RCauth Online CA service

CA Update I: RCauth HA and its evolution

rcauth.eu

@eoscfuture

Dissemination level: Public

EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777536.
and EOSC Future grant agreement id 101017536

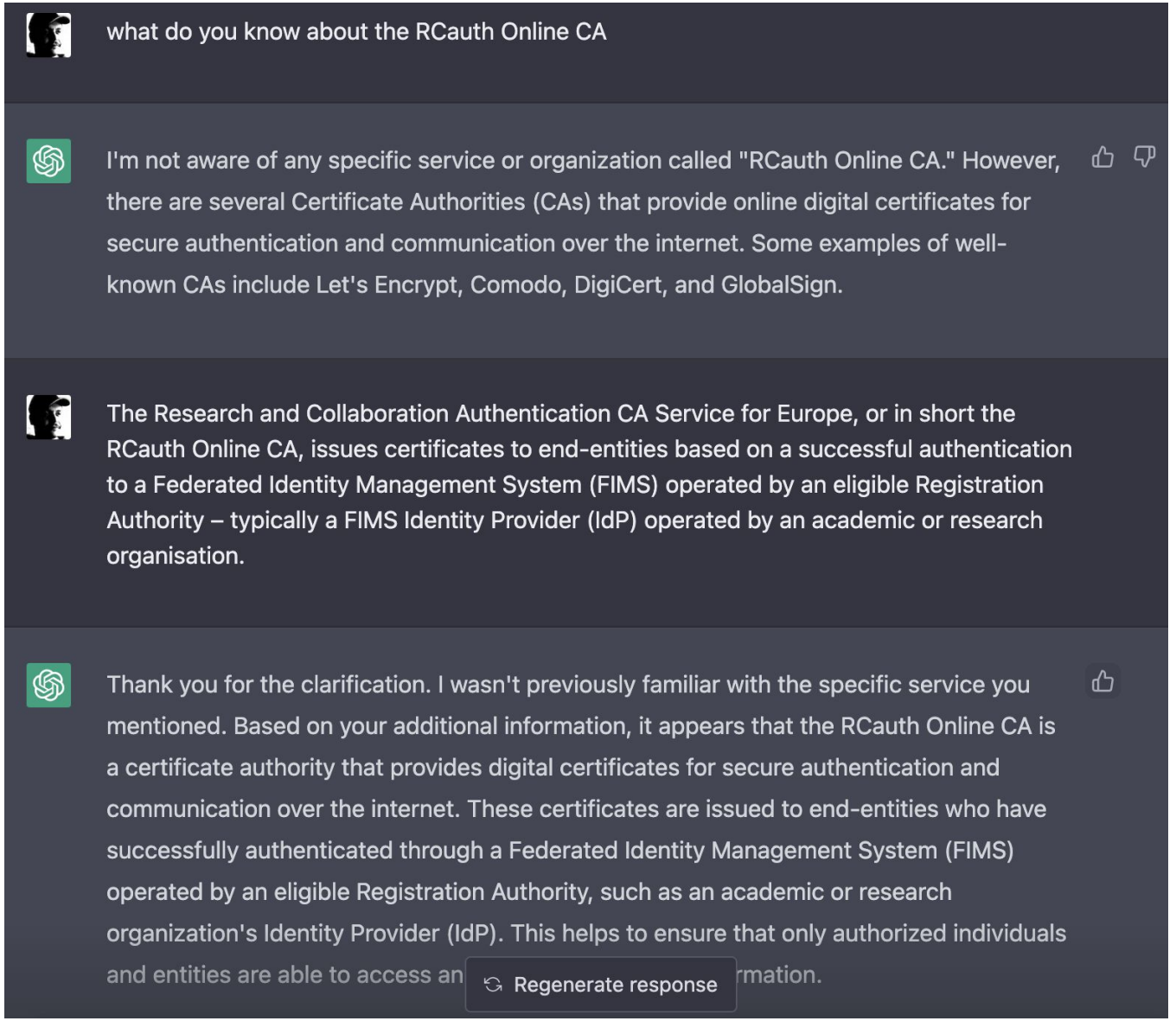
RCauth.eu

Outline (very, very approximate)

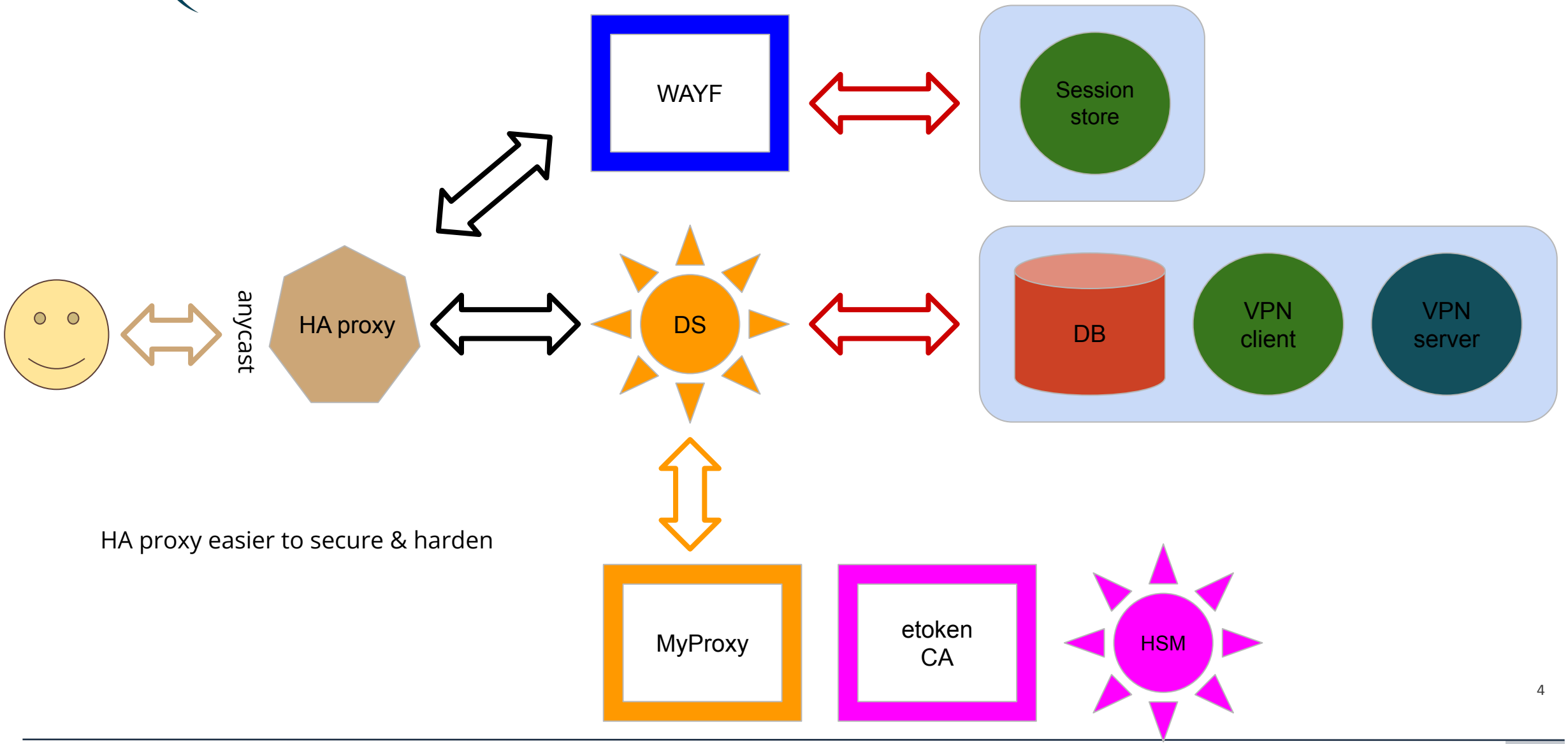
- Big Picture
- Overview of architecture
- Current status
- Next steps

Big Picture

- 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 and eduTEAMS
- EOSC Future implementing a **High Availability setup across 3 sites**
  - Work started in EOSC Hub



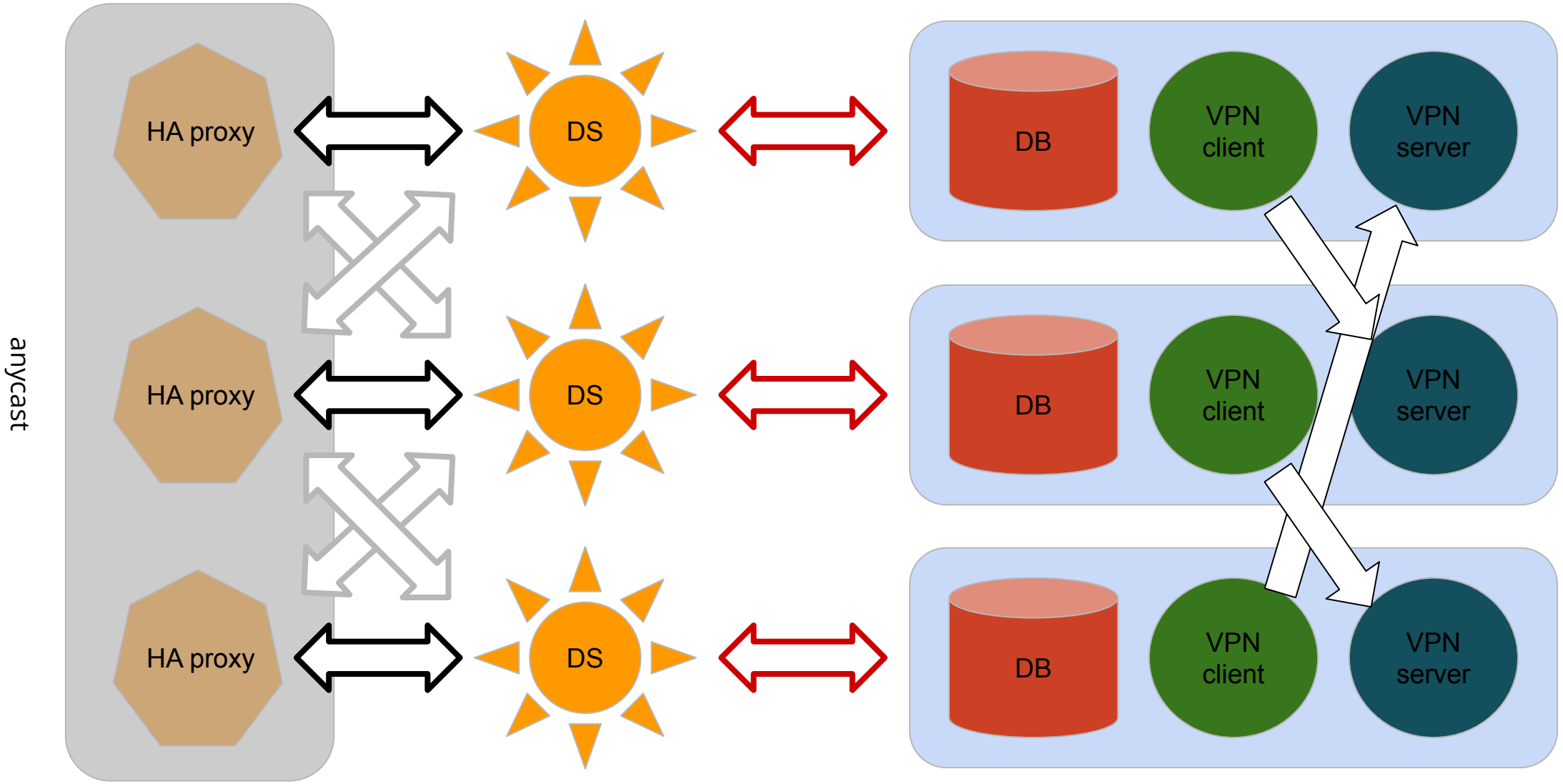
Final Architecture (1/3) - Site view



HA proxy easier to secure & harden

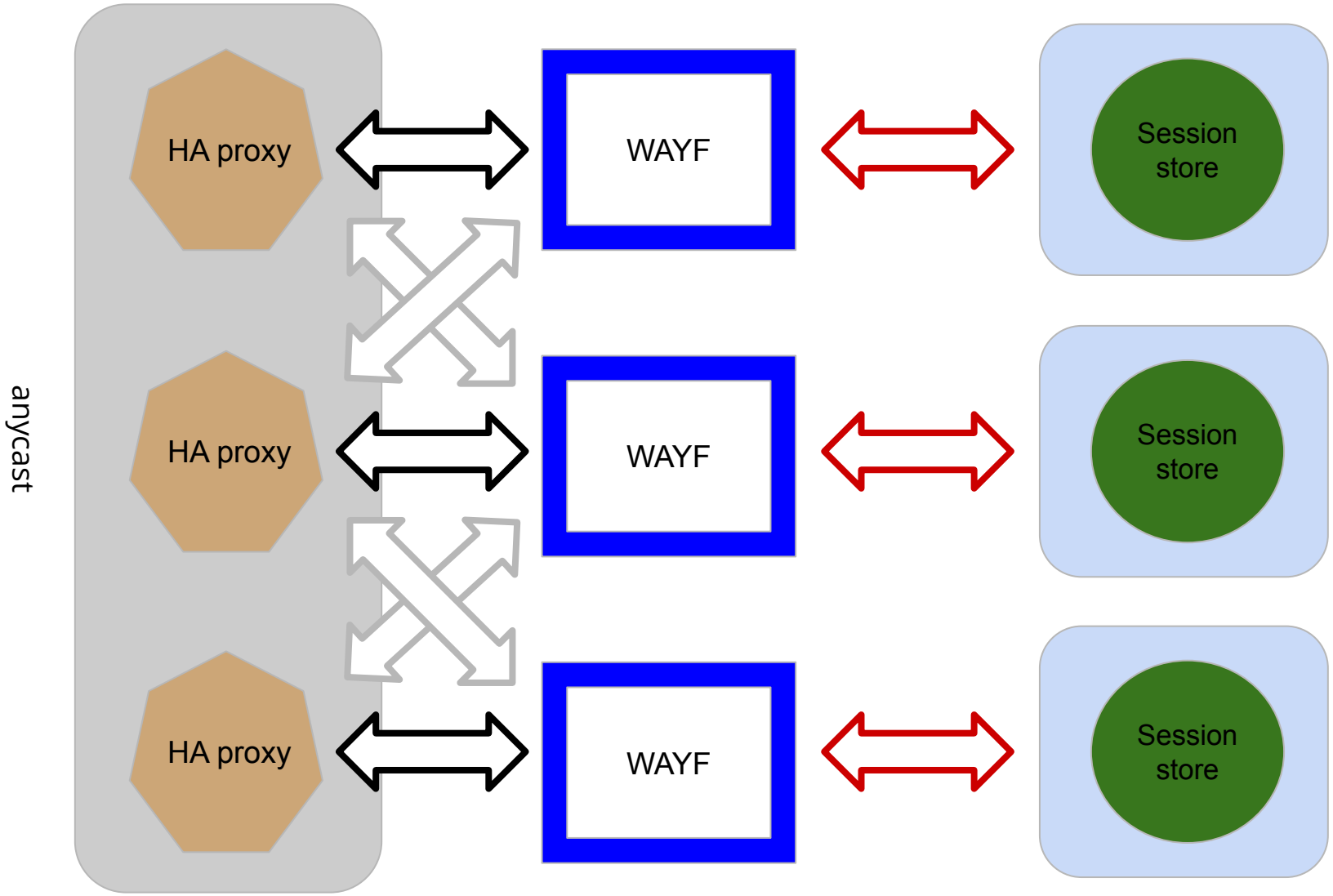
RCauth.eu

Final Architecture (2/3) - HA Proxy | DS & DB



RCauth.eu

Final Architecture (3/3) - HA proxy | WAYF



RCauth.eu

Current Status

- All sites can sign production certificates
- DS databases cross-site replication using Galera over VPN
- HA CRL cross site synchronisation and issuance
- WAYF servers (GRNET and Nikhef)

Next steps

- STFC to join ANYCAST for HAHAP (work in progress)
  - Expected after last year network reorg but needs new hardware which has now arrived
- WAYF at STFC
  - To be fronted by the anycasted HAProxies
- HA for **acceptance** instances of RCauth running on the three sites so that they appear as a single instance
  - Will probably use the SUNET DNS based solution - Särimner - (BGP anycast is not supported by GRNET's Data Centre that hosts the acceptance instance)
- Tidy up documentation
- Dev environment - relatively little to do
  - Intended to be built on demand (even at a single site's cloud)
- Paper on how to reuse the technologies developed for RCauth to make other web services HA

Reusing RCauth Researched Resources

HA distributed web service with HA database backend:

- HA database:
  - 3x node peer-peer redundant VPN: automatic failover
    - In principle extensible to >3 but what topology?
  - Galera cluster is well known
    - Although using MySQL/MariaDB has certain (dis)advantages
- Web service:
  - 3x HAproxy: stability and flexibility
  - HAHAP | BGP Anycast

Credential issuance:

- Splitting secrets - theory and practice
  - The difference between theory and practice is that, in theory, there is no difference
- Distributed CRL updates
  - Lower latency-to-revoke => higher LoA (well, slightly)

Thank you for your attention!

Questions?

Contact

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

rcauth.eu @eoscfuture