Call for Participation -- The Multi-factor Authentication (MFA) "Cohortium"

Factoring the Authentication Equation: The Multi-factor Authentication (MFA) "Cohortium"

Call for Participation

Summary

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, as well as federated access to services. 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 a 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 26, 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.

This document outlines the intent and goals of the Multi-factor Authentication (MFA) "Cohortium", and the requirements and expectations for participating institutions.

Table of Contents

Program Dates

- April 12, 2013: "One pager" participation document submission deadline. (Details below.)
- Week of April 29 - May 3: Organizational & Kickoff call for the Cohortium.
- Bi-weekly calls through to June 2014.
- April 22 - 24, 2013: Cohortium support staff will be available for conversations during the 2013 Internet2 Annual Meeting.
- Fall 2013: Broad release of MFA integration artifacts for Shibboleth and CAS
- November 2013 (mid-month): Potential opportunity for Cohortium meeting during the in-discussion Internet2 Identity Week.
- Spring 2014: Begin to finalize the structure, organization, and content of the public-facing "MFA for Higher Education" website.
- June 2014:
    - Wrap-up Meeting of the MFA Cohortium.
    - Each participating institution must submit a case study or similar document by the Wrap-up Meeting.
    - Conclusion to the formal activities of the Cohortium.

Program Information

A key deliverable of the Internet2 Scalable Privacy Project (ScalePriv) is the promotion of multi-factor authentication (MFA), under the tenet that "good privacy begins with good security". Just a few of the links between privacy and MFA are:

- 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 before authorizing the release of sensitive identity attributes.

Establishing the MFA Cohortium will provide a supported and collaborative environment focused on advancing the use of MFA in higher education. The MFA Cohortium will be supported by ScalePriv project staff, who will facilitate all of the Cohortium activities and help the member institutions to learn from experts, early adopters, and each other about effective implementation of MFA. The Cohortium participants will be sharing their explorations, experiences, expertise, artifacts, and overall roadmap to learning about, planning for, and deploying multi-factor authentication for a variety of key use cases within each institution, as well as federated access to services. The Cohortium will unite a committed group of campuses in a 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.

Coordination and facilitation for the Cohortium will be provided by ScalePriv staff, along with a collaboration environment and tools, and the building of a resource and reference website focused on MFA for higher education and the R&E community. The Cohortium will also be able to leverage the expertise and work of the three institutions – Massachusetts Institute of Technology (MIT), University of Texas System, University of Utah – who have funding under the NSTIC grant for significant MFA deployments. It may also include the availability of some limited consulting services, facilitation of campus events and outreach focused on MFA, help with documentation, and perhaps other ideas that are generated within the Cohortium itself, all targeted at the participating institutions.

Several "sub-Cohortiums" (working groups) may be formed within the larger Cohortium to focus on particular topics and/or based on "clustering" of mutual interests and concerns as identified from the "One Pager" Proposal Submissions from the participating campuses. The need for other sub-Cohortiums may also arise in the course of the overall work of the Cohortium.

Cohortium Goals and Outcomes

- Help **you** get MFA deployed within your institution, and for federated services, where it is needed.
- Identify a key body of use cases and applications where MFA deployment is particularly critical.
- Identify and resolve technical and policy questions around the use and integration of MFA technologies with a variety of authentication frameworks, applications, cloud services, communities, and Bring Your Own Device (BYOD) environments, leading to a set of MFA deployment roadmaps for institutions.
- Identify and resolve technical and policy issues related to federation of Identity Providers that have implemented MFA technologies.
- Produce integration strategies and plugins for the effective use of MFA with the Shibboleth and CAS SSO solutions.
- Leverage the experience and expertise of the pilot institutions, the work and support of the Cohortium, the technical work around MFA integration, and the licensing efforts of the Internet2 NET+ initiative to launch significantly more deployments of MFA across the spectrum of Higher Educational institutions.
- Produce analyses and summaries of the experiences, success factors, lessons learned, and benefits and ROI of MFA based on the deployments of the pilot and Cohortium institutions. Including a focus on factors affecting MFA deployments within institutions such as the audience, scale of deployment, target applications and services, authentication frameworks (e.g SSO), MFA technology, large number of remote users/distance learners, and/or the existing environment (e.g. legacy MFA already in use).
- Create a "MFA for Higher Education" web resource site 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.
- Summarize what **you** (your institution) got out of your involvement in the MFA Cohortium.

Program Expectations

- One pager submission to identify your desire to join the Cohortium, key reasons why you wish to participate, and your willingness to share MFA plans and artifacts more broadly. (See the next section for more details on this "one pager".)
- Must identify at least one individual who will participate in the MFA Cohortium on behalf of the institution. Ideally, a team of individuals, representing key stakeholders for MFA deployment within the institution, would participate. The number of participants from an accepted institution will not be limited.
- Participate in bi-weekly calls (should have at least one representative on most bi-weekly calls).
- Actively participate on the mailing list(s), wiki, etc.
- Contribute artifacts (sample use cases, plans, strategies, planning documents, cost/benefit analyses, etc.) as appropriate.
- Participating institutions must submit at least one MFA case study, or similar document or artifact, by the Wrap-up Meeting in June 2014.

"One Pager" Participation Submission Information

Interested institutions should submit a document (one page is sufficient) describing:

- your reasons/objectives for wanting to participate in the Cohortium,
- how the Cohortium can help achieve those objectives,
- your willingness to share MFA plans and artifacts more broadly,
- whether your institution has any current deployments of MFA, or active efforts to do so,
- target use cases, applications/services, or a given community of users that might be your initial focus for MFA (to the extent known),
- identify one or more individuals who will be participating on behalf of the institution. Please include contact information for these individuals, and
- contact information for the executive-level sponsor(s) (e.g., CIO) for your participation, if that person is not you.

Two easy ways to create this "one pager" and submit as an application to join the Cohortium are:

- use this web form containing the above questions to create and submit your "one pager" application to join the Cohortium, or
- use this text file template containing these same questions to help format an email that you then send to cohortium-reg@internet2.edu.

There may be a limit to the number of institutions that are accepted to participate, but there will be no limit to the number of participants from each accepted institution. (A campus team approach is encouraged, with key stakeholders represented.)

About the Internet2 Scalable Privacy Project

The National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative is a "White House initiative to work collaboratively with the private sector, advocacy groups and public-sector agencies" with the goal of advancing the "NSTIC vision that individuals and organizations adopt secure, efficient, easy-to-use, and interoperable identity credentials to access online services in a way that promotes confidence, privacy, choice and innovation." The Internet2 Scalable Privacy Project (ScalePriv) is one of five pilot projects to receive funding from the first round of pilot funding in September 2012. 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), the University of Texas System, and the University of Utah, as well as the commitment of building the MFA Cohortium described in this Call for Participation.

For more detailed information on the MFA Cohortium, please visit the **Details on the Multi-factor Authentication Cohortium effort** page.