Open Group (OSF - X/Open)
Security Business Requirements Group (BRG)
Public Key Infrastructure (PKI) Task Group (TG)

U.S. comments and suggestions to be sent to Will Frazier by email only to: frazier@sst.ncsl.nist.gov

Technical input to Dean Adams by email only to: d.adams@xopen.org

All other contributions by email only to: xosecrtg@xopen.org

Draft Version 0.5

Input for Version 0.6 to be transmitted to OGsecurity@opengroup.org by 13th August 1996. Version 0.6 to be drafted by 27 August 1996.

Baseline Requirements for a Global PKI and PK Services

An interoperable global PKI is required to provide privacy and digital signature services in support of international commerce, balancing the legitimate needs of commerce, governments and privacy of citizens.

The global PKI must support multiple governance policy models within a single global PKI framework, and must enable the enforcement of all existing governance policy mandates.

The global PKI will support the following Services:

- establishment of domains of trust and governance
- confidentiality (sealing)
- integrity and authentication (signing)
- non-repudiation service
- end-to-end monitoring, reporting and auditing of PKI services

The global PKI will have the following functionality and characteristics:

1. Key life-cycle management

   The actual life cycle of a key depends on whether it is used for confidentiality or signature purposes. Generic facilities to be supported are:

   - Key recovery facilities
     - use of key recovery facilities implies acceptance of a mandatory policy for the protection and recovery of keys. The policy defines how the keys are to be protected and under what conditions and to whom a key will be made available. The mandatory aspect of policy arises as the operations of a key recovery facility may be regulated by legislation or procedures required under commercial contracts for liability management.
     - only key recovery enabled systems to be usable within a PKI.
     - a key recovery facility shall be unconditionally trusted and be liable to uphold the stated policy with redress for loss arising from failures to uphold policy through contractual liability and penalties.

    - a key recovery centre shall be able to verify the legitimacy of a key submitted to it for storage.
    - a user of a key recovery repository shall be able to verify that it is an authorised repository.
    - coordination between the management of public and private keys in PKI and in data recovery centres. Note that public and private key parts do not have the same life cycle and key parts may be archived.
    - aging / revocation / repudiation of keys
    - discretionary key fragmentation between key recovery facilities
  - Key Generation facility
    - the method of key generation shall be discretionary, subject to commercial decision and business requirement.
    - the discretionary aspect applies to selection of levels of quality, uniqueness, secrecy and recoverability.
  - Key Distribution, Revocation, Repudiation and Archive
    - the PKI shall support facilities for the distribution of keys and to appropriate storage devices and directories.
    - a certification authority shall be able to revoke certificates for individual keys under the terms of the applicable policy.
    - the PKI shall support facilities to enable a user to repudiate his public key under the terms of the applicable policy.
    - the PKI shall support the archive and subsequent retrieval of certificates in support of the retrieval and verification of long term information.
  - Warranted retrieval
    - Law enforcement retrieval (subject to policy conditions)
    - Corporate agency retrieval (subject to policy and authorisations)
    - Individual retrieval (subject to policy and authorisation)
    - An electronic vehicle for the delivery of a notarised electronic warrant is required to support the automation of key retrieval under due process (able to take advantage of existing legal agreements)
    - Requires a permanent, non-repudiable and independently verifiable record of key retrieval operations.
    - Warranted retrieval policy includes policy on disclosure or non-disclosure of key retrieval to owner of key

2. Distributed Certificate Management Structure (driven by requirements of Transaction/business domain)

  - policing and enforcing policy (governance model)
    - policy creation and maintenance. The policies include those covering key generation, key recovery, warranted retrieval.
    - registration of a key and the binding between the key and a name.
    - query which keys are bound to a name
    - for services built on PKI access control policies are not required to be based on individual identity.
    - certification of the binding between a public key and a directory name is mandatory
    - certification of the binding between additional attributes and a directory name is discretionary

    - auditing and support for the monitoring of policy compliance is required
    - a CA shall be able to suspend and revoke certificates
  - concurrent support of multiple policies
  - certificate authority policy mapping services shall be provided to establish cross certification between CAs.
  - support for arbitration to determine acceptability of certificates in the event of multiple conflicting certification paths.
3. Security of the PKI
  - protection of the confidentiality, integrity and availability of the PKI services, for example key generation, key distribution, key storage
  - PKI services shall not be able to repudiate their own actions. Strong non-repudiation services are required for certification and certificate revocation services.

Known Issues

For interoperability there is a dependency upon the definition of standard application program interfaces to and protocols between the component services of the Public Key Infrastructure.

Work is required to define and agree profiles of option fields in certificates.

Recommendations

Adopt X.509 version 3 as a basis for certificates in the development of the PKI

Adopt and adapt existing standards and protocols wherever possible, only invent as a last resort.

Contributing Organisations

Barclays Bank	Shell International	Sweden Post
UK Ministry of Defence	BCTEL	DISA
The Open Group	Telecom Finland Ltd	Pacific Gas & Electric
Electronic Data Systems	Jet Propulsion Laboratory	Boeing Information & Support Group
Harris Corporation	ICL	Lockheed Martin
Guide International	J P Morgan	IBM
Bellcore	Nortel	HP
NIST	SUN	Siemens Nixdorf
Dynasoft	SCO	Bull
NCR	NSA	Digital
Amdahl	OpenVision	Citicorp
Fujitsu-ICL	Mitre	

Parties known to have interests in the development of public key infrastructure include:

- U.S. Government (NIST as conduit to all U.S. government agencies)

- Canadian Government
- European Information Security Business Advisory Group (IBAG) & Member Organisations
- European Commission DG III & DG XIII
- European Commission DG XIII Senior Officials Group - Information Security (SOG-IS)
- OECD
- ICC
- CommerceNet
- Japanese Govt Initiative (JapanNet)
- Verisign
- Open Group (OSF -X/Open)
- IETF
- Electronic Mail Associations
- Lotus
- Microsoft
- RSA DSI
- DMS
- Trusted Information Systems (TIS)
- Bankers Trust