SLI Identity Integration – RFP Guidance

SLC Project Document
January 27, 2012

Change Log

Date	Version	Name	Change Summary
1/23/12	V1	EFloyd	Initial draft submission to SLC
1/26/12	V1.1	EFloyd	Incorporated A&M feedback, completed the SLI Bulk Data Ingestion section, removed LRMI section

Table of Contents

1. Introduction

This document is part of a series of documents that contain specifications for application software and system procurement where integration with SLI technologies is required. This *Draft Specification Document* provides a draft view of a future SLC released document and is intended to be referenced in vendor RFPs. As of this writing, the SLI standards are still in development. The technical information in this document should be considered preliminary.

This document provides specifications for Identity Integration.

1.1. Structure of Document

The draft specification is divided into five sections:

- **Overview** – Provides a broad description of the SLI technology upon which the requirements are based, including use case summaries.
- **Integration Approach** – Describes one or more approaches for integrating with a core SLI technology.
- **Relationship to Other Standards and Technologies** – Describes how a proposed solution is expected to make use of, or facilitate the use of, other SLI technologies.
- **Configuration Options** – Discusses areas of potential configurability.
- **Standards and Technologies** –Identifies applicable standards and technologies, and specifies their applicability to this standard. This section also identifies related projects, initiatives, and organizations.
- **Constraints** – Specifies constraints and exclusions that a proposed solution must satisfy.

2. Overview

This section provides an overview of Identity Integration.

2.1. What is Identity Integration?

Identity Integration is set of services that enable an SLI application to reliably identify a user (authentication), and to establish what actions that user is permitted to take with SLI data (authorization). It also facilitates Single Sign-On (SSO) – sharing of identity information among applications so that it is not necessary for the user to enter identification credentials (e.g., user ID and password) for each application separately.

In order to achieve authentication integration and SSO with SLI, a State (SEA) or Local (LEA) Education Agency must have a Directory that stores all of the user identities that will access SLI, and that is able to associate each identity with the roles that will govern the user's permissions within SLI. This Directory must be integrated with SLI so that it contains a mapping of the local identifier for each user to the "universal" identifier of that same user in the SLI data store. Once Directory integration is established, when an end user establishes a "session" by logging into the SLI portal or any SLI application, that user's identity will be authenticated by the SEA/LEA Directory, not by the SLI system

itself. The SEA/LEA Directory will verify that the username and password credentials supplied are valid and then return this information to SLI for further access control, authorization, and auditing purposes. Identity Integration also facilitates sharing among SLI applications the identity of the user and the fact that the user has established a session by recently entering valid credentials.

2.2. The Objective

The objective of Identity Integration is to ensure that only authorized individuals can gain access to the information that they are authorized to view or change. To that end, the following security controls will be strictly enforced by SLI:

- All traffic between the SLI platform and the SEA/LEA directories will be encrypted
- All login activities that include the user Id and password will be encrypted
- All login activity (both success and failure) will be logged and reviewed
- All failed access attempts to data will be logged for audit purposes and to identify access model issues
- All application and user access to the SLI API will require authentication
- No anonymous access will be allowed
- Controls will be established to ensure that session identification mechanisms will be protected to ensure that a session cannot be compromised

2.3. Use Case Summaries

Selected use case summaries are provided below in order to facilitate a general understanding of Identity Integration.

Title	Summary
Ms. Harrison, 9th grade social studies teacher	Signs on to the Portal which authenticates using Identity Integration. Clicks the Dashboard button. The Dashboard, a fully-integrated Portal application, contacts the SLI API to check for a valid session. The API recognizes that a valid session already exists for her and immediately returns a list of the resources and services for which she and the Dashboard application are authorized. She uses Dashboard to identify a reading comprehension as a common underlying cause of a student's performance problems in multiple subjects. Clicks the Recommendation Engine button. The Recommendation Engine, using information from the session established earlier, determines that the current user is a Teacher and presents a menu of instructional applications. She uses the Engine to select a unit of study and age-appropriate instructional materials focusing on ELA standards. Post intervention, student assessment results are prepared for batch ingestion and identified with District credentials and institution identification so that they will appear on the appropriate teachers' dashboards and in the students' learning maps. The District Super Administrator authorizes student result summary statistics and teacher evaluations of instructional materials to be available on teacher dashboards across the district and state to help inform future recommendations for students like this one.

Title	Summary
Julia Sanford, District English Language Learner Coordinator	Upon returning from her lunch break, clicks the ELL app button triggering a request to the ELL application. The ELL application recognizes that a previously-established user session has timed out and is no longer valid. It redirects the portal browser to the local sign-on authority which requests user credentials and authenticates against the local Active Directory. The local sign-on authority then redirects the browser back to the ELL application with appropriate session information appended to the request. The ELL app determines that the current user is an administrator/researcher and provides data analytics functionality. With this, she identifies students ready to be designated as Fluent that have also been flagged as at risk of dropping out based on criteria identified by a data analytics tool. Clicks the Dashboard button. Dashboard recognizes that she has a valid session. She is again identified as a researcher and authorized to view statistical summary data approved for access by her district and others. She researches similar student populations across multiple districts and finds that math intervention program that is centered on a specific kind of app that has been successful. Using the resource search capability, she locates a highly-rated app that also happens to be SLI-compatible, significantly reducing the IT Department's effort to get the app integrated with district systems.

3. Identity Integration Approach

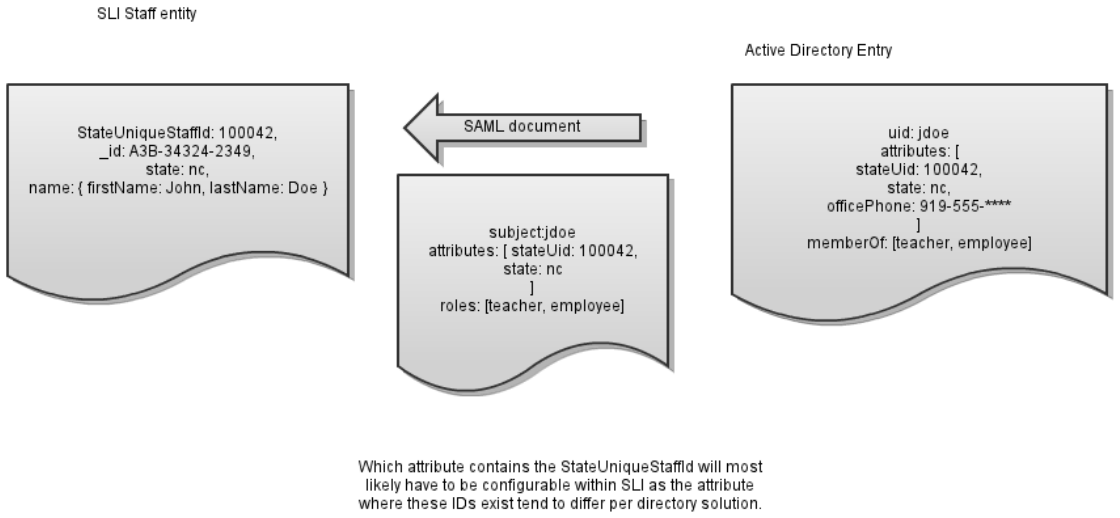
In order for an Institution's users to access SLI, the Institution's Super-Administrator must identify a local Directory[1] that contains the users and associated Roles that will be used to access SLI. SLI will access this Directory using one of the methods described below. When a user logs into the SLI portal or an SLI application, that user's identity will be authenticated by the Institution's designated Directory. The Directory will verify that the username and password credentials supplied are valid and return this information to SLI.

[1] The Directory may consist of one or more local directories. In this document, we will use the term "Directory" to refer to any and all local directories that are integrated with SLI by the institution's Super-Administrator.

After a user is authenticated, the SLI API will issue a time-limited authenticated user token. All subsequent calls to the SLI API for this user's session must include this authenticated user token. The API will use this token to determine the user's identity and which actions the user is allowed to perform.

3.1. SLI Roles

Each user is associated with one or more SLI Roles. These Roles, along with context drawn from the data in SLI, will be used to determine what operations a user can perform in SLI. Each Super-Administrator must either create Roles in the local Directory that correspond directly to the SLI Roles, or create a mapping from roles in the local Directory to SLI Roles.



At each successful user login, SLI will retrieve role information from the local Directory and map those roles to SLI Roles (if necessary) to determine what the logged in user is allowed to access.

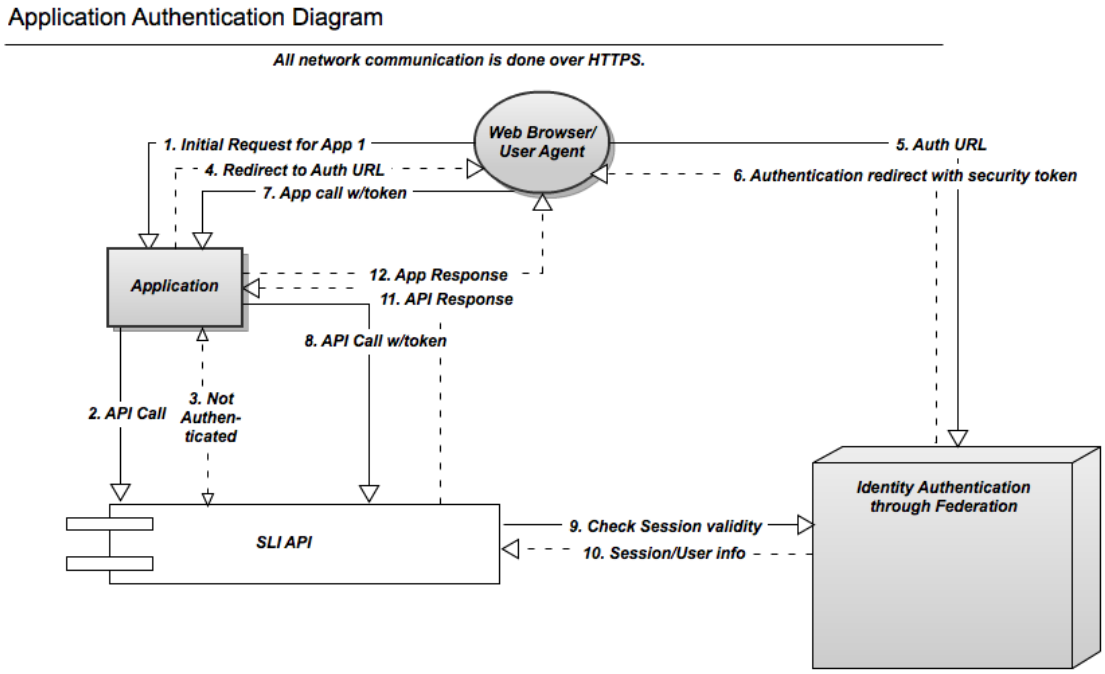
3.2. Integration Strategies

SLI will initially support two integration strategies: Federated and Delegated. The preferred strategy is Federated.

The SLI Federated strategy uses SAML 2.0. A SAML-based strategy allows SLI to provide secure access to SLI data without providing applications with access to user IDs and passwords. SAML is a widely used industry standard for implementing data sharing across applications and is often used as part of a Single Sign-on (SSO) solution. SAML is extremely flexible and applicable in a large variety of situations. Because of its feature-richness and flexibility, SAML may be somewhat complex for developers to implement. In a SAML implementation, a server known as an Identity Provider (IdP) is required. This server is responsible for capturing credentials from a user, validating those credentials

and returning a Token that may be used by SAML-aware applications. Some Institutions may already have a SAML IdP solution in place, while others may not.

The following diagram illustrates the SLI Federated authentication strategy from the viewpoint of the web browser-based SLI Portal.



Directory products distributed by major vendors typically support SAML IdP services for Federated authentication either out-of-the-box, or with an optional add-on. For directory products that do not provide SAML support, there are both commercial and open source solutions that layer SAML IdP services over LDAP.

As an alternative to a SAML-based Federated strategy, SLI will also support a simpler Delegated strategy. In this strategy, users are still authenticated against the Institution's Directory; however, the credentials are visible to applications and to the API. The delegated solution is easier to implement for both Institutions and Developers. In the simplest Delegated implementation, SLI will use LDAP to directly authenticate users.

The Delegated strategy requires a custom authentication agent to be built, installed, and maintained. The authentication agent receives authentication requests and user credentials from the SLI API, determines the validity of these credentials using the local directory service, and responds with validity and role information.

3.3. Integration Approaches by Proposer Category

Integration approaches vary by proposer category. The following table provides integration guidance for each vendor category:

Proposer Category	Integration Approach
System integrator	1. Recommend a SAML 2.0 compatible IdP or provide a SAML 2.0 integration layer over the existing directory service 2. Recommend web-based applications with SAML 2.0 Service Provider (SP) identity integration capability 3. Assist the State or District with SLI directory integration, including a. User ID and attribute mapping b. Initial SLI set-up to identify the directory services and attribute mappings 4. Configure security for batch extract, transform, and load (ETL) processes for SLI data ingestion
SLI Portal application provider	Build SAML 2.0 SP identity integration capability into applications. Assist District staff in configuring applications for SLI integration
Directory product provider	Provide SAML 2.0 IdP capability. Assist District staff in configuring directory for SLI integration

Additional information on SLI Identity integration is available at http://www.slcedu.org.

4. Relationship to Other Standards and Technologies

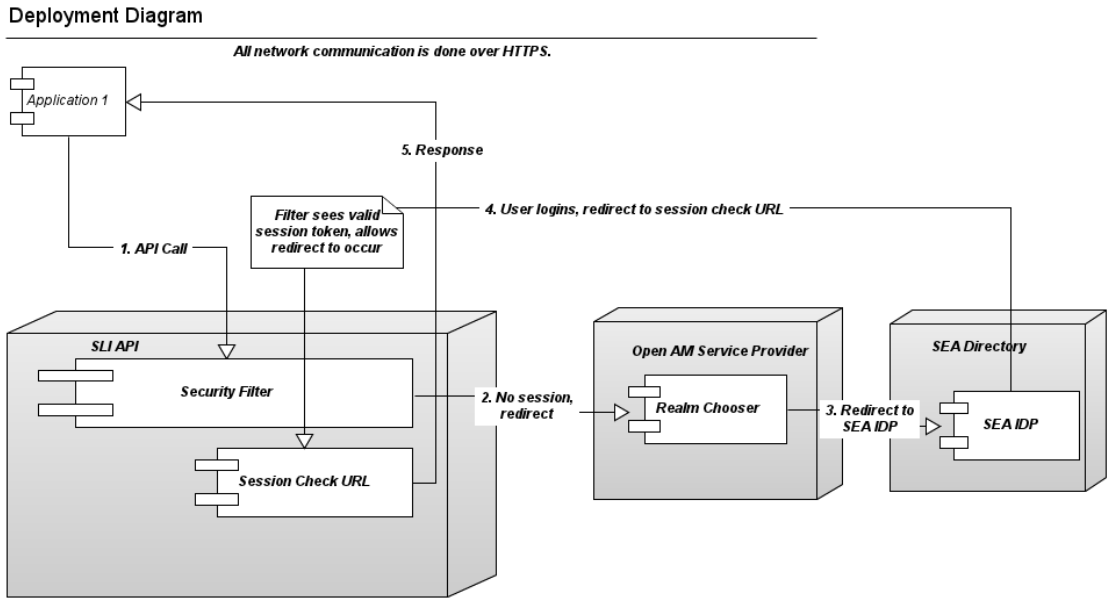
Identity Integration makes use of, and facilitates the use of, the following standards and technologies:

4.1. SLI Application Programming Interface (API)

The Application Programming Interface contains the building blocks that are necessary to create SLI applications. Application access to the SLI Data Store is strictly governed by this API. The overall objective of the API is to provide a stable, well-defined interface for software developers. The API is a real-time transactional interface intended for interactive applications, including fully-integrated SLI Portal applications that access the SLI Data Store.

The SLI API is RESTful. It is designed to have predictable, resource-oriented URLs, to use HTTP response codes to indicate API errors, and to use built-in HTTP features, like HTTP authentication and HTTP verbs, which can be understood by off-the-shelf HTTP clients. The SLI API is designed to be a Level 3 RESTful API in the Richardson Maturity Model. It employs the HATEOAS (Hypertext As The Engine Of Application State) model. Applications that integrate with the SLI Data Store will be consumers of the API RESTful web services.

The API and SAML Identity Integration are inextricably intertwined. Identity integration determines who can do what with the API. The following diagram provides some additional insight into the API authentication mechanism.



The SLI API is the subject of another Draft Specification document.

4.2. SLI Portal and Dashboard

The SLI Portal is designed to provide an easy way to navigate between SLI web applications. Links to a user's applications are displayed on his or her Homepage. This page allows users to switch between web applications approved for use by an SEA or LEA.

The SLI Dashboard Application is a fully integrated portal application created and maintained by the SLC. It allows educators to see data about their students individually, and summarized by class, school, and various other organizational levels. Users can see lists of students, schools, etc. to compare student populations, or drill down to just one student (or school, etc.) profile for more targeted information.

Three application integration strategies are supported by the SLI Portal.

- Application is web-based, designed and built specifically for SLI Portal integration. It supports SAML 2.0 federated authentication.
- Application is embedded as a portlet in the SLI Portal application display area. It may or may not support SAML 2.0 federated authentication.
- Application is embedded in an iframe within the application display area. It may or may not support SAML 2.0 federated authentication.

An SLI Portal Application that provides access through the SLI API to protected information, such as student data, must provide SAML 2.0 Service Provider functionality.

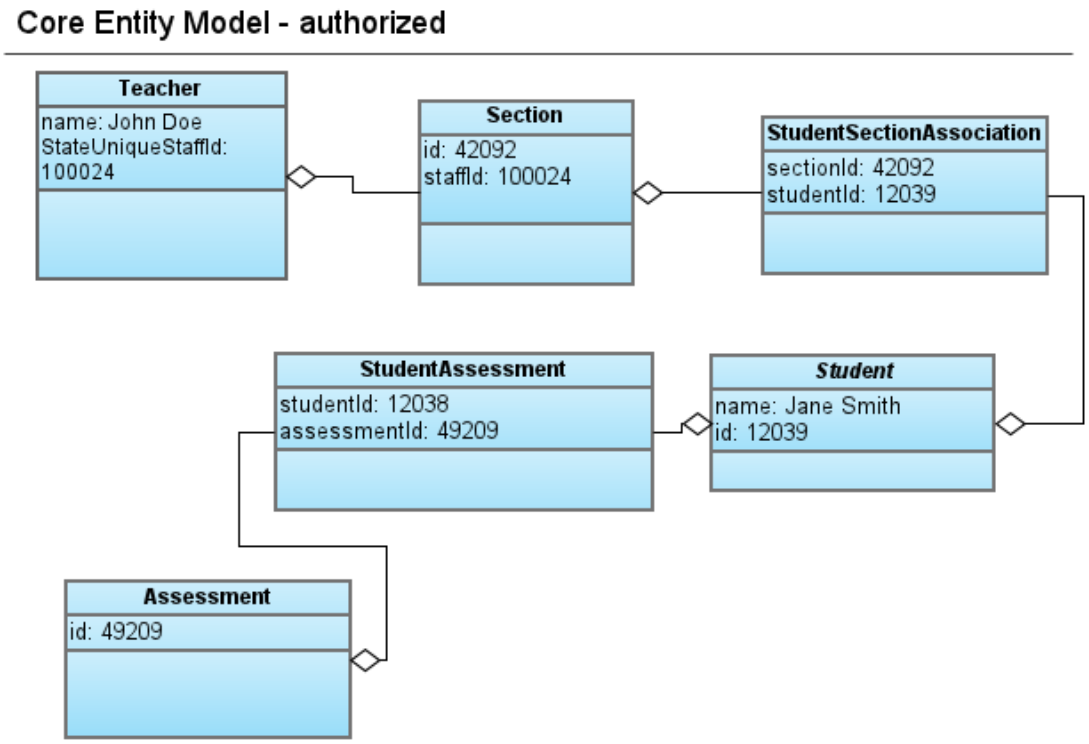
The SLI Portal is the subject of another Draft Specification document.

4.3. Core Entity Model

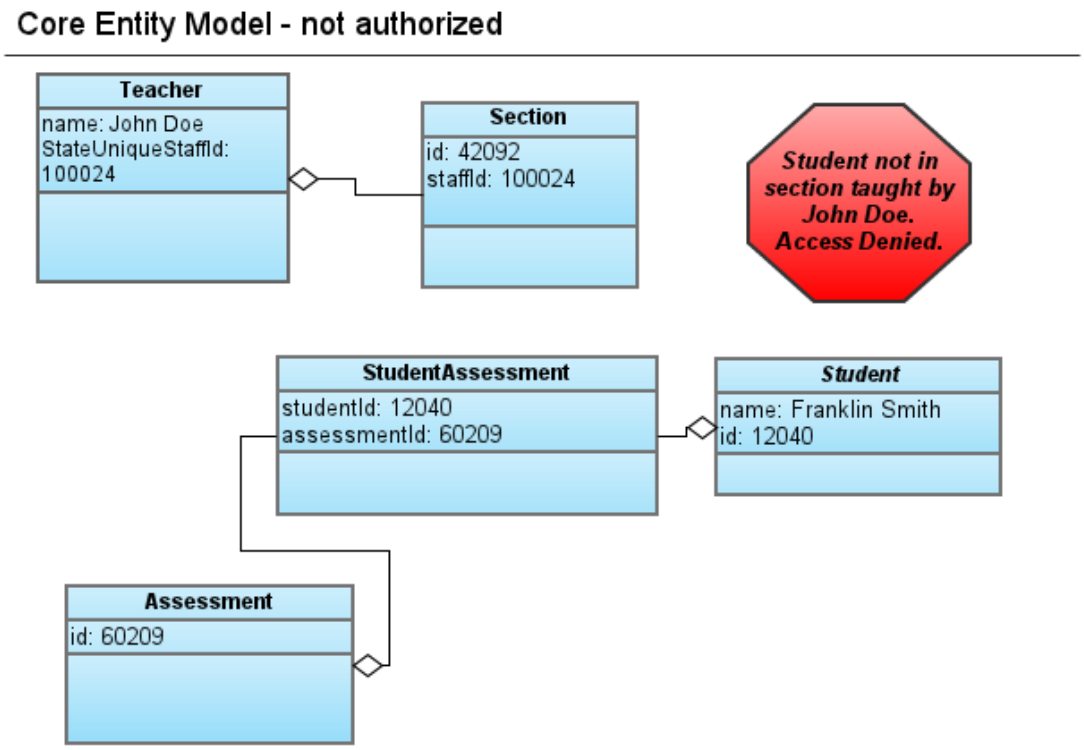
The Dashboard and other SLI Portal applications provide a view into information in the SLI Data Store which is organized according to the SLI Core Entity Model (SLI CEM). The SLI CEM is an abstract, technology-agnostic representation of the K-12 education information domain. The model includes entities that are easily recognized, including: school, student, course, and section. Those entities contain attributes that are also easily recognized, though a complete listing of entities and attributes are beyond the scope of this document.

SLI CEM contains entities along with the relationships that define how the entities interact with one another. Each entity includes sufficient number of attributes to make the model applicable to real-world data. SLI CEM focuses on granular information rather than aggregate statistics. In addition, the model includes information that is necessary to produce aggregate and other types, of statistics.

Entity relationships defined within the CEM, along with the identity of the person requesting access, determine whether or not access to specific entities is permitted. The following diagram illustrates a case in which a teacher's access to a student's assessment data would be permitted because a relation chain exists from the teacher, to a section taught by that teacher, to the student enrolled in that section.



In contrast, the following diagram illustrates a case in which access would be denied because the student is not enrolled in a section taught by the teacher.



4.4. SLI Bulk Data Ingestion

Bulk Data Ingestion is the process by which batches of information are loaded into the SLI Data Store. The process of enabling districts for Bulk Data Ingestion is called "Onboarding". For the purpose of loading information, districts within a state are organized into one or more "Realms". A Realm is a hierarchical segment of a state school system comprised of one or more Districts, entities belonging to those Districts (Schools, Teachers, Students, Courses, Assessments, etc.), and their associations. A Realm is the smallest unit of onboarding.

A Realm is created when a group of District SLI Super Administrators contract together to provide certain defining information to the central SLI administration repository and designate a Realm Administrator.

A Realm Administrator is a special SLI operator role which is authorized to perform administrative tasks for the Realm. As part of the Onboarding process, the Realm Administrator's and Super Administrators' accounts are created in the SLI Platform Directory, data store and ingestion resources are provisioned, and the Districts' federated directory services are configured to communicate with the SLI Identity Service.

A Super Administrator has the full set of IT Administrator permissions by default, but can also delegate authority to ingest District's data to other IT Administrator(s) in that District. The Realm Administrator can provision these IT Administrator accounts within the SLI Platform Directory when granted this permission by a Super Administrator.

Once IT Administrators for districts within the Realm are identified and provisioned, they are securely notified of login credentials, the SLI-hosted directory to be used for authentication, a unique Realm ID, and a “landing zone” URI for data files.

SLI will ultimately support three different ingestion vectors:

1. A SFTP interface to upload ingestion jobs to a designated landing zone.
2. A web-based submission interface.
3. A SIF agent interface.

All ingestion vectors provide a way to authenticate, create and submit a job, monitor its progress throughout the ingestion pipeline, and to be notified of any errors encountered along the way. The specifics of ingestion jobs initiated through the web interface and an event-based ingestion via a SIF agent are currently TBD. The SFTP server authenticates the Realm Administrator, Super Administrators, and IT Administrators against the SLI Platform directory, so Super Administrators and IT Administrators must login with the credentials provided to them at the time of Realm provisioning

5. Configuration

Areas of potential configurability include:

Product Type	Potential Configuration Items
IdP service providers	Attribute mappings between local and SLI identifiers and roles, SAML configuration for federation
Portal integrated applications	SSO parameters, header/footer interface, data sources
Applications that access the SLI Data Store	SAML SP parameters, authentication method (federated / delegated), SLC-assigned registration key
Bulk Data Tools	Realm identifier, landing zone URI, encryption keys, local data sources

6. Standards and Technologies

The following standards and technologies are applicable to this specification:

Standard / Technology	Applicability
Security Assertion Markup Language (SAML) 2.0 http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf	SAML 2.0 is the preferred method of Identity Integration. Particularly useful is Section 5.2 – Web Browser SSO Profile
Claims Based Identity and Access Control http://msdn.microsoft.com/en-us/library/ff423674.aspx	Microsoft strategy for Identity Integration upon which several MS products in this space are or will be based
Windows Identity Foundation (WIF) http://msdn.microsoft.com/en-us/security/aa570351	Windows mechanism for Identity Integration for applications
Active Directory Federation Services http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory-overview.aspx	Microsoft product that supports SAML IdP services with Active Directory
OpenSAML https://wiki.shibboleth.net/confluence/display/OpenSAML/Home	A library for constructing SAML XML objects in Java or C++
Shibboleth http://shibboleth.internet2.edu/	An open source SAML 2.0 SP and IdP solution that can be layered over and existing LDAP directory

6.1. Related and Affiliated Efforts

Initiative / Project / Organization	Applicability
SLI Application Programming Interface (API) http://www.slcedu.org	The API relies on Identity Integration through SAML to control access to the SLI Data Store.
SLI Core Entity Model http://www.ed-fi.org/wp-content/uploads/2011/06/Public-Ed-Fi-Unifying-Data-Model-1.0-111111.pdf	The SLI Data Store is organized according to the Core Entity Model.

Initiative / Project / Organization	Applicability
SLI Data Integration http://www.slcedu.org	Bulk Data Ingestion and Validation are the means by which SEAs and LEAs store information in the SLI Data Store
Learning Resource Metadata Initiative http://www.lrmi.net/	Tagging standards to facilitate content management and discovery
Learning Maps	Pathways through learning objective standards

7. Constraints

To be compliant with this specification, solutions will be subject to the following constraints:

1. Third party Applications will access SLI data through either the Record-Level API or the Bulk Import/Export API.
2. Application developers (including Institution developers) must register their applications according to a process that is defined by the SLC. Each registered application will be assigned a unique ID that will be used in API calls to identify that application.
3. Districts will approve any application accessing data controlled by that District.
4. Applications that provide access to information in the SLI Data Store must be capable of SAML 2.0 federated authentication and SSO.
5. Preference will be given to Portal applications that are capable of participating in a SAML-mediated SSO.