Dogtag Open Source PKI Update
Bob Lord, Consultant
Ebbe Hansen, Spyrus
A Little History...

- Netscape servers
  - Web
  - Directory (LDAP)
  - Mail
  - Certificate
- AOL/iPlanet
- Red Hat
  - Open sourced DS in 2005
  - Open sourced CS in 2008
What is the Certificate System (CS)?

- Architecture
- Use cases
- Problem it solves
- Integration with other technologies
Main Components (1)

- Certificate Authority (CA): Issues X.509 digital certificates and CRLs

- Token Management:
  - Token Processing System (TPS) & Token Key Service (TKS)
  - Supports Global Platform smartcards
  - Makes smartcards as easy to use as an ATM
  - Manages symmetric keys for securing communication to tokens
Main Components (2)

- **Data Recovery Manager (DRM):**
  - Secure repository for backup/recovery of user's private keys
  - Configurable multi-person approval for recovery

- **Online Certificate Status Protocol (OCSP) Responder:**
  - Responds to OCSP requests to verify certificate validity in real time

- **Enterprise Security Client (ESC):**
  - Multiplatform middleware package
Dogtag/CS Subsystems

Client
- User
- HT
- ML
- ESC
- APDU
- NSS
- Smart card

Server Subsystems
- Firewall
  - TPS
  - OCSP
  - CA
  - DRM
  - TKS
  - LDAP
What is Dogtag?

- The **entire** source tree from the Red Hat Certificate System
- Includes **all** CS subsystems
- Binaries, source, wiki, IRC, mailing lists
- Growing community of related technologies and people
Open Source Effort

- Process
- Licenses
- Repository
- Wiki
- IRC
- Bug tracking
Related technologies

- Crypto consolidation
- Directory Server
- IPA
- Samba
- Kerberos
- Mozilla
Unified IdM Framework

VPN
Firefox
Thunderbird
RHEL Login
OS-provided UI

Common Security, Identity APIs

- Smartcard module
- Secure key module
- Secure password module
- Biometrics module
- Policy Enforcement

Credential Management

Secure Protocols

SSL
S/MIME
Kerberos
RHEL Smart Card Login

RED HAT ENTERPRISE LINUX 5

Smart card password:

Smart card inserted.
Welcome kevinu [Kevin Unthank]!
Roadmap

- Dogtag
- Certificate System
- IPA
Ebbe Hansen, Spyrus
SPYRUS Overview

- **U.S. Company**
  - Privately held, HQ in San Jose, CA
  - Offices and support staff in New Jersey, Virginia, Florida, Oregon, Canada, and Australia

- For 15 years, our focus has been on providing high-assurance encryption and public key security products for the government and the public sector world-wide
  - Products are designed and built in U.S.A. to protect both Sensitive But Unclassified and Classified data.
  - U.S. Defense Message System (> 400,000 Fortezza tokens)
  - First Commercial Personal Encryption Device Approved to Protect Tactical Secret
  - Only USB Encryption Device Approved for DAR BPA
Hydra PC Enterprise Edition – Features

**Dual Function Device:**
Doubles as a smart card!
Supports PKE Applications
such as smart card logon,
S/MIME, TLS, IPSEC

**All encryption performed on hardware** – encrypts and seals every file
(with strong protection against passive and active attacks)

**Suite B On Board™**
Supports Suite B & legacy cryptographic algorithms
(ECC, SHA-2, AES)

**Data Containment:**
Host Authorization Code ensures Hydra PC will work only on authorized computers

**Enterprise Management:**
Provides enterprise wide configuration and control of security policies, auditing, enclave creation, and Recovery Agent assignment

**Unlimited Storage:**
Write data to removable miniSD/miniSDHC cards

Can also write encrypted files/folders to hard drive, network drive, or other removable media and portable drives, and even to Internet-accessible storage drives

Copyright © 2008 SPYRUS, Inc.
Hydra PC Digital Attaché – Features

- Provide hardware-based full disk encryption for removable miniSD and microSD cards
- Simultaneously use hardware-based file encryption
- MiniSD and MicroSD cards support clear compartment and encrypted compartment
  - Clear drive supports Read/Write and Read Only access control
  - Encrypted drive provides on-the-fly encryption and decryption
    - Encrypted file headers and meta data for Hydra PC file-based encryption
- Share encrypted miniSD and microSD cards amongst users in a Unit
  - Encrypted miniSD/microSD cards can be sent by ordinary mail and shared with multiple recipients.
Operational Requirement

- Pocket CA for Tactical Purposes
  - Within the US Government DOD (as well as numerous commercial enterprises), Units/Groups will be formed and deployed for special operations.
  - They have requirements to establish and maintain PKI infrastructure for their operation.
  - The CA must be secure, portable, and meet high assurance data-at-rest and data-in-transit requirements.
MySafeID as Subordinate CA or AA

(PKI Integration mod phase 1 – Subordinate to RedHat and Microsoft CAs)

Legend:
1: PKCS#10 + cert-profile
2: Subordinate CA cert
3: Public Key
4: End Entity Cert
MySafeID CA as standalone & offline PKI system

Fig 2

Single LYNKS CA HSM

CA1
RSA
1024

CA2
RSA
2048

CA2
RSA
4096

CA3
ECC
384

CA3
ECC
384

CA4
ECC
521

End Entity Token(s)

Cert1
RSA
2048

Cert2
RSA
2048

Cert3
ECC
384

Cert4
ECC
348
MySafeID as Subordinate CA
In on-line or off-line mode

Off-line generated certs transferred (out-of-band) for publishing.

On-line generated certs transferred (in-line) for publishing & possible revocation.

MySafeID CA4 operates in on-line or off-line mode.
RedHat and MySafeID as Subordinate CA
In on-line or off-line mode

Off-line generated certs transferred (out-of-band) for publishing.

On-line generated certs transferred (in-line) for publishing & possible revocation.

RedHat CA1 operates in on-line or off-line mode.
RedHat Directory

Certificate Publishing & Revocation Services

Key Management Services

Central PKI Support Services

RedHat Root CA

RedHat Issuing CA

Software Booting Directly on Hydra

Digital Attaché

Mobile CA application booting from Hydra, invokes HSM based Key Generation, central Key Archival & certificate / CRL publishing

LDAP

OCSP
Red Hat PKI with SPYRUS token support (06-05-08)

Windows Platforms

- MS-IE WEB Clients
  - Windows Cert Store
    - SPYRUS Tokens
    - Soft Tokens
  - PKI Enabled Applications
    - Smart Card Logon
    - Secure Email
    - Secure WEB
    - Other

Linux & Solaris Platforms

- FireFox WEB Clients
  - FireFox Cert Store
    - SPYRUS Tokens
    - Soft Tokens
  - PKI Enabled Applications
    - Secure WEB
    - Other

- CMS
  - CMS Hard Tokens
    - SPYRUS Tokens
    - Java Card Tokens
  - PKI Enabled Applications
    - Smart Card Logon
    - Secure Email
    - Secure WEB
    - Other

Red Hat CA
- HSM
Working with Pocket CA

- Fedora LiveCD Boot
- Fedora9 with Data Persistence
- Loading RedHat Dir & PKI
- Issuing certificates on-line
- Issuing certificates off-line
- Uploading certificates for publishing
- Revocation of certificates
PKI: providing unique certificates for Hydra PC Digital Attaché to enforce Secure Media & File Sharing

1. User-1 can share encrypted media cards with User-2. User-3 will not be able to decrypt.
2. User-2 can share files and media with User-3 and user-1.
4. Everyone can use PKI services, loop-back, and file sharing as supported in the Hydra PC Enterprise Edition.
Contact Info

**Corporate Headquarters
SPYRUS, Inc.**
1860 Hartog Drive
San Jose, CA 95131
(408) 392-9131 phone
(408) 392-0319 fax

www.spyrus.com
E-mail:
info@spyrus.com

Bob Lord, Consultant
bob.lord@gmail.com

Kevin Unthank, Red Hat
Product Manager
kevinu@redhat.com

Karl Wirth, Red Hat
Engineering Director
kwirth@redhat.com