UK Access Management Federation - technical update for FAM26

Alex Stuart
Trust & Identity technical architect
Jisc

Overview

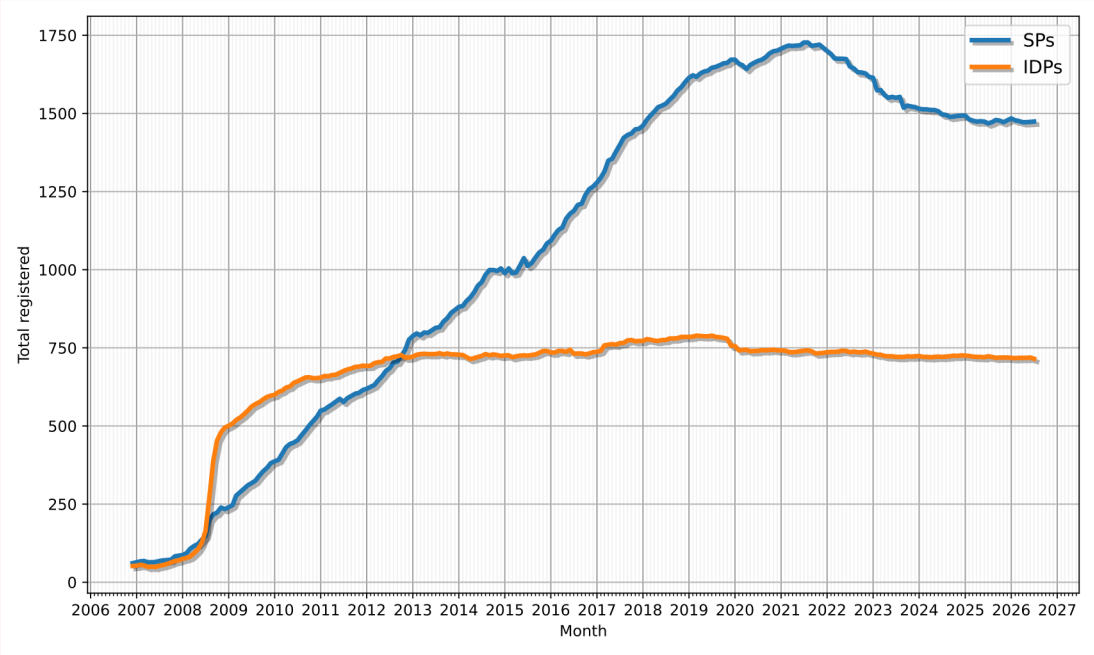
1. *The UK federation and eduGAIN*
2. *A short history of profiles*
3. *A pathway to including post-quantum cryptography in the UK federation*
4. *UK federation signing key transition from 2K to 4K RSA keys in 2027*
5. *Shibboleth SP re-architecture*

1. UK federation and eduGAIN

What is the UK federation?

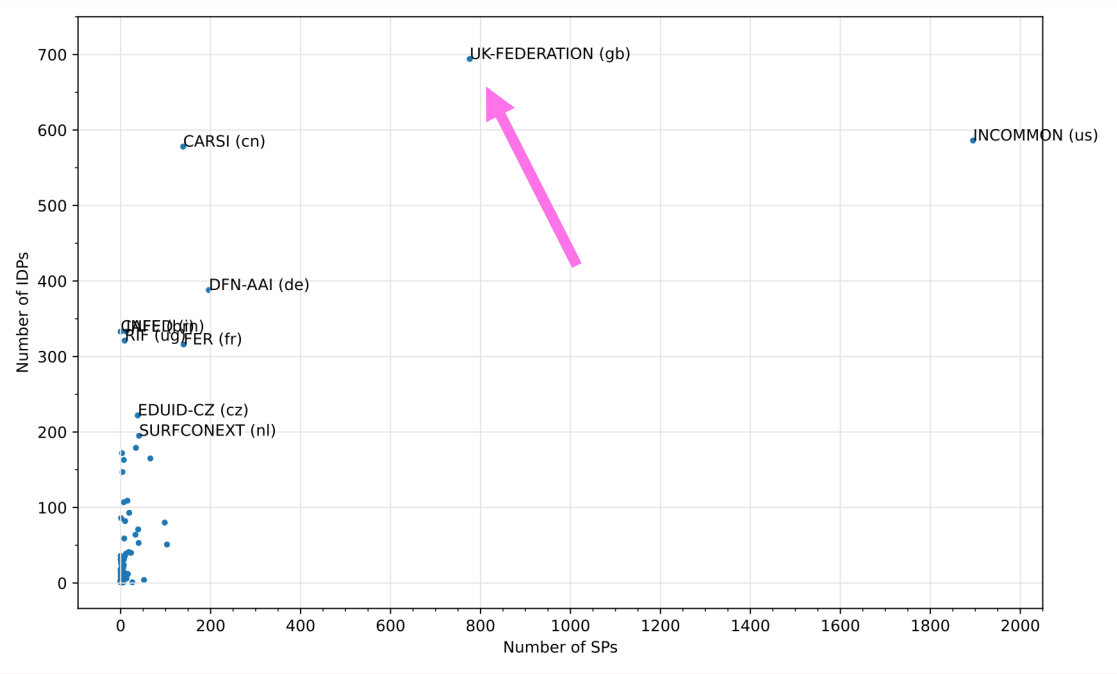
Number of IdPs and SPs

Registered Entities by Type



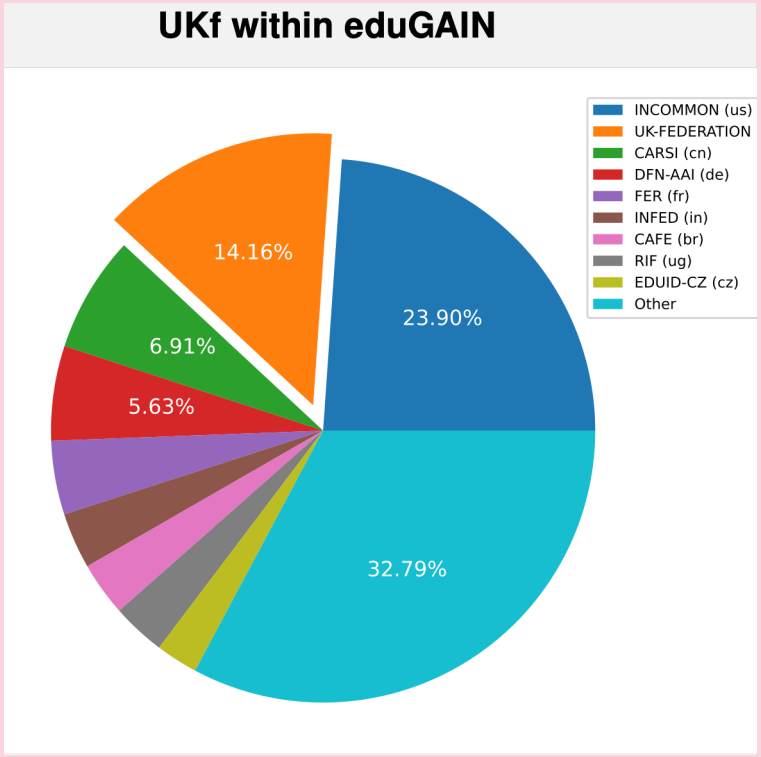
Integration with eduGAIN

Size of federations in eduGAIN



UK federation and eduGAIN

- *UK registers 1469 SPs and 715 IdPs*
- *Has eligibility policy, and metadata registration practice statement*
- *peer with 83 other "national" federations through the eduGAIN inter-federation*



		Government role in NREN governance				
		No government representation	Represented by public funding body	Board representation	Government-appointed board	Government agency
Funding model	User-financed	DeIC, DFN, GRENA, RHnet, URAN	GARR	ACOnet, IUCC, RENAM, SWITCH		
	Mixed funding	ASNET-AM, CESNET	Jisc, SUNET, SURF	BREN, HEAnet, RENATER	CyNet, CSC/ Funet, LITNET	Belnet, Sikt
	Government-subsidised	SANET		AMRES, RESTENA	ARNES, CARNET, GRNET, RedIRIS	AzScienceNet, EENet, FCCN, KIFÜ, LAT, MARnet, MREN, RoEduNet, ULAKBIM

Table 2.2: Funding models and formal government involvement in NREN governance. *Not too surprisingly, there is a slight correlation between government influence and funding model (see Figure 2.5 for details) – increasing government influence is correlated with government funding and vice versa. Some NRENs do not appear in the table as either their governance model (RASH) or their funding model (PSNC and UoM) have not been shared.*

2. A short history of baseline profiles

Abbreviated timeline of profiles

- *200x UK federation Rules of Membership – UserAccountability*
- *…*
- *2018 InCommon (US) Baseline expectations, version 1 (Metadata elements)*
- *2019 UK federation draft "export guarantee"*
- *2021 REFEDS Identity Federation Baseline Expectations (high level obligations on IdP operators, SP operators, Federation operators; https://refeds.org/baseline-expectations)*
- *2022 InCommon (US) Baseline expectations, version 2 (TLS strength, Sirtfi, errorURL)*
- *2025 SWAMID (SE) Identity Assurance profiles*
- *2026 IDEM (IT) starts working group on security and baseline expectations*
- *2026 eduGAIN technical profile working group starts*

3. Deploying post-quantum cryptography in the UK federation

National and international guidance

UK National Cyber Security Centre

By 2028

- *Define your migration goals*
- *Carry out a full discovery exercise (assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded to PQC)*
- *Build an initial plan for migration*

By 2031, we must carry out the earliest, highest-priority PQC migration activities

By 2035, we must complete migration to PQC of all systems

NIS Coordination Group: First steps by end 2026

- *Identify and involve stakeholders*
- *Support mature cryptographic asset management*
- *Create dependency maps*
- *Include the supply chain*

NIST Transition to PQC Standards

- RSA security strength 112 deprecated after 2030 (2048 bit key, RSA-SHA256 signature, SHA256 digest)
- All RSA disallowed after 2035

Jisc

Using SAML metadata for discovery exercise

Line	Algorithm/ Element	Specification
7	RSA-SHA256	XMLDsig
7	Implicitly, a key	X509Certificate?
13	SHA256	XMLEnc
20	algsupport	Oasis
21	SHA512	XMLEnc
22	algsupport	Oasis
23	RSA-SHA256	XMLDsig
29	X509Certificate	ITU
32	AES128-GCM	XMLEnc
33	RSA-OAEP	XMLEnc
36	TLS	IETF RFC


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_"
  entityID="https://test.ukfederation.org.uk/entity">
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="#_">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>0rlBlxAc47wHWGyuNM7l5ArRo7XCGWewAv/3qqnCTXk=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>BThj+8aCJJDtESX32...</SignatureValue>
  </Signature>
  <Extensions>
    <alg:DigestMethod xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
      Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
    <alg:SigningMethod xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
      Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha512"/>
  </Extensions>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIC3DCCA...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
      <EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
      <EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#rsa-oaep"/>
    </KeyDescriptor>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://test.ukfederation.org.uk/Shibboleth.sso/SAML2/POST" index="1"/>
  </SPSSODescriptor>
</EntityDescriptor>
```

RSA security strength 112 deprecated after 2030

Survey of federations in eduGAIN (May 2026)

Key size	Signature	Digest	Number of federations	Security strength
2048	RSA-SHA256	SHA256	27	112
3072	RSA-SHA256	SHA256	9	128
4096	RSA-SHA256	SHA256	43	128
4096	RSA-SHA512	SHA512	1	150

- UK federation currently has a 2048 bit key (aggregates) and a 4096-bit key (MDQ).
- Work item for 2026/27: migrate away from the 2K key
  - build capacity for change
  - Increases MDQ usage
  - Simplify toolchain

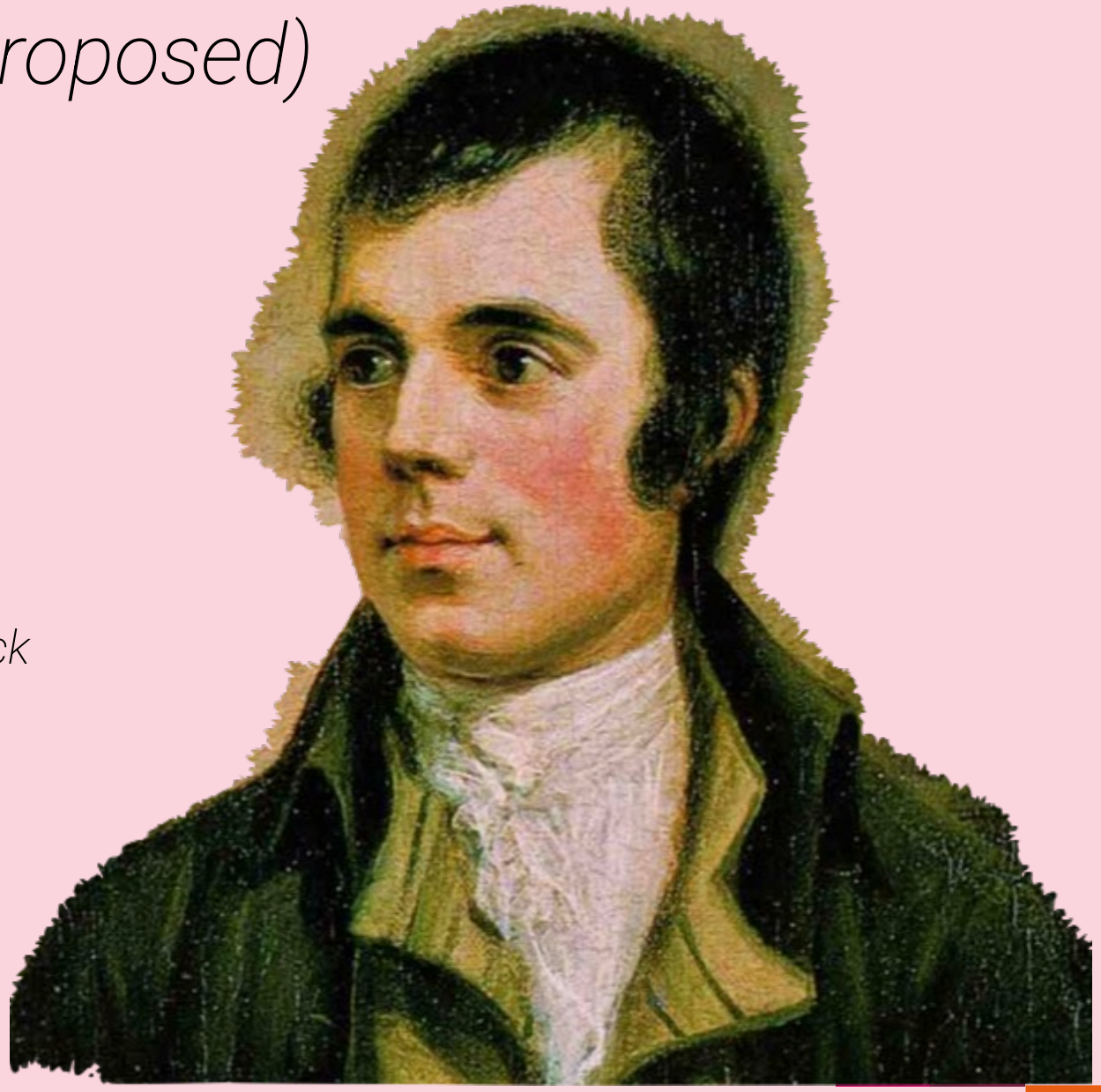
4. 2K 4K RSA key transitions

Dates of 4K key transitions (proposed)

Some constraints:

- *There is lots to do in T&I, so get it out of the way!*
- *UK federation hardware refresh at end 2027*
- *Give as much notice to deployers as possible*
- *Don't introduce transition during change freezes (exams, enrolment)*
- *Decent interval between test, production and fallback*

Transition	Date
Test	August 2026
Production	Monday 25 January 2027
Fallback	Summer 2027



Jisc

Processes for migrating to 4K keys

Process for IdP deployers using MDQ

Nothing! You're already using the 4K key

IdP deployers considering using MDQ

You could do that today!
See https://www.ukfederation.org.uk/content/Documents/MDQ

Process for (confident) deployers

1. *Understand your metadata download process*
2. *Download new certificate, check out of band*
3. *Wait until production cut-over date*
4. *Change certificate in config*
5. *Ensure metadata is refreshing*

Risk-averse / using non-standard software

1. *Understand your metadata download process*
2. *Download new certificate, check out of band*
3. *Use a test deployment, configure it to use our test aggregate.*
4. *If all is well, go to step 3 in right hand column*

5. Shibboleth SP re-write

Shibboleth SP V4.0 rewrite is underway – 1

Aims

- Move XML handling out of barely-maintained C++ libraries
  (10K LoC, legacy style, hard to modify)
- Re-write SP code as a module of the main Shibboleth IdP product
- Facilitate using new SSO protocols (OpenID Connect, OAuth2.0, OpenID Federation)
- Application integration will be as similar as possible to previous versions

Timeline

- V4 Alpha version 2 released on 18 June
- Shibboleth Consortium members-only webinar June 2026
- Software release V4.0 expected in late 2026
- No date set for EOL of SP version V3.x yet

Shibboleth SP V4.0 rewrite is underway – 2

Shibboleth lead developer said in his November 2025 blog post:

“I encourage anybody using the SP now to [review the documentation], so you can make an honest determination as to your plans. I do not advise waiting on this. If it’s not what you want, then jump, and do it sooner than later.”

Relevant documentation to help you decide:

- https://shibboleth.atlassian.net/wiki/spaces/spagent4/overview
- https://shibboleth.atlassian.net/wiki/spaces/sphub1/overview
- https://shibboleth.atlassian.net/wiki/spaces/DEV/pages/4075978758/Expected+SP+Changes+from+V3

Jisc

For the future of education and research

Alex Stuart

Trust & Identity technical architect

alex.stuart@jisc.ac.uk

help@jisc.ac.uk

0300 300 2212

jisc.ac.uk

@jisc.bsky.social

@jiscsocial

linkedin.com/company/jisc

References and thanks

- *Slide 4: please ask for datasets behind the 2 graphs on this slide*
- *Slide 5: please ask for the dataset behind the graph on this slide*
- *Slide 5: table data taken from section 2.3 of the GÉANT Compendium 2023, available from https://resources.geant.org/geant-compendia/*
- *Slide 13: picture of Robert Burns by Alexander Nasmyth, available on https://commons.wikimedia.org/wiki/File:Robert_burns.jpg*