

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



**Security Architecture Status Report –
June – July 2003**

Deliverable #120.2.1

***Task Order #120:
Security and Privacy Support***

**Version 0.1
Draft**

July 31, 2003

Document Revision History

Version Number	Date	Author	Revisions Made
1.0	July 31, 2003	Jesse Bowen	Initial draft

Table of Contents

1	Executive Summary	4
2	Introduction.....	5
3	Security Architecture Status Report.....	6
3.1	Background.....	6
3.2	Objectives	6
3.3	Progress to Date	7
4	Draft Security Architecture Communications Plan	8
4.1	Introduction.....	8
4.2	Goals of the Security Architecture Communications Plan	8
4.3	Scheduling Considerations.....	8
4.4	Audience Segments for Security Architecture Communciations	8
4.5	Content and Major Messages.....	9
4.5.1	Security Architecture Guiding Principles	9
4.5.2	Identity and Access Management Business Case Considerations	10
5	Status of Certification and Accreditation Support	14
6	Appendix.....	15
6.1	Revised Security Architecture Vision Diagram.....	16
6.2	BIG Meeting Presentation on Security Architecture	19
6.3	Meeting Notes for CDDTS Security Assessment.....	20

1 Executive Summary

This document constitutes a required interim deliverable for Federal Student Aid Task Order 120 – Security and Privacy Support.

A new Task Area, 3.12, was recently added to TO 120 to cover security architecture support activities. The security architecture support will include specific tasks as well as *ad hoc* support for security architecture and integration questions. It will also cover integration issues and activities arising from other FSA projects.

Following an introduction, this report consists of the following major sections:

- Security Architecture Status Report (Section 3)
- Draft Security Architecture Communications Plan (Section 4)
- Certification and Accreditation Support (Section 5)

The Security Architecture Status Report provides the background and objectives for the security architecture support activities that have been added to Task Order 120 – Security and Privacy Support.

The Draft Security Architecture Communications plan covers draft elements for communications activities to increase awareness of the FSA security architecture vision and begin initial steps for adoption of security architecture services. The communications plan identifies the overall communication goals, audiences that need to be addressed, and scheduling considerations. The draft plan also summarizes some the major content and messages to develop support for the FSA security architecture.

Certification and Accreditation Support provides an overview of the activities that have been accomplished to perform a security risk assessment for CDDTS.

An Appendix to the document contains a presentation to support the Security Architecture Communications Plan, and meeting minutes from the in-progress security assessment of CDDTS.

2 Introduction

This document is a required deliverable for Task Order 120 – Security and Architecture Support. TO 120 provides support to FSA for a variety of security and privacy support activities. A recent modification to the task order added activities related to security architecture to TO 120. This document is a status report on the activities that are in progress related to security architecture.

This deliverable consists of the following major sections:

- Security Architecture Status Report (Section 3)
- Draft Security Architecture Communications Plan (Section 4)
- Certification and Accreditation Support (Section 5)
- Appendix (Section 6), consisting of:
 - Revised Security Architecture Vision Diagram
 - Security Architecture Presentation for the Business Integration Group
 - Meeting Notes for CDDTS Security Assessment

3 Security Architecture Status Report

3.1 Background

FSA recently completed a project under Task Order 124 to create a Security and Privacy Architecture Framework, Specification, and Implementation Strategy. The implementation strategy recommended several actions that will prepare FSA for development and deployment of security standards and services to promote understanding and adoption of the FSA security architecture. FSA defined several tasks to support follow-on activities related to continued development of security architecture components. FSA created an SOO to define this work, and submitted it to the Integration Partner Program on June 23, 2003. The Security Architecture support activities will be organized as a modification to Task Order 120 – Security and Privacy Support. A modified Technical Proposal for Task Order 120 was submitted by the Integration Partner Program on July 7, 2003. FSA accepted the modified Technical Proposal, and subsequently awarded a modification to Task Order 120 to cover the security architecture support objectives and deliverables.

3.2 Objectives

A new Task Area, 3.12, was added to TO 120 to cover security architecture support activities. This task area will provide half-time staffing of a Senior Security Architect to act as a security Subject Matter Expert. The security architect will also aid the FSA security organization with planning and delivering initial components of the security architecture. The security architecture support will include specific tasks as well as *ad hoc* support for security architecture and integration questions. It will also cover integration issues and activities arising from other FSA projects (such as Data Strategy and PIN Reengineering Analysis) that have security architecture implications.

The specific objectives of Task Area 3.12 are:

1. Begin preparation work for developing the FSA security architecture
 - Assist FSA with communicating the Security Architecture vision to CIO and business groups
 - Perform a gap analysis of the existing FSA IT Security and Privacy Policy to define policies and standards that will require modification or development to support the FSA Security Architecture
 - Create recommended web security guidelines
 - Recommend data classification definitions for classifying the sensitivity of FSA data
 - Provide general security architecture support, such as attending *ad hoc* meetings and advising FSA as a security subject matter expert
2. Support system risk assessments and Certification & Accreditation activities
 - Assist preparation of up to four Tier 2 systems for Certification & Accreditation
 - Tier 2 systems in scope may include PGA, LMS, IFAP, and eCB
 - Assess any additional information needed to prepare for C&A
 - Work with SSOs for the systems to prepare C&A documentation
 - Support risk assessment of the Disability Discharge Tracking System (CDDTS)

3.3 Progress to Date

The recently completed security architecture project developed a set of recommendations based on the following assumptions and findings:

- FSA serves a diverse user population through an extensive, heterogeneous set of systems and applications.
- No single set of technology solutions are likely to satisfy all FSA business objectives, so security functional requirements may vary between systems.
- Even so, many commonalities exist among FSA systems, and a security and privacy architecture can be developed to serve as a unifying and consistent vision of technology approaches to deploying reusable services and components.

The recommendations resulting from the initial security architecture work covered three general areas as described below:

- Define, communicate, and enforce a security and privacy policy framework to support the security architecture;
- Deploy a set of technology components to provide consistent security functionality
- Create consistent standards and requirements for technical and security functions that are outsourced to contractors and vendors.

Current work during the period covered by this status report is focused on the following areas:

- Developing plans for communicating security architecture decisions to FSA business and CIO units.
- Integrating the FSA Security Architecture vision with ongoing projects, including:
 - Enrollment and Access Management (Data Strategy)
 - Technical Strategies (Data Strategy)
 - ED PIN Reengineering
 - Integrated Technology Architecture
 - Enterprise Application Integration
- Supporting FSA Certification and Accreditation activities by performing a security assessment of the Conditional Disability and Discharge Tracking System

Plans for communicating security architecture issues within FSA are addressed in Section 4. The status of the CDDTS security assessment is covered in Section 5 of this document.

Weekly status meetings with the FSA Chief Security Officer have been established to plan detailed support activities for the FSA security architecture and to provide updates on the status of work in progress.

4 Draft Security Architecture Communications Plan

4.1 Introduction

Development of an effective FSA security architecture will require communication of security architecture goals and plans to a wide audience. This section of the status report summarizes draft elements for a security architecture communications plan. It identifies the overall goals of the communications plan, the major audience segments that must be addressed, and summarizes some of the major content and messages that have been developed to date.

4.2 Goals of the Security Architecture Communications Plan

The major goals of the security architecture communications plan are to:

- Identify the primary and secondary internal and external audiences for messages about the FSA security architecture.
- Promote integration of the FSA security architecture into FSA business planning and development of new capabilities.
- Convey the major security architecture principles that form the basis for development and operation of the FSA security architecture.
- Provide opportunities to solicit feedback from system owners as a means of enhancing understanding and acceptance of the FSA security architecture.
- Develop effective communications vehicles for continued development and improvement of FSA security architecture services.

4.3 Scheduling Considerations

Communications about the FSA security architecture vision have already been taking place in the context of business planning discussions and ongoing FSA projects. Additional opportunities will need to be defined to update the various audiences as security architecture planning proceeds. Potential points at which communication efforts will be most effective include:

- During the initial budgeting process for analysis of security architecture tools and services.
- In coordination with recommendations for related projects such as Enrollment and Access Management and ED PIN Reengineering Analysis.
- During the design phase of pilot projects to identify the FSA systems and business units that will participate in pilot efforts.
- Periodically during development phases for security architecture services.
- Prior to initial production roll-out of security architecture services.

4.4 Target Audiences for Security Architecture Communications

There are a variety of internal and external audiences that must be addressed during development of the FSA security architecture. Some of these audiences, and progress to date in delivering initial messages about the FSA security architecture, are summarized below.

FSA Business Units

Business Integration Group: a presentation was delivered to the FSA Business Integration Group about the results of the FSA Security Architecture project. The presentation summarized the major goals and results of the project, and provided an overview of the major security architecture elements being proposed for development as security architecture services. The slides used in this presentation are attached to this report in Appendix 6.2.

FSA and Department of Education Technical Architecture Groups

Presentations to CIO personnel should include representatives from major technical and operational areas of the organization. Briefings should be arranged for CIO management-level and technical architecture personnel.

System Security Officers

A briefing on the security architecture to FSA System Security Officers will provide a way to communicate the current status of security architecture planning. System security officers were consulted in business objective meetings during initial development of the security architecture vision. A follow-up session with this group will provide an opportunity to solicit feedback on the security architecture vision that resulted from their input.

Related Projects

Several FSA projects in progress have a close relationship to FSA security architecture plans. Within the Data Strategy project, meetings have been held on a regular basis with the Enrollment and Access Management team, the Technical Strategies team, and the Data Framework team. The ED PIN Reengineering Analysis project has solicited input on the FSA security architecture, and is including a description of how they plan to integrate with the security architecture vision in their design deliverables. The Integrated Technical Architecture team and the Enterprise Application Integration team have been engaged in communications about specific security architecture issues as they arose. Briefings have also been held on the FSA Security Architecture for representatives from the Students Portal team and the Case Management Office team. These communications will continue and will be tracked in future status reports.

4.5 Content and Major Messages

The sections below summarize the major areas of content and primary messages that need to be communicated to describe the FSA security architecture vision for the audiences defined above. The content areas summarized below include:

- Security Architecture Guiding Principles
- Identity and Access Management Business Case Considerations

4.5.1 Security Architecture Guiding Principles

Development of an implementation approach for the FSA Security and Privacy Architecture should be driven by basic principles that account for the unique aspects of the FSA computing environment. These principles and assumptions are themselves part of the message that needs to be communicated to FSA management, business sponsors, and technical personnel. They are summarized below.

- The FSA security and privacy architecture should define security services and standards that apply across system and business unit boundaries
- FSA security architecture components must support outsourced operations through standards and requirements that become incorporated into contractual outsourcing agreements.
- FSA security architecture implementation strategy must incorporate a high degree of flexibility for implementing security controls that fit the different risk profiles and access privileges of diverse FSA users.
- Business units will be involved throughout the planning and deployment stages for security services and components.
- Deployment of security components and services should be planned in manageable increments that represent feasible deployment efforts while still providing demonstrable benefits.
- Although isolated, “one-off” security solutions should be avoided, a process will be defined to obtain approval for appropriate exceptions to security architecture standards as new FSA capabilities are developed. Development plans for exception-based solutions should include creation of a migration strategy for integration into the FSA Security and Privacy Architecture.
- The goal of security architecture development should be to create a standard set of security products and components to prevent proliferation of divergent solutions for similar problems. However, this does not imply that only a single instance of each capability can be deployed. For example, the Access Management Service could consist of multiple instances, one system for the borrower population and a separate system for trading partners.
- FSA use of security architecture standards will decrease licensing costs, complexity, training requirements, and maintenance overhead.

4.5.2 Identity and Access Management Business Case Considerations

A major element of the deployment recommendations defined in the initial security architecture work was centered on development of services and capabilities for Identity and Access Management. The benefits, capabilities, and deployment implications for these services will need to be communicated to a wide audience. The goals for this effort will be to:

- Foster understanding of the security functions provided by the various access management and identity management services.
- Develop support for implementation of identity and access management functions as enterprise services.
- Convey the relative benefits and costs of implementation identity and access management services compared to continued reliance on the inconsistent, redundant, and effort-intensive methods currently used by FSA today to develop and manage these functions on a system-by-system basis.
- Provide input to the budget-planning process for support of identity and access management functions.
- Create understanding of implementation strategy options to aid decisions for planning deployment of identity and access management services.

- To gain cooperation from business units for the collaboration that will be required to integrate tools and processes for identity and access management into FSA business functions.

Some of the key messages about business drivers, major benefits, and business case justifications for identity and access management are summarized in the bullet points below.

Major Business and Technical Challenges for Identity and Access Management

- There are a variety of users with access to FSA applications and data, such as business partners, customers, FSA and Department of Education employees, and contractors.
- There are an increasing number of applications – providing mission critical functionality – that are undergoing continuous revision and consolidation.
- FSA has many different classes of users with different security and control requirements.
- Currently, each information asset (system, application, database, etc.) has its own security and control subsystem.
- Applications can no longer rely on perimeter security for protection
- FSA needs effective methods to develop and manage security controls and user administration processes.

Identity and Access Management Solution Overview

- Align organization, processes and technology to allow consolidation and integration of Identity and Access Management services
- Provide individualized security and access rights based on a person's identity.
- Deliver the most straightforward solution possible using best practices.

Business Case Justifications for Identity and Access Management

Identity and Access Management services provide an integrated set of business process controls and an integrated architecture to streamline operations, reduce costs, and regain control of user access while providing a significant return on investment. The major justifications for development of these services are:

- Reduced administrative and development costs
- Improved productivity and internal service levels
- Increased security
- Improved and more comprehensive audit capabilities
- More effective regulatory compliance tools
- More innovative and richer interactions with employees, business partners and customers

Business Drivers for Identity and Access Management

With the large number of mission critical applications accessed by the various FSA user populations, critical questions must be answered about how to maintain control of access to FSA systems and data. Identity and Access Management services can address the following business needs:

- Reduce application maintenance costs through automation of user administration.

- Reduce call center volume by automating the resetting of forgotten usernames and passwords.
- Increase productivity by reducing the lead time of granting access to business resources.
- Gain operational advantages by building the capability to quickly and efficiently add new services for FSA users.
- Increase FSA knowledge about the users of FSA services by tying different users of different applications and systems to a single, clearly defined identity.
- Facilitate regulatory compliance.
- Reduce development costs for new applications by re-using consolidated identity, authentication and access control services.

Functional Drivers for Identity and Access Management Services

A comprehensive identity and access management solution can provide functionality that is highly desirable to the FSA user population and business sponsors:

- Improve quality of service by reducing lead time for enabling access or resetting passwords.
- Reduce the number of user IDs and passwords each user must manage.
- Provide simplified sign-on for applications and single sign-on for web based applications.
- Delegate security administration decisions to the business and information owners, relieving the administrative burden on FSA.
- Maintain central control over security policies and security administration and approval workflow.
- Provide instant access to consistent and rich user data through various connectivity options and reporting tools for identity and user activity information.

Security Drivers for Identity and Access Management

Implementing an identity and access management solution improves the security of FSA by giving the right people access to the right resources at the right time and at the right level, with full audit capabilities. Examples of the improvements in security controls and operations include:

- Enforce consistent password policies for all systems and applications.
- Disable user access privileges immediately when a user leaves the organization or changes positions.
- Maintain effective control of the account lifecycle with full auditing capabilities.
- Have a complete view of access privileges for the user population across the enterprise.
- Manage a consistent security framework across the enterprise.
- Remove shared user IDs throughout the enterprise.
- Enforce approved, consistent business processes for enabling access to FSA systems and data.

Benefit and Cost Analysis Factors for Identity and Access Management

The major factors to consider in developing the benefits vs. cost analysis for identity and access management are summarized below.

Benefits

- **Cost savings:** reduction of IT resources, headcount and time spent on provisioning-related processes today; ability to decommission obsolete and costly legacy security systems for user administration and data synchronization.
- **Improved productivity:** enhancement of employees' or trading partners' productivity by efficiently provisioning resources necessary to do their job.
- **Reduced waste:** reduction of costs for use of resources by employees or business partners who have not been disconnected from FSA user accounts.
- **Decreased number of security incidents:** reduction of costly security incidents by maintaining better control over user accounts, ability to quickly and accurately report on user access privileges, more effective enforcement of password policies, etc.

Costs

- **Software costs:** typically a function of the number of users and number of adaptors or connectors for target systems and managed platforms, but some tool vendors offer enterprise licenses.
- **Hardware costs:** servers for provisioning engines, access control engines, directory servers, management utilities, workflow tools, etc.
- **Development and implementation costs:** effort and resources to assess requirements, create a development and sequencing plan, design systems and integration components, install tools and build and custom components, test systems and integration, and migrate new capabilities to production status.

5 Status of Certification and Accreditation Support

The security architecture support activities added to the modified TO 120 – Security and Privacy Support include assistance with FSA Certification and Accreditation efforts in two major areas:

- Assistance with Certification and Accreditation for FSA Tier 2 systems
- Performing a security assessment on CDDTS.

Support for Tier 2 Certification and Accreditation activities will begin during August.

The CDDTS security assessment is in progress. Meetings were held on July 17 with several ACS personnel at the ACS facilities in Rockville, MD that house the CDDTS servers and support. The meeting minutes from the assessment visit are presented in Appendix 6.3, attached to this report. The minutes cover the following topics:

- Purpose of Meeting
- History of CDDTS
- System Overview
- Data Inputs
- Operational Controls
- Physical Access
- Data Center Environmental Controls
- Disaster Recovery
- System Architecture
- Logical Access Controls
- Change Management Requirements
- Anti-Virus Controls
- Network Security
- Application Security
- Audit Log Management
- Data Center Walkthrough

Documentation collected to support the CDDTS risk assessment includes:

- CDDTS Security Plan
- CDDTS Configuration Management Document
- CDDTS Disaster Recovery Plan
- CDDTS Network Diagram
- Department of Education GSS & MA Inventory Submission Form for CDDTS

The CDDTS security assessment is being conducted in accordance with the FSA Risk Assessment Guidance methodology, and will be reported in the recommended format. A draft version of the CDDTS risk assessment will be available by August 8, 2003. The risk assessment will be finalized by August 15, 2003.

6 Appendix

This appendix contains the following information.

- Section 6.1 – Revised Security Architecture Vision Diagram
- Section 6.2 – Security Architecture Presentation for the Business Integration Group
- Section 6.3 – Meeting Notes for CDDTS Security Assessment

6.1 Revised Security Architecture Vision Diagram

The Security Architecture Vision has been updated since it was originally submitted as a deliverable for TO 124 Security and Privacy Architecture Framework. This diagram defines security services and components that FSA can use to implement a comprehensive set of technical security controls. The security and privacy architecture components define reusable security services for FSA systems and applications. In discussions subsequent to completion of the Security and Privacy Architecture Framework task order, some of this terminology used in the architecture description has changed. The changes are outlined below, and the updated diagram is provided in Figure 6.1 on the next page.

1. The name of the “Access Management” component within the Access Management Services layer was changed to “Access Control”. This change was made to improve consistency and avoid confusion with the usage of the term “access management” in the Data Strategy project. The current usage in that work is to reserve “access management” for the overall set of processes and tools used to provide both access control and identity management functions. This distinction in security functionality is shown in Figure 6.2, which is adapted from a presentation to the FSA Business Integration Group by the Enrollment and Access Management team.
2. The depiction of FSA Systems and Applications that interact with the Security Architecture was simplified. The original version of the diagram showed “mainframe” systems in addition to systems for students, trading partner, and financial partners. This part of the diagram was removed to avoid confusion, since all of the three major types of FSA systems have at least some components deployed on mainframe platforms.
3. The shading and footnote used to designate “future functions or systems” was removed from the detailed security components. This change was made to make the security architecture vision diagram more accurately reflect its status as a target state rather than a depiction of currently deployed services.

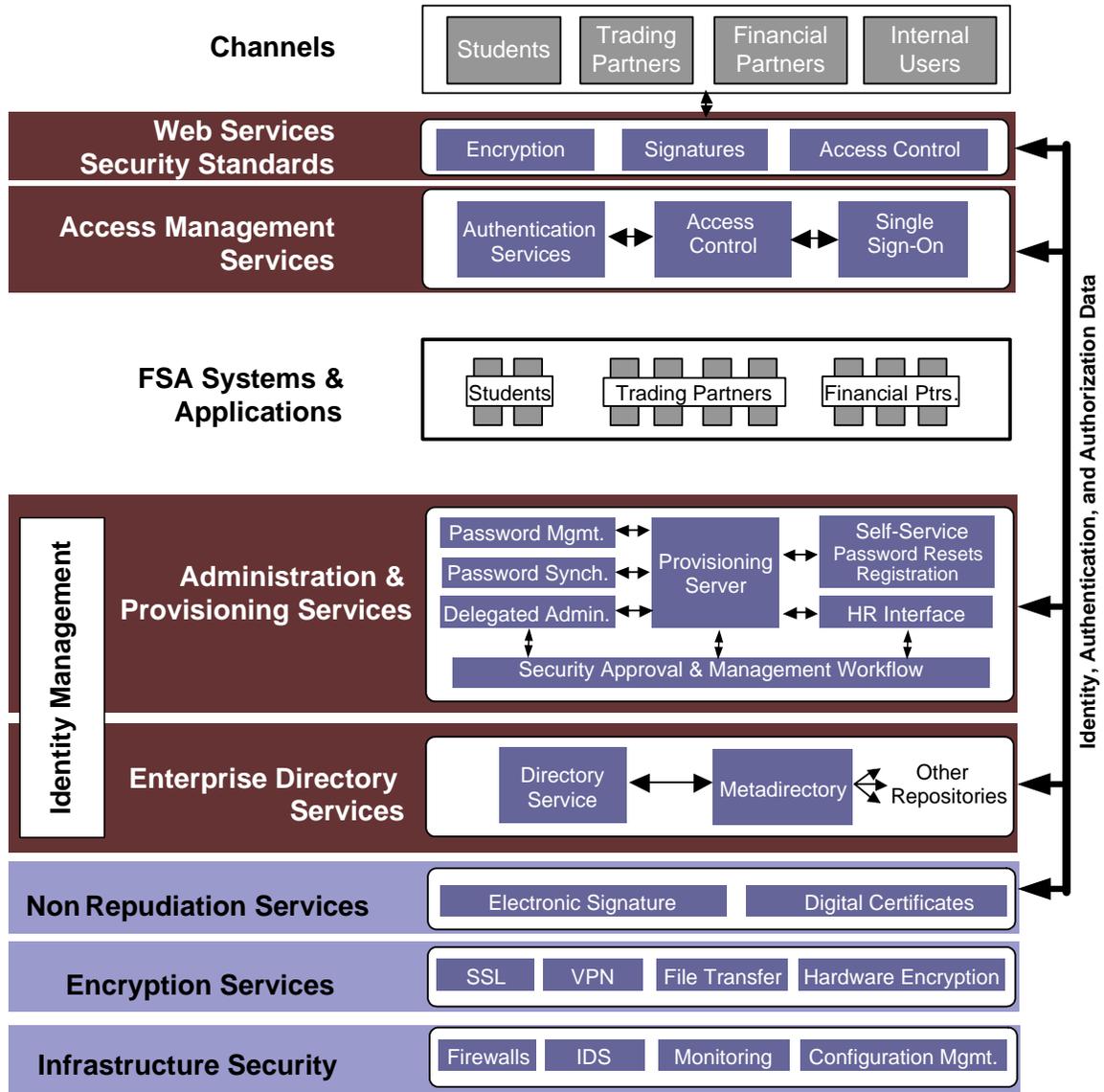


Figure 6.1. Revised FSA Security Architecture Vision diagram.

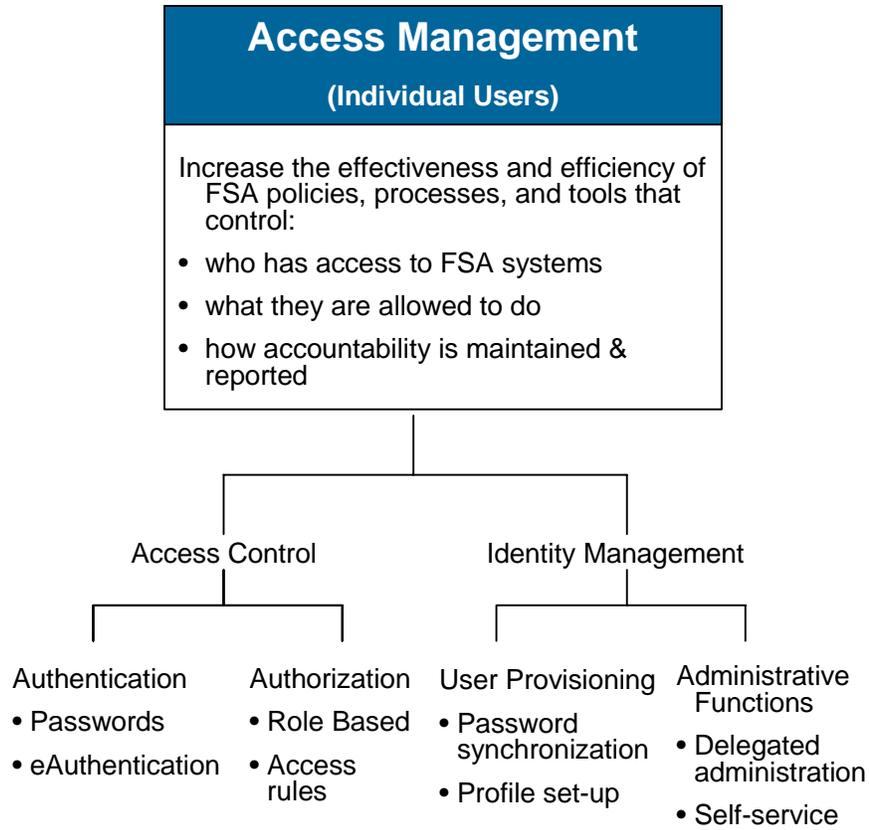


Figure 6.2. Diagram developed by the Enrollment and Access Management team to define security functions and project scope

6.2 Security Architecture Presentation for the Business Integration Group

A briefing was held for the FSA Business Integration Group on July 24, 2003. The purpose of the meeting was to summarize the results of the Security Architecture project, describe the next steps for deploying the FSA security architecture, and define the relationships between the security architecture effort and the Enrollment and Access Management work.

The presentation covered the following topics:

- Objectives for the Security and Privacy Architecture
- Summary of the Security and Privacy Architecture Vision
- Next steps
- Appendix A: Generic Application Security Functions
- Appendix B: Typical FSA Application Architectures
- Appendix C: Proposed Security Services

A copy of the complete Powerpoint presentation used in the meeting is included with this deliverable. In the electronic version of this deliverable, the presentation is included in the archive file as “BIG Briefing 7-24-3003”. In the printed version of this deliverable, the presentation is included as an addendum at the end of the document.

6.3 Meeting Notes for CDDTS Security Assessment

[As part of the security and privacy support being provided through this Task Order, as security assessment is being conducted for the Conditional Disability and Discharge Tracking System (CDDTS). The notes below summarize meetings held with the ACS personnel who operate CDDTS and staff the ACS Data Center.]

CDDTS Security Assessment Notes

Topic: Site Visit to Rockville ACS Data Center to review the security of the FSA Conditional Disability and Discharge Tracking System (CDDTS)

Date of visit: 7/17/2003

Attendees:

David Yang (FSA) – CDDTS SSO
Raj Raghu (ACS) – CDDTS Project Manager
Maylon Hayes (ACS)
Brian Kissel (ACS)
Michael Groover (ACS)
Abner Sangalan (ACS)
Ray Baker (ACS)

Documentation to be provided by ACS:

System Architecture description
Department of Education System Inventory
System Security Plan
Network Architecture
Operational Procedures
Previous Assessments/Audits (OIG report not available until October)

Topics Covered by Meeting Notes

- Purpose of Meeting
- History of CDDTS
- System Overview
- Data Inputs
- Operational Controls
- Physical Access
- Data Center Environmental Controls
- Disaster Recovery
- System Architecture
- Logical Access Controls
- Change Management Requirements
- Anti-Virus Controls
- Network Security
- Application Security
- Audit Log Management

- Data Center Walkthrough

Meeting Notes:

Purpose of Meeting

The purpose of the meeting was to collect information for a formal security assessment conducted on behalf of FSA. The security assessment will follow the published FSA Security Assessment Guideline. This meeting was the initial information-gathering session with ACS representatives responsible for operation of the data center that houses the CDDTS system.

History of CDDTS

The CDDTS contract was awarded in May 2002. The initial release of the system was in July 2002. There were two additional releases, with the last in October 2002, referred to as 'Phase III'. The system has been in 'operational/maintenance' mode since July 2002.

System Overview

CDDTS is a closed system used only by a limited number of personnel. No Department of Education users access the system. CDDTS functions are used primarily by representatives at the call center in Utica, NY. The network connection between the call center and the ACS Data Center is via ATM, and does not traverse the public Internet. The system consists of one production server and one test server. These servers are housed in a server environment within the ACS Data Center that also contains about 60 other Windows servers, all of which are devoted to FSA systems. An audit of this server environment was recently completed by the OIG. The audit primarily focused on DLSS. Although some audit findings have been communicated informally to ACS, and are being addressed, the OIG report will not be available until approximately October.

Data Inputs

CDDTS inputs may be in paper, tape, or electronic form. Electronic data is transmitted directly from the DLSS system, or via FTP. FTP files are received approximately once per week. Types of input data include promissory notes, medical certifications, payment information, and borrower applications. Paper documents are imaged and stored. Tapes will be stored a minimum of 45 days (see Data Center section for tape handling process). Data is loaded into the system (paper forms are entered by manual keying), then reviewed for errors and completeness.

Tapes are not used by any other system at the ACS data center that houses CDDTS. Tapes are processed by nightly CDDTS jobs. Tape data is loaded into a staging area and metarules are applied to validate the data. The process is checked the next morning by a dedicate ACS resource who is responsible for contacting the sender and obtaining corrections if required. After processing, the data is archived in a database on the server. System requirements call for retaining tape data at least 45 days, but the amount of data archived so far is relatively small and none of it has been removed yet. Currently the database holds records for about 27,000 loans, and each record contains about 1400 characters.

Operational Controls

Data tapes are initially shipped by Guarantee Agencies to the call center at Utica, New York. They are logged, and a transmittal form is prepared. They are shipped by UPS to the ACS location in Rockville, MD. When received, they are logged and transferred to the ACS data

center via inter-building courier. The tape librarian picks up the tapes from the tape drop box, loads them on the system, then secures them in the tape vault within the data center. Approximately one tape per day is received from Guarantee Agencies (GA). (There are total of 26 GAs.)

The CDDTS server is backed up weekly, with nightly incremental backups.

ACS services for CDDTS in the Washington, D.C. area consist of a hardware support group, network and system administration, database administration, and a production group. Other users who have access to the CDDTS server include data center personnel.

ACS is in the process of enhancing its written procedures in preparation for obtaining ISO9000 certification, but the procedures are not yet available. The operational procedures for CDDTS are the same as those for the DLSS system, except for the processes for handling CDDTS tapes.

The CDDTS production and development machines are Compaq servers. Compaq Insight Manager is the tool used to monitor the health and performance of the CDDTS server and to send alerts for abnormal situations. Network activity and performance is monitored with Cisco Works.

Security monitoring and security incident response is handled by the ACS Defense Division. This organization performs vulnerability assessments, including network and host scanning. Intrusion detection sensors are being deployed in some network segments (including the CDDTS environment?) and logs will be monitored daily when this function is fully deployed.

All personnel who work with CDDTS at ACS have at least a level 5c clearance. Managers must have a 6c clearance. Personnel are briefed on ACS security policy and procedures and proper use of systems as a part of their orientation. New users must submit an application for access to specific systems that must be approved by authorized managers. ACS has an email newsletter that provides security notices and information. A new security awareness program is being developed that will provide training and updates on security. This program is due to start on August 1. It will be a web-based program that takes 35-40 minutes to complete and will be required annually.

There is an ACS termination policy that defines procedures and checklists to define requirements for removing physical and logical access for employees and contractors that leave ACS. The termination process is overseen by the administrative group for contractors, and by managers for employees.

Physical Access

Access to the data center building is secured. There are guards who man a reception desk and patrol the building during the day, and periodically patrol the building at night. Access to the building at night, and to several defined building zones areas during the day, is controlled by electronic ID key cards and readers. When a new employee starts with ACS or changes job positions, their manager must submit an access request form which must be approved. The data center itself is in a limited access area. People without ID cards must call ahead to arrange entry. Vendors and other visitors must sign in at the front desk, and must justify their access

requirements, including the times of entry and exit. A video surveillance system covers both building entrances, as well as both doors into the data center.

The data center is physically manned 24 hours per day, seven days per week. CDDTS tapes are stored in the tape vault, a separate room within the data center. The vault is fireproof, and the door is shut, although not locked, during routine business hours.

Data Center Environmental Controls

There is a fire alarm and sprinkler system in the data center. The system is controlled from a central alarm panel near the guard station. The fire suppression system uses Halon, which will be converted to newer agents when replacement is required.

Air handler systems have alarms that monitor for high and low temperature conditions.

Power backup is provided by a UPS system consisting of a battery bank and a diesel generator. The system automatically switches to backup power when low voltage conditions are sensed, and the generator has an auto-start system. Transfer to battery power can occur within the millisecond range, and approximately 15 minutes of battery power is available to allow the generator to start.

The data center has a single location, and disaster recovery and disaster recovery services for a cold site are contracted through Sungard.

The data center was built especially for that purpose. The foundation and subfloor are recessed, so the raised floor is at the same level as the surrounding building areas. There are no overhead plumbing lines in the ceiling. Partition walls around the data center are full-height, and it is not possible to enter the data center through a suspended ceiling. The data center is not in a flood plain, and there is no significant history of hurricane damage in the area.

Disaster Recovery

The ACS disaster recovery plan is documented and has been provided to FSA. A copy will be provided as documentation for this assessment. The plan has not yet been tested. Testing of the plan is scheduled for mid-September. The test will use the Philadelphia, PA Sungard site. Business resumption facilities are located in Herndon, VA. Business continuity plans and procedures are included in the disaster recovery plan.

The disaster recovery plan defines procedures for recovering CDDTS from tape, including the installation of an Oracle database and the operating system. The production CDDTS is installed on a single server, and backup is through a cold stand-by machine. The disaster recovery plan specifies a 48 hour recovery time. There is a plan to migrate to a failover environment. A clustered server environment is being developed, and should be available before the end of August, which is before the planned disaster recovery test.

System Architecture

CDDTS runs on a Compaq server under Microsoft Windows 2000 Advanced Server.

CDDTS is not available only through intranet connections. It is placed in a network segment defined by a firewall that prevents direct access via the public Internet.

Database services are provided by Oracle 8i running on the same server as CDDTS.

Logical Access Controls

Login access to CDDTS is provided to the CDDTS project manager (to validate and fix problems) and to one person from the interface group. Database administrators have Oracle database accounts, but no login access to CDDTS. System operators and system administrators have operating system access, but do not have CDDTS accounts.

Change Management Requirements

CDDTS is currently in operational maintenance mode. There are no plans for major changes to the system. If major system changes become necessary, and upon submission of specific requirements to ACS, operational personnel will put together a change plan for approval. System development would take place in the CDDTS development environment. System code is managed using the Source Safe software management system. There is an established change management procedure for moving code from the development to the test environment, then to production. Separation of duties is enforced by having a different people responsible for moving code from development to testing and from the test environment to production. The production manager must approve all moves to the production environment.

The development environment is physically isolated from the CDDTS production environment, and sits on a separate network segment in the ACS data center. Access to the development environment is controlled with an access control list.

Hardware changes are controlled at the ACS data center. Changes are only implemented during a weekly change control window. Planned changes are published through a change control procedure to communicate them for management review. There are internal ACS requirements for approval by production representatives for all changes to systems, including network security and system patches or upgrades. A user conference call is held for data center users to inform them of planned changes. Operating system upgrades and patches are identified through a variety of sources, including hardware and network notices from vendors, CERT organizations, and the FSA security team. Notices from the FSA security team are usually sent as FSA directives for upgrades, and include time requirements within which the changes must be implemented. ACS analyzes production implications before installing patches or upgrades.

The Peregrine Service Center tool is used for management of systems in the data center.

Anti-Virus Controls

Norton anti-virus tools are used on administrator and developer workstations used for CDDTS. Currently, virus signature updates are installed manually. There is a plan to automate virus file updates, but the schedule is not yet finalized.

Security Operations

Responses to security incidents are coordinated by the ACS Security Officer in Elk Ridge. ACS will also use the security incident response methodology defined in the guidelines recently published by the Department of Education. The same monitoring and response procedures in place for DLSS are also used for CDDTS. Any security incidents that are identified are communicated to the FSA security team using the procedures by the Department Guidelines.

Network Security

Department of Education systems are on separate subnets defined by firewalls and routers within the ACS environment. Access control lists on the firewalls and routers limit traffic to authorized sources and destinations. All FSA development systems are also isolated from other ACS environments.

Network firewalls are deployed to protect the ACS environment perimeter, and are not used to protect individual systems.

Application Security

Authentication to CDDTS is by way of a user ID and password. System administrators require a separate user ID and password for access to the CDDTS operating system that is separate from authentication to the CDDTS system itself.

The system defines security roles for specific types of users.

Remote administration of CDDTS is performed from the Rockville ACS environment using PCAnywhere and Microsoft Terminal Services. About six people are permitted to log in remotely (i.e., from home or other external locations.) All remote administration connections are through a Shiva VPN site, which requires a separate login via a dial-up line or and Internet connection.

Audit Log Management

A log is kept for data collected by the intrusion detection system. IDS logs are viewed through a special console and are available only to the ACS security team through an SSH session. System logs for CDDTS up to now are being stored for one year on the server. This procedure is being modified. Security logs are monitored and reviewed for security-relevant issues by the ACS security team. Currently, audit logs are not archived off the server—this is not an FSA requirement. System logs are used primarily for troubleshooting. Audit logs are protected by the native Windows OS access controls for system logs.

Data Center Walkthrough (Conducted 7/17/2003)

The ACS Data Center in Rockville, MD is operated by a government unit of ACS.

The guard station at the main entrance to the ACS building that houses the Data Center is manned by a guard during the day, from 6:30 am to 6:30 pm. After hours, the site is also visited periodically by a guard. Access control at other times is enforced via an electronic ID card and reader.

The ACS Data Center building is not marked externally as a data center location. The lobby to the building has glass doors and plate glass windows. Entry doors, the loading dock, and the parking areas around the building are covered by a video surveillance camera. There are separate doors to the two entrances to the Data Center area itself, which is positioned toward the rear of the building near the loading docks and a parking area. There are no other buildings immediately behind the data center side of the ACS facility. None of the Data Center doors lead directly to the exterior of the building.

The Data Center is manned continuously. A separate Data Center area badge is required for entry. All ACS personnel and other visitors to the Data Center must sign in at the Data Center entrance, wear a visitor badge, and be escorted by Data Center personnel.

There are no plumbing lines that run through the ceilings. Walls extend the entire distance from the floor to the solid ceiling.

Fire controls consist of a Halon fire suppression system that is kept full and checked periodically. The control panel for the fire control system is within the Data Center.

Data tapes received by the Data Center are logged in a notebook—the format, number of records, date, and time are recorded. Tape data is loaded onto the disk in CDDTS. If successful, an email message is sent to the interface group to report the nature of the data and the outcome. There is also a daily operations report that describes the number of records and the outcome of the processing. Tapes are stored in the tape vault until they are approved for destruction via bulk degaussing. When destroyed, a transmittal form will be submitted to the sender. At present, the standard is to keep tapes for at least 45 days. Data taped returned to a sender is also logged. The Data Center has some off-site storage for tapes, but because of the relatively low volume, none of the CDDTS tapes are stored there. The tape vault provide fire protection, and is in a secure area within the data center, although it is not locked during periods of use. The tape vault is also protected by the Halon fire suppression system. When the current Halon system needs to be recharged, an approved replacement agent will be used.

The production CDDTS server is in an unlocked equipment rack near the center of the Data Center space. The Data Center is manned 24 X 7 with a minimum of two people. IDS sensors provide network and security monitoring for the Data Center network. Firewalls and routers for the ACS network are also housed in the Data Center, and all connections for network access, including both voice and data communications, enter the Data Center. Network devices connect to a Cisco 6509 switch, which is connected to redundant ATM routers with service carried by MCI. There are two different ATM hubs: the primary is in Baltimore, MD, and the secondary is in Washington, D.C. Local network loops and routers are redundant, with two routers in place set up for cold fail-over. Network routers are configured with access control lists to limit traffic to approved trading partners. Network firewalls are a combination of Cisco PIX and Checkpoint Firewall-1 devices. The service agreement with Cisco provides for a four-hour response time.

Backup for the CDDTS server is now a warm backup server. A new server is being built for CDDTS to allow integration with a distributed server configuration. A separate room houses the battery-powered backup electrical supply system, which connects to all Data Center equipment. There is battery capacity for at least 30 minutes, and there is a sensor system that detects power fluctuations and automatically switches Data Center power over to the UPS. A diesel generator, located outside the building near the loading dock, is configured to start automatically. The generator has a 500 gallon fuel capacity, enough to run continuously for at least three days.

The Data Center has a monitoring console area that provides oversight for Data Center operations. On-call staff can be contacted through email and pagers when alerts require a response.

The CDDTS server is Windows 2000 Enterprise Server running service pack 3. The Oracle database runs on the CDDTS server and is version 8i. CDDTS application code is written in VisualBasic, and uses COM objects, HTML pages, and Active Server Pages.

There are three doors into the Data Center area. All doors are locked and require electronic keys with Data Center access privileges to enter the Data Center unaccompanied. A printer room is connected to the Data Center, and a mailbox with an unlocked outer door and no inner door is used to pass data tapes to Data Center personnel.

The backup diesel generator and fuel tank is behind a locked door within an external, open-topped brick enclosure approximately 10 feet high. Major maintenance on the generator is performed every two years. Power distribution lines to the Data Center run underground. The fuel tank is double-walled and has a 3000 gallon capacity. The UPS battery capacity is at least 15 minutes at full load. The UPS and generator system are tested formally every two years, but informally more often. During periods of possible power disruption, such as when severe thunderstorms approach the area, the generator may be started as a contingency measure.