Ministerie van Volksgezondheid,
Welzijn en Sport

Securing the largest infrastructures with little boxes. And we love it.

Oscar Koeroo

CISO Concern voor het Ministerie van Volksgezondheid, Welzijn en Sport

HET
DONORREGISTER

HOE WILT U ER IN STAAN?

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

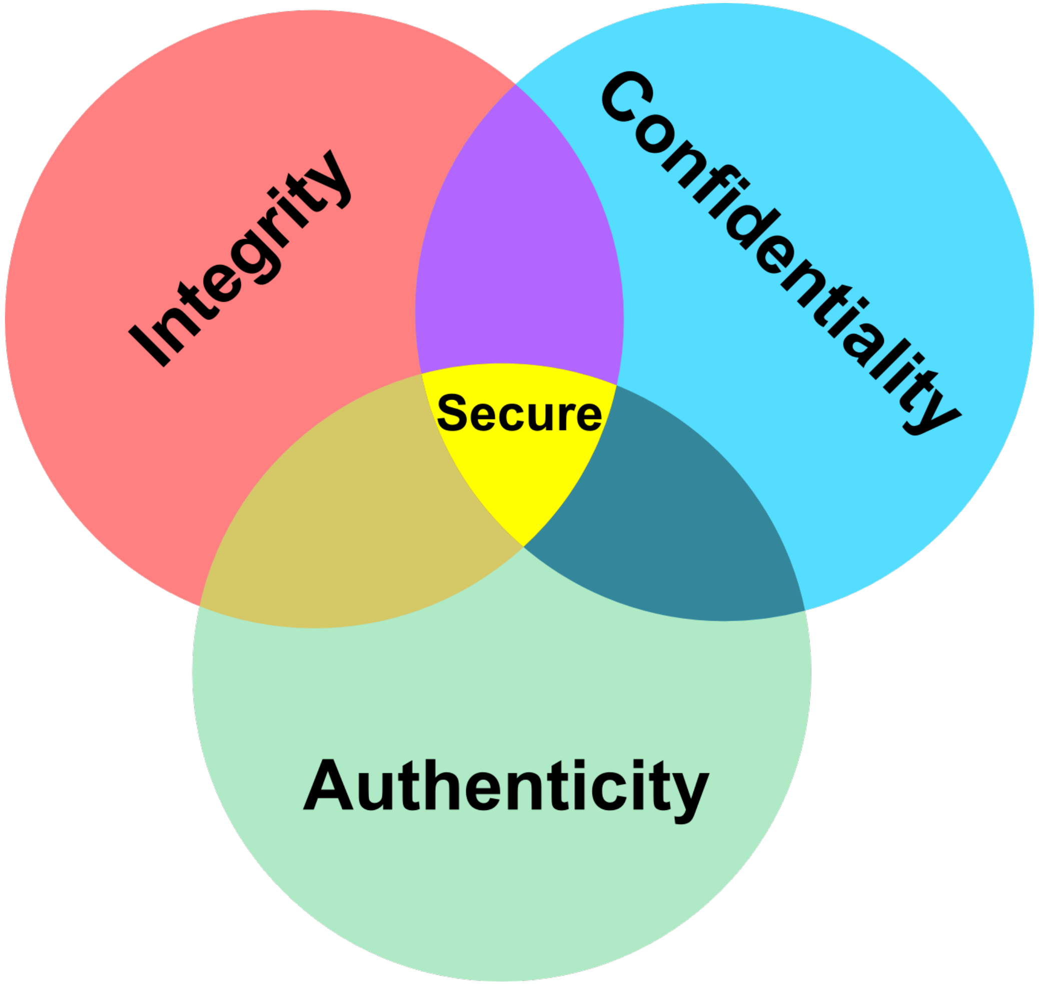
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

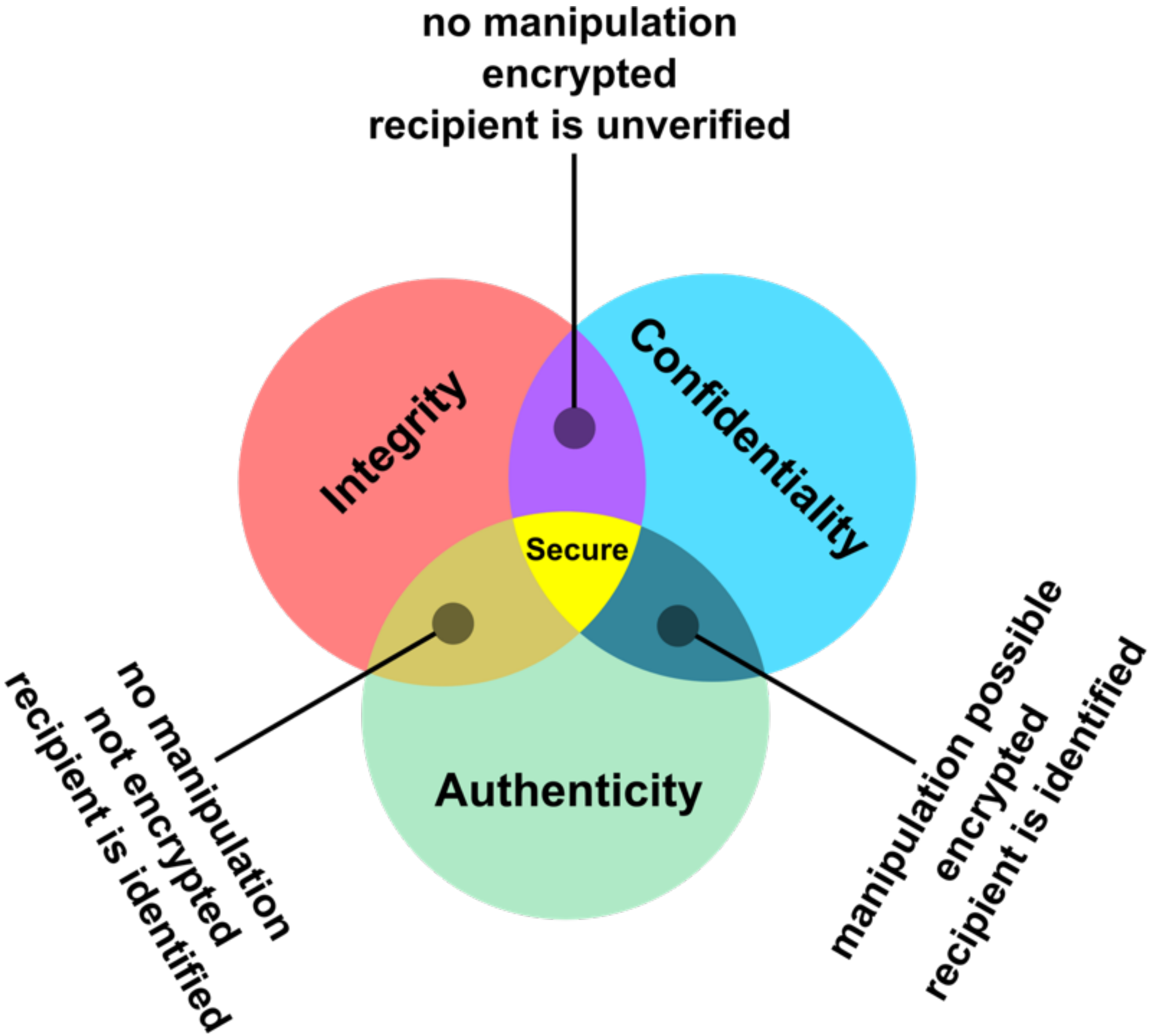
   eyDnsh-fSebwG-yPU1Av-ybXzTa-B1CqTi-4GWHTW-11SnPk-MpAF58-KEhgW1-wLhPRb

If you already purchased your key, please enter it below.
Key: _

```
sh-3.2$ env x='
rable' bash -c
■
vulnerable
this is a test
```

What makes a connection secure?



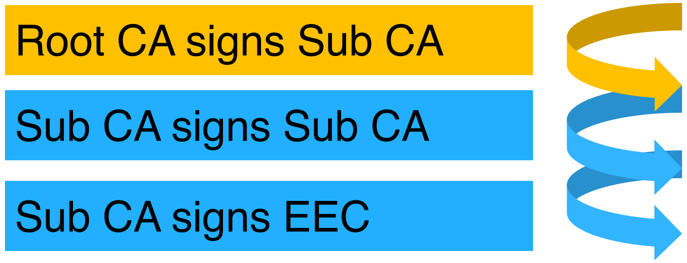


no manipulation
encrypted
recipient is unverified

no manipulation
not encrypted
recipient is identified

manipulation possible
encrypted
recipient is identified

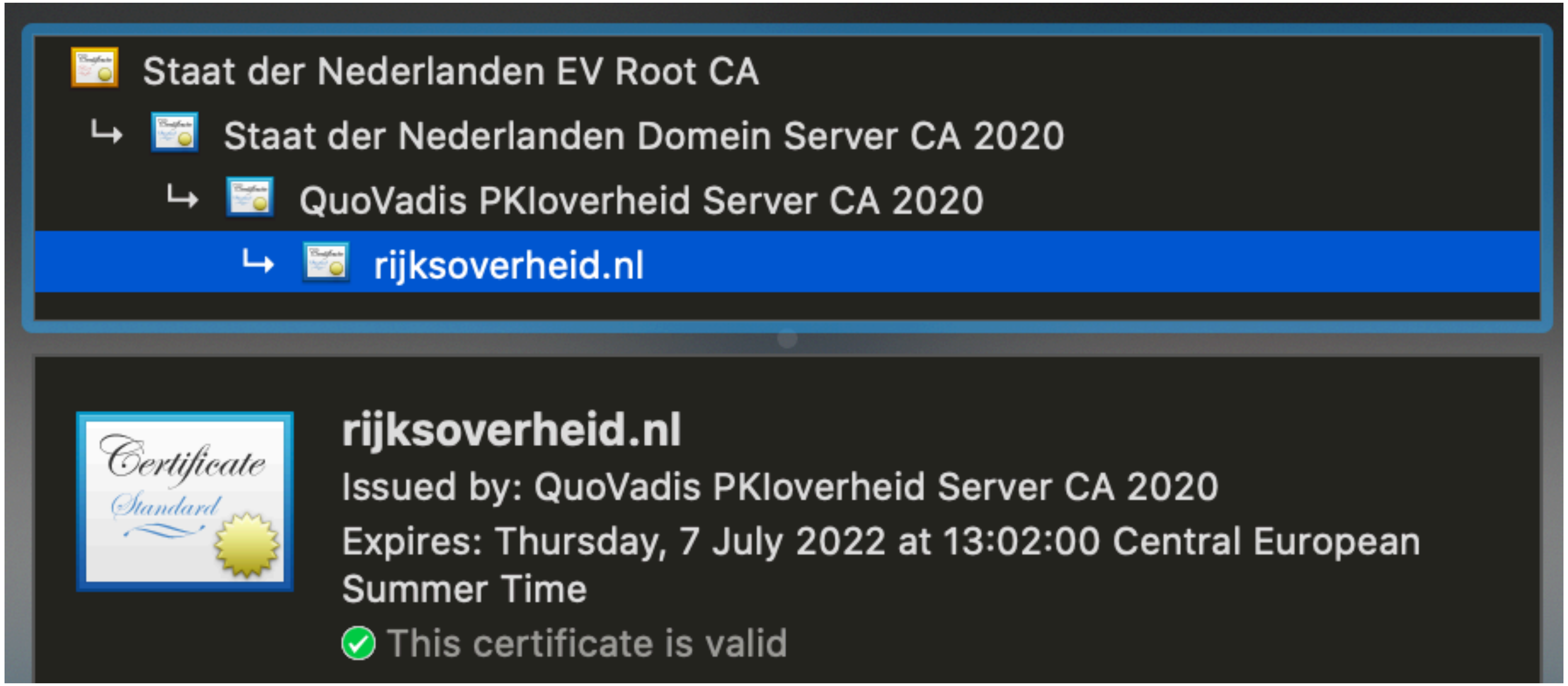
Certificate chain signing



Root CA signs Sub CA

Sub CA signs Sub CA

Sub CA signs EEC



Staat der Nederlanden EV Root CA
↳ Staat der Nederlanden Domein Server CA 2020
↳ QuoVadis PKIoverheid Server CA 2020
↳ rijksoverheid.nl

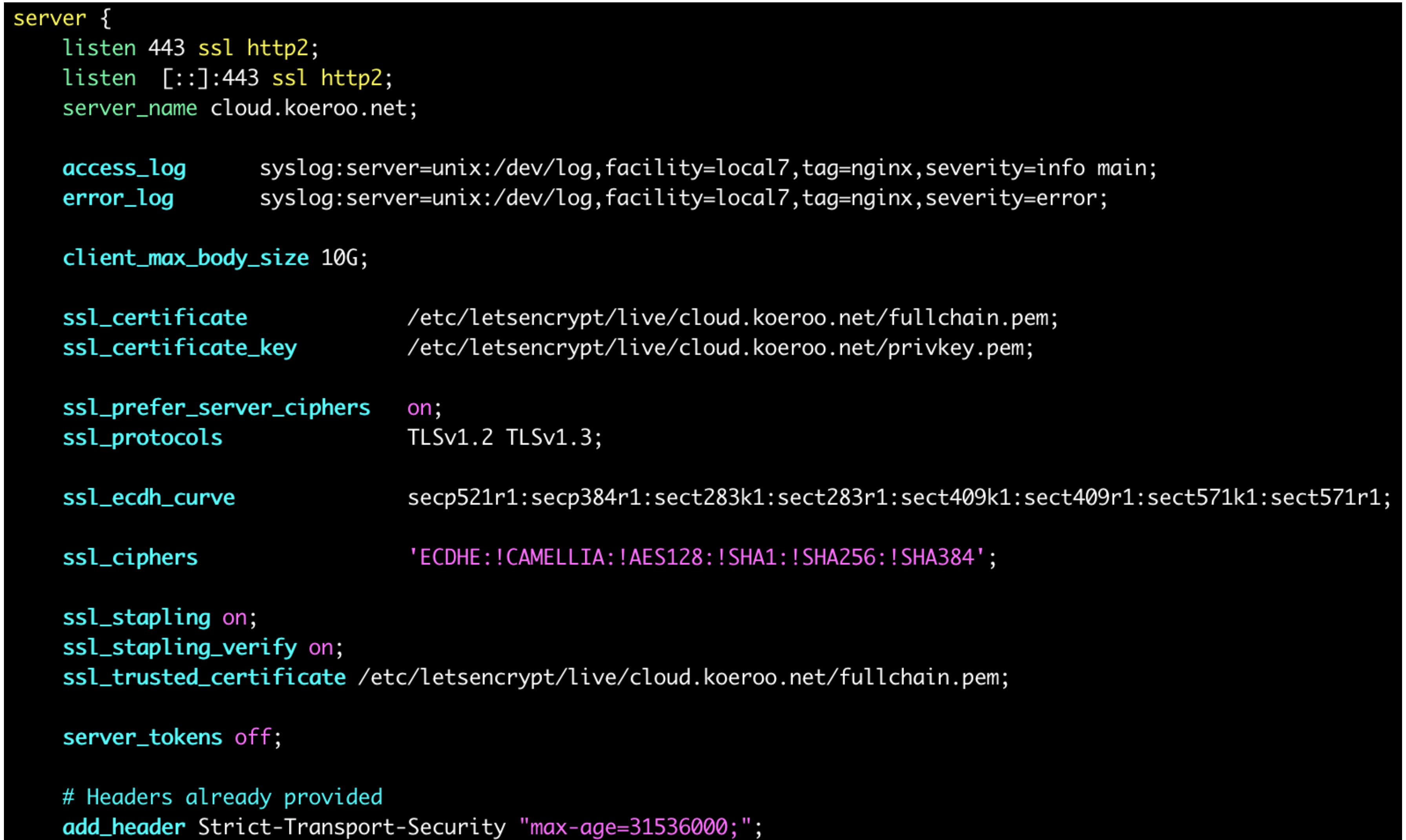
rijksoverheid.nl

Issued by: QuoVadis PKIoverheid Server CA 2020

Expires: Thursday, 7 July 2022 at 13:02:00 Central European Summer Time

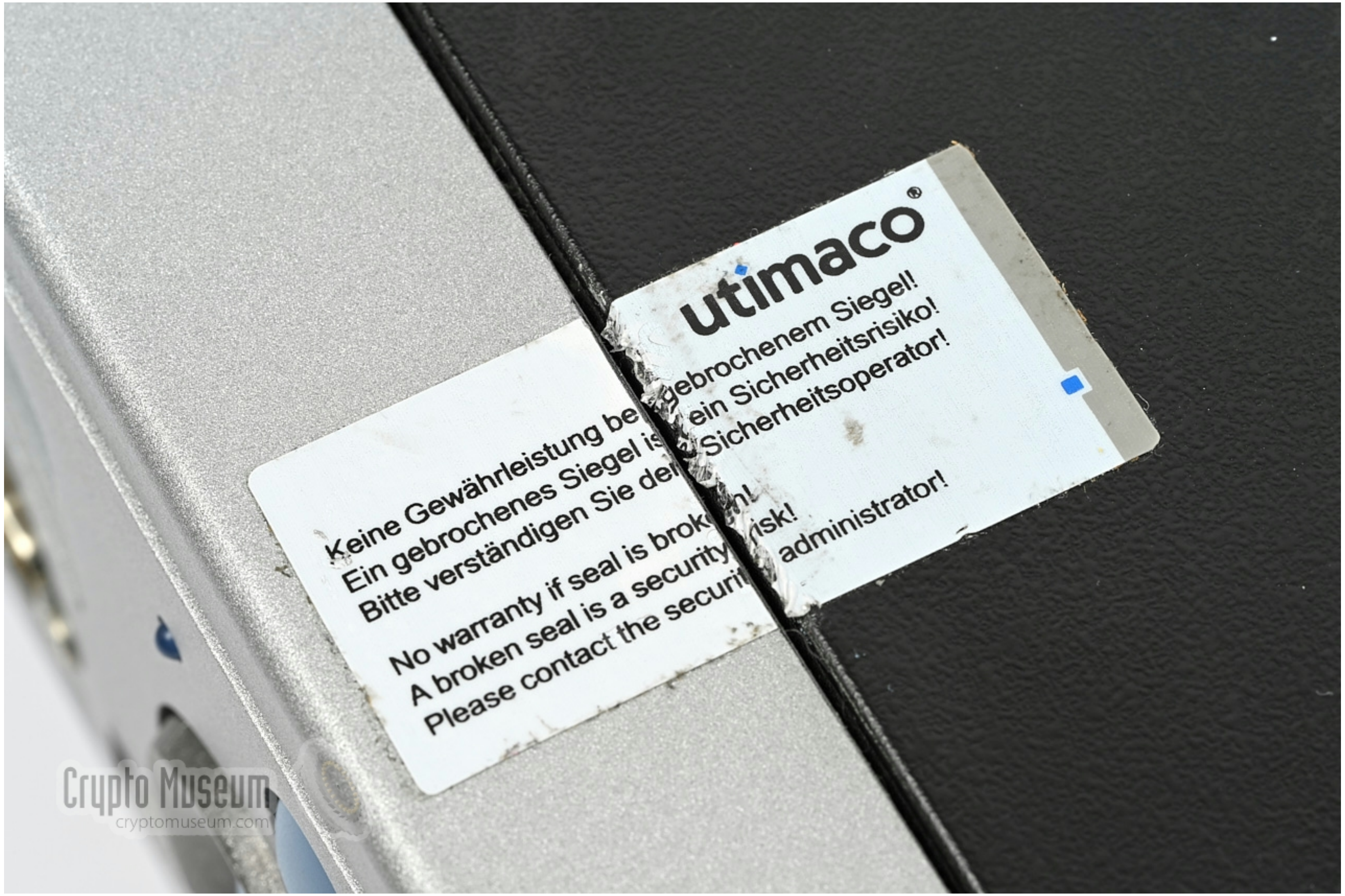
✓ This certificate is valid

Where do you leave your webserver keys?

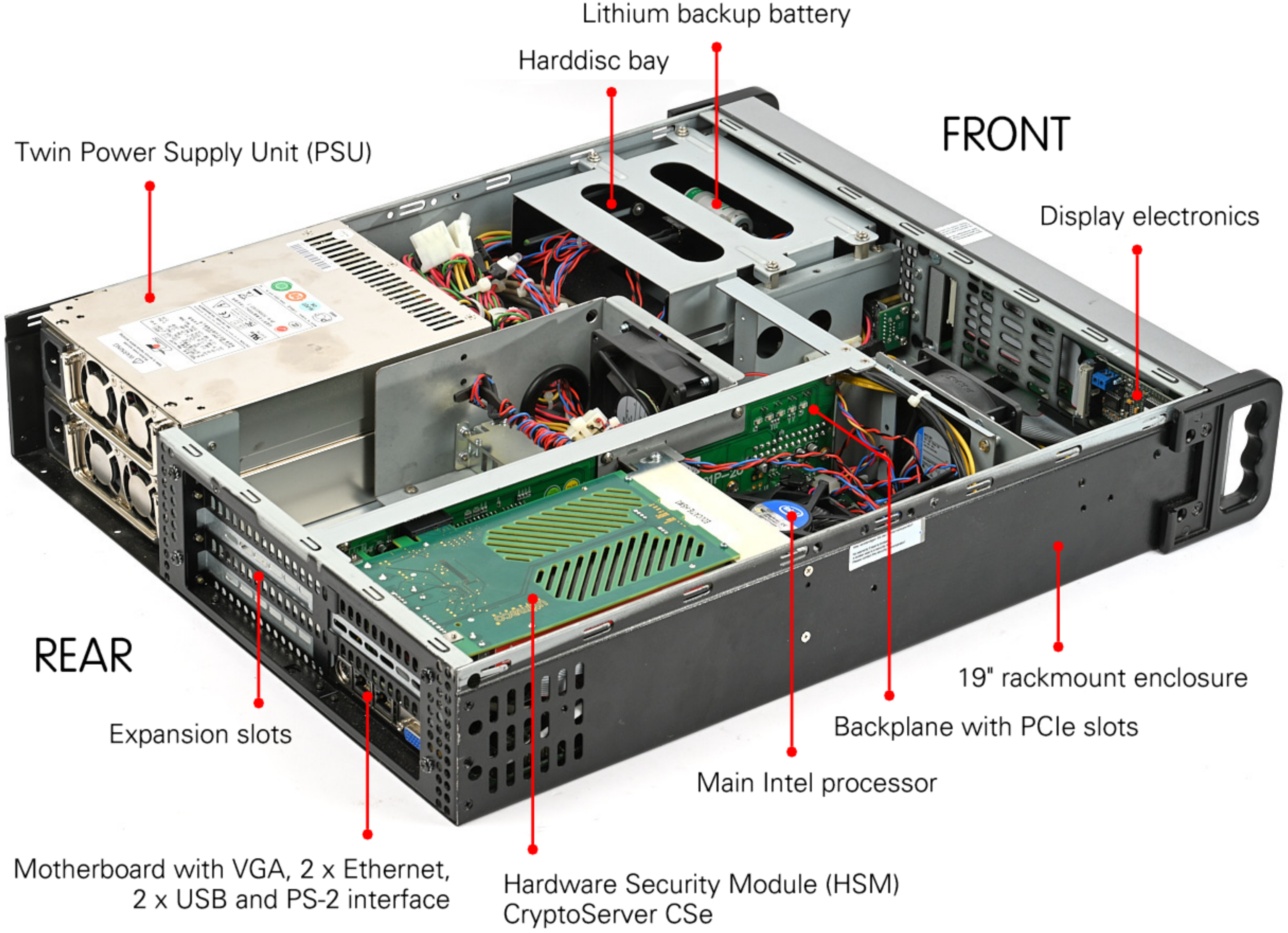


```
server {
    listen 443 ssl http2;
    listen  [::]:443 ssl http2;
    server_name cloud.koeroo.net;

    access_log      syslog:server=unix:/dev/log,facility=local7,tag=nginx,severity=info main;
    error_log       syslog:server=unix:/dev/log,facility=local7,tag=nginx,severity=error;

    client_max_body_size 10G;

    ssl_certificate             /etc/letsencrypt/live/cloud.koeroo.net/fullchain.pem;
    ssl_certificate_key         /etc/letsencrypt/live/cloud.koeroo.net/privkey.pem;

    ssl_prefer_server_ciphers   on;
    ssl_protocols               TLSv1.2 TLSv1.3;

    ssl_ecdh_curve              secp521r1:secp384r1:sect283k1:sect283r1:sect409k1:sect409r1:sect571k1:sect571r1;

    ssl_ciphers                 'ECDHE:!CAMELLIA:!AES128:!SHA1:!SHA256:!SHA384';

    ssl_stapling on;
    ssl_stapling_verify on;
    ssl_trusted_certificate /etc/letsencrypt/live/cloud.koeroo.net/fullchain.pem;

    server_tokens off;

    # Headers already provided
    add_header Strict-Transport-Security "max-age=31536000;";
```

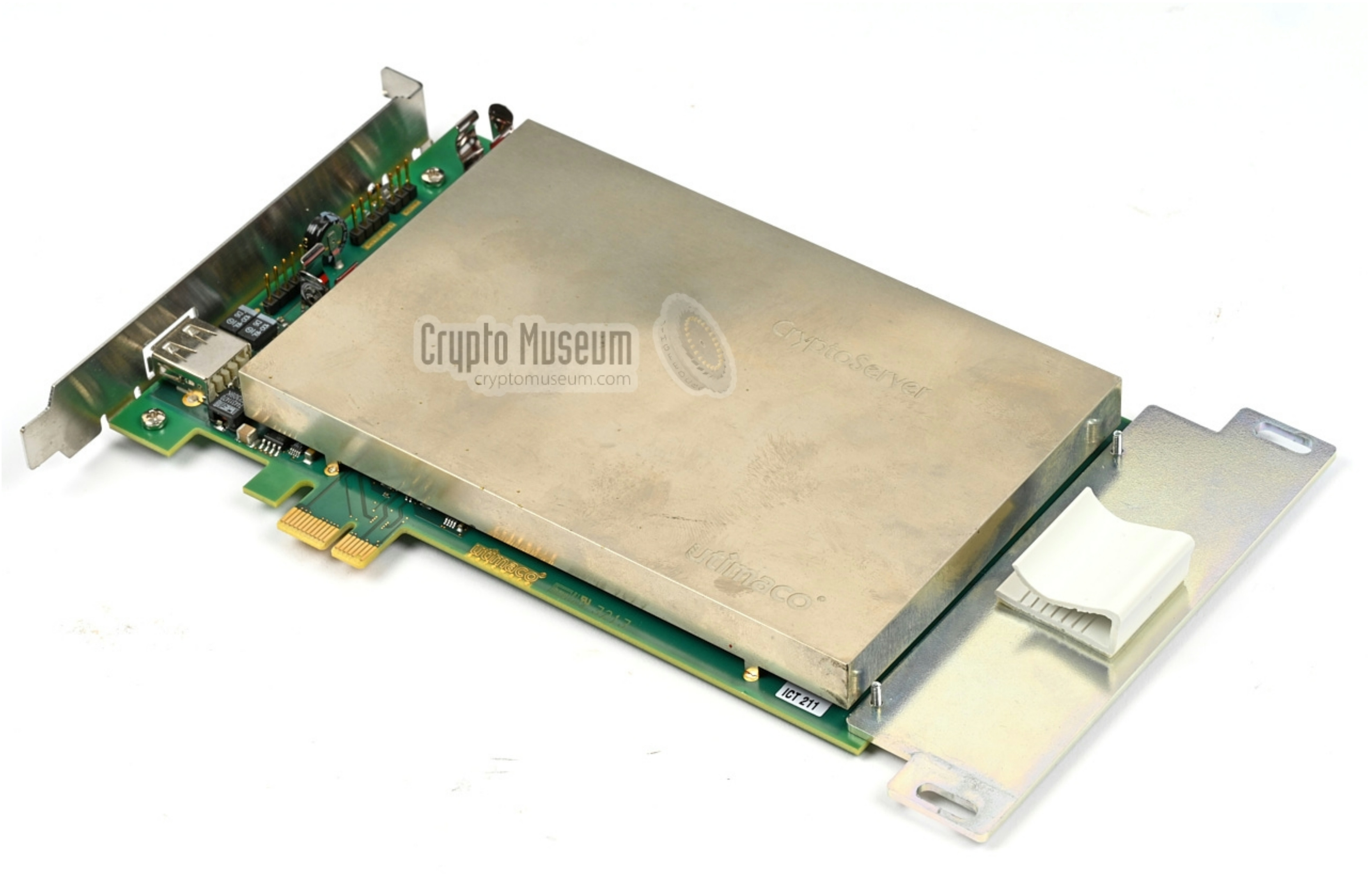
Hardware Security Module (HSM)


utimaco®
Keine Gewährleistung be gebrochenem Siegel!
Ein gebrochenes Siegel is ein Sicherheitsrisiko!
Bitte verständigen Sie de Sicherheitsoperator!
No warranty if seal is brok n!
A broken seal is a security risk!
Please contact the securit administrator!
Crypto Museum
cryptomuseum.com

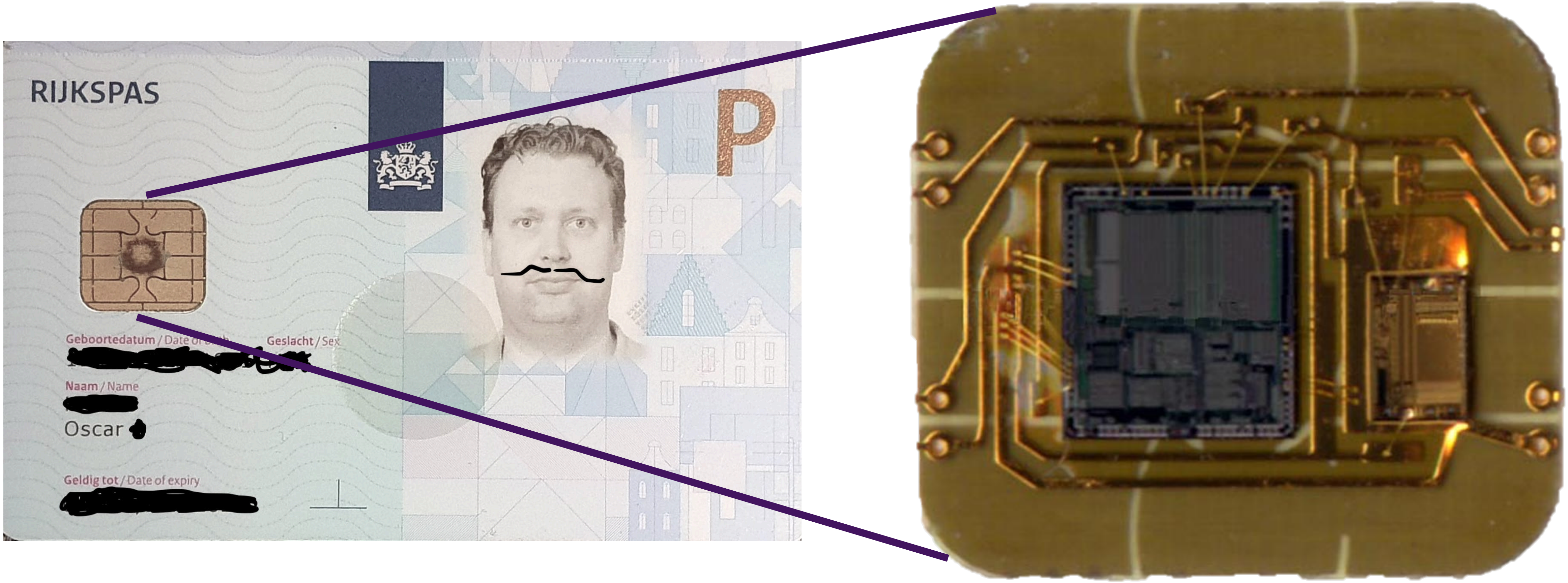
https://www.cryptomuseum.com/crypto/utimaco/cs_lan/


Lithium backup battery
Harddisc bay
FRONT
Twin Power Supply Unit (PSU)
Display electronics
REAR
19" rackmount enclosure
Backplane with PCIe slots
Expansion slots
Main Intel processor
Motherboard with VGA, 2 x Ethernet,
2 x USB and PS-2 interface
Hardware Security Module (HSM)
CryptoServer CSe

https://www.cryptomuseum.com/crypto/utimaco/cs_lan/



https://www.cryptomuseum.com/crypto/utimaco/cs_lan/



RIJKSPAS

P

Geboortedatum / Date of birth

[redacted]

Geslacht / Sex

Naam / Name

[redacted]

Oscar [redacted]

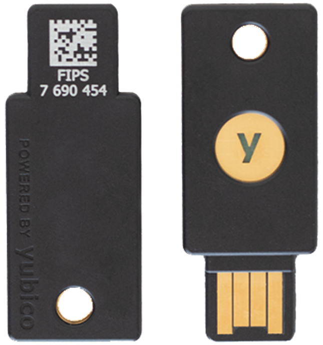
Geldig tot / Date of expiry

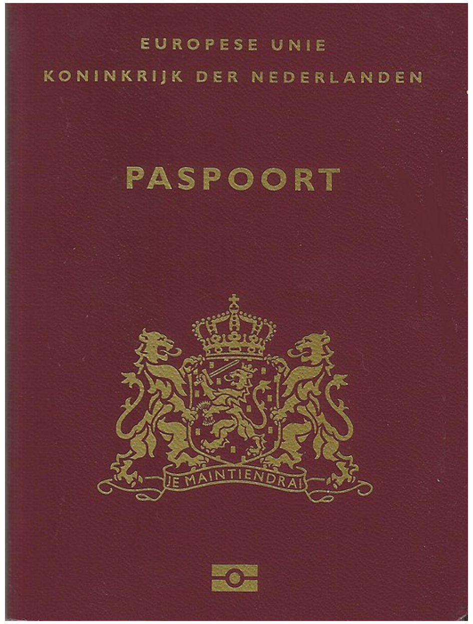
[redacted]

Nitrokey
FIDO2

yubico
yubico

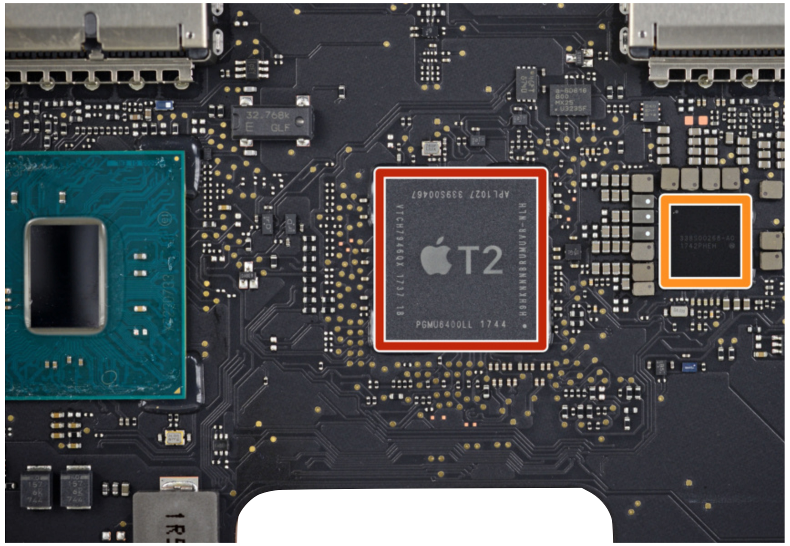
SECURE COMPUTING
SAFEWORD
RSA
SecurID
800 732
RSA
SecurID
00EE06
citibank
UOB
12541393
www.uobgroup.com
HSBC
411541
375 165


FIPS
7 690 454
POWERED BY yubico

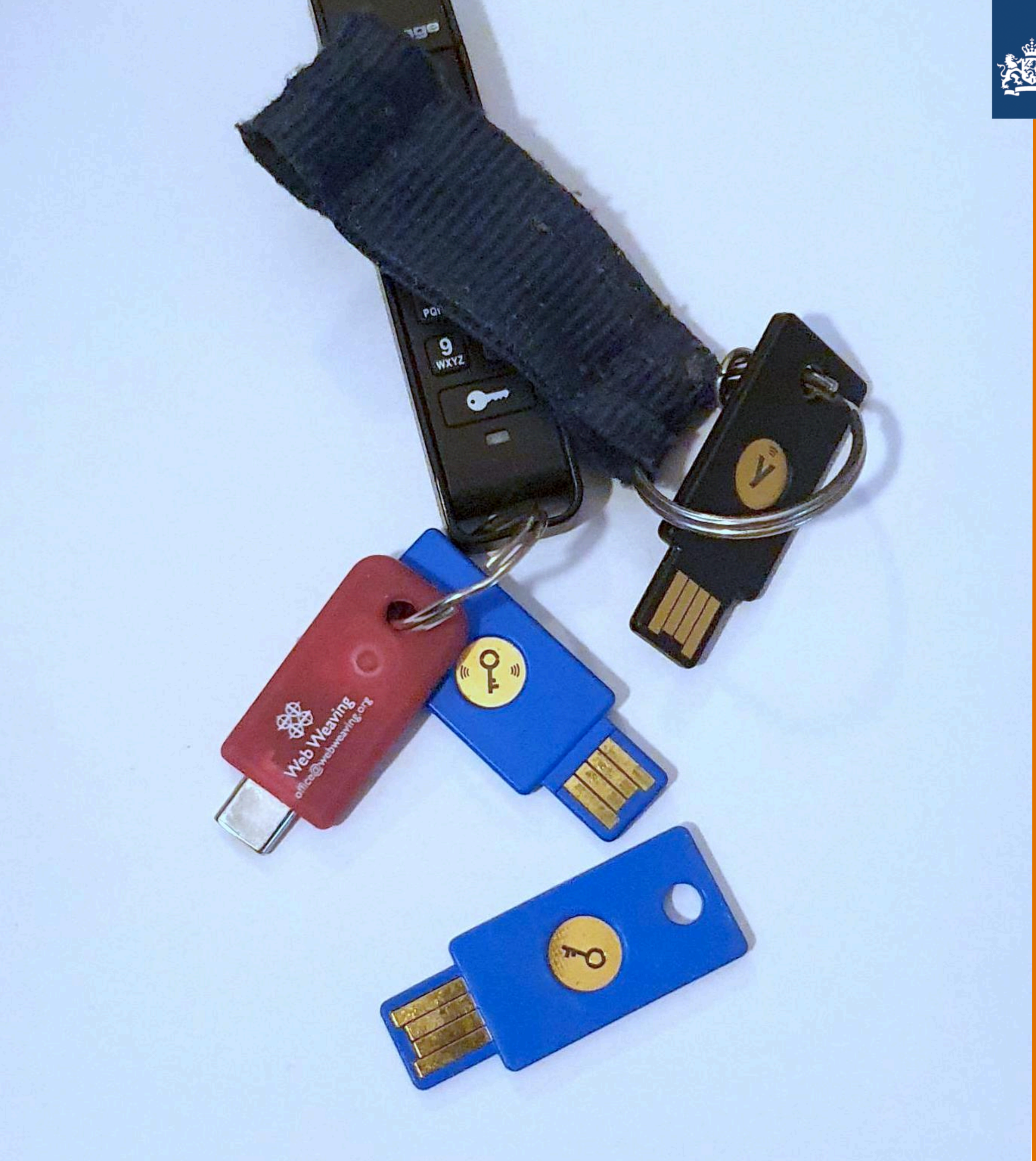

EUROPESE UNIE
KONINKRIJK DER NEDERLANDEN
PASPOORT
JE MAINTIENDRAI

SAMSUNG
KNOX
Draw your unlock pattern.
Forgot your KNOX unlock method?

INTEL® CORE™ i3
i3-8100
SR3N5 3.60GHZ
X819D174


T2

Infineon
TPM1.2
SLB 9635 TT 1.2



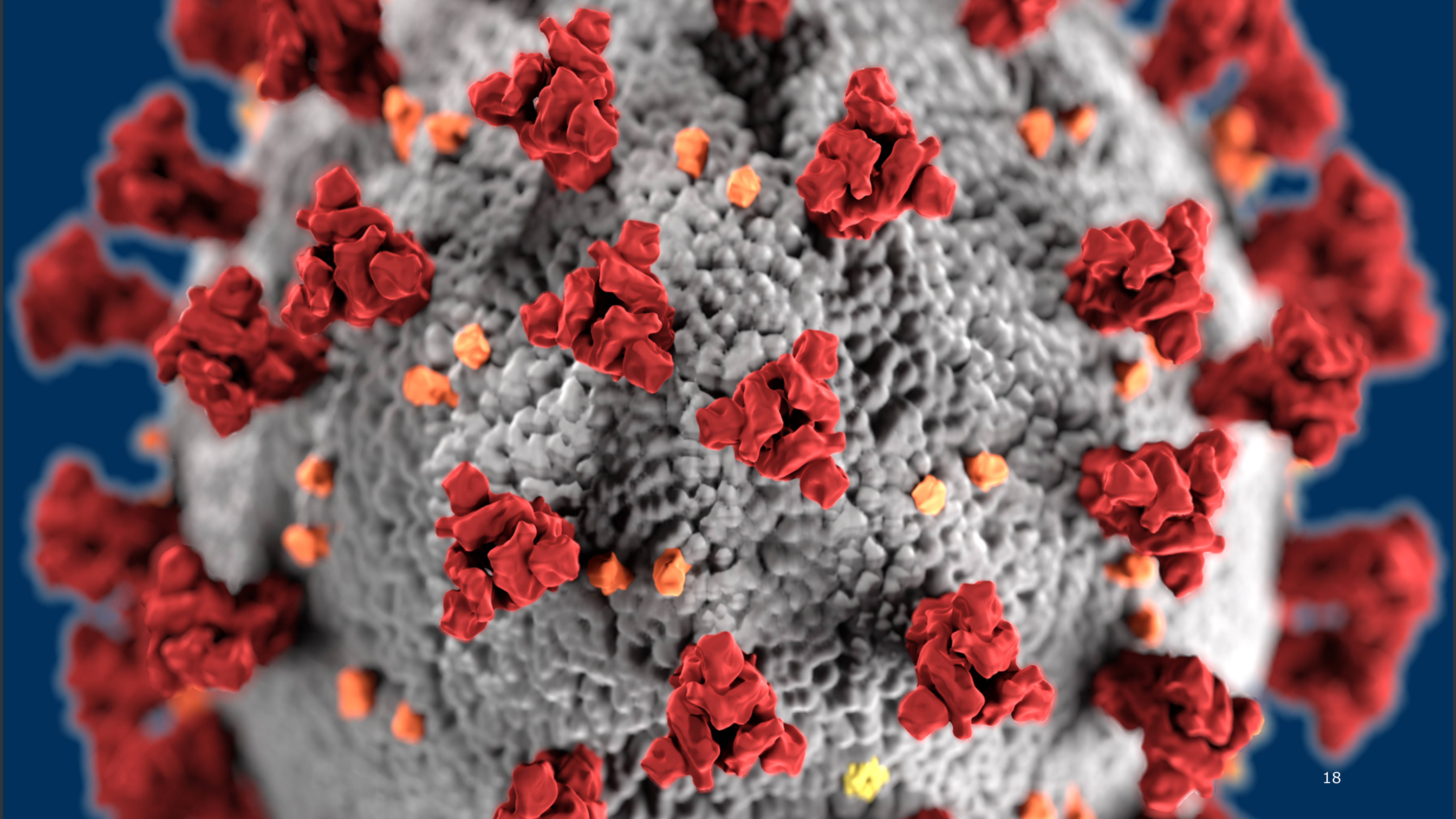
Key features of hardware security devices

1. Crypto engine on-chip, most run Java Card
2. Key operations run on-chip: Create, delete, roll-over
3. Data handling in-chip: decryption, signing
4. Interfaces: PKCS#11, KMIP, XKMS or higher protocols (WebAuthN)
5. Certifications: FIPS140-3 or Common Criteria

FIPS140-2/3 levels

- Level 1: basic security
- Level 2: show evidence of tampering
- Level 3: prevent the intruder from gaining access. Typically, adds support for multiple operational roles
- Level 4: Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected

Identity, authenticity and associated procedures combined provide a Level of Assurance



NOS
npo politiek
LIVE
Alleen samen krijgen we corona onder controle
rijksoverheid.nl/coronavirus
Afstand
Testen
Lucht

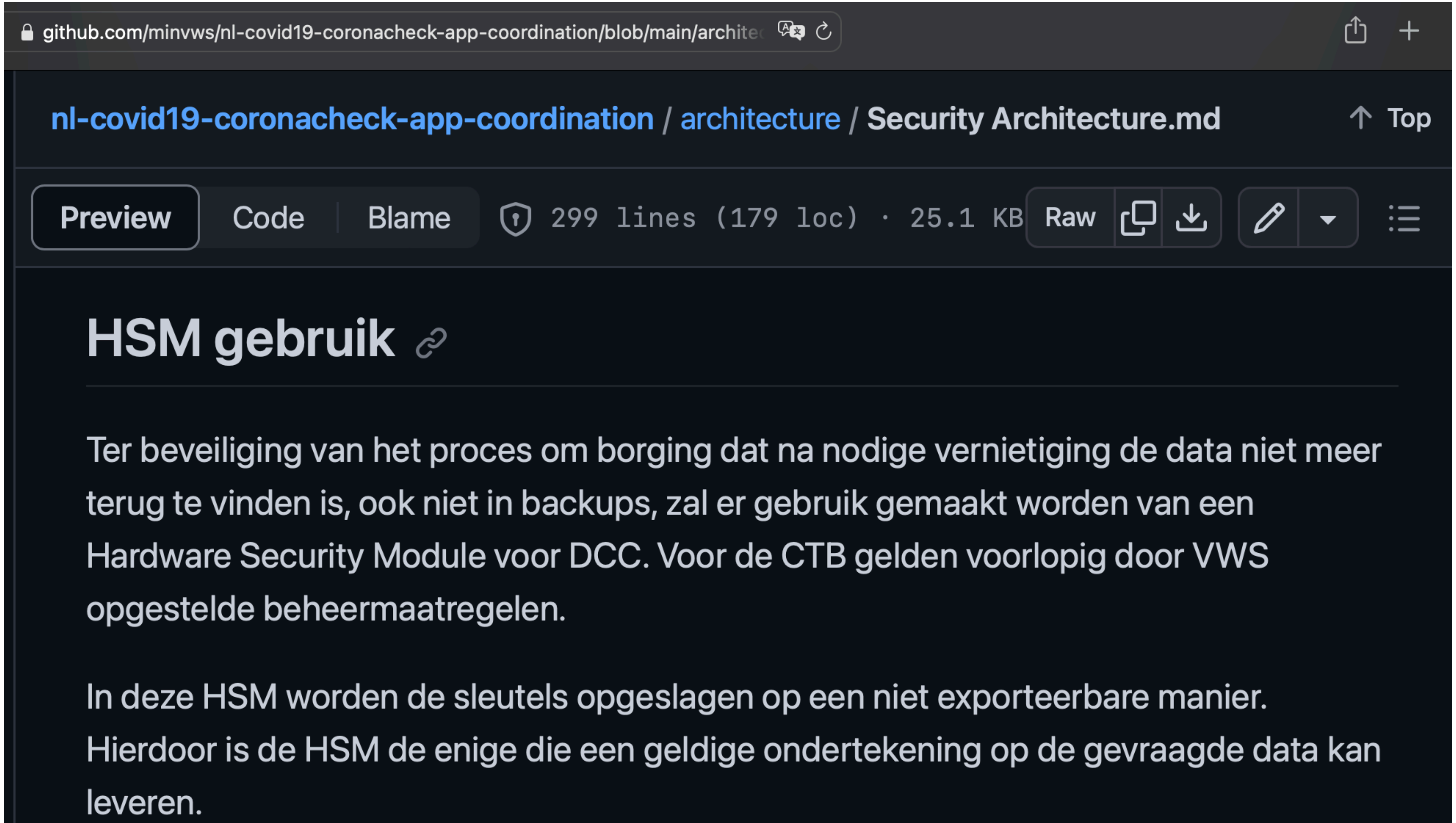
OMT: Create **two apps** for contact tracing

- Alert contacts whom you do not know and can’t remember
- Support contact tracing

CoronaMelder
Zo beschermen we elkaar

Ministerie van Volksgezondheid, Welzijn en Sport
CoronaCheck app
coronacheck.nl
CoronaCheck
Zo werkt het coronabewijs

Open source: architecture, (crypto) analysis and code, including where all keys are stored.



github.com/minvws/nl-covid19-coronacheck-app-coordination/blob/main/archite
nl-covid19-coronacheck-app-coordination / architecture / Security Architecture.md
Top
Preview
Code
Blame
299 lines (179 loc) · 25.1 KB
Raw

HSM gebruik

Ter beveiliging van het proces om borging dat na nodige vernietiging de data niet meer terug te vinden is, ook niet in backups, zal er gebruik gemaakt worden van een Hardware Security Module voor DCC. Voor de CTB gelden voorlopig door VWS opgestelde beheermaatregelen.

In deze HSM worden de sleutels opgeslagen op een niet exporteerbare manier. Hierdoor is de HSM de enige die een geldige ondertekening op de gevraagde data kan leveren.

Wikipedia:
Auguste Kerckhoffs

Perfect solution?

Oscar Koeroo
CISO Concern, Ministerie van Volksgezondheid Welzijn en Sport

Securing the largest infrastructures with little boxes. And we love it.