Vince McCullough (TRW) presented the following to the Business Working Group:

TRW Enterprise Directory and Security Services, Overview and Lessons Learned

TRW got involved in PKI three years ago.

TRW Global Network:
- failings (uses PGP PKI)
- manually intensive
- expensive (1hour per employee, per year)
- 130,000 users in 40 countries

Driving PKI requirements:
- less than 3 minutes per year, per employee
- every person with TGN access will have a certificate
- virtually every server will be converted to SSL
- certificates used for everything (from ordering supplies to filling out timecards)

Phase I PKI was implemented with:
- centralized CA
- automated RA
- "virtual" RA officers
- escrow style key recovery authority (recover encrypt. key, sig. keys never recoverable)
- replicated directory

Types of Certificates:
- all users have a signature certificate
- users who need them may also have encryption certificates
- there were also server signature certificates

TEDS PKI:
When a new employee is added to the HR database, within 24 hours, that employee has an entry in the PKI LDAP server. The PIN and password (1-time only) is sent to the user via USPS. You create your own password after you use the initial one. When you leave the company, HR will upload your termination data (stop payment) to the directory. Within 24 hours, your access (certificate) will be revoked. In the near future, it will be revoked in 3 hours.

How were certificates expired and revoked?
All certificates expire in one year (users return to RA web site and replace their expiring certificate). Removal of employee from the HR database deletes the user certificate from the directory server (immediate loss of access). CRL's are generated, but are not used by internal web servers. Employees can revoke their own signature certificate.

Private keys were stored:
- on the enterprise directory (least secured)
- on the users PC (better, but still vulnerable)
- on a hardware token (the best)

What if a certificate is compromised?
Users can revoke their own signature certificate and obtain a new one.

Examples:
1. Directory Storage - somebody looked over their shoulder
2. Hard Drive Storage - somebody copied their encrypted certificate from their PC
3. Token Storage - employee loses their hardware token

Directory Server used:
- LDAP interface
- centralized server
- directory server

Lessons Learned - General
- the directory is more important than the CA
- focus on the design of the directory
- designing 2 distinct systems [Enterprise directory and PKI (CA, RA)]

Lessons Learned - Directory
The directory should not be an authoritative data source.

Directory architecture:
Keep the hierarchy as flat as possible.

Directory construction:
- secure the directory
- replicate the directory
- LDAP over SSL v3
- DNS names make useful branch names within directories

Lessons Learned - PKI
General:
- automating PKI processes (reduces operational costs, and increases reliability security)
- certificates should be designed so identity rarely changes
- encryption certificates should be distinct from signing certificates

Security Model:
Few organizations wish to treat all data as equally sensitive.

Key Management:

- single key management strategy (store keys in directory, on hard drive, on h/w tokens)
- it should be easy for a user to revoke and replace their private key

Certificate Content:

- pay close attention to x.509 v3 “extensions”
- x.509 standards and usage continue to evolve with new extensions gaining importance