Authentifizierung

Die folgenden Authentifizierungsmethoden stehen in IT-Systemen zur Verfügung:

Lokale Authentifizierung

IT-Systeme mit der lokalen Authentifizierungsmethode (LA) verwalten die Anmeldeinformationen lokal auf dem System. Auf dieser Art von IT-Systemen muss also eine Kombination aus Benutzername & Passwort erzeugt und gepflegt werden, Benutzer & Benutzerinnen erhalten also bei mehreren IT-Systemen dieser Art **möglicherweise mehrere Benutzernamen mit mehreren Passwörtern**.

- IT-Systeme mit der lokalen Authentifizierungsmethode verwenden individuelle Anmeldeinformationen
- Benutzer & Benutzerinnen können mehrere Kombinationen aus Benutzernamen & Passwörtern erhalten
- Anmeldung an jedem IT-System erforderlich

Single Password

IT-Systeme mit der Single Password Authentifizierungsmethode (SP) befragen eine zentrale Benutzerverwaltung nach der Richtigkeit der eingebenen Anmeldeinformationen. Benutzer & Benutzerinnen verwenden bei dieser Art von IT-Systemen **immer denselben Benutzernamen und dasselbe Passwort**, lediglich der Benutzername hat in seltenen Fällen eine etwas abweichende Form (vgl. Standard- und Domänenanmeldung).

- IT-Systeme mit der Single Password Authentifizierungsmethode verwenden zentral gespeicherte Anmeldeinformationen
- Benutzer & Benutzerinnen erhalten genau eine Kombination aus Benutzername & Passwort
- Anmeldung an jedem IT-System erforderlich

Single Sign-On

IT-Systeme mit der Single Sign-On Authentifizierungsmethode (SSO) befragen einen zentralen Identitätsprovider nach der Richtigkeit der eingebenen Anmeldeinformationen. Benutzer & Benutzerinnen verwenden bei dieser Art von IT-Systemen **immer denselben Benutzername und dasselbe Passwort. Mittels Autorisierung sind diese Systeme zusätzlich in der Lage ihre Anmeldeinformationen an weitere Systeme durchzureichen**.

- IT-Systeme mit der Single Sign-On Authentifizierungsmethode verwenden einen Identitätsprovider zur Prüfung der Anmeldeinformationen
- Benutzer & Benutzerinnen erhalten genau eine Kombination aus Benutzername & Passwort
- Anmeldung nur einmalig innerhalb der Systemfamilien Kerberos und OAuth / OpenID Connect / SAML erforderlich

Multi-Faktor-Authentifizierung (MFA)

Bei der MFA wird die Anmeldung durch einen zusätzlichen Authentifizierungsfaktor abgesichert. Neben dem Benutzernamen und Passwort wird dabei ein weiterer Faktor benötigt, z. B. ein Einmalpasswort (TOTP), ein Hardware-Token oder eine biometrische bzw. passwortlose Anmeldung. MFA kann dabei mit verschiedenen Authentifizierungsmethoden kombiniert werden, beispielsweise mit SP oder SSO.

Die Verwendung von MFA erhöht die Sicherheit insbesondere dann, wenn ein Passwort kompromittiert wurde.

Bei einigen IT-Systemen ist MFA verpflichtend. In diesem Fall ist eine Anmeldung ohne eingerichtete MFA nicht möglich. Bei anderen IT-Systemen ist MFA freiwillig. Ist MFA für einen Account eingerichtet, wird der zusätzliche Faktor bei der Anmeldung abgefragt; ist kein MFA eingerichtet, ist eine Anmeldung weiterhin ohne MFA möglich.

IT-Systeme

Service	Authentifizierungsmethode	Bemerkungen
Collaboration Cloud	Single Password	
Datenlaufwerke	Single Password	Im PC-Verbundsystem: SSO - Kerberos
Dokumentenmanagement	Single Password	
Drucken	Single Password	Im PC-Verbundsystem: SSO - Kerberos
E-Mail - Exchange Online	Single Password	
eCampus	Single Password	
Moodle	SSO & MFA (falls bereits eingerichtet)	MFA wird verwendet, sofern für den Account eingerichtet
Multifunktionsgeräte	Single Password	Im PC-Verbundsystem: SSO - Kerberos
PC-Verbundsystem	SSO - Kerberos	
Plotten	Single Password	Im PC-Verbundsystem: SSO - Kerberos
Videokonferenz	SSO	
Virtuelle Desktops	Single Password	
VPN	Single Password & MFA (verpflichtend)	MFA ist für die Nutzung erforderlich
Zeiterfassung	SSO & MFA (falls bereits eingerichtet)	MFA wird verwendet, sofern für den Account eingerichtet

From:
https://hrz-admin-wiki.jade-hs.de/ - **HRZ-Admin-Wiki**

Permanent link:
https://hrz-admin-wiki.jade-hs.de/de/tp/uadm/authentication

Last update: **2026/08/27 12:12**