Florida Department of Education

REQUEST FOR INFORMATION

FOR

Identity and Access Management Administration Software

RFI 2012-44

Florida Department of Education
325 West Gaines Street
Tallahassee, Florida 32399-0400

Please email submissions to:

Florida Department of Education
Attn: Christina Davis
Email: Christina.Davis@fldoe.org

Florida Department of Education
Identity and Access Management
Administration Software

I. INTRODUCTION

The Florida Department of Education (FLDOE, Department) is requesting information regarding portal and single sign-on software solutions. This software will be used to provide one web address where FLDOE stakeholders enter one username and password (credentials) to access the FLDOE data and applications they are authorized to use. FLDOE's intent is to learn more about potential software solutions that can fulfill the Department's technical requirements for a portal and single sign-on solution.

II. BACKGROUND

FLDOE currently provides a number of data and application resources to its stakeholders from school districts, charter schools, state colleges, universities, researchers, and others. These applications currently require a unique set of credentials specific to their application for each user. Further, administrators must use different user provisioning tools to create, update, and disable accounts within their purview. This means users must remember multiple sets of credentials and administrators must duplicate user provisioning effort in multiple applications to give a single user appropriate access to more than one FLDOE resource.

In order to provide single sign-on access to FLDOE resources and centralize user administration, the Department will implement a claims-based architecture consisting of the following key components:

- *Portal* to serve as a single web address to simplify navigation for stakeholders;
- *Directory* to serve as the single repository for all FLDOE Portal user account and application information, and to authenticate users (expected volume over 1 million accounts);
- *User Provisioning* tools to centralize identity and access management administration for all FLDOE resources available via the portal;
- *Identity Provider* to issue trusted tokens for authenticated users; and
- *Federation Provider* to serve as a broker between known and trusted Identity Providers within the FLDOE Federation and FLDOE resources.

The logical design for the Department's portal and single sign-on solution is depicted below in *Figure 1 – FLDOE Portal and SSO Logical Design*.

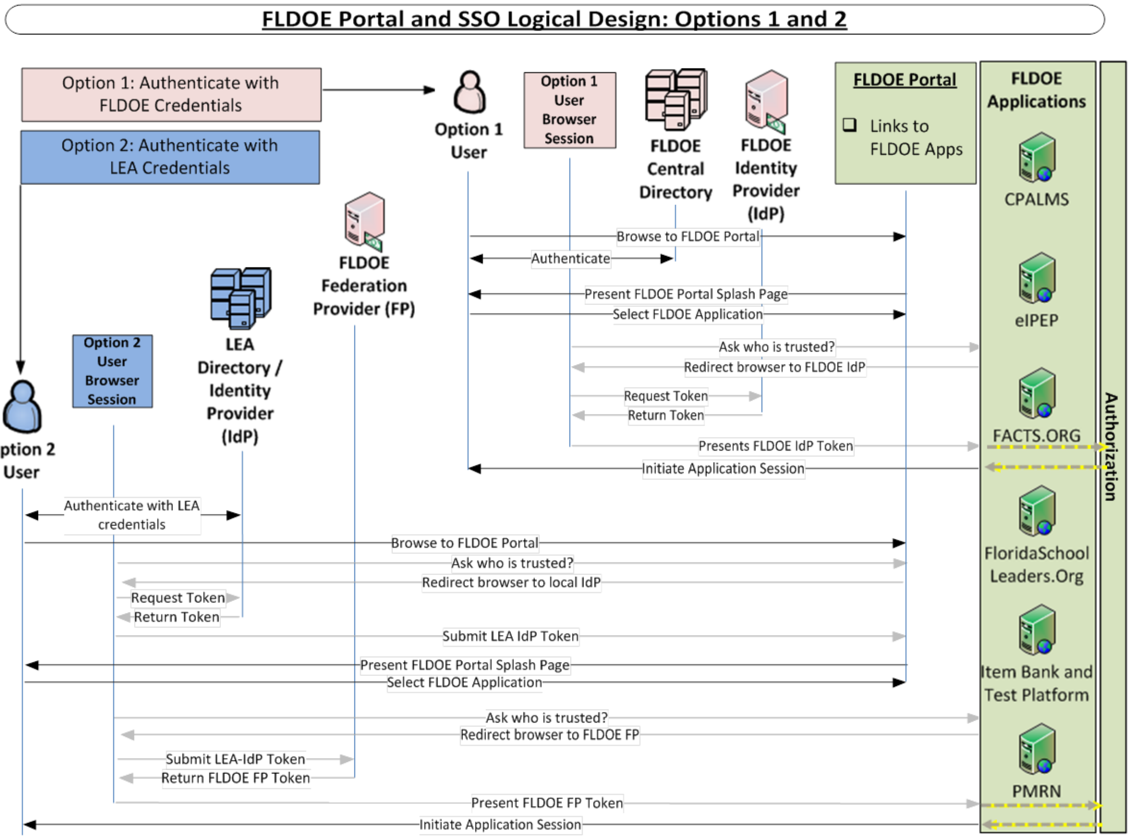
FLDOE Portal and SSO Logical Design: Options 1 and 2
Option 1: Authenticate with FLDOE Credentials
Option 2: Authenticate with LEA Credentials
Option 1 User
Option 1 User Browser Session
FLDOE Central Directory
FLDOE Identity Provider (IdP)
FLDOE Portal
❑ Links to FLDOE Apps
FLDOE Applications
CPALMS
eIPEP
FACTS.ORG
FloridaSchool Leaders.Org
Item Bank and Test Platform
PMRN
Authorization
FLDOE Federation Provider (FP)
LEA Directory / Identity Provider (IdP)
Option 2 User Browser Session
Option 2 User
Browse to FLDOE Portal
Authenticate
Present FLDOE Portal Splash Page
Select FLDOE Application
Ask who is trusted?
Redirect browser to FLDOE IdP
Request Token
Return Token
Presents FLDOE IdP Token
Initiate Application Session
Authenticate with LEA credentials
Browse to FLDOE Portal
Ask who is trusted?
Redirect browser to local IdP
Request Token
Return Token
Submit LEA IdP Token
Present FLDOE Portal Splash Page
Select FLDOE Application
Ask who is trusted?
Redirect browser to FLDOE FP
Submit LEA-IdP Token
Return FLDOE FP Token
Present FLDOE FP Token
Initiate Application Session

Figure 1 – FLDOE Portal and SSO Logical Design

III. TECHNICAL REQUIREMENTS

The Department is seeking technical (not marketing) information from vendors regarding available software, and associated hardware, to implement the claims-based architecture as described in Section II Background. The following are high-level requirements associated with the components of the design:

a. Proposed software should be proven technologies (i.e. standards-based and widely used) that are customizable to FLDOE needs, scalable, highly-available, and secure (i.e. role-based access control).

b. The Portal should support current and most recent past versions of common browsers (i.e. Internet Explorer, Safari, FireFox, and Chrome), including mobile mini-browsers.

c. The Directory should include an extensible schema to accommodate anticipated future attribute needs of FLDOE applications.

d. The Directory should include the ability to identify duplicates and enable merge or split of records.

e. The Identity Provider should sign and encrypt tokens, and handle a large volume of simultaneous requests.

f. The User Provisioning Tool should integrate with the Directory and include the ability for users to manually provision accounts individually or in bulk, and provide the ability to fully automate the provisioning process.

g. The User Provisioning Tool should provide the ability to create and manage workflows.

h. The User Provisioning Tool should include self service and user account notification capabilities.

IV. RESPONSE FORMAT

Potential vendors are asked to address all of the following requirements in their response. Vendors may collaborate to submit a combined response, if desired.

i. Clearly explain if and how the product(s) proposed meet the technical requirement listed in Section III Technical Requirements. If the proposed product(s) do not meet all technical requirements, list the other product(s) that fully integrate with the proposed product and meet the remaining requirements.

j. Provide detailed **technical** (NOT marketing materials) product information.

k. Provide server, hardware, licensure, and any other infrastructure requirements. Hardware specifications should indicate how many concurrent users can be accommodated by the recommended infrastructure as well as the anticipated average storage requirements.

l. Given that all traffic is authentication and claims-creation only, and the solution will be ultimately sized to accommodate a total user community in the million-plus range, provide an estimate of the bandwidth required to support a concurrent subset of this user-base totaling up to 300,000 concurrent sessions and state the throughput that would be achieved.

m. Provide basis of cost for software including, but not limited to:

    1. Licensing:
        i. Licensing Unit Cost
        ii. Licensing Unit of Measure (e.g. per user, per server, enterprise, etc.)
        iii. Licensing Period
    2. Installation and Configuration:
        i. Installation and Configuration Cost (if included in licensing cost, please mention)
        ii. Additional Hours Rate
    3. Maintenance:
        i. One-time Cost
        ii. Recurring Cost (indicate Period and Rate/Period)

n. Provide basis of cost for staff training and customer support including, but not limited to:

    1. Technical Support:
        i. How many hours of Support included in Licensing cost
        ii. Rate for Additional hours

iii. Description of Support provided during initial installation and configuration

iv. Description of Support provided during warranty or paid maintenance period

2. Training:
   i. How many hours of Training included in Licensing cost
   ii. Type of Training provided (e.g. User, Administrator, etc.)
   iii. Venue for Training (e.g. on-site, off-site, etc.)

o. Provide description, estimated time, and typical human resources associated with installation and configuration.

p. Describe human resource requirements for "on-going" maintenance and administration.

q. Provide information or suggestions regarding necessary requirements.

r. Provide product information regarding compliance with Section 508 of the Rehabilitation Act of 1973 and Sections 282.601 – 282.606, Florida Statutes.

V. PROCESS

FLDOE will review and analyze information received from this Request for Information (RFI) to determine the feasibility of issuing a competitive solicitation for these services. Any request for cost information is only to gain a perspective of the potential budgetary magnitude.

Responses to this request will be reviewed for **informational purposes only** and will not result in the award of a contract. Vendors submitting answers to the RFI are not prohibited from responding to any related subsequent solicitation.

SCHEDULE OF EVENTS

A. Procurement Time Schedule

The following timetable shows the approximate dates for this procurement. All times indicated are Eastern Time (ET).

Request for Information Issued	**February 02, 2012**
Questions Due to no later than	**February 09, 2012 at 3:00pm**
Answers to Vendors on or before	**February 15, 2012**
Receipt of e-mailed RFI responses	**February 23, 2012**

PLEASE PROVIDE RESPONSES VIA EMAIL

B. Questions And Restrictions

The Department of Education may be contacted via email or fax regarding the submission of questions concerning this RFI. Any respondent's questions must be submitted in writing and received by the Department on or before the specified due date at the following email address or fax:

Please deliver questions to:
Florida Department of Education
Attn: Christina Davis
325 W. Gaines Street, Suite 324
Tallahassee, Fl 32399
Fax number: 850-245-9189
Telephone number: 850-245-9191
Email: Christina.Davis@fldoe.org

The Department will provide written answers to all questions that respondents submit by the specified due date. Questions and Answers and notice of changes (addenda), will be posted on the Florida Vendor Bid System (VBS) at www.myflorida.com (click on Business & Industry, under Doing Business with the State of Florida click on State Purchasing, click on Everything for Vendors and Customers, then Vendor Bid System and Search Advertisement, select the Department of Education in the Agency window and initiate search), under this RFI number. It is the responsibility of all respondents to monitor this site for any changing information prior to submitting a response.

GLOSSARY

Glossary Entry	Definition
Account Management	The process of maintaining credentials and assigning roles for a user. Also called "User Provisioning."
Application, FLDOE	See FLDOE Application
Authentication	Proving the user logging in is who they say they are.
Authorization	Granting an authenticated user appropriate access to resources. For FLDOE RTTT Portal: The process of verifying the access an authenticated user has to an FLDOE application.
Claim	The contents of a Token which makes claims about the user to the target application, i.e. UserID, Name, Role, Email address, etcetera, as defined by the application owner.
Claims-based Architecture	Architecture built upon interoperable chains-of-trust that permits the creation and transfer of tokens containing claims between entities that would not otherwise trust one another.
Credential	The combination of username and password required to uniquely identify each user within the FLDOE Portal.

Glossary Entry	Definition
Directory	The repository for all user account information and FLDOE application attributes required for the authentication process.
eIPEP	Electronic Institutional Program Evaluation Plan
FACTS.org	Florida's Academic Counseling and Tracking for Students
Federation Provider	The Claims-Based component within FLDOE which will accept and process tokens issued by trusted Server Token Server issuers located in LEA's.
FLDOE	Florida Department of Education
FLDOE Application	FLDOE applications available to stakeholders by entering a username and password on the FLDOE Portal. The applications include: (1) CPALMS, (2) eIPEP, (3) FACTS.org, (4) FloridaSchoolLeaders.org (5) Interim Assessment Item Bank and Test Platform, and (6) PMRN. Also called a Primary Application.
FLDOE Portal	One web address provided by FLDOE to access FLDOE applications via single sign-on.
FLDOE Single Sign-on	The ability for a stakeholder to enter one username and password to access FLDOE applications.
Identity Management	The process of authentication and authorization of users to access FLDOE applications.
Identity Provider / IdP	An IdP is one or more servers which issue a token to an authenticated client for presentation to the target application. Located within both FLDOE for use by portal users (Option 1), and in each LEA which uses LEA credentials to authenticate (Option 2).
LEA	Local Education Agency including districts, charter schools, colleges, universities or other organizations using FLDOE applications.
LEA/Local Application Administrator	LEA/Local staff assigned the role of Application Administrator of an FLDOE Application.
LEA Staff	LEA staff using FLDOE Applications.
Maintain	Relates to user / role maintenance, and means to create, update, or disable a user within the FLDOE Central Directory using the FLDOE Directory Manager.
Management, Account	See Account Management
Management, Identity	See Identity Management
Management, Role	See Role Management
PEER	Portal to Exceptional Education Resources
PKI	Public Key Infrastructure is a standards-based set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. This extensive and long-standing set of standards include, but are not limited, to the ITU-T (formerly CCITT) X.509 standard which defines the format and certain usages for digital certificates.

Glossary Entry	Definition
PMRN	Progress Monitoring and Reporting Network
Portal, FLDOE	See FLDOE Portal
Primary Application	See FLDOE Application
Replying Party	The target application which relies on the tokens and claims for determining permissions to be granted to the user. Used interchangeably by vendors with “Service Provider”.
Role	A collection of user access rights within an FLDOE application.
Role Management	The process of maintaining roles and their access rights within an FLDOE application.
RTTT	Race to the Top
Single Sign-on, FLDOE	See FLDOE Single Sign-on
SLDS	Statewide Longitudinal Data Systems
SLDS Program	Group of projects comprising the initiatives from three (3) distinct grants - 2009 SLDS (Round 3), 2009-ARRA SLDS (Round 4), and RTTT (specifically, Data Assurance Area [Section C, Data Systems to Support Instruction]).
SSL	Secure Sockets Layer. A PKI-derived certificate normally associated with HTTPs (Hyper-Text Transfer Protocol – Secure) traffic to websites. Used also for server and individual identification.
Stakeholder	An individual or organization that is involved in or may be affected by project activities. Ref. PMBOK® Guide.
Security Token Server	Role carried out by the Identity Provider and Federation Provider for issuing encrypted tokens to users.
Token	Encrypted packets which contain claims about the user. Issued by Identity Provider or Federation Provider and used by the client browser to present information about the user to the application in order to permit access and define appropriate permissions.
Trust	The agreement between components that tokens issued by one will be trusted and processed by another.
User Provisioning	See Account Management.
Workflow	A sequence of steps intended to automate a process.