Scalable Consent: Intro and Benefits/Costs

As federated identity moves towards maturity, a cluster of issues around attribute release, privacy and consent has become central to realizing the capabilities of an attribute-rich infrastructure. A set of activities facilitated by Internet2 is beginning to develop technologies, deployment strategies, considerations of legal and international issues, and other materials. Taken together these are intended to help an institution create an infrastructure and end-user experience for offering effective consent services.

These consent capabilities are significant. Consent will be informed. It will be revocable. Either the institution or the user can manage the frequency with which consent is given. It is adaptive. It can be highly customized and skinned. It has accessibility considerations in mind. The information and metadata that supports consent – from UI dialogues to icons and trust marks – can be local or global.

There are a number of benefits to providing such capabilities.

It is a scalable and effective way to meet campus privacy requirements for end-user consent. A number of campuses have requirements for explicit user consent for the external release of common attributes. This infrastructure is intended to support those needs.

It is a mechanism to address internal needs for attribute release. Some universities have student-app marketplaces, where applications developed by students can interact with each other and with official information, such as class schedules. Other universities have departmental administrative applications with similar desires to access each other and official systems of record. In these cases, consent may be needed since the attributes are being shared with individuals and units not within the central IT organization.

It is a step to providing fine-grain scalable consent and attribute release. For example, giving a user the ability to manage which group associations to release allows services to provide access control and authorization in a scalable, yet privacy-preserving manner. Internet scale access control will greatly benefit the missions of R&E. Fine-grain attribute release is part of that capability.

It integrates well with remarkable new accessibility approaches being developed by initiatives such as Access4All and GPII.net. For the first time ever, we can provide accessibility, across devices and applications, while preserving privacy.

It is complementary to the user profile management efforts being worked at a number of institutions and can use those efforts to help implement revocation of consent and other features.

There are side benefits that come with the infrastructure, such as time stamps on when consent was given and non-repudiation, effective mechanisms to withdraw consent, etc. Ad hoc business processes can be replaced with automated log and audit mechanisms.

While the consent work fits in very closely with the emerging consensus around IdM architectures, it includes some additional components, as well as policy management around the services that those components enable.

There are new components being added to an IdM infrastructure, such as data storage for user attribute release preferences, capabilities to translate attribute names and values from arcane "geek" to human palatable forms, informed consent support, etc. The components are intended to have a common installation and a common enterprise management console, but are modular to permit organizations to sub-select individual components. They are all part of the TIER initiative and will be packaged and supported in those standard mechanisms.

There are new policies to be considered. Which of the technology options aligns best with institutional interests? Who determines when consent is needed, or parameters on the options that users are presented with when managing consent? Who sets the basic policies for the user interface? Who provides the information in informed consent dialogues? Who has access to the audit logs? How are international campuses addressed?

The capstone work in federated identity is now beginning. It is time to deliver on the attributes, use control and privacy capabilities of the infrastructure.