Virtual Smart Card

Andrew Hanushevsky

Robert Cowles

Stanford Linear Accelerator Center

Stanford Linear Accelerator Center

Enmeshed Private Keys

- Premise: Private keys and users don't mix
  - Inherently insecure model
    - No guarantee of good or any password choice
    - 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
- User managed keys *cannot* be trusted

Stanford Linear Accelerator Center

Solitary Private Keys

- Premise: Never give a user their private key
  - Can't mishandle something you don't have
- Can provide a ***stronger*** security guarantee
  - Signed cert as secure as institution's accounts
- Must provide agent-based key handling
  - E.g., smart cards

Stanford Linear Accelerator Center

Virtual Smart Card (vsc)

- Premise: Physical smart cards (psc) in software
  - vsc's have a 1-to-1 concept correspondence to psc's

Concept	Physical	Virtual
Procurement	Purchase/download	Request/generate
Possession	Physical	Authentication
Operations	Indirect	Indirect
Tamper protection	Self-destruct	Restricted access
Theft protection	Settable pin	Settable password

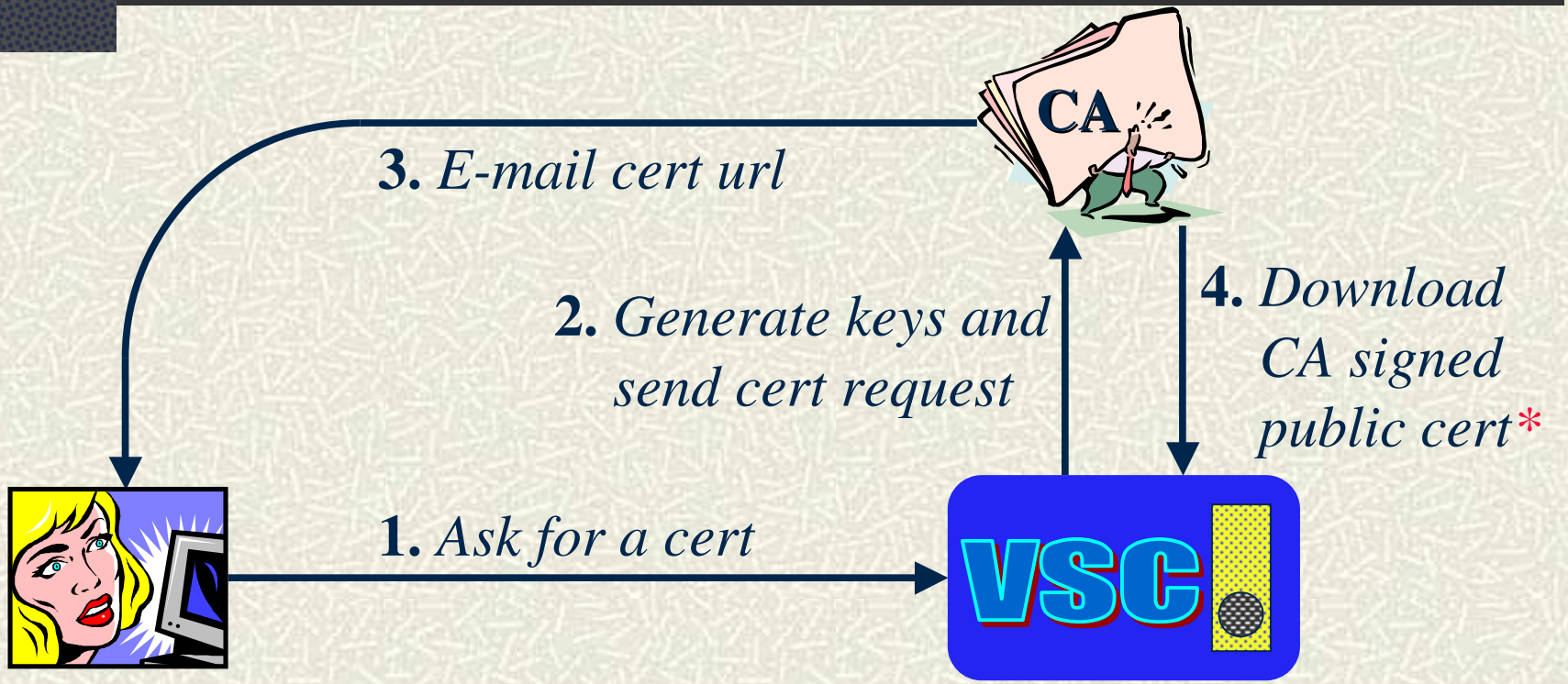
Stanford Linear Accelerator Center

VSC Conceptualization

- A vsc is implemented using a secure, access restricted server
  - One server holds many user's private keys
    - Hence, one server instantiates many vsc's
  - Can be well secured
    - Restricted physical access
      - Cages, keyed room, etc.
    - Restricted logical access
      - Only three access protocols needed: dns, ntp, and vsc
    - Keys can be encrypted via user-supplied passwords

Stanford Linear Accelerator Center

VSC Procurement



User never sees the private key!

**When available on 1st request or automatic poll.*

VSC Operation (vsc-proxy)

Externally authenticated **(e.g., Kerberos)**

Private key never sees the network!

Stanford Linear Accelerator Center

VSC Theft Protection

Externally authenticated **(e.g., Kerberos)**

2. ***Send encrypted key-string***

1. *Generate key-string from a strong user password*

3. *Encrypt user's x509 private key and discard key-string*

User must now supply key-string for vsc to use private key

Stanford Linear Accelerator Center

VSC Advantages I

- Simple and effective
  - Models well-known physical object -- smart card
  - Initial certificate request is trivial
- 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

Stanford Linear Accelerator Center

VSC Advantages II

- Can provide special extensions
  - EDG VOM extensions (natural fit)
- Can provide special always-on services
  - Perhaps proxy cert revalidation
- Can provide *stronger* security guarantee
  - Signed cert as secure as institution's accounts

Stanford Linear Accelerator Center

VSC Disadvantages

- Private keys are concentrated
  - Can be user-encrypted
  - Similar problem in Kerberos
- May violate current CA CP/CPS
  - Political vs. practical reality
- No more secure than external authentication
  - Need good authentication (e.g., K5)

Stanford Linear Accelerator Center

Conclusion

- Virtual Smart Cards effective
  - Simple, relatively transparent, secure
- Provides a path to more stringent security
  - Physical smart cards
- Simplify user's lives
  - Ease of use reduces security lapses
- Promotes a congenial grid security environment!