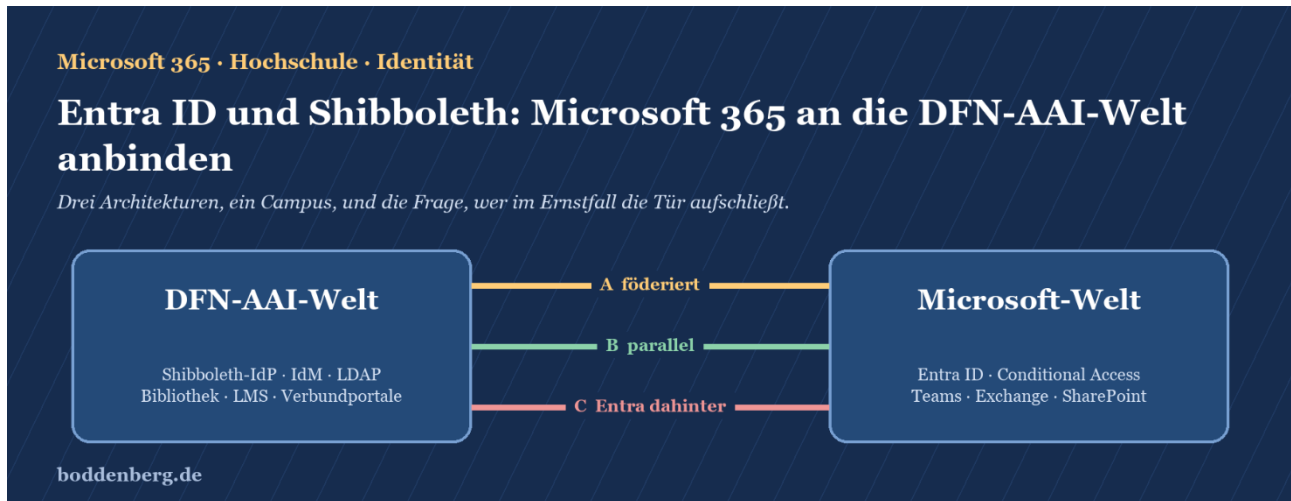


Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden



WISSEN

Alle Beiträge der Serie zu Microsoft 365 in Hochschule und Forschung an einem Ort.

› [Microsoft 365 in Hochschule und Forschung](#)

BERATUNG

Architekturentscheidung zwischen Shibboleth, DFN-AAI und Entra ID: Varianten bewerten, Pilot planen, Ausfall üben.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Rechenzentrum und Fakultäts-IT: Entra ID, Föderation und Conditional Access aus Sicht eines Shibboleth-Betriebs.

› [Schulungen für Hochschulen und Forschung](#)

Im Hochschulrechenzentrum gibt es Dinge, die man nicht anfasset, weil sie funktionieren. Der Shibboleth-IdP gehört dazu. Er läuft seit Jahren, er spricht mit der DFN-AAI, er gibt dem LMS, der Bibliothek, den Verlagsportalen und einem Dutzend Verbundprojekten genau die Attribute, die sie brauchen, und keine mehr. Der Kollege, der ihn eingerichtet hat, ist inzwischen vielleicht schon im Ruhestand, aber die Konfiguration ist dokumentiert, mehr oder weniger. Und dann beschließt das Präsidium Microsoft 365, und plötzlich steht ein zweiter Identitätsanbieter im Raum, der ebenfalls die Anmeldung für sich beansprucht.

Dieser Beitrag ist der technische Kern der Frage „Entra ID Shibboleth: wie passt das zusammen?“. Ausgangslage ist eine Hochschule oder Forschungseinrichtung, bei der Shibboleth-IdP und DFN-AAI gesetzt sind und Entra ID hinzukommt. Wir stellen drei Architekturvarianten gegeneinander: Shibboleth als föderierter Identitätsanbieter für Entra ID, Entra ID mit eigener Anmeldung per Kennwort-Hash-Synchronisierung parallel zum Shibboleth-IdP und Entra ID als Authentifizierungsquelle hinter dem Shibboleth-IdP. Für jede Variante klären wir, wo die MFA stattfindet, wie Conditional Access greift, was beim Ausfall passiert, wer welche Attribute sieht und wie viel Betrieb sie kostet. Am Ende ordnen wir noch die Altlast ADFS ein, die an manchen Einrichtungen still im Keller läuft.

Der Beitrag gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#). Wer zuerst wissen möchte, warum Identität an der Hochschule grundsätzlich komplizierter ist als in einem Unternehmen, liest vorher [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#). Universitätsklinika mit eigener KRITIS-Welt und allgemeinbildende Schulen sind hier ausdrücklich nicht gemeint, die haben ihre eigenen Sorgen.

FAKTEN · Auf einen Blick

Entra ID kann eine verifizierte Domäne mit einem SAML-2.0-Identitätsanbieter föderieren. Microsoft unterstützt dabei die Integration des Clouddienstes, nicht aber Bereitstellung, Konfiguration oder Fehlersuche des Drittanbieter-IdP.

Microsoft prüft unabhängige Identitätsanbieter inzwischen nicht mehr selbst auf Kompatibilität. Die Verantwortung für einen sauber konfigurierten Shibboleth-IdP liegt bei Ihnen.

Benutzerkonten müssen in Entra ID vorhanden sein, bevor sie sich föderiert anmelden können. Die SAML-NameID muss der ImmutableID des Kontos entsprechen, das Attribut IDPEmail dem Benutzerprinzipalnamen.

Ohne WS-Trust beim föderierten IdP stellt Entra ID auf eingebundenen Windows-Geräten kein Primary Refresh Token aus. Der Shibboleth-IdP spricht kein WS-Trust.

Föderation wird je Domäne eingerichtet, nicht je Benutzer. Das Umstellen einer Domäne kann laut Dokumentation bis zu zwei Stunden Beeinträchtigung bedeuten.

Zwei Welten, ein Benutzer: die Ausgangslage im Rechenzentrum

Die DFN-AAI ist eine SAML-Föderation. Hochschulen und Forschungseinrichtungen betreiben darin Identitätsanbieter, Dienstanbieter vom LMS bis zum Verlagsportal vertrauen ihnen über gemeinsam gepflegte Metadaten. In der Praxis heißt der Identitätsanbieter auf deutschen Campus fast immer Shibboleth. Er sitzt vor einem LDAP-Verzeichnis oder einem Active Directory, bezieht seine Daten aus einem Identity-Management-System, das wiederum vom Campus-Management und vom Personalsystem gespeist wird, und entscheidet je Dienst, welche Attribute freigegeben werden. Dieses Prinzip der sparsamen, gezielten Attributfreigabe ist eine der stillen Stärken der Föderation, und Datenschutzbeauftragte wissen es zu schätzen.

Entra ID ist ein anderes Modell. Es ist kein Föderationsteilnehmer, der Metadaten aus einem Aggregat liest, sondern ein Verzeichnis mit eigener Anmeldung, in dem jedes Konto als Objekt existieren muss. Microsoft 365 vertraut ausschließlich Entra ID. Wer also Teams, Exchange Online und SharePoint nutzen will, braucht Konten in Entra ID, egal, wie die Anmeldung technisch abläuft. Die Frage ist nur, wer das Kennwort prüft, wer die MFA fragt und wer im Ernstfall die Tür aufschließt.

Was sich nicht wegdiskutieren lässt

- **Konten in Entra ID sind Pflicht.** Auch bei vollständiger Föderation müssen Benutzerobjekte vorher angelegt werden, über Entra Connect, Cloud Sync, die API-gesteuerte eingehende Bereitstellung oder Skripte gegen Microsoft Graph. Das Identity Management bekommt also in jeder Variante ein weiteres Zielsystem.
- **Conditional Access lebt in Entra ID.** Egal, wer authentifiziert: Die Richtlinien für Microsoft 365 wertet Entra ID aus. Shibboleth kann vorher zusätzliche Hürden aufbauen, ersetzen kann es Conditional Access nicht.
- **Die DFN-AAI braucht weiterhin einen Föderationsteilnehmer.** Entra ID liest keine Metadaten-Aggregate und kennt keine Attributfreigabe nach Föderationsregeln. Der Shibboleth-IdP bleibt deshalb in allen drei Varianten bestehen.
- **Windows will mehr als SAML.** Für die Anmeldung an Entra-eingebundenen oder hybrid eingebundenen Windows-Geräten erwartet Entra ID bei föderierten Domänen WS-Trust vom Identitätsanbieter. Das wird bei Variante A noch wichtig.

WICHTIG · Koexistenz ist der Normalfall

Keine der drei Varianten schafft Shibboleth ab, und keine sollte es versuchen. Die DFN-AAI ist für

Lehre und Forschung unverzichtbar, und kein Rechenzentrum hat Lust, sämtliche Verlags- und Verbundanbindungen neu zu verhandeln, nur weil jemand Teams eingeführt hat. Die Frage lautet nicht „Shibboleth oder Entra ID“, sondern „wer macht was, und wer hängt von wem ab“. Wie diese Koexistenz bei den übrigen Campusdiensten aussieht, beschreibt [Microsoft 365 oder Open Source? Koexistenz mit BigBlueButton, Nextcloud, Moodle und Matrix](#).

Drei Architekturen im Detail

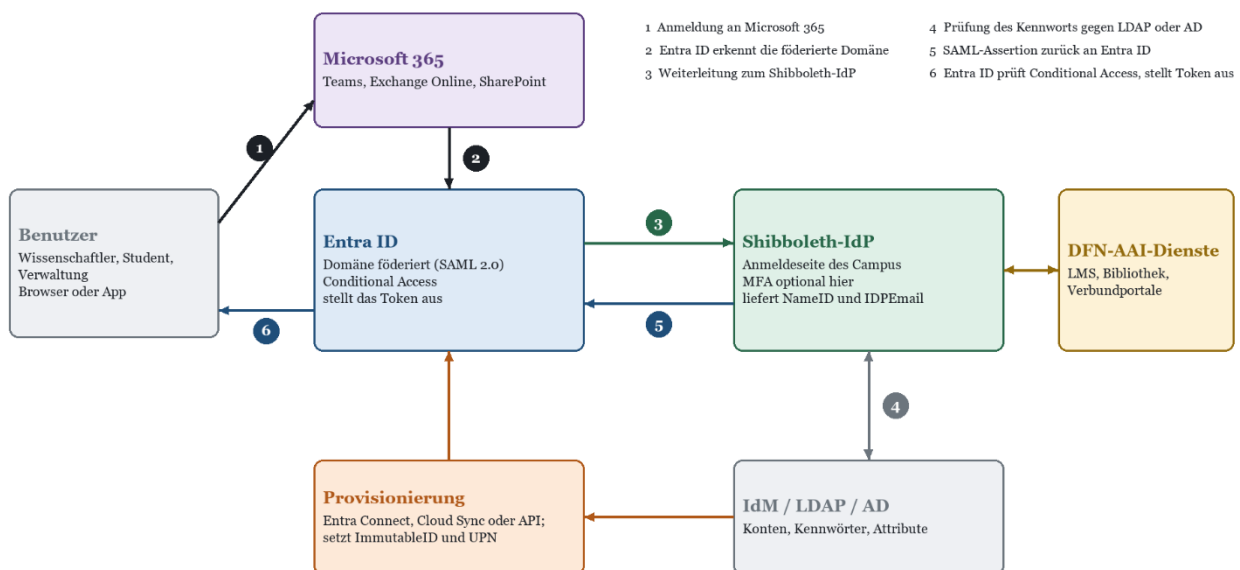
Die drei Varianten unterscheiden sich in einer einzigen Frage: Wer ist die Wurzel der Anmeldung? Alles andere, von der MFA bis zum Ausfallverhalten, folgt daraus. Wir beschreiben jede Variante nach demselben Raster, damit Sie am Ende nicht Äpfel mit Birnen vergleichen, sondern Äpfel mit leicht angefaulten Äpfeln.

Variante A: Shibboleth als föderierter Identitätsanbieter für Entra ID

Die Domäne der Hochschule wird in Entra ID von „veraltet“ auf „föderiert“ umgestellt, mit SAML 2.0 als Protokoll und dem Shibboleth-IdP als Identitätsanbieter. Gibt jemand bei der Microsoft-Anmeldung eine Adresse dieser Domäne ein, leitet Entra ID auf die vertraute Anmeldeseite des Campus weiter. Shibboleth prüft das Kennwort gegen LDAP oder AD und schickt eine signierte Assertion zurück. Entra ID stellt daraufhin das Token aus, nachdem es Conditional Access ausgewertet hat. Für die Anwender ist das elegant: eine Anmeldeseite, ein Kennwort, ein Logo.

Skizze 1: Variante A – Shibboleth als föderierter Identitätsanbieter

Die Domäne in Entra ID ist föderiert. Wer sich bei Microsoft 365 anmeldet, landet auf der Anmeldeseite des Shibboleth-IdP.



Fällt der Shibboleth-IdP aus, gibt es keine neue Anmeldung an Microsoft 365. Laufende Sitzungen tragen noch eine Weile.

Schematische Darstellung, vereinfacht. Hostnamen und Produkte beispielhaft.

Microsoft dokumentiert dieses Szenario auf Microsoft Learn unter dem Stichwort SAML-2.0-Identitätsanbieter mit SP-Lite-Profil. Die Formulierung zur Unterstützung ist bemerkenswert präzise: Microsoft unterstützt die Integration des Clouddienstes mit einem korrekt konfigurierten SAML-2.0-IdP, leistet aber keinen Support für Bereitstellung, Konfiguration und Fehlersuche des IdP selbst. Eine Validierung unabhängiger Identitätsanbieter findet nach Auskunft der Dokumentation nicht mehr statt. Übersetzt: Wenn die Anmeldung nicht geht, schauen beide Seiten zuerst einmal auf die jeweils andere.

Anforderung	Was Entra ID erwartet	Was das für Shibboleth heißt
NameID	Format persistent, Wert identisch mit der ImmutableID des Kontos in Entra ID	Eigene Attributdefinition, die genau den Wert liefert, den die Provisionierung als ImmutableID setzt. Nicht die DFN-AAI-üblichen pairwise-IDs.
IDPEmail	Benutzerprinzipalname des Kontos in Entra ID	Attribut mit dem UPN, der zur föderierten Domäne passt
Issuer	URI des IdP, je Domäne passend konfiguriert	entityID des Shibboleth-IdP; bei mehreren Domänen sauber planen
Bindings	HTTPS; HTTP-POST für Anfrage und Antwort, Redirect für die Abmeldung	Relying-Party-Konfiguration für Entra ID mit den Metadaten von Microsoft
Signatur	Assertion muss signiert sein; die Beispiele nennen SHA-1, die Dokumentation empfiehlt SHA-256	Signaturalgorithmus bewusst wählen und im Pilot testen
Metadaten	Entra ID liest keine IdP-Metadaten, Zertifikate werden per Microsoft Graph hinterlegt	Zertifikatswechsel am IdP ist ein manueller Termin im Kalender, keine Automatik

WARNUNG · Die Windows-Falle

Microsoft schreibt in der Dokumentation zum Primary Refresh Token ausdrücklich: Wer Entra ID mit einem Identitätsanbieter eines Drittherstellers föderiert, muss dort WS-Trust bereitstellen, sonst bekommen Benutzer auf Entra-eingebundenen und hybrid eingebundenen Windows-Geräten kein Primary Refresh Token. Ohne dieses Token fehlt die nahtlose Anmeldung an Office-Apps, Teams und Browser, und gerätebasierte Conditional-Access-Regeln laufen ins Leere.

Der Shibboleth-IdP bietet kein WS-Trust. Für Verwaltungsrechner, die mit Intune verwaltet und in Entra ID eingebunden werden sollen, ist Variante A deshalb eine Sackgasse, jedenfalls für die Domäne, mit der sich diese Benutzer anmelden.

Auch die Liste der Clients, die Microsoft für dieses Szenario aufführt, sollten Sie lesen, und zwar mit einer Tasse Tee und einem gewissen Sinn für Industriegeschichte. Dort finden sich Outlook 2010 und Windows Phone 7. Moderne Clients mit browserbasierter Anmeldung durchlaufen in der Praxis denselben passiven Ablauf wie das Web. Was im Einzelnen funktioniert, gehört trotzdem in einen Pilot mit jeder Client-Art, die an Ihrem Campus vorkommt, vom Verwaltungsrechner über das private Tablet des Studenten bis zum Linux-Notebook im Institut.

MFA, Conditional Access und Ausfall bei Variante A

Die MFA kann an zwei Orten stattfinden. Entweder fragt der Shibboleth-IdP den zweiten Faktor ab, etwa über ein vorhandenes Token-Verfahren des Rechenzentrums, oder Entra ID übernimmt die MFA nach der föderierten Anmeldung. Gesteuert wird das über die Einstellung `federatedIdpMfaBehavior` der Domänenföderation: Entra ID kann die MFA des IdP akzeptieren und nur bei Bedarf selbst nachfordern, sie beim IdP erzwingen oder sie grundsätzlich ablehnen und immer selbst prüfen. Ist nichts gesetzt, akzeptiert Entra ID eine MFA des föderierten IdP und fordert sonst selbst eine an. Damit Entra ID eine Shibboleth-MFA überhaupt als solche erkennt, muss der IdP sie in der Assertion in einer Form signalisieren, die Entra ID versteht. Das ist Konfigurationsarbeit und gehört in den Pilot, nicht in die Annahmen.

Conditional Access funktioniert für föderierte Benutzer wie für alle anderen, mit der genannten Einschränkung bei gerätebasierten Regeln auf Windows. Beim Ausfall gilt eine harte Regel: Ist der Shibboleth-IdP nicht erreichbar, gibt es keine neue Anmeldung an Microsoft 365. Bestehende Sitzungen und Token laufen noch eine Weile weiter, bis sie erneuert werden müssen. Eine

Kennwort-Hash-Synchronisierung als Rückfallebene ist nur möglich, wenn die Konten aus einem Active Directory kommen, und das Umschalten der Domäne von föderiert auf verwaltet dauert laut Microsoft bis zu zwei Stunden. Ein Notfallschalter ist das nicht, eher ein Notfallplan mit Wartezeit.

Die Attributfreigabe ist bei Variante A übersichtlich: Shibboleth liefert an Entra ID im Kern NameID und IDPEmail. Die eigentlichen Profildaten kommen über die Provisionierung. Die Betriebslast verlagert sich auf den Shibboleth-IdP, der zur kritischen Komponente für Microsoft 365 wird, mit allem, was das für Hochverfügbarkeit, Wartungsfenster und Bereitschaft bedeutet.

TYPISCHE SITUATION · Typische Situation: der Identitätsanbieter als Nadelöhr

Aus Projekten bei öffentlichen Auftraggebern, etwa einer Stadtverwaltung mit eigenem Föderationsdienst, kennen wir das Muster: Der vorgeschaltete Identitätsanbieter lief jahrelang als Einzelsystem, weil die angebundenen Fachverfahren einen Ausfall von einer Stunde verkraften konnten. Mit der Föderation von Microsoft 365 wurde aus dem Einzelsystem über Nacht der einzige Weg zu Mail, Kalender und Telefonie. Der erste Patchtag ohne Wartungsfenster fiel entsprechend lebhaft aus.

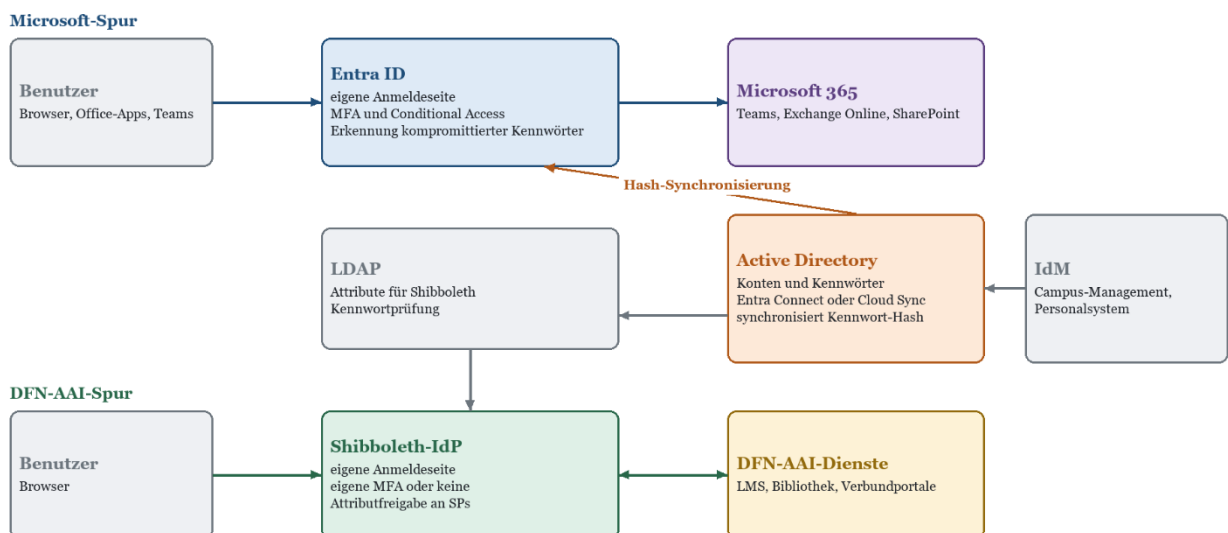
Übertragen auf die Hochschule: Wer Variante A wählt, muss den Shibboleth-IdP mindestens so verfügbar betreiben wie den Mailserver, den er indirekt ersetzt. Das kostet Server, Monitoring und Bereitschaftsregelungen, und es sollte im Betriebskonzept stehen, bevor die Domäne umgestellt wird.

Variante B: Entra ID mit eigener Anmeldung parallel zum Shibboleth-IdP

Bei Variante B bleibt die Domäne in Entra ID verwaltet. Entra Connect oder Cloud Sync synchronisiert Konten aus dem Active Directory und dazu einen abgeleiteten Hash des Kennworts, sodass Entra ID die Anmeldung selbst prüfen kann. Der Shibboleth-IdP arbeitet unverändert weiter und bedient die DFN-AAI. Für Anwender heißt das: ein Kennwort, aber zwei Anmeldeseiten, je nachdem, ob sie gerade in Teams oder im LMS unterwegs sind.

Skizze 2: Variante B – Entra ID mit eigener Anmeldung parallel zu Shibboleth

Zwei Anmeldewege, ein Kennwort: Der Hash kommt per Synchronisierung in die Cloud, der Shibboleth-IdP bleibt für die DFN-AAI zuständig.



Zwei Anmeldeseiten, zwei Sitzungen, zwei MFA-Welten. Fällt eine Seite aus, läuft die andere weiter.

Schematische Darstellung. Ob LDAP und AD getrennte Verzeichnisse sind oder eines, unterscheidet sich von Hochschule zu Hochschule.

Diese Variante ist das, was Microsoft für die meisten Organisationen als Standard vorsieht, und sie hat handfeste technische Vorteile. Die Anmeldung an Windows-Geräten mit Primary Refresh Token funktioniert, Hybrid Join funktioniert ohne Föderationsserver, und Entra ID kann laut Dokumentation durch die Hash-Synchronisierung Kennwörter erkennen, die in öffentlich aufgetauchten Zugangsdatensammlungen stehen. An einem Campus mit Zehntausenden Konten, von denen ein erheblicher Teil mit demselben Kennwort auch beim Pizzadienst angemeldet ist, ist das kein Luxus.

Die Voraussetzung ist ein Active Directory als Quelle der Kennwörter. Viele Hochschulen haben eines, aber nicht für alle Personengruppen: Studentenkonten leben an manchen Einrichtungen ausschließlich im LDAP. Dann bleibt die Wahl, die Studentenkonten ins AD zu bringen, sie als reine Cloudkonten mit eigenem Kennwort zu führen oder für diese Gruppe eine andere Variante zu wählen. Da die Föderation an der Domäne hängt, lassen sich Varianten je Domäne kombinieren, etwa verwaltete Anmeldung für die Domäne der Mitarbeiterinnen und Mitarbeiter und eine andere Lösung für die Studentendomäne. Das muss sauber geplant werden, damit niemand mit der falschen Adresse an der falschen Tür steht.

HINWEIS · Kennwort-Hash in der Cloud: eine Frage für Datenschutz und Gremien

Bei Variante B verlässt ein abgeleiteter Hash des Kennworts das Rechenzentrum. Technisch ist das kein Klartext, organisatorisch ist es trotzdem eine Verarbeitung, die in Verzeichnis der Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung und gegebenenfalls Dienstvereinbarung gehört. Wie die Datenschutzaufsicht Ihres Landes dazu steht und welche Beteiligungsrechte Ihr Personalvertretungsgesetz vorsieht, unterscheidet sich je Bundesland. Dieser Kasten ist keine Rechtsberatung; die Einordnung gehört zu Ihrer oder Ihrem Datenschutzbeauftragten.

› [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)

MFA, Conditional Access und Ausfall bei Variante B

Die MFA für Microsoft 365 findet in Entra ID statt, gesteuert über Conditional Access mit allen Möglichkeiten, von Authenticator über FIDO2-Schlüssel bis zu Windows Hello for Business. Der Shibboleth-IdP hat seine eigene MFA oder keine. Das Ergebnis sind zwei MFA-Welten mit unterschiedlichen Verfahren, Registrierungen und Helpdesk-Prozessen. Wer das vermeiden will, braucht eine bewusste Entscheidung, welche Welt welches Verfahren nutzt, und eine Kommunikation, die Studenten im ersten Semester nicht überfordert.

Beim Ausfall ist Variante B die gutmütigste: Fällt der Shibboleth-IdP aus, laufen Microsoft 365 und die Anmeldung daran unverändert weiter. Fällt das lokale AD aus, prüft Entra ID weiterhin gegen den synchronisierten Hash. Ist Entra ID gestört, arbeitet die DFN-AAI-Welt weiter. Nur Kennwortänderungen brauchen eine Weile, bis sie auf beiden Seiten angekommen sind, und das sollte der Helpdesk wissen, bevor sich der erste Professor beschwert, dass das neue Kennwort „nur halb“ funktioniert.

Bei der Attributfreigabe bleibt alles beim Alten: Shibboleth gibt wie bisher an DFN-AAI-Dienste frei, Entra ID erhält seine Daten ausschließlich über die Synchronisierung. Die Betriebslast entsteht bei der Synchronisierung und beim doppelten MFA-Betrieb, nicht bei einer zusätzlichen Hochverfügbarkeitsanforderung an Shibboleth.

TIPP · Kerberos im Verwaltungsnetz nicht vergessen

Die Anmeldung an domänengebundenen Rechnern in Verwaltung und Bibliothek läuft unabhängig von allen drei Varianten über Kerberos gegen das AD, ebenso der Zugriff auf Dateiserver und

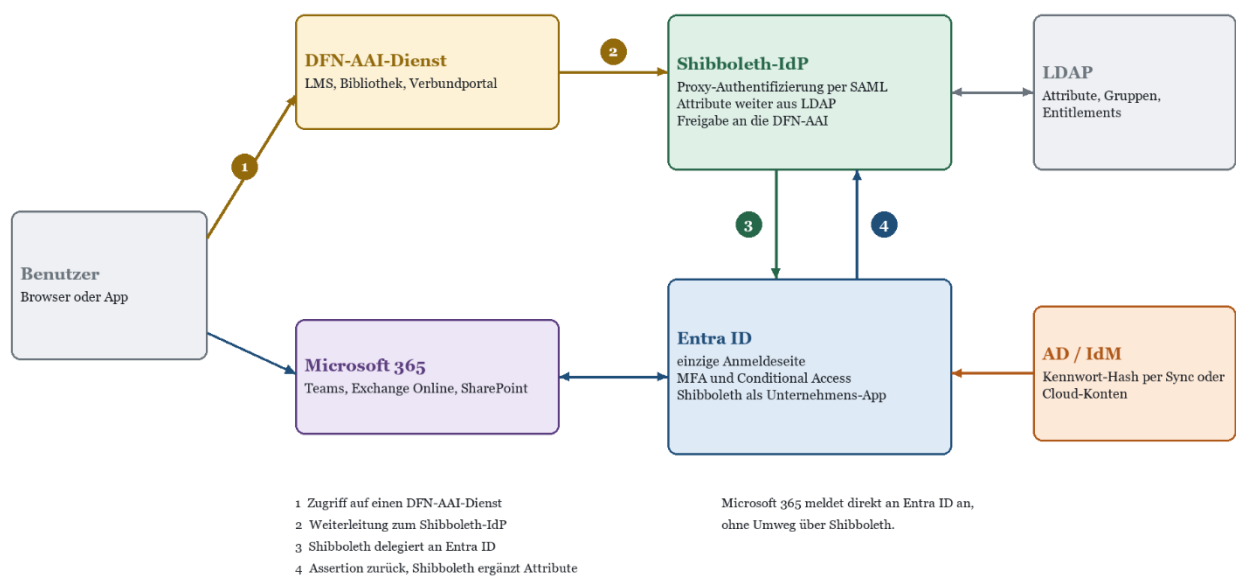
Drucker. Wer Geräte in Entra ID einbindet und trotzdem auf lokale Ressourcen zugreifen will, landet bei Fragen wie Cloud Kerberos Trust und Kerberos-Tickets für Entra-eingebundene Geräte. Die Grundlagen dazu finden Sie im [Kompetenzbereich Kerberos](#).

Variante C: Entra ID als Authentifizierungsquelle hinter dem Shibboleth-IdP

Variante C dreht die Rollen um. Entra ID wird zur einzigen Stelle, an der Kennwort und zweiter Faktor geprüft werden. Der Shibboleth-IdP bleibt Föderationsteilnehmer in der DFN-AAI, delegiert aber die eigentliche Authentifizierung per SAML an Entra ID, indem er dort als Unternehmensanwendung eingetragen ist. Nach der Rückkehr der Assertion löst Shibboleth die Attribute wie gewohnt aus LDAP auf und gibt sie nach den bekannten Regeln an die Dienstanbieter frei. Aktuelle Shibboleth-IdP-Versionen bringen diese Proxy-Authentifizierung mit.

Skizze 3: Variante C – Entra ID als Authentifizierungsquelle hinter Shibboleth

Der Shibboleth-IdP bleibt das Gesicht zur DFN-AAI, delegiert die eigentliche Anmeldung aber per SAML an Entra ID.



Entra ID wird zur Wurzel der gesamten Webanmeldung. Ist Entra ID gestört, stehen auch Bibliothek und LMS vor verschlossener Tür.

Schematische Darstellung. Die Proxy-Authentifizierung ist Bestandteil aktueller Shibboleth-IdP-Versionen, die Details sind Konfigurationsarbeit.

Der Reiz liegt auf der Hand: eine Anmeldeseite, eine MFA, ein Satz Conditional-Access-Regeln für alle Webdienste, auch für die DFN-AAI. Wer eine MFA-Pflicht für den Zugriff auf Prüfungsverwaltung oder Forschungsdatenportale über die DFN-AAI durchsetzen will, bekommt das bei Variante C mit den Mitteln von Entra ID, ohne einen zweiten MFA-Dienst zu betreiben. Shibboleth kann eine in Entra ID erfolgte MFA prinzipiell gegenüber den Diensteanbietern signalisieren, sofern das Mapping des Authentifizierungskontexts konfiguriert wird. Auch das ist kein Häkchen, sondern Arbeit.

Der Preis ist ebenso offensichtlich. Entra ID wird zur Wurzel der gesamten Webanmeldung. Ist Entra ID gestört oder sperrt eine Conditional-Access-Regel versehentlich zu viel, stehen nicht nur Teams und Mail, sondern auch LMS, Bibliothek, Verlagsportale und Verbundplattformen still. Dazu kommt eine Frage, die in Senat und Präsidium nicht nur technisch diskutiert wird: Die Anmeldung an Diensten, die mit Microsoft nichts zu tun haben, läuft dann über einen Microsoft-Clouddienst. Wer das Thema digitale Souveränität ernst nimmt, sollte diese Abhängigkeit bewusst

entscheiden und nicht als Nebenwirkung entdecken; mehr dazu in [Digitale Souveränität an Hochschulen: Was realistisch ist und was Sonntagsrede bleibt](#).

MFA, Conditional Access und Ausfall bei Variante C

Die MFA findet ausschließlich in Entra ID statt. Conditional Access greift für Microsoft 365 direkt und für DFN-AAI-Dienste indirekt, über die Unternehmensanwendung, die den Shibboleth-IdP repräsentiert. Entra ID sieht dabei nur, dass sich jemand am Shibboleth-IdP anmeldet, nicht an welchem Dienst dahinter. Eine Regel „MFA nur für das Prüfungsportal“ lässt sich deshalb nicht in Entra ID formulieren, sondern nur in Shibboleth, das gegebenenfalls eine erneute Anmeldung mit höherem Authentifizierungskontext anfordert.

Da Entra ID die Kennwörter selbst prüfen muss, braucht Variante C entweder Kennwort-Hash-Synchronisierung aus einem AD oder Cloudkonten mit eigenem Kennwort, idealerweise ergänzt um kennwortlose Verfahren. Im Ausfallverhalten ist sie das Gegenstück zu Variante A: Fällt Shibboleth aus, läuft Microsoft 365 weiter, die DFN-AAI steht. Fällt Entra ID aus, steht beides. Die Attributfreigabe bleibt im Shibboleth-IdP und damit unter Kontrolle des Rechenzentrums. Die Betriebslast ist gemischt: weniger eigene MFA-Infrastruktur, aber zwei Systeme, deren Zusammenspiel bei jeder Änderung getestet werden will.

HINWEIS · Anmeldeprotokolle und Mitbestimmung

Bei Variante C protokolliert Entra ID jede Anmeldung am Shibboleth-IdP, also auch Zeitpunkte, zu denen Wissenschaftler oder Verwaltungsmitarbeiter auf DFN-AAI-Dienste zugreifen. Bei Variante A und B entstehen ähnliche Protokolle für Microsoft 365. Ob und wie solche Daten zur Leistungs- oder Verhaltenskontrolle geeignet sind und was das für die Mitbestimmung bedeutet, regeln die Personalvertretungsgesetze der Länder unterschiedlich. Hier ist keine Rechtsberatung gemeint, sondern der Hinweis, das Thema früh mit dem Personalrat zu besprechen.

› [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)

Die Varianten im direkten Vergleich

Spätestens jetzt verlangt das Präsidium nach einer Tabelle, und es hat recht. Die erste Tabelle vergleicht die fünf Kriterien aus dem Raster, die zweite fasst Vorteile, Risiken und typische Einsatzfälle zusammen.

Kriterium	A: Shibboleth föderiert	B: parallel mit Hash-Sync	C: Entra ID hinter Shibboleth
MFA-Ort	Shibboleth oder Entra ID, gesteuert über federatedIdpMfaBehavior	Entra ID für Microsoft 365, Shibboleth separat für DFN-AAI	Entra ID für alles
Conditional Access	Ja, aber gerätebasierte Regeln auf Windows ohne WS-Trust eingeschränkt	Voller Funktionsumfang für Microsoft 365	Voller Umfang für Microsoft 365, für DFN-AAI nur pauschal über die Shibboleth-App
Ausfall Shibboleth	Keine neue Anmeldung an Microsoft 365 und DFN-AAI	Nur DFN-AAI betroffen	Nur DFN-AAI betroffen
Ausfall Entra ID	Microsoft 365 betroffen	Microsoft 365 betroffen	Microsoft 365 und DFN-AAI betroffen
Attributfreigabe	An Entra ID nur NameID und IDPEmail; Profildaten über Provisionierung	Unverändert; Entra ID nur über Synchronisierung	Unverändert in Shibboleth; Entra ID sieht jede IdP-Anmeldung

Betriebslast	Hoch beim Shibboleth-IdP: Verfügbarkeit, Zertifikate, Fehlersuche ohne Herstellersupport	Mittel: Synchronisierung, zwei MFA-Welten	Mittel bis hoch: Proxy-Konfiguration, Abhängigkeitsmanagement
---------------------	--	---	---

Variante	Vorteile	Risiken	Passt zu
A: Shibboleth föderiert	Eine vertraute Anmeldeseite; Kennwortprüfung bleibt vollständig im Haus; kein Kennwort-Hash in der Cloud	Kein Primary Refresh Token auf eingebundenen Windows-Geräten; Shibboleth wird kritisch für Microsoft 365; kein Herstellersupport für den IdP; Rückweg dauert	Einrichtungen, die Microsoft 365 überwiegend im Browser nutzen, kaum verwaltete Windows-Geräte haben und einen hochverfügbaren Shibboleth-Betrieb stemmen
B: parallel mit Hash-Sync	Voller Funktionsumfang von Entra ID; Ausfälle bleiben auf eine Welt begrenzt; Erkennung kompromittierter Kennwörter	Zwei Anmeldeseiten und zwei MFA-Welten; Kennwort-Hash in der Cloud; setzt AD als Kennwortquelle voraus	Die meisten Hochschulen und Institute mit AD, Intune-Plänen und dem Wunsch, die DFN-AAI unberührt zu lassen
C: Entra ID hinter Shibboleth	Eine MFA und ein Regelwerk für alle Webdienste; Attributfreigabe bleibt im Rechenzentrum	Entra ID als Single Point of Failure auch für die DFN-AAI; Souveränitätsdebatte; anspruchsvolle Konfiguration	Einrichtungen, die MFA für DFN-AAI-Dienste wollen, keinen eigenen MFA-Dienst betreiben möchten und die Abhängigkeit bewusst tragen

Skizze 4: Was steht still, wenn etwas ausfällt?

Neue Anmeldungen je Variante und Störfall. Bereits laufende Sitzungen und zwischengespeicherte Token sind nicht berücksichtigt.

	Shibboleth-IdP fällt aus	Entra ID gestört	LDAP / AD vor Ort fällt aus
A föderiert	M365: nein DFN-AAI: nein	M365: nein DFN-AAI: ja	M365: nein DFN-AAI: nein
B parallel	M365: ja DFN-AAI: nein	M365: nein DFN-AAI: ja	M365: ja DFN-AAI: nein
C Entra dahinter	M365: ja DFN-AAI: nein	M365: nein DFN-AAI: nein	M365: ja DFN-AAI: eingeschränkt

Rot: beide Welten betroffen. Gelb: eine Welt betroffen. Grün: Anmeldung geht, Attribute fehlen womöglich.

Variante B setzt voraus, dass der Kennwort-Hash bereits in Entra ID liegt. Variante C setzt bei LDAP-Ausfall voraus, dass Entra ID eigene Kennwörter kennt; Shibboleth kann dann aber keine Attribute aus LDAP auflösen.

eduroam läuft über RADIUS und hängt in keiner Variante an SAML, solange der RADIUS-Server nicht gegen Entra ID prüft.

Vereinfachte Betrachtung. Wer es genau wissen will, übt den Ausfall, statt ihn in der Matrix nachzuschlagen.

Mischformen und Übergänge

In der Praxis sieht man selten eine Variante in Reinform. Häufig beginnt eine Hochschule mit Variante B, weil sie schnell und gut dokumentiert ist, und denkt später über Variante C nach, wenn die MFA für Microsoft 365 etabliert ist und die Frage aufkommt, warum das LMS eigentlich weniger geschützt ist als der Kalender. Umgekehrt landen Einrichtungen, die mit Variante A gestartet sind, oft bei Variante B, sobald die ersten Verwaltungsrechner in Intune verwaltet werden sollen und die Windows-Falle zuschnappt.

Bei außeruniversitären Forschungseinrichtungen kommt eine weitere Ebene hinzu: Institute großer Forschungsgesellschaften hängen teils an einer zentralen Identitätsinfrastruktur, teils betreiben sie eigene Shibboleth-IdPs für die DFN-AAI. Welche Variante dort passt, hängt stark davon ab, wer den Tenant betreibt und wer die Föderation, siehe [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#). An Hochschulen mit starker Fakultäts-IT stellt sich dieselbe Frage im Kleinen, etwa wenn Institute eigene Anmeldewege für Speziallösungen betreiben, siehe [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#).

Die Altlast ADFS: warum der dritte Identitätsanbieter keine Lösung ist

An manchen Einrichtungen läuft neben Shibboleth noch ein ADFS-Server, eingerichtet in einer frühen Phase von Office 365, als föderierte Anmeldung noch als Königsweg galt. Gelegentlich wird ADFS auch als Brücke vorgeschlagen: ADFS spricht WS-Trust, löst also die Windows-Falle von Variante A, und könnte seinerseits gegen Shibboleth föderieren. Das funktioniert technisch, ist aber ein klassischer Fall von „Problem gelöst, drei neue gekauft“.

Microsoft empfiehlt seit Jahren, Anwendungen von ADFS zu Entra ID zu migrieren, und beschreibt dafür einen gestuften Migrationsweg. Die Unterstützung von Hybrid Join und Primary Refresh Token für föderierte Domänen ist in der Dokumentation auf ADFS zugeschnitten, inklusive der Warnung, bestimmte WS-Trust-Endpunkte auf keinen Fall ins Internet zu stellen. Wer ADFS behält, betreibt also eine weitere Server-Farm mit Zertifikaten, Web Application Proxy und Patchpflicht, die ausschließlich existiert, um zwei andere Identitätsanbieter miteinander zu versöhnen.

Situation	Empfehlung
ADFS föderiert die Domäne für Microsoft 365, Shibboleth bedient die DFN-AAI	Umstieg auf Variante B planen: Hash-Synchronisierung aktivieren, Pilotgruppen testen, Domäne auf verwaltet umstellen, ADFS zurückbauen
ADFS dient nur noch einzelnen Fachanwendungen	Anwendungen nach Entra ID oder Shibboleth umziehen, je nachdem, wer sie nutzt; danach abschalten
ADFS als Brücke zwischen Shibboleth und Entra ID im Gespräch	Erst prüfen, ob Variante B oder C das Ziel ohne dritten IdP erreicht; in aller Regel ist das der Fall
Niemand weiß, ob ADFS noch gebraucht wird	Anmeldeprotokolle auswerten, Vertrauensstellungen inventarisieren, Abschalttermin mit Rückfallplan setzen

TYPISCHE SITUATION · Typische Situation: der vergessene Föderationsserver

In einem Krankenhausverbund in kirchlicher Trägerschaft fand sich bei einer Bestandsaufnahme ein Föderationsserver, dessen Tokensignaturzertifikat in wenigen Wochen ablief. Niemand im aktuellen Team hatte ihn eingerichtet, drei Anwendungen hingen noch daran, eine davon unbemerkt geschäftskritisch. Die Migration war am Ende unspektakulär, die Wochen davor waren es nicht.

Übertragen auf die Hochschule: Ein ADFS aus der Office-365-Frühzeit ist kein Sammlerstück, sondern ein Risiko mit Ablaufdatum. Ein Inventar gehört in die Konzeptionsphase, nicht in die

Woche vor dem Zertifikatsablauf.

Vom Vergleich zur Entscheidung

Die Entscheidung zwischen den Varianten ist keine reine Technikfrage, sondern eine Abwägung zwischen Verfügbarkeit, Kontrolle, Funktionsumfang und Abhängigkeit. Sie gehört in ein Konzept, das Präsidium oder IT-Lenkungsgremium beraten können, und nicht in ein Ticket, das ein Administrator an einem Freitagnachmittag schließt. Wie eine solche Konzeptionsphase aufgebaut ist, beschreibt [Microsoft-365-Einführung an der Hochschule: Konzeptionsphase in 4,5 Tagen und die Vorlage fürs Präsidium](#).

Fragen, die vor der Entscheidung beantwortet sein sollten

- **Geräte:** Sollen Windows-Geräte in Verwaltung oder Instituten in Entra ID eingebunden und mit Intune verwaltet werden? Wenn ja, scheidet Variante A für die betroffene Domäne praktisch aus.
- **Kennwortquelle:** Liegen alle Kennwörter in einem AD, oder leben Studentenkonto nur im LDAP? Davon hängt ab, ob Hash-Synchronisierung für alle Gruppen möglich ist.
- **MFA-Strategie:** Gibt es bereits ein MFA-Verfahren im Rechenzentrum, und soll die DFN-AAI künftig ebenfalls MFA verlangen?
- **Verfügbarkeit:** Kann der Shibboleth-IdP so betrieben werden, dass er Microsoft 365 tragen kann? Und ist die Hochschule bereit, die DFN-AAI von Entra ID abhängig zu machen?
- **Datenschutz und Mitbestimmung:** Sind Kennwort-Hash, Anmeldeprotokolle und Attributflüsse mit Datenschutzbeauftragten und Personalrat besprochen?
- **Ausfallplan:** Wer entscheidet im Störfall, und ist der Rückweg geübt?

TIPP · Pilot mit echten Menschen

Testen Sie jede Variante mit einer Pilotgruppe, die die Vielfalt des Campus abbildet: Verwaltung mit verwalteten Windows-Rechnern, ein Institut mit Linux-Arbeitsplätzen, studentische Hilfskräfte mit privaten Smartphones, ein Gastwissenschaftler mit fremdem Notebook und ein Emeritus, der seine Mail seit zwanzig Jahren mit demselben Client abrufen. Wer nur das eigene Admin-Notebook testet, testet vor allem das eigene Admin-Notebook.

Wer die Entscheidung mit externer Unterstützung vorbereiten möchte, findet auf der Seite [Microsoft-365-Beratung für Hochschulen und Forschung](#) den Rahmen, in dem wir das mit Hochschulen und Forschungseinrichtungen angehen. Für das Rechenzentrumsteam, das Entra ID danach selbst betreiben soll, gibt es [Microsoft-365-Schulung für Hochschulen und Forschung](#).

Häufige Fragen

Unterstützt Microsoft die Föderation von Entra ID mit Shibboleth offiziell?

Microsoft unterstützt die Anmeldung an Microsoft 365 über einen korrekt konfigurierten SAML-2.0-Identitätsanbieter mit SP-Lite-Profil und dokumentiert die Protokollanforderungen auf Microsoft Learn. Für Bereitstellung, Konfiguration und Fehlersuche des Drittanbieter-IdP selbst leistet Microsoft keinen Support, und eine Kompatibilitätsprüfung unabhängiger Anbieter findet nicht mehr statt. Für Shibboleth sind Sie also selbst zuständig, mit der Community im Rücken.

Können wir Entra ID direkt als Identitätsanbieter in der DFN-AAI anmelden?

Entra ID ist nicht als Föderationsteilnehmer im Sinne der DFN-AAI gebaut: Es verarbeitet keine Metadaten-Aggregate und keine föderationsweiten Attributfreigaberegeln. Deshalb bleibt der Shibboleth-IdP in allen hier beschriebenen Varianten das Gesicht zur DFN-AAI.

Warum funktioniert die Windows-Anmeldung bei Variante A nicht sauber?

Für das Primary Refresh Token auf Entra-eingebundenen oder hybrid eingebundenen Windows-Geräten verlangt Entra ID bei föderierten Domänen WS-Trust vom Identitätsanbieter. Shibboleth bietet das nicht. Ohne das Token fehlen die nahtlose Anmeldung an Microsoft-365-Apps und die Grundlage für gerätebasierte Conditional-Access-Regeln.

Brauchen wir für Variante A trotzdem eine Synchronisierung?

Ja. Entra ID akzeptiert föderierte Anmeldungen nur für Konten, die bereits existieren und deren ImmutableID zur NameID der Assertion passt. Die Konten kommen über Entra Connect, Cloud Sync, die API-gesteuerte eingehende Bereitstellung oder Skripte gegen Microsoft Graph in den Tenant.

Können wir Studenten und Mitarbeiter unterschiedlich anbinden?

Grundsätzlich ja, weil die Föderation je Domäne eingerichtet wird. Liegen Studenten und Mitarbeiterinnen und Mitarbeiter auf unterschiedlichen Domänen, kann eine Domäne verwaltet und eine andere föderiert sein. Das erhöht allerdings die Komplexität im Helpdesk und sollte nur gewählt werden, wenn es einen echten Grund gibt.

Ist Variante C nicht einfach die modernste Lösung?

Sie ist die konsequenteste, nicht automatisch die beste. Eine MFA und ein Regelwerk für alle Webdienste sind attraktiv, aber dafür hängt die DFN-AAI vollständig an Entra ID. Ob eine Hochschule diese Abhängigkeit tragen will, ist eine strategische Entscheidung für Präsidium und Gremien.

Was ist mit eduroam?

eduroam authentifiziert über RADIUS und ist von den hier beschriebenen SAML-Varianten unabhängig, solange der RADIUS-Server gegen das lokale Verzeichnis prüft. Wer auch eduroam an Entra ID koppeln möchte, öffnet ein eigenes Kapitel.

Sollten wir ADFS als Zwischenschicht behalten?

In aller Regel nicht. Microsoft empfiehlt die Migration von ADFS zu Entra ID, und die Probleme, die ADFS als Brücke lösen soll, lassen sich meist mit Variante B oder C ohne dritten Identitätsanbieter lösen.

Fazit: Wer die Tür aufschließt, muss auch den Schlüssel hüten

Entra ID und Shibboleth schließen sich nicht aus, sie müssen sich nur einigen, wer wofür zuständig ist. Variante A hält die Kennwortprüfung vollständig im Haus, macht den Shibboleth-IdP aber zur kritischen Infrastruktur für Microsoft 365 und stolpert über Windows. Variante B ist der pragmatische Standard mit zwei Anmeldewelten, die sich gegenseitig nicht in den Abgrund ziehen. Variante C vereinheitlicht MFA und Regeln für alle Webdienste und bezahlt das mit einer Abhängigkeit, die man bewusst eingehen muss.

Für die meisten Hochschulen und Forschungseinrichtungen ist Variante B der vernünftige Startpunkt, Variante C eine Option für später, Variante A ein Sonderfall für Einrichtungen ohne verwaltete Windows-Geräte. ADFS ist in keiner dieser Geschichten der Held. Und wer sich nicht sicher ist, welche Variante passt, sollte den Ausfall jeder Variante einmal durchspielen, bevor er sie einführt. Die Matrix in Skizze 4 ist ein guter Anfang. Ein echter Testlauf an einem Dienstagvormittag in der vorlesungsfreien Zeit ist ein besserer.

WEITERLESEN • Weiterlesen

Die Serie zu Microsoft 365 in Hochschule und Forschung. Für diesen Beitrag besonders passend:

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#)
- › [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)
- › [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#)
- › [Digitale Souveränität an Hochschulen: Was realistisch ist und was Sonntagsrede bleibt](#)
- › [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#)
- › [Microsoft-365-Einführung an der Hochschule: Konzeptionsphase in 4,5 Tagen und die Vorlage fürs Präsidium](#)
- › [Kompetenzbereich Kerberos](#)
- › [Microsoft-365-Beratung für Hochschulen und Forschung](#)
- › [Microsoft-365-Schulung für Hochschulen und Forschung](#)