1EdTech Advisory on the Use of LTI Shims for Tool Integrations

Executive Summary

In the educational technology landscape, the bond between a Learning Platform and an Educational Tool is not merely technical. It signifies an alliance between two vendors (platform and tool) and a learning institution, merging commercial interests with the safeguarding of sensitive student data, including PII. This partnership, underpinned by rigorous authentication frameworks, plays a pivotal role in the academic journey, influencing outcomes such as grades and transcripts.

1EdTech® Learning Tools Interoperability (LTI)® was originally developed and continues to evolve to support the needs of the suppliers and institutions in the edtech ecosystem. Learning Tools Interoperability™ is by far the most widely used standard for learning tool integrations with learning platforms of all types. LTI™ Advantage from 1EdTech provides a set of services that result in a much more seamless user experience (for faculty and learners) and secure rich interactions between learning tools and platforms. LTI Advantage also has some 16 new services that are being developed by the members as open standards to continue to evolve the best possible user experiences and data exchange.

One emerging concept for integrating learning tools with learning platforms is the LTI "shim." The term shim refers to software that provides translation to enable two incompatible software products to integrate. One approach is to add the shim to a product and thus become part of the product. Another approach is to rely on a 3rd-party that attempts to provide the shim as a service that sits between the two applications that are to be integrated.

This document delves into the role and nuances of these shim patterns within the LTI framework. While examining instances where a shim deployment is beneficial, we also highlight 3rd-party providers of shim services that may introduce serious risks. These risks include security, privacy, phishing attacks, security management, dependence on 3rd-party security practices, non-transparency, complexity, dependence on proprietary integrations, and service reliability.

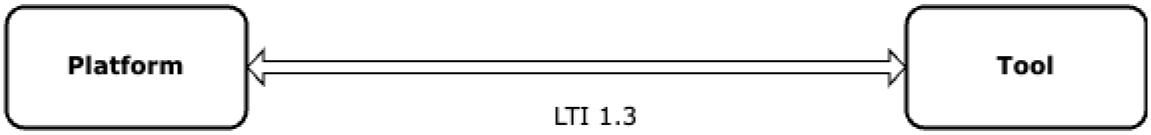
Third-party shims can provide a short-term “fix” to enable integration, but they also may potentially undermine the benefits of the LTI standard, such as ease of migration, full-featured functionality, security, and privacy. In addition, direct standards integration means that institutions and suppliers can take advantage of 1EdTech’s interoperability diagnostic tools. Ultimately, using a third-party provider of a shim will likely create much greater cost and risk for all partners involved in supporting an edtech integration. Market experience has shown that it is much more cost-efficient and effective to support standards such as LTI in all products natively.

For institutions and suppliers alike, 1EdTech provides the community and technical resources to avoid making a poor choice when it comes to edtech integrations:

1. Check to ensure your partner is a 1EdTech member because this means they have the means to be up-to-date on the latest evolution of LTI and other 1EdTech standards. The 1EdTech member directory is always up to date.
2. Check to see if a product has a current certification for LTI and other standards in the TrustEd Apps Directory. If the product is certified, 1EdTech will stand behind the integration and provide technical support if an issue is encountered. If a product is not certified, this is a red flag. Through the certification process, 1EdTech provides suppliers with the latest technical resources for ensuring correct implementation of LTI and other standards.
3. For help in procurement, check out the 1EdTech resources on how to add wording to RFPs or in talking with your partners to ensure you are getting authentic standards from qualified parties. Through this process you can ensure that use of open standards is non-negotiable and also require commitment to standards as they evolve into the future.
4. Contact 1EdTech for help with your particular situation.

Understanding LTI 1.3, the Core of LTI Advantage

LTI 1.3 leverages globally recognized security standards (OAuth 2.0, OpenID Connect) to ensure top-tier security for educational data, aligning the education sector with the best practices of other industries.



LTI 1.3 is a technical connection that reflects a pre-established relationship between multiple parties (institution, learning platform, and educational tool) to deliver a piece of a learning journey for a student. The relationships are complex and often underpinned through certification, auditing with security/ privacy rubrics, and contracts.

LTI 1.3, therefore, provides the technical assurance that the security model and the data transfer are appropriate, secure, and adhere to pre-established/ known parameters within relevant compliance frameworks.

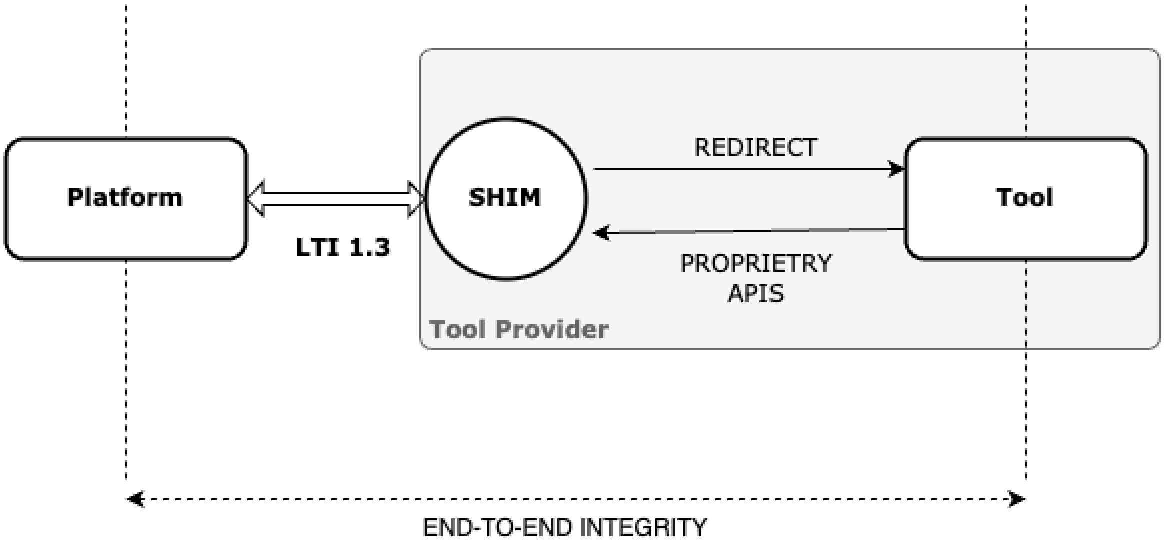
What is an LTI Shim?

At its core, a shim is an intermediary piece of software that bridges the connection between two systems. Instead of modifying original systems to ensure compatibility with LTI 1.3, a shim can act as a bridge, ensuring that systems can interface with LTI 1.3 without altering their intrinsic functionalities or modifying too deeply.

Are Shims Useful?

The appeal of shims is largely rooted in getting to a working integration faster or supporting integration with a product that is unlikely to implement an open standard, such as LTI, for instance, a legacy product. Many mainstream tool providers build and maintain their own LTI 1.3 shims within their own infrastructure for their tools to leverage. This is a well-established pattern that delivers LTI 1.3 integration without compromising the assurance that LTI 1.3 can offer security and privacy. Shims can be grouped into 3 different patterns:

1. Internal Shims: Tool-hosted

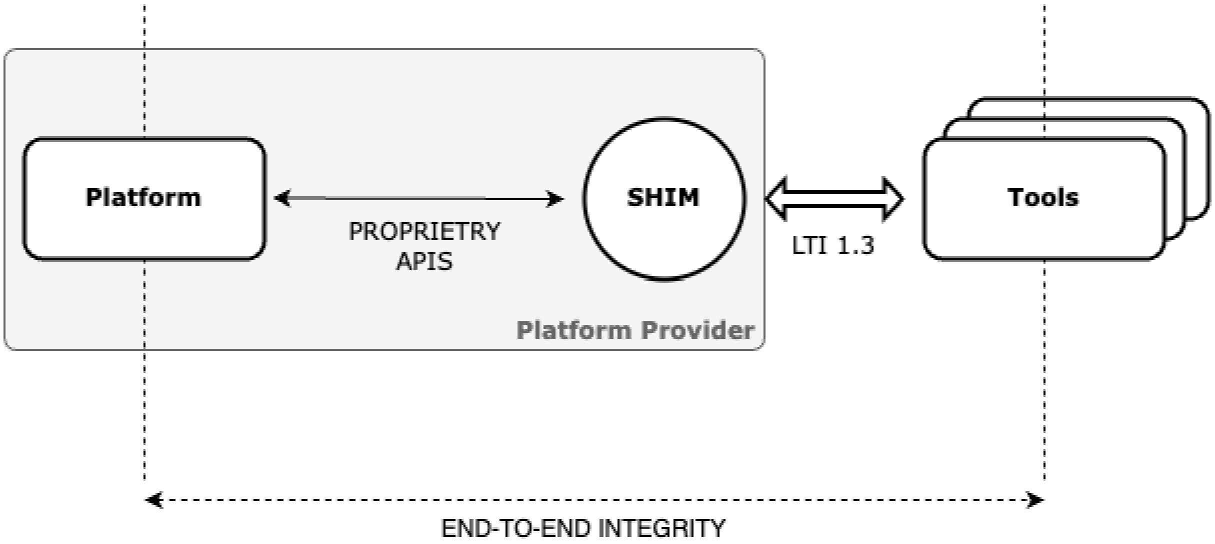


For tool providers, shims facilitate integration with multiple learning platforms, offering a unified interface. This means that instead of tailoring their tool to the unique requirements of every platform, they can interface with the shim, which then manages the intricacies of each specific platform.

If a tool provider offers multiple tools, typically, they may use the same internal shim to handle the LTI 1.3 connections for all of their tools.

In this pattern, the LTI 1.3 connection provides end-to-end integrity between two known entities—the tool and platform.

2. Internal Shims: Platform-hosted

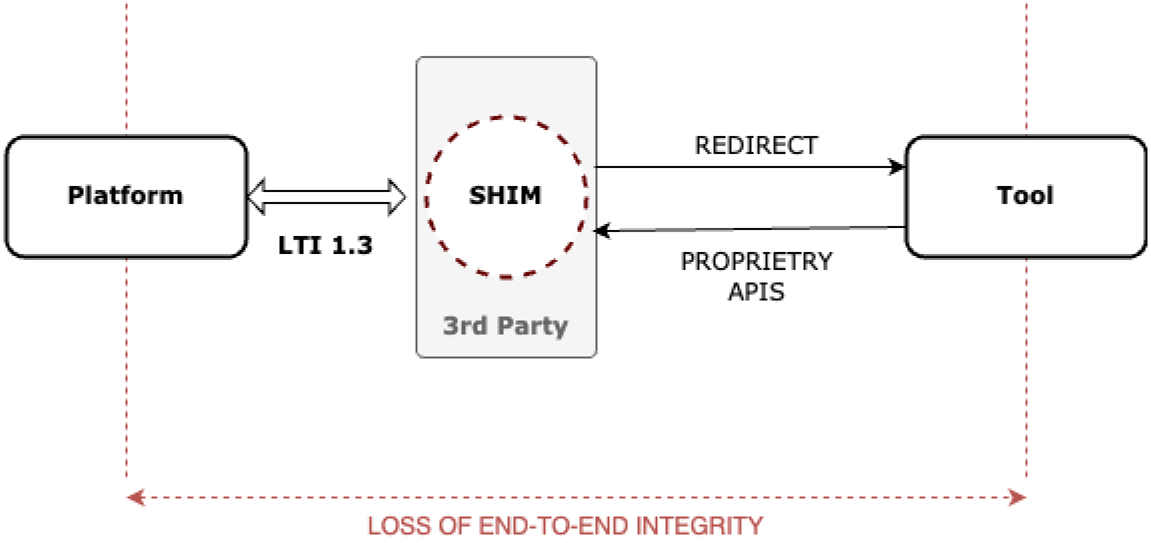


Similarly, for platform providers, shims can serve as LTI 1.3 gateways, enabling them to easily connect with a myriad of LTI 1.3 tools without necessitating individualized integrations for each tool.

Some providers separate the core platform functionality and keep the specific LTI 1.3 functionality within a dedicated shim gateway. This pattern allows a clean separation of concerns between the core platform and the specific LTI 1.3 data model. It also makes it trivial to add support for future versions of LTI by adding additional shim components.

This pattern also provides LTI 1.3 end-to-end integrity between two known parties—the tool and platform.

3. Third-Party Shims



Recently, a newer model has surfaced with some notable implications: third-party shims. A handful of independent platforms have introduced 'shim as a service' offerings, linking LTI 1.3 to their unique proprietary APIs.

These intermediaries present themselves as simplified routes to market for tools, but they also pose a risk to the inherent integrity of the LTI 1.3 connection. By channeling all LTI 1.3 data through these platforms, they inadvertently allow tool providers to bypass the safeguards that institutions have established for the secure management and exchange of student data with vendors and external parties.

Risks introduced by Third Party Shims

False Security Assurance:

This topology may give educational establishments a deceptive sense of security regarding the tool's safety. Even if the shim provider secures its services, the tool could adopt minimal or no security measures, presenting a hidden vulnerability. This misconception could lead institutions to trust an inadequately protected tool mistakenly or lose trust in LTI when a security incident occurs.

Data Privacy Exposure:

Intercepting LTI launches means the shim provider can access potentially sensitive data between the learning platform and the tool. This can include information about students, instructors, courses, or institutional data. Unauthorized access or breaches at the shim level can expose this data.

Additional Point of Failure:

Introducing a shim service creates an additional potential point of failure. If the shim service goes down or experiences issues during critical assessments, it could prevent the learning platform and educational tool from interacting, even if both are fully operational.

Man-in-the-Middle Attacks:

Introducing an intermediary service increases the risk of man-in-the-middle attacks where an attacker intercepts or alters the communication between the learning platform and the tool.

Increased Attack Surface:

The more services and interfaces you introduce into a system, the larger the attack surface. 3rd-Party Shim services, especially if not properly secured, could become a cyberattack target.

Dependency on Third-Party Security Practices:

Institutions and tool providers will depend on the security practices and policies of the shim provider. If the third party fails to maintain robust cybersecurity standards, it poses a risk to everyone in the chain. Shim services may operate within varied, or even absent, geographical and institutional compliance frameworks, presenting potential risks to institutions bound by stricter regulatory standards.

Token and Key Management:

LTI 1.3 uses JWTs (JSON Web Tokens) and other cryptographic methods for security. The shim service must manage, store, and potentially renew tokens and cryptographic keys securely. Mismanagement can lead to unauthorized access.

Lack of Transparency and Auditing:

If the shim service isn't transparent about its operations, it becomes difficult for institutions and tool providers to audit interactions, diagnose issues, or verify that data is handled correctly.

Integration Complexity:

While the main goal of the shim is to simplify integrations for tool providers by offering a proprietary API, it adds another layer of complexity for troubleshooting, updates, and maintenance. This can lead to unforeseen security vulnerabilities if not carefully managed.

Latency Concerns:

Another layer in the communication chain can introduce latency, leading to slower response times. While this is more of a performance concern, in certain cases, excessive latency can introduce or amplify security risks, especially if it causes timeouts or other unexpected behaviors.

Dependency on Proprietary Systems:

For tool providers, building on the proprietary APIs from the shim provider creates a concerning dependency. If the shim provider changes or becomes obsolete, the tool might face significant disruptions or require extensive rework. Relying on open standards, in contrast, ensures broader compatibility and future adaptability.

Service Reliability and Dependency:

If the shim provider faces an outage or failure, it poses a substantial operational risk to institutions. In the worst-case scenario, institutions could lose immediate access to vital tools. Even in a best-case recovery, tool providers would need considerable time to revert to direct LTI 1.3 integrations.

Additionally, institutions would face the daunting task of updating or replacing every LTI launch link across their systems, resulting in further delays and potential disruptions in service.

Stifling Adoption of LTI Services:

Third-party shim services hinder the adoption of emerging LTI 1.3 services. With over 16 LTI services in the standardization pipeline, tool providers that rely on 3rd-party shims will be constrained, unable to utilize these advancements until they expose them as part of their service.

Impact on LTI Certification

There is no certification pathway for intermediary third-party shims because LTI 1.3, as a standard, is designed to provide critical technical assurances that secure the agreements to exchange data between known parties (platform, tool, and institution).

There is no certification pathway for tools that do not implement LTI 1.3 directly. If a tool uses a 3rd-party shim provider, it introduces risk to any data-sharing agreements or RFPs from institutions that require 1EdTech certifications to be in place for their vendors.

The certification process will allow tool vendors to use LTI libraries or shims internally within their tool as long as they do not break the end-to-end integrity of an LTI connection.

In 2024, the certification process will be strengthened to add additional checks to ensure the LTI 1.3 connection for a tool is direct to the tool and not via 3rd party providers. This way, institutions can continue to be assured that 1EdTech-certified products listed in the 1EdTech Trusted Apps Directory offer genuine end-to-end LTI 1.3 secured connections.

Summary

Shims present a versatile pattern that can be utilized by both learning tools and platforms, ensuring the integrity of an LTI 1.3 connection remains intact. It is important to ensure that the tool provider directly hosts the LTI 1.3 connection.

While third-party shim services may offer tool providers a simplified integration route, they also open a range of security concerns for institutions, learning platforms, and tool providers. These concerns necessitate rigorous evaluation and mitigation.

LTI 1.3 aligns with the strict security and privacy mandates of institutions. Rooted in universally acclaimed best practices, the standard offers strong security assurances, especially concerning student data handling. For development teams acquainted with the foundational security principles and protocols, LTI 1.3 is simple to adopt. This evolving landscape reveals varying proficiencies: while some tool providers can adeptly implement LTI 1.3, others may be tempted to lean towards third-party shim providers. Authentic security and efficiency are anchored not in circumventions but in an in-depth grasp of these fundamental protocols. 1Edtech stands ready to guide institutions in selecting robust tools and to assist member platforms and tool providers in direct LTI 1.3 implementation.

About 1EdTech

1EdTech is a member-based non-profit community partnership of leading education providers at all levels, government organizations, and edtech suppliers who collaborate to accelerate an open, trusted, and innovative digital learning ecosystem. We power learner potential by creating the foundation for a learner-centered and future-ready ecosystem where products work together to improve teaching and learning for all.

1EdTech hosts the annual Learning Impact Conference, Digital Credentials Summit, and other engagement opportunities to advance the leadership and ideas that shape the future of learning. The 1EdTech Foundation, an affiliated public charity, puts philanthropic funds to work in support of 1EdTech's vision. Visit our website at 1edtech.org.