INSPECTING ePASSPORTS AT THE BORDER
Maximizing Security that Biometric Travel Documents offer

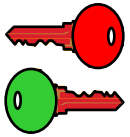
Tom Kinneging
Senior expert standardization, Morpho, Netherlands
Convenor ISO/IEC JTC1 SC17 WG3

Electronic security features

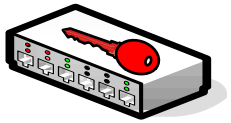
- Privacy protection
  - Basic Access Control
  - Supplemental Access Control
- Anti copying
  - Active Authentication
- Data authenticity and integrity
  - Passive Authentication

Passive Authentication

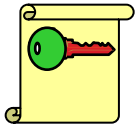
- Digital signature
  - Private Key for signing
  - Public Key for verification



- Private Key safe keeping
  - Confidentiality
  - HSM

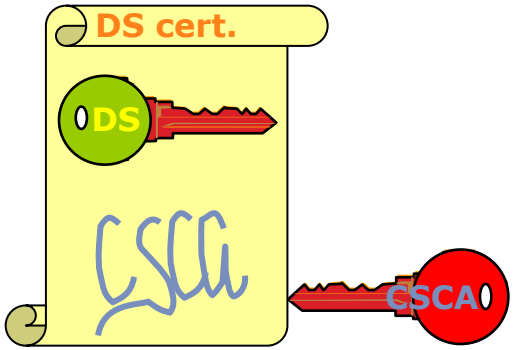


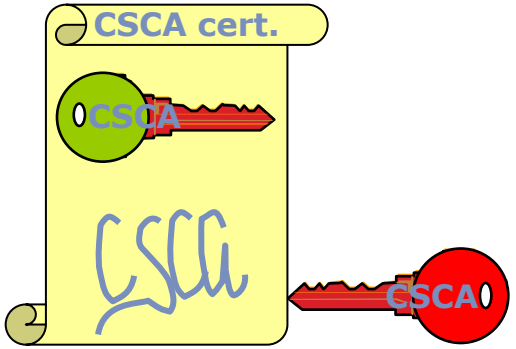
- Public Key distribution
  - Trust
  - Authenticity
  - Integrity
  - Public Key certificate



Certificates

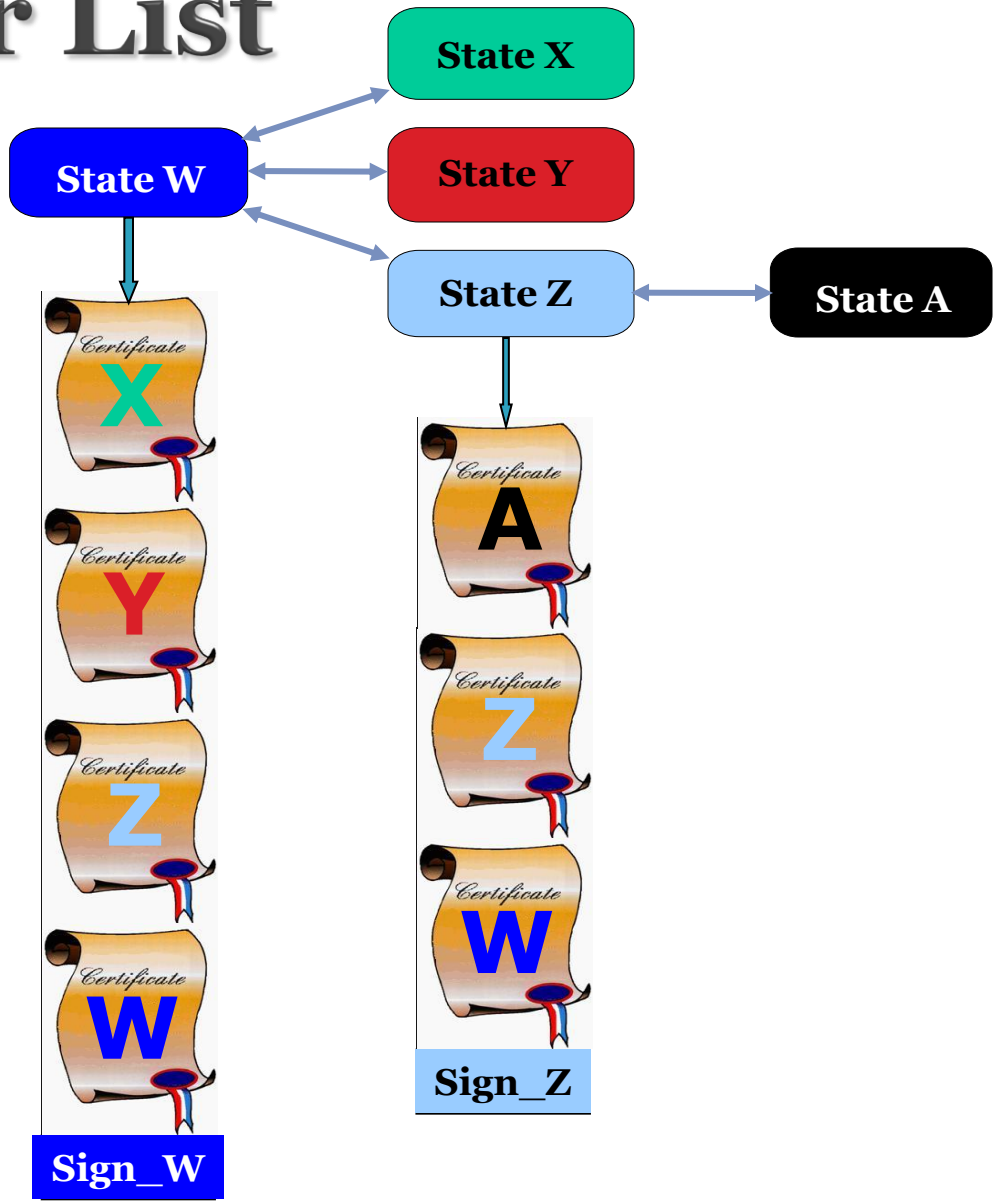
- Document Signer
  - DS certificate
  - Many documents
  - Short lifetime
  - Automated distribution
- Country Signing Certificate Authority
  - CSCA certificate
  - Not so many Document Signers
  - Longer lifetime
  - Manual (bilateral) distribution





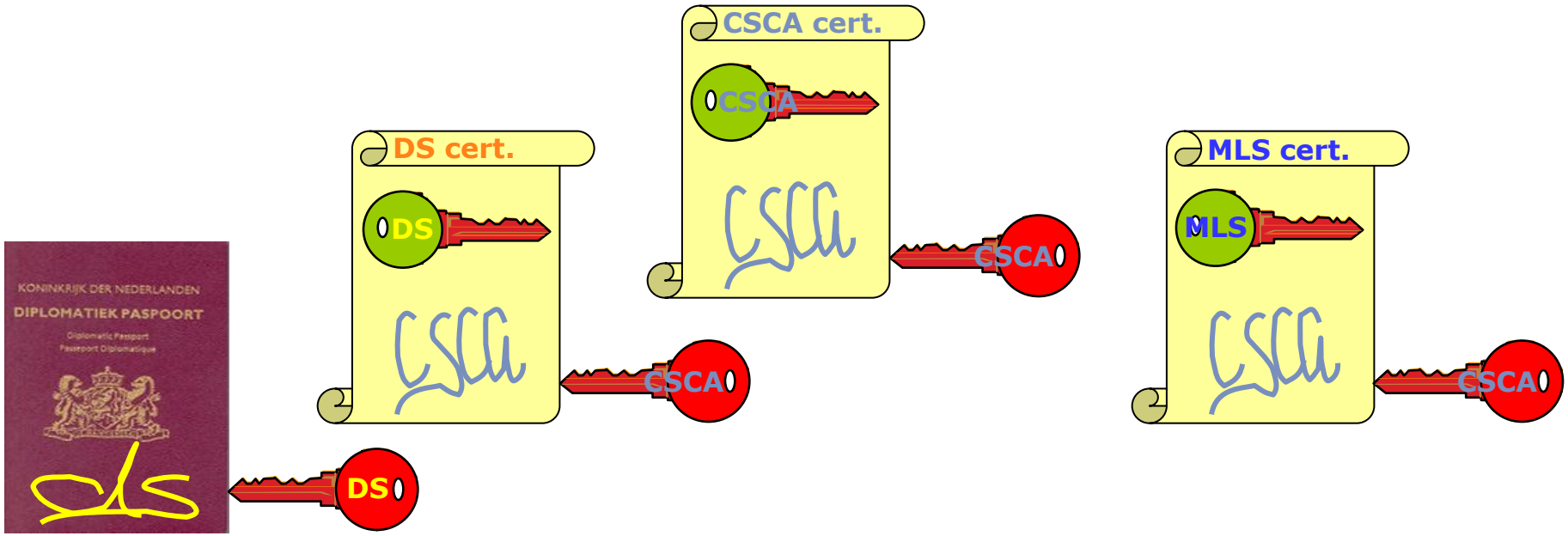
CSCA Master List

- State-to-State service
- Automated distribution



Certificates

- Master List Signer
- ML Signer certificate
  - Automated distribution



Revocation

- Private Key compromised
  - Trust in signatures damaged
  - Trust in ePassports damaged?
- Inform relying parties
- Certificate Revocation List (CRL)
  - Signed
  - Revoked certificates…
  - …or Empty
  - Automated distribution

Distribution

- Document Signer certificate
  - ePassport chip
  - PKD
- Country Signing CA certificate
  - Bilateral
  - Master List
- Master List
  - PKD
- Certificate Revocation List
  - Bilateral
  - PKD

ICAO Public Key Directory

- IS
  - a central repository for
    - CSCA Master Lists
    - Document Signer certificates
    - Certificate Revocation Lists
- OFFERS
  - Upload and download facilities
  - Document Signer certificate validation
  - CSCA Master List validation
  - CRL validation
  - Information on non-conformities
  - A platform to discuss certificate issues

BUT

ICAO Public Key Directory

- IS NOT
  - a Certificate Authority
  - an Inspection System
  - replacing border control systems and policies
- DOES NOT OFFER
  - ‘WSCA’ certificates
  - liability for validation procedures
  - prevention of illegal entry
  - Passive Authentication

Maximizing security

- Proper inspection preparation
  1. *Trusted* CSCA certificates
     - Bilateral/diplomatic
       - Verify identity
     - *Trusted* Master List
       - Verify Master List Signer certificate's signature (with *trusted* CSCA public key)
       - Verify Master List's signature (with *trusted* ML signer public key)
  2. *Trusted* DS certificates
     - MRTD's chip
       - Verify DS certificate's signature (with *trusted* CSCA public key)
     - PKD
       - Verify DS certificate's signature (with *trusted* CSCA public key)
  3. *Trusted* CRLs
     - Bilateral
       - Verify CRL's signature (with *trusted* CSCA public key)
     - PKD
       - Verify CRL's signature (with *trusted* CSCA public key)

Maximizing security

- Proper inspection execution
  4. Document Security Object
     - MRTD's chip
       - Verify SO_D's signature (with *trusted* DS public key)
  5. Data Groups
     - MRTD's chip
       - Passive Authentication

Conclusions

- Security that Biometric Travel Documents offer is powerful
  - Passive Authentication
    - Data integrity and authenticity
  - Active Authentication
    - Chip authenticity
- Maximizing Security that Biometric Travel Documents offer
  - Proper use of the MRTD Public Key Infrastructure
  - Full certificate chain verification
  - ICAO Public Key Directory
    - MRTD program's central repository
    - not the 'solution to all your problems'
  - Inspection authorities
    - policies
    - procedures
    - systems

Thank you for your attention

SAFRAN
Morpho

Tom KINNEGING
Senior Expert Standardization
Product Line ID Documents

tom.kinneging@morpho.com
M +31 65 12 13 702
T +31 23 79 95 218

Morpho B.V.
P.O. Box 5300, 2000 GH Haarlem, The Netherlands
www.morpho.com