Universität Siegen

Zentrum für Informations- und Medientechnologie

Nutzungsbedingungen MFA

Version 1.1

Stand vom: 30. Januar 2026

An der Universität Siegen wird der Zugriff auf IT-Dienste durch ein stärkeres Authentifizierungsverfahren, die sogenannte Multi-Faktor-Authentifizierung (MFA), geschützt. Bei der Multi-Faktor-Authentifizierung wird zum Identitätsnachweis eines Nutzenden zusätzlich zur persönlichen Benutzerkennung, bestehend aus Benutzername und Passwort, eine weitere und insbesondere unabhängige Komponente, das sogenannte Token (z. B. Einmalpasswort-Token), abgefragt.

1. Die Berechtigung zur Nutzung eines Tokens besteht für Mitglieder und Angehörige der Universität Siegen sowie für sonstige Personen, denen auf Grundlage eines Vertrags, einer Beauftragung oder einer sonstigen Berechtigung der Zugriff auf IT-Dienste der Universität Siegen gewährt wurde (z. B. Dienstleister, Projektbeteiligte, Gäste) und ein von ihr/ihm zu nutzender Dienst eine Multi-Faktor-Authentifizierung voraussetzt. Nutzende erhalten das Token mittels:
    a) Ausgabe durch das Zentrum für Informations- und Medientechnologie (ZIMT) (Hardware-Token, z. B. YubiKey); gilt nur für Beschäftigte der Zentralverwaltung.
    b) Abruf im eduMFA-Portal der Hochschule (Software-Token); gilt für Beschäftigte, Studierende, Dienstleister und Gäste.
2. Das Token ergänzt die Benutzerkennung. Es darf nicht anderen Personen zugänglich gemacht werden. Die Weitergabe an einen Dritten ist nicht gestattet.
3. Die/Der Nutzende sollte ihr/sein Hardware-Token wie einen Dienstschlüssel stets mit sich führen. Das Token kann an einem verschlossenen Ort hinterlegt werden. Die/Der Nutzende muss sicherstellen, dass keine Zugangsdaten zusammen mit dem Token gelagert werden.
4. Software-Token sollten nicht auf demselben Gerät gespeichert sein, auf dem Kennwörter (z. B. Passwortmanager) gespeichert werden.
5. Die/Der Nutzende ist unter folgenden Bedingungen verpflichtet, das Token unverzüglich zu sperren oder vom Supportdesk sperren zu lassen:
    a) Die/Der Nutzende hat den Verdacht, dass ihr/sein Token verloren, gestohlen, offengelegt oder anderweitig kompromittiert bzw. missbraucht wurde.
    b) Das Token wurde verloren, gestohlen, offengelegt oder anderweitig kompromittiert bzw. missbraucht.
6. Die Token werden automatisch gesperrt, sobald die/der Nutzende nicht mehr berechtigt ist, die Token zu nutzen (z. B. bei Ausscheiden, Ende der Vertragsbeziehung). Hardware-Token sind spätestens innerhalb von 14 Tagen an die ausgebende Stelle zurückzugeben.
7. Die ausgebende Stelle ist berechtigt, das Token von Nutzenden zurückzuverlangen, sofern dieses vom Nutzenden (z. B. bei fehlender Berechtigung oder beim Austausch des Tokens) nicht mehr benötigt wird.

8. Die private Nutzung des dienstlich ausgegebenen Hardwaretokens (Absicherung privater Accounts, die nicht unmittelbar einen dienstlichen Bezug haben) ist gestattet, aber nicht empfehlenswert, da nach Rückgabe des Geräts eine Übertragung privater Schlüssel nicht möglich ist. Kommt es zu einem Konflikt zwischen dienstlicher und privater Nutzung (z. B. gemeinsam genutzter Slot), hat die dienstliche Nutzung Vorrang.