

TRUSTED EXCHANGE OF STUDENT DATA

WHY PLATFORMS AND TOOLS SHOULD ADOPT LTI 1.3

RESPONDING TO MARKET CONCERNS ABOUT STUDENT DATA PRIVACY AND SECURITY

CIOs and platform providers have security-related concerns about sensitive and personally identifiable information (PII) being passed between platforms and tools. Older security frameworks have demonstrated vulnerabilities. **IMS Global Learning Consortium** members—over 500 leading school districts, higher education institutions, states, and edtech solution providers—are leading efforts to improve student privacy and security by adopting the new IMS Security Framework.

Learning Tools Interoperability® (LTI®) 1.3 and LTI Advantage are the first IMS standards to leverage the new security model. Beyond the privacy and security benefits, LTI 1.3 has a more straightforward upgrade path than other versions and the full support and endorsement of major platform providers.

LTI 1.3 HAS BETTER SECURITY

IMS Security Framework adopts the industry standard protocol IETF OAuth 2.0 for authentication services along with JSON Web Tokens (JWT) for secure message signing and adopts the Open ID Connect workflow paradigm.

- **Agile**—Tools and platforms can leverage up-to-date OAuth 2.0 libraries and common industry standard practices in their implementations, which accelerates their development.
- **Flexible**—A modernized security model that is independent of the core spec, allowing for the evolution of security without driving change into the core. Likewise, core changes can evolve without impacting security.
- **Protected Launch**—OAuth 2.0 is an established industry model leveraging HTTPS (using TLS) encryption in place of the complex cryptographic signatures required in OAuth 1.0.

- **Mobile Ready**—The model is independent of web browsers, a better solution for server-to-server, native desktop and mobile applications.
- **Scalable**—OAuth 2.0 scales better, supporting separate roles and servers for authorization versus resource servers handling API calls.
- **Robust**—OAuth 2.0 libraries are actively maintained and a strong community of use and stability.

A SIMPLER UPGRADE PATH

As a specification, LTI 1.3 is based upon LTI 1.1, the LTI version adopted by the vast majority of LTI implementations today, therefore LTI 1.3 is more compatible with LTI 1.1 services and messages and provides a simpler upgrade path for the most implementers.

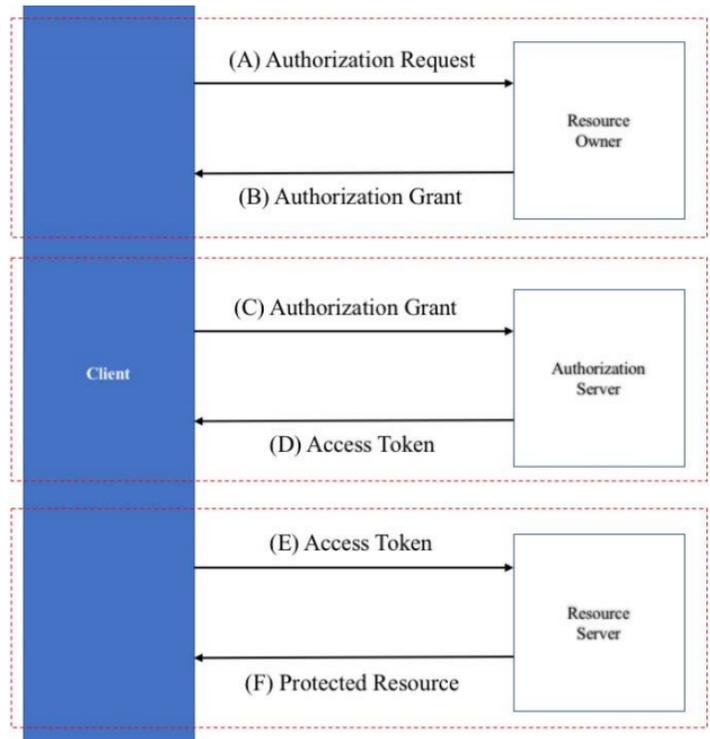


FIGURE 1. IMS OAUTH2-BASED SECURITY FRAMEWORK ABSTRACT PROCESS FLOW

MORE SECURE THAN CUSTOM, NON-LTI AND OLDER LTI SOLUTIONS

To achieve IMS certification and to maintain compliance, each tool must recertify at least annually. This process verifies the proper operation of the security and the data transfer processes against a conformance specification. Tools and platforms that pass LTI 1.3 certification have demonstrated operational compliance with OAuth 2.0 and JWT message signing protocols. Non-standard or older implementations of LTI that use proprietary security schemes or OAuth 1.0 variations have known risks or vulnerabilities requiring much deeper, time-consuming security evaluations. LTI 1.3 and LTI Advantage certification provides peace of mind to administrative and security officers alike.

NEW SINGLE-REGISTRATION OPTION

The updated security comes with a cost, as management of public/private keys can be an additional step for tool providers. This, however, is offset by the fact OAuth 2.0 does not require special message signing and is a well-understood protocol in the market, the developer learning curve should be lower. And, it appears most platforms will be adopting LTI 1.3 in such a way that offer workflows to simplify processes for tools and for their users. For example, in many cases it will be possible for a tool to register once globally with a platform allowing implementers to adopt the tool without requiring additional communication with the tool provider; e.g. Tool X can register with an LMS once and users of the LMS will be able to easily find and adopt the tool without having to contact Tool X for keys or configuration information.

LTI ADVANTAGE IS BASED ON LTI 1.3

LTI Advantage is a set of three LTI services based on the core LTI 1.3 specification that make it easier for faculty to build, manage, and offer courses with a premium user experience while providing world-class security. The availability of specific features is based solely upon the platform and tools in use. The current LTI Advantage services include:

- **Assignment and Grade Services** seamlessly syncs grades, progress, and comments from multiple sources into an LMS platform's gradebook, greatly reducing faculty effort and the chance of errors.
- **Deep Linking** supports a natural and efficient user workflow between a learning object repository or content tool and the LMS platform when developing courses and programs, again saving teachers' time.
- **Names and Role Provisioning Services** securely shares course roster/enrollment information with the requesting tool to enhance users' experiences and provide administrators a basis for who has used the tool and importantly, who has not.

Each of these services requires the new and improved security model available with LTI 1.3, enabling the foundation for a better, more secure user experience.



Purchasers of IMS Certified products are confident their integrations will be secure and fully interoperable with other certified tools. Reliable and consistent product integrations minimize the technical barriers often encountered with custom tool integrations.

Visit the IMS Certified Product Directory—the official catalog of products with current IMS certifications—at imscert.org. Products listed in this directory are *guaranteed* to meet the IMS standards for which they have passed testing.