

# Internet2 PKI Lab Proposal

Peter Honeyman  
Center for Information Technology Integration  
University of Michigan  
Ann Arbor

**1. Introduction.** The Center for Information Technology Integration at the University of Michigan is pleased to respond to your Request for Proposals to establish a Public Key Infrastructure Lab. CITI is an active developer of public key technologies, as well as technologies related to the challenge of testing and deploying real-world software prototypes.

**2. Qualifications.** CITI was established in 1986 to enhance the University of Michigan's information technology environment and to transfer the results of its research and advanced development to industry, government, and education. Working primarily with industrial partners, CITI has accomplished much in its 15-year history, including the development and deployment of the University's computing infrastructure, based on centralized administration of distributed services.

CITI is staffed by seven University of Michigan faculty and technologists with over 15 years of professional experience on average and a dozen graduate, undergraduate, and high school students, primarily enrolled in the Department of Electrical Engineering and Computer Science. CITI faculty produce a regular stream of EECS PhDs and are active in organizing focused conferences and workshops, both domestically and internationally. CITI staff publish frequently in refereed conferences, also domestically and internationally.

We believe that CITI is singularly well suited to host one of the Internet2 PKI Labs. The University of Michigan is one of the largest and most comprehensive research universities in the US and is one of only a handful of universities with targeted programs in collaborative studies. The University of Michigan is nationally recognized as one of the most innovative in linking undergraduate education and research (RAIRE Award, UROP program). CITI has distinguished itself over its 15 year history as one of the world's leading middleware research and development labs focused on near- to intermediate-term solutions to enterprise-scale problems.

**3. Experience.** Computer security has always played a role in CITI's research; for example, when developing the Institutional File System, CITI worked closely with IBM to identify and correct a security flaw in their distributed file system protocol; later CITI published a paper describing the flaw. Security was the focus for CITI's Bellcore (now Telcordia) sponsored project, "A Testbed for Intrusion Detection, Firewalls, and Cryptographic Protocols."

In that project, CITI began working with smart cards, and is now the leading academic research institution in N. America applying tamper-resistant hardware solutions to everyday computer security problems. For example, CITI has developed and deployed smartcard-based Kerberos authentication, and is actively working to extend the benefits of tamper resistant hardware to Kerberos servers as well, using an IBM secure coprocessor that sits on a PCI bus.

In the Bellcore project, CITI also developed its Secure Videoconferencing application (see below), which has continued to play a role in CITI's research in secure, high-speed, multiparty communication. In addition, CITI initiated its Secure Packet Vault technology, which relies on PK technologies for protecting the security and privacy of network users.

CITI's interest in interoperability is reflected in several Single Signon research and development projects. In one, we explored interoperability between Kerberos and Novell authentication, and developed a system that provided credentials for both systems with a single pass phrase. CITI has also used GSS-API in several projects, and is currently developing an open source implementation of RPCSEC-GSS (RFC 2023) as part of its NFSv4 open source reference implementation, under contract to Sun and Network Appliance.

An extension of RPCSEC-GSS to LIPKEY, a low infrastructure PK mechanism under IETF development, is also anticipated.

CITI has been directly involved in PK research and development for some time. In the mid-90s, CITI developed and deployed a Kerberized PGP key signer for Macintosh and Windows (MIT built a UNIX version), but did not gain much advantage from it, due to the paucity of PGP-aware applications. CITI is presently engaged in research and development directly relevant to the PK arena, including PK extensions to its Secure Videoconferencing prototype and the KX509 project, which provides for interoperability between services protected by Kerberos and those relying on PK-based authorization.

*3.1. Secure Videoconferencing.* CITI's Secure Videoconferencing prototype, based on VIC, initially supported two parties and used a smart card-based key distribution algorithm known as Shoup-Rubin. Later developments extended the prototype to support multiparty communication and a PK key distribution method, based on Globus and GSS-API. Current research activities are focused on identifying appropriate "micro-protocols" that can be combined to meet the communications security needs of distributed applications.

CITI is also extending its secure videoconferencing application to use Akenti to control Quality of Service resource reservations. Akenti allows resource stakeholders to determine the attributes necessary for application-specific resource control and easily handles decentralized authorization and multiple CAs. In partnership with Merit, CITI plans to employ Akenti and Bandwidth Broker requests to establish QoS guarantees. This will result in a demonstration of current technology by deploying CITI's Secure Videoconferencing across a transatlantic link connecting Ann Arbor and CERN.

*3.2. KX509.* The KX509 project is directly relevant to the Internet PKI Lab interests. The goal of this project is to deploy secure web services that interoperate with the University's well-established Kerberos infrastructure. For a variety of reasons, Kerberos is not a good match for web access control; on the other hand, PK support is "baked-in" to all of the common web browsers and servers deployed today. KX509 is based on two fundamental building blocks: short-term certificates, or *junk keys*, issued at login, and secure proxy authentication.

Although the web has excellent support for PK-based client authentication, it is rare for users to have PKs in their possession. There are two principal reasons for this: (1) obtaining client certificates is a complex and tedious process, subjecting users to a form of "click hell"; and (2) to obtain a client certificate of any significant value generally requires a purchase decision by the user. Users will not appreciate the value of commercial PKs until the web offers valuable PK-protected services; yet these commercial web services can not be established until there is a significant base of users with PKs in their possession.

To escape this "catch-22", many enterprises are engaging in privately issued PK certificates and deploying PK-protected services internally. CITI's KX509 project is an example of this. CITI addresses the usability deficiencies of PK issuance by associating PK creation and certification with the login process. After authenticating a user's Kerberos credentials, the login procedure constructs a public/private key pair. The public key is signed by a Kerberized certificate authority and is stored along with the private key in the place where browsers look for them. (For Navigator, we use PKCS#11, while for Explorer we use Microsoft's CAPI library.)

We assign a short lifetime to the certificates, for two reasons. First, the security association is based on Kerberos authentication, which assigns comparably short lifetimes to its security credentials (called *tickets*.) Second, by expiring certificates quickly, we avoid the necessity of maintaining and distributing certificate revocation lists.

Junk keys are fully interoperable with any service that authenticates clients with their public keys, so long as the chain of CA signatures is valid.

*3.3. Secure proxy authentication.* We use junk keys to authorize access to Kerberos-protected resources. This has the palpable advantage of not sending Kerberos tickets (or pass phrases!) over HTTP connections:

even if protected with SSL: passing capabilities (such as Kerberos service tickets) over the web exposes users to malicious spoofing attacks. Blunting this type of attack requires focused education of users as well as comprehensive system administration of their workstations, including the installation of relevant certificates and a browser plug-in or local web proxy. Our experience with centralized service administration proves that it is feasible and economical to concentrate administrative resources on servers, leaving workstations alone insofar as possible.

We now describe the mechanics of proxy authentication. We use Apache/SSL to authenticate the user. SSL authentication is fairly elaborate, but boils down to a PK-based challenge/response authentication. We modified the Kerberos Ticket Granting Server to create the challenge and pass it to the web server. The web server then authenticates the user. In the course of doing so, the web server records a transcript of the SSL handshake. The web server passes this transcript to the modified TGS (TGS+), which checks the value and timeliness of the challenge and uses the user's certificate to validate the response. If these tests are passed, the TGS+ issues a short-term Kerberos service ticket to the web server. This provides the web server with the authority to act on the user's behalf for a limited time.

We have already described the advantages of inhering trust in the web server, rather than requiring browsers to pass service tickets or pass phrases. A disadvantage of the proxy authentication approach is the requirement of stringent web server security administration. While we hold that any service provider has these requirements, yet a compromise of a service that can request tickets on a user's behalf can be particularly severe. We do mitigate potential damage through the TGS+ modifications: the TGS+ will not issue tickets unless there is an authentic user on a browser initiating a timely request. In addition, we do not allow CGI scripts or other user-initiated extensions to run on our trusted web servers.

CITI is using junk keys and secure proxy authentication internally and has begun distributing them as open source to interested developers. We anticipate that the University of Michigan's Information Technology Division will deploy these tools sometime in the current calendar year. The proxy authentication system is independent of the issuance of junk keys, i.e., it is fully interoperable with any X.509v3-based system

*3.4. KX509 applications.* ITD's initial target for using KX509 uses the technology to extend AFS access control through the web. AFS is universally deployed at the University of Michigan. With KX509 and TGS+ in place, students, faculty, and staff are able to produce web pages that are rigidly controlled by the existing AFS authorization methods. Because our users are well versed in AFS technology, we anticipate a system that is transparent, convenient, and easy-to-use.

We are investigating a means of bootstrapping short-term certificates into long-term digital signatures using the IETF PKIX Time Stamp Authority. TSA generates a secure time stamp that proves when the time stamp was issued and the identity of the requestor. Using the TSA and an associated short-term certificate, it is possible to validate a digitally signed document, even though the associated certificate has expired, as long as the certificate was valid when the time stamp was issued. This has immediate application in arenas such as digitally signed Email and other documents requiring strong authentication. Observe how this application "outsources" CRL management to the TSA.

We are also investigating the use of Akenti for distributed delegable authorization using junk keys. Akenti allows resource stakeholders to determine the attributes necessary for application-specific resource control and easily handles decentralized authorization and multiple CAs. We are investigating extending KX509 to manufacture the attribute and use condition certificates required by Akenti.

**4. Vision.** CITI is eager to serve as a PKI Lab to extend our vision of scalable and manageable PK services in an enterprise environment. Our experience in developing and helping to deploy a campus-wide security infrastructure provides invaluable perspective on the "dos and don'ts" in enterprise-scale system management. Centralized management of services is fundamental to scalability; for example, this enables the UMICH.EDU Kerberos realm to serve over 70,000 active users and a user population of over 170,000. (CITI developed the Kerberos V replication engine that permits this degree of scalability.)

To date, PKI administration has required active engagement on the part of each user; we hold that this has retarded its widespread deployment. Other factors that have blunted the potential impact of PK include cost (but CITI is committed to open source distribution of its research products), lack of interoperability with existing systems (but CITI is developing its PK solutions with interoperability firmly in mind), and the difficulty of managing CRLs (solved with junk keys).

By integrating Akenti into our research products, we obtain the advantage of interoperability with multiple CAs, which relaxes the restriction of a single, centralized administration of user identities.

CITI is also investigating the storage security requirements of user keys, such as private keys, Kerberos keys, and capabilities such as Kerberos tickets. From this, we hope to identify and develop appropriate models and abstractions that integrate our smartcard and tamper-responding hardware expertise with our development of secure and scalable solutions for PKI.

**5. Resources.** CITI is led by Peter Honeyman, a Research Scientist reporting to José-Marie Griffiths, the University of Michigan's Chief Information Officer. Dr. Honeyman also holds an appointment as Adjunct Professor of EECS, where he teaches regularly and chairs several EECS Doctoral Committees. While Dr. Honeyman anticipates serving as Principal Investigator for the PKI Lab; his salary will continue to be funded by the CIO.

CITI's KX509 project is led by Bill Doster, an ITD staff member on loan to CITI. Mr. Doster has worked with campus authentication systems for over 10 years, and is the principal developer of the University of Michigan's UNIQNAME and Authenticated Billing systems. CITI anticipates transferring Mr. Doster to a more permanent role at CITI, and anticipates his role as Technical Lead for the PKI Lab. ITD will continue to fund Mr. Doster.

Kevin Coffman, CITI Technologist, is also funded by ITD to work on KX509. Mr. Coffman has been participating in KX509 development for the past year. Earlier, he developed the University of Michigan's Kerberos V replication engine.

Olga Kornievskaja, a Doctoral Candidate studying under Dr. Honeyman's direction, developed the TGS+ component of KX509. CITI has funded Ms. Kornievskaja with internal resources to date; a proposal to ITD to fund her continuing research is under consideration.

CITI has a proposal outstanding to fund the pilot Akenti-controlled QoS reservation of a secure videoconferencing channel between Ann Arbor and Geneva. This project will use KX509 junk keys.

Internet2 funding will add to these resources already in place. We hope to use the additional funds to broaden our reach, e.g., to extend our PK interoperability research and development to commercial products, such as the AT&T software.

## **6. Relevant publications**

The following selected publications, available on CITI's Technical Report web page, <http://www.citi.umich.edu/techreports/> reflect CITI's interests and skills in interoperable security frameworks.

N. Itoi, "Secure Coprocessor Integration with Kerberos V5," to appear in *Proc. USENIX Security'2000*, Denver, Colorado (September 2000).

N. Provos, "Encrypting Virtual Memory," to appear in *Proc. USENIX Security'2000*, Denver, Colorado (September 2000).

W.A. Adamson, C.J. Antonelli, K.W. Coffman, P.D. McDaniel, and J. Rees, "Secure Distributed Virtual Conferencing: Multicast or Bust," in *Proc. CMS'99*, Leuven, Belgium (September 1999).

- P.D. McDaniel, A. Prakash, and P. Honeyman, "Antigone: A Flexible Framework for Secure Group Communication," in *Proc. 8th USENIX Security Symp.*, Washington, D.C. (August 1999).
- N. Itoi and P. Honeyman, "Pluggable Authentication Module for Windows NT," in *Proc. 2nd USENIX Windows NT Symp.*, Seattle (August 1998).
- P. McDaniel, P. Honeyman, and A. Prakash, "Lightweight Secure Group Communication," CITI Technical Report 98-3 (April, 1998).
- R. Jerdonek, P. Honeyman, K.W. Coffman, J. Rees, and K. Wheeler, "Implementation of a Provably Secure, Smartcard-based Key Distribution Protocol," in *Proc CARDIS'98*, Louvaine-la-Neuve, Belgium (September, 1998)
- C.J. Antonelli, M. Undy, and P. Honeyman, "The Packet Vault: Secure Storage of Network Data," in *Proc. USENIX Workshop on Intrusion Detection and Network Monitoring*, Santa Clara (April 1999)
- N. Itoi and P. Honeyman, "Smartcard Integration with Kerberos V5," in *Proc. USENIX Workshop on Smartcard Technology*, Chicago (May 1999).
- N. Itoi, P. Honeyman, and J. Rees, "SCFS: A UNIX Filesystem for Smartcards," in *Proc. USENIX Workshop on Smartcard Technology*, Chicago (May 1999).
- P. Honeyman, W.A. Adamson, K.W. Coffman, J.E. Janakiraman, R. Jerdonek, and J. Rees, "Provably Secure Videoconferencing," in *Proc. 7th USENIX Security Conf.*, San Antonio (January, 1998).
- W.A. Adamson, J. Rees, and P. Honeyman, "Joining Security Realms: A Single Login for NetWare and Kerberos," in *Proc. Fifth USENIX UNIX Security Symp.*, Salt Lake City (June 1995).