known, like a password; something possessed, like your ATM card; or something unique about your appearance or person, like a fingerprint.

AUTHORIZATION

The act of granting a person or other entity permission to use resources in a secured environment. This is usually tightly linked to authentication. A person or other identity first authenticates and then is given pre-determined access rights. They now have the authority to take specific actions.

CREDENTIALS

Credentials are the components or attributes of identity that are assessed to prove a person, device, or computer program is who they claim to be. Common credential stores include databases, directories and smart cards.

DIGITAL CERTIFICATE

In general use, a certificate is a document issued by some authority to attest to a truth or to offer certain evidence. A digital certificate is commonly used to offer evidence in electronic form about the holder of the certificate. In PKI it comes from a trusted third party, called a certification authority (CA) and it bears the digital signature of that authority.

FID

Federated Identity Management (FID) is a set of policies, practices, and technologies that enable single/reduced sign-on across organizational boundaries. FID allows a verified user to be authenticated across organizational boundaries in order to access state agency and educational resources and services.

FID requires a combination of business and architectural components including: a trust relationship between the cross-organizational partners; agreements built on legally binding policies, contracts, and principles; agreed upon assurance levels and risk assessment models; and technologies

IDENTITY PROOFING

Identity proofing is the process of validating the claimed identity of an individual. It is central to a secure and authoritative process for the issuance and use of identity credentials.

Identity proofing can be accomplished through a variety of processes that establish a history of identity by collecting identity information (e.g. personal, demographic, and biographical information) and validating the accuracy and legitimacy of the information collected by conducting a face-to-face interaction and/or verifying the validity of identity source documents against third-party databases

Level of Assurance

Level of Assurance describes the degree of certainty that the user has presented a valid set of identifier attributes (credentials, etc.) that refer to his or her identity. In this context, assurance is defined as:

The degree of confidence in the vetting process used to establish or validate the identity of the individual to whom the credential was issued, therefore establishing the degree of confidence (assurance) the person who accepts the credential should have, that the provider is the individual to whom the credential was issued.

PKI

Public-Key Infrastructure is the infrastructure needed to support asymmetric cryptography. At a minimum, this includes the structure and services needed to do the following:

- Register and verify identities
- Build and store credentials
- Certify the credentials (issue digital certificates)
- Disseminate the public key
- Secure the private key and yet make it available for use

SGN

The State Government Network, managed by the Department of Information Services, is a managed network for Washington state government organizations. The SGN provides Washington state government with a shared, fault-tolerant, economical network to meet the diverse business needs across state government. The SGN also provides the necessary security layers, including but not limited to firewalls, authentication gateways and intrusion detection to allow Washington state government organizations to perform government business securely over the Internet.

SSO

Single/Reduced Credentials and Sign-on - Reduce the number of credentials (e.g., login IDs and passwords) that a user must remember and manage, and reduce the number of sign-ons (e.g. login prompts) presented to the user, when accessing state agency and educational resources and services across organizational boundaries.

Describes the ability of a user to leverage one sign-on act, for example entering an ID and password or passcode, to authenticate and access information across system, application and organizational boundaries. Is sometimes also referred to as Web SSO when everything is accessed through a browser

Tier one

Business processes, data, or technologies that are common for the state. The various elements that are defined in the statewide Enterprise Architecture are comprised of business processes, data, or technologies.

Those EA elements can be categorized into different tiers depending on the degree to which they should be common, and what other entities with which they should be common. A description of the state's Tiers is available at: http://isb.wa.gov/committees/enterprise/concepts/

7. References

EA Principles Washington State Information Services Board (2004). *Over-Arching Enterprise Architecture Principles*.

Investment Standards Washington State Information Services Board (2003). *Information Technology Investment Standards*.

NASCIO Enterprise Security – A conversation with Bruce Schneier, (June 2007)

Teleconference with NASCIO executives, (June 2007)

Gartner Analyst Inquiry, Identity Management Trends, Earl Perkins, (Aug 2007)

Networking Standards Washington State Information Services Board (2006). *Networking Standards*.

Security Standards Washington State Information Services Board (2008). *IT Security Policy and Security Standards*.

SGN Washington State Information Services Board, Enterprise Architecture Committee (2006). *State Government Network Solution Set*, Enterprise Architecture Committee Document

Appendix A: Documenter Team

This document resulted from the enterprise architecture Identity Management initiative, chartered March 8, 2007 by the Information Services Board. The following individuals were members of the initiative Documenter Team and participated as subject matter experts throughout documentation and review process.

- Renee Alexander, Department of Revenue
- Tammy Anderson, Department of Transportation
- Kent Andrus, Office of Financial Management
- Brian Barta, Department of Corrections
- Rupert Berk, University of Washington
- Mark Borgaard, Employment Security Department
- Scott Boyd, Legislative Service Center
- Jerry Britcher, Department of Social and Health Services
- Doug Buster, Department of Social and Health Services
- Kyle Chandler, Department of Revenue
- Tami Clawson, Department of Revenue
- Dan Cole, Office of Financial Management
- Jeff Colorossi, Department of Personnel
- Stephen Comfort-Mason, Administrative Office of the Courts
- Colin Corbin, Department of Revenue
- Brian Criss, Department of Information Services
- Jim Cristofono, Community, Trade, and Economic Development
- Marjorie Dausener, Department of Labor and Industries
- Phil Davis, Department of Information Services
- Mark Delaplane, Department of Labor and Industries
- John Ditto, Department of Information Services
- Nathan Dors, University of Washington
- Chuck Dorsett, Department of Transportation
- Melanie Esslinger, Department of Information Services
- Paul Warren Douglas, Department of Information Services
- Gary Dubuque, Department of Revenue
- Yousef Fahoum, Department of Health
- Dan Francis, Department of Health
- Mike Frost, Department of Social and Health Services
- John Garrison, Department of Revenue
- Tom Gigstead, Office of Financial Management
- Sue Gordon, Department of Retirement Systems
- Phil Grigg, General Administration
- Robin Griggs, Department of Licensing

- David Hamrick, Department of Transportation
- Anne Hopkins, University of Washington
- Peter Jekel, Department of Corrections
- Joanna Jones, Department of Transportation
- Agnes Kirk, Department of Information Services
- Ila Kowalski, Department of Personnel
- Deasy LaNae, Department of Personnel
- Roger LaPrelle, Liquor Control Board
- Jerome Lindley, Department of Information Services
- Sharie McCafferty, Department of Health
- Fred McDowell, Legislative Service Center
- Jason McKinney, Liquor Control Board
- Zephyr McLaughlin, University of Washington
- Mike McMahon, General Administration
- Randy Moore, Department of Ecology
- Bob Morgan, University of Washington
- David Morris, Department of Information Services
- Miles Neale, Department of Ecology
- Bill Norris, Department of Health
- Rebekah O'Hara, Department of Information Services
- Laura Parma, Department of Information Services
- Karen Peterson, Department of Information Services
- Julian Pietras, South Puget Sound Community College
- Aaron Purcell, Employment Security Department
- Pat Ramsdell, Washington State Patrol
- Laurie Ross, Department of Transportation
- John Sadie, Department of Social and Health Services
- Cliff Schiller, Department of Labor and Industries
- Carl Schwarmann, Department of Revenue
- Vicki Smith, Department of Revenue
- Matt Stevens, Department of Information Services
- Debbie Stewart, Department of Ecology
- Brian Stoll, Department of Information Services
- Ian Taylor, University of Washington
- Lyle Tillett, Department of Retirement Systems
- Corey Wade, Washington State Patrol
- Bill Wildprett, Community, Trade, and Economic Development
- Carol Wyckoff, Department of Personnel

Appendix B: Review Log

The following feedback on this document was received by the Enterprise Architecture Program; the response to each contribution is noted below.

Review by whom and when	Contribution	Response
EA Committee June 11, 2008	• Minor sentence structure changes to lines 23 and 30 to move Dec 31, 2010 due date to beginning of sentences.	Incorporated into document
Information Services Board July 10, 2008	• Adopted as state standards	Incorporated into document
July 14, 2008	• Added Documenter Team names in Appendix A • Added Terms in document to Glossary • General edits for readability	Incorporated into document

Appendix C: Charter Objectives

The Initiative Charter was adopted on March 8, 2007 by the Information Services Board.

- Establish common terminology and key concepts that will help guide the design and development of Identity Management solutions.
- Reduce the number of security credentials required by a system user to access state resources and services.
- Reduce the number of authentications and authorizations required by a system user to access state resources and services.
- Identify state standards to enable interoperability, user convenience, and reduce the number of disparate solutions. Align with ISB policies and standards.
- Establish common definitions and identity proofing requirements for varying levels of assurance.
- Identify common Identity Management services that promote reuse of government resources and minimize system redundancy.
- Improve the protection of information resources from fraud and misuse by unwanted intruders.

Appendix D: 2008-2014 State Strategic Information Technology Plan

Goal 1: Invest in Common Systems

Adopt a common system approach for the state's back-office systems such as the Office of Financial Management's Roadmap project, the Department of Personnel's Human Resources Management System, and the Health Care Authority's Benefits Administration/Insurance Accounting System.

- Financial: accounting, chart of accounts, • budget, performance measurement, grants, contracts, and loans
- Personnel
- Health Insurance
- Receivables
- Security
- User Authentication

Goal 2: Promote Data Sharing

Allow for the sharing of data through common data standards and management, data archiving, and the adoption of common platforms and infrastructure.

- Education, including Higher Education
- Health and Human Services
- Criminal Justice
- Economic Vitality

Goal 3: Promote Common IT Practices

Adopt standards, frameworks, and infrastructures that promote data sharing, an integrated end-user experience, and provide for common functionality across the state such as licensure and revenue collection.

- Security
- Data Standards
- Infrastructure Standards
- Application Development Standards
- Disaster Readiness

Goal 4: Provide an Integrated End-user Experience

Ensure citizens and businesses can interact seamlessly with multiple federal, state, and local agencies.

- Adopt common methodology for user authentication
- Adopt common methodology for application development
- Adopt common methodology for data management
- Adopt common user interface for cross agency systems
- Adopt common E-mail conventions