



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

HSM usage for RPKI at the RIPE NCC

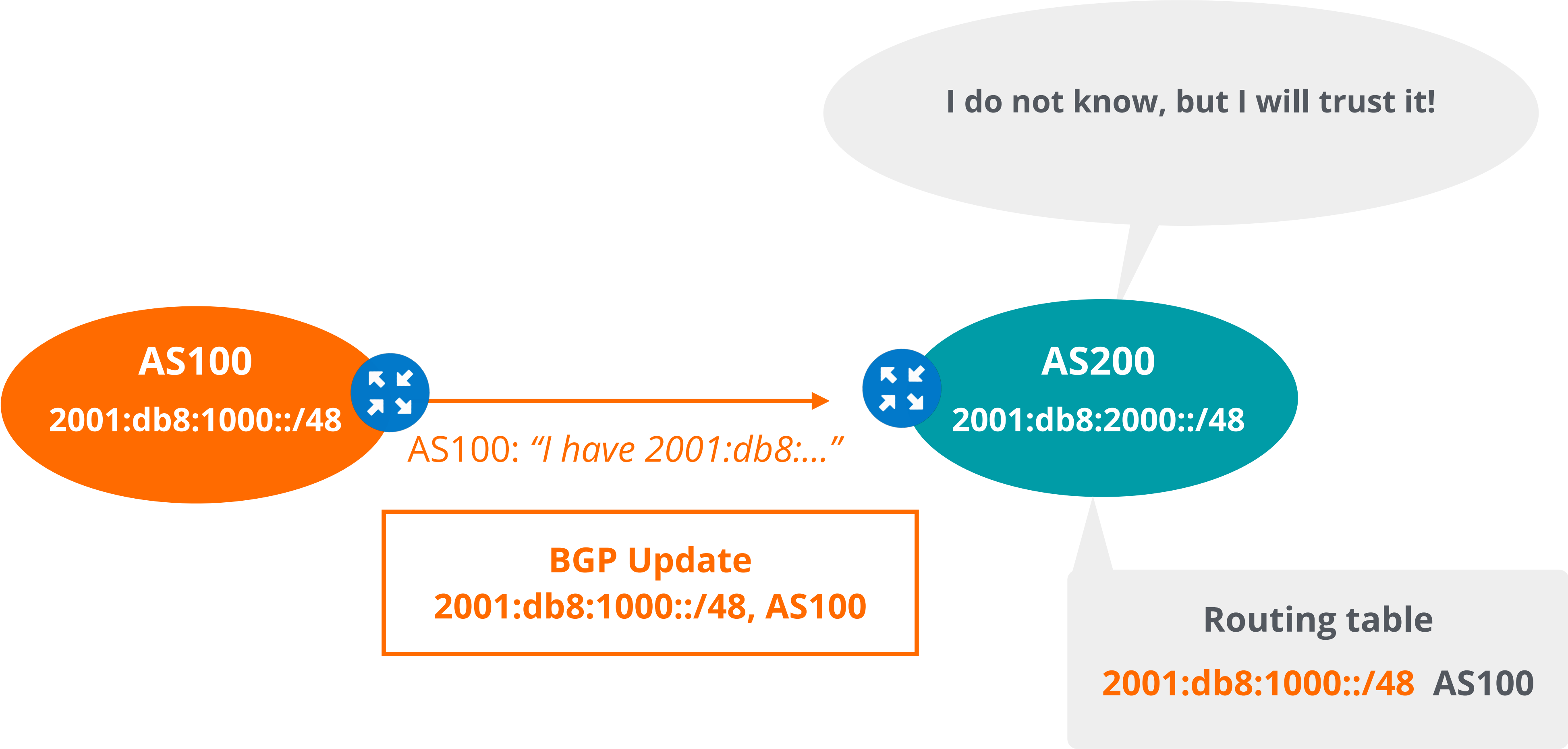
Ties de Kock | NLNOG Day 2024 | 21-10-2024

Outline



- Resource Public Key Infrastructure (RPKI)
- RPKI at the RIPE NCC
- HSMs in practice

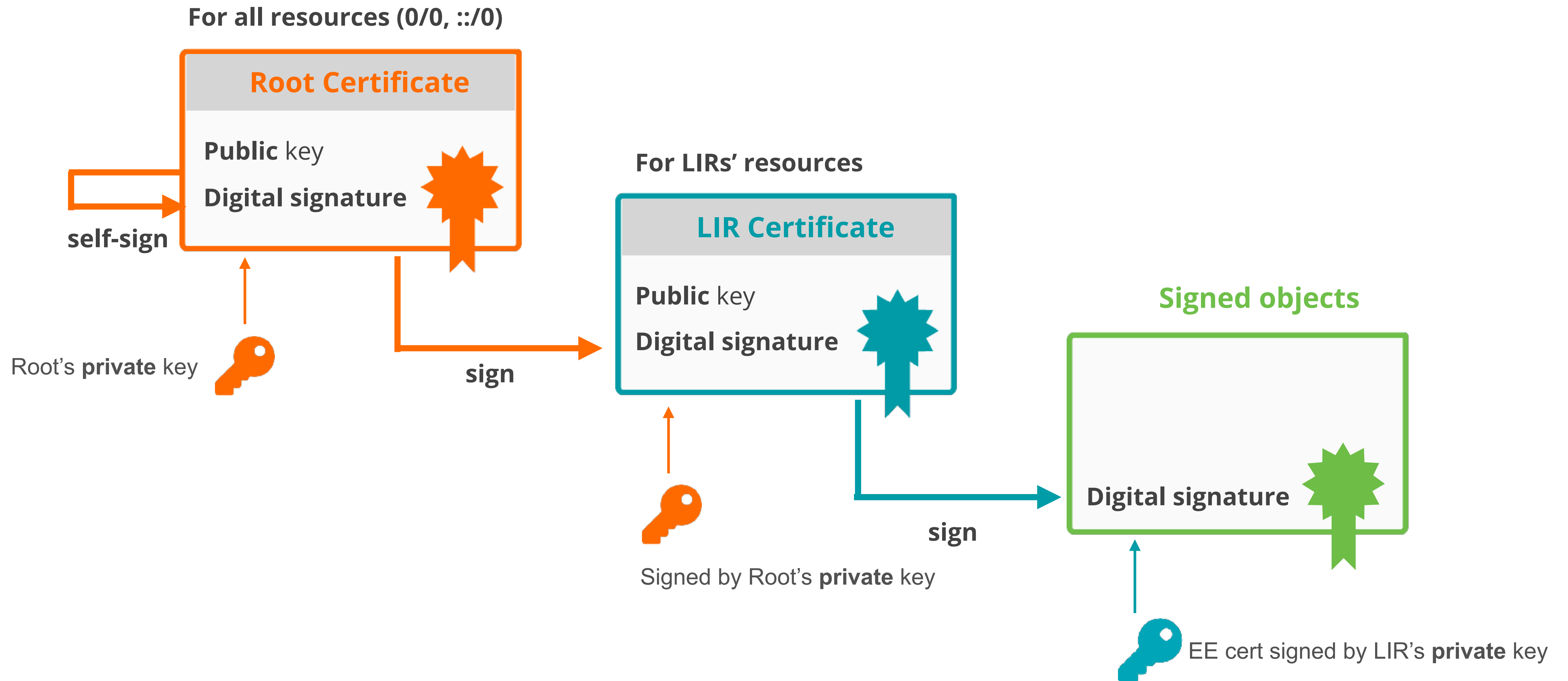
How does BGP work?





Not all BGP incidents are intentional!

RPKI Chain of Trust



Root Certificate

- RIRs have a **self-signed** root certificate for all resources (0/0 for IPv4, ::/0 for IPv6)
- This signs the resource certificates for all member allocations



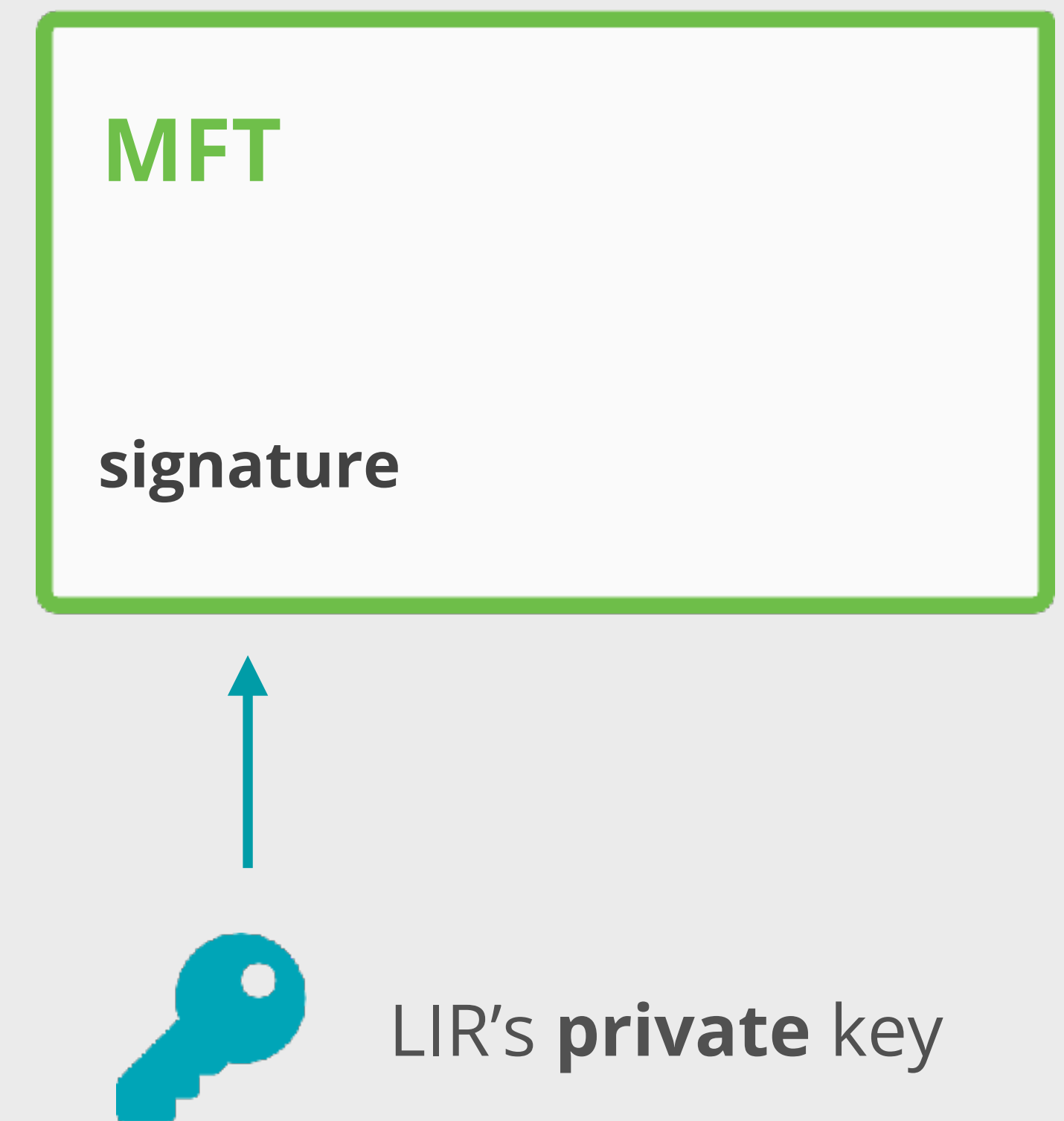
LIR Certificate

- Resource certificate for member allocations
- Signed by intermediate CA's private key
- Binds LIR's resources to LIR's public key
- Proves legitimate holdership for the LIR's resources



Manifests

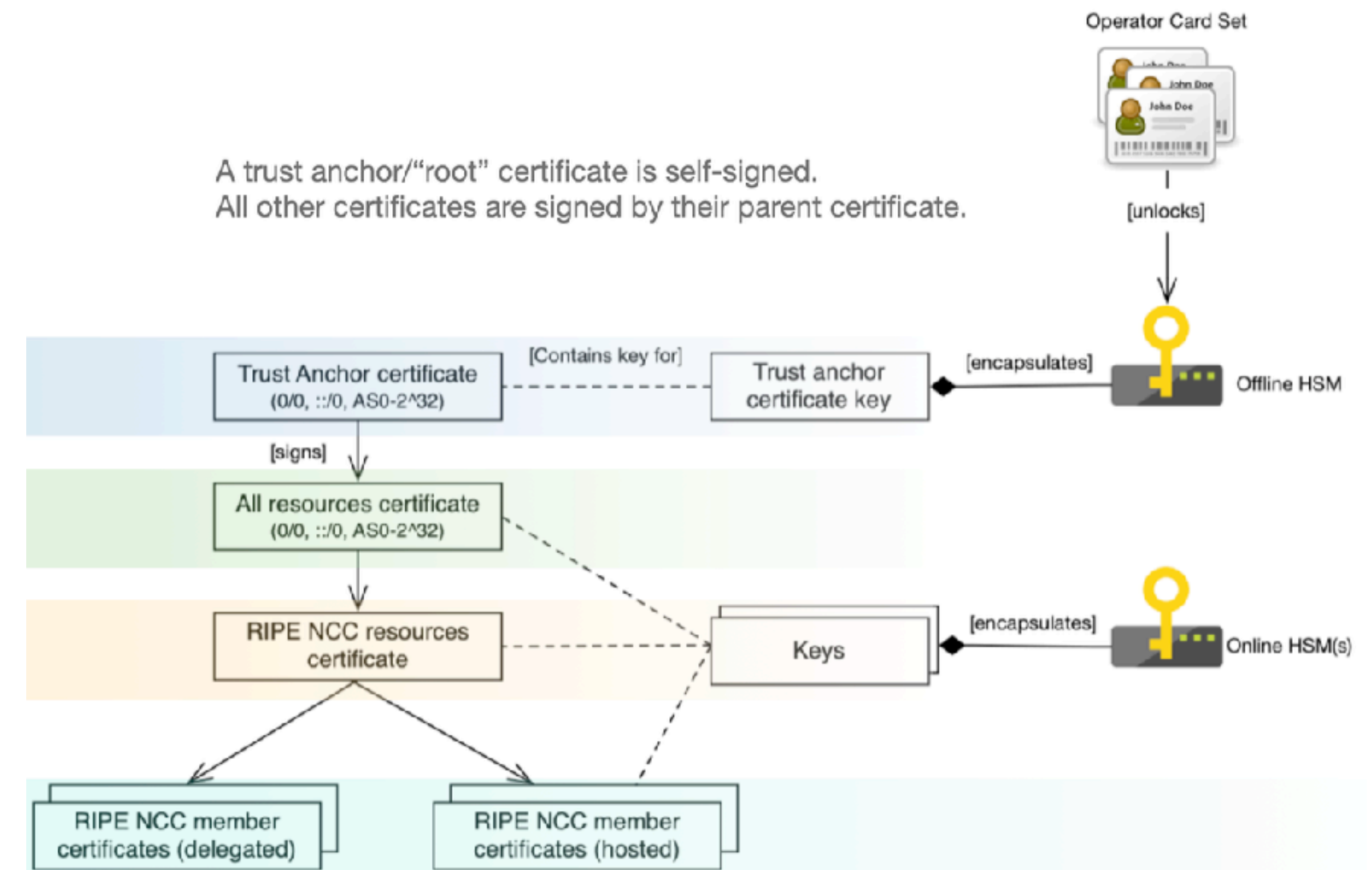
- Cryptographic Message Syntax (CMS) signed object
 - EE certificate signed by LIR's private key
- Contains
 - filename+hash all objects currently valid for CA
 - Validity period
- Enumerates objects:
 - CRL
 - sub-CA certificates
 - ROAs, ...



RPKI at the RIPE NCC: RPKI Team



- Develop RPKI CA software
- Maintain relevant infrastructure
- Operational
 - Operate offline CA
 - Operate online CA
 - Monitor the on-line CA
- Includes on-call shifts
- Includes operational responsibility for the HSMs

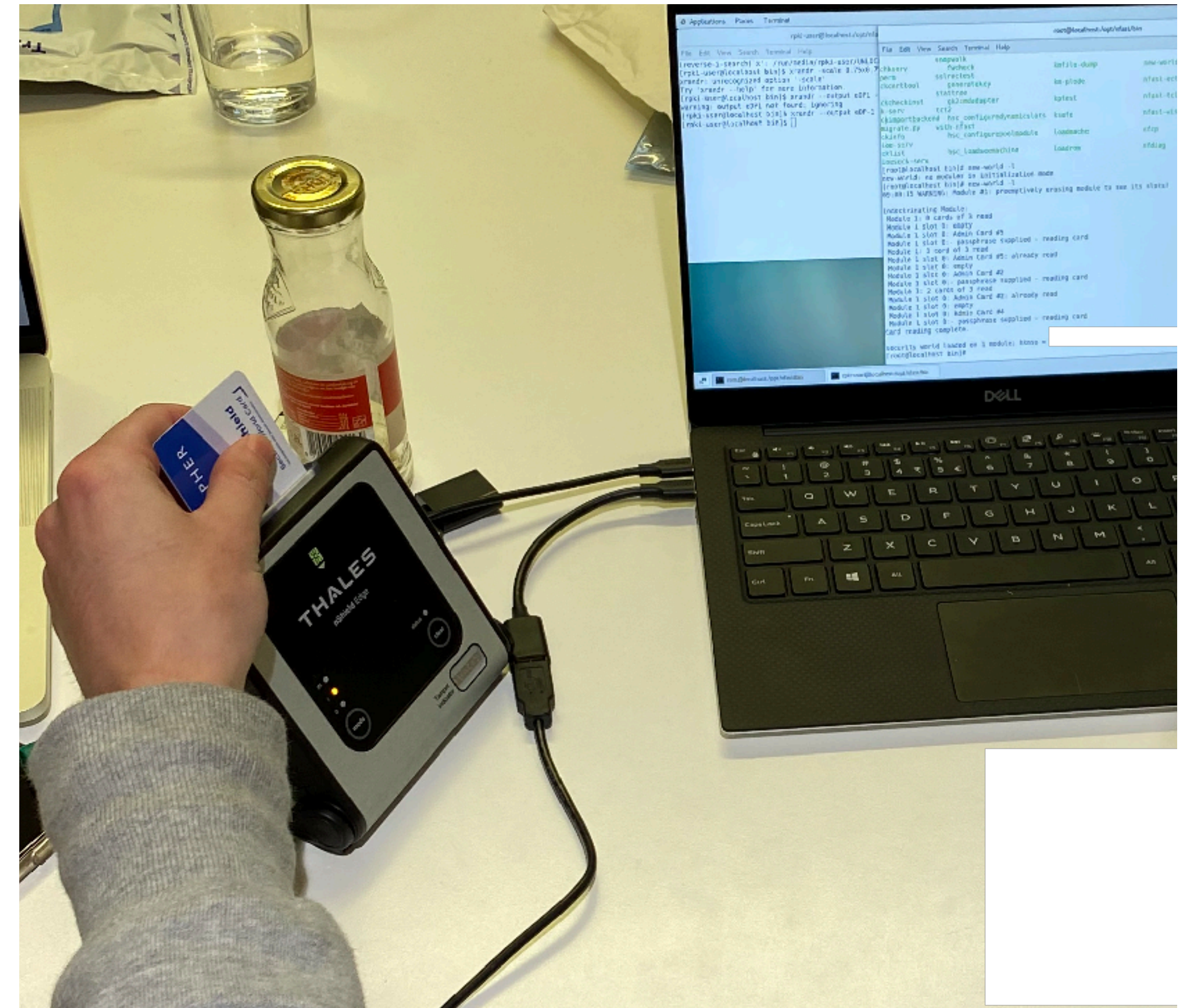


Off-line CA



- One CA key (Operator Card Set)
 - Hard to key-roll. Embedded in software
- High separation of roles
- Optimise for security
- Manifests and CRLs with 90d validity

CPS: <https://www.ripe.net/publications/docs/ripe-824/>



On-line CA(s)



- 20921 CAs
- 20660 manifests
- 20660 certificate revocation lists
- 40351 ROAs



On-line CA(s)



- 20921 CAs
- 20660 manifests
- 20660 certificate revocation lists
- 40351 ROAs
- HSM keys stored in database (module protected)
- Manifests and CRLs with 24hr validity

```
> rpki-client -t ~/ripe.tal -H rrdp.ripe.net -H rpki.ripe.net
Processing time 46 seconds (19 seconds user, 10 seconds system)
Skiplist entries: 0
Route Origin Authorizations: 40352 (0 failed parse, 0 invalid)
AS Provider Attestations: 0 (0 failed parse, 0 invalid)
BGPsec Router Certificates: 0
Certificates: 20921 (0 invalid)
Trust Anchor Locators: 1 (0 invalid)
Manifests: 20660 (0 failed parse)
Certificate revocation lists: 20660
Ghostbuster records: 0
Trust Anchor Keys: 0
Repositories: 2
New files moved into validated cache: 0
Cleanup: removed 0 files, 1 directories
Repository cleanup: kept 1 and removed 1 superfluous files
VRP Entries: 259168 (259168 unique)
VAP Entries: 0 (0 unique, 0 overflowed)
VSP Entries: 0 (0 unique)
~ 47s
>
~
>
```


On-line CA(s)



- Optimise for availability
- Redundant HSMs
- Two data-centres
- 16 hour window before objects expire.



On-line HSMs



- Legacy: PCIe HSM
- DB9-style connector for card reader



On-line HSMs (2018-2023)




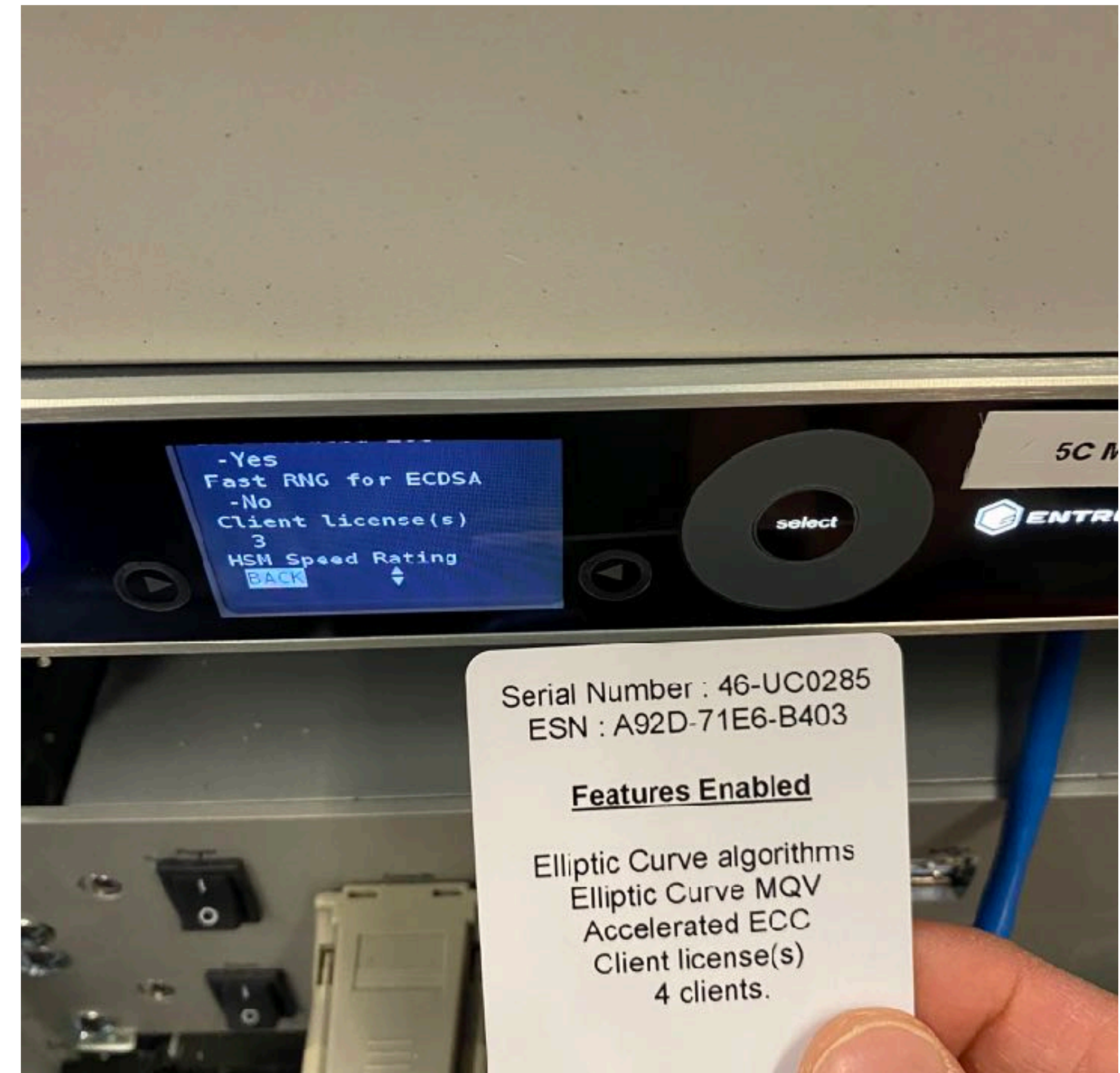
- nShield connect 6000+
- built-in card reader
- tamper detection
 - Except for fan or PSU replacement.
- openbsd based



On-line HSMs (2023-)



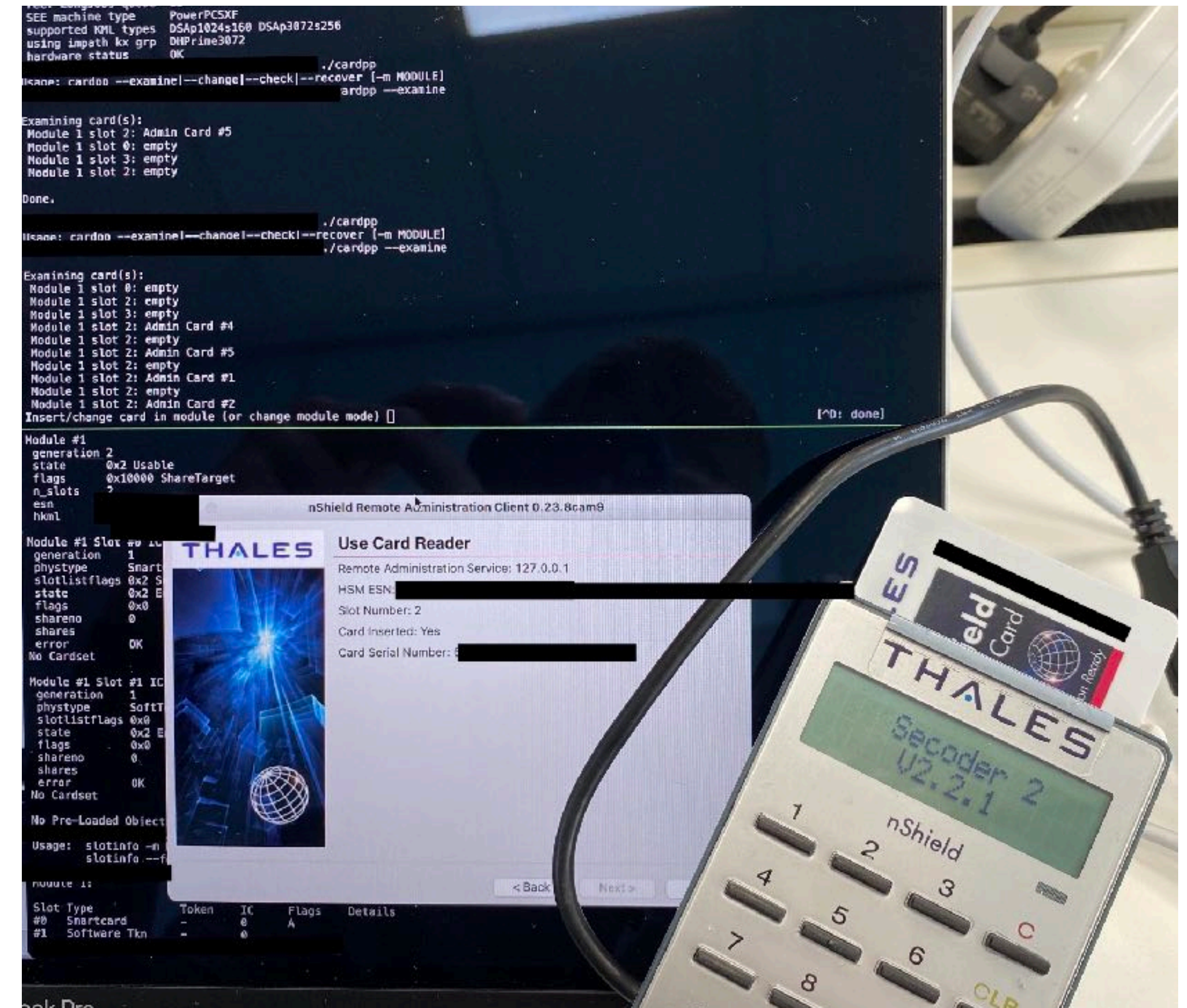
- nShield 5C
- linux + gresec patches
- Allegedly uses containerisation
- Fully remote manageable (serial)
- IPv6 only setup in production 
 - One bug: NTP over IPv6 did not work in earlier firmwares



Management of on-line HSMs



- On-line HSMs are in two DCs
- Each “hardserver” connects to both HSMs
- Networked HSMs can be mostly remote managed
 - Telnet serial console for initial settings,
 - Config from management machine (“RFS”) for further setup
 - 5C/2023 generation: IPv6 only



Management of on-line HSMs



- On-line HSMs are in two DCs
- Each “hardserver” connects to both HSMs
- Networked HSMs can be mostly remote managed
 - Telnet serial console for initial settings,
 - Config from management machine (“RFS”) for further setup
 - 5C/2023 generation: IPv6 only

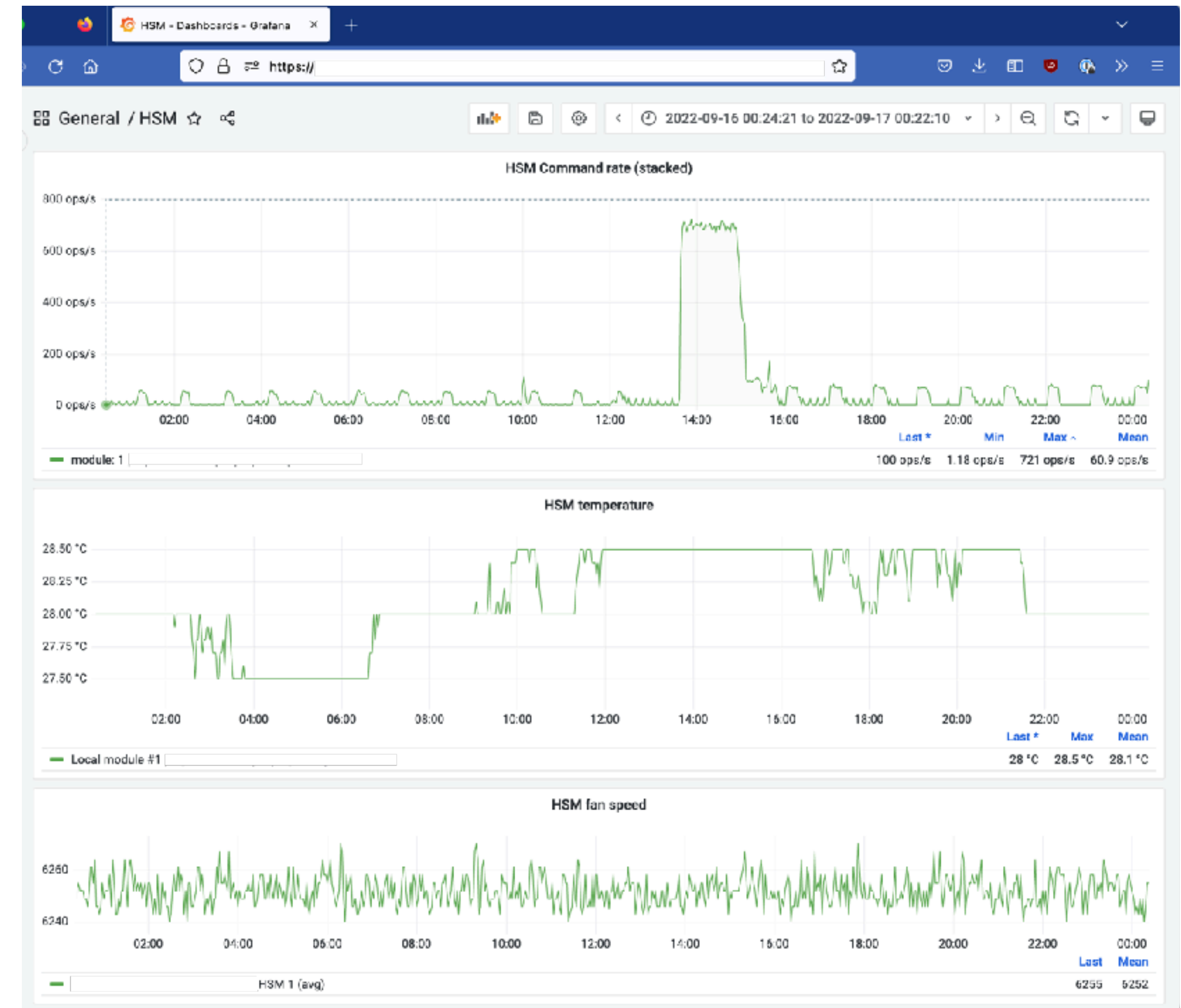
```
nethsm login: cli
Password:
Welcome to the nShield Connect Serial Console.  Type help or ? to list commands.

(cli)uptime
224 days, 0:03:06.460000
(cli)netcfg6
Ethernet 1 IPv6 address: Not Set
Ethernet 0 IPv6: 2001:67c:2e8:[redacted] 64 auto (1000BaseTX-FDX UP)
Ethernet 1 IPv6: :: 64 auto (0)
(cli)rfsaddr
RFS IP address: 2001:67c:2e8:[redacted] 9004
RFS authentication: Key hash=2ab1627d388d061ddf4fc3c4585eea794e2b3b56, Software key
RFS config push: AUTO
(cli)
(cli)
(cli)
(cli)
(cli)
```

Monitoring and alerting



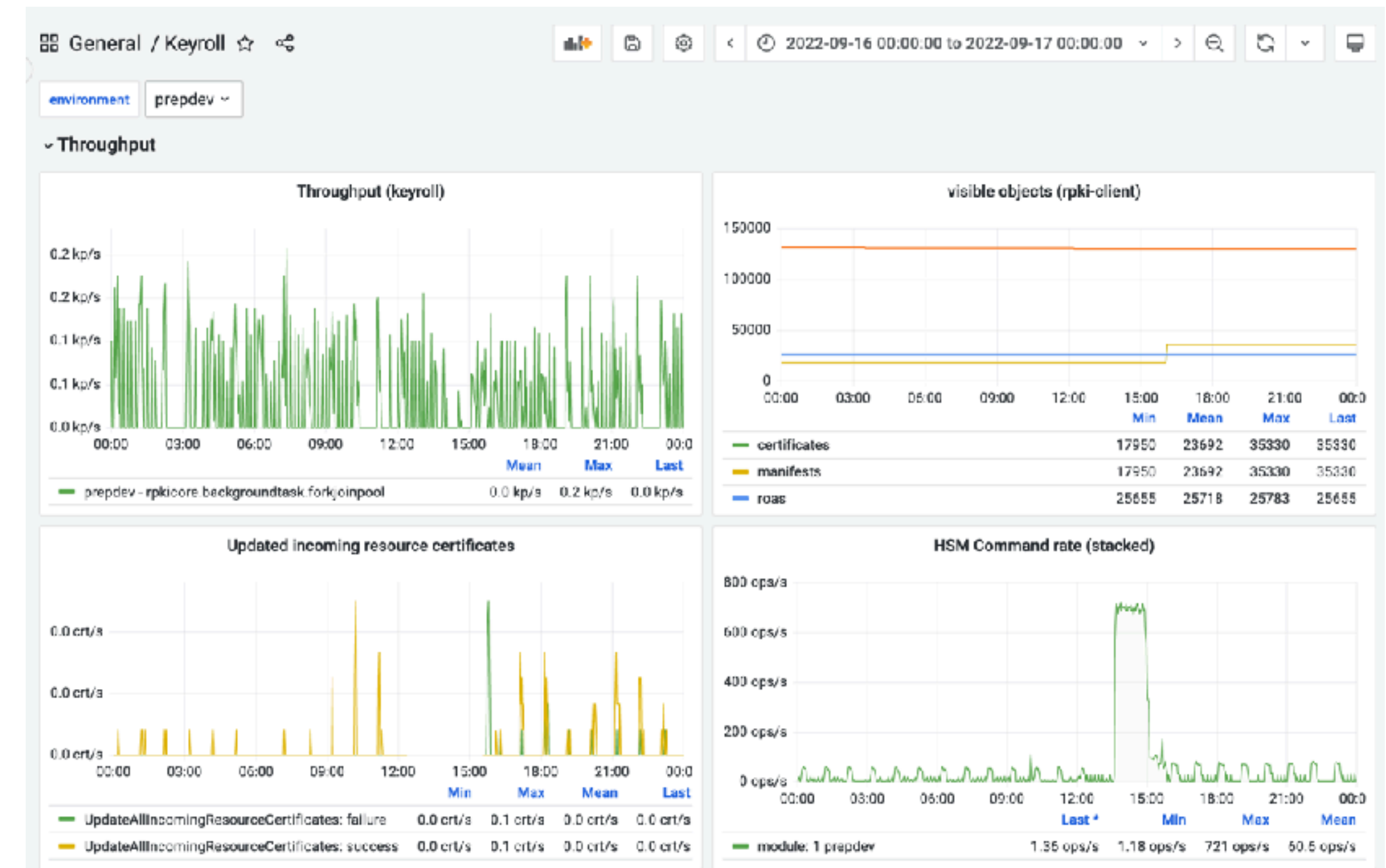
- Prometheus
 - snmp-exporter
- Alertmanager
- Grafana
- Application monitoring
- End-to-End tests



Monitoring and alerting



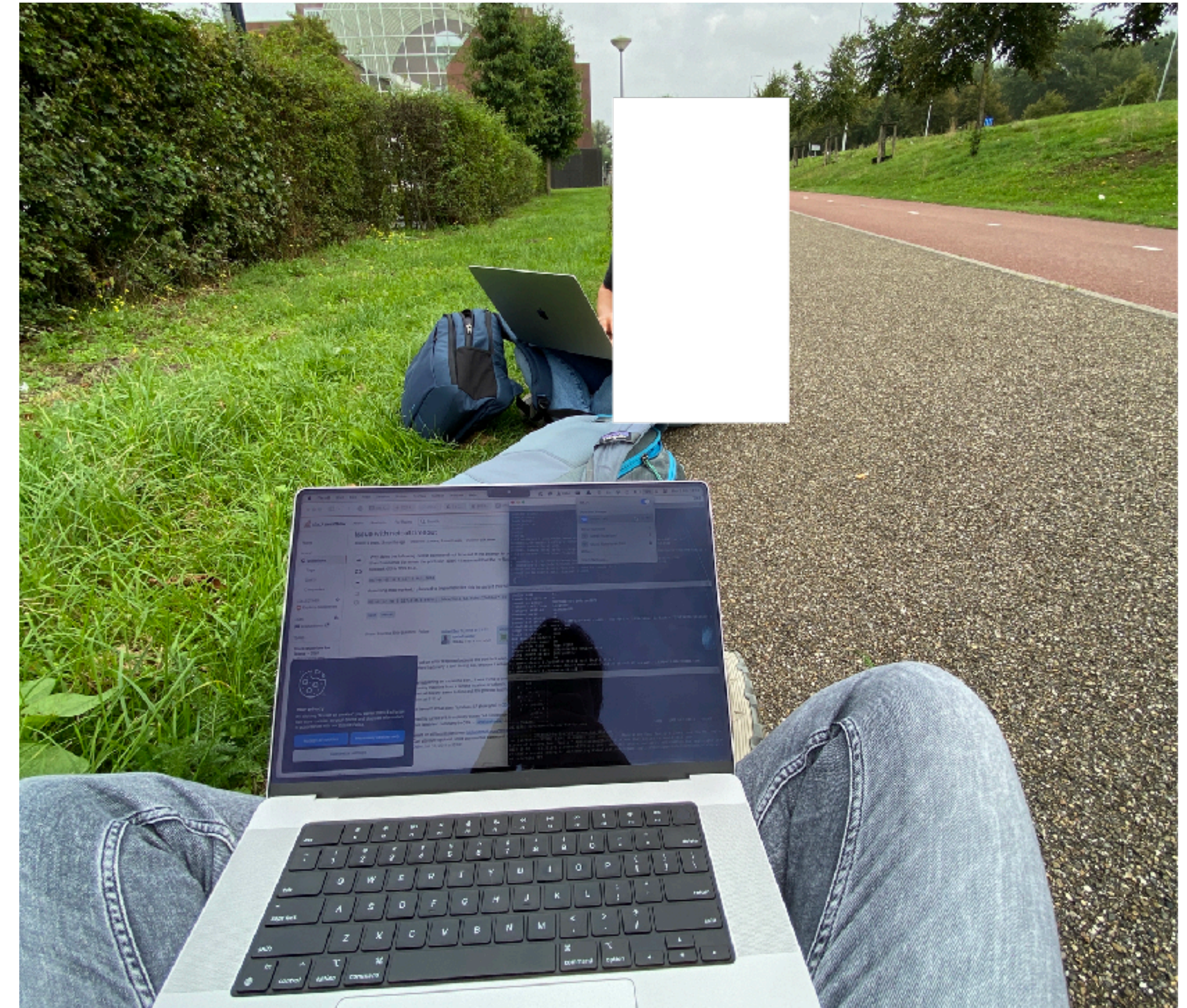
- Responsibilities shifted to DevOps team
- Strong focus on resiliency and availability
- Monitoring HSMs integrated with application monitoring



Monitoring and alerting



- HSMs are the team's pets
- The devices usually work very well
- Hardware fails
- Configurations fail, especially after changes





Questions



tdekock@ripe.net
@TiesDeKock



More information

- **Public article on HSM migration:**
 - <https://labs.ripe.net/author/ties/securing-the-ripe-ncc-trust-anchor/>
- **Webinars and training on (securing) internet routing and RPKI:**
 - <https://learning.ripe.net/>

Steps of signing process

