

FSA Integration Partner
United States Department of Education
Federal Student Aid



**Data Strategy Enterprise-Wide
Enrollment and Access Management Team
123.1.29 Access Management High-Level Design**

Task Order #123

Version 2.0

December 02, 2003



Executive Summary

Currently, FSA's diverse user population and numerous platforms and security processes create challenges for both Trading Partners and FSA. Trading Partners are often frustrated because they must obtain and remember different UserIDs and passwords. The absence of an enterprise view of enrollment and access management makes it difficult for FSA to efficiently manage and monitor its systems. For example, existing security tools do not allow FSA to readily view or report on the access privileges of a user across multiple FSA systems. Some user access management tasks require significant manual processing by administrators for each system. As a result, it is not possible to quickly revoke access for a user or an entire Trading Partner across multiple FSA systems.

FSA has defined a series of business objectives to improve the processes and tools available to manage Trading Partner access to FSA systems and data. Primary goals are to:

- Develop an enterprise approach for managing access that will minimize administrative overhead associated with individual FSA systems.
- Simplify the interaction of Trading Partners with FSA systems.
- Provide more effective oversight and reporting capabilities to track who has access to FSA systems.
- Facilitate FSA compliance with security and privacy regulatory requirements.

This deliverable presents a high-level design for Trading Partner access management that identifies tools and processes to help FSA achieve these goals. The enrollment and access management vision described in the high-level design advances the concept of a consolidated view of enrollment and Trading Partner access management. The proposed solution will provide capabilities to manage access at the enterprise level that help insulate Trading Partners from the underlying complexity of FSA's systems. Consistent user identity and privilege information will improve security effectiveness and increase administrative efficiency. The solution provides functions for enterprise access management that will make it easier to perform common business processes such as configuring access for a new institution or changing a user's access permissions.

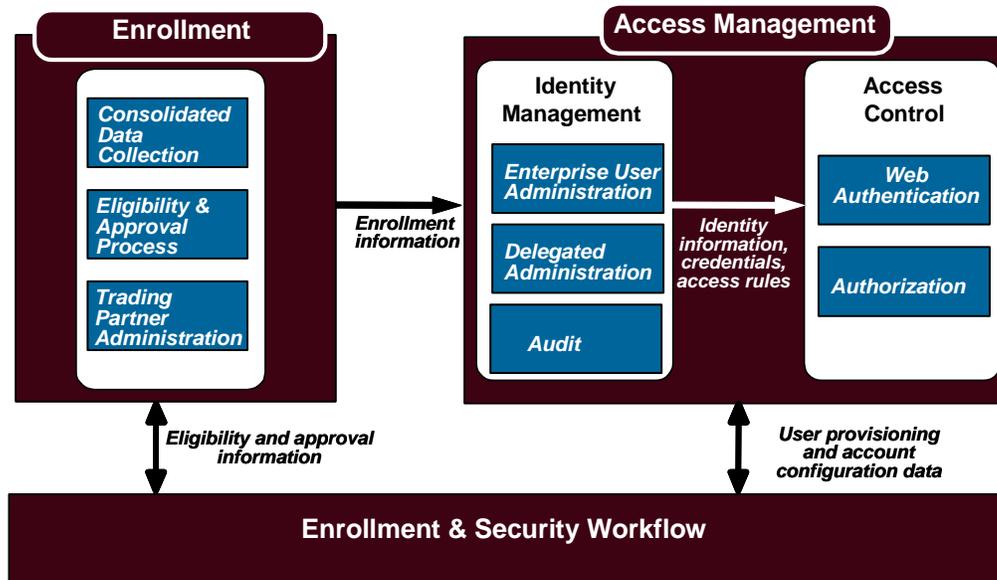
The key elements of the high-level design for access management are:

- A conceptual vision for managing Trading Partner access to FSA systems that maps directly to FSA requirements for access management.
- An overview of major access management components.
- Integration with common Trading Partner and user business processes.
- A discussion of Access Management benefits for Trading Partners and FSA.
- A discussion of implementation approach options and considerations.



Conceptual Vision for Managing Trading Partner Access

The figure below illustrates the vision for both Enrollment (described in the Enrollment High Level Design - Deliverable 123.1.28) and for Access Management. The figure also shows the two primary components of the Access Management solution, Identity Management and Access Control, and the major functions they provide.



Enrollment and Access Management Conceptual Design

These Access Management functions and components support FSA business objectives for Enrollment and Access Management. A requirements mapping was developed to summarize and validate the effectiveness of the proposed Access Management solution. Each business objective is supported by one or more identity management or access control functions.

Overview of Major Access Management Components

The Identity Management component provides several critical enterprise functions for user administration and management. These functions provide automated tools for the process of creating and maintaining user identity information: Enterprise User Administration, Delegated Administration, and Audit functions.

- The Enterprise User Administration function manages the creation and maintenance of a user's identity information. Rules based on business requirements can be used to assign user access rights that enforce FSA security policies. The enterprise user administration function would be able to use a Roles Based Access Control (RBAC) approach to grant access rights to users based on their assignment to a defined role in the organization. RBAC allows for access control to be managed at a level that corresponds closely to the organization structure.



- Delegated administration functions enable the allocation of user account administration tasks to trusted administrators as designated by external Trading Partners. This would allow administrative tasks (such as requesting access for a user or approving a change in access) to be performed by administrators who have the most accurate knowledge about the user and their access needs.
- The ability to audit access to FSA systems is important for compliance and reporting purposes. The Identity Management system will provide auditing functions to design and run reports that provide enterprise views of access privileges across the FSA environment.

The Access Control system provides flexible authentication services and access control for web applications. Single sign-on (SSO) and session management functions would also be provided by this component:

- A typical implementation for access control would include a Web access control product, which would manage and administer user authentication and authorization for Web applications, but not for legacy applications. The Web Authentication service validates the identity of the user through a user authentication process. Although most user authentication for FSA systems currently use passwords, the Web access control system would also provide flexibility to configure alternate authentication mechanisms, such as tokens or digital certificates.
- The authorization service validates that a user has approved privileges to access specific protected resources. The validation could be based on a user's role and enterprise security rules and policies.

Integration with Trading Partner and User Business Processes.

Implementation of an enterprise Access Management System will provide new capabilities to support greater efficiency in the management of Trading Partner access to FSA systems. The deliverable includes integration scenarios to demonstrate how access management components will support existing FSA business processes, or provide opportunities to develop new and more effective business processes for management of Trading Partner access.

These scenarios are not intended to describe comprehensive process designs for each of the business activities presented. Rather, the scenarios depict examples of how FSA business processes can take advantage of the new capabilities that would be provided by the Access Management System.

The analysis of business process integration is divided into two major areas. The first addresses business processes related to managing access for Trading Partners, and the second focuses on processes for managing access for individual users. The example business processes discussed are:



For Trading Partners:

- Trading Partner Enrollment
- Trading Partner Changes
- Trading Partner Termination

For Trading Partner users:

- Add new user
- Support self-service processes
- Change of status
- User termination

Benefits

The Access Management solution provides benefits for both Trading Partners and FSA.

For Trading Partners, the solution:

- Enhances and simplifies the Trading Partner experience when using FSA systems by providing a single sign-on capability for users who login to multiple Web applications.
- Decreases the number of UserIDs and passwords Trading Partner users need to interact with FSA.
- Integrates with a redesigned enrollment process to streamline steps for gaining access to FSA systems.
- Provides more direct Trading Partner control over setting up user accounts by allowing delegated administrators the ability to perform authorized account management functions.

For FSA, the solution:

- Consolidates and simplifies user account management across multiple FSA systems
- Increases the security of FSA systems by improving the accuracy of assigning and managing access privileges for FSA systems.
- Decreases administrative costs by reducing the number of independent account management steps currently required for individual FSA systems.
- Improves oversight and regulatory compliance for FSA systems by providing enterprise views and reports of access to FSA systems for internal and external access audits.

Options and Considerations

During planning for future design and deployment activities of an Access Management solution, FSA will need to take into account the following major considerations.

- **Commercial Software Options:** Although it would be possible to deploy the Access Management solution with custom-developed software, a variety of commercial security



software tools could be integrated to provide the major functions required. Commercial software tools would provide significant advantages to FSA in terms of security of the final solution, cost and speed of development, and flexibility for integration with existing FSA systems.

- **Integrated Deployment:** There are significant advantages for FSA to consider when deciding whether to integrate deployment of access management components. FSA will need both the Access Control and the Identity Management functions to achieve its business objectives for simplifying access for Trading Partners and achieving efficiencies by managing access at the enterprise level.
- **Coordination with Federal Initiatives and External Standards:** During design and deployment of an Access Management solution, FSA should consider how best to integrate with developing federal and external initiatives for sharing authentication credentials and defining security for Web services. The federal e-Authentication project has recently changed its approach from developing a physical authentication gateway to defining an authentication architecture based on commercial standards, such as Security Assertion Markup Language (SAML) and the Liberty Alliance. FSA will need to include consideration of support for security and authentication standards when evaluating tools for developing the Access Management solution.
- **Prototype Development:** An effective method for FSA to evaluate Access Management technologies and tools will be to conduct a prototype implementation of access control and identity management functions. Integrating these technologies with an existing FSA application in a development and testing environment will provide opportunities to understand how Access Management components can be integrated across FSA enterprise systems.

Next Steps

The next step for the Access Management effort will be to evaluate tools and technologies available for development of the required functionality. Task Order 143, Identity and Access Management Tools Analysis, has been awarded and is scheduled to begin immediately. The goal of this task order is to evaluate commercial products and analyze how they can be used to meet FSA Access Management business objectives defined during the earlier phases of this project. This effort will provide technology recommendations for implementation of Identity and Access Management technologies to satisfy FSA needs for security services across FSA user groups and environments. This effort will also include the development of a prototype of the selected Identity and Access Management tools and integrate them with a role-based FSA web application in a development environment. Findings and recommendations from this effort will then be used to continue integration of the Access Management solution with redesigned Trading Partner enrollment processes that are part of the overall planning for Trading Partner Management.



Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY
11/14/03	All	Document submitted for FSA-wide review.	N/A	Anu Sharma
12/02/03	Sections: 2.1 2.3 Figures: 1 Appendices: C	FSA comments incorporated into document, where appropriate	Core Team	Anu Sharma



Table of Contents

EXECUTIVE SUMMARY	2
1 INTRODUCTION	11
1.1 PURPOSE	11
1.2 BACKGROUND.....	11
1.3 DEFINITION OF TERMS	12
1.4 SCOPE	13
1.5 APPROACH	14
1.6 ORGANIZATION OF THIS DOCUMENT	14
2 ACCESS MANAGEMENT HIGH-LEVEL DESIGN.....	16
2.1 PRIORITIZATION OF FSA BUSINESS OBJECTIVES FOR ENROLLMENT AND ACCESS MANAGEMENT.....	16
2.2 CONCEPTUAL DESIGN- ENROLLMENT AND ACCESS MANAGEMENT VISION SOLUTION	17
2.3 DESCRIPTION OF ACCESS MANAGEMENT COMPONENTS	19
2.3.1 <i>Identity Management</i>	20
2.3.2 <i>Access Control</i>	25
2.4 BUSINESS OBJECTIVES MAPPING TO ACCESS MANAGEMENT COMPONENTS.....	28
3 IMPLEMENTATION CONSIDERATIONS	30
3.1 DEVELOPMENT OPTIONS	30
3.1.1 <i>Commercial Software vs. Custom Development</i>	30
3.1.2 <i>Evaluation of Commercial Access Management Software</i>	32
3.2 ACCESS MANAGEMENT DEPLOYMENT OPTIONS	32
3.2.1 <i>Approach A: Deploy Access Control System First</i>	34
3.2.2 <i>Approach B: Deploy Identity Management System First</i>	35
3.2.3 <i>Approach C: Deploy Access Control and Identity Management Together</i>	36
3.3 DEPLOYMENT APPROACH CONSIDERATIONS	37
3.3.1 <i>Deployment Approach Considerations</i>	37
3.3.2 <i>Deployment Planning</i>	38
4 ACCESS MANAGEMENT BUSINESS INTEGRATION.....	40
4.1 COMMON BUSINESS PROCESSES - TRADING PARTNERS	41
4.1.1 <i>Trading Partner Enrollment</i>	43
4.1.2 <i>Trading Partner Changes</i>	44
4.1.3 <i>Trading Partner Termination</i>	45
4.2 COMMON BUSINESS PROCESSES- TRADING PARTNER USERS.....	46
4.2.1 <i>New User</i>	48
4.2.2 <i>Self-Service</i>	49
4.2.3 <i>Change of Status</i>	51
4.2.4 <i>User Termination/User Leaves Trading Partner</i>	52
4.3 USER AUDIT FUNCTIONS.....	52
4.4 ORGANIZATIONAL & POLICY IMPLICATIONS.....	54
4.4.1 <i>Major Functions</i>	54
4.4.2 <i>General Security Implications</i>	55
5 EXTERNAL INTEROPERABILITY: SHARING IDENTITY AND AUTHENTICATION CREDENTIALS	57
5.1 BACKGROUND.....	57



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

5.2	BENEFITS OF FEDERATED IDENTITY	58
5.3	MAJOR FEDERATED IDENTITY STANDARDS	58
5.3.1	<i>Liberty Alliance</i>	58
5.3.2	<i>WS-Federation</i>	59
5.3.3	<i>Other Federated Identity Efforts</i>	59
5.4	INTEGRATION WITH FEDERAL SECURITY ARCHITECTURE EFFORTS	59
5.4.1	<i>e-Authentication</i>	59
5.4.2	<i>Progress and Current Status</i>	59
5.4.3	<i>Future E-Government Directions</i>	60
5.5	RECOMMENDATIONS	60
6	NEXT STEPS	62
	APPENDIX A: BUSINESS OBJECTIVES PRIORITIZATION	63
	APPENDIX B: PROPOSED FSA SECURITY AND PRIVACY TECHNICAL ARCHITECTURE	68
	APPENDIX C: BUSINESS OBJECTIVE MAPPING	69
	APPENDIX D: BACKGROUND ON FEDERAL EGOV E-AUTHENTICATION EFFORT	95



Figures

Enrollment and Access Management Conceptual Design	3
Figure 1 - Business Objective Prioritization	17
Figure 2 - Enrollment and Access Management Conceptual Design	18
Figure 3 - Access Management Components	19
Figure 4 - Identity Management	20
Figure 5 - Enterprise User Administration	21
Figure 6 - Delegated Administration	22
Figure 7 - Audit	23
Figure 8 - Access Control	25
Figure 9 - Web Authentication	26
Figure 10 - Authorization	27
Figure 11 - High Level Requirements Mapping	29
Figure 12 - Access Management Solution Deployment Components	33
Figure 13 - Implementation Strategy Approach A	34
Figure 14 - Implementation Strategy Approach B	35
Figure 15 - Implementation Strategy Approach C	36
Figure 16 - Sample project plan for access control (WAC) and identity management (Provisioning) systems	39
Figure 17 - Common Business Process Trading Partners	42
Figure 18 - New Trading Partner Enrollment	43
Figure 19 - Change of Affiliation	44
Figure 20 - TP Termination	45
Figure 21 - Common Business Process Trading Partner Users	47
Figure 22 - New User Enrollment	48
Figure 23 - Password Reset	49
Figure 24 - Password Renewal	50
Figure 25 - Change of Status	51
Figure 26 - User Termination	52
Figure 27 - User Audit Process	53
Figure 28 - Sample Federated Identity Architecture	58
Figure 29 - Proposed FSA Security and Privacy Technical Architecture	68
Figure 30 - Interim e-Authentication Users	96
Figure 31 - eGov Portal Overview	97
Figure 32 - eGov Portal Detailed Architecture	99
Figure 33 - Authentication Level and Appropriate Credentials	101
Figure 34 - Potential eGov Integration Approach	105
Figure 35 - Potential eGov Integration Architecture	108



1 Introduction

1.1 Purpose

Like the majority of public and private sector organizations, FSA has integrated security and access management functions into each information system it has developed. This has resulted in the proliferation of different administrative and technical controls for common security functions, such as user authentication, access privilege authorization, and user account management. As a result, processes for managing access to information systems across FSA are fragmented and complex. The enrollment and access management initiative reviewed the current methods for managing access and developed a high-level solution design to improve the efficiency and reliability of access management processes. The high-level design described in this document will provide a roadmap for implementing a new vision for access management. The primary goal of the proposed solution is to provide FSA with capabilities to effectively manage access to systems and data in a manner consistent with business objectives, while also satisfying internal and federally-mandated security and privacy requirements.

The purpose of the Access Management High-Level Design document is to present a high-level design that provides enterprise functions for managing Trading Partner access to FSA systems. This deliverable describes the Access Management solution options that will enable FSA to meet the business objectives and high-level requirements identified in the first phase of this effort. Each of the major components of the proposed Access Management solution are defined and their integration to achieve overall FSA goals is discussed. The high-level design is validated by mapping its functions and features to the specific business objectives and high-level requirements for access management. The solution includes an explanation of how access management components can be integrated into FSA business activities. The deliverable presents options and considerations for how the Access Management solution can be implemented.

Related federal initiatives in the E-Government e-Authentication program are defining an architecture for authentication of individuals who use online government services. This work addresses methods for sharing user identity information across federal agencies. These efforts primarily address user authentication functions and a few of the other critical access management requirements that FSA has identified (such as authorization, auditing, and enterprise account management). The E-Government activities and their relevance for FSA are also addressed in this document.

1.2 Background

The Department of Education's Office of Federal Student Aid (FSA) seeks improvements to data quality and data consistency. FSA is examining its overall approach to data to ensure accurate and consistent data exchange between customers, Trading Partners, and compliance and oversight organizations. FSA will also leverage a targeted data strategy to support program-wide



goals of maintaining a clean audit and removing FSA from the General Accounting Office (GAO) high-risk list.

Task Order 123 defines FSA's Enterprise Data Vision and its overall Enterprise Data Strategy. The end result of this task order will be an enterprise data framework that integrates the Framework, Technical Strategies, XML Framework, Common Identifiers, and Enrollment and Access Management into an overall FSA Enterprise-wide Data Strategy. The purpose of the FSA Enterprise-Wide Data Strategy is to define FSA's enterprise data vision and strategy for how it will combine the tools, techniques and processes, documented in the FSA Data Strategy Framework, to handle its enterprise data needs.

The Enrollment and Access Management deliverables were defined to identify FSA business objectives and a high-level design for processes and tools that improve the initial sign-up and management of access that Trading Partners need to FSA systems and data. The previous deliverables Enrollment Business Objective High-Level Requirements (Deliverable 123.1.26) and Access Management Business Objectives High-Level Requirements (Deliverable 123.1.27) documented business objectives and high-level requirements for enrollment and for access management, respectively.

Analysis and design activities for enrollment and access management have been coordinated with the Routing ID (RID) project and other Data Strategy projects. Integration and coordination of analysis and design activities across these projects will streamline and simplify Trading Partner enrollment and user access management for all FSA systems.

1.3 Definition of Terms

For the purposes of this deliverable, *Access Management* is the term used to describe policies, processes, and tools that:

- Define user access privileges and roles.
- Issue and approve user identity credentials linked to access privileges.
- Create, modify, audit, and remove user access to FSA systems.
- Provide user services to facilitate access to FSA systems and data.

Access Control provides user identification, authentication, authorization, and secure session management services to applications and resources within the enterprise. Depending on design, an Access Control system can also provide single or simplified sign-on to applications and help reduce the number of UserIDs and passwords.

Identity Management provides centralized user access, account administration, resource provisioning, and identity data management services. Additional capabilities that may be included in an identity management system are password management, password synchronization, delegated administration, and self-service functionality. These additional functions can be implemented in a modular fashion after the basic identity management system is deployed.



Trading Partner is defined as all non-student business entities that use FSA systems. Trading Partners include post-secondary institutions (Schools), Lenders, Guaranty Agencies (GAs), State Agencies, Federal Agencies and other entities, such as Servicers, authorized to act on their behalf. For the purposes of this deliverable, FSA staff and contractors, collectively referred to as Internal Users, are also included within the definition of Trading Partner.

Trading Partner Enrollment is defined as the initiation of a business relationship with FSA, specifically in the existing areas of Title IV certification process, Student Aid Internet Gateway (SAIG) enrollment and the initial registration of the Trading Partner's designated administrator in required FSA systems.

1.4 Scope

This deliverable covers work defined in Task Order 123 related to documentation of the Access Management High-Level Design. The intent of the access management effort is to review and analyze FSA's current access management processes and look for ways to simplify the business process for Trading Partners. This effort will begin the process of defining potential future solutions for FSA access management. While the enrollment covers the processes for Trading Partners to sign-up, access management provides processes and tools to control Trading Partner access privileges and administrative functions.

Key elements of the high-level design included in this deliverable are:

- The conceptual, high-level design vision for the Access Management solution.
- An overview of access management components including access control and identity management systems.
- A mapping of the high-level design to FSA high-level requirements that validates the ability of the Access Management solution to meet FSA business objectives.
- Implementation approach considerations.

This is the second phase of the enrollment and access management initiative. This phase consists of documenting solution options and high-level design for enrollment and access management and culminates in the following two deliverables:

- Deliverable 123.1.28 – Enrollment High-Level Design. This deliverable defines the high-level design for providing an integrated enrollment management for Trading Partners.
- Deliverable 123.1.29 - Access Management High-Level Design. This deliverable defines the high-level design for providing an integrated access management process for Trading Partners.



1.5 Approach

Prior to beginning development of the high-level design for access management, FSA business objectives were prioritized to define which functional areas are most important. Available technologies and processes were then investigated to identify candidate components. The FSA Security and Privacy Architecture was used as a guideline for technology options that meet FSA business objectives. The technology options that were identified were then integrated in a solution vision. The solution vision and implementation options were then reviewed through several meetings with FSA stakeholders.

Meetings were held with FSA team members to obtain input on the enrollment and access management areas and update FSA on the progress of this initiative. Core Team meetings were held on September 4, 2003 and October 9, 2003. Major elements of the high-level design were presented to the Business Integration Group (BIG) on July 29, 2003. This discussion included a review of major implementation options for Access Control and Identity Management components. The progress of enrollment and access management was a topic covered at BIG meetings on September 9, 2003 and October 16, 2003.

1.6 Organization of This Document

This document, Deliverable 123.1.29, and its companion document, Deliverable 123.1.28, present the Enrollment and Access Management High Level Design activities for Task Order 123. This document contains a summary of access management related work accomplished during this phase of the project, future state conceptual diagrams incorporating information gathered from FSA Core Team members, solution options, evaluation criteria, deployment approach considerations, and an overview of current business processes employed at FSA that impact access management processes. This is a starting point that will facilitate further discussion and refinement of the future access management solution that FSA may implement.

The organization of this document is summarized below:

- Section 1 – *Introduction* discusses the context and background for the project and this deliverable.
- Section 2 – *Access Management High-Level Design* documents the access management conceptual design and describes the access management conceptual design components. This section also contains a mapping of the access management components to the high-level requirements defined in the previous phase of this effort.
- Section 3 – *Implementation Considerations* describes the access management development strategies and deployment options. This section concludes with a deployment approach recommendation.
- Section 4 – *Access Management Business Integration* discusses access management related common Trading Partner and user business processes. Organizational and policy implications are also identified.



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

- Section 5 – *External Interoperability* describes the approaches for sharing identity and authentication credentials. The issue of integration with federal security architecture efforts is addressed.
- Section 6 – *Next Steps* describes recommended next steps for the Enrollment and Access Management High-Level Design.



2 Access Management High-Level Design

2.1 *Prioritization of FSA Business Objectives for Enrollment and Access Management*

In the first phase of this effort, FSA business objectives and high-level requirements for enrollment and access management were identified. These enrollment and access objectives were created in conjunction with the Business Integration Group (BIG) objectives. The BIG defined five major goals for FSA:

- Integrate FSA systems and provide new technology solutions.
- Improve program integrity.
- Reduce program and administrative costs.
- Improve human capital management.
- Improve products and services to provide better customer service.

To assist in evaluating enrollment and access management solution options, the enrollment and access management business objectives were prioritized by applying the following criteria:

- **Benefits to FSA:** The business objectives being considered should provide benefits to FSA such as improving security or reducing the time or resources required to complete enrollment and access management activities.
- **Minimal Impact to FSA:** The business objectives that will be implemented should have minimal impact on the current operation of FSA.
- **Benefits to Trading Partners:** These business objectives should provide benefits to FSA's Trading Partners by making it easier for them to conduct business with FSA.
- **Minimal Impact to Trading Partners:** The business objectives being considered should have minimal impact on Trading Partners and should not disrupt their normal business functions with FSA.
- **Applicability to Enrollment and Access Management:** These business objectives should be applicable to enrollment and access management at FSA.
- **Alignment with FSA Strategic Objectives:** These business objectives should also align with the FSA Strategic Objectives. This category measures how closely the business objective match with the FSA Strategic Vision.
- **Overall:** The overall priority of the enrollment and access management business objective based on the average of the other qualitative criteria.

These business objectives were rated on each of the above factors utilizing a scale of High (H), Medium (M) and Low (L). Details on this evaluation can be found in Appendix A- Business Objectives Prioritization. Below is a summary list of top business objectives for FSA based on the cumulative average of the factors above.



#	Business Objective	Importance
A2.1	Manage enrollment and access privileges at the enterprise level.	H
A1.1	Focus on registration processes and access decisions at the enterprise level instead of on a per system basis.	H
A3.1	Streamline enrollment and access management for Trading Partner services.	H
B2.1	Provide effective oversight of user access to FSA systems.	H
A2.4	The enrollment and access solution should be flexible enough to support the requirements of current and future FSA systems.	H
C2.2	Maintain security of FSA systems.	H
C3.2	Adopt enrollment and access management policies that improve business processes.	H
A2.2	Improve self-service capabilities.	M
B3.1	Meet FSA regulatory compliance requirements.	M
C2.3	Provide users with access to FSA systems appropriate for their job function.	M
A2.3	Balance easier access and system security.	M
C3.1	Provide effective training and customer support across FSA systems.	M
B1.1	Adopt a uniform decision making process for evaluating users requesting access to FSA systems.	M
C1.1	Facilitate access to sets of data at the enterprise level.	M
C2.1	Create enterprise policy and standards for enrollment and access management.	M
A2.5	Allow users to customize their experience with FSA systems.	L

Figure 1 - Business Objective Prioritization

2.2 Conceptual Design- Enrollment and Access Management Vision Solution

The enrollment and access management initiatives are integral parts of simplifying and improving Trading Partner interaction with FSA. Today, Trading Partners enroll in FSA services on a system-by-system basis. A unified enrollment process would provide a single management point for enrollment data and eliminate organization-specific or system-specific anomalies in user sign-up or user permissions.



The Access Management System in the conceptual design is comprised of:

- Identity Management Components
- Access Control Components.

Identity Management manages enterprise security functions across environments and platforms, reduces the number of passwords needed for log in (simplified sign-on and password synchronization), provides self-service functions, and allows for delegated security administration of selected tasks. Access Control functions reduce the number of UserIDs and passwords for Web based applications (single sign-on), provide tools to implement Web services security standards, and supply flexible authentication methods for Web applications.

Enrollment and Security Administration Workflow automates the enrollment and access management data flow between systems. This automation includes routing requests and managing the approval process. The combination of a simplified enrollment process coupled with an enterprise Access Management solution will greatly improve the Trading Partner’s experience with FSA and provide additional security for FSA systems.

The Enrollment and Access Management Conceptual Design diagram illustrates the key components of the solution. The interaction between the enrollment component and access management component is depicted in the following figure.

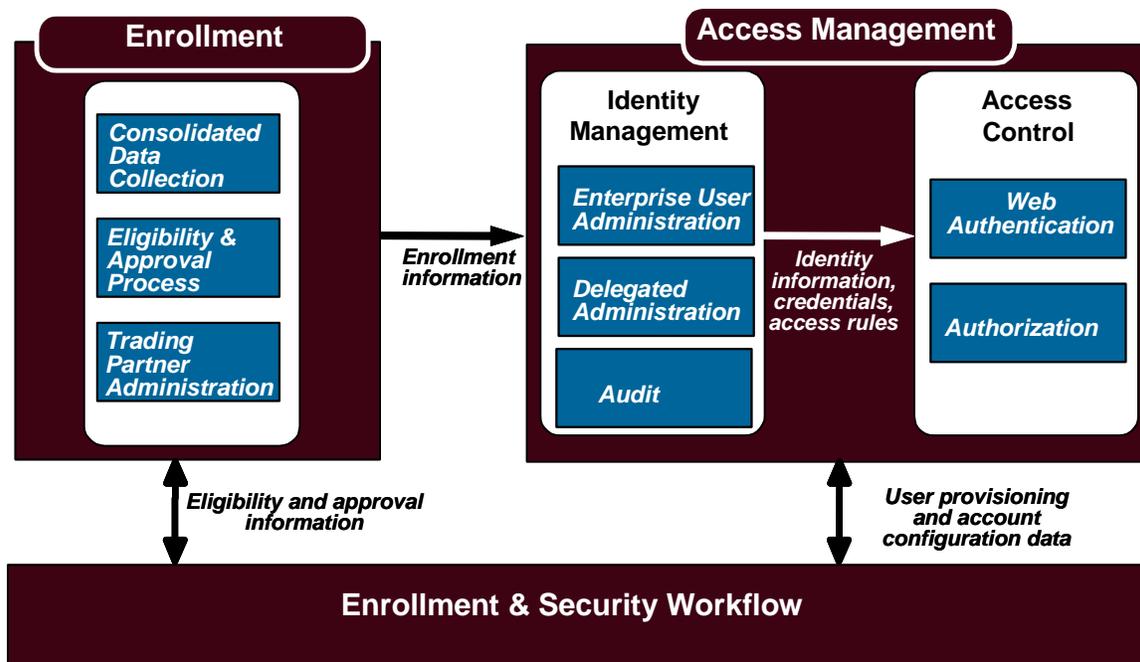


Figure 2 - Enrollment and Access Management Conceptual Design



2.3 Description of Access Management Components

The following sections document the access management component of the conceptual design. The access management solution has two components: Identity Management and Access Control. Additional access management components not shown in the conceptual design are described in the end of each section.

This Access Management Conceptual Design is consistent with the proposed security and privacy technical architecture found in Appendix B- Proposed FSA Security and Privacy Technical Architecture. Additional information on the enrollment process can be found in the Enrollment High-Level Design (Deliverable 123.1.28).

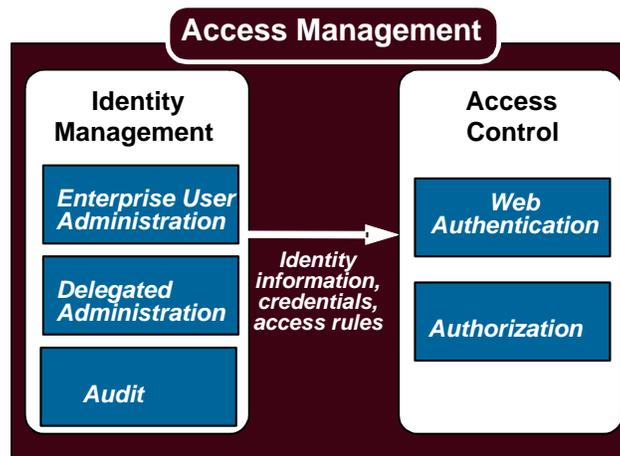


Figure 3 - Access Management Components



2.3.1 Identity Management

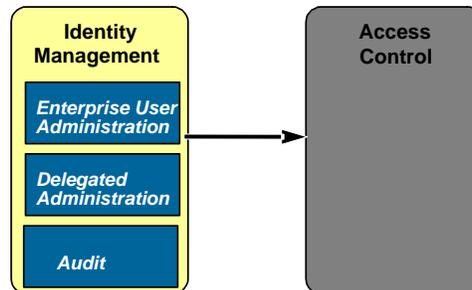


Figure 4 - Identity Management

Identity Management solutions provide several critical enterprise functions for user administration and management. These functions automate the process of creating and maintaining identity information. The identity management system has the following major design features and functions:

- Able to manage security functions across all environments (Web, client/server, legacy, mainframe) and platforms (Operating System (OS), Commercial Off-the-Shelf (COTS) applications, custom applications).
- Has a minimal impact on managed targets and does not require application code changes or new user directories.
- Can integrate with a workflow system to manage security approval and provisioning.
- Provides password synchronization across multiple systems.
- Can integrate with non-standard applications through development of a custom interface using application program interfaces (APIs) or toolkits.
- Does not affect runtime authentication services, runtime access control services, or single sign-on or Web session management functions.

An Identity Management solution provides four general types of functionality:

- Enterprise User Administration
- Delegated Administration
- Audit
- Additional Identity Management Capabilities

Each of these general functional areas are discussed in greater detail in the following sections.



Enterprise User Administration

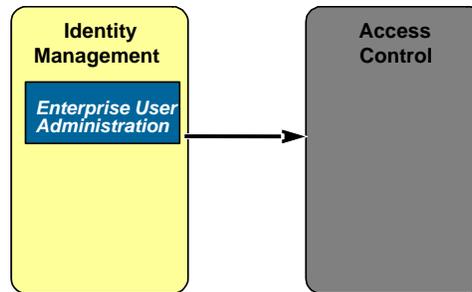


Figure 5 - Enterprise User Administration

The enterprise user administration function manages the creation and maintenance of a user's identity information. Rules based on business requirements can be used to assign user access rights that enforce FSA security policies. The enterprise user administration function would be able to use a Roles Based Access Control (RBAC) approach to grant access rights to users based on their assignment to a defined role in the organization. RBAC allows for access control to be managed at a level that corresponds closely to the organization structure.

The enterprise user administration functions will manage large numbers of users across disparate FSA systems. Functions will also be available to monitor and modify user access privileges for Trading Partners according to FSA security policies. Any change to information about a Trading Partner will be evaluated to determine if it alters the access privileges required for that user. For example, if a Trading Partner is debarred by FSA, enterprise user administration functions will enable FSA security administrators to quickly terminate access for all of that Trading Partner's users. This functionality will improve the security of FSA systems by providing methods to manage users as a group. By associating users with a Trading Partner, and through the use of provisioning and de-provisioning functions that manage access to multiple systems at the same time, FSA will have the ability to manage user access at the enterprise level, decreasing the need for individual user account administration tasks within each FSA system.



Delegated Administration

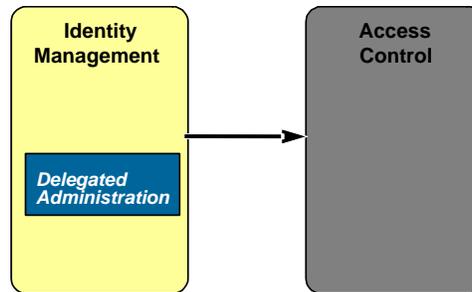


Figure 6 - Delegated Administration

Delegated administration functions enable the allocation of user account administration tasks to trusted administrators as designated by external Trading Partners. This would allow administrative tasks (such as requesting access for a user or approving a change in access) to be performed by administrators who have the most accurate knowledge about the user and their access needs.

Delegated administration enables FSA to filter information so that only the authorized administrative functions and user information is presented to the external administrator. For example, various Trading Partners may be provisioning users into a common Identity Management system, but each Trading Partners data must remain invisible to the others. Therefore, distinct FSA Trading Partners would be able to assign users and define functionality for their specific user base, but the Trading Partners would not be able to see or modify the user profiles or capabilities of other FSA Partners.

The delegated administration model allows administrators to manage users and groups from a single location across their infrastructure. Key benefits of this model include reduced administration costs, improved ease of use, and increased security.



Audit

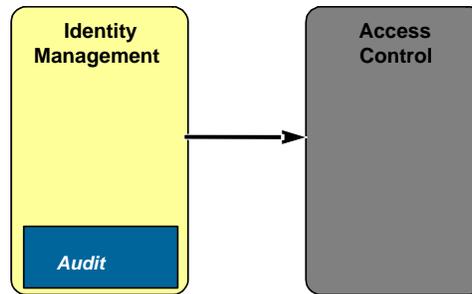


Figure 7 - Audit

The ability to audit access to FSA systems is important for compliance and reporting purposes. Currently, auditing user access privileges requires system-by-system examination of user security information. The Identity Management system will be able to communicate with the security functions within each FSA system. This will make it possible to design and run audit reports to produce enterprise views of access privileges across the FSA environment.

Access privilege audit functions will include the ability to:

- Construct audit reports to identify access privileges and security settings for individuals or groups of individuals across all connected FSA systems.
- View or report on user access privileges within individual systems based on specific user attributes or affiliations.
- View or report on changes to user access privileges, such as who made the modification or when it was made.

Additional Identity Management Capabilities

Provisioning

Provisioning is the process of user account creation and configuration across multiple systems. It allows for administrating user access privileges to enterprise applications, networks, databases and other essential resources. Identity Management solutions allow for the automation of provisioning functions. Some of the benefits of provisioning are:

- Faster user account creation and access modification.
- Consistent and accurate enforcement of security policy.
- Fewer resources required due to automation.
- Compatibility with delegated administration.
- Integration with auditing and reporting mechanisms.



Provisioning Workflow

The identity management solution can implement customized business processes for user management. Pre-configured approval workflows for key tasks, such as creating user profiles or assigning users to roles and groups, could be integrated into the identity management system. These workflows can be modified and extended in support of specific FSA business requirements.

Identity Management Connectors

The identity management solution will need to communicate with the FSA systems being managed to allow for automated user provisioning. Connectors or software agents can be deployed to communicate with managed resources, such as applications, operating systems, or databases. The communication link between the identity management system and the managed platform must be secured, and is usually encrypted to prevent interception or compromise of the sensitive security configuration data it carries. The connectors and agents should provide enough flexibility to allow for communication with a wide variety of custom-developed and commercial systems.

Self-service

The process of self-service allows users to perform functions related to their access, independent of system administrators. For example, users can reset their password by answering authentication questions on a Website. Self-service capabilities reduce some of the burdens on help desks and administrators by allowing users to perform a limited range of tasks without administrative assistance. Some of these activities include:

- Requesting access to enterprise applications.
- Changing user profiles (such as updating address or phone number).
- Accessing online help.
- Password policy management.
- Password resets or synchronization across multiple systems.

Password Management – Password Polices and Reset Functions

Password management allows for an enterprise to control password quality in such a way that the organization security polices are followed. Self-service password management capabilities allow users to reset or update their accounts and passwords by visiting a website. The passwords they select are evaluated against rules on their formation to ensure uniform conformance with organizational password polices. Poor password management increases the workload on the FSA helpdesks, for example, to reset forgotten passwords.

Password Management - Password Synchronization

Password synchronization propagates password changes between systems effectively resulting into a single unified password and enables access control mechanisms to provide Single sign-on. Currently, since FSA has many systems that provide individual access control capabilities, users are required to remember a large number of passwords. These numerous passwords pose a risk



to FSA as users have a tendency to write down their passwords in order to keep track of them. Besides the obvious convenience to the user, if password synchronization is employed, FSA can make its password policy stricter (number of characters and types required). Password synchronization reduces support costs since users who remember their passwords have far fewer password problems, and do not need the help desk as frequently.

2.3.2 Access Control

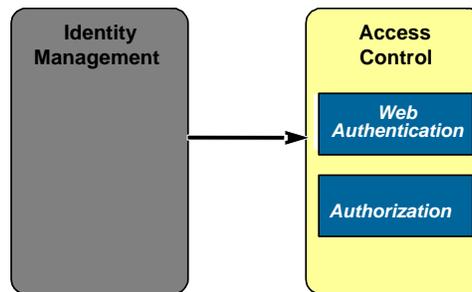


Figure 8 - Access Control

The Access Control system would provide flexible runtime authentication services and access control for Web applications. Single sign-on and session management functions are provided by this component. A typical implementation for access control would include a Web access control product, which would manage and administer user authentication and authorization for Web applications, but not for legacy applications. Application coding changes may be required to integrate a Web access control system with applications, portals, personalization engines, etc. Application changes are also required to integrate login functions, credential passing, and other access control functions.

Access Control addresses three major functional areas, described below in greater detail:

- Web Authentication
- Authorization
- Additional Security Capabilities



Web Authentication

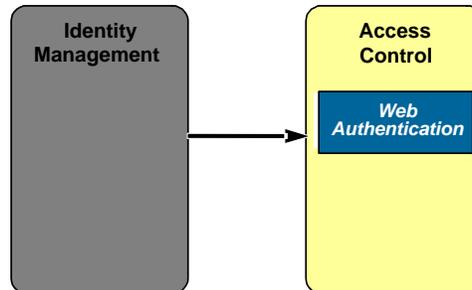


Figure 9 - Web Authentication

The Web Authentication service validates the identity of the user. The validation can be done through many different methods such as UserID and password validation, token-based authentication, or digital certificate validation. To provide stronger security, authentication technologies can be combined to provide multi-factor authentication.

Web Single sign-on (SSO)

Single Sign-on (SSO) 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 authentication information when switching from one application to another. SSO is typically deployed to streamline the authentication process for users. SSO can integrate with multiple authentication mechanisms to address different authentication requirements.

SSO mechanisms can be integrated in various ways in a heterogeneous environment. An SSO system could be integrated with the operating system (OS) login/logout process, or with non-Web applications such as legacy systems. However, the Access Management solution envisions SSO capabilities will be provided only for Web applications. There are two major reasons for this recommendation:

- Implementation of SSO for non-Web applications is significantly more difficult and costly to implement compared to SSO for Web applications.
- All new major online capabilities for Trading Partners are expected to either be deployed as Web applications, or to provide a Web-based interface.

SSO Session Management

A session represents the period of time after a successful user authentication until logout from a Web-based resource. FSA administrators may choose to set policies around sessions to ensure security and optimize network bandwidth. FSA can define idle session timeouts, maximum session timeouts, and user or application logout procedures. For example, an FSA session could have a maximum lifetime of two hours, at the conclusion of which the session would be



automatically terminated. FSA could also limit the number of concurrent sessions that are allowed for a single user.

Authorization

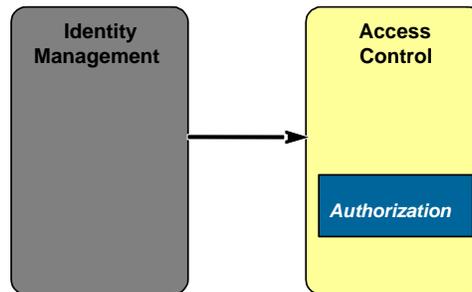


Figure 10 - Authorization

The authorization service validates that a user has approved privileges to access specific protected resources. The validation could be based on a user's role and enterprise security rules and policies. The user authorization step follows the Web authentication step. Access control authorization can be implemented with static access control lists (ACLs), dynamic rules based on business logic, or with some combination of ACLs and rules. ACLs 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. ACLs and access rules are usually stored within the Access Control system, typically in the same directory or database repository that houses user security data.

Initially, authorization functions can remain within existing applications to minimize the integration effort required to deploy a Web access control system. As FSA systems are consolidated or redeployed, this approach can be revisited to assess the advisability of moving some authorization functions to the access control component of the Access Management System. For example, if multiple Web applications are being managed by a single access control site as part of a portal, it would be useful to apply authorization rules to limit the applications and links displayed for each user to only those functions for which that user is authorized. For example, a Financial Aid Administrator visiting the schools portal could be presented a page with a link to Common Origination and Disbursement (COD) website but not links to applications for financial partners.

Additional Security Capabilities

Repository Components

Repository components in an Access Control system provide the ability to leverage external directories and databases to store authentication and authorization information such as user credentials, user roles, or other user attributes. Access Control systems provide interoperability with enterprise user data stores including relational databases and Lightweight Directory Access Protocol (LDAP) directories. These components communicate with the user data store for the



exchange of authentication credentials. The credentials are requested by the Access Control system during the runtime user authentication. Repository components will allow FSA to tap into the existing repository of profile information to leverage existing user information and security data.

User Activity Logging

Saving relevant user data is necessary to audit compliance with FSA policies and procedures. Audit capabilities are also used to detect misuse and abuse. Identity Management provides end-to-end auditing of all transactions with full reporting of all security events. Auditing capabilities enhance an enterprise's security by providing the records required to review compliance with security policy.

The audit trail begins with detailed logs that serve as proof of user activity. The administrator can use audit logs to confirm transactions and prove that specific user activity occurred. For reporting, data can be filtered by a variety of attributes. For example, if FSA suspects an account was compromised at a particular school, the Identity Management solution can generate a report of all activity for that account.

2.4 Business Objectives Mapping to Access Management Components

Figure 11 shows which Access Management functions and components support FSA business objectives for Enrollment and Access Management. The requirements mapping was developed as a way of summarizing and validating the effectiveness of the proposed Access Management solution. Each business objective is supported by one or more identity management or access control functions.

Appendix C- High-Level Requirements Mapping provides a detailed analysis comparing each component of the identity management and access control solutions with the enrollment and access management high-level requirements.



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

	Enrollment and Access Management Business Objectives															
	A1.1 Enterprise process focus	A2.1 Manage across systems	A2.2 Self-service capabilities	A2.3 Balance access and security	A2.4 Flexibility for future requirements	A2.5 User customization	A3.1 Streamline enrollment and registration	B1.1 Uniform process for access decisions	B2.1 Audit user access	B3.1 Meet regulatory requirements	C1.1 Facilitate enterprise access to data	C2.1 Enterprise policies and standards	C2.2 Security of FSA systems	C2.3 Match access to job functions	C3.1 Effective training and support	C3.2 Adopt policies to improve processes
Identity Management & Access Control Functions																
Identity Management (IM)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
IM- Enterprise User Administration	✓	✓					✓	✓				✓			✓	✓
IM- Delegated Administration			✓		✓			✓				✓		✓	✓	
IM- Audit	✓			✓				✓	✓	✓		✓	✓	✓	✓	✓
IM- Provisioning		✓	✓	✓				✓						✓	✓	
IM- Self Service		✓	✓	✓		✓	✓							✓		
IM- Password Management			✓	✓										✓		
IM- Password Synchronization		✓		✓												✓
Access Control (AC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AC- Basic Authentication				✓				✓			✓	✓	✓			
AC- Flexible Authentication	✓	✓		✓				✓			✓	✓	✓			
AC- Single Sign-on (SSO)	✓	✓		✓			✓				✓	✓	✓			
AC- Session Management	✓	✓		✓			✓				✓	✓	✓			
AC- Password Policy Management		✓	✓	✓					✓	✓			✓	✓	✓	✓
AC- Custom User Interface			✓		✓	✓		✓								
AC- Administrative Interfaces	✓	✓		✓	✓			✓	✓			✓			✓	
AC- Registration Pages			✓		✓	✓	✓	✓								
AC- Audit Logging	✓	✓		✓					✓	✓		✓	✓	✓		
AC- Migration Utility		✓		✓	✓					✓	✓					
AC- Flexible Data Storage Communications	✓						✓		✓	✓	✓	✓				
AC- APIs/ SDKs	✓	✓			✓						✓					
AC- Support of Multiple Web Application Platforms	✓	✓			✓											
AC- Role Based Authorization	✓	✓			✓			✓	✓			✓		✓		✓
AC- Dynamic Authorization		✓		✓				✓		✓	✓	✓				

Figure 11 - High Level Requirements Mapping



3 Implementation Considerations

The Access Management vision defined in Section 2 consists of two major components. The access control capability will consolidate authentication and other security services for Web applications. The identity management system will satisfy enterprise administration requirements for user account management, provide audit and oversight functions, and supply several associated security functions such as password reset and synchronization. This section analyzes the considerations for deployment of these new capabilities for management of access to FSA systems and data. The following major topics are addressed in this section:

- Use of commercial software vs. custom development.
- Deployment options.
- General Deployment Considerations.

3.1 Development Options

The access control and identity management functions described in Section 2- Access Management High-Level Design could be either custom developed or could be implemented by integration of commercial products. The Enrollment and Access Management team recommends consideration of commercially available (commercial off the self) products to implement an Access Management System. There are numerous security administration and control products that provide the functionality to achieve FSA objectives for access management. The rest of this section describes the justification considerations for choosing between commercially-available access management tools and custom-developed solutions.

Consider commercially available (COTS) software to implement the Access Management solution.

3.1.1 Commercial Software vs. Custom Development

Mature commercial software is available that provides all of the major functionality required for implementation of the Access Management System. In contrast, custom development of the necessary functionality would face several major challenges, as outlined below.

There are a large number of functional requirements

The Access Management solution envisions integration of several major functions to meet the FSA business objectives. Custom development of all required functions would require a major development effort compared to integration of existing commercial software components. The major functional components that would need to be developed are summarized below.



- Access Control system functions and components include: http traffic filter, authentication engine, policy and rules engine, session management functions, LDAP directory/repository communications modules, encryption modules for security communications between system components, secure auditing functions, administrative interfaces, application programmer interfaces and software development kits (SDKs) to support access control for unique platforms and applications, rules configuration and testing interfaces, utilities for migrating existing user data to new directory formats, or the ability to use existing identity stores.
- Identity Management system functions and components include: provisioning engine, administrative interface, communications protocols for existing security repositories, connectors or agents for all platforms or applications to be managed, auditing functions, password synchronization, password policy management, password reset systems, and integration with security approval workflow system, security data communication and migration systems.

Components would need to be developed to support flexibility for multiple platforms and future changes in requirements and functions.

For example, support requirements for authentication may change as the need for stronger authentication develops in the future. Existing commercial software is available that provides flexibility in configuration of user authentication mechanisms. This would allow selection of strong authentication mechanisms, such as digital certificates or hardware tokens, when password authentication would be inappropriate. Commercial software packages also provide a variety of utilities for migrating existing user data to new directory formats, as well as the ability to use existing identity stores.

Commercial access control software will provide support for emerging security standards, such as SAML, Web services security, and various Federated Identity approaches.

Custom-developed software would need to provide specialized functions to address important risks and performance issues associated specifically with security software. For example, commercial software typically provides encryption of sensitive communications between system components. Implementation of encryption functions is particularly susceptible to introduction of security vulnerabilities because of the difficulty of avoiding compromise of encryption algorithms during implementation. It would be difficult to replicate the extensive testing applied to mature commercial software to check for vulnerabilities in authentication and access control mechanisms. Scalability and performance testing of policy engines and data stores is another area that would require a major effort for custom system development to insure reliability for FSA systems as number of users and transactions increase.



3.1.2 Evaluation of Commercial Access Management Software

Commercial software is currently available to satisfy most if not all of the FSA access management requirements. However, careful evaluation of the technology and products that are available will be required to select software that can meet FSA functional objectives, support existing and planned FSA systems, and satisfy FSA security and privacy requirements. There are Federal recommendations for evaluation of security software, developed by the National Information Assurance Partnership (NIAP), a joint effort of the National Institutes of Standards and Technology (NIST) and the National Security Agency (NSA). These guidelines are based on the Common Criteria¹. However, these evaluation guidelines currently have limited usefulness for FSA. The Common Criteria approach to software evaluation relies on protection profiles that may or may not be suitable for any specific organization. In addition, Common Criteria evaluations only demonstrate that the defined protection profile is satisfied. Finally, the list of protection profiles listed in the NIAP does not currently include software that provides access control or identity management functions. As a result, FSA will need to conduct its own evaluation of commercial access control and identity management products against FSA functional and security requirements.

3.2 Access Management Deployment Options

The two major components of the proposed Access Management solution are an access control system and an identity management system. These two major capabilities could be deployed either sequentially or in parallel. There are specific advantages and disadvantages to initial deployment of access control, initial deployment of identity management, or simultaneous implementation. This section will describe the deployment considerations for each of these three major implementation approaches.

Figure 12 shows the major components of the complete Access Management solution. Major elements include a Web access control system, an identity management system, Web applications, mainframe and legacy systems, and one or more data stores for user information. The access control and identity management components are described in greater detail in Section 2.3 – Description of Access Management Components. Access control and identity management components will communicate with existing Web applications (and new Web applications that will be deployed in the future) to provide both access control and user management security functions. In addition, identity management components will integrate with the mainframe and legacy systems in the enterprise to manage user accounts and provide other identity management services, such as password reset, password synchronization, or access privilege auditing services. One or more user data stores (for example, an LDAP directory or Oracle database) will be used by the access control and identity management systems as a

¹ National Information Assurance Acquisition Policy, National Security Telecommunications and Information Systems Security Committee (now the Committee on National Security Systems, January 2000, revised June 2000 URL: <http://niap.nist.gov/cc-scheme/NSTISSP%2011%20revised%20Fact%20Sheet.pdf>)



repository for user information such as authentication credentials, role and access privilege information, and other user attributes required to make security access decisions.

Each of the three major approaches for deploying these components are discussed below. Advantages, disadvantages, and other implementation considerations are discussed for each approach. The following section will then identify the approach recommended by the Enrollment and Access Management team.

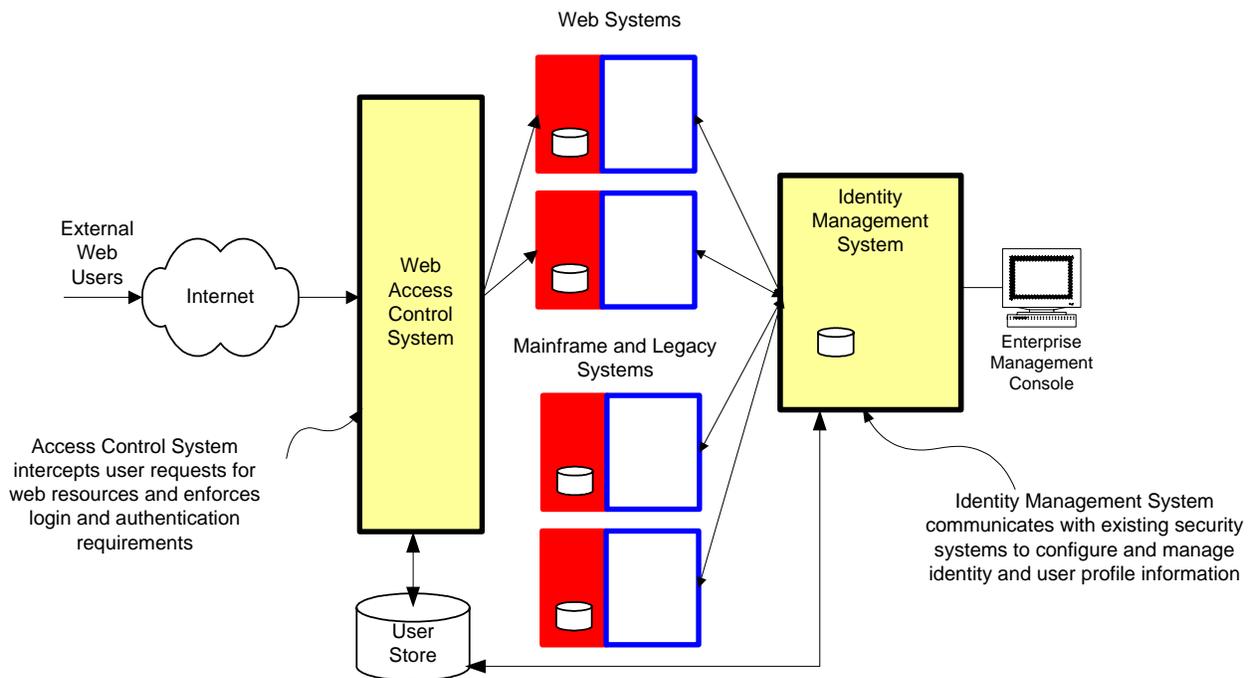


Figure 12 - Access Management Solution Deployment Components



3.2.1 Approach A: Deploy Access Control System First

This approach would first implement a Web Access Control system to provide authentication services and Single sign-on for multiple Web applications. Once the basic Web Access Control capabilities are deployed, an identity management system would be added to supply user account management functions for both Web applications and other FSA systems such as mainframe and legacy systems.

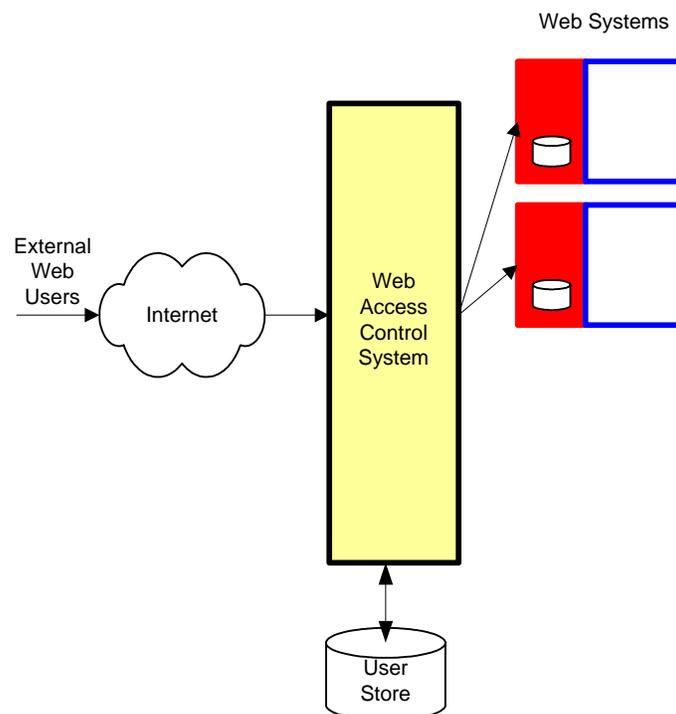


Figure 13 - Implementation Strategy Approach A

Advantages

- Rapid support for Single sign-on to multiple Web applications, providing simpler sign-on for users of multiple applications and an improved user experience.
- Support for other security functions for Web portals and other Web applications, including flexible authentication options, authorization controls, and user activity auditing.

Disadvantages

- Does not address many of the security management and administration requirements identified as FSA business objectives for enrollment and access management.
- Addresses security functions only for Web application users, not for FSA legacy systems.
- Requires application code changes to support authentication, Single sign-on, authorization, and session management functions.



3.2.2 Approach B: Deploy Identity Management System First

This approach would first deploy an Identity Management system to provide administrative functions for both legacy systems and Web applications, including user account management services, user provisioning functions, user self-service capabilities such as password reset, password synchronization, and delegated administration.

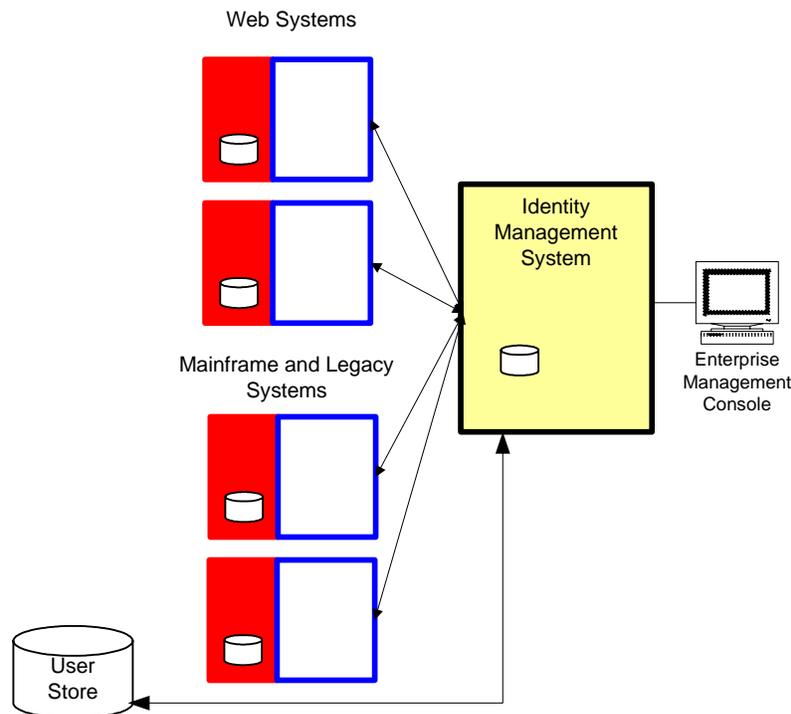


Figure 14 - Implementation Strategy Approach B

Advantages

- Addresses many of the high-priority administrative requirements identified by FSA, including centralized administration, auditing and reporting functions, and streamlined support for administration of user account parameters across multiple FSA systems.
- Low impact on FSA systems and application because no program changes are required to integrate administrative functions.

Disadvantage

- Can synchronize user passwords across multiple systems, but does not provide true single sign-on capability for Web applications.



3.2.3 Approach C: Deploy Access Control and Identity Management Together

This approach would integrate the implementation effort for both the Access Control system and the Identity Management system.

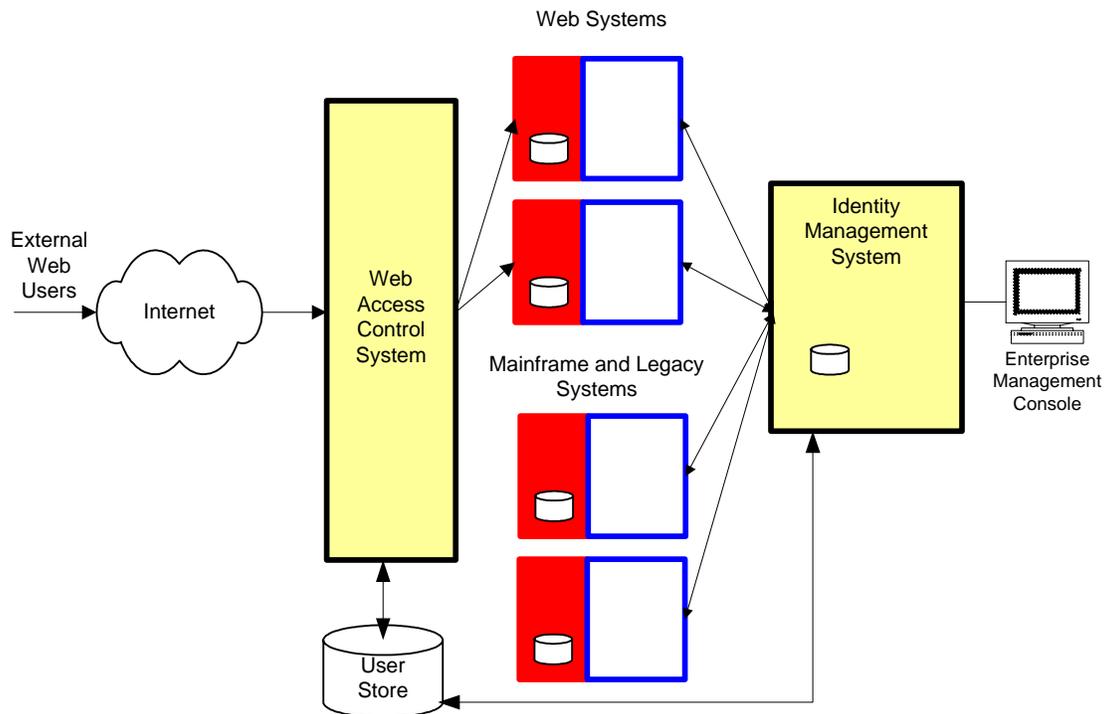


Figure 15 - Implementation Strategy Approach C

Advantages:

- Achieves all major FSA business objectives for enterprise administration, auditing, and user self-service improvement.
- Provides security functions for Web applications, including Single sign-on and Web authentication.
- Allows coordinated integration of Access Control and Identity Management capabilities, including enterprise directory development to manage user security data stores, auditing of user activity and access, and definition of enterprise user roles to manage access privileges.

Disadvantages

- Implementation will require a larger team than for approaches that deploy only a single component.
- Budget will need to cover technologies for both major components.



3.3 *Deployment Approach Considerations*

Section 3.2 above defines three major options for deploying Access Management solutions. The approach recommended by the Enrollment and Access Management team is to design, develop and deploy tools and processes to implement both the Access Control and Identity Management components of the Access Management solution at the same time.

Approach C, deployment of both access control and identity management components in a coordinated implementation project, satisfies both major FSA business objectives of improving the Trading Partner experience and providing enterprise management of access.

This section analyzes factors important for selecting the recommended deployment approach, and describes major considerations for planning the deployment of an Access Management solution that best meets FSA requirements.

3.3.1 Deployment Approach Considerations

Simultaneous development of access control and identity management components for the Access Management solution provides several advantages. The primary benefit to this approach is that FSA will be able to more quickly realize the high-priority business objectives that motivate development of new access management capabilities: easier user access to FSA applications, and more effective enterprise management of access across multiple FSA systems. These benefits, as well as other deployment considerations, are discussed in greater detail below.

Integration Benefits

Coordinated development of access control and identity management components will allow an integrated design of a comprehensive Access Management System. This approach will decrease the amount of rework necessary for designing and retrofitting integration points between the two technologies. For example, administrative functions in the identity management system can be used to provision the access control system. In addition, communications links with directory servers (or other repositories of user information) will be needed between both the access control system and the identity management system.

Technical Integration Considerations

Both access control systems and identity management systems require integration with the FSA systems to be managed. Access control systems typically require installation of a software agent on the Web server or application server to intercept requests for protected resources. As a result, using products with this form of access control technology requires that the Web applications be modified so they are able to interpret the user information passed from the access control system. Identity management systems usually do not require modification of the systems to be managed, but may require installation of communications agents or configuration of adapters that facilitate data exchange with the security modules of the managed systems. Common platforms (including



operating systems, Web servers, directory servers, mainframe security systems, and major business applications) are usually supported by vendor-developed components. Custom applications generally require custom development of communications adapters, or extensive configuration of generic adapters.

Integrated deployment of both access control and identity management components will also decrease the effort associated with sequential development of user directories or other user data stores. Migration of data from existing stores, or establishing communications links to take advantage of existing directory information, is usually a significant element of the design and deployment effort for both types of technology. Coordinated development will provide the opportunity to create a more efficient and effective user directory strategy compared to development of each technology in isolation.

Cost

Software licensing, hardware, and implementation costs are roughly equivalent for the two different types of technologies that will be part of the Access Management System, so there is no direct budgetary advantage to the acquisition of one over the other. However, simultaneous acquisition of these two types of software tools may provide licensing advantages because of the larger volume purchasing arrangements that software vendors may provide, especially if selected vendors have either reciprocal licensing agreements, or if an integrated solution for both access control and identity management software components are selected from the same vendor. Coordinated development of access control and identity management may also lead to some reduction in costs because of more efficient use of resources for a joint development effort.

3.3.2 Deployment Planning

The recommended deployment approach is to coordinate the design, build, and roll out of both access control functions and an enterprise identity management system. This strategy will best meet FSA business objectives while creating a more efficient and effective integrated system for managing access to FSA systems and data.

Technologies to implement access control and identity management functions must be further investigated through an evaluation of the technologies available to implement these access management capabilities. Assuming suitable technologies and commercial products are identified, a pilot implementation that includes integration with an example FSA system should be conducted to better understand how these systems will integrate with the FSA technical environment. Based on the pilot implementation effort, a detailed strategy will need to be developed to sequence future deployment steps.

Deployment of the Access Management solution with a prototype implementation provides multiple benefits for planning future enterprise rollout of access control and identity management components.



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

Although simultaneous development of both access control and identity management components will require a larger implementation team, the work itself can be organized as modular units. Access control technology and identity management systems typically require separate server software, so there will initially be little interaction between the access control agents installed on Web applications and the connectors or adapters required for communication between the identity management server and the FSA systems to be managed. As noted above, an area where there will be interaction is the user data store or user directory, depending on the final design of the two types of Access Management Systems.

A sample, generic implementation strategy is shown in Figure 16. Note that efforts for technical infrastructure design and build can be combined, while the phases for design, build, and test of access control (WAC, for Web access control, in the diagram) and the identity management system (Provisioning Application, in the diagram) can be conducted in parallel.

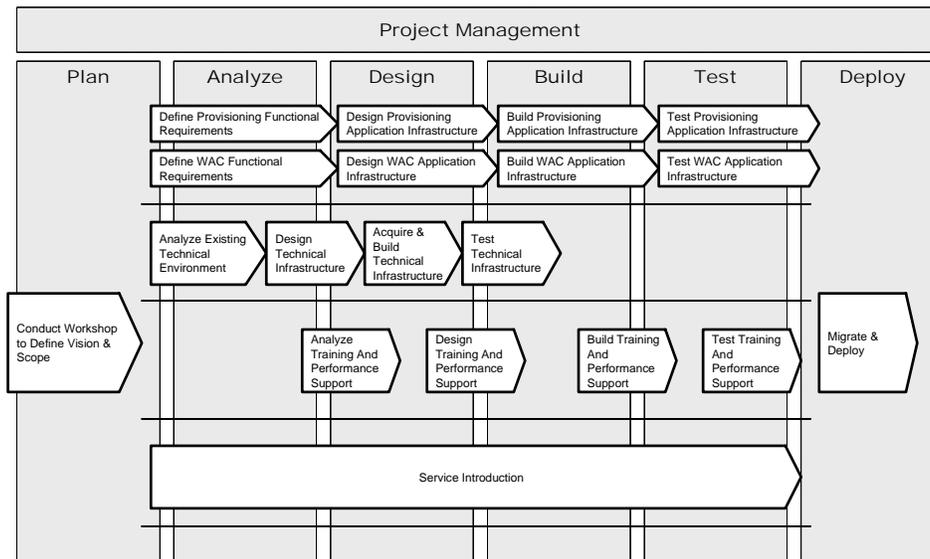


Figure 16 - Sample project plan for access control (WAC) and identity management (Provisioning) systems.



4 Access Management Business Integration

Implementation of an enterprise Access Management System will provide new capabilities to support greater efficiency in the management of Trading Partner access to FSA systems. This section presents integration scenarios to demonstrate how access management components will support existing FSA business processes, or provide opportunities to develop new and more effective business processes for management of Trading Partner access.

This section is not intended to describe comprehensive process designs for each of the business activities presented. Rather, these scenarios depict examples of how FSA business processes can take advantage of the new capabilities that would be provided by the Access Management System. These process descriptions also provide an aid for understanding the functional benefits and improvements that would result from deployment of the system. Future design and deployment planning steps for the Access Management System would need to develop more detailed processes for each of these activities.

The analysis of business process integration is divided into two major areas. The first addresses business processes related to managing access for Trading Partners, and the second focuses on processes for managing access for individual users. The example business processes discussed are:

For Trading Partners:

- Trading Partner Enrollment
- Trading Partner Changes
- Trading Partner Termination

For Trading Partner users:

- Add new user
- Support self-service processes
- Change of status
- User termination

This section concludes with a discussion of the how the Access Management System can support audit functions, and the organizational and policy implications for deployment of an Access Management System.



4.1 *Common Business Processes - Trading Partners*

The Access Management System will make it much easier to perform common business processes that are required by FSA to control access to its systems. High-level process flows for typical FSA activities related to Trading Partners are described in figure 17. The following sections describe how the Access Management System would support or facilitate FSA processes for the creation of a new Trading Partner, changes in Trading Partner status, and termination of a Trading Partner.



Common Business Processes - Trading Partners

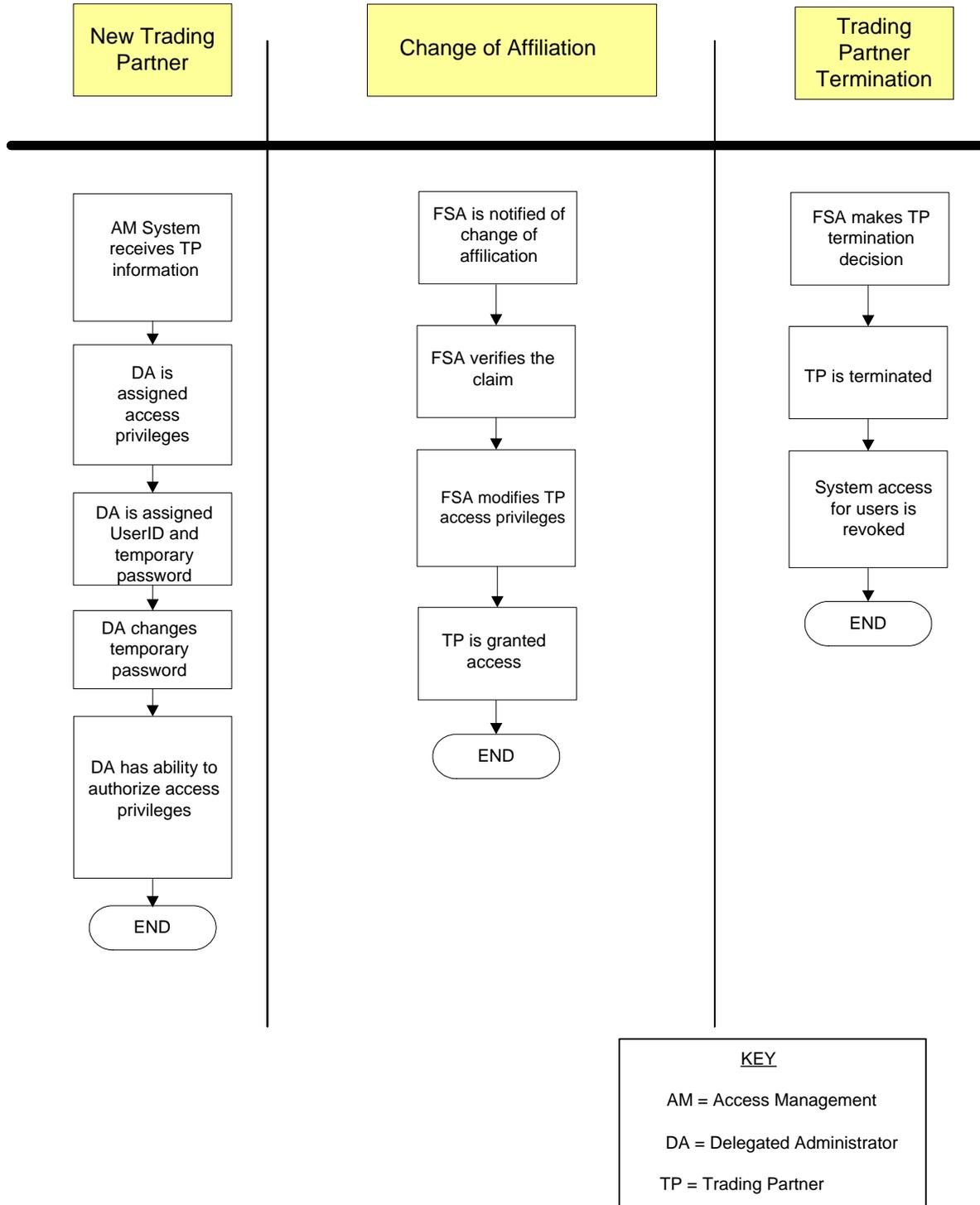


Figure 17 - Common Business Process Trading Partners



4.1.1 Trading Partner Enrollment

This process covers the steps necessary to sign up a new Trading Partner for access to FSA systems, including authorization and access configuration of a delegated administrator to manage the new Trading Partner’s users.

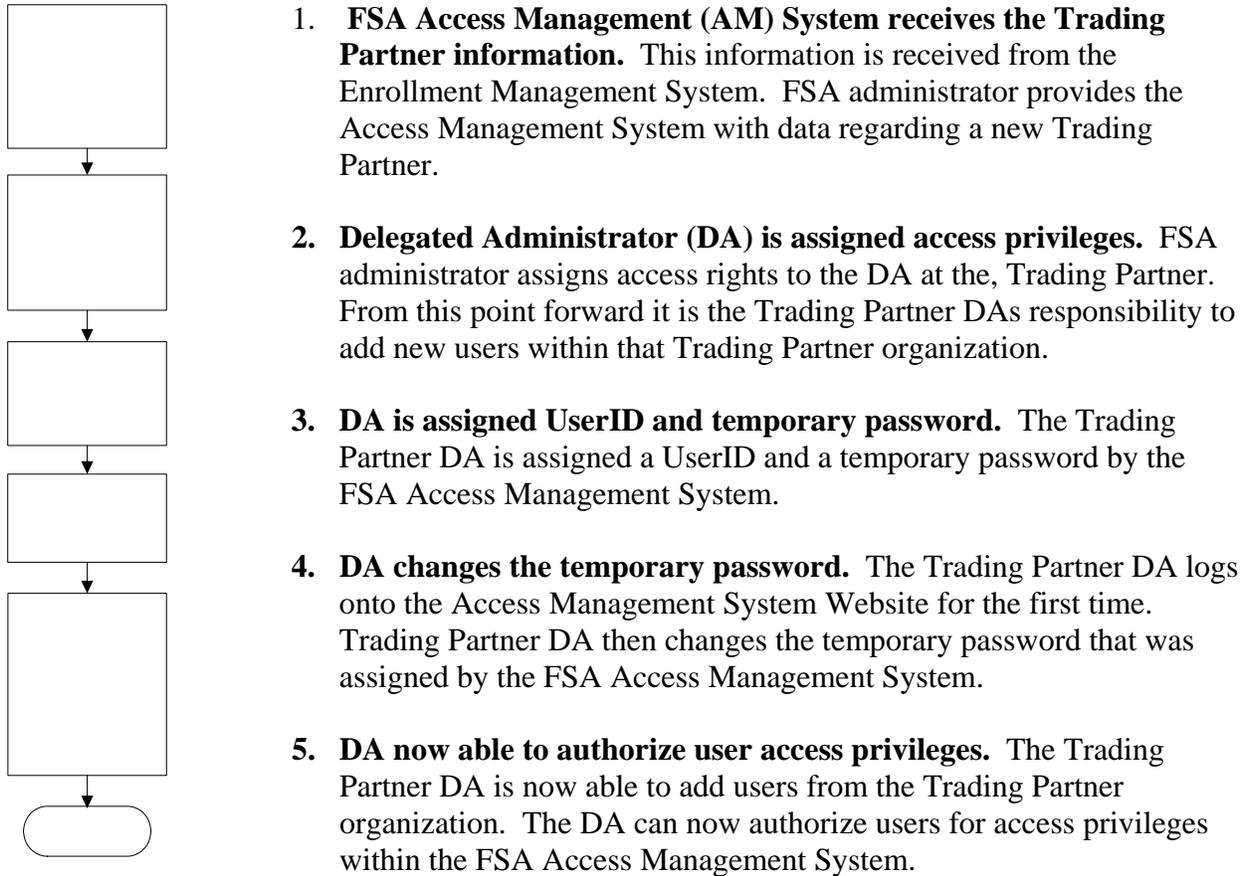


Figure 18 - New Trading Partner Enrollment

Delegated Administrator Access Rights

The Trading Partner DA has system privileges that allow the DA to add, delete and modify system access for users within the DA’s organization. The DA does not have access privileges to perform any other function on FSA systems. The FSA administrator can monitor, review, and overwrite any of the functions that were performed by the DA, if required.

Benefits

AM System receives TP information



The Access Management System allows for a streamlined process for setting up new Trading Partners on FSA systems. Since the FSA administrator only has to assign access privileges to the DA, it reduces FSA workload.

4.1.2 Trading Partner Changes

The process example below describes typical steps for a Trading Partner change of affiliation.

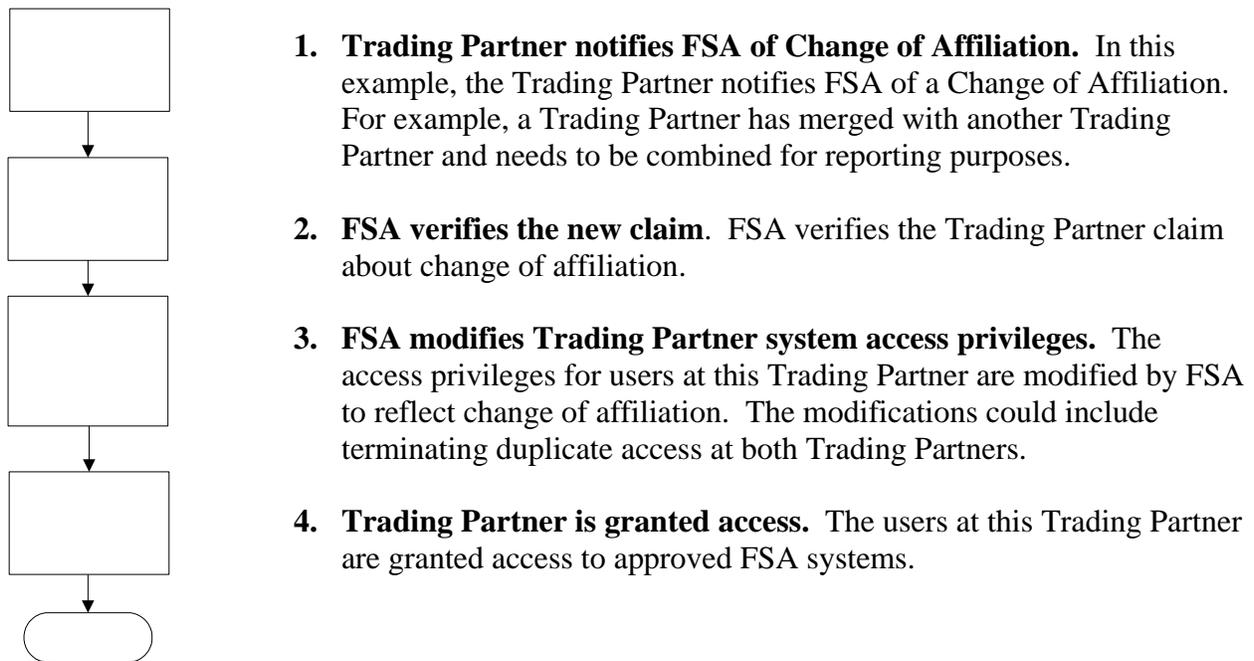


Figure 19 - Change of Affiliation

Access Management Issues with Trading Partner Changes

FSA will need to examine its policy and business rules that apply to a Trading Partner after a change of affiliation has happened. Issues of how the system access privileges for affected users are handled after the change of affiliation has occurred need to be examined.

Benefits

A significant advantage of enterprise Access Management is the ability to have an enterprise view of users. With a change of affiliation, the access privileges of users at both impacted Trading Partners will likely need to change to reflect this new information. Identity management solutions provide a mechanism to accurately determine and modify access privileges.

FSA is notified of
change of
affiliation



4.1.3 Trading Partner Termination

The process below describes typical steps required to terminate Trading Partner access to all FSA systems.

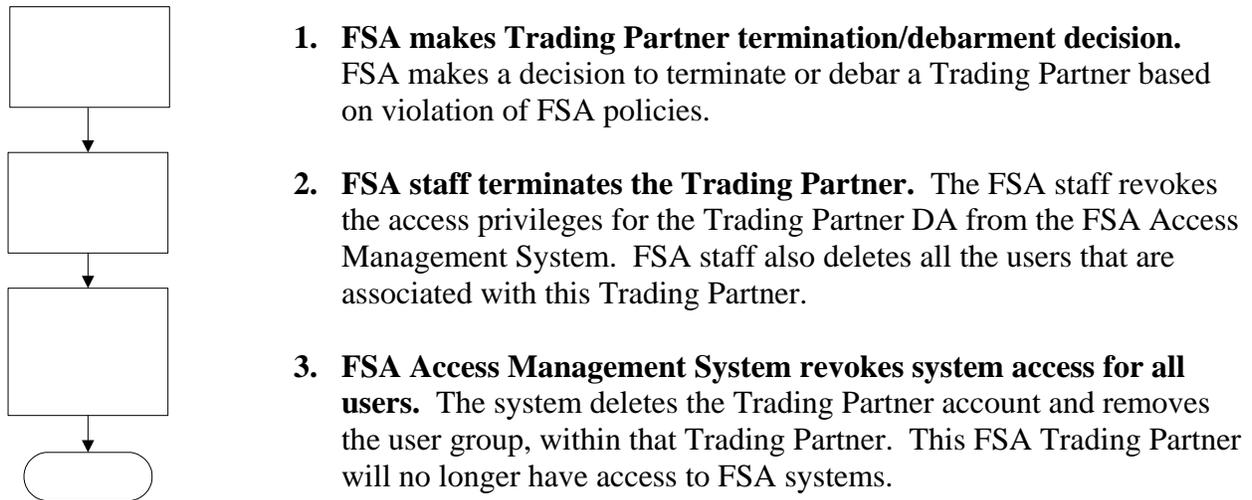


Figure 20 - TP Termination

Benefits

The Access Management System makes the Trading Partner termination/debarment process easier and more efficient. Access management allows for removal of users by revoking access privileges of user groups across all FSA managed systems, instead of canceling individual user access within each system. This means an FSA administrator would be able to remove all users associated with a Trading Partner by relating all users for each Trading Partner with an administrative group linked to that Trading Partner.

FSA makes TP
termination
decision



4.2 Common Business Processes- Trading Partner Users

The Access Management System provides administrative and support functions for many common business processes associated with controlling access for individual users. Several typical process flows for users are shown in figure 21. The following sections explain how the Access Management System will be able to support new user creation, user self service functions, changes in user status, and termination of users.



Common Business Processes - Trading Partner Users



Figure 21 - Common Business Process Trading Partner Users



4.2.1 New User

In this process it is assumed that the Trading Partner has already been approved and a delegated administrator has been assigned for this organization.

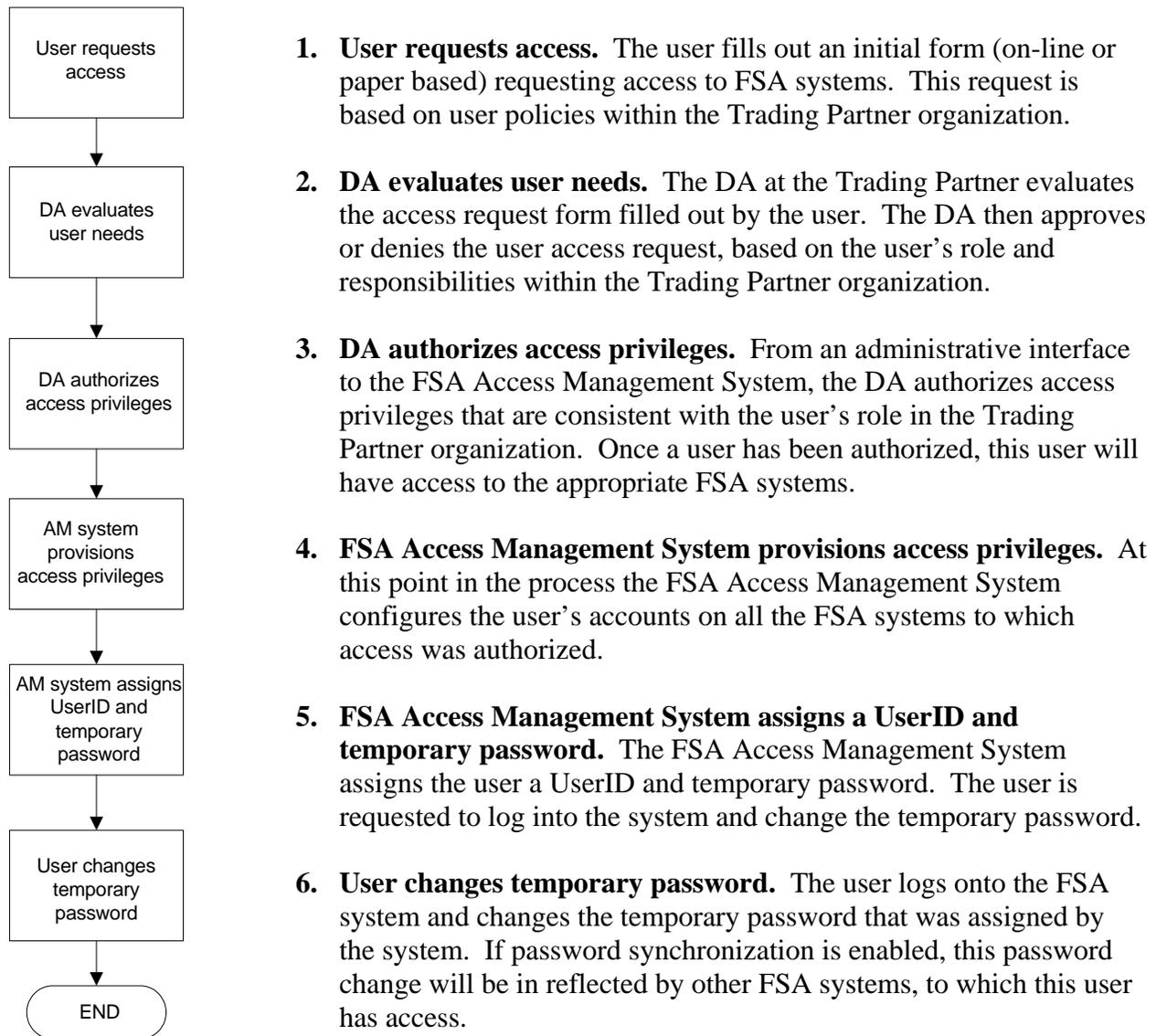


Figure 22 - New User Enrollment

Benefits

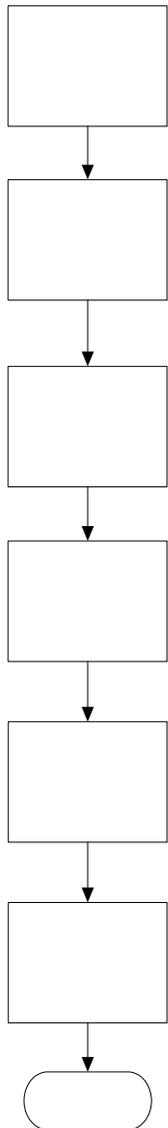
The new user creation process in the Access Management System allows the DA to provide access only to the required users within the Trading Partner organization. Since the DA is much more aware of the Trading Partner organizational structure and its needs, the DA is able to make better decisions in assigning system access rights to users.



4.2.2 Self-Service

The process of self-service provides user's the ability to perform functions related to their access on managed systems independent of system administrators.

Password Reset



1. **User goes to the FSA Access Management Website.** The first step a user has to take to reset her password is to log on the main Access Management Website. Then the user navigates from the Access Management main page to the password reset page.
2. **User selects "Password Reset" and enters UserID.** The user selects "Password Reset" and enters her UserID which is associated with the FSA Access Management System. This ID is used by the system to determine the authentication questions for this user.
3. **User answers authentication questions.** The FSA Access Management System asks the user to answer a set of authentication questions. These questions are designed in such a way that only the true owner of this UserID should be able to answer them correctly.
4. **FSA Access Management System confirms user's identity.** At this point, the FSA Access Management System verifies the answers to authentication questions and validates the user. If the authentication process fails, FSA Access Management System requests the user to contact the FSA helpdesk/ FSA system administrator.
5. **System assigns user a temporary password.** At this point in the password reset process the FSA Access Management System assigns user a temporary password. This is a one time password, and system requests the users to change it on their first login.
6. **User changes temporary password.** The user logs into the FSA system and changes the temporary password. After the user has changed password and confirmed it, the FSA Access Management System grants system access to the user.

User logs to AM system web site

Figure 23 - Password Reset

Benefits

This process makes it much more convenient for users to reset a password. Since the user does not have to call the FSA helpdesk, it reduces the workload at FSA. The users are not bound by the FSA helpdesk hours and can reset the password anytime.



Password Renewal

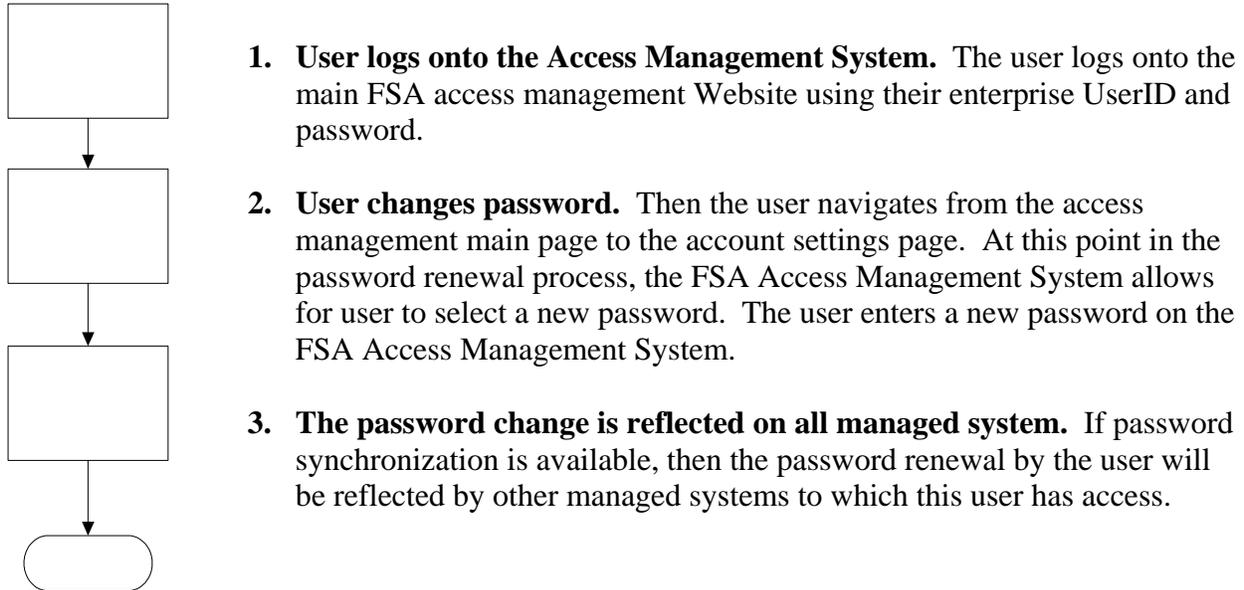


Figure 24 - Password Renewal

Benefits

The password renewal process allows FSA to enforce its security policies. Since the renewal process is completed by the user, it removes any workload burden on FSA.

User logs to AM
system

User changes
password



4.2.3 Change of Status

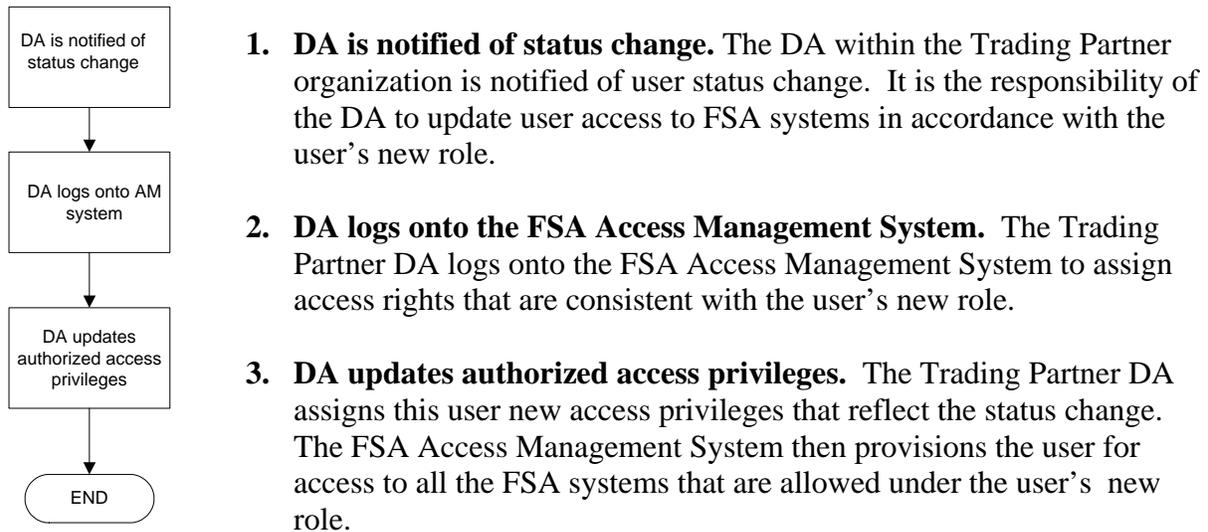


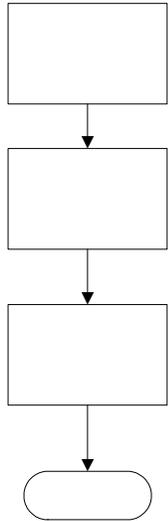
Figure 25 - Change of Status

Benefits

The Access Management System allows for the Trading Partner DA to update user access privileges. The change of status process is being performed by the DA. This reduces FSA's workload and allows for a quick change to user access privileges.



4.2.4 User Termination/User Leaves Trading Partner



- 1. DA is notified of termination.** The Trading Partner DA is notified that the user has either left the organization or the user employment has been terminated. This notification can occur by a formal process (e-mail, memo) or in an informal manner.
- 2. DA deletes user access privileges.** The Trading Partner DA logs on the FSA Access Management System to delete the users who have left the Trading Partner organization. The DA removes access privileges for the user within the FSA Access Management System.
- 3. Access is removed from all managed systems.** After the Trading Partner DA deletes the user from FSA Access Management System, the user no longer has access privileges to the impacted FSA systems.

Figure 26 - User Termination

Benefits

This user termination process allows for a quick removal of access privileges for users who are no longer with the Trading Partner. If the same process was performed by the FSA administrator, there would be a time gap before the information about the user termination filters down to FSA. By allowing Trading Partner DA to revoke user access, the security issue of unauthorized access by this particular user is quickly resolved.

DA is notified of termination

4.3 User Audit Functions

The user audit process has two primary components, user access auditing and user activity auditing. User access auditing monitors user access privileges across multiple systems and tracks changes in user access privilege assignments. User activity auditing allows for tracking of user activities, such as requesting access, logging into FSA systems or applications, gaining access, viewing data, or executing system or application functions (e.g., modifying data or conducting transaction). These audit processes are depicted at a high level in Figure 27. Note that this process involves feedback between the various components described in the diagram. For example, the content and format of audit reports can be refined over time to improve the effectiveness and quality of the audit process.

DA deletes access privileges

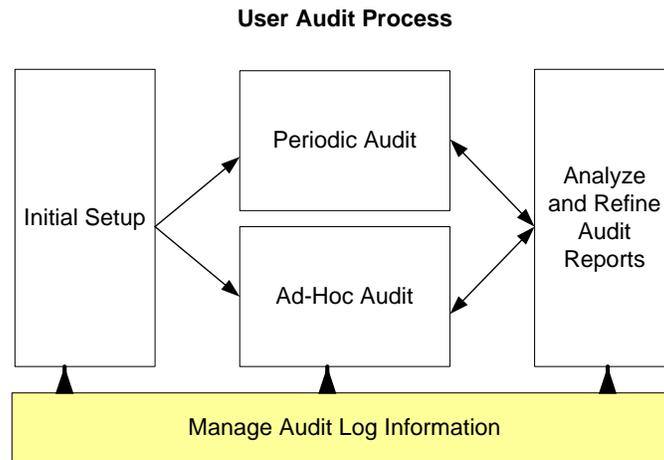


Figure 27 - User Audit Process

The major components of the audit process supported by the Access Management System are described below.

Initial Setup

Initial setup configures the audit criteria that will be used to collect audit information. The FSA administrator selects the user activities or administrative actions that will be tracked. The criteria can be modified based on analysis of the audit reports or changes in auditing requirements due to regulatory or compliance demands.

Periodic Audit

In the initial setup stage, the system administrator selects a time interval for a periodic audit. These periodic audits provide the administrator the ability to analyze any changes in user activity patterns over time.

Ad-Hoc Audit

Ad hoc audit reports can be generated in response to specific requests or to investigate special circumstances as required. The audit interface will provide viewing and reporting capabilities that allow creation and formatting of audit reports for special purposes.

Analyze and Refine Audit Reports

The system administrator analyzes the periodic and audit reports to address specific requirements, demonstrate regulatory compliance, or provide input for investigations of suspected problems. System administrators can also make changes to tailor audit views and reports for to improve the quality and effectiveness of the audit.

Manage Audit Log Information

Audit information must be carefully managed during all audit stages. Audit information must be stored, protected from corruption, and periodically moved to archival storage. The Access



Management System will also manage access rights for viewing audit information and configuring the audit functions so that only authorized users can gain access.

This process also involves the issue of access rights to this data. Only certain employees within an organization (e.g., FSA System Security Officer) are given rights to view and analyze this information.

Benefits

The Access Management System allows FSA to monitor access privileges and user actions that are inconsistent with FSA security policy. The Access Management System will allow FSA to quickly and efficiently generate audit reports across all FSA systems. In situations involving user termination, audit trails that record user activity can provide FSA with evidence of policy violations that can be communicated to the FSA Trading Partners to justify remedial actions.

4.4 Organizational & Policy Implications

4.4.1 Major Functions

Security policies and procedures are only effective when supported with the proper security organizational structure. At FSA, the CIO security organization is primarily responsible for facilitating the proper use of FSA systems while protecting FSA systems from unauthorized use. The access management processes discussed in this deliverable will progress FSA into a more secure environment but cannot do so without the necessary security organization infrastructure. The access management effort cannot be completely successful without taking into account organizational implications in the following areas:

- **Oversight of Access Management Operations** – Currently, System Security Officers are assigned to and managed by the organization responsible for each FSA system. System Security Officers report to individual system owners. In order to leverage the benefits of an enterprise Access Management solution, the organization of System Security Officers will need to be evaluated during deployment planning for the Access Management System. For example, the enterprise management functions of the Access Management System would allow an enterprise-level System Security Officer to effectively manage user administration tasks for multiple systems. Enterprise-level System Security Officers would also facilitate consistent enforcement of FSA Security and Privacy Policy, an important benefit of access management.
- **Classification of Access Management Tools** – In addition to impacts on Trading Partner Management, the Access Management Tools that would be in place could form the basis for security services across FSA. FSA must make a decision as to whether access management is considered a support application or separate major application in its enterprise. A support application is available to provide shared services to numerous other applications. A major application is a distinct application that stands separate from the other applications.



- **Access Management System Support** – Parties need to be identified that will be responsible for administering, provisioning, updating, maintaining, and trouble-shooting the Identify Management and Access Control tools implemented as a part of an Access Management solution. While the majority of security administration tasks are greatly simplified by access management tools, some manual user intervention could be required for error cases, etc.
- **End User Customer Service** – In the event that a user has an access management related issue, such as an inability to access a system, the user must be given a clear point of contact to assist in resolving their issue. A trained and supportive customer service staff will make a significant positive impression on FSA system users.
- **Decision Making Authority** – It is necessary to establish decision making authority between system security and enterprise security efforts. For example, in the event of a security breach, system business owners and enterprise security officers must follow defined processes and have a clear understanding of how to work together.
- **Standards and Policy Changes** – With enterprise security tools, policy and standards discussions will need to occur to resolve any differences between systems. Policies include background checks relative to specific levels of access. Standards include items such as password lengths. FSA standards and policies will need to be explicitly resolved to organize enterprise tools.

4.4.2 General Security Implications

In addition to the organizational and policy implications noted in Section 4.4, several more general security items will need to be taken into account. The Access Management solution must address the following general security implications:

- **Consistency with FSA Security and Privacy Policy** – The Access Control and Identity Management tools which make up FSA’s Enterprise access management must take into account and remain consistent with FSA Security and Privacy Policy.
- **Security Infrastructure Controls** – All Access Control and Identity Management components will need to be protected resources because they contain very sensitive information. FSA will need to implement security infrastructure controls in accordance with FSA Security and Privacy Policy to protect these resources. For example, all servers used to run software components of the Access Management System must be configured for secure operation according to appropriate security hardening guidelines.
- **Deployment Plan** – A comprehensive Enterprise Security Tools deployment plan must include the development of system security plan and must follow the Software Lifecycle (SLC) for system security, including appropriate security review and testing steps.
- **Deployment of Enterprise Security Tools** – Due to the sensitive information such as user information and passwords stored within the security databases, enterprise security tools will need to be housed in a secure environment. The FSA Virtual Data Center (VDC) is a logical choice due to proximity to other applications and network security precautions already in place. Access Management System components will need appropriate protection from network security threats. This may require housing the



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

components on servers in isolated network segments protected by appropriately configured firewalls, monitoring with network-based and host-based intrusion detection systems, and use of host and network vulnerability scanners to test system components.



5 External Interoperability: Sharing Identity and Authentication Credentials

A business objective identified for Access Management in the first phase of this project described requirements for flexibility (Business Objective A2.4; refer to Access Management Business Objectives and High-Level Requirements – Deliverable 123.1.27 for details). One of the issues that the Access Management solution must address is how FSA will be able to interact with Trading Partners and other external organizations to facilitate authorized access to FSA systems and data. Sharing identity credentials would allow users to seamlessly navigate across different systems within an organization and across systems of other partner organizations. FSA has already encountered the concept of sharing identity and authentication credential within both the federal government (e.g. the EGov e-Authentication initiative; described in Section 5.4) and the commercial sector (e.g. services proposed by Meteor; described in Section 5.3). This section describes major issues related to approaches for sharing identity information and user credentials, and provides an overview of their relevance for FSA and the Access Management High-Level Design.

5.1 Background

Management of authentication credentials for users has traditionally been based within individual systems. This creates ‘identity islands’ that isolate users’ identity information, limiting its usefulness and increasing the effort required to register and maintain credentials across an organization. This approach to managing identity information is currently the general practice at FSA. A more sophisticated approach rapidly gaining acceptance in the business community is to deploy enterprise identity management systems that link identity information across different systems within an organization. Identity management systems usually deploy credential databases, mapping databases, or meta-directories to share and manage identity information across multiple directories or user repositories. Another credential-sharing method is to manage identity information for business partners. In this approach, a single identity store manages identity information for a group of related business partners. Utilizing this approach, FSA would maintain the credential store for all Trading Partners. The Microsoft Passport solution for sharing identity, which is utilized by Hotmail, is similar to this method.

There is a relatively approach to credential sharing, termed ‘Federated Identity’, that has the potential to improve FSA interactions with Trading Partners. In the Federated Identity approach, credential information is distributed among many organizations that agree on methods to exchange and trust authentication credentials among themselves. Figure 4.4.1 describes a sample Federated Identity approach involving FSA and three different Trading Partners (TP). The sharing of authentication credentials in this manner requires mutual trust and confidence between the business partners. Each business partner will need to establish acceptable privacy and security standards, so that other partners can trust the credential information.

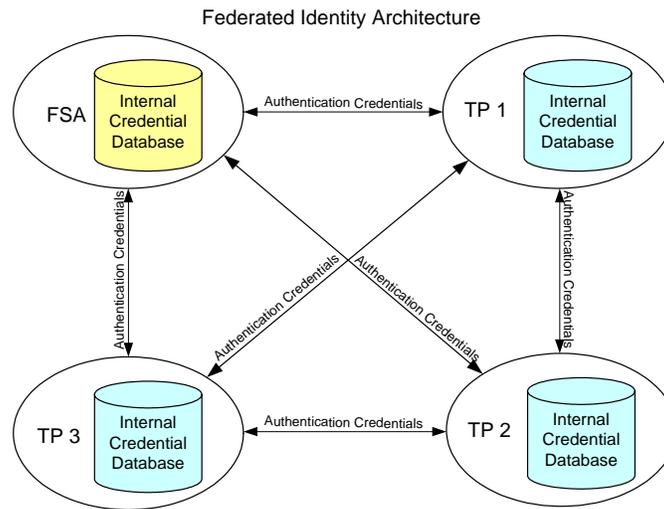


Figure 28 - Sample Federated Identity Architecture

5.2 Benefits of Federated Identity

Key benefits of Federated Identity include the ability to deploy cross-site Single Sign-on functions and increased ease of use for Trading Partners that need access to multiple Web applications. Federated Identity also provides for transitive trust. This means, for example, that a user may log in to a site operated by Trading Partner 1, access services from Trading Partner 2 through a link on the site of Trading Partner 1, then link on the second site to FSA services, all without authenticating again. This requires that the authentication credentials established during the initial login at Trading Partner 1 be passed on to Trading Partner 2, then to FSA. This capability allows for borrowers and FSA Trading Partners to easily navigate across systems that are operated by different organizations.

5.3 Major Federated Identity Standards

There are several major business and technical issues that present challenges to the implementation of Federated Identity solutions. Technical issues include establishing the format and protocols for communication of credentials and other security information between organizations. The major business issues include how to establish trust policy structures that can be appropriately monitored, how to deal with liability issues and resolution of problems, and how to create common risk definitions and risk management procedures. Standards are being developed to address these issues and this section summarizes those efforts.

5.3.1 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, distributed way. Liberty Alliance has issued specifications to make identities portable across autonomous domains. The Liberty Alliance standards use the Security Assertion



Markup Language (SAML) for exchanging credential information online. More details on Liberty Alliance and SAML are provided in Appendix D – Current EGov and e-Authentication Efforts.

5.3.2 WS-Federation

The WS-Federation has a broader focus on Web services standards. Its charter is to promote Web services interoperability across platforms, operating systems, and programming languages. The standards are in an early stage of development by Microsoft, IBM, Verisign and RSA, the primary organizations supporting WS. These standards also utilize SAML for credential exchange.

5.3.3 Other Federated Identity Efforts

There are a variety of other proprietary and open approaches to federated identity. PingID is a commercial product based on the Liberty Alliance standards. Shibboleth also provides Federated Identity standards but only for Internet2, the research network used primarily by universities. 3-D Secure is a proprietary product developed by Visa as a key component of the Visa authenticated payment program. Meteor, which supplies services for FSA Trading Partners, also has a proprietary method for Web-based Single Sign-on (SSO) and for sharing authentication credentials.

5.4 *Integration with Federal Security Architecture Efforts*

While not yet mature, several efforts are under way to create a federal security architecture. One of the most prominent efforts is the eGov initiative which has been developing an eAuthentication capability. This section summarizes the status of the current eGov eAuthentication effort, and its impact on FSA. More details about the original design and development of eAuthentication capabilities are provided in Appendix D – Current eGov and eAuthentication Efforts.

5.4.1 e-Authentication

The E-Government (eGov) initiative started in November 2001, when the Bush administration outlined an E-Government strategy to significantly improve the government's quality of service for citizens, businesses, government and internal operations. Since many of these initiatives involve transmission of sensitive and private information, trust is critical for the success of this initiative. The e-Authentication initiative was launched to streamline the delivery of authentication services for the E-Government. e-Authentication also involves the creation of a policy structure for sharing credentials.

5.4.2 Progress and Current Status



The General Services Administration (GSA) is managing the e-Authentication initiative. The goal of the GSA is to establish a gateway to provide common government wide authentication services. The GSA had a pilot gateway in operation that was providing limited authentication services to some government agencies. The details on the workings of the gateway and possible integration solution for FSA identity and Access Management solution are provided in Appendix D – Current eGov and eAuthentication Efforts.

The General Accounting Office recently published a report on the challenges faced by the current eAuthentication approach². The report outlines major issues for a centralized authentication service managed at the federal level, and recommends new approaches to sharing authentication services. Recently, the General Services Administration also issued a memorandum summarizing the results of the e-Authentication Technical Advisory Board, in which a Federated Identity approach is proposed. As a result of these analyses, OMB recently directed GSA to halt development of the physical e-Authentication Gateway, and the value of the services provided by the e-Authentication gateway in its current form is under review. Since the current pilot gateway is based on a centralized authentication approach, the scalability of this architecture is in question.

5.4.3 Future E-Government Directions

The e-Authentication initiative is continuing work on developing an authentication architecture for the federal government. Authentication architecture guidelines will be published by GSA in December 2003. The architecture description is expected to include standards for sharing credentials and defining authentication levels. The e-Authentication initiative will also propose a method to identify authentication levels for government agency applications.

The future direction of the e-Government initiative is to move towards a Federated Identity approach based on commercial standards. The major evolving security architectures (including Liberty Alliance and WS- Federation) are based on a federated approach. The new approach for E-Government is also expected to include methods that incorporate authorization services (for communicating access privilege information) in addition to authentication.

5.5 Recommendations

FSA should continue to monitor development of standards for shared identity credentials and Federated Identity. While current FSA security and privacy policies do not address issues related to credential sharing, future policies will need to be developed to address advances in this area. An effort to analyze the impact on FSA of identity credential sharing in general and Federated Identity efforts should be conducted to fully understand these implications. This effort should develop strategies for credential sharing at FSA to utilize the Federated Identity approach.

² *Planned e-Authentication Gateway Faces Formidable Development Challenges*, Report to the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House of Representatives, U.S. General Accounting Office, GAO-03-952, September 2003.



FSA should design the Access Management System to provide support for development of credential sharing strategies that are consistent with the federal authentication architecture and industry standards for Federated Identity.

The e-Authentication initiative has established an Electronic Authentication Council. The objective of this council is to develop standards for assurance levels. The council includes members from both industry and government. Stephen Timchak, GSA Program Director for e-Authentication, has suggested that FSA should participate on the authentication council. Our recommendation is that FSA should join the electronic authentication council to provide input to that standards development process that reflect FSA requirements. FSA should also look for opportunities to become involved in credential-sharing pilot projects.

FSA should participate in the Federal Electronic Authentication Council and look for opportunities to pilot credential sharing approaches.

FSA will need to coordinate Federated Identity efforts with work being conducted to understand and implement Web services standards. The Data Strategy initiative for Technical Strategies is developing Web Services recommendations that will need to be accounted for as policies and plans are developed for Federated Identity and related security issues. Because credential sharing standards are still in flux, FSA needs to monitor development of these standards and look for opportunities to influence them. Such opportunities include participating in government-wide eAuthentication forums (including the Electronic Authentication Council) or participating in groups that are shaping the standards for Federated Identity.



6 Next Steps

FSA's diverse user population and varying platforms and security structures create challenges for Trading Partners and FSA. The absence of an enterprise view of enrollment and access management makes it difficult for FSA to properly monitor and review access to its systems while frustrating end users with multiple UserIDs and passwords. The enrollment and access management vision described in the high-level design advances the concept of a consolidated view of Enrollment and Trading Partner access management. It will provide capabilities to manage access at the enterprise level to insulate Trading Partners from the underlying complexity of FSA's systems. Consistent user identity and privilege information will improve security effectiveness and increase administrative efficiency. Enterprise access management will make it easier to perform common business processes such as configuring access for a new Trading Partner or changing a user's status.

The enrollment and access management initiatives are an integral part of the overall Trading Partner Management (TPM) effort to simplify Trading Partner interaction with FSA. Enrollment as a part of TPM would simplify and consolidate the data collection process and approval process in order to streamline the entire Trading Partner Enrollment process. After a Trading Partner is successfully enrolled in FSA Systems, the access management portion of TPM will provision and manage authentication, authorization, and audit functions for subsequent Trading Partner participants. The combination of this simplified enrollment process coupled with an enterprise Access Management Solution will greatly improve the Trading Partner's experience with FSA and provide additional security for FSA systems.

In parallel with the TO 147 TPM Gap Analysis effort, the next step in the Access Management effort will be work awarded under TO 143, Identity and Access Management Tools Analysis. The goal of this task order is to work with FSA business and technical representatives to evaluate commercial products and analyze how they can be used to meet FSA business objectives. This effort will provide technology recommendations to help FSA select Identity and Access Management technologies that satisfy FSA needs for security services across FSA user groups and environments. This effort will also include the development of a prototype of the selected Identity and Access Management tools, and integration with a role-based FSA Web application in a development environment.



Appendix A: Business Objectives Prioritization

In the first phase of this effort, the Enrollment and Access Management Business Objectives and High-Level Requirements were documented without trying to determine relative priorities. To assist in evaluating solution options and recommending an approach, the Business Objectives were prioritized according to the following criteria:

- **Benefits to FSA:** The business objectives being considered should provide benefits to FSA in terms of reduced time and resources.
- **Minimal Impact to FSA:** The business objectives that will be implemented should have minimal impact on the current operation of FSA.
- **Benefits to Trading Partners:** These business objectives should provide benefits to FSA's Trading Partners by making it easier for them to conduct business FSA.
- **Minimal Impact to Trading Partners:** The business objectives being considered should have minimal impact on Trading Partners and should not disrupt their normal business functions with FSA.
- **Applicability to Enrollment and Access Management:** These business objectives should be applicable to Enrollment and Access Management at FSA.
- **Alignment with FSA BIG Strategic Objective:** These business objectives should also align with the FSA Business Integration Group (BIG) strategic objectives. The BIG objectives define five major goals that FSA wants to achieve. This category measures how closely the business objective matches with the FSA Strategic Vision.
- **Overall:** The overall priority of the Enrollment and Access Management Business Objective based on the average of the other qualitative criteria.



Summary of Results:

#	Description	Benefits to FSA	Minimal Impacts to FSA	Benefits to TP	Minimal Impacts to TP	Applicability to EAM	Alignment w FSA BIG Strategic Obj	Freq. Of Mention	Overall
A2.1	Manage enrollment and access privileges at the enterprise level.	M	H	H	H	H	H	M	H
A1.1	Focus on registration processes and access decisions at the enterprise level instead of on a per system basis.	H	L	H	H	H	H	H	H
A3.1	Streamline enrollment and Access Management for Trading Partner services.	M	M	H	H	M	M	M	H
B2.1	Provide effective oversight of user access to FSA systems.	H	L	M	M	M	M	H	H



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

#	Description	Benefits to FSA	Minimal Impacts to FSA	Benefits to TP	Minimal Impacts to TP	Applicability to EAM	Alignment w FSA BIG Strategic Obj	Freq. Of Mention	Overall
A2.4	The enrollment and access solution should be flexible enough to support the requirements of current and future FSA systems.	H	L	L	H	M	H	H	H
C2.2	Maintain security of FSA systems.	L	L	H	M	L	L	L	H
C3.2	Adopt Enrollment and Access Management policies that improve business processes.	M	L	H	H	H	H	M	H
A2.2	Improve self-service capabilities.	M	M	M	H	M	L	M	M
B3.1	Meet FSA regulatory compliance requirements.	H	L	L	H	H	H	H	M
C2.3	Provide users with access to FSA systems appropriate for their job function.	H	M	L	H	M	H	H	M



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

#	Description	Benefits to FSA	Minimal Impacts to FSA	Benefits to TP	Minimal Impacts to TP	Applicability to EAM	Alignment w FSA BIG Strategic Obj	Freq. Of Mention	Overall
A2.3	Balance easier access and system security.	H	L	L	H	L	M	H	M
C3.1	Provide effective training and customer support across FSA systems.	M	L	L	H	L	M	M	M
B1.1	Adopt a uniform decision making process for evaluating users requesting access to FSA systems.	M	M	L	H	M	H	M	M
C1.1	Facilitate access to sets of data at the enterprise level.	M	L	H	H	M	M	M	M
C2.1	Create enterprise policy and standards for enrollment and access management.	M	L	H	H	L	M	M	M



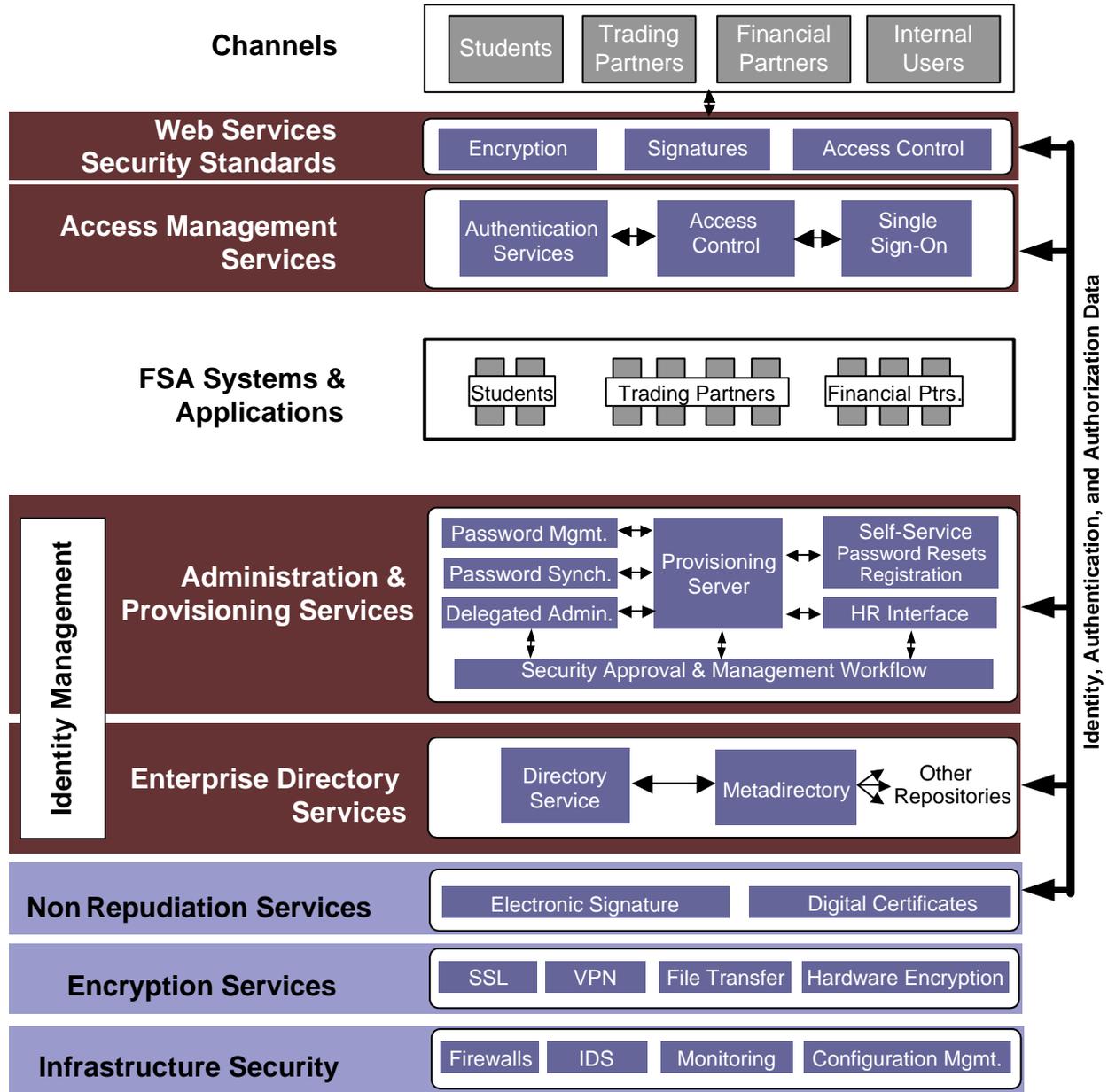
**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

#	Description	Benefits to FSA	Minimal Impacts to FSA	Benefits to TP	Minimal Impacts to TP	Applicability to EAM	Alignment w FSA BIG Strategic Obj	Freq. Of Mention	Overall
A2.5	Allow users to customize their experience with FSA systems.	H	M	H	H	L	M	H	L



Appendix B: Proposed FSA Security and Privacy Technical Architecture

FSA Security and Privacy Technical Architecture Vision



U.S. Department of Education - Office of Federal Student Aid

Version 7-31-2003

Figure 29 - Proposed FSA Security and Privacy Technical Architecture



Appendix C: Business Objective Mapping

The first phase of the enrollment and access management effort identified 16 major business objectives and 70 associated high-level requirements. The tables below explain how the enrollment and access management high-level solutions address each business objectives and requirement. Business objective and high-level requirement are numbered to be consistent with the Enrollment Business Objectives and High Level Requirements (Deliverable 123.1.26) and Access Management Business Objectives and High Level Requirements (Deliverable 123.1.27) deliverables.

Business Objective A1.1 – “Enterprise process focus”

Scope:	Enrollment and Access Management	
Identifier/Title:	A1.1 - Focus on registration processes and access decisions at the enterprise level instead of on a per system basis.	
Description:	The intent of this objective is to provide an enterprise view of the registration and Access Management processes, instead of having different processes for different systems. Consolidation of the decision-making processes for registration and user access will help provide a more consistent application of FSA policies, streamline the registration and access processes for Trading Partners, and improve the ability of Trading Partners to quickly gain access to the FSA services they need.	
High-Level Requirements:	A1.1.1	<p>Support making access decisions at the enterprise level instead of by system.</p> <p>Solution functions that will provide decision support at the enterprise level for enrollment and access management include:</p> <ul style="list-style-type: none"> • Consolidated enrollment data: enrollment data maintained in TPM will provide a single repository for queries about Trading Partner enrollment status and history. • Access reporting functions: reporting capabilities in the identity management system will provide a cross-system view of assigned user access privileges and history of user Access Management changes. • User activity audit logging: audit trails maintained for Web applications by the Web access control system will support tactical and strategic decisions about Web application performance, functionality, and development planning.
	A1.1.2	Take into account unique requirements of foreign schools



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

	<p>when making decisions about registration and access.</p> <p>Information unique to foreign schools will be captured in the Enrollment and Access Management System through use of custom-defined attributes created in the Enrollment database and the identity management system.</p>
A1.1.3	<p>Facilitate decision making with an effective registration and access approval workflow process.</p> <p>Efficient decision-making will be supported by a workflow system. In the long term, this function will be provided by an enterprise workflow capability. Identity management systems also provide workflow functions that could be used in the short term to deploy a security approval workflow process to manage security access requests, approval steps by authorized approvers, and communication of approval decision results.</p>



Business Objective A2.1 – “Manage across systems”

Scope:	Enrollment and Access Management	
Identifier/Title:	A2.1 - Manage enrollment and access privileges at the enterprise level.	
Description:	Management of enrollment and access privileges includes administrative and reporting tasks associated with registration of Trading Partners and granting access to FSA systems. Currently, most administrative processes take place on a system-by-system basis. Enterprise management of these processes will improve their efficiency and consistency.	
High-Level Requirements:	A2.1.01	<p>Administer access privileges at the enterprise level.</p> <p>Enterprise administration of access privileges will be provided by the automated and centralized account provisioning and management functions of the identity management system. The identity management system will also provide an administrative interface that provides display functions for viewing access privileges for a user or group of users across multiple systems.</p>
	A2.1.02	<p>Enable integration across business processes to support use of a single UserID and password.</p> <p>Consolidation of UserID and password requirements across FSA systems will be supported through several features. For Web applications, the single sign-on function of the Web access control system will decrease the number of passwords or other authentication credential that must be managed by individual users. The identity management system can provide password synchronization mechanisms to automatically reset passwords for a user across multiple FSA systems simultaneously.</p>
	A2.1.03	<p>Ensure that each UserID is associated with a single user or entity.</p> <p>The Identity Management system will provide centralized user account management functions for effective user account creation, modification, and termination. User management functions will include display capabilities to create a view of user access across all FSA systems. Audit logging functions in both the identity management system and the access control system will provide information about when a user logs on to each system, and will be able to detect (and limit, if desired) multiple concurrent logins.</p>



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

A2.1.04	<p>Support single sign-on functions.</p> <p>“Single Sign-on” (SSO) functions will be provided by the Access Control system to enable simplified login procedures for Web applications. Sets of Web applications can be configured to allow use of any application in the set after a user logs in to any of the applications. The Identity Management system will provide functions to assign users to roles that can be associated with groups of applications appropriate for a specific level of user access privileges. The Identity Management system can also provide password synchronization capabilities to simplify use of systems other than Web applications by automatically detecting password resets and propagating them to other systems.</p>
A2.1.05	<p>Support multiple user sessions.</p> <p>The Access Control system will implement session management functions to regulate the number of allowable concurrent sessions for each user.</p>
A2.1.06	<p>Provide methods to enable and disable user access at specified begin and end dates.</p> <p>The user account provisioning function of the Identity Management system will be able to automatically configure account access to begin and end on specified dates. This function can decrease delays associated with initial account setup, and can efficiently remove all access privileges for a use when no longer needed.</p>
A2.1.07	<p>Provide cost effective tools for managing registration and access.</p> <p>Technology and product evaluations will consider costs and benefits to help FSA understand the business case justification for deployment of identity management and access control solution components.</p>
A2.1.08	<p>Provide, where possible, automated tools for enrollment and access management.</p> <p>The Identity Management system will provide automated capabilities for user account management. Examples of automated functions that will be provided include automated provisioning of user accounts on multiple systems, integration with security approval workflow processes, automated termination of accounts based on pre-</p>



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

	<p>defined dates, and automated password resets and synchronization.</p>
A2.1.09	<p>Support unique requirements associated with enrollment and access management of foreign schools.</p> <p>The proposed access control and identity management systems will be configurable for the unique information and processing requirements of foreign schools. User attributes will be configurable to capture special data elements required for these users.</p>
A2.1.10	<p>Provide workflow tools that support registration and access approval processes.</p> <p>Both the access control system and the identity management system will be capable of receiving information from workflow tools to support registration and access approval processes.</p>
A2.1.11	<p>Effectively terminate access rights across systems.</p> <p>The identity management and the access control system can be configured to terminate access upon receiving appropriate termination messages from workflow systems. Deployment of these technologies will need to include development of the appropriate policies and procedures to identify relevant termination events and define procedures for executing and monitoring termination of user privileges.</p>
A2.1.12	<p>Provide a method for easy password reset.</p> <p>The identity management system will provide functions to efficiently and consistently reset user passwords for FSA systems. Depending on how FSA policies and procedures are defined, functions will be available for either allowing the help desk to reset user passwords across all FSA systems at the same time, or letting a user reset their own password by answering appropriate questions or entering authentication information in a password reset application.</p>



Business Objective A2.2 – “Self-service capabilities”

Scope:	Enrollment and Access Management	
Identifier/Title:	A2.2 - Improve self-service capabilities.	
Description:	As part of the overall FSA effort to improve access to FSA systems and increase efficiency of FSA services for Trading Partners, Enrollment and Access Management Systems should provide functions that allow users to conduct appropriate transactions or obtain information on their own, without having to contact FSA.	
High-Level Requirements:	A2.2.1	Support self-service administration of user access by the Trading Partner. Trading partners will be able to manage user accounts for their own users through the delegated administration function of the Identity Management system, subject to FSA policy and procedure restrictions that will guide configuration of administrator privileges.
	A2.2.2	Provide Trading Partner Enrollment status via the Web. The Enrollment System will have consolidated information about the status, Enrollment history, and eligibility decisions. This information can be used to develop a Web-based application for displaying Enrollment and eligibility status if desired by FSA.
	A2.2.3	Provide users a view of their access status. The identity management system will have consolidated information about the approval status, current access privileges, and configuration parameters for each user. This information can be used to develop a Web-based application for displaying security approval and access privileges for users if desired by FSA.



Business Objective A2.3 – “Balance access and security”

Scope:	Access Management	
Identifier/Title:	A2.3 - Balance easier access and system security.	
Description:	Make enrollment and access management easier for Trading Partners to the extent that is consistent with FSA security objectives and regulatory requirements. Develop policies, processes, and tools that define and implement a balanced approach that minimizes barriers to access yet appropriately protects FSA systems and data.	
High-Level Requirements:	A2.3.1	<p>Mitigate risk of single access point to the Title IV Aid Delivery process.</p> <p>The Enrollment system, access control system, and identity management systems will implement security controls to mitigate the effects of system failure. Each system will adhere to FSA SLC security requirements, and will be developed according to appropriate security standards and policies. IT components of these systems will be deployed in standard FSA data center environments that will provide infrastructure security controls and security monitoring, including network access control, intrusion detection and security monitoring, platform hardening, and protection against virus, malicious software, and other forms of external network attack.</p>
	A2.3.2	<p>Provide business continuity processes that allow easy recovery of Access Management Systems.</p> <p>The enrollment, access control, and identity management systems will be deployed with appropriate high-availability controls and back-up procedures to provide for continuity of operations and protect against potential compromise of system availability.</p>
	A2.3.3	<p>Provide session timeout features that balance usability with FSA security requirements.</p> <p>The access control system and identity management system will provide configurable settings for enforcement of user parameters, such as password policies (expiration, complexity requirements) and limits on user sessions.</p>
	A2.3.4	<p>Minimise restrictions on public information.</p> <p>The access control system and the identity management system will be able to assign a range of user access privileges. Public information can be configured for</p>



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

		unrestricted access, while more sensitive FSA information or data subject to Privacy Act restrictions can be configured for access only with users possessing appropriate authorization.
--	--	--



Business Objective A2.4 – “Flexibility for future requirements”

Scope:	Enrollment and Access Management	
Identifier/Title:	A2.4 - The Enrollment and access solution should be flexible enough to support the requirements of current and future FSA systems.	
Description:	Changes are expected in FSA systems, processes, and the technology used to deploy FSA services. FSA Enrollment and Access Management Systems should be flexible enough to account for anticipated changes in FSA systems and processes.	
High-Level Requirements:	A2.4.1	<p>Provide flexible provisioning services for existing and future systems.</p> <p>System flexibility will be provided by several design features and functions that are incorporated into the solution vision:</p> <ul style="list-style-type: none"> • Access control and identity management systems will provide application programmer interfaces (APIs) and software development kits (SDKs) that will provide tools for integration of these systems with the FSA IT environment and individual Web applications and legacy systems. • Access control and identity management systems will adhere to accepted security standards, such as SAML, that will promote interoperability between FSA systems. • Access control and identity management systems will provide interfaces and connectors for common operating system and IT platforms to facilitate integration and deployment of management functions.
	A2.4.2	<p>Support future system consolidation efforts.</p> <p>System consolidation will be supported by use of standard interfaces and connectors for integration of access control and identity management systems with common operating system and IT platforms.</p>
	A2.4.3	<p>Support easier Access Management for legacy systems with minimal or no rework.</p> <p>The identity management system will provide adapters or connectors to support communication with existing security functions that are part of mainframe systems and legacy databases. The identity management system will be able to provision and manage user accounts on existing</p>



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

	<p>FSA systems without requiring changes to system program code.</p>
A2.4.4	<p>Support simplified User identification/certification between FSA and other government agencies.</p> <p>The access control system and the identity management system will provide tools for sharing identity credentials. The access control system will support standards such as SAML and other federated identity mechanisms to let FSA accept user authentication credentials from Trading Partners, subject to FSA security policies and procedures.</p>
A2.4.5	<p>System needs to support adoption of e-signatures.</p> <p>The access control system will support a variety of user authentication mechanisms, including digital signatures and other forms of strong authentication that can be employed in electronic signature systems.</p>
A2.4.6	<p>Provide flexibility to accommodate changes in business process, regulations, and statutes.</p> <p>Enrollment, access control, and identity management systems will provide configurable parameters for system functions and access control to allow for changing business processes and compliance with regulatory requirements.</p>



Business Objective A2.5 - “User customization”

Scope:	Data Strategy	
Identifier/Title:	A2.5 - Allow users to customize their experience with FSA systems.	
Description:	Users should be able to customize the appearance and functionality of FSA systems to adapt to the way they work. This objective is not limited to Enrollment and Access Management Systems. The scope of this objective extends across the entire Data Strategy project, as well as any FSA effort to develop new systems or applications for Trading Partners.	
High-Level Requirements:	A2.5.1	(No specific requirements identified.) While not a primary focus of the Enrollment and Access Management project, user interaction with FSA systems can be customized through the access control system. Individualized Web pages can be displayed by the access control system, based on user access privileges or membership in an access role or group.



Business Objective A3.1 – “Streamline Enrollment and registration”

Scope:	Enrollment and Access Management	
Identifier/Title:	A3.1 - Streamline enrollment and access management for Trading Partner services.	
Description:	Simplify, consolidate, and integrate Enrollment and access management processes to provide faster and more efficient services to Trading Partners.	
High-Level Requirements:	A3.1.1	<p>Consolidate duplicated system Enrollment processes.</p> <p>The Enrollment system high-level design provides a consolidated set of processes and functions for enrolling in all FSA systems.</p>
	A3.1.2	<p>Provide a common collection point and storage location for Trading Partner data.</p> <p>The Enrollment system provides a consolidated Enrollment data management capability to manage all Trading Partner data related to Enrollment, eligibility, and administrator access processes.</p>
	A3.1.3	<p>Share information across FSA systems throughout the Student Aid Lifecycle.</p> <p>The consolidated process and data management functions defined the Enrollment system high-level design will provide a single system that promotes communication of Enrollment and eligibility information across all FSA systems.</p>
	A3.1.4	<p>Provide a method for viewing enrollment and access management data from a single location.</p> <p>The Enrollment system provides a set of unified functions for FSA to view and manage Trading Partner Enrollment and eligibility data. The access control and identity management system will provide display and reporting functions for access privileges of all users across FSA systems.</p>
	A3.1.5	<p>Minimize the number of initial contact points for the system Enrollment process and for obtaining user access to systems.</p> <p>The Enrollment system will be the initial point of contact for Trading Partners to initially enroll in all FSA systems. Individual users will be able to request access to FSA</p>



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

		systems through the identity management system and its delegated administration functions.
	A3.1.6	<p>Support a common method or communicating information about enrollment and access management to users.</p> <p>Consolidation of enrollment functions in the enrollment system and user account management functions in the identity management system will provide common communication vehicles for Enrollment and access information to all Trading Partners and users.</p>



Business Objective B1.1 – “Uniform process for access decisions”

Scope:	Access Management	
Identifier/Title:	B1.1 - Adopt a uniform decision making process for evaluating users requesting access to FSA systems.	
Description:	Different systems currently perform different eligibility verification checks during Enrollment and registration processes. A uniform process for evaluating and processing access requests would provide a more consistent decision about eligibility.	
High-Level Requirements:	B1.1.1	<p>Provide the capability to review default and overpayment records.</p> <p>The Enrollment system will provide an interface to eligibility management processes related to default and overpayment records. Other financial management functions will be part of Trading Partner Management, which will be closely integrated with the Enrollment system.</p>
	B1.1.2	<p>Enable access decisions at the business process level.</p> <p>The identity management system will be integrated with access approval decisions implemented as business processes or as workflows managed by a workflow system. Business process decisions will define the FSA security access policies and procedures to be incorporated into the rules and authorization policies required for configuration of access rules for both the access control system and identity management components.</p>



Business Objective B2.1 – “Audit user access”

Scope:	Access Management	
Identifier/Title:	B2.1 - Provide effective oversight of user access to FSA systems.	
Description:	Security policy defines rules and procedures to safeguard the enterprise. In order for those policies to be success, the policies must be strictly enforced. An effective Access Management System must provide effective oversight of user access to FSA systems by ensuring compliance with FSA Enterprise Security Policies.	
High-Level Requirements:	B2.1.1	<p>Provide the ability to efficiently identify accounts that should be removed or disabled.</p> <p>The identity management system will provide display and reporting functions for management of access privileges across FSA systems. Either scheduled or <i>ad hoc</i> reports can be created to identify access privileges assigned to individuals or groups of users on multiple systems.</p> <p>While not envisioned for initial deployment in the identity management system, functions will be available to accept automated data feeds from external systems to identify users who should have their access privileges modified or removed. For example, if data from school systems is available to identify users no longer associated with a Trading Partner, the identity management system will be able to automatically remove access for those users across all FSA systems.</p>
	B2.1.2	<p>Provide a convenient, effective way to view and report on access privileges of users across multiple systems.</p> <p>As described above, a variety of reporting and display functions will be available in the identity management system to identify and document access privileges assigned to users of FSA systems. The access control system will provide its own reporting facilities to log user activity on FSA Web applications.</p>
	B2.1.3	<p>Provide an audit trail sufficient to track updates and perform historical research.</p> <p>The Enrollment, access control, and identity management system will all provide audit trail capabilities to capture data about user activity and changes to user access privileges. Procedures will need to be developed for the efficient archiving of the audit data created by these</p>



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

	<p>systems, and storage in formats that can be readily queried to answer questions about historical system events.</p>
B2.1.4	<p>Provide ability to view user access privileges over time.</p> <p>The identity management system and access control system will be able to record changes in user access privileges, including information about which administrator performed or authorized the changes. The system deployment plan will need to define the appropriate processes and policies for archiving and protecting the audit data that will be collected.</p>
B2.1.5	<p>Provide automated procedures to identify anomalies in access or inappropriate combinations of access privileges across systems.</p> <p>Some anomaly detection capabilities will be immediately available in the access control system. For example, an intrusion detection capability will be able to detect when a specific number of login attempts have failed (indicating a potential password-guessing attack) and lock the user account. More sophisticated monitoring of access activity or inappropriate combinations of access privileges will need to be enforced by either the identity management system configuration rules, or through investigation of audit log information. Tools are available to assist with consolidation of security monitoring information as add-on capabilities to the access control and identity management systems.</p>
B2.1.6	<p>Support consolidated reporting of enrollment and access management across FSA systems.</p> <p>The enrollment system will be able to report on enrollment processes across FSA because it will provide centralized functions for Trading Partner sign-up functions for all FSA systems. Similarly, the identity management system will provide centralized reporting for all FSA systems that are integrated with the provisioning and user account management functions.</p>



Business Objective B3.1 – “Meet regulatory requirements”

Scope:	Enrollment and Access Management	
Identifier/Title:	B3.1 - Meet FSA regulatory compliance requirements.	
Description:	FSA systems operate in a complex federal government environment with numerous regulatory compliance and reporting requirements. (E.g. The Privacy Act of 1974, The Government Information Security Reform Act, U.S. Department of Education Information Technology Security Policy, etc.) This environment must be considered when designing and implementing an Enrollment and Access Management System.	
High-Level Requirements:	B3.1.1	<p>Consider and incorporate external regulatory requirements affecting enrollment and access management.</p> <p>The enrollment, access control, and identity management systems will be configured to incorporate all regulatory and compliance requirements that FSA must meet.</p>
	B3.1.2	<p>Provide methods to track FSA compliance with regulations as they change.</p> <p>The primary means of tracking FSA compliance will be the centralized configuration and auditing functions of the Enrollment, access control, and identity management systems.</p>



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

Business Objective C1.1 – “Facilitate enterprise access to data”

Scope:	Data Strategy	
Identifier/Title:	C1.1 - Facilitate access to sets of data at the enterprise level.	
Description:	As discussed in Section 1.1 of this document, the enrollment and access management is one team in the overall Data Strategy effort. While Enrollment and Access Management must support this business objective, the content of this objective is relates to the overall Data Strategy effort.	
High-Level Requirements:	C1.1.1	<p>(No specific requirements identified.)</p> <p>This business objective is beyond the specific scope of the enrollment and access management project. Satisfying this business objective will require other Data Strategy team efforts, including the Data Framework and Tech Strategies projects.</p> <p>The access control system and the identity management system will be able to facilitating access to sets of data at the enterprise level through efficient management of access privileges to FSA systems</p>



Business Objective C2.1 – “Enterprise policies and standards”

Scope:	Enrollment and Access Management	
Identifier/Title:	C2.1 - Create enterprise policy and standards for Enrollment and access management.	
Description:	Automation and technical components are only as strong as the underlying enterprise policy and standards. FSA must have enterprise policies and procedures that define standards and support enrollment and access management operations.	
High-Level Requirements:	C2.1.1	<p>Establish standards for initial identification of users.</p> <p>As part of the deployment efforts for the Enrollment, access control, and identity management systems, standards will be developed to define procedures for appropriately identifying and verifying applicant Trading Partners and individuals.</p>
	C2.1.2	<p>Define enterprise user access privileges and roles.</p> <p>The access control system and identity management system that provides Access Management functions across multiple systems. Deployment of these systems will require that FSA develop enterprise policies to define access privileges and roles in a consistent manner for all FSA systems.</p>
	C2. 1. 3	<p>Define delegated administration standards for Trading Partners.</p> <p>The identity management system will provide delegated administration functions. Deployment efforts for this system will need to define the FSA policies and standards that will be used to configure the delegated administration system.</p>
	C2.1.4	<p>Define enterprise standards for authentication of users.</p> <p>Although current practice is to authentication users of FSA systems with either a PIN or password, developments in federal authentication standards will require that FSA develop standard definitions of authentication mechanisms and security levels for different classes of FSA systems and data. The access control system will provide flexible authentication methods to allow implementation of alternate authentication credentials, including digital certificates, tokens, and biometric procedures.</p>
	C2.1.5	<p>Define signature standards for both wet signatures and on-</p>



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

	<p>line signatures.</p> <p>The Enrollment system vision will provide opportunities to streamline Trading Partner sign-up processes that currently require manual signatures on paper forms. Use of online or digital signature mechanisms implies that FSA will need to create the policy structures and standards required to authorize use of online signature methods.</p>
C2.1.6	<p>Define standards for periodic review of access privileges across systems.</p> <p>The access control and identity management systems will provide reporting tools to monitor access privileges across all FSA systems. Standards and procedures will need to be defined in deployment plans to define the schedule, processes, and responsibilities for performing access reviews.</p>
C2.1.7	<p>Define standards for periodic review of audit logs across systems.</p> <p>Audit logs will be created by the Enrollment, access control, and identity management systems. These systems will provide tools and functions to capture and archive audit data, but standards to define procedures and responsibilities for audit log review will need to be created as part of deployment planning.</p>
C2.1.8	<p>Create enrollment and access management standards to define integration guidelines for future systems.</p> <p>The access control system will require application integration to enable interaction with existing and planned FSA Web applications. The identity management system will require integration with FSA systems to allow management of user accounts and other administrative functions. In both cases, the deployment efforts for these systems will need to include development of integration standards to guide application and system development efforts for future systems.</p>



Business Objective C2.2 – “Security of FSA systems”

Scope:	Access Management	
Identifier/Title:	C2.2 - Maintain security of FSA systems.	
Description:	Previous FSA Security and Privacy Policy efforts outlined the FSA security fundamentals as individual accountability, least privilege, separation of duties and functions, principle of proportionality, and security and privacy by design. An Access Management System needs to be technically secure and support proper security procedures.	
High-Level Requirements:	C2.2.1	<p>Provide secure infrastructure for access management.</p> <p>The access control and identity management components will be particularly sensitive points of potential attack within the FSA computing environment. For example, single points of control for user accounts and a single sign-on capability represent some increase in risk if these system are compromised, compared to current distributed security administration functions, even though current systems are less efficient and more difficult to use. Therefore, it will be critical to design and deploy the access control and identity management systems in a security manner. FSA security and privacy policies provide basic guidance for the security controls that will be required to protect these systems, and the deployment should adhere to recommendations of the FSA Security and Privacy Architecture Vision. Infrastructure support for access control and identity management components will also be protected by development of appropriate system security plans and Service Level Agreements with contractors responsible for operating the data center housing these systems.</p>
	C2.2.2	<p>Provide controls to mitigate risks associated with consolidated UserIDs.</p> <p>The deployment plan for the access control and identity management systems will include a security risk assessment and development of procedures and standards for configuration requirements and processes to protect consolidated UserIDs.</p>
	C2.2.3	<p>Provide centralized oversight of system security to identify potential security breaches.</p> <p>Both the access control system and the identity management system will provide centralized oversight</p>



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

	<p>functions to detect potential security breaches. Access privileges for both Web applications and legacy systems will be configurable and can be monitored across multiple systems. This will allow more efficient monitoring of access privileges and security operations compared to current systems are difficult to monitor because security administration procedures are isolated and inconsistent from system to system.</p>
C2.2.4	<p>Enforce individual accountability across FSA systems.</p> <p>The Enrollment, access control, and identity management systems will encourage individual accountability by creating enterprise procedures for approving, managing, and enforcing access privileges for each user.</p>
C2.2.5	<p>Establish enterprise-wide policy, participation agreements, and audits to limit a single UserID to a single user.</p> <p>The Enrollment, access control, and identity management systems will provide configuration interfaces and auditing tools to enforce and monitor individual use of UserIDs.</p>



Business Objective C2.3 – “Match access privileges to job functions”

Scope:	Access Management	
Identifier/Title:	C2.3 - Provide users with access to FSA systems appropriate for their job function.	
Description:	A fundamental of FSA Security and Privacy Policy is least privilege – each individual is authorized access to only those FSA information assets required to perform his or her job. The definition of flexible role based users will help Access Management support this policy.	
High-Level Requirements:	C2.3.1	<p>Provide role-based access to FSA systems.</p> <p>The Enrollment system will collect the access information required for FSA to assign roles to Trading Partner users. The access control system will enforce access rules for use of FSA Web applications based on roles assigned to each user. The identity management system will facilitate configuration and management of role based access by providing administrative interfaces for defining roles and by allowing user account provisioning and management based on user roles that define required access privileges based on the job function each user performs.</p>
	C2.3.2	<p>Create flexible roles to allow for changes and additions independent of lifecycle phase.</p> <p>The access control and identity management systems will allow great flexibility in how access roles are defined and managed. For example, roles will be configurable as hierarchical roles that allow inheritance of access privileges between roles, as well as compound roles that allow creating new roles based on the union of access privilege sets defined for component roles.</p>
	C2.3.3	<p>Support exceptions to standard access roles.</p> <p>The access control and identity management system will provide for flexible management of access privileges by allowing exception-based access privilege definition. For example, access privileges for a user can be managed by assigning a standard role then adding specific privileges, or by deleting specific access privileges from a standard role.</p>
	C2.3.4	<p>Integrate Trading Partner access with Dept of Education Staff access processes.</p>



**Data Strategy Enterprise-Wide
Enrollment and Access Management
Access Management High-Level Design**

	<p>The access control system and the identity management system will be able to manage and enforce access privileges for both FSA Trading Partners and for Department of Education staff and other internal users.</p>
C2.3.5	<p>Provide the ability to control access at different levels of granularity.</p> <p>The access control system will be able to define access rules at granular levels down to individual data fields. However, the initial deployment plan will probably focus on use of the access control system for authentication functions only, retaining native granular access control systems currently part of existing applications. The identity management system will be able to manage roles that are defined for any level of granularity.</p>
C2.3.6	<p>Support ability to designate the recipient of a requested file.</p> <p>Authentication and account management functions for entities and individual users of file transfer systems will be managed by the access control system and the identity management system. However, neither system will provide the actual file transfer mechanisms to manage batch transmission of data.</p>



Business Objective C3.1 – “Effective training and customer support”

Scope:	Enrollment and Access Management	
Identifier/Title:	C3.1 - Provide effective training and customer support across FSA systems.	
Description:	Training and outreach to users is a cornerstone of enterprise security policy. Without proper communication, users could be equally unaware of the current policies and the possible disastrous results of not following the security policy.	
High-Level Requirements:	C3.1.1	Provide efficient help desk support for Trading Partners. Help desk support will be planned during detailed design and deployment planning for the Enrollment Management System.
	C3.1.2	Provide common processes that allow help desk staff to handle cross-enterprise support issues. The Enrollment Management System will define common processes for signing up Trading Partners across all FSA systems.
	C3.1.3	Provide Enrollment status to help desk staff for customer support. The Enrollment Management System and the identity management system will provide effective tools for help desk staff to view and manage Enrollment and access status information for Trading Partners and users.
	C3.1.4	Create effective communication and education channels for explaining the enrollment and access management process. Detailed designs and deployment plans for Enrollment and Access Management Systems will need to incorporate communications plans for providing education to Trading Partners on use of the Enrollment and Access Management Systems.
	C3.1.5	Provide training on expected user responsibilities. Detailed designs and deployment plans for Enrollment and Access Management Systems will need to develop training plans to define and inform users of their individual responsibilities. Training on FSA security and privacy policy will be developed in compliance with the FSA IT Security and Privacy Policy and any other training procedures defined by FSA.



Business Objective C3.1 – “Adopt policies to improve processes”

Scope:	Enrollment and Access Management	
Identifier/Title:	C3.2 Adopt enrollment and access management policies that improve business processes.	
Description:	In addition to the general enterprise balance of easier access and system security, it is important to keep FSA’s business processes in mind and look for ways to improve the flow of business through Enrollment and access management.	
High-Level Requirements:	C3.2.1	Consider access needs during peak processing periods. The detailed design and system deployment plan for Access Management components will define access configurations that are consistent with both user access needs and the FSA IT Security and Privacy Policy.
	C3.2.2	Provide for proactive notification of password expiration. The access control system and the identity management system will be able to notify users of their password expiration dates.



Appendix D: Background on Federal eGov e-Authentication Effort

The Enrollment and Access Management effort at FSA is developing an Identity and Access Management solution that will fulfill FSA's business objective of providing easier system access for Trading Partners. FSA requirements were identified for interacting with Trading Partners that may require sharing user authentication credentials from third parties or from other government agencies. The federal e-Government initiative is developing an architecture that addresses this concept of sharing user credentials. Known as e-Authentication, this initiative will facilitate access to multiple federal agencies. This section provides background on the progress of the e-Authentication initiative to date.

Note: The background material below is primarily based on architecture designs developed prior to October 2003³. Recent published reports have indicated that recent decisions will probably change the course of the e-Authentication work, and a new architecture is being designed. Therefore, the e-Authentication architecture presented here will need to be updated when the new design is published.

Authentication services will be provided by the e-Authentication gateway. The e-Authentication gateway will be providing services that are also part of the Access Management solution for FSA. The possibility of integrating FSA access control solution and the e-Authentication gateway, to make FSA applications part of the E-Government initiative is examined and analyzed in this section. A possible high level design for integration with the future production version of e-Authentication gateway is also discussed.

eGov & e-Authentication Background

The eGov portal was created to meet the goals of the E-Government initiative. The role of the eGov portal is to act as a single entry point for various government services for both citizens and businesses. For example the eGov portal will allow a citizen the ability to access both their tax returns and student loan information without logging into the IRS and FSA websites separately.

The e-Authentication initiative was launched to streamline the delivery of authentication services for the eGov portal. Authentication is the process of establishing confidence in the identities and attributes of a user, after she electronically presents them to an information system. Once the users have been authenticated, they have the ability to access multiple government agency applications without entering their passwords and UserIDs again.

Benefits of e-Authentication

The e-Authentication initiative seeks to provide a centralized means of authentication for government systems. Since users do not have to register for each application, it saves time for citizens and requires fewer resources from the government agencies. Time and resources are

³ *Interim e-Authentication Gateway Concept of Operations*, GSA February 2003



also saved in the maintenances of user credential databases, since fewer government agencies would manage them for everyone. Some of the other benefits of e-Authentication are:

- Reduce authentication system development and acquisition costs, and reallocate labor resources used to develop such systems
- Reduce burden on the public in complying with repeated, duplicate or inconsistent processes of identity proofing
- Consistent authentication decisions
- Increased public trust in the use of online service delivery
- Use of existing and future e-Authentication processes, within their organizations or those that are available Government-wide
- Reduced number and type of electronic credentials that Federal employees, citizens, and businesses need to conduct business electronically with the Government

Current Status

The eGov initiative is testing an interim (pilot) e-Authentication gateway that is providing services to some agency applications. The table below provides a list of agencies who are integrating with the gateway on an interim basis and also the credential providers that are being used.

Interim e-Authentication Users

Agency	Application	Credentials
USDA NFC	WebStar	PKI & P/P
GSA	ACMIS	OPM E/E
FEMA	DMI	PKI
Treasury	SSA	Pay.Gov
GSA	3GS	TBD
SSA	Secure File Xfer	PKI ACES
NDGRO	Seed/Agriculture	WebCAAF

Figure 30 - Interim e-Authentication Users

The gateway is not operating in full production mode and does not provide full functionality for these applications. e-Authentication initiative is in the process of issuing a Request for Proposal (RFP) for the development of a production version of the e-Authentication gateway. The front-end interface of the interim e-Authentication Gateway provides interface for government agency applications, portals and users. The back-end handles the validation process and communicates with electronic credential providers.

eGov Details

A very high level view of how the eGov portal works is shown below in the eGov portal overview diagram. This diagram explains how the eGov Portal works in general. This figure demonstrates a user utilizing the eGov portal to access a government agency application. The



eGov portal passes the user credentials to the gateway. The gateway passes the user information to the electronic credential provider. Electronic credential provider authenticates the user and assigns an authentication level to her. Depending on the user's authentication level the user is logged onto the agency application. If the required authentication level for the agency 1 application is lower or equal to that of the agency 2 application; the user is able to gain access to the agency 1 application without reentering the login credentials again.

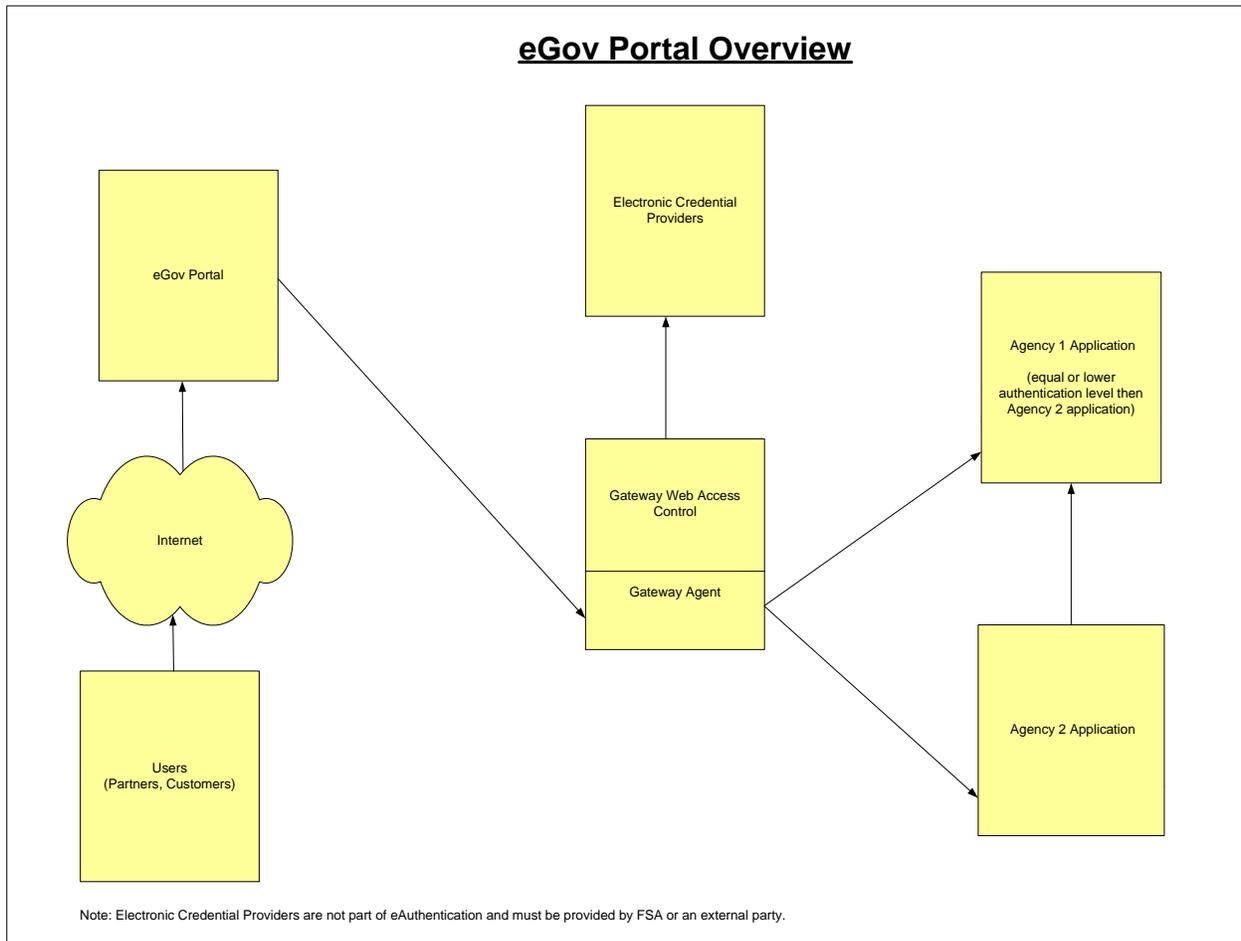


Figure 31 - eGov Portal Overview



The eGov portal architecture in figure 32 below provides a more detailed step-by-step account of the authentication process. The software agents in this architecture reside on a Web server and intercept the incoming data. These agents are used to communicate between different components of e-Authentication gateway. The agents being used in this architecture are proprietary and vary from vendor to vendor.

Authentication Process Steps

The steps in this authentication process below correspond to the numbers in figure 32. Each step number below describes the process that is being performed during that step in the architecture diagram.

1. Users enter the eGov portal and provide their credentials.
2. Credentials are sent to the e-Authentication gateway agent.
3. e-Authentication gateway agent passes this information to the policy server.
4. The policy server checks the user information before passing it to the electronic credential provider.
5. At this point the credential provider assigns user an authentication level and the next two steps can occur in parallel.
 - a. If the user meets or exceeds the required authentication level for agency 1 application, she is granted access to that application.
 - b. If the user meets or exceeds the required authentication level for agency 2 application, she is granted access to that application.
6. If this users authentication level meets or exceeds the one required by agency 2 application, the user is granted access (from agency 1 application) without retyping credentials

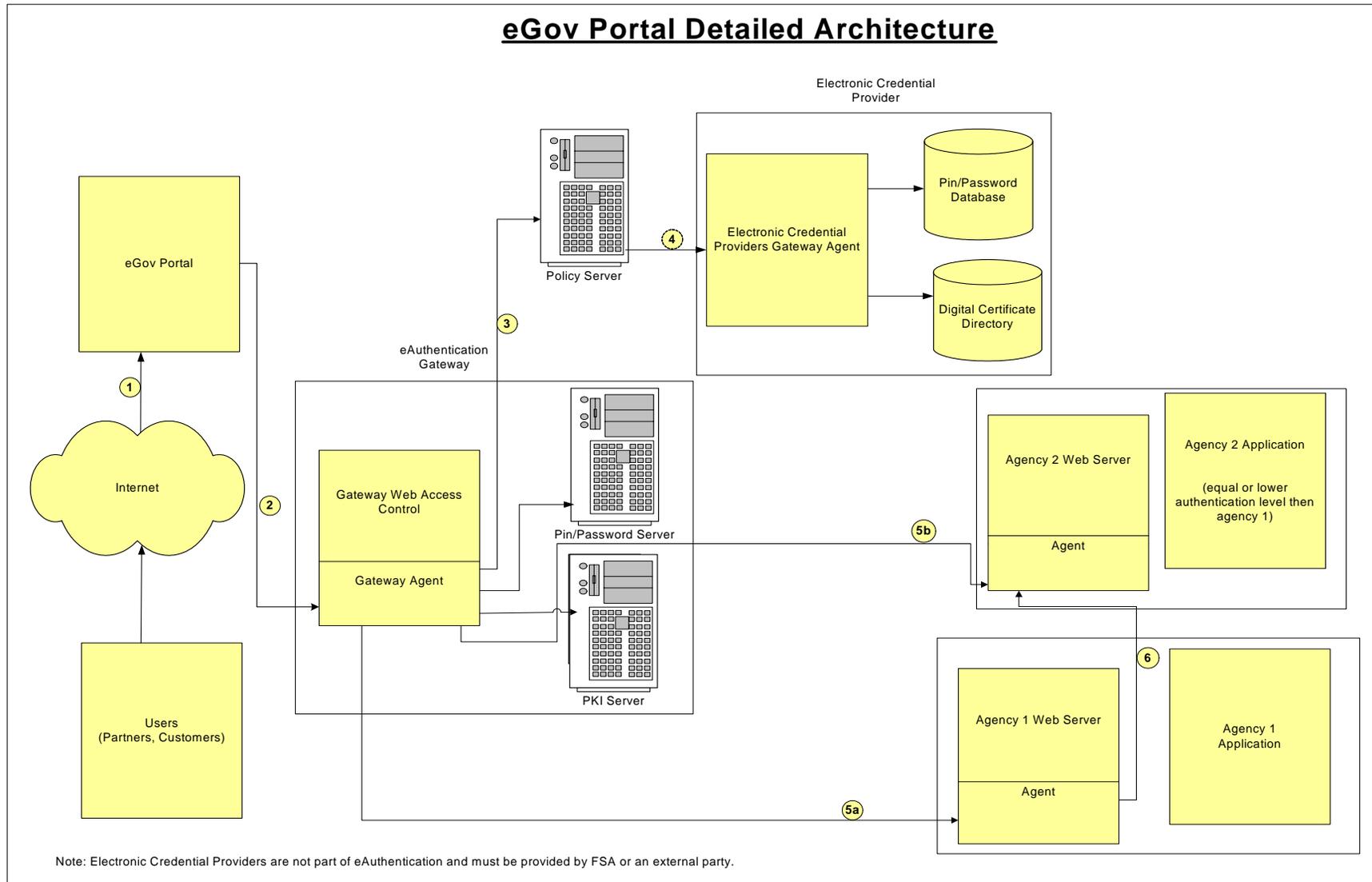


Figure 32 - eGov Portal Detailed Architecture



Authentication Levels

Authentication Levels have been defined by General Services Administration (GSA) to provide guidelines to federal agencies, so that electronic transactions can incorporate the appropriate level of security. These authentication levels were published by the office of Electronic Government and Technology at GSA⁴. Government agencies will have a choice of authentication levels that they can choose for particular applications. Risk assessment will help agencies determine the risk level of the application and will allow them to assign an appropriate authentication level based on those needs. These authentication levels are defined below:

Level 1- Minimal Assurance

At this level little or no confidence is placed in the identity of the electronic users and authentication error of a user's identity will not cause any harm to the agency application or a 3rd party.

Level 2- Low Assurance

This level is appropriate for electronic transactions in which it is sufficient that the probability of having an authentication error of a user's identity is below average. In this case only minor harms/damages will be caused to agency/government applications and third parties.

Level 3- Substantial Assurance

Level 3 should be used for transactions that require a high degree of confidence in the electronic identity of the user. An authentication error of a user's identity will cause significant damage to the agency and other 3rd parties.

Level 4- High Assurance

Level 4 should be used for transactions that require a very *high degree of confidence* in the electronic identity of the user. An authentication error of a user's identity will cause considerable damage to the agency/government and other 3rd parties. This level should also be used for applications where an authentication error of a user's identity can risk a party's personal safety.

Based on the authentication levels described above it is possible to come up with a possible list of credentials that can be used to satisfy the requirements for each level. The table below provides a quick overview of the possible credential types that might be needed for each authentication level mentioned above.

⁴ Federal Register/ Vol. 68, No. 133/Friday, July 11, 2003/ Notices



Authentication Level	Credential Types
Level 1. Minimal Assurance	None required
Level 2. Low Assurance	Strong Password (required number of characters/text & numbers combination), PIN/Password
Level 3. Substantial Assurance	PIN/Password, Two factor authentication
Level 4. High Assurance	Two factor authentication, Biometric authentication
Level 1. Minimal Assurance	None required

Figure 33 - Authentication Level and Appropriate Credentials

Authentication Levels have been defined to provide guidelines to federal agencies, so that electronic transactions can incorporate the appropriate level of security. The four authentication levels proposed by the Office of Electronic Government and Technology at General Services Administration (GSA) have limitations. The number of levels and the degree of confidence that these levels provide is not flexible enough for many of the applications at FSA. Since these four authentication levels cover a range from “Low Assurance” to “High Assurance”, most of the FSA applications will either fall under authentication level 2 or 3. Since level 2 and 3 cannot be broken down into sub-levels, these levels do not provide enough flexibility to FSA application in assigning user privileges.

The technical guidelines for these authentication levels are to be published by the National Institute of Standards & Technology (NIST), sometime next year. Lack of these guidelines in the short term will affect FSA’s ability to define authentication levels for its applications.

Future Trends in Authentication

Some of the future trends in establishing trust and exchanging credentials between different organizations are described below.

Security Assertion Markup Language (SAML)

SAML is becoming the standard for exchanging authentication information online. SAML is an Extensible Markup Language (XML) based framework for Web services that lets business partner’s exchange authentication and authorization information using Web services standards. SAML allows Web-base security interoperability functions such as Single sign-on (SSO) across websites hosted by different companies. The use of SAML for passing credentials between different agencies will need to be examined by FSA before the integration with the production version of gateway.



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 with respect to the 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 standards, organizations can implement a federated identity model that enables faster integration between heterogeneous environments. 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.

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 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 to enable federation of online communities. Membership in the Alliance is open, and GSA and DOD recently announced that they joined the Liberty Alliance project in effort to standardize Web authentication.

Electronic Credential Providers

Electronic Credential Providers (ECP) are organizations (government or commercial) that issue and might maintain credentials. The main functions performed by ECP's are:

- Provides user identity management services
- Collects and verifies identity information for the user
- Issues and manages credentials

ECP's are not a part of the e-Authentication gateway itself, these credentials must be provided separately either by FSA or by a 3rd party. The direction of the eGov integration effort for FSA will depend on whether or not FSA is wants to act as a credential provider. The two general types of ECP's are described below.



PIN & Password

PIN & Password based ECP's utilize a database with stored user information. When the e-Authentication gateway sends a request for user authentication, the ECP validates the credentials based on the information in the database. This information is transferred back to the gateway and at which time the user is either granted or denied access based on the authentication level of the user.

PKI-Based

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet. Electronic Credential Providers will issue digital certificates that will validate a user's identity.

ECP's embed an individual's or an organization's public key along with other identifying information into each digital certificate and then cryptographically "sign" it as a tamper-proof seal, verifying the integrity of the data within it and validating its use. Some of the benefits of using PKI are:

- User identity is authenticated by the issuance of digital certificates that allows parties to confidently conduct an internet transaction
- A digital certificate ensures that the message or the document has not been corrupted in transit
- PKI digital certificates protect information from interception during an online transaction
- PKI digital certificates also provide support for nonrepudiation making it nearly impossible to repudiate a digitally "signed" transaction

Advantages of PKI (Digital Certificates) for Electronic Signatures

Digital Certificates will be a much more robust form of authentication for FSA compared to the PIN/Password method. Nonrepudiation is the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Digital Certificates provide better Nonrepudiation ability because a digital signature can only be created by one person. Digital Certificates can provide better non-repudiation capabilities to FSA applications and can thus help reduce fraud.

Credential Issues for FSA

Electronic Credential Providers are not part of e-Authentication and FSA will have to make a decision if they are willing to act as a credential provider. If FSA decides on acting as a credential provider then a decision will have to be made on the types of credentials that will be used to validate a user. The FSA PIN database seems like a potential candidate for electronic



credentials. But the PIN database is intended to be used by students and borrowers and this leaves Trading Partners out of the mix.

Another issue that FSA will need to consider is that of credentials being provided from other government agencies. FSA will have to decide whether its policy will allow acceptance of credentials from these other government agencies. FSA uses the PIN database for user credentials. PIN registration process includes a level of control more stringent than most PIN or Password processes, because the user information is matched with a valid social security number.

FSA will need to evaluate their willingness to accept a weaker authentication mechanism (simple PIN/password matching) from other government agencies. This issue will need to be analyzed in detail before integration with the production version of e-Authentication gateway can be achieved.

eGov Portal Integration

A very high level view of how our proposed Access Management solution for FSA; might integrate with the eGov portal is provided below. This figure shows two possible options through which a user might be able to access FSA applications. In the first option a user uses the e-Authentication gateway to log into Agency 1 application and then enters the FSA application. The other option shows the user entering the FSA application first and then logging on to Agency 2 application.

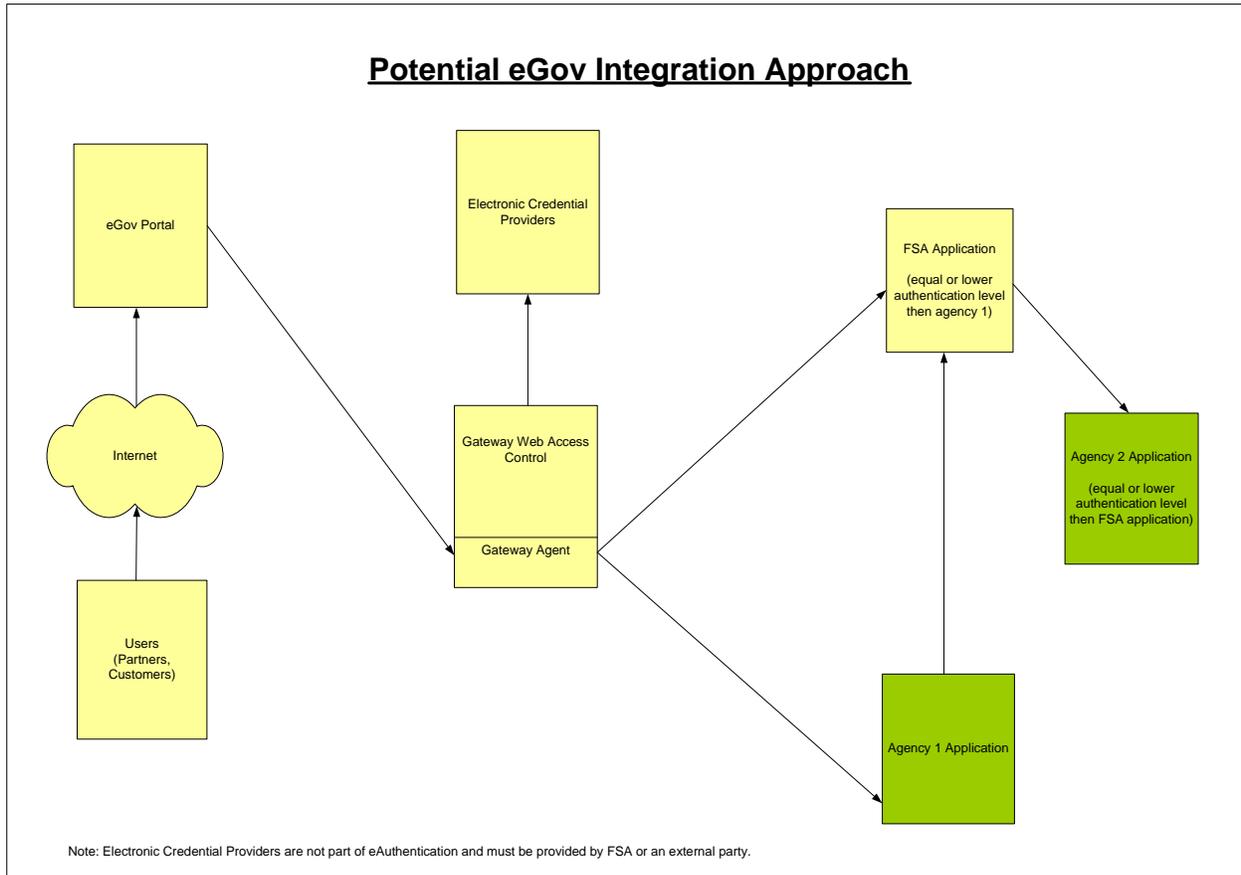


Figure 34 - Potential eGov Integration Approach



Authentication Process Steps

The potential eGov integration architecture diagram below describes the processes that a user will go through to access FSA applications. The steps in this authentication process below correspond to the numbers in figure 35. Each step number describes the process that is being performed during that step in the architecture diagram.

A user trying to connect to FSA has three options:

- Connect Directly to FSA
- Use the eGov portal to connect to agency 1 and then to FSA
- Use the eGov Portal to directly connect to FSA and then to agency 2

The direct connection to FSA is not show in the architecture diagram below for the sake of simplicity. The other two user options are depicted with the use of different colors.

Direct User Connection to FSA (not shown in the diagram)

1. A user will directly access the Web based front end of the FSA Access Management application and will provide credentials.
2. These credentials will be validated based on the information stored in *Enrollment & LDAP database*. Once the credentials are validated, the user will be granted access to the appropriate FSA application.

User Option A (Gateway-Agency 1 App- FSA)

1. The user providers credentials at the eGov portal.
2. These Credentials are sent to the e-Authentication gateway
3. The gateway sends the credentials to the policy server
4. The policy server checks the information and then passes it to the Electronic Credential Provider, who determines the user authentication level based on the information provided.
5. If the user meets or exceeds the required authentication level for agency 1 application, the user is granted access to that application.
6. If the FSA applications authentication level is equal or lower then that of agency 1 application, the user is granted access to FSA application (from agency 1 application) without retyping the credentials.

User Option B (Gateway- FSA- Agency 2 App)

1. The user provides credentials at the eGov Portal
2. These Credentials are sent to the e-Authentication gateway
3. The gateway sends the credentials to the policy server



Data Strategy Enterprise-Wide Enrollment and Access Management Access Management High-Level Design

4. The policy server passes on this information to Electronic Credential Provider, who determines the user authentication level based on the information provided.
5. If the user meets or exceeds the required authentication level for FSA application, access is granted to that application.
6. If users authentication level meets or exceeds the one level required by agency 2 application, the user is granted access (from the FSA application) without reentering credentials.

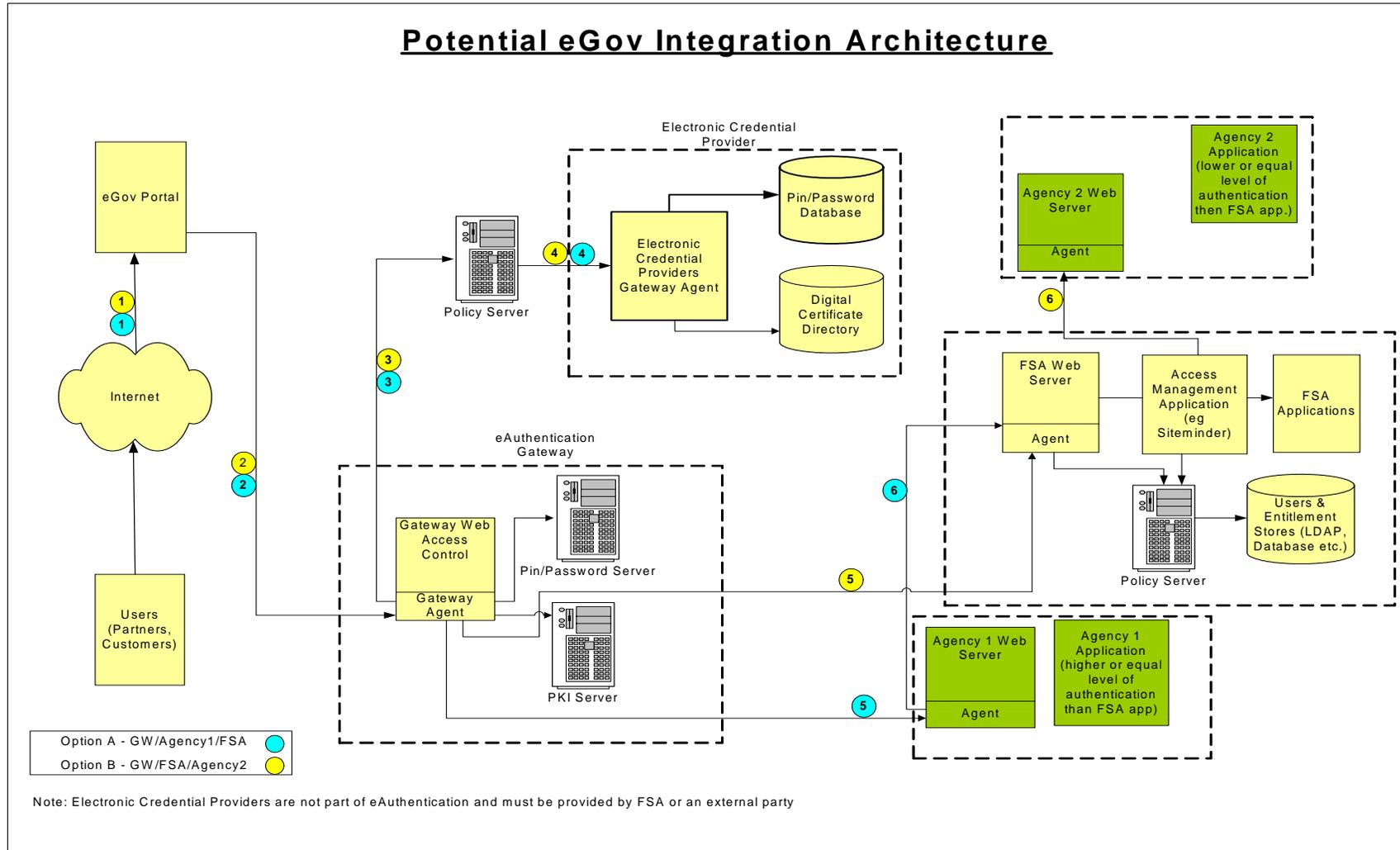


Figure 35 - Potential eGov Integration Architecture



eGov/e-Authentication Conclusion

The various pieces of the puzzle for the e-Authentication gateway are yet not in place. The eGov initiative is still in the process of publishing guidelines for government agencies. Some of the reasons why the eGov portal will not fully satisfy FSA's needs at this time are listed below:

- The services provided by the eGov portal are much more suited towards individual citizens than towards business entities. Since FSA deals with quite a large number of Trading Partners, the Trading Partner benefits of integrating with eGov needs to more closely analyzed.
- The E-Government solution would only provide authentication for FSA applications but lacks much of the other functionality that is important for FSA. These functions have been identified as business needs by FSA, and are part of the goal to provide better service quality to Trading Partners. Some of the functions that will not be provided as part of eGov but are business requirements for FSA applications are:
 - Access control
 - Auditing function
 - User provisioning
 - Account management
- Since few federal agencies will be integrated with the e-Authentication gateway in the short term, the eGov portal's ability to provide a single access point to multiple government services will be very limited.

The eGov portal is still in development and it cannot meet the needs of FSA at this point in time. The Identity and Access Management solution will be able to integrate with the future production version of the e-Authentication gateway. The technical requirements for the production version of the gateway are still not defined. These issues will need to be fully resolved before I&AM solution can integrate with the gateway.

Enrollment and Access Management will continue to track the progress of the interim (pilot) version of the e-Authentication gateway towards production. Any new development and plans will be taken into account in the eGov integration approach. The e-Authentication gateway can be a useful mechanism for some FSA authentication services, but it will still need to be supplemented by a full Access Management solution.