



F E D E R A L
S T U D E N T A I D

We Help Put America Through School

accenture

High performance. Delivered.

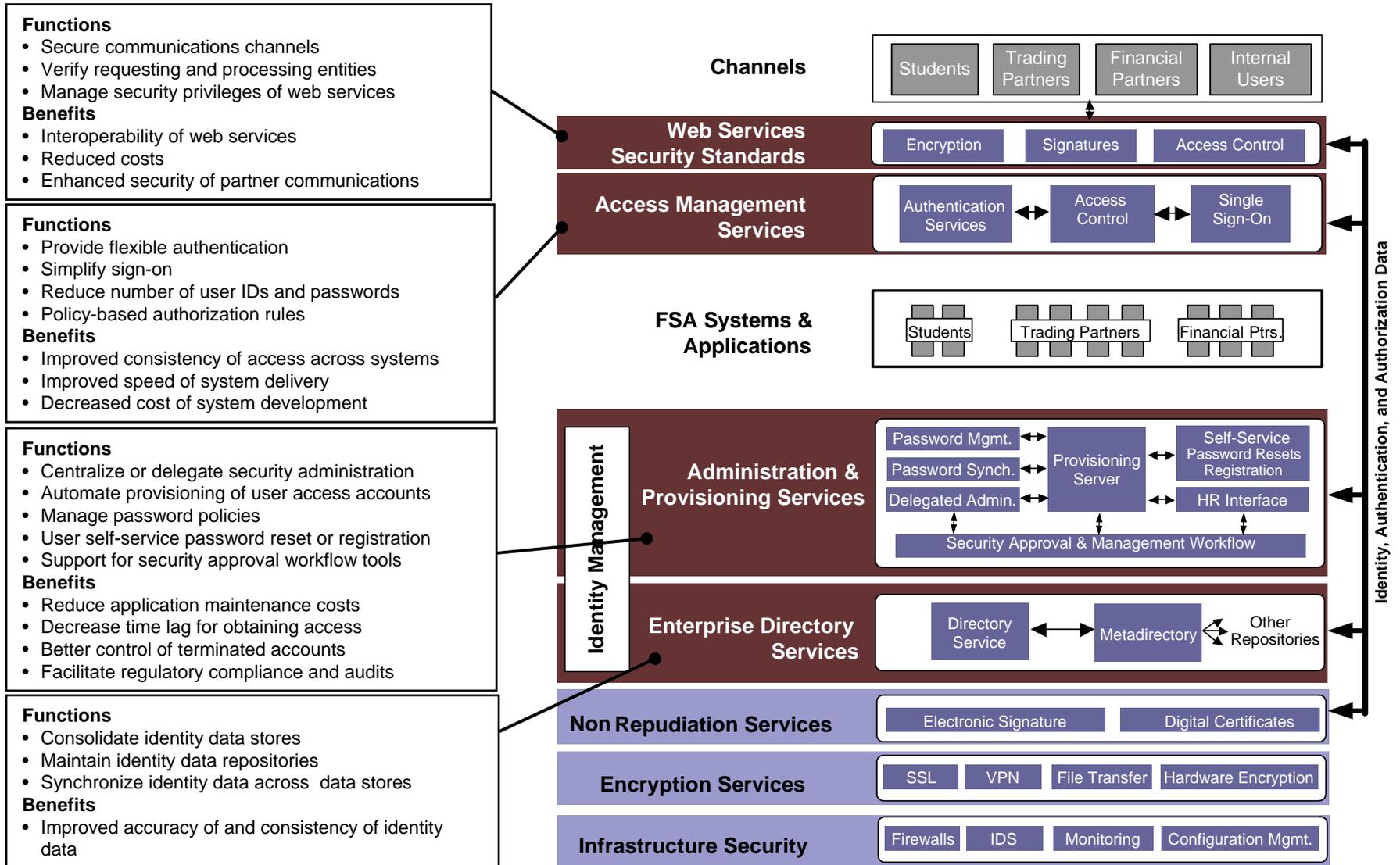
Integration Partner Transition Security Architecture Briefing

May 2004

Project Overview

- FSA Security Architecture Projects have developed architecture descriptions and performed analysis of security architecture technologies. The overall goal is to develop security infrastructure components that allow FSA to comply with security and privacy standards while offering improved user services.
- Security architecture work has involved three related efforts conducted over the past year:
 - Security and Privacy Architecture Development (TO 124) created a generic security and privacy framework, an FSA Security and Privacy Technical Architecture Specification, and Security and Privacy Architecture deployment recommendations.
 - Enrollment and Access Management (a sub-project of Data Strategy, TO 123) identified business objectives and high-level requirements for trading partner enrollment procedures, user authentication, and access controls.
 - Identity and Access Management Tools Analysis (TO 143) selected software tools for user authentication, access control, and account administration. Selected tools (Tivoli Identity Manager and Tivoli Access Manager) were installed as a proof-of-concept system in the FSA Virtual Data Center development environment and integrated with the Ez-Audit application.

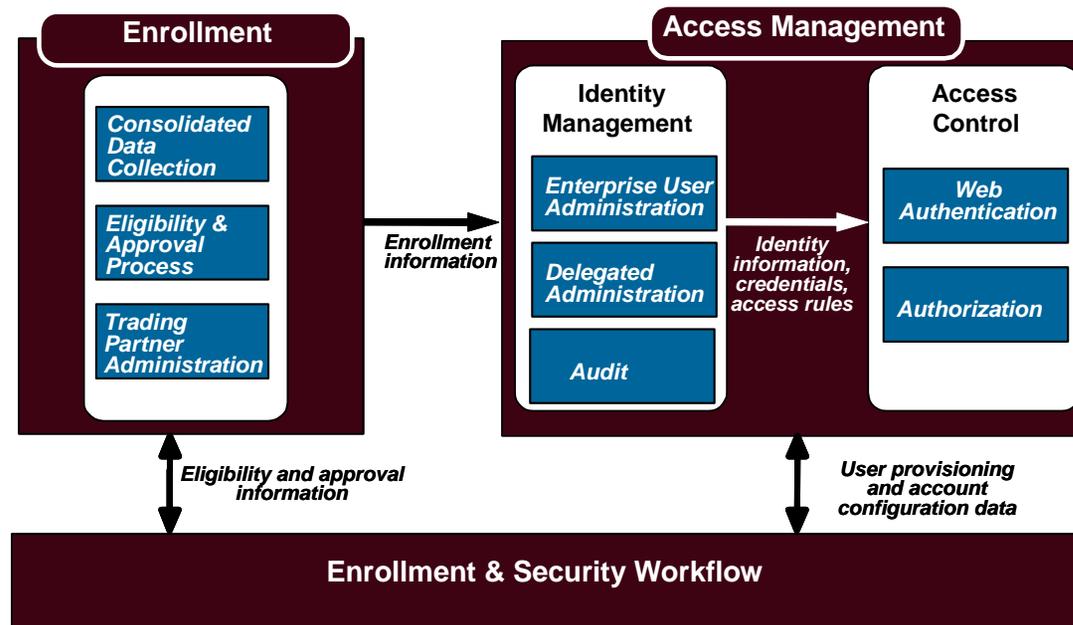
FSA Security & Privacy Architecture



Project Owners

- FSA project managers:
 - Srinik Kankanahalli, 377-3361, srinik.kankanahalli@ed.gov
 - Robert Ingwalson, 377-3563, robert.ingwalson@ed.gov
- CIO Sponsors
 - Ganesh Reddy, 377-3557, ganesh.reddy@ed.gov
 - Keith Wilson, 377-3591, keith.wilson@ed.gov
- Business Sponsor
 - Paul Hill, 377-4323, paul.hill.jr@ed.gov

Business Functions



The Identity and Access Management components of the FSA Security Architecture provides benefits for both FSA and its Trading Partners.

Business Functions

- **For FSA, the solution provides:**
 - 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.
- **For FSA Trading Partners, the solution provides:**
 - 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.

Relationship to FSA's Strategic Goals

Strategic Goal	Applicable to Project?	If yes, why?
Modernize & Integrate Systems	Yes	The security architecture will integrate and improve security functions across multiple systems.
Improve Program Integrity	Yes	The security architecture will consolidate and standardize access control and data integrity protections.
Reduce Costs	Yes	Identity management functions in the security architecture will decrease administrative costs.
Improve Products & Services	Yes	Single sign-on and delegated administration will improve user access to FSA systems.
Improve Human Capital	Yes	Security training will be part of the security architecture deployment.

Relationship to FSA's 'Big Picture'

- The overall FSA Security and Privacy Architecture provides an important tool for the design and deployment of controls to provide effective and efficient protections for FSA systems and data. The architecture can be used:
 - As a guide for security strategy and planning
 - As a security design and deployment aid to promote structured, systematic, and repeatable planning and development of security and privacy controls
 - To communicate technical standards and decisions, both internally and externally
 - To capture successful and proven security solutions for future use
- The Identity and Access Management components of the FSA Security and Privacy Architecture will provide:
 - Consistent security services (for authentication, authorization, user administration, and auditing) across FSA systems
 - Improved access for FSA users and trading partners with lower administrative costs
 - Compatibility with developing security standards for federated identity and compliance with federal eGov initiatives

Delivery Process

- The Security Architecture team has been working closely with FSA CIO security personnel and System Security Officers to plan and execute project tasks
- Periodic workshops and briefings have been held to collect requirements, communicate progress, and obtain feedback on project recommendations
- Deliverables for Security Architecture projects have used the standard deliverable creation and submission processes

Project Schedule

- TO 124 – Security and Privacy Architecture Framework: Started March 2003, Completed May 2003
- TO 123 – Data Strategy / Enrollment & Access Management: Started April 2003, Completed November 2003
- TO 143 – Identity and Access Management Tools Analysis: Started December 2003, Completion Due May 2004

Project Deliverables

- Deliverables from Task Order 124 – Security and Privacy Architecture Framework (all completed)
 - 124.1.1 – Interim Security and Privacy Architecture Report
 - 124.1.2 – Final Security and Privacy Architecture Report
 - 124.1.3 – Security and Privacy Architecture Framework Specification
- Related deliverables from Task Order 123 – Data Strategy (all completed)
 - 123.1.26 – Enrollment Business Objectives and High-Level Requirements
 - 123.1.27 – Access Management Business Objectives and High-Level Requirements
 - 123.1.28 – Enrollment High-Level Design
 - 123.1.29 – Access Management High-Level Design
- Deliverables from Task Order 143 – Identity and Access Management Tools Analysis
 - 143.1.1 – Identity and Access Management Tools Vendor Analysis (completed)
 - 143.1.2 – Identity and Access Management Tools Recommendations (completed)
 - 143.1.3 – Identity and Access Management Tools Prototype (in progress)

Next Steps

- Plan deployment of identity and access management services
- Procure licenses for identity management and access management components
- Deploy identity and access management infrastructure components
- Integrate FSA systems and applications with identity and access management components
- Plan development of additional Security and Privacy Architecture components, e.g., data privacy services, patch management services, centralized encryption services