Science and Technology Facilities Council

++JJ = JK Soapbox

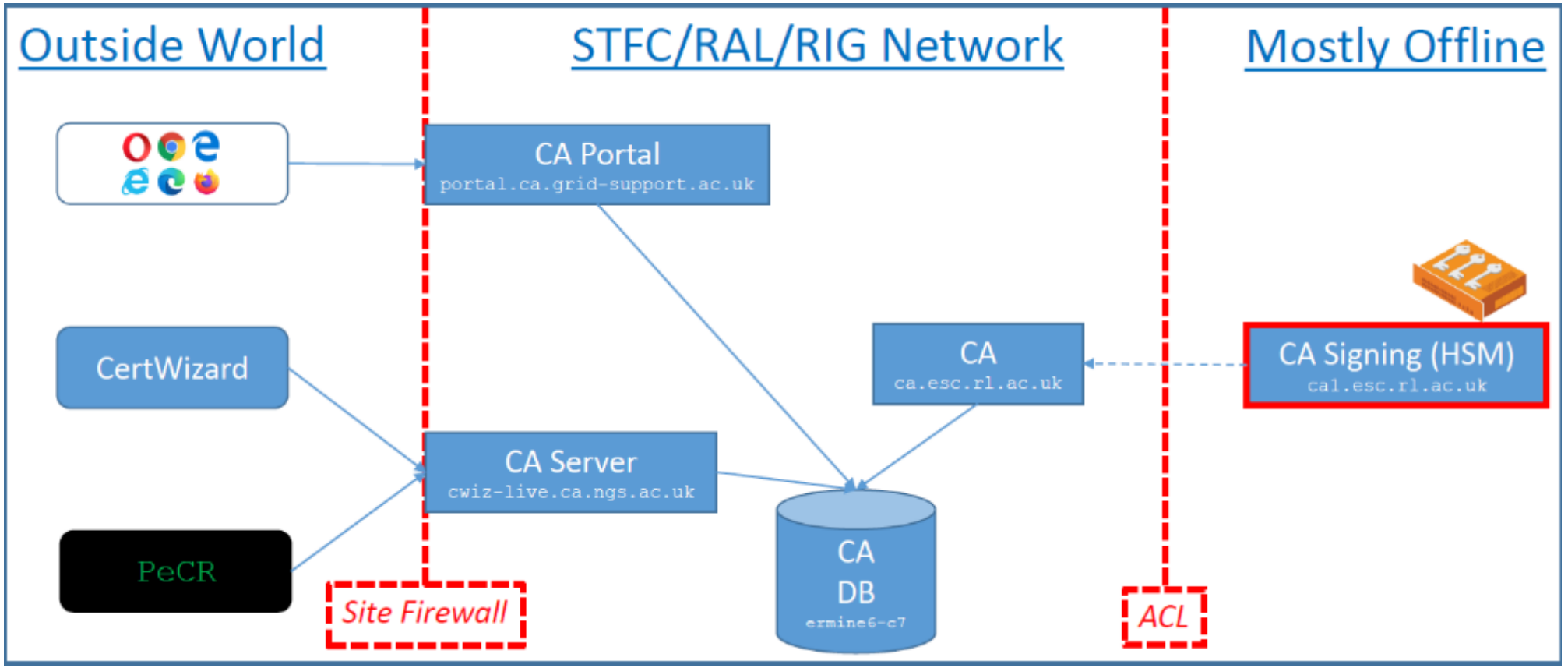
John Kewley
UK eScience CA Service Manager
STFC Daresbury Laboratory
John.Kewley@stfc.ac.uk

Aided and abetted by
Jens Jensen, Will Furnell
and Jon Roddom

Background

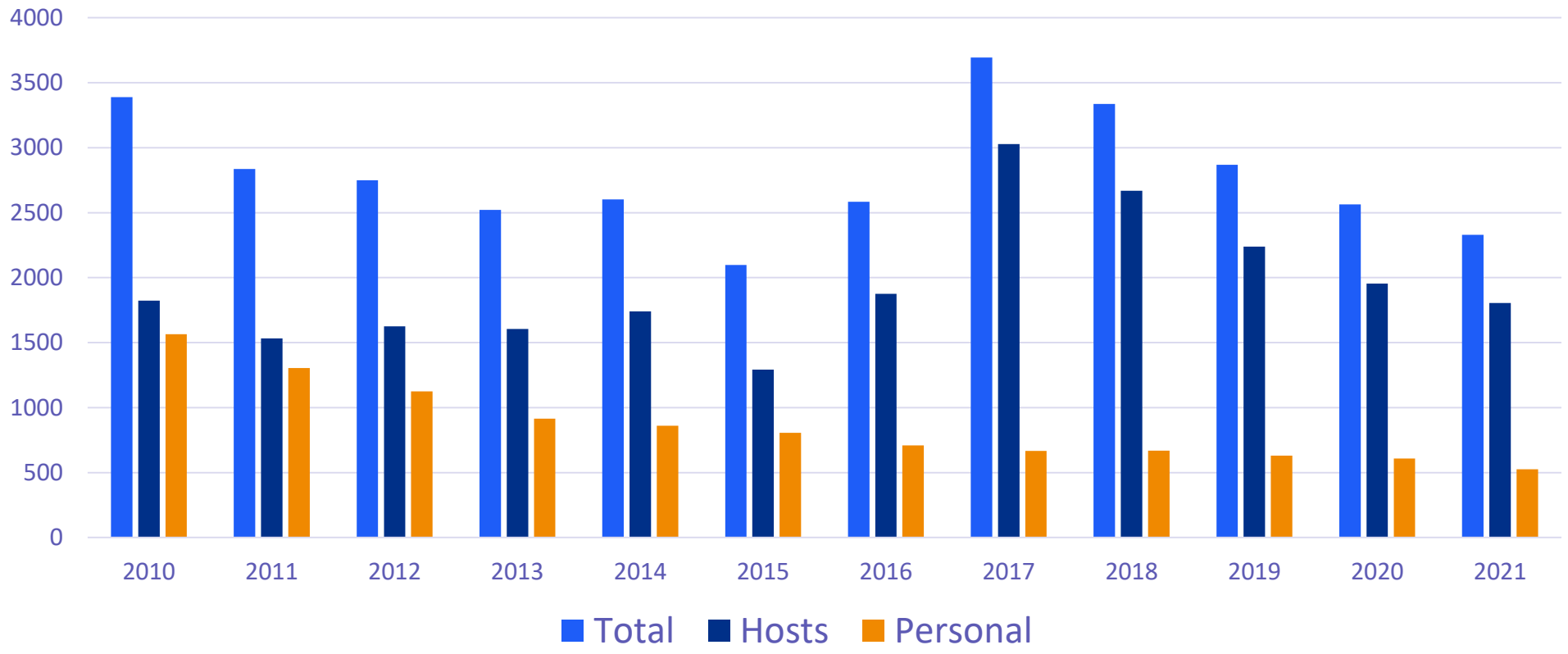
- The UK eScience CA have been considering re-issuing our PKI hierarchy as SHA2 only for a while
- Deciding when/if to upgrade has caused much discussion
- How paranoid should we be?

The UK eScience CA s/w infrastructure



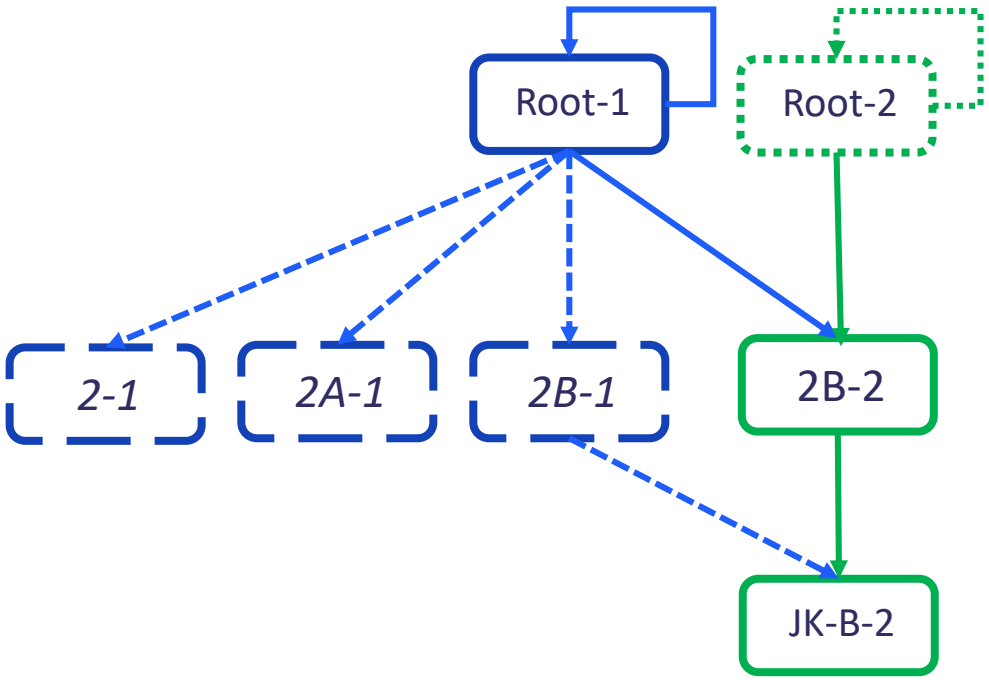
Science and Technology Facilities Council

UK eScience CA CSRs over time



Science and Technology Facilities Council

Our hierarchy (simplified!)



- Root-1 is the eScience Root certificate, self-signed with SHA1
- 2-1 expired in 2016, it had a different key-pair to the others
- 2B-1 is the old eScience CA 2B certificate, signed by the eScience Root with SHA1 *(we no longer release it, but it is still "out there"). 2A-1 was for our online CA.*
- 2B-2 is the current eScience CA 2B certificate, signed by eScience Root with SHA256
- JK-B-2 is a UK eScience user/host certificate signed by 2B with SHA256 (as almost all UK eScience CA certs have been for some years)
- The arrows show a signer-signee relationship so you can use 2B-1 or 2B-2 to check JK-B-2's signature (as they have identical keys and as both were also signed by Root (and not revoked) you can authenticate with either "chain".

Science and Technology Facilities Council

Notes

- Our previous SHA1-signed unexpired/unrevoked intermediate certificate “2B” (different serial) is still “in the wild” (as are a number of other SHA1-signed subordinates not mentioned above) 2A for instance is still mentioned in the IGTF-117 Root `.signing_policy`)
- 2B-1 shares a CRL with 2B-2 so we cannot monitor downloads to see if the old “2B” is still in use.

The [potential*] Problem

- Anything that trusts our Root (even if re-signed with SHA256), trusts anything it has signed, transitively (assuming intermediates are available to “join the dots”)
- So old SHA1-signed subordinate CAs are still implicitly trusted
- If SHA1 is broken enough to allow malicious certs that appear to be signed by that old certificate then they’ll therefore still be trusted

** There are however mitigations*

Mitigations

Browser world

- Support for SHA1 has been removed for subordinates and EECs (unless already installed!?) so previous attack wouldn't work … if using a modern browser and your trusted keystore has been updated

Grid World

- Most grid systems will obey `.namespaces` and/or `.signing_policy` files so that should give some protection. Many sites will also not trust SHA1.

Other Worlds or misconfigured / poorly updated systems

- All bets are off

A lot of IFs

Ok, so that is a lot of IFs, so are we just being a bit paranoid?

Science and Technology Facilities Council

Impact of changing

- Opportunity to modernise – consider crypto, etc for new CAs; the longer we delay moving the better support will be, but we have to do something before 2027 anyway
- ?2-3 months for new hierarchy to percolate around the Grid
- Tweaks to various bits of s/w – depending on size of change
- Start signing New and Renewal requests with new CA and generate new CRL
- *** Communication to ensure that VOMS servers that include IssuerDN as part of their user's identity are updated ***
- 13 months for all old certs to have expired
- Remove old hierarchy from IGTF
- Sign final CRLs for old hierarchy

Opportunity to modernise

- Should we use larger keys?
- Is it too soon to move to EC?
- Should we wait a bit longer for SHA3 to be more widespread?
- What else is around the corner? Quantum-safe?

So we are also paranoid about moving too quickly and being too *bleeding edge*!

https://blog.jessriedel.com/2020/09/15/quantum-computing-timelines/

https://www.networkworld.com/article/3619229/the-timeline-for-quantum-computing-is-getting-shorter.html

Science and Technology Facilities Council

Prior art: some stats for IGTF 117

88 accredited certs

- 5 are EC: 2x 256, 3x 384
- 83 are RSA: 1x 1024, 47 x 2048, 4x 3072, 29x 4096, 2x 8192

- 62 are self-signed: 15 are Roots, 47 sign EECs
- 26 are subordinates

- 26 are signed with SHA1: 2 of which are subordinates which sign EECs
  - *Also 2x unaccredited and 1x experimental which are self-signed*
- 43 are signed with SHA2: 43x SHA256, 13x SHA384, 3x SHA512

Reissuance of roots?

ASGCCA-2007
BYGCA
CNIC
DZeScience
DigiCertGridCA-1-Classic
DigiCertGridTrustCA-Classic
GridCanada
KEK
MARGI
RDIG
SRCE
TRGrid
cilogon-basic
seegrid-ca-2013

ArmeSFo
CESNET-CA-Root
DFN-GridGermany-Root
DigiCertAssuredIDRootCA-Root
DigiCertGridRootCA-Root
GermanGrid
IHEP-2013
LIPCA
QuoVadis-Root-CA2
RomanianGRID
SiGNET-CA
UKeScienceRoot-2007
cilogon-silver

To rekey or not rekey?

A paraphrasing of the Shakespearean tautology “0x2b | !0x2b” ?

“If you're paranoid long enough, sooner or later you're gonna be right.”, Kinky Friedman

Options

1. Risk is negligible: ignore for now, reconsider next year
2. To avoid some logistical issues, could consider doing some housekeeping:
   a) Re-signing Root with SHA256
   b) Revoking previous SHA1 subordinate certs
   c) Remove 2A CA from our `.namespaces` and `.signing_policy` files
   d) Extend lifetime when re-signing to later than 2027
3. Re-issue whole new hierarchy:
   a) All SHA256 signed; Consider >2048 RSA (or even EC) keys; and other “modernisation”
   b) EEC SubjectDNs remain the same, their IssuerDNs will change (since old/new signing Cas must coexist);
   c) After “percolation period”, New and Renewed certs would be signed with new CA cert (minor s/w update)
4. Move Online or maybe separate Offline (personal) and Online (host) hierarchies
   a) New s/w required for Online; opportunity to go ACME
   b) Would need to develop/support even more software (and would need to co-exist with existing)

Is Security binary

- I used to complain when folks said “well that is fairly secure”, surely it is either secure or it isn’t
- I later changed my thinking and decided that what we wanted was something along the lines of “Secure to a certain Level of Assurance (LoA)”
- But maybe that should be Levels of Paranoia (LoP)?

Science and Technology Facilities Council

Final thoughts

- When to move – when we are forced or proactively? Can you be too proactive?
- Our role is to be paranoid, but how paranoid is too paranoid?
- We can be paranoid about standing still, but also paranoid about moving too quickly

Science and Technology Facilities Council