Attribute Release and Consent

For those following the course of Internet identity, the challenge in getting the "right" attributes released to applications is proving unexpectedly hard. A number of factors have hobbled the task, from inconsistent institutional policies to limited technology options and shifting regulations. If we are to achieve the security and privacy that federated identity can truly provide, we need to make progress on several fronts.

This is a critical issue. The lack of effective attribute release is frustrating the research communities that have been told that federated identity is the way to address their identity and access control needs. Poor release tools are limiting how we can manage our medical information. It is stifling a next-generation of accessibility tools that will give users with special needs adaptive mechanisms that work across devices and web sites. It is the impediment to extending federated identity to federated access control.

Many attribute release issues can be handled through a contract if one exists between the institution and the service provider. That contract can specify the attributes to be released, and how they might be managed once receive. The relationship between the user and the institution allows the institution to do this, often invisibly to the user.

Trust marks, such as the Research and Scholarship end-entity category are another approach. They can be used either at the institutional level or the individual layer. At the institutional level, they can convince a relevant institution to release the appropriate attributes for that mark, with or without user consent. At the individual level, they can allow users to select certain attributes for release to an application.

Consent is another arrow in the quiver. It can provide users with fine grain controls, and information that fuels effective use of those controls. It allows users to choose what to release, and the consequences in terms of both privacy and their own capabilities within the relying application. To minimize intrusiveness in the user experience, it can offer a variety of options for continuing release, and revocation of those choices if desired. It can also serve as a notification mechanism once appropriate attribute release. It will come at some cost, in infrastructure and in user awareness. Over the next year, Trust and Identity will be working in a coordinated fashion with leadership institutions to deploy an infrastructure, called Scalable Consent, to enable effective and informed end-user consent.

From the beginning, federated identity was really about sharing attributes more than identities. Until we can, we have unfinished business to do.