Keyfactor
Tech Days
2023

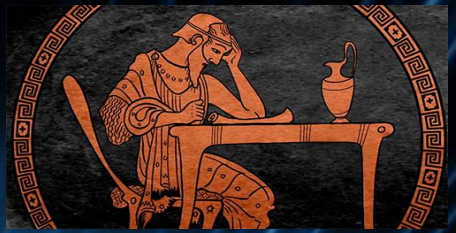
Dutch Ministry of Justice Chiptechnology and PKI use cases

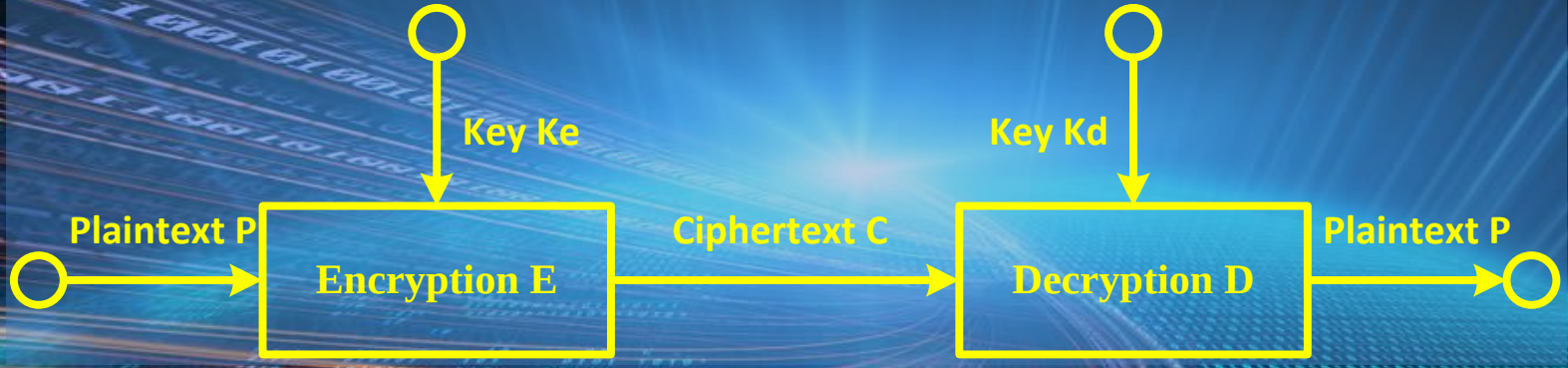
Jeen de Swart

Senior Information / Security Architect

Judicial Information Services

Cryptography





Symmetric encryption

Ke = Kd

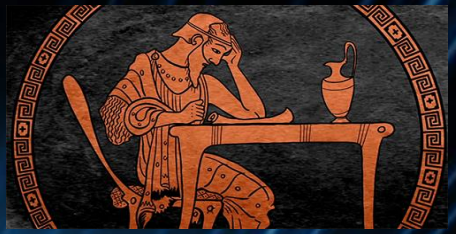
E and D are algorithmes

C = E(T) **T = D(C)**

Asymmetric encryption

Ke ≠ Kd

PKI and HSM



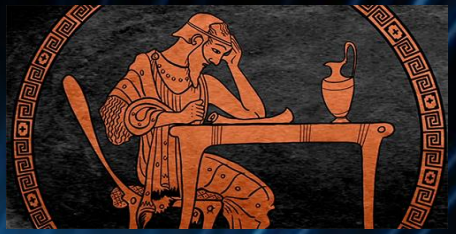
PKI = Public Key Infrastructure

- A set of hardware, software, people, resources, policy and procedures for certificates (create, administrate and revoke).

HSM = Hardware Security Module

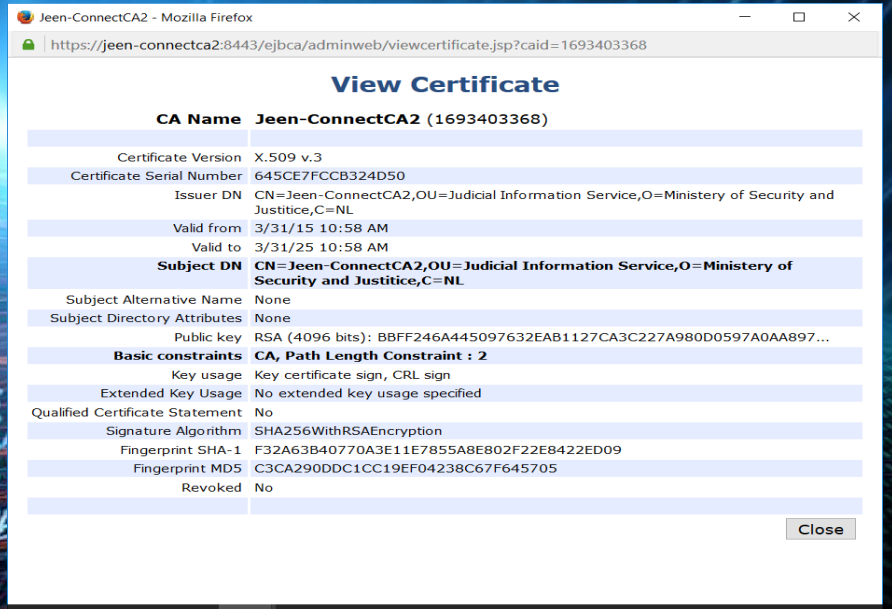
- Physic, tamper-proof, hardware for cryptokeys, creating and administrating.

Certificates

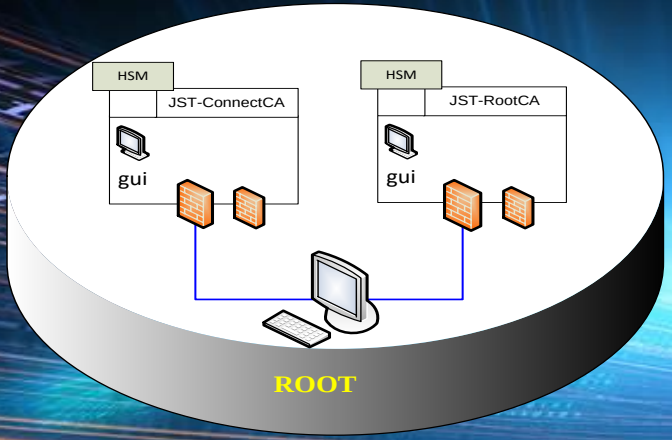


A certificate is a computer file which acts as a digital passport

- Information about functionality and use of keys

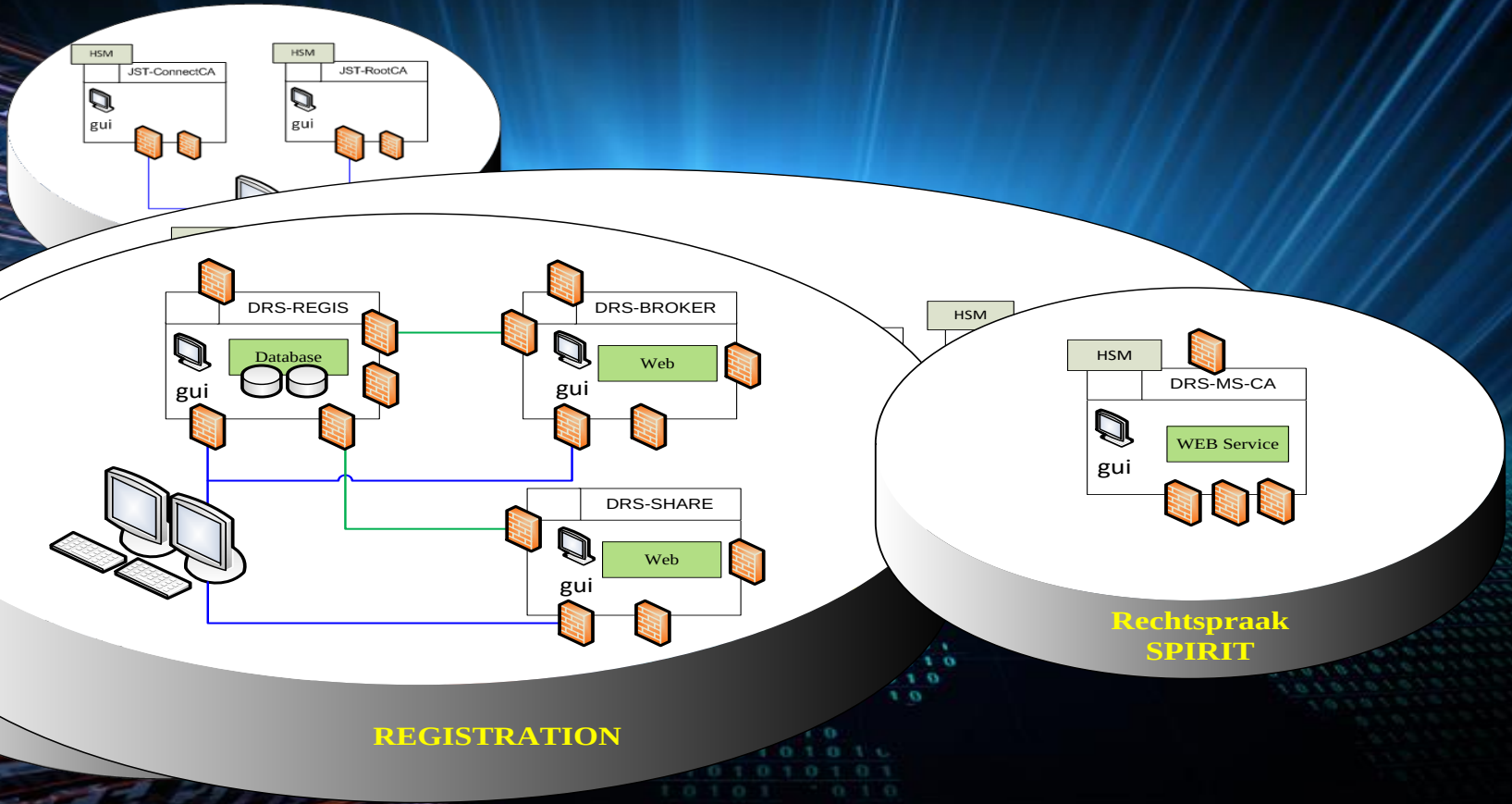


ROOT DOMAIN

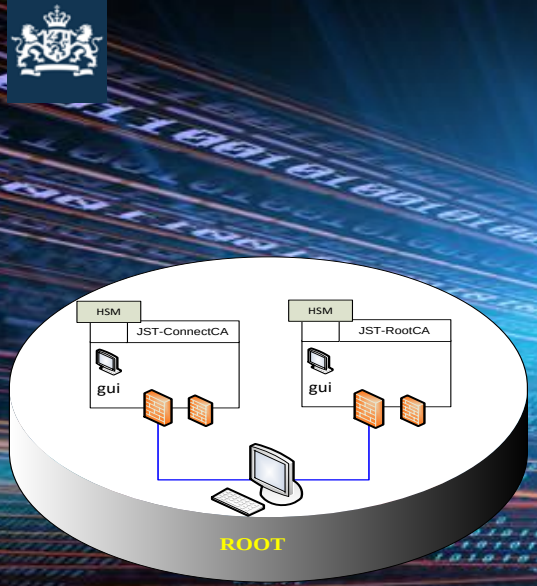

HSM
JST-ConnectCA
gui
HSM
JST-RootCA
gui
ROOT

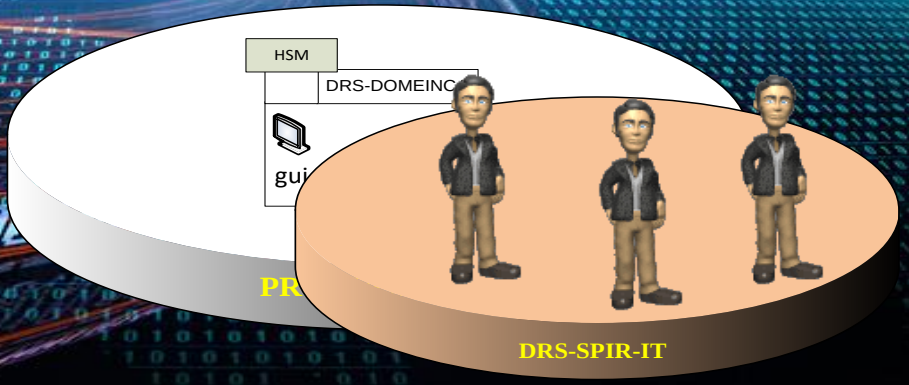

Policy Authority

Landscape Example

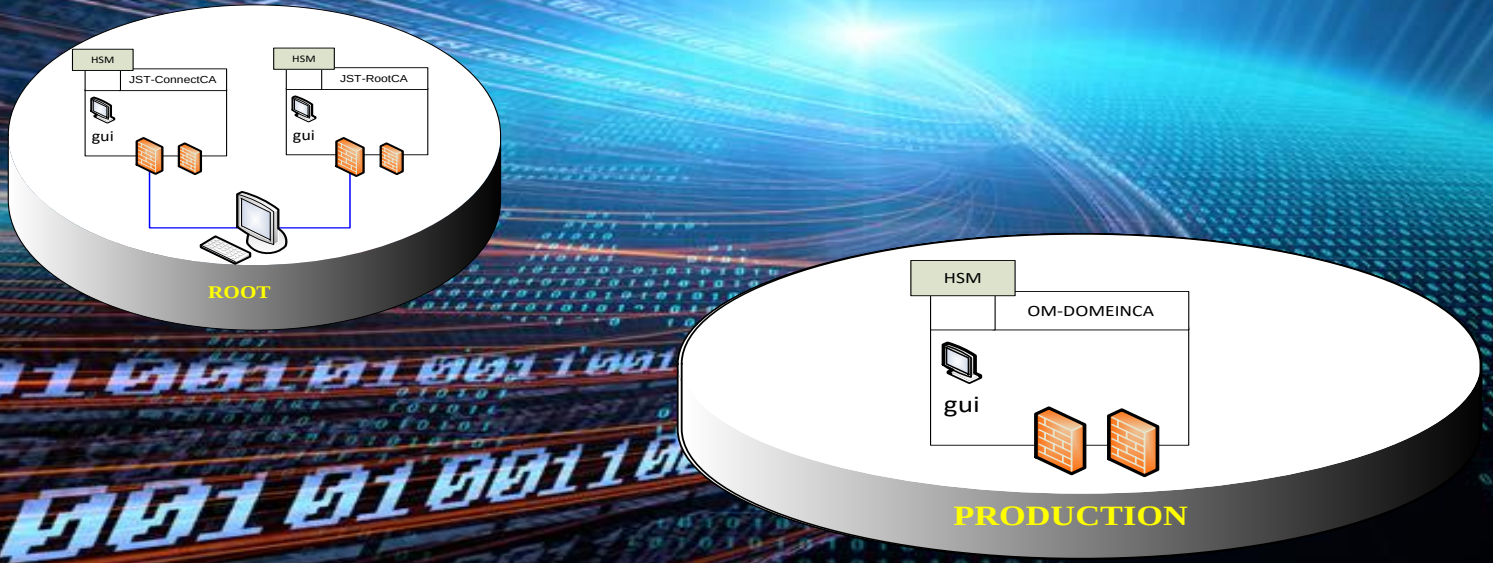


Policy Authority





PRODUCTION DOMAINS



PKI as a Service

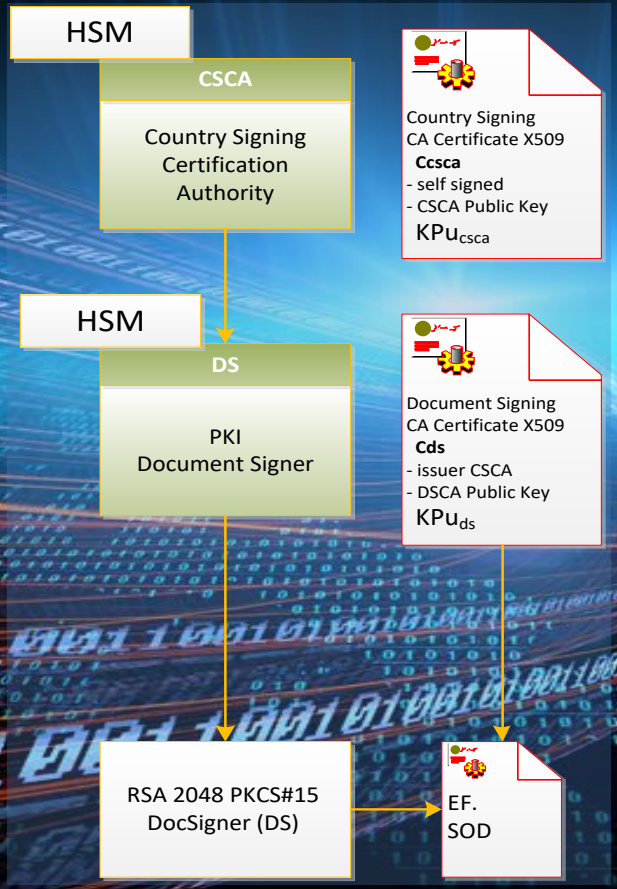
DATA HOLDER PAGE

MRZ machine readable zone

MRP machine readable passport

eMRTD
electronic Machine Readable Travel Document

eMRTD and Health, CSCA PKI chain



eMRTD CHIP LDS (Logical Data Structure)

MF

DF:eMRTD Application
AID='A0 00 00 02 47 10 01'

F

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

EF.SOD
1

EF.DG1
0

EF.DG2
02

EF.DG3
03

EF.DG4
04

EF.DG15
0F

EF.DG16
10

EF.CardAccess
1C

EF.DIR

<BRUIJN
142NLD6

ISELOTTE<<<<<<<<<<<
0696999999900<<<<<84

EF.ATR/INFO
01

EF.CardSecurity
1D

Passive Authentication
- Checking DS against CSCA

MF = Master File
DF = Dedicated File
EF = Elementary File

eMRTD Passive Authentication

So the digital signature must be checked ?

Chip contains data
Signed by
DS
Document Signer

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

Country Signing
CA Certificate X509
Ccsca
- self signed
- CSCA Public Key
KPu_{csca}

CSCA

Country Signing
Certification
Authority

2D Barcode for Visa

So the digital signature must be checked ?

CSCA

Country Signing Certification Authority

Country Signing CA Certificate X509
Ccsca
- self signed
- CSCA Public Key
KPu_{csca}

Barcode Signing CA Certificate X509
Cbs
- issuer CSCA
- BSCA Public Key
KPU_{bs}

COVID International QR code

So the digital signature must be checked ?

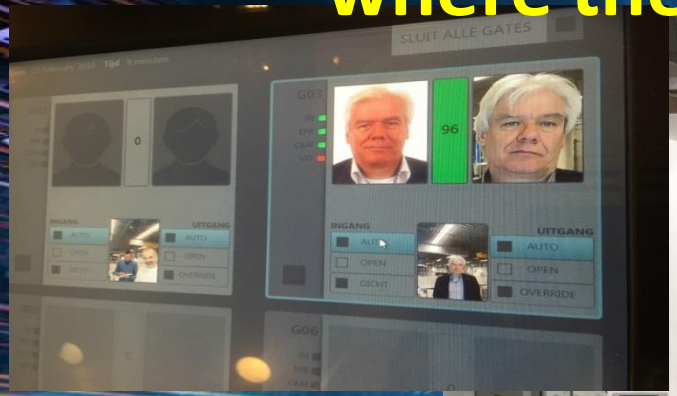
QRcode Signing
CA Certificate X509
Cqs
- issuer CSCA
- QSCA Public Key
KPU$_{qs}$

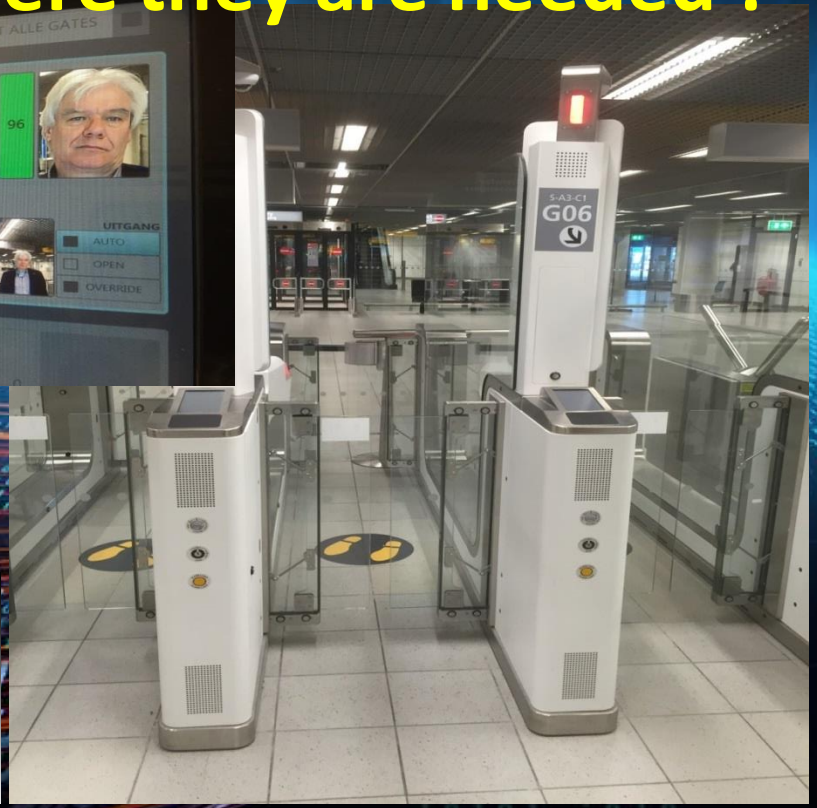
CSCA

Country Signing Certification Authority

Country Signing
CA Certificate X509
Ccsca
- self signed
- CSCA Public Key
KPu$_{csca}$

How to get the certificates where they are needed ?





A National Public Key Directory

	NL-NPKD
The Dutch National Public Key Directory	LDAP

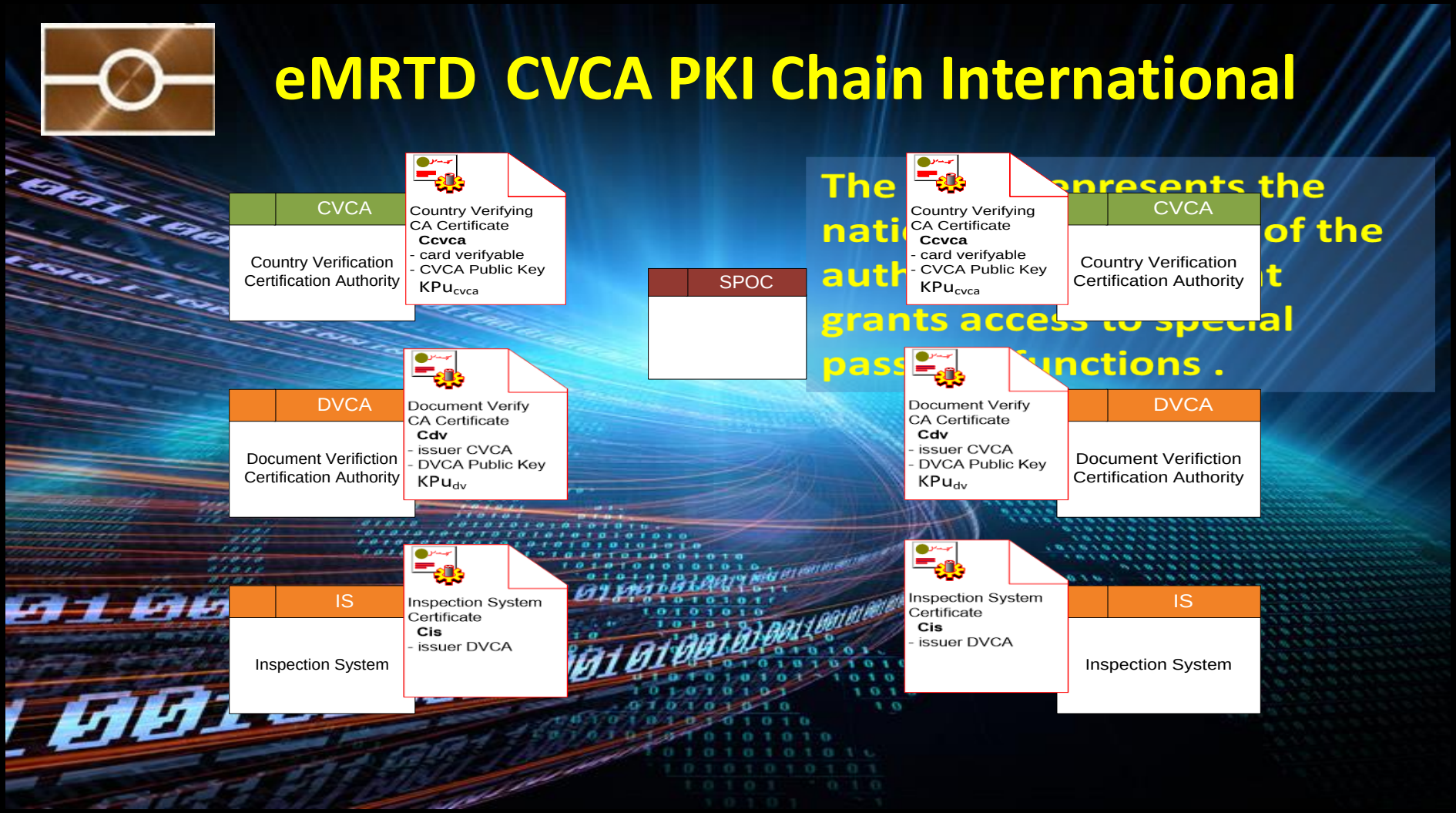
Country Signing
CA Certificate X509
Ccsca
- self signed
- CSCA Public Key
KPu_{csca}

	NL-NSPOC
The Dutch National Single Point of Contact	WSDL

	NL-TCC
The Dutch National Terminal Control Center	WSDL

	NL-TCC
The Dutch National Terminal Control Center	WSDL

eMRTD CVCA PKI Chain International




AB UNO DISCE OMNES
STUDY PASSPORT
Passport/
Passeport
KONINKRIJK DER NEDERLANDEN
KINGDOM OF THE NETHERLANDS
ROYAME DES PAYS-BAS
Type/ Type
P
Country code/ Code du pays
NLD
Passport Number/ N° de passeport
NFH0JDS01
Surname/ Nom
Frisia
Given names/ Prénoms
Magnus Dux
Nationality/ Nationalité
Nederlandse
Date of Birth/ Date de naissance
03 FEB/ FEB 1959
Sex/ Sexe
M/ M
Date of Issue/ Date de délivrance
2 MEI/ MAY 2018
Date of Expiry/ Date d'expiration
2 MEI/ MAY 2028
Lenght/ Taille
1,78 m
Place of Birth/ Place de naissance
Leeuwarden
Authority/ Autorité
Burg. van
Ferwerderadiel
Holder's Signature/ Signature du
P<NLDFRISIA<<MAGNUS<DUX<<<<<<<<<<<<<<<<<<<<
NFH0JDS010NLD5902039M2805025987654321<<<<
MDF001
MDF002


Chiptechnology
and
PKI
Excercises
Chiptechnology
and
PKI

f$endtime

Judicial Information Service
Ministry of Justice and Security

That's it, you made it ……
You can wake up now …

“

We are walking around during these Tech Days. Don’t hesitate to contact us when you have questions or want more
ion

Jeen de Swart

j.deswart@justid.nl

Cor de Jonge

c.dejonge@justid.nl