

Internet2 PKI Early Adopters' Call for Participation: August-2005

1. Introduction

This document outlines the requirements for submitting a proposal to participate in the Internet2 Public Key Infrastructure (PKI) Early Adopters' Program.

The intent of the initiative is to advance the deployed use of PKI in higher education and research. This is not a research or development project. Rather, it is oriented to introducing PKI as a significant tool in the campus identity management infrastructure. The emphasis is on applications and on specific deployment efforts that advance campus business and academic goals.

There are several goals for this initiative:

- Promote the use of PKI as a tool for the business and academic needs of institutions
- Improve the security and efficiency of networked interactions
- Focus on local applications that might have broad and/or inter-institutional use. Examples might include: subordinate Certificate Authority (CA) approaches, digitally signed document deployments using specific packages, signed email deployments, etc.

We anticipate several outcomes of this initiative. These include:

- Gathering of technical wisdom. We intend to develop case studies of the technology issues, best practices, etc. The knowledge will be leveraged both as a knowledge base, available for inquiry on an as needed basis by the community for working knowledge of the quirks of technologies, and as a set of technical blueprints for institutions seeking to establish their own projects.
- Richer understanding of applications/infrastructure interactions. A particular challenge in PKI has been the “I” – infrastructure. Most uses of PKI have deployed infrastructure in an application-specific fashion. While many of the projects within the initiative may use ad hoc or application-oriented infrastructure, we hope to pool our experiences and point to a single consistent infrastructure to support a wide variety of applications.
- User/client issues and resolutions. Many of the barriers to PKI deployment are associated with client issues. Interoperability across software vendors is typically difficult. Installation of certs, path validation, and token approaches are related issues. We recognize that many campuses can minimize interoperability issues by adopting single brand (including open source) approaches. By working together among a variety of single brand implementations, we intend to explore interoperability approaches. We may even have enough leverage to influence vendor directions.
- Business plans. Real world deployments require a set of important tactical decisions, including demonstrating return on investments (often in the form of

enhanced security), management, roll-out strategies, etc. We hope to aggregate and analyze the work done across the participant campuses.

- Recommendations for next steps. This bottom-up approach is intended to build our collective understanding of PKI engineering and provide value to individual campuses. There are several ways this work can grow, from converged Certificate Profile/Certificate Practices Statement (CP/CPS) and new certificate profile standards, to ways to link campus efforts together in federated digital signatures, bridges to other PKIs, etc. The Early Adopter experiences will shape future work in this space.

2. Participation

This CFP is intended to select several institutions to participate in this Early Adopter Program. We are looking for institutions planning a real, if limited (in scope, Level of Assurance, etc.) deployment in the next year. We are not interested in broad campus planning efforts that lay unrealized and unused. We are interested in initiatives that push beyond the current, relatively pedestrian uses of PKI (e.g. campus VPN and local server SSL) into more end-entity uses. Examples of interesting projects might include signed docs, signed or encrypted email, two-factor authentication, IPsec, Lionshare support, support for campus grids, etc. Simple uses in non-standard situations (e.g., medical schools or hospitals) or in extremely broad use (e.g., every student) also are of interest. In addition, we are particularly interested in approaches that could be implemented at other campuses or in inter-institutional scenarios.

Proposals can use in-source and out-source components for CA software, certificates, etc. Since we see PKI as a core enterprise infrastructure, we are particularly interested in deployments that address enterprise-wide implementation issues, including creation and delegation of subordinate CAs, management of desktop roots, escrow, etc.

3. Resources

Institutions provide local project support. Participants have the opportunity to take an early and active role in shaping the direction and assisting in the development of a system that we anticipate will become an essential component of enterprise infrastructure. The participating institutions looking to take this important, difficult step will leverage a wider community of expertise, focused on similar problems in the same time frames and will take advantage of early work among other leading-edge deployments. Their pain, and their successes, will be visible.

Institutions are free to use whatever certificates they choose, commercial or self-signed. If institutions are interested in using United States Higher Education Root (USHER) certificates, those certs would be issued at no cost for both the verification by USHER's Registry Authority and the first year of subscription to the USHER CA. The USHER Policy Authority will follow this work closely and will incorporate findings in its future directions.

Internet2 will provide the “sharing/leveraging” support. This includes financial support for kick off and mid-point meetings of the initiative. It will also provide scribes and flywheels to conduct the process of the initiative, including facilitation of technical exchanges, assistance in development of planning documents, contact with vendors, etc. It will also provide visibility for the institutions that participate in the initiative.

4. Key Dates

- September 14, 2005: Proposal deadline.
- By September 21, 2005: Project leads will receive notification of acceptance.
- September 18, 2:00 – 5:00 pm EDT: Meeting at Fall Internet2 Member Meeting

Potential submitters should be aware that we will have a meeting on Sunday, September 18, 2:00 – 5:00 pm EDT at the Internet2 Fall Member Meeting in Philadelphia, PA to meet with the members of the PKI working group, the USHER team, and colleagues to discuss the challenges and opportunities. Internet2 Fall Member Meeting info is available at: <http://events.internet2.edu/2005/fall-mm/>

5. Proposal Submission Information

Submission Format

Interested submitters should email their response in HTML, ASCII text, OpenOffice, or MS Word file format on or before September 14, 2005, to pki-ea-admin@internet2.edu. In order to minimize the proposal preparation work for the campus, the response need not exceed three to four pages in length (additional attachments, letters of support, and appendices are welcome) in the following format:

A. Project Summary

A paragraph that describes the basic intent and approach for the campus initiative

B. Project Description

Issues to address include:

- the use cases addressed
- planned technical approaches, and how they address the use cases
- scope of deployment, indicating initial communities and possible plans for extending the reach
- type of applications being deployed
- approach to certificate authority services
- plans to address policy issues, such as Level of Assurance
- integration with existing identity management infrastructure
- time frames
- Business or academic unit that is the local champion, and the economic or policy drivers that motivate their interest

- User support approaches

Please also address:

- Are there particular issues or areas of concern on which you are looking forward to group guidance?
- If the project/initiative is successful, how could the work be extended to new communities or new purposes on campus?
- Are there inter-institutional use cases for which the campus approach might be appropriately extended?
- Your level of comfort and commitment to community building processes, including the sharing of processes and approaches with peer institutions, and the occasional fitful starts to consensus...

C. Project Personnel

Include the names/titles of the intended lead(s) for the project and their estimated time commitments to the local PKI work.

D. An indication of support from organizational management/participants at appropriate levels (such as CIOs, CFOs, or senior IT/administrative leadership).