

SAML

Inhaltsverzeichnis

- [1 Funktionsweise](#)
- [2 Typische Einsatzbereiche](#)
- [3 Wichtige Hinweise](#)
- [4 Fazit](#)

SAML (Security Assertion Markup Language) ermöglicht Single Sign-On zwischen Identity Provider und Anwendungen über XML-basierte Assertions. Es ist in Unternehmensumgebungen weit verbreitet.

1 Funktionsweise

Der Benutzer meldet sich am IdP an; dieser stellt eine signierte Assertion aus, die die Service Provider-Anwendung akzeptiert und daraus die Sitzung ableitet.

- **IdP:** zentrale Authentifizierung
- **SP:** angebundene Anwendung
- **Assertion:** Aussagen zu Identität und Attributen

2 Typische Einsatzbereiche

- Unternehmens-SSO für SaaS und interne Portale
- Föderierte Anmeldung zwischen Organisationen
- Zentrale MFA-Durchsetzung am IdP

3 Wichtige Hinweise

- Zertifikate, Metadata und Entity-IDs müssen gepflegt werden.
- Uhrzeitabweichungen brechen häufig SAML-Logins.
- Neben SAML ist OIDC oft die modernere Web-Alternative.

4 Fazit

SAML bleibt ein tragender SSO-Standard in Enterprise-Landschaften – robust, aber mit spürbarem Integrations- und Zertifikatsaufwand.