Fun@Learn

学習における安全、安心を実現する

IMS Security Framework

2020年　6月 30日

常盤　祐司

tokiwa@fun-at-learn.jp

ブラウザでサービスを利用するときのセキュリティ

- TLS 1.2/1.3

- ユーザID
- パスワード

\+ SMS (2段階認証)

エコシステムの時代

LTI Platform

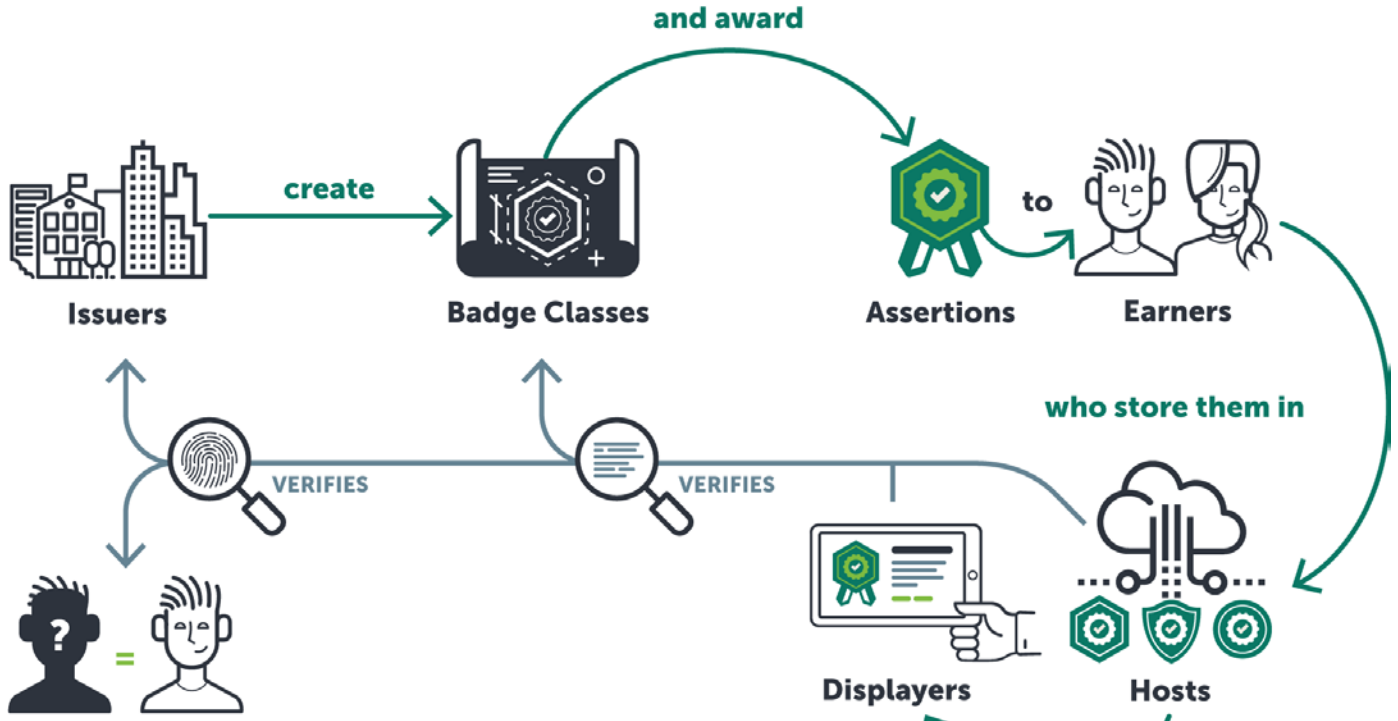
Sakai

moodle

turnitin

CENGAGE

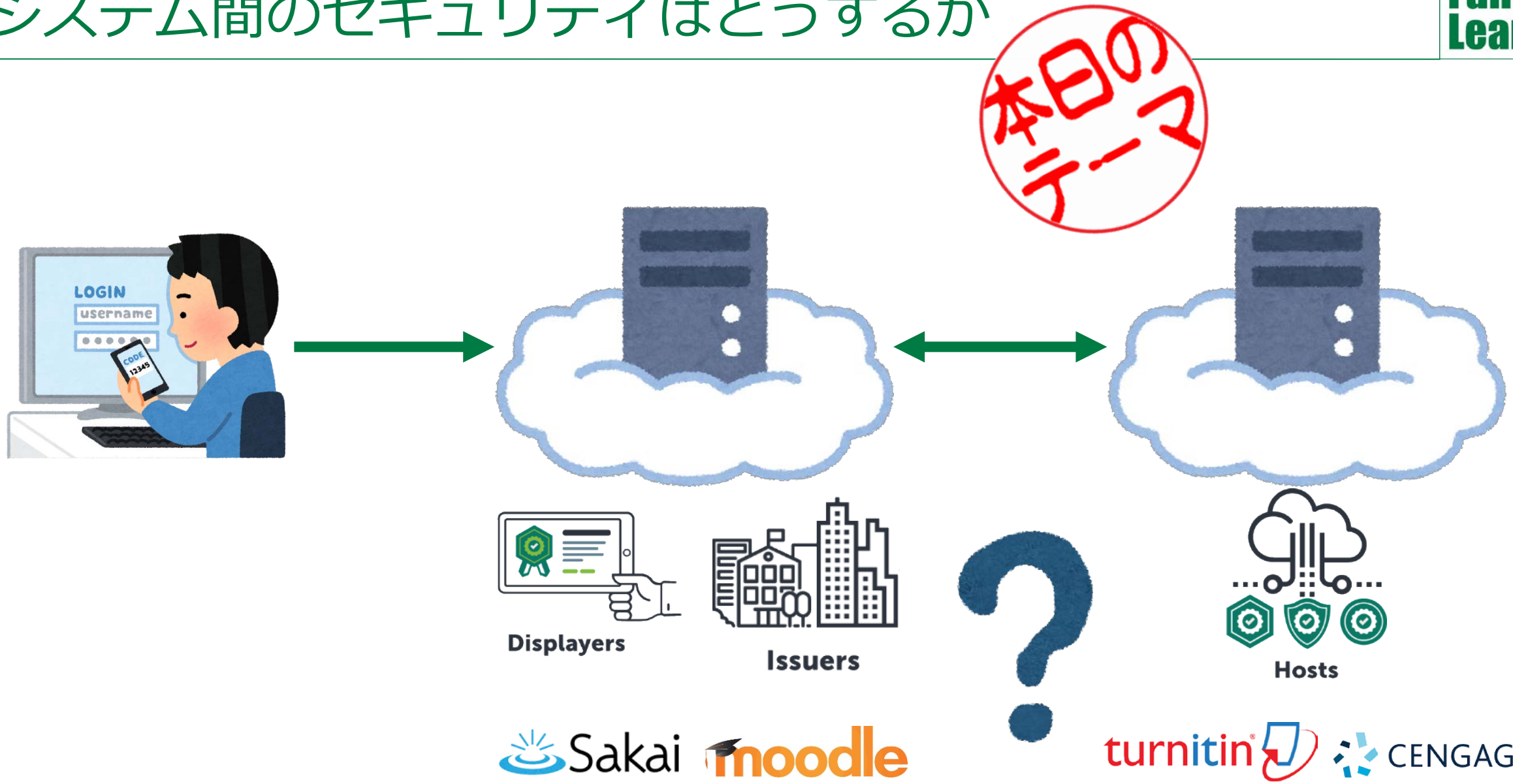
LTI Tool



Open Badges Context

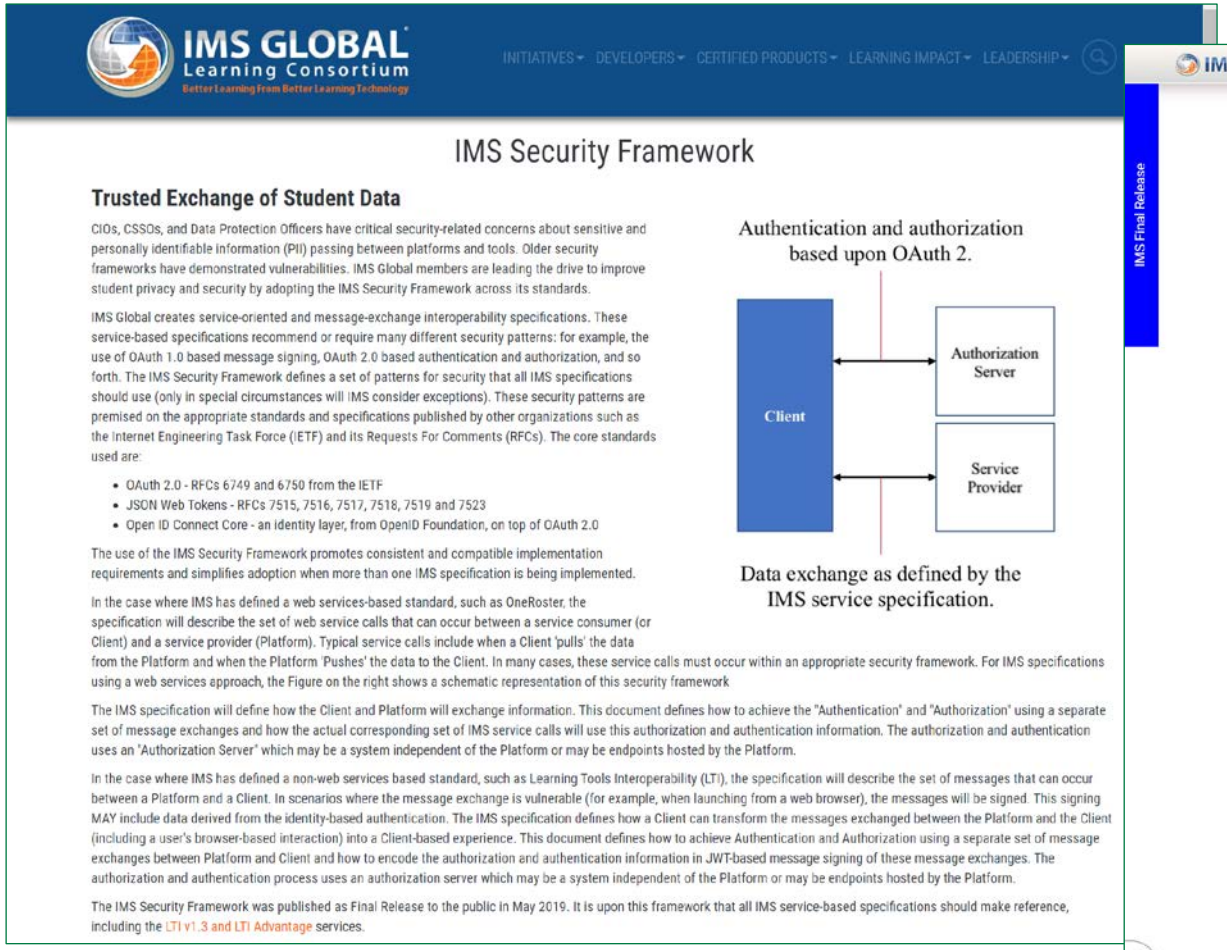
イメージは各社の商標です。

システム間のセキュリティはどうするか



イメージは各社の商標です。

IMS Security Framework



IMS GLOBAL Learning Consortium
Better Learning From Better Learning Technology

INITIATIVES DEVELOPERS CERTIFIED PRODUCTS LEARNING IMPACT LEADERSHIP

IMS Security Framework

Trusted Exchange of Student Data

CIOs, 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
- Open ID 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.

Authentication and authorization based upon OAuth 2.

Data exchange as defined by the IMS service specification.

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

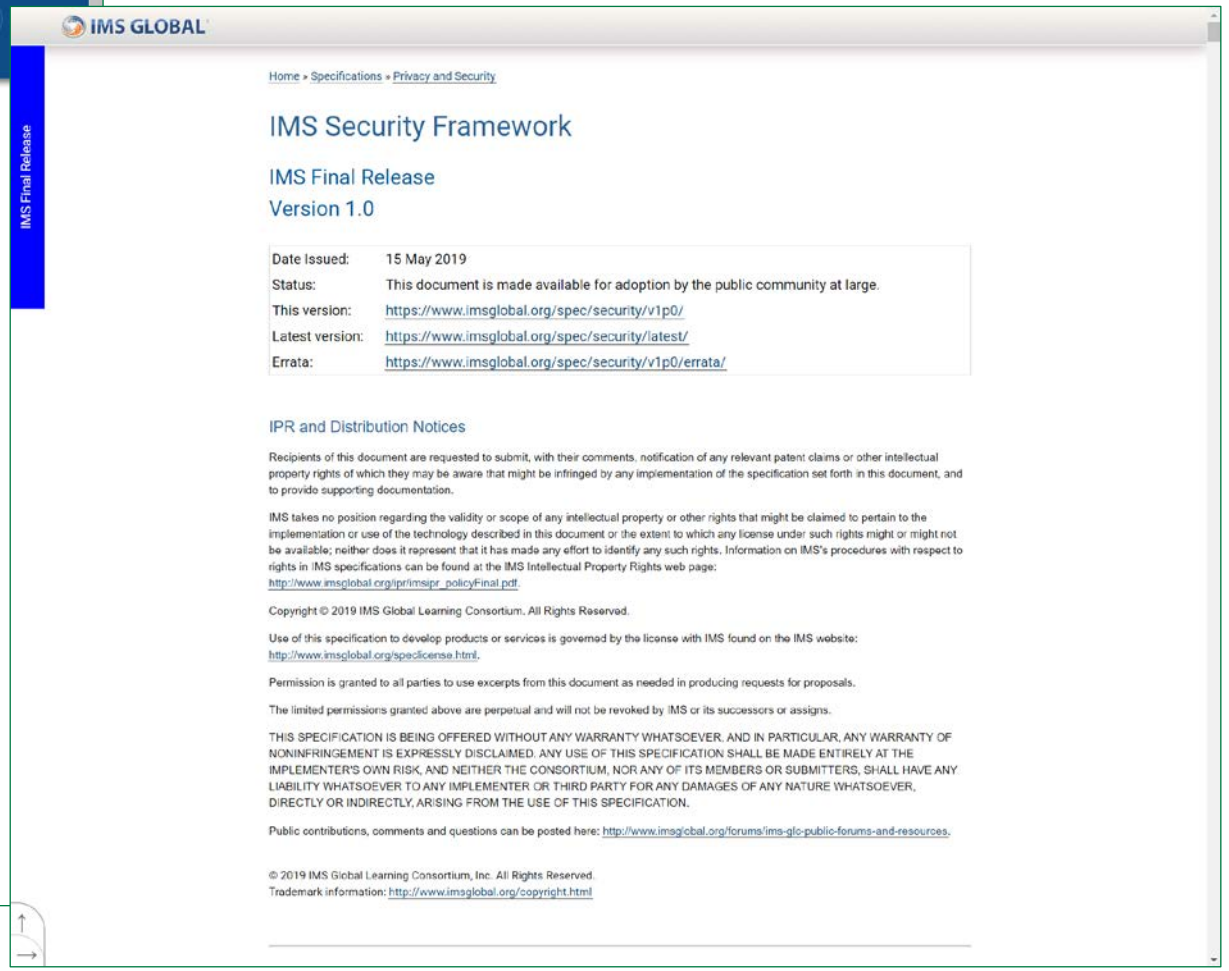
The IMS specification will define how the Client and Platform will exchange information. This document defines how to achieve the "Authentication" and "Authorization" using a separate set of message exchanges and how the actual corresponding set of IMS service calls will use this authorization and authentication 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.

概要

https://www.imsglobal.org/ims-security-framework



IMS GLOBAL

IMS Final Release

Home » Specifications » Privacy and Security

IMS Security Framework

IMS Final Release
Version 1.0

Date Issued:	15 May 2019
Status:	This document is made available for adoption by the public community at large.
This version:	https://www.imsglobal.org/spec/security/v1p0/
Latest version:	https://www.imsglobal.org/spec/security/latest/
Errata:	https://www.imsglobal.org/spec/security/v1p0/errata/

IPR and Distribution Notices

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

IMS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on IMS's procedures with respect to rights in IMS specifications can be found at the IMS Intellectual Property Rights web page: http://www.imsglobal.org/ipr/imsipr_policyFinal.pdf.

Copyright © 2019 IMS Global Learning Consortium. All Rights Reserved.

Use of this specification to develop products or services is governed by the license with IMS found on the IMS website: http://www.imsglobal.org/speclicense.html.

Permission is granted to all parties to use excerpts from this document as needed in producing requests for proposals.

The limited permissions granted above are perpetual and will not be revoked by IMS or its successors or assigns.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE CONSORTIUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Public contributions, comments and questions can be posted here: http://www.imsglobal.org/forums/ims-glo-public-forums-and-resources.

© 2019 IMS Global Learning Consortium, Inc. All Rights Reserved.
Trademark information: http://www.imsglobal.org/copyright.html

仕様

OAuth 2.0 と非対称鍵暗号によるセキュリティ

- TLS 1.2/1.3

- トークン (アクセス/ID)
- JSON
- 非対称鍵暗号(公開鍵暗号)

OAuth 2.0 事例

Fun@Learn

■ OAuth 2.0

- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant
- Client Credentials Grant
- Refresh an Access Token

■ OpenID Connect

IMSの選択

■ OAuth 2.0

- Authorization Code Grant
- Implicit Grant
- Resource Owner Password Credentials Grant
- Client Credentials Grant
- Refresh an Access Token

■ OpenID Connect

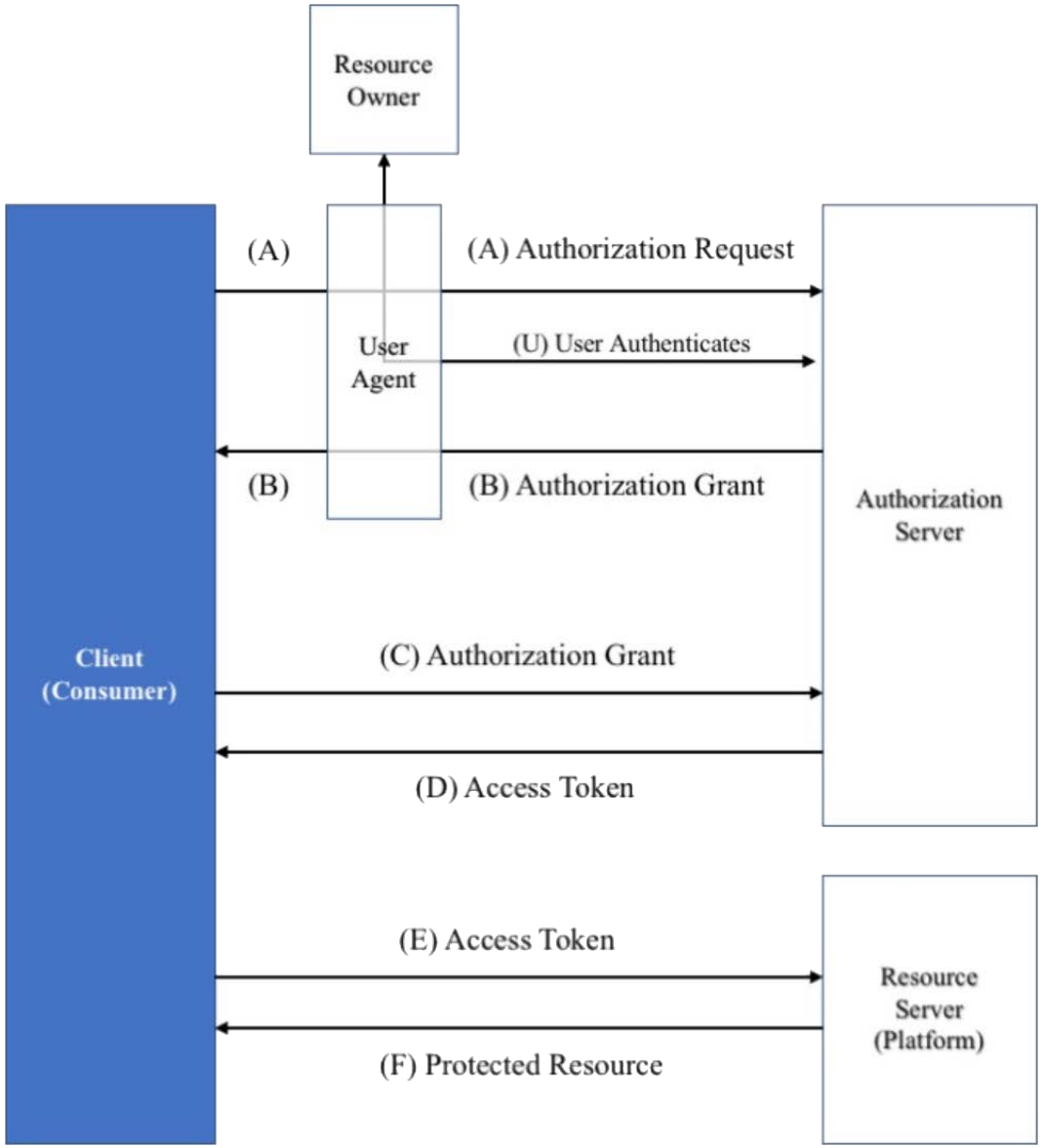
IMS Security Frameworkのパターンと適用

接続方式	利用個所	IMS標準	ユースケース
OAuth 2.0 Client-Credentials Grant	ブラウザを経由しない サーバ間の接続	One Roster v1.1	LMSと教務システム間 でのデータ転送
OAuth 2.0 Authorization Code Grant	特定のリソースをサー バから取得する接続	Open Badges v2.1	Issuer, Displayer, Host 間 でのAssertion移動
OpenID Connect Implicit Flow + Initiating Login from a Third Party	ユーザがブラウザで 外部ツールにアクセス する接続	LTI v1.3	LMSログインユーザに よる外部ツールの起動

OAuth 2.0 authorization code grant 事例

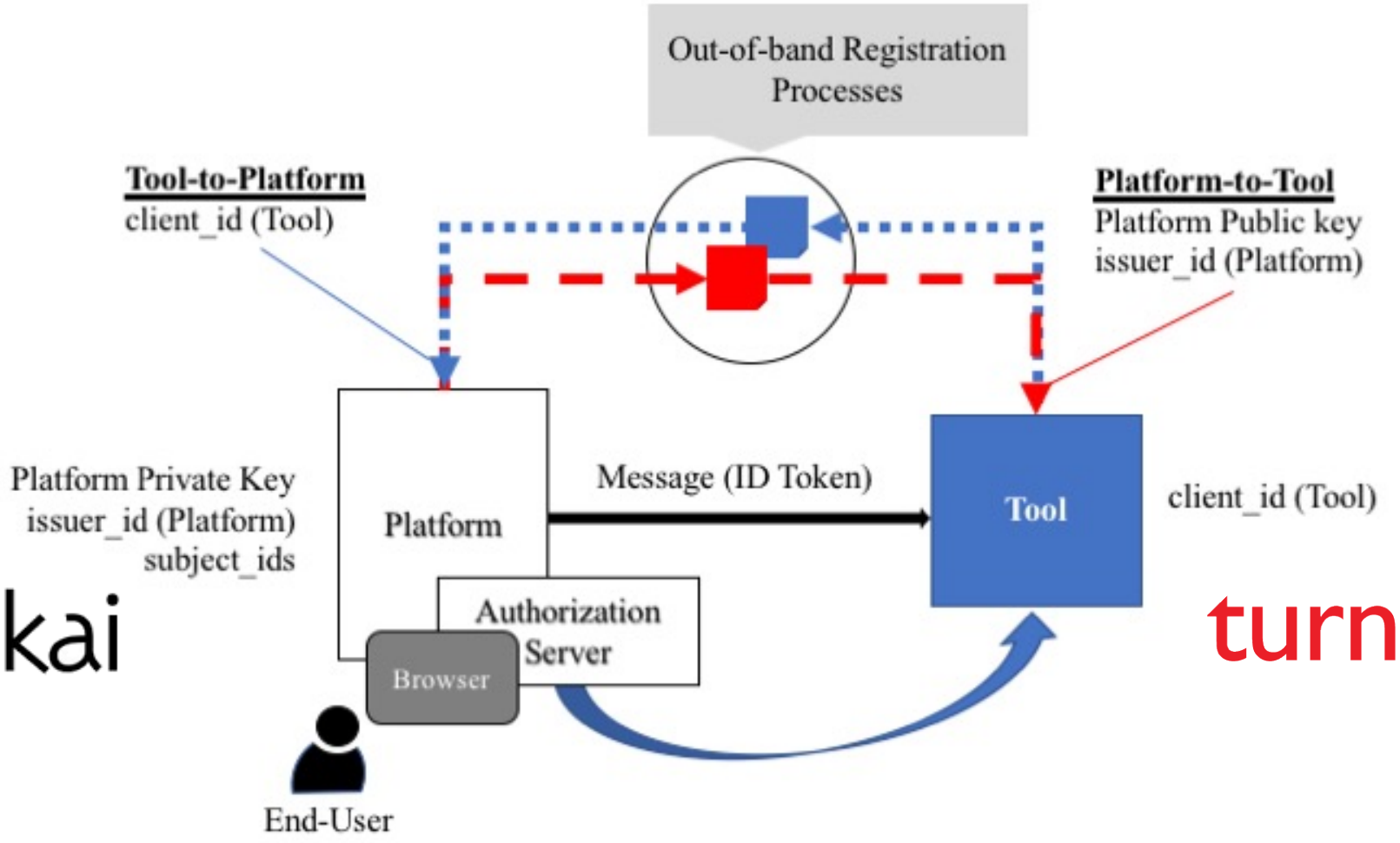
Displayers

Issuers



Hosts

OpenID Connect 事例



Sakai

turnitin

イメージは各社の商標です。

IMS Security Framework により
安全、安心な学習を提供する
エコシステムを構築できます

Fun@Learn

fostering future IT engineers with fun learning