



The University of Virginia: Campus PKI Services/Bridge CA

NSF Middleware Initiative (NMI) Integration Testbed Case Study Series

Series contact: Mary Fran Yafchak, Southeastern Universities Research Association,
maryfran@sura.org.

The NMI Integration Testbed Program provided practical evaluation of NMI components within the context of real projects and application scenarios from June 2002 through November 2004. During that time, NMI Testbed sites collectively submitted over 220 evaluation reports to middleware component developers as direct feedback into the NMI development cycle. Site representatives also actively inspired, promoted and facilitated the integration of middleware throughout their institutions.

The NMI Integration Testbed Case Study Series documents the most significant outcomes and influences of NMI Testbed sites' middleware integration efforts, highlighting intersections with established projects, application contexts and influences, drivers for innovation, decision points and challenges. Through this documentation, the work of these pioneering institutions is captured to provide a breadth of insight and approaches for others to use towards successful middleware development and deployment.

This NMI Integration Testbed Case Study Series is sponsored by the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium of EDUCAUSE, Internet2, and SURA. Additional support was provided by the National Science Foundation Cooperative Agreement NSF 02-028, ANI-0123937.

Copyright © 2005 The University of Virginia. The University of Virginia permits use of this content for noncommercial purposes with proper attribution. All rights reserved.



Executive Summary

The University of Virginia (UVa) has deployed public key infrastructure (PKI) as a key component of their campus authentication infrastructure. UVa's PKI deployment coincided with their participation as a Testbed site within the NSF Middleware Initiative (NMI) Integration Testbed. The goals and timing of the Testbed presented UVa with an opportune venue to work with PKI-related NMI components and evaluate them against the actual campus PKI infrastructure being deployed.

UVa designed their PKI as a complementary authentication mechanism to their existing infrastructure. By adding a PKI, UVa could bring the benefits of PKI to their campus, enabling applications that leverage digital certificates. Also, since PKI readily integrates with two-factor authentication solutions, UVa has been able to deploy new services that require the high level of assurance such authentication provides.

UVa's deployment approach and the ease with which a PKI can, with some planning, be implemented rather transparently to integrate with an existing authentication infrastructure, minimized the impact on users and IT staff. UVa deployed PKI mechanisms into their existing environment, leveraging them first for authentication in new, non-mandatory applications and then as alternative authentication for many existing campus applications. Currently, the

most widespread use of PKI is for authentication to UVa's wireless LAN and VPN (virtual private network) services. PKI authentication is also used in UVa's [Pubcookie](#) deployment, which will enable access to a large number of Web-based applications, and for access to grid-based resources on and off campus.

By leveraging evaluation of specific NMI components within the NMI Testbed program, UVa made several enhancements to their central campus directory infrastructure. UVa's directory services are a key component of their campus PKI, since the UVa directory stores authorization data that PKI authenticated services rely on.

While deploying PKI infrastructure on their own campus, UVa's discussions with other NMI Integration Testbed sites helped facilitate UVa's development of a Bridge Certificate Authority (CA) to create inter-organizational trust relationships among Testbed sites in the NMI Testbed Grid project. The Testbed Bridge CA is designed to show how Higher Education grids will be able to leverage the future Higher Education Bridge CA as a key component of an inter-institutional trust model.

For more information about UVa campus PKI services and the Bridge CA, contact Jim Jokl at jaj@virginia.edu.



NMI Components Highlighted in this Case Study

The NMI components discussed in this case study series encompass NMI Releases 1 through 4. Information about NMI Releases can be found at <http://nsf-middleware.org/>.

Campus Certificate Policy for use at the Higher Education Bridge Certification Authority (Higher Education PKI (HEPKI) Model Campus Certificate Policy)

NMI-EDIT's Certificate Policy (CP) statement defines the terms and conditions under which a Certificate Authority (CA), issuing Public Key Certificates (PKC) that reference the policy object identifier (OID) for the HEBCA CP, must operate.

Home site: <http://middleware.internet2.edu/certpolicies/>

Conventions and Best Practices

These NMI-EDIT documents reflect current NMI research in campus core middleware. The architecture approaches and policies promulgated here are in use at several leading campuses and institutions. Discussion includes the "Practices in Directory Groups" document.

Home site: <http://www.nsf-middleware.org/NMIR5/nmi-edit/bestpractices.asp>

Globus

The GRIDS Center's Globus Toolkit is an open-source collection of modular technologies that simplifies collaboration across dynamic, multi-institutional virtual organizations. It includes tools for authentication, scheduling, file transfer and resource description.

Home site: <http://www-unix.globus.org/toolkit/>

Lightweight Campus Certificate Policy and Practice Statement (PKI-Lite)

PKI-Lite focuses on employing PKI technology for standard assurance applications that already have established and implemented requirements for initial user authentication and overall system security.

Home site: <http://middleware.internet2.edu/hepki-tag/>

Pubcookie

Pubcookie is open source software that supports intra-institutional web initial sign-on.

Home site: <http://www.pubcookie.org/>

Shibboleth

The Shibboleth technology supports inter-institutional sharing of web-based resources subject to access controls.

Home site: <http://shibboleth.internet2.edu>



The University of Virginia: Campus PKI Services/Bridge CA

Many computer users in higher education and other communities take for granted the authenticity and security of their computing transactions. Yet in carrying out their daily computing tasks, whether they realize it or not, end-users on higher education campuses depend on the authentication capabilities computing staff have built into the myriad of applications and services found on the typical campus. Throughout higher education, as well as the business world, there has been a growing use of public key infrastructure (PKI) technologies for providing authentication and encryption capabilities.

At the University of Virginia, where providing for the authenticity of logins and the security of data transmissions for the 30,000 students, faculty and staff on campus is a large and complex task, PKI technology has become a key component of the campus authentication infrastructure. While deploying this PKI infrastructure on their campus, UVa also actively contributed to projects focused on the deployment of PKI beyond the University, and the development of the recommendations and materials for campus PKI implementers to facilitate the adoption of PKI and bring its benefits to their peers in the higher education community.

UVa's work with PKI coincided with their participation as a Testbed site within the NSF Middleware Initiative (NMI) Integration Testbed¹. Managed by the Southeastern Universities Research Association (SURA) on behalf of the NMI-EDIT² Consortium, the Testbed consisted of eight universities that participated in a closely coordinated effort to deploy and evaluate NMI technologies. The goals and timing of the Testbed presented UVa with an opportune venue for evaluating various NMI components for their utility and fit within UVa's new PKI infrastructure. This article will provide an overview of UVa's campus PKI deployment, including a review of the NMI components tested and used in the process, and how UVA designed their PKI infrastructure to serve multiple applications.

NMI Integration Testbed Influence on UVa's PKI

Jim Jokl at UVa is a leader in security and interoperability issues associated with PKI. Jokl chairs the Higher Education PKI Technical Activities Group (HEPI-TAG), and is a member of the Middleware Architecture

¹ As part of its overall effort to develop and disseminate software that lets scientists and educators share resources across the Internet, NMI began a practical deployment and evaluation effort called the NMI Integration Testbed. <http://www1.sura.org/3000/NMI-Testbed.html>

² NSF Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT): <http://www.nmi-edit.org/>



Committee for Education (MACE). UVa supports Jokl in these endeavors as a way to contribute to the development of Internet technologies and to help bring cutting-edge Internet technologies to their campus. When the NMI Testbed began in June 2002, UVa's PKI team was actively working on the deployment of PKI infrastructure for the campus, as well as a set of PKI-enabled applications. With staff at UVa significantly experienced in PKI issues, they were eager to lead the development of solutions to PKI interoperability and policy issues that would be raised within the NMI Integration Testbed.

During UVa's participation in the NMI Integration Testbed, they worked with PKI-related NMI components, evaluating them against the actual campus PKI infrastructure being deployed. UVa was able to evaluate specific NMI components in the Testbed and incorporate them into the UVa PKI environment when appropriate. One of UVa's goals for their campus middleware integration with the GRIDS Center's [Globus Toolkit](#) was to ensure that certificates issued by the UVa Standard Assurance Certification Authority (CA) would work well with [Globus](#). This would enable researchers to leverage central authentication instead of having to operate their own CA. The use of this central authentication would also help facilitate the construction of a UVa campus grid in the future.

Why PKI?

Computing staff at UVa have long been providing for user authentication based on verifying login-ids and passwords using a variety of techniques such as NIS, RADIUS, and Active Directory. In fact, UVa first implemented globally unique, enterprise-wide computing identifiers for the entire university community in the 1980s. These identifiers continue to provide both user login names for campus computer systems and a means for email routing. UVa's current authentication mechanisms leverage the university's central LDAP (Lightweight Directory Access Protocol) directory for authorization information. The LDAP directory contains records for all faculty, staff, and students. UVa's primary centralized Web authentication service is a locally developed Apache module that validates user passwords from central email and network storage services. This Apache module uses the RADIUS and SMB protocols to validate email and storage system passwords. Together, these elements comprised UVa's central authentication infrastructure.

In early 2000, UVa recognized they would be able to enhance their authentication infrastructure and enable new applications by deploying a campus PKI. UVa would design the new PKI infrastructure to be complementary to existing campus authentication mechanisms and to leverage existing password-based systems as one component in the process of issuing digital



certificates to users. Along with supporting user authentication via cryptographically strong mechanisms, a PKI also lays the foundation for enhanced services such as digital signatures for business processes, signed and encrypted email, and other similar services. Knowing that PKI is supported natively in nearly all web browsers and that good operating system PKI-support exists on most desktop computers, UVa believed supporting a PKI would not require much additional overhead from IT staff.

Additionally, UVa has several application services that require a high level of assurance and, since PKI is easily used in applications that require this type of security, UVa saw PKI as a means to properly secure their high security applications. Two-factor authentication solutions, which use two different items to verify a person's identity, are often used to secure applications that require a high level of assurance. Single-factor authentication is typically based on *something the user knows* (e.g. a password), whereas two-factor authentication is typically based both on something the user knows plus *something they have* (e.g., a hardware token). PKI technology integrates readily into two-factor authentication solutions as several manufacturers make smart card and USB devices that protect a user's private key (something the user has) and require a password (something the user knows) to unlock the device.

Having decided that the benefits of PKI would benefit their campus users and their applications, UVa began preparations for the PKI deployment in late 2000. Wanting to deploy their PKI infrastructure as transparently as possible to their users, UVa approached the deployment by easing PKI mechanisms into their existing environment, leveraging them first for authentication in new, non-mandatory applications. Later, UVa would enable their PKI to support new services and use it as an alternative authentication means for many existing campus applications. This deployment approach enabled users and staff to gain familiarity with PKI technology, and its support, before its widespread campus use.

Certification Authorities in UVa's PKI Deployment

Certification Authorities (CAs) are central to a PKI infrastructure. A PKI is typically thought of in terms of a Certification Authority (CA) and a Registration Authority (RA). While these roles are often blurred in practical implementations, the CA generally signs and issues certificates while the RA acts as the entity that interfaces with the user, verifies the user's identity, and requests that the CA issue a certificate to the user. The UVa PKI infrastructure was designed to support two different levels of assurance, using a Standard Assurance CA and a High Assurance CA. The Level of Assurance of a PKI relates to the strength of the binding between the user (the holder of a certificate) and the private key associated



with the certificate. In technical terms, a high level of assurance is obtained via a strong identity proofing process in the RA, by a carefully managed and strongly protected CA, and by other factors such as how the user's private key is protected after the certificate is issued.

UVa deployed its Standard Assurance CA in December 2002, basing it on NMI-EDIT's [Lightweight Campus Certificate Policy](#). The UVa Standard Assurance (CA) is designed to support the use of strong cryptography in applications where, traditionally, login-id and password solutions were used. These applications include web authentication, VPNs (virtual private networks) and wireless network access. This CA was also designed to facilitate new services such as signed electronic mail and [Globus](#)-based campus grid services. This CA uses the PKI-Lite Policy and Practices³ and is presently part of the CREN PKI Higher Education CA⁴ hierarchy. UVa will migrate their Standard Assurance CA to become part of the US Higher Education Root (USHER) hierarchy¹ once Internet2 has completed the work to make USHER available to its members.

UVa rolled out their High Assurance CA in November 2003 and based it on NMI-EDIT's [Higher Education PKI \(HEPKI\) Model](#)

[Campus Certificate Policy \(CP\)](#)⁵. The UVa High Assurance CA requires the use of hardware tokens for a user's private key protection and mobility, and is designed to support processes that require a higher level of assurance than most traditional applications. Example applications include access to protected data (HIPAA, FERPA, etc), Unix SSH authentication for system and database administrators of critical systems, and other similar services. This High Assurance CA is intended to be cross-certified with the EDUCAUSE Higher Education Bridge Certification Authority (HEBCA)⁶ when that service is available.

PKI Use In UVa Directory Services

UVa's central user identification and account management system receives data from all of the various sources of payroll and student information, and generates a unique identifier for each individual affiliated with the university. This system is also a core component of UVa's central directory infrastructure. Once a person is in the directory, they can activate their accounts on any of UVa's central systems (e.g., electronic mail, network file storage, Unix) and thus obtain a password. During the course of the NMI Testbed project, UVa made several enhancements to their central campus directory infrastructure. After

³ PKI-Lite Policy and Practices:
http://middleware.internet2.edu/hepki-tag/index.html#PKI_Lite

⁴ CREN PKI Higher Education CA⁴ hierarchy:
<http://www.cren.net/crenca/>

⁵ Higher Education PKI (HEPKI) Model Campus Certificate Policy:

<http://middleware.internet2.edu/certpolicies/>

⁶ HEBCA information:

http://www.educause.edu/content.asp?page_id=623&hcp=1



reviewing NMI-EDIT's [eduPerson](#)⁷ schema, UVa made a key decision to migrate their InetOrgPerson-based directory system to the [eduPerson](#) schema. This migration was done in order to promote interoperability and to support UVa's deployment of NMI-EDIT's [Shibboleth](#)⁸ software. The design for the directory group infrastructure currently being deployed is based, in part, on NMI-EDIT's best practices document for directory groups, "[Practices in Directory Groups](#)"⁹.

UVa's directory services are also a key component of their campus PKI deployment. Directories store the authorization data for services that are authenticated by the two-factor PKI-based High Assurance CA,

control authorization for other services that leverage the Standard Assurance CA, and also store the CRL (certification revocation) lists¹⁰ that are part of the base PKI infrastructure. The Registration Authority (RA) process for the UVa Standard Assurance CA leverages the directory infrastructure to properly identify the user requesting the certificate. Along with verifying a user's password, the Standard Assurance CA requires that the user also be able to supply a few other attributes about themselves (see Figure 1).

These attributes are verified using the directory infrastructure before a certificate is issued to the user.

Figure 1

PKI In order to obtain a certificate you will first need to provide some personal information.

This information will be used to confirm that you are authorized to have an account at the University of Virginia. All of the information below must be entered as it appears in official U.Va. records.

<input type="text"/>	Your U.Va. computing ID (e.g., mst3k)
<input type="password"/>	Your current password on a Blue, Home Directory, CMS, or HSC Exchange account
<input type="text"/>	Your last name
<input type="text"/>	Your university ID (usually social security number, e.g.; 222881111)
<input type="text"/>	Your birthdate in the format YYYYMMDD (e.g.; 19810610 for June 10, 1981)

Submit information Reset abort

⁷ eduPerson information:

<http://www.educause.edu/eduperson/>

⁸ Shibboleth information: <http://shibboleth.internet2.edu/>

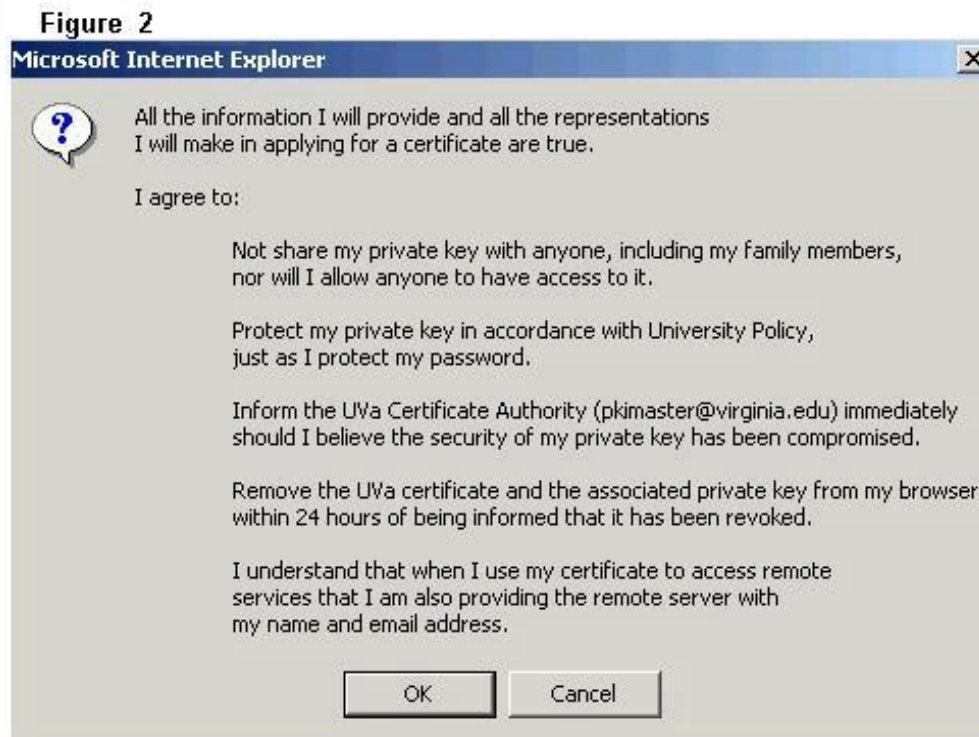
⁹ "Practices in Directory Groups" information: <http://middleware.internet2.edu/dir/>

¹⁰ A CRL list is a signed object that contains cryptographic records of certificates that have been revoked.



Upon verification of the attribute information, the user is fully authenticated to the CA website. During this process, the person

receiving the certificate must also accept their responsibilities as a certificate owner (see Figure 2).



A copy of this text is also emailed to the user after the new certificate is issued. Next, the user's web browser generates the user's key pair and sends a certificate request to the CA. The CA then generates and signs a certificate for the user based on the certificate request, automatically downloads the result and places the certificate into the user's certificate store. Once in the certificate store, the certificate can be used by the browser and other applications as needed. A second interface to the CA is available for operating systems and browsers that do not support the same level

of PKI automation as Windows¹¹. Users are able to use a web interface to select their preferred certificate and it is this preferred certificate that is published to the main LDAP directory. The preferred certificate concept is in place for the future and is targeted to support potential encrypted email applications.

¹¹ Users of operating systems such as MacOS 10 and Linux use this second interface to receive a certificate and key pair bundled into an industry standard PKCS-12 object. Once this object is downloaded to the user's desktop, they can import the keys and certificates as needed into the operating system or directly into applications.

PKI-Based Services at UVa

PKI credentials have been deployed for use by multiple applications on the UVa campus. Currently, the most widespread use of PKI is in UVa's wireless and VPN (virtual private network) services. UVa originally designed the VPN services to use PKI credentials and deployed the PKI and VPN services once the VPN infrastructure was ready for production use. Authentication for UVa's encrypted wireless networks was converted from a vendor proprietary solution to use standards-based PKI authentication as the second main PKI-enabled application. In addition, some UVa Computer Science researchers and central IT staff are using their campus PKI credentials to access [Globus](#)-based resources and remotely access grids at other organizations (see "UVa Experience Benefits the NMI" section below). PKI-based authentication is also used in UVa's deployment of NMI-EDIT's [Pubcookie](#)¹², a Web initial sign-on package.

EAP-TLS Wireless Services

UVa's initial encrypted wireless LAN deployment used Cisco's proprietary LEAP (Lightweight Extensible Authentication Protocol) protocol to authenticate users and provide for encrypted wireless services. UVa had expected LEAP to become widely supported on most platforms (that is, for LEAP to be natively supported by the major desktop operating systems they use), but unfortunately, this did not come about. Security issues also became a concern with

LEAP: vulnerability to dictionary-based attacks (first described in fall 2003) and the release of a hacking tool in April 2004. These issues coupled with the lack of native OS support compelled UVa to replace LEAP as a security mechanism for the wireless service. Instead, UVa chose to leverage the campus PKI infrastructure with the fully standards-based EAP-TLS (Extensible Authentication Protocol-Transport Level Security) solution. UVa technical staff found EAP-TLS to be technically strong, capable of performing mutual authentication and well-supported in common desktop operating systems (including Windows XP and MacOS 10.3). EAP-TLS based wireless authentication also proved easier for end-users since no software installation is required. Once the user is logged into their workstation, their certificate key store is unlocked and the PKI cryptography to log into the wireless network happens without direct user action to log in to the network.

During UVa's preparation for its summer 2004 EAP-TLS deployment, they found that the PKI-Lite certificate profiles didn't support EAP-TLS in the Windows environment. The feedback about this that UVa submitted as an NMI Integration Testbed Site to PKI-Lite developers resulted in a change to the PKI-Lite profiles. Wireless authentication can now be deployed at any site that deploys their PKI infrastructure based on the PKI-Lite profiles.

¹² Pubcookie information: <http://www.pubcookie.org/>



VPN

The first production service at UVA that used end-user digital certificates for authentication was the remote access VPN service, “UVa-Anywhere”. UVa-Anywhere is based on Cisco’s 3000 series VPN concentrator and IPSec software client. The service provides both an encrypted path back to the UVA network and tunnels all user network traffic, effectively providing a UVA IP address for the remote user’s computer. UVa-Anywhere, supported on Windows platforms and MacOS X, went live at UVA in the winter of 2002. The next PKI-authenticated service deployed was VPN access to the standard firewalled “More-Secure” segments of the campus network. This service leverages both PKI-based authentication and the main directory services system for user authorization. In order to provide access to network segments containing sensitive HIPAA data, UVA deployed the next major VPN service, the JointVPN, in the winter of 2003. This service leverages the UVA High Assurance CA, along with two-factor authentication and LDAP-based authorization.

Globus-based Grid Access

UVA Computer Science researchers and central IT staff are using their campus PKI credentials to access Globus-based resources and remotely access grids at other organizations. UVA expects this PKI-based usage to grow with further development of the campus grid and as more users need to access resources on remote grids. While UVA found the PKI-Lite

profile certificates worked well at a technical level with the Globus software contained in NMI Release 4, UVA had to document the OpenSSL commands a user must enter so that they can extract their key and certificate in the format required by Globus. Thus, in UVA’s current process, a user first exports their certificate and private key into a PKCS-12 formatted file using native operating system commands or uses the second interface to the CA to directly obtain a PKCS-12 formatted object containing their certificates and keys. With the PKCS-12 object in hand, the user enters these commands in order to obtain the separate files for the certificate and key that the Globus Toolkit requires. As more users begin using Globus on campus, UVA intends to provide a simple web interface for splitting the certificate and key into individual files.

Pubcookie

After evaluating Pubcookie as a potential Web authentication solution as part of their NMI Integration Testbed work, UVA chose to implement it as a campus-wide Web authentication solution to replace its internally developed UVaAuth Apache module. Along with providing all of the functionality of the UVaAuth module, Pubcookie also enabled the Web single-sign-on (SSO) function that UVA wanted to offer, provided a solution for applications based on Windows IIS servers, and enabled easy deployment for departmentally developed applications. UVA incorporated Pubcookie into the campus environment by enhancing the base package with the user



authentication mechanisms for Active Directory (SMB protocol), mail and UNIX password stores (RADIUS protocol), and PKI digital certificates. By incorporating digital certificate authentication into [Pubcookie](#), UVA greatly expanded the number of campus applications that can be accessed using PKI credentials. UVA enhanced [Pubcookie](#) by adding a UNIX-like last-login display to the [Pubcookie](#) status page. This feature enables users to look at a log of the last ten times they logged in, where they logged in from, and what authentication mechanism they used. When users have authenticated using PKI, the log also shows which certificate was used for authentication. UVA found that users of the new [Pubcookie](#)-authenticated services have had very few problems and generally needed nothing more than the documentation on the SSO login site to use the services.

As of April 2005, [Pubcookie](#) is providing authentication services for the UVA Portal, network device registration, and course evaluations. UVA expects to complete the work to incorporate [Pubcookie](#) authentication into their main WebMail system, Web Home Directory storage interface, and Web calendar/scheduling system in May 2005. Once the work on these main services is complete, UVA will start to migrate remaining Web-based applications to the new system.

UVA Experience Benefits the NMI

The opportunity for discussion of common issues in varying contexts among NMI Integration Testbed sites provided UVA with insights that enabled them to extend the benefits of PKI beyond the UVA campus. Through discussions with Testbed members who were focused on grid components, UVA learned that the manner in which inter-campus trust is established in a grid environment is often ad-hoc and is frequently different among various grids. During their participation in the NMI Integration Testbed, UVA was also participating in the EDUCAUSE HEBCA (Higher Education Bridge Certificate Authority) project that was developing a PKI Bridge to serve the higher-education community. With key segments of the PKI space in higher-education slowly converging on the Bridge CA model to create inter-organizational trust relationships, UVA leveraged their concurrent participation in these two projects to promote the idea that higher education grids using the [Globus Toolkit](#) would be natural applications for HEBCA.

Given the [Globus Toolkit's](#) use of certificates for authentication, a PKI Bridge appeared to be a logical solution to solve the inter-institutional authentication problem for multi-institutional grids. A bridge could both provide the technical cross-certification infrastructure to enable certificate authentication to function and be the catalyst



for the policy discussions and decisions that must be made when building a grid. UVa performed initial proof-of-concept testing of the [Globus Toolkit](#) functioning in a bridge environment using a simple Bridge CA that it had created as part of its HEPKI-TAG contributions.

Once the technical proof of concept was complete, the UVa team proposed that NMI Integration Testbed sites work with UVa to base the NMI Testbed Grid¹³ they were building on a PKI Bridge CA. The focus of this work was to resolve any implementation problems, build a production grid that uses a PKI Bridge as the core of its inter-institutional trust fabric (until the HEBCA is ready to provide the core of the trust fabric) and create a model for other grids to follow in the future. Within the time frame of the NMI Testbed Grid project, UVa created a more secure Bridge CA using a dedicated laptop, successfully cross-certified five of the participating sites¹⁴, and began the development of a website detailing the cross-certification process¹⁵. This development effort is being carried forward within the SURAgrid project¹⁶, an outgrowth of the NMI Testbed Grid effort.

¹³ This project was begun during the NMI Integration Testbed in September 2003 and continues as the SURAgrid, as a cooperative, collaborative endeavor to investigate, implement and develop grid infrastructure.

¹⁴ See NMI Testbed Grid Case Studies: *Exploring Technical and Policy Considerations for Inter-Institutional Grids* and its technical supplement *Authentication & Authorization in SURAgrid: Concepts and Technologies* at: <http://www1.sura.org/3000/NMI-Testbed.html>

¹⁵ <https://www.pki.virginia.edu/nmi-bridge>

¹⁶ SURAgrid: <http://www1.sura.org/3000/SURAgrid.html>

Conclusion

UVa's methodology to deploy their PKI using a step-wise approach and the relative ease with which a PKI can, with some planning, be implemented rather transparently to integrate with an existing authentication infrastructure, have minimized IT support overhead and user inconvenience. UVa's PKI deployment allowed them to use PKI mechanisms to improve security in the authentication process of both new and existing campus services.

While PKI credentials have already been deployed for use by multiple applications on the UVa campus, UVa anticipates there will be future opportunities to use their PKI infrastructure to enhance the application services it offers campus-wide. This is especially true of the High Assurance CA as the security requirements for access to sensitive data continue to increase. UVa also expects the use of PKI credentials to access grid resources to grow as the campus grid evolves and researchers' need for access to resources on remote grids increases. With its PKI infrastructure in place, UVa is also well positioned to leverage the new services that will be supported using HEBCA and USHER.

More Information

For more information about campus PKI services and the Bridge CA at, contact Jim Jokl at jaj@virginia.edu.



Links of Interest

The University of Virginia <http://www.virginia.edu/>

GRIDS Center <http://www.grids-center.org/>

Higher Education PKI Technical Activities Group (HEPI-TAG)
<http://middleware.internet2.edu/hepi-tag/>

MACE <http://middleware.internet2.edu/MACE/>

NMI Integration Testbed Program <http://www1.sura.org/3000/NMI-Testbed.html>

NSF Middleware Initiative <http://www.nsf-middleware.org/>

NMI-EDIT <http://www.nmi-edit.org/>

UVa-Anywhere <http://www.itc.virginia.edu/desktop/pki/vpn/home.html>

UVa-More-Secure-Network <http://www.itc.virginia.edu/desktop/vpn/uvamore-secnet/>

ⁱ The USHER CA anticipates leveraging institutional identification process deployed to support InCommon™ (<http://www.incommonfederation.org/>) to issue authority certificates to campus CA operators. The campus CAs would then use their authority certificates and associated keys to issue PKI credentials to their campus users. All certificates issued under the USHER hierarchy could be validated and used by any campus participating in USHER using traditional hierarchical PKI methods.