Managing user identities in a heterogeneous authentication environment

Asad Ali, Laurent Castillo & Karen Lu
Gemalto, Inc.
{ asad.ali , laurent.castillo , karen.lu }@gemalto.com

Online Identity Management deals with creation, organization, tracking, and eventual deletion of information related to individuals. It is complex because information may be scattered across different repositories that may not always be interconnected. In this paper we will explore solutions to reduce this complexity for online service providers (SP) by using an architecture that allows an Identity Provider (IdP) to consolidate user information from disparate sources and present a consistent and unique identity of the user. The focus will be on achieving this consolidation when users authenticate with different login credentials.

Online SPs require these login credentials before granting users access to their services and resources. Identity federation has alleviated some of the usability, deployment, and security issues associated with login credentials by separating the role of SP and IdP, and by allowing single signon. However, identity management is still complex when service providers, such as government services and banks, want to balance usability and risk management by allowing users to login with multiple authentication methods depending on the risk associated with the account accessed. Such adaptive authentication, where users can access critical resources only after authenticating with a stronger method, often uses identity credentials in multiple formats. Examples of these authentication methods include passwords, OTP and certificate based PKI. For each of these methods the user identity may come from a different repository, and has to be merged into a single view of the user.

Such a mapping of identities from different authentication methods has traditionally been done by the SP, but this runs contrary to the principles of identity federation where identities should be managed by IdP and not SP. We propose an architecture where the IdP manages the complexities of gathering user identities based on the login method, so that each SP is not forced to create an ad-hoc mapping to uniquely identify a user. The IdP should also allow a user to be acknowledged at a SP with different pseudo identities (i.e. different usernames) depending upon the selected authentication method. However, such an approach should be driven by user preference, and not mandated by the rigidness of an IdP architecture. We will explore various architectures and business cases that allow creation of such flexible frameworks.