Change of the Shibboleth Identity Provider SAML certificate

19.05.2024 02:38:41

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::Single-Sign-On	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	12:28:25 - 15.12.2023

Schlüsselwörter

Shibboleth IdP SAML Certificate IdP SAML Shibboleth

Lösung (öffentlich)

For SAML communication between Service Provider (SP) and Identity Provider (IdP), certificates are used on both sides to sign and encrypt data transmissions. If one of the parties no longer knows the corresponding public certificate of the communication partner, e.g. as a result of an exchange of the private key, a malfunction occurs. This FAQ serves to prevent such cases and presents options for Single Sign On (SSO) operation.

Recommended option

For transparent and trouble-free SSO operation, membership in a federation is recommended for all participating parties (SP and IdP). The Shibboleth IdP of TU Dresden is therefore a member of the DFN AAI Federation ([1]https://doku.tid.dfn.de/de:aai:about). The DFN AAI Federation ensures the secure provision of metadata [1], which also includes the public certificates and which can be obtained by any party. Every SP is advised to obtain the IdP metadata [2] regularly via an automated process.
The old and new certificates are offered in parallel for a period of time so that no disruption occurs when a certificate is changed.

Alternative option

If you do not have the option of regularly obtaining the metadata of the DFN AAI Federation automatically, e.g. because your service does not have access to the outside world or the SP application does not allow it, you must provide your SP with the IdP metadata manually. You can obtain the metadata of the IdP of TU Dresden as follows:

- From the IdP of TU Dresden itself:
[2]https://idp.tu-dresden.de/idp/shibboleth
- Via the federation:
[3]https://met.refeds.org/met/entity/https://idp.tu-dresden.de/idp/shibboleth/

If you use this option, you are dependent on the IdP operators notifying you when a certificate change is due. A fault will occur if this notification is overlooked or ignored. The certificate must be exchanged within a transition period during which both certificates (old and new) are offered by the IdP.
For further information see: IdP certificate change TU Dresden.

IdP certificate change TU Dresden A certificate change of the IdP of TU Dresden is usually announced in advance to all known SPs via the contacts known to us. Upon receipt of the announcement, the IdP metadata already contains the new certificate. The certificate change is offered for at least 14 days in advance. During this time, operation is possible with both certificates.
Note: If your SP does not have the possibility to use both certificates in parallel for a certificate change, please use the new certificate (cert_idp.tu-dresden.de.pem), which is attached in this FAQ.

[1] Metadata overview of the DFN AAI Federation:
[4]https://doku.tid.dfn.de/de:metadata
[2] IdP metadata: [5]http://www.aai.dfn.de/metadata/dfn-aai-idp-metadata.xml

[1] https://doku.tid.dfn.de/de:aai:about
[2] https://idp.tu-dresden.de/idp/shibboleth
[3] https://met.refeds.org/met/entity/https://idp.tu-dresden.de/idp/shibboleth/
[4] https://doku.tid.dfn.de/de:metadata
[5] http://www.aai.dfn.de/metadata/dfn-aai-idp-metadata.xml