

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

Oscar Koeroo CISO Concern voor het Ministerie van Volksgezondheid, Welzijn en Sport







WannaCry's
EternalBlue
On Windows 10



killed, the anonymous of all the id to declare war on you terrorists.











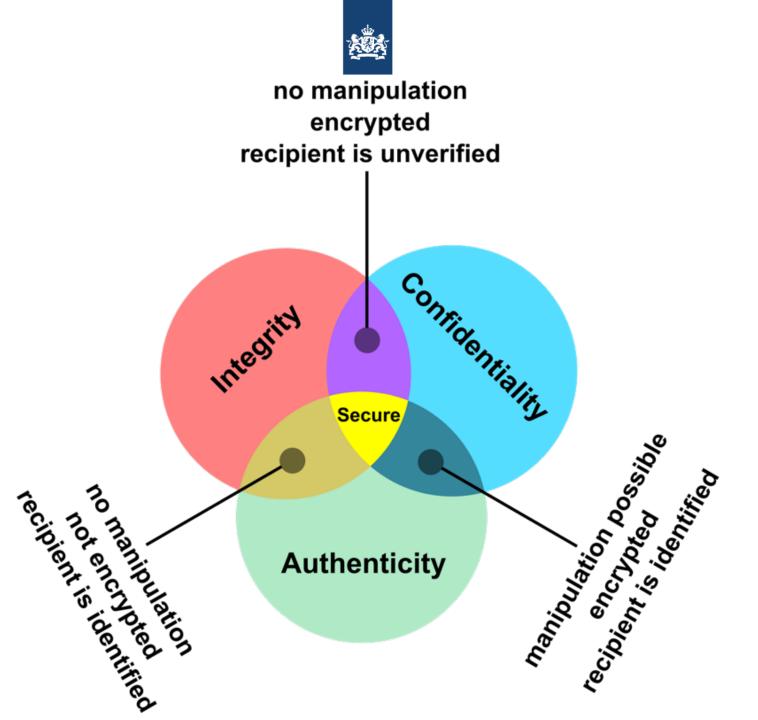


uuS::\$::\$::\$::\$::\$uu uu\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$ u\$ u\$ u\$ u222222222222222222222222 u\$\$\$\$\$\$ #\$\$\$# \*\$\$\$\$\$\$u \*\$\$\$\$# u\$u \$\$\$\$\* \$\$\$u u\$u u\$\$\$ u\$\$\$u usss \*\$\$\$\$uu\$\$\$ \$\$\$uu\$\$\$\$\* **+\$\$\$\$\$\$\$ +\$\$\$\$\$\$\$** usssssssusssssssu U\$#\$#\$#\$#\$#\$#\$U SSuS S S S SuSS uuu ussss u\$\$\$\$ uuuu\$\$\$\$\$\$\$\$\$ \$\$\$\$=##\$\$\$\$\$\$\$\$\$\$\$uuu uu\$\$\$\$\$\$\$\$=##\$\$\$# --\$\$\$\$\$\$\$\$\$\$\$\$uu --\$--uuuu \*=\$\$\$\$\$\$\$\$\$\$uuu u\$\$\$uuu\$\$\$\$\$\$\$\$\$uu \*\*\$\$\$\$\$\$\$\$\$uuu\$\$\$ \$\$\$\$\$\$\$\$\$\$\*\*\*\* \*\*\$\$\$\$\$\$\$\$\$\$\$ \*\$\$\$\$\$\* \*\*\$\$\$\$\*\* PRESS ANY KEY! \$\$\$\$\*



#### What makes a connection secure?







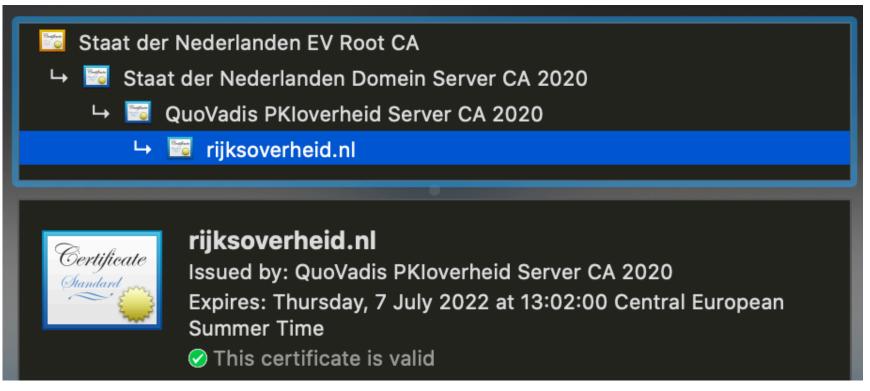
#### Certificate chain signing

Root CA signs Sub CA

Sub CA signs Sub CA

Sub CA signs EEC







#### 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)

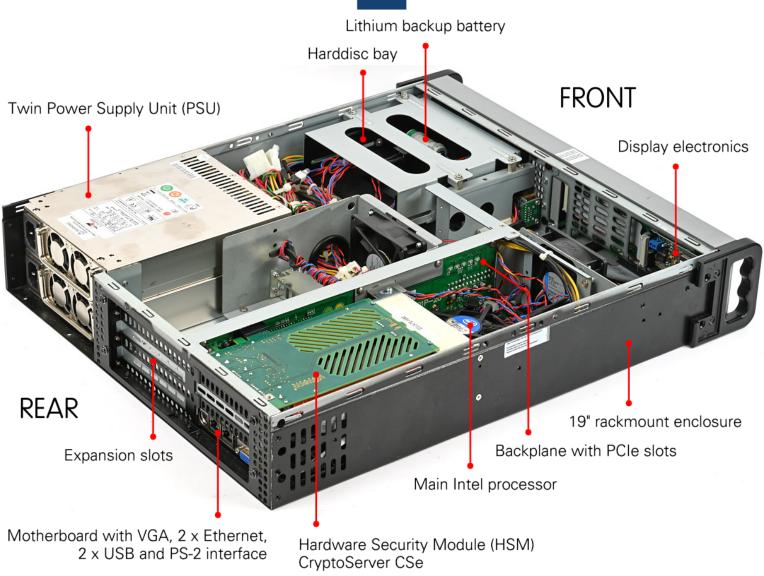






C





https://www.cryptomuseum.com/crypto/utimaco/cs\_lan/

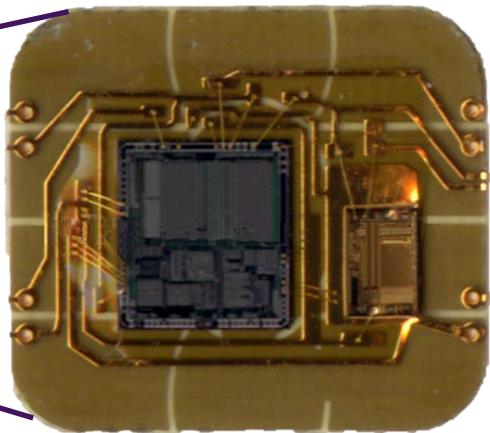




11

















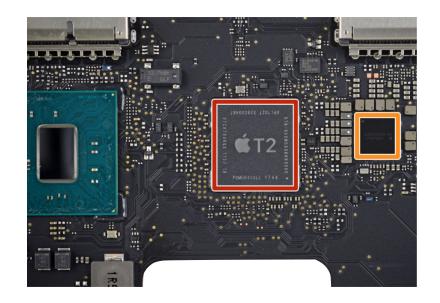
















# Key features of hardware security devices

- 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

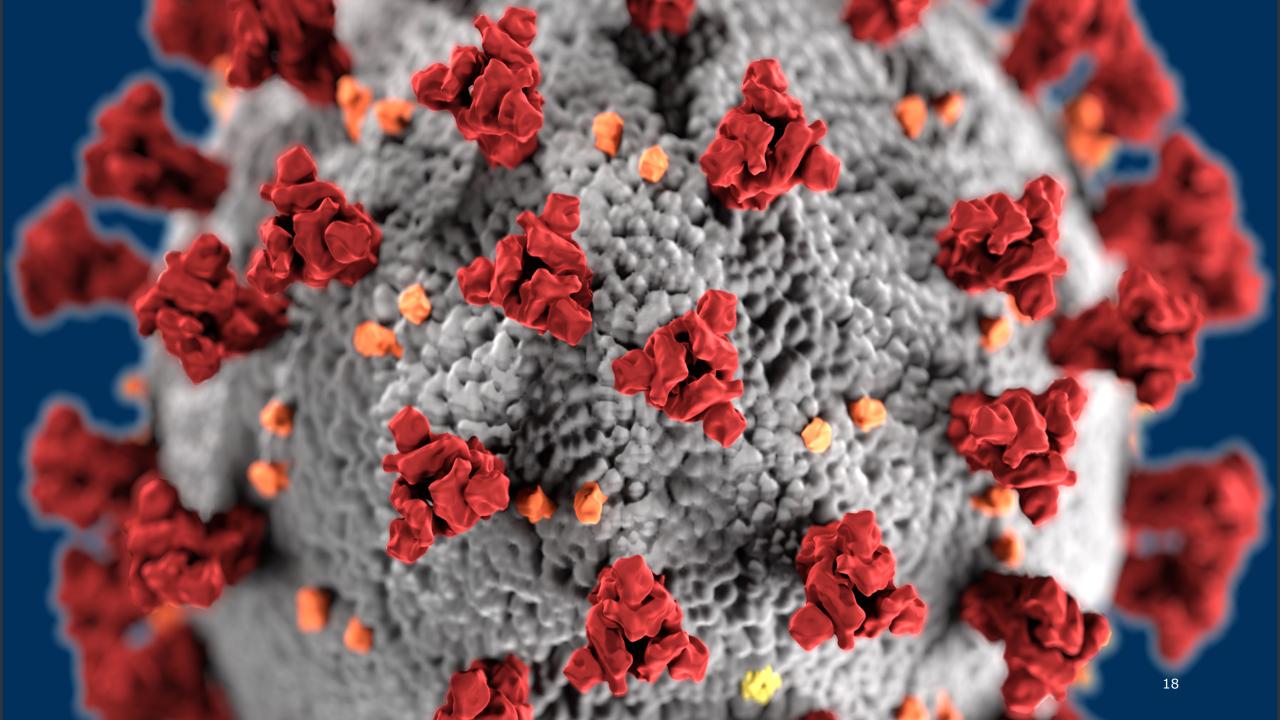




### Identity, authenticity and associated procedures combined provide a Level of Assurance









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

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







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





Wikipedia:
<a href="#">Auguste Kerckhoffs</a>







Oscar Koeroo CISO Concern, Ministerie van Volksgezondheid Welzijn en Sport

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