

Background

In the electronic self-service environment where physical cues such as inked signatures, passports, and facial expressions are absent, our assurance level that we're interacting with the right person (or the same person) is increasingly coming under question. State research and education communities increasingly rely upon a growing variety of online interactions that require satisfying multiple authentication systems with multiple user-IDs and passwords. This cumbersome and confusing state-of-affairs also increases the risk of fraud, privacy compromise and identity theft. When collaborating campuses want to streamline processes associated with shared courses and enable research partnerships among faculty, access management becomes an obstacle difficult to overcome.

This topic has been discussed for a number of years in both the StateNets and Higher Education Systems communities. Resources and services that require more efficient statewide identity and access management include: administrative (benefits enrollment), teaching and learning related resources (shared course ware, video portals, library resources), and research (Grid infrastructures), among others. The current methods used for authentication and authorization don't scale and compromise security, privacy or both. Using federated identity, the service provider's account management burden is significantly reduced and the security and privacy is increased for the participating campus or state entity.

But getting a consortium started with federated identity is difficult. Collaborating with diverse audiences such as K20, corporate partners, state government, and non-profit service providers such as state and regional networks is a challenging task. How does one start? Who should be included in the federation efforts? How does one make the case to K12? There are precious few hard answers to these questions and even fewer individuals who have successfully built a federation. Leveraging the community to help each other develop implementation strategies and emerging practices is the most expedient way to grow collective knowledge in this area.

Other issues that need to be considered include whether to build your own Identity Federation by creating consortium-specific rules for trust or by leveraging the InCommon Federation as the basic infrastructure and addressing additional requirements as necessary. Why would one choose one approach over the other? These two models are represented in the University of Texas Federation in the first case and University of California system in the second, the only two groups within the US that currently have a functioning higher-ed federation aside from the national InCommon infrastructure. Both will be asked to join the discussions and help participants determine which approach is right for them. Other related issues include questions regarding inter-federation interoperability (e.g., between two StateNet-based federations, a federation and the federal government); also what criteria guide the optimal sizing of a federation.