IMS Europe Summit 2019
Advancing Next Generation EdTech, Digital Credentials, and Actionable Data

BARCELONA, SPAIN
10-11 OCTOBER 2019
Realizing the IMS Roadmap

Learn about the essential technical elements forming the foundation for a plug-and-play interoperable ecosystem and share your ideas on areas of collaboration that are relevant and most beneficial to Europe. Hear about the new Unified Data Model approach as a new way of representing data interoperability in a transparent and relatable way.

Colin Smythe
IMS Chief Architect
IMS Global
csmythe@imsglobal.org
Content

- IMS Specifications Context
- Technical Highlights 2018-2019
- Technical Objectives 2019-2020
Short Biography

• Joined IMS in May 1999

• Responsible for the development of many IMS specifications inc.
  • Question & Test Interoperability (QTI)
  • Learning Information Services (LIS)
  • OneRoster
  • OpenVideo Metadata

• Currently IMS Chief Architect and responsible for:
  • How the specifications fit together to create the IMS ECOSYSTEM
  • Overseeing the technical details of the specifications
  • Supporting adoption of the specifications
  • Unified Data Model
On this Day …

1985 – Death of Orson Welles

1813 – Birth of Giuseppe Verdi

1718 – Funding for Yale College at New Haven secured
IMS Specifications Context

Technical Highlights 2018-2019

Technical Objectives 2019-2020
A wide range of specifications (29) published since 1999.

We have an extensive legacy responsibility.
Current Specification Activity

**New Specification**
- Comprehensive Learner Record
- Open Video
- Computer Adaptive Testing

**New Version**
- OneRoster 1.2
- QTI 3.0
- Badge Connect 2.1
- Thin CC 1.4
- Caliper 1.2 + MPs

**Profile**
- Proctoring
- SBAC of QTI
- Japanese OneRoster
- **European OneRoster 1.2 Profile**
- Assessment Results Profile

**Evaluation**
- CASE
- Caliper Metric Profiles
- EDU APIs
Published Documentation

Overview
Implementation Guide
Conformance & Certification

Information Model
Technology Binding
Validation Artefacts
Conformance Test Systems

Reference Material

©2019 IMS Global Learning Consortium, Inc. All Rights Reserved.
IMS Specifications Context

Technical Highlights 2018-2019

Technical Objectives 2019-2020
Trusted Exchange of Student Data

GPOs, CSSOs, and Data Protection Officers have critical security-related concerns about sensitive and personally identifiable information (PII) passing between platforms and tools. Older security frameworks have demonstrated vulnerabilities. IMS Global members are leading the drive to improve student privacy and security by adopting the IMS Security Framework across its standards.

IMS Global creates service-oriented and message-exchange interoperability specifications. These service-based specifications recommend or require many different security patterns; for example, the use of OAuth 1.0 based message signing, OAuth 2.0 based authentication and authorization, and so forth. The IMS Security Framework defines a set of patterns for security that all IMS specifications should use (only in special circumstances will IMS consider exceptions). These security patterns are premised on the appropriate standards and specifications published by other organizations such as the Internet Engineering Task Force (IETF) and its Requests For Comments (RFCs). The core standards used are:
- OAuth 2.0 - RFCs 6749 and 6750 from the IETF
- JSON Web Tokens - RFCs 7515, 7516, 7517, 7518, 7519 and 7523
- OpenID Connect Core - an identity layer, from OpenID Foundation, on top of OAuth 2.0

The use of the IMS Security Framework promotes consistent and compatible implementation requirements and simplifies adoption when more than one IMS specification is being implemented.

In the case where IMS has defined a web services-based standard, such as OneRoster, the specification will describe the set of web service calls that can occur between a service consumer (or Client) and a service provider (Platform). Typical service calls include when a Client 'pulls' the data from the Platform and when the Platform 'pushes' the data to the Client. In many cases, these service calls must occur within an appropriate security framework. For IMS specifications using a web services approach, the figure on the right shows a schematic representation of this security framework.

The IMS specification will define how the Client and Platform will exchange information. This document defines how to achieve the 'Authorization' and 'Authentication' using a separate set of message exchanges and how the actual corresponding set of IMS service calls will use this authorization and authentication information. The authorization and authentication uses an "Authorization Server" which may be a system independent of the Platform or may be endpoints hosted by the Platform.

In the case where IMS has defined a non-web services based standard, such as Learning Tools Interoperability (LTI), the specification will describe the set of messages that can occur between a Platform and a Client. In scenarios where the message exchange is vulnerable (for example, when launching from a web browser), the messages will be signed. This signing MAY include data derived from the identity-based authentication. The IMS specification defines how a Client can transform the messages exchanged between the Platform and the Client (including a user's browser-based interaction) into a Client-based experience. This document defines how to achieve Authentication and Authorization using a separate set of message exchanges between Platform and Client and how to encode the authorization and authentication information in JWT-based message signing of these message exchanges. The authorization and authentication process uses an authorization server which may be a system independent of the Platform or may be endpoints hosted by the Platform.

The IMS Security Framework was published as Final Release to the public in May 2019. It is upon this framework that all IMS service-based specifications should make reference, including the LTI v1.3 and LTI Advantage services.

Public Resource

Security Framework

LTI Security Update
- IMS LTI Security Update v1.0 - Final Release (22 July 2019) addresses a potential Cross-Site Request Forgery threat in earlier versions of LTI (v1.0 and v1.1).
Learning Tools Interoperability Advantage

- LTI 1.3 Core
  - IMS Security Framework
- LTI Extensions
  - LTI Deep Linking
  - LTI Names & Role Service
  - LTI Assignment and Grade Service
- Reference Implementation
This report is generated for every comparison and is available to both Districts and Suppliers helping them and the 1EdTech team identify areas that require additional testing on implementation.
CASE® Network of Academic Standards & Workforce Competencies

is live!
New Specifications Final Release

- Competency Learner Record (CLR) 1.0
- Computer Adaptive Testing (CAT) 1.0
- Open Video Metadata 1.0
## New Versions Final Release

<table>
<thead>
<tr>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caliper 1.2</td>
</tr>
<tr>
<td>OneRoster 1.2</td>
</tr>
<tr>
<td>Question &amp; Test Interoperability 3.0</td>
</tr>
<tr>
<td>Open Badges / Badge Connect 2.1</td>
</tr>
<tr>
<td>Common Cartridge (CC) / Thin CC 1.4</td>
</tr>
</tbody>
</table>
# New Profiles Final Release

<table>
<thead>
<tr>
<th>Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proctoring 1.0 – profile of LTI Advantage</td>
<td></td>
</tr>
<tr>
<td>Assessment Results Profile of Gradebook 1.0 – profile of OneRoster 1.2 Gradebook Service</td>
<td></td>
</tr>
<tr>
<td>OneRoster 1.2 European Profile 1.0</td>
<td></td>
</tr>
<tr>
<td>Smarter Balanced Assessment Consortium (SBAC) QTI 3.0 Profile</td>
<td></td>
</tr>
</tbody>
</table>
EDU-API

**EduAPI** is a set of industry standard extensible APIs to support user provisioning, common source ID and administrative data exchange.

- **SIS**
  - Common Source ID
  - Provisioning
  - Grades
- **LMS**
  - Provisioning
  - Usage Data
- **CALIPER Analytics Events**
  - Provisioning
  - Usage Data
- **Learning Record Warehouse**
  - Unified Data Model
  - Provisioning
  - Usage Data
- **Card Access System**
  - Provisioning
- **Digital Content**
- **makerspace**
- **Library**

**EDU-API** is an open standard that enables interoperability across learning management systems (LMS) and other educational technologies. It supports user provisioning, common source ID, and administrative data exchange, facilitating seamless data exchange and management across different platforms.
New Technical Activities

- Security Committee
- IMS Extensions Framework
- LTI Advantage / Assessment Results Profile integration
- Next Generation Metadata
Unified Data Model

Data at Rest
- Db Schema

Data in Motion
- APIs + Data Models

Common Data Models

Visualizations
Future IMS Europe Technical Briefings

- December 2019 - November IMS Quarterly Review (tbd - specification review)
- March 2020 - February IMS Quarterly Review (tbd - specification review)
- June 2020 - LILI 2020 Review (including IMS Members Meeting)
Questions & Comments?
THANK YOU!
IMS Europe 2019 Sponsors