An Introduction to Scalable Consent for CIO’s

As federated identity moves towards maturity, a cluster of issues around attribute release, privacy and consent has become central to realizing the capabilities of a federated, 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 in support of consent. Taken together these are intended to help an institution create an infrastructure and end-user experience for offering effective services. This briefing is intended to inform interested parties of the work underway. More information can be found at https://spaces.internet2.edu/display/ScalableConsent

The consent capabilities being enabled are significant. Consent will be informed. It will be revocable. It will be fine-grain in its attribute release capabilities. Either the institution or the user can manage the frequency with which consent is given. It can be 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 as well. 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 access control. For example, giving a user the ability to manage which group associations they might want 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.
* It can be integrated into local self-serve user profile management.
* There are “freebies” that come with the infrastructure, such as non-repudiation via the time-stamps on consent and effective mechanisms to withdraw consent, etc.
* It will prove valuable for managing the impacts of the new EU GDPR (General Data Protection Regulation) on data protection.

While the consent work fits in very closely with the emerging consensus around IdM architectures, it adds some additional components, and 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 the arcane to human palatable, 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.

There are technology considerations that interact with policy decisions. An accompanying document on Consent Deployment Options discusses those.

There are new policies to be considered. 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?