Stanford
Linear
Accelerator
Center

Mechanisms to Secure x.509 Grid Certificates

Andrew Hanushevsky

Robert Cowles

CA Manager’s Meeting, 13 June 2003

X.509 Difficult to Secure

- Certificate Authorities and relying parties have no formal agreements
- Secure private keys and users don't mix
  - No guarantee of good or any password choice
    - In fact, many users don't *want* password on their keys
  - No guarantee of secure private key location
    - E.g., users store keys in network based file systems
  - No guarantee how private key was handled
    - E.g., users copy/e-mail keys to remote machines & leave them

Stanford
Linear
Accelerator
Center

VSC (Virtual Smart Card)

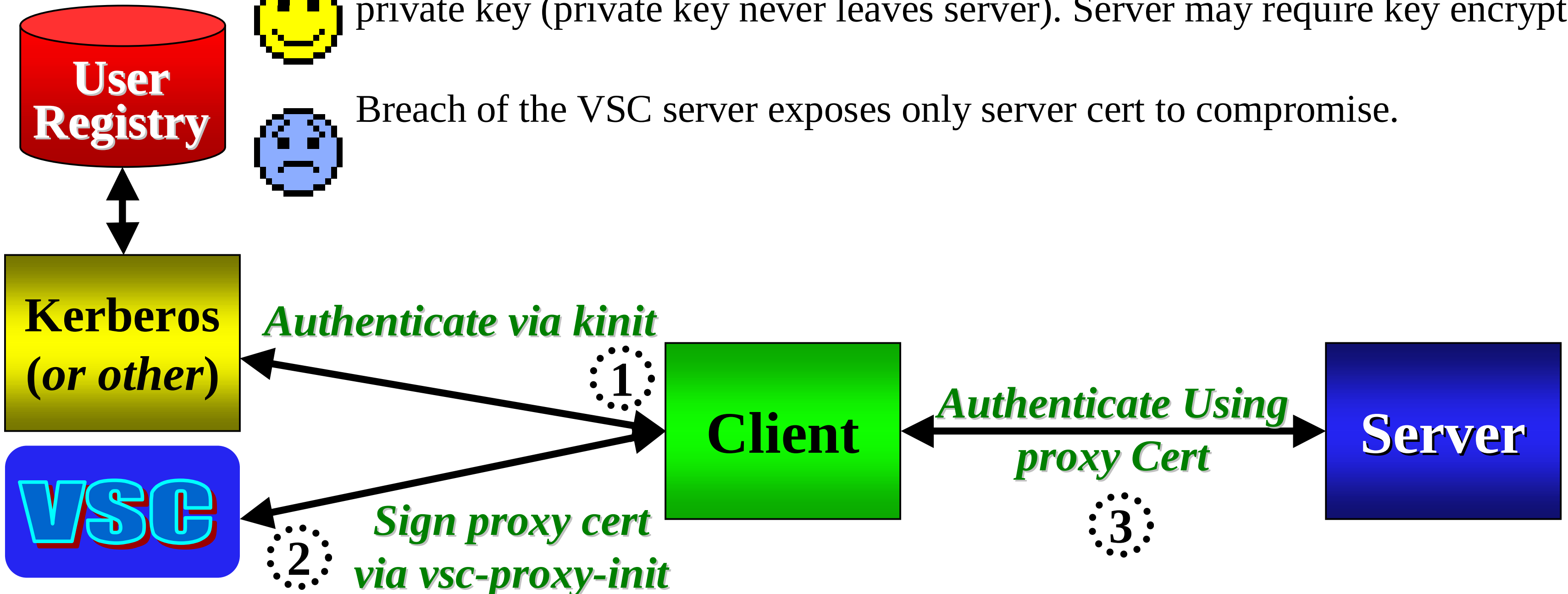
***VSC Steps*:**

kinit; vsc-proxy-init

- User registers with a known organization.
- Authenticate and get proxy cert signed by long-term cert.
- Use VSC proxy certificate as you would a normal proxy certificate.

☺ User can obtain a fresh proxy cert from anywhere in the world & never see the private key (private key never leaves server). Server may require key encryption.

☹ Breach of the VSC server exposes only server cert to compromise.



VSC Advantages

- Simple Model
  - Registration is normal site model
- Private keys never exposed
  - Can be further encrypted by user
- Can get proxy cert anywhere in the world
  - No need to copy public/private keys
- Can provide special always-on services
  - Perhaps proxy cert (re)validation
- Can provide *stronger* security guarantee
  - Signed cert as secure as institution’s account

References

- Virtual Smart Card
  - http://slac.stanford.edu/~abh/vsc
  - http://www.cs.dartmouth.edu/~pki02/Sandhu/paper.pdf

Stanford
Linear
Accelerator
Center

VSC Deployment for BaBarGrid

BaBar Primary VSC Server

- Maintained at SLAC
- Generates BaBarGrid proxy certificates for all BaBar users
- Accessible from any workstation
- Two possibilities
  - Holds long-term private key/cert signed by accepted CA
  - Signs proxy with CA cert accepted by VO gatekeepers (eliminate 3rd party)

Optional VSC Servers

- Holds longer-term delegated proxy
- Avoid single point of failure
- Allow authentication by alternative local credentials
- More distributed control (good / bad)

VSC Tradeoffs

- Needs to be acceptable to BaBar sites
- Breaks some PKI “rules”
- Central point of attack / failure

- Improves flexibility of X.509
  - Certs available from more places
  - Allows more flexible authentication policies
- Improves security of private keys
  - Key not in user’s file system
  - Can enforce passphrase strength rules