IT.NRW
Information und Technik Nordrhein-Westfalen

Föderierte Identitäts-Infrastruktur für NRW
ADFS – Active Directory Federation Services

Hintergrund

Bei IT.NRW wird eine Infrastruktur zum Betrieb von Applikationen (Verfahren) mit hohem Schutzbedarf betrieben[redacted]. Die darin genutzten Verzeichnisdienste (Microsoft Active Directory) verfügen über **keine Verbindungen** zu Verzeichnisdiensten außerhalb dieser Umgebung.

Für behördliche Anwender*innen (im Landesverwaltungsnetz **LVN**, aber außerhalb von IT.NRW) ermöglicht IT.NRW eine Authentifizierung und ein Single-Sign-On mittels Microsoft Active Directory Federation Services (kurz: **ADFS**).

Hiermit wird eine sichere, **Claim-basierte** Authentifizierung und je nach Bedarf auch Autorisierung jener „externer" Anwender*innen (fremder Behörden-ADs) gegenüber den bei IT.NRW intern betriebenen Anwendungen im hohen Schutzbedarf ermöglicht.

Infrastruktur

Eine sogenannte „Federation" besteht aus zwei Parteien, dem „Identity Provider" und dem „Application Provider".

- Der **Identity Provider** verwaltet die Benutzerkonten der Anwenderinnen / der Anwender (hier: Landesbehörden).
- Der **Application Provider** stellt die Anwendungen zur Verfügung.
  In dem hier betrachteten Kontext ist IT.NRW als Application Provider zu verstehen, der zentral Anwendungen für die Nutzerinnen / Nutzer der Landesbehörden in NRW betreibt.

Zwischen den behördlichen Identity Providern und dem Application Provider bei IT.NRW sind jeweils **Vertrauensbeziehungen** eingerichtet.

Darüber hinaus muss für **jede Anwendung**, auf die per ADFS zugegriffen werden soll, eine Vertrauensbeziehung als Schnittstelle zwischen der eigentlichen Anwendung und dem Application Provider etabliert werden.

Über diese Schnittstelle können in einem **Sicherheitstoken** verschiedene Informationen über die anfragende Identität (den/die behördlichen Nutzer*in) als Ansprüche (Claims) versendet werden.

Schnittstelle

Die folgenden Claims wurden für IT.NRW als „erweitertes Standard-Claim-Set“ definiert. Weitere Ansprüche und Anspruchstypen können nach Rücksprache mit IT.NRW realisiert werden.

CLAIM	ATTRIBUT AUS AD	BEMERKUNG
givenname	givenName	Vorname
surname	sn	Nachname
emailaddress	Mail	E-Mail Adresse
upn	User-Principal-Name	Benutzerprinzipalname für Kerberos
objektID	objectGUID	zur eindeutigen Identifikation, als Base64-enkodierter String
mandantID	mail	4stelliger alphanumerischer String, der jede Behörde eindeutig identifiziert. Wird von IT.NRW vergeben.
displayname	displayName	Anzeigename
Access	<flexibel>	wird zwingend verwendet, um den Zugriff auf eine Applikation zu erlauben bzw. zu verweigern
<App<n>>_Perm	<flexibel>	wird optional verwendet, um Zugriffe innerhalb der Applikation zu steuern

[redacted]

[redacted]