



RCauth Online CA service

Distributed operations and plans



eosc-hub.eu

Dissemination level: Public



[@EOSC_eu](https://twitter.com/EOSC_eu)



Reminder - for n00bs and people with dodgy memories

- RCauth is an IGTF accredited IOTA (DOGWOOD class) CA
 - Online credential conversion
 - Connected to eduGAIN (R&S+Sirtfi) plus direct e.g. EGI Check-in
- EOSC Hub is implementing a High Availability setup across three sites
- Private key is to be cloned and hosted in HSMs at each site
- Cloning is done by XORing key with random strings
- OTP randomness exchanged using different means (usually in-person)
- => key is 3-of-3 encrypted
 - Any part, or any two of the three, will have *no information* about the key

- Overview of where we are
 - Operational status
- Review of tasks
 - Key cloning
 - Deployment
 - Database (and network)
 - Documentation
- Site specific reports
- Q&A

Overview of where we are

- Power outage incident
- Activity overview

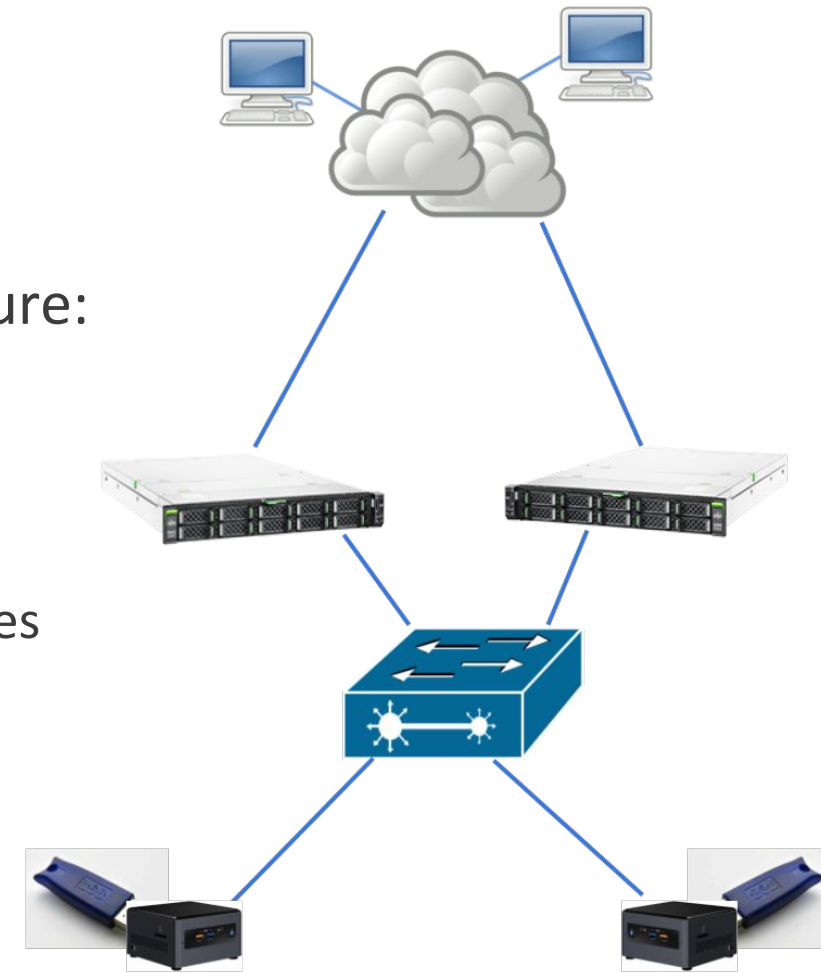
Power outage at Nikhef 14 August 2020

- Hardware issue with Nikhef UPS (=1st level emergency power)
- Powergrid at the time unstable: using generator during repairs
- During repair of UPS, generator failed (underlying cause is now fixed)
- Result:
 - entire non-commercial part of data center went down
 - multiple hardware components failing, probably due to resulting surge
- Effects on RCauth specifically
 - backend CA (Intel NUC with eToken) broken
 - emergency temporary workaround in place within +/- 2 hours
 - network very shaky till Monday morning
 - overall user impact: probably very few users impacted & on Monday morning only

- Longer term response:

Create local HA setup to ease recovery from hardware failure:

- duplicate backend nodes (i.e. 2 NUCs)
 - duplicate frontend nodes (i.e. 2 Delegation Servers)
 - all 4 on private LAN
 - automatic failover in case of failure of one of the backend nodes
 - 2nd frontend node probably hot spare for now
- Could add both Delegation Servers to the European-wide HA setup



- Use the opportunity to implement further improvements:
 - Add feature to revoke certificates from one of the frontends:
Operator no longer needs to be physically present
 - Remote syslog of backend servers:
easier to debug hardware issues

- **Operational tooling** (Task 5.1.7)
 - Operator comms (205, 206)
 - Self audit (207)
- **High Availability setup** (Task 5.1.8) - run across NIKHEF, GRNET, STFC
 - Key cloning (201)
 - Deployment (202)
 - Database (203)
 - HA testing (204)
- **Operations** (WP13)
 - Service integration (208)
 - End user docs (209)
 - Monitoring docs (210)
 - Final PMA review (211)

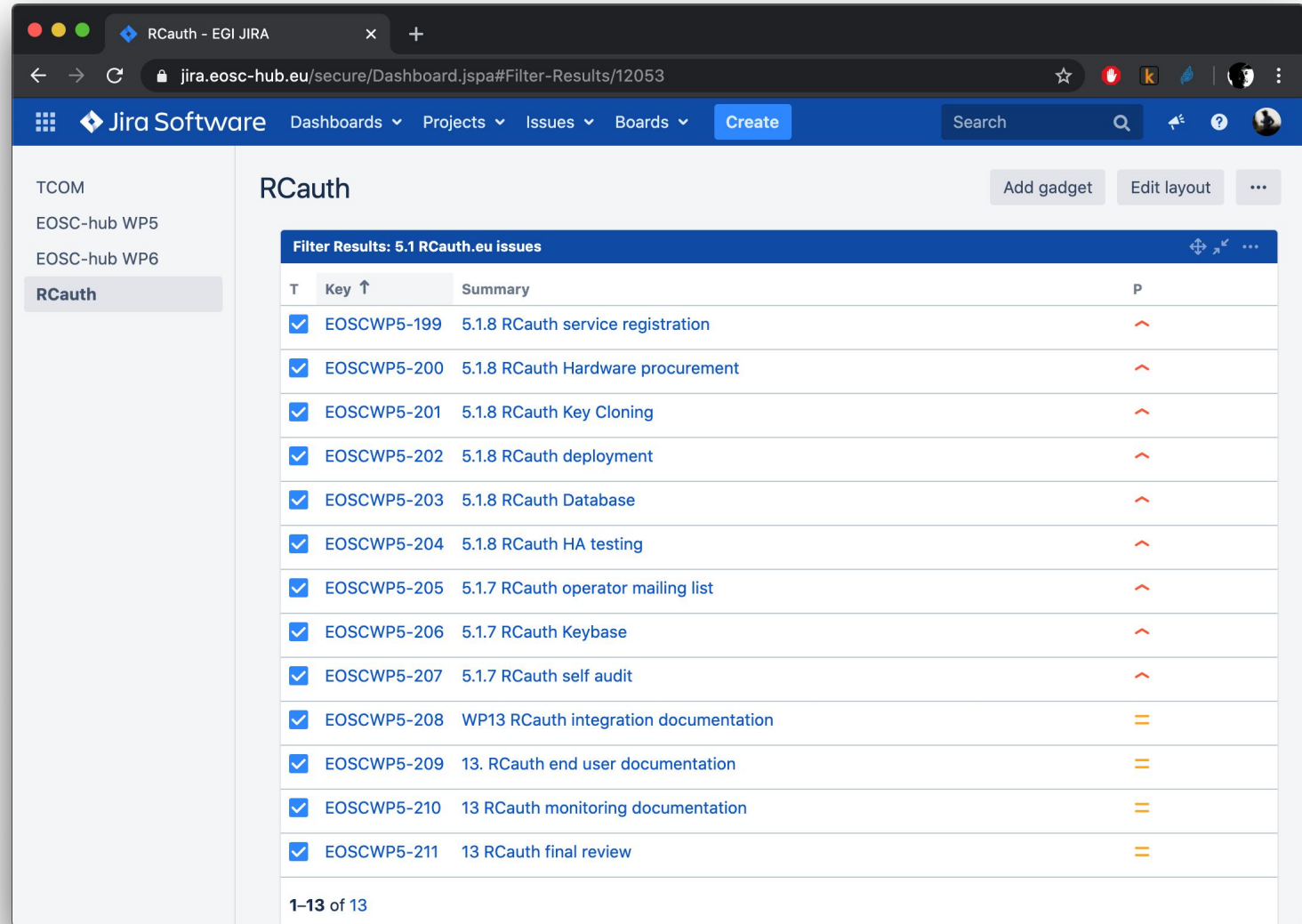
Project view

WP5 = Federation & Collaboration
Services: Integration & Maintenance

T5.1 = Identification, Authentication,
Authorisation, Attr Mgmt.

WP13 = Access Provisioning

- JIRA dashboard
- Regular biweekly ops calls for reviewing/planning



The screenshot shows a JIRA dashboard for the 'RCauth' project. The dashboard is titled 'RCauth' and displays a list of 13 issues. The issues are filtered to show 5.1 RCauth.eu issues. The issues are listed in a table with columns for 'Key', 'Summary', and 'P' (Priority). The issues are:

| T | Key ↑ | Summary | P |
|-------------------------------------|-------------|---------------------------------------|---|
| <input checked="" type="checkbox"/> | EOSCWP5-199 | 5.1.8 RCauth service registration | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-200 | 5.1.8 RCauth Hardware procurement | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-201 | 5.1.8 RCauth Key Cloning | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-202 | 5.1.8 RCauth deployment | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-203 | 5.1.8 RCauth Database | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-204 | 5.1.8 RCauth HA testing | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-205 | 5.1.7 RCauth operator mailing list | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-206 | 5.1.7 RCauth Keybase | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-207 | 5.1.7 RCauth self audit | ↑ |
| <input checked="" type="checkbox"/> | EOSCWP5-208 | WP13 RCauth integration documentation | = |
| <input checked="" type="checkbox"/> | EOSCWP5-209 | 13. RCauth end user documentation | = |
| <input checked="" type="checkbox"/> | EOSCWP5-210 | 13 RCauth monitoring documentation | = |
| <input checked="" type="checkbox"/> | EOSCWP5-211 | 13 RCauth final review | = |

1-13 of 13

Review of tasks: Key cloning (task 201) - 1/4

Cloning steps 1/2

Note: This task is the one most affected by the current lockdown

- Agree plan with PMA [STFC, NIKHEF, GRNET] - **DONE**
- Develop software [STFC, NIKHEF] - **DONE**
- Generate secret A [STFC] - **DONE**
- Exchange A with NIKHEF [STFC] - **DONE**
- Share recipe for generating random numbers in HSM with GRNET [NIKHEF, STFC] - **DONE**
- Generate secret B [GRNET] - **DONE**
- Select additional methods for sharing keys - courier/snailmail, keybase or PGP email - **DONE**
- Exchange B with NIKHEF [GRNET] - **TODO**

...

Review of tasks: Key cloning (task 201) - 2/4

Cloning steps 2/2

- ...
- Generate C1 [NIKHEF]
- Exchange C1 with STFC [NIKHEF]
- Generate C2 [NIKHEF]
- Exchange C2 with GRNET [NIKHEF]
- Calculate $S1 = S+A+C1$ [NIKHEF]
- Exchange S1 with STFC [NIKHEF]
- Calculate $S2 = S+B+C2$ [NIKHEF]
- Exchange S2 with GRNET [NIKHEF]
- Calculate S from S1 [STFC]
- Install S in HSM [STFC]
- Calculate S from S2 [GRNET]
- Install S in HSM [GRNET]

DONE (DRY RUN)

*Should be done **without** writing the key to disk*

Review of tasks: Key cloning (task 201) - 3/4

Methods used for random data exchange

- In person exchange of random data (pre-lockdown)
 - Written to portable and destructible media (CD, paper)
 - Paper is only machine readable with OCR...
- Sending random data via courier
 - Destination depends on people getting back to the office
- Keybase (self-destructing) exchange of dry run random data
- PGP-encrypted mail
 - So far only used for dry run
 - Will use also for final secret

Review of tasks: Key cloning (task 201) - 4/4

Lessons learnt

- Fixed a few bugs in the encoding/decoding scripts
- Hand-written secrets can be difficult
- Exchanging self-destructing messages over keybase
- Need python to de-/reconstruct keys in a portable way
- Python scripts written to support multiple versions:
 - Useful as they'd work with the system's default
 - Means many features from python could not be used

Review of tasks: Deployment (task 202)

1. Package/containerise software [NIKHEF] - **DONE**
2. Generate deployment recipe (ansible) [NIKHEF] - **DONE**
3. Set up infrastructure [STFC] - **DONE**
4. Set up infrastructure [GRNET] - **DONE**
5. Deploy delegation server [STFC]- **IN PROGRESS**
6. Deploy delegation server [GRNET] - **IN PROGRESS**
7. Access keybase git and deploy MyProxy/signing on infrastructure [STFC] - **IN PROGRESS**
8. Access keybase git and deploy MyProxy/signing on infrastructure [GRNET] - **DONE**

Note: steps 7 and 8 will likely require software adaptation

Review of tasks: Database (task 203)

1. Generate OpenVPN recipe [STFC, NIKHEF, GRNET] - **DONE**
2. Set up VPN endpoint [STFC] - **DONE**
3. Set up VPN endpoint[GRNET] - **DONE**
4. Set up VPN endpoint [NIKHEF] - **DONE**
5. VPN functional tests [all] - **IN PROGRESS**
6. VPN performance tests [all] - **IN PROGRESS**
7. VPN monitoring [all]
8. Database deployment recipe [NIKHEF] - **IN PROGRESS**
9. Database synchronisation configuration [NIKHEF]
10. Deploy database [STFC] - **DONE**
11. Deploy database [GRNET] - **IN PROGRESS**
12. Database monitoring [STFC]
13. Database monitoring [GRNET]
14. Set up synchronisation [STFC] - **DONE**
15. Set up synchronisation [GRNET] - **DONE**
16. Database synchronisation testing [NIKHEF]

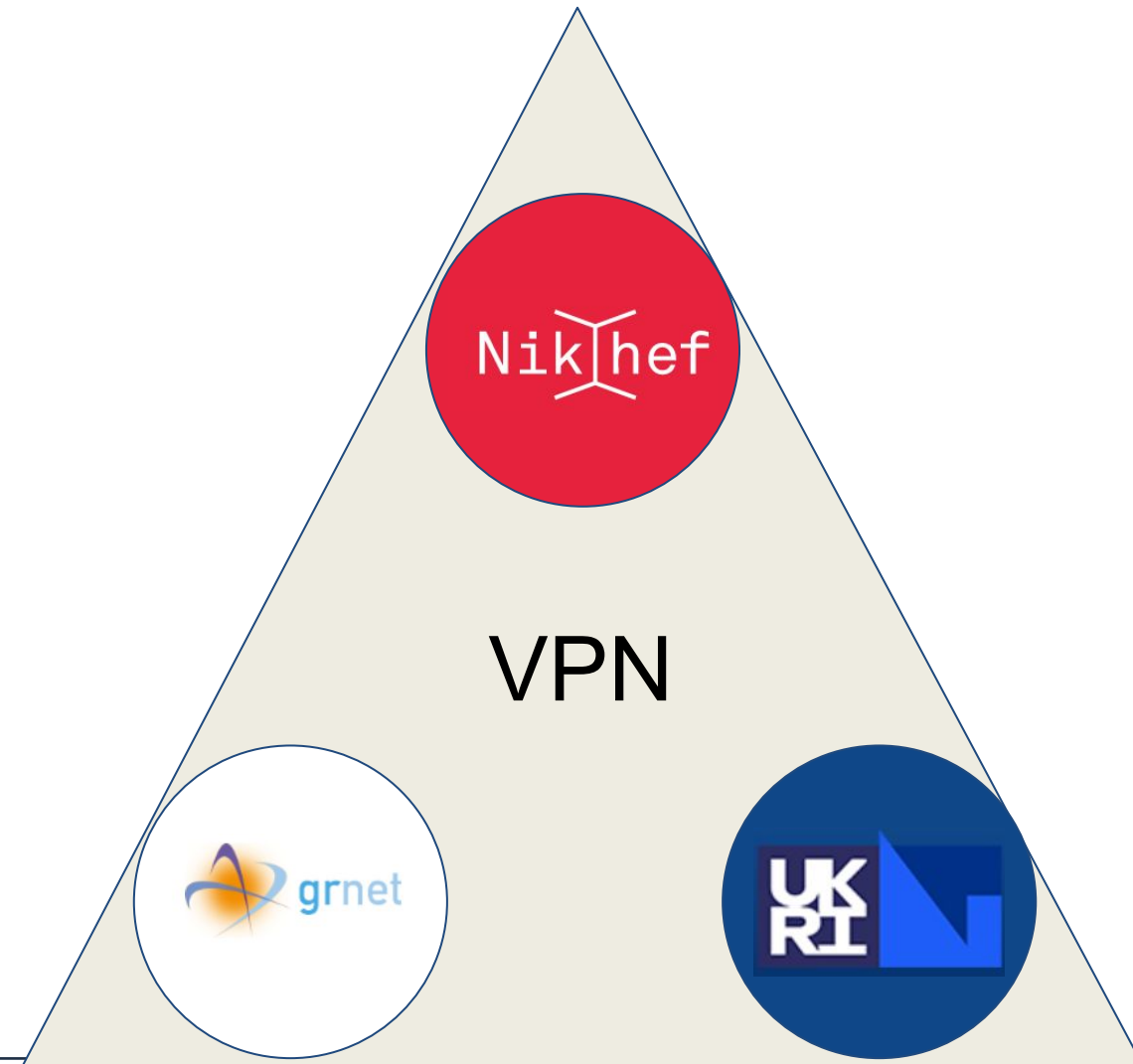
- Database connection done over OpenVPN
- MariaDB with Master-Master replication between the sites
- Replication already tested between GRNET and STFC
- Some productionisation still required

Review of tasks: Database (task 203)

Networking subtask

Interim solution - VPN

- Eventually should have dedicated VPC
- Currently protected with any IGTF certificate (Classic and MICS)
- Server run by STFC
- Databases accessible from outside only over VPN



Review of tasks: Database (task 203)

Steps for production

VPN networking

- Firewall VPN Server
- Clients may need dedicated certs
 - (As opposed to reusing host cert)
- VPN Server to allow only specific DNs

Database

- Final 3x primary replication
 - Each becomes replica to the two others
- Monitoring
- Backups (one site sufficient?)
- Local MariaDB root passwords
 - Previously replicated *any* database (including the 'mysql' one)



Site specific reports

Updated connection between GRNET delegation service and CA signing service:

- CA signing system connected exclusively to the CA web server through a private VLAN (instead of a physical link)
- Connection secured using OpenVPN with a pre-shared static key --> Should not deteriorate the protection level compared to the physical link
- CP/CPS document needs updating on <https://rcauth.eu/policy/>

COVID related:

- STFC is now in (progressing to) Level 3 (selected staff can come on site beyond core ops)
 - Intended production HSM is offline and needs on-site activation
 - Also its target host is not connected to its KVM (in the secured rack)
 - Boss claims L2 is in sight?
- Random secret data from NIKHEF is in the office, offline (it's a CD)

What's good?

- Remote operations have gone well

What's bad?

- Suleman (sysadmin on all CA services) resigned; some difficulty getting enough sysadmin support

See before: incident recovery & local HA setup

Thank you for your attention!

Questions?



EOOSC-hub

Contact

RCaauth Operations team
ops-management(AT)rcauth.eu

 eosc-hub.eu  [@EOOSC_eu](https://twitter.com/EOOSC_eu)



This material by Parties of the EOOSC-hub Consortium is licensed under a Creative Commons Attribution 4.0 International License.