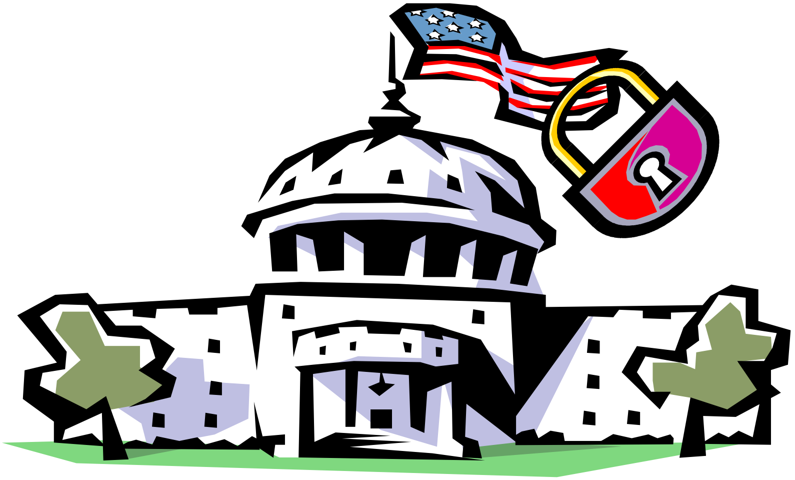


PKI Components to Support HSPD-12 Registration and Certificate Issuance

Mark L. Silverman, CISSP

HSPD-12 PKI Implementation Workshop
April 10, 2006

Talking Points

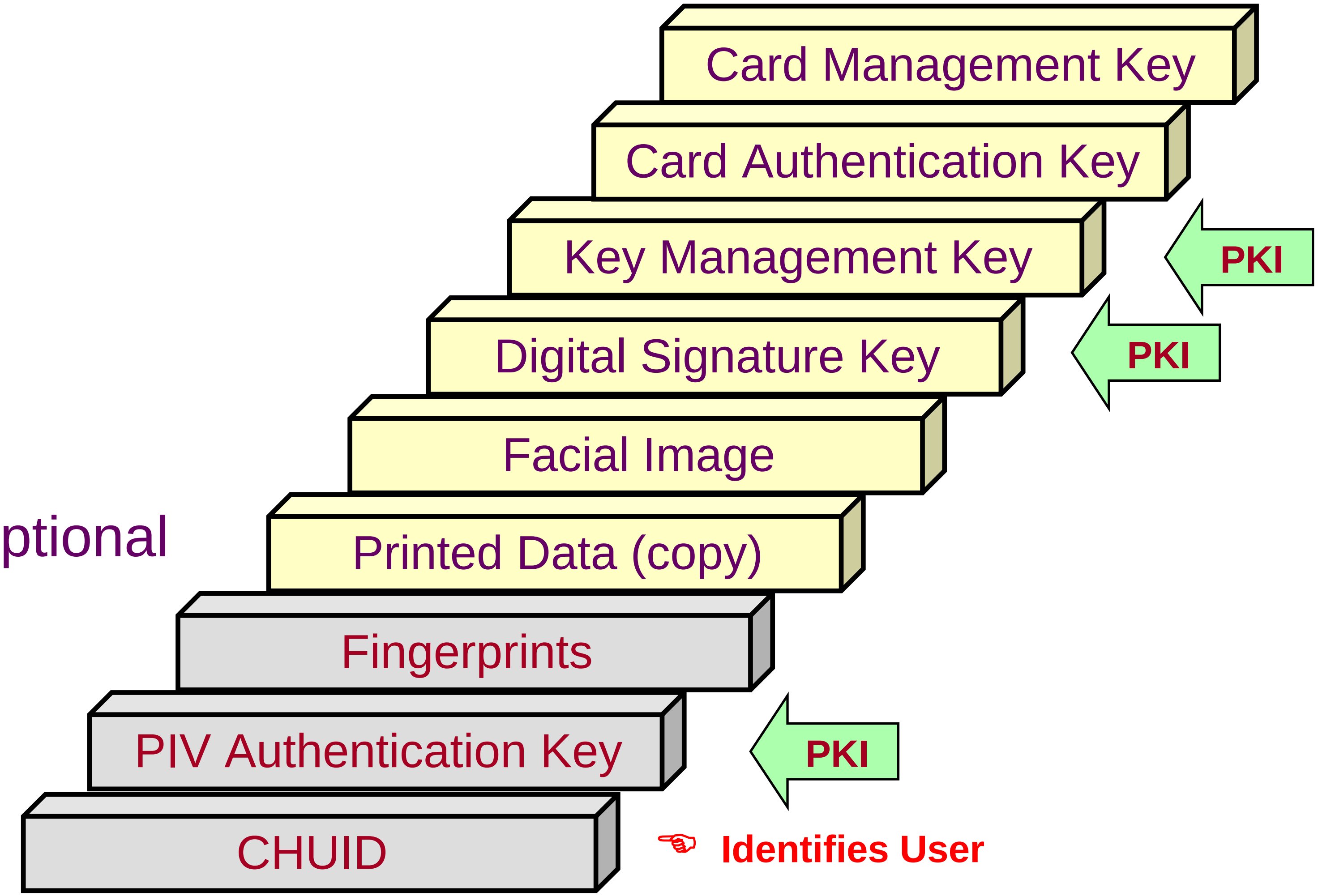
- ☑ Registration Issues
- ☑ Electronic Components of PIV Card
- ☑ CHUID and Personal Identifier
- ☑ PIV Card PKI Related Data Elements
- ☑ Shared Service Providers
- ◇ Discussion

Registration Issues

If PIV identity proofing process is used for PKI registration, then the process must meet the requirements of the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*

- ☑ A signed declaration by the registration authority (RA) that he or she verified the identity of the Applicant as required by the CPS (Section 3.1.9)
- ☑ A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the RA (Section 3.1.9)
- ☑ The CA shall ensure that registration information is accepted only from approved RAs. (Section 2.1.3)
- ☑ RAs shall conduct an annual compliance audit. (Section 2.7.1)
- ☑ A Registration Practice Statement (Section 4.0 FICC RA Requirements)

Electronic Components of PIV Card



Card Management Key

Card Authentication Key

Key Management Key ← PKI

Digital Signature Key ← PKI

Facial Image

Optional

Printed Data (copy)

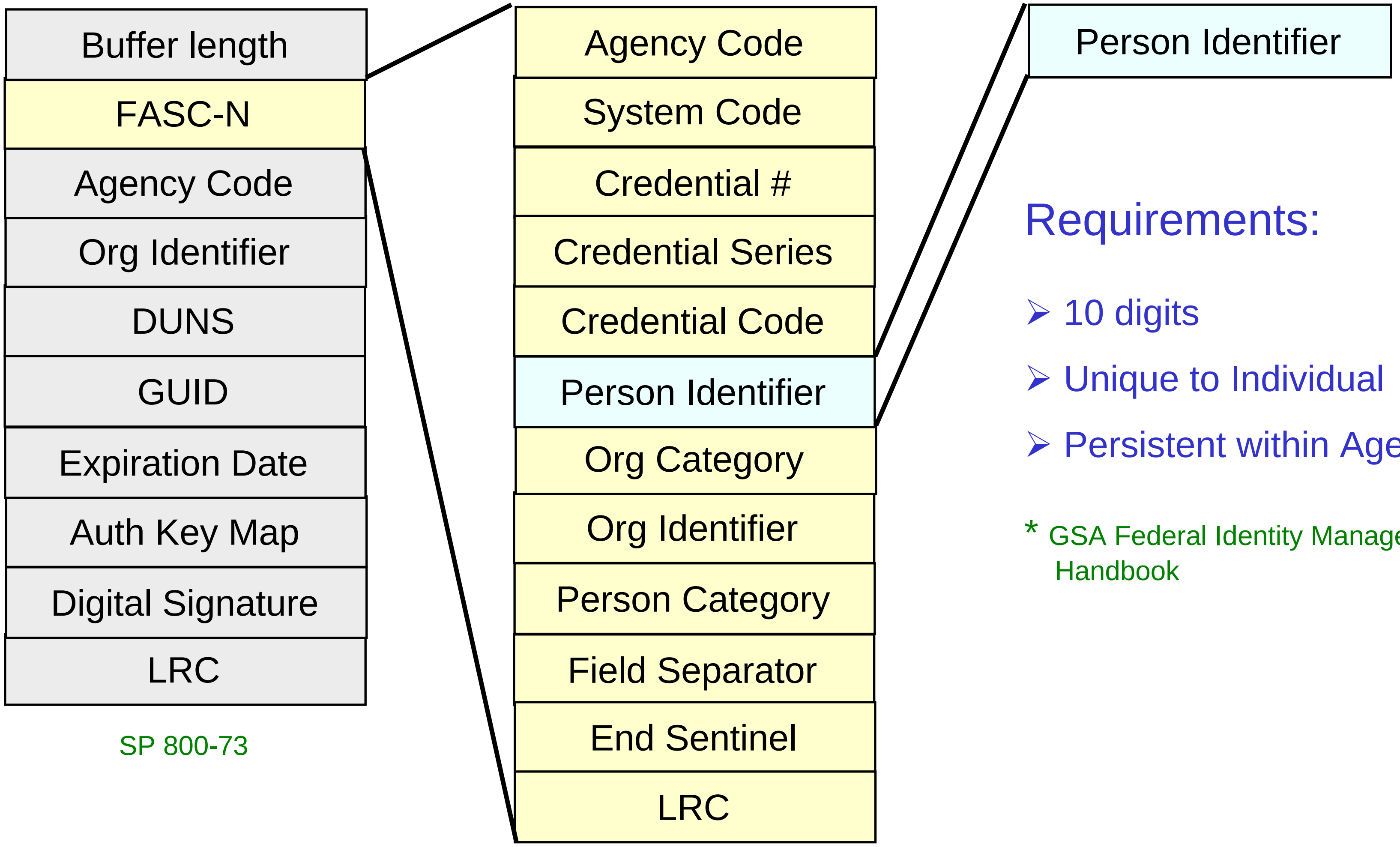
Fingerprints

PIV Authentication Key ← PKI

Required

CHUID ☜ **Identifies User**

Card Holder Unique Identifier (CHUID)



CHUID

- Buffer length
- FASC-N
- Agency Code
- Org Identifier
- DUNS
- GUID
- Expiration Date
- Auth Key Map
- Digital Signature
- LRC

SP 800-73

FASC-N

Federal Agency Smart Credential Number

- Agency Code
- System Code
- Credential #
- Credential Series
- Credential Code
- Person Identifier
- Org Category
- Org Identifier
- Person Category
- Field Separator
- End Sentinel
- LRC

TIG SCEPACS 2.2

PI

- Person Identifier

Requirements:

- 10 digits
- Unique to Individual
- Persistent within Agency*

* GSA Federal Identity Management Handbook

PIV Card PKI Related Data Elements

Data fields loaded onto card's smart chip

CHUID	The Cardholder Unique Identifier is a multi-part data field that identifies the card holder to IT systems and the badge to physical access control systems (PACS).
Certificates	Three digital certificates: 1. Authentication certificate for logical access 2. Digital signature certificate (optional) 3. Key management certificate for encrypted email (optional)
PIN	Numeric password that protects the PKI keys and biometrics.
Biometrics	Fingerprint biometrics used to verify the owner of the card when issuing PKI certificates or enforcing strong logical or physical access controls.

Data contained in the digital certificates

DN	Distinguished Name in a ***recommended*** form of: CN= Name + [affiliation]; UID = PI; OU = Organization
FASC-N	Federal Agency Smart Credential Number is a multi-field component of the CHUID
email	Primary SMTP email address required for encrypted and digitally signed email.
UPN	User principle name required for native Microsoft desktop smartcard login.
NACI	FIPS 201-1, adds NACI indicator extension showing NACI completion status.

Shared Service Provider

HSPD-12 Requires the use of PIV Card to gain logical access to Federally controlled information systems.

FIPS 201 Certificates issued to support PIV Card authentication shall be issued under Federal PKI Common Policy Framework

☞ CAs that issue certificates to subscribers must issue CRLs at least once every 18 hours

M-05-05 Agencies must move to commercial managed services for public key infrastructure (PKI) ... to mitigate risks, Agencies must use shared service providers.

Currently, the commercial shared service providers are:

- Cybertrust (formerly BeTrusted U.S. Inc.)
- Operational Research Consultants, Inc.
- VeriSign, Inc

But….

What if your CA goes suddenly out of business......

Enron **Worldcom**

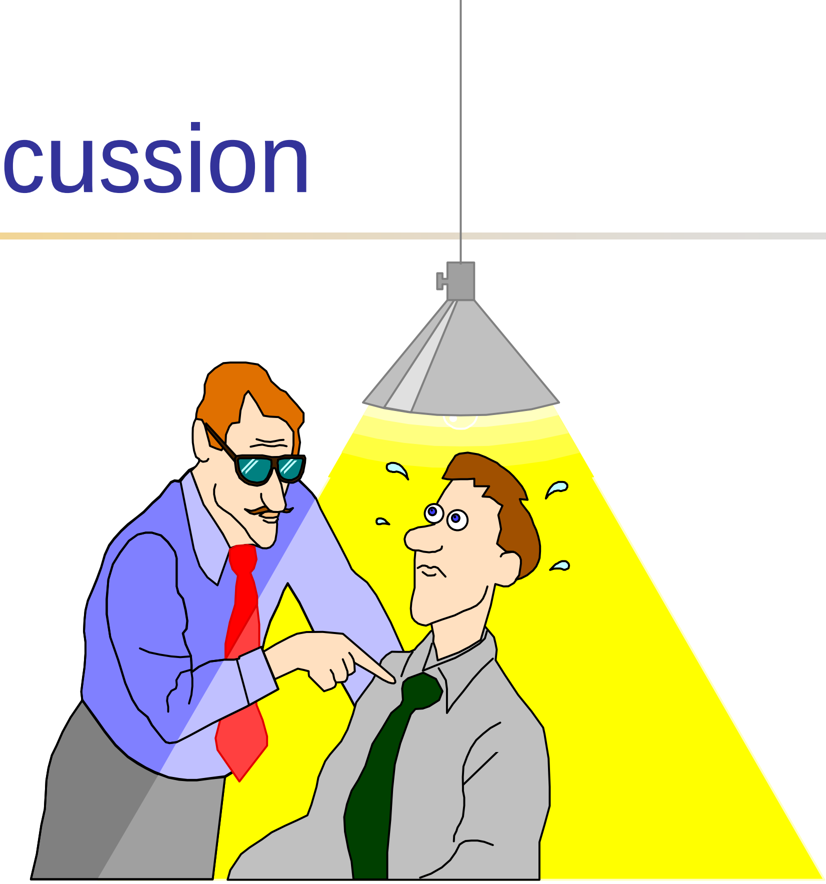
If a CRL is not published within 18 hours....

The certificate can not be validated!

The user should not be authenticated!

You now have a massive denial of service to your most critical (secure) applications

Questions & Discussion



Mark L. Silverman
301-496-2317
mls@nih.gov