Early Jan 2013 Mtg -- Topics and questions to frame discussion

The following have been raised implicitly or explicitly in the various discussions this year (note some of these items overlap):

1. What scenarios do we think should apply?
    a. User goes to tool via LMS
    b. User goes to tool via portal (i.e., not in a class context)
    c. User goes directly to tool (unmediated)
    d. other?
2. n-tier delegation: who is trusting whom? Who are or should be the actors?
    a. to assert authenticated user
    b. to assert attributes
3. SSO and session (may or may not relate to the use of iframe). What is the bearing on user experience?
4. How do our questions about the LTI TP relate to the generic problem of launching a widget?
5. What are the principles/constraints that inform our proposed solutions?
    a. E.g., Do not require the back-end service to trust the LMS/1st tier's assertions about a user session

---
Here are some thoughts I came away with after our Friday IAM for LTI call. Please correct/supplement/contradict as appropriate. --Keith

---
Terms from SAML: Identity Provider (IdP); Relying Party or Service Provider (RP/SP)
Terms from LTI: Tool Consumer (TC); Tool Provider (TP)

There are two basic models:
1) LMS/TC as Identity Provider(IdP): Fits well when tool provider (TP) services are widget-like things running in some sense in the context of the LMS/TC
2) LMS/TC as just another Relying Party (RP) from security perspective: Fits better when the tool provider (TP) services are more free standing or when one can imagine a learner/instructor going directly to the TP service NOT mediated by an LMS/TC

In model 1), the LMS by definition incorporates an SSO solution and the advice is rely on an existing SSO protocol, whether SAML, OpenIDConnect or whatever. In any case, don't create yet another SSO solution--security is a hard problem.

In model 2), a newer component--Attribute Providers or Attribute Authorities might help solve some of the challenges of TPs getting access to needed user information.

Here are some further reflections:
There seemed to be general agreement with the assertion that LTI fits the definition of SSO where the TC plays the role of IdP.
Scott C noted that LTI can pass both user context and application context. There was some discussion to the effect that an application requiring both is unnecessarily constrained and constraining.
Scott C mentioned deep linking as a model for flexible support of various workflows.

All participants felt scenario 1a (from https://spaces.at.internet2.edu/x/qgEVAg) applies. Several are interested in scenario 1c. Yours truly is also interested in 1b (our portal does not suck all that much)

The group used the two examples to illustrate the range of TP types (relating to Keith's points 1 and 2 below). The first is the widget that launches in the browser. The second is CourseLoad, a cloud-based etext reader that allows annotations and provides faculty with usage data for analytics. Some less comfortable with LTI for the second case.

Many acknowledged that LTI is essential to support LMSs and allows for independent tools and a multi-LMS environment.