# Security and Policy considerations for MRTDs

*Doc 9303 - Machine Readable Travel Documents*

Tom Kinneging

*Senior advisor, OT-MORPHO*
*Convener ISO/IEC JTC1 SC17 WG3*

Hong Kong ICAO TRIP Regional Seminar

# ICAO Doc 9303 - 7th edition

1. Introduction
2. Specifications for the Security of Design, Manufacture and Issuance of MRTDs
3. Specifications common to all Machine Readable Travel Documents
4. Specifications specific to TD3 size MRTDs, Machine Readable Passports
5. Specifications specific to TD1 size MRTDs, Machine Readable Official Travel Documents
6. Specifications specific to TD2 size MRTDs, Machine Readable Official Travel Documents
7. Machine Readable Visas
8. Emergency Travel Documents
9. The Deployment of Biometric Identification and Electronic Storage of Data in MRTDs
10. Logical Data Structure
11. Security Protocols
12. Public Key Infrastructure for Machine Readable Travel Documents

# Doc 9303 - Part 1

## Introduction

1. Foreword
2. Scope
3. General considerations
4. Definitions and Abbreviations
5. Guidance on the use of Doc 9303
6. References

# Doc 9303 - Part 2

## Specifications for the Security of Design, Manufacture and Issuance of MRTDs

1. Scope
2. Security of the MRTD and its Issuance
3. Machine Assisted Document Verification
4. Security of MRTD Production and Issuance Facilities
5. Provision of Information on Newly Issued MRTDs
6. Provision of Information on Lost and Stolen MRTDs

Appendix A – Security Standards for MRTDs

Appendix B – Machine Assisted Document Security Verification

Appendix C – The Prevention of Fraud Associated with the Issuance Process

Appendix D – ASF/SLTD Key Considerations

# Doc 9303 - Part 3

## Specifications Common to all Machine Readable Travel Documents

1. Scope
2. Physical Characteristics of MRTDs
3. Visual Inspection Zone (VIZ)
4. Machine Readable Zone (MRZ)
5. Codes for Nationality, Place of Birth, Location of Issuing State/Authority and other Purposes
6. Transliterations Recommended for Use by States
7. Deviations
8. References

Appendix A – Examples of Check Digit Calculation

Appendix B – Arabic Transliteration, Details and Examples

# Doc 9303 - Part 4

## Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs

1. Scope
2. Construction and Dimensions of the MRP and MRP Data Page
3. General Layout of the MRP Data Page
4. Contents of the MRP Data Page
5. References

Appendix A – Examples of a Personalized MRP Data Page

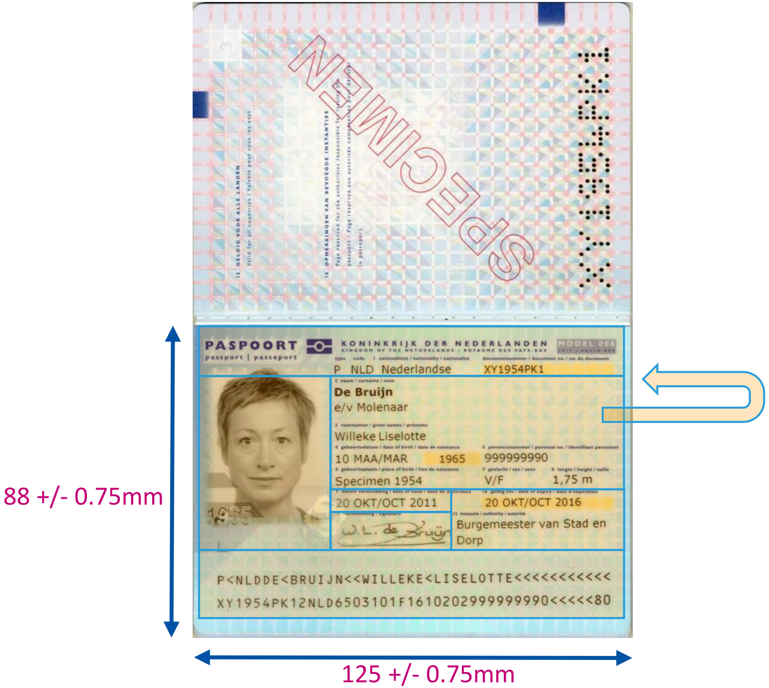
Appendix B – Construction of the Machine Readable Zone of the Passport Data Page

# Doc 9303 - Part 4

## Specifications for Machine Readable Passports (MRPs) and other TD3 size MRTDs

Data Page

1. Zone I - Header
2. Zone II - Personal data elements
3. Zone III - Document data elements
4. Zone IV - Signature
5. Zone V - Identification feature
6. Zone VI - Optional data elements (on reverse side)
7. Zone VII - Machine Readable Zone (2x 44)



PASPOORT passport | passeport
KONINKRIJK DER NEDERLANDEN
KINGDOM OF THE NETHERLANDS | ROYAUME DES PAYS-BAS
MODEL 008

P NLD Nederlandse XY1954PK1

De Bruijn
e/v Molenaar

Willeke Liselotte

10 MAA/MAR 1965 999999990

Specimen 1954 V/F 1,75 m

20 OKT/OCT 2011 20 OKT/OCT 2016

W.L. de Bruijn

Burgemeester van Stad en Dorp

```
P<NLDDE<BRUIJN<<WILLEKE<LISELOTTE<<<<<<<<<<<<
XY1954PK12NLD6503101F1610202999999990<<<<<80
```

# Doc 9303 - Part 5

## Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs)

1. Scope
2. Dimensions of the TD1 size MROTD
3. General Layout of the TD1 size MROTD
4. Contents of a TD1 size MROTD
5. References

Appendix A – Examples of a Personalized TD1 size MROTD

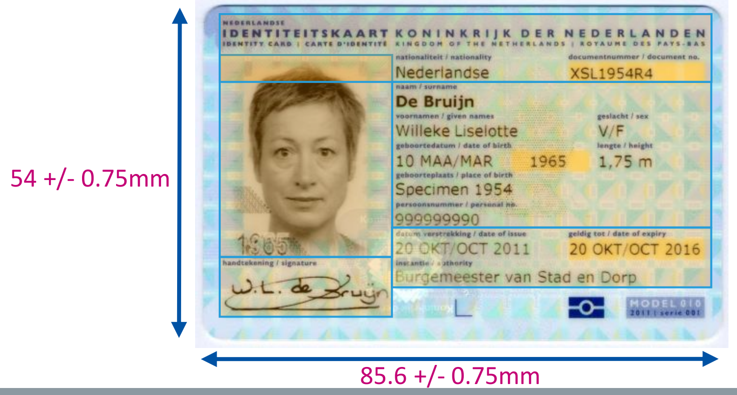
Appendix B – Construction of the Machine Readable Zone of a TD1 size MROTD

Appendix C – Technical Specifications for a Machine Readable Crew Member Certificate (CMC)

# Doc 9303 - Part 5

## Specifications for TD1 size Machine Readable Official Travel Documents (MROTDs)

1. Zone I - Header
2. Zone II - Personal data elements
3. Zone III - Document data elements
4. Zone IV - Signature
5. Zone V - Identification feature
6. Zone VI - Optional data elements
7. Zone VII - Machine Readable Zone (3x 30 characters)

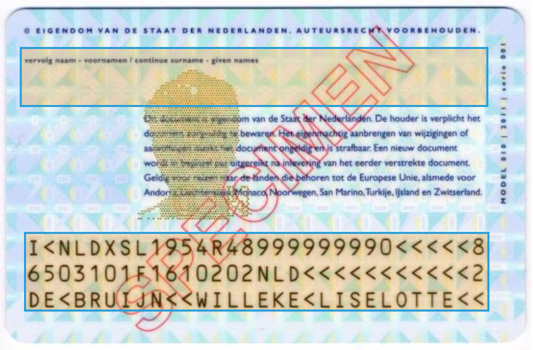


NEDERLANDSE
IDENTITEITSKAART KONINKRIJK DER NEDERLANDEN
IDENTITY CARD | CARTE D'IDENTITÉ KINGDOM OF THE NETHERLANDS | ROYAUME DES PAYS-BAS

nationaliteit / nationality: Nederlandse
documentnummer / document no.: XSL1954R4
naam / surname: De Bruijn
voornamen / given names: Willeke Liselotte
geslacht / sex: V/F
geboortedatum / date of birth: 10 MAA/MAR 1965
lengte / height: 1,75 m
geboorteplaats / place of birth: Specimen 1954
persoonsnummer / personal no.: 999999990
datum verstrekking / date of issue: 20 OKT/OCT 2011
geldig tot / date of expiry: 20 OKT/OCT 2016
instantie / authority: Burgemeester van Stad en Dorp
handtekening / signature: W.L. de Bruijn

MODEL 010
2011 | serie 001

1965
54 +/- 0.75mm
85.6 +/- 0.75mm



© EIGENDOM VAN DE STAAT DER NEDERLANDEN. AUTEURSRECHT VOORBEHOUDEN.

vervolg naam - voornamen / continue surname - given names

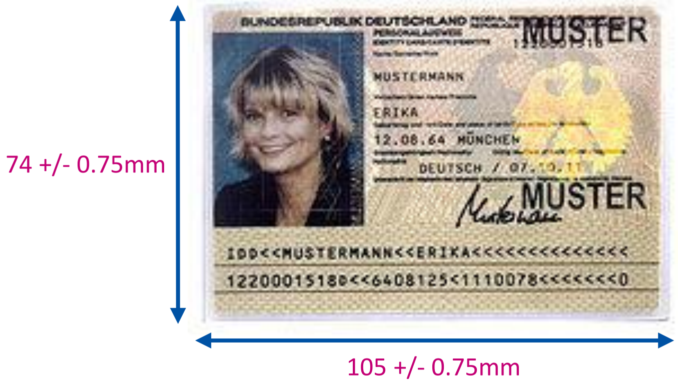
Dit document is eigendom van de Staat der Nederlanden. De houder is verplicht het document zorgvuldig te bewaren. Het eigenmachtig aanbrengen van wijzigingen of aantekeningen maakt het document ongeldig en is strafbaar. Een nieuw document wordt in beginsel pas uitgereikt na inlevering van het eerder verstrekte document. Geldig voor reizen naar de landen die behoren tot de Europese Unie, alsmede voor Andorra, Liechtenstein, Monaco, Noorwegen, San Marino,Turkije, IJsland en Zwitserland.

MODEL 010 | 2011 | serie 001

```
I<NLDXSL1954R48999999990<<<<<8
6503101F1610202NLD<<<<<<<<<<<2
DE<BRUIJN<<WILLEKE<LISELOTTE<<
```

# Doc 9303 - Part 6

## Specifications for TD2 size Machine Readable Official Travel Documents (MROTDs)



BUNDESREPUBLIK DEUTSCHLAND MUSTER

MUSTERMANN

ERIKA

12.08.64 MÜNCHEN

DEUTSCH / 07.10.11

MUSTER

IDD<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<

1220001518D<<6408125<1110078<<<<<<<<0

# Doc 9303 - Part 7

## Machine Readable Visas

1. Scope
2. Technical Specifications for Format-A Machine Readable Visas (MRV-A)
3. General Layout of the MRV-A
4. Detailed Layout of the MRV-A
5. Technical Specifications for Format-B Machine Readable Visas (MRV-B)
6. General Layout of the MRV-B
7. Detailed Layout of the MRV-B
8. Use of Optional barcodes on Machine Readable Visas
9. References

Appendix A – Examples of a Personalized MRVs

Appendix B – Construction of the MRZ

Appendix C – Positioning in Passport

Appendix D – Materials and Production Methods

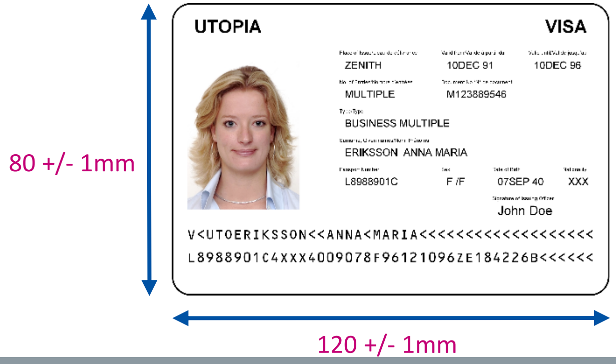
# Doc 9303 - Part 7

## Machine Readable Visas

MRV

- Zone I - Header
- Zone II - Personal data elements
- Zone III - Document data elements
- Zone IV - Signature
- Zone V - Identification feature
- Zone VII - Machine Readable Zone (MRV-A: 2x 44 characters / MRV-B: 2x 36 characters)

**MRV-A**


80 +/- 1mm
120 +/- 1mm

UTOPIA VISA

ZENITH 10DEC 91 10DEC 96

MULTIPLE M123889546

BUSINESS MULTIPLE

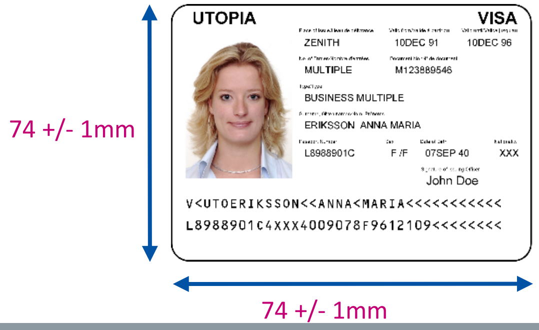
ERIKSSON ANNA MARIA

L8988901C F /F 07SEP 40 XXX

John Doe

```
V<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L8988901C4XXX4009078F96121096ZE184226B<<<<<<
```

**MRV-B**


74 +/- 1mm
74 +/- 1mm

UTOPIA VISA

ZENITH 10DEC 91 10DEC 96

MULTIPLE M123889546

BUSINESS MULTIPLE

ERIKSSON ANNA MARIA

L8988901C F /F 07SEP 40 XXX

John Doe

```
V<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<
L8988901C4XXX4009078F9612109<<<<<<<<
```

# Doc 9303 - Part 8

## Emergency Travel Documents

1. Scope
2. Introduction
3. Background
4. Principles and Recommended Practices
5. Summary
6. References

Expected 2017

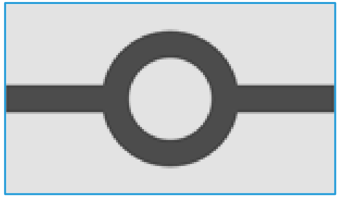
# Doc 9303 - Part 9

## Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs

1. Scope
2. eMRTD
3. Biometric Identification
4. The Selection of Biometrics Applicable to eMRTDs
5. Storage of the Biometric and other Data in a Logical Format in a Contactless IC
6. Test Methodologies for (e)MRTDs
7. References

Appendix A – Placement of the Contactless IC in an eMRP

Appendix B – Process for Reading eMRTDs



# Doc 9303 - Part 9

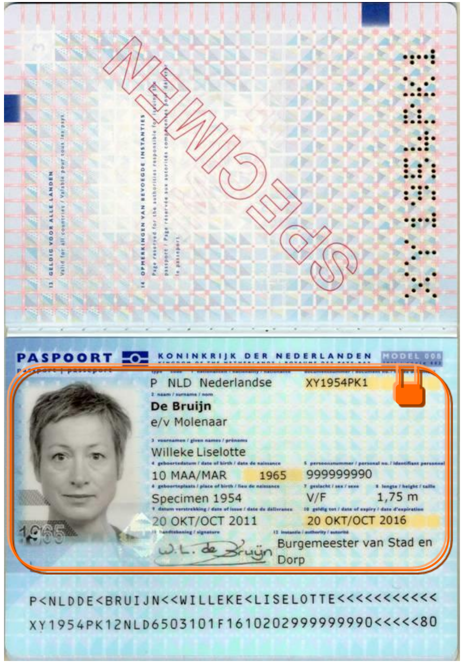
## Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs

Physical document

- Data Page
- Personal and Document data elements
- MRZ
- Physical security features

Electronic document

- RFID chip
- Personal and Document data elements
- MRZ
- Electronic security features



PASPOORT KONINKRIJK DER NEDERLANDEN MODEL 008
Paspoort | passeport

P NLD Nederlandse XY1954PK1

2 naam / surname / nom
De Bruijn
e/v Molenaar

3 voornamen / given names / prénoms
Willeke Liselotte

4 geboortedatum / date of birth / date de naissance
10 MAA/MAR 1965

5 persoonsnummer / personal no. / identifiant personnel
999999990

6 geboorteplaats / place of birth / lieu de naissance
Specimen 1954

7 geslacht / sex / sexe
V/F

8 lengte / height / taille
1,75 m

9 datum verstrekking / date of issue / date de délivrance
20 OKT/OCT 2011

10 geldig tot / date of expiry / date d'expiration
20 OKT/OCT 2016

11 handtekening / signature
W.L. de Bruijn

12 instantie / authority / autorité
Burgemeester van Stad en Dorp

```
P<NLDDE<BRUIJN<<WILLEKE<LISELOTTE<<<<<<<<<<<<
XY1954PK12NLD6503101F1610202999999990<<<<<80
```

# Doc 9303 - Part 9

## Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs

RFID chip

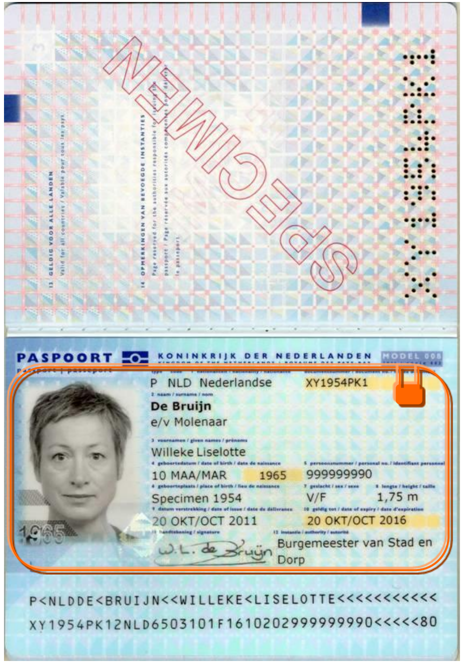
- High capacity
- Independent of location in document
- Capable of performing cryptographic operations
- Existing standards (ISO/IEC)

Biometrics - Face

- Least cultural obstructions
- Everybody has it
- Capture at a distance
- Interoperable (image)
- Also usable without biometric verification

Secondary Biometrics

- Finger
- Iris


SPECIMEN
XY1954PK1

PASPOORT KONINKRIJK DER NEDERLANDEN MODEL 008

Paspoort | passeport

P NLD Nederlandse XY1954PK1

2 naam / surname / nom

De Bruijn

e/v Molenaar

3 voornamen / given names / prénoms

Willeke Liselotte

4 geboortedatum / date of birth / date de naissance

10 MAA/MAR 1965

5 persoonsnummer / personal no. / identifiant personnel

999999990

6 geboorteplaats / place of birth / lieu de naissance

Specimen 1954

7 geslacht / sex / sexe

V/F

8 lengte / height / taille

1,75 m

9 datum verstrekking / date of issue / date de délivrance

20 OKT/OCT 2011

10 geldig tot / date of expiry / date d'expiration

20 OKT/OCT 2016

11 handtekening / signature

W.L. de Bruijn

12 instantie / authority / autorité

Burgemeester van Stad en Dorp

```
P<NLDDE<BRUIJN<<WILLEKE<LISELOTTE<<<<<<<<<<<<
XY1954PK12NLD6503101F1610202999999990<<<<<80
```

# Doc 9303 - Part 10

## Logical Data Structure (LDS) for Storage of Biometrics and other Data in the Contactless IC

1. Scope
2. Requirements of the Logical Data Structure
3. Application Profile for the Contactless IC
4. File Structure Specifications
5. Elementary Files
6. Data Elements Forming Data Groups 1 through 16
7. References

Appendix A – Logical Data Structure Mapping Examples

# Doc 9303 - Part 10

## Logical Data Structure (LDS) for Storage of Biometrics and other Data in the Contactless IC

1. Data Group 01 - Machine Readable Zone
2. Data Group 02 - Encoded face
3. Data Group 03 - Encoded fingers
4. Data Group 04 - Encoded Irises
5. Data Group 05 - Displayed portrait
6. Data Group 06 - Reserved for future use
7. Data Group 07 - Displayed signature or usual mark
8. Data Group 08 - Data features
9. Data Group 09 - Structure features
10. Data Group 10 - Substance features
11. Data Group 11 - Additional personal details
12. Data Group 12 - Additional document features
13. Data Group 13 - Optional details
14. Data Group 14 - Security options for secondary biometrics
15. Data Group 15 - Active Authentication public key info
16. Data Group 16 - Persons to notify

# Doc 9303 - Part 11

## Security Mechanisms for MRTDs

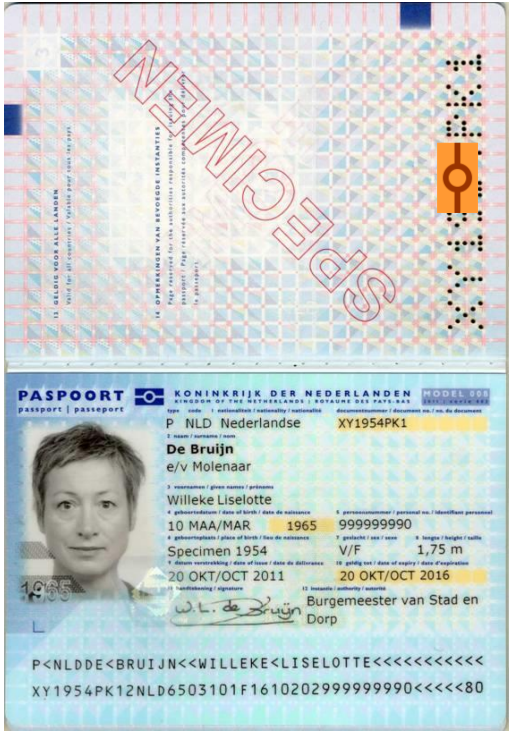
# Doc 9303 - Part 11

## Security Mechanisms for MRTDs

Access

- You can’t read a closed book
  - Hand over willingly
  - Open passport
- Skimming
  - Unauthorized contacting & reading
- Eavesdropping
  - Intercepting communications
- Access Control Mechanism
  - Enforce opening passport…
  - before providing access to the chip
  - Encrypt communications

???



SPECIMEN

PASPOORT passport | passeport

KONINKRIJK DER NEDERLANDEN
KINGDOM OF THE NETHERLANDS | ROYAUME DES PAYS-BAS

MODEL 008

type code 1 nationaliteit / nationality / nationalité — documentnummer / document no. / no. du document
P NLD Nederlandse XY1954PK1

2 naam / surname / nom
De Bruijn
e/v Molenaar

3 voornamen / given names / prénoms
Willeke Liselotte

4 geboortedatum / date of birth / date de naissance — 5 persoonsnummer / personal no. / identifiant personnel
10 MAA/MAR 1965 999999990

6 geboorteplaats / place of birth / lieu de naissance — 7 geslacht / sex / sexe — 8 lengte / height / taille
Specimen 1954 V/F 1,75 m

9 datum verstrekking / date of issue / date de délivrance — 10 geldig tot / date of expiry / date d'expiration
20 OKT/OCT 2011 20 OKT/OCT 2016

11 handtekening / signature — 12 instantie / authority / autorité
W.L. de Bruijn Burgemeester van Stad en Dorp

1965

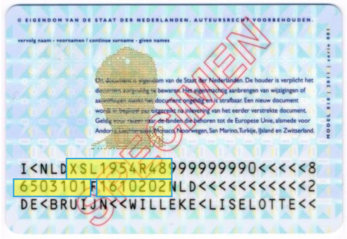
```
P<NLDDE<BRUIJN<<WILLEKE<LISELOTTE<<<<<<<<<<<<
XY1954PK12NLD6503101F1610202999999990<<<<<80
```

# Doc 9303 - Part 11

## Security Mechanisms for MRTDs

Access

- BAC
  - Basic Access Control
- PACE
  - Password Authenticated Connection Establishment
- Machine Readable Zone
  - Document Number
  - Date of Birth
  - Expiry Date
- Card Access Number



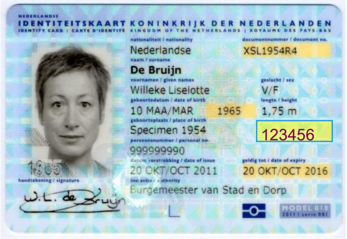
© EIGENDOM VAN DE STAAT DER NEDERLANDEN. AUTEURSRECHT VOORBEHOUDEN.

vervolg naam - voornamen / continue surname - given names

Dit document is eigendom van de Staat der Nederlanden. De houder is verplicht het document zorgvuldig te bewaren. Het eigenmachtig aanbrengen van wijzigingen of aantekeningen maakt het document ongeldig en is strafbaar. Een nieuw document wordt in beginsel pas uitgereikt na inlevering van het eerder verstrekte document. Geldig voor reizen naar de landen die behoren tot de Europese Unie, alsmede voor Andorra, Liechtenstein, Monaco, Noorwegen, San Marino, Turkije, IJsland en Zwitserland.

MODEL 010 | 2011 | serie 001

```
I<NLDXSL1954R489999999990<<<<<8
6503101F1610202NLD<<<<<<<<<<<2
DE<BRUIJN<<WILLEKE<LISELOTTE<<
```



NEDERLANDSE IDENTITEITSKAART KONINKRIJK DER NEDERLANDEN

IDENTITY CARD | CARTE D'IDENTITÉ KINGDOM OF THE NETHERLANDS | ROYAUME DES PAYS-BAS

nationaliteit / nationality: Nederlandse

documentnummer / document no.: XSL1954R4

naam / surname: **De Bruijn**

voornamen / given names: Willeke Liselotte

geslacht / sex: V/F

geboortedatum / date of birth: 10 MAA/MAR 1965

lengte / height: 1,75 m

geboorteplaats / place of birth: Specimen 1954

123456

persoonsnummer / personal no.: 999999990

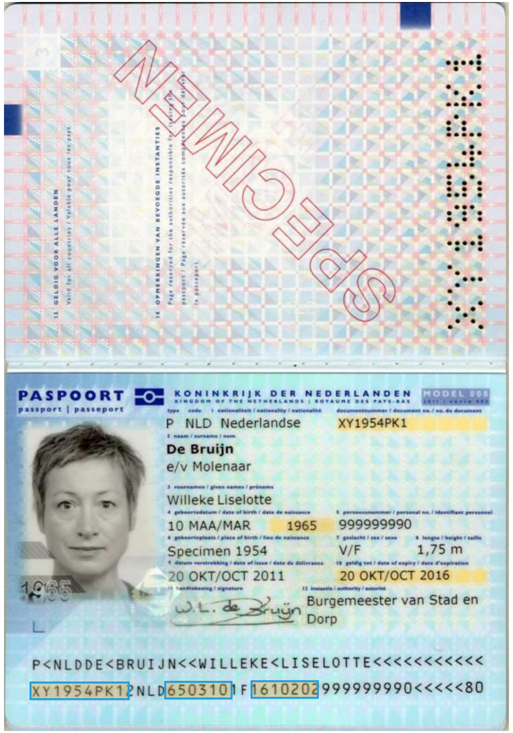
datum verstrekking / date of issue: 20 OKT/OCT 2011

geldig tot / date of expiry: 20 OKT/OCT 2016

handtekening / signature: W.L. de Bruijn

instantie / authority: Burgemeester van Stad en Dorp

MODEL 010 2011 | serie 001



PASPOORT passport | passeport KONINKRIJK DER NEDERLANDEN KINGDOM OF THE NETHERLANDS | ROYAUME DES PAYS-BAS MODEL 008

type: P code: NLD 1 nationaliteit / nationality / nationalité: Nederlandse

documentnummer / document no. / no. du document: XY1954PK1

2 naam / surname / nom: **De Bruijn** e/v Molenaar

3 voornamen / given names / prénoms: Willeke Liselotte

4 geboortedatum / date of birth / date de naissance: 10 MAA/MAR 1965

5 persoonsnummer / personal no. / identifiant personnel: 999999990

6 geboorteplaats / place of birth / lieu de naissance: Specimen 1954

7 geslacht / sex / sexe: V/F

8 lengte / height / taille: 1,75 m

9 datum verstrekking / date of issue / date de délivrance: 20 OKT/OCT 2011

10 geldig tot / date of expiry / date d'expiration: 20 OKT/OCT 2016

11 handtekening / signature: W.L. de Bruijn

12 instantie / authority / autorité: Burgemeester van Stad en Dorp

```
P<NLDDE<BRUIJN<<WILLEKE<LISELOTTE<<<<<<<<<<<<
XY1954PK12NLD6503101F1610202999999990<<<<<80
```

# Doc 9303 - Part 11

## Security Mechanisms for MRTDs

Copy Protection

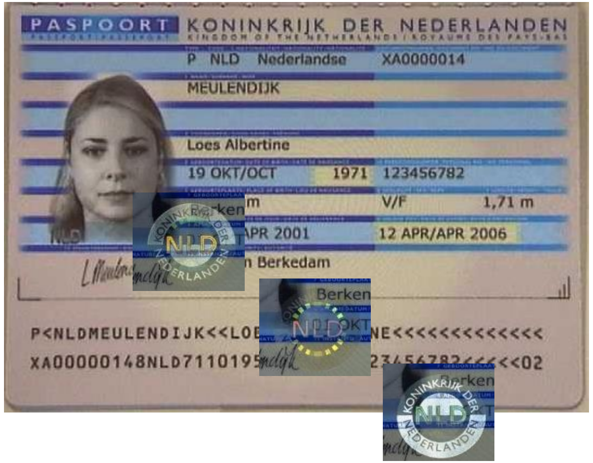
- Physical
  A copy is easily recognizable
  - Materials
  - UV Printing
  - OVDs
- Digital
  A copy is easily recognizable
  - Active Authentication
  - Digital Signature
  - Private Key (sign) in Secure Memory
  - Public Key (verify) in DG15

# Doc 9303 - Part 11

## Security Mechanisms for MRTDs

Data Authenticity & Integrity

- Physical
  Manipulation attempts leave recognizable traces
  - Personalization Techniques
  - OVDs
- Digital
  Manipulation attempts leave recognizable traces
  - Passive Authentication
  - Digital Signature
  - Private Key for signing
  - Public Key for verification
- Private Key securely stored
  - Confidentiality
- Public Key Distribution
  - Trust
  - Authenticity
  - Integrity
  - Public Key Certificate



PASPOORT KONINKRIJK DER NEDERLANDEN
KINGDOM OF THE NETHERLANDS / ROYAUME DES PAYS-BAS

P NLD Nederlandse XA0000014

MEULENDIJK

Loes Albertine

19 OKT/OCT 1971 123456782

Berken m V/F 1,71 m

APR 2001 12 APR/APR 2006

n Berkedam

P<NLDMEULENDIJK<<LOE NE<<<<<<<<<<<<<

XA00000148NLD7110195 23456782<<<<<02

# Doc 9303 - Part 12

## Public Key Infrastructure for MRTDs

1. Scope
2. Overview of the Public Key Infrastructure
3. Roles and Responsibilities
4. Key Management
5. Distribution Mechanisms
6. PKI Trust and Validation
7. Certificate and CRL Profiles
8. CSCA Master List Structure
9. References

Appendix A – Lifetimes

Appendix B – Certificate and CRL Profile Reference Text

Appendix C – Earlier Certificate Profiles

Appendix D – RFC 5280 Validation Compatibility

# Doc 9303 - Part 12

## Public Key Infrastructure for MRTDs

Digital signing by Document Signer (DS)

- Private Key (sign) stored securely
- Public Key (verify) distribution
- Trust in authenticity Digital Signature

Certificate Revocation List (CRL)

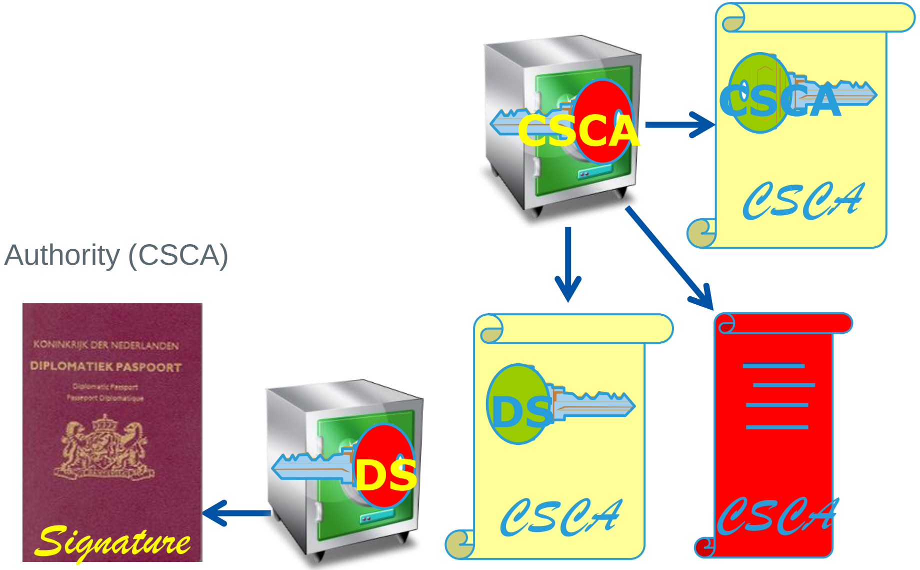
- Revoked DS certificates

DS certificates & CRL signed by Country Signing Certification Authority (CSCA)

- Private Key (sign) stored securely
- Public Key (verify) distribution
- Trust in authenticity DS Public Key

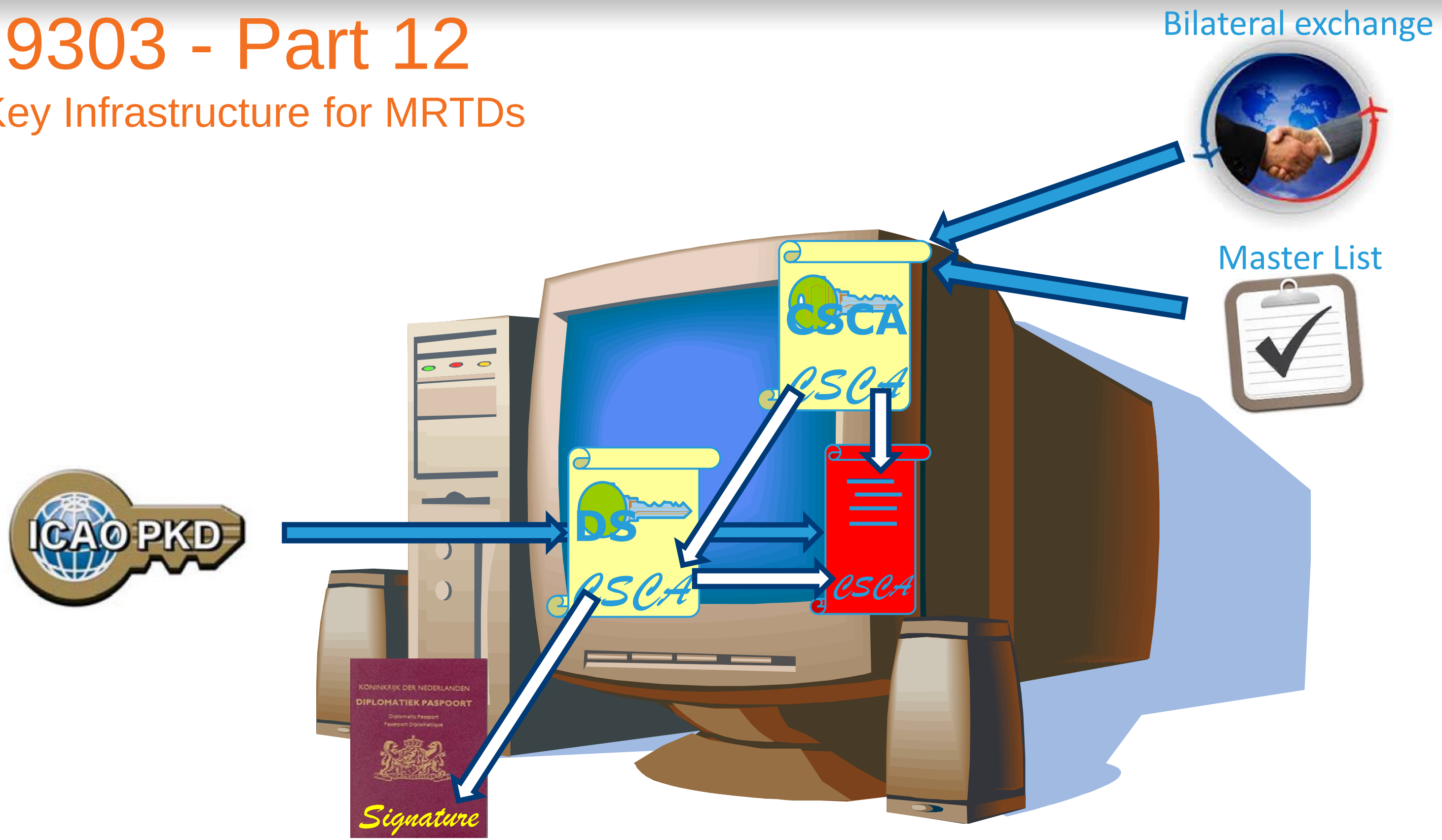
CSCA certificate self-signed

- Bilateral exchange
- Trust in authenticity CSCA Public Key



# Doc 9303 - Part 12

## Public Key Infrastructure for MRTDs

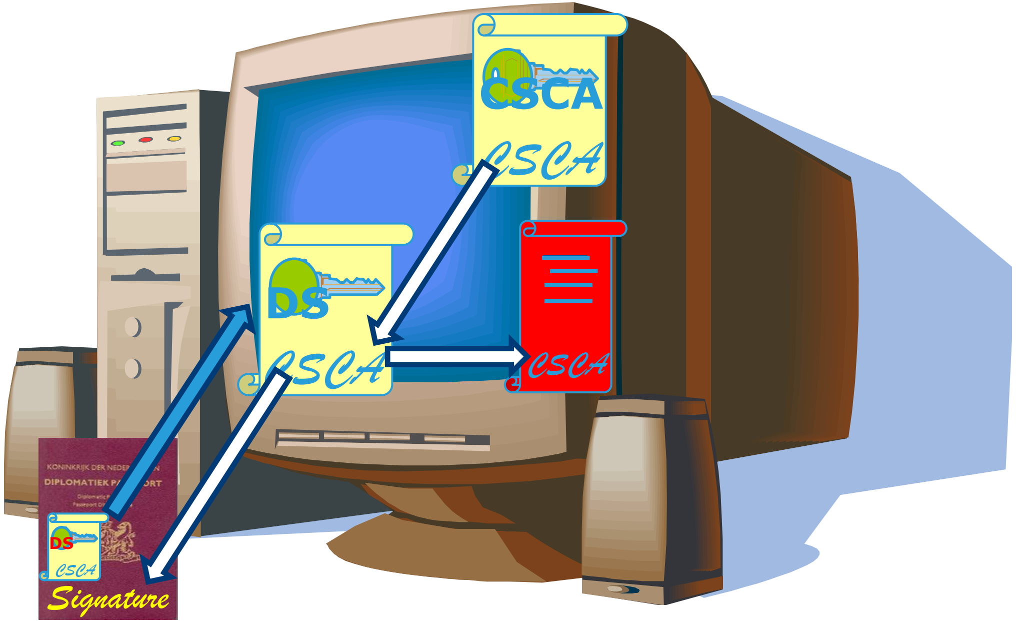


Bilateral exchange

Master List

# Doc 9303 - Part 12

Public Key Infrastructure for MRTDs



# Summary

## Proper Inspection

**Issuing Authority**

- Establish CSCA
- Issue CSCA certificates
  (bilateral exchange)
- Issue CRLs
  (PKD)
  (bilateral)
- Establish DSs
- Issue DS certificates
  (ePassport chip)
  (PKD)
- Sign ePassports
- Issue ePassports

**Inspecting Authority**

- Obtain CSCA certificates
  (bilateral)
  (Master Lists)
- Distribute CSCA certificates internally
- Obtain CRLs
  (PKD)
  (bilateral)
- Verify CRLs
- Obtain DS certificates
  (ePassport chip)
  (PKD)
- Verify DS certificates
- Read ePassport
- Perform Passive Authentication
  (verify digital signature)
  (verify data)
- Use data

# Thank you!

OT MORPHO

**Tom KINNEGING**
Senior Advisor | BU Europe | GIS
Morpho

Oudeweg 32 | 2031 CC Haarlem | Netherlands
P.O. Box 5300 | 2000 GH Haarlem | Netherlands

**P** +31 (0)23 7995 218
**M** +31 (0)6 512 137 02
tom.kinneging@morpho.com

http://www.icao.int/Security/FAL/TRIP