Current experience

» Third party PKI products are successfully deployed with Microsoft Active Directory

» Entrust has several customers at various stages of deployment including
  - Architectural design
  - Pilot
  - Full deployment

» Current deployments use
  - Entrust Authority Security Manager 6.0
  - Active Directory with Windows 2000
General goals

- **Client interoperability**
  - Enable multi-vendor PKI clients in the environment to find necessary data where they expect it
- **Cross-certification interoperability**
  - Facilitate certification path development
  - Support revocation checking
  - Directory interoperability
Deployment considerations

**Single CA environment**

- **Data population**
  - PKI client expectations of schema & configuration container
  - Authentication to Active Directory
  - Unix applications (CA, relying party apps)

- **Permissions management**
  - CA requirement to write certificates, CRLs etc

- **Naming**
  - Directory entry creation versus credential issuance
  - Multi-valued versus single-valued RDNs

- **Additional certificate subjects**
  - Certificates for domain controllers, eg to support W2K smartcard login
Deployment considerations

Cross-certified environment

⇒ **Naming**
  - Integration of geo-political and dc-based schemes

⇒ **Data population**
  - Various client expectations w.r.t. schema

⇒ **Anonymous user access requirements**
  - Retrieval of certificates and CRLs by remote users

⇒ **CA key rollover techniques**
  - Old key/new key certificates / additional trust anchor

⇒ **Directory interoperability**
  - Referral versus chaining
  - LDAP profile, etc.
Deployment considerations

Name scheme integration

➤ Key requirement for FPKI and Bridge CA

➤ FPKI Directory profile option is aliases
  – Security concerns regarding substitution attacks

➤ Some additional options for discussion
  – Indexing support for directories (web search engine style)
  – Dual search base standard support
    • Bridge has 2 distinct subtrees
    • Clients try each subtree (different search base in query)
  – LDAP cross-references
  – DNS SRV records enhanced to identify name scheme
  – Registry service, e.g. UDDI to identify name scheme
Third party PKI products are successfully deployed with Active Directory today

Deployment of third party PKI products with Active Directory should consider
- Initial PKI deployment environment
- Plans for future cross-certification environments

Vendors collaborating to
- Identify deployment considerations
- Improve integrated deployment with future releases

Key issues for FPKI and Bridge CA
- Integrated name schemes
- Inter-agency information retrieval expectations