
Development of a Multi-Enterprise Public Key Infrastructure

Bradley J. Wood

Senior Member of Technical Staff
Information Systems Surety Department

Sandia National Laboratories

Albuquerque, New Mexico

The Contributors

- **Tim Sharick**
 - Lawrence Livermore National Lab
- **John Long**
 - Sandia National Laboratories / New Mexico
- **Brian Desind**
 - Allied Signal / Federal Manufacturing & Technology
- **Vickie Hamilton**
 - Sandia National Laboratories / New Mexico

Outline

- **Motivation / Requirements**
- **Approach / Deployment**
- **Issues / Observations**
- **Next Steps**

Motivation

- **New applications for security based on Public Key Cryptography**
 - Applications of the World Wide Web, messaging, and workflow automation
 - Needs demonstrated in advanced manufacturing
- **Unique features US Dept. of Energy / Nuclear Weapons Complex**
 - Multiple companies serving the same primary customer
 - Mix of cultures: universities, government, & industry
 - Geographic diversity

The Project

- **Survey**
 - Existing products and applications within the complex
- **Design**
 - System to satisfy perceived requirements
- **Evaluate**
 - Commercial products against perceived requirements
- **Deploy**
 - Common architecture & products within complex
- **Evaluate**
 - Lessons learned

System Design and Requirements

- **Features of the Public Key Infrastructure (PKI)**
 - Support both certificate hierarchies & cross-certification
 - System readily accessible over public networks
- **Support for existing applications / standards**
 - Netscape and other Web infrastructures
 - Oracle database clients and servers
 - X.500 Directory Services
- **Support for Emerging Standards**
 - FIPS 140 & Federal PKI standards
 - Various APIs

Product Evaluation

- **Evaluation during Summer 1995**
- **Evaluated products**
 - **Certificate Issuing System & other tools (RSA / Verisign)**
 - **MOSS/PEM (Trusted Information Systems)**
 - ***Entrust* (Northern Telecom / NORTEL)**
 - ***PGP* (MIT and Viacrypt)**
 - **Other products**
 - » ***Secret Agent* (AT&T), *Digisign* (Apple), others**
- **Selected product**
 - ***Entrust* (NORTEL)**

Current Assessment of *Entrust*

- **Likes**

- Emphasis on automating key management processes
- Seamless key escrow & other archives
- Keys for both encrypting & signing
- Algorithm flexibility

- **Dislikes**

- Costs for licensing key pairs
- Lack of access to certificate through API
- Poor support for multiple signatures
- Playing catch up with Netscape?

Deployment

- **Lawrence Livermore**
 - Spring 96, electronic forms
- **Sandia / New Mexico**
 - Summer 96, privacy & authentication for cc:Mail
- **Allied Signal / Kansas City**
 - Fall 96, cross-site authentication for orders with Sandia / New Mexico
- **US Dept. of Energy / Headquarters**
 - Spring 97 (speculative), authentication for travel reimbursement system

Deployment Issues

- **Identify vs. authority**
- **Unique personal identifiers**
- **Tracking personnel changes**
- **Individual's naming conventions**
- **Deploying / updating X.500 directory**
- **Emergency access to protected data**
- **Development of common trust model**

Other Issues & Impressions

- **Hierarchies are problematic.**
- **Human factors cannot be ignored.**
 - Difficulty describing PKI concepts to non-technical management and staff
 - Training, ease of use, and ease of installation are important
- **Emerging Federal PKI efforts**
 - Federal PKI based on GCS-API, *Entrust* based on GSS-API
 - Expected enthusiasm for US Postal Service PKI
- **Integration with other systems is essential**
 - Legacy applications, human resources systems, ...
 - Emerging security systems: Netscape, DCE, Kerberos, Win NT, and others

Next Steps

(Author's Speculation)

- **Deploy system at other DOE sites**
 - Los Alamos, Oak Ridge, Pantex, and others
- **Further integrate system into the workplace**
 - Web-based applications for electronic commerce
 - Prepare for wide-spread deployment
- **Applications to new problems**
 - Separate need-to-know groups on secure networks
 - Tighter integration with database management systems
- **Demonstrate applications to “new standards”**
 - Federal PKI & other PKI infrastructures / standards
 - Netscape *Navigator* and S/MIME (mail)

Summary

- Security using public key technology is only now becoming viable for large enterprises.
- Much of today's public key technology is still in the "developmental" stage.
- Deployment is based on much more than technology and product choices.
- There are no clear directions, and some new developments are expected.
- Still, there there are many advantages to deploying this technology.