PRELIMINARY DRAFT

W. E. Burr
19 May 1998
TWG-98-29

Proposed Federal PKI Architecture

Introduction

This is a preliminary draft that outlines a revised architecture for a Federal PKI. It is a significant change to the architecture proposed in the present CONOPS document, and is intended to allow the federal PKI to be assembled, largely bottom up, from the many different certificate based systems that are now coming into use in various departments and agencies.

Discussion

There are now a considerable number of more or less independent efforts in Federal agencies to set up independent CAs to support individual applications. In most cases, the cost of setting up and operating the CA(s) is born by some application that supports the agency mission, such as purchasing, grants, or travel, etc. and the use of public key technology must be justified in terms of its direct benefit to that agency application. In other cases the government will use commercial CA service providers to issue certificates to the public, to facilitate delivering services to the public, and the cost will be born by the various agency projects that rely upon those certificates. In the absence of a separately budgeted Federal PKI program, this is the approach we must use. But relatively little thought is generally given to broader government-wide PKI needs, and the systems that are set up do not generally facilitate interagency operation, or the creation of a broader national PKI.

The situation is analogous to the early days of Local Area Networks (LANs). LANs were initially installed in Federal Agencies and in businesses to support a small set of local applications that were fairly easy to implement and brought an immediate return, such as a substitute for terminal concentrators, for print and file servers, for local e-mail and the like. Several very effective LAN protocols came into wide use, such as NETBIOS and IPX, however these protocols did not scale well to large networks. In the end, however, as Bob Metcalf observed, it became apparent that the utility of networks is a function of the number of users on the network, and as useful as a LAN is, its greatest benefit is as an efficient connection to a wide area network. So the LANs were connected to the Internet, and, by and large, the Internet TCP/IP protocols have replaced the LAN oriented protocols; we now often talk to our print server in the room next door, using the same protocols that we use to communicate with our colleagues in Australia.

It seems quite apparent that there are similar benefits to a system that propagates trust not just in the local environment, but throughout the entire Federal Government, the nation, and the world. Trust in a PKI propagates through certification paths. Given that many, often quite different systems that use certificates are now being implemented by agencies, how do we create certification paths between them, in a sufficiently consistent and coherent fashion, to allow reasonably reliable and broad propagation of trust?

I propose that we should simply offer agencies with CAs the opportunity to cross certify with what I am calling a Federal Bridge CA. (BCA). The BCA is not a root CA, in that it does not start certification paths, it simply connects what I am calling “trust domains” through cross certificate pairs to a designated “principal CA” in that trust domain. It is a “bridge of trust.” The BCA would be operated by a Federal Policy Management Authority (FPMA), which would establish the requirements for cross certifying with the BCA. These trust domains might be within the government or outside the government.

As a further aid to trust propagation (i.e., certification path creation and validation), the BCA would maintain a repository that focuses on CA certificates, and the BCA would issue an indirect CRL that covers all the CAs in the Federal PKI (the Federal PKI being defined simply as all the CAs within the Federal trust domains that cross certify with the BCA). The total number of certificates issued by the BCA should be quite modest, and the total number of CA certificates not large, so the repository database would not be big. CA certificates should not be nearly as volatile as end-entity certificates (although their validity periods will be larger), so the consolidated CA CRL for the Federal PKI should remain fairly small. The BCA repository would then be a key resource for creating and validating certification paths, and would have high availability requirements, medium bandwidth requirements, and low storage requirements.

Another possibility, that I have not yet proposed, is a BCA OCSP responder for Federal CA certificates. If the OCSP standard progresses and becomes popular, then the BCA could also operate an OCSP responder for CA certificates.

The intention of this proposal is to embrace as many PKI approaches as we can get to work together (hierarchical, mesh, and large scale web oriented commercial CA oriented approaches), as well as we can arrange. Given the limitations of current PKI clients, the existence of certification paths does not guarantee interoperability, but it is a necessary precondition.

Architecture Components

The certification path elements of the proposed architecture are illustrated in Figure 1. The complete architecture is composed of the following components:

- **Federal Policy Management Authority (FPMA)**: this management authority sets the overall

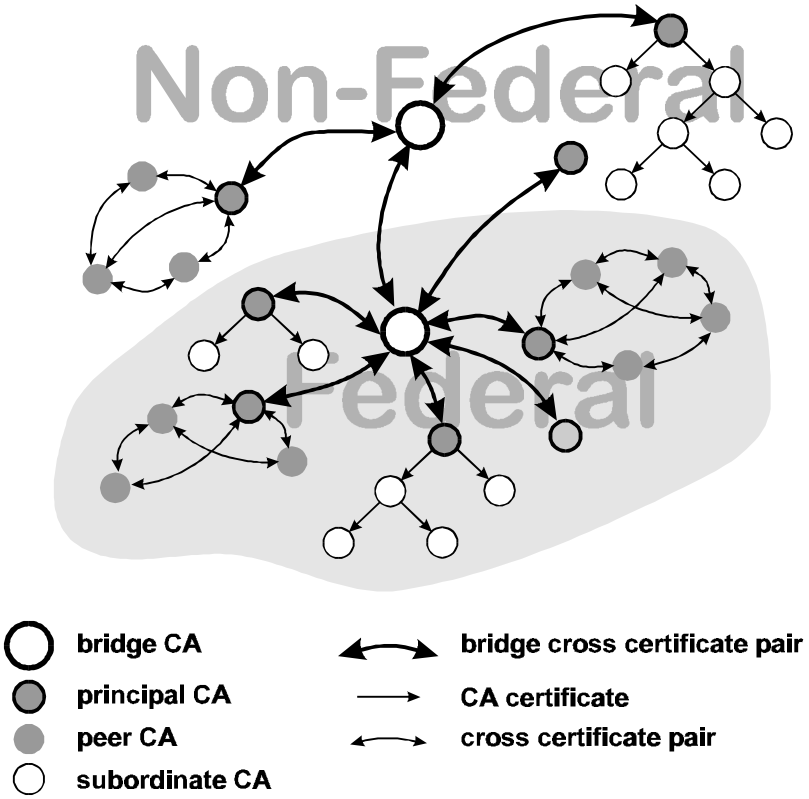

Figure 1 - Proposed Federal PKI Certification Path Architecture

policies of the Federal PKI, and approves the policies and procedures of trust domains within the federal PKI. It operates a Federal Bridge CA, and repository;

- **Trust Domains**: In the Federal context a trust domain is a portion of the Federal PKI that operates under the management of a single *policy management authority*. One or more Certification Authorities exist within the trust domain. Each trust domain has a single *principal CA*, but may have many other CAs. Each trust domain has a domain repository. In the non-Federal Context, trust domains, may be more loosely organized, but consist at a minimum of a group of CAs that share trust and operate under consistent policies.
- **Domain Policy Management Authorities (DPMA)**: a policy management authority approves the certification practice statements of the CAs within a trust domain, and monitors their operation. The DPMAs operate or supervise a domain repository. In the non-federal context, a DPMA may be an association of CAs that share trust and use consistent or comparable CA policies;
- **Certification Authorities (CA)**:
  - **Bridge CA (BCA)**: the Federal Bridge CA is operated by the Federal Policy Management Authority.[1] Its purpose is to be a bridge of trust that provide trust paths between the various trust domains of the Federal PKI, as well as between the Federal PKI and non-federal trust domains. Trust domains that operate with policies and practices that are approved by theFPMA, designate a principal CA that is eligible to cross-certify with the Federal BCA. Note that the BCA is not a *root CA*, since it does not ordinarily begin certification paths. When the BCA cross certifies with CAs it may include nameConstraints, pathLengthConstraints or policyConstraints that limit the propagation of trust to other, cross-certified domains. The BCA also issues a consolidated Federal CA CRL;
  - **Principal CA**: A CA within a trust domain that cross-certifies with the Federal BCA. Each trust domain has one principal CA. In the case of a domain with hierarchical certification paths it will be the root CA of the domain. In the case of a domain with mesh certification paths, the principal CA may be any CA in the domain, however it will normally be one operated by, or associated with, the domain policy management authority;
  - **Peer CA**: A CA in a mesh domain, that has a self-signed certificate which is distributed to its certificate holders, and which is used by them to start certification paths. Peer CAs cross-certify with other CAs in their trust domain;
  - **Root CA**: In a hierarchical trust domain, the CA that starts all trust paths. In the hierarchical domain, certificate holders and relying parties are given the self-signed root CA certificate, by some authenticated, out-of-band means, and start all trust paths from that point. For hierarchical trust domains the root CA is also the principle CA for that domain;
  - **Subordinate CA**: A CA in a hierarchical domain that does not begin trust paths; rather trust starts from some root CA. In a hierarchical trust domain, a subordinate CA receives

[1] Note that "operated by" is not meant to rule out the possibility of contracting out the operation of the Federal BCA to a commercial CA company. The BCA does not start trust paths, so it would be comparatively easy to change Bridge CA contractors, since it would not then be necessary distribute a new authenticated "root CA" key to all relying parties.

a certificate from it’s superior CA, and may also have subordinate CAs of its own, to which it issues certificates;

- **Repositories:** Repositories are on-line facilities that provide certificates and certificate status information. Repositories in the Federal PKI will provide information via the LDAP protocol and they may also provide information in other ways. The FPMA will maintain an open LDAP repository for CA certificates and revocations. Repositories that contain end-entity certificates and CRLs for end-entity certificates, or other certificate status responders, are a policy matter for individual trust domains. Some domains may choose to make end entity certificates available in open repositories, and other domains may restrict access to end-entity certificates. Similarly some domains may implement CRL based certificate revocation while others may choose to implement OCSP responders. Some domains may elect to make certificates and certificate status information available only to relying parties that have entered into an agreement with the CA or domain management authority;
- **BCA Repository**: The BCA repository will be open to Internet access by anyone, and will make available:
    - ♦ All certificates issued by the BCA;
    - ♦ All certificates held by the BCA;
    - ♦ All cross certificate pairs containing certificates held or issued by the BCA;
    - ♦ All CA certificates issued by CAs within the overall Federal PKI;
    - ♦ All cross certificate pairs between CAs in the Federal PKI;
    - ♦ A consolidated Federal CA (indirect) CRL, that covers all CAs in the Federal PKI. This implies a requirement to include appropriate CRL Issuer and CRL Distribution Point extensions in all CA Certificates issued by CAs within the Federal PKI;
    - ♦ Other certificates and CRLs as determined by the FPMA;

Conclusion

We need an approach that will graft a tolerably coherent Federal PKI together out of disparate parts that are being implemented now, in a host of agency efforts that use digital signature certificates. It has to be as catholic as possible, and accommodate quite different approaches, ranging from CAs operated by agencies for their employees, to commercial CAs that certify the identities of members of the public, and Federal servers that provide service to the public. Some application oriented CAs will follow policies oriented to high value, high security transactions, and others will accommodate routine electronic commerce or service to the public. We have limited power to enforce any approach we adopt on agencies and, I believe, little prospect of getting a lot of appropriated money to build a big, top down PKI..

I have proposed that we create an overall policy management authority that I have called a Federal Policy Management Authority, and concentrate on making a trust bridge between these many systems, using a Bridge CA to cross certify with principal CAs in Government and non-government trust domains, as well as a repository for CA certificates and CRLs.

If we do this effectively, we will supply one of the key missing pieces to the PKI, and create a way to lead, rather than push, government users of public key certificates (and, I believe others as well) to sound policies and practices. I believe that once we get such a program up, the pressure to join will be considerable, and this will give us an opportunity to really lead.

The actual facilities needed are fairly modest, because we are only talking about cross-certifying with major (that is principal) CAs, or other bridge CAs, and maintaining a repository only for CA certificates, and CA certificate revocation information. But this is a critical missing piece that we can supply. I don’t mean to minimize the mechanical effort required (largely because of the many quirks that we are now discovering in getting commercial CA products to cross-certify, and getting directories to work with each other), but the hardest part will be to agree on the basic requirements to cross certify and join the PKI.. This, however, is unavoidable in any meaningful Federal PKI.