FPKI: INTEROPERABILITY OF FEDERAL AGENCIES AND E-BUSINESSES

Ludwig Slusky, College of Business and Economics, California State University,5151 State University Drive, Los Angeles, CA 90032, 1-323-3432922, lslusky@calstatela.edu
Parviz Partow-Navid, College of Business and Economics, California State University, 5151 State University Drive, Los Angeles, CA 90032, 1-323-3432800, ppartow@calstatela.edu

ABSTRACT

All branches of federal government are required to migrate their business practices to paperless operations. The Public Key Infrastructure (PKI) is the simplest, most widely used architecture for secure data exchange over not-secure networks. It integrates computer hardware and software, cryptography, information and network security, policies and procedures to facilitate trust in distributed electronic transactions and mitigate the associated risks. Together with e-Authentication, PIV card, and Real ID, FPKI provides a comprehensive solution to Privacy and Information Security protection of information shared over networks internally between the US Government agencies and externally with non-Federal organizations (businesses; state, local, and foreign governments; academia; etc.) or individuals

FEDERAL PKI ARCHITECTURE

The Federal Bridge Certification Authority (FBCA) is a bridge CA, which acts as an anchor and the root for related CAs. It does not itself does not issue certificates to end entities (except those required for its own operations) but establishes unilateral or bilateral cross-certification with other CAs.
The FBCA allows discrete PKI to trust digital certificates issued by other entities, which policies have been mapped and cross-certified with the FBCA. It is two way cross-certified with government agencies and external PKIs. A trusted Federal PKI CA can issue certificates that are accepted nationwide for government, commercial, and financial transactions.

The Federal PKI Policy Authority (FPKIPA), also known as Federal PKI Common Policy Framework Certification Authority (FCPF), has its mission in enforcing "digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities." (http://www.cio.gov/fpkipa/)
It administers all policy issues of the FPKI Infrastructure and is charged with responsibility to oversee cross-certification and interoperability of non-Federal PKIs and FPKI.
It also approves applicants for cross-certification with the FBCA and for cross-certification with the C4CA. Cross-certificates issued by the FBCA or C4CA are issued and revoked at the sole discretion of the FPKIPA.

The FPKIPA facilitates outsourcing of PKI services to Shared Service Providers (SSP). Therefore, these SSPs are inherently one-way (optionally, two-way) cross-certified with the FBCA.

The FCPFCA provides policy mapping to enable *Common Policy Object Identifiers (Common Policy OID)* and interoperability between two organizations that apply similar issuance and application policies, but have deployed different policy OIDs.

Certificate Policy (CP) defines requirements and standards for issuance and management of keys and certificates. It determines the level of trust the certificate provides and the requirements for the CA

operations in order to maintain the trustworthiness of its certificates' status information. CP also defines user's responsibilities for requesting and using certificates and keys.

The Citizen and Commerce Class Common Certification Authority (C4CA) operates at the lowest levels of assurance using a memorandum of agreement rather than detailed review of the certificates for compliance. It authenticates citizens and commercial enterprises as subordinates (with the option of two-way cross-certification) for many electronic services with the U.S. Federal Government. It is not cross-certified with any other CA in the FPKI Architecture. The C4 CA is lightweight and is designed for entry-level PKIs..

An E-Governance Certification Authority (E-GovCA) supports *The e-Authentication Service Component (ASC)*, which represents a common infrastructure for electronically authenticating Government-wide the identity of users of Federal E-Government services [2].

Cross-Certification establishes a trust relationship between two PKIs by issuing and relying on certificates from each other as if they had issued them themselves, by reviewing each other's policies, and mapping policy information of one CA into another CA so trust can be propagated despite differences among policies of cross-certified CA. In Federal PKI, cross-Certification process involves two CAs where each CA certifies a public key of the other by issuing a public-key certificate to that other CA. FPKI standards allow for cross-certification creating a chain of trust with other bridges. In PKI cross-certification, a Relying Party (i.e., a party that utilizes digital certificates for electronic identity authentication) may trust that PKI's digital certificates at the Level(s) of Assurance stated by those certificates with no other trust instruments required

In addition to industry-bound cross-certification bridges, FBCA is open to approved commercial bridges, for example, CertiPath [1].

RECORDKEEPING

Recordkeeping for the required period of time is the responsibility of the subscriber, the recipient, and the trusted PKI service provider(s).
FPKI authenticated transaction records contain the following data [5]:

- Human-readable signer's name or its metadata representation;
- Human-readable transaction signing date and time; and
- Purpose (explicit or implicit) for applying the PKI digital signature to the transaction – derived implicitly from the context or stated explicitly as a purpose statement.

The retention period of recordkeeping is from the record creation to its final disposition. However, the retention period for Public Key certificates could be shorter, typically 12 to 36 months. Validity of a certificate issued by FPKI is limited to a maximum of 3 years. For comparison, FIPS-201 stipulates a maximum of 5-year lifetime for ID cards. Security requirements for CA are stringent [4] as a CA can attract a higher risk of external attacks.

E-AUTHENTICATION, PIV CARD AND REAL ID

Trust in distributed electronic transactions with identity authentication is the cornerstone of e-business, e-government, and e-health. Identity authentication (but not authorization or access control), addressed in the e-Authentication Guidance for Federal Agencies, issued by OMB.

An e-Authentication objective is to provide citizens and businesses easy access to multiple applications through the re-use of existing credentials and established identities. The e-Authentication provides the critical capability of establishing trust relationship between users and applications by validating users' electronic credentials.
These e-Authentication levels are based on (1) the degree of confidence in the process of establishing the identity of the individual to whom the verifiable credential was issued, and (2) the degree of confidence that the individual who presented the credential is the individual to whom the credential was issued. The FBCA facilitates transaction interoperability by allowing the "relying party" to create a certificate trust path to the certificate issuer, and determine the certificate's e-authentication level of trust [3].

Validation of FPKI certificates, signatures, and asymmetric key pairs is now extended to Personal Identity Verification (PIV). PIV System is amandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

Real ID Act 0f 2005 focuses on developing identity system to create/improve privacy and security; help protect citizens information with tools for self-protection; improve identity functions, and integrate identity functions into wide range of commerce, interactions and transactions for government and non-government participants. [6] Although, not a part of defined FPKI architecture, Real ID can provide credentials for initial steps of e-Authentication of citizens. De-facto National Identity Card, the Real ID is being implemented by placing federal mandatory improved security requirements on issuance of Driver's License' and Personal Identification Cards.

REFERENCES

[1] CertiPath. Retrieved July 8, 2007 from http://www.certipath.com/ Cooper, D. (2004), *Public Key Infrastructures - PKI Research. Security Technology Group.* July 28, 2004, retrieved May 29, 2006 from http://csrc.nist.gov/pki/PKIResearch.html.

[2] *Establishment of e-Authentication Service Component. AGENCY: Office of Government wide Policy,* General Services Administration [C–05–N01], GSA, August 5. 2005. Retrieved May 29, 2006 from http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/pdf/05-15515.pdf.

[3] *FBCA – Federal Bridge Certification Authority*, Retrieved May 28, 2006 from http://www.cio.gov/fbca/.

[4] FIPS Pub 140-2. Change Notices (12-03-2002), Federal Information Processing Standards Publication (Supersedes FIPS PUB 140-1, 1994 January 11), *Security Requirements for Cryptographic Modules, Information Technology Laboratory*, National Institute of Standards and Technology, May 25, 2001.

[5] PKI Transaction Records Management Guidance, Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records, Federal Public Key Infrastructure Steering Committee. March 11, 2005. Retrieved May 20, 2006 from http://www.cio.gov/fpkisc/library.htm.

[6] *Real ID Act Of 2005 Driver's License Title Summary*. Retrieved September 29, 2007. http://www.ncsl.org/standcomm/sctran/realidsummary05.htm