

**Enterprise Directory Infrastructure  
For a  
Community of Interest**

**A White Paper**

Art Vandenberg  
Director, Advanced Campus Services  
Georgia State University  
**July 2000, revised August 15, 2000**

**Abstract**

The electronic, next-generation realm of higher education, the “eUniversity” requires an enterprise directory infrastructure as a secure foundation for identification, authentication, and authorization. The maturing technology, development of legal basis, and articulation of policy has been conducted through collaborative research and development. Industry analysts have monitored the evolution of enterprise directory solutions and can recommend strategic deployment as a valuable investment. National working groups such as the Directory Interoperability Forum, the Internet2 Middleware initiative, and the Federal PKI Steering Committee have advanced the state of development to the point that “roadmaps” and guidelines are available. Models for interoperability are available that provide scalable solutions for communities of interest. Successful deployment of enterprise directory infrastructure must take a strategic enterprise approach, utilize collaboration and communication, and leverage existing initiatives in a community of interest.

**Introduction**

Analogous to the commercial sector’s engagement with eCommerce, today’s institutions of higher education are rapidly entering a system of basic communications and transactional services that could be called the “eUniversity,” or the electronic, next-generation institution of higher education.

These basic communications and transactional services are part of an emerging definition of “middleware” services that sit between the hardware of the Internet and the learning, research, and administrative applications of the higher education community. In support of the core functions of the academy's eUniversity initiatives and collaborative research challenges, it is critical that middleware provide the fundamental security infrastructure enabling the identification and authorization of individuals or services, providing for confidentiality and privacy, and ensuring integrity of transactions.

There is a strategic requirement, and competitive advantage, for developing mechanisms for secure, collaborative sharing of higher education resources such as online libraries, vendor database services, and advanced research facilities. This secure, interoperable higher education environment requires:

- A broader paradigm of directory services than application-specific solutions
- Comprehensive, scalable methodologies to validate authenticity
- Association of specific validations with pre-specified authorizations – such as matching research applications to quality of service providing needed bandwidth
- Seamless, comprehensive interfaces to integrate all components of the eUniversity and its community of interest

The breadth of scope of these security issues and solution mechanisms requires significant inter-operation in the higher education community, including institutions themselves, state and federal agencies, vendors, and other partners. The Department of Education initiative in student digital signatures, the Internet2 Middleware initiative, the CREN certificate authority pilot, and the Federal PKI Working Group activities reflect an important emphasis on national interoperability. Indeed, State and Federal agencies are enacting legal mandates.

The 1997 *Senate Bill 103 Georgia Electronic Records and Signatures Act* [GERS1997] was established “to authorize the use of electronic signatures instead of written ones and provide for the legal effect of such usage.” Technology solutions for electronic signatures were called for with Senate Bill 103 explicitly amending the Information Technology Policy Act of 1995 in regards pilot implementation projects. Georgia’s *Senate Bill 465*, effective July 1, 2000 continues the call for implementation projects (updating references to a newly created Georgia Technology Authority), recommending:

“All state agencies, authorities, and boards are authorized to establish pilot projects, which are to serve as models for the application of technology such as electronic signatures.... Such projects shall consider both commercial and government applications, [and] be inclusive of major categories of electronic signature technology... The pilot projects are intended to provide a proof of concept for the application of technology, such as electronic signatures, and to serve to educate the General Assembly and the public at large as to the benefits of electronic signatures.... One such pilot project may involve digital signatures and the use of a public key infrastructure established by a service provider.” [GTA2000]

At the Federal level, “*The Government Paperwork Elimination Act (P.L. 105-277, Title XVII)* allows citizens to use electronic technologies when filing information with, or retrieving it from the Federal Government. The Act, was signed into law October 1998, directs Federal agencies to provide public access to government services and documents by 2003 and give the public the option of submitting government forms electronically.” [FECPI1998].

A more recent enactment of federal legislation that has international as well as national implications occurred when President Clinton signed the *Electronic Signatures in Global and National Commerce Act* on June 30, 2000, to be effective October 1, 2000. “This Bill... directs the Department of Commerce to promote the use and acceptance of electronic signatures on an international basis by following certain principles outlined in the bill.” [ESIG1999]

In 1998 Clifford Lynch edited *A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources* for the Coalition for Networked Information [LYNC1998], recognizing the topic of authentication and authorization as increasingly important for inter-institutional interoperability. The white paper's introduction set expectations for cross-organizational progress:

“While considerable work has been done over the last two decades on authentication within institutions and, more recently, in support of consumer-oriented electronic commerce on the Internet, a series of new technical and policy issues emerge in the cross-organizational authentication and access management context. This white paper... is intended to serve several purposes:

- To identify and scope the new issues that emerge in the cross-organizational setting and to provide a framework for analyzing them.
- To map out the various best-practice approaches to solving these problems using existing and emerging technology so that institutions and information providers can make informed choices among the alternatives...
- To provide a common vocabulary and framework to assist in the development of licensing and resource-sharing agreements, and to highlight technical and policy considerations that need to be addressed as part of these business negotiations.
- To lay the foundation for possible follow-on formal or de facto community standards development in access management. If large scale use of networked information resources is to flourish, we need to move away from the specialized case-by-case access management systems... towards... general approaches which will let institutionally-based access management infrastructures interoperate with arbitrary resources.”

Higher education, the Internet community, vendors, and standards groups have devoted significant effort and resources to collaborative discussions, investigations, and pilot implementations of the authentication and authorization infrastructure. Indeed, the environment now is such that practical solutions to security infrastructure should be part of an organization's strategic planning. The purposes stated in the CNI White paper - to investigate issues and map out approaches - have been significantly advanced, if not accomplished. This white paper proposes several new purposes:

- To act on recommendations, roadmaps, and frameworks resulting from ongoing cross-organizational discussions
- To implement informed technology solutions based on best practices which have been piloted and tested
- To leverage the common vocabulary and solution sets that have been discovered and to implement technical and policy models
- To build management infrastructures upon the foundational standards that have emerged.

For Georgia State University, specific directions and detailed action plans must be developed and undertaken regarding establishment of security infrastructure:

- University-wide directory services and metadirectory solutions;
- Public-private key technology;

- Definition of universal account creation, userids and password synchronization;
- Interface to other electronic domains like the “one-card,” library patron, or email systems.

The context of and the success of Georgia State University’s enterprise directory infrastructure work is absolutely dependent on successful collaboration with its community of interest: the University System of Georgia, higher education learning & research, application and technology partners, and government agencies.

### **Industry Analysts Advise Strategic Planning for Directories**

GartnerGroup recommends that clients now move from investigating issues of enterprise directories and actively establish enterprise directory strategies. In GartnerGroup’s Research Note *Business Strategy Will Drive Directory Services* [HAYW1999], the key issue for analysis is “How will enterprise investments in directory technology provide business value while avoiding vendor lock-in and dead-end technologies?”

“Pressures from intranet, extranet and E-commerce applications are increasing the need for an enterprise strategy for directories. This will not be easy to achieve, but tactical solutions will cause greater problems.” [GartnerGroup is] “now recommending that enterprises proactively plan for directory implementation as part of their overall Internet and electronic workplace strategies. Why this change of emphasis? Directories are moving from an incidental support role in workgroup systems toward the core of the required infrastructure.” [HAYW1999]

GartnerGroup notes that clients should pursue a proactive directory strategy and that “Two implementation paths are available: extending a workgroup user repository (from NOS or E-mail system) with additional data to form a fully fledged directory system, or implementing an independent directory solution that will subsequently absorb existing facilities.” Whichever path chosen, GartnerGroup cautions clients to take an open approach:

“Not surprisingly, those vendors which have traditionally provided the former capabilities [NOS based directories] (notably Novell and Microsoft) would have enterprises take that path; other directory vendors would have enterprises take the latter [independent directory path]. Even if enterprises choose to implement a directory solution starting from the NOS directory, GartnerGroup advises them to treat their directory strategy as an independent issue. The fundamentals are a clear analysis of requirements and a flexible architecture to support requirements over the medium term - independent of product choices.” [HAYW1999]

Flexible architecture can be found in open systems technology solutions, such as Lightweight Directory Access Protocol for directories, as well by taking advantage of the significant work already done. For instance, work done by Internet2 Middleware “Early Adopters” group is intended to provide a “roadmap” for other institutions to follow.

This flexibility will also be reflected in an enterprise directory strategy that is not parochial but that considers issues related to an enterprise's extended community of interest. For Georgia State University that community includes the University System of Georgia, higher education learning and research community in general, as well as the State of Georgia and Federal agencies such as the Department of Education, all of which also have strategic interest in enterprise directory infrastructure solutions. As noted in the case of State and Federal agencies, this strategic interest is, in some instances, mandated by law [GTA2000], [FECF1998].

GartnerGroup clearly states its "Bottom Line: Renewed requirements and opportunities for enterprisewide directory services mandate that all enterprises have in place a strategy based on a broad architectural framework independent of product choices." [HAYW1999]

The Burton Group, specializing in helping companies with network infrastructure management, also advocates a strategic approach to directories and to directory enabled application environments that directories can support. The Burton Group recognizes the evolution of enterprise solutions and the business need to blend short-term and long-term strategies to achieve long-term return on investment (ROI). The Burton Group analysis, *Directory-Enabled Computing: The Directory's Expanding Role* [GAUT1999], summarizes its conclusion:

"The term 'directory-enabled computing' defines the directory's role as a significant component of the enterprise computing infrastructure. That role is coming into sharper focus as products mature and the industry consolidates. Organizations once were forced to deal with special-purpose directory technology that isolated information and increased the management burden. Now, however, they can begin to build an enterprise directory infrastructure around general-purpose products... [that] can participate in an integrated enterprise directory infrastructure that reduces management overhead and supports a variety of applications. Customers must invest in and plan for that infrastructure now to take full advantage of these new roles as they mature." [GAUT1999]

The Burton Group's analysis focuses on the enterprise-wide strategies that will result in true ROI and also points out that, just as an individual company can realize benefits from moving from its many directories to a consolidated solution, clearly companies in an industry group should strive to achieve improved ROI: "When e-business emerged as a primary driver for intranet and extranet architectures, however, the need to rationalize directory architecture reached critical mass. Companies need to simplify user and resource management internally while creating a scalable, secure, and manageable e-business infrastructure." [GAUT1999]

The Burton Group foresees that enterprises that adopt a strategic plan for enterprise directory infrastructure will gain industry advantage, since building the infrastructure logically progresses with an increasing ability to leverage the investment. This advantage accrues from the nature of basic directory functions since

“Regardless of the different applications directories can support or the role they’re playing, directories provide a common set of functions that most applications, and the directory itself, use in day-to-day operations. These basic functions are:

- Authentication and authorization
- Naming and locating network resources
- Administering and managing network resources
- Enabling applications

“While no empirical model is ever perfect, these four functional categories are sufficient to define the range of directory-related activities in today’s market. Although there is significant overlap and interdependence between the categories, in general each category represents a progression of sophistication that is dependent on the function of the previous category(s).” [GAUT1999]

The Burton Group’s network strategy analysis on *The Enterprise Directory Value Proposition* [LEWI1999] discusses some specific details on ROI and provides a cost/benefit calculation model and a case study. Using this cost analysis The Burton Group presents a convincing argument that overall a company may realize five times return on enterprise directory investment. The conclusion reached is that

“IT managers can demonstrate the value of, and the return on, an enterprise directory project by quantifying the short-term benefits in terms of dollars, and defining the long-term benefits in terms of strategic initiatives... But those savings will come only through the hard work and significant resource commitments that directory projects require, which includes dealing with dirty directory data and internal politics, both of which can derail directory projects.” [LEWI1999]

The short-term benefits are related to savings accrued from reducing administrative overhead required for managing multiple, disparate directories and from the increasing the quality of data, which reduces costs associated with errors or rechecking or resolving data discrepancies. As to long-term ROI, the analysis observes

“It’s more difficult to measure the long-term benefits, but they’re equally important. Over the long term, the directory will become an essential part of the enterprise computing infrastructure, providing the foundation for a variety of applications and services. E-commerce, extranet, and other distributed applications will not scale without a solid directory foundation.” [LEWI1999]

The challenges to enterprise directory deployment are not insignificant:

“In many cases, directory managers must find ‘dirty’ directory data, and end up mired in lengthy and unexpected information scrubbing exercises. Many customers find the cost and effort of creating a unique directory ID for users tougher than they initially thought. Disorganized directory management processes also can present an obstacle that managers must overcome. Finding authoritative sources for information amongst

a myriad of sources and processes can be difficult. And political difficulties are always a threat... Organizational units and divisions of a company must share the desire to create a unified directory if the project is to succeed.” [LEWI1999]

*The Enterprise Directory Value Proposition* analysis goes on to note that organizations typically look for a “killer” application that can of itself justify an enterprise directory. While such “killer” applications may include white pages, an ecommerce application, or a consolidated human resources directory, The Burton Group cautions:

“While any one of these applications play an important part in any directory project, directory planners must be careful to define a broad context for their directory plans. An enterprise directory is more than just a certificate repository or a glorified phone book. A directory strategy has an impact on many applications, so we often say that the overall integration and unification a general-purpose directory infrastructure enables is the real ‘killer app’ many managers seek.” [LEWI1999]

“Overall integration and unification” is a critical success factor. Both GartnerGroup and The Burton Group analyses of enterprise directories stress the strategic importance of directory infrastructure, especially when designed at the enterprise level. Moreover, the greater degree to which that enterprise level strategy includes consideration of a business’s extended community of partners and those partners’ directory strategies, the greater the potential benefit and competitive advantage that results.

Indeed, this overall “integration and unification” can be seen as the theme of several workshops conducted by The Burton Group for the University System of Georgia. The recommendations from these workshops re-enforce the importance of establishing enterprise directory and PKI strategy within a broader context than just, for instance, within a single institution, or any few University System institutions, alone. A directory workshop in October 1999 and a *Public Key Infrastructure (PKI) Strategy Workshop* [BURT2000] in March 2000 had broad participation, with six institutions and the Board of Regents represented for the University System of Georgia, and additional representatives from Emory University and Emory Health Care.

The PKI Workshop in March 2000 resulted in recommendations being made to the University System, including:

*“Major recommendations*

- The University System must begin implementation of the common directory infrastructure discussed in the October [1999] Directory Services Workshop. The long-term success and scalability of the GLOBE, Banner, PeopleSoft, GALILEO, and GIL applications [see Note 1] are dependent upon this happening immediately....
- Member institutions should not deploy PKI without a clear understanding of their directory plans. And to create scalable and manageable inter-institutional capabilities, the University System must build a directory infrastructure that binds the member institutions to a community, allowing them to view each other as

authoritative sources for information on their own students, faculty, and services.” [BURT2000]

In discussing recommendations related to public key infrastructure, The Burton Group explicitly emphasized the importance of the higher education community and government initiatives in PKI and enterprise directory implementation. “Since it must deal with government agencies, the University System should also monitor the efforts on the part of the Georgia state and federal governments to deploy PKI. The Federal PKI (FPKI) project in particular will provide a resource and its leaders are generally very open to collaboration.” [BURT2000]

### **National Working Groups Address Interoperable Infrastructure**

The pervasive interconnections that the internet enables in higher education naturally models the extensive intercommunications of a community that works together, collaborates on research, shares resources, and offers a learning environment that is characterized by the mobility of not only its student body but also its faculty and administrative professionals. The technology of higher education requires interoperability, especially as the pressures of ecommerce and online learning, research, and administrative environments build. While directories are important foundations for such infrastructures, there are a number of “middleware” services that sit between the Internet per se and the applications which are enabled. Nationally based forums and initiatives have taken on the task of developing interoperability standards for middleware technology infrastructures.

The *Directory Interoperability Forum* was formed in July 1999 with its first meeting September 1999 in Atlanta and reflects the increased vendor interest in advancing overall ecommerce technology infrastructure by collectively addressing interoperability issues.

“The *Directory Interoperability Forum* was formed to accelerate the evolution and adoption of open directory-based applications. The membership of DIF, including directory customers, vendors and Independent Software Vendors (ISVs), are working through existing standards bodies to ensure interoperability and reduce the investment risk for companies doing e-business. Directories are an essential part of the infrastructure necessary to conduct e-business...

“The Directory Forum is interested in helping to advance open directories based on the LDAP standards, to make directories more useable, to help ensure that any application written to utilize an open directory will be able to run with any directory without regard to the supplier, and to make it easy for software developers to create those applications.” [DIFa]

The Directory Forum’s *Advancing Directory Standards White Paper* [DIFb] notes the importance of directories, echoing the observations made by industry analysts such as The Burton Group that an overall directory strategy can reduce the administrative overhead of redundant directories:

“Forrester Research reported that the typical Fortune 1,000 corporation has 181 different directories in the enterprise. The lack of consistent, standard-compliant directory implementations forced developers to build their own. The result is excessive redundancy and cost to customers because each of those directories generally stored and managed application-related information in its own proprietary way. With a standard protocol, information can be used by multiple applications, networks, and systems across a variety of platforms, which can significantly reduce the time-consuming process of updating individual application-side files and directories.” [DIFb]

The membership of the Directory Interoperability Forum at the very least indicates the industry wide concern for finding interoperable solutions. Vendor members include IBM, Novell, Sun/Netscape Alliance, Oracle, DCL, Lotus Development, Critical Path, Unisys, Syntegra, and the list of other members and supporters is over 60. [DIFc]

“[These] members intend to:

- Promote Open Directory Standards
- Collaborate to define, create and implement Software Development Kits ("SDKs")...
- Develop new directory-enabled applications to open directory standards...
- Encourage ISVs to write to open directory standards
- Collaborate with the standards bodies...to advance and mature the definition of open directory standards
- And participate in activities promoting open directory standards.

“Cross-industry support of open directory standards (e.g., LDAP) should help make standard, open directory-based applications a safe investment. Then, as more interoperable applications become available customer confidence should build which in turn can increase market opportunities. [DIFb]

Clearly, the Directory Interoperability Forum members understand the competitive advantage to promoting a standards based approach to directory infrastructure. Of course, Directory Interoperability Forum members understand the bottom line impact of a “save investment” for their customers, and ultimately themselves. The promise of “increase [in] market opportunities” is a strong motivator.

The importance of competitive advantage is equally important in higher education and the implications of ecommerce pushing the boundaries of higher education’s information technology environments is apparent at the highest levels. Zell Miller, former governor of Georgia and recently appointed U.S. Senator, writes in *The Chronicle of Higher Education* on *10 Crucial Things the Next President Should Do for Colleges* [MILL2000]. The next U.S President is encouraged to:

“Recognize the tremendous ramifications of information technology for higher education. John T. Chambers, chief executive officer of the high-tech company Cisco

Systems, recently observed in *The New York Times*, ‘The next big killer application for the Internet is going to be education. Education over the Internet is going to be so big it is going to make e-mail usage look like a rounding error.’

“Although traditional campuses will continue to attract young students who want a residential experience, growth in electronic delivery systems will greatly expand the context of higher education. Such new systems will change the assumptions on which universities and federal and state governments base their decisions about the content, delivery, structure, and financial policies of higher education, as well as the public's expectations of higher education....

“What's more, the development of Internet-based education has removed higher education from the sole possession of traditional colleges and universities, and placed it in the field of open competition.” [MILL2000]

Senator Miller sets the tone of his open letter with no mistaking of the contribution which higher education can make.

“The future clearly belongs to communities that can match innovative ideas that drive technology forward with educated workers who can make something, literally, of those ideas. Both need the research and education that only universities can provide. In our knowledge-based economy, universities form the crucial infrastructure of economic development.” [MILL2000]

The Internet2 Middleware initiative is exactly such a contribution by the higher education research and information technology community, bringing university expertise to bear on solving over arching enterprise infrastructure issues. As one would expect from higher education, the Internet2 Middleware initiative began with several activities in 1999 to define and articulate the interrelationship of specific elements of the eUniversity with IT infrastructure.

“The items included under the heading of middleware differ depending on who is making the list... These categorizations are all centered around sets of tools and data that help applications use networked resources and services...

“Middleware has emerged as a critical second level of the enterprise IT infrastructure. The need for middleware stems from growth in the number of applications, in the customizations within those applications and in the number of locations in our environments. These and other factors now require that a set of core data and services be moved from their multiple instances into a centralized institutional offering...

“Interoperable middleware between organizations is a particular need of higher

The Internet2 Middleware group web site (<http://www.internet2.edu/middleware/>) brings together various information to serve as resources and a “roadmap” for those who are

-

“The early drivers for directories are likely to be campus based applications, but the higher ed and research communities will need interoperability between campuses and standards at several levels. For example, there will likely be needs for standardized naming of directory services so that multicampus applications can do lookups across servers. Schema extensions to accommodate research applications may need to be

installed at participating campuses. Consistent practices in interpreting the contents of standard schema items would insure that meaning was preserved. Campus and multicampus directory issues should be considered in parallel as an institution develops its local services....

“Policy issues -

“The greater difficulties in building a true enterprise-wide directory service in higher ed lies in conducting consensus processes for policy and funding. With their ad hoc data administration environments, many campuses have not crisply defined issues of data ownership and access. A directory project brings all these issues to the fore. Similarly, there are many unresolved issues on directory data concerning privacy, Open Records, FERPA, etc.

“The funding of a directory initiative may also challenge campuses. The cost of a central infrastructure includes multiple servers, development of interfaces to legacy systems, and management of the schema....

“Advocacy of a directory initiative should draw senior leadership as befits infrastructural issues. At the same time, there are some external drivers that can be used to build urgency and importance. Federal initiatives in digital signatures for students, scientific communities need to exchange management data, and licensing of scholarly materials are some of the levers that can be used.” [IMI2000c]

These directory issues speak directly to challenges which Georgia State University faces:

- multi-campus issues with GSU being part of the extended University System of Georgia
- data policy issues that are not yet completely “crisply defined”
- funding challenges
- coordinating University System wide advocacy and staying ahead of government initiatives (State and Federal) which may quickly become mandated

The break out of the Internet2 Middleware definition of “*Certificates* and public-key infrastructures” service also provides a component breakdown that helps chart the PKI activities that Georgia State University should undertake:

“There is considerable interest in the use of X.509 certificates to address a number of network computing needs in higher education. The technology itself is powerful and elegant, but there are several major challenges to the widespread successful use of certificates... A PKI has several components.

- A Certificate Authority (CA), that manages and signs certificates...
- Registration Authorities... that validate users as having been issued certificates
- PKI management tools... to manage revocations, validations and renewals
- Directories to store certificates, public keys, and certificate management information
- Databases and key-management software to store escrowed and archived keys

- Applications that can make use of certificates and can seek validation of others' certificates
- Trust models that extend the realm of secure communications...
- Policies that identify how an institution manages certificates, including legal liabilities and limitations, standards on contents of certificates, and actual campus practices" [IMI2000d]

As intended, the details provided by the Internet2 Middleware site could provide a helpful roadmap to a higher education institution's enterprise directory and public key infrastructures. As well, there is great value in the corroborative validation of one's own local activities that this site provides, given that it has come from a higher ed community interest, and the guidelines offered have effectively undergone a process of peer review and collaborative discussion. Clearly, to recognize and leverage the work already done by organizations like Internet2 Middleware group can contribute to an effective strategy.

CREN, the Corporation for Research and Educational Networking (<http://www.cren.net/>), whose "mission is to support higher education and research organizations with strategic IT knowledge services and communication tools," also provides a number of resources. "On November 17, 1999, CREN deployed a top-level Certificate Authority Service that provides authentication services to CREN's member institutions and other academic and research institutions." [CREN1999] Of particular interest for the University System of Georgia is that Georgia Institute of Technology was one of the three pilot institutions for this service, and as much as we can learn from the efforts of others, certainly others can benefit from the experiences of our institutions.

CREN's Tech Talk series provide additional resources on a range of information technology of topics in higher education (<http://www.cren.net/know/techtalk/topics.html>). These technical dialogues with guest experts cover such topics such as directories, middleware, and campus certificates services and can provide specific insights or perspectives that help clarify details or summarize a topic. In responding to questions from technology anchor Howard Strauss, Keith Hazelton and Ken Klingenstein offered the following comments on *Building Directories: the Fundamentals*, highlighting key tasks in establishing an enterprise-wide directory or "meta-directory":

**“HS:** Why don't we start by ... talking about what services a general purpose, enterprise-wide directory would provide?

**“KH:** ... What we'd really like ... is ... one logical place we could go to ask about all people or any person of interest within our university community ... or roles they might have ... say, a vendor or a contractor or a federal researcher visiting...

**“HS:** ... Does that mean there's one directory on a campus or on a bunch of campuses?

“**KH:** One logical place, meaning from the point of view of the application or the person looking for information ... But no, the information in the back there might very well be federated across several directories and connected up invisibly...

“**KH:** ... [nonetheless] I think I have yet to hear of any institution of higher ed that has that one logical place ... And the reason we don't have it ... is that they [the multiple directories] aren't integrated...

“So the critical function of the directory ... is a directory that does something some of us call **identity reconciliation**. It's pulling all these things together and knowing that Susie Q is or isn't Susan Quinlan, and knowing that in the student system, she's known by an ID, PeopleSoft-Student/Administration-ID-such-and-such, and in the HR she's known as Oracle-Financials-person-such-and-such. And so you can map across those systems of interest within the directory.

“Now, the other term that this person registry ... goes by is the **metadirectory**. ... Stanford University and Bob Morgan in particular are responsible for this very useful notion of a person registry performing that identity reconciliation function...

“**KK:** ... But as we get to literally scores and hundreds of applications on our campus, we don't want to re-enter... all kinds of other information time and time again ... and then worry about whether or not the information per application is fresh.

“So we need to move a lot of this common information from the silos of applications into a general purpose broad infrastructure, and that's part of what directories do. And with that definition, then the scope increases beyond some of the basic information that you might find in the White Pages that's an electronic phone book. [cf. group information, printers, servers, all of these other entities in our computational world, this issue of mobility , PKI and X509 certificates...]”  
[KLIN2000]

In fact, this Tech Talk exchange rather neatly summarizes the basic challenges around building an enterprise directory: the driver to have a logical single directory, the reality that a federated directories model may remain, the necessity to reconcile object identities, and the way the directory scope increases when it becomes an enterprise strategy. It should be noted that while Klingenstein and Hazelton spoke from an institutional perspective, the extrapolation of the discussion to multi-campus, system-wide, or higher education community is obvious.

An earlier CREN Tech Talk with Frank Grewe and Mike LaHaye covered *Directories on Campus: Getting Started*, with similar issues being raised as to the proliferation of existing directories and the goal of an integrated solution. Further, Grew and LaHaye commented on some of the data stewardship and ownership issues - a case where policy resolution is a core underpinning required for any technical solution.

**“HS:** ... do the universities have one LDAP directory or do they have a dozen of them? Or are there any guidelines as to what they should have, or shouldn't?

**“FG:** ... a university may have multiple LDAP directories. Nonetheless, the major thing that everybody will need is a central repository that is sort of the master copy of absolutely everybody. There may, in fact, be LDAP-enabled directories that are subsets of this larger directory, that the data is fed either one direction or another from a larger master copy...

**“HS:** Could we talk a little bit about where the data for the LDAP directory comes from?...

**“FG:** In our situation, the data comes from Human Resources records, ... student records, ... the Alumni Association... But additionally to that, we have various groups that have affiliate-type individuals that they wish to have in the directory, so that we really do not have one central source for everybody in the directory...

**“ML:** And as you're dealing with data source issues, that's one of the largest challenges in deploying a directory.

“As it stands on our campus today, we do get the data feeds out of central repositories. Users can modify that data. We, however, do not push it back to the authoritative source.

**“FG:** In our situation, the main data sources of HR and Student Systems do have Web interfaces for self-service. So our student and staff population can go to those sources and change their home address and this type of information and then we get a feed with that update. They don't make those changes directly to the directory.

“On the other hand, there are attributes that are quite specifically directory owned because there are applications that make rather instantaneous use of them. An example is the e-mail address or the password. Those types of attributes are owned by the directory, and the way our population changes them is directly through the directory interface...

**“HS:** Michael, you said that this whole idea of dealing with the institutional data sources and things was one of the real difficult issues with directories... Why is that so difficult?

**“ML:** They are owners of all the data and you have to make sure that you have the permission to use whatever data you are going to either make publicly available or use for private purposes within applications. Within the university community, registration or privacy issues -- registration data must be protected. And if you are going to publish data, you have to make sure you have the permission of the owner of that data.” [GREW1999]

In this case of policy resolution, a case can probably be made that resolution may come more quickly if the scope is broadened to an enterprise level. Certainly, that will help focus on the governmental and legal constraints that already exist, such as FERPA [FERP1974] or Open Records acts, which should take precedence over local access policies. In deed, such a “top-down” policy approach to data stewardship and ownership may best serve the enterprise and its strategic goals.

In a CREN Tech Talk on *Campus Certificate Authorities*, Jeff Schiller describes his experience at MIT in establishing digital certificate infrastructure. As he describes the set up and use of certificates at MIT, Jeff points out an issue of interoperability and how the CREN Certificate Authority [CREN1999] can provide a solution:

**“JS:** ... if you look at the problem we have here at MIT, we’ve set up our own CA and we’re issuing credentials to our own students and we use it for our own purposes. In fact, every student at MIT, in order to register for classes, has to have a certificate because they authenticate themselves to an online system run by the registrar...

“But the catch is, that's great as long as you’re staying within the MIT campus, but now, what if I wanted to offer ... library access to ... students at another university? Very often, there will be joint agreements between universities to share certain resources. Well, what if we have a service provider that wants to provide access to a whole range of universities? Well, ... I would have to install on my servers the Harvard root CA and then the Princeton root CA and actually, I’ll wind up with I don’t know how many root CAs that I have to know about and if any of them change, I have to be updated....

“So what CREN has done is by establishing a root CA for higher education, we can wind up getting our certificates signed by CREN.” [SCH12000]

The CREN certificate service intermediates between institutions by basically providing assurance that certificates issued by an institution can be trusted, and so an institution can rely on CREN’s services to better manage interoperation of authentication. The CREN Certificate Service is still in formative stages and Jeff was asked to discuss the differences of the “Federal Bridge CA model vs. the traditional root CA model.”

**“JS:** It's hard to explain what the difference is because it’s sort of very subtle. Traditionally,... the root CA usually establishes a policy that governs how inferior CA’s operate. And to be honest with you, that type of let’s enforce policy through the PKI hierarchy only works within an institution where there can be common policy. When we’ve tried in the Internet community ... to have a root CA that dictate what policies institutions have,’ that never works.

[Jeff gives an example of a policy issue that a Registration Authority (RA) may encounter with initially validating identities and issuing certificates. A school’s RA may require in person verification of id before issuing a certificate. This in person verification may work for a smaller institution’s population. However, this policy

would be unacceptable to a large school's RA and result in a different policy standard for issuing a certificate. How do you resolve these two different approaches to verification? Jeff suggests "bridge CAs."]

"Now, when you do these bridge CA schemes, in essence ... you're basically saying, 'We're not setting up a root. We're not in essence propagating merely saying is that we're introducing different CAs to each other.' And that is pretty much what CREN is doing in that it is basically saying to Princeton, 'This is MIT.' And similarly to MIT, 'This is Princeton.' But it's still up to the individual organizations to set up their own policies.

"Now, I believe the Federal PKI Bridge stuff ... is ... more formal than what CREN has been doing ... as they actually required a published policy so that if I get a certificate from a different CA than my own through the bridge, then I should be able [go] to a repository and obtain what the policy that CA in fact used before it issued credentials, so I could know whether or not ... that's an acceptable solution, an  
CHI2000]

As Schiller notes, the Federal Bridge CA is a model, like CREN's CA, that evolved to solve interoperability issues for an extended community, with an added repository capability so that various policies can be inspected. The Burton Group recommended to the University System of Georgia "the Federal PKI (FPKI) project in particular will provide a resource." [BURT2000] Since 1998 the Government Information Technology Services FPKI Steering Committee (<http://gits-sec.treas.gov/oofpkisteer.htm>) has provided leadership in investigation of issues and development of PKI solutions that have been underway since 1994. An extensive set of resources has been provided through the business, legal, and technical working groups addressing public key infrastructure.

One of the PKI Technical working Group subcommittee resources is a *Federal PKI Directory Concept of Operations* [FPKI1999] that describes an integrated technical architecture for PKI infrastructure, enabling the inter-operation of separate directory infrastructures.

"The Federal Public Key Infrastructure (FPKI) is intended to support security services for communication between the public and government employees and between government employees associated with different agencies and organizations. A Federal Bridge Certification Authority (BCA) has been proposed to cross-certify agency and organizational principal certification authorities (PCAs), providing the necessary mapping information to support the verification of certificates between differing trust domains.

"[The document] describes the architecture for a proposed Federal PKI repository, composed of a collection of interconnected directory servers. The paper addresses the interconnectivity of a Federal BCA [Bridge Certificate Authority] directory server with a number of border directory servers providing information on behalf of interconnected trust domains. The paper provides a proposed concept of operation,

examines protection issues, and describes a strategy for the evolution of the Federal PKI Directory.” [FPKI1999]

The concept of border directory has obvious applicability to Georgia State University and the University System of Georgia’s environment, where some mechanism needs to be implemented that enables interoperability while allowing the de facto local autonomy that exists in institutions’ local configuration.

“...Generally, a border directory server is a directory server that has been designated to provide the primary public directory system interface for a trust domain. By providing a separate border directory server, an organization can retain its existing directory infrastructure and still be able to communicate within the Federal PKI.” [FPKI1999]

As an architectural roadmap, the *Federal PKI Directory Concept of Operations* provides guidance that, in conjunction with other resources, permits an enterprise to make sound strategic decisions. The details include definition and functions of Trust Domains, Policy Management Authorities, Certification Authorities, and Directory Servers. An architectural overview outlines how

“Border directory servers will connect via the bridge CA directory server to provide a government-wide certificate management repository. The border directory server will provide each trust domain with a publicly visible repository for certificates, certification revocation information, and certification practice statements...” [FPKI1999]

The document goes on to provide example configurations for different levels of trust, how the directory information is protected, operational considerations, directory integrity, directory management as to availability, key management, and unique user identification, and shadowing and replication. Importantly, the Federal PKI recognizes that the process of implementing a PKI directory infrastructure is evolutionary and that organizations may require incremental solutions or even the option of subscribing via an out-sourced border directory service. Three models of implementation that accommodate various levels of readiness are described:

“The Federal PKI Directory will be an evolutionary enterprise. The initial BCA directory implementation will support the following three models of client access:

1. The client accesses its internal directory server as is done today (i.e., via whatever mechanism is currently in place). The internal server chains to its border directory server, which chains to the BCA directory server, which may continue the chain as necessary.
2. The client accesses its internal directory server as is done today. The internal server chains directly to the BCA directory server, which may continue the chains as necessary.

3. The client accesses its internal directory server using LDAP v3. If the server does not have the data, it returns a referral to the client. The referral may identify the BCA directory server or one or more border directory servers or both....

“The goal is to provide a border directory server to host each agency’s externally accessible certificate information. This does not, however, mean that each trust domain is expected to ‘stand up’ its own border directory server. Some trust domains have indicated a willingness to host the certificate information for ‘subscriber’ trust domains on their border directory server. Such subscriber agreements could help in populating the Federal PKI Directory in the near term. Alternatively, a trust domain could engage an external contractor to provide the border directory server service on their behalf.” [FPKI1999]

An important note on the Federal Bridge Certificate Authority is the participation of Georgia Tech Research Institute in the Technical Working Group. In April 2000 the Technical Working Group conducted *The FBCA Testing and the EMA Challenge* [POLK2000] with the goal being to demonstrate support of interagency PKI interoperability with respect to both technical and policy interoperability. Georgia Tech Research Institute participated as a node in that successful demonstration, and provides the University System of Georgia with a readily available resource reference for PKI solutions it seeks.

### **Conclusion**

The importance of an enterprise infrastructure to support the eUniversity is recognized. Industry analysts have well researched and documented justifications for their recommendation that enterprise directory strategies can indeed result in significant returns on investment. State and Federal governments are moving to mandating that organizations and businesses provided secure online environments for business transactions. The higher education community has been in the forefront of research and development of technical and policy solutions and continues to participate at a national level in collaborating on solutions. The Internet2 Middleware initiative and the Federal PKI Technical Working Group are among those that are laying out roadmaps and guidelines for technical implementations.

These technical implementations are achievable, practical, and sound investments and it is not surprising that the Georgia Technology Authority is among those actively calling for strategic investments in pilot implementations and demonstrations. Georgia State University should leverage its community relations with the University System of Georgia and higher education to implement practical solutions to enterprise PKI directory infrastructures.

## **NOTE 1**

GLOBE, Banner, PeopleSoft, GALILEO, and GIL are State wide, or University System wide, enterprise information technology application initiatives in Georgia:

### **GLOBE**

“Georgia G.L.O.B.E. (Global Learning Online for Business and Education) is an administrative office of the Board of Regents and of the University System of Georgia (USG). Georgia G.L.O.B.E. markets online courses and telecourses offered by several USG Affiliate institutions. Through its Web site, Georgia G.L.O.B.E. provides convenient access to a variety of support services for students.

“Georgia G.L.O.B.E. is not a college or university. Students who enroll in courses or degree programs marketed by Georgia G.L.O.B.E. earn their credits and degrees from one of the public colleges and universities that comprise the [University System of Georgia](#). The colleges and universities are accredited by the Southern Association of Colleges and Universities.

“Designed for students who cannot attend traditional classes on a college campus, Georgia G.L.O.B.E. offers new educational opportunities through distance education.”  
<http://www.georgiaglobe.org/>

### **Banner**

Banner is the University System of Georgia implementation of Systems & Computer Technology Corporation’s BANNER application suite for Student, Financial Aid, and Alumni Development functions. (<http://www.usg.edu/cgi-bin/sfa.pl>)

### **PeopleSoft**

“The Georgia *FIRST* Project, by implementing PeopleSoft's HR Payroll and Financial Systems, will support the mission of the University System of Georgia, empower individuals, promote innovative changes, and support the creation of effective partnerships among USG institutions.” (<http://www.usg.edu/gafirst/>)

### **GALILEO**

“GALILEO [Georgia Library Learning Online] is an [award-winning](#) initiative of the University System of Georgia initially funded by Governor Miller and the General Assembly in 1995, with continuing funding from Governor Barnes and the General Assembly for the Citizens of Georgia.” (<http://www.galileo.peachnet.edu/cgi-bin/homepage.cgi>)

### **GIL**

“GALILEO Interconnected Libraries, or GIL, is an extension of the GALILEO initiative funded by the Governor and the General Assembly of the state of Georgia to enhance and expand educational opportunities for the citizens of Georgia. The successes that GALILEO has had in leveling the information access opportunities for the citizens of Georgia are being extended to University System's Libraries through GIL by providing

students, faculty and staff expanded access to the information resources of the University System's Libraries...

“GIL will offer a gateway to information resources held in the University System of Georgia (USG) libraries... The addition of a single integrated library automation system to GALILEO will make online access even easier for patrons and staff. GIL will integrate into one system, a web-based online union catalog of all the book collections of the University System (over six million volumes - 60% of the titles are unique), a circulation system with self-service options, fund accounting, cataloging, and check-in and control functions.” (<http://gil.peachnet.edu/>)

## REFERENCES

- [BURT2000] *Public Key Infrastructure (PKI) Strategy Workshop Summary Observations and Recommendations*, The Burton Group, Prepared for the University System of Georgia, March 22, 2000.
- [CREN1999] *Certificate Authority Service*, <http://www.cren.net/ca/index.html>.
- [DIFa] *Introducing the Directory Interoperability Forum*, The Directory Interoperability Forum, <http://www.directoryforum.org/>.
- [DIFb] *Advancing Directory Standards White Paper*, The Directory Interoperability Forum, <http://www.directoryforum.org/whitepaper.html>.
- [DIFc] *Membership*, The Directory Interoperability Forum, <http://www.directoryforum.org/membership.html>.
- [ESIG2000] *Electronic Signatures in Global and National Commerce Act (1999 House Bill 1714)*, <http://www.mbc.com/ecommerce/legis/congress.html#hb1714>.
- [FECF1998] *Government Paperwork Elimination Act*, Federal Electronic Commerce Program Office, 1999, <http://ec.fed.gov/gpea.htm>.
- [FERP1974] *Family Educational Rights and Privacy Act (FERPA)*, U.S. Department of Education, <http://www.ed.gov/offices/OM/fpco/ferpalist.html>.
- [FPKI1999] *Federal PKI Directory Concept of Operations*, Cygnacom Solutions, National Institute of Standards and Technology, Public Key Infrastructure Program, PKI Technical Working Group, 20 April 1999, <http://csrc.nist.gov/pki/twg/papers/twg-99-29.pdf>.
- [GAUT1999] Gauthier, L. *Directory-Enabled Computing: The Directory's Expanding Role*, The Burton Group, Research & Advisory Services, Network Strategy Service, v2, 28 Dec 1999, <http://www.tbgroup.com/content/OVERVIEW.asp?DocID=80>.
- [GERS1997] *Senate Bill 103 Georgia Electronic Records and Signatures Act*, 22 April 1997, [http://www.cc.emory.edu/BUSINESS/digital\\_signature\\_draft.html](http://www.cc.emory.edu/BUSINESS/digital_signature_draft.html).
- [GREW1999] Grewe, F., M. LaHaye. *Directories on Campus: Getting Started*, CREN Knowledge Services, Tech Talk, 4 November 1999, <http://www.cren.net/know/techtalk/events/getstarted.html>.
- [GTA2000] *Senate Bill 465 Georgia Technology Authority - GeorgiaNet Division*, <http://www.state.ga.us/cgi-bin/pub/leg/legdoc?billname=1999/SB465&docpart=full>.

[HAYW1999] Hayward, S., J. Graff, N. MacDonald. *Business Strategy Will Drive Directory Services*, The GartnerGroup, Tactical Guidelines, TG-07-4615, Research Note, 11 March 1999.

[IMI2000a] *Overview of Middleware*, Internet2 Middleware Initiative, 2000, <http://www.internet2.edu/middleware/overview/>.

[IMI2000b] *Core Middleware*, Internet2 Middleware Initiative, 2000, <http://www.internet2.edu/middleware/core/>.

[IMI2000c] *Directories*, Internet2 Middleware Initiative, 2000, <http://www.internet2.edu/middleware/core/directories.shtml>.

[IMI2000d] *Certificates and PKI*, Internet2 Middleware Initiative, 2000, <http://www.internet2.edu/middleware/core/certificates.shtml>.

[KLIN2000] Klingenstein, K., K. Hazelton. *Building Directories: The Fundamentals*, CREN Knowledge Services, Tech Talk, 17 February 2000, <http://www.cren.net/know/techtalk/events/directauthen.html>.

[LEWI1999] Lewis, J., D. Blum, G. Rowe. *The Enterprise Directory Value Proposition*, The Burton Group, Research & Advisory Services, Network Strategy Service, v1, 23 Feb 1999, <http://www.tbgroup.com/content/Overview.asp?DocID=89>.

[LYNC1998] Lynch, C., editor. *A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources*, Coalition for Networked Information, revised discussion draft of 14 April 1998, <http://www.cni.org/projects/authentication/authentication-wp.html>.

[MILL2000] Miller, Z. *10 Crucial Things the Next President Should Do for Colleges*, The Chronicle of Higher Education, 14 July 2000, p. B4, <http://chronicle.com/weekly/v46/i45/45b00401.htm>.

[POLK2000] Polk, T. *The FBCA Testing and the EMA Challenge*, TWG Meeting Report: 11 May 2000, <http://csrc.nist.gov/pki/twg/y2000/presentations/twg-00-19.pdf>.

[SCHI2000] Schiller, J. *Campus Certificate Authorities*, CREN Knowledge Services, Tech Talk, 13 April 2000, <http://www.cren.net/know/techtalk/events/cca2000.html>.