

***FSA Modernization Program***  
**United States Department of Education**  
**Federal Student Aid**



**Single Sign-On**  
**Alternatives Evaluation**

***Task Order #82***  
***Deliverable #82.1.4 Part B***

**Final**

**May 29, 2002**

## Document Revision History

Version No.	Date	Author	Revisions Made
1.0	May 3, 2002	Michael Bruce	Initial released
1.1	May 17, 2002	Michael Bruce	Revised released
1.2	May 29, 2002	Michael Bruce	Final approved by IPT Project Manager
1.3			
1.4			

## Table of Contents

EXECUTIVE SUMMARY .....	3
Business Problems To Be Addressed.....	3
Approach Alternatives and Recommendation .....	3
Solution Recommendation.....	4
Single Sign-On Services RFI Overview .....	5
Method.....	5
Summary Results .....	6
1. Introduction.....	9
2. Vendor Evaluation – Quadrant Charts .....	11
3. Vendor Evaluation Summary .....	13
4. Solution Synopses .....	14
4.1 Aventail.....	14
4.2 Entrust.....	17
4.3 Netegrity SiteMinder.....	19
4.4 IBM Access Manager & Identity Manager.....	21
4.5 Waveset Lighthouse.....	23
4.6 Yodlee.....	25
4.7 RSA Security – Cleartrust .....	27
Appendix A. Vendor Information Summaries.....	29
Appendix B. Vendor Evaluation Matrix .....	40
B.1 Criteria and Weighting Scheme.....	40
B.2 Vendor Evaluation Summary .....	41
B.3 Solution prioritizing .....	54
Appendix C - Response Evaluation Criteria.....	55
C.1 Partner Evaluation Criteria – Business Criteria .....	55
C.2 Partner Evaluation Criteria – Technical Criteria.....	65
C.3 Partner Evaluation Criteria – Other Criteria .....	85
Appendix D – Preliminary Benefit / Cost Summary.....	86

## EXECUTIVE SUMMARY

This document presents the IPT's recommendation for an FSA Identification and Authentication (I&A) solution, and summarizes the results of the Request for Information for Identity and Authentication Services conducted by the IPT for Department of Education, Federal Student Aid (ED/FSA).

### ***Business Problems To Be Addressed***

Then IPT determined that any feasible FSA "Single Sign-on" solution must assist FSA to rectify the following business problems:

- Identification and Authentication
  - Identify users requesting access
  - Accept or deny access to systems via a shared secret or other FSA adopted authentication methods
  - Inter-operate with the Federal Bridge Certificate Authority and other Transient Trust services
- Enrollment / User Management
  - Manage access to services, i.e., enroll, suspend, change, and revoke user access
  - Operate with Consistent Answers participation management functionality
- Provisioning
  - Broker and manage user access to legacy systems

### ***Approach Alternatives and Recommendation***

Based on the Requirements Definition and the result of the RFI process, the IPT recognized the following as feasible alternatives for implementing a consistent identification and authentication capability at FSA.

1. Implementation of an Identification, Authentication, and Unified Enrollment service for modernized applications. This provides a standard infrastructure for access management for all modernized systems; single sign-on is an added benefit of this approach. Legacy applications can leverage this infrastructure, as needed.
2. Implementation of an Identification and Authentication service for existing legacy applications. This solution will provide users a single login ID; the technology infrastructure will broker and manage access to legacy systems on the behalf of a user.
3. Implementation of an Identification, Authentication, and Unified Enrollment service for legacy and modernized systems. This solution will provide a standard infrastructure for access management for new and legacy systems; single sign-on is a coincident benefit of this alternative. Legacy applications can leverage this infrastructure directly or via a brokering approach, as needed.

### ***Solution Recommendation***

The IPT recommends that FSA adopt Alternative #1 above. This option will establish a business operations and technology infrastructure that provides a:

- Common I&A infrastructure for all systems to be modernized and future, yet to be identified, systems
- Unified enrollment capability inter-operate able with the Consistent Answer participation management functionality
- Infrastructure for establishing a common user identifier
- Central user access control repository

Based on the results of the Single Sign-On Services RFI, the IPT recommends that final candidates for FSA's Identification, Authentication, Enrollment, and Provisioning services (IAE&P) services are:

- IBM's Access Manager and Identity Manager products
- RSA (Cleartrust) and Waveset (Lighthouse) partnership

This recommendation is based upon the following criteria:

- Pre-modernization legacy applications will be re-engineered or retired according to the Modernization Blueprint,
- Applications already developed and deployed during FSA Modernization will require a Provisioning mechanism to utilize the standard IAE&P services;
- Each vendors products are rated "Best-of-Breed" by Gartner/Giga
- Each alternative is extendable for eGov initiatives (eAuthentication)
- Each alternative is installed at government & financial organizations
- Each vendor has a history of commitment to the FSA and ED infrastructure
- Enterprise acquisition and ongoing maintenance costs of each finalist are competitive

Specific strengths of each finalist are the following:

- IBM Access Manager and Identity Manager
  - Provides integration capabilities to FSA's existing MQ-Series and WebSphere technology assets,
  - IBM is a multi-billion dollar global leader in information technology,
  - IBM is the web access control market leader outside the United States and #2 in market share within the US. IBM has over 550 customers for Access Manager,
  - IBM has scalable production implementations – T. Rowe Price supports 1.2 million retail investment customers; SSA expects to support over 25 million users,
- RSA Cleartrust and Waveset Lighthouse
  - Provides an user-centric enrollment and account management capabilities,
  - RSA is the leader in information technology security,

- Waveset Lighthouse supports over 1 million customers at Fidelity Investments;
- RSA and Waveset technology emphasizes the use of non-invasive agents and filters placed on existing web server, rather than the use of a web proxy server, as a means to protect access to protected resources.

### ***Single Sign-On Services RFI Overview***

The purpose of this RFI was to evaluate, rank and recommend a vendor solution with the ability to partner with FSA in the development and implementation, on-going operations, and enhancement of a “Single Sign-on” service. This service requires capabilities to support Identification and Authentication of users, as well as Enrollment of users to FSA business applications. Vendors were asked to respond to detailed series of questions to identify the extent that each product or service:

- Meets FSA business and technical requirements,
- Can be supported within the FSA operational environment,
- Provides the scalability and performance levels to meet the expected level of demand,
- Meets FSA security and privacy requirements.

As the project progressed, the IPT became aware that FSA faces the following challenges that are addressed by the IPT’s recommendations:

- Simplifying user access to existing and new production applications.
- Establishing a common and reusable Identification & Authentication, and Enrollment infrastructure for new and modernized systems as they a developed and deployed in future years.
- Creating a simplified framework for users to manage their access to legacy applications.

### ***Method***

The IPT team contacted leading vendors, and solicited their participation in the RFI. Each vendor was sent an RFI with questions which covered business capabilities necessary to support FSA and the vendor’s product/service on an ongoing basis, as well as the vendor’s capabilities to meet FSA solution requirements as defined in Deliverable 82.1.3, Single Sign-On Requirements Definition - Final, March 15, 2002. The IPT team also conducted independent research to confirm these capabilities and to acquire independent knowledge and insight into each vendor. Each vendor’s responses to the RFI questions were rated against an objective “evaluation scale” developed prior to contacting vendors. The summary results were summarized on a four-quadrant chart to display the relative rankings of each vendor against FSA business and technology requirements.

Each vendor, following receipt of their written response, provided the IPT an oral presentation to highlight the distinguishing features of their product/service with respect to FSA requirements. Vendors were also asked to compare and contrast their product/service to other offerings in the marketplace. The IPT members collected additional information from these presentations, provided written summaries of their perceptions of each vendor, and discussed their perspectives during IPT meetings. These viewpoints were used to revise vendor ratings, based upon written responses.

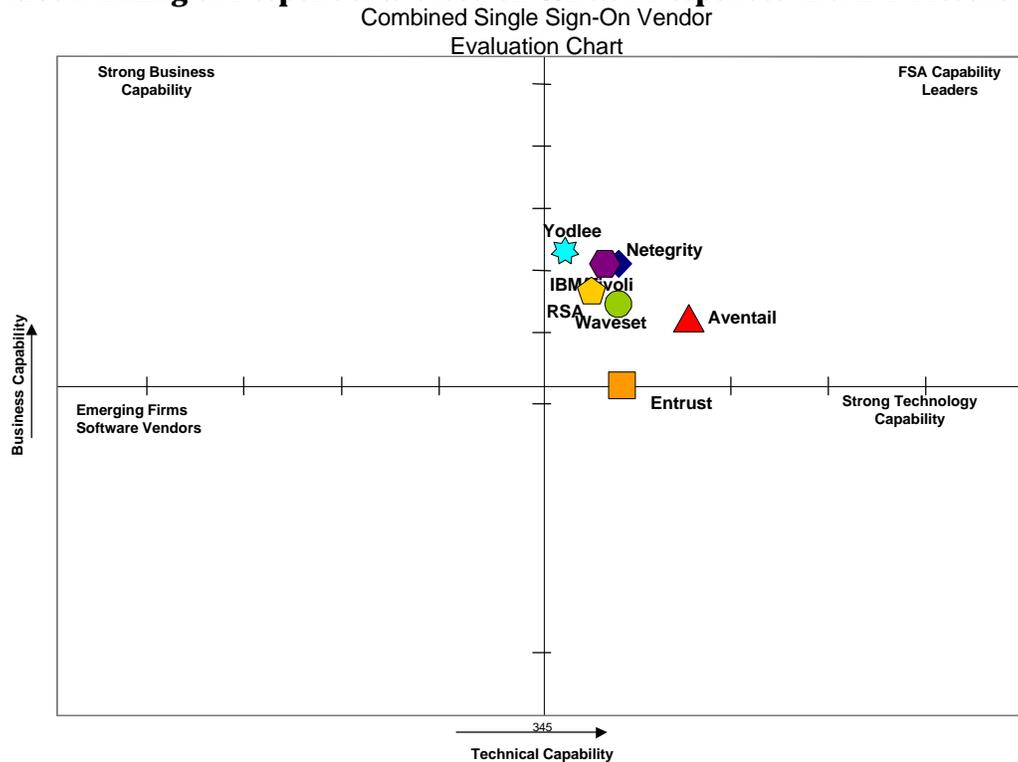
The IPT team contacted eight vendors with competency in user access control products and/or services. The eight vendors selected to receive the RFI represent industry leading vendors in each of the following areas:

1. Leading Web Access Control (WAC) vendors:
  - a) Commercial of the Shelf tools (COTS):
    - Netegrity (SiteMinder)
    - Entrust (GetAccess)
    - IBM (Access Manager)
    - RSA Security (ClearTrust)
  - b) Managed Access Control Services:
    - Aventail (Aventail.NET)
2. Leading Provisioning vendors in the Provisioning market space:
  - a) Commercial of the Shelf tools (COTS):
    - Waveset (Lighthouse)
    - Entrust (GetAccess)
    - IBM (Identity Manager)
  - b) Managed Access Control Services:
    - Yodlee (Yodlee e-Personalization Platform)
3. Existing Authentication systems at FSA:
  - NCS-Pearson (FSA PIN)

### ***Summary Results***

Each of these vendors provided a written response to the RFI. NCS-Pearson submitted a written response, but decided to withdraw from the RFI prior to the start of oral presentations. The seven responding vendors (Aventail, Entrust, IBM, Netegrity, Waveset, RSA Security, and Yodlee) were ranked based on their written responses to the RFI, oral presentations, and external research. The following chart shows the relative ranking of the respondents:

## FSA Single Sign-On Service RFI Relative Ranking of Respondents based on Written Responses and IPT Presentations



Based on this survey, the leading firms that are capable of partnering with FSA in order to provide Single Sign-On services are the following (listed by rank order):

### Web Access Control:

1. Netegrity (Siteminder)
2. IBM (Access Manager)
3. Aventail
4. Entrust (GetAccess)
5. RSA Security (ClearTrust)

### Provisioning tools:

1. Yodlee (Yodlee e-Personalization Platform)
2. Waveset (Lighthouse)
3. IBM (Identity Manager)
4. Entrust (GetAccess)

### Web Access Control & Provisioning:

1. IBM (Access Manager & Identity Manager)
2. Entrust (GetAccess)
3. RSA + Waveset
4. RSA + Yodlee

The IPT has also developed a basic benefit-cost model for this effort based upon rough-order-of-magnitude cost and benefit data. Costs were developed from vendor provided software and hosting costs, estimated development and hosting fees, and estimated operations support and licensing costs. Benefits were estimated from data derived from prior modernization projects and current customer support costs. The preliminary benefits and costs of each alternative are summarized in Appendix D.

## 1. Introduction

This document presents the results of the Single Sign On Request for Information conducted for the Department of Education, Federal Student Aid from March 28, 2002 to April 30, 2002. The purpose of this survey was to evaluate, rank and recommend a vendor to provide a “Single Sign-On” product or service to FSA. Respondents were asked to respond to detailed series of questions to identify the extent that each product/service:

- Meets FSA business and technical requirements,
- Can be supported within the FSA operational environment,
- Provides the scalability and performance levels to meet the expected level of demand,
- Meets FSA security and privacy requirements

Business and technical areas, which each vendor was asked to address included questions in each of the following areas:

### **Business Requirements**

- Customer Support
- Customer Install Base
- Professional Support
- Organization
- Product Vision
- Legal Requirements Support
- Business Strength

### **Technical Requirements**

- Identification and Authentication
- User Management
- Access Management
- Session Management
- Environment
- ISO 15408 Security/Common Criteria
- Operations

The following compilations present the results for those vendors responding to this RFI:

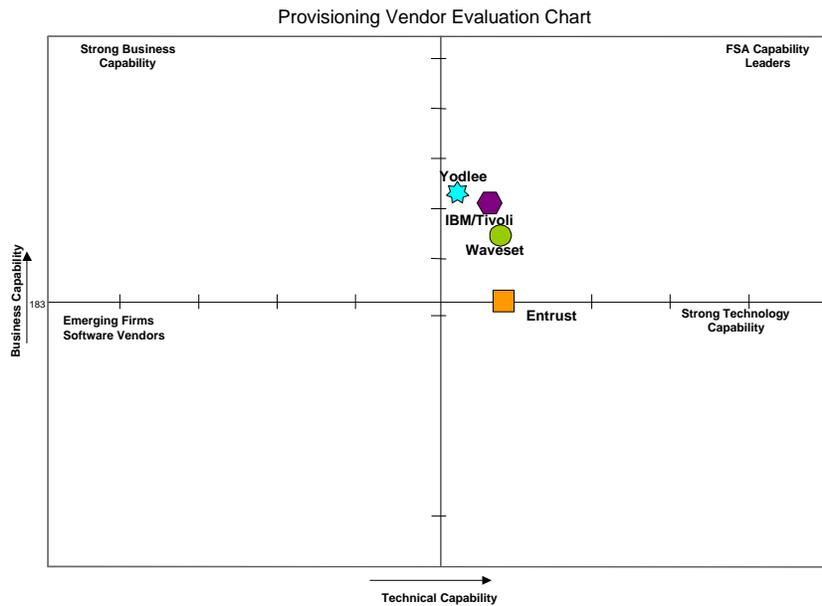
- **Single Sign-On Vendor Evaluation – Quadrant Charts.** Two four-quadrant charts are used to present each vendor’s ‘scores’ with respect to the evaluation of each vendors business and technology capabilities. Vendors were evaluated based upon their survey responses, and external research (e.g., market analyst reports, industry analyst reviews, research papers, news articles, press releases, etc.). Each quadrant groups vendors as Industry Leaders, Strong Business Capabilities, Strong Technology Capabilities, and Emerging Firms/Software Vendors.

- **Vendor Response Status.** This table lists each vendor invited to participate in the survey, and the status of their survey participation (i.e., responded, declined to participate, non-responsive, response in progress).
- **Evaluation Summary.** Presents a summary table depicting the assessed capabilities of each vendor responding to the survey.
- **Vendor Qualification Criteria and Weighting Scheme.** This document describes the how vendors were scored against each survey capability questions, and how each survey capability was weighted.
- **Evaluation Criteria.** Provides the objective qualifications for ranking each vendor as possessing “limited”, “basic”, or “extensive” capabilities for each vendor survey question. These qualifications were review with IPT members and finalized prior to contacting vendors. If a vendor and outside research could not provide a response against a question, the vendor was not ranked against that criterion/capability. This provides an objective mechanism for evaluating vendor responses and external information used to answer each survey questions for each vendor.
- **Vendor Summaries.** Provides a high-level information summary of the financial condition and equity market outlook for each vendor responding to the survey as of March 2002. For public firms basic financial information and key liquidity, operating and solvency financial ratios are provided. For private firms a description of investors and private equity is provided.
- **Preliminary Benefit Cost Summary.** Provides a summary of the development and operations costs and planned benefits for implementing each vendor alternative, and a baseline (“Do nothing”) alternative.

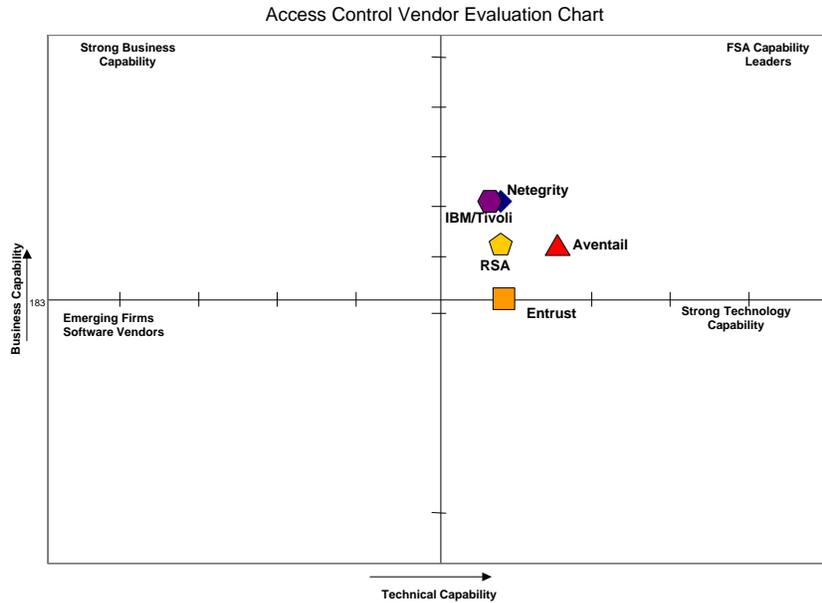
## 2. Vendor Evaluation – Quadrant Charts

The following charts summarize the comparison of each product and service in the two categories evaluated by the IPT team. The scores for each vendor represent a combination of ratings gained from written responses to the RFI, oral presentations to the IPT team, and research from industry analyst and trade organizations.

The first Quadrant chart (See below) shows the provisioning providers capable of providing I+A services to existing legacy systems.



The second Quadrant chart (See below) shows the Access Control vendors capable of providing I+A+E services to new FSA systems.



Section 3 below presents the summary scores from which these quadrant charts were developed. Appendix B presents the detailed scoring for each vendor across each evaluation question.

### 3. Vendor Evaluation Summary

Evaluation Rationale: Each vendor was evaluated based on the same objective evaluation criteria. These criteria are shown in the section “Evaluation Criteria” of this document.

CRITERIA	WAC-VENDOR			WAC & Provisioning		Provisioning	
	Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee
<b>Business Criteria</b>							
Customer Support	70	60	70	60	80	80	85
Customer Install Base	30	40	40	30	40	40	45
Professional Support	25	30	35	15	20	25	30
Organization	3	8	5	7	8	5	4
Product Vision	60	69	66	57	69	60	54
Legal Requirements Support	20	15	30	15	30	25	0
Business Strength	3	6	5	3	5	2	6
<b>SUB-TOTAL BUSINESS SCORE</b>	<b>211</b>	<b>228</b>	<b>251</b>	<b>187</b>	<b>252</b>	<b>237</b>	<b>260</b>

CRITERIA	WAC-VENDOR			WAC & Provisioning		Provisioning	
	Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee
<b>Technical Criteria</b>							
Identification and Authentication	55	55	55	70	55	60	45
User Management	84	81	81	75	81	75	78
Access Management	84	72	78	72	69	75	69
Session Management	20	20	20	20	20	10	20
Environment	48	42	51	51	57	51	42
ISO15408 Security / Common Criteria	75	75	70	65	75	85	80
Operations	42	36	36	30	30	24	33
<b>SUB-TOTAL TECHNICAL SCORE</b>	<b>408</b>	<b>381</b>	<b>391</b>	<b>383</b>	<b>387</b>	<b>380</b>	<b>367</b>
<b>TOTAL SCORE</b>	<b>619</b>	<b>609</b>	<b>642</b>	<b>570</b>	<b>639</b>	<b>617</b>	<b>627</b>

## 4. Solution Synopses

Section provides a brief overview of each vendor, its solution, and an overall summary rating, based on experience, market rating and independent third parties evaluations.

### 4.1 Aventail

**Category:** *Managed Access Control*

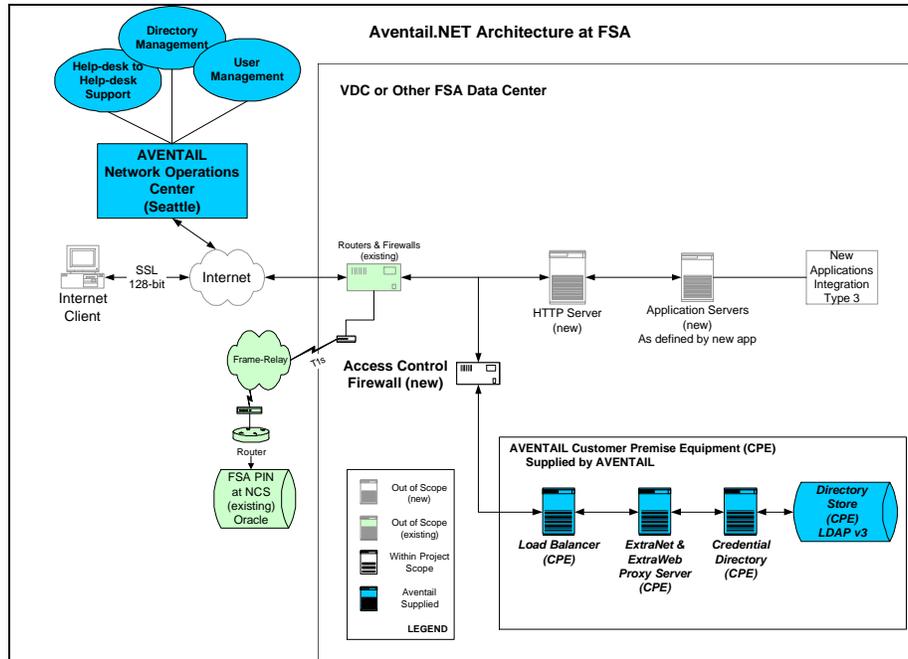
**Competes with:** *Netegrity, IBM, RSA, Entrust*

#### **How It Works:**

Aventail provides secure access over the Internet to an enterprise's network, or specific elements of that network. Aventail installs Customer Premise Equipment (CPE) connected to the network and sitting behind the corporate firewall. Aventail monitors and manages the CPE from a Network Operations Center (NOC) based in Seattle, WA. The CPE's contents are replicated to Aventail's data center, thereby providing a real-time back up and fail over. Aventail's managed services include authentication, authorization, and encryption, plus the option for Aventail to provision the end-user with the requisite credentials. Tier 1 support of end-users and Tier 2 "helpdesk-to-helpdesk" support can be offered through a 24x7 helpdesk. Users login to the portal through the Aventail logon. The browser receives a non-persistent cookie after successful authentication against the Aventail directory. Single Sign On access to protected content occurs via Aventail's proxy server. An encrypted non-persistent cookie is passed with each access request. This cookie keeps track of identity, authorization, and maintains the session.

#### **Architecture:**

Aventail's CPE consists of a redundant servers which would be hosted within an FSA approved data center. Aventail's network operations center (NOC) operates and supports this platform remotely. The NOC holds a duplicate copy of the data maintained in the FSA data center. Aventail's user self-service components are accessed from Aventail's NOC; this data is replicated in real-time from Aventail's NOC to the FSA data center directory.



**Key Technologies:**

- LDAP
- SSL
- DES, Triple-DES, and RC4 encryption; MD4, MD5, and SHA hashes

**Advantages:**

- Complete management of access control technology operations and help desk support for administrators.
- Utilizes redundant LDAPs – one in FSA data center, failover in Aventail NOC - to manage and store user access credentials.
- All internal and external communications of credentials encrypted.

**Disdvantages:**

- Minimal experience with provisioning users on mainframe systems/RACF.
- Requires meta-directory as a central user credential and data store.
- No mechanism to acquire user credentials from back-end user repositories and map these to single sign on users.
- Protected resources require a “Single Sign On Adaptor” for proxy

**Business Overview:**

Aventail is a private venture-funded firm based in Seattle, WA. Aventail currently has 158 employees. Aventail, since its inception in 1996, has raised over \$111 million in capital to fund product development and business expansion; the most recent round of funding was a Series E round of \$55 million in 2001. Aventail will not have any cash flow issues for the next 12 to 18 months, based on this latest funding. Aventail has sold over 400 installs of its products/services; leading commercial clients

include DuPont, FMC, Ernst & Young, and Mount Sinai Hospitals. Aventail has only recently started marketing to government organizations.

**Overall Rating:**

Business Strength	+
Enrollment	++
Identification & Authentication	+++
Invasiveness	++
Provisioning (Legacy)	0
Security	+

## 4.2 Entrust

**Category:** Web Access Control

**Competes with:** Netegrity, IBM, RSA, Aventail

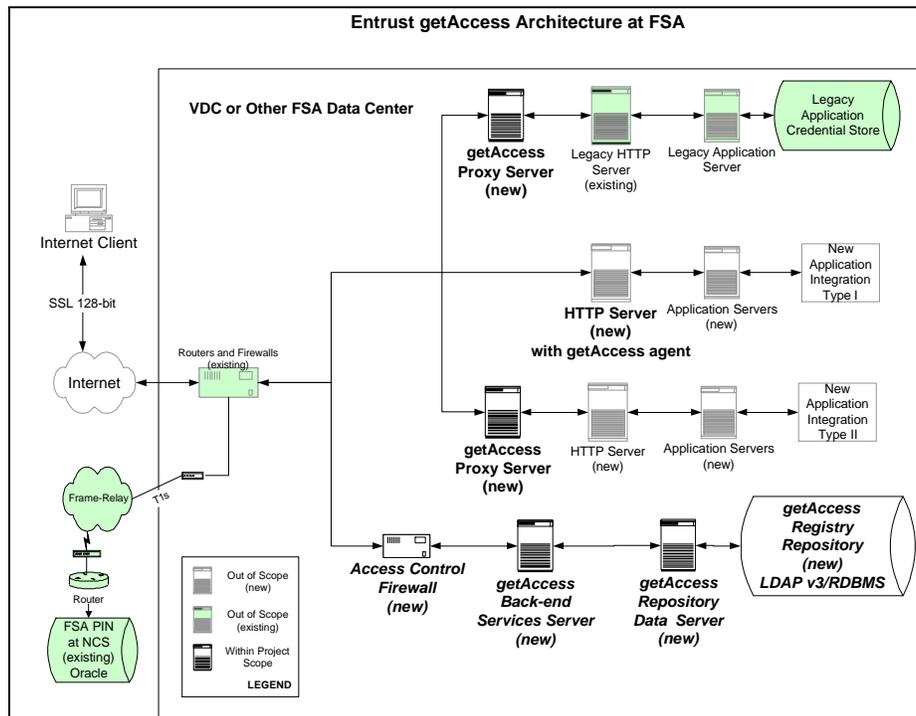
### How It Works:

The first time the user accesses a legacy system; a GetAccess .jsp will collect a username and password from the user to perform a “onetime registration”. This process will 1) verify the username/password with the legacy system, 2) store the username in the Entrust repository entry for the user, 3) encrypt the password and store that in the Entrust repository entry for the user.

On subsequent accesses to an enabled application, the user logs into GetAccess and receives his/her secure userID cookies. When the user arrives at a GetAccess runtime protected resource for a legacy application, GetAccess will have the legacy user ID and password in the extended userID cookie. The legacy user ID and password can be handed to the legacy application based on mechanisms it supports, like accepting information from an http header environment variable..

The GetAccess repository holds mapped account information. This correlates the GetAccess user to the usernames and passwords in the single sign-on enabled backend systems. The mapped account information can be loaded into the repository by: 1) bulk load of user accounts and passwords from the legacy system, or 2) users do a one time registration for each application by logging in with the legacy username and password that is then stored in the GA repository. The one time registration also allows GetAccess to encrypt the users password so it can be stored encrypted in the repository.

### Architecture:



**Key Technologies:**

- Non-persistent cookie
- Reverse Proxy Server OR Runtime Agents
- ODBC Repository

**Advantages:**

- Allows for different authentication types (username/password, X.500, x.509)
- System flexibility

**Disadvantages:**

- Configuration and setup can be complex
- Stability of runtime services in production
- Stores credentials in non-persistent cookie

**Business Overview:**

Entrust is a public company based in Ottawa, Ontario Canada. Entrust currently has 792 employees. Entrust, since 1998 offers it's Single Sign-On product GetAccess. Entrust current assets is worth approximately \$182 Million. Entrust has over 10% market share in the Single Sign-On market. Leading commercial clients include 3COM, Washington Mutural, Sprint, Chevron, Ericsson. Entrust's main market remains the PKI solutions the company has to offer.

**Overall Rating:**

Business Strength	-
Enrollment	+
Identification & Authentication	+++
Invasiveness	++
Provisioning (Legacy)	+
Security	+

### 4.3 Netegrity SiteMinder

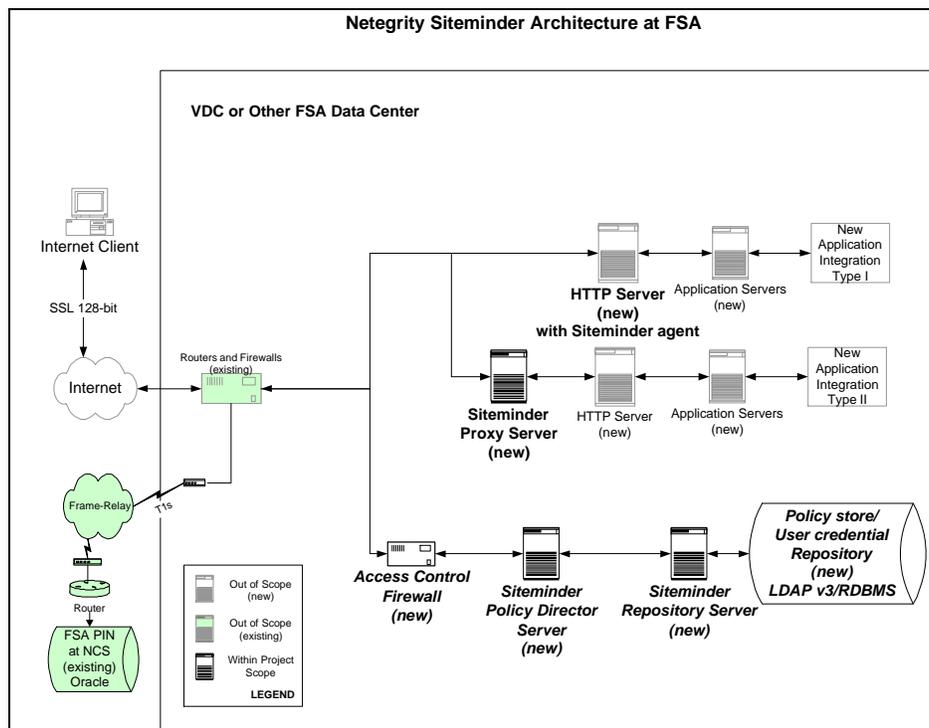
**Category:** Webaccess Control

**Competes with:** Entrust, IBM, RSA, Aventail

#### How does it work?

When a user is registered with Siteminder he receives a non-persistent cookie after successful authentication against the Siteminder Policy server. This cookie is passed with each page request to the Siteminder agent/Siteminder-Proxy server, which keeps track of authorization and performs session management. The cookie has an expiration time, which allows for session timeouts. In case the user clicks on the logout button, the cookie gets overwritten/deleted. If a user session is no longer valid, Siteminder will not allow a user to access any protected resources and instead request the user to authenticate him.

#### Architecture



#### Key technologies

- Non persistent Cookies
- LDAP
- Web-agents (installed on web-server)

### **Advantages**

- Mature product
- Integration to applications via Header variables
- Supports many authentication methods

### **Disadvantages**

- Web agents need to be installed on web server
- Needs LDAP

### **Business Overview:**

Netegrity is a publicly held company based in Waltham, MA. Netegrity currently has 486 employees. Netegrity's current assets are worth \$122 Million. Netegrity has offered its key product Siteminder since 1996. Netegrity has approximately 60% market share. Leading commercial clients include American Express, E\*Trade, General Electric. Netegrity is in the process of expanding the product offer by acquiring other companies. A recent purchase expanded the product offer to include a portal product.

### **Overall Rating**

Business Strength	+
Enrollment	-
Identification & Authentication	+++
Invasiveness	+
Provisioning (Legacy)	0
Security	+++

## 4.4 IBM Access Manager & Identity Manager

**Category:** Web access Control

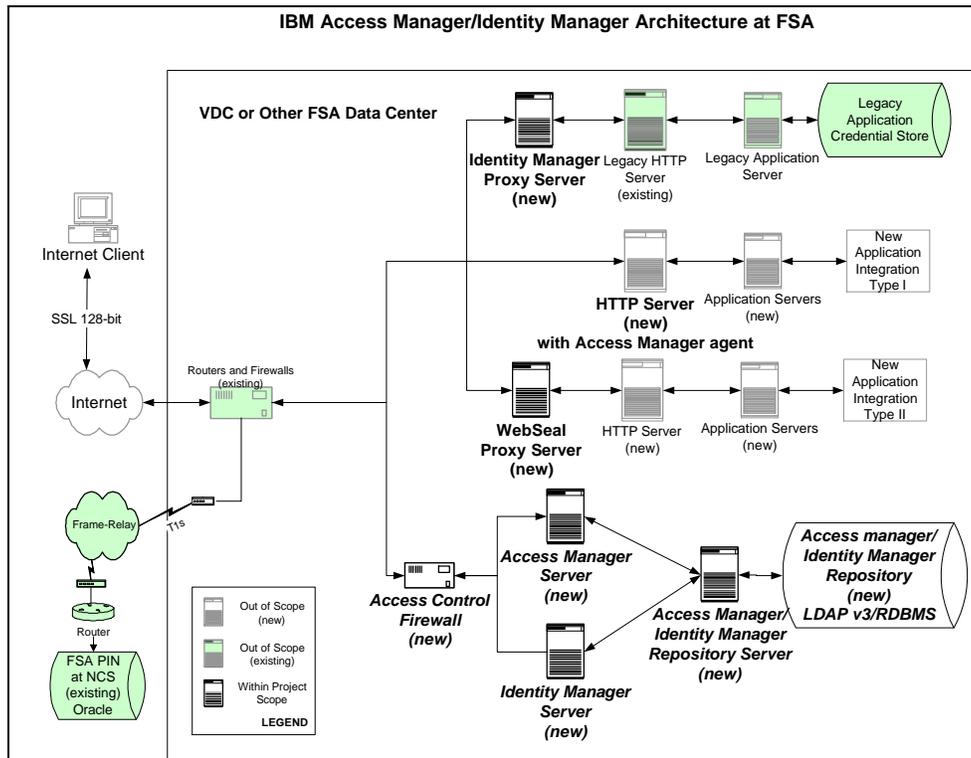
**Competes with:** Entrust, Netegrity, RSA, Aventail

### How It Works:

When users are authenticated, Access Manager grants authorization credentials that include identity information, such as to which groups the users belong and with which roles they are associated.

Access Manager positions a WebSeal server to act as a proxy in front of an existing Web server and its corporate Web resource tree. WebSeal prompts a user for authentication data (i.e., password, certificate, token, or other supported method) to authenticate a user against the LDAP Registry. A session is established and a cookie containing an encrypted session identifier is created on the users browser. When a user requests a resource, the WebSeal server intercepts the request and identifies the protected resource to be accessed. The session identifier is used to identify and obtain credential(s) for the user. Access Manager's Authorization Service then uses this credential to permit or deny access to the resource based on permissions associated with the protected resource.

### Architecture:



**Key Technologies:**

- LDAP
- Supports many authentication methods: User ID and password over HTTP or HTTP-S, Forms-based, X.509 v.3 certificates, RSA SecurID tokens, Mobile identities—phone number/PIN, Wireless Transport Layer Security (WTLS) certificate, Mainframe authentication via SecureWay Security Server for RACF userid and password, Pluggable authentication module (PAM)

**Advantages:**

- Integration Websphere server
- Session cookie maintains session ID only, no user identity information.
- Java 2 and J2EE security support.
- Linkage with SAF APIs to Policy Director services with the capability to authenticate users against RACF.
- Extendable to MQ-Series, UNIX systems, and client security systems.
- Built-in LDAP/DB2 registry, built-in certificate management tools, built-in replication of directory servers, and full administration, including delegated, Web-based GUI.

**Disadvantages:**

- Complex system to integrate
- No mechanism to acquire and map back-end system credentials
- Scalability of solution
- Ability to allow user without single sign on access to Access Manager protected resources

**Business Overview:**

IBM is a public held company based in Austin, TX. IBM currently has over 319,000 employees. IBM current assets are worth over \$41 billion. IBM acquired Tivoli, which offered a product called “Global Sign On” since 1997. IBM has less than 10% market share in the Single Sign-On market. Leading commercial clients include Broadvision, Accenture, PWC. IBM is an experience player in the government market.

**Overall Rating:**

Business Strength	+++
Enrollment	++
Identification & Authentication	+++
Invasiveness	++
Provisioning (Legacy)	+++
Security	+++

## 4.5 Waveset Lighthouse

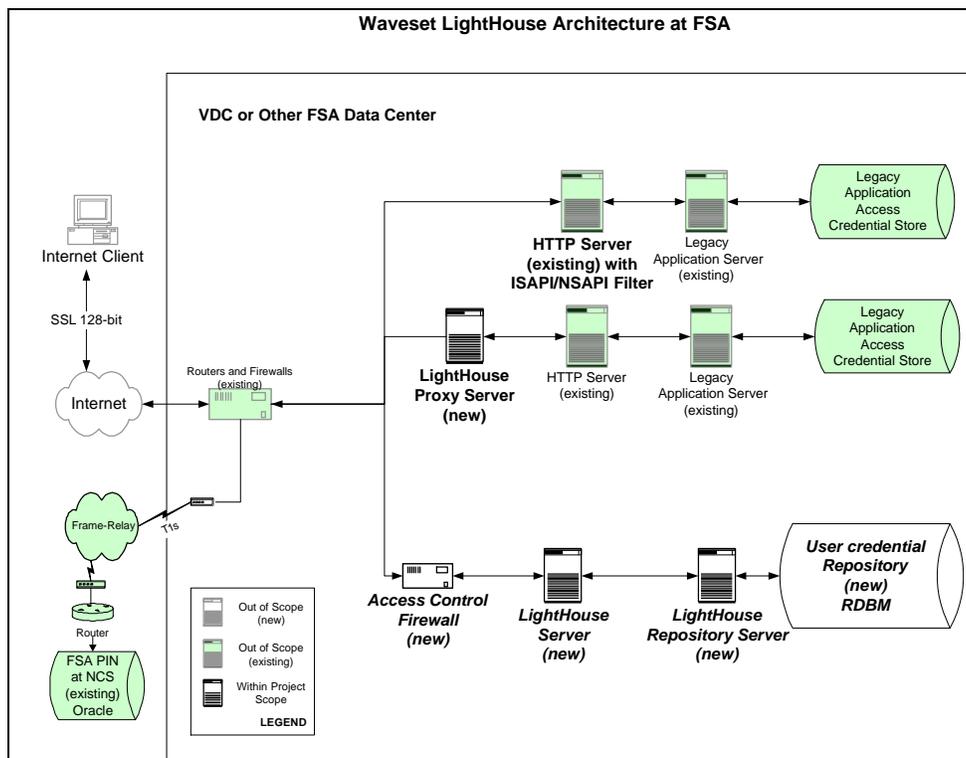
**Category:** Provisioning tools

**Competes with:** Yodlee

### How does it work?

Lighthouse offers Identity management with existing user credential stores. It intercepts an authentication request and provides the necessary credentials for an already authenticated user. If the user is not authenticated, the user is requested to authenticate against Lighthouse. Once authenticated, a non-persistent cookie is sent to the browser, which is sent when a web page is requested and intercepted by Lighthouse-proxy. Through the cookie session management is done. The cookie is deleted once a user clicks on the logout button or the session becomes invalid due to other reasons (e.g. Administrator logs user out).

### Architecture:



### Key technologies

- Java
- Non persistent Cookies
- LDAP

### **Advantages**

- Supports many user credential storages
- Allows for easy administration of complex user data environments

### **Disadvantages**

- Cookie not protected against spoofing
- Proxy solution
- New product

### **Business Overview:**

Waveset is a private venture-funded firm based in Austin, TX. Waveset currently has approximately 60 employees. Waveset, since its inception in January 2000, has raised over \$50 million in capital to fund product development and business expansion. Waveset has announced alliances with all major Single Sign-On vendors. Waveset market share in the Provisioning market is less than 5%. Leading commercial clients include GMAC Financial Services, VISA, and State of Texas. Waveset has only recently started marketing to government organizations.

### **Rating:**

Business Strength	-
Enrollment	+
Identification & Authentication	+
Invasiveness	+++
Provisioning	+++
Security	+

## 4.6 Yodlee

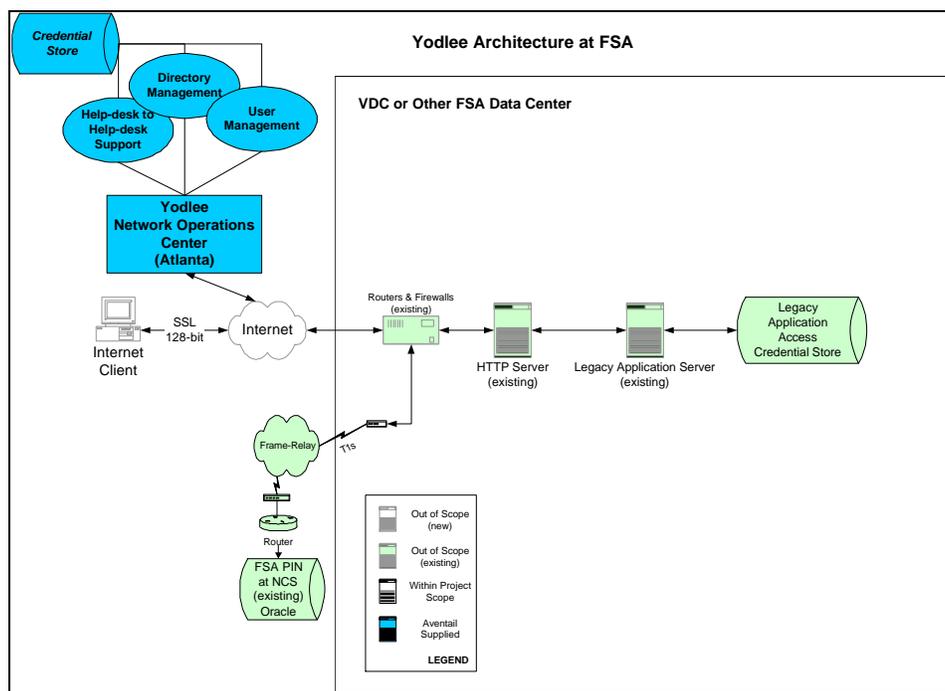
**Category:** Provisioning tools

**Competes with:** Waveset

### How does it work?

Yodlee provides the user with a self-registration service, which allows the user to store all user credentials he/she has with Yodlee. Yodlee can automatically log a user into an account he/she has with an application they registered. Session management is done with a non-persistent cookie. Yodlee provides a completely non-invasive solution. User data is stored in at Yodlee in their data-center. Data is encrypted with two-way encryption or one-way encryption.

### Architecture



### Key technologies

- Soap
- Non persistent Cookies

### Advantages

- Non Intrusive at all
- Security focused
- Experience with financial clients

## Disadvantages

- User credentials stored at Yodlee
- Small company, not public
- New product

## Business Overview:

Yodlee is a private venture-funded firm based in Redwood, CA. Yodlee currently has 161 employees. Yodlee, since its inception in 1999, has raised over \$50 million in capital to fund product development and business expansion. Yodlee is offering its service through a variety of branded services like MyCiti. Yodlee has started as a data aggregation company but has fast expanded into the Single Sign-On market. Leading commercial clients include American Express, Bank of America, Maerica Online, Charles Schwab, Chase, Citigroup, E\*Trade, Fidelity, Palm and Plumtree. Yodlee has so far no experience in the government market space but extensive experience with clients in the financial market space.

## Overall Rating:

Business Strength	-
Enrollment	+
Identification & Authentication	0
Invasiveness	+++
Provisioning (Legacy)	+
Security	+

## 4.7 RSA Security – Cleartrust

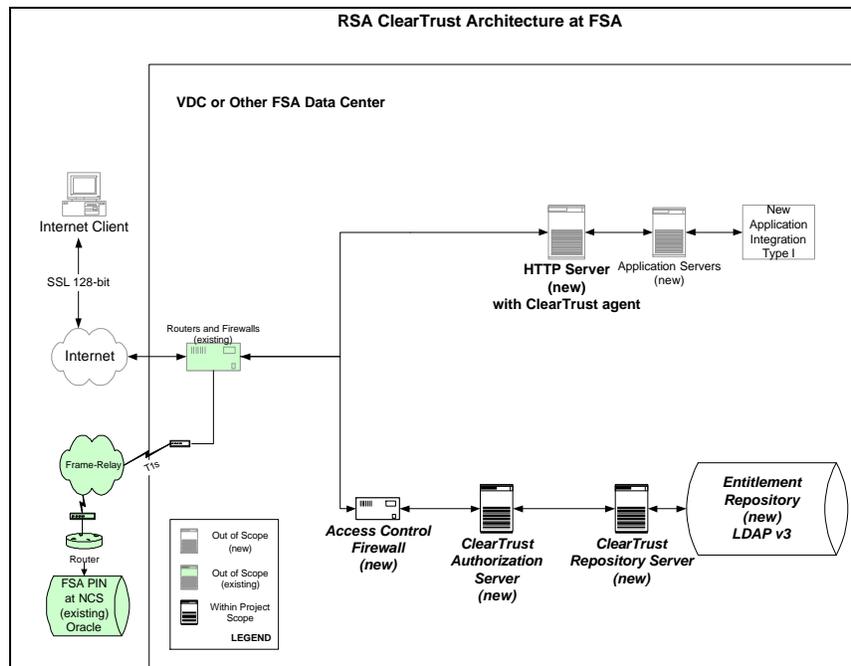
**Category:** Web access Control

**Competes with:** IBM, Netegrity, Entrust, Aventail

### How does it work?

RSA ClearTrust uses a web-plug-in approach. The Plug-Ins get installed on the various web-servers, which check for a valid session each time a user requests a web page that is protected by ClearTrust. The model is close to the model Netegrity uses but is different in the capabilities each Plug-In has. This is true in regards of data replication, which is done for performance reasons. In addition to the Plug-In model a proxy sever model is available. Session management is done with non-persistent cookies. The Cleartrust agent intercepts the cookie and checks for a valid session. If the cookie is not present, the user is requested to authenticate. No access is granted to protected resources if the user is not authenticated and authorized to have access.

### Architecture:



### Key technologies

- LDAP
- Java based application

### **Advantages**

- Agent or reverse proxy architecture
- Supports RSA Secure-ID tokens and certificates

### **Disadvantages**

- Supports only the use of iPlanet's LDAP with release 4.7
- Not certified on HP-UX

### **Business Overview:**

RSA is a publicly held company based in Bedford, MA. RSA currently has over 51,000 employees. RSA, since its inception in 1984, has acquired several companies. In 2001 RSA acquired Securant and became a player in the Single Sign-On space. RSA current assets are worth over \$146 million. RSA main market stays the PKI, encryption and token-based authentication market space. RSA has only recently started integrating Securant's Single Sign-On product into it's overall product suite.

### **Overall Rating:**

Business Strength	++
Enrollment	+
Identification & Authentication	+++
Invasiveness	+
Provisioning (Legacy)	0
Security	+++

## Appendix A. Vendor Information Summaries

### Entrust:

Vendor Name:	Entrust
Vendor Address:	<p>One Hanover Park                  16633 Dallas Parkway                  Suite 800                  Addison, TX 75001</p> <p><u>RFI Contacts:</u>                  Jennifer Moran                  Systems Engineer  <a href="mailto:jennifer.moran@entrust.com">jennifer.moran@entrust.com</a>                  Phone: 703-269-2031                  Patty Arcano                  Account Executive  <a href="mailto:patricia.arcano@entrust.com">patricia.arcano@entrust.com</a>                  Phone: 703-269-2015</p> <p>Entrust                  8300 Greensboro Rd Ste 250                  McLean VA 22102</p> <p>Wayne Throop                  Strategic Partner Relationship Manager                  Phone: 613-270-3758                  Cell: 613-715-3758                  Fax: 613-270-3050  <a href="mailto:Wayne.Throop@entrust.com">Wayne.Throop@entrust.com</a></p> <p>Entrust                  1000 Innovation Drive                  Ottawa, Ontario Canada                  K2K 3E7</p>
Years in Single Sign-On Business:	Single sign on solutions offered since January, 1998. getAccess single sign on product acquired through acquisition of enCommerce.
Private or Publicly Held:	Publicly Held (ENTU on Nasdaq)
Type of Product:	COTS access control, PKI
Major Clients:	3COM, Washington Mutual, Sprint, Chevron, Ericsson
Alliances/Partnerships:	Microsoft, BEA Systems, etc., Accenture, Deloitte & Touche, KPMG, PwC, etc.
Rank in total SSO Marketplace:	#2 vendor
Total percent of SSO market that they represent:	Over 10%
Other Major Products	<p>Products: Authority (PKI based security management), Entelligence (security for client side enterprise applications), TruePass (Identification, verification and privacy)</p> <p>Solutions: Certificate Services, Enterprise Desktop, Secure Web Portal, VPN</p>

Fundamentals (\$millions)  
 Current Assets = \$182.489  
 Receivables = \$25.452

Total Assets = \$229.438  
Current Liabilities = \$93.477  
Total Liabilities = \$93.593  
Retained Earnings = \$-645.190  
Sales = \$47.8  
EBITDA = \$-.475.0  
Market Cap (5/07/02) = \$262.9

Liquidity Ratios

Current Ratio = 1.95  
Current Cash = \$ 24.241 million  
Cash Flow = \$ -58.5 million  
\$ 21 million for Year 2001 due to financing activities  
Cash Flow Trend = Downward for Operations

Operating Ratios

Sales/Receivables = 1.9  
Return on Assets = -141.82%

Solvency Ratios

Debt to Worth Ratio = .6881  
Working Capital = \$89.012 million  
Z-Score = -10.37

---

**Netegrity:**

Vendor Name:	Netegrity
Vendor Address:	Netegrity 52 Second Ave Waltham, MA 02451  RFI Contacts: Robert M. Marti II Netegrity Proposal Manager Work: (781) 663-8715 Cell: (781) 308-5475 <a href="mailto:rmarti@netegrity.com">rmarti@netegrity.com</a>  Eric Hay Systems Engineer <a href="mailto:ehay@netegrity.com">ehay@netegrity.com</a>  Peter Morrison Account Executive Phone 703.715.3002 Cell 703.282.6622 <a href="mailto:pmorrison@netegrity.com">pmorrison@netegrity.com</a> Netegrity
Years in Single Sign-On Business:	SiteMinder has existed since 1996
Private or Publicly Held:	Public (NETE Nasdaq)
Type of Product:	COTS Solution
Major Clients:	American Express, E*Trade, General Electric
Alliances/Partnerships:	Verisign, Deloitte & Touche, Ernst & Young, Microsoft
Rank in total SSO Marketplace:	First
Total percent of SSO market that they represent:	Approximately 60%
Other Major Products	SRM Platform, Interaction Server, SiteMinder, SiteMinder DMS, SiteMinder Secure Proxy Server, Affiliate Services, SiteMinder Security Bridge, SAML Knowledge Center, JSAML Toolkit, SDK

**Fundamentals (\$millions)**

Current Assets = \$122.523  
 Receivables = \$16.122  
 Total Assets = \$204.179  
 Current Liabilities = \$30.038  
 Total Liabilities = \$30.038  
 Retained Earnings = \$-20.432

Sales = \$23.036  
 Market Cap (5/7/02) = \$239.2

**Liquidity Ratios**

Current Ratio = 4.1  
 Current Cash = \$ 118.059 million  
 Cash Flow = \$ -8.28 million for Operations  
 \$ 7.1 million in Year 2001 due to financing activities  
 Cash Flow Trend = Downward for Operations

Operating Ratios

Sales/Receivables = 1.429  
Return on Assets = -2.61%

Solvency Ratios

Debt to Worth Ratio = .1725  
Working Capital= \$92.485 million  
Z-Score = 4.2

---

**IBM:**

Vendor Name:	IBM
Vendor Address:	IBM Center of Operations for Tivoli Software 11400 Burnet Rd Austin, TX 78758  RFI Contacts: Bob Rosscoe IBM Global Services - Federal 6710 Rockledge Drive Bethesda, MD 20817 Phone: 301-803-6974 Cell Phone: 410-908-8754 Fax: 410-750-1329 Pager: 800-946-4646, 6055700 Internet: <a href="mailto:rosscoe@us.ibm.com">rosscoe@us.ibm.com</a>  Michael Tucker IBM Contracts Representative for Accenture, <a href="mailto:mtucker@us.ibm.com">mtucker@us.ibm.com</a> 301-803-2081  Sean McDonald 703-287-4427  Rayette Lantzy 703-287-4400
Years in Single Sign-On Business:	Global Sign On has existed since July 1997
Private or Publicly Held:	Publicly Held – IBM
Type of Product:	COTS Solution
Major Clients:	T. Rowe Price
Alliances/Partnerships:	Broadvision, Accenture, PwC
Rank in total SSO Marketplace:	unknown
Total percent of SSO market that they represent:	Less than 10%
Other Major Products	e-business infrastructure, Configuration and Operations, OS/390, Storage, Web, Performance & Availability

**Fundamentals (\$billions)**

Current Assets = \$41.461  
 Receivables = \$29.420  
 Total Assets = \$88.313  
 Current Liabilities = \$35.119  
 Total Liabilities = \$64.699  
 Retained Earnings = \$24.997

Sales = \$21.044  
 EBITDA= \$14.1  
 Market Cap (5/9/02) = \$137.4

**Liquidity Ratios**

Current Ratio = 1.8  
 Current Cash = \$ 7.72 billion  
 Cash Flow = \$ 15.265 billion

Cash Flow Trend = Positive cash flows for IBM Corp.

Operating Ratios

Sales/Receivables = .715  
Return on Assets = 8.38%

Solvency Ratios

Debt to Worth Ratio = 1.4872  
Working Capital= \$6.3420 billion  
Z-Score= 2.5

---

**Aventail:**

Vendor Name:	Aventail
Vendor Address:	<p>Aventail Corporation                  808 Howell St.                  Second Floor                  Seattle, WA 98101</p> <p>RFI Contacts:                  Brandon Conley (primary)                  Sr. Territory Manager - Mid Atlantic                  Aventail, Inc.                  Office (410) 576 8977                  Mobile (301) 775 6250  <a href="mailto:bconley@aventail.com">bconley@aventail.com</a>                  400 East Pratt Street                  Suite 807                  Baltimore, MD 21202</p> <p>Todd Haugen                  c) 206.619.2833                  o) 206.808.0202    <a href="mailto:richard@aventail.com">richard@aventail.com</a></p> <p>Suzie Bailey                  Manager, Engagements                  Office: 206.808.0234                  Mobile: 206.617.9152                  fax: 206-576-0388</p>
Years in Single Sign-On Business:	Since April 1997
Private or Publicly Held:	Private, founded 1996
Type of Product:	Managed Service Provider
Major Clients:	NBC, Kraft, Dupont
Alliances/Partnerships:	Exodus, Verisign, RSA Security
Rank in total SSO Marketplace:	Leader in the Gartner 2002 Managed Remote Access Magic Quadrant for North America.
Rank in product specific SSO marketplace:	First for managed service providers. Ranked best product by Gartner Group for Managed Remote Access.
Total percent of SSO market that they represent:	unknown
Other Major Products	VPN, Extranet Services

Fundamentals (\$millions)  
 Venture Capital Raised = \$111 million +

Aventail is a private company, therefore financial data is not available:

**Waveset:**

Vendor Name:	Waveset
Vendor Address:	<p>Waveset Technologies, Inc.                  6850 Austin Center Blvd., Suite 205                  Austin, TX 78731</p> <p>RFI Contacts:                  Martin D. Fredrickson                  Vice President, Strategic Channels                  Phone 703-496-011                  Cell 703-407-5372  <a href="mailto:martin.fredrickson@waveset.com">martin.fredrickson@waveset.com</a>                  6850 Austin center Blvd.                  Suite 205                  Austin, TX 78731</p> <p>Shawn B. Benson                  Regional Sales Manager                  Phone: 703-904-7411                  Fax: 703-478-0936                  Cell: 703-623-0540  <a href="mailto:shawn.benson@waveset.com">shawn.benson@waveset.com</a>                  171 Elden St.                  Suite 160                  Herndon, VA 20170</p> <p>Phil McQuitty                  Senior Software Engineer                  Phone: 703-904-7123                  Fax: 703-478-0936                  Cell: 703-626-9997  <a href="mailto:phil@waveset.com">phil@waveset.com</a>                  171 Elden St.                  Suite 160                  Herndon, VA 20170</p>
Years in Single Sign-On Business:	Since January 2000
Private or Publicly Held:	Private
Type of Product:	COTS Provisioning Solution, SSO Toolkit
Major Clients:	GMAC Financial Services, VISA, State of Texas
Alliances/Partnerships:	BEA, IBM, Netegrity, Microsoft, RSA, Booz Allen & Hamilton,
Rank in total SSO Marketplace:	Rated 1 <sup>st</sup> in Enterprise User Administration by Gartner, Most Innovative Product by eWeek
Rank in product specific SSO marketplace:	Second in the Provisioning space
Total percent of SSO market that they represent:	Less than 5%
Other Major Products	None

Fundamentals (\$millions)

Venture Capital Raised = \$50 million +

Waveset is a private company therefore the following financial data is not available:

- Liquidity Ratios
- Operating Ratios

**Yodlee:**

Vendor Name:	Yodlee
Vendor Address:	Yodlee, Inc. 3600 Bridge Parkway, Suite 200 Redwood City, CA 94065  RFI Contact: Jeff Neasmith Yodlee, Inc. Senior Business Development Manager 3600 Bridge Parkway, Suite 200 Redwood City, CA 94065 650-980-3640 Direct 650-980-3840 Fax <a href="mailto:jeff@yodlee.com">jeff@yodlee.com</a>
Years in Single Sign-On Business:	Since 1999
Private or Publicly Held:	Private
Type of Product:	ASP singles sign on and data aggregator
Major Clients:	American Express, Bank of America, America Online, Charles Schwab, Chase, Citigroup, e*Trade, Fidelity, Palm, Plumtree
Alliances/Partnerships:	Quicken
Rank in total SSO Marketplace:	Unknown
Total percent of SSO market that they represent:	Unknown
Other Major Products	e-Personalization, Financial Aggregation, "screen scrapers"

Fundamentals (\$millions)

Venture Capital Raised = \$50 million +

Waveset is a private company therefore the following financial data is not available:

- Liquidity Ratios
- Operating Ratios

**RSA Security:**

Vendor Name:	RSA Security
Vendor Address:	RSA Security Inc. 174 & 175 Middlesex Turnpike Bedford MA, 01730 <a href="http://www.rsasecurity.com">www.rsasecurity.com</a>  Sales Point of Contact: Zia Fatemi Federal Strategic Account Manager RSA Security 8230 Leesburg Pike Suite 620 Vienna, VA 22182 703-288-9300 Ext 306 Cell 301-266-5978 <a href="mailto:zfatemi@rsasecurity.com">zfatemi@rsasecurity.com</a>  Technical Point of Contact: Sean Murray System Engineer RSA Security 8230 Leesburg Pike Suite 620 Vienna, VA 22182 703-288-9300 Ext 307 <a href="mailto:smurray@rsasecurity.com">smurray@rsasecurity.com</a>
Years in Single Sign-On Business:	Since 2001 (Purchased Securant Technologies). RSA established 1984.
Private or Publicly Held:	Public
Type of Product:	COTS access control
Major Clients:	
Alliances/Partnerships:	
Rank in total SSO Marketplace:	
Total percent of SSO market that they represent:	
Other Major Products	PKI; encryption; system security; token authentication (SecureID)

**Fundamentals (\$millions)**

Current Assets = \$ 146.215  
 Receivables = \$ 61.282  
 Total Assets = \$ 509.114  
 Current Liabilities = \$ 79.599  
 Total Liabilities = \$ 155.701  
 Retained Earnings = \$ 451.320  
 Sales = \$ 261.9  
 EBITDA = \$ -43.9  
 Market Cap (9/21/00) = \$ 336.5

**Liquidity Ratios**

Current Ratio = 1.8  
 Current Cash = \$ 539.001 million  
 Cash Flow = \$ -7.685 million from Operations

Cash Flow Trend = Downward for Operations

Operating Ratios

Sales/Receivables = 4.27  
Return on Assets = -4.80%

Solvency Ratios

Debt to Worth Ratio = .2252  
Working Capital= \$66.62 million  
Z-Score= 3.2

## Appendix B. Vendor Evaluation Matrix

### B.1 Criteria and Weighting Scheme

In order to rank the responding vendors, the evaluation links a numeric value to both the evaluation survey question and the weighting factor of each capability area. The relationships between the qualitative and quantitative analysis follows:

#### Survey Question Scale Relationship

Evaluation Scale	Numeric Equivalent
No Response/No Qualifications	0
Limited or None	1
Basic or Some	2
Extensive or Complete	3

#### Weighting Factor Relationship

Capability Area Scale	Weighting Factor	Capabilities Included In This Weighting
Required but not differentiating	1	Business Organization Business Strength
Important to business or technical requirement	3	Business Product Vision Technical User Management Access Management Environment Operations
Critical to FSA needs	5	Business Customer Support Customer Installation Base Professional Support Legal Requirements Support Technical Identification and Authentication Session Management Security/Common Criteria

The weighting relationship was put on a 1-3-5 scale to emphasize the differences in importance.

The following table presents each capability area and capability weighting factor; and each criteria/survey question and the rating justifications for each criteria/survey question.

### B.2 Vendor Evaluation Summary

Evaluation Rationale: Each vendor was evaluated based on the same objective evaluation criteria. These criteria are shown in the section “Evaluation Criteria” of this document.

Business Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Customer Support	5	70	60	70	60	80	80	85	105
Describe your customer service model, including help desk operations and customer communications methods. Describe your model for Tier 1, Tier 2, and Tier 3 support, as appropriate.	.	3	2	3	2	2	2	3	3
What is the mix of customer service and operations personnel types (permanent, sub-contract, outsourced)? How many certified staff do you have for providing implementation support?	.	1	3	3	3	3	3	3	3
How do you hire, train, maintain skilled employees?	.	2	2	0	1	3	2	3	3
Describe the product/service documentation and tutorials provided to customers.	<input type="checkbox"/>	2	3	3	2	3	3	2	3
Describe the training provided to customer users, administrators, and IT staff: documentation, classes, CBT, tutorials, certifications, other.	<input type="checkbox"/>	1	2	3	1	2	2	2	3
Describe the customer self service capabilities contained within your product/service. Describe how your product/service provides tools for help desk support of users.	<input type="checkbox"/>	3	1	0	3	1	3	2	3
Describe your development, administrator and end user technical support capabilities.	.	2	2	2	0	2	1	2	3
Describe and identify corrective actions taken and the process of communicating remedies/fixes/patches to customers.	Not Evaluated	-	-	-	+	-	-	-	-
Customer Install Base	5	30	40	40	30	40	40	45	60

Business Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Describe how your product/service supports system login/access support for business-to-business users. Can your product/service support access by 30,000 b-to-b users?	<input type="checkbox"/>	1	1	3	2	2	2	3	3
How many total users, by average installation, does your product/service support?	*	2	1	1	1	2	2	2	3
How many users can your product/service support? What is the size, in terms number of supported single sign on user, of your largest installation?	*	1	3	3	3	3	3	3	3
How many users identified and authenticated by complex mechanisms (i.e., other than simple username/password – using multi-factor, biometrics, PKI, etc.) does your product support?	*	2	0	1	0	1	1	1	3
<b>Professional Support</b>	<b>5</b>	<b>25</b>	<b>30</b>	<b>35</b>	<b>15</b>	<b>20</b>	<b>25</b>	<b>30</b>	<b>45</b>
How much elapsed time does a typical installation of your product/service require? What is the typical team required, including vendor, client, and integrator resources? What is the typical cost of these installations? Consider installations against ODBC, ERP, mainframe/RACF, and web front-end interfaces.	<input type="checkbox"/>	2	2	3	no response	no response	1	2	3
What levels of implementation, ongoing support, and professional services support do you offer?	<input type="checkbox"/>	1	2	3	2	3	3	2	3
What types of professional services are bundled with the initial service installation? Are professional services staff internal, contract, or partner resources?	<input type="checkbox"/>	2	2	1	1	1	1	2	3
<b>Organization</b>	<b>1</b>	<b>3</b>	<b>8</b>	<b>5</b>	<b>7</b>	<b>8</b>	<b>5</b>	<b>4</b>	<b>9</b>

Business Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
How many people are permanent employees of your company? Identify numbers in each of the following roles: Sales & Marketing, Research & Development, Customer Support and Training, Professional Services, Management, Administration.	•	1	3	2	2	3	1	1	3
What is the management organization of your company?	•	1	2	1	2	3	2	2	3
Describe your firm's membership and participation in software security industry groups, technology organizations, and standards committees?	•	1	3	2	3	2	2	1	3
<b>Product Vision</b>	<b>3</b>	<b>60</b>	<b>69</b>	<b>66</b>	<b>57</b>	<b>69</b>	<b>60</b>	<b>54</b>	<b>81</b>
What supplier and service alliances have you developed? Identify any other partnerships or investments.	•	3	3	3	3	3	2	2	3
What is your marketing and sales approach for this product?	•	2	3	2	3	3	2	2	3
What is the current installed base of customers? How many implementations have you performed for government/not-for-profit customers? How many customers are supported in each geographic area your firm operates?	□	2	2	3	3	3	2	2	3
Describe upcoming modifications or enhancements to your products/services.	•	2	2	3	0	2	2	2	3
Describe your user provisioning operations.	•	2	2	0	2	2	3	1	3
What is your product/service's release history? Describe products, current releases supported, and when the product/service was first released.	•	3	3	3	3	3	3	1	3
What external functionality is available to your product/service via interface or API?	•	2	3	3	3	2	2	2	3

Business Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Describe Research and Development (i.e., future product development) activities you are pursuing within security, privacy, access control, and related areas. Describe your product roadmap.	•	3	3	3	0	3	2	3	3
Describe your firm's capabilities to integrate external applications, systems, and technologies into your product/service	•	1	2	2	2	2	2	3	3
<b>Legal Requirements Support</b>	<b>5</b>	<b>20</b>	<b>15</b>	<b>30</b>	<b>15</b>	<b>30</b>	<b>25</b>	<b>40</b>	<b>60</b>
Describe how your product/service supports providing legal notices and protections for Privacy Act and proprietary/confidential data maintained within the Single Sign-On service.	<input type="checkbox"/>	1	1	2	1	1	1	2	3
Describe your product/service's compliance with Federal ADA/Section 508 requirements.	<input type="checkbox"/>	0	0	0	0	2	2	1	3
Describe how your product/service supports the display of legal messages and other messages to users connecting to business systems through the Single Sign-On service.	<input type="checkbox"/>	1	1	1	1	2	1	2	3
Does your product/service support application requests to re-authenticate users to a business application they are already logged into?	<input type="checkbox"/>	2	1	3	1	1	1	3	3
<b>Business Strength</b>	<b>1</b>	<b>3</b>	<b>6</b>	<b>5</b>	<b>3</b>	<b>5</b>	<b>2</b>	<b>2</b>	<b>6</b>
Provide a copy of the latest annual and quarterly report (if public), Dun & Bradstreet number or report.	•	0	3	2	1	3	0	0	3
Provide a synopsis of market and industry analysts reports describing your firm and product and comparing your product to competitor products/services.	•	3	3	3	2	2	2	2	3

Business Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Describe your firm's documented strengths and weaknesses over your competitors in the Access Control marketplace.		-	-	-	-	-	-	-	
Describe what you perceive as weaknesses in your competitors' solutions?		-	-	-	-	-	-	-	
<b>SUB-TOTAL BUSINESS SCORE</b>	<input type="checkbox"/>	<b>211</b>	<b>228</b>	<b>251</b>	<b>187</b>	<b>252</b>	<b>237</b>	<b>260</b>	<b>366</b>

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
<b>Identification and Authentication</b>	<b>5</b>	<b>55</b>	<b>55</b>	<b>55</b>	<b>70</b>	<b>55</b>	<b>60</b>	<b>45</b>	<b>90</b>
Describe support for configurable username formats which support Federal/NIST 800-18 guidelines. Describe how username formats/business rules are configurable.		2	2	1	3	2	2	1	3
Describe support for configurable password formats which support Federal/NIST 800-18 guidelines. Describe how password formats/business rules are configurable.		2	2	3	2	2	2	1	3
Describe how the product/service allows for extensions and additions to its authentication mechanism. Describe any APIs supported and any support for Pluggable Authentication Modules.		1	2	2	2	2	2	2	3
Describe your solutions capabilities to allow for flexible creation of usernames.		2	1	1	2	1	2	1	3
What types of identification credentials does your service support? What types of authentication data stores does your service support? Do you provide support capability for custom credentials?		2	2	2	2	2	2	2	3
Describe your ability to use CA/PKI, tokens, or other mechanisms to provide authentication services		2	2	2	3	2	2	2	3
<b>User Management</b>	<b>3</b>	<b>84</b>	<b>81</b>	<b>81</b>	<b>75</b>	<b>81</b>	<b>75</b>	<b>78</b>	<b>126</b>
Identify how your product/service provides a mechanism for a privileged administrator to change access rights of individuals, roles, and/or groups.		2	2	2	2	2	2	1	3
Describe your product/service's ability to create usernames and passwords or accept usernames and passwords created by trusted sources.		1	2	1	2	3	2	2	3

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Describe your product/service's ability to enable the categorization of like users using roles and/or groups. Are roles and groups handled the same way individual users are handled? Explain.		2	3	3	2	2	3	11	3
Describe your product/service's ability to communicate Single Sign-On user credentials to existing credential repositories. Identify types of credential stores supported - e.g., RACF, ODBC, UNIX, NT, Novell, LDAP, Oracle Financials, ERPs, etc.)		2	1	2	2	3	3	1	3
Describe how your product/service supports delegated administration of access policies and functions for users, roles, groups of users, an application, or a set of applications by appointed administrators granted limited administration and management rights.		2	2	3	2	2	2	1	3
FSA desires to store minimal user data in the Single Sign-on user data repository. Identify your product/service's ability to configure a user data store and/or credential store.		2	2	2	1	2	1	2	3
Describe your product/service's capabilities to allow manual and/or automatic revocation of users.		2	2	2	2	1	2	1	3
Describe your product/service's capabilities to disable accounts based on inactivity and/or a definable number of unsuccessful login attempts.		2	2	3	2	1	0	2	3
Password administration must be automated and only require minimal manual interaction with the single sign-on administrator. Describe your product/service's capabilities to administer passwords within the single sign-on service and within enabled back-end systems.		2	2	1	2	1	2	1	3

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Describe your product/service's capabilities to automatically audit/check single sign-on user credential(s) against definable rules/standards.		1	1	1	1	2	1	1	3
Describe your product/service's capabilities to store Single Sign-On user credentials securely and in a protected manner.		2	2	0	2	1	2	2	3
Describe your products/service's user registration, and service update/change processes		3	2	2	1	3	3	1	3
Describe capabilities to assign access control against resources		3	2	3	2	3	1	0	3
Describe the controls in place to administer access controls, and to permit management of access credentials		2	2	2	2	1	1	0	3
<b>Access Management</b>	<b>3</b>	<b>84</b>	<b>72</b>	<b>78</b>	<b>72</b>	<b>69</b>	<b>75</b>	<b>69</b>	<b>135</b>
Describe your product/service's support for exit/signoff options to end a user's active session with all applications accessed through Single Sign-On.		1	2	3	3	2	1	2	3
Describe your product/service's support for the removal/deletion of users from the Single Sign-On service		3	2	3	2	2	3	2	3
Identify and describe your product/service's tools to administer access to applications and resources		0	1	1	1	2	1	1	3
Identify the user access mechanisms supported by your product/service - e.g., internet, voice response unit, dedicated, etc.		1	1	1	1	1	1	1	3
Describe your product/service's support for user authentication via passwords, tokens, or other devices compliant with NIST 800-18.		2	1	1	2	1	1	1	3
Describe your product/service's controls to restrict users to authorized Single Sign-On transactions and functions compliant with NIST 800-18		2	1	1	1	1	2	1	3

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
NIST 800-18									
Describe your product/service's ability to audit/log activity involving access to and modification of sensitive or critical Single Sign-On files in compliance with NIST 800-18. Describe the capabilities to capture, record and report events related to access requests and access control administration.		2	2	2	2	1	2	1	3
After a successful login, describe your product/service's capability to provide a message with information about last successful login and how many unsuccessful login attempts have been made in the meanwhile.		1	2	1		1	2	1	3
Describe your product/service's capability to define custom access rules.		3	2	1	1	1	2	1	3
Describe your product/service's ability to capture user actions to allow for accountability logging and auditing.		1	1	1	1	2	1	1	3
Describe your product/service's support for secure communication between systems and the Single Sign-On data store.		3	2	3	2	2	2	3	3
Describe your product/service's capabilities to protect data at rest and in transit.		2	2	2	2	1	2	3	3
Describe your product/service's support for services/mechanisms allowing administrators and users to be enrolled and authorized for single sign-on administration and use.		2	1	1	1	2	1	2	3
Describe your capabilities to record privileged activity against secured resources, and to ensure that users without proper privileges have not accessed a secured resource.		2	2	2	3	1	2	2	3

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Describe your access control / authentication security operations.		3	2	3	2	3	2	1	3
<b>Session Management</b>	<b>5</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>10</b>	<b>20</b>	<b>30</b>
Describe your product/service's mechanism(s) for session management. Describe your use/non-use of cookies.		2	2	2	2	2	2	2	3
Describe your product/service's capabilities to establish, manage and monitor user sessions		2	2	2	2	2	0	2	3
<b>Environment</b>	<b>3</b>	<b>48</b>	<b>42</b>	<b>51</b>	<b>51</b>	<b>57</b>	<b>51</b>	<b>42</b>	<b>90</b>
Identify the operating systems supported by your product/service. What is your preferred operating system?		2	1	1	2	2	1	3	3
Identify the web servers supported by your product/service. What is your preferred web server?		2	2	2	2	2	2	2	3
Identify the application servers supported by your product/service. What is your preferred application server?		3	2	2	2	1	2	0	3
Identify the proxy servers supported by your product/service. What is your preferred proxy server?		2	1	1	1	1	2	1	3
Identify the databases, directories, and other credential data stores supported by your product/service. Identify other security products/repositories (e.g., RACF, ACF2, TOPSECRET, etc.) are supported by your product/service.		1	1	2	2	2	2	1	3
Identify the Internet browsers supported by your product/service.		2	2	2	2	2	2	2	3
Identify the EAI, middleware, and other products/service supported by your product/service. Identify your product/service's ability to integrate to character-based systems web-enabled by		1	0	1	1	3	1	1	3

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Citrix.									
Identify changes or additions to existing business application software or technical infrastructure required by your single sign-on product/service to enable an application.		2	2	2	1	2	2	1	3
Describe your support of standards for access control, data, authentication, communications, Federal guidelines (e.g., Section 508, OMB A-130, FIPS PUBS, NIST 800, Common Criteria/ISO15408, etc.), and other industry standards.		1	2	2	2	2	3	1	3
What is the typical response time to an authentication/access request via the internet for your product/service?		0	1	2	2	2	0	2	3
Provide the ability to synchronize single sign-on service user credentials with the following business applications and credential stores: COD credentials maintained in a two-way encrypted state within an Oracle database; GAPS/FMS credentials maintained in a one-way encrypted state within an Oracle Financials ERP access control database; NSLDS, eCB, and CPS credentials maintained within RACF.		-	-	-	-	-	-	-	-
Identify and describe each of the architectural components that make up your product/service. Provide documentation describing each of these components.		-	-	-	-	-	-	-	-
Identify and describe each of the APIs and SDKs supplied with your product/service		-	-	-	-	-	-	-	-
<b>ISO15408 Security / Common Criteria</b>	<b>5</b>	<b>75</b>	<b>75</b>	<b>70</b>	<b>65</b>	<b>75</b>	<b>85</b>	<b>80</b>	<b>165</b>

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Identify how your product/service satisfies ISO15408 Auditing requirements.		1	1	1	1	1	3	2	3
Identify how your product/service satisfies ISO15408 Secure communication requirements.		2	2	2	1	2	3	2	3
Identify how your product/service satisfies ISO15408 identification and authentication, non-repudiation, trusted path, trusted channel and data separation requirements.		1	1	1	1	2	2	2	3
Identify how your product/service satisfies ISO15408 requirements to protect user data from unauthorized access or manipulation.		1	1	1	1	1	2	2	3
Identify how your product/service satisfies ISO15408 requirements to establish and verify a user identity and to ensure that the right security attributes are associated.		2	2	2	2	2	2	2	3
Identify how your product/service satisfies ISO15408 requirements with respect to separation of user administrator duties.		2	1	1	2	2	1	1	3
Identify how your product/service satisfies ISO15408 requirements to protect against discovery and misuse of identity by other users.		1	2	1	1	1	0	0	3
Identify how your product/service satisfies ISO15408 requirements to ensure the integrity and manageability of the mechanism providing Single Sign-On functionality and all the data related to it.		1	1	1	1	1	1	2	3
Identify how your product/service satisfies ISO15408 requirements to control resource utilization.		1	1	1	1	1	0	0	3
Identify how your product/service satisfies ISO15408 requirements to control the establishment of a user's session.		1	1	1	1	1	1	1	3

Technical Criteria	Weight	WAC-VENDOR			WAC & Provisioning		Provisioning		Max
		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	
Identify how your product/service satisfies ISO15408 requirements to establish and maintain trusted communication between entities.		2	2	2	1	1	2	2	3
<b>Operations</b>	<b>3</b>	<b>42</b>	<b>36</b>	<b>36</b>	<b>30</b>	<b>30</b>	<b>24</b>	<b>33</b>	<b>54</b>
Describe business process support for delegated / decentralized administration.		2	2	2	2	2	2	1	3
Describe your product/services means to ensure/provide "high availability".		3	2	2	2	2	2	2	3
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. Describe recommended procedures for disaster recovery for your product/service.		2	2	2	1	1	1	2	3
Describe your product/service's capabilities for backup and recovery of data and system.		2	2	2	2	2	1	2	3
Describe your product/service's typical or tested login response time and session establishment time. Identify the hardware configuration.		-	-	-	-	-	-	-	-
Describe your product/service's performance and rating for user self-service response times.		-	-	-	-	-	-	-	-
Describe your product/service's capabilities to support 25,000 school and financial partner users in a business-to-business operational environment.		2	2	2	2	2	1	2	3
Describe your product/service's capabilities to maintain and measure Quality of Service and a high-level of system availability.		3	2	2	1	1	1	2	3
<b>SUB-TOTAL TECHNICAL SCORE</b>	<input type="checkbox"/>	<b>408</b>	<b>381</b>	<b>391</b>	<b>383</b>	<b>387</b>	<b>380</b>	<b>367</b>	<b>690</b>
<b>TOTAL SCORE</b>		<b>619</b>	<b>609</b>	<b>642</b>	<b>570</b>	<b>639</b>	<b>617</b>	<b>627</b>	<b>1056</b>

### ***B.3 Solution prioritizing***

All products have been evaluated according to common business and technical criteria. Depending on the Single Sign-On solution, which will be chosen, one product provides a better solution than another. The table below takes this in consideration by introducing a Solution prioritizing factor, which is based on these assumptions:

- Provisioning tools can enable legacy applications for Single Sign-On.
- Web Access Control (WAC) tools can enable new applications.
- Applications offering both, provisioning and web access control capabilities, can provide Single Sign-On for new and legacy applications.

		Aventail	RSA	Netegrity	Entrust	IBM	Waveset	Yodlee	Max
<b>TOTAL SCORE</b>		<b>619</b>	<b>609</b>	<b>642</b>	<b>570</b>	<b>639</b>	<b>617</b>	<b>627</b>	<b>1056</b>
Solution prioritizing	100	<b>100</b>							
Provisioning standalone solution		0	0	0	1	2	3	3	3
Web Access Control (WAC) standalone solution		3	3	3	3	3	1	0	3
WAC & Provisioning solution		1	2	2	3	3	2	1	3
Provisioning only		<b>619</b>	<b>609</b>	<b>642</b>	<b>670</b>	<b>839</b>	<b>917</b>	<b>927</b>	<b>1356</b>
WAC only		<b>919</b>	<b>909</b>	<b>942</b>	<b>870</b>	<b>939</b>	<b>717</b>	<b>627</b>	<b>1356</b>
WAC & Provisioning		<b>719</b>	<b>809</b>	<b>842</b>	<b>870</b>	<b>939</b>	<b>817</b>	<b>727</b>	<b>1356</b>

#### Solution 1: Enable legacy applications

Yodlee can provide the best solution if it comes to enabling legacy applications for Single Sign-On. The best alternative to Yodlee is Waveset.

#### Solution 2: Enable new applications

Netegrity can provide the best solution if it comes to enabling new applications for Single Sign-On. The best alternative to Netegrity is IBM.

#### Solution 3: Enable new and legacy applications

IBM can provide the best solution if it comes to enabling new and legacy applications for Single Sign-On within a single product suite. The best alternative to IBM is Entrust.

## Appendix C - Response Evaluation Criteria

The following charts provide the reference criteria used to score vendor written responses to RFI questions. These rating justifications serve as a guide to ensure fair and objective evaluation of each vendor's responses. The criteria used to evaluate each questions are taken directly from the Single Sign-On Requirements Definition completed during Phase I of this effort.

### C.1 Partner Evaluation Criteria – Business Criteria

The following table presents each business capability area and capability weighting factor; and each criteria/survey question and the rating justifications for each criteria/survey question.

Business Criteria	Weight	Rating Justification
Customer Support	5	FSA's reputation is being leveraged for promotion of this project. The system, once complete, must live up to customer standards and expectations.
Describe your customer service model, including help desk operations and customer communications methods. Describe your model for Tier 1, Tier 2, and Tier 3 support, as appropriate.	<input type="radio"/> limited	Customer service and help desk available only during standard working hours. No online help capabilities beyond FAQ's. Problem resolution processes not documented or defined. No privacy protection notice. Service terms and conditions not clear to customers.
	<input type="radio"/> basic	Limited 24x7 customer service and help desk support. Limited online self help includes FAQ's and email only, no faxback or chat. Problem resolution processes in place, but not clearly defined. Unaudited personal privacy practices. Customers notified of terms and conditions of service.
	<input checked="" type="radio"/> extensive	Full 24x7 telephone and online customer service and help desk support. Online self help capabilities including FAQ's, email, faxback and chat. Documented processes to capture incident and problem tickets and contact tier 1, tier 2, tier 3 problem resolution staffs both within and to external partners. Personal privacy policies and procedure audited and verified by privacy agent. Clear customer notification and acknowledgement of service terms and conditions.
What is the mix of customer service and operations personnel types (permanent, sub-contract, outsourced)? How many certified staff do you have for providing implementation support?	<input type="radio"/> limited	Few customer services performed in-house. Many customer services staff are contract employees and/or not full-time staff. All CSR services outsourced to a vendor with limited capabilities. In-house less than 60% employees.
	<input type="radio"/> basic	Limited customer services performed in-house. CSR services outsourced to sophisticated outsourced services organization with multiple customer contact capabilities. In-house staff 60% to 80% employees.

Business Criteria	Weight	Rating Justification
	● extensive	Customer service operations performed in-house by employees. Customer service rep operations outsourced to a sophisticated customer services outsourcing organization. No sub-contractors or contract staffs perform in-house customer care services. In-house 80%+ employees.
How do you hire, train, maintain skilled employees?	○ limited	No targeted recruiting effort. No programs to train customer service staff beyond basic product knowledge. No rewards programs in place for customer care staff.
	▶ basic	Recruits for customer care staff directly. Customer service staff trained in basic company products and support processes. Incentives for performance limited.
	● extensive	Recruitment programs aimed to identify and hire qualified staff. Documented plans and schedules for train customer service staff in vendor products, and customer service skills. Rewards programs in place for customer care staff.
Describe the product/service documentation and tutorials provided to customers.	○ limited	Limited product documentation. General purpose documentation without specific content targeted to specific customer groups/roles.
	▶ basic	Detailed documentation specific for user, administrator, and developer. Media limited to hardcopy and online documents (e.g., Word, PDF, etc.).
	● extensive	Extensive documentation of the product, integration/extension capabilities, and operations. User, operator, and developer training available on multiple subjects including - policy management, administration, customization, trouble shooting, etc. Documentation available in multiple media formats: online, PDF, hardcopy, CD-ROM/DVD, etc.
Describe the training provided to customer users, administrators, and IT staff: documentation, classes, CBT, tutorials, certifications, other.	○ limited	Classroom training for administrators, operators, and developers. No user groups. No customer/partner web site.
	▶ basic	Classroom training for multiple administrator, operations, and developer groups. Training available for client-group or general training. Web customer/partner site with online materials and updates. User group organized and periodic user conference held.
	● extensive	Multiple classroom/hand-on training capabilities including: vendor campus training, client on-site training, customized training classes, role-based training, and component-specific training. Multiple training vehicles including: classroom, CBT, online, virtual seminar, other self-study. Product certification and testing. Vendor sponsored periodic user conferences.
Describe the customer self-service capabilities contained within your product/service. Describe how your product/service provides tools for help desk support of users.	○ limited	A user must be able to change certain user information via the self-service feature.
	▶ basic	Username changes can only be done through an Administrator Email Address changes can only be done through an Administrator.
	● extensive	Full user self service including password administration

Business Criteria	Weight	Rating Justification
Describe your development, administrator and end user technical support capabilities.	<input type="radio"/> limited	
	<input type="radio"/> basic	Users can still access the systems participating with Single Sign-On directly without going through the Single Sign-On portal.
	<input checked="" type="radio"/> extensive	
Describe and identify corrective actions taken and the process of communicating remedies/fixes/patches to customers.	Not Evaluated	

Customer Install Base	5	FSA's reputation is being leveraged for promotion of this project. The system, once complete, must live up to customer standards and expectations.
Describe how your product/service supports system login/access support for business-to-business users. Can your product/service support access by 30,000 b-to-b users?	<input type="radio"/> limited	Provide a scalable solution to allow for extending the user support easily.
	<input type="radio"/> basic	Provide customer care support to 30,000 non-student Single Sign-On users
	<input checked="" type="radio"/> extensive	
How many total users, by average installation, does your product/service support?	<input type="radio"/> limited	0-15,000
	<input type="radio"/> basic	15,000 - 50,000
	<input checked="" type="radio"/> extensive	50,000+
How many users can your product/service support? What is the size, in terms number of supported single sign on user, of your largest installation?	<input type="radio"/> limited	No single client with more than 25,000 end users.
	<input type="radio"/> basic	Clients with 50,000+ end users.
	<input checked="" type="radio"/> extensive	At lease one client with 100,000+ end users.
How many users identified and authenticated by complex mechanisms (i.e., other than simple username/password – using multi-factor, biometrics, PKI, etc.) does your product support?	<input type="radio"/> limited	0-15,000 complex (multiple roles; multiple back-end architectures; multiple access credentials and credential types) authentication profiles
	<input type="radio"/> basic	15,001-50,000 complex authentication profiles
	<input checked="" type="radio"/> extensive	50,000+ complex authentication profiles

Professional Support	5	The abilities and services provided by a vendor that are part of the startup/installation services, and available on an ongoing support basis.
How much elapsed time does a typical installation of your product/service require? What is the typical team required, including vendor, client, and integrator resources? What is the typical cost of these installations? Consider installations against ODBC, ERP, mainframe/RACF, and web front-end interfaces.	○ limited	120 days +, 12+ FTE developers and project managers.
	▶ basic	60 to 120 days. 8 to 12 FTE developers and managers
	● extensive	0 to 60 days. 4 to 8 FTE developers and managers.
What levels of implementation, ongoing support, and professional services support do you offer?	○ limited	Single level of support. Technical services for installation and troubleshooting only. No partner support.
	▶ basic	Limited service level agreements. Services from vendor and partners. Limited professional services.
	● extensive	Multiple service level agreements. Services provided by vendor and partners. Includes professional services support. User group support and customer web self-service.
What types of professional services are bundled with the initial service installation? Are professional services staff internal, contract, or partner resources?	○ limited	Implementation of product only. No start-up support or training included with purchase of product/service.
	▶ basic	Implementation and support training. Installation support. Part-time professional services support on a limited basis. Integration support for first legacy system.
	● extensive	Implementation and support training for administration staff. Full-time professional services support for initial legacy system integration. Shadow training on an active engagement.

Organization	1	The size and organization of a company indicates the ability to handle large projects. A smaller company of equal ability should not be disqualified based upon their size.
How many people are permanent employees of your company? Identify numbers in each of the following roles: Sales & Marketing, Research & Development, Customer Support and Training, Professional Services, Management, Administration.	<input type="radio"/> limited	Number of staff less than 250
	<input type="radio"/> basic	Number of staff 251 to 1000
	<input checked="" type="radio"/> extensive	More than 1000 staff
What is the management organization of your company?	<input type="radio"/> limited	Small corporate executive staff - 6 or fewer senior officers (e.g., C-level executives and VPs). Single operating entity with little clearly defined divisional structure. Non-public entity. Small board consisting of management and investors.
	<input type="radio"/> basic	Moderate corporate executive staff consisting of up to 12 senior officers (e.g., C-level and VPs). Up to three operating groups with profit and loss responsibility. Public or private entity. Board consists of management, investors, and outside directors.
	<input checked="" type="radio"/> extensive	Large corporate executive staff consisting of more than 12 senior officers (e.g., C-level and VPs). More than three operating groups with profit and loss responsibility. Public or private entity. Board consists of management, investors, executives from outside firms, and other outside directors; management has a minority of board seats.
Describe your firm's membership and participation in software security industry groups, technology organizations, and standards committees?	<input type="radio"/> limited	Little official corporate membership and participation in leading trade and technology associations. Individual membership and participation in industry groups without explicit corporate sponsorship. No industry awards or patents awarded to organization.
	<input type="radio"/> basic	Corporate membership in trade association. Sponsorship of trade association and technical standards committees. Attendance by management and technology executives at major trade and technology seminars and conventions. Small number of industry awards or patents awarded to organization.
	<input checked="" type="radio"/> extensive	Full corporate membership in two or more industry trade associations. Executives sit on association Boards. Technologists sit on technological standards and research boards. Corporation and technologists hold patents. Corporation and its executives and technologists recognized by industry by speaking engagement and awards.

Product Vision	5	Marketing, alliances and pricing are direct indicators of a company's willingness to partner with a customer and make investments into the future of that partnership.
What supplier and service alliances have you developed? Identify any other partnerships or investments.	<input type="radio"/> limited	No alliances developed. Purchase hardware or software on a strict customer level or provide services internally.
	<input checked="" type="radio"/> basic	Have built alliances with support suppliers to maintain systems. Partnerships with mid-tier integrators. No joint ventures or equity relationships.
	<input type="radio"/> extensive	Have several joint venture and equity relationships with suppliers. Extensive channel relationships with mid-tier and top-tier integrators.
What is your marketing and sales approach for this product?	<input type="radio"/> limited	Have website, small, centralized sales force.
	<input checked="" type="radio"/> basic	Direct B2C or B2B marketing, small regional sales forces, channel partner sales agreements.
	<input type="radio"/> extensive	National sales force, client-specific account teams, sales teams integrated with channel alliance partners.
What is the current installed base of customers? How many implementations have you performed for government/not-for-profit customers? How many customers are supported in each geographic area your firm operates?	<input type="radio"/> limited	Operations limited to the United States only. Fewer than 30 installations. No government implementations.
	<input checked="" type="radio"/> basic	Regional operations in two or more of the following regions: North America, Europe, East Asia/Australia/NZ, South Asia, Africa, and South America. More than 30 to 100 installations. Less than 5% of customers are government organizations.
	<input type="radio"/> extensive	Worldwide operations in four or more of the following: North America, Europe, East Asia/Australia/NZ, South Asia, Africa, and South America. More than 100 installations. 10% or more of customers are government organization.
Describe upcoming modifications or enhancements to your products/services.	<input type="radio"/> limited	No modifications or changes planned currently
	<input checked="" type="radio"/> basic	Policy management, credential audit, user self-administration, enrollment support, registration support. Extensions to add tokens and digital signatures. Security patches.
	<input type="radio"/> extensive	Real-time monitoring and alerts. Security patches and enhanced capabilities.
Describe your user provisioning operations.	<input type="radio"/> limited	Manual provisioning of credentials after enrollment/authorization. Resource needs for expansion monitored manually
	<input checked="" type="radio"/> basic	Semi or fully automated identity and authentication provisioning. Automated credential notification. Infrastructure monitored to identify the need for expansion to accommodate growth. Supplier agreements in place to accommodate expected growth.

	<input checked="" type="radio"/> extensive	Fully automated provisioning of credentials/authorizations based on automated enrollment/registration approval notification. Automated monitoring of measures to alert operations for the need to expand infrastructure to accommodate growth. Supplier agreements exist to accommodate planned and unexpected growth.
What is your product/service's release history? Describe products, current releases supported, and when the product/service was first released.	<input type="radio"/> limited	No product upgrades or bugs fixed since initial release.
	<input type="radio"/> basic	Bug fixes released on an "as completed" basis, no scheduled upgrades.
	<input checked="" type="radio"/> extensive	Upgrades released at regular intervals and bug fixes released as completed.
What external functionality is available to your product/service via interface or API?	<input type="radio"/> limited	No previous inclusion of external functionality. No plans to allow inclusion.
	<input type="radio"/> basic	Have included basic/minor external functionality (Simple security, etc.). Uses a proprietary API.
	<input checked="" type="radio"/> extensive	Has a robust API interface with multiple external functionality providers. Continues to develop methods for including new technology. Standards based API.
Describe Research and Development (i.e., future product development) activities you are pursuing within security, privacy, access control, and related areas. Describe your product roadmap.	<input type="radio"/> limited	No research being performed or planned.
	<input type="radio"/> basic	Research being performed to enhance existing functionality up to a level equivalent with competitors or to maintain marketability.
	<input checked="" type="radio"/> extensive	Research being performed to enhance existing functionality as well as to offer new functions for competitive advantage and market share growth.
Describe your firm's capabilities to integrate external applications, systems, and technologies into your product/service	<input type="radio"/> limited	No previous inclusion of external functionality. No plans to allow inclusion. Utilize off-the-shelf components without any integration or customization
	<input type="radio"/> basic	Have included basic/minor external functionality. Have linked internal services to external value-added providers. Have customized off-the-shelf components for customer needs.
	<input checked="" type="radio"/> extensive	Has a robust API interface with multiple external functionality providers. Continues to develop methods for including new technology. Incorporates internal components, external services, and off-the-shelf technologies. Products and services separable for unique and distinct client needs.

Legal Requirements Support	5	FSA operations must adhere to Federal and ED regulations
Describe how your product/service supports providing legal notices and protections for Privacy Act and proprietary/confidential data maintained within the Single Sign-On service.	<input type="radio"/> limited	Provide notices (i.e., banners) for Privacy Act Provide notices (i.e., banners) for confidential data
	<input type="radio"/> basic	Provides encryption and banners
	<input checked="" type="radio"/> extensive	Provides extensive logging if Privacy Act data is handled
Describe your product/service's compliance with Federal ADA/Section 508 requirements.	<input type="radio"/> limited	
	<input type="radio"/> basic	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.
	<input checked="" type="radio"/> extensive	Solution complies with best practices. Close to being certified by major security compliance organization.
Describe how your product/service supports the display of legal messages and other messages to users connecting to business systems through the Single Sign-On service.	<input type="radio"/> limited	Does not provide this feature
	<input type="radio"/> basic	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.
	<input checked="" type="radio"/> extensive	For each system an individual message can be displayed
Does your product/service support application requests to re-authenticate users to a business application they are already logged into?	<input type="radio"/> limited	Actions that commit FSA to legally binding commitments with significant business impact, require the user to re-authenticate to the application.
	<input type="radio"/> basic	A message must be displayed to users notifying them of the need to re-authenticate to the business application as required by the application.
	<input checked="" type="radio"/> extensive	

<b>Business Strength</b>	<b>1</b>	A company need only be able to maintain its product and personnel to be able to be eligible for evaluation.
Provide a copy of the latest annual and quarterly report (if public), Dun & Bradstreet number or report.	<input type="radio"/> limited	Balance sheet shows stagnant or negative growth, or extreme financial liability.
	<input type="radio"/> basic	Balance sheet shows no growth or short-term growth or revenues are not approaching costs.
	<input checked="" type="radio"/> extensive	Balance sheet shows steady growth over a period of years with revenues and costs approaching equal or revenues exceeding costs.
Provide a synopsis of market and industry analyst reports describing your firm and product and comparing your product to competitor products/services.	<input type="radio"/> limited	Market analysts recommend divesting of this company. Industry analysts rate product/service below average.
	<input type="radio"/> basic	Market analysts recommend a "wait and see" approach or recommend acquisition on a short-term gain basis, only. Industry analysts rate product/service above average with some shortcomings, but none that are severe deterrents to purchase.
	<input checked="" type="radio"/> extensive	Market analysts recommend acquisition of stock in this company in terms of both short-term gain and long term viability. Dividend future shows promise of payback within the next 2 years. Industry analysts rate this a leading product/service.
Describe your firm's documented strengths and weaknesses over your competitors in the Access Control marketplace.	Not Evaluated	
Describe what you perceive as weaknesses in your competitors' solutions?	Not Evaluated	

**C.2 Partner Evaluation Criteria – Technical Criteria**

The following table presents each technical capability area and capability weighting factor; and each criteria/survey question and the rating justifications for each criteria/survey question.

Technical Criteria	Scale/Weight	Rating Justification
Identification and Authentication	5	The identification and authentication abilities and services provided by a solution provider are core to the proposed solution.
Describe support for configurable username formats that support Federal/NIST 800-18 guidelines. Describe how username formats/business rules are configurable.	<input type="radio"/> limited	Support a minimum username length of 1 character; maximum of 256 characters.
	<input type="radio"/> basic	Support use of the FSA-PIN Username (i.e., SSN, Date of Birth, First two letter of last name), two or more ID factors
	<input checked="" type="radio"/> extensive	Support syntax rules that allow the following elements to be incorporated into usernames: First Initial of First Name, Last Name, Defined data elements and codes, numeric values.
Describe support for configurable password formats, which support Federal/NIST 800-18 guidelines. Describe how password formats/business rules are configurable.	<input type="radio"/> limited	Support a minimum password length of 1 character, maximum 256. Support the definition and enforcement of password policies. Enforce limits on password reuse.
	<input type="radio"/> basic	Enforce rules on the format, content, and complexity of passwords. Assignment of userids and passwords by the service. Support use of the FSA-PIN “Password” (i.e., 4-digit number generated by the FSA-PIN service). Support non-FSA PIN minimum lengths of 8 characters. For non-FSA PIN passwords, support syntax rules that enforce at least three of the following conditions: Uppercase alphabetic characters (A-Z), Lowercase alphabetic characters (a-z), Numerals (0-9), Non-alphabetic and non-numeric characters ( < ! @ # etc.). For non-FSA PIN passwords support rules that enforce: 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, Automatic account lockout for 30 minutes after 3 unsuccessful login attempts, Unsuccessful login counter reset to 0 from 3 after 30 minute lockout. Store passwords in an encrypted state.
	<input checked="" type="radio"/> extensive	Translate unlike User Login Information from different platforms. Support rules that enforce the following capabilities: Password lifetime from 0 to 120 days, Unlimited password lifetime, Comparison to previous passwords for the user, Disabling of the account after a period of inactivity of 0 to 365 days. Assignment of userids and passwords by an external credentials generation service

Describe how the product/service allows for extensions and additions to its authentication mechanism. Describe any APIs supported and any support for Pluggable Authentication Modules.	<input type="radio"/> limited	Allow the display to an end user of user data. Be able to perform logon emulation to Single Sign-On enabled business applications.
	<input type="radio"/> basic	Provide standards based API (Plug-able Authentication Modules - PAM) to allow for additional authentication mechanisms. Allow different groups to utilize different authentication methods. Communicate to Single Sign-On enabled business applications identification and authenticated user information. Extensions for number of access credentials, credential business rules, user administration tools.
	<input checked="" type="radio"/> extensive	Provide pre-built components to allow integration to I&A modules and APIs (e.g., X.509 certificates, X.500 Directory, MS Crypto-API, MS Active Directory, biometrics, kerberos, others.). Extensions for multi-factor authentication, user self service tools
Describe your solutions capabilities to allow for flexible creation of usernames.	<input type="radio"/> limited	User data is stored electronically Username creation is automated. Initial password generation is automated. User is forced to change initial password at first login
	<input type="radio"/> basic	Username creation is based on definable rules (i.e., length, character set, words, and names). Initial password generation is based on definable rules (i.e., length, character set, words, and names). Initial password is communicated securely to the user.
	<input checked="" type="radio"/> extensive	A batch registration of users must be offered.
What types of identification credentials does your service support? What types of authentication data stores does your service support? Do you provide support capability for custom credentials?	<input type="radio"/> limited	Support logon emulation to a web application transparent to the user (intercept logon page and pass logon credentials). Support ODBC (e.g., Oracle, SQL Server, Informix, Sybase, DB2) integration for authentication and credentials synchronization.
	<input type="radio"/> basic	Ability to allow a user to access multiple applications within a single portal. Provide support for HTML forms. Provide APIs for integration of other authentication methods. Support RACF, CA-ACF2 (Citrix web interface), Oracle Financials, Siebel integration for authentication and credentials synchronization
	<input checked="" type="radio"/> extensive	Ability to allow a user to access multiple applications cross-integrated portals. Provide support for digital certificates (X.509), SecureID, biometric methods, kerberos, smart cards, RADIUS.
Describe your ability to use CA/PKI, tokens, or other mechanisms to provide authentication services	<input type="radio"/> limited	No CA/PKI or other authentication mechanisms integrated into services
	<input type="radio"/> basic	Ability to use single type of CA/PKI for authentication. Limited support for policy administration, CA, and RA functions.
	<input checked="" type="radio"/> extensive	Fully integrated CA/PKI capability for user authentication. Ability to perform all policy administration, CA, and RA functions using multiple vendor certificates. Full compatibility with OCSP standards.

User Management	3	The abilities and services provided by an access control solution to manage user identity and privilege profiles.
Identify how your product/service provides a mechanism for a privileged administrator to change access rights of individuals, roles, and/or groups.	○ limited	Administrator changes will be logged and audited. Provide capabilities to administer – Passwords, Usernames, User data, and Session management.
	▸ basic	Logon required to access user data. Provide a display for administrators to view access rights and privileges of all users.
	● extensive	Allow access control rules to include configurable conditions based on data from multiple data sources. Real-time user status monitoring and user management.
Describe your product/service's ability to create usernames and passwords or accept usernames and passwords created by trusted sources.	○ limited	Allow users or system administrators to manually create user names
	▸ basic	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. Allow for the use of the FSA PIN – username and PIN. 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.
	● extensive	Allow the Single Sign-on service to generate new target systems passwords for users.
Describe your product/service's ability to enable the categorization of like users using roles and/or groups. Are roles and groups handled the same way individual users are handled? Explain.	○ limited	No group support.
	▸ basic	Supports assignment of users to one or more groups for support of group accounts for system access.
	● extensive	Supports assignment to multiple groups for one business application.
Describe your product/service's ability to communicate Single Sign-On user credentials to existing credential repositories. Identify types of credentials stores supported - e.g., RACF, ODBC, UNIX, NT, Novell, LDAP, Oracle Financials, ERPs, etc.)	○ limited	ODBC Database (Oracle, SQL Server, Informix)
	▸ basic	IBM RACF, Oracle Financials ERP, Directory (LDAP v3), FSA PIN Service
	● extensive	NT Network, Unix Network

Describe how your product/service supports delegated administration of access policies and functions for users, roles, groups of users, an application, or a set of applications by appointed administrators granted limited administration and management rights.	<input type="radio"/> limited	Provide an administration interface for administrators. A privileged administration interface must be widely accessible from the FSA Intranet or the internet. Provide a graphical interface for end users and administrators. Provide remote access capabilities for users and administrators. Support remote administration and delegated administration
	<input type="radio"/> basic	Provide a graphical interface for administrators. Provide integration capabilities to Call Center technologies via APIs, web-link, or other mechanisms.
	<input checked="" type="radio"/> extensive	Provide remote access capabilities for administrators. Provide a customizable user interface for users and administrators. Provide APIs for integration of existing user management services.
FSA desires to store minimal user data in the Single Sign-on user data repository. Identify your product/service's ability to configure a user data store and/or credential store.	<input type="radio"/> limited	
	<input type="radio"/> basic	First Name, Last Name, Last four digits of the users social security number, Telephone contact number, Single Sign-On user identifier, Single Sign-On user authenticator, For Single Sign-on enabled systems store: system addresses, user identifiers and authenticators
	<input checked="" type="radio"/> extensive	
Describe your product/service's capabilities to allow manual and/or automatic revocation of users.	<input type="radio"/> limited	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.
	<input type="radio"/> basic	The process of revocation of a user must be automatic, once invoked by the administrator.
	<input checked="" type="radio"/> extensive	System capable of integrating onto official systems of record, e.g., human resources, financial management, etc.
Describe your product/service's capabilities to disable accounts based on inactivity and/or a definable number of unsuccessful login attempts.	<input type="radio"/> limited	If an account encounters multiple failed login attempts, it must be disabled after a configurable number of failed attempts.
	<input type="radio"/> basic	If a user does not login for a specific time, users account is disabled. The timeframe must be configurable.
	<input checked="" type="radio"/> extensive	The Single Sign-On must allow disabling a user account for an unlimited timeframe.
Password administration must be automated and only require minimal manual interaction with the single sign-on administrator. Describe your product/service's capabilities to administer passwords within the single sign-on service and within enabled back-end systems.	<input type="radio"/> limited	Challenge questions are based upon data stored in the Single Sign-On user data store. A user must get a confirmation of a password change.

	<input checked="" type="radio"/> basic <input type="radio"/> extensive	User is limited to a configurable number of password changes per day. Users wanting to change their password must do this by providing their old password and/or answering one or more free definable challenge questions. Users who have forgotten their password must request a new password by answering one or more free definable challenge questions.
Describe your product/service's capabilities to automatically audit/check single sign-on user credential(s) against definable rules/standards.	<input type="radio"/> limited	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.
	<input checked="" type="radio"/> basic <input type="radio"/> extensive	Provide the ability to check for weak credentials based on definable syntax rules (i.e. Minimum password length, combination of number and letters, etc.). Provide the ability to check for weak credentials based on dictionaries. A definable number of credentials used before must be stored. (e.g. Do not allow repeating passwords)
	<input type="radio"/> limited	No encryption.
Describe your product/service's capabilities to store Single Sign-On user credentials securely and in a protected manner.	<input checked="" type="radio"/> basic	Basic two-way encryption.
	<input type="radio"/> limited	Single Sign-On user credentials must be stored with one-way encryption in place (i.e. salted Hash). Storage of Single Sign-On user credentials must allow for easy data synchronization/replication between FSA systems and the Single Sign-On data store.
	<input type="radio"/> limited	Registration services provided by third party. Changes and updates processed manually or with limited automation.
Describe your products/service's user registration, and service update/change processes	<input checked="" type="radio"/> basic	Semi or fully automated registration. All processes not completely integrated for real time processing - many batch processes and some manual processing. Difficult to modify registration process for unique client needs.
	<input type="radio"/> limited	Registration processes developed in-house or procured from third parties are fully automated and integrated with automated provisioning systems. Able to modify registration and change processes to meet unique client needs.
	<input type="radio"/> limited	Access control based on security rules / policy management. Specification of which resources need to be authorized.
Describe capabilities to assign access control against resources	<input checked="" type="radio"/> basic	Support for Role-based management of users. Support for delegated management/administration of users.
	<input type="radio"/> limited	Access control enforced on URLs and Physical files. Support for authentication rules based on authentication methods.
	<input type="radio"/> limited	Privileges required to access authentication data. Password and user credential management. Session management rules and enforcement. Display for administrators to view rights and privileges of all users.

	<input type="radio"/> basic	Real-time user status and user management tools. Ability for users to view access rights to services.
	<input checked="" type="radio"/> extensive	Access rules designed based on client-specified attributes. Access control rules include arbitrary conditions based on information from multiple data sources.

Access Management	3	The ability of the service to manage user accounts and access, record and report activity to users and administrators.
Describe your product/service's support for exit/signoff options to end a user's active session with all applications accessed through Single Sign-On.	○ limited	Provide the ability to end Internet session upon termination of a browser instance. Provide a logout button for users to close a session directly
	▶ basic	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)
	● extensive	An administrator can terminate an active user.
Describe your product/service's support for the removal/deletion of users from the Single Sign-On service	○ limited	Deletion in the database.
	▶ basic	Remove users from the Single Sign-On service within one business day after receiving notification by FSA. Given notification within 24 hours.
	● extensive	Instant deletion /removal based on integration to systems of record.
Identify and describe your product/service's tools to administer access to applications and resources	○ limited	Provide user self-service administration/help
	▶ basic	Allow users to maintain multiple sessions with applications. Applications will determine whether single or multiple sessions are allowed.
	● extensive	
Identify the user access mechanisms supported by your product/service - e.g., internet, voice response unit, dedicated, etc.	○ limited	Provide access to application via the Internet
	▶ basic	Provide access to application via VRU (Voice Response Unit)
	● extensive	Dedicated access.
Describe your product/service's support for user authentication via passwords, tokens, or other devices compliant with NIST 800-18.	○ limited	Maintain and approve a current list of authorized users and their access. Access scripts with embedded passwords are prohibited. Emergency and temporary access can be authorized. Terminated, transferred, or otherwise ineligible individuals are removed from system access. Passwords are changed at least every ninety days or earlier. Passwords are not displayed when entered. Procedure exists to terminate lost and compromised passwords. Vendor-supplied passwords are replaced immediately. A limited number of invalid access attempts are allowed for a given user.

	<ul style="list-style-type: none"> <li><input checked="" type="radio"/> basic</li> </ul>	<p>Passwords are unique and difficult to guess (e.g., passwords require alpha numeric, upper/lower case, and special characters)                  Inactive user identifications are disabled after a specified period of time. Passwords are transmitted and stored using secure protocols/algorithms. Passwords are distributed securely and users are informed not to reveal their passwords to anyone (social engineering).</p>
<p>Describe your product/service's controls to restrict users to authorized Single Sign-On transactions and functions compliant with NIST 800-18</p>	<ul style="list-style-type: none"> <li><input checked="" type="radio"/> extensive</li> </ul>	<p>Digital signatures, if used, conform to FIPS 186-2.</p>
	<ul style="list-style-type: none"> <li><input type="radio"/> limited</li> </ul>	<p>Access to security software is restricted to security administrators                  Inactive users' accounts are monitored and removed when not needed.                  Controls exist to restrict remote access to the system                  Activity logs are maintained and reviewed                  The network connection automatically disconnects at the end of a session                  Guest and anonymous accounts, if used, are authorized and monitored                  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                  A privacy policy is posted on the web site</p>
	<ul style="list-style-type: none"> <li><input checked="" type="radio"/> basic</li> </ul>	<p>Access controls prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion. Sensitive data transmissions are encrypted.                  Encryption when used, meets federal standards (AES, DES/triple-DES). When encryption is used, there exist procedures for key generation, distribution, storage, use, destruction, and archiving.</p>
<p>Describe your product/service's ability to audit/log activity involving access to and modification of sensitive or critical Single Sign-On files in compliance with NIST 800-18. Describe the capabilities to capture, record and report events related to access requests and access control administration.</p>	<ul style="list-style-type: none"> <li><input checked="" type="radio"/> extensive</li> </ul>	<p>Access is restricted to files at the logical view or field. Access monitored to identify apparent security violations</p>
	<ul style="list-style-type: none"> <li><input type="radio"/> limited</li> </ul>	<p>Audit trail(s) provides a trace of user actions related to the Single Sign On mechanism.                  Audit trail(s) can support after-the-fact investigations of how, when, and why normal operations ceased of the Single Sign-On.                  Access to online audit logs provided by the Single Sign-On is strictly controlled.                  Record successful and unsuccessful logon attempts.                  Record activities that change user access rights and credentials.</p>
	<ul style="list-style-type: none"> <li><input checked="" type="radio"/> basic</li> </ul>	<p>Automated tools are available to review audit records in real time or near real time provided by the Single Sign-on.                  Record and report specific events (e.g., login, logout, resets, changes, adds, revokes, expirations, suspends, retires, authorizations, sessions, login attempts, credential changes, policy changes, changes to access rights, etc.) within audit logs.                  Describe specific information contained in individual audit records (e.g., user identifier, timestamp, action, etc.).                  Provide an audit trail when confidential data is accessed.                  Support reporting tools to access and report against audit records.</p>

	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	<p>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.</p> <p>Record activities that require privileged access.                  Support APIs to the access control audit mechanism.                  Support reporting of historical/past transactions and user activity.                  Support alerting mechanisms for communicating system and security events.</p>
After a successful login, describe your product/service's capability to provide a message with information about last successful login and how many unsuccessful login attempts have been made in the meanwhile.	<ul style="list-style-type: none"> <li>○ limited</li> </ul>	No login/logout history provided.
	<ul style="list-style-type: none"> <li>▸ basic</li> </ul>	Provide a logout history for Single Sign-On.
	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	Provide a login history for Single Sign-On. Provide a failed login history through Single Sign-On.
Describe your product/service's capability to define custom access rules.	<ul style="list-style-type: none"> <li>○ limited</li> </ul>	Configurable access restrictions based on user-group.
	<ul style="list-style-type: none"> <li>▸ basic</li> </ul>	Configurable access restrictions based on time and location.
	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	Configurable access restrictions based on combinable criteria (time, location, user group, role, etc.)
Describe your product/service's ability to capture user actions to allow for accountability logging and auditing.	<ul style="list-style-type: none"> <li>○ limited</li> </ul>	<p>Audit tools must be available for authorized users, to review audit logs.                      The Administrator must be able to select specific security events.                      The Single Sign-On mechanism must be able to create and maintain a secure audit trail.                      Audit logs must be only available to authorized users.</p>
	<ul style="list-style-type: none"> <li>▸ basic</li> </ul>	The Single Sign-On mechanism must offer the option to define actions if certain events have taken place. The information that is captured and stored for audit must be configurable.
	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	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.
Describe your product/service's support for secure communication between systems and the Single Sign-On data store.	<ul style="list-style-type: none"> <li>○ limited</li> </ul>	None
	<ul style="list-style-type: none"> <li>▸ basic</li> </ul>	The Single Sign-On solution must allow for secure communication between systems and the Single Sign-On data store.
	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	Encryption of data and authentication of machine interfaces/communications.

Describe your product/service's capabilities to protect data at rest and in transit.	<input type="radio"/> limited	Storage of confidential data must be done securely.
	<input type="radio"/> basic	The Single Sign-On service must be able to provide secure web communication.
	<input checked="" type="radio"/> extensive	
Describe your product/service's support for services/mechanisms allowing administrators and users to be enrolled and authorized for single sign-on administration and use.	<input type="radio"/> limited	Allow for business users to be enrolled in the single sign-on service Allow for single sign-on service administrators to be enrolled in single sign-on administration services.
	<input type="radio"/> basic	Provide a mechanism to integrate to online registration services.
	<input checked="" type="radio"/> extensive	Provide a mechanism to integrate to enrollment services.
Describe your capabilities to record privileged activity against secured resources, and to ensure that users without proper privileges have not accessed a secured resource.	<input type="radio"/> limited	No capabilities to track and compare access events and privilege-based events. No capabilities for digital signature or other user high-level of confidence authentication mechanisms.
	<input type="radio"/> basic	Basic tracking capabilities for access events and privilege-based actions. Use of single factor authentication mechanisms (e.g., passwords)
	<input checked="" type="radio"/> extensive	Capabilities to track and compare all access to secured resources and privilege-based actions. Able to use mechanism that supports a high-level authentication confidence. Use of double-factor authentication mechanisms (e.g., PIN and token, PIN and certificate, etc.). Event correlation.
Describe your access control / authentication security operations.	<input type="radio"/> limited	User access by logon and password. Persistent web session. User profile and privileges reside on same server in unencrypted form.
	<input type="radio"/> basic	Access by logon and password (or other simple credentials). Web connection time out. User profile and privilege data reside on independent servers. All credential data stores encrypted.
	<input checked="" type="radio"/> extensive	Access by logon and password. Web connection time out after non-use. Authentication of user by digital certificate. User profile and privilege data reside on separate servers. All data encrypted. User profile and privilege data encrypted and unable to be decrypted by data center staff, only by user and appropriately cleared "super" administrators.

Session Management	5	The ability of the service to manage individual user sessions with applications
Describe your product/service's mechanism(s) for session management. Describe your use/non-use of cookies.	○ limited	The Single Sign-On mechanism must provide a configurable session timeout. Any "cookies" or other items created by the Single Sign-on service and placed on user PCs will be removed or deleted upon termination of the user session
	▸ basic	A logout button must be available at any time.
	● extensive	The Single Sign-On solution must provide the option to prevent concurrent sessions for a user.
Describe your product/service's capabilities to establish, manage and monitor user sessions	○ limited	Close user sessions after a period of inactivity to be set by the administrator.
	▸ basic	Maintain session using an encrypted transient cookie. Maintain transient cookies not stored on the users hard disk. Ensure that encryption keys are only known to the access control server; Ensure that the key is changed periodically.
	● extensive	Maintain session in conjunction with third-party ASP session management (i.e., client must allow multiple transient cookies).

Environment	3	The ability of the service to support specific technology hardware/software platforms currently for or planned for use for FSA applications.
Identify the operating systems supported by your product/service. What is your preferred operating system?	<input type="radio"/> limited	Windows NT Windows 2000 Sun Solaris 2.6 and 8 Hewlett-Packard Unix 11.x
	<input type="radio"/> basic	Mainframe MVS Mainframe OS 390
	<input checked="" type="radio"/> extensive	Linux, VAX/VMS
Identify the web servers supported by your product/service. What is your preferred web server?	<input type="radio"/> limited	Microsoft IIS
	<input type="radio"/> basic	Apache IBM HTTP Server iPlanet Enterprise Server
	<input checked="" type="radio"/> extensive	
Identify the application servers supported by your product/service. What is your preferred application server?	<input type="radio"/> limited	Websphere 3.55
	<input type="radio"/> basic	Coldfusion JRUN Weblogic
	<input checked="" type="radio"/> extensive	Oracle Citrix
Identify the proxy servers supported by your product/service. What is your preferred proxy server?	<input type="radio"/> limited	Apache
	<input type="radio"/> basic	CoolGen Webcache
	<input checked="" type="radio"/> extensive	
Identify the databases, directories, and other credential data stores supported by your product/service. Identify other security products/repositories (e.g., RACF, ACF2, TOPSECRET, etc.) are supported by your product/service.	<input type="radio"/> limited	ODBC Database (Oracle, SQL Server, Informix). Provide a data store for access control/policy rules

	<input checked="" type="radio"/> basic <input type="radio"/> extensive	RACF NT Network Directory (LDAP v3) Provide user administration tools to allow delegated administration of user attributes stored in the access control data store. Provide access to a standards based external LDAP directory. Provide access to an access credential store via LDAP
	<input type="radio"/> limited <input checked="" type="radio"/> extensive	Oracle Financials ERP FSA PIN Service Access multiple directories for authentication lookups.
Identify the Internet browsers supported by your product/service.	<input type="radio"/> limited	Support Microsoft Internet Explorer 4.01 and higher
	<input checked="" type="radio"/> basic	Support Netscape Navigator 4.06 and higher (Windows 95/98/Me, Windows NT/2000); Support the America Online browsers:- AOL 5.0 and higher
	<input type="radio"/> extensive	
Identify the EAI, middleware, and other products/service supported by your product/service. Identify your product/service's ability to integrate to character-based systems web-enabled by Citrix.	<input type="radio"/> limited	Provide support for HTTP reverse proxy architecture. Provide the ability to integrate to a Viadom portal, IBM Websphere portal. Provide support for IBM Websphere and iPlanet web application servers. Provide the ability to integrate to internet portal via API or other mechanism.
	<input checked="" type="radio"/> basic	IBM MQ Series
	<input type="radio"/> extensive	Provide the ability to integrate with a Search Engine to provide a privileged search.
Identify changes or additions to existing business application software or technical infrastructure required by your single sign-on product/service to enable an application.	<input type="radio"/> limited	
	<input checked="" type="radio"/> basic	Minimize changes to applications for single sign-on enablement. Minimize changes to infrastructure for single sign-on enablement.
	<input type="radio"/> extensive	
Describe your support of standards for access control, data, authentication, communications, Federal guidelines (e.g., Section 508, OMB A-130, FIPS PUBS, NIST 800, Common Criteria/ISO15408, etc.), and other industry standards.	<input type="radio"/> limited	Full support for industry standards for common functions and capabilities - file formats, access, encryption, transport. Most Federal standards supported.
	<input checked="" type="radio"/> basic	Support industry standards for all common functions. Utilizes some proprietary mechanisms for advanced or state of the art capabilities. Complies with all Federal standards.

	<input checked="" type="radio"/> extensive	Support industry standards for all common functions. Follows all standards and a leader in defining standards for state-of-the-art and advanced access control features. All current and known future Federal standards supported.
What is the typical response time to an authentication/access request via the internet for your product/service?	<input type="radio"/> limited	Support login response times of more than 15 seconds
	<input type="radio"/> basic	Support login response times of 2 to 15 seconds
	<input checked="" type="radio"/> extensive	Support login response times of less than 2 seconds
Provide the ability to synchronize single sign-on service user credentials with the following business applications and credential stores: COD credentials maintained in a two-way encrypted state within an Oracle database; GAPS/FMS credentials maintained in a one-way encrypted state within an Oracle Financials ERP access control database; NSLDS, eCB, and CPS credentials maintained within RACF.	See credential stores supported	
Identify and describe each of the architectural components that make up your product/service. Provide documentation describing each of these components.	Not Evaluated	
Identify and describe each of the APIs and SDKs supplied with your product/service	Not Evaluated	

ISO15408 Security / Common Criteria	5	Security within the new system is paramount. The reputation of the FSA is being used to promote confidence in the product. Support of that reputation is mandatory.
1. Identify how your product/service satisfies ISO15408 Auditing requirements.	<input type="radio"/> limited	Audit review – Audit tools must be available for authorized users, to review audit data. 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.
	<input checked="" type="radio"/> basic	Audit data generation - The level of which information is stored for audit, must be configurable. Audit analysis – Abnormal user behavior must be detected and the ability to pass this data to intrusion detection systems must be provided. Audit event selection – The ability to select specific security events must be provided.
	<input checked="" type="radio"/> extensive	Automatic response to events - Certain audit events (Incidents) must result in actions, which are executed automatically. Audit analysis – Abnormal user behavior must be detected and the ability to pass this data to intrusion detection systems must be provided.
2. Identify how your product/service satisfies ISO15408 Secure communication requirements.	<input type="radio"/> limited	The ability to verify if a system is the intended recipient for a communication request.
	<input checked="" type="radio"/> basic	The ability to verify if a communication request is originating from the system it claims to come from.
	<input checked="" type="radio"/> extensive	
3. Identify how your product/service satisfies ISO15408 identification and authentication, non-repudiation, trusted path, trusted channel and data separation requirements.	<input type="radio"/> limited	
	<input checked="" type="radio"/> basic	Cryptographic key management – A key management function must be offered that allows the management of cryptographic keys throughout their lifecycle (generation through deletion). Cryptographic operation – Functions like strong encryption/decryption, cryptographic-checksum and secure hash must be offered.
	<input checked="" type="radio"/> extensive	
4. Identify how your product/service satisfies ISO15408 requirements to protect user data from unauthorized access or manipulation.	<input type="radio"/> limited	Access control policy – Access to user data must be controlled and protected based on access policies. Access control functions – Access to user data is controlled by these functions, which are configured according to the access policies. Information flow policy – Allow for read or write only access to user data for specific entities. 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.

	<ul style="list-style-type: none"> <li>▶ basic</li> </ul>	<p>Export of user data – Security attributes associated with user data can be explicitly preserved or ignored when exporting user data.                  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.                  Internal data transfer – User data protection is provided when data is transferred internally.                  Rollback – Offering an Undo for the last operation.                  Stored data integrity – Ensure that stored user data is protected from unauthorized access.                  User data confidentiality transfer protection – Ensure that user data is protected from unauthorized access during transfer between entities.                  User data integrity transfer protection – Ensure that user data is not manipulated during transfer between entities.</p>
	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	<p>Data authentication – Data authentication allows for verification of data if it has been forged or fraudulently modified..                  Residual data protection – Ensure that purged information is no longer accessible.</p>
<p>5. Identify how your product/service satisfies ISO15408 requirements to establish and verify a user identity and to ensure that the right security attributes are associated.</p>	<ul style="list-style-type: none"> <li>○ limited</li> </ul>	<p>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.                  User attribute definition – Each user has security attributes associated to him/her, which define users access rights appropriate to his/her role.</p>
	<ul style="list-style-type: none"> <li>▶ basic</li> </ul>	<p>Specification of secrets – Secrets (e.g. Password) must be checked against certain definable quality standards.                  User authentication – Offer a scalable robust authentication mechanisms.                  User identification – Before a user can take any actions, he/she has to be identified. Only exception is the login process.                  User subject binding – Processes accessing, changing or deleting objects are executed with the user's security attributes.</p>
	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	
<p>6. Identify how your product/service satisfies ISO15408 requirements with respect to separation of user administrator duties.</p>	<ul style="list-style-type: none"> <li>○ limited</li> </ul>	<p>Management of functions – Security functions must only be accessible by authorized users.                  Management of security attributes – Security attributes can be modified, established or deleted only by authorized users.</p>
	<ul style="list-style-type: none"> <li>▶ basic</li> </ul>	<p>Management of internal data – Audit, configuration or any other critical data must be accessible only by authorized users.                  Revocation – Security attributes must be revocable for each entity.                  Security attribute expiration – Security attributes must have a limited lifetime.</p>
	<ul style="list-style-type: none"> <li>● extensive</li> </ul>	
<p>7. Identify how your product/service satisfies ISO15408 requirements to protect against discovery and misuse of identity by other users.</p>	<ul style="list-style-type: none"> <li>○ limited</li> </ul>	

	<ul style="list-style-type: none"> <li><input type="checkbox"/> basic</li> </ul>	<p>Anonymity – A user can use a resource or service without disclosing the user’s identity to other users.                  Pseudonymity – A user’s identity is not disclosed to other users. But the user is still accountable for his/her action.                  Unlinkability – A user can use a resource multiple times without other users being able to link these sessions to each other.                  Unobservability – A user can utilize a resource without unauthorized parties being able to observe his/her actions or the usage.</p>
<p>8. Identify how your product/service satisfies ISO15408 requirements to ensure the integrity and manageability of the mechanism providing Single Sign-On functionality and all the data related to it.</p>	<ul style="list-style-type: none"> <li><input type="radio"/> limited</li> </ul>	<p>Timestamp – A reliable timestamp mechanism must be offered.                  Internal data consistency – Data must be consistent across the whole Single Sign-On mechanism.                  Internal data replication consistency – Data must be consistent between the Single Sign-On mechanism and the IT products utilizing the data provided by it.                  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.                  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.</p>
	<ul style="list-style-type: none"> <li><input type="checkbox"/> basic</li> </ul>	<p>Fail Secure – In the event of failures the Single Sign-On mechanism must go into a “safe mode”.                  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.                  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.                  Integrity of exported data - Protection from unauthorized modification of data during transmission between the Single Sign-On mechanism and another IT product.                  Internal data transfer – Protection of data transmitted between different pieces of the Single Sign-On mechanism must be provided.                  Physical protection – Restrictions on physical access to the Single Sign-On mechanism and the underlying hardware must be ensured.                  Trusted recovery – The Single Sign-On mechanism must start up in a controlled state.                  Self-test – The Single Sign-On mechanism must test itself when starting up and before users are allowed access.</p>
	<ul style="list-style-type: none"> <li><input type="radio"/> extensive</li> </ul>	<p>Replay detection – Replay of various entities (e.g. messages, service request, service responses) must be detected.                  Domain separation – Security functions of the Single Sign-On mechanism must live in their own domain to avoid tempering.                  State synchrony protocol – State synchronization between the different parts of the Single Sign-On mechanism must be done with a secure exchange protocol.</p>

9. Identify how your product/service satisfies ISO15408 requirements to control resource utilization.	<input type="radio"/> limited	
	<input checked="" type="radio"/> basic	Fault tolerance – In event of failures the Single Sign-On mechanism should maintain normal operation. Priority of service – High priority tasks cannot be interrupted by tasks with a lower priority. Resource allocation – Use of resources by users and subjects is controlled to avoid a denial of service.
	<input type="radio"/> extensive	
10. Identify how your product/service satisfies ISO15408 requirements to control the establishment of a user's session.	<input type="radio"/> limited	Session locking – Inactive sessions must be locked or closed. Limitation on concurrent sessions – Users are only allowed one or more concurrent sessions, as configured by the access service.
	<input checked="" type="radio"/> basic	Scope of selectable attributes – Limit the scope of session security attributes that a user may select for a session. Access banner – An access banner must be present to display a configurable advisory warning message. 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.
	<input type="radio"/> extensive	Session establishment – A function must be offered to define rules to deny access based on user location, time, credentials, authentication-method, etc.
11. Identify how your product/service satisfies ISO15408 requirements to establish and maintain trusted communication between entities.	<input type="radio"/> limited	Trusted Path - Confidential data must never be transmitted in the clear between user and the single-sign-on mechanism.
	<input checked="" type="radio"/> basic	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.
	<input type="radio"/> extensive	

Operations	3	The ability of a service to maintain and customize its capabilities indicates its ability to provide a service desired by the FSA.
Describe business process support for delegated / decentralized administration.	<input type="radio"/> limited	Delegated administration must be configurable based on user groups.
	<input checked="" type="radio"/> basic	Group administration must be shareable between two or more administrators within the same-delegated administration group.
	<input type="radio"/> extensive	
Describe your product/services means to ensure/provide "high availability".	<input type="radio"/> limited	
	<input checked="" type="radio"/> basic	Support for redundant deployment with built-in fail-over capabilities.
	<input type="radio"/> extensive	
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. Describe recommended procedures for disaster recovery for your product/service.	<input type="radio"/> limited	
	<input checked="" type="radio"/> basic	Disaster recovery procedures are in place.
	<input type="radio"/> extensive	
Describe your product/service's capabilities for backup and recovery of data and system.	<input type="radio"/> limited	
	<input checked="" type="radio"/> basic	Off-site media storage procedures, backup procedures and policies per capability are in place.
	<input type="radio"/> extensive	
Describe your product/service's typical or tested login response time and session establishment time. Identify the hardware configuration.	<input type="radio"/> limited	
	<input checked="" type="radio"/> basic	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.
	<input type="radio"/> extensive	
Describe your product/service's performance and rating for user self-service response times.	<input type="radio"/> limited	

	<input type="radio"/> basic	The achievement of this performance goal depends on other components of the FSA infrastructure and is outside the scope of the project.
	<input checked="" type="radio"/> extensive	
Describe your product/service's capabilities to support 25,000 school and financial partner users in a business-to-business operational environment.	<input type="radio"/> limited	
	<input type="radio"/> basic	Support FSA peak student concurrent logins. Support FSA peak school, financial partner, employee, and operating partner concurrent logins.
	<input checked="" type="radio"/> extensive	
Describe your product/service's capabilities to maintain and measure Quality of Service and a high-level of system availability.	<input type="radio"/> limited	System availability less than 99%. Monitoring of systems activity divided between services providers and internal operations staff. Staff on-call 24x7 (not necessarily on site) to respond to problems.
	<input type="radio"/> basic	System availability from 99% to 99.9%. Staff onsite 24x7 to respond to problems. Reliance on service supplier staff for some systems monitoring of problem resolution.
	<input checked="" type="radio"/> extensive	System availability greater than 99.9%. Fully redundant monitoring of all systems and transport functions. Staff available on-site 24x7 to respond to all systems problems. Support real-time monitoring of systems resources and protected resources.

### ***C.3 Partner Evaluation Criteria – Other Criteria***

The following table presents additional solution criteria and contractual terms and conditions that each vendor is expected to be able to fully satisfy.

<b>TERMS AND CONDITIONS</b>
Proposal Terms and Conditions
1. Provide a demonstration pilot of your product for one or more actual instances of access to FSA back-end applications.
2. Provide FSA a copy of your standard contractual terms and conditions.
3. A contract can be canceled by FSA, if FSA is not fully satisfied that the product meets specification claimed by the service provider.
4. A vendor must be willing to provide documented "benchmark" SLA data.
5. Describe the standard Service Level Agreements your product/service meets
6. Describe any anticipated out-year non-recurring costs expected with your product/service.
7. Provide a description of your pricing model(s).
8. Provide standard pricing for monthly licensing/service fees based on appropriate service levels (e.g., number of users, applications, CPUs, etc.) used in your pricing model.
9. Provide standard pricing for basic and enhanced products and services.
10. Describe the process and timeliness of notifications to customers of security issues and code fixes. Describe your policies for distribution of patches, product maintenance, and new product releases.
11. Describe policies for customer requirement modifications and extensions.

## **Appendix D – Preliminary Benefit / Cost Summary**

The following identifies the categories of alternative benefit and cost information being captured for each solution alternative.

### **Benefits – Non-recurring**

- Reusable Sign-on Architecture (Large Enterprise System)
- Reusable Sign-on Architecture (Departmental Systems)

### **Benefits – Recurring**

- Customer Call Helpdesk – Password Resets, other Tier 1 access control support

### **Costs – One-time**

- Development/Deployment
- Software/Hardware Purchase
- Training

### **Costs – Recurring**

- Software/Hardware License
- VDC Operations
- System/Security Administration

The following table displays a summary of preliminary benefits and costs for each potential alternative. These benefits and costs will be finalized for presentation in the Phase III business case for this effort.

**FSA Vendor Alternatives – Preliminary Benefit/Cost Summary**  
**Final Benefit/Cost Analysis To Be Completed With Business Case/Implementation Plan**

Vendor		FY 02'	FY 03'	FY 04'	FY 05'	FY 06'
<b>Yodlee - Managed Service</b>						
Benefits	Non Recurring	0	0	0	0	0
	Recurring	0	571,429	914,286	914,286	914,286
Costs	Non Recurring	-2,101,677	0	0	0	0
	Recurring	-633,600	-633,000	-633,600	-633,600	-633,600
	<i>Total Benefit/(Cost)</i>	<i>-2,735,277</i>	<i>-61,571</i>	<i>280,686</i>	<i>280,686</i>	<i>280,686</i>
<b>Waveset - COTS Product</b>						
Benefits	Non Recurring	0	0	0	0	0
	Recurring	0	571,429	914,286	914,286	914,286
Costs	Non Recurring	-2,307,573	0	0	0	0
	Recurring	-130,800	-751,425	-845,025	-845,025	-845,025
	<i>Total Benefit/(Cost)</i>	<i>-2,438,373</i>	<i>-179,996</i>	<i>69,261</i>	<i>69,261</i>	<i>69,261</i>
<b>Aventail</b>						
Benefits	Non Recurring	0	1,380,000	276,000	276,000	276,000
	Recurring	0	571,429	685,714	800,000	914,286
Costs	Non Recurring	-1,443,422	-3,228,000	-2,028,000	-2,028,000	-2,028,000
	Recurring	0	-384,000	-384,000	-384,000	-384,000
	<i>Total Benefit/(Cost)</i>	<i>-1,443,422</i>	<i>-1,660,571</i>	<i>-1,450,286</i>	<i>-1,336,000</i>	<i>-1,221,714</i>
<b>Netegrity</b>						
Benefits	Non Recurring	0	1,380,000	276,000	276,000	276,000
	Recurring	0	571,429	685,714	800,000	914,286
Costs	Non Recurring	-1,681,871	-1,200,000	0	0	0
	Recurring	-272,679	-929,679	-1,023,279	-1,023,279	-1,023,279
	<i>Total Benefit/(Cost)</i>	<i>-1,954,550</i>	<i>-178,250</i>	<i>-61,565</i>	<i>52,721</i>	<i>167,007</i>
<b>Entrust</b>						
Benefits	Non Recurring	0	1,380,000	276,000	276,000	276,000
	Recurring	0	571,429	685,714	800,000	914,286
Costs	Non Recurring	-1,594,323	-1,200,000	0	0	0
	Recurring	-242,016	-899,016	-992,616	-992,616	-992,616
	<i>Total Benefit/(Cost)</i>	<i>-1,836,339</i>	<i>-147,587</i>	<i>-30,902</i>	<i>83,384</i>	<i>197,670</i>
<b>RSA</b>						
Benefits	Non Recurring	0	1,380,000	276,000	276,000	276,000
	Recurring	0	571,429	685,714	800,000	914,286

---

Costs	Non Recurring	-1,636,323	-1,200,000	0	0	0
	Recurring	-267,300	-924,300	-1,017,900	-1,017,900	-1,017,900
	<i>Total Benefit/(Cost)</i>	-1,903,623	-172,871	-56,186	58,100	172,386