Identity decision points provide identity data for autho­rization rule evaluation and can utilize Security Assertion Markup Language (SAML) assertions or HTTP headers today and OAuth 2.0 in the future. For example, OAuth leverages a delegated trust model to realize the benefits of abstracting user identity data from user credentials and supports tokenization of authorization. It does require an OAuth-aware architecture of entitlements enforcement. Regardless of the technology used, these authorization decisions must happen quickly and support high volumes of traffic.

**User account management and provisioning**

Today’s apps, even those that are federated, need a local account for user identity management. The challenge is managing data about users, especially routine changes like password resets and account registrations. With cloud-enabling user management, every app performs user management differently and usually does it internal to the application; user management APIs are neither con­sistent nor standardized.

Ideally, developers will use the SAML equivalent for provisioning, the Service Provisioning Markup Language (SPML), but there are only a handful of real-world SPML implementations. Without federated provisioning APIs to enable automated synching of local accounts, SAML adoption will remain limited. There is also a lack of sup­port for integrating SAML attributes for personalization, session context, or just-in-time provisioning. The absence of universal user schemas for directories makes building general-purpose management tools difficult.