LDS & PKI Maintenance

Tom Kinneging

ISO/IEC JTC1 SC17 WG3

New Technology Working Group (NTWG)
TAG/MRTD 20

20st Meeting of the Technical Advisory Group on Machine Readable Travel Documents

TAG/MRTD 19 - Information Paper 2

- ePassport's 5th anniversary
- Evaluation of LDS and PKI specifications
  - Technology evolution
  - Increasing computer power
  - Preserve level of accuracy and security
- Technical Report "LDS and PKI Maintenance"
  - To be presented at TAG/MRTD 20
  - Review cycles by NTWG

TR “LDS and PKI Maintenance”

- Drafting by ISO/IEC SC17 WG3/TF5
- NTWG reviews
  - Sydney, October 2009
  - Bangkok, March 2010
  - Tokyo, October 2010
  - Bern, May 2011
- Subjects
  - LDS version information
  - Certificate profiles
  - Access control
  - Active Authentication
  - Extended Length

LDS version information

- File EF.COM
  - Not electronically signed
- Undetected manipulation possible
  - Masking of new security features
- Extension of SO_D with signed attribute
  - LDS version
  - Unicode version
  - Protected by Passive Authentication
- Implementation strategy
  - LDS V1.8
  - Removal of EF.COM in next version after LDS V1.8

Certificate profiles

- CSCA and DS certificates
  - In some cases too strict
  - In some cases not strict enough
- Interoperability issues
- Revised certificate profiles
  - CSCA certificates
  - DS certificates
- Added profiles
  - CSCA Master List signer certificates
  - Communications certificates
- Implementation strategy
  - At next CSCA roll-over

Access control

- BAC evaluated
  - Future technology developments
  - Passport validity periods
- Revised access control mechanism
  - TR Supplemental Access Control
  - Endorsed at TAG/MRTD 19
- Implementation strategy
  - BAC remains default access control mechanism
  - Promote implementation within 5 years from TAG/MRTD 19

Active Authentication

- Cryptographic algorithms in Doc 9303
  - RSA
  - DSA
  - ECDSA
- Supplement to Doc 9303, Release 7
  - Conflicting references (X9.62 vs. ISO/IEC 9796-2)
  - RSA for Active Authentication
- Use of ECDSA for AA specified
  - Unambiguous
- Implementation strategy
  - n/a

Extended Length

- Specifications under development
  - ISO/IEC JTC1 SC17 WG4
  - Information exchange between IC and Reader concerning Extended Length communications
  - Not concluded yet
- Still open
  - Conclusions in Doc 9303 or referenced to once finalized

Working Paper

- The TAG-MRTD is invited to
  - Recognize the necessity of a regular evaluation of the specifications in Doc 9303 to preserve the appropriate level of accuracy and security
  - Approve the Technical Report “LDS and PKI Maintenance” containing the revised specifications for inclusion into Doc 9303

Thank you
for your attention

Tom Kinneging

ISO/IEC JTC1 SC17 WG3

New Technology Working Group (NTWG)
TAG/MRTD 20

20st Meeting of the Technical Advisory Group on Machine Readable Travel Documents