Wechsel des Shibboleth Identity Provider SAML Zertifikates

09/10/2024 18:47:26

FAQ Article Print

Category:	IT-Sicherheit & Anmeldung an Diensten::Single-Sign-On	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	de	**Last update:**	12:28:04 - 12/15/2023

Keywords

Shibboleth IdP SAML Zertifikat IdP SAML Shibboleth

Solution (public)

Für die SAML-Kommunikation zwischen Service Provider (SP) und Identity Provider (IdP) werden beidseitig Zertifikate zur Signierung und Verschlüsselung der Datenübertragungen verwendet. Sollte eine der Parteien, z. B. in Folge eines Austauschs des privaten Schlüssels, das zugehörige öffentliche Zertifikat des Kommunikationspartners nicht mehr kennen, tritt eine Störung auf. Dieses FAQ dient der Vorbeugung vor solchen Fällen und stellt Optionen für den Single Sign On (SSO) Betrieb vor.

Empfohlene Option Für einen transparenten und störungsfreien SSO Betrieb wird allen teilnehmenden Parteien (SP und IdP) die Mitgliedschaft in einer Föderation empfohlen. Der Shibboleth IdP der TU Dresden ist daher Mitglied der DFN AAI Föderation ([1]https://doku.tid.dfn.de/de:aai:about). Die DFN AAI Föderation sorgt für eine sichere Bereitstellung der Metadaten [1], welche auch die öffentlichen Zertifikate beinhalten, und die von jeder Partei bezogen werden können. Jedem SP wird nahgelegt, die IdP-Metadaten [2] regelmäßig über einen Automatismus zu beziehen.
Damit bei einem Zertifikatswechsel keine Störung auftritt, wird dabei das alte und das neue Zertifikat eine Zeit lang parallel angeboten.
Alternative Option Falls Sie nicht die Möglichkeit haben, die Metadaten der DFN AAI Föderation regelmäßig automatisiert zu beziehen, z. B. da Ihr Dienst keinen Zugang zur Außenwelt hat oder es die SP-Anwendung nicht ermöglicht, müssen Sie Ihrem SP die IdP-Metadaten manuell zur Verfügung stellen. Die Metadaten des IdP der TU Dresden können Sie wie folgt beziehen:
- Vom IdP der TU Dresden selber: [2]https://idp.tu-dresden.de/idp/shibboleth
- Über die Föderation:
[3]https://met.refeds.org/met/entity/https://idp.tu-dresden.de/idp/shibboleth/

Verwenden Sie diese Option, so sind Sie davon abhängig, dass die IdP-Betreiber Sie, bei einem anstehenden Zertifikatswechsel, benachrichtigen. Es kommt zur Störung, wenn diese Benachrichtigung übersehen oder nicht beachtet wird. Das Zertifikat muss innerhalb einer Übergangszeit, in der vom IdP beide Zertifikate (alt und neu) angeboten werden, ausgetauscht werden.
Weitere Informationen siehe: IdP Zertifikatswechsel TU Dresden.
IdP Zertifikatswechsel TU Dresden Ein Zertifikatswechsel des IdP der TU Dresden wird in der Regel allen bekannten SP über die uns bekannten Kontakte im Voraus angekündigt. Mit Erhalt der Ankündigung enthalten die IdP-Metadaten bereits das neue Zertifikat. Der Zertifikatswechsel wird mindestens für 14 Tage im voraus angeboten. Während dieser Zeit ist der Betrieb mit beiden Zertifikaten möglich.
Hinweis: Sofern Ihr SP nicht die Möglichkeit besitzt beide Zertifikate parallel für einen Zertifikatswechsel zu verwenden, so verwenden sie bitte das neue Zertifikat (cert_idp.tu-dresden.de.pem), was in diesem FAQ angehangen ist.

[1] Metadaten-Übersicht der DFN AAI Föderation:
[4]https://doku.tid.dfn.de/de:metadata
[2] IdP-Metadaten: [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