UK federation update

REFEDS 44
13 June 2022

Alex Stuart, Technical Development Manager (Trust & Identity), Jisc
alex.stuart@jisc.ac.uk

Remembering Rhys Smith

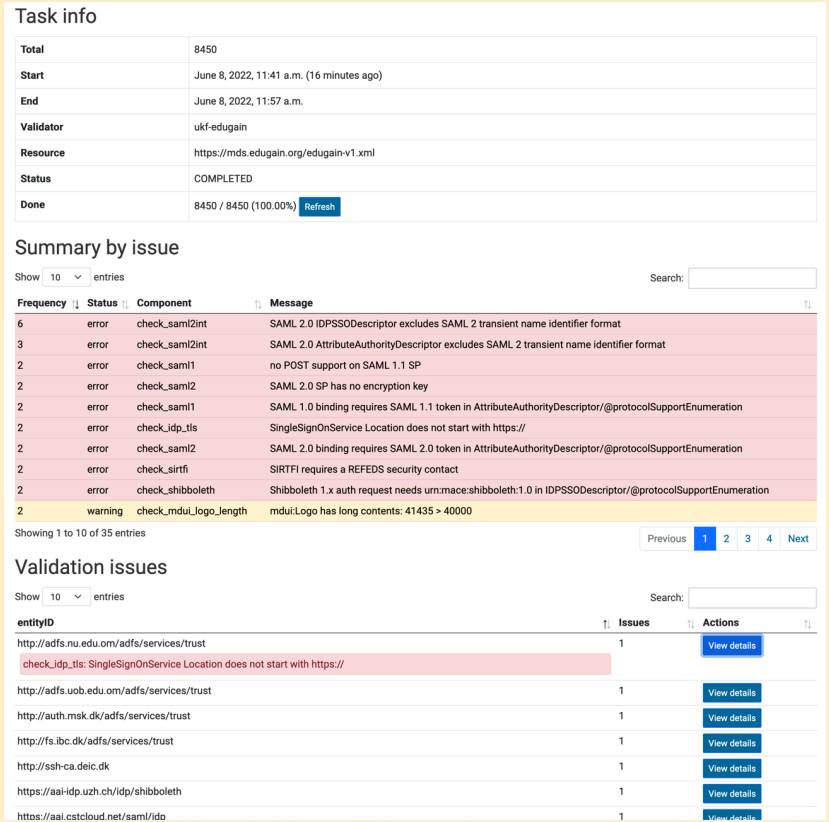
Re-engineering UKf service infrastructure

- Replacing HSM by end July 2022
- Developing workflow-based UIs for managing metadata
- Moving away from Jenkins as orchestrator
- Containerising services
- Move to signing aggregates with 4K key by 2030

UKf product	Key	Digest algorithm	Signing algorithm	Shibboleth product
Aggregate	2K RSA	SHA256	RSA-SHA256	xmlsectool
MDQ fragments	4K RSA	SHA256	RSA-SHA256	MDA
MDA all entities	4K RSA	SHA256	RSA-SHA256	xmlsectool

Jisc

Metadata validation service



Task info

Total	8450
Start	June 8, 2022, 11:41 a.m. (16 minutes ago)
End	June 8, 2022, 11:57 a.m.
Validator	ukf-edugain
Resource	https://mds.edugain.org/edugain-v1.xml
Status	COMPLETED
Done	8450 / 8450 (100.00%) Refresh

Summary by issue

Show 10 entries Search:

Frequency	Status	Component	Message
6	error	check_saml2int	SAML 2.0 IDPSSODescriptor excludes SAML 2 transient name identifier format
3	error	check_saml2int	SAML 2.0 AttributeAuthorityDescriptor excludes SAML 2 transient name identifier format
2	error	check_saml1	no POST support on SAML 1.1 SP
2	error	check_saml2	SAML 2.0 SP has no encryption key
2	error	check_saml1	SAML 1.0 binding requires SAML 1.1 token in AttributeAuthorityDescriptor/@protocolSupportEnumeration
2	error	check_idp_tls	SingleSignOnService Location does not start with https://
2	error	check_saml2	SAML 2.0 binding requires SAML 2.0 token in AttributeAuthorityDescriptor/@protocolSupportEnumeration
2	error	check_sirtfi	SIRTFI requires a REFEDS security contact
2	error	check_shibboleth	Shibboleth 1.x auth request needs urn:mace:shibboleth:1.0 in IDPSSODescriptor/@protocolSupportEnumeration
2	warning	check_mdui_logo_length	mdui:Logo has long contents: 41435 > 40000

Showing 1 to 10 of 35 entries Previous 1 2 3 4 Next

Validation issues

Show 10 entries Search:

entityID	Issues	Actions
http://adfs.nu.edu.om/adfs/services/trust	1	View details
check_idp_tls: SingleSignOnService Location does not start with https://		
http://adfs.uob.edu.om/adfs/services/trust	1	View details
http://auth.msk.dk/adfs/services/trust	1	View details
http://fs.ibc.dk/adfs/services/trust	1	View details
http://ssh-ca.deic.dk	1	View details
https://aai-idp.uzh.ch/idp/shibboleth	1	View details
https://aai.cstcloud.net/saml/idp	1	View details

- We already publish Apache 2-licensed validation toolchain and output the results of our daily validation run of eduGAIN
- Move to microservice-based architecture will need frequent validation. Why not make this available?
- Help estimate effect of new profiles e.g. any proposals for an eduGAIN baseline
- Proof of concept exists

Jisc

IdP discovery

- Shibboleth EDS-compatible JSON Discovery feeds
  - Is this a missing piece of the puzzle for moving SPs to MDQ?
  - We now publish 2 feeds alongside every publication of SAML metadata
  - Currently exploring trust models and deployment options (not much luck ☹)

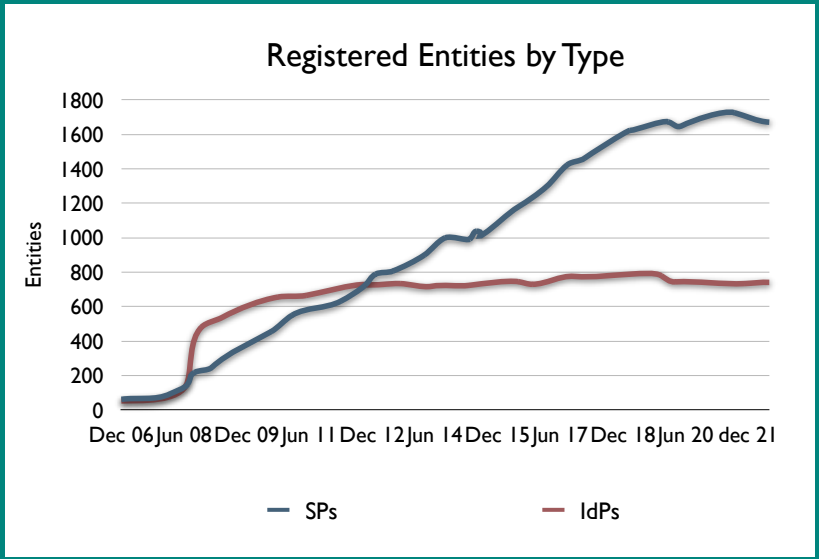
- Removing WAYF protocol from our CDS later this month

- Evaluating options for replacing our venerable CDS

Jisc

Charging SPs

- Membership of the UK federation is part of Jisc membership for HE/FE. Has been free for SPs.
- Income contributes to UK federation staff costs
- Creates opportunities for incentivising behaviour change
- Reducing number of registered entities!



UK federation update

REFEDS 44
13 June 2022

Alex Stuart, Technical Development Manager (Trust & Identity), Jisc
alex.stuart@jisc.ac.uk