

FSA Integration Partner Program
United States Department of Education
Office of Federal Student Aid



Security and Privacy Architecture Framework Specification

Deliverable 124.1.3

***Task Order 124:
Security and Privacy Architecture Framework***

**Version 1.0
DRAFT**

May 30, 2003

Confidential – For Official Use Only

Document Revision History

Version Number	Date	Author	Revisions Made
1.0	May 30, 2003	Hector G. Mezquida, Jesse Bowen	Initial draft released

Table of Contents

1	Executive Summary	5
2	Introduction.....	6
2.1	Project Objectives	6
2.2	Security Architecture	7
2.2.1	Architecture Objectives	7
2.2.2	Intended Use of the FSA Security and Privacy Architecture	7
2.3	Organization and Maintenance of This Document	8
3	Scope.....	9
3.1	Project Overview	Error! Bookmark not defined.
3.2	Security and Privacy Architecture Scope	Error! Bookmark not defined.
4	Security Process Model for Identity and Access Management.....	10
4.1	Purpose.....	10
4.2	Security Process Model Description.....	10
4.2.1	Primary Security Access Processes	10
4.2.2	User Administration and Provisioning Processes	11
4.2.3	Audit and Logging Processes.....	12
4.2.4	Delegated Administration Processes.....	12
4.2.5	Supporting Policy and Procedures	14
5	FSA Security and Privacy Business Requirements.....	17
6	Proposed FSA Security and Privacy Architecture	22
6.1	Security and Privacy Architecture Vision.....	Error! Bookmark not defined.
6.2	Security and Privacy Architecture Overview	Error! Bookmark not defined.
6.3	Technical Services and Components	Error! Bookmark not defined.
6.3.1	Access Management Service	Error! Bookmark not defined.
6.3.2	Provisioning	Error! Bookmark not defined.
6.3.3	Enterprise Directory Services	Error! Bookmark not defined.
6.3.4	Non-Repudiation Services	Error! Bookmark not defined.
6.3.5	Encryption Services	Error! Bookmark not defined.
6.3.6	Infrastructure Security Services	Error! Bookmark not defined.
7	Validation of Security and Privacy Architecture	43
7.1	Introduction.....	43

7.2	Validation against business objectives.....	43
7.2.1	Control access	43
7.2.2	Manage Access	Error! Bookmark not defined.
7.2.3	Audit Access	Error! Bookmark not defined.
7.2.4	Protect Data.....	Error! Bookmark not defined.
7.2.5	Sign Transactions.....	Error! Bookmark not defined.
7.2.6	Protect FSA infrastructure	Error! Bookmark not defined.
8	Conclusion	52
9	Appendix.....	53
9.1	Diagram of Generic Security and Privacy Framework.....	Error! Bookmark not defined.
9.2	Summary of Draft FSA Information Technology Security and Privacy Policy	55
9.2.1	Introduction.....	60
9.2.2	Enterprise Management Controls	60
9.2.3	System Operational Controls	61
9.2.4	System Technical Controls.	61
9.3	Summary of FSA Security Solution Lifecycle Guide.....	62
9.3.1	Introduction.....	62
9.3.2	Vision Phase System Security	62
9.3.3	Definition Phase System Security.....	62
9.3.4	Construction Phase System Security	62
9.3.5	Deployment Phase System Security	63
9.3.6	Support and Retirement Phase System Security.....	63

1 Executive Summary

This document is a required deliverable for Federal Student Aid Task Order 124 – Security and Privacy Architecture Framework. This deliverable defines a proposed Security and Privacy Architecture Framework Specification for FSA. The business objectives on which the architecture description is based are detailed, followed by a description of the layers, services, and components that comprise the proposed security architecture. Each of the business objectives is then addressed to demonstrate how the required security function is satisfied by the proposed architecture structure.

This remainder of this document consists of the following major sections:

Section 2 – Introduction

Section 3 – Scope

Section 4 – Security Process Model for Identity and Access Management

Section 5 – FSA Security and Privacy Business Requirements

Section 6 – Proposed FSA Security and Privacy Architecture Framework Specification

Section 7 – Validation of Security and Privacy Architecture

Section 8 – Conclusion

Appendix – Contains supplemental material:

Appendix 9.1 – Diagram of the Technical Generic Security and Privacy Framework

Appendix 9.2 – Detailed business objectives matrix

Appendix 9.3 – Summary of FSA Information Technology Security and Privacy Policy

Appendix 9.4 – Summary of FSA Security Solutions Lifecycle Guide

2 Introduction

This document describes a proposed Security and Privacy Architecture Framework Specification to guide development and deployment of FSA security technologies. The Security and Privacy Framework was developed to meet the set of business objectives for security that were identified through a variety of contacts (see Section 5 for details). The proposed FSA Security and Privacy Architecture Framework Specification is described in detail in Section 6 of this report. The framework is then validated against each business objective in Section 7.

A companion deliverable, 124.1.2 -- Final Security and Privacy Architecture Report, contains a final status report and describes an implementation strategy for the framework defined in this specification.

2.1 Project Objectives

The goal of the Security and Privacy Architecture Framework task order was to define an overall vision to guide planning and development of FSA security and privacy technical services and components. The ultimate objective of the security and privacy architecture framework is to increase FSA's effectiveness in the following critical protection areas:

- Integrity – Prevent data theft from FSA and maximize transactional accuracy.
- Confidentiality – Prevent unauthorized viewing or alteration of other people's data.
- Availability – Prevent service disruption.
- Accountability – Provide for clean security audits.

The specific purpose of this task order was to produce the first version of a Security and Privacy Architecture Framework, in cooperation with FSA business units, contractors, and partners. To accomplish this, the following tasks were planned:

- Conduct a Security Architecture Workshop.
- Develop a Generic Framework for the FSA Security and Privacy Architecture.
- Develop an FSA Security and Privacy Architecture Framework Specification.
- Define a Security and Privacy Architecture Implementation Strategy.

Because of the diverse nature and scope of its computing environment, FSA faces a variety of challenges to deployment and operation of effective security controls. The major problems and issues that will be addressed by creation of the Security and Privacy Architecture Framework are:

- Lack of consistent security implementations across FSA systems and applications
- Lack of long-term security vision for FSA technical infrastructure
- Challenge of communicating security directions and requirements to business owners and development teams without an effective method for depicting and explaining FSA security standards and solutions

- Need to coordinate collection of security requirements and objectives with common terminology and conceptual basis, leading to misunderstandings, duplicated work, and delays in security design and development
- Need for a security framework to communicate with and integrate security objectives into technical architecture at both the FSA and Dept. Ed. Levels.
- Need to define common security services to provide reusable functions that meet common security function requirements, and can be deployed in robust, proven form, instead of reinventing security implementations as each system or application is developed

2.2 Security Architecture

2.2.1 Architecture Objectives

In addition to the business objectives for security that are detailed in Section 5 of this report, the following general objectives were used to guide the creation of the Security and Privacy Architecture Framework.

- Business input to development of the FSA Security and Privacy Architecture Specification is critical to understanding and incorporating appropriate business objectives and security goals.
- FSA has an existing IT Security and Privacy Policy that provides management guidelines for implementing security procedures. The Security and Privacy Architecture Framework must integrate with existing FSA security and privacy policies.
- The FSA security and privacy architecture will need to be flexible enough to respond to changes in requirements, technologies, and security threats over time.

2.2.2 Intended Use of the FSA Security and Privacy Architecture

The final FSA Security and Privacy Architecture specification will provide an important tool for the design and deployment of security measures. The architecture can be used:

- As a guide for security strategy and planning
- As a security design and deployment aid to promote structured, systematic, and repeatable development of security controls
- To communicate technical standards and decisions, both internally and externally
- As part of the FSA Solution Life Cycle to:
 - Integrate security architecture checkpoints into SLC checklists (e.g., during the vision, definition, and construction phases)
 - Describe how designers and developers can take advantage of existing security solutions or services to avoid custom builds
 - Align technical system design and configuration with FSA security policy
- To capture successful and proven security solutions for future use

- To document security architecture updates based on analysis of results from development projects and changes in system or technology requirements.

2.3 Organization and Maintenance of This Document

The remainder of this document consists of the major sections described below.

Section 3 – Scope

Section 4 – Security Process Model for Identity and Access Management

Section 5 – FSA Security and Privacy Business Requirements

Section 6 – Proposed FSA Security and Privacy Architecture Framework Specification

Section 7 – Validation of Security and Privacy Architecture

Appendix – Contains supplemental material

This document should be updated periodically to account for changes in the following factors that have an impact on security and privacy architecture deployment and operations:

- Changes or updates in federal legislation or regulations that address requirements for information security or data privacy
- Changes in the nature or frequency of security threats faced by FSA systems and applications
- Changes in FSA business objectives or requirements
- Changes in technology solutions that could alter relationships between architecture components and services.

3 Scope

This deliverable defines technology components of a proposed FSA Security and Privacy Architecture Framework. An effective information security capability must provide an integrated set of administrative, procedural, physical, and technical controls selected through an explicit risk management process. Although the primary focus of the security and privacy framework discussed in detail below is security technology, it is important to emphasize that few security solutions will consist solely of technical mechanisms. In most cases, security objectives can only be achieved with thorough integration of security policies and processes with other security controls. For example, a significant fraction of security incidents (more than half according to some studies) can be attributed to accidents or mistakes by system users. Technical security mechanisms are an important element of security, but the prominence given security technologies in the following security and privacy framework does not imply that most security problems have technology solutions. More commonly, security objectives will dictate a combination of procedural and technical controls based on appropriate supporting processes and management structures.

The Security and Privacy Architecture Framework does not directly include the following security components or functions:

- Security management controls, such as policy and procedures or personnel security
- Security process controls, including security testing processes or disaster recovery
- Physical security and data center environmental controls.

4 Security Process Model

4.1 Purpose

There is a notable lack of standard definitions for security concepts and functions among security products vendors, security organizations, and federal agencies. This is especially true in the emerging area of what this document calls “Identity and Access Management”. For example, the term “access management” may be used variously to refer to “front-end” security controls (user authentication and access control lists), administration of system user access accounts, development of access authorization policies, or the processes and forms used to approve a user request for access.

A security process model for identity and access management was developed to guide discussions of security requirements and objectives. The objective was to define a common set of security concepts and functions related to: management of user identities; security functions that directly control user access; administration of user accounts; user activity and access privilege auditing; and data repositories that store security information or rules concerning users and their access privileges. The intent was to aid communications during the collection and validation security objectives and requirements for the FSA Security and Privacy Architecture.

The diagrams below introduce and briefly describe the security process model. It consists of process and procedure elements that build progressively toward a holistic set of identity and access management functions and supporting elements. Note that, since the process model focuses on identity and access management functions, it does not include the entire set of security controls needed for a complete and effective security capability. For example, this model does not include functions for transaction signing, data encryption, or network and infrastructure security operations.

4.2 Security Process Model Description

The security process model provides an overview of security functions related to management of user identities and their access to information assets. The model does **not** define implementation details. For example, this model does not define the technology components or integration requirements needed for implementation of these functions for specific systems or applications. The Identity & Access Management security processes shown on these diagrams may be implemented within individual applications, as external security services, or as a combination of both. In addition, the processes shown are aggregate processes composed of multiple steps; e.g., ‘Approve Access’ may include steps to route approval requests, one or more access authorization decisions, alternate steps in the event that primary approvers are unavailable, and communication of approval decisions to users, managers, and system administrators.

4.2.1 Primary Security Access Processes

Figure 4.1 shows the primary security process associated with logging in a user at the time the user wishes to use a system or application. The login process includes an initial authentication step, followed by control of access to specific information assets, such as applications or data, based on stored authorization policies or rules. Information assets may include various system resources, as shown by examples in the diagram.

Security and Privacy Architecture Version 1.0

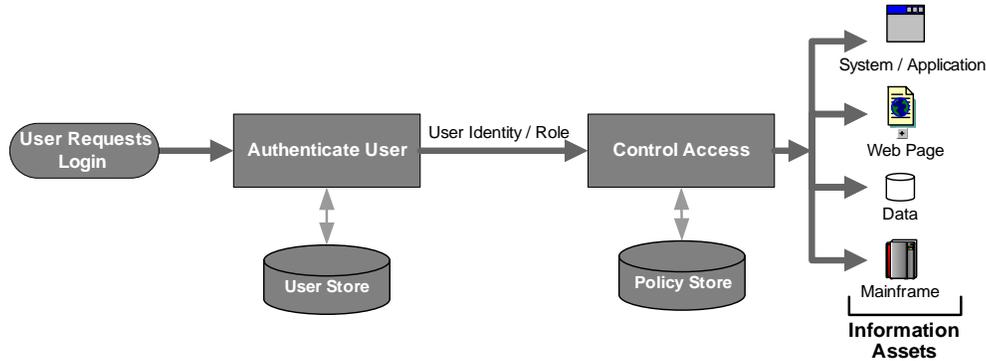


Figure 4.1. Primary Security Access Processes

4.2.2 User Administration and Provisioning Processes

Figure 4.2 adds to the security process model functions to support management of users and their identities. These functions include administrative and provisioning capabilities for identifying and registering users, steps required to approve their access, adding users to systems and applications by creating new user accounts and configuring the authorized access privileges, and modifying or terminating access when the user’s job functions or access requirements change. The security process model also depicts automatic capture of information from Human Resources systems to add or terminate employees and contractors, if such a capability is available. Note that an HR feed of user information is not contemplated at the current time for FSA systems.

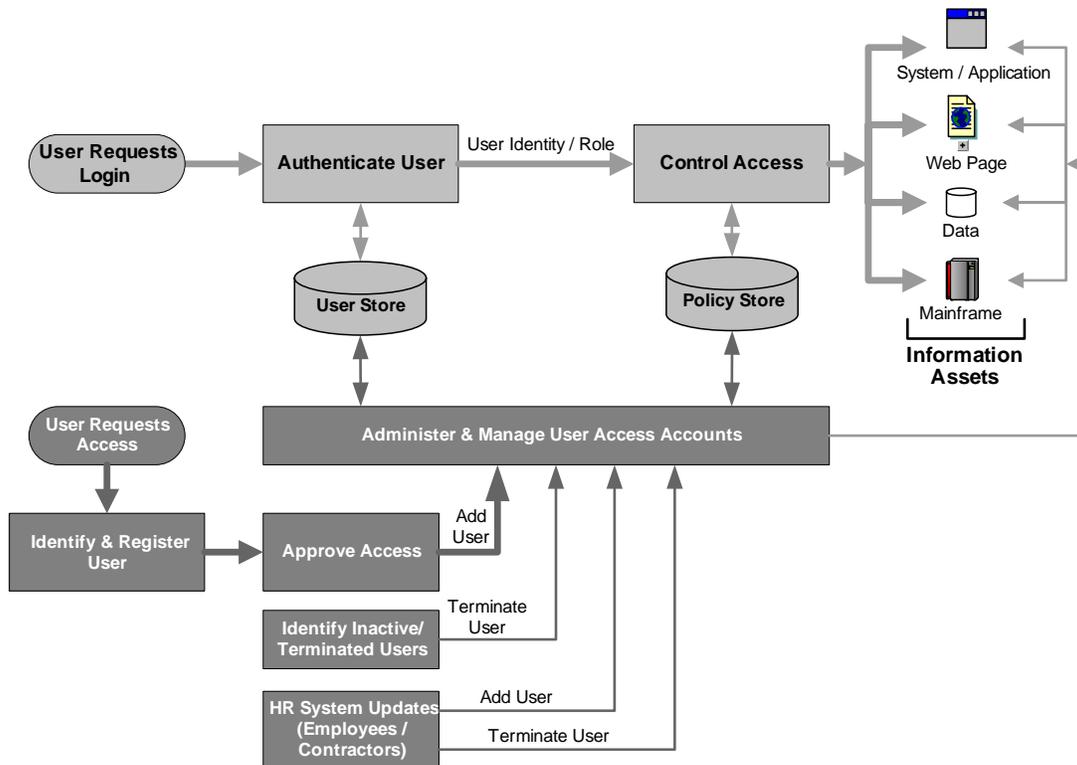


Figure 4.2 User Administration and Provisioning Processes

Security and Privacy Architecture Version 1.0

4.2.3 Audit and Logging Processes

Figure 4.3 adds to the model security processes for auditing and logging. Auditing and logging processes are shown in two different contexts:

- 1) Tracking user activity, such as requesting access, logging in to systems or applications, gaining access, viewing data, or executing system or application functions (e.g., modifying data or conducting transactions; shown in upper highlighted processes)
- 2) Auditing and reporting on user access privileges, including records of who approved a user’s access privileges, details of user account creating and administration, reporting on user access privileges on specific systems or application, or reporting on all access privileges granted to selected users across multiple systems and applications (shown in the lower highlighted box).

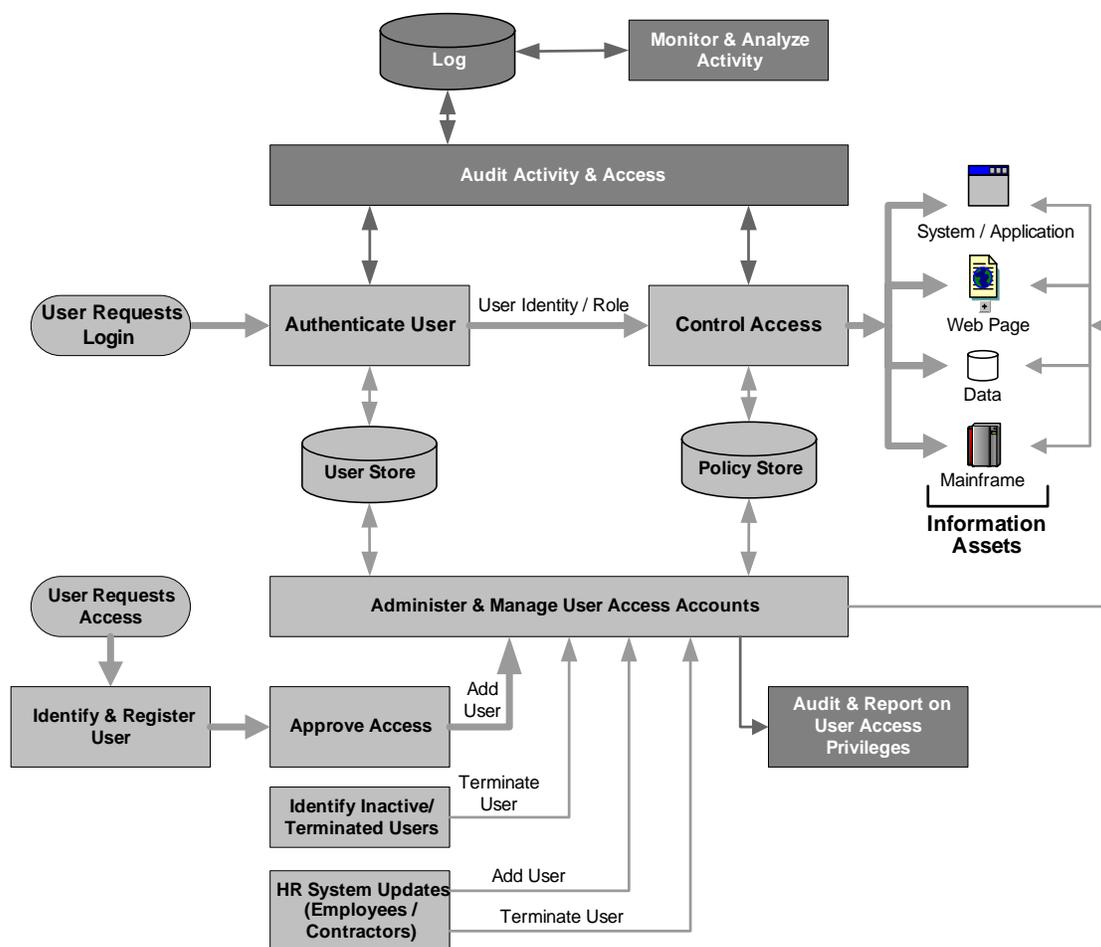


Figure 4.3. Audit and Logging Processes

4.2.4 Delegated Administration Processes

To offload the overhead associated with administering access for external users, a common step is to delegate responsibility for user administration to the external organization itself. This arrangement requires that contractual agreements be in place to define and enforce the transfer of

Security and Privacy Architecture Version 1.0

trust and responsibility assumed by the external organization. Typically, processes and tools implemented to control and monitor the privileges of security administrators associated with external organizations. Benefits of such an arrangement include a decrease in costs associated with managing external users, as well as placing the responsibility for assigning and monitoring security privileges in the hands of administrators with better understanding of the access privileges those users require.

Figure 4.4 adds functions to the security process model that for a delegated administration interface for external security administrators. The delegated administration process must also manage the administrative privileges to control the user population that can be managed and the type of access privileges that can be assigned to the external users.

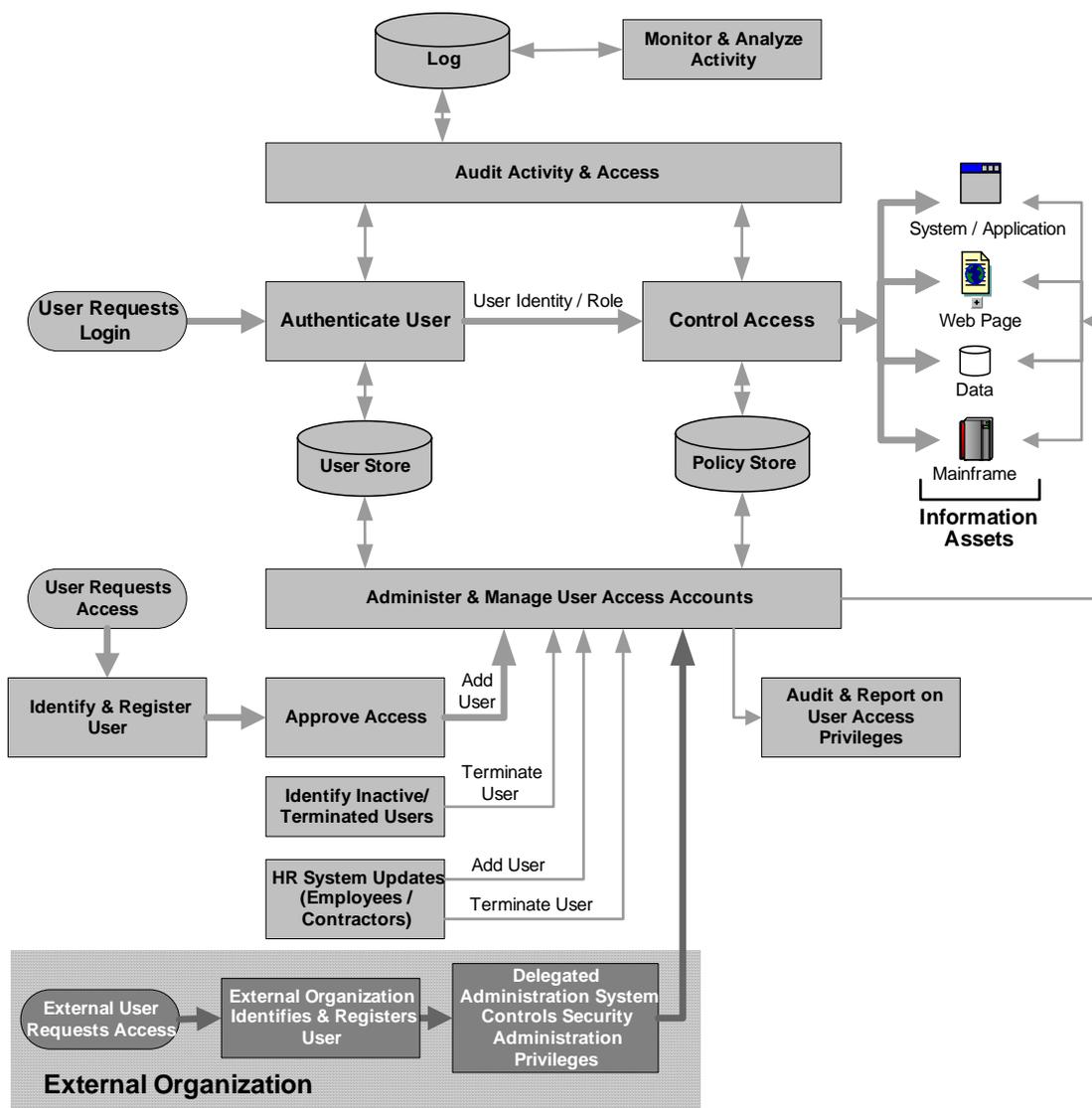


Figure 4.4. Delegated Administration Processes

Security and Privacy Architecture Version 1.0

4.2.5 Supporting Policy and Procedures

Security and privacy policy and supporting procedures are critical to the effectiveness of the Security Process Model for identity and access management. Table 4.1 shows a representative list of security policy, standards, and procedures typically implemented to define the configuration and operation of identity management functions. All of the policies, standards, and procedures should be developed consequent to a risk assessment of individual requirements for specific systems and users.

Most of the general policy covering these areas for FSA is documented in the FSA Information Technology Security and Privacy Policy (see Appendix X.X for a summary). However, supplemental standards and more detailed procedures may be needed to support new identity and access management services or systems.

Table 4.1 Example Policy and Procedures to Support Identity and Access Management Processes

Policy, Standard, or Procedure	Typical Content	Associated Security Process	Processes, Policy, or Procedures to Coordinate
Access Audit	<ul style="list-style-type: none"> • Standards for access privilege queries; • Standards for reporting on access; • Procedures for periodic review of access reports; • Procedures for requesting and reviewing access to investigate suspected incidents 	Audit & Report on User Access Privileges	Activity Logging; Audit Activity & Access
Access Termination	<ul style="list-style-type: none"> • Standards for periodic review of unused accounts • Standards for periodic review of terminated users • Procedures for disabling or removing access of terminated users 	Identify Inactive and Terminated Users; Administer and Manage User Access Accounts	Security Approval; Delegated Administration
Account Administration	<ul style="list-style-type: none"> • Common standards and procedures for adding, modifying, or removing user access • Standards and procedures for monitoring security administrator activities 	Administer and Manage User Access Accounts; Delegated User Administration	Security Access Approval; Delegated Administration; Security Approval; Security Termination; Audit and Report on User Access Privileges

Security and Privacy Architecture Version 1.0

Policy, Standard, or Procedure	Typical Content	Associated Security Process	Processes, Policy, or Procedures to Coordinate
Activity Logging	<ul style="list-style-type: none"> • Standards defining user activities that must be logged • Standards governing protection and archiving of activity logs • Standards defining activity log retention periods 	Audit Activity and Access	Access Audit; User Identification and Authentication; User Access Roles; Enterprise User Authorization
Delegated Administration	<ul style="list-style-type: none"> • Standards and procedures for selecting and approving delegated administrators • Policy for security administrator responsibilities that can be delegated external organizations 	External User Access Request; External Identification and Registration of Users; Delegated Administration	Security Access Approval; Account Administration; Security Approval; Security Termination; Audit and Report on User Access Privileges
Enterprise User Authorization	<ul style="list-style-type: none"> • Standards and procedures to classify data • Procedures to define and maintain access requirements for system users based on data classification and user job function • Procedures to define and maintain access control rules 	Control Access	User Access Roles; Security Access Approval; Identification and Authentication
Identification / Authentication	<ul style="list-style-type: none"> • Standards for collecting and validating user identification information • Standards to define level of authentication based on type of user and data classification 	Authenticate User	Security Access Approval; Enterprise User Authorization; User Access Roles; Control Access
User Access Roles	<ul style="list-style-type: none"> • Standards and procedures to define and maintain user access roles • Standards and procedures to assign users to roles 	Control Access	Security Access Approval; Enterprise User Authorization; User Access Roles; Identification and Authentication

Security and Privacy Architecture Version 1.0

Policy, Standard, or Procedure	Typical Content	Associated Security Process	Processes, Policy, or Procedures to Coordinate
Risk Assessment	<ul style="list-style-type: none"> • Standards and procedures for conducting risk assessments of identity management functions • Standards and procedures for conducting risk assessments of delegated administration functions 	Develop Policy and Procedures for Identity Management Functions	Access Audit; Access Termination; Account Administration; Activity Logging; Delegated Administration; Enterprise User Authorization; Identification / Authentication; User Access Roles; Security Access Approval
Security Access Approval	<ul style="list-style-type: none"> • Access request procedures and forms • Access approval standards and forms • Approval routing procedures • Approval communication procedures 	Approve Access; Delegated Administration	Access Termination; Identification and Authentication; Enterprise User Authorization; User Access Roles

5 FSA Security and Privacy Business Requirements

5.1 Introduction

FSA Security & Privacy business objectives were collected through meetings, security workshops, and discussions with the Business Integration Group. Meetings were conducted with key FSA business and technical personnel. Security workshops were held to stimulate discussion of standards and business requirements with FSA, Integration Partner resources, and key contractors. The business objectives were used to formulate and validate the services and components included in the Security and Privacy Architecture Framework.

5.2 Business Objectives & Proposed Security Requirements

The following section describes FSA high-level business objectives and assigns priorities based on the results of the workshop and related discussions. The proposed security requirements, shown below, are used to validate with the proposed FSA Security Architecture and Privacy specification in section 7 of this document. The business objectives questionnaire was circulated to meeting and workshop participants for comment. All feedback received has been incorporated in the validation of requirements and assignment of priorities.

The ‘Priority’ column in the table indicates whether most contacts described the objective as an immediate need (I) or an objective that is either: 1) desirable but not critical, or 2) may be needed in the future.

	High-Level Business Objective	Proposed Objective	Description	Priority I = Immediate F=Future
1.0	Manage Access Control access of individual users and system entities to FSA systems, networks and data			
1.1		Identification and Registration	Provide consistent identification and enrollment/registration of users and the access level required	I
1.2		Entity Authentication	Authenticate users and entities who request login to FSA systems and applications	I
1.3		Authentication Levels	Provide different levels of authentication according to user role and resources that will be accessed	I
1.4		Simplified Sign-on	Reduce the need for multiple logins and passwords for groups of systems or applications commonly used together	I
1.5		Access Control System	Provide access control mechanisms that systems and applications can use to manage	I

Security and Privacy Architecture Version 1.0

	High-Level Business Objective	Proposed Objective	Description	Priority I = Immediate F=Future
			information assets available to users	
1.6		Role-based Access Control	Base user access on roles to provide standardized, consistent "need-to-know" access privileges	I
1.7		Access rule flexibility	Access rule flexibility: provide flexible access control rules based on business logic	I
1.8		Call External Systems or Files for Authorization Data	Provide method for access rules to communicate with external systems or files to obtain information needed for controlling access to resources based on user roles or business logic	I
2.0	Administer & Provision Access Approve, assign, and maintain access of entities (individual users and system users) to FSA information assets (systems, applications, and data)			
2.1		User Access Account Management	Improve the consistency and efficiency of managing users access accounts on FSA systems and applications	I
2.2		Security Approval Workflow Tools	Improve the efficiency of user provisioning by automating workflow processes for access requests, security approvals, and personnel clearances	F
2.3		Consolidate Security Repositories	Consolidate the management and maintenance of user security data repositories	F
2.4		Manage Repositories	Increase the efficiency and accuracy of directory administration and management	F
2.5		Password Management	Enforce policies to improve password authentication methods	I
2.6		Password Resets	Simplify the password reset process for users and administrators	F
2.7		Password Synchronization	Automatically synchronize passwords across systems	F

Security and Privacy Architecture Version 1.0

	High-Level Business Objective	Proposed Objective	Description	Priority I = Immediate F=Future
2.8		Delegated Administration	Distribute user security administration to partner organizations to decrease costs and improve accuracy	I
3.0	Audit Access View and report on user activity and access to FSA systems and data			
3.1		Audit User Access Privileges	Provide effective, accurate methods for auditing access requests, approval actions, and assigned access privileges	I
3.2		Log User Activity	Consistently track and report on user activity on sensitive systems, applications, and data	I
3.3		Archive Audit Data	Maintain audit information securely for defined time period	I
3.4		Report Access	Provide a convenient, effective way to view and report on access privileges of users across multiple systems	I
4.0	Protect Data Protect the confidentiality and integrity of FSA data			
4.1		Confidentiality of Transmitted Data	Maintain confidentiality of FSA information by encrypting data during transmission across networks	I
4.2		Confidentiality of Stored Security Data	Maintaining the confidentiality of stored security data	I
4.3		Secure File Transfer	High volume trading partners need options for transmitting secure data	I
5.0	Sign Transactions Authenticate the authorship and content of FSA online transactions			
5.1		Strong Authentication	Provide strong authentication methods suitable for users signing online transactions electronically	F
5.2		Notarization	Provide digital notarization functions to timestamp and datestamp transactions	F

Security and Privacy Architecture Version 1.0

	High-Level Business Objective	Proposed Objective	Description	Priority I = Immediate F=Future
			timestamp transactions	
5.3		Audit Electronic Signatures	Provide audit tracking and reporting for details of authentication and user activity related to electronically signing transactions	I
5.4		Non-Repudiation	Be able to prove the origination details and validate the content of online transactions to prevent repudiation	F
6.0	Protect FSA Infrastructure Monitor and control access to FSA networks, information systems, and data centers			
6.1		Control Network Access	Monitor and filter unauthorized network traffic that could compromise the integrity or availability of FSA networks and systems	I
6.2		Block Malicious Code	Filter harmful software (such as viruses, worms, trojans, and malicious mobile code) to prevent damage to FSA systems or data	I
6.3		Detect and Prevent Intrusions	Monitor FSA networks and systems for activity that could indicate potential security attacks and produce alerts or take automated actions to prevent or limit the attack	I
6.4		Monitor Network and System Security	Monitor the overall security posture of FSA networks and systems by analyzing and correlating security data from network devices, intrusion detection systems, system logs, etc.	I
6.5		Detect System and Application Security Vulnerabilities	Provide procedures, standards, and tools to detect and address security vulnerabilities in FSA systems and applications	I
6.6		Manage Updates, Patches, and System Configuration Changes	Provide methods to efficiently detect and deploy system patches, updates, or fixes, and to maintain the integrity of FSA systems and applications	I
6.7		Physical Security	Control and monitor physical access to FSA data centers and systems	I

Security and Privacy Architecture Version 1.0

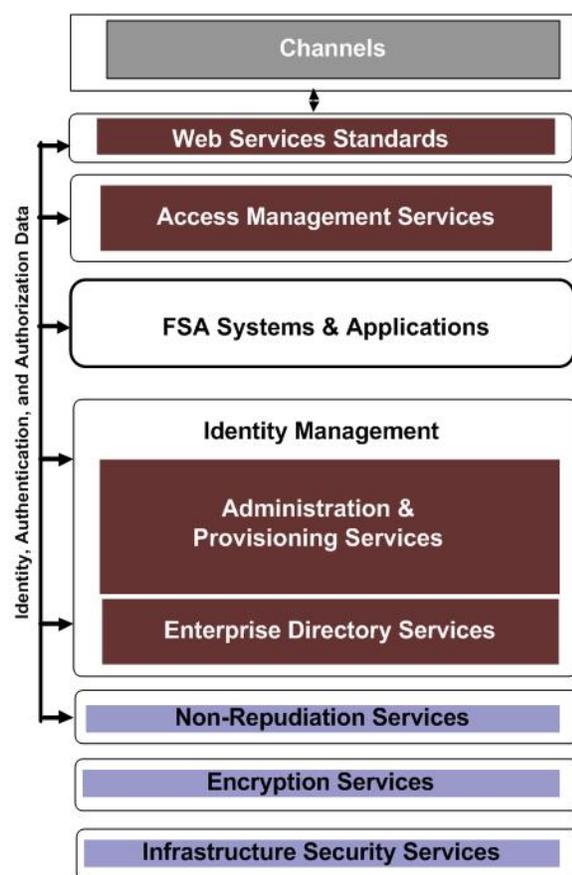
	High-Level Business Objective	Proposed Objective	Description	Priority I = Immediate F=Future
6.8		Environmental Security	Control and monitor the physical environment of FSA data centers and systems to mitigate damage from natural or man-made disasters	I

6 Proposed FSA Security and Privacy Architecture

6.1 Security and Privacy Architecture Vision

The proposed FSA Security & Privacy Architecture defines a consistent and coherent set of security services that provide integration points and identifies technology directions for FSA systems and applications to effectively and efficiently meet FSA security and privacy objectives. Additionally, it provides guidance for application developers and business owners in the selection of appropriate security controls to address risk. Consequently, the proposed FSA Security and Privacy architecture promotes the reuse of security components in order to reduce deployment and development costs of existing and new applications. Nevertheless, the proposed FSA Security and Privacy Architecture is flexible enough to respond to changes in requirements, technologies, and security threats over time. Finally, the proposed FSA Security and Privacy Architecture is vendor and service provider agnostic, meaning that it can be implemented with a variety of technology products or service (in-sourced or outsourced) providers.

6.2 Security and Privacy Architecture Overview



The primary focus of the proposed security and privacy architecture specification discussed in detail below is security technology services, it is important to emphasize that few security solutions will consist solely of technical mechanisms. In most cases, security objectives can only be achieved with though integration of security policies and processes with other security controls. More commonly, security objectives will dictate a combination of procedural and technical controls based on appropriate supporting processes and management structures.

The following sections provide an overview of how a variety of security components can be integrated as whole to provide enterprise security services. The proposed security and privacy architecture will describe the security components that could provide reusable security services to most applications. For example, web applications can leverage the use of authentication services to address the security requirements of different authentication levels. As illustrated in the diagram to the left, this is a an overview of the proposed FSA security and privacy architecture,

with identity and access management components highlighted in red to indicate their focus as the subject of the detailed descriptions in section 6.3.

Security and Privacy Architecture Version 1.0

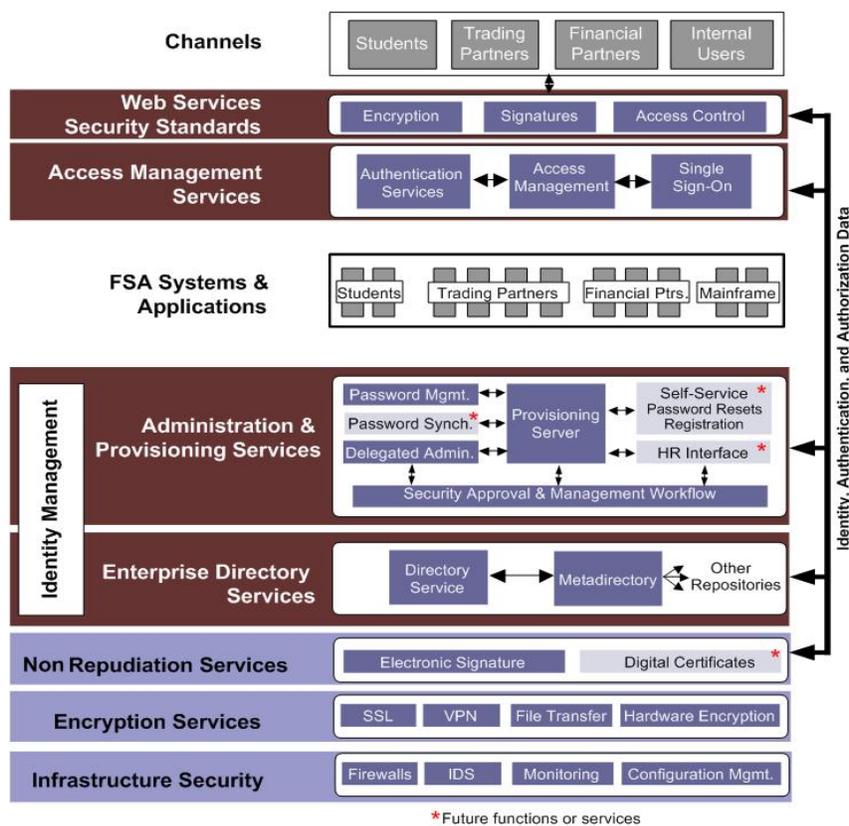
6.3 Technical Services and Components

The proposed FSA Security and Privacy Technical Architecture defines security services and components that can be used to implement security controls. Technical security components rarely, if ever, function without the support of appropriate security management structures and security processes. Security management activities, such as strategy development and risk management, are critical to the selection and deployment of technical controls that achieve the desired security objectives. Support processes for the operation, maintenance, and upgrade of technical security systems are vital to their effectiveness.

Technical security components are classified for convenience into the following categories, illustrated below, and explained in detail in Section 6.3.

- Web Services Security Standards
- Access Management services
- Administration & Provisioning Services
- Enterprise Directory Services
- Non-Repudiation Services
- Encryption Services
- Infrastructure Services

Proposed FSA Security and Privacy Technical Architecture



6.3.1 Web Services Security Standards



Web services standards provide standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available. Used primarily as a means for businesses to communicate with each other and with clients, Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

Unlike traditional client/server models, such as a Web server/Web page system, Web services do not provide the user with a GUI. Web services instead share business logic, data and processes through a programmatic interface across a network. The applications interface, not the users. Developers can then add the Web service to a GUI (such as a Web page or an executable program) to offer specific functionality to users.

Web Services Security Standards major functions include

- Encryption
- Signatures
- Access Control

Definitions

- **WS-I Security** - WS-I is an open, industry organization chartered to promote Web services interoperability across platforms, operating systems, and programming languages. The organization works across the industry and standards organizations to respond to customer needs by providing guidance, best practices, and resources for developing Web services solutions. The WS-I intends to give corporations guidance on how to use security effectively with Web services in different business situations and clarify any ambiguities in the security specifications for IT providers.
- **Extensible Markup Language (XML) documents** are made up of storage units called entities, which contain either parsed or unparsed data. Parsed data is made up of characters, some of which form character data, and some of which form markup. Markup encodes a description of the document's storage layout and logical structure. XML provides a mechanism to impose constraints on the storage layout and logical structure
- **XML Encryption** will provide an encrypted key mechanism and a method for providing a Uniform Resource Identifier (URI) for a known key. It will support XML Signature's selective signing, and will support or interoperate with XML Schemas.
- **XML Signatures** are digital signatures designed for use in XML transactions. The standard defines a schema for capturing the result of a digital signature operation

Security and Privacy Architecture Version 1.0

applied to arbitrary data (often XML). XML signatures add authentication, data integrity, and support for non-repudiation to the data that they sign.

- XML Key Management Specification (XKMS) defines protocols for the registration and distribution of public keys. The keys may be used with XML Signatures, a future XML Encryption specification, or other public key applications for secure messaging.
- XML Access Control Markup Language (XACLM) is a framework for defining a set of privileges required to perform an operation, including access to identity information and external functions (like access policy and time of day).
- Security Assertion Markup Language (SAML) defines mechanisms to exchange authentication, authorization and non-repudiation information, allowing single sign-on capabilities for Web services. Additionally, SAML is a framework for exchanging identification information; for example, a trusted third-party (such as a PKI CA or a network login server) could provide a signed set of assertions identifying my identity. SAML is the basis of the Liberty Alliance federated single sign-on facility; Microsoft may also adopt Passport to use it.

Benefits of deploying web services security standards

Web services are leveraged to exchange data between heterogeneous applications. Web services security standards provide the capability to securely exchange information that would otherwise be easily readable as its transmitted in clear text. Consequently, web services security standards provide a framework that enables organizations to embed security services, like encryption, signatures, and access control, in their markup language. As a result, organizations can achieve message security without having to rely on the transport protocol (i.e. SSL) for security services.

Additionally, use of web services security standards like SAML enables organizations to exchange identity and access management information between trading partners. Therefore, establishing trust and removing some of the intrinsic complexities of integrating dissimilar identity and access management systems. However, web services security standards are needed to secure the exchange of messages between organizations. Finally, web services security standards provide a set of reusable security services that can be leveraged to effectively secure XML messages between applications.

Implementation & integration considerations:

Secure messaging

WS-Security defines a standard set of extensions that implement message-level integrity and confidentiality for secure message exchanges. WS-Security enables the maintenance of a secure context over a multi-point message path. It denotes three Web participants—a "sender" Web service, an "intermediary" Web service, and a "receiver" Web service. Rather than carrying a separate security context from one participant to another (as would be necessary using SSL/TLS), WS-Security allows the security context to be carried over the entire interaction. WS-Security is designed to support a wide variety of security models—i.e. it is designed to support multiple security token formats, multiple trust domains,

Security and Privacy Architecture Version 1.0

multiple signature formats, and multiple encryption technologies. This includes existing security models, as well as security models that may be released in the future. Examples of "security tokens" are: a username/password, an X.509 certificate, a Kerberos ticket, or a Security Assertion Markup Language (SAML) assertion.

Liberty Alliance

The Liberty Alliance Project is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way. The role of the Liberty Alliance Project in all of this is to support the development, deployment and evolution of an open, interoperable standard for federated network identity. The Liberty Alliance is comprised of 150 member companies representing a wide variety of industries and over a billion customers, with operations all over the globe. Each of the member companies either owns and operates large communities of interest or is the developer of core technology that can enable a federation of online communities. However, membership in the Alliance is still open and all organizations are invited and encouraged to join. Consequently, GSA and DOD recently announced that they joined the Liberty Alliance project in effort to standardize web authentication.

6.3.2 Access Management Service



The access management layer provides authentication, single sign-on, and policy enforcement services. Access management services enforce user access rights that are transparent to the user once they successfully authenticate. Contrary to identity management services, access management services are not typically used to provision accounts across the enterprise. However, a successful implementation of access management services is contingent on the fact that identities are managed effectively and properly. As a result, access management services are dependent on identity management services to grant access to a system or application.

An integral feature of Access Management systems is the centralized application of security policy to perform access control. Access management functions protect information systems by mediating access of internal or external users to specific application data, function, or other resources. Access Management systems typically integrate authentication services, and access control capabilities with directory services, and administrative functions. Additionally, Access management systems enable centralized administration of security policy to enforce access control rules.

Access management systems include includes role-based access control, federation of identity across multiple organizations, and single or reduced sign-on for groups of applications. Ancillary functions that may be incorporated into Access Management include password synchronization, enforcement of password policies and other authentication credential requirements, support for multiple authentication mechanisms, password reset capabilities, self-service registration

Security and Privacy Architecture Version 1.0

functions, security approval workflow, and automated user account updates fed by Enterprise Resource Planning systems.

The major components of the Access Management Layer include:

- Authentication Services
- Access Management Server
- Single Sign-On Services

Each of these service components are discussed in greater detail below, including relevant definition, integration points, and implementation considerations.

Authentication

Authentication is the process of validating a user credential associated with a previously identified entity. Authentication within computing systems encompasses both users and systems or processes. Typically, a user wishing access to a system presents credentials (such as a password, token, digital certificate, or biometric characteristic) that is validated by comparison with or analysis of information or characteristics collected during registration of the entity. Authentication services are required by any system that must restrict use to a defined set of users. Establishing an authenticated identity is also critical to several other security functions required to maintain individual accountability, such as assigning access privileges, auditing user activity, or asserting authorship of a transaction. As a result, it is possible to use multiple authentication methods to provide a level of assurance commensurate with the sensitivity of the systems being accessed or the information being requested

Definitions

- Username/Password - Username and passwords are a combination of an identifier and a shared secret, typically an alphanumeric string of characters. Username and password authentication mechanisms are the most commonly deployed, but suffer numerous, well-documented shortcomings and vulnerabilities.
- Strong Authentication – is the process of identifying an individual to fulfill the requirements of an application that requires stronger assurance of identity. Strong authentication mechanisms are typically integrated with the deployment of tokens, smart cards and biometric devices.

Benefits of Deploying Authentication as a Service

Authentication services can be leveraged to supply a range of authentication mechanisms and provide appropriate protection to resources in a cost-effective and manageable manner that balances cost and risk. Based on a risk assessment, application owners can integrate authentication services to replace embedded application authentication mechanisms. Authentication services enable applications owners to reduce the time of deployment and total operations cost of authentication solutions. This is accomplished by spreading the cost across multiple environments that leverage the authentication mechanisms instead of deploying independent solutions. Additionally, it allows organizations to centrally support various authentication technologies to address each situation and risk. Finally, it presents the possibility in the near future for organizations

Security and Privacy Architecture Version 1.0

to federate authentication using third party assertions between domains or trading partners.

Implementation and integration considerations:

Password Authentication Mechanisms vs. Strong Authentication Mechanisms

Password authentication mechanisms include the combination of username and passwords to validate the identity of a user. Username and passwords mechanisms are the most commonly deployed standard authentication mechanisms to authenticate users. However, username/password mechanisms suffer numerous shortcomings and vulnerabilities. For example, passwords can be “brute forced” in a short timeframe with dictionary attacks.

Alternatively, strong authentication mechanisms provide additional credentials to increase the resilience of the system to such attacks and add assurance to the validation of a user identity. Usually strong authentication mechanisms leverage multiple authentication methods to provide a level of assurance commensurate with the sensitivity of information being accessed. At the same time, strong authentication mechanisms need to be aligned with data classifications standards and business objectives to appropriately select adequate security controls.

Typically, strong authentication mechanisms integrate with a variety of architecture components and systems. Because of this, it’s important to conduct a thorough evaluation of strong authentication mechanisms, business processes, and system requirements to avoid overlooking possible compatibility issues and mandatory technical requirements that may impede a successful implementation.

Access Management

Access Management consists of processes and tools that regulate the access privileges of entities (either users or processes). An Access Management system ensures that an authenticated user has sufficient rights to perform required operations.

Access Management can be implemented with static access control lists (ACL’s), dynamic rules based on business logic, or some combination. ACL’s contain a list of rights to data or functions that a user can perform on an object, such as read, write, and execute. However, access rules based on context or business logic can make more sophisticated access decisions that analyze the current state of the user. ACL’s and business rules are usually stored within the Access Management system, typically in the same directory or database repository that houses user security data.

Definitions

- Objects – an object can be any system resource subject to access control, such as a file, printer, terminal, database record, etc.
- Operations - An operation is an executable image of a program, which upon invocation executes some function for the user.
- Permissions - Permission is an approval to perform an operation on one or more protected objects.

Security and Privacy Architecture Version 1.0

- **Role** - A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.

Benefits of deploying role based access control (RBAC) technologies

Role based access control (RBAC) implementations primary benefit is the decrease of overhead in the assignment and management access rights privileges across the enterprise. Additionally, it segregates management of access privileges and reuses access roles profiles reducing complexity. Also enables automation, which reuses past work, and possibly reduces the number of administrators that perform access management functions. As a result, RBAC models have shown its relevance in meeting the complex needs of Web-based applications.

RBAC models bring simplicity by using role hierarchies and constraints. In addition, security administration is also greatly reduced by the use of roles to organize access privileges. For example, if a user moves to a new function within the organization, the user can simply be assigned to the new role and removed from the old one, whereas in the absence of an RBAC model, the user's old permissions would have to be individually revoked, and new permissions would have to be granted. Furthermore, using constraints on the activation of user assigned roles, users can sign on with the least privilege set required for any access. In case of inadvertent errors, such least privilege assignments can contain damage.

Implementation and integration considerations:

Role-Based Access Control (RBAC)

The basic concept of RBAC is that users are assigned to roles, permissions are assigned to roles and users acquire permissions by being members of roles. As well, a RBAC mechanism should require that users could simultaneously exercise permissions of multiple roles. Furthermore, hierarchical RBAC adds functions for supporting role hierarchies. A hierarchy is a partial order defining a seniority relationship between roles that acquire the permissions of their juniors, and junior roles acquire the user membership of their seniors. Additionally from a policy perspective, separations of duty relations are used to enforce conflict of interest policies. Conflict of interest in a role-based system may arise because of a user gaining authorization for permissions associated with conflicting roles.

Typically, RBAC functionality is embedded in the native application and operating system mechanisms. However, the functionality that a RBAC system provides can be flexibly integrated by the use of web access control products. Web Access control mechanisms allow administrators to hierarchically assign users to roles with the appropriate object permissions to perform a task. Even though web access controls functionality can be limited to session management, overseeing the authorization function of the native application layer.

Security and Privacy Architecture Version 1.0

Web Services & Federated identity

Web Services security mechanisms provide the ability to assemble solutions dynamically from a series of application services operating to common standards. Because Web services are built using existing standard Internet technologies, they are agnostic to any particular technology platform. Additionally, Security Assertion Markup Language (SAML) is a web services standard that enables the exchange of authentication and authorizations information. By leveraging SAML, authentication and authorization assertions, organizations can establish transitive trust to obtain access to resources. Consequently, by leveraging web services security standard organizations are implementing a federated identity model that enables faster integration between heterogeneous environments. As a result, federated identity provides a flexible identity and access management architecture for establishing trust and exchanging credentials between trading partners. Similarly, SAML mechanisms can be used to exchange authentication, authorization and non-repudiation information, allowing single sign-on capabilities for Web services.

Single Sign-On (SSO)

Single Sign-On authentication provides access to two or more applications following a single login. Additionally, it reduces or eliminates the need for the user to enter further authentications when switching from one application to another. Single Sign-On is typically deployed to streamline the authentication process for users. Single Sign-On mechanisms can be integrated in various ways in a heterogeneous environment. A Single Sign-On system could be integrated with the operating system (OS) Login/Logout process. Many Single Sign-on products only provide encryption between the SSO client and the SSO server, ignoring encryption between clients and applications servers. In other words, an approach to securing communications of a Single Sign-On system is one that secures the management and application transport channel. Similarly, SSO integrates with multiple authentication mechanisms to address different authentication requirements.

Definitions

- Policy Server- defines and enforces “business” rules for applications logical operations including authentication, authorization, administration, session management, and auditing. Generally, policy servers can store policy and user information in existing directories and databases, and does not require the installation of an application specific repository.
- Repository – stores all the policy and user information. Usually the repository may be an Oracle database, SQL server, LDAP directory or a proprietary database repository.
- Server Agent – an agent is frequently a small application that performs a specific task in a server. Usually SSO server agents intercept resource request and re-direct communication to the authentication and policy servers.

Security and Privacy Architecture Version 1.0

Benefits of Single Sign-On Technology

Single Sign-On technology is being implemented to tackle the problem of access management in highly fragmented environments with a variety of applications and systems. SSO merges enterprise requirements for cost containment, security administration, and ease of use by making it transparent to the end-user. SSO achieves this through authentication at the beginning of a session, thus eliminating authentication prompts as new applications or resources are requested. Additionally, SSO can consolidate user administration resulting in fewer help desk password inquiries by choosing to leverage a consolidated view of access profiles, and a central point of password administration. Users only need to sign-on once to access all authorized systems as SSO takes care of all additional logins. Also minimizes the time spent on login procedures as login only happens once per session. As well, SSO minimizes the trial and error process when login incorrectly because users will have only a single password and user ID to remember.

Single Sign-On Implementation and Integration Considerations

SSO Identity

An SSO system crosses many identity stores usually under different departmental and system administration boundaries. Within many organizations, there will be confusion over the definition of what constitutes an identity, role, accounts, and the unique ID used for these. It may be the case that an individual assumes several identities with each having one or more roles along with unique ID's for the roles and/or the identities. Indeed a crucial step of a SSO project is the need to be confident that there is a one-to-one mapping between a unique ID and a person. Unfortunately, many systems may not communicate well or at all with each other in providing identity updates. For instance, a SSO system might still allow a particular identity into the applications months after the person whom the identity maps was terminated. Therefore, having a thorough understanding of identities, roles, and people is critical in implementing a successful SSO system. Without this, you may be opening yourself to additional, unplanned, unbudgeted time, money, and resource allocations.

SSO Authentication

SSO authentication requires careful planning by the organization to determine what authentication mechanisms are acceptable for different applications. For instance, the use of a username and password may be an acceptable risk for authenticating a student but this mechanism can be considered weak to authenticate trading partners that have access to a broad set of privacy act data. An SSO tool needs to be flexible for different authentication levels as allow room for future technologies and changes to security policies. Additionally, there are many things to consider like app-to-app authentication, integration with SSL, SOAP, XML and web services security.

Security and Privacy Architecture Version 1.0

SSO Authorization

SSO authorization begins with some type of post-authentication action. Equally important is how a change in authorization models and/or applications makes its way to the SSO system. Further, it is useful to create use scenarios for authorization exceptions. Application security management is full of exceptions that require focus on testing and managing SSO authorization rules. Oftentimes, changes need to be made to business processes, management models, and code in the SSO product and applications. In any event, it's essential to understand the business process in great depth to clearly analyze how the SSO system fulfills those business requirements.

SSO Session Management

Each application you integrate into the SSO is going to have its own session management conditions based on risk for timeouts and logouts. Therefore, the creations of session management standards are necessary to decide how to provide exceptions to the standard applications. For instance, what are their idle session timeouts, what is the application maximum session timeouts, what are the user and application logout procedures? After all, there is a need for caution when it comes to integrating session management requirements with applications such as portals, proxies, and others as it may require lots more planning, coding, workarounds, time, and expense than anticipated.

SSO Auditing

While many applications will have their own in-depth security mechanisms, it's important to have an end-to-end audit view of all applications touched by a user during a SSO session. In general, it makes sense to have a high level overview of what applications a user touched during a session and when they did it. Additionally the SSO can provide audit granularity by specifying which HTTP actions are going to be monitored because of audit rules. Indeed the SSO system should trigger alarms from audit log information in near real time. Furthermore, business and technical processes should be built into the SSO system to monitor disk usage and performance implications.

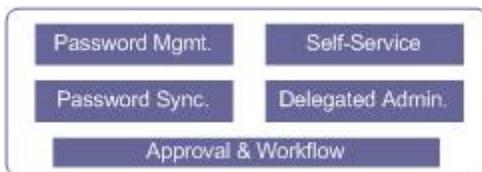
SSO architecture

SSO functionality is frequently integrated via an agent-based model with a policy server and repository service as core components of the system. It also relies on session cookies to manage sessions and re-authenticate users across different systems. Typically, SSO products are integrated with the use of reverse proxy architecture to intercept traffic and back-end policy and directory servers for authorization and entitlements evaluation. Because the reverse proxy architecture can represent a single point failure, additional consideration should be taken to enable high-availability and disaster recovery of this component. Another approach to SSO uses scripting to automate the login procedure. The scripting approach is a simple approach to avoid being invasive in either the client or server. Scripts can be designed in a variety of programming languages although most vendors offer pre-built scripts for a wide variety of systems. Regardless,

Security and Privacy Architecture Version 1.0

most applications have different identity repositories that need to be aggregated and consolidated. Instead of application authenticating users themselves, the SSO architecture should implement a solution that leverages a central repository and authentication mechanism. However, not all applications may be able to seamlessly integrate with this centralized approach.

6.3.3 Provisioning



Provisioning mechanisms collect, manage, and communicate user identity and access privilege information through the administrative interfaces of applications, operating systems, and other managed platforms. In contrast to authentication and access control mechanisms, provisioning systems do not mediate real-time security decisions. Instead, they provide account setup, management, and other centralized support functions critical to the effective assignment and monitoring of user identities, access authorizations, and audit records. Traditionally, setting up access privileges for new users has taken days, if not weeks, to complete, delaying access workers need to do their jobs. A key function of provisioning mechanisms is the automation of account setup, allowing new users to be immediately productive when joining an organization. In addition, automated account management functions facilitate local flexibility and rapid response to changes in personnel, roles or policies, most importantly to terminate an account when a user leaves or no longer requires access.

Provisioning service major functions include:

- Password Management
- Password Synchronization
- Delegated Administration
- Self-Service
- Approval & Management Workflow

These service components are discussed in detail below, including relevant component definitions, integration points, and implementation considerations.

Definitions

- Provisioning – refers to the automation of digital resources for an employee, partner or customer. Provisioning streamlines the completion of provisioning tasks by automating the process based on people’s business profiles. At its, core provisioning translates business needs into IT tasks and ensures their completion while automating the process wherever possible.
- Provisioning manager/engine – functions as a central point of control and enforcement of security policy over managed systems. In addition, it enables management of resource access assignment and of immediate revocation of all access rights upon termination of business relation.

Security and Privacy Architecture Version 1.0

- Provisioning data repository – links disparate account repositories throughout the organization into a single point of centralized management.

Benefits of deploying provisioning technology

Organizations are constantly granting, modifying and revoking access rights. Often, the time to assign accounts rights for new employees can range from days to weeks. Likewise, the number of employees supported by administrators may seem unreasonable taking into consideration the average timeframe it takes to assign user rights across the enterprise. However, a provisioning solution can streamline the process by automating the deployment of user access to systems, applications and resources.

Fundamentally, a provisioning solution will automate and reduce the time to deploy user access in the organization. It will enhance your operations by replacing manual processes with an automated workflow component that can route request for access rights to designated authorized individuals. At the same time, it synchronizes and propagates access rights changes with the majority of systems and applications in the organization. Additionally, it enables end-users to self-service and password management obtaining the benefit of fewer related password helpdesks calls while reducing support costs and increasing productivity of new joiners. In conclusion, it supports the deployment and compliance of policies for providing user access to enterprise resources.

Implementation & Integration considerations

Process Management

Provisioning software should be able to manage a complicated process operating across multiple systems both internal and external to the organization. Usually the entire provisioning process is not only complex, but also highly interrelated with many tasks depending on prior completion of other tasks. Activities must be coordinated so that all aspects of provisioning runs smoothly; task dependencies, as well as processes that take considerable time should be taken into account. An escalation procedure should exist so that if the problem is without resolution after a given time another e-mail notification is sent to the administrator, or even to a different person if desired. There should also be reporting features that help identify where problems exist in the provisioning process in order to find ways to resolve those problems.

Automated workflow

A provisioning solution needs to supply a comprehensive automated workflow engine that can control and monitor the delicate processes related to assigning people with access rights to mission critical systems. Automation is faster than manual processing, reduces the need for administrative staff and decreases the timeframe attached to manual authorization. Automation also helps ensure timely “termination” of employees or business partners who leave the organization. Workflow enabled provisioning mechanisms can be configured to notify people or other applications to begin the work required to provide a resource to an individual. Requests are automatically routed through an electronic process to approvers that can grant, terminate or modify access permissions. Administrators and those submitting requests can use a variety of options to monitor request status. In other words, the workflow solution must allow non-technical users to make workflow changes rather than having to fit individuals into pre-defined,

Security and Privacy Architecture Version 1.0

“static” roles which may not reflect their actual responsibilities. Additionally, workflow links can be provided through API’s to other applications, or with web services” protocols such as XML.

Self-service Password management

Typically, provisioning password management modules enforce configurable password policies to facilitate the creation, modification, and terminations of accounts. A self-service password management application enables an end user to perform password changes independently. This system provides the capability to automate the password reset function, allowing the user to authenticate to the system using a personalized challenge-response approach. For example, an employee may spend considerable time obtaining new passwords from the help desk. On the contrary, a provisioning solution will enable an end-user to reset their password within minutes by visiting a web site. Finally, a provisioning solution reduces most of the password management inefficiencies by creating a single management point from which business owners can automate password policies.

Synchronization

Organizations with heterogeneous computing environments typically have end-users with multiple accounts and different passwords for each system, platform or application. The synchronization functionality decreases the need for end-users to remember numerous passwords. Using the password synchronization capability, a change in the end-user’s password can be automatically propagated to all IT resources to which the end-user has access rights. Organizations have the alternative to allow end-users to synchronize their passwords across all their accounts, including legacy and web-based applications.

Delegated Administration

Delegated Administration allows distribution of account management tasks to designated administrators who are responsible for specific subsets of users. Typically, delegated administration tasks are subdivided based on organizational structure. Consequently, delegated administrators can properly assign defined access roles and privileges while maintaining central control of account management functions. After all, delegated administration provides a highly granular model for delegating administrative capabilities to other departments and organizations. Additionally, it decreases, the administrative overhead associated with user account management.

Directory and ERP integration

Rather than requiring HR personnel or administrators to manually add or change user information as IT resources are assigned, modified, or deleted, a provisioning solution programmatically updates the information in all enterprise repositories including directories and ERP systems. This integration with ERP and directory systems enables the organization to streamline the mapping of user identities as they join, move or leave the organizations. Consequently, much of what is done for provisioning involves security, thus the provisioning application must work in tandem with enterprise security subsystems to control access to resources in a manner that expedites task completion and minimizes associated cost.

Security and Privacy Architecture Version 1.0

Reporting, tracking and auditing capabilities

A provisioning application must supply the ability to monitor and report on all aspects of the provisioning progress from a variety of perspectives. Additionally, provisioning tools record changes to the access rights or other resources granted to users, as well as modifications to the access policies themselves and pinpoint the type of business change that triggered the access right modifications. Such audit trails help IT and security managers verify compliance with service level agreements and corporate security policies, as well as with legal or regulatory security requirements. After all a mechanism of reporting, tracking, and auditing has to be in place to provide reports about the various IT processes and outcomes resulting from business activities. Each task in the process could be logged, maintaining not only the history of each change for a particular person, but the linkage with the business reason for that change.

Provisioning Architecture

Enterprise provisioning is typically deployed in two forms: agents and agent-less. Provisioning agents mediate the provisioning of accounts on the end-systems. Nevertheless, there is the notion in which agents are usually considered invasive with performance implications. Also agent-based solutions often require time-consuming design plans to deploy and configure the provisioning agent on the end system. On the other hand, agents can be tightly integrated to perform provisioning functions minimizing the network load for data gathering. On the other hand, agent-less provisioning solutions leverage the use of scripts and OS login procedures to provision accounts on end-systems without having to install agents or software on production systems. However, some other system needs to poll the target system and an agent-less adapter need to be created for each application and operating system being provisioned. In any event, due to the heterogeneous environment of devices and applications, a provisioning architecture will include both agent-less and agent components to effectively provision accounts enterprise-wide. Additionally in order to accommodate the needs of different provisioning applications and uses, a provisioning system needs to provide an open architecture with accessible API's enabling developers to be able to seamlessly integrate the provisioning solution into existing environments.

6.3.4 Enterprise Directory Services



Directory services provide storage mechanisms for security information used to make authentication and access control decisions. Security data may include user passwords, credentials, digital certificates, access privileges, organizations, groups, roles, resources, etc. Distributed security systems rely heavily on the directory as an information repository and a communication protocol. Application-specific identity-stores support some of the same basic functions as traditional directory servers. The role of directories is evolving to encompass more middleware functions that can integrate heterogeneous applications. As a result, directory hub environments help to bind diverse application components into a logically integrated application environment from a security perspective.

Security and Privacy Architecture Version 1.0

Enterprise directory major functions include:

- Directory Services
- Metadirectory

These service components are discussed in detail below, including relevant definition, integration points, and implementation considerations.

Definitions

- Directory server – is a repository that contains objects with attributes and values, referenced to facilitate querying and retrieval. What these objects and their attributes actually are is down to the directory designers. Typically, they will be people, organizations or computers and their attributes will be anything from e-mail addresses to public key certificates.
- Directory information base – the directory information base acts as the database for the directory server. Queries are submitted to the directory server using some form of directory access protocol (e.g. LDAP). The directory server processes the queries against the directory information base.
- Schema – the schema defines the structure of the directory by dictating the types of information that can be stored, and the relationships allowed between the various object types.
- Meta-Directories - collect identity information from other directories and repositories. Meta-directories enable organizations to integrate disparate identity repositories. Meta-Directories are typically deployed to provide a uniform source of identity information by integrating heterogeneous application repositories.
- Relational Database Management Systems (RDBMS) - store data in the form of related tables. Relational databases are powerful because they require few assumptions about how data is related or how it will be extracted from the database. RDBMS are typically deployed to store the data that needs to be frequently searched and updated, or when complex queries and reporting functions are required.

Benefits of deploying directory technologies:

Directories are an essential part in the foundation for developing distributed computing in an organization. Most applications continue to house data in some form of proprietary directory. Nevertheless, these proprietary directories are often only useful to the application and unlikely to disappear anytime soon. However, these proprietary directories are generally not useful as an enterprise directory. The role of an enterprise directory requires general enterprise architecture.

In the enterprise, directories fill several roles that support and integrate with a variety of infrastructure components to deliver critical business functions. Typically, directories are used as an authoritative repository of identity information providing central authentication services to applications. Consequently, making it easier to support applications authentication functions and maintaining a standard common identification profile for individuals in the enterprise. As a result, directories are needed to support the enterprise management of identity and access management functions.

Security and Privacy Architecture Version 1.0

Implementation & Integration considerations

Scalability

Any directory service must be scalable. Without the ability to scale the directory service over geographical and organizational boundaries, many of the benefits of employing a directory service will be lost. Because searching is the most heavily used service in most directories, scalability of search performance is a critical factor for organizations. Fortunately, nearly all enterprise directory vendors have focused on scalable search performance over the last few years and have made significant progress in this area. The most important technologies for helping search performance so far have been catalogs, filtered replicas, and indexes.

X.500 & LDAP

X.500 has been designed as one of the most comprehensive directory technology available. However, most commercial x.500 products now come with an LDAP interface that provides users with a simple interface to the directory through an LDAP enabled user agent such as a web browser or e-mail address book. LDAP was originally designed to be a simpler and easier interface to an X.500 directory. However, vendors have extended the original idea and built their entire directory product upon LDAP principles. Despite its popularity and simplicity, LDAP does still have some serious disadvantages when compared to X.500. For example, X.500 was designed with security in mind from the outset, whereas LDAP v2 still employed clear text password authentication. Although this issue has been addressed in LDAP v3, it illustrates that LDAP is still a developing protocol.

Integration with SSO

A Single Sign-On service enables users to automatically log on to multiple passwords protected resources by logging in only once to the directory. The SSO service works by login details and passwords being contained as attribute values within the users entry in the directory. The attribute values are stored in the directory server and are provided to the user once they have been successfully authenticated. The passwords and login details are then typically stored in an encrypted cache, which is used to communicate directly with the application requesting login.

Namespace

Usually organizations create an inventory of legacy directory namespaces before deploying a directory. The list of namespaces likely includes at least two standard namespaces, the DNS and X.500, as well as a long list of administrative and application-centric directories. Given the value of enterprise directory and the costs associated with maintaining multiple directories, companies will naturally want to reduce the number of directory namespaces they must manage. However, organizations cannot simply throw out the existing namespaces and the applications they support, in an attempt to change directory implementations. A practical transition path will be necessary, allowing organizations to accommodate the applications they have today while moving toward a more unified approach to directory services.

Security and Privacy Architecture Version 1.0

Schema & Extensibility

Within the enterprise directory, organizations must either choose or define a schema that matches their business needs. While there are already a handful of object and attribute definitions, standards bodies are not likely to address the full array of schema requirements. The schema must be extensible to fit advances in technology and customer needs. While organizations can rely on certain conventions to meet basic schema requirements, there will always be a need to move beyond any static schema definition. Fortunately, the advent of XML, specifically its ability to transform documents from one schema to another has made fixed industry-wide schemas a lot less important.

Distribution & Replication

A centralized data store cannot yield the performance necessary to support applications with diverse, often conflicting data requirements. Applications vary in their need for indexing, physical location of the data, hierarchy, and data sets. As multiple applications make heavy use of directory services, it often becomes necessary to separate directory data onto multiple servers to create horizontal scalability. Directories that span large organizations often operate more efficiently using a distributed design. One form of distribution is to create multiple copies, or replicas, of the entire directory on several different servers. This type of distribution offers fault tolerance and improves performance. To ensure fault tolerance at the partition level, administrators can create multiple replicas of any partition. However, replicas vary in their ability to support write access to the directory.

Meta Directories

The meta-directories sit centrally in an organization's directory service environment collecting and combining data from other connected directories or from its own entries. The key to making a meta-directory work, and pay its way, is the concept of "joining" related entries to form the single unified directory entry. A choice can be made whether to simply use the collated information the collated information as the main source of information, or to export the meta-directory information back to the connected directories. The choice usually depends on the requirements and structure of the organizations concerned. Some may choose to allow users direct access to the meta-directory either through web browsers or LDAP enabled applications. The advantage of allowing users direct access to the meta directory is that they can be empowered to directly administer certain of their attributes within the directory such as personal contact details.

Federated Directories

Federation is a feature that enables multiple directories to work as one. For example, with federation, administrators can create groups composed of entries from several different directories and create access policies to any network resource for the group. Some forms of federation are available today, but only to unify directories from the same vendor.

Security and Privacy Architecture Version 1.0

6.3.5 Non-Repudiation Services

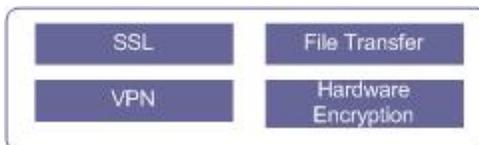


Non-repudiation mechanisms provide tamperproof evidence that a specific action or transaction has occurred. In addition, non-repudiation services are able to produce legally binding evidence. Non-repudiation may require auxiliary services such as time stamping, receipting, or other functions that validate the success or failure of a transaction. Controls the implement non-repudiation prevents an individual from being able to deny receipt, submission, or delivery of a message. Non-repudiation can be achieved through a combination of message integrity, digital signing, and digital notarization functions.

Non-Repudiation services major functions include:

- ❑ Electronic signatures
Currently, students use electronic signatures to sign a promissory note for the disbursement of a loan as part of a financial aid package. This electronic signature mechanism establishes a legally binding agreement between the student, the lenders, and FSA. However, at this moment electronic signatures are being implemented with a blend of processes, procedures, audit trails and lack of strong authentication mechanisms.
- ❑ Digital Certificates
Digital certificates are usually implemented in organizations to provide authentication, encryption and non-repudiation services to applications or end-users. At this moment, FSA considers that digital certificates provide value added functionality that could become an enterprise requirement in the near future. However, the implementation of digital certificates should be considered to address specific instances of applications were the deployment of this service is cost-effective and properly address risk.

6.3.6 Encryption Services



Data and Privacy Protection mechanisms use encryption and non-repudiation services to safeguard the confidentiality and integrity of information. Encryption is one of the most effective ways to achieve data security. In order to read an encrypted file, an individual must have access to a secret key or password that enables decryption of the data. These security components enable widespread implementation of cryptographic services in applications and the enterprise infrastructure. Usually organizations aggregate information types into data classifications that guide the selection of appropriate Data & Privacy Protection mechanisms.

Encryption services major functions include:

Security and Privacy Architecture Version 1.0

❑ **Communication Encryption**

Communication encryption systems include hardware and software mechanisms that protect the confidentiality of data in transit. . Typically, encryption mechanisms for network communications include the use of SSL, VPN's, IPSEC, and other encryption algorithms.

❑ **Data Encryption**

Data encryption services are mechanisms that protect the confidentiality of stored data. Typically, encryption mechanisms for stored security data include the use of digital certificates, PGP, and other encryption algorithms.

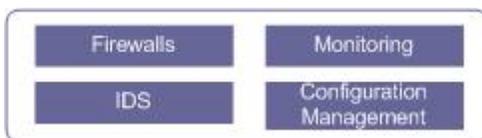
❑ **File Transfer**

Secure Messaging & File Transfer mechanisms use authentication, authorization, and encryption services to protect the confidentiality and integrity of file transfers, and other electronic transactions. Encryption services are usually used provide a holistic end-to-end file transfer security solution.

❑ **Hardware Encryption**

Hardware encryption mechanisms are typically used to standardize the provisioning of encryption services in the FSA environment. For instance, Hardware encryption devices are in place to encrypt communication over ATM communication circuits.

6.3.7 Infrastructure Security Services



Infrastructure security services provide policy enforcement mechanisms designed to implement security policy at boundaries between networks. In fact, FSA has outsourced infrastructure security services to contractors that are responsible for providing network connectivity, traffic filtering, remote access, intrusion detection, and configuration management operational functions. Consequently, it is important that FSA properly incorporates specific security requirements for the functions being outsourced in contractual mechanisms.

Infrastructure services major functions include:

❑ **Firewalls**

Firewalls systems enforce a boundary between two or more networks. They are typically deployed to segregate networks (i.e. Private Networks vs. Internet). In addition, Firewalls enable organizations to enforce security policy on network traffic at the Internet gateway.

❑ **Intrusion Detection Systems**

Intrusion detection systems are used to detect the existence of potential network or host attacks on systems so that protective action can be taken. Intrusion monitoring systems recognize common attack patterns from a database of known

Security and Privacy Architecture Version 1.0

“attack signatures” developed by vendor and industry research. Some intrusion detection and prevention systems also analyze traffic and usage patterns to allow detection of anomalous patterns

❑ **Monitoring**

Monitoring Tools provide the capability to acquire, archive, analyze, and report on event information from various environments. Monitoring tools also provide a means to make better use of audit and logging data by facilitating comparison of activity across different environments, providing multiple visualizations and reporting functions.

❑ **Configuration Management**

Configuration management tools automate the deployment of patches and system configurations in accordance with organizational guidelines, standards, and security policy. In addition, configuration management tools enable organizations to standardize the deployment of system changes in a heterogeneous computing environment. Configuration management tools monitor, analyze and report security updates in order to keep pace with newly discovered and reported system vulnerabilities.

7 Validation of Security and Privacy Architecture

7.1 Introduction

The proposed FSA Security and Privacy Architecture contains a variety of components to implement security services and functions. To insure the proposed architecture satisfies FSA business needs, it was validated against the major business objective identified during the course of meetings conducted with business owners and subject matter experts from business and technical areas. The sections below list each major business objective and related requirements and described which component, service, or function within the architecture address that particular need.

7.2 Validation Against Business Objectives

The requirements and objectives listed in the sections below follow the same organization as the table in Section 5 and Appendix 9.2 of this report.

7.2.1 Control access

7.2.2 Control access

Requirement 1.1 – Identification and Registration

Administration and Provisioning

An administration and provisioning system integrates with identification and registration processes to register users across target systems. An end-user can register for access by leveraging self-service capabilities. Additionally, the automated workflow module routes registration information to business managers that validate and approve registration for access.

Access Management

An access management system delivers sign-up mechanisms to register users to target systems. Using self-service mechanisms end-users can submit registration information that is validate and manually routed for access approval. Additionally, the access management system would provide pre-defined roles in which users are categorized into roles with a selected set of permissions.

Requirement 1.2 & 1.3 – Entity Authentication/Authentication levels

Authentication Services

Authentication systems can completely support different authentication levels by integrating different authentication mechanisms. Authentication mechanisms are then integrated with applications through the use API's and connectors that enable heterogeneous systems to reuse authentication systems. Additionally, application owners are able to select from a variety of authentication mechanisms to obtain a higher level of assurance in validating end-user identity.

Requirement 1.4 – Simplified Single Sign-on

Authentication Services

An authentication system reduces the need for multiple logins and passwords for a group of systems or applications. An SSO system transparently passes user credentials to each target system for which the user is requesting access. Additionally, SSO systems support the integration of various authentication mechanisms and directory technologies. As a result, an end-user would need to provide credentials initially for access to the SSO system. At that point the SSO system would manage the user session to achieve transparency in the validation of credentials with systems.

Requirement 1.5 – Access Control System

Access Management

Access control mechanisms could provide authorization policy and procedure for all FSA user groups, both internal and external. Additionally, roles can be configured to restrict access to specific applications, data, and functions. As a result, access control systems typically integrate with existing applications and systems by leveraging the use of API's and system adapters. Consequently, end-users and resources permissions can centrally be managed to obtain increase access management efficiencies.

Requirement 1.6 – Role Based Access Control

Access Management

Access control mechanisms provide role based access control mechanisms to assign user access privileges across the enterprise. Additionally, RBAC systems enable organizations establish enterprise access roles that can be integrate across systems. Consequently, end-users are logically grouped with a defined set of roles and permissions. As result, RBAC eases the burden of continually having to define access permissions across all target systems.

Administration & Provisioning

Administration and provisioning mechanisms are used in the provisioning process to assign and deploy appropriate access privileges to end-users across all target systems. Additionally, by using the delegated administration module, administrators can assign roles and access privileges to a defined set of users in specific target systems. Also by leveraging, the synchronization functionality embedded in most administration and provisioning solutions changes in roles and access privileges can easily be propagated across the enterprise.

Requirement 1.7 – Access Rule Flexibility

Access Management

Access control & authorization systems are constructed to address business logic and processes. Additionally, access control rules can be constructed to address specific

organizational units or applications. Typically, access control systems enforce access rules by leveraging some type of policy server. A policy server is then managed to enforce access rules that address evolving business relationships and needs.

Requirement 1.8 – Call External Systems or Files For Authorization Data

Access Management

Access management systems provide the functionality to integrate with applications using API's to provide authorization information. Usually, access management systems leverage the use of roles to effectively and timely mediate authorization decisions. Additionally, access management systems are able to import access control list and permissions from other applications.

7.2.3 Manage Access

Requirement 2.1 - User Access Account Management

Administration & Provisioning

Administration & provisioning systems provide a single point to manage and administer user access privileges. Consequently, provisioning systems enable organizations to manage user accounts across all systems and applications. In addition, administration & provisioning systems enable end-users to self-service related account management functions. As a result, organizations are able to improve the consistency and efficiency of managing user accounts.

Requirement 2.2 – Security Approval Workflow Tools

Administration & Provisioning

Administration & provisioning systems are able to automate the security approval process by leveraging the use of the automated workflow module. An automated workflow module enables organizations to improve the process for access requests, security approval, personnel clearances, and related business processes. Additionally, the provisioning system enables the organization to manage approval-processing steps before access is granted.

Requirement 2.3 & 2.4 – Consolidate Security Repositories / Manage Repositories

Directory Services

Directory services enable organizations to manage the complexities of an environment that contains multiple repositories. Typically, directory services provide a standard mechanism for applications and systems to store and validate authentication credentials. However, currently organizations store identity information in multiple repositories. Therefore, consolidation of repositories enables organizations to decrease the management overhead of managing and maintaining multiple repositories. Additionally, a directory provide a common user profile that decreases inefficiency associated with

Security and Privacy Architecture Version 1.0

time consuming task of managing and synchronizing multiple repositories across the environment.

Requirement 2.5 – Password Management

Administration & Provisioning

An administration and provisioning system integrates with target systems to support the enforcement of password policies across the enterprise. Using self-service mechanisms, an end user password changes can trigger the replication of the password change to all target systems in which that user holds an account. Additionally, the administration and provisioning system automates, delegates, and increases the efficiency of password management lifecycle (creation, modification, and termination).

Authentication Services

Authentication systems partially enforce password management functions. For instance, authentication systems provide the limited functionality for end-user to self service password resets across all systems. Additionally, authentication systems are not able to synchronize passwords across the enterprise. However, authentication systems enable end-users to self-service their password changes and resets.

Requirement 2.6 & 2.7 – Password Resets / Password Synchronization

Administration & Provisioning

Administration & provisioning systems enable end-users to self-service password management capabilities like password resets. As a result, the end-user is able to reset its password by validating its registration credentials against an identity repository. Additionally, administration & provisioning systems enable end-users password changes to be replicated or synchronized across all target systems in which the end-user holds an account. As a result, end-user password changes are transparently communicated to all target systems in which the user holds an account.

Requirement 2.8 – Delegated Administration

Administration & Provisioning

Administration & provisioning systems enable organizations to distribute user account administration to organizational units or partners minimizing the administrative overhead associated with user account management. Therefore, the delegated administrator would access the account management system to perform account management functions for a defined set of users. As a result, a delegated administrator would be able to perform account management functions more efficiently because of the insight he has to that particular unit's user populations' needs.

7.2.4 Audit Access

Requirement 3.1 – Audit User Access Privileges

Monitoring

Auditing & logging systems are capable of preserving an audit trail of user account administration activity. Typically, Identity & Access management systems log a variety of event information as it relates to user access activity. However, identity & access management systems typically lack the capability to provide a holistic solution to auditing across the provisioning process. Therefore, audit & logging systems would deliver an effective and accurate method for auditing access requests, approval actions, and access privileges modifications. As a result, auditing & logging systems would acquire, and archive user activity logs were they could be analyzed for trends and anomalies.

Requirement 3.2 – Log User Activity

Monitoring

Typically, user activity is independently logged by identity and access management systems. However, this data is never aggregated and analyzed for correlation of user access in systems across the enterprise. An audit & logging system provides the tools to capture and store user activity logs for a defined period. Additionally, it provides tools to aggregate and analyzed logged user activity data across the enterprise.

Requirement 3.3 – Archive Audit Data

Monitoring

Usually, logging information is stored independently in some type of application repository that fails to protect the confidentiality and integrity of this data. Auditing & logging systems have the capability to archive and store audit data for a defined timeframe while protecting its confidentiality from unauthorized individuals. Additionally, audit and logging systems use mechanisms to protect the confidentiality of audit log information by leveraging RBAC roles or access control lists.

Requirement 3.4 – Report Access

Monitoring

Commonly, information systems lack the ability to provide an aggregated view of user access reports across all systems in an enterprise. An audit and logging system has the ability to provide detailed audit reports of user access and privileges to systems. Additionally, it provides flexible query tools to report on access of all users to specific systems, or for access across all systems by specific users.

7.2.5 Protect Data

Requirement 4.1 – Confidentiality Of Transmitted Data

Encryption Services

Usually organizations define encryption standards for transmission of data across the networks. These standards are then implemented by the use of encryption services in applications and the enterprise infrastructure. As result, encryption mechanisms are usually implemented in a standardize way to safeguard the confidentiality of data when traveling across a network. Typically, encryption mechanisms for network communications include the use of SSL, VPN's, IPSEC, and other encryption algorithms.

Requirement 4.2 – Confidentiality Of Stored Security Data

Encryption Services

A different set of encryption standards is defined to safeguard the confidentiality of stored security information. Typically, stored security information includes user information, user security credentials, user access privileges, access control rules, etc. Therefore, security information is usually categorized as sensitive data that should be safeguarded with the use of previously defined encryption standards and mechanisms. Typically, encryption mechanisms for stored security data include the use of digital certificates, PGP, and other encryption algorithms.

Requirement 4.3 – Security File Transfer

File transfer

Secure file transfer mechanisms use authentication, authorization, and encryption services to protect the confidentiality and integrity of file, and batch data transfers. Secure file transfer is typically deployed to address security concerns of the FTP protocol when transmitting sensitive information between systems. Additionally, secure file transfer services are used to provide a holistic end-to-end messaging security solution between FSA and its trading partners.

7.2.6 Sign Transactions

Requirement 5.1 – Strong Authentication

Authentication Services

Authentication systems support different authentication mechanisms to provide a higher level of assurance of identity information. “Strong Authentication” mechanisms are usually integrated with existing applications to achieve a higher level of assurance that is crucial to the use of electronic signatures. Strong authentication mechanisms are typically integrated with the use of digital certificates, tokens, smart cards, and other authentications mechanisms. In any event, it is up to the application owner to select the appropriate authentication mechanism to properly address the security requirements for that application.

Requirement 5.2 & 5.3 & 5.4 – Notarization / Auditing / Non-Repudiation

Non-repudiation Services

Non-repudiation mechanisms provide binding evidence that a specific action or transaction has occurred. Non-repudiation services are deployed to validate author and content of an electronic signature transaction. Additionally, Non-repudiation mechanisms may require auxiliary services such as time stamping, receipting, or other functions that validate the success or failure of a transaction. Notarization functions provide timestamp and date stamp functions for transactions to support the audit trail of electronic transaction signatures. As a result, electronic transactions are typically audited to detect fraud or tampering. Consequently, the non-repudiation system provides an appropriate audit trail of signatures and transactions to maintain accountability of individual actions and facilitate the audit process.

7.2.7 Protect FSA infrastructure

Requirement 6.1 – Control Network Access

Firewalls

Firewalls are implemented to inspect and regulate network access and traffic usually based on source, destination, type of message, and content. For instance, firewalls examine and constrain network traffic, thereby allowing certain applications and resources to send or receive traffic thorough the perimeter. Typically, traffic-filtering mechanisms include the use of firewalls, and routers.

Requirement 6.2 – Block Malicious Code

Infrastructure Security

Virus and Content Control capabilities are able to filter malicious content at various enforcement points. Their capabilities enable organizations to enforce security policies at network boundaries. Virus & content control mechanisms are usually deployed in two forms: E-mail desktop/server-based and gateway based. Because of this layered approach, malicious content is screened out before it reaches the end-user or systems.

Requirement 6.3 – Detect & Prevent Intrusions

Intrusion Detection Systems

Intrusion monitoring and prevention tools are used to detect the existence of potential network or host attacks on systems so that protective action can be taken. Intrusion monitoring and prevention tools provide a fast and automated mechanism for organizations to be pro-active in identifying and stopping intruders. Typically, Intrusion monitoring and prevention tools include the use of network and host intrusion detection systems that leverage industry research of know security vulnerabilities.

Requirement 6.4 – Monitor Network & System Security

Monitoring

Analysis and correlation mechanisms collect and examine event information from multiple sources (i.e. network devices, intrusion detections systems, system logs, application logs, etc) to recognize patterns that indicate potential security attacks. Additionally, analysis and correlations systems provide reporting features to analyze the aggregated data into different views. Typically, analysis & correlation systems are provided by managed security services providers or by the use of an enterprise co-relational engine.

Requirement 6.5 – Manage Updates, Patches, and System Configuration Changes

Configuration Management

Patch and configuration management tools automate the deployment of patches and system configurations in accordance with organizational guidelines, standards, and security policy. Configuration management tools standardize the deployment of system changes in a heterogeneous computing environment. Additionally, configuration management tools are able to monitor system patch levels, report potential vulnerabilities and recommended actions, and install required patches and system updates.

Requirement 6.6 – Detect System and Application Security Vulnerabilities

Configuration Management

Typically, vulnerability assessment tools are used to detect and monitor the existence of systems and application vulnerabilities. Network vulnerability scanners probe the host using the network to verify that system and application patches are in place. On the other hand, application security scanners probe the application logic and coding standards to eradicate common security coding vulnerabilities. Finally, configuration management tools monitor system patch levels, report potential vulnerabilities and recommended actions, and install required patches and system updates.

Requirement 6.7 – Physical Security

Facility Access Control

Appropriate facility access control mechanisms control personnel access to data centers and system. Common physical access controls include key cards, smart cards, identification badges, security cameras, motion sensors, cages, fences, and security guards. The access management system can provide some of the authentication functions required to satisfy this requirement. In general, physical security controls fall outside the scope of technical architecture layers defined by this specification.

Requirement 6.8 – Environmental Security

Environmental controls

Environmental controls monitor physical facilities to reduce the risk or effects of a disruption of service. Common environmental controls include HVAC, fire alarms, water sprinklers, flood alarms, redundant power, etc. Environmental controls fall outside of the functions included in the Security and Privacy Architecture.

8 Conclusion

This document has described a proposed Security and Privacy Architecture Framework Specification to guide development and deployment of FSA security technologies. The architecture structure has been validated by demonstrated that the major FSA business objectives related to security can be satisfied by the technical security components and services that make up the security and privacy framework.

A companion document, 124.1.2 – Final Security and Privacy Architecture Report, describes an implementation approach for developing and deploying the security services and components defined in the framework.

9 Appendix

This Appendix contains:

Appendix 9.1 – The Technical Security Architecture layer of the Generic Security and Privacy Framework as defined in Deliverable 124.1.1 – Interim Security and Privacy Architecture Report

Appendix 9.2 – Detailed business objectives matrix that identifies the business objectives identified and validated through meetings with business owners and subject matter experts.

Appendix 9.3 – Summary of FSA Information Technology Security and Privacy Policy

Appendix 9.4 – Summary of FSA Security Solutions Lifecycle Guide

APPENDIX 9.1

Technical Security Architecture

Application Services

Integration Interfaces

Interfaces or APIs used to integrate applications with external security services

Web Services Security

Security standards and functions for protecting web services transactions

Transaction Security

<p>Network & Perimeter</p> <p>Traffic Filtering</p> <p>Inspect and block harmful network traffic based source and destination addresses & ports, or existence of valid sessions; includes network segmentation strategy and design</p> <p>Virus & Content Control</p> <p>Inspect traffic and block malicious content such as viruses, worms, Trojan horses, or other unacceptable content</p> <p>Intrusion Monitoring</p> <p>Detect attempted attacks on networks, operating systems, and servers; alert operations personnel to initiate appropriate incident response</p> <p>Intrusion Prevention</p> <p>Detect and block attempted attacks on host operating systems and applications</p> <p>Remote Access</p>	<p>Identity & Access Management</p> <p>Identification & Registration</p> <p>Identify and enroll users, and create security credentials</p> <p>Authentication</p> <p>Validate user credentials when access to a system is requested; includes single sign-on and session management functions</p> <p>Authorization & Access Control</p> <p>Assign and enforce access privileges for specific data and resources based on authenticated identity of user</p> <p>Directory Services</p> <p>Store and manage user information, security credentials, & other security data</p> <p>Administration & Provisioning</p> <p>Provision and manage user and</p>	<p>Monitoring Tools</p> <p>Auditing & Logging</p> <p>Recording, storing, and reporting user and system activity and access privileges</p> <p>Analysis & Correlation</p> <p>Consolidating and processing audit data, log data, and other security information to detect patterns that indicate potential security incidents</p> <p>Vulnerability Assessment</p> <p>Tools to inspect networks, host systems, and applications for potential security weaknesses</p> <p>Forensics Tools</p> <p>Tools to inspect systems and security information to gather evidence about suspected security breaches</p> <p>Patch & Configuration Management</p> <p>Tools to detect or deploy system patches, updates, or fixes; tools</p>
---	--	--

Data & Privacy Protection

Communications Encryption

Protect confidentiality and integrity of communications channels with encryption techniques

Data encryption

Protect confidentiality and integrity of data stored in databases with encryption

Message Integrity & Non-repudiation

9.2 Detailed Business Objectives for Security

	High-Level Business Objective	Proposed Requirement	Description	Details	Priority I = Immediate F=Future
1.0	Manage Access	Control access of individual users and system entities to FSA systems, networks and data			
1.1		Identification and Registration	Provide consistent identification and enrollment/registration of users and the access level required	-Support identification and validation processes for users -Register users to collect information required for assigning access privileges	I
1.2		Entity Authentication	Authenticate users and entities who request login to FSA systems and applications	-Authenticate users by validating credentials presented to support a claimed identity -Support existing and planned authentication mechanisms	I
1.3		Authentication Levels	Provide different levels of authentication according to user role and resources that will be accessed	-Support different levels of authentication by providing flexibility to access multiple authentication services -Be able to base user authentication mechanism on identity of user or resources requested at time of login	I
1.4		Simplified Sign-on	Reduce the need for multiple logins and passwords for groups of systems or applications commonly used together	-Reduce need for multiple logins required for access to a group of related applications -Increase ease of use	I
1.5		Access Control System	Provide access control mechanisms that systems and applications can use to manage information assets available to users	-Provide authorization policy and procedure for all FSA user groups, both internal and external -Provide access control mechanisms and roles that can be configured to restrict access to specific applications, data, and functions	I
1.6		Role-based Access Control	Base user access on roles to provide standardized, consistent "need-to-know" access privileges	-Define roles or job functions across the organization for access privileges required across multiple systems by defining access policies -Implement and enforce access roles on individual systems in a manner consistent with FSA policy	I
1.7		Access rule flexibility	Access rule flexibility: provide flexible access control rules based on business logic	-Configure access control rules that meet business needs -Base access control rules on organizational affiliation, specific unit within an organization, and context of application usage	I

	High-Level Business Objective	Proposed Requirement	Description	Details	Priority I = Immediate F=Future
1.8		Call External Systems or Files for Authorization Data	Provide method for access rules to communicate with external systems or files to obtain information needed for controlling access to resources based on user roles or business logic	-Implement access control systems able to query external files or systems to appropriately limit access to a specified set of records -Example: Be able to call the PEPS file to limit access to records for a specific organization	I
2.0	Administer & Provision Access Approve, assign, and maintain access of entities (individual users and system users) to FSA information assets (systems, applications, and data)				
2.1		User Access Account Management	Improve the consistency and efficiency of managing users access accounts on FSA systems and applications	-Provide single point to manage user access privileges -Provide tools to terminate user accounts -Provide 'single sign-up' capability	I
2.2		Security Approval Workflow Tools	Improve the efficiency of user provisioning by automating workflow processes for access requests, security approvals, and personnel clearances	-Support business processes related to user registration, enrollment, and account management -Manage and automate approval processing steps such as requiring personnel clearance before access is granted	F
2.3		Consolidate Security Repositories	Consolidate the management and maintenance of user security data repositories	-Decrease the overhead and inefficiencies associated with managing multiple repositories of user and security data	F
2.4		Manage Repositories	Increase the efficiency and accuracy of directory administration and management	-Increase the effectiveness and accuracy of tools or interfaces for managing directories and users	F
2.5		Password Management	Enforce policies to improve password authentication methods	-Enforce configurable password policies at time of password change. -Example password policies include: password length, complexity (alphanumeric, upper/lower case, special characters), expiration period, history, forced change at first login	I
2.6		Password Resets	Simplify the password reset process for users and administrators	-Provide simplified systems for resetting passwords -Where appropriate, consider allowing users to reset their own passwords through supplementary authentication processes	F

	High-Level Business Objective	Proposed Requirement	Description	Details	Priority I = Immediate F=Future
2.7		Password Synchronization	Automatically synchronize passwords across systems	-Be able to define a set of systems or applications to link for synchronizing passwords -Detect when a password change occurs on one of the systems then automatically update linked systems	F
2.8		Delegated Administration	Distribute user security administration to partner organizations to decrease costs and improve accuracy	-Configure and manage delegated security administrators at partner organizations -Allow partner organizations to manage users within their organizations -Provide tools to limit administrative functions of delegated administrators	I
3.0	Audit Access				
	View and report on user activity and access to FSA systems and data				
31.0		Audit User Access Privileges	Provide effective, accurate methods for auditing access requests, approval actions, and assigned access privileges	-Record relevant details of security approval steps -Track user account administration activity that adds or modifies user access privileges	I
3.2		Log User Activity	Consistently track and report on user activity on sensitive systems, applications, and data	-Capture and store logs of user activity -Provide tools to configure logged data (types of events, frequency, user details, etc.)	I
3.4		Archive Audit Data	Maintain audit information securely for defined time period	-Protect audit log data from modification -Archive and store audit data for time period required by FSA policy	I
3.5		Report Access	Provide a convenient, effective way to view and report on access privileges of users across multiple systems	-Create audit reports of user access to systems and privileges assigned within each system -Provide flexible query tools to report on access of all users to specific systems, or for access across all systems by specific users	I
4.0	Protect Data				
	Protect the confidentiality and integrity of FSA data				
4.1		Confidentiality of Transmitted Data	Maintain confidentiality of FSA information by encrypting data during transmission across networks	-Define encryption standards for transmission of data across networks -Provide encryption standards for secure file transfer	I

	High-Level Business Objective	Proposed Requirement	Description	Details	Priority I = Immediate F=Future
4.2		Confidentiality of Stored Security Data	Maintaining the confidentiality of stored security data	-Encrypt security data stored in databases -Security data includes user information, user security credentials, user access privileges, access control rules or policies, etc.	I
		Secure File Transfer	High volume trading partners need options for transmitting secure data	-Methods for authentication and encryption of file and batch data transfers -Need to define standards and educate trading partners	I
5.0	Sign Transactions Authenticate the authorship and content of FSA online transactions				
5.1		Strong Authentication	Provide strong authentication methods suitable for users signing online transactions electronically	-Support strong authentication to increase the assurance level for use in electronic signature system	F
5.2		Notarization	Provide digital notarization functions to timestamp and datestamp transactions	-Provide timestamp and datestamp functions for transactions to support electronic signatures	F
5.3		Audit Electronic Signatures	Provide audit tracking and reporting for details of authentication and user activity related to electronically signing transactions	-Record details of electronic signature transactions to provide an audit trail to validate signature details -Capture date, time, user details, and other context information (location, system or application ID, other attributes of user or event)	I
5.4		Non-Repudiation	Be able to prove the origination details and validate the content of online transactions to prevent repudiation	-Provide strong authentication method to validate author of transaction -Verify that content of transaction has not been altered after the electronic signature was applied	F
6.0	Protect FSA Infrastructure Monitor and control access to FSA networks, information systems, and data centers				
6.1		Control Network Access	Monitor and filter unauthorized network traffic that could compromise the integrity or availability of FSA networks and systems	-Block unauthorized network services -Filter traffic based on source and destination addresses and ports -Filter traffic based on valid session status	I
6.2		Block Malicious Code	Filter harmful software (such as viruses, worms, trojans, and malicious mobile code) to prevent damage to FSA systems or data	-Detect and block traffic containing malicious software -Provide effective methods to promptly update malicious software signatures when new attacks are discovered	I

	High-Level Business Objective	Proposed Requirement	Description	Details	Priority I = Immediate F=Future
6.3		Detect and Prevent Intrusions	Monitor FSA networks and systems for activity that could indicate potential security attacks and produce alerts or take automated actions to prevent or limit the attack	<ul style="list-style-type: none"> -Detect potential security attacks by recognizing attack signatures in network traffic -Detect potential security attacks based on pattern recognition of normal and abnormal traffic -Prevent attack damage to applications and systems 	I
6.4		Monitor Network and System Security	Monitor the overall security posture of FSA networks and systems by analyzing and correlating security data from network devices, intrusion detection systems, system logs, etc.	<ul style="list-style-type: none"> -Collect security information from network devices, intrusion detection systems, server and application audit logs, virus detection systems, etc. -Analyze and correlate security data to detect potential attacks -Provide status views, reports, and alerts 	I
6.5		Detect System and Application Security Vulnerabilities	Provide procedures, standards, and tools to detect and address security vulnerabilities in FSA systems and applications	<ul style="list-style-type: none"> -Procedures to review and approve security design and implementation of systems and applications -Provide assessment and scanning tools to detect potential security vulnerabilities and weaknesses -Report potential vulnerabilities and recommended actions 	I
6.6		Manage Updates, Patches, and System Configuration Changes	Provide methods to efficiently detect and deploy system patches, updates, or fixes, and to maintain the integrity of FSA systems and applications	<ul style="list-style-type: none"> -Monitor system patch levels -Identify and analyze security patches and updates -Download, test, and install required patches and system updates 	I
6.7		Physical Security	Control and monitor physical access to FSA data centers and systems	<ul style="list-style-type: none"> -Control personnel access to data centers and other locations where FSA systems are housed -Monitor premises for unauthorized activities 	I
6.8		Environmental Security	Control and monitor the physical environment of FSA data centers and systems to mitigate damage from natural or man-made disasters	<ul style="list-style-type: none"> -Monitor physical facilities: HVAC, fire alarms, fire sprinklers, flood alarms, electrical power, etc. -Provide monitoring and protection for tornadoes, hurricanes, earthquakes, floods 	I

APPENDIX 9.3

9.3 Summary of Draft FSA Information Technology Security and Privacy Policy

This Appendix summarizes the draft version of the FSA Information Technology Security and Privacy Policy. It is based on the version of the policy document issued in March 2003. The complete document is available from Bob Ingwalson.

9.3.1 Introduction

FSA systems must be developed as systems worthy of trust. This draft of FSA’s policies sets the minimum level of security required at FSA and establishes the criteria against which FSA will measure results.

Information security and privacy jurisdiction covers all information assets (property of the U.S. Government), beginning with the electronic or manual input of data and ending when the data are transferred to non-FSA systems, persons or facilities.

This policy applies to all FSA operations. FSA employees, consultants, contractors, interns, temporary employees, or other parties accessing FSA information assets are subject to this policy, and have the same responsibilities as FSA employees.

Security and privacy are addressed by the policy in three major areas, summarized in the tables below: Enterprise Management, System Operational Controls, and System Technical Controls.

9.3.2 Enterprise Management Controls

The Enterprise Management Controls section outlines security topics that are normally addressed by management in the organization's information security program.

Control	Description
Risk Management	Each FSA System Manager must budget for and oversee the completion of risk assessments for all Information Technology (IT) systems under his/her control. These assessments must be updated every three years at a minimum by an independent evaluator, or whenever a major change ¹ to the system occurs.
Security Control Reviews	System Managers are responsible for periodic management testing and evaluation of the effectiveness of security control policies, procedures and techniques, and for remediation of any noted deficiencies found during these tests.
System Security Plan	The system security plan must describe the system and its relationship with all interconnected systems. The system security plan includes synopses of supporting documents (e.g., Disaster Recovery Plan, Configuration Management Plan).
Rules of Behavior	Rules of Behavior reflect administrative as well as technical security controls. They also delineate responsibilities, detail the expected behavior of all individuals with access to the system and define penalties for their violation.
Solution Life Cycle	Each phase of the lifecycle contains a corresponding security requirements checklist to be completed at the conclusion of each phase by the System Security Officer (SSO).
Certification and Accreditation	FSA General Support Systems (GSS) and Major Applications must perform the Certification and Accreditation (C&A) process before becoming operational.
Security and Privacy Awareness and Training	All FSA employees are responsible for the confidentiality, integrity and availability of FSA information systems and must receive annual information security awareness

¹ See NIST Special Publication 800-18 for a definition of a major change.

APPENDIX 9.3

	training.
System Interconnections	FSA must have a security control review of every system and interconnected systems on a periodic basis. Every system must have a network diagram and documentation of any interconnected systems including access to the Internet, its names/unique identifiers, and a description of the interaction(s) between or among them.

9.3.3 System Operational Controls

The System Operational Controls section addresses security controls that are implemented and executed by people as opposed to systems.

Control	Description
Personnel Security	Covers establishing and terminating accounts, documenting duties, determining the sensitivity of each position, background screening, confidentiality agreements, and other policies dependent on the individual.
Physical & Environmental Protection	Protects FSA’s systems, buildings, and supporting infrastructures against physical threats (e.g. unauthorized presence) and environmental threats (natural or man-made disasters).
Production Input/Output Controls	Only authorized users may pick up, receive, or deliver input and output information and media.
Contingency Planning	FSA’s Contingency Planning policy defines the emergency operating procedures that must be followed to make sure FSA’s critical functions continue to operate and support IT systems in the event of disruptions, both large and small.
Data Integrity	Each FSA System Manager must document data integrity procedures to detect or prevent unauthorized alteration of data.
Documentation	Every FSA system must have sufficient security documentation to describe adequately the security controls and procedures governing the operation and maintenance of the system.
Configuration Management	Ensures that new configurations introduced into FSA systems work in the intended way and do not adversely impact other security or functionality aspects of the system.
Incident Response	FSA must adequately train system security personnel to recognize security incidents. FSA must establish procedures for reporting and responding to those incidents.

9.3.4 System Technical Controls.

The System Technical Controls section focuses on security controls that the system executes, as opposed to controls performed by people.

Identification and Authentication	Each FSA system must use identification and authentication procedures to prevent unauthorized use or access. This draft covers system logins, passwords, PKI, and biometrics.
Logical Access Controls (Authorization/Access Controls)	FSA’s logical access security controls are system-based mechanisms that must restrict users to authorized transactions and functions only. These controls must detect and log unauthorized transaction attempts by authorized and unauthorized users.
Audit Trails	FSA audit trail records must maintain a log of system and network activity both by system or application processes and by user activity for a minimum of one year. In conjunction with appropriate tools and procedures, audit trails must provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems.

APPENDIX 9.4

9.4 Summary of FSA Security Solution Lifecycle Guide

This Appendix summarizes the FSA Security Solution Lifecycle (SLC) Guide. The SLC Guide defines security review and approval steps and deliverables for each major phase of the system development lifecycle.

9.4.1 Introduction

As part of its commitment to customers and partners, FSA manages risks on a continuous basis. Faced with a public and administration that has a heightened awareness of security concerns, FSA needs to demonstrate that its systems are worthy of trust and consistent with best security practices and U.S. Public Law and policy.

Security is an integral component throughout the Security Solution Lifecycle Guide. The sections and appendices of the SLC describe system security in sufficient detail to allow a project team to confidently implement security into their system. For additional security-related information, FSA maintains a Security Reference Guide on its intranet.

9.4.2 Vision Phase System Security

The Vision Phase initiates the concept of the system. During the vision phase, personnel with security responsibilities should be identified. The certification and accreditation (C&A) requirement for each system stresses the appointment of key personnel to manage the C&A process.

9.4.3 Definition Phase System Security

As the system progresses through the definition phase, several security actions should occur.

- The system should be defined as a new system or major modification
- The system's sensitivity should be classified criticality defined.
- The roles and responsibilities of the user and developer community should be defined.
- Security documentation from any interconnected systems should be obtained and reviewed.
- The SSO should undergo appropriate training for the responsibilities of an SSO during the life of the system.
- The certificate and accreditation process should begin.
- The system rules of behavior should be developed.
- FSA employees and contract support personnel should have background screening
- The SSO should submit a definition phase checklist to the System Manager for signature.

9.4.4 Construction Phase System Security

Primarily, the system security plan should be drafted during this phase. Guidance for completing the security plan can be found in NIST Special Publication 800-18. The certification and accreditation process directs the project team to draft a System Security Authorization Agreement (SSAA). A risk assessment should also be performed to determine if the intended security controls are adequate. Findings from the risk assessment should be addressed in a Corrective Action Plan. The SSO should then obtain and review the MOU/SLA for inclusion of appropriate security controls. Finally, the SSO should submit a construction phase checklist to the System Manager for signature

APPENDIX 9.4

9.4.5 Deployment Phase System Security

The corrective action plan developed in the construction phase risk assessment should be implemented. To determine if the security controls were implemented properly, they should undergo a series of. The Certification and Accreditation process should approach completion. The System Security Plan should be completed prior to the system becoming operational. The SSO should then identify opportunities for training that will directly support the job's performance. All personnel who need access to the system should receive user access forms.

9.4.6 Support and Retirement Phase System Security

After deployment, the system enters a period of support that maintains security through the final period in the system's lifecycle when the system is retired. The security related activities can be broken down into two periods: Support, and Retirement. The support period specifies re-certification, personnel security maintenance, training and risk management. The retirement period ensures that all sensitive data is sanitized or destroyed when the system is no longer in service.