

FSA Modernization Program
United States Department of Education
Federal Student Aid



Single Sign-On
Requirements Definition – DRAFT

Task Order #82
Deliverable #82.1.3

FINAL

March 5, 2001

Document Revision History

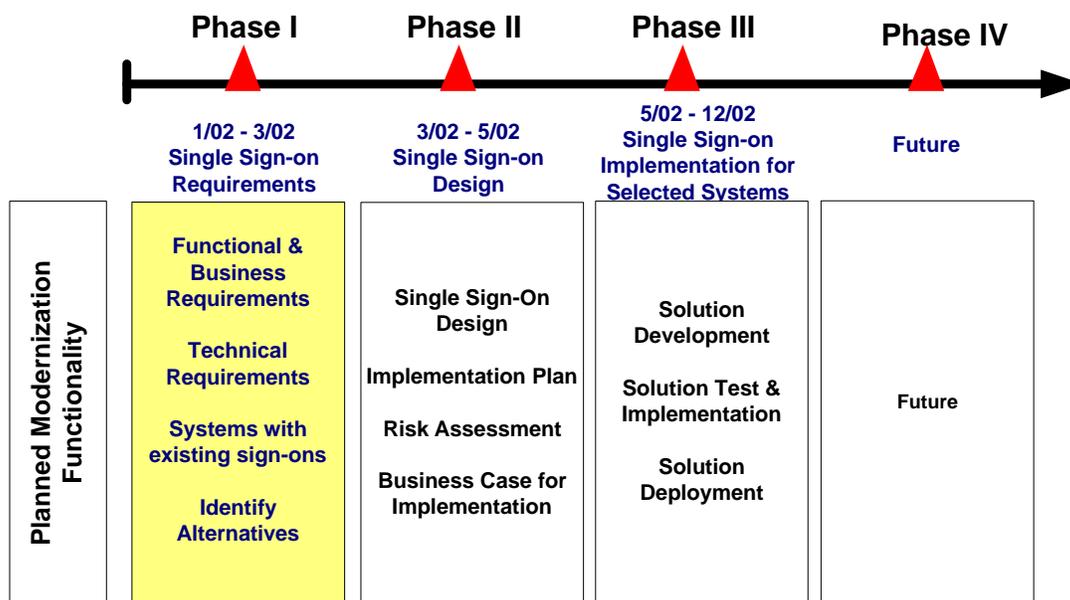
Version No.	Date	Author	Revisions Made
1.0	February 15, 2002	Michael Bruce	Initial draft released
1.1	February 22, 2002	Michael Bruce	Revised draft released
1.2	March 5, 2002	Michael Bruce	Draft Final Requirements Definition
1.3	March 8, 2002	Single Sign-On IPT	Final document to be released by Single Sign-On IPT

Table of Contents

EXECUTIVE SUMMARY	1
1 INTRODUCTION.....	3
BACKGROUND.....	3
PURPOSE	3
SCOPE	3
DOCUMENT REFERENCES.....	4
ORGANIZATION OF THIS DOCUMENT.....	4
2 TARGETED USERS	5
3 REQUIREMENTS.....	6
REQUIREMENTS TRACEABILITY MATRIX	7
1. Authentication and Identification.....	7
2. User Management.....	11
3. Session Management.....	17
4. Access Management.....	18
5. Customer Care.....	26
6. Legal	27
7. Environment.....	29
8. Operations.....	33
9. ISO/IEC 15408 Security / Common Criteria.....	36
4 POTENTIAL ALTERNATIVES.....	43
A. CUSTOM DEVELOPED SINGLE SIGN-ON SERVICE	43
B. SINGLE SIGN-ON BY ENHANCED CURRENT FSA CAPABILITY	43
C. COTS ENABLED SINGLE SIGN-ON SERVICE	44
D. SINGLE SIGN-ON SERVICE FROM A MANAGED SERVICE PROVIDER	45
APPENDICES.....	46
APPENDIX A: IPT TEAM.....	47
APPENDIX B: ACRONYMS AND ABBREVIATIONS	48
APPENDIX C: FSA LOGIN/ACCESS SURVEY RESULTS AND SUMMARY.....	49

Executive Summary

This document identifies business and technical requirements for a Federal Student Aid (FSA) Single Sign-On service, compiled and recommended by an enterprise IPT and IPT advisory team. This constitutes Phase I of the Single Sign-On effort. These requirements were compiled as a result of interviews conducted within FSA, industry and market research, and past efforts related to Single Sign-On services. The requirements include ED, FSA, NIST, ISO, and “best in industry” guidance. The following picture illustrates the overall Single Sign-On effort:



These requirements will serve as the basis for Phase II, i.e., selection, design, implementation plan, and business case for an FSA Single Sign-On service, as approved and to be funded by the FSA IRB upon agreement by FSA business channel general managers.

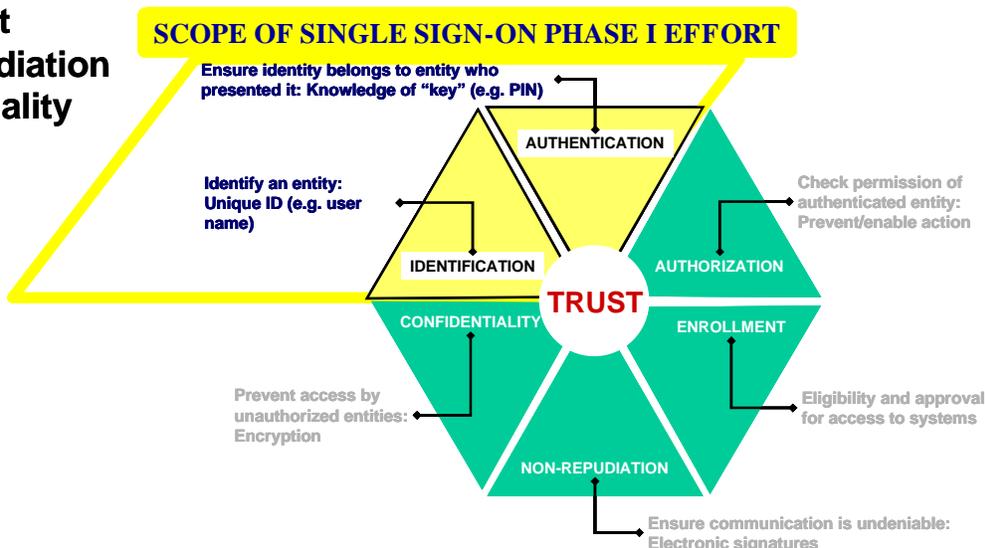
The **business drivers** for a Single Sign-On service at FSA are:

- Improve customer access to FSA Systems – provide a **Common** user identifier
- Strengthen Cyber-Security – provision a **Trusted** user identifier
- Establish a **Reusable** Single Sign-On service for FSA business systems
 - Existing FSA system users have multiple logins/passwords
 - Modernization and integration efforts will implement additional logins without Single Sign-On services

The **scope** of this Phase I effort is to identify requirements for Identification and Authentication. The scope does not include the areas of Authorization, Enrollment, Non-repudiation, and Confidentiality.

Phase I IPT Scope does not include:

- **Authorization**
- **Enrollment**
- **Non-Repudiation**
- **Confidentiality**



The effort has resulted in the following:

- Assessment of 39 current and future FSA business systems for login and access needs
- Identification of 26 unique usernames for FSA business systems:

1. COD Login	9. EDNet User ID	18. IAM Username
2. Pell ID + TG Number	10. DMCS/FFEL Username	19. CPS UserID
3. TG (TIVWAN) Number	11. OPEID	20. NSLDS UserID
4. DLO Login ID	12. OPEID + TIN (Taxpayer Identification Number)	21. OCTS Username
5. DSLS Login ID	13. ERM Username	22. PEPS Username
6. DLSS Username	14. FMS Username	23. Social Security Number
7. DLCS Login ID	15. GAPS UserID	24. Schools Portal username
8. FSA PIN (SSN, first 2 letters of last name, DOB, PIN)	16. Jamcracker UserID	25. Student Portal Username
	17. IFAP Username	26. FP Portal Username

The Requirements in Section 3 of this document represent the needs of an enterprise identification and authentication capability as defined by FSA. The requirements incorporate current technologies and access implementation at FSA. The requirements are scalable to accommodate technology advances, and future government and industry standards.

1 Introduction

Background

As part of its commitment to customers and partners, FSA manages risk on a continuous basis. In view of this, FSA recognizes that there is a need to provide system access controls that enhance a user's online experience allowing for a closer relationship to FSA and greater reliance upon FSA services and applications. At the same time access services must adhere to FSA identification and authentication policies, and U.S. Public Law and policy.

Currently, system users may utilize multiple access credentials to logon to FSA systems. This places the unnecessary burden on users of having to remember multiple username/password combinations. Approximately 25,000 School and Financial Partner users access FSA systems on a regular basis as part of regular student financial aid processing and administration. Over 23 million Students have on-line access to FSA systems in order to complete FAFSA submissions and conduct other student aid related business.

In addition, as new and reengineered systems are released, additional access credentials and rights may also be created. This could create increasing opportunities for unauthenticated access to FSA systems, undermining the credibility of FSA, and affecting its ability to help put America through school. To reduce the risk inherent in multiple access points, a Single Sign-On service is being considered.

Purpose

The purpose of this task is to define the enterprise requirements for the development of a Single Sign-On service for FSA systems. The key objective of this document is to:

- Capture and document the requirements that apply to the design, implementation, and operation of a Single Sign-On service for FSA system users and administrators

Scope

This document defines the business and technical requirements for a Single Sign-On service for FSA systems. The requirements were gathered by an enterprise IPT, and included past Single Sign-On studies, discussions with channel stakeholders, market research, and interviews with FSA staff. The IPT leveraged guidance from the Single Sign-On advisers throughout the process.

It is anticipated that an FSA Single Sign-On service can provide the following benefits:

- Improved customer access to FSA systems – [Common](#) Identifier
- Support the access needs for FSA's Portals and overall eCommerce strategies
- Strengthened cyber-security – [Trusted](#) Identifier
- Establish a [Reusable](#) Single Sign-On service for FSA systems
- Provide potential future economic [Savings](#):

- System enrollment
- User access management
- Reduced customer support for login

The scope of this Phase I effort is to identify requirements for Identification and Authentication. The scope does not include the areas of Authorization, Enrollment, Non-repudiation, and Confidentiality.

Document References

The following documents were used in establishing the requirements for the Single Sign-On initiative:

- RFI for Single Sign-On Software, Department of Education, Student Financial Assistance, July 2001
- Single Sign-On Requirements Analysis for DLOS, June 14, 2001.
- OMB Circular A-130, Appendix III
- Common Criteria v2.1 (ISO: IS15408), September 2000
- NIST Special Publication 800-18, December 1998
- RFI response review, TO59, August 31 2001
- Statement of objectives – Single Sign-On Requirements and Design
- Business Case, Single Sign-On Requirements and Design

Organization of this Document

The following information outlines the organization of this document:

- **Executive Summary**
- **Section 1³/₄ Introduction** provides an overview of Single Sign-On task.
- **Section 2³/₄ Targeted Users** provides a list of the targeted users of the Single Sign-On service.
- **Section 3³/₄ Requirements** represents the business, functional and technology needs for an FSA Single Sign-On service in the form of a traceability matrix.
- **Section 4³/₄ Potential Alternatives** are high-level alternatives of possible Single Sign-On designs for FSA.
- **Appendix A – IPT List** identifies the individuals involved in completing and reviewing this requirement definition document, and includes IPT members, advisers, and management sponsors.
- **Appendix B - Acronyms and Abbreviations** contains definitions for key acronyms and abbreviations used in this documents and within the FSA environment.
- **Appendix C – FSA Login/Access Matrix** contains the results of the FSA login/access survey data collection, and a summarization across 45 FSA and ED current and planned systems.

2 Targeted Users

The Single Sign-On service is directed to external as well as internal users and administrators. Upon deployment of Single Sign-On, these users will be able to access systems from FSA portals with a single set of user identification/authentication credentials (e.g., User-id and Password).

The following table identifies targeted users:

User	Description
Students	
Students	User of FSA systems
Parents	User of FSA systems
Schools	
School Financial Aid Staff	User of FSA systems
Bursar's Office	User of FSA systems
Registrar	User of FSA systems
President's Office	School executives
Destination Point Administrator	Designated School employee to administer school-only access to FSA systems for school staff
Third Party Servicers	User of FSA systems on behalf of Schools
Financial Partners	
Lenders	User of FSA systems
Secondary Markets	User of FSA systems
Guaranty Agencies	User of FSA systems
Servicing Agencies	User of FSA systems
Access Administrator	Designated Financial Partner employee to administer financial partner-only access to FSA systems for financial partner staff
Special Interest Groups	
Congress	User of FSA systems
Trade Associations	User of FSA systems
ED/FSA Staff and Contractors	
FSA System Security Officer	Provide access to a particular FSA system for all internal and external users
FSA System Manager	Manage overall operations, including access, to a particular FSA system for all internal and external users
FSA Staff	FSA employees granted access to FSA business systems
ED Staff	ED employees granted access to FSA business systems
Higher ED Authorities	Higher ED employees granted access to FSA business systems
Contractor/Operating Partner Support Staff	Support staff to add users to a particular FSA system for all internal and external users.

3 Requirements

The requirements are divided into various sections, each focusing on an area representing a set of related requirements. All the requirements in this document are presented in a uniform and traceable format. The fields in the traceability matrix are defined in the **example** below:

Identifier	Unique identifier (i.e., number) for each requirement.	
Title	Short description of the requirement.	
Description	Description of the requirement.	
Source	The origination source of the requirement. Sources include: FSA Login/Access Survey, Official Sources (e.g., ED OIG, OMB, NIST, etc.), and Best Industry Practice (i.e., requirements derived from successful Single Sign-On implementations).	
Assumptions	Any specific assumptions made for this requirement (e.g., business channels to which the requirement applies, noteworthy consequences of this requirement and dependency of this requirement on others not in the scope of this project for fulfilling the requirement in its entirety).	
Sub-requirements	Identifier Number + Number	ID and short description of sub-requirements of the present requirement. Sub-requirements represent detailed implications or further refinements of the broader requirement. The identifier is in the form <requirement id>.<number>, where number starts from 1.

Requirements Traceability Matrix

The following presents the requirements for a Single Sign-On service to support FSA systems.

1. Authentication and Identification

Identifier	1.1	
Title	Support username formats as required by FSA business units	
Description	Ability to implement user name syntax rules, defined by FSA.	
Source	FSA Login/Access Survey	
Assumptions	This enables the Single Sign-On application to utilize current and future user name formats.	
Sub-requirements	1.1	Support a minimum username length of 1 character
	1.2	Support a maximum username length of 256 characters
	1.3	Support use of the FSA-PIN Username (i.e., SSN, Date of Birth, First two letter of last name)
	1.4	Support use of the EDNet Username
	1.5	Support syntax rules that allow the following elements to be incorporated into usernames: <ul style="list-style-type: none"> • First Initial of First Name • Last Name • Office Code • OPEID • FSA PIN Username (SSN + First two letter of Last Name + DOB) • Defined numeric value • Two or more data elements

Identifier	1.2	
Title	Support password formats as required by FSA business units	
Description	Ability to implement password syntax rules, defined by FSA.	
Source	FSA Login/Access Survey	
Assumptions	This enables the Single Sign-On application to utilize current and future password formats.	
Sub-requirements	1.2.1	The service should include features to translate unlike User Login Information from different platforms.
	1.2.2	Support a minimum password length of 1 character
	1.2.3	Support a maximum password length of 256 characters

	1.2.4	Support use of the FSA-PIN “Password” (i.e., 4-digit number generated by the FSA-PIN service)
	1.2.5	Support use of free-format Passwords
	1.2.6	Support syntax rules that allow the following elements to be incorporated into passwords: <ul style="list-style-type: none"> • Alphanumeric values • Alpha-only values • Numeric-only values
	1.2.7	Support rules that enforce the following capabilities: <ul style="list-style-type: none"> • Password lifetime from 30 to 120 days • Unlimited password lifetime • Comparison to previous passwords for the user • Disabling of the account after a period of inactivity of 90 to 365 days
	1.2.8	Store passwords in an encrypted state in the credential repository

Identifier	1.3	
Title	Support ED password syntax rules and management rules	
Description	Ability to adhere to ED password policies	
Source	ED OIG	
Assumptions	Adherence to ED policy guidelines.	
Sub-requirements	1.3.1	Support a minimum password length of 8 characters
	1.3.2	Support syntax rules that enforce at least three of the following conditions on every password: <ul style="list-style-type: none"> • Uppercase alphabetic characters (A-Z) • Lowercase alphabetic characters (a-z) • Numeral values (0-9) • Non-alphabetic and non-numeric characters (< ! @ # etc.)

	1.3.3	<p>Support rules that enforce the following capabilities:</p> <ul style="list-style-type: none"> • Password expires on the first logon attempt for a new user • Current user passwords expire and must be reset after 90 days • Password uniqueness set to 12 - i.e., systems stores and recalls past 12 passwords • Automatic account lockout after 3 unsuccessful login attempts • Set Account Lockout button • Automatic lockout duration set to 30 minutes • Unsuccessful login counter reset to 0 from 3 after 30 minutes
--	-------	---

Identifier	1.4
Title	Display User Data
Description	The Single Sign-On service should allow the display to an end user of user data.
Source	Best In Industry
Assumptions	None

Identifier	1.5	
Title	Centralized user authentication	
Description	Centralize user authentication across Single Sign-On enabled business applications.	
Source	Best In Industry, CIO Requirements Review	
Assumptions	Portals and applications must be capable of delegating user authentication to the Single Sign-On service, either explicitly or by allowing for logon emulation.	
Sub-requirements	1.5.1	Communicate to Single Sign-On enabled business applications identification and authenticated user information.
	1.5.2	Be able to perform logon emulation to Single Sign-On enabled business applications.

Identifier	1.6 (Technical)	
Title	Authentication Mechanism	
Description	The authentication mechanism must be configurable and extensible.	
Source	Best In Industry, CIO Requirements Review, CIO-Security Requirements Review	
Assumptions	None	
Sub-requirements	1.6.1	Provide standards based API (Plug-able Authentication Modules - PAM) to allow for additional authentication mechanisms.
	1.6.2	Provide Username/Password authentication module.
	1.6.3	Provide Username/PIN authentication module.
	1.6.4	Based on the risk, different groups may utilize different authentication methods.

2. User Management

Identifier	2.1	
Title	Access rules administration	
Description	Provide a mechanism for a privileged administrator to change access rights of individuals or groups.	
Source	FSA Login/Access Survey, CIO Requirements Review	
Assumptions	None	
Sub-requirements	2.1.1	Administrator changes will be logged and audited
	2.1.2	Logon required to access user data.
	2.1.3	Provide capabilities to administer – <ul style="list-style-type: none"> • Passwords • User names • User data • Session management
	2.1.4	Provide a display for administrators to view access rights and privileges of all users.
	2.1.5	Real-time user status monitoring and user management.
	2.1.6	Allow access control rules to include configurable conditions based on data from multiple data sources.

Identifier	2.2	
Title	Username and Password Generation	
Description	Provide the capability to create usernames and passwords or accept usernames and passwords created by trusted sources.	
Source	FSA Login/Access Survey, EAC Focus Group	
Assumptions	None	
Sub-requirements	2.2.1	Usernames will adhere to FSA username syntax rule
	2.2.2	Allow users or system administrators to manually create user names
	2.2.3	Passwords will adhere to FSA password syntax rule
	2.2.4	Allow for the use of the FSA PIN – user name
	2.2.5	Allow for the use of the FSA PIN as the authentication credential
	2.2.6	New users of the Single Sign-On service must change the system or administrator created password upon initial login, except when the FSA PIN is used to authenticate a user.

	2.2.7	Allow the Single Sign-on service to generate new target systems passwords for users.
--	-------	--

Identifier	2.3	
Title	Ability to Group Users	
Description	The service should enable the grouping or categorization of like users where able. These groups should be handled the same way individual users are handled.	
Source	Best In Industry/Access Survey	
Assumptions	This will enable more efficient administration of access authority.	
Sub-requirements	None	

Identifier	2.4	
Title	Single Sign-On User Credential Store	
Description	Provide the capability to communicate Single Sign-On user credentials to existing FSA user credential repositories	
Source	FSA Login/Access Survey	
Assumptions	None	
Sub-requirements	2.4.1	ODBC Database (Oracle, SQL Server, Informix)
	2.4.2	RACF
	2.4.3	NT Network
	2.4.4	FSA PIN Service
	2.4.5	Directory (LDAP v3)
	2.4.6	Oracle Financials ERP

Identifier	2.5	
Title	Delegated administration	
Description	Allow for delegated administration of access policies and functions for an application or a set of applications to appointed administrators granted limited administration and management rights.	
Source	Best In Industry, CIO Requirements Review, Schools Requirements Review	
Assumptions	None	

Sub-requirements	2.5.1	A privileged administration interface must be widely accessible from the FSA Intranet or the internet.
	2.5.2	Provide a graphical interface for administrators.
	2.5.3	Provide remote access capabilities for administrators.
	2.5.4	Provide integration capabilities to Call Center technologies via APIs, web-link, or other mechanisms.
	2.5.5	Provide an administration interface for administrators.

Identifier	2.6	
Title	User data elements	
Description	Store user data	
Source	FSA Login/Access Survey	
Assumptions		
Sub-requirements	2.6.1	First Name
	2.6.2	Last Name
	2.6.3	Last four digits of the users social security number
	2.6.4	Telephone contact number

Identifier	2.7 (Technical)	
Title	User setup	
Description	The Single Sign-On solution must allow for flexible creation of usernames.	
Source	Best In Industry	
Assumptions	None	
Sub-requirements	2.7.1	User data is stored electronically
	2.7.2	Username creation is automated.
	2.7.3	Username creation is based on definable rules (i.e., length, character set, words, and names).
	2.7.4	Initial password generation is automated.
	2.7.5	Initial password generation is based on definable rules (i.e., length, character set, words, and names).
	2.7.6	Initial password is communicated securely to the user.
	2.7.7	User is forced to change initial password at first login.
	2.7.8	A batch registration of users must be offered.

Identifier	2.8 (Technical)	
Title	User revocation	
Description	The Single Sign-On solution must allow for immediate and automatic revocation of users.	
Source	Best In Industry, FSA Login/Access Survey	
Assumptions	None	
Sub-requirements	2.8.1	A Single Sign-On administrator must be able to revoke Single Sign-On access for a user to any FSA systems within the administrator's domain.
	2.8.2	The process of revocation of a user must be automatic, once invoked by the administrator.

Identifier	2.9 (Technical)	
Title	Temporary disabling of user accounts	
Description	The Single Sign-On solution must allow for the option to disable accounts based on inactivity, definable number of unsuccessful login attempts.	
Source	Best In Industry	
Assumptions	None	
Sub-requirements	2.9.1	If a user does not login for a specific time, users account is disabled. The timeframe must be configurable.
	2.9.2	If an account encounters multiple failed login attempts, it must be disabled after a configurable number of failed attempts.
	2.9.4	The Single Sign-On must allow disabling a user account for an unlimited timeframe.

Identifier	2.10 (Technical)	
Title	Password administration	
Description	Password administration must be automated and only require minimal manual interaction with the Single Sign-On administrator.	
Source	Best In Industry, FSA Login/Access Survey	
Assumptions		
Sub-requirements	2.10.1	Users who have forgotten their password must request a new password by answering one or more free definable challenge questions.
	2.10.2	Users wanting to change their password must do this by providing their old password and/or answering one or more free definable challenge questions.
	2.10.3	User is limited to a configurable number of password changes per day.
	2.10.4	A user must get a confirmation of a password change.
	2.10.5	Challenge questions must be configurable to rotate.
	2.10.6	Challenge questions are based upon data stored in the Single Sign-On user data store.

Identifier	2.11 (Technical)	
Title	Single Sign-On user credential(s) creation	
Description	Single Sign-On user credential(s) are subject to definable quality standards.	
Source	Best In Industry, FSA Login/Access Survey	
Sub-requirement	2.11.1	Provide the ability to check for weak credentials based on definable syntax rules (i.e. Minimum password length, combination of number and letters, etc.).
	2.11.2	Provide the ability to check for weak credentials based on dictionaries.
	2.11.2	Single Sign-On user credentials must have a definable lifetime. A warning message must be provided at a definable time before a credential is going to expire.
	2.11.3	A definable number of credentials used before must be stored. (e.g. Do not allow repeating passwords)

Identifier	2.12 (Technical)	
Title	Single Sign-On User Credential Storage	
Description	Single Sign-On user credentials must be stored securely and protected.	
Source	Best In Industry	
Assumptions	None	
Sub-requirements	2.12.1	Single Sign-On user credentials must be stored with one-way encryption in place (i.e. salted Hash).
	2.12.2	Storage of Single Sign-On user credentials must allow for easy data synchronization/replication between FSA systems and the Single Sign-On data store.

3. Session Management

Identifier	3.1
Title	Integrated session management
Description	The Single Sign-On service must be able to establish a session with the end user, allowing him/her to connect seamlessly across multiple sites with the initial successful login and authentication.
Source	Best In Industry
Assumptions	Single Sign-On enabled business applications may be able to directly use the session management services provided by the Single Sign-On service for their session tracking purposes.

Identifier	3.2 (Technical)	
Title	Session Timeout	
Description	The Single Sign-On mechanism must offer session management	
Source	Best In Industry, FSA Login/Access Survey	
Assumptions	None	
Sub-requirement	3.2.1	The Single Sign-On solution must provide the option to prevent concurrent sessions for a user.
	3.2.2	The Single Sign-On mechanism must provide a configurable session timeout.
	3.2.3	A logout button must be available at any time.

4. Access Management

Identifier	4.1	
Title	Support User Exit/Signoff functions	
Description	Support exit/signoff options to end a user's active session with all applications accessed through Single Sign-On.	
Source	FSA Login/Access Survey	
Assumption	This provides the capability to end user sessions upon culmination of user activity	
Sub-requirements	4.1.1	Provide the ability for the Single Sign-On service to end an active user session after a predetermined period of user inactivity (i.e., timeout period)
	4.1.2	Provide the ability to end Internet session upon termination of a browser instance.
	4.1.3	Provide a logout button for users to close a session directly

Identifier	4.2	
Title	Removal of users from Single Sign-On access	
Description	Support the removal of users from the Single Sign-On service	
Source	FSA Login/Access Survey	
Assumption	None	
Sub-requirements	4.2.1	Remove users from the Single Sign-On service within one business day after receiving notification by FSA

Identifier	4.3	
Title	Access administration	
Description	Provide tools to administer access to applications and resources	
Source	FSA Login/Access Survey, Schools Requirements Review	
Assumption	None	
Sub-requirements	4.3.1	Provide user self-service administration/help
	4.3.2	Allow users to maintain multiple sessions with applications. Applications will determine whether single or multiple sessions are allowed.

Identifier	4.4	
Title	System access mechanisms	
Description	Provide access to applications by various mechanisms	
Source	FSA Login/Access Survey	
Assumption	Browser-based sessions are the preferred means to connect to applications	
Sub-requirements	4.4.1	Provide access to application via the Internet
	4.4.2	Provide access to application via VRU (Voice Response Unit)

Identifier	4.5	
Title	User Authentication	
Description	Users are individually authenticated via passwords, tokens, or other devices	
Source	NIST SP 800-18, CFO Requirements Review	
Assumption	None	
Sub-requirements	4.5.1	Maintain and approve a current list of authorized users and their access.
	4.5.2	Digital signatures, if used, conform to FIPS 186-2.
	4.5.3	Access scripts with embedded passwords are prohibited.
	4.5.4	Emergency and temporary access can be authorized.
	4.5.5	Terminated, transferred, or otherwise ineligible individuals are removed from system access.
	4.5.6	Passwords are changed at least every ninety days or earlier.
	4.5.7	Passwords are unique and difficult to guess (e.g., passwords require alpha numeric, upper/lower case, and special characters)
	4.5.8	Inactive user identifications are disabled after a specified period of time.
	4.5.9	Passwords are not displayed when entered.
	4.5.10	Procedure exists to terminate lost and compromised passwords.
	4.5.11	Passwords are distributed securely and users are informed not to reveal their passwords to anyone (social

		engineering).
	4.5.12	Passwords are transmitted and stored using secure protocols/algorithms.
	4.5.13	Vendor-supplied passwords are replaced immediately.
	4.5.14	A limited number of invalid access attempts are allowed for a given user.

Identifier	4.6	
Title	Logical Access Controls	
Description	Provide controls to restrict users to authorized Single Sign-On transactions and functions	
Source	NIST SP 800-18, CFO Requirements Review, CIO Requirements Review, CIO-Security Requirements Review	
Assumption	None	
Sub-requirements	4.6.1	Access controls prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion
	4.6.2	Access to security software is restricted to security administrators
	4.6.3	Inactive users' accounts are monitored and removed when not needed.
	4.6.4	Encryption when used, meets federal standards (AES, DES/triple-DES)
	4.6.5	When encryption is used, there exist procedures for key generation, distribution, storage, use, destruction, and archiving
	4.6.6	Access is restricted to files at the logical view or field
	4.6.7	Access monitored to identify apparent security violations
	4.6.8	Controls exist to restrict remote access to the system
	4.6.9	Activity logs are maintained and reviewed
	4.6.10	The network connection automatically disconnects at the end of a session
	4.6.11	Guest and anonymous accounts, if used, are authorized and monitored
	4.6.12	An approved standardized log-on banner is displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished
	4.6.13	Sensitive data transmissions are encrypted
	4.6.14	A privacy policy is posted on the web site

Identifier	4.7	
Title	Audit Trails	
Description	Activity involving access to and modification of sensitive or critical Single Sign-On files is logged	
Source	NIST SP 800-18, CFO Requirements Review	
Assumption	None	
Sub-requirements	4.7.1	Audit trail(s) provides a trace of user actions related to the Single Sign On mechanism.
	4.7.2	Audit trail(s) can support after-the-fact investigations of how, when, and why normal operations ceased of the Single Sign-On.
	4.7.3	Access to online audit logs provided by the Single Sign-On is strictly controlled
	4.7.4	Automated tools are available to review audit records in real time or near real time provided by the Single Sign-on
	4.7.5	Retention of Records - Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the information in the future. While electronic information is generally easier to retrieve and store, the technology used to create the records may not be readily available in the future. Measures may also have to be taken for the future use of data that has been encrypted, such as taking appropriate steps to ensure the secure long-term storage of cryptographic keys. It is important to consider legal requirements for records retention when disposing of IT systems. For federal systems, system management officials should consult with their office responsible for retaining and archiving federal records.

Identifier	4.8 (Technical)	
Title	Access history	
Description	After a successful login, the Single Sign-On service must provide a capability to provide a message with information about last successful login and how many unsuccessful login attempts have been made in the meanwhile.	
Source	Best In Industry	
Assumptions	None	
Sub-requirement	4.8.1	Provide a login history for Single Sign-On.
	4.8.2	Provide a logout history for Single Sign-On.
	4.8.3	Provide a failed login history through Single Sign-On.

Identifier	4.9 (Technical)	
Title	Access Restrictions	
Description	The Single Sign-On mechanism must offer the capability to define access rules.	
Source	Best In Industry	
Sub-requirement	4.9.1	The Single-Sign-On mechanism must offer configurable access restrictions based on time.
	4.9.2	The Single-Sign-On mechanism must offer configurable access restrictions based on location.
	4.9.3	The Single-Sign-On mechanism must offer configurable access restrictions based on user-group.
	4.9.4	Access restriction criteria must be combinable.

Identifier	4.10 (Technical)	
Title	Audit and logging	
Description	To allow for accountability logging and auditing must capture user actions.	
Source	Best In Industry/Common Criteria, CFO Requirements Review	
Sub-requirements	4.10.1	The Single Sign-On mechanism must offer the option to define actions if certain events have taken place.
	4.10.2	The information that is captured and stored for audit must be configurable.
	4.10.3	The Single Sign-On mechanism must be able to detect abnormal user behavior and provide the ability to pass this data to intrusion detection systems.
	4.10.4	Audit tools must be available for authorized users, to review audit logs.
	4.10.5	The Administrator must be able to select specific security events.
	4.10.6	The Single Sign-On mechanism must be able to create and maintain a secure audit trail.
	4.10.7	Audit logs must be only available to authorized users.

Identifier	4.11 (Technical)	
Title	Data handling – Communication between systems and the Single Sign-On data store	
Description	The Single Sign-On solution must allow for secure communication between systems and the Single Sign-On data store.	
Source	Best In Industry, CIO Requirements Review	
Assumptions	User data is synchronized between FSA systems and the Single Sign-On data store.	
Sub-requirements	4.11.1	Ensure encryption of Single Sign-On data.

Identifier	4.12 (Technical)	
Title	Data handling – User data	
Description	Protection of confidential data must be ensured at all time.	
Source	Best In Industry, Financial Partners Requirements Review	
Sub-requirements	4.12.1	The Single Sign-On service must be able to provide secure web communication.
	4.12.2	Storage of confidential data must be done securely.

Identifier	4.13	
Title	System access integration	
Description	Provide identification and authentication access integration to the following FSA business applications	
Source	FSA Login/Access Survey	
Assumption	The Single Sign-On solution must be able to provide identification and authentication access to the following FSA business applications. The specific applications to be Single Sign-On enabled and the timing of enablement are to be addressed by FSA implementation plans.	
Sub-requirements	4.13.1	Provide single sign-on access to GAPS
	4.13.2	Provide single sign-on access to Financial Partners Datamart
	4.13.3	Provide single sign-on access to CPS
	4.13.4	Provide single sign-on access to COD
	4.13.5	Provide single sign-on access to NSLDS for Financial Aid Professionals
	4.13.6	Provide single sign-on access to NSLDS for Students
	4.13.7	Provide single sign-on access to Pell/RFMS
	4.13.8	Provide single sign-on access to DLOS-Financial Aid Professionals
	4.13.9	Provide single sign-on access to DLSS-Non Students
	4.13.10	Provide single sign-on access to eServicing
	4.13.11	Provide single sign-on access to DLCS-Non Students
	4.13.12	Provide single sign-on access to Consistent Answers
	4.13.13	Provide single sign-on access to Credit Management Datamart
	4.13.14	Provide single sign-on access to Delinquent Loans Datamart
	4.13.15	Provide single sign-on access to CFO Datamart
	4.13.16	Provide single sign-on access to DMCS
	4.13.17	Provide single sign-on access to FFEL
	4.13.18	Provide single sign-on access to e-App
	4.13.19	Provide single sign-on access to ERM
	4.13.20	Provide single sign-on access to FMS
	4.13.21	Provide single sign-on access to HR Modernization

4.13.22	Provide single sign-on access to IFAP
4.13.23	Provide single sign-on access to IAM
4.13.24	Provide single sign-on access to MDE/CPS
4.13.25	Provide single sign-on access to OCTS
4.13.26	Provide single sign-on access to PEPS
4.13.27	Provide single sign-on access to EDPUBS
4.13.28	Provide single sign-on access to students.gov
4.13.29	Provide single sign-on access to SAIG
4.13.30	Provide single sign-on access to eCB
4.13.31	Provide single sign-on access to DLCS-Students
4.13.32	Provide single sign-on access to DLSS-Students
4.13.33	Provide single sign-on access to FAFSA on the Web
4.13.34	Provide single sign-on access to FAA Access Online
4.13.35	Provide single sign-on access to Schools Portal
4.13.36	Provide single sign-on access to Financial Partners Portal
4.13.37	Provide single sign-on access to Students Portal
4.13.38	Provide single sign-on access to ED-Express
4.13.39	Provide single sign-on access to EDNET

5. Customer Care

Identifier	5.1	
Title	Non-student system access help	
Description	Provide system login/access support to non-student users	
Source	FSA Login/Access Survey	
Assumption	None	
Sub-requirements	5.1.1	Provide customer care support to 21,000 non-student Single Sign-On users
	5.1.2	Provide access support for non-Student Single Sign-On user calls related to access (estimated at 21,000 calls per month)
	5.1.3	Provide a scalable solution to allow for extending the user support easily.

Identifier	5.2 (Technical)	
Title	Self-service	
Description	The Single Sign-On portal must provide tools for self-service and a contact for more complex problems.	
Source	Best In Industry	
Assumptions	The Single Sign-On does not replace direct access to systems.	
Sub-requirements	5.2.1	A user must be able to change certain user information via the self-service feature.
	5.2.2	Username changes can only be done through an Administrator
	5.2.3	Email Address changes can only be done through an Administrator.

6. Legal

Identifier	6.1	
Title	Privacy and confidentiality protections	
Description	Provide legal notices and protections for Privacy Act data and confidential data maintained within the Single Sign-On service	
Source	FSA Login	
Assumption	None	
Sub-requirements	6.1.1	Provide notices (i.e., banners) for Privacy Act
	6.1.2	Provide notices (i.e., banners) for confidential data

Identifier	6.2	
Title	Section 508 Compliance	
Description	Comply with FSA guidelines for implementing Section 508 needs.	
Source	Legal	
Assumption	None	
Sub-requirements	6.2.1	Solution(s) must meet the general requirements of Public Law 99-506 Reauthorization of the Rehabilitation Act of 1973, Section 508-Electronic Equipment Accessibility, October 1986; and Public Law 100-542 Telecommunication Accessibility Enhancement Act, October 1988. Solution(s) will develop or use a set of tests to determine whether deliverables are in substantial conformance to the general requirement. The government will review and approve these tests prior to the commencement of the work.

Identifier	6.3 (Technical)	
Title	Legal notice	
Description	A legal message must be displayed outlining the legal aspects of connecting to FSA systems through the Single Sign-On portal(s).	
Source	Best In Industry	
Assumptions	None	
Sub-requirements	6.3.1	A message must be displayed to users notifying them when they leave the Single Sign-On realm and enter another system outside the control and jurisdiction of the FSA Single Sign-On service.

7. Environment

Identifier	7.1 (Technical)	
Title	Supported operating systems	
Description	Provide the ability to support and integrate with a variety of server operating systems supporting FSA business applications.	
Assumption	None	
Sub-requirements	7.1.1	Windows NT
	7.1.2	Windows 2000
	7.1.3	Sun Solaris 2.6, 8
	7.1.4	Hewlett-Packard Unix 11.x
	7.1.5	Linux
	7.1.6	Mainframe MVS
	7.1.7	VAX/VMS
	7.1.8	Mainframe OS 390

Identifier	7.2 (Technical)	
Title	Supported web servers	
Description	Provide support for major web servers.	
Assumption	None	
Sub-requirements	7.2.1	Apache
	7.2.2	Microsoft IIS
	7.2.3	IBM HTTP Server
	7.2.4	iPlanet Enterprise Server

Identifier	7.3 (Technical)	
Title	Supported application server	
Description	Provide support for major application servers.	
Assumption	None	
Sub-requirements	7.3.1	Coldfusion
	7.3.2	Websphere 3.55
	7.3.3	JRUN
	7.3.4	Weblogic
	7.3.5	Citrix
	7.3.6	Oracle

Identifier	7.4 (Technical)	
Title	Supported proxy servers	
Description	Provide support for major proxy servers.	
Assumption	None	
Sub-requirements	7.4.1	CoolGen
	7.4.2	Apache
	7.4.3	Webcache

Identifier	7.5 (Technical)	
Title	User data storages	
Description	Provide support for major user data repositories	
Assumption	None	
Sub-requirements	7.5.1	ODBC Database (Oracle, SQL Server, Informix)
	7.5.2	RACF
	7.5.3	NT Network
	7.5.4	FSA PIN Service
	7.5.5	Directory (LDAP v3)
	7.5.6	Oracle Financials ERP

Identifier	7.6 (Technical)	
Title	Web browser support	
Description	Provide support for the FSA supported Internet browsers.	
Source	FAFSA on the Web, CFO Requirements Review	
Assumption	None	
Sub-requirements	7.6.1	Support the following Netscape browsers: <ul style="list-style-type: none"> • Netscape Navigator 4.06 and higher. • Netscape Navigator 4.5 and higher. • Netscape Navigator 4.73 and higher. • Netscape Navigator 4.76 (Windows 95/98, Windows NT, Windows 2000, and Macintosh) • Netscape Navigator 6.2 (Windows 98, Windows NT)
	7.6.2	Support the following Microsoft browsers: <ul style="list-style-type: none"> • 4.01 - Internet Explorer (and higher) for Oracle Financials support. • 4.72.3612.1713 – Internet Explorer 4.7 (and newer) currently used by internal SFA users. • 5.00.2014.0216 - Internet Explorer 5.0 (Windows 95/98, and Windows NT) • 5.00.2314.1003 - Internet Explorer 5.0 (Office 2000) • 5.00.2614.3500 - Internet Explorer 5.0 (Windows 98 Second Edition) • 5.00.2919.6307 - Internet Explorer 5.01 and 5.01 with Service Pack 1 (Windows 95/98, and Windows NT, and Windows 2000) • 5.00.2920.0000 - Internet Explorer 5.01 (Windows 2000, build 5.00.2195) • 5.00.3103.1000 - Internet Explorer 5.01 with Service Pack 1 (Windows 2000) • 5.00.3105.0106 - Internet Explorer 5.01 with Service Pack 1 (Windows 95/98 and Windows NT) • 5.00.3314.2101 - Internet Explorer 5.01 with Service Pack 2 (Windows 95/98/ME, and Windows NT) • 5.00.3315.1000 - Internet Explorer 5.01 with Service Pack 2 (Windows 2000) • 5.50.4134.0600 - Internet Explorer 5.5 (Windows 95/98, Windows NT, Windows 2000, and Windows ME) • 5.50.4522.1800 - Internet Explorer 5.5 with Service Pack 1 (Windows 95/98, Windows NT, Windows 2000, and Windows ME) • 6.0.2600.0000 - Internet Explorer 6.0 (Windows NT, Windows XP Home, and Professional)

	7.6.3	<p>Support the following America Online default browsers:</p> <ul style="list-style-type: none">• AOL 5.0 (Windows 95/98)• AOL 6.0 (Windows 95/98, Windows NT, and Windows 2000)• AOL 7.0 (Windows 98)
--	-------	--

8. Operations

Identifier	8.1	
Title	Administration	
Description	Administration is delegated	
Source	Best In Industry, CIO Requirements Review, FP Requirements Review	
Sub-requirements	8.1.1	Delegated administration must be configurable based on user groups.
	8.1.2	Group administration must be shareable between two or more administrators within the same-delegated administration group.

Identifier	8.2 (Technical)	
Title	High availability (24x7)	
Description	The Single Sign-On service must be designed for “high availability”.	
Source	Best In Industry	
Assumptions	Several dependencies on network and other Single Sign-On and non Single Sign-On infrastructure components.	
Sub-requirements	8.2.1	Support for redundant deployment with built-in fail-over capabilities.

Identifier	8.3 (Technical)	
Title	Technical Support	
Description	Technical support for Single Sign-On mechanism must be available.	
Source	Best In Industry, Schools Requirements Review	
Assumptions	Users can still access the systems participating with Single Sign-On directly without going through the Single Sign-On portal.	

Identifier	8.4 (Technical)
Title	Availability - Disaster recovery/Continuity of Operations
Description	After a major disaster, the Single Sign-On portal must be able to return to operational state in a timeframe consistent with the FSA disaster recovery procedures.
Source	Best In Industry
Assumption	Disaster recovery procedures are in place.

Identifier	8.5 (Technical)
Title	Availability - Protection against data loss
Description	The Single Sign-On solution must be designed to allow for backup and recovery consistent with the FSA backup /recovery procedures.
Source	Best In Industry
Assumptions	Off-site media storage procedures, backup procedures and policies per capability are in place.

Identifier	8.6 (Technical)
Title	Performance and Scalability - Login response time
Description	The Single Sign-On service must support a login response time and session establishment time per FSA guidelines.
Source	Best In Industry
Assumptions	The achievement of this performance goal depends on other components of the FSA infrastructure outside the scope of the project. Support of third party and remote sites may impose some additional delays, because of the number of redirections that may be necessary to establish a session with these external sites.

Identifier	8.7 (Technical)
Title	Performance and Scalability - User self-service response time
Description	The Single Sign-On service must support a user self-service response time per FSA guidelines.
Source	Best In Industry
Assumptions	The achievement of this performance goal depends on other components of the FSA infrastructure and is outside the scope of the project.

Identifier	8.8 (Technical)
Title	Number of user self-service requests
Description	The Single Sign-On service must support user self-service requests as defined per FSA guidelines.
Source	Best In Industry
Assumptions	The achievement of this performance goal depends on other components of the FSA infrastructure and is outside the scope of the project.

Identifier	8.9 (Technical)	
Title	User scalability	
Description	The Single Sign-On service must be able to support 23 million student users, and 25,000 school and financial partner users.	
Source	Best In Industry	
Assumptions	This requirement critically depends on the design of the Single Sign-On access control data store.	
Sub-requirements	8.9.1	The Single Sign-On service must be able to support FSA peak student concurrent logins.
	8.9.2	The Single Sign-On service must be able to support FSA peak school, financial partner, employee, and operating partner concurrent logins.

9. ISO/IEC 15408 Security / Common Criteria

Identifier	9.1	
Title	Auditable	
Description	Auditing involves recognizing, recording, storing and analyzing information related to security relevant activities. The resulting audit records can be examined to determine which security relevant activities took place and who is responsible for them.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.1.1	Automatic response to events - Certain audit events (Incidents) must result in actions, which are executed automatically.
	9.1.2	Audit data generation - The level of which information is stored for audit, must be configurable.
	9.1.3	Audit analysis – Abnormal user behavior must be detected and the ability to pass this data to intrusion detection systems must be provided.
	9.1.4	Audit review – Audit tools must be available for authorized users, to review audit data.
	9.1.5	Audit event selection – The ability to select specific security events must be provided.
	9.1.6	Audit event storage – The ability to create and maintain a secure audit trail must be provided. Only authorized users are allowed to view or modify audit data.

Identifier	9.2	
Title	Secure Communication	
Description	Secure communication is concerned with assuring the identity of a party participating in a data exchange. This ensures that the originator cannot deny having sent the message, nor can the recipient deny having received it.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.2.1	The ability to verify if a communication request is originating from the system it claims to come from.
	9.2.2	The ability to verify if a system is the intended recipient for a communication request.

Identifier	9.3	
Title	Cryptographic support	
Description	Cryptography ensures that the following objectives are satisfied: identification and authentication, non-repudiation, trusted path, trusted channel and data separation.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.3.1	Cryptographic key management – A key management function must be offered that allows the management of cryptographic keys throughout their lifecycle (generation through deletion).
	9.3.2	Cryptographic operation – Functions like strong encryption/decryption, cryptographic-checksum and secure hash must be offered.

Identifier	9.4	
Title	User data protection	
Description	User data must be protected from unauthorized access or manipulation.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.4.1	Access control policy – Access to user data must be controlled and protected based on access policies.
	9.4.2	Access control functions – Access to user data is controlled by these functions, which are configured according to the access policies.
	9.4.3	Data authentication – Data authentication allows for verification of data if it has been forged or fraudulently modified.
	9.4.4	Export of user data – Security attributes associated with user data can be explicitly preserved or ignored when exporting user data.
	9.4.5	Information flow policy – Allow for read or write only access to user data for specific entities.
	9.4.6	Information flow control function – An Information flow control is provided based on the information flow policy allowing for users to read, write, modify, delete or create specific data.

	9.4.7	Import of user data – Security attributes associated with user data can be explicitly preserved or ignored when importing user data. This allows keeping access rights confidential if user data needs to be exported to other systems.
	9.4.8	Internal data transfer – User data protection is provided when data is transferred internally.
	9.4.9	Residual data protection – Ensure that purged information is no longer accessible.
	9.4.10	Rollback – Offering an Undo for the last operation.
	9.4.11	Stored data integrity – Ensure that stored user data is protected from unauthorized access.
	9.4.12	User data confidentiality transfer protection – Ensure that user data is protected from unauthorized access during transfer between entities.
	9.4.13	User data integrity transfer protection – Ensure that user data is not manipulated during transfer between entities.

Identifier	9.5	
Title	Identification and authentication	
Description	Establish and verify a claimed user identity, to ensure that the right security attributes are associated.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.5.1	Authentication failures – Actions (For example: A user is locked out after three unsuccessful login attempts) must be definable if a certain number of failed authentication attempts occur.
	9.5.2	User attribute definition – Each user has security attributes associated to him/her, which define users access rights appropriate to his/her role.
	9.5.3	Specification of secrets – Secrets (e.g. Password) must be checked against certain definable quality standards.
	9.5.4	User authentication – Offer a scalable robust authentication mechanisms.
	9.5.5	User identification – Before a user can take any actions, he/she has to be identified. Only exception is the login process.
	9.5.6	User subject binding – Processes accessing, changing or deleting objects are executed with the user’s security attributes.

Identifier	9.6	
Title	Security management	
Description	Management of security attributes of users allowing for separation of duties.	
Origin	Common Criteria/ISO15408	
Sub-requirements	9.6.1	Management of functions – Security functions must only be accessible by authorized users.
	9.6.2	Management of security attributes – Security attributes can be modified, established or deleted only by authorized users.
	9.6.3	Management of internal data – Audit, configuration or any other critical data must be accessible only by authorized users.
	9.6.4	Revocation – Security attributes must be revocable for each entity.
	9.6.5	Security attribute expiration – Security attributes must have a limited lifetime.

Identifier	9.7	
Title	Privacy	
Description	Protection against discovery and misuse of identity by other users.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.7.1	Anonymity – A user can use a resource or service without disclosing the user’s identity to other users.
	9.7.2	Pseudonymity – A user’s identity is not disclosed to other users. But the user is still accountable for its action.
	9.7.3	Unlinkability – A user can use a resource multiple times without other users being able to link these sessions to each other.
	9.7.4	Unobservability – A user can utilize a resource without unauthorized parties being able to observe his/her actions or the usage.

Identifier	9.8	
Title	Protection	
Description	Ensure the integrity and manageability of the mechanism providing Single Sign-On functionality and all the data related to it.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.8.1	Underlying abstract machine test – Functions, which are provided by the OS or the hardware platform, which the Single Sign-On mechanism relies on, need to be tested at start-up and on regular basis.
	9.8.2	Fail Secure – In the event of failures the Single Sign-On mechanism must go into a “safe mode”.
	9.8.3	Availability of exported data – Critical data, which is exported to another IT product, must be still available for the Single Sign-On mechanism at the time of export.
	9.8.4	Confidentiality of exported data – Protection from unauthorized disclosure of data during transmission between the Single Sign-On mechanism and another IT product must be provided.
	9.8.5	Integrity of exported data - Protection from unauthorized modification of data during transmission between the Single Sign-On mechanism and another IT product.
	9.8.6	Internal data transfer – Protection of data transmitted between different pieces of the Single Sign-On mechanism must be provided.
	9.8.7	Physical protection – Restrictions on physical access to the Single Sign-On mechanism and the underlying hardware must be ensured.
	9.8.8	Trusted recovery – The Single Sign-On mechanism must start up in a controlled state.
	9.8.9	Replay detection – Replay of various entities (e.g. messages, service request, service responses) must be detected.
	9.8.10	Reference mediation – Before executing any action, the action must be evaluated against the security policies established for the specific user group and type of action.
	9.8.11	Domain separation – Security functions of the Single Sign-On mechanism must live in their own domain to avoid tempering.
	9.8.12	State synchrony protocol – State synchronization between the different parts of the Single Sign-On mechanism must be done with a secure exchange protocol.

	9.8.13	Timestamp – A reliable timestamp mechanism must be offered.
	9.8.14	Internal data consistency – Data must be consistent across the whole Single Sign-On mechanism.
	9.8.15	Internal data replication consistency – Data must be consistent between the Single Sign-On mechanism and the IT products utilizing the data provided by it.
	9.8.16	Self-test – The Single Sign-On mechanism must test itself when starting up and before users are allowed access.

Identifier	9.9	
Title	Resource Utilization	
Description	The Single Sign-On mechanism must provide a mechanism to control resource utilization	
Source	Common Criteria/ISO15408	
Sub-requirements	9.9.1	Fault tolerance – In event of failures the Single Sign-On mechanism should maintain normal operation.
	9.9.2	Priority of service – High priority tasks cannot be interrupted by tasks with a lower priority.
	9.9.3	Resource allocation – Use of resources by users and subjects is controlled to avoid a denial of service.

Identifier	9.10	
Title	Access and Session management	
Description	Controlling the establishment of a user’s session.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.10.1	Scope of selectable attributes – Limit the scope of session security attributes that a user may select for a session.
	9.10.2	Limitation on concurrent sessions – Users are only allowed one or more concurrent sessions, as configured by the access service.
	9.10.3	Session locking – Inactive sessions must be locked or closed.
	9.10.4	Access banner – An access banner must be present to display a configurable advisory warning message.

	9.10.5	Access history – Upon successful login, provide a capability to allow presentation to the user a history of successful and unsuccessful attempts to access the user’s account.
	9.10.6	Session establishment – A function must be offered to define rules to deny access based on user location, time, credentials, authentication-method, etc.

Identifier	9.11	
Title	Trusted path/channels	
Description	Establish and maintain trusted communication between entities.	
Source	Common Criteria/ISO15408	
Sub-requirements	9.11.1	Secure transit of data – Confidential data must never be transmitted in the clear over any network connection, whether it is to/from internal or external systems.
	9.11.2	Trusted Path - Confidential data must never be transmitted in the clear between user and the single-sign-on mechanism.

4 Potential Alternatives

High-level potential alternatives are listed in this section. The next phase, upon approval, will determine the appropriate design for FSA. The alternatives are:

A. Custom Developed Single Sign-On Service

Implement a proprietary Single Sign-On service by developing user authentication business processes and policies that are enabled by a new technical capability that is owned, operated and maintained by FSA.

Business processes and IT enablers, which will require integration or definition, include:

- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

Technologies to be considered for integration into a custom solution may include:

- SAML / XML
- SOAP
- LDAP
- RDBMS
- Encryption
- Web-based development tools (Java, C/C++, others as needed)
- Web application server (Websphere)
- Credential/Tokens (PKI, smart card, etc.)
- Web services (UDDI)
- Others as needed

B. Single Sign-On By Enhanced Current FSA Capability

Existing FSA business and technology capabilities may be reused with possible modifications and enhancements to provide a Single Sign-On service capable of meeting FSA requirements.

Business processes and IT enablers, which will require integration or definition, include:

- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

Current existing capabilities include:

- FSA PIN
- FSA to the Internet

- EDNet
- Others

Technologies to be considered for integration to enhance a current FSA capability may include:

- SAML / XML
- SOAP
- LDAP
- RDBMS
- Encryption
- Web-based development tools (Java, C/C++, others as needed)
- Web application server (Websphere)
- Credential/Tokens (PKI, smart card, etc.)
- Web services (UDDI)
- Others as needed

C. COTS enabled Single Sign-On Service

Implement a Single Sign-On service by integrating a commercial-off-the-shelf (COTS) system to FSA systems and user access control business processes.

Business processes and IT enablers, which will require integration or definition, include:

- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

Solution vendors may include the following firms:

- Waveset (Lighthouse)
- Thor Technologies
- Access360
- Netegrity (Siteminder)
- Entrust (getAccess)
- Tivoli (Policy Director)
- Oblix
- Securant
- Computer Associates
- BMC Software
- Evidian

D. Single Sign-On Service from a Managed Service Provider

Implement a Single Sign-On service by outsourcing user authentication processes to a managed service provider specializing in system access control integration and operations.

Business processes and IT enablers, which will require integration or definition, include:

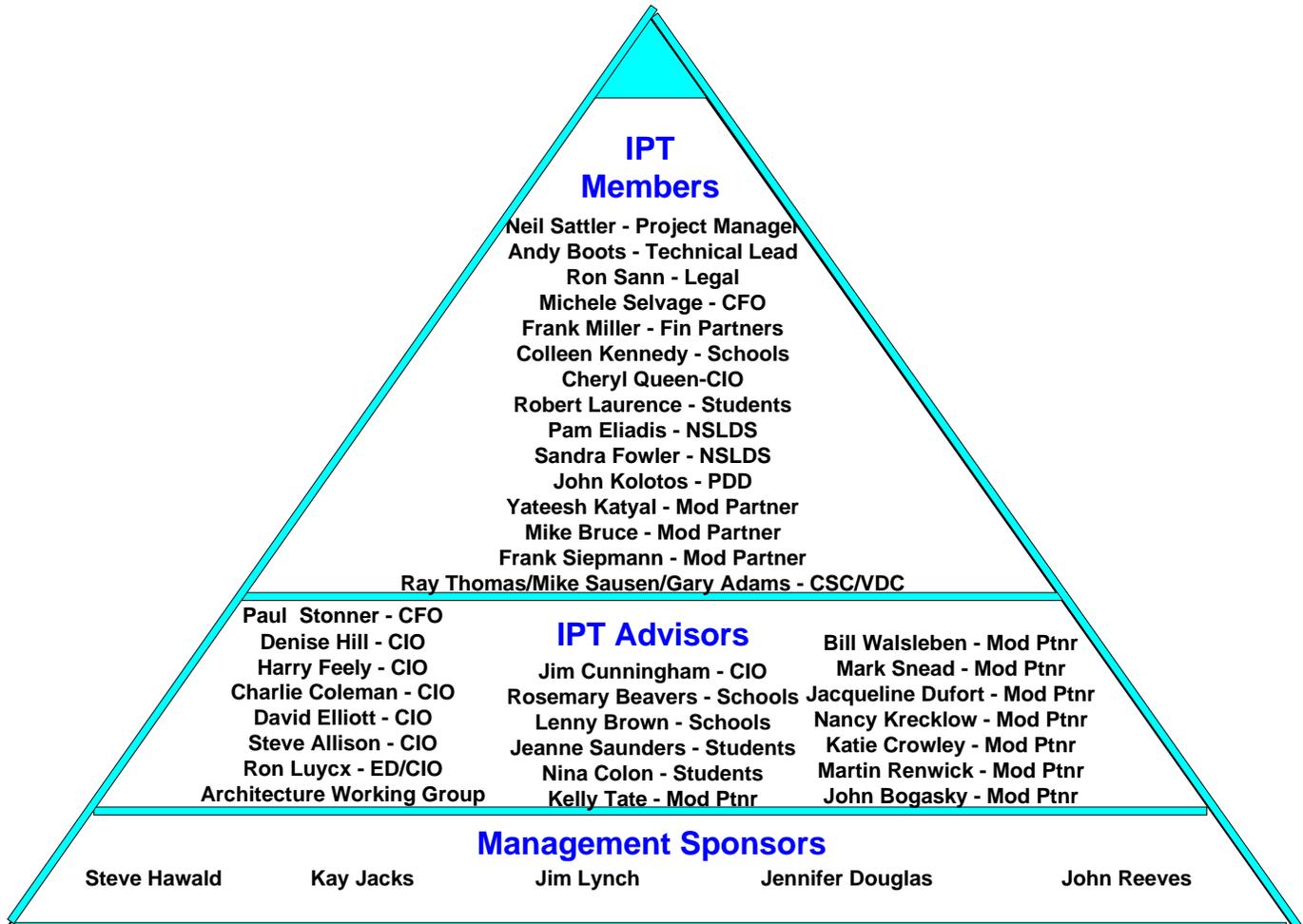
- Logon and Session Establishment
- Application Access
- Logout and Session Termination
- Access Credential Administration (session timeout, credential suspension, credential revocation, credential reset)

Managed Service Providers may include the following:

- Microsoft Passport/.NET Services
- Sun Microsystems (Liberty Alliance)
- AOL (Magic Carpet)
- Aventail
- Jamcracker
- VeriSign

Appendices

Appendix A: IPT team



Appendix B: Acronyms and Abbreviations

Acronym	Definition
API	Application Program Interface
CBS	Campus-Based System
COD	Common Origination and Disbursement
COTS	Commercial Off-the-Shelf (Software)
CRM	Customer Relations Management
CPS	Common Processing System
DLCS	Direct Loans Consolidations System
DLOS	Direct Loans Origination System
DLSS	Direct Loans Servicing System
DMCS	Debt Management and Collection System
EAI	Enterprise Architecture Infrastructure
ECB	eCampus Based
ED	US Department of Education
EDCAPS	US Department of Education Consolidated Accounting and Payment System
ERM	Electronic Records Management
FAA	Financial Aid Administrator
FFEL	Federal Family Education Loan
FAFSA	Free Application for Federal Student Aid
FISAP	Fiscal Operations Report and Application to Participate
FMS	Financial Management System
GAPS	Grant Administration Payment System (subsystem of EDCAPS)
IAM	Institutional Assessment Model
IEC	International Engineers Consortium
IFAP	Information for Financial Aid Professionals
IPT	Integrated Product Team
IDS	Intrusion Detection System
ISO	International Standards Organization
MDE	Multiple Data Entry System
NSLDS	National Student Loan Data System
PEPS	Postsecondary Education Participants System
PPA	Program Participation Agreement
RFMS	Recipient and Financial Management System (Pell originations & disbursement)
RDBMS	Relational Database Management System
SAIG	Student Aid Internet Gateway
SAR	Student Aid Report
FSA	Federal Student Aid
TIVWAN	Title IV Wide Area Network
VDC	Virtual Data Center
VRU	Voice Response Unit

Appendix C: FSA Login/Access Survey Results and Summary

See Attached MExcel File - 82.1.3 FSA Logon Access Survey - Requirement Definition Draft.xls