The U.S. Federal PKI and the Federal Bridge Certification Authority

Peter Alterman, Ph.D.
Senior Advisor to the Chair, Federal PKI Steering Committee and
Acting Director, Federal Bridge Certification Authority

1. The U. S. Federal PKI

The goals of the U.S. Federal PKI are to create a cross-governmental, ubiquitous, interoperable Public Key Infrastructure and the development and use of applications which employ that PKI in support of Agency business processes. In addition, the U.S. Federal PKI must interoperate with State governments and with other national governments. Our goals recognize that the purpose of deploying a PKI is to provide secure electronic government services utilizing Internet technology, not only to satisfy the little hearts of a dedicated cadre of techno-nerds and paranoiac security gurus but to serve the citizenry.

While it is fair to say that PKI technology today is powerful and deployable, nobody who is even the least familiar with it would claim that it is simple and straightforward to implement, let alone structure an aggregation of PKIs. Which leads us to ask the question: Why a U.S. Federal PKI?

The simple answer is that U.S. Federal Agencies are mandated by the Government Paperwork Elimination Act of 1998 to begin providing electronic government services by October 21, 2003. While this Act does not require us to implement PKI – the law is technology neutral – it is clear that PKI, especially coupled with biometrics and hardware tokens, offers higher levels of identity security than can be provided by handwritten signatures or any other electronic signature alternative at the present time. For a good, brief comparison of electronic signature alternatives currently available I recommend that you look at the guidance provided by the U.S. Office of Management and Budget for the Government Paperwork Elimination Act. (Links to this and all other U.S. Government PKI-related documents may be found at either the Federal Public Key Infrastructure Steering Committee website, http://www.cio.gov/fpkisc or at the PKI website of the National Institute of Standards and Technology (NIST) at http://csrc.nist.gov/pki.)

If you look behind the bureaucracy of the Act – and of several like bills under consideration by the U.S. Congress at the present time – you discover that there is a strong belief on the part of legislators and economists that government productivity may be dramatically improved by replacing people and paper processes with electronic processes. While there is much truth to this assumption, we must be candid and admit that the transition to electronic processes entails substantial investments of time and money, especially where we are implementing a new technology that is unfamiliar and complex, and which challenges preconceptions about law and security. Nevertheless, the public wants more and better government services at lower cost with greater security, and for all practical purposes only electronic government, with security provided by PKI (and in some cases by other means) can hope to satisfy those requirements.

Notwithstanding privacy concerns, the public increasingly buys products and services on the Internet. In many U.S. States, drivers' licenses may be renewed on the

Internet. What was once a novelty has rapidly become an expectation; that is, the citizen who only a year ago may have marveled at her ability to buy books and music on the Internet now takes it for granted that she can pay her bills and conduct her banking on line at two o'clock in the morning, and she is impatient to receive all her government services the same way. Early successes breed increasingly great expectations of technology, and since the cost and complexity required to satisfy such expectations are invisible to the end-user, they become impatient and intolerant of delays. The phenomenon is well-known and has been documented frequently in a variety of professional and popular journals.

The success of electronic business has given birth to a category of regulatory requirements – for guaranteeing personal privacy, ensuring information security, combating identity theft, establishing standards for encouraging business interoperability, and more. E-government is an inevitable consequence of e-business. Furthermore, other nations, notably those of the European Union, are moving steadily towards electronic government and the U.S. must be able to function as a member of the international community in that venue, as well.

Given these reasons to field a PKI, we must also acknowledge that there are strong arguments against fielding a U.S. Federal PKI, especially under a single root. The first and foremost of these is the active opposition of privacy advocates, who see in a U.S. Federal PKI a significant challenge to individual privacy. They believe that issuance of a single electronic identity document will enable the government to aggregate too much personal information in a single place and make that information available to Agencies with power to do much harm. These advocates acknowledge, however, that just such a circumstance is already occurring in the private sector business marketing environment, where on-line firms, credit card companies, banks and even spyware-enabled websites are aggregating personal information into data banks used to try to sell ever more goods and services. It may be that privacy advocates focus on government PKI initiatives because such efforts are visible and the entity responsible can be identified easily. Attacking marketing firms that aggregate personal data is much more difficult since they maintain as much anonymity as they can. This situation is changing, of course. The first gun of that battle in the U.S. was fired by Congress in passing a modest law to prevent websites and online businesses from collecting data about children under twelve years old, but many European nations have had strong privacy protections for several years now.

An argument against fielding a U.S. PKI under a single root is Federal Agencies' opposition to participating in a single PKI run by an entity other than themselves. Many fear operation of a PKI run by one of the security Agencies of the U.S. Government, an early initiative, or one run by the U.S. Postal Service – another early option recently revived as a strategic direction in light of the ongoing decline in first class mail volume. Putting aside the argument for national defense and security bruited by the Departments of Defense, State and Justice, the problem is that many Agencies insist that a PKI run by another Agency cannot possibly satisfy their unique, mission-based requirements. Whether this is true or not isn't the point. The point is, most Agencies refuse to allow another Agency to run their PKIs for them. This is a fact of bureaucratic life.

A third argument against a single U.S. Federal PKI is vendor concern. In the absence of a single, dominant PKI vendor, the ongoing battle for market share would be

over if the U.S. were to do what the Government of Canada did and select a single vendor for a government-wide PKI. To the vendor community, the potential benefits of such a huge win are far outweighed by the disastrous probability of losing such a competition. It is just too much of a gamble for vendors to support a single U.S. Federal PKI, and that being the case they don't lobby Congress to force Agencies' hands by mandating one.

Finally, arguing against implementing a U.S. PKI, single or not, is cost. While there are statutory requirements for implementing electronic government services using electronic signature technologies, Congress has not appropriated new funds to support such initiatives. Agencies must implement their e-government initiatives within their existing budgets. This immediately suggests that the cheapest solution will be the most popular, and PKI is not by any means the cheapest solution, only the most secure (although rumors of the high cost of deploying digital signature technology have been overstated). In fact, the earliest Federal e-government initiatives in the U.S. have not been PKI-based, but have used the PIN-Password alternative. This follows the model familiar to the American public from automated teller machines, network and ISP logons.

Nevertheless, a U.S. Federal PKI there must be. There are simply too many requirements for high-security, high-assurance applications in government that the PIN-Password approach cannot satisfy. Thus, the challenge has been to design and deploy a U.S. Federal PKI given the requirements and constraints noted above.

2. The Federal Bridge Certification Authority

The solution we've come up with, as much political as technical, is to create a consolidated PKI infrastructure consisting of discrete Federal Agency PKIs interoperating through a *non-hierarchical* Bridge certification authority (or CA). Known as the Federal Bridge CA and following a hub-and-spoke model, it sits at the center of the U.S. Federal PKI design architecture. It has been created using commercial, off-the-shelf products with some special code written to allow different CA products to cross-certify and interoperate within the "membrane" of the Bridge CA.

The Federal Bridge CA does not operate as a root. It does not issues certificates to subordinate CAs or relying parties. Rather, it exchanges a pair of cross-certificates with each participating Federal Agency CA. It has been designed to create trust paths among the individual Federal Agency PKIs. Technically, the Bridge CA is composed of multiple commercial CAs with their directories that cross-certify and interoperate within a "membrane." These CAs are offline, having no network connectivity. The CAs issue certificates to each other which include multiple policy Object Identifiers. The CAs are connected to the networked directory via sneakernet. The Bridge CA directory is maintained online 24 hours a day, 7 days a week, every day of the year. The whole is secured physically and logically and requires two persons for access.

(FPKI snapshot.jpg goes here)

By employing a voluntary, distributed, non-hierarchical architecture, the Federal Bridge CA forges a single PKI out of a multitude of discrete PKIs. Thus, it neatly sidesteps the political problems of trying to field a single authoritative government CA from which all other Federal government CAs would acquire their legitimacy. And while this model quite possibly increases the overall cost of the aggregate entity PKI, it spreads the cost out among a large number of budgets, making it possible to stand up the whole

piece by piece as local funding and local will appear. In this model vendors of PKI products have a larger pool of potential customers with a ready requirement for their products and services and a side effect of this situation is that vendors are each eager either to be incorporated into the Bridge CA "membrane" or to demonstrate that their products may interoperate with those CA products that are in the "membrane." Since products that are incorporated into the "membrane" are required to demonstrate their ability to cross-certify and to interoperate with each other, the Bridge CA fosters the overall adoption of PKI standards and the PKI customers' need for product interoperability. This is a significant benefit for all current and future users of PKI products and services.

The specific goals of the Bridge CA – all U.S. Federal Government initiatives have to have clearly-defined goals that may be measured – are, as previously noted, to leverage the emerging Federal Agency PKIs to create a unified Federal PKI, to limit workload on Agency CA staff, to support Agencies' use of any FIPS-approved cryptographic algorithm and a broad range of commercial CA products, and to propagate policy information to certificate users in different Federal Agencies.

The Federal Bridge CA offers three services: policy mapping, cross-certification and interoperability. Federal Agencies may choose to cross-certify with the Bridge CA or not; participation is entirely optional. However, the technical and administrative advantages of cross-certifying with the Federal Bridge CA are compelling to Federal Agencies and we know that most of them are working towards putting up PKIs that will cross-certify with it.

The benefits of a bridge model over a mesh model are intuitively obvious. Without a bridge model, that is, in a mesh, four CAs would have to create six separate cross-certificate paths, six CAs would have to create fourteen separate cross-certificate paths, and so forth. Replacing the mesh with a centrally-located bridge means that four CAs require only four cross-certificate paths, six CAs require six, and so forth. At any number over three CAs, a bridge model significantly reduces the complexity of cross-certificate paths. When considering the number of Federal Agencies planning to set up PKIs, a mesh would be impossible to maintain. A bridge, however, can easily handle the required number of cross-certification paths.

The Federal Bridge CA offers three services: policy mapping, cross-certification and interoperability. Federal Agencies may choose to cross-certify with the Bridge CA or not; participation is entirely optional. However, the technical and administrative advantages of cross-certifying with the Federal Bridge CA are compelling to Federal Agencies and we know that most of them are working towards putting up PKIs that will cross-certify with it.

Policy mapping is done by a subcommittee of the Federal PKI Policy Authority, another inter-governmental body created to oversee the policy operations of the Federal Bridge CA. This is the domain of the security wonks, policy analysts and lawyers.

(policy mapping example.jpg goes here)

As noted before, code running on the Bridge CA servers facilitates interoperability among the disparate products within. The software library developed for this purpose is freely available upon request.

A fundamental service of the Bridge CA is to ensure directory compatibility, and in fact some of the thorniest issues the Bridge CA team has had to deal with have revolved

around directory issues. This is not surprising, since PKI and directory services are intimately intertwined. The Bridge CA directory architecture consists of chained X.500 directories, of which the multi-rooted FBCA directory is the hub. LDAP is supported for non-X.500 directories through a border directory server interoperating with the X.500 directories through a firewall, and we expect that this will come to be the predominant directory approach in the near future. The following X.500 naming components are used: dc=gov, o=U.S. Government, and c=US. For all other technical specifications, please see our websites, whose addresses have already been noted, above.

Operationally, remember that the Bridge CA issues certificates to participating Federal CAs only. It issues no end-user certificates, that is, certificates to individuals. We expect to issue well under three hundred certificates in the near and mid-term future, and maybe never more than this number. It will not even issue certificates to the Federal PKI Steering Committee, which oversees Bridge CA development and operations.

It is true that all Federal business processes must reach out beyond other Federal Agencies to private industry, other governments and to the general public. We envision a PKI infrastructure where the Federal Bridge CA interoperates with other Bridge CAs serving business sectors such as the health care industry, higher education and other governmental entities. We are already working closely with the health care sector and the higher education sector to create interoperable PKI services.

Interoperability with the general public will come at first through relationships individuals have with Federal Agencies, most likely through use of digital certificates issued through the General Services Administration's Access Certificates for Electronic Services (ACES) for acquiring PKI products and services. This program offers U. S. Federal Agencies a method for issuing basic-level digital certificates free to the public for supporting secure electronic transactions. The Federal Bridge CA is working to ensure that it can interoperate with the vendors supplying CA services and digital certificates through this mechanism. It is quite likely that other emerging mechanisms for granting digital certificates to the public are bound to appear and the U.S. Federal government will have to be able to interoperate with those mechanisms.

The Bridge CA has been running in prototype mode for about a year with the Entrust and Cybertrust CAs inside the Bridge "membrane," that is, with these CA products interoperating within the Bridge hardware environment. Along with a Baltimore CA, this configuration successfully demonstrated interoperability in exchanging secure electronic mail at the 2000 EMA Challenge. Since then we are actively working to get other CAs into the "membrane." We expect to have between four and six separate CA products interoperating within the Bridge CA before the end of this year.

3. The Federal PKI Policy Authority

While overall responsibility for the Bridge CA falls to the Federal PKI Steering Committee, direct policy and management oversight of it is the responsibility of the Federal PKI Policy Authority. This body, consisting of voting representatives of all Federal Agencies who have cross-certified with the Bridge CA. The charter members of the Policy Authority are the Office of Management and Budget, which has overall management oversight for intergovernmental information technology management issues

for the U.S. Federal Government; the Department of Defense for the usual reasons, but also including their expertise in digital security; the Department of Justice, which has overall responsibility for the legal framework under which the Federal Agencies operate; the National Institute of Standards and Technology, which in the U.S. is pre-eminent in PKI technology and standards issues for digital cryptography; the Department of the Treasury, that volunteered up the chair of the Policy Authority and that, after all, prints our money; and the General Services Administration, whose mission is to provide overarching services to all Federal Agencies, and that is staffing the Bridge Operational Authority, the team that is actually deploying and operating the hardware and software.

The Policy Authority determines which Agencies may participate in the Bridge CA and the assurance levels of cross-certification for each member CA. This is done through policy mapping, in which a candidate Agency's Certificate Policy and Certification Practices Statement are evaluated against the Bridge CA's Certificate Policy and Certification Practices Statement. The purpose of this is to evaluate the strength of identity binding and the relative security of the candidate's CA and to map the various levels of assurance of their certificates (high, medium, basic, rudimentary) to other Agencies' certificates so that they may interoperate at mutually-understood levels of trust. The Policy Authority administers the Bridge CA's Certificate Policy and votes on changes to it and to the Certification Practices Statement.

I have already noted that policy mapping imposes a de facto standard on Federal Agencies for defining levels of strength of digital certificates. This is one of the broad benefits of the Federal PKI architecture to the whole PKI community.

The Policy Authority enforces compliance by member Agencies. It reviews annual audits of the operations of the member CAs and has the authority to revoke certificates issued to them at any time if they operate contrary to their stated Certificate Policies and Certification Practices Statements. The Policy Authority will also revoke the certificate of any CA whose private key has been compromised.

4. Current Status and A Look Ahead

The Bridge CA and the interoperability lab are operational. The Entrust CA product has been certified to operate within the "membrane." We are currently testing additional CA products for interoperability and we expect them to be included in the "membrane" soon. We have approved the designs, completed the Certificate Policy – Certification Practices Statement compliance audit, the Systems Security Plan is complete and the hardware and software of the production Bridge CA are working. We have already begun working on the first set of enhancements to the Bridge CA and we are already planning numerous technical enhancements to improve online performance and capability. We have already begun to address the need to simplify utilization of the Bridge CA. Although we have been working with the private sector for the last two years to encourage them to design into their desktop clients software that can utilize the Bridge CA, we want to do more to make desktop clients more Bridge-aware and we have specific plans for funding such initiatives.

The first two Agencies to cross-certify with the Bridge are expected to be the National Aeronautics and Space Administration and the National Finance Center of the

U.S. Department of Agriculture, which provides interagency financial management services to client Agencies.

Although it may be premature, I'd like to take a moment to look ahead a bit and share with you a vision of the future of PKI in the U.S. Let me preface this by telling you that back in 1976 I wrote a foreword to a collection of science-fiction stories entitled *2076: The American Tricentennial,* in which I predicted that we would have fusion-based electrical power within five years. Since not a single tokamak has come on line in the 25 years since I made that prediction, take my comments for what they're worth. First, I think it is inevitable that within the near future PKI will become a transparent part of the computing infrastructure. Second, I think that the PKI infrastructure of the future will consist of webs of interconnected bridges, switches and directories, with directory interoperability an inevitable feature of the worldwide computing infrastructure. Third, it is not unlikely that current PKI technology will be superceded before it is refined. Finally, I think we will see evolving invisible authentication mechanisms within the operating systems on our desktops, the infrastructures on our Local Area Networks, on the Internet and the successors to the Internet. We've seen the evolution of fundamental services from the applications layer to the infrastructure before, and in this recursive universe of ours, patterns repeat.

In as little as ten years, engineers, computer scientists and users will wonder what all the fuss about PKI was back at the turn of the millennium. With luck, we will still be around to explain it all to them.