iTunesU Shib Technical Approach

Posted by RL Bob Morgan, Jul 23, 2007

Abstract: Apple iTunesU is becoming a popular service for online media management for HE. This document describes several desirable features regarding iTunesU identity and access management. It proposes a technical approach for authentication and attribute delivery from campus IdM systems to iTunesU that can take advantage of existing SAML/Shibboleth deployments and the InCommon Federation.

The Current Situation

Apple's iTunesU service works with Apple iTunes clients. The client and service communicate using XML/HTTP(s) but the client is not a generic web browser.

Access to some iTunesU content requires authentication. Scalable authentication requires taking advantage of existing campus accounts via federation. A user authenticates to a campus signon service, which passes a secure authentication token, via the iTunes client, to the iTunes service, which validates the token and initiates a secure session. In some cases it is also useful for the campus to provide user attributes indicating things like course membership, which can be used for access control at the iTunesU server.

Apple's "iTunes U Administrator's Guide", chapter 2, specifies the technical details of this signon. The campus implements a service protected by local campus web signon which generates a signed user authentication and attribute token according to Apple's spec. This token is provided to the user's web browser, which calls the user's iTunes client as a helper app to post the token and the resource URL to the iTunesU server.

Campuses that have implemented SAML/Shibboleth observe that the SAML web browser signon profile provides all the services needed by this communication (authentication token, user attributes, defined flow, etc) in a standard fashion, and that many campuses and vendor partners have existing deployments of these services. They also observe that the InCommon Federation provides a multi-party operational trust infrastructure that simplifies SAML trust management, with many existing HE and vendor participants.

Objectives

There are several possible objectives for InCommon campuses working with Apple on improvements to iTunesU in this area.

SAML/Shibboleth for SSO
The primary objective is for campuses that have existing SAML/Shibboleth infrastructures to be able to access iTunesU using federated authentication and attribute delivery using that infrastructure alone, without having to implement iTunesU-specific security services.

Standardized User Attribute Usage
The iTunesU spec defines both how to authenticate the user and how to send other user information, including course membership, primarily using a "credentials" element. This usage should be recast as recommendations for using SAML attributes, including potentially both eduPerson attributes and other (e.g. inetOrgPerson) attributes. In particular it is likely to be useful for Apple and the InCommon community agree on a SAML attribute representation for course membership. This would likely use http://middleware.internet2.edu/courseid/docs/internet2-mace-dir-courseid-educourse-ldap-200507.html, "LDAP representations of eduCourse attributes and an auxiliary object class" as a basis. It might accomodate local variations as well.

Federated Access Among iTunesU Instances
Currently each campus iTunes instance only supports protected access via user accounts from a single campus. A fully federated iTunesU would permit content to be restricted to users from many institutions, or even unaffiliated users via open identity providers. Some campus iTunesU scenarios would find this capability to be valuable.

Details: SAML/Shibboleth for SSO

It is proposed that Apple run a Service Provider (SP) compatible with the Shibboleth profile of the SAML web browser signon protocol, in conjunction with the iTunesU service. This SP would be a registered SP in the InCommon Federation. When a user wishes to access protected iTunesU content, they would be directed (perhaps via a campus-based navigation page) to the iTunesU SP. This SP would have distinct protected areas for each campus customer, to avoid the user having to go through IdP discovery (aka WAYF). The user would authenticate at their campus IdP in the usual fashion, returning to the SP with SAML authentication and attribute info. Further steps, including iTunes client invocation, are under the control of Apple. The SP might implement Apple's existing authentication/attribute spec, sending the browser info to invoke the iTunes client with authn/attribute info to be sent to the iTunesU server.