

SSTL-01 Identity- und Access-Management (Microsoft Active Directory oder LDAPS)

Schnittstellensteckbrief

Anzubindendes Verfahren:	Microsoft Active Directory oder LDAPS
Hersteller des Drittsystems:	Microsoft
Technologie/Datenbank des anzubindenden Systems:	<p><u>Beschreibung:</u></p> <p>Microsoft Active Directory stellt einen zentralen Verzeichnisdienst zur Verwaltung von Benutzer-, Gruppen- und Computerobjekten in einer Domänenumgebung bereit.</p> <p>Hat das anzubindende System Webservice-Funktionalität? ja</p> <p>Export- und Importfunktionalitäten stehen zur Verfügung? ja</p> <p>View-basierte Anbindung kann durch Anwendungsbetreuer bereitgestellt werden? nein</p>
Systembetrieb:	<p><u>Beschreibung:</u></p> <ul style="list-style-type: none"> System wird On-Premises betrieben <p>Management der Serverinfrastruktur erfolgt durch: SfH</p>
Zweck und Kurzbeschreibung der zukünftigen Anbindung:	<p>Für die zukünftige HR-Software sollen eine Schnittstellen zum Microsoft Active Directory (AD) realisiert werden:</p> <ol style="list-style-type: none"> Single Sign-On (SSO) über Microsoft Active Directory Federation Services (ADFS): Nach Anmeldung am Windows-System wird über ADFS eine SSO-Integration realisiert. Dadurch wird beim Zugriff auf die HR-Software erkannt, ob bereits eine gültige Authentifizierungssitzung vorliegt. In diesem Fall erfolgt der Zugriff ohne erneute Anmeldung. Direkte Authentifizierung über LDAPS: Falls SSO nicht möglich ist, erfolgt nach manueller Eingabe der Anmeldedaten in der HR-Software eine Authentifizierungsanfrage über LDAPS an das Microsoft Active Directory. Die eingegebenen Benutzerdaten werden dabei validiert, und das Ergebnis wird an die HR-Software zurückgegeben.
Beschreibung der aktuellen	<ul style="list-style-type: none"> Die Schnittstelle existiert bei der SfH aktuell nicht, da

Systemanbindung (IST-Stand):	noch keine HR-Management Lösung im Einsatz ist.
Beschreibung der gewünschten Systemanbindung (SOLL-Stand):	<ul style="list-style-type: none"> ▪ Die Anbindung der HR-Software an das Microsoft Active Directory erfolgt auf einem der nachfolgenden Wege: ▪ über Active Directory Federation Services (ADFS) wird ein Single Sign-On realisiert. Dadurch erkennt die HR-Software bei Zugriff automatisch aktive Windows-Sitzungen, und eine erneute Anmeldung ist nicht erforderlich. ▪ alternativ erfolgt eine direkte Authentifizierung per LDAPS. Dabei stellt die HR-Software eine Authentifizierungsanfrage an das Active Directory. Die eingegebenen Benutzerdaten werden anhand hinterlegter Benutzerattribute geprüft und validiert.
Kommunikation:	<ul style="list-style-type: none"> ▪ Bidirektional (Authentifizierungsanfrage und Rückmeldung)
Datenart (Eingang):	<ul style="list-style-type: none"> ▪ Authentifizierungsdaten
Datenart (Ausgang):	<ul style="list-style-type: none"> ▪ Validierte Nutzerdaten
Datenaustauschform und -format:	<ul style="list-style-type: none"> ▪ Webservice (z. B. SAML via ADFS) ▪ Datenbankanbindung (LDAPS)
Rhythmus der Datenübergabe:	<ul style="list-style-type: none"> ▪ Ereignisbezogen/Echtzeit
Geschätzte Anzahl Datensätze:	<ul style="list-style-type: none"> ▪ Sämtliche Nutzende
Abhängigkeiten von / zu Drittsystemen oder manueller Zuarbeit:	<ul style="list-style-type: none"> ▪ Keine
Relevanz §9 DSGVO (Schutzbedarf der zu verarbeitenden Daten)	<ul style="list-style-type: none"> ▪ Hoch, verarbeitet werden personenbezogene Nutzerdaten Erfordert strenge technische und organisatorische Maßnahmen zum Datenschutz (z. B. verschlüsselte Übertragung, Rechtekonzepte)