LTI, SAML, and Federated ID - Oh My!

Charles Severance, Ph.D.
Stephen P Vickers
IMS Global Learning Consortium

http://www.imsglobal.org/

Problem Statement

- We need a way to align IMS Learning Tools Interoperability and SAML (or other web-based SSO authentication system).

Use Case

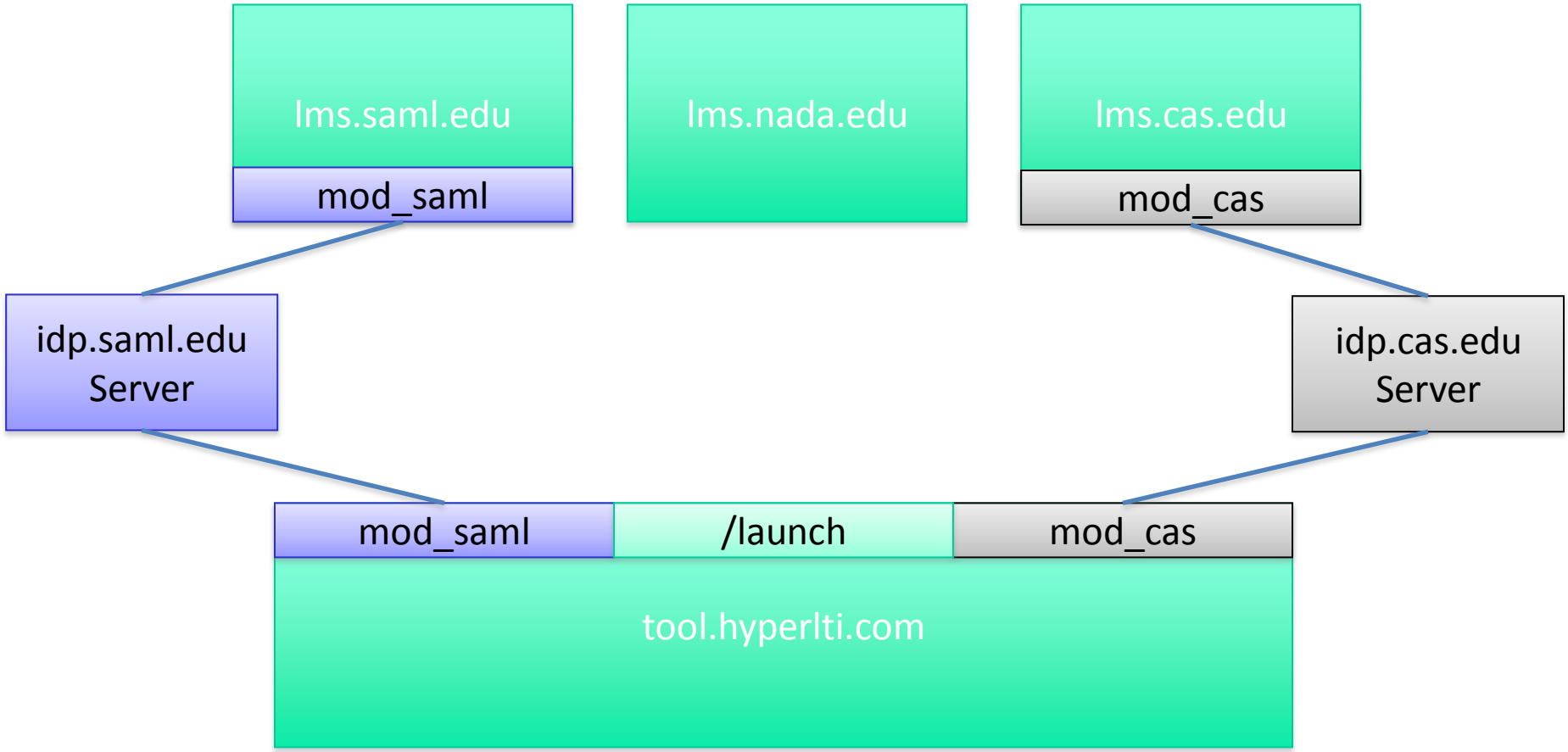
- When an LMS is protected using an SSO and launches an external tool using LTI, we wish to communicate the SSO identity to the external tool; this enables:
  - the external tool to connect the user_id value from LTI with an SSO identity;
  - the user to connect directly to the external tool and log in using the SSO for their LMS.

IMS GLOBAL™
Learning Consortium

Example Scenario

- We have three LMS's at three schools, one protected using SAML, one protected using CAS, and one that has no SSO.
- They all connect to an external tool that supports LTI, CAS and SAML, and has relationships with the appropriate SAML IDP and CAS Server.

Scenario Diagram



Essential Design Concept

- The LTI Launch is completely normal providing the standard within-LMS data like user_id, role, context_id, etc.
- If the LMS is protected using an SSO and the current user is logged in through the SSO, we add the type of SSO (SAML, CAS, etc) and the Identity Provider for the SSO.
- The LTI launch does **not** include the SSO identity as there is no way to do this reliably.

Design For External Tool: 1

- The external tool has an unprotected LTI launch URL to receive LTI requests (/launch)
- The external tool has SSO-protected URLs for all the Identity Providers and SSO types it has a relationship with (/cas_edu, /saml_edu)

IMS GLOBAL™ Learning Consortium

Design for External Tool: 2

- If the LTI launch URL receives parameters including an SSO type and Identity Provider that it is capable of handling, it sets up the LTI data (user, course, role, etc.) in the session and forwards to the appropriate SSO-protected URL on its own server.
- Since the user is already signed in via the SSO, they simply fall through with REMOTE_USER properly set.

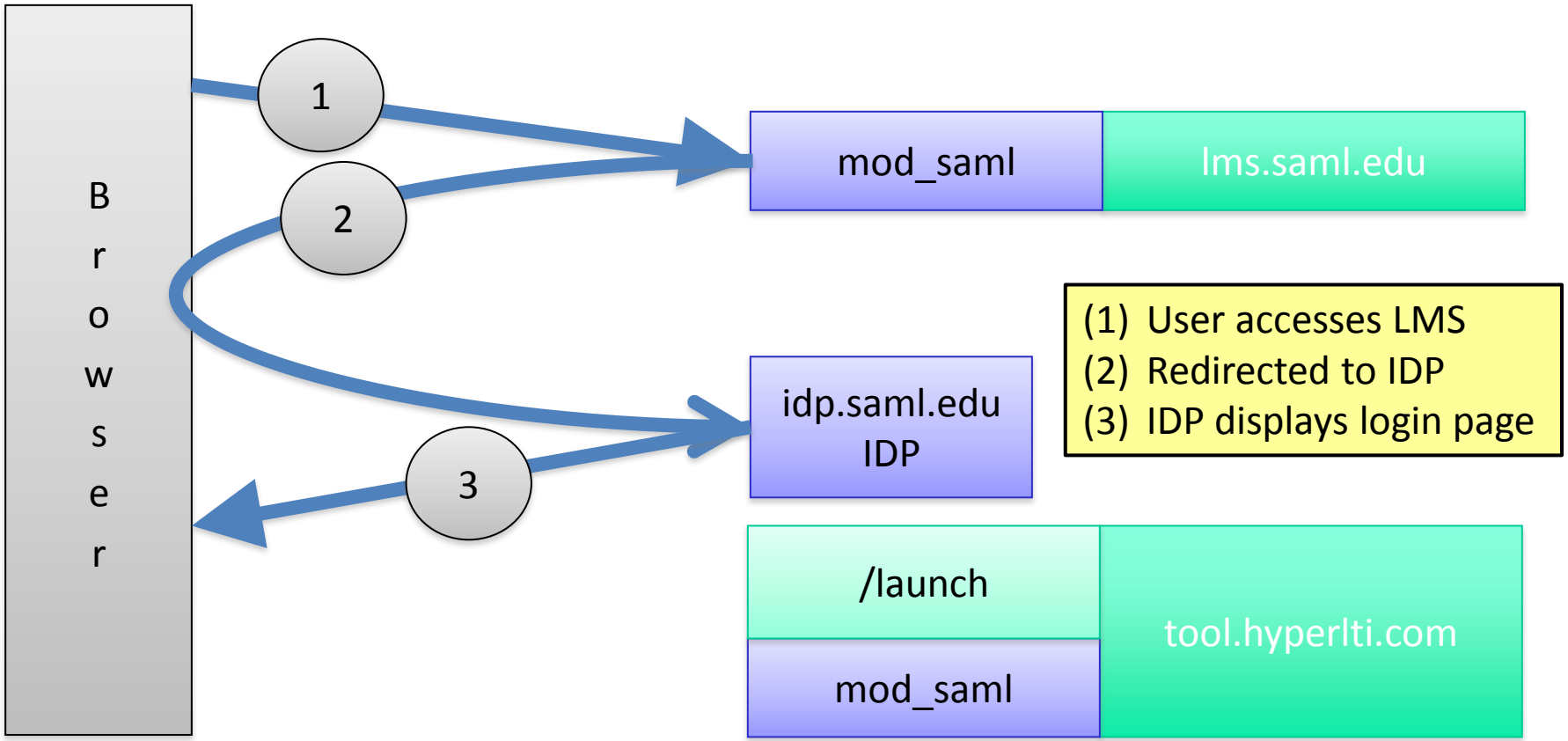
Design for External Tool: 3

- Under the SSO-protected URL, the code knows the LTI user's course and role, as well as the Identity Provider and enterprise identity.
- The tool can link all of these together within its data structures.

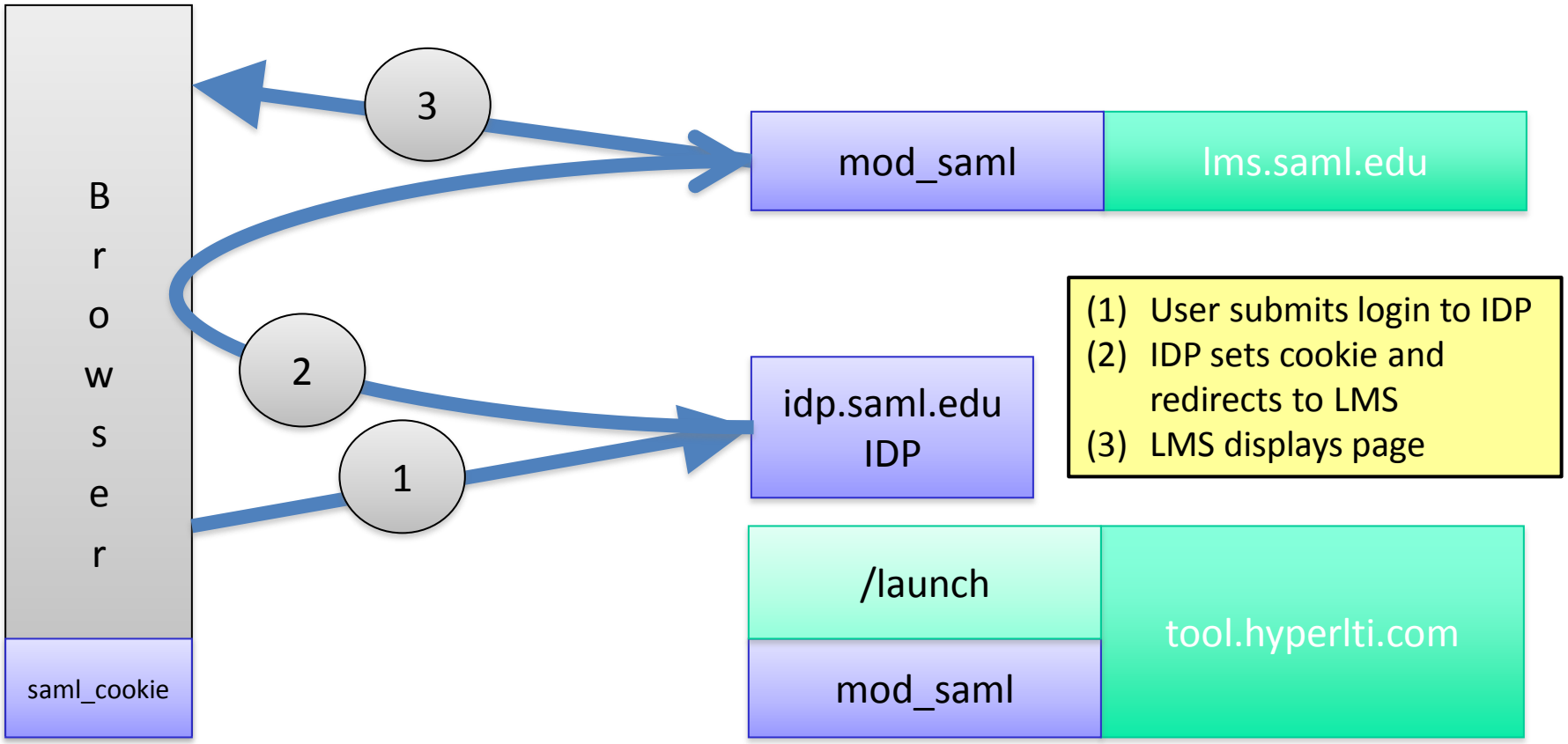
Design for External Tool: 4

- From that point forward, the tool can identify the user either:
  - via an LTI launch through user_id; or
  - through a direct login to an SSO-protected URL that provides REMOTE_USER

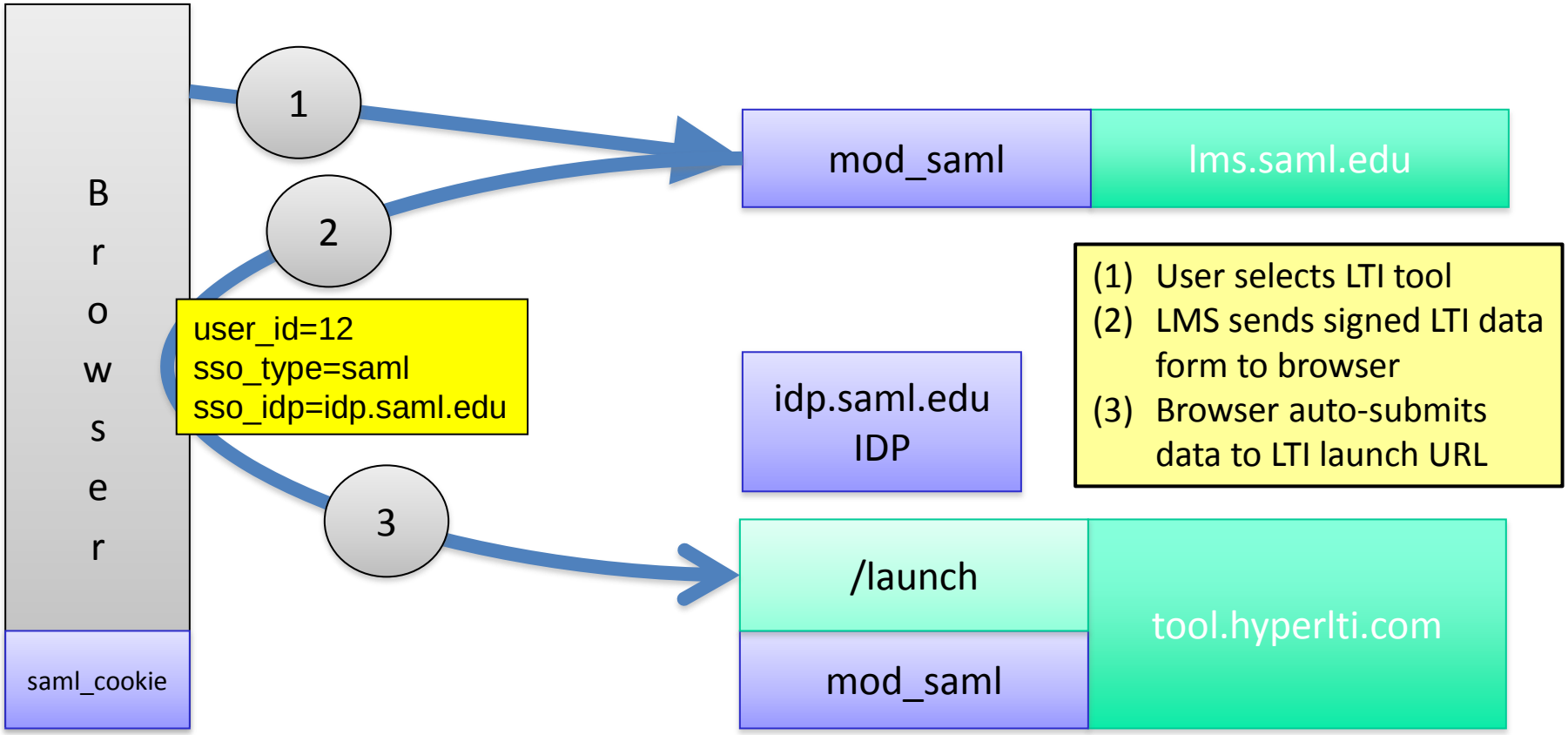
Log into LMS via SSO: 1



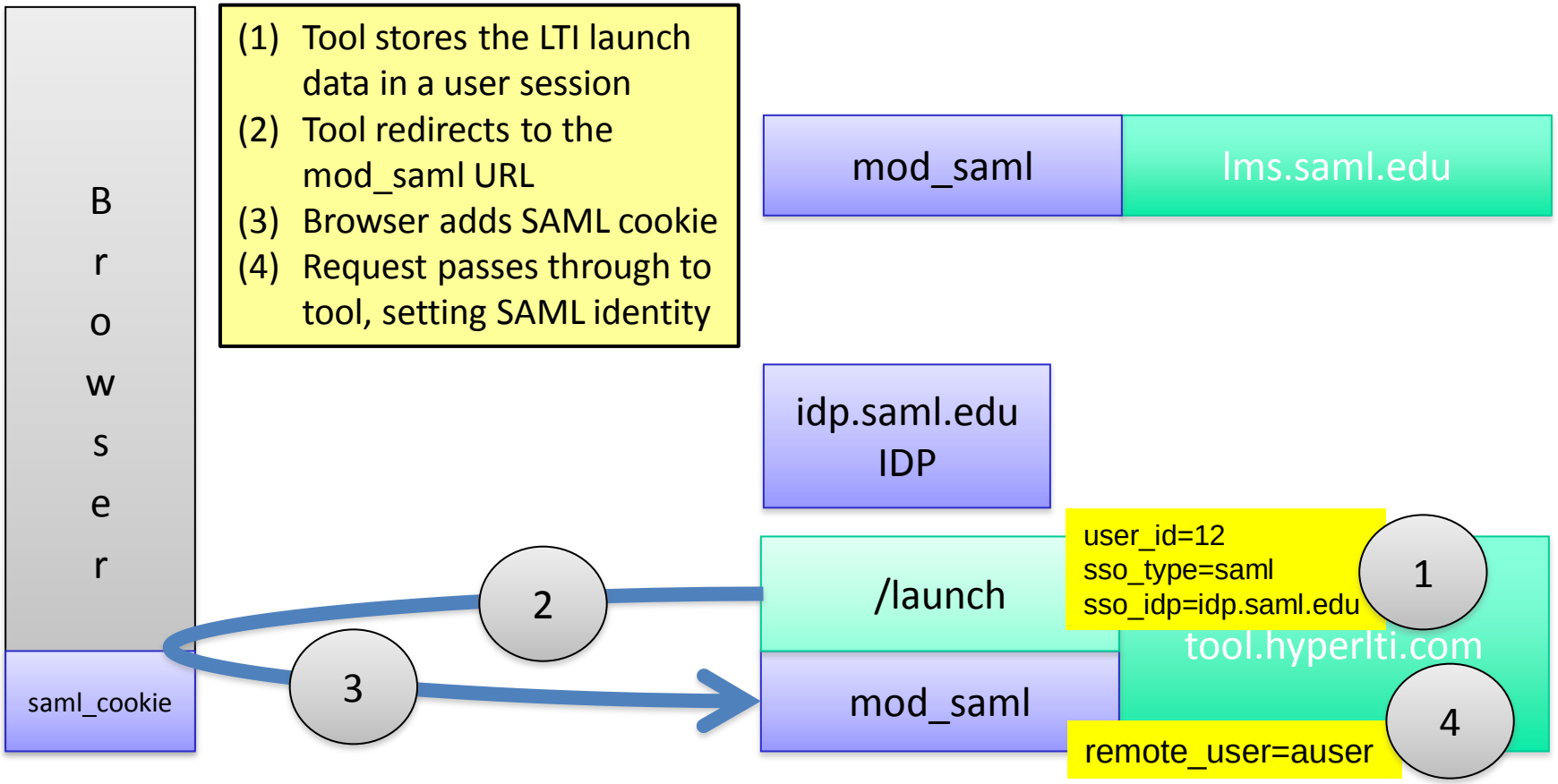
Log into LMS via SSO: 2



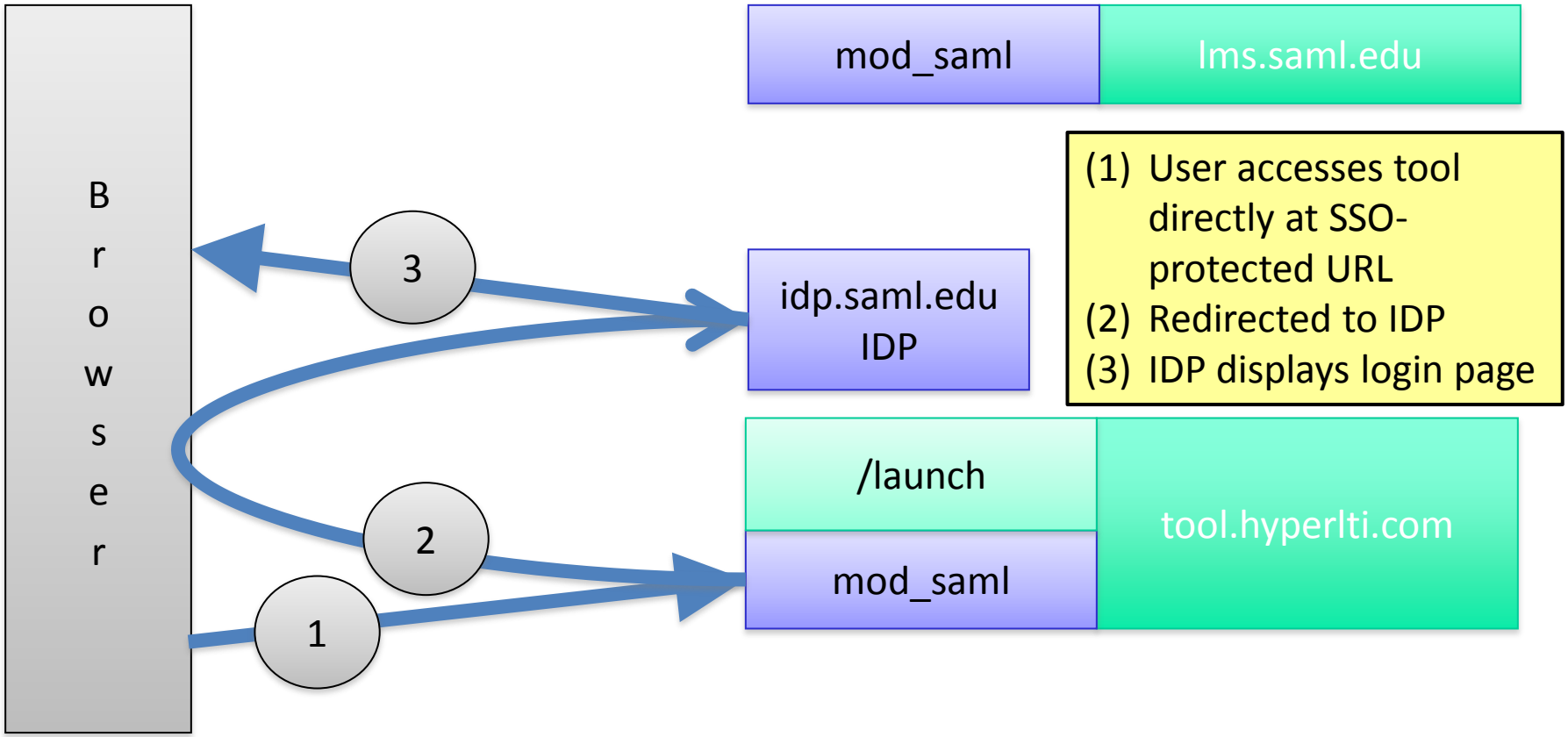
Launch external tool from LMS: 1



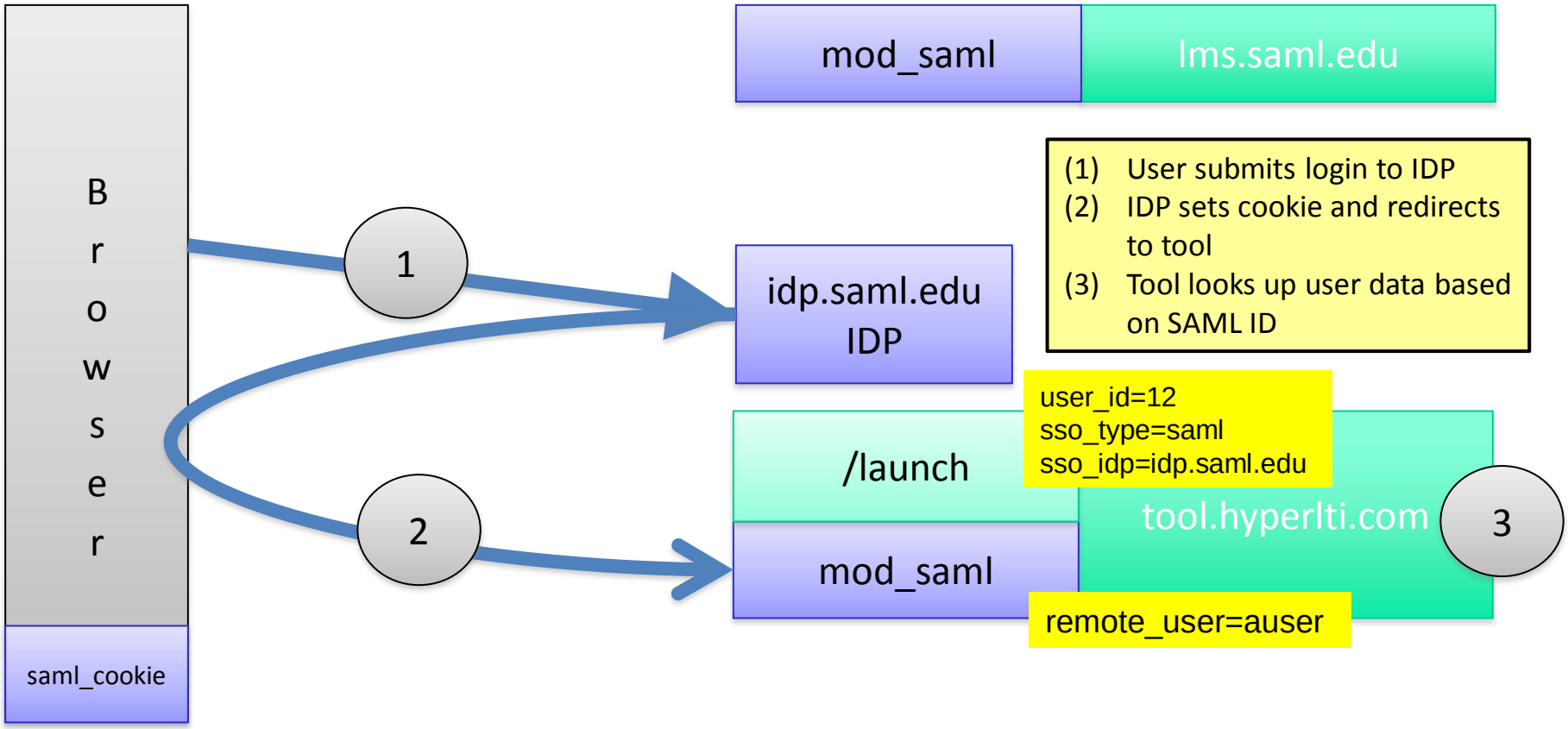
Launch external tool from LMS: 2



Log into External Tool via SSO: 1



Log into External Tool via SSO: 2



Further Comments

- The model extends to multiple types of SSO providers and multiple identity providers per SSO.
- It carefully avoids the LMS forwarding the SSO identity, but instead provides a mechanism for the tool to "add" the SSO identity to a session through a redirect.
- Tool providers may obtain additional attributes about a user from the IDP (e.g. telephone number).

Questions / Comments

- This is a draft proposal – comments welcome