



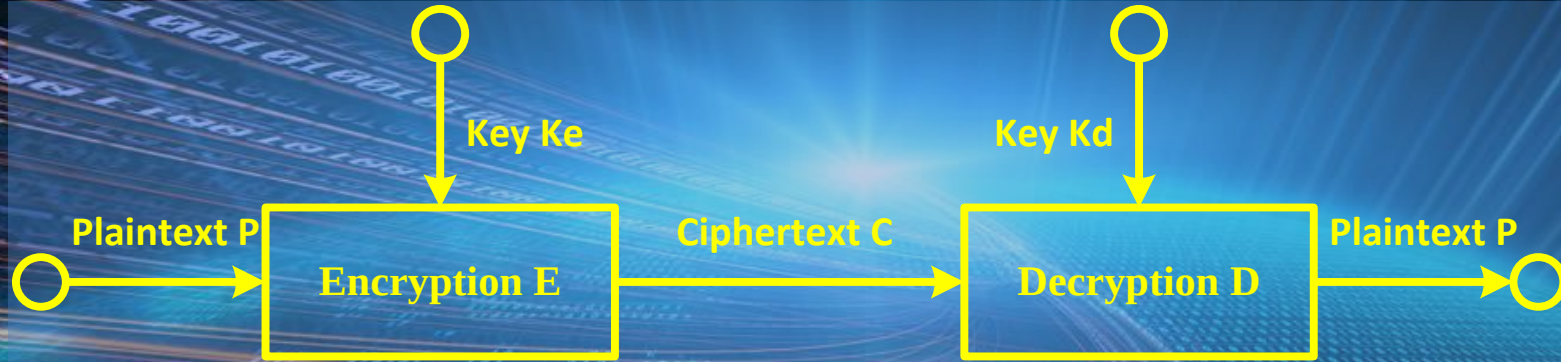
Dutch Ministry of Justice Chiptechnology and PKI use cases



Jeen de Swart

Senior Information/ Security Architect
Judicial Information Services

Cryptography



Symmetric encryption

$$K_e = K_d$$

E and D are algorithms

$$C = E(T)$$

$$T = D(C)$$

Asymmetric encryption

$$K_e \neq K_d$$

asdtlkuaoleuta;lkdsht;aiwervya
lusi714327697rpk;19907333
9e=23471631de1809a1uer;aihd
aiud;gdueto;uad;ue;acim;it
10aaa94207371;isid73;u;v;u;K1.6
ditroqua;lkahup;40332761ak;leu
likur;lkue;05715735941;lee
in;ka;lkur;aut;0a9324761a;v38
09123011uod7up;hams;hase;1809
12oum;0100;0057;mm11;040411
161u900274900752231mhai;u9308
702134u111k2a1k4d096707043ads

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.



asdtikuoieuta;lkdsht;aiwcvya
lusi714327697mpak199077934
991amuss172no;010047q251
9e=234716151de1889a1uwr1alind
aiudmgiueto1uud1uwtas1mwt1
10aae942673511shp12;u1vp;K10
d1troqua;lkahup140332761ak1eur
1kuar1kure0637;575594711ee
in1ka1;lkure100a932761a1v218
89123811uws1up1ams1nase11889
12ou1uwr100;00011100a11
161u98827498075231mha11u9888
782134u111k2a1k4d896787c4sads

Certificates

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

- Information about functionality and use of keys



Jeen-ConnectCA2 - Mozilla Firefox

https://jeen-connectca2:8443/ejbca/adminweb/viewcertificate.jsp?caid=1693403368

View Certificate

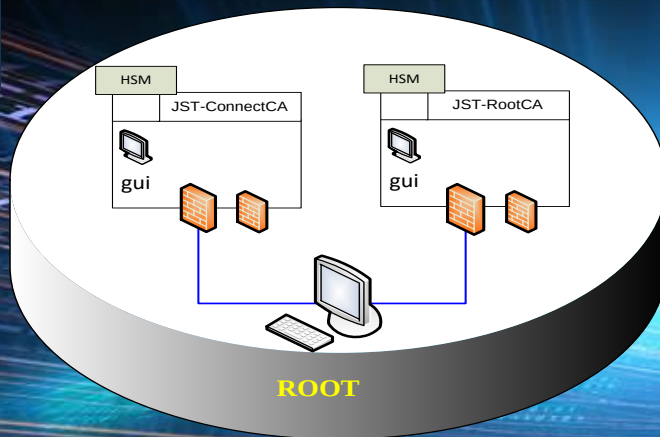
CA Name	Jeen-ConnectCA2 (1693403368)
Certificate Version	X.509 v.3
Certificate Serial Number	645CE7FCCB324D50
Issuer DN	CN=Jeen-ConnectCA2,OU=Judicial Information Service,O=Ministry of Security and Justice,C=NL
Valid from	3/31/15 10:58 AM
Valid to	3/31/25 10:58 AM
Subject DN	CN=Jeen-ConnectCA2,OU=Judicial Information Service,O=Ministry of Security and Justice,C=NL
Subject Alternative Name	None
Subject Directory Attributes	None
Public key	RSA (4096 bits): BBFF246A445097632EAB1127CA3C227A980D0597A0AA897...
Basic constraints	CA, Path Length Constraint : 2
Key usage	Key certificate sign, CRL sign
Extended Key Usage	No extended key usage specified
Qualified Certificate Statement	No
Signature Algorithm	SHA256WithRSAEncryption
Fingerprint SHA-1	F32A63B40770A3E11E7855A8E802F22E8422ED09
Fingerprint MD5	C3CA290DDC1CC19EF04238C67F645705
Revoked	No

Close



```
padtlkuaopigutalldshgtaieocerya  
kwi142576997rpak186071814w  
9671aw48as10ppn01q547q588a  
8y2547467548991awrt4iaw  
aiudropwiewtoiwaoiweutaoiweut  
toaaa945075511shqfzmyvukLS  
q1troqwa1k4q0155767claw  
lkua1kare063757743uek1saw  
r1kua1kurew15892376741758  
9a12561lues7up1hmo01h4506  
12oiuagthp06857mnh1120ak1  
lk1uaw5745976cc1waa1luy896  
702134u11k2alk4d096707c43afds
```

ROOT DOMAIN

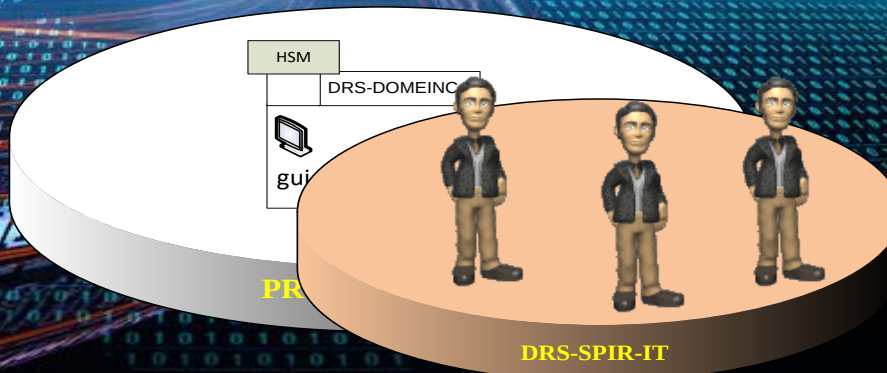
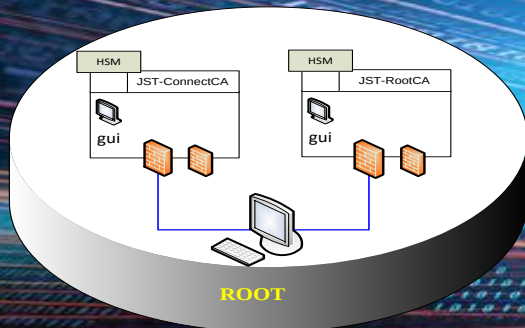






```
psdtkluoioeute;lkdsgh;aiwercva
pssk143297567papak;lsdtklclw
98r;wmdas;lgbrn;bcq4;gq3sdw
gc=2347176;lsdtk1889alwut;lsdhw
aiudropuioeute;aiuoioeuteaiueute
toaa9460755;lsghg;mvn;v;KLS
ditroqua;ikeruut4059276;akjwv
lkua;lkup;lkup;lkup;lkup;lkup;lkup
lkup;lkup;lkup;lkup;lkup;lkup;lkup
091226;luoioeute;hamso;haa947908
12oiuueh;lkup;lkup;lkup;lkup;lkup
lkup;lkup;lkup;lkup;lkup;lkup;lkup
702134;lkup;lkup;lkup;lkup;lkup;lkup
702134;lkup;lkup;lkup;lkup;lkup;lkup
```

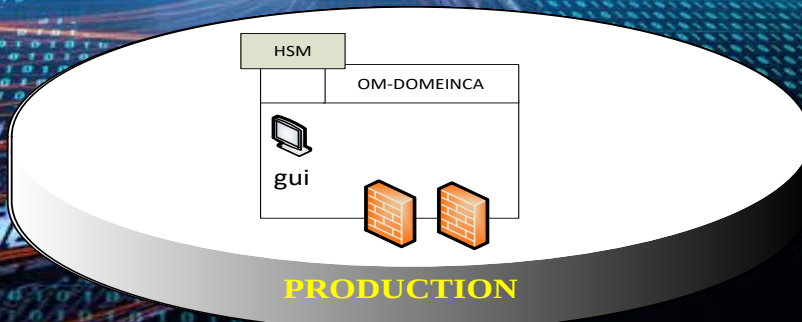
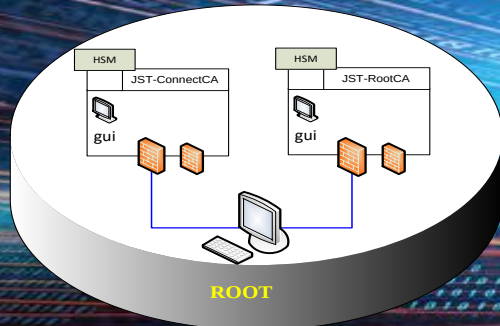
Policy Authority





padtlkxopigutatlkdshgt:aisocerya
wsl1r43257699rpk1860r1a14w
98718w438s110ppn010q341q388s=
9x254r461e1d518991lwr141w1w
aiudropwleutoiuaolweutaoiweut1
03aa945073511shqf3xmp01KLS
01r00w118m103037614k1aw
lkua:lkwe063750r43uek1:1am
r1lk1:lkwe063750r43uek1:1am
09125611u0s7up1hameo1h0847506
12oiuag0th06857mnh11206k11
01w0007699rpk1860r1a14w
702134u11k2alk4d096707c43afds

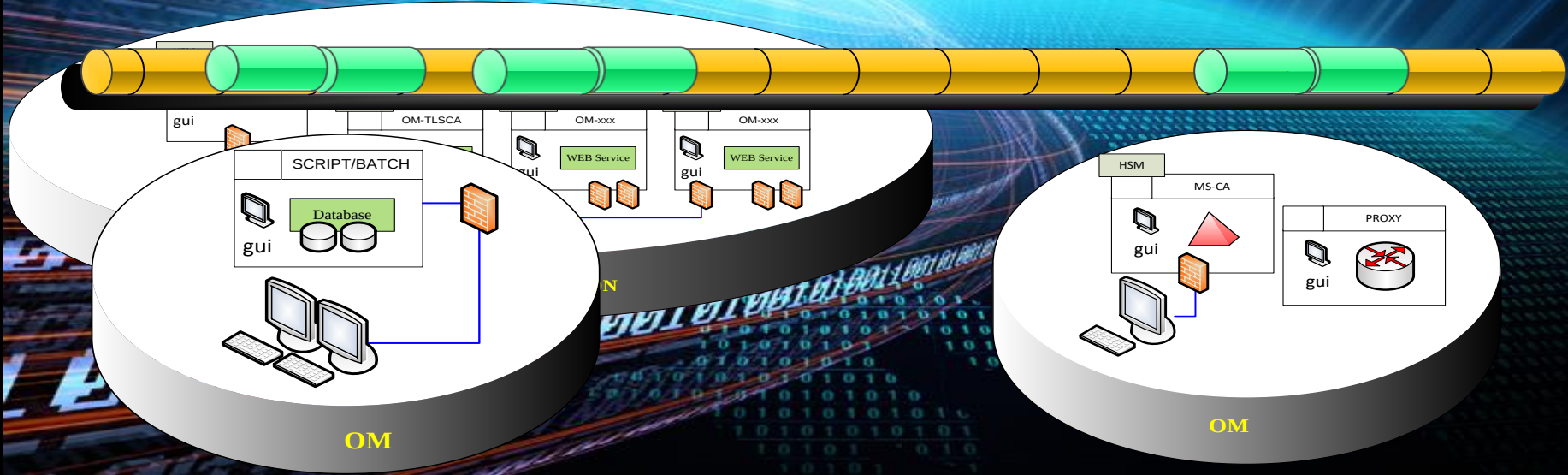
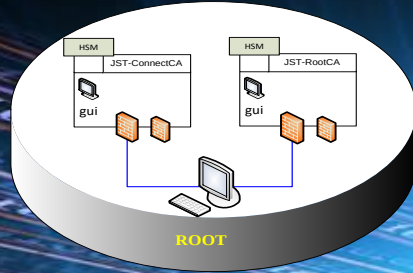
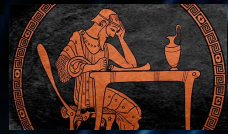
PRODUCTION DOMAINS





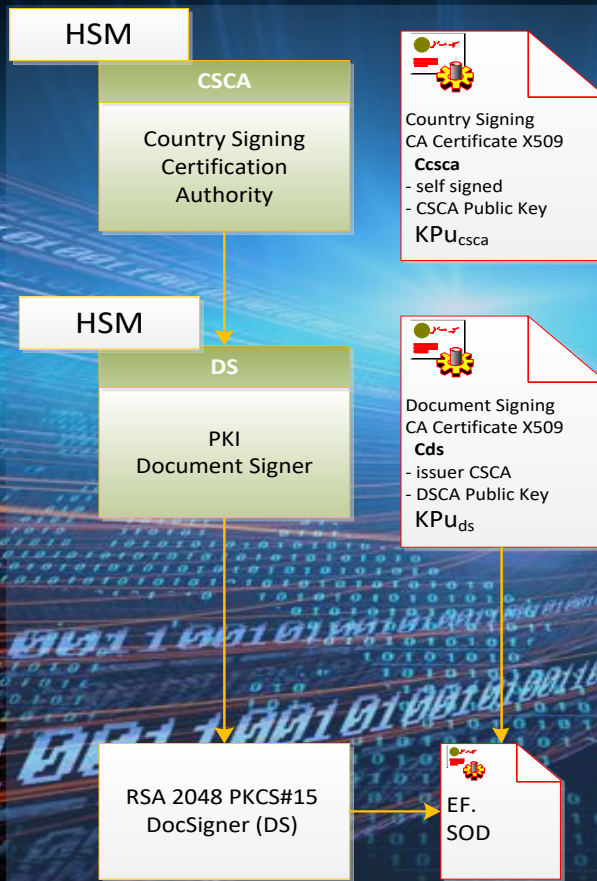
psdtklkuoieuts:lkdsgh:aiwoneu
 9891:48848:397:psk:18017:17474
 0891:48848:397:psk:18017:17474
 c:23:77615d:618094aiw:aiw
 aiwdurowieuto:iauiaweiutoaiwuiw
 toaa9460755:ishgrf:mvynv:KLS
 ltrroqua:ikeruol:30334:614k:jeur
 ikuu:jeur00636:97245aiw:aiw
 0912361:kuowup:hams0:habs0:738
 120iueuot:08570mm:120k:1k
 1k:1u0021:18301:1mm:1u0021
 702134u11k12ak4d095707645a1d5

PKI as a Service





eMRTD and Health, CSCA PKI chain







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
 $KP_{u_{ds}}$


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

CSCA
Country Signing
Certification
Authority



2D Barcode for Visa



So the digital signature must be checked ?



CSCA

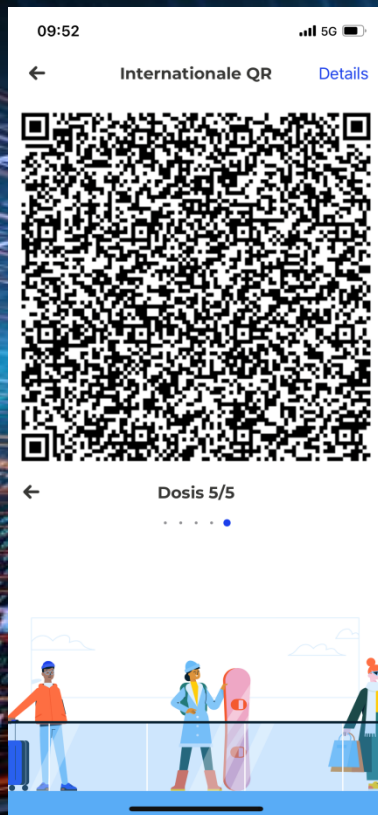
Country Signing
Certification
Authority


Country Signing
CA Certificate X509
Ccsca
- self signed
- CSCA Public Key
KPU_{csc}

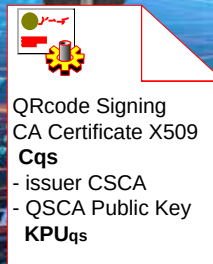

Barcode Signing
CA Certificate X509
Cbs
- issuer CSCA
- BSCA Public Key
KPU_{bs}



COVID International QR code



So the digital signature must be checked ?



QRcode Signing
CA Certificate X509
Cqs
- issuer CSCA
- QSCA Public Key
KPU_{qs}



Country Signing
CA Certificate X509
Ccsca
- self signed
- CSCA Public Key
KPU_{cscsa}

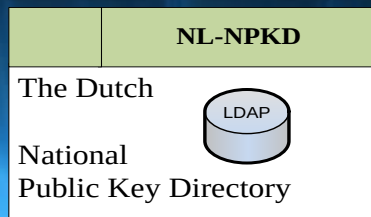
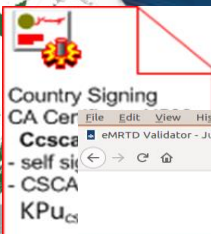


How to get the certificates where they are needed ?



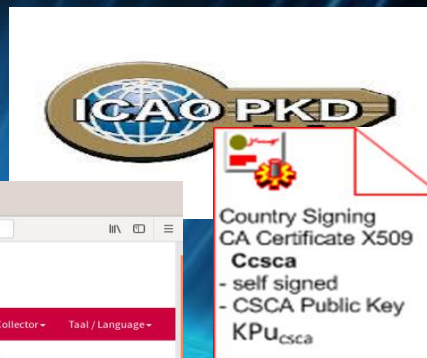


A National Public Key Directory



The Dutch

National
Public Key Directory



The Dutch

National
Single Point of Contact



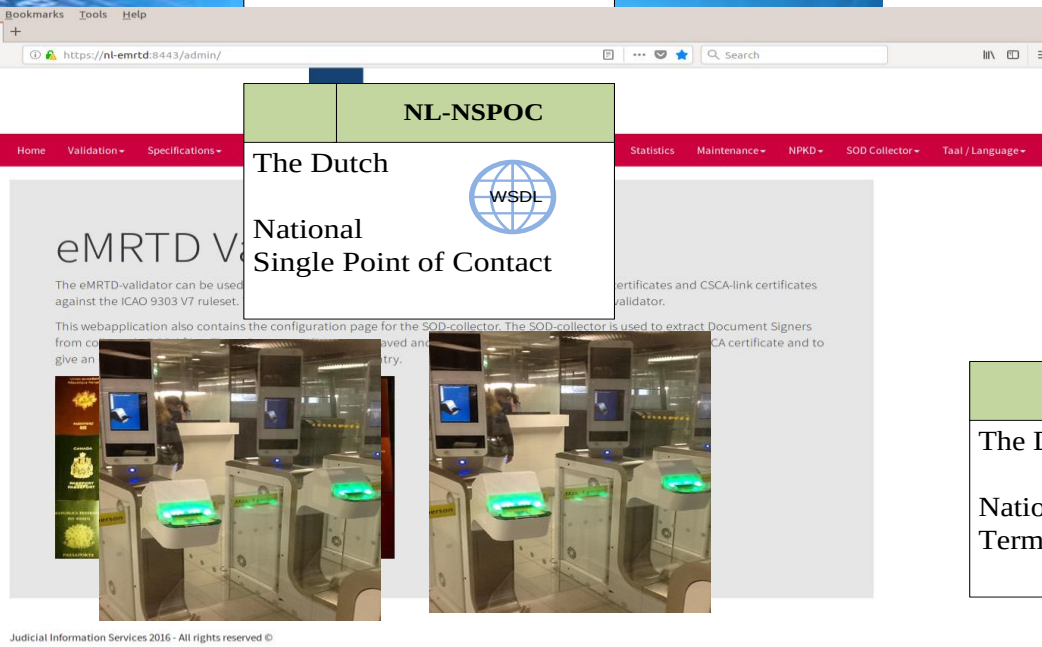
The Dutch

National
Terminal Control Center



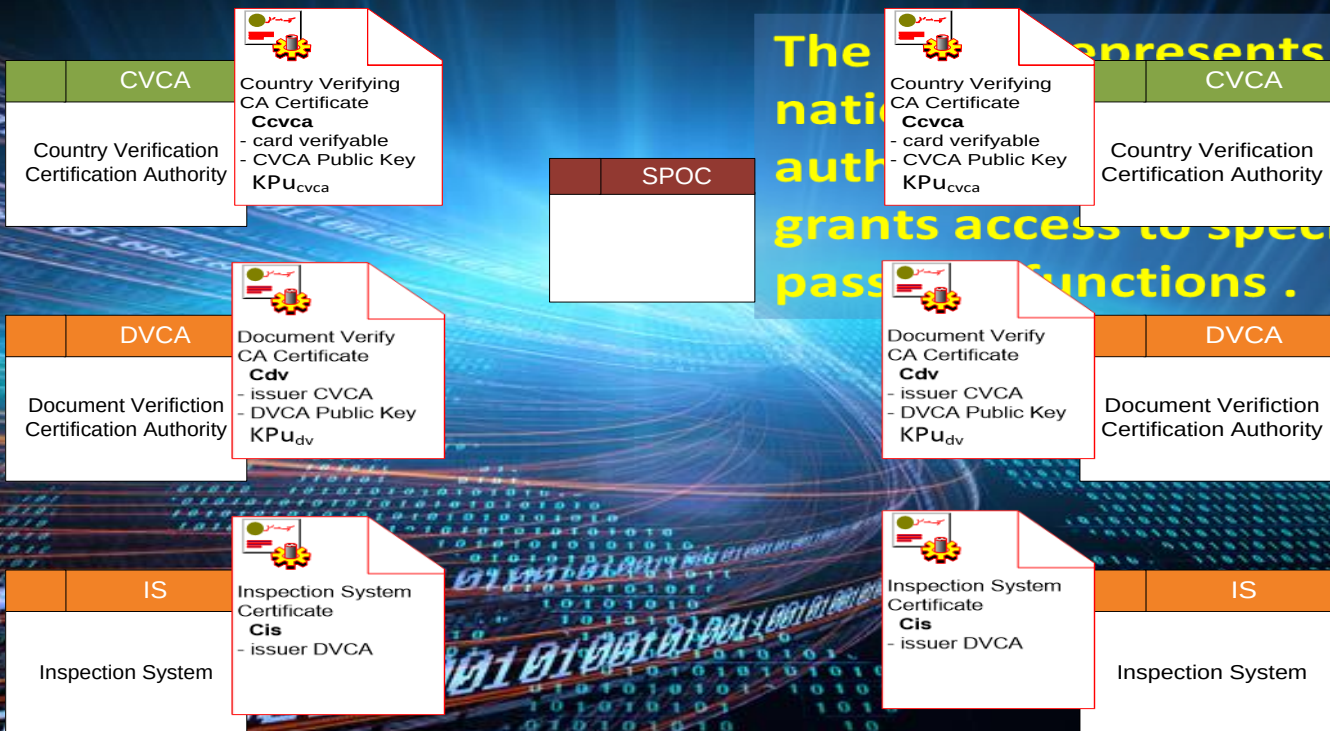
The Dutch

National
Terminal Control Center

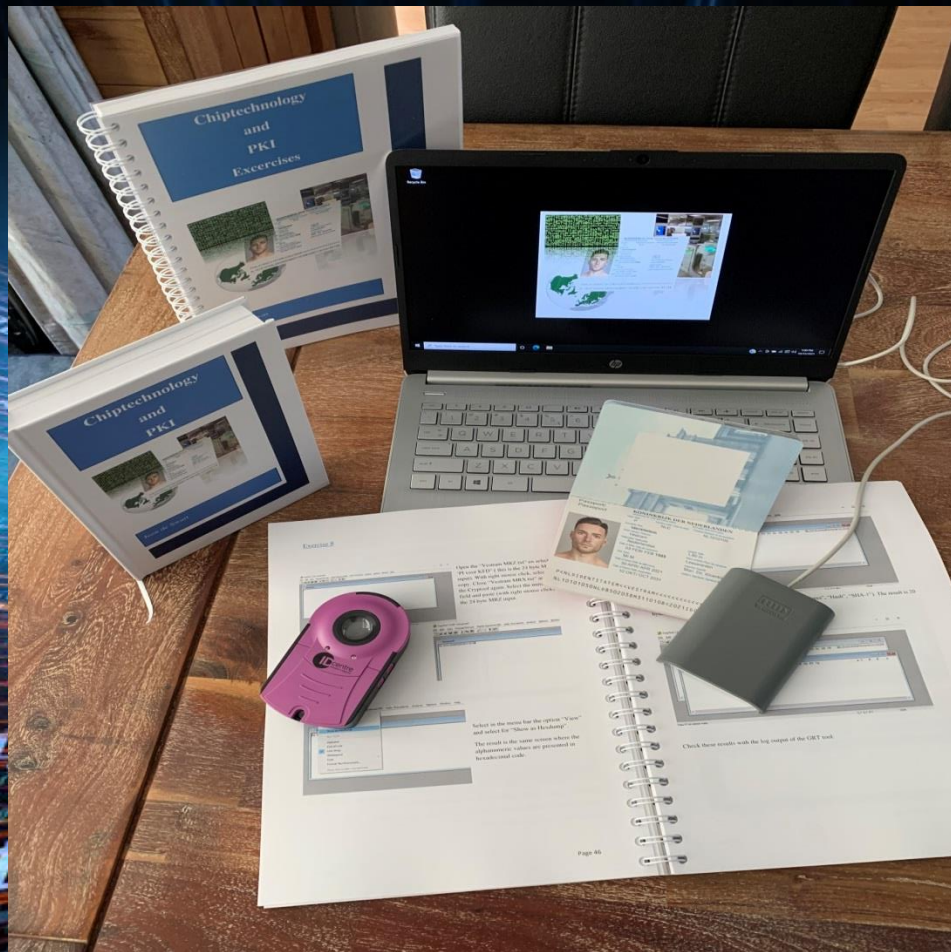




eMRTD CVCA PKI Chain International







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

information



Jeen de Swart

j.deswart@justid.nl



Cor de Jonge

c.dejonge@justid.nl