The Use of LTI® Shims for Tool Integrations

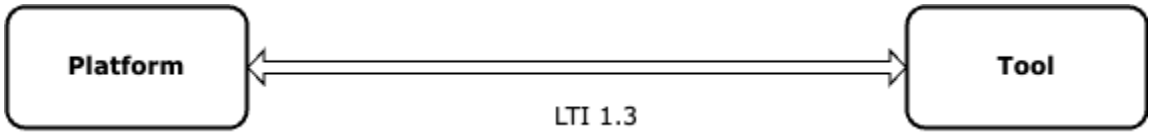
Executive Summary

The bond between a learning platform and an educational tool is not merely technical in the educational technology landscape. It signifies an alliance between two vendors (platform and tool) and a learning institution, merging commercial interests with safeguarding 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.

One emerging concept in this ecosystem is the LTI "shim." This document delves into the role and nuances of the shim pattern within the LTI framework. While examining instances where its deployment is beneficial, it also highlights situations where the shim could introduce risks, potentially undermining the standards that facilitate the seamless integration between learning platforms and educational tools.

Understanding LTI 1.3

1EdTech's Learning Tools Interoperability® (LTI) 1.3 standard 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 student's learning journey. The relationships are complex and often underpinned by certification, auditing with security/privacy rubrics, and contracts.

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

What is an LTI Shim?

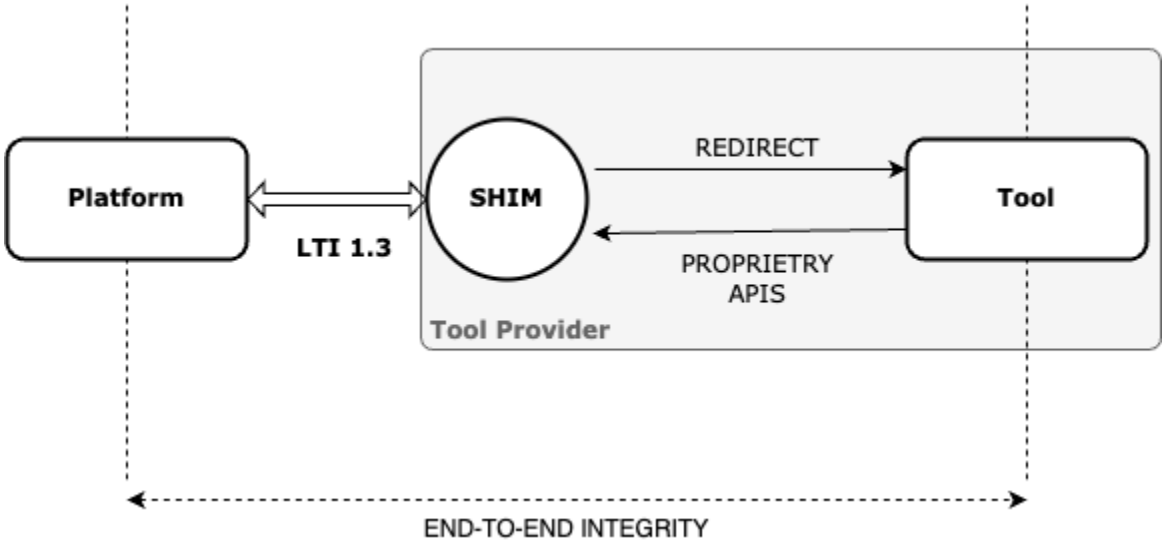
At its core, a shim is an intermediary piece of software that bridges the connection between two systems. Instead of modifying original systems to ensure compatibility with LTI 1.3, a shim can act as a bridge, ensuring that systems can interface with LTI 1.3 without altering their intrinsic functionalities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

Why the Rise of Shims?

The appeal of shims is primarily rooted in simplification. Many mainstream tool providers build and maintain their own LTI 1.3 shims within their own infrastructure for their tools to leverage. This well-established pattern delivers LTI 1.3 integration without compromising the assurance that LTI 1.3 can offer security and privacy. Shims can be grouped into three different patterns:

1. Internal: Tool-hosted
2. Internal: Platform-hosted
3. Third-party

1. Internal Shims: Tool-hosted

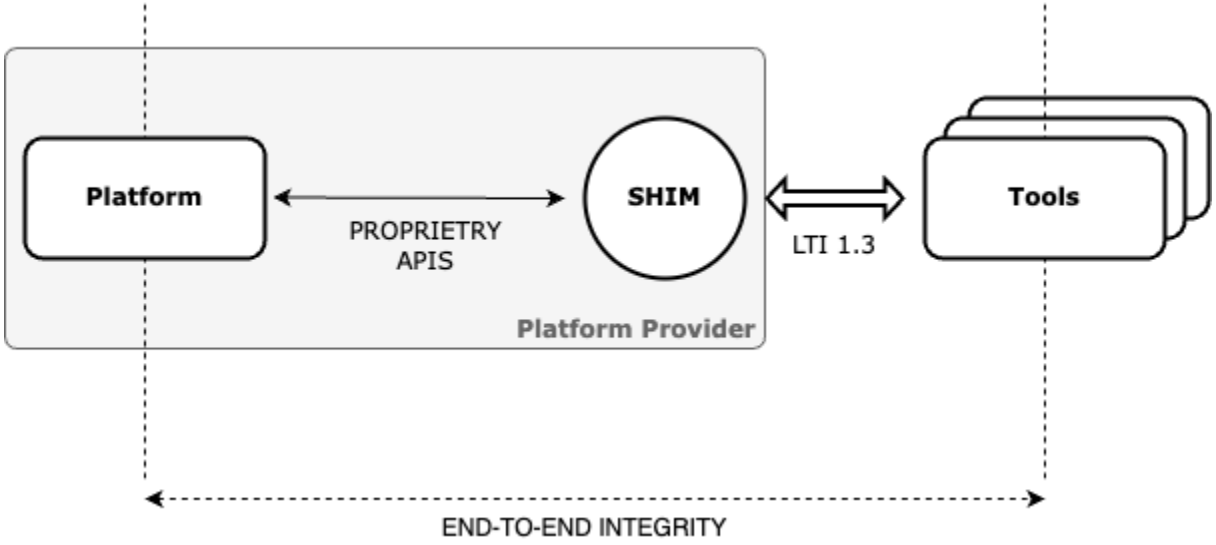


For tool providers, shims facilitate integration with multiple learning platforms, offering a unified interface. This means that instead of tailoring their tool to the unique requirements of every platform, they can interface with the shim, which then manages the intricacies of each specific platform.

If a tool provider offers multiple tools, they typically use the same internal shim to handle 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

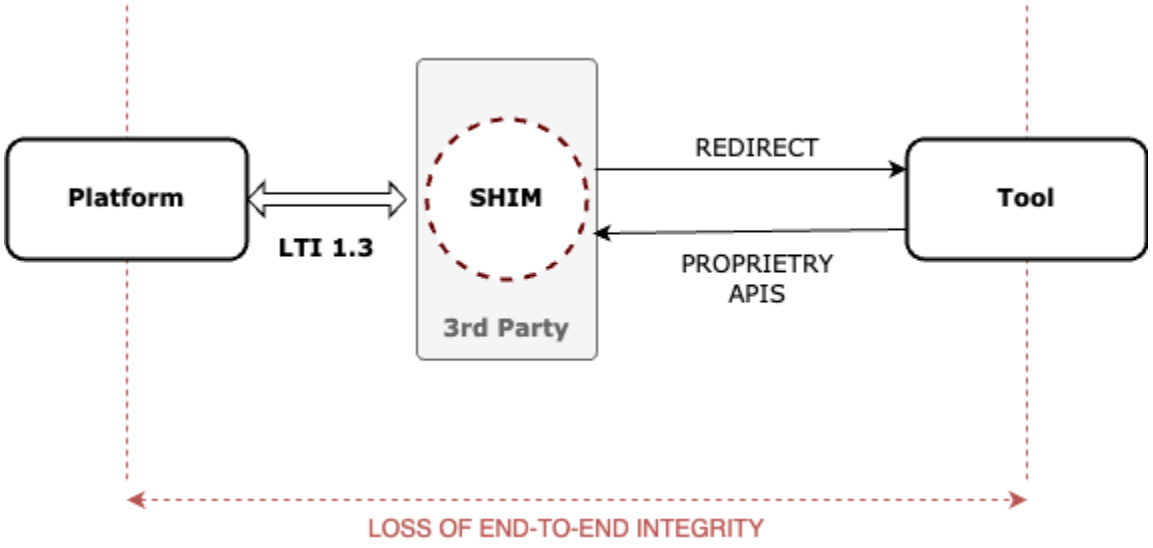


Similarly, for platform providers, shims can serve as LTI 1.3 gateways, enabling them to connect easily with a myriad of LTI 1.3 tools without requiring individualized integrations for each tool.

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 mistakenly trust an inadequately protected tool or lose trust in LTI when a security incident occurs.

Data Exposure and Privacy:

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.

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. Third-party Shim services could become a cyberattack target, especially if they are not properly secured.

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.

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, which would result in further delays and potential service disruptions.

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.

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 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 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 LTI 1.3 implementation.