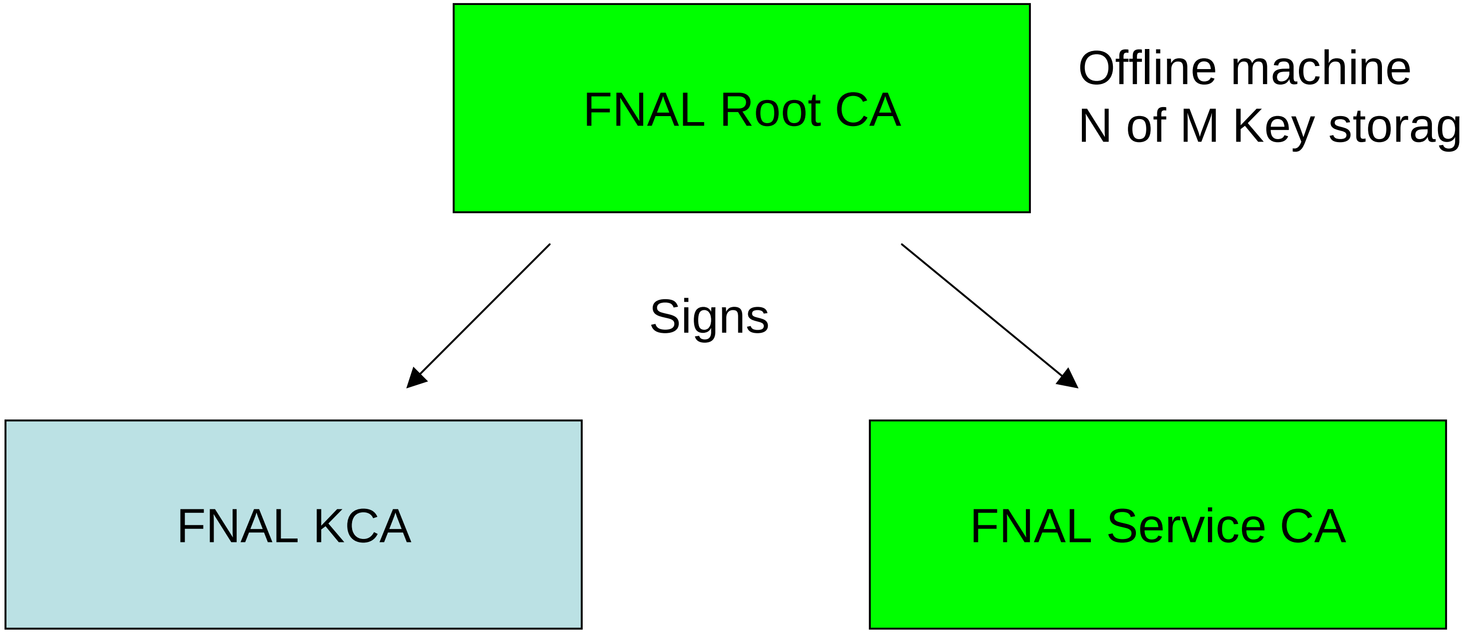
Fermilab CA Infrastructure

EDG CA Managers Mtg

June 13, 2003

Overall Architecture



FNAL Root CA

Offline machine
N of M Key storage

Signs

FNAL KCA

FNAL Service CA

Online protected machine

Offline “traditional” CA config

Salient Features

- Scope is FNAL internal and collaborators
- Registration tied to FNAL user registration
- Root CA used solely for signing subordinate CAs
- Service CA is traditional
- KCA issues short-lived user certificates only.

User registration

- Users register with FNAL.
- Information vetted by experiment delegates.
- All users revalidated twice within past 2 yrs.
- Users office collects signatures from experiment
- All users can get a Kerberos credential and with that can get a KCA credential.

What would we like?

- Accept FNAL Root CA and Service CA as “traditional” CAs
- Accept FNAL KCA as first instance of “online” CA

Status

- Root CA created and have certificate here now for transmission.
- KCA went production in March
  - 4000 registered users
  - ~100 unique users/month getting proxies
- Production Service CA not yet operational. Finalizing plans now.

Why Short-Lived Certificates?

- Intuition and measurement both tell us that a significant number of long-lived authentication secrets ***will be*** compromised.
- The frequency of this event is reduced if the secrets:
  - are not stored on computers;
  - are not transmitted on the network;
  - can be held in organic memory.
- The impact of this event is reduced if:
  - The owner of the secret can quickly and easily invalidate it and establish a new one.

Passwords vs. Private Keys

- Passwords are small secrets (most) users can remember. Private keys are sets of large integers which must be stored - usually in one or more online file systems.
- Passwords are easy to change, private keys difficult.
- On the other hand, passwords can sometimes be guessed - *if an offline attack is possible.* Private keys are seldom guessable.

KCA

- KCA = Kerberized Certificate Authority
  - An online CA which is a Kerberos service.
- Client generates an RSA key pair, sends public key to KCA with authentication and integrity protection.
- KCA generates the Subject DN, other extensions, and signs a certificate.
  - Valid until expiration time of Kerberos ticket.
- Client receives certificate, inserts it in the browser cache or Globus proxy file.
- Software originated at CITI, U of Michigan. Distributed with the NMI package and client in VDT next version.

CA Considerations

- The KCA host must be as well protected as any comparable part of the authentication infrastructure - KDC, Domain Controller, ...
- Since the CA private key is on-line, it should be short-lived* and easy to replace.
  - * Short relative to some other CAs, not to the certificates it signs!
- Relying parties (Grid or SSL services) need the KCA public key on file, or another CA key which certifies the KCA.
- Certificate revocation: moot.

KCA - LDAP Connection

- The KCA accepts only the public key and Kerberos identity from a client. The Kerberos identity is algorithmically transformed into a UserID and an Email address, but the CommonName ("John Smith") is also wanted.
  - The CommonName is obtained through a secure LDAP query to the Windows 2000 directory.
  - All our Windows 2000 domain user accounts are synchronized with Kerberos v5 user principals.

KCA - DNS Connection

- KCA's client, "kx509,” locates the KCAs through DNS SRV records, based on the Kerberos realm name.
- This obviates any client configuration and achieves failover and load-balancing among redundant servers.

Uses - Grid

- Grid users can delegate proxy credentials from a KCA certificate in the usual way.
- As long as the Globus toolkit on a grid server can trace a path from a trusted root CA to a user's certificate or proxy, that server can verify a user's identity.
  - Simplest deployment: store the KCA's self-signed certificate and signing policy on each server.
  - More elegant deployment: KCA fit into a hierarchy of CA's

Uses - Web

- Windows client stores user certificate & private key in the registry for browser's use.
- *n*x client includes a Netscape cryptographic module which can access the certificate and private key stored among the tickets in the Kerberos credential cache.
- An SSL-enabled web server can securely determine the client's UserID, name, Email address and Kerberos principal name.
  - Subject DN available to CGI, PHP, etc.
- Alternative to IP-based access control

Uses - Other

- The Nessus security scanner can act as a TLS-authenticated server.
- We provide servers inside and outside the site border and generate, for each registered sysadmin, a list of IP addresses they are responsible for and allowed to scan.
- On their own schedules, they authenticate through KCA/kx509, connect to the Nessus server with a GUI client, initiate scans, and receive the reports directly or return for them later.

Summary

- Deploying KCA has linked many TLS/SSL services into our sitewide authentication infrastructure.
- Either W2K or KRB5 is a sufficient base to allow deployment of this technology.
  - Can serve both at once
- The security concerns of an online CA issuing short-lived certificates are no more severe than KDC, kaserver, W2K DC,...
- Short-lived certificates require less storage protection than long-lived ones, and fulfill all the most common user requirements.