ShibAndEdugain

Loading metadata

Metadata downloaded from https://mds.edugain.org

Strange things

- Metadata is not signed by a third party
- Line breaks and indentation is quite by chance, however running through `xml_pp` of course invalidates the signature of the individual `<EntityDescriptor>`s
- Metadata cannot be validated to the schema (see later)

Problems loading metadata to Shibboleth SP

For perl processing, MDS output is run through `xml_pp`, an XML pretty-printer.

Here is the command I use to load MDS output to a Shibboleth 2.0 SP:

```
wget -O- --ca-certificate=/home/bajnokk/edugain_bundle.crt https://mds.edugain.org |xml_pp \
| perl -pe 's/(<(md:)?EntitiesDescriptor)/\1 xmlns="urn:oasis:names:tc:SAML:2.0:metadata"/;
s/.*RoleDescriptor.*//g; s/.*OnlineCA.*//g; \
           s/cacheDuration[>](^)*//g; ' >/tmp/mds-pp.xml
```

Explanation follows:

Unable to connect

For some reason, Shibboleth 2.0 cannot connect to https://mds.edugain.org. It seems to be a `libcurl` issue, which is not easy to circumvent. (See this shib-users thread) Newer cURL's can handle the SSL handshake (the ones in Ubuntu Intrepid and Debian Lenny can not). So it's necessary to `wget` the metadata.

It turned out that newer versions of Shibboleth can connect to mds.edugain.org, however the following errors prevent the metadata from being loaded directly.

No default namespace

There is no default namespace for the outer `EntitiesDescriptor`, the root element. No problem with that, but there is at least one `EntityDescriptor`, which is not correctly namespaced (and assumes that the default namespace is `urn:oasis:names:tc:SAML:2.0:metadata`)

Solution:

```
| perl -pe 's/(<(md:)?EntitiesDescriptor)/\1 xmlns="urn:oasis:names:tc:SAML:2.0:metadata"/;'
```

Invalid use of RoleDescriptor

SAML Metadata Schema declares that RoleDescriptor is an abstract element, whatever it means. Shibboleth (2.0) cannot load an entity with such an element.

Solution: | perl -pe 's/.*RoleDescriptor.*//g;' At the time of writing, it only affects Fresco-AAI. For some unknown reason, Fresco-AAI metadata is a one-liner (even after pretty printing), so it's possible to remove it such a way. If it wasn't the case, proper XSLT would be necessary.

Invalid extension of the schema

GIdP entity contains an `egmd:OnlineCADescriptor` element, which is not a standard extension of the SAML schema.

Solution:

```
| perl -pe 's/.*OnlineCA.*//g;'
```

At the time of writing, it only affects GIdP. For some unknown reason, GIdP metadata is a one-liner (even after pretty printing), so it's possible to remove it such a way. If it wasn't the case, proper XSLT would be necessary.

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:16 CEST
cziernorbert frissítette 2026-04-14 13:24:20 CEST