Zugangsschutz

SAML

SAML-Authentifizierung mit Microsoft Entra ID- Microsoft Entra | Microsoft Learn

Für SAML muss der Dienstleister pro Applikation die Informationen als Entra ID kompatible Metadaten File für SAML oder alternativ die Felder „Identifier (Entity ID)“sowie „Reply URL (Assertion Consumer Service URL)“ liefern. Weiter ist es verpflichtend, dass eine „Sign on URL“ geliefert wird, die direkt den SAML-Aufruf durchführt, um ein Single Sign On bereitstellen zu können.
Die Attributes und Claim sind wie in Kriterium 3.4 / 4 mit der IT des Helmholtz Zentrum München abzustimmen.
Das Helmholtz Zentrum München stellt für SAML das Token „signing certificate“ mit einer Gültigkeit von maximal 3 Jahren zur Verfügung. Ein Austausch des Zertifikats muss ohne zusätzliche Kosten binnen 3 Tagen gewährleistet sein.

OpenID Connect

OpenID Connect-Authentifizierung mit Microsoft Entra ID- Microsoft Entra | Microsoft Learn

Für den Einsatz von OpenID Connect sind vorab die angeforderten Permissions zu definieren und mit Compliance und der IT abzustimmen. Es gilt immer der Ansatz so viel wie nötig, so wenig wie möglich.
Der Dienstleister hat einen Redirect URI zu liefern, sowie die Information, ob ID oder Access Tokens benötigt werden.
Im Anschluss zu den Informationen stellt die IT die Endpoints, Tennant ID, Application (client) ID sowie ein Secret als Temporären Link zur Verfügung. Das Secret darf nur im Zielsystem verschlüsselt gespeichert werden. Unverschlüsselte Speicherung, Benutzung eines Secrets in mehreren Applikationen ist unzulässig.

Oauth 2.0

OAuth 2.0-Autorisierung mit Microsoft Entra ID- Microsoft Entra | Microsoft Learn

Für den Einsatz von OAuth 2.0 sind vorab die angeforderten Permissions zu definieren und mit Compliance und der IT abzustimmen. Es gilt immer der Ansatz so viel wie nötig, so wenig wie möglich.
Der Dienstleister muss dem Auftraggeber einen Redirect URI liefern und die Information, ob ID oder Access Tokens benötigt werden.
Im Anschluss zu den Informationen stellt die IT die Endpoints, Tennant ID, Application (client) ID sowie ein Secret als temporären Link zur Verfügung. Das Secret darf nur im Zielsystem verschlüsselt gespeichert werden. Unverschlüsselte Speicherung, Benutzung eines Secrets in mehreren Applikationen ist unzulässig.