ICAO 80

2024 ICAO TRIP SYMPOSIUM

MONTRÉAL , CANADA | NOVEMBER 13-15

Judicial Information Service
Ministry of Security and Justice

Jeen de Swart

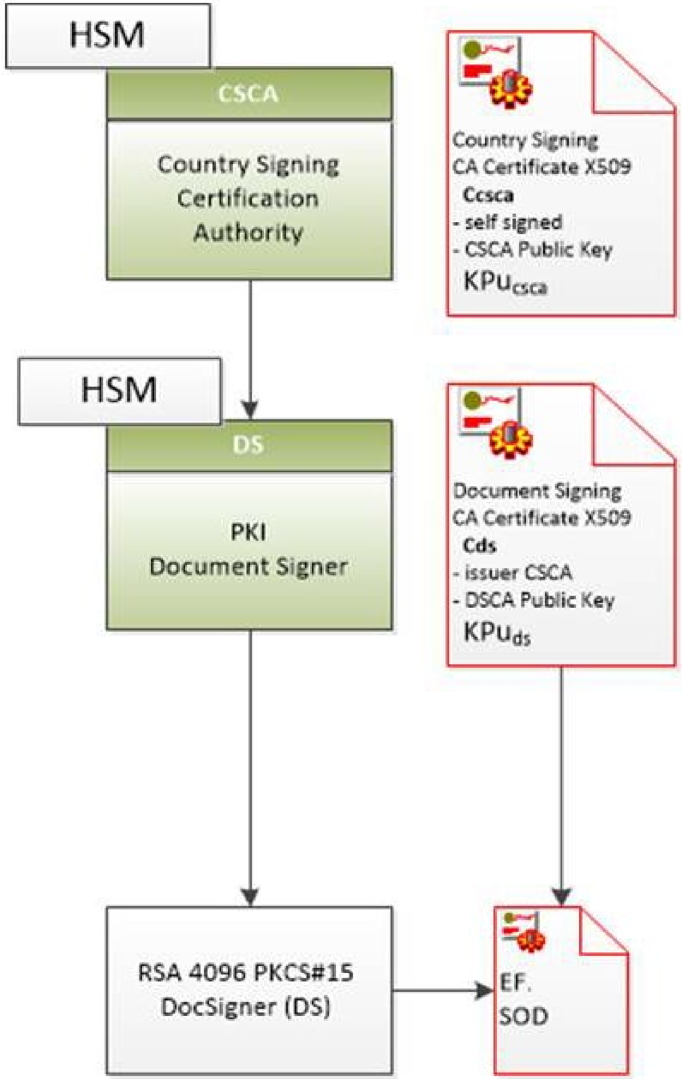
Senior Information Security Architect

CSCA DS PKI chain

PASSPORT
PASSEPORT
ABROADIA
Type
P
Code
NLD
Name / Nom
Vestram
Given names / Prénoms
Identitatem
Nationality / Nationalité
Netherlands
Date of birth / Date de naissance
03-02-1985
Date of issue / Date de délivrance
14-11-2022
Date of expiry / Date d'expiration
14-11-2032
Place of birth / Lieu de naissance
Eindhoven
1985
Signature
Authority / Autorité
Managing
Director
IDcentre
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<
NL10101050NLD8502038M3110108<2021IDCENTRE<58

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}



HSM
CSCA
Country Signing Certification Authority
HSM
DS
PKI Document Signer
RSA 4096 PKCS#15 DocSigner (DS)
EF. SOD

Country Signing
CA Certificate X509
Ccsca
- self signed
- CSCA Public Key

KPu_{csca}

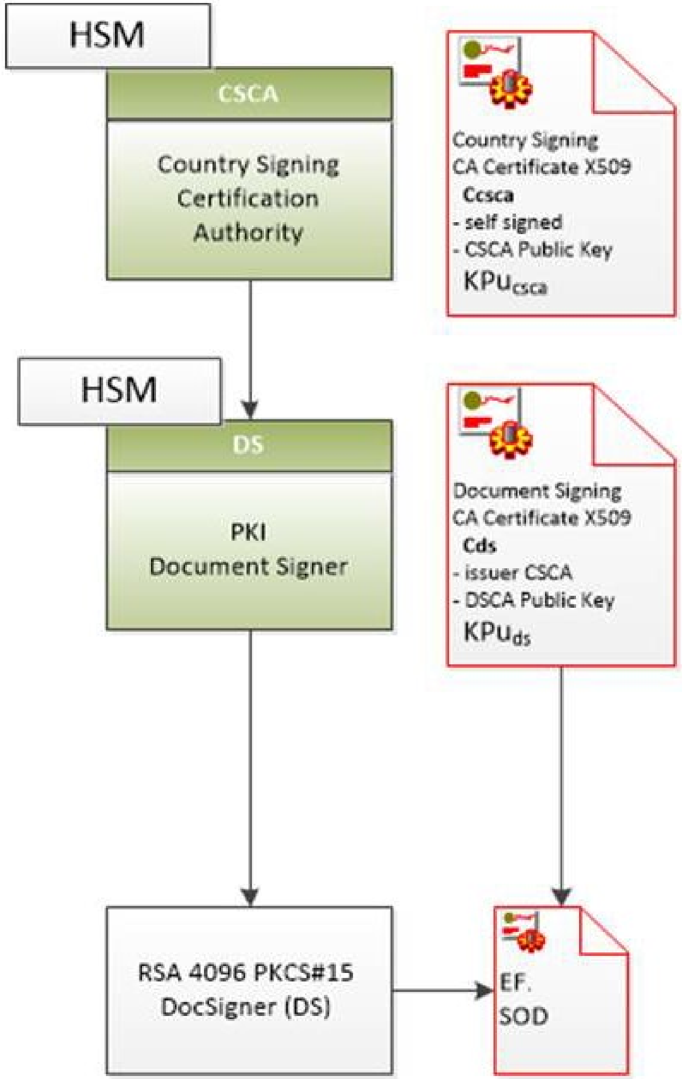
Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

CSCA DS PKI chain

A serious threat ....

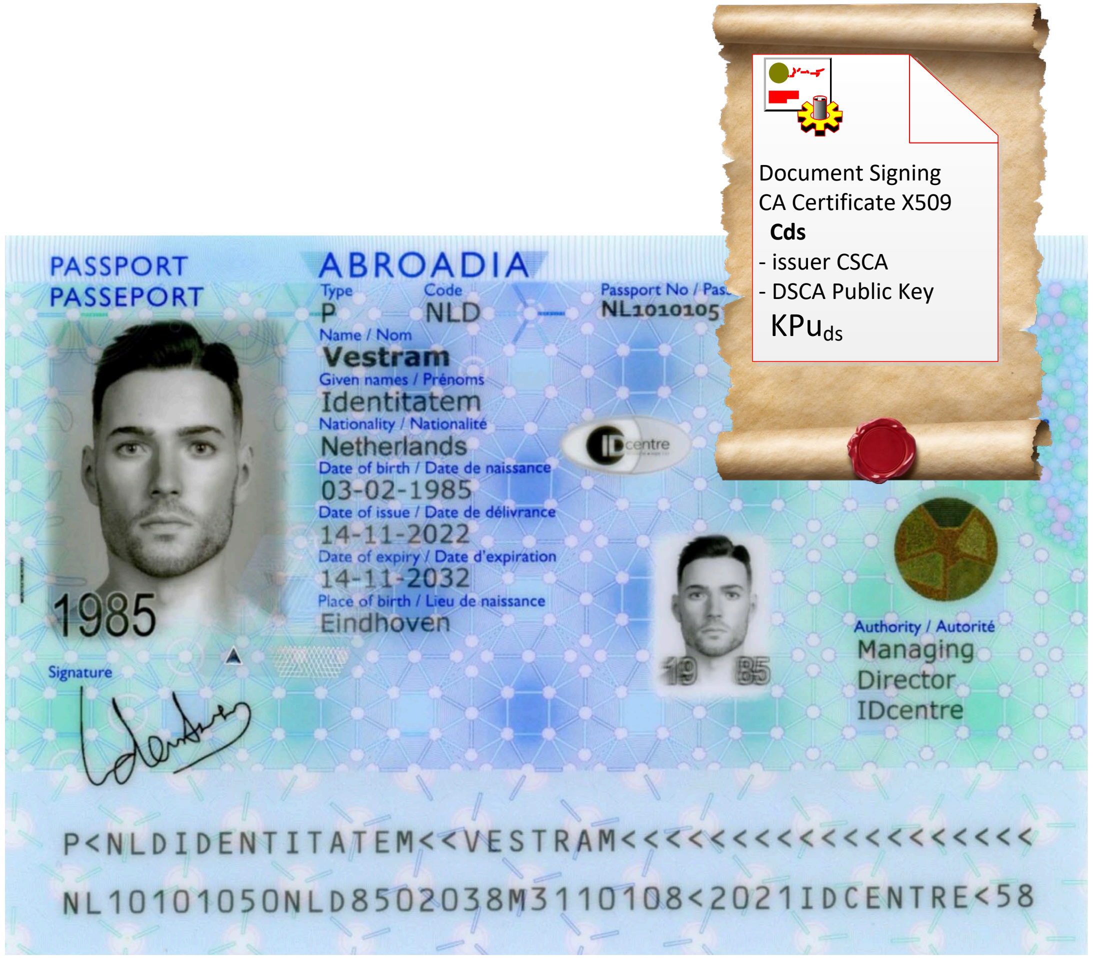
- Quantum Computer breaks the PKI
- Passive Authentication is broken
- A worldwide threat



The Good News !

A Quantum Proof Passport is created

- A PKI with Post Quantum Algorithms
- A Quantum Proof Signature



Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

PASSPORT
PASSEPORT

ABROADIA

Type: P
Code: NLD
Passport No / Pas: NL1010105

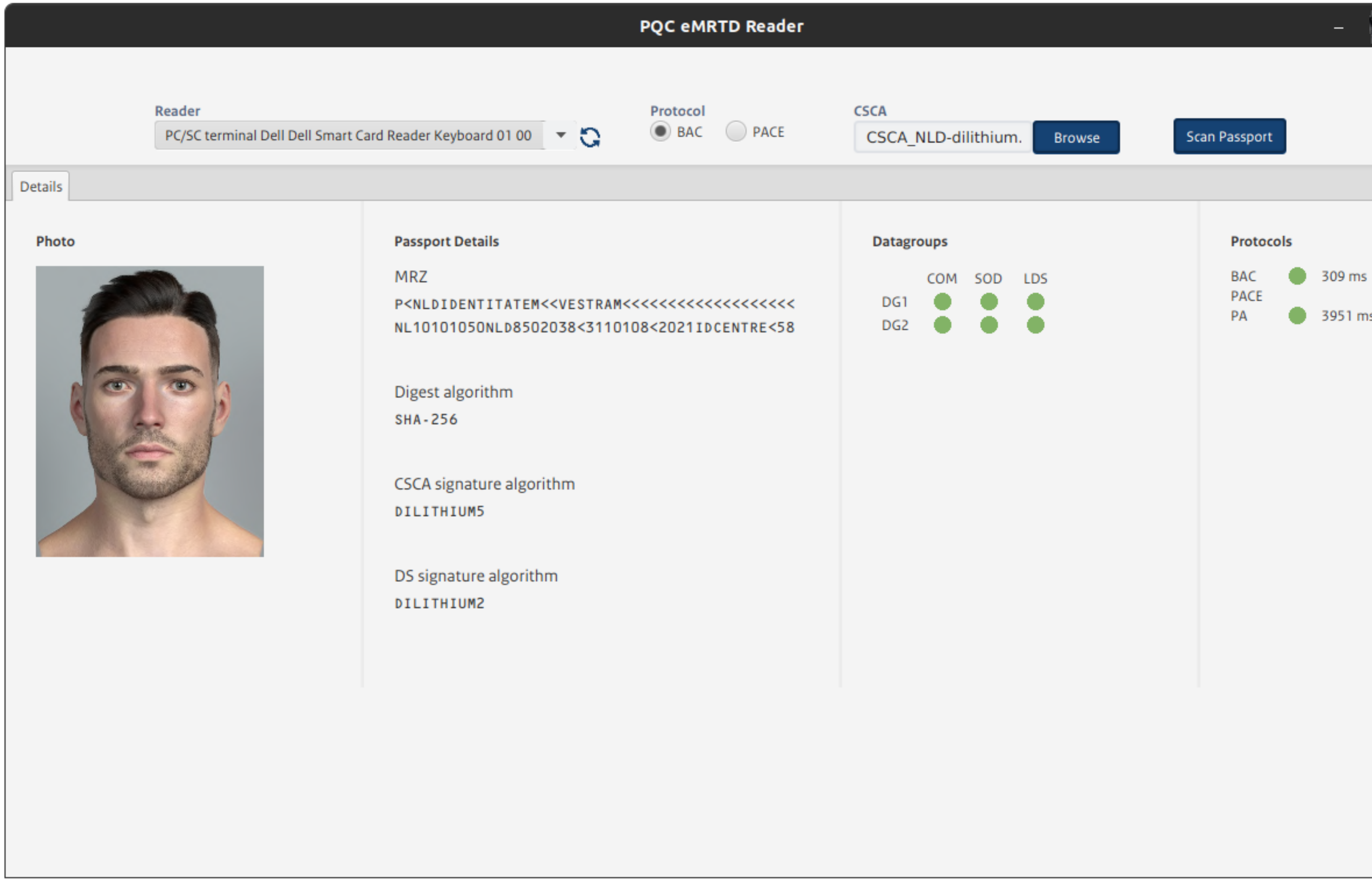
Name / Nom: Vestram
Given names / Prénoms: Identitatem
Nationality / Nationalité: Netherlands
Date of birth / Date de naissance: 03-02-1985
Date of issue / Date de délivrance: 14-11-2022
Date of expiry / Date d'expiration: 14-11-2032
Place of birth / Lieu de naissance: Eindhoven

Authority / Autorité: Managing Director IDcentre

Signature

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<<
NL10101050NLD8502038M3110108<2021IDCENTRE<58
```

The Good News !



Reader: PC/SC terminal Dell Dell Smart Card Reader Keyboard 01 00

Protocol: ● BAC ○ PACE

CSCA: CSCA_NLD-dilithium.

Photo

Passport Details

MRZ

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<<
NL10101050NLD8502038<3110108<2021IDCENTRE<58
```

Digest algorithm

SHA-256

CSCA signature algorithm

DILITHIUM5

DS signature algorithm

DILITHIUM2

Datagroups

	COM	SOD	LDS
DG1	●	●	●
DG2	●	●	●

Protocols

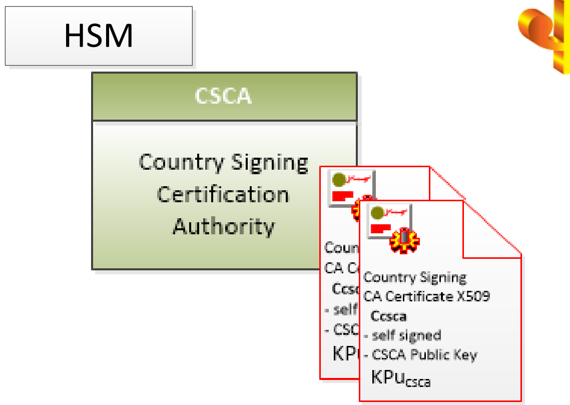
BAC	●	309 ms
PACE		
PA	●	3951 ms

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

From Governmental Perspective

Costs and Effectiveness

PKI



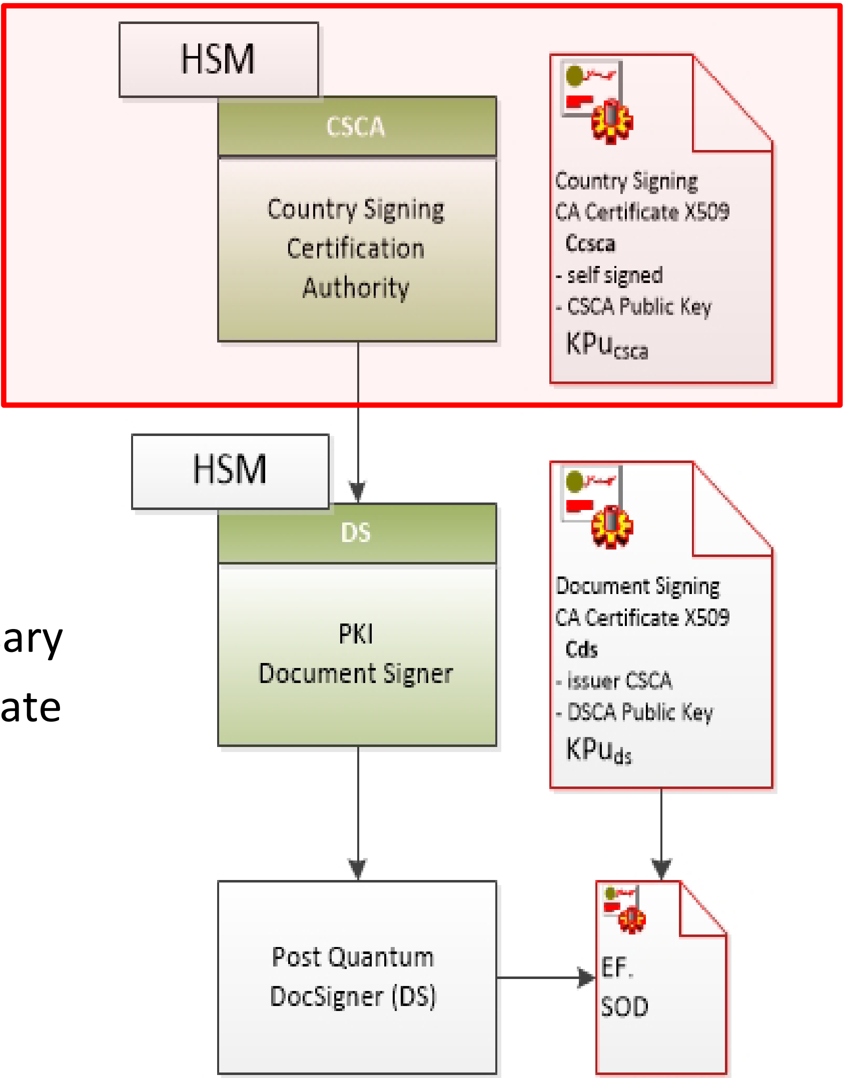
A new HSM is necessary

An update of CA is necessary

A X.509 PQC CSCA certificate

Create a link certificate

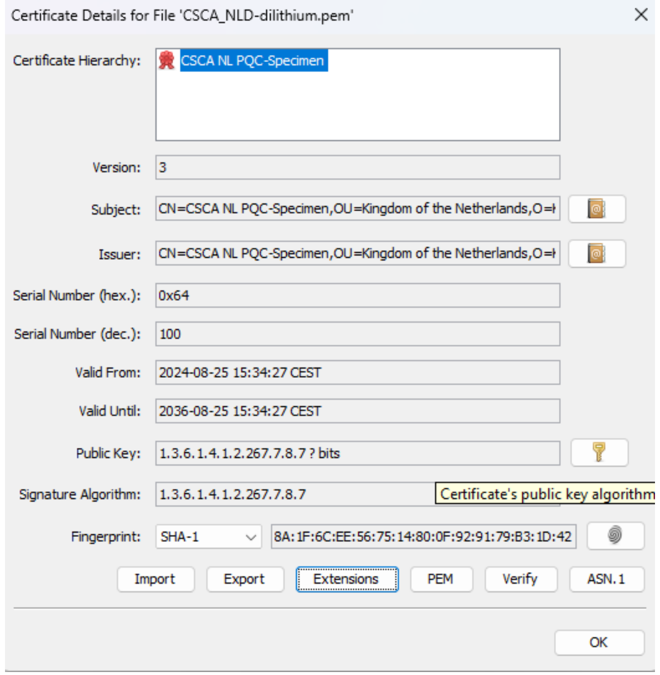
Publish and Upload



WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

X.509 Certificates

- Conform profile ICAO9303
- Only new algorithms



Certificate Details for File 'CSCA_NLD-dilithium.pem'

Certificate Hierarchy: CSCA NL PQC-Specimen

Version: 3

Subject: CN=CSCA NL PQC-Specimen,OU=Kingdom of the Netherlands,O=I

Issuer: CN=CSCA NL PQC-Specimen,OU=Kingdom of the Netherlands,O=I

Serial Number (hex.): 0x64

Serial Number (dec.): 100

Valid From: 2024-08-25 15:34:27 CEST

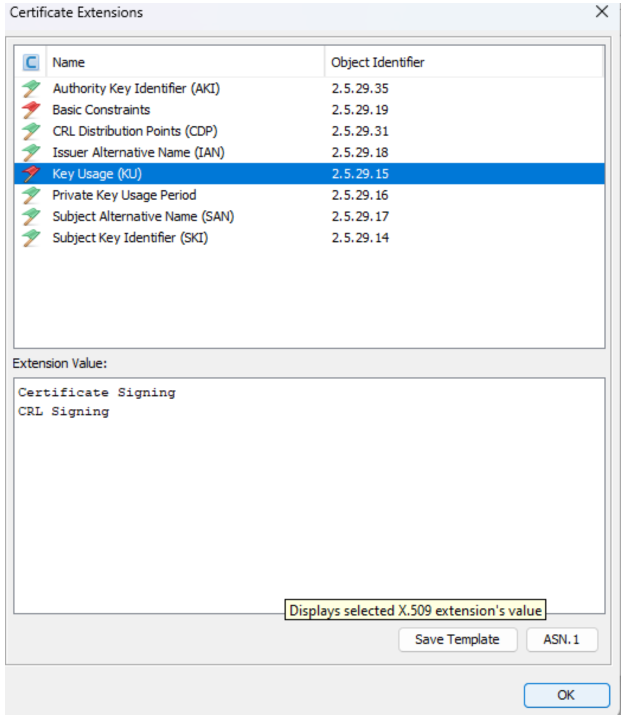
Valid Until: 2036-08-25 15:34:27 CEST

Public Key: 1.3.6.1.4.1.2.267.7.8.7 ? bits

Signature Algorithm: 1.3.6.1.4.1.2.267.7.8.7

Certificate's public key algorithm

Fingerprint: SHA-1 8A:1F:6C:EE:56:75:14:80:0F:92:91:79:B3:1D:42



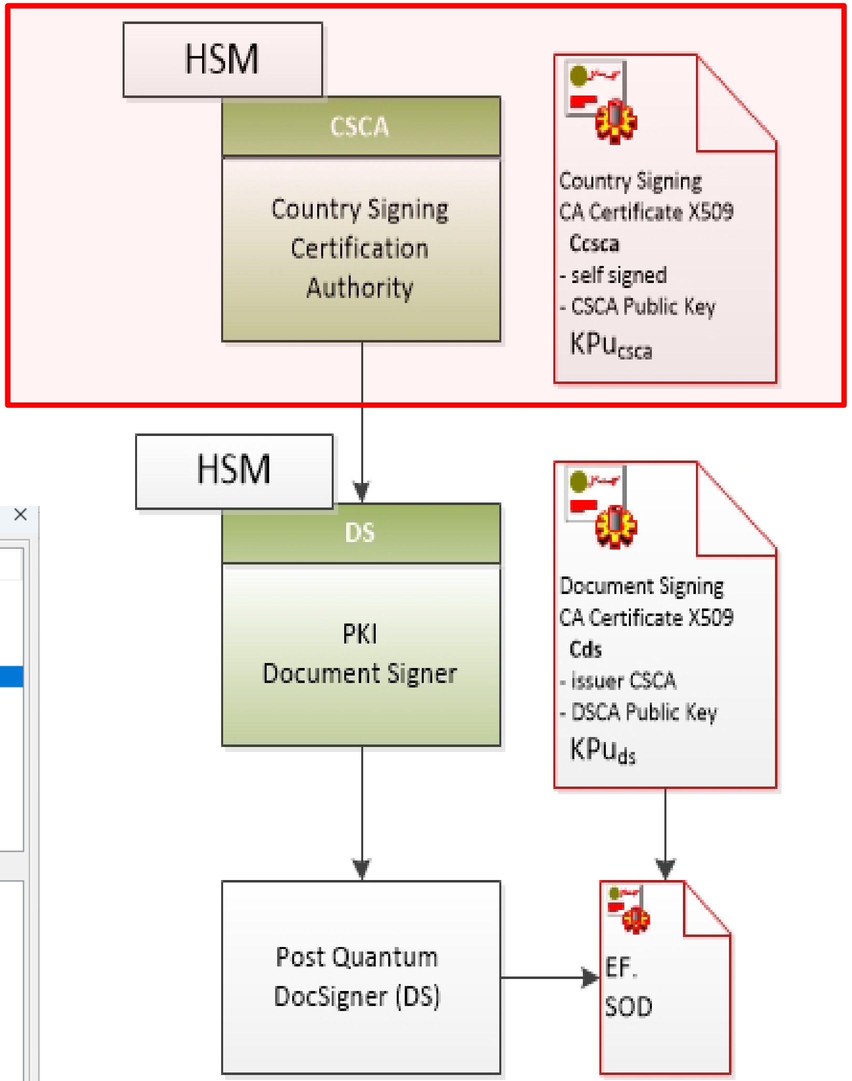
Certificate Extensions

Name	Object Identifier
Authority Key Identifier (AKI)	2.5.29.35
Basic Constraints	2.5.29.19
CRL Distribution Points (CDP)	2.5.29.31
Issuer Alternative Name (IAN)	2.5.29.18
Key Usage (KU)	2.5.29.15
Private Key Usage Period	2.5.29.16
Subject Alternative Name (SAN)	2.5.29.17
Subject Key Identifier (SKI)	2.5.29.14

Extension Value:

```
Certificate Signing
CRL Signing
```

Displays selected X.509 extension's value



HSM

CSCA

Country Signing Certification Authority

Country Signing CA Certificate X509 Ccsca
- self signed
- CSCA Public Key

KPu_{csca}

HSM

DS

PKI Document Signer

Document Signing CA Certificate X509 Cds
- issuer CSCA
- DSCA Public Key

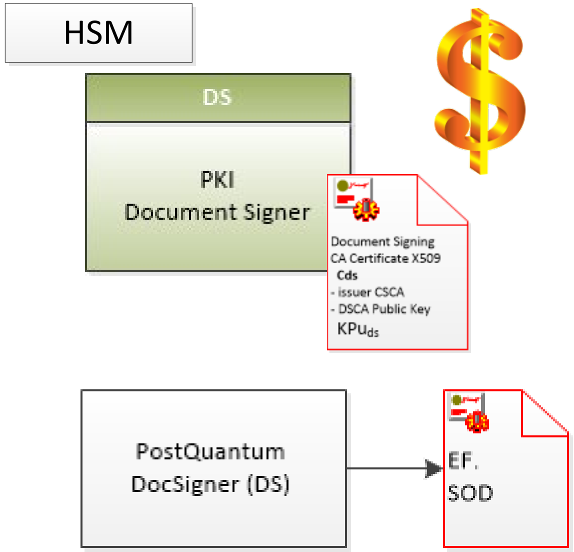
KPu_{ds}

Post Quantum DocSigner (DS)

EF. SOD

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

PKI and Printing Facility

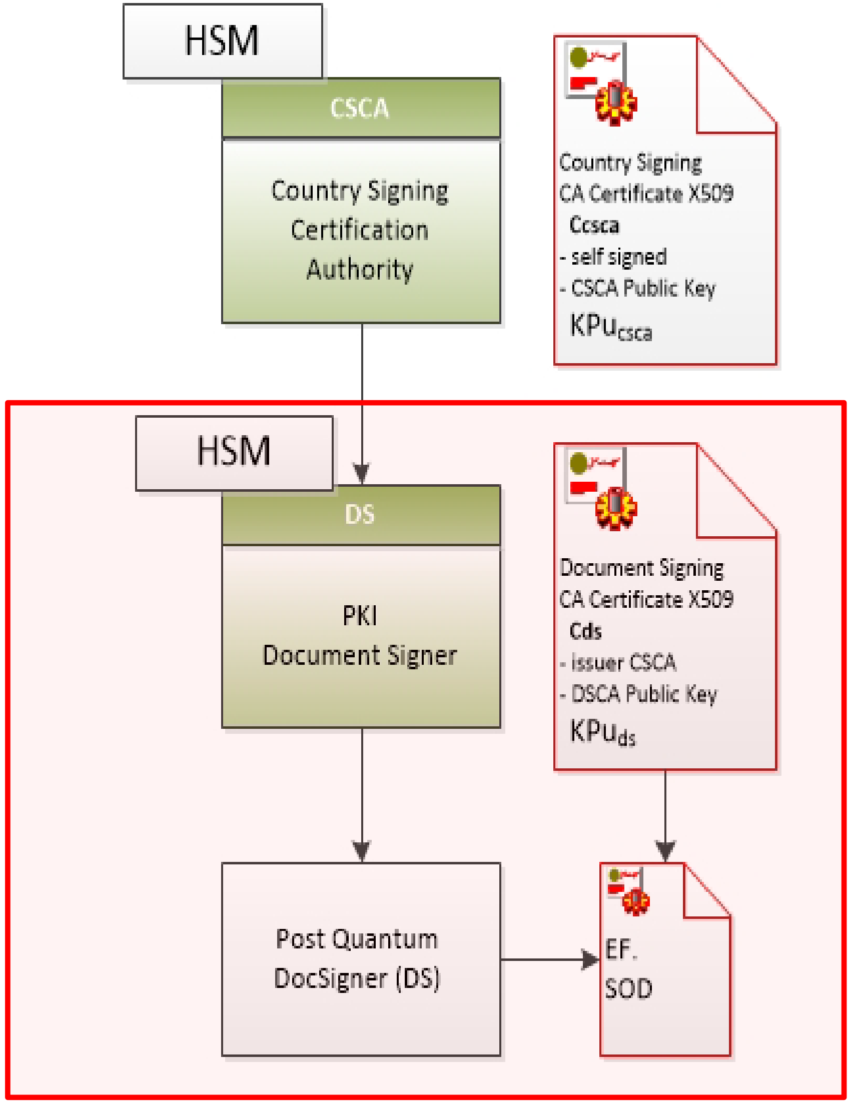


A new HSM is necessary

An update of DS is necessary

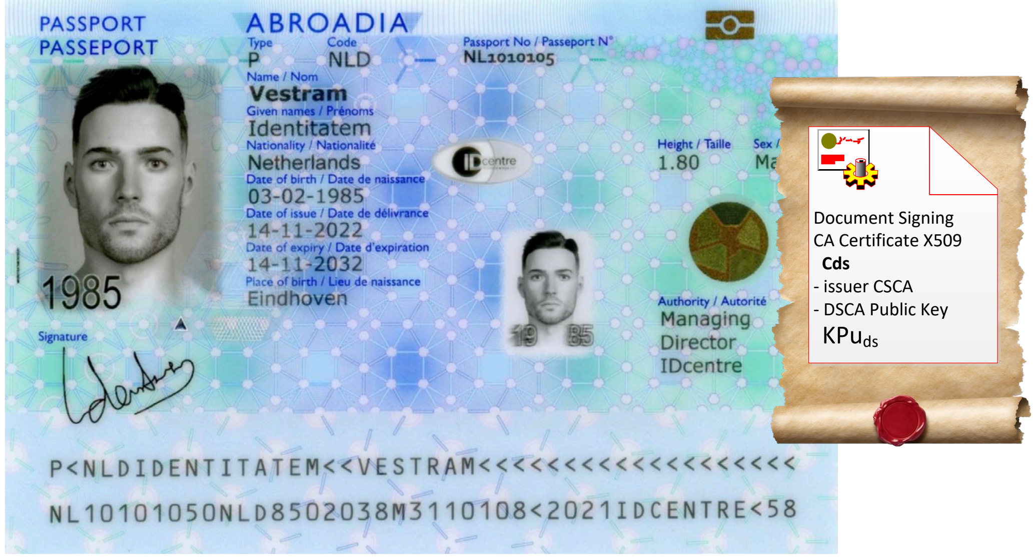
A X.509 PQC DS certificate

EF.SOd signed by PQC DS



WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

A Quantum Proof Passport is created



PASSPORT
PASSEPORT

ABROADIA

Type: P
Code: NLD
Passport No / Passeport N°: NL1010105
Name / Nom: Vestram
Given names / Prénoms: Identitatem
Nationality / Nationalité: Netherlands
Date of birth / Date de naissance: 03-02-1985
Date of issue / Date de délivrance: 14-11-2022
Date of expiry / Date d'expiration: 14-11-2032
Place of birth / Lieu de naissance: Eindhoven
Height / Taille: 1.80
Sex / Ma
Authority / Autorité: Managing Director IDcentre

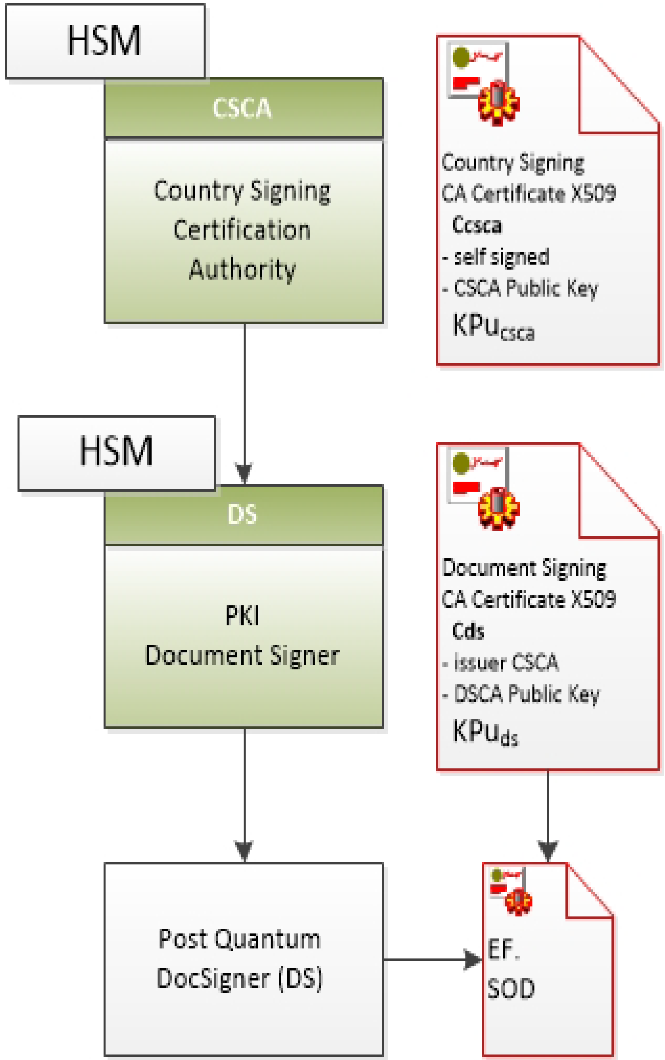
1985

Signature

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<<
NL10101050NLD8502038M3110108<2021IDCENTRE<58
```

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu$_{ds}$



HSM

CSCA

Country Signing Certification Authority

Country Signing
CA Certificate X509
Ccsca
- self signed
- CSCA Public Key

KPu$_{csca}$

HSM

DS

PKI Document Signer

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu$_{ds}$

Post Quantum DocSigner (DS)

EF. SOD

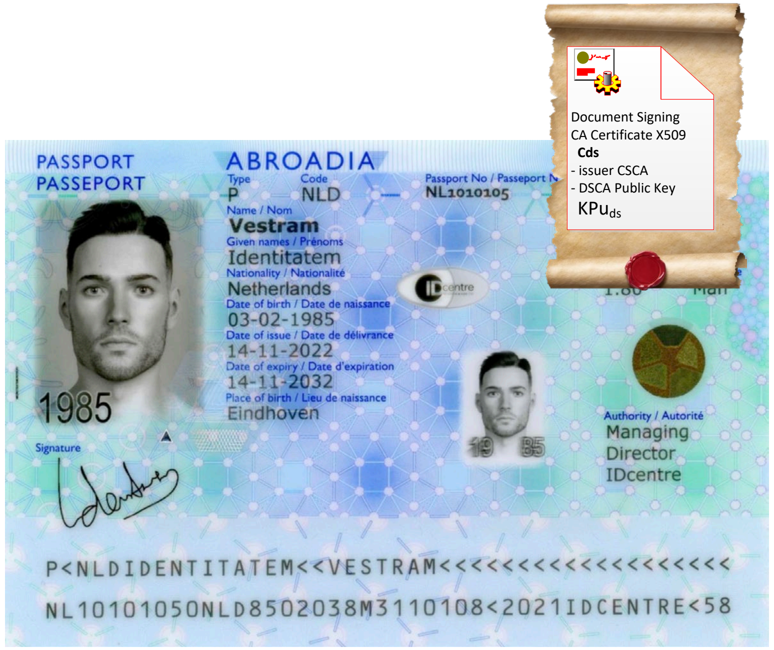
WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Border Control

$ Some vendors are already updating

An update of BC system is necessary

Passive Authentication
- Mandatory proces
- Does not change



PASSPORT
PASSEPORT

ABROADIA

Type: P
Code: NLD
Passport No / Passeport N: NL1010105

Name / Nom: Vestram
Given names / Prénoms: Identitatem
Nationality / Nationalité: Netherlands
Date of birth / Date de naissance: 03-02-1985
Date of issue / Date de délivrance: 14-11-2022
Date of expiry / Date d'expiration: 14-11-2032
Place of birth / Lieu de naissance: Eindhoven

1985

Signature

Authority / Autorité: Managing Director IDcentre

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<
NL1010105ONLD8502038M3110108<2021IDCENTRE<58
```

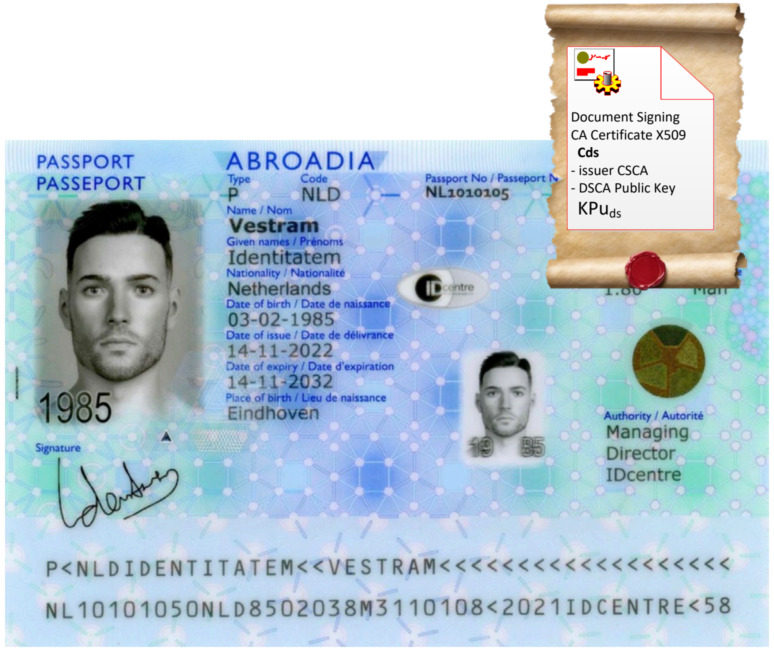
Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Full Switch Over At Once solution

Hybrid solution



PASSPORT
PASSEPORT

ABROADIA

Type: P

Code: NLD

Passport No / Passeport N: NL1010105

Name / Nom: Vestram

Given names / Prénoms: Identitatem

Nationality / Nationalité: Netherlands

Date of birth / Date de naissance: 03-02-1985

Date of issue / Date de délivrance: 14-11-2022

Date of expiry / Date d'expiration: 14-11-2032

Place of birth / Lieu de naissance: Eindhoven

Authority / Autorité: Managing Director IDcentre

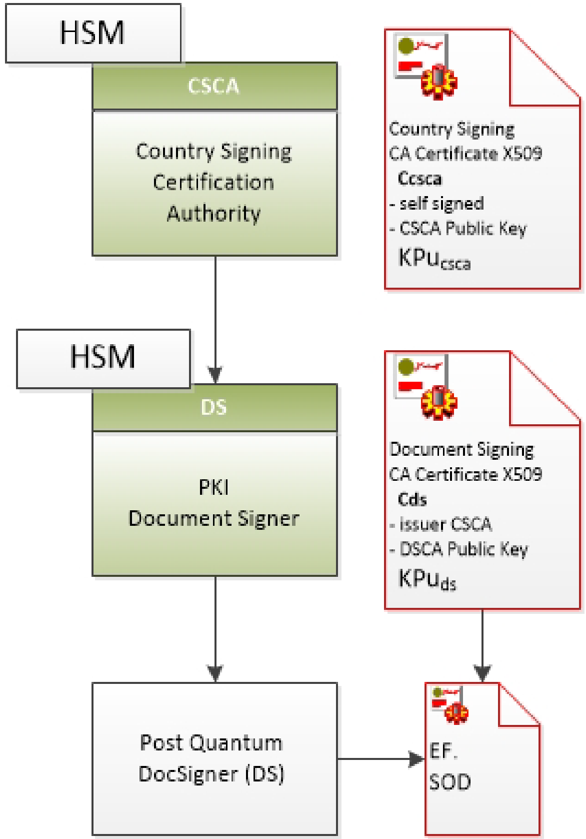
Signature

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<<<
NL1010105ONLD8502038M3110108<2021IDCENTRE<58
```

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key
KPu$_{ds}$

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Full Switch Over At Once solution


HSM

CSCA

Country Signing Certification Authority

Country Signing CA Certificate X509
Ccsca
- self signed
- CSCA Public Key

KPu_{csca}

HSM

DS

PKI Document Signer

Document Signing CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

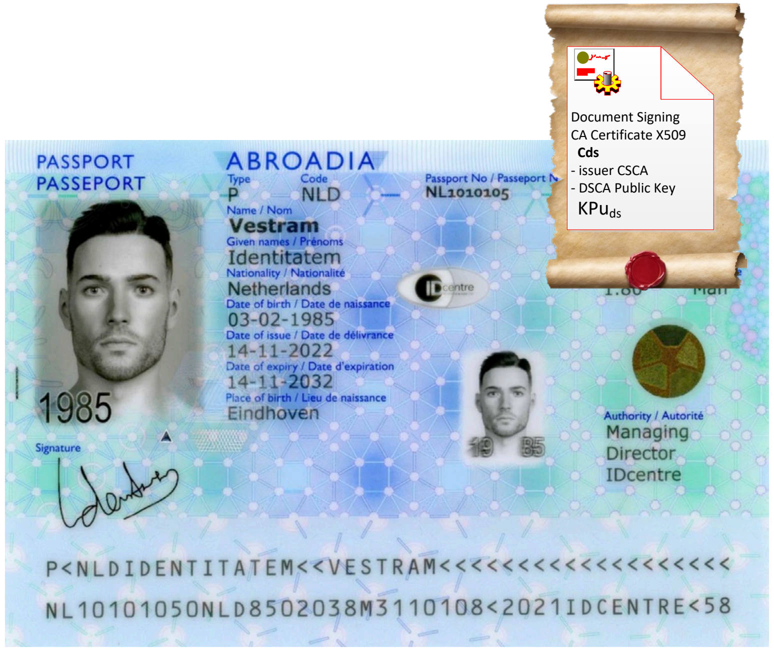
KPu_{ds}

Post Quantum DocSigner (DS)

EF. SOD

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key
KPu_{ds}

PASSPORT PASSPORT ABROADIA
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<
NL1010105ONLD8502038M3110108<2021IDCENTRE<58


Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

PASSPORT
PASSPORT

ABROADIA

Type
P

Code
NLD

Passport No / Passport N
NL1010105

Name / Nom
Vestram

Given names / Prénoms
Identitatem

Nationality / Nationalité
Netherlands

Date of birth / Date de naissance
03-02-1985

Date of issue / Date de délivrance
14-11-2022

Date of expiry / Date d'expiration
14-11-2032

Place of birth / Lieu de naissance
Eindhoven

1.80 Man

1985

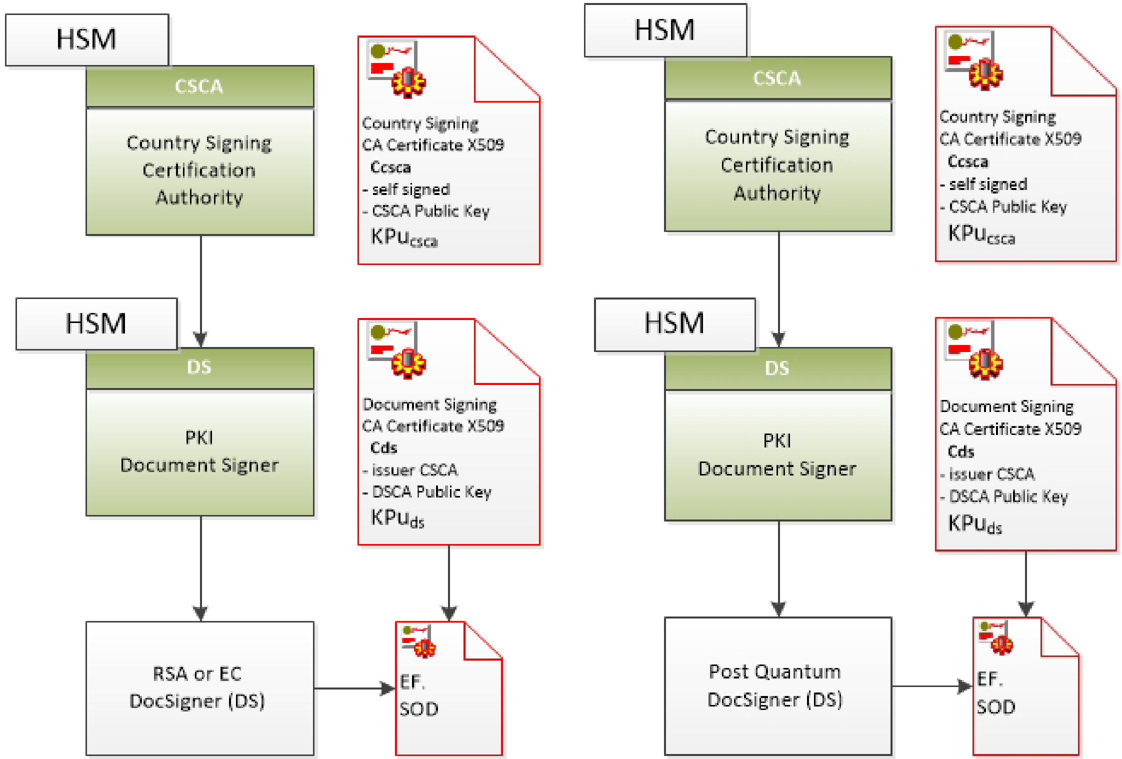
Signature

Authority / Autorité
Managing
Director
IDcentre

P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<
NL1010105ONLD8502038M3110108<2021IDCENTRE<58

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Full Switch Over At Once solution



HSM

CSCA

Country Signing Certification Authority

Country Signing CA Certificate X509
Ccsca
- self signed
- CSCA Public Key

KPu_{csca}

HSM

DS

PKI Document Signer

Document Signing CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

RSA or EC DocSigner (DS)

EF. SOD

HSM

CSCA

Country Signing Certification Authority

Country Signing CA Certificate X509
Ccsca
- self signed
- CSCA Public Key

KPu_{csca}

HSM

DS

PKI Document Signer

Document Signing CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

Post Quantum DocSigner (DS)

EF. SOD

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

PASSPORT
PASSEPORT

ABROADIA

Type: P
Code: NLD
Passport No / Passeport N: NL1010105
Name / Nom: **Vestram**
Given names / Prénoms: Identitatem
Nationality / Nationalité: Netherlands
Date of birth / Date de naissance: 03-02-1985
Date of issue / Date de délivrance: 14-11-2022
Date of expiry / Date d'expiration: 14-11-2032
Place of birth / Lieu de naissance: Eindhoven
Authority / Autorité: Managing Director IDcentre

Signature

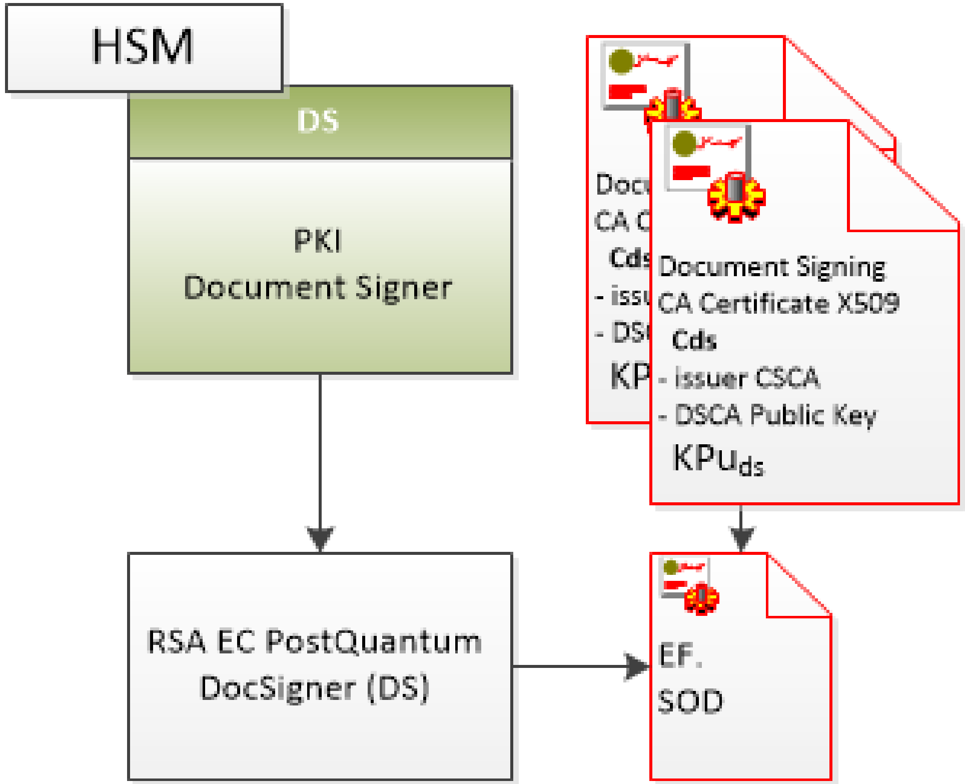
```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<
NL10101050NLD8502038M3110108<2021IDCENTRE<58
```

Maintenance of two PKI chains

No more trust:
One country One CSCA

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Hybrid solution 1

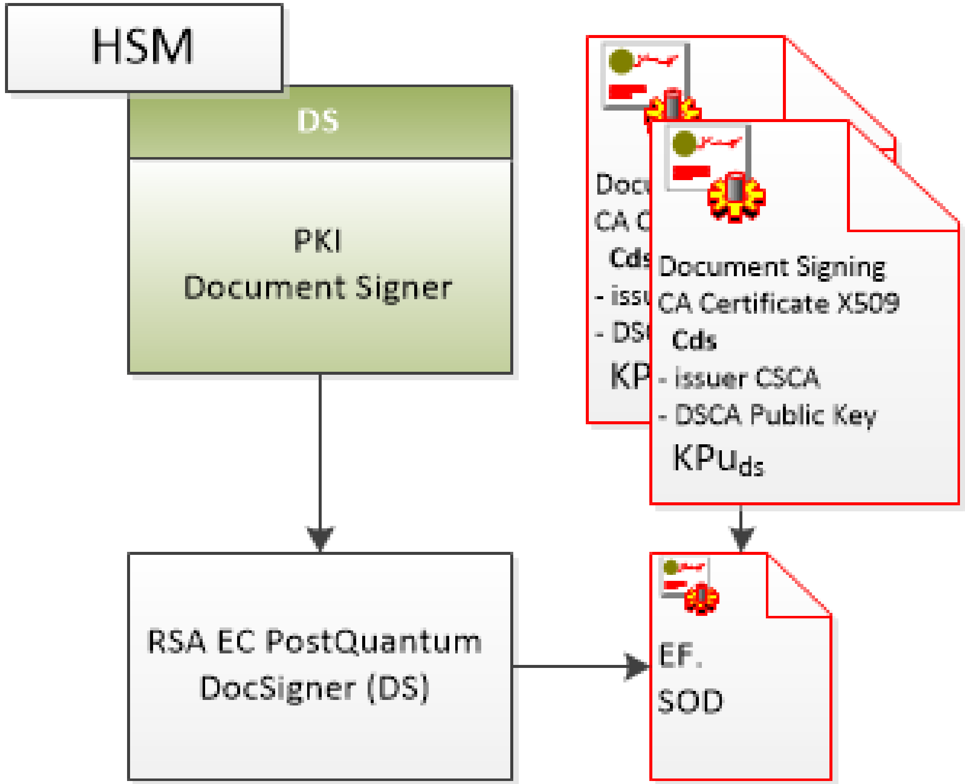


Double Signing in One EF.SOd

Needs **extra** coding in DocSigner

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Hybrid solution 1



HSM

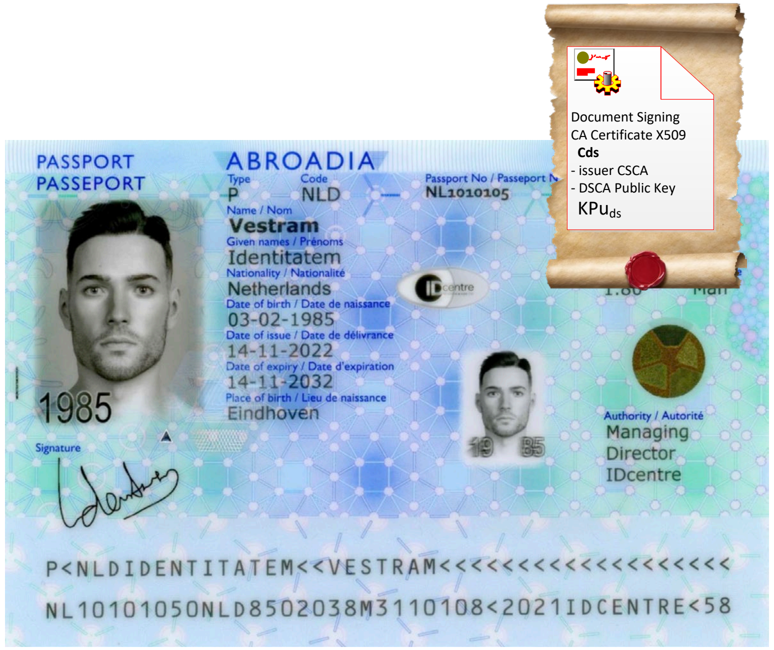
DS

PKI
Document Signer

RSA EC PostQuantum
DocSigner (DS)

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key
KPu_{ds}

EF.
SOD



Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu_{ds}

PASSPORT
PASSEPORT

ABROADIA

Type
P

Code
NLD

Passport No / Passeport N
NL1010105

Name / Nom
Vestram

Given names / Prénoms
Identitatem

Nationality / Nationalité
Netherlands

Date of birth / Date de naissance
03-02-1985

Date of issue / Date de délivrance
14-11-2022

Date of expiry / Date d'expiration
14-11-2032

Place of birth / Lieu de naissance
Eindhoven

1985

Signature

Authority / Autorité
Managing
Director
IDcentre

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<
NL1010105ONLD8502038M3110108<2021IDCENTRE<58
```

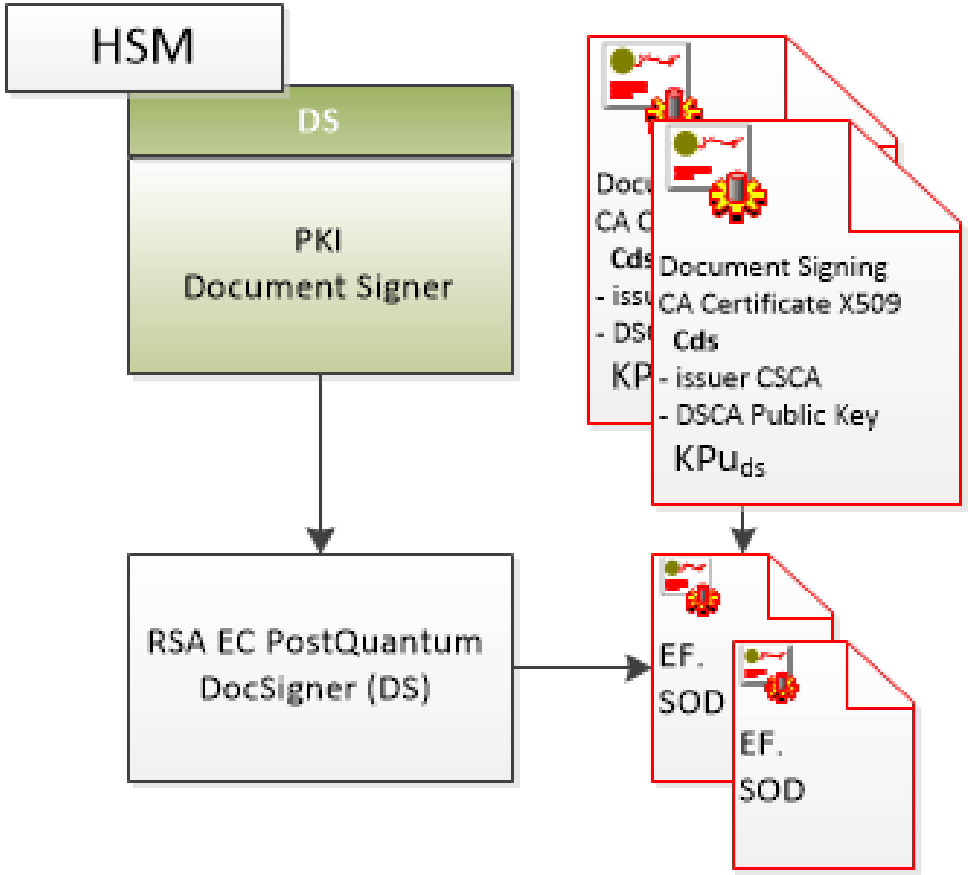
Double Signing in One EF.SOd

Needs **extra** coding in DocSigner

Needs **extra** coding in BC System

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Hybrid solution 2



HSM

DS

PKI Document Signer

RSA EC PostQuantum DocSigner (DS)

Document Signing CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key
KPu$_{ds}$

EF. SOD

EF. SOD

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key
KPu$_{ds}$

PASSPORT
PASSEPORT
ABROADIA
Type P
Code NLD
Passport No / Passport N
NL1010105
Name / Nom
Vestram
Given names / Prénoms
Identitatem
Nationality / Nationalité
Netherlands
Date of birth / Date de naissance
03-02-1985
Date of issue / Date de délivrance
14-11-2022
Date of expiry / Date d'expiration
14-11-2032
Place of birth / Lieu de naissance
Eindhoven
1985
Signature
Authority / Autorité
Managing Director IDcentre

P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<
NL1010105ONLD8502038M3110108<2021IDCENTRE<58

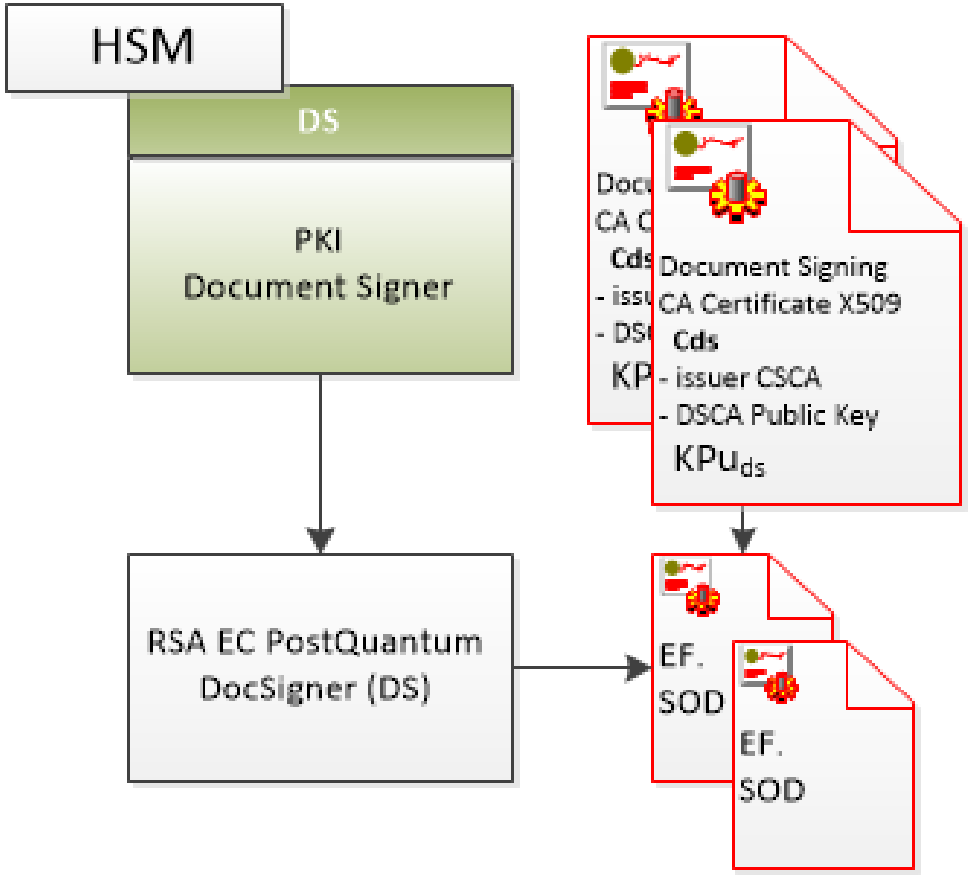
Signing in two different EF.Sod's

Needs **significant** change in chip

Needs **complex** coding in DocSigner

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

Hybrid solution 2



Signing in two different EF.Sod’s

Needs **significant** change in chip

Needs **complex** coding in DocSigner

Needs **complex** coding in BC System

WORLDWIDE IMPLEMENTATION OF PQC IN EMRTDs

	Government costs	Complexity	PKI	Border Control
Full Switch Over At Once	$	+	Needs new HSM for CSCA and DS Needs CA and DS update for handling PQC	Needs Inspection System update for handling PQC
Hybrid Solution 1	$$	++ Needs change in chip with EF.SOd, double signature	Needs new HSM for CSCA and DS Needs CA and DS update for handling PQC Needs maintenance for double PKI	Needs Inspection System update for handling PQC Needs extra Inspection System update for handling EF.SOd.
Hybrid Solution 2	$$$	+++ Needs change in chip with two EF.SOd's. Extra secure token (marking) in chip is necessary.	Needs new HSM for CSCA and DS Needs CA and DS update for handling PQC Needs maintenance for double PKI	Needs Inspection System update for handling PQC Needs extra complex Inspection System update for handling more EF.SOd's.

PASSPORT
PASSEPORT
ABROADIA
Type P
Code NLD
Passport No / Passeport N
NL1010105
Name / Nom
Vestram
Given names / Prénoms
Identitatem
Nationality / Nationalité
Netherlands
Date of birth / Date de naissance
03-02-1985
Date of issue / Date de délivrance
14-11-2022
Date of expiry / Date d'expiration
14-11-2032
Place of birth / Lieu de naissance
Eindhoven
Authority / Autorité
Managing
Director
IDcentre
Signature

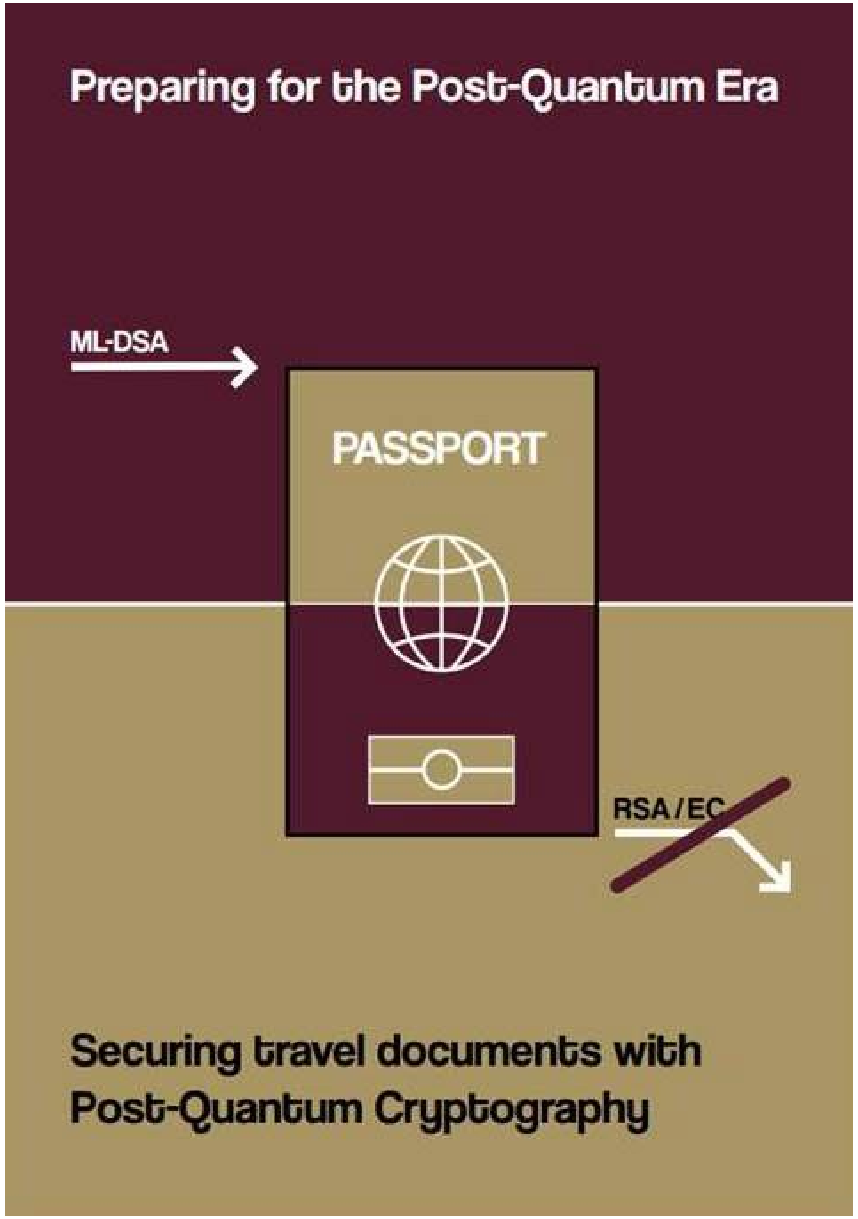
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<<<
NL1010105ONLD8502038M3110108<2021IDCENTRE<58

Document Signing
CA Certificate X509
Cds
- issuer CSCA
- DSCA Public Key

KPu$_{ds}$

Book with thesis, use case and implementation

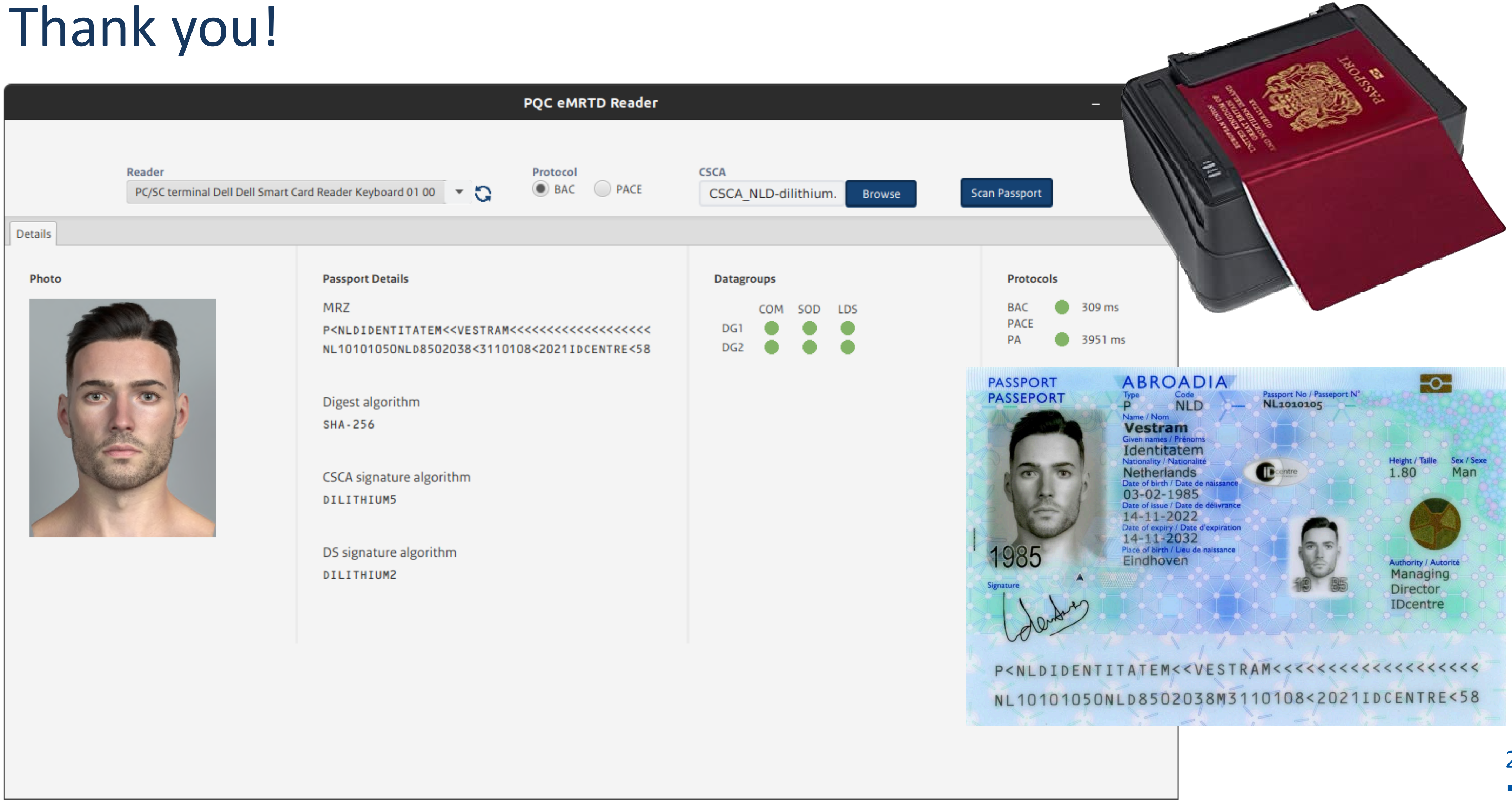
Mail:
s.lepstra@justid.nl
j.deswart@justid.nl



Preparing for the Post-Quantum Era

Securing travel documents with Post-Quantum Cryptography

Thank you!



PQC eMRTD Reader

Reader: PC/SC terminal Dell Dell Smart Card Reader Keyboard 01 00

Protocol: ● BAC ○ PACE

CSCA: CSCA_NLD-dilithium.

Photo

Passport Details

MRZ

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<<
NL10101050NLD8502038<3110108<2021IDCENTRE<58
```

Digest algorithm
SHA-256

CSCA signature algorithm
DILITHIUM5

DS signature algorithm
DILITHIUM2

Datagroups

	COM	SOD	LDS
DG1	●	●	●
DG2	●	●	●

Protocols

BAC	●	309 ms
PACE		
PA	●	3951 ms

PASSPORT
PASSEPORT

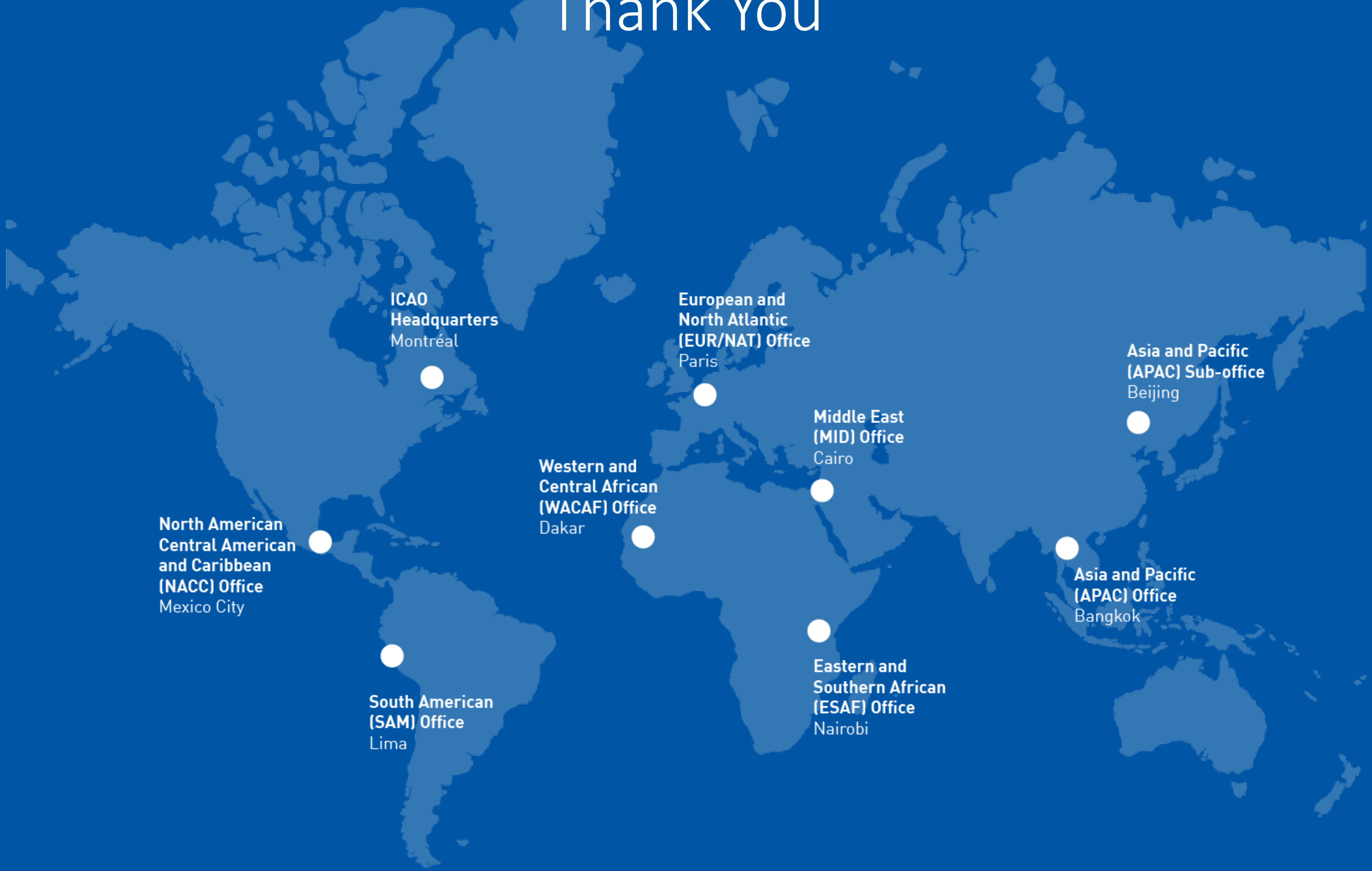
ABROADIA

Type: P
Code: NLD
Passport No / Passeport N°: NL1010105
Name / Nom: **Vestram**
Given names / Prénoms: Identitatem
Nationality / Nationalité: Netherlands
Date of birth / Date de naissance: 03-02-1985
Date of issue / Date de délivrance: 14-11-2022
Date of expiry / Date d'expiration: 14-11-2032
Place of birth / Lieu de naissance: Eindhoven
Height / Taille: 1.80
Sex / Sexe: Man
Authority / Autorité: Managing Director IDcentre

Signature

```
P<NLDIDENTITATEM<<VESTRAM<<<<<<<<<<<<<<<<<<<
NL10101050NLD8502038M3110108<2021IDCENTRE<58
```

Thank You


ICAO Headquarters
Montréal
European and North Atlantic (EUR/NAT) Office
Paris
Asia and Pacific (APAC) Sub-office
Beijing
Middle East (MID) Office
Cairo
Western and Central African (WACAF) Office
Dakar
North American Central American and Caribbean (NACC) Office
Mexico City
Asia and Pacific (APAC) Office
Bangkok
Eastern and Southern African (ESAF) Office
Nairobi
South American (SAM) Office
Lima

ICAO