

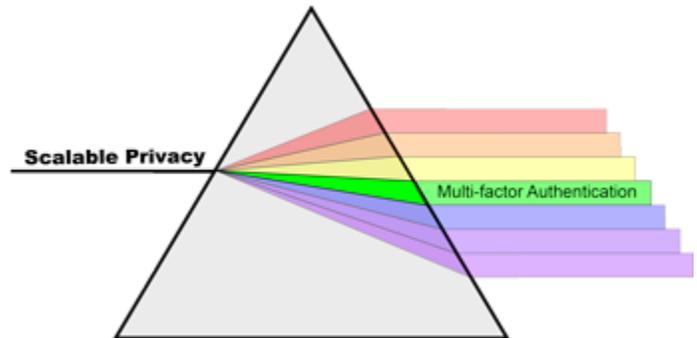
# Multi-factor Authentication in Higher Education -- MFA Cohortium and Pilots

## Multi-factor Authentication in Higher Education

The ScalePriv Project contains several major thrusts around identity and privacy, including a focus on promoting the adoption of Multi-factor Authentication (MFA) across Higher Education institutions. The ScalePriv Project includes three partially supported leadership deployments of MFA at the Massachusetts Institute of Technology (MIT), University of Texas System, and University of Utah, as well as the commitment of building the MFA Cohortium (see below).

Promoting the adoption of MFA fits into the overall ScalePriv Project in multiple ways:

- *Good privacy begins with good security*, with several examples being:
  - better assurance that individuals with privileges to see and/or manage other's personal data are indeed the individuals intended to have such access,
  - a more secure account makes phishing harder,
  - privacy managers can leverage higher levels of assurance (i.e., ones requiring MFA) before authorizing the release of sensitive identity attributes.
- A number of approaches to MFA involve biometric or other data (e.g. geolocation from an SMS 2nd factor activity) that has the potential of "privacy spillage". Having MFA behind a campus' Identity Provider (IdP), and then using federation to leverage that MFA for a broad spectrum of services, allows the advantages of MFA while gaining a potential "privacy firewall" in the form of the IdP.
- It helps to minimize the number of Service Providers that might otherwise feel compelled to offer their own MFA implementations that don't have the advantage of the "IdP privacy firewall", and have the potential to confuse users with the multitude of approaches, devices, etc.



## The MFA Pilot Institutions

The ScalePriv Project includes three partially supported leadership deployments of MFA at the Massachusetts Institute of Technology (MIT), University of Texas System, and University of Utah, as well as the commitment of building the MFA Cohortium. As these pilots progress, more information about each will be added to this space and a page focused on the pilot deployments at each institution. The work and expertise of these three institutions will also be contributing to the broader MFA Cohortium initiative described next.

## The MFA Cohortium

- **Factoring the Authentication Equation: The Multi-factor Authentication (MFA) "Cohortium" Call for Participation.**

Join the Cohortium and help advance your own MFA efforts, and the MFA efforts for all of higher education. This solicitation will officially be sent out the week of March 11 - 15, 2013, recruiting campuses to become a member of the The MFA Cohortium.

- **Multi-factor Authentication for Higher Education**

The MFA Cohortium will, by the time it concludes in June 2014, have built a website that will provide a lasting and living set of resources and roadmaps that captures the richness of use cases, requirements, MFA technologies and integration strategies, costs and ROI, planning documents, implementation and deployment strategies, training and support plans and materials, and outreach examples (e.g. news releases, ads, videos, social marketing strategies) generated by the participants. By the time the formal lifetime of the Cohortium ends, the intent is that this "Higher Education MFA web site" will contain answers, samples and examples for all of the questions and artifact categories identified on this web page.

## Summary from the draft MFA Cohortium Call for Participation

The [Internet2 Scalable Privacy Project \(ScalePriv\)](#) is seeking campuses to participate in the Multi-factor Authentication (MFA) "Cohortium". The MFA Cohortium will be a ScalePriv-supported group of institutions sharing their explorations, experiences, expertise, artifacts, and overall "journey" in learning about, planning for, and deploying multi-factor authentication for a variety of key use cases within each institution. It will be a facilitated and focused 15-month effort to help **you** (as a participating institution) make real progress towards MFA deployments. It will enable your institution, and higher education more broadly, to answer the questions "where do we need MFA?", "how do we deploy it?", and "what will it cost and what is our ROI?". And it will be focused on the research and education (R&E) community, dealing with issues and use cases of particular concern within R&E such as integrating MFA into WebSSO, sensitive data, cloud services, distance learners, bring-your-own-device, and the return on investment (ROI) within the R&E environment.

What is a Cohortium? A Cohortium is:

**cohortium:** "Group of institutions sharing their explorations, experiences, expertise, artifacts, and overall journey", in this case of planning for and deploying multi-factor authentication.

- **Cohort:** *In statistics and demography, a cohort is a group of subjects who have shared a particular event together during a particular time span* [cohort (statistics) from Wikipedia].
- -tium added to noun base to create abstract noun, "something connected with the act", could mean "act, condition, office of..."

This MFA Cohortium opportunity, and the overall ScalePriv project of which it is part, is made possible by a grant from the [National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#) initiative, and by support from [InCommon](#) and [Internet2](#).

#### Important highlights:

- Will provide your institution broader access to expertise, resources, and collaborators to help you accomplish your MFA goals.
- Enable a significant advancement in the deployment of Multi-factor Authentication across Higher Education.
- Combining MFA with federation can multiply the impact and reach of MFA to inter-institutional, shared resource, and cloud service environments.
- [A key effort within the Internet2 Scalable Privacy Project](#).
- 15-month facilitated collaborative effort beginning in April 2013 and ending in June 2014.
- Participation document submission deadline: April 12, 2013.
- Number of institutions accepted for participation in the Cohortium may need to be restricted, depending on response, to ensure value and effective collaboration for the member institutions.

## More Information

[Call for Participation -- The Multi-factor Authentication \(MFA\) "Cohortium"](#)

[Client Certificate Deployment strategies](#)

[Details on the Multi-factor Authentication Cohortium effort](#)

[Multi-factor Authentication \(MFA\) "Cohortium"](#)

[Multi-factor Authentication for Higher Education](#)

[Multi-factor Authentication Reference Materials](#)

[Phone-based Multi-factor Authentication Vendors](#)

[Top Ten Applications for MFA in Higher Education](#)

## Some Key links

- [Multi-factor Authentication Reference Materials](#)
- **InCommon/Net+ Multifactor information:** <http://www.incommon.org/multifactor/>
- **Assurance effort and Multi-factor:** [CIC Multi-factor Working Group](#)
- [NSTIC Multi-Factor Authentication Cohortium Questionnaire](#)