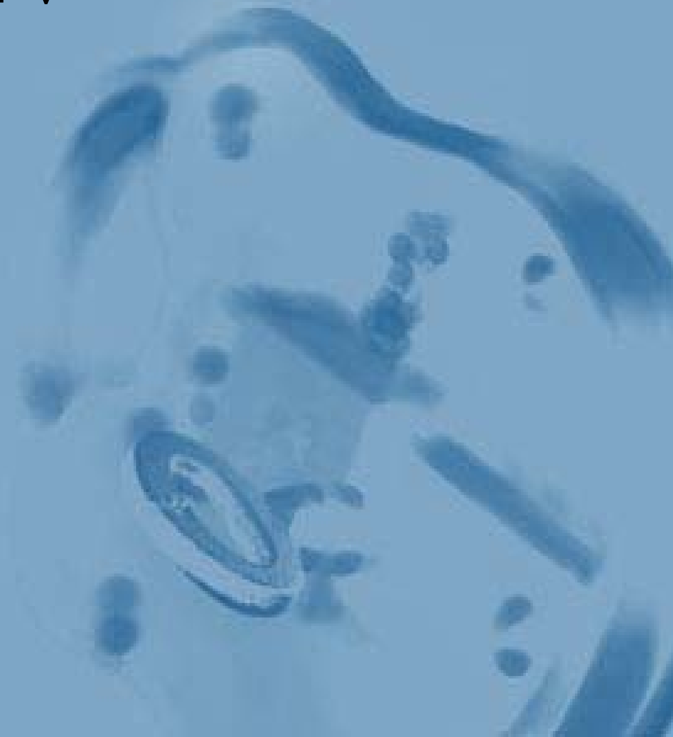
Department of State PKI Plan for PIV

R. Kenner Brent

2006/04/10



Agenda

- DoS Plan for Card Personalization
- DoS Smart Card and Certificate Usage
- PIV Challenges

PIV & PKI/BLADE Containers on new DoS Smart ID Card

PIV Container: PIN Access Required Used for Interoperable PIV authentication

CHUID — Card Holder Unique ID

PIV Biometric

SO — Security Object (Also appears in ePassport)

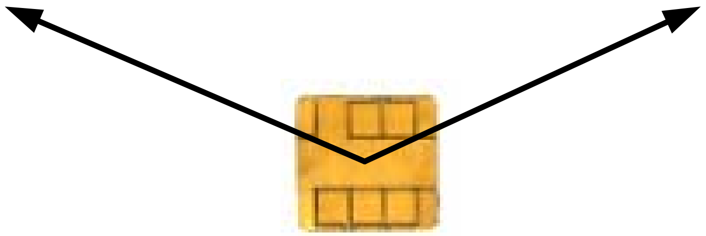
PIV Authentication Certificate

PKI/BLADE: Biometric match-on-card Used for Logical Access and PKE

Match-on-Card activation

eGov private keys and certificates

- Network Logon
- Secure Email
- Web applications
- Electronic Forms
- Financial Transactions
- Laptop Security
- eAuthentication
- Mainframe logon



Why the Split?

- Minimal impact to existing installed base
- Lack of existing PIV based applications
- Uncertainty of future requirements (affiliate) or (*affiliate*)?
- Ease of migration to end point
- Compatibility with non PIV Smart ID cards
- Existing user certificates do not comply with FPKI Common Policy yet

DoS PIV Authentication Certificate Options

- Issued by new CA subordinate to existing FBCA cross-certified Root, that meets the FPKI Common Policy
- RSA 2048
- SHA 256 for CA certificates (SCL issue for XP?)
- No Optional Extensions

Card/Certificate Applications

- PIV
- MS CAPI
  - Web Authentication
  - Smart Card Logon
  - Digital Signatures for Documents
- PKCS #11
  - Secure Email
  - eForms
  - Laptop Security

Certificate Size

1869 > 1612

Validity Period

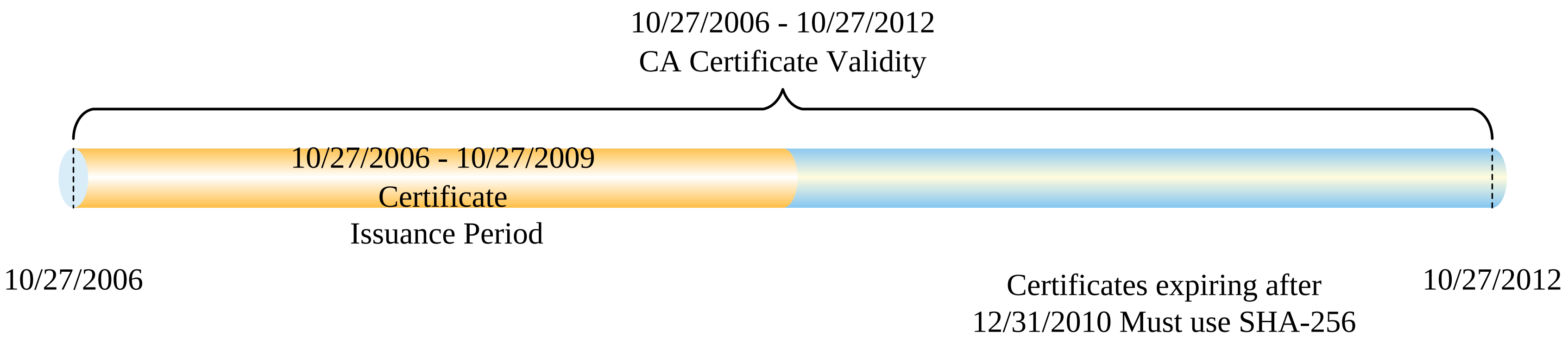
- FIPS 201: Maximum 5 Year ID card lifetime
- FPKI Common Policy: Maximum 3 year certificate lifetime
- PIV Authentication Certificate
- PIV Issuer Certificate
- State Department Solution 2 years 11 months maximum validity period

Other Challenges

- Selection of a Shared Service Provider
- Timeline (Accreditation)
- FBCA = Common Policy ?
- Decryption Key History
- Product Availability
- Remote Access – deployment of card readers
- OCSP
- Web Presence for CRLs and OCSP responses
- AD Naming vs. FPKI Common Policy

Confusing Tidbits

- NIST SP 800-73-1 errata Table in Appendix-A never updated
- FPKI Common Policy Profile has work sheet for PIV Authentication Certificate not referenced by FIPS 201-1



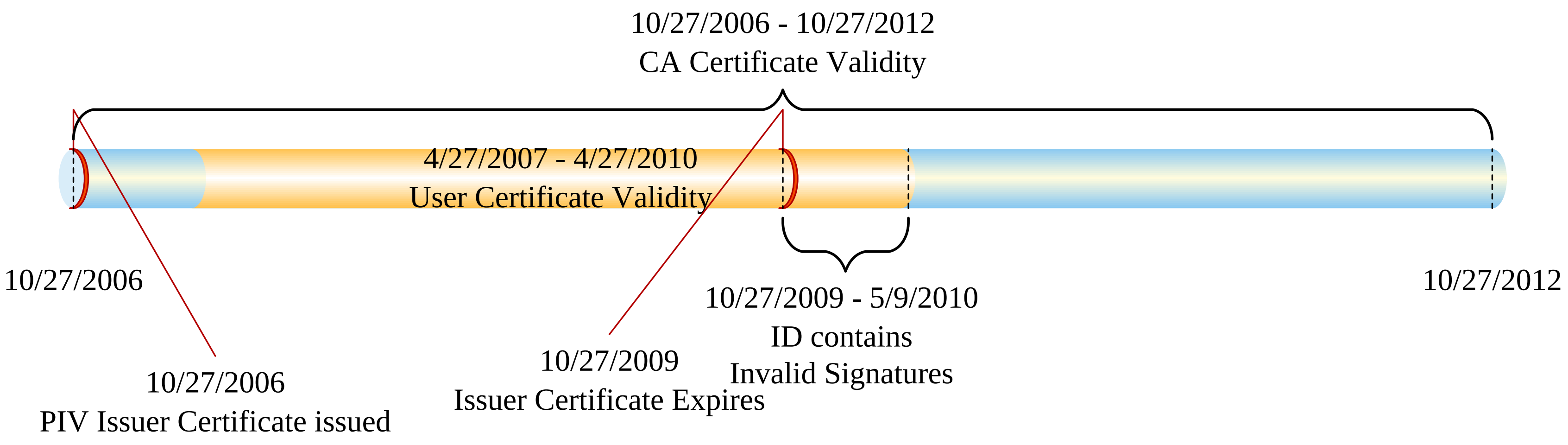
10/27/2006 - 10/27/2012
CA Certificate Validity

10/27/2006 - 10/27/2009
Certificate
Issuance Period

10/27/2006

Certificates expiring after
12/31/2010 Must use SHA-256

10/27/2012



10/27/2006 - 10/27/2012
CA Certificate Validity

4/27/2007 - 4/27/2010
User Certificate Validity

10/27/2006

10/27/2012

10/27/2009 - 5/9/2010
ID contains
Invalid Signatures

10/27/2009
Issuer Certificate Expires

10/27/2006
PIV Issuer Certificate issued

PIV & PKI/BLADE Containers on new PIV Smart ID Card

HAPPI: Physical Access and PIV Interoperability

Buffer Description	M/O	Dig Sig	Source	Notes
Card Capabilities Container	M	N	DS	
Card Holder Unique Identifier	M	Y	DS	Contains key map for Card Authentication Key
X.509 Certificate for PIV Authentication	M	Y	IRM	
Card Holder Fingerprints	M	Y	DS	minutia
Printed Information	O	N	DS	
Card Holder Facial Image	O	N	DS	
X.509 Certificate for Card Authentication	O	Y	DS	Symmetric Key - Not X.509
Security Object	M	Y	IRM	Contains signed hashes of all buffers

PKI/BLADE: Activated by biometric match-on-card

Buffer Description	Notes
X.509 Certificate for Digital Signatures	Also used for Authentication
X.509 Certificate for Key Encipherment	Encryption/Decryption
Decryption Key History	Field size will increase as history gets longer
Entrust Options	Proprietary management options

- Network Logon
- Secure Email
- Web applications
- Electronic Forms
- Financial Transactions
- Laptop Security
- eAuthentication