The Story of XIDs

April 2011 Harvard University's Self-Service Guest ID Option: XID xid.harvard.edu

Since the late 90's, Harvard has offered campus authentication and authorization services for use by schools and departments. Many groups register their local applications with the University "PIN system" and leverage the web access management technology to enable a broad community of users to access University resources. Traditional University populations (faculty, students, staff, contractors, some unpaid affiliates, library borrowers, etc.) use their Harvard ID number and password to log in to over 400 applications. All employees and students use the PIN system to access library e-resources, course tools, Oracle HR and financial systems, and many other web-based services.

As early as 2001, campus administrators leading various business functions at the University expressed the need to extend their services to other communities of users. Some groups responded to this need by issuing Harvard ID numbers to some of the previously excluded non-employee and non-student populations. But there were many cases where the affiliation of the individual to the University was too loosely defined. Many groups pointed out that their members were not interested in divulging information such as date of birth required to get an HUID. Also, the groups managing these users were not interested in handling that information either. It was also true that often the user login was needed not so much for security (authentication) but to enable session management; a user account would enable that individual to pull up content from prior visits to the site.

In response to this growing business need, a secondary population of ID numbers, called Extended IDs (XID) was proposed. These XIDs would work with the PIN systems and the authorization LDAP instance and be supported by the central helpdesk that currently handled the PIN calls. This was a real selling point for system owners who were not interested in managing a local authentication system of logins and passwords, much less helpdesk calls. But the XID would be issued using a very different process than the Harvard ID number.

Self-service XIDs were envisioned as simple anonymous guest accounts available over the web to anyone in the world. With a name and a valid email an individual could request an XID, set-up a password, and establish a challenge-response question to be used for self-service password reset. To gain access to a system that was willing to accept an XID involved simply communicating the XID to the site administrator. For any system already accepting HUIDs and PINs, a simple registration change with the PIN system turned on authentication for XIDs as well. The PIN system has always provided only authentication, so system administrators were accustomed to managing lists of HUIDs or looking up HUID holders using the LDAP service to authorization access. XIDs were easily incorporated into the existing access lists and could be queried in LDAP (for a handful of attributes). XIDs were an immediate hit with users and system owners. It has proven to be a very handy tool in the toolbox for those managing access to campus resources.

What made the XID system a success?

- Open to anyone in the world
- Quick self-service process
- Helpdesk support
- Simple to integrate for an application already using the PIN system
- Alleviates system owner of any user management (other than the access list)
- Ability for XID manager to tailor the "welcome to XID" email that is sent to a group of new users

Important Considerations

- Hard at first for system owners to know whether they could trust XIDs
- Businesses who accept XIDs need to understand how it works, and make sure their processes work for anonymous users.
- The anonymous nature of an XID may not be an appropriate credential for certain University resources

Recap Key Features:

- User can create an XID in a couple minutes
- User can select their own user login (email is the suggested login)
- Account management page that allows the user to modify any and all data provided to the system.
- Integration with PIN system; validation of a user's XID authentication assertion (XID and password) using a service interface
- XID Manager function enables account administrators to create and modify accounts for a group of users.
- XID manager is able to:

o issue an account based simply on email address

o tag a set of accounts with a group identifier

- Only a user or that individual's XID manager is able to modify the accounts they created.
- The XID manger information is being used as a attribute of the account to do some coarse grained authorization queries using data in LDAP
- XIDs are unique for life and will never collide with the HUID value. Once generated, an XID will never be re-issued.
- Application owners are assured that application state, indexed by an XID, will never be compromised.
- An individual may have more than one XID as long as they are willing to supply a different email address
- System enforces a strong password and lockout mechanism at the LDAP level. (There is no requirement to force users to change their passwords.)
- XID accounts can be terminated.

What we might change about how XID works today:

- User interface is awkward
- For those using the managed XID model, there is a need to have more than one person be able to act as the manager of a set of IDs (e.g. issue password reset emails, or modify attributes such as end dating an account)

Future of XID

- In a world with OpenID, does Harvard still need XID?

o The needs met by the XID manager function are not met by OpenID alone.

Jane E. Hill (jane_hill@harvard.edu)

Directory Services Product Manager, Harvard University Information Technology