

**Regional Seminar on MRTDs, Biometrics and Identification Management
Sint Maarten, 9-11 July 2013**



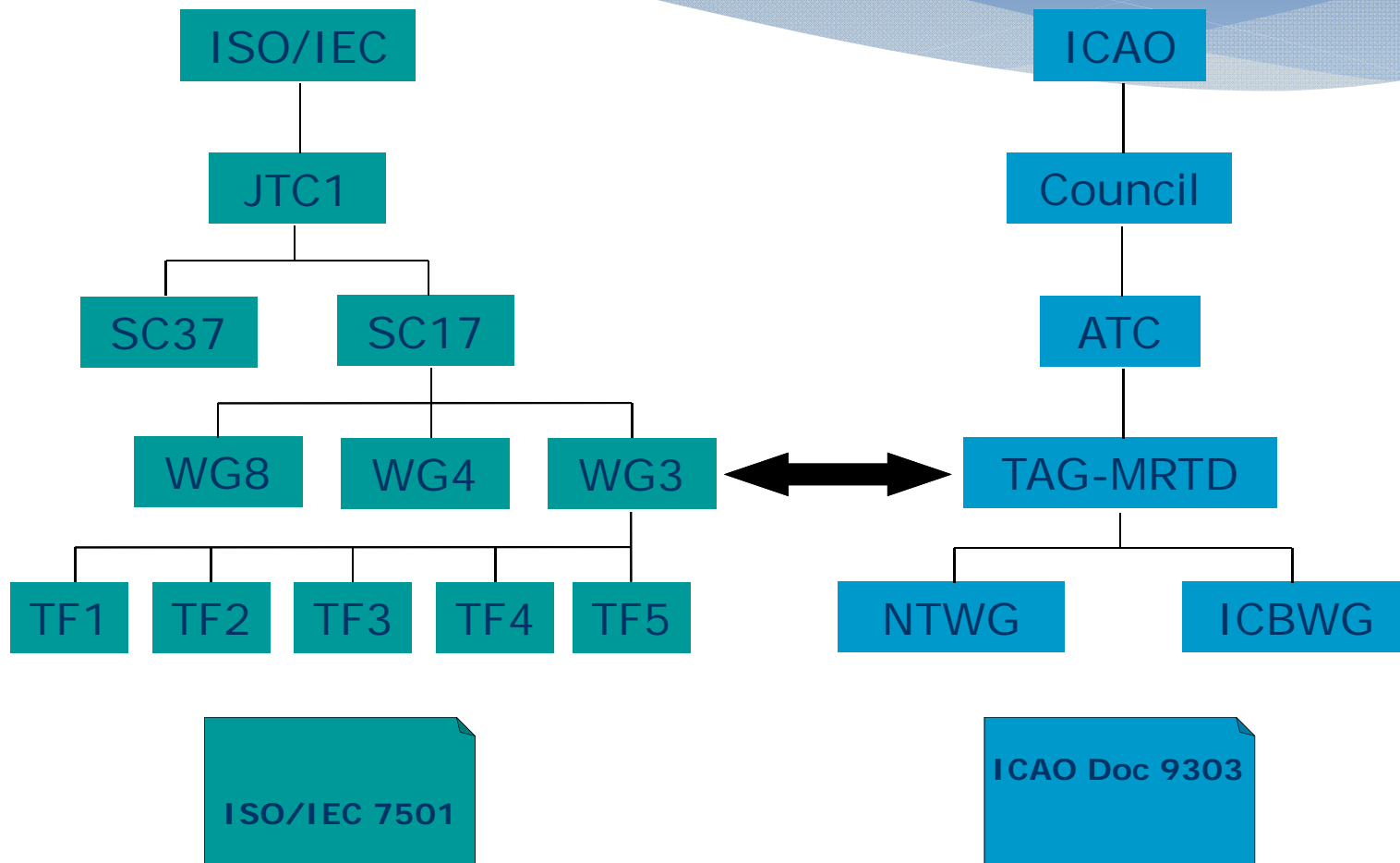
ICAO MRTD and eMRTD Standards and Specifications

Tom Kinneging

Senior expert standardization, Morpho, Netherlands

Convenor ISO/IEC JTC1 SC17 WG3

ICAO-ISO collaboration



Doc 9303

- Part 1 - Machine Readable Passports, Sixth edition - 2006
- Part 2 - Machine Readable Visas, Third edition - 2005
- Part 3 - Machine Readable Official Travel Documents, Third edition - 2008

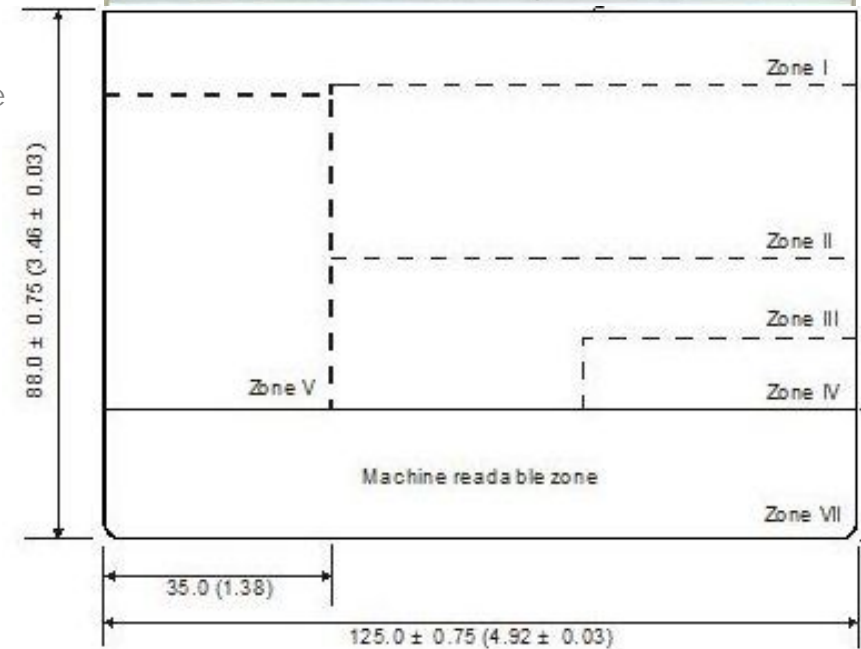
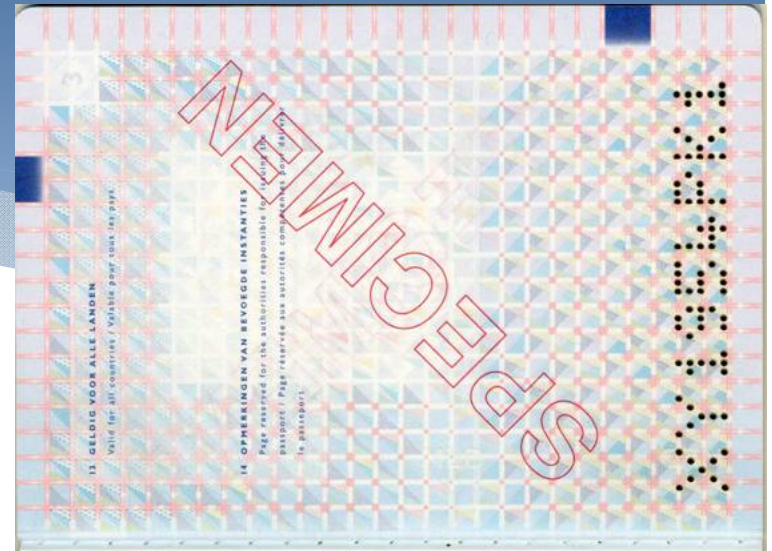
Doc 9303 - Part 1

Machine Readable Passports

- Introduction
- References and definitions
- Security of design, manufacture and issuance
 - Security standards
 - Machine assisted document security verification
 - Prevention of fraud associated with the issuance process
- Technical specifications of MRPs
 - Physical characteristics
 - Layouts and zones
 - Data structures
 - Representations of States, Nationalities, Dates
 - Three letter codes
 - Transliterations
 - Guidelines for portraits

Doc 9303 - Part 1

- Data Page
 - Zone I - Header
 - Zone II - Personal data elements
 - Zone III - Document data elements
 - Zone IV - Signature
 - Zone V - Identification feature
 - Zone VI - Optional data elements on reverse side
 - Zone VII - Machine Readable Zone (2x 44)



Doc 9303 - Part 2

Machine Readable Visas

- Introduction
- Technical specifications for Machine Readable Visas
- Technical specifications common to all MRVs
 - Physical characteristics
 - Security aspects
 - Layouts and zones
 - Representations of States, Nationalities, Dates
 - Machine reading requirements
 - Three letter codes
 - Transliterations
- Technical specifications for format-A MRVs
- Technical specifications for format-B MRVs

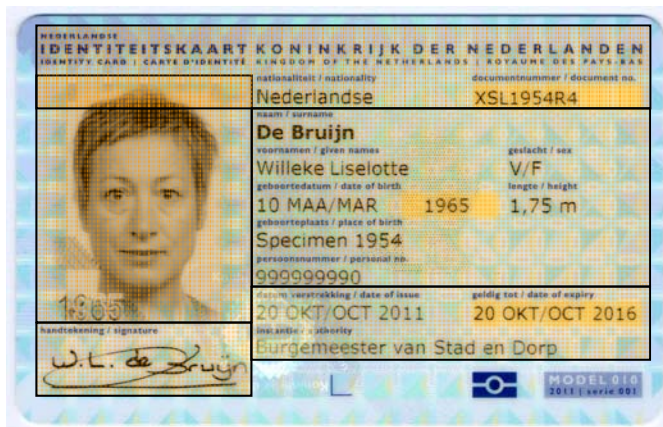
Doc 9303 - Part 3

Machine Readable Official Travel Documents

- Introduction
- References and definitions
- Security of design, manufacture and issuance
 - Security of the MRtd and its personalization
 - Machine assisted document security verification
 - Prevention of fraud associated with the issuance process
- Technical specifications common to both Size 1 and Size 2
 - Physical characteristics
 - General layouts and zones
 - Representations of States, Nationalities, Dates
 - Three letter codes
 - Transliterations
 - Guidelines for portraits
- Technical specifications unique to Size 1
 - Dimensions
 - Data structures
- Technical specifications unique to Size 2
 - Dimensions
 - Data structures

Doc 9303 - Part 3

- Size 1
 - Zone I - Header
 - Zone II - Personal data elements
 - Zone III - Document data elements
 - Zone IV - Signature
 - Zone V - Identification feature
 - Zone VI - Optional data elements
 - Zone VII - Machine Readable Zone (3x 30 characters)



Doc 9303 - Part 1/3 Volume 2

- RFID chip
 - High capacity
 - Independent of location in document
 - Capable of performing cryptographic operations
 - Existing standards (ISO/IEC)
- Biometrics - Face
 - Least cultural obstructions
 - Everybody has it
 - Capture at a distance
 - Interoperable (image)
 - Also usable without biometric verification

Doc 9303 - Part 1/3 Volume 2

- Logical data Structure (LDS)
 - Data Group 01 - Machine Readable Zone
 - Data Group 02 - Encoded face
 - Data Group 03 - Encoded fingers
 - Data Group 04 - Encoded Irises
 - Data Group 05 - Displayed portrait
 - Data Group 06 - Reserved for future use
 - Data Group 07 - Displayed signature or usual mark
 - Data Group 08 - Data features
 - Data Group 09 - Structure features
 - Data Group 10 - Substance features
 - Data Group 11 - Additional personal details
 - Data Group 12 - Additional document features
 - Data Group 13 - Optional details
 - Data Group 14 - Security options for secondary biometrics
 - Data Group 15 - Active Authentication public key info
 - Data Group 16 - Persons to notify

Doc 9303 - Part 1/3 Volume 2

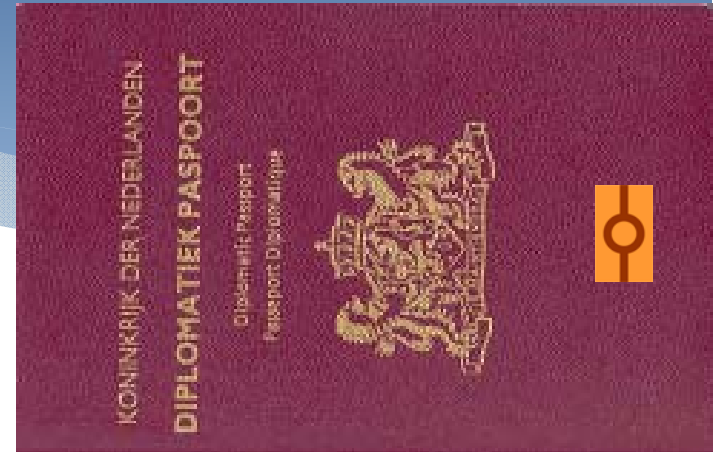
- Electronic security
 - Basic Access Control
 - Passive Authentication
 - Active Authentication
 - Public Key Infrastructure

Basic Access Control

Privacy protection

???

- You can't read a closed book
 - Hand over willingly
 - Open passport book
- Skimming
 - Unauthorized contacting and reading
- Eavesdropping
 - On existing communications



Passive Authentication

Authenticity and Integrity

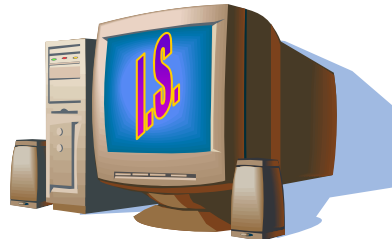
- Digital Signature
 - Cryptographic operation
 - Calculated over LDS Data Groups contents
 - Stored on MRTD's chip
 - Verifiable at inspection
- Private / Public key pair
 - Private Key for signing
 - Public Key for verification



Active Authentication

Anti copying

- Digital Signature
 - Private Key in chip's secure memory
 - Public Key in LDS Data Group 15



Passive Authentication

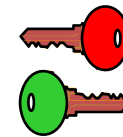


Public Key Infrastructure

For Passive Authentication

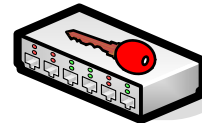
- Digital Signature

- Private Key for signing
- Public Key for verification



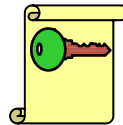
- Private Key safe keeping

- Confidentiality
- HSM



- Public Key distribution

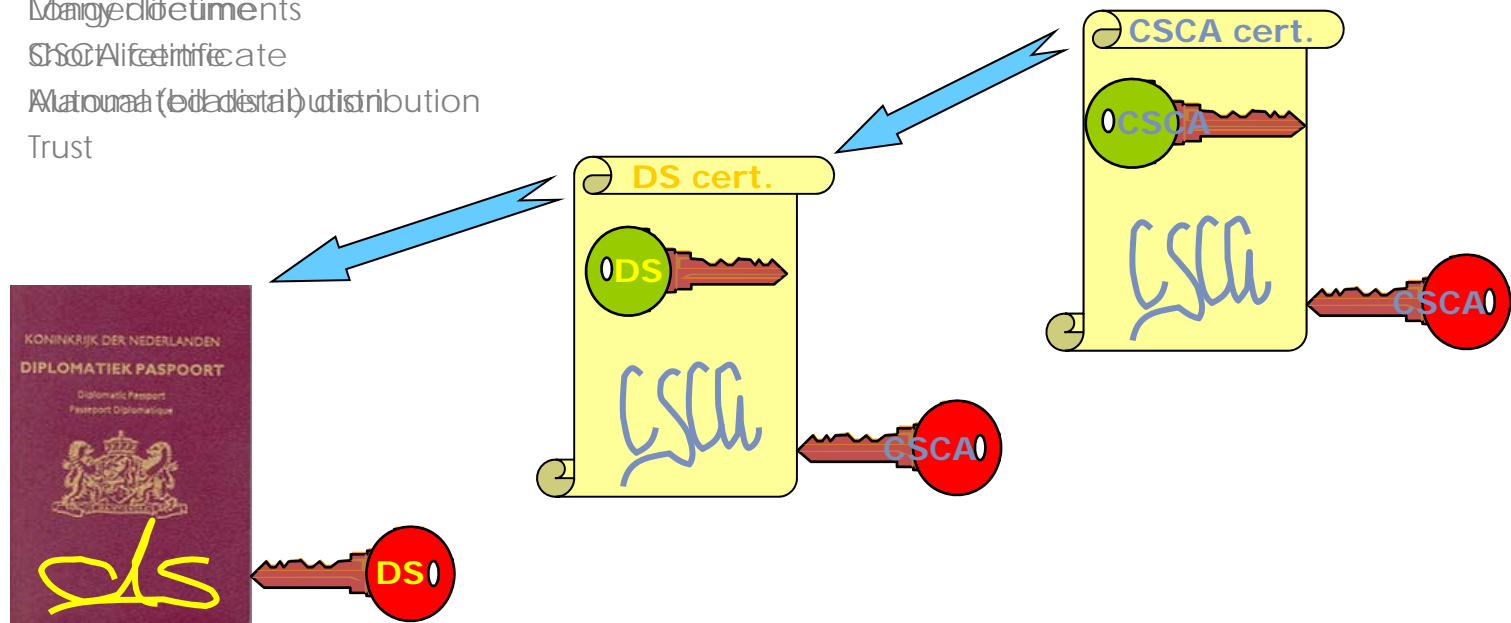
- Trust
- Authenticity
- Integrity
- Public Key certificate



Public Key Infrastructure

Certificates

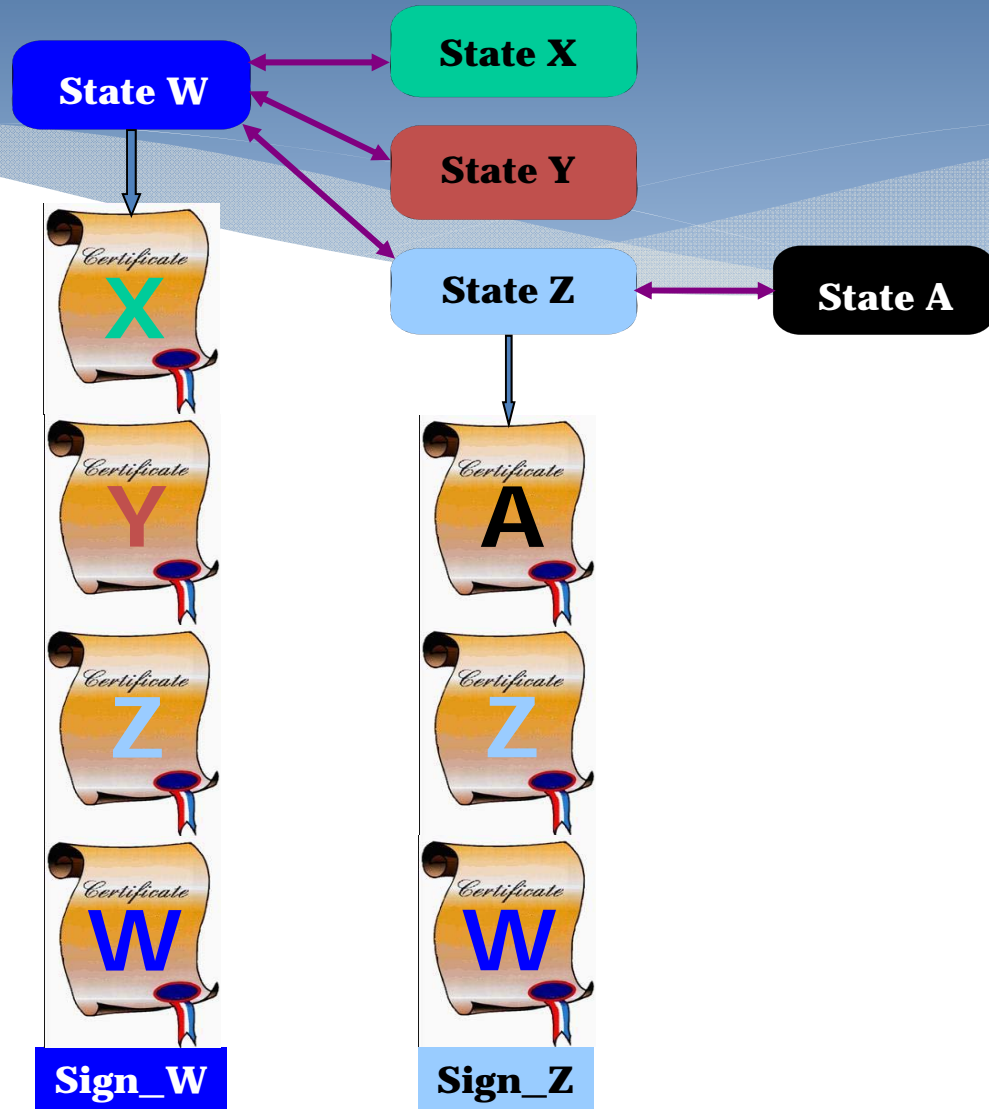
- Document Signer
- ~~Document~~ Signing Certification Authority
 - Not so many Document Signers
 - Many lifetimes
 - Self certificate
 - Manual (or distal) distribution
 - Trust



Public Key Infrastructure

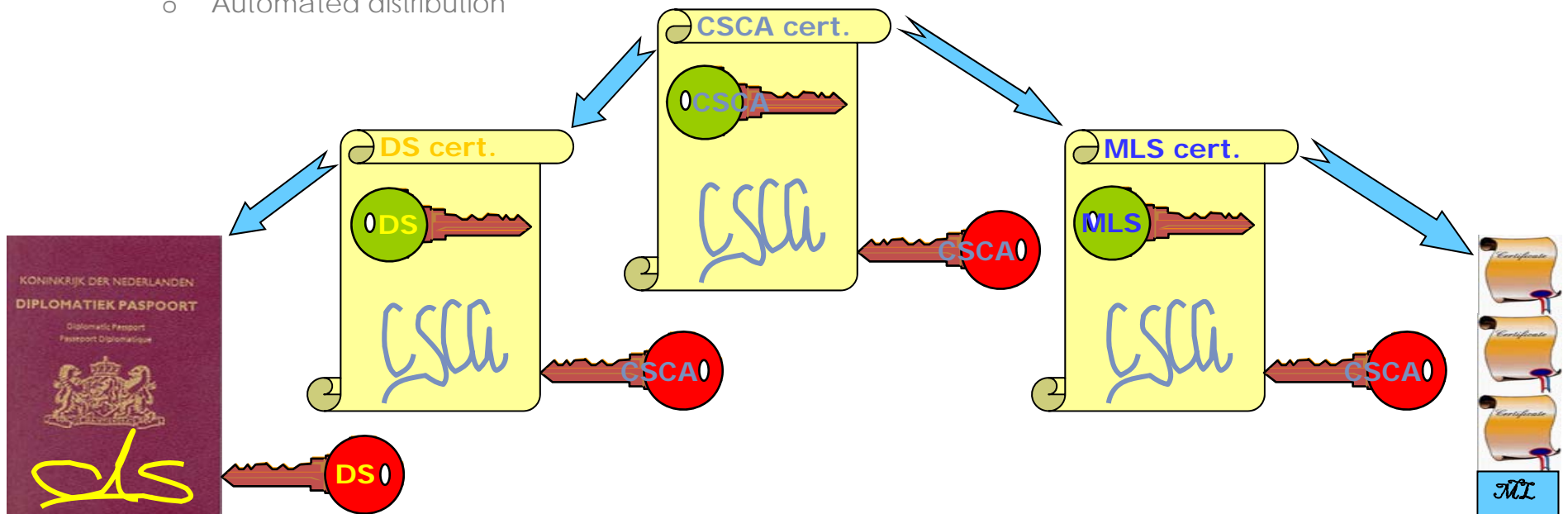
Certificates

- CSCA Master List
 - State-to-State service
 - Automated distribution



Public Key Infrastructure Certificates

- Master List Signer
- Master List Signer certificate
 - Signed by CSCA
 - Automated distribution



Public Key Infrastructure

Revocation

- Private Key compromised
 - Trust in certificates damaged
 - Trust in ePassports damaged?
- Inform relying parties
- Certificate Revocation List (CRL)
 - Signed by CSCA
 - Revoked certificates
 - ... or Null
 - Automated distribution

Public Key Infrastructure Distribution

- Document Signer certificates
 - ePassport's chip
 - PKD
- Country Signing CA certificates
 - Bilateral
 - CSCA Master List
- CSCA Master Lists
 - PKD
- Certificate Revocation Lists (CRL)
 - Bilateral
 - PKD

Public Key Infrastructure

ICAO Public Key Directory

- The PKD is a central repository
 - Upload and download facilities
 - Document Signer certificates
 - CSCA Master Lists
 - Certificate Revocation Lists
 - Doc 9303 compliancy reference and validation service
- The PKD is not
 - A certification authority
 - An inspection system
 - Replacing border control systems and policies
 - Preventing illegal entry

The Doc 9303 standard

- Part 1 - Machine Readable Passports, Sixth edition - 2006
 - Volume 1 - Passports with Machine Readable data stored in OCR format
 - Volume 2 - Electronically enabled Passports with Biometric Identification Capability
- Part 2 - Machine Readable Visas, Third edition - 2005
- Part 3 - Machine Readable Official Travel Documents, Third edition - 2008
 - Volume 1 - MRtds with Machine Readable data stored in OCR format
 - Volume 2 - Electronically enabled MRtds with Biometric Identification Capability

<http://www.icao.int/security/mrtd/pages/default.aspx>



THANK YOU



Tom KINNEGING

Senior Expert Standardization
Business Unit 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