AR009 – Architekturrichtlinie Microsoft 365 im SD-Büroautomation. Beilage 1

Beilage zu einer IKT-Vorgabe

Sachtitel (der Beilage):	**Microsoft 365 Soll-Architektur im IKT Standarddienst Büroautomation**
Ausgabedatum dieser Beilage:[1]	07.05.2025
Gehört zu:	AR009, Version 1.0
Status der Weisung:	Genehmigt

[1] Das *Ausgabedatum* stimmt bei der Erstpublikation einer Beilage mit dem *Beschlussdatum* der genehmigten Version einer Weisung zur Bundesinformatik überein. Bei einer geringfügigen Änderung in der Beilage wird auf eine Anpassung der Version der Weisung verzichtet. Es ist lediglich das *Ausgabedatum* der Beilage anzupassen sowie die Änderung in *Anhang A der Beilage* festzuhalten.

Inhaltsverzeichnis

1 Microsoft 365 Soll-Architektur ... 3

1.1 Hybrides Cloud Modell ... 3
1.2 Netzwerkanbindung ... 4
1.3 Hybride SD Büroautomation Services ... 4

1.3.1 Hybrididentitäten ... 4

1.3.1.1 Benutzerkonten in Entra ID ... 4

1.3.1.2 Entra Connect Sync ... 5

1.3.1.2.1 Authentifizierungsmethoden ... 5

1.3.2 Exchange Hybrid ... 6

1.3.3 SharePoint Hybrid ... 7

1.3.4 Skype for Business mit Teams ... 7

1.3.4.1 Coexistence Modes ... 7

1.3.4.2 Telefonie Anbindung ... 8

1.4 Einbindung der Endgeräte ... 9

1.4.1 Co-Management ... 9

1.4.2 Geräteidentität ... 10

1.4.3 Authentifizierungsmethoden ... 10

1.4.4 Zugriffsmatrix ... 12

1.5 Stufen der Zusammenarbeit ... 16

1.5.1 Konfiguration mit B2B-Collaboration ... 18

Anhänge ... 19

A. Referenzen ... 19
B. Abkürzungen ... 19

1 Microsoft 365 Soll-Architektur

1. In dieser Beilage wird die Soll-Architektur mit Microsoft 365 im IKT-Standarddienst Büroautomation (SD/BA) beschrieben.
2. Wie das Hauptdokument ist auch die hier vorliegende Beilage verbindlich. Die Soll-Architektur beschreibt nur die wichtigsten Punkte, die insbesondere Einfluss auf die Kosten und Risiken (ISDS-Konzept) haben können.

1.1 Hybrides Cloud Modell

1. Im Zeitalter der digitalen Transformation wird die Flexibilität und Skalierbarkeit von Cloud-Computing-Modellen immer wichtiger. Insbesondere das hybride Cloud-Modell, das die Vorteile der öffentlichen und privaten Cloud kombiniert. M365 bietet diese hybride Cloud-Infrastruktur. Die lokalen SD Büroautomation Services, um M365 cloudbasierte Services zu erweitern, ermöglichen eine nahtlose Integration zwischen den verschiedenen Umgebungen.
2. Die folgende Architektur Abbildung MUSS durch den LE umgesetzt werden. Aufgrund der Integration von Auslandsstandorten in der Architektur des LE EDA, weicht die Implementierung mit den in der AR009 dokumentierten Differenzen leicht ab. Die Differenzen werden dem BK-DTI ausgewiesen. Die übergeordneten Architektureigenschaften werden jedoch entsprechend umgesetzt.

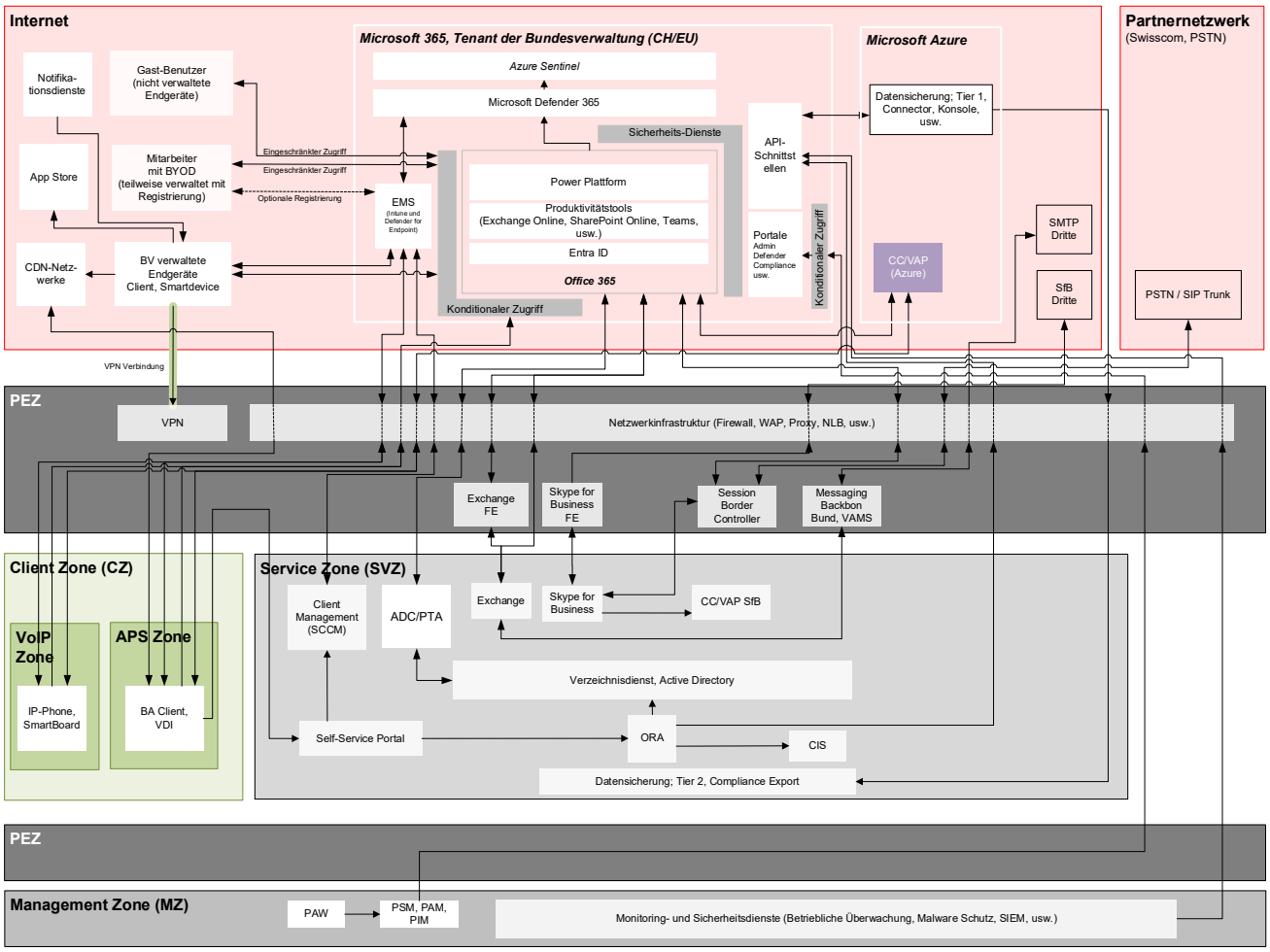


Abbildung 1: Hybrid Cloud Modell des SD/BA

1.2 Netzwerkanbindung

1. Für die Internetverbindung MÜSSEN die Dienste von SD DAKO, mit Ausnahme von Always-On-VPN, verwendet werden.
2. Die Anbindung mit Express Route KANN für die in der Liste von Microsoft[2] aufgeführten Verbindungen mit Unterstützung für Express Route (ER) verwendet werden, wenn hierfür ausreichend Bandbreite verfügbar ist.
3. Die Anbindung der ausländischen Niederlassungen (z.B. Botschaften) DARF entsprechend mittels DIA erfolgen (Direct Internet Access sowie OptiraEDA). Dort wo kein direkter Zugang zum Internet erlaubt ist (aus Sicherheitsgründen), MUSS dieser über die Schweiz erfolgen.

1.3 Hybride SD Büroautomation Services

1.3.1 Hybrididentitäten

#	Sync Mode	Soll-Architektur
1	Entra Connect Sync	MUSS
2	Entra ID Connect Cloud Sync	DARF NICHT

Tabelle 1: Hybrididentitäten

1.3.1.1 Benutzerkonten in Entra ID

1. Damit die M365 Anwendungen und Services genutzt werden können, bedingt es einem Benutzerkonto im Entra ID.
2. Die Tabelle zeigt welche Benutzerkonten verwendet werden DÜRFEN.

Typ	Benutzerkonto	Eigenschaften	Lokales AD[3]	Entra ID
Member	Hybrides Benutzerkonto der BA	Abgeklärte Identität Vertragsverhältnis mit der BV Benutzerkonto wird synchronisiert	X	X
Member	Konto für spezifische Nutzung	Spezifische Einsatzgebiete Unpersönliche Ressourcen Durchführen von Tests	(X); können Hybrid sein, müssen aber nicht	X

[2] Microsoft 365-URLs und-IP-Adressbereiche: Microsoft 365-URLs und-IP-Adressbereiche

[3] Lokales AD des SD/BA

Typ	Benutzerkonto	Eigenschaften	Lokales AD[3]	Entra ID
Guest für SD/BA	Gastkonto	Es MUSS eine Kollaborationsvereinbarung vorhanden sein [AR009, Kapitel 2.6] LifeCycle durch das ORA Einladung zur Zusammenarbeit durch den Typ Member (Bundesmitarbeiter), beschränkt auf die zur Zusammenarbeit eingeladene Ressource		X
Administratoren	Privilegierte Benutzerkonten	Administrative Tätigkeiten		X

Tabelle 2: Benutzertypen in Entra ID

1.3.1.2 Entra Connect Sync

1. Mit Entra Connect Sync MÜSSEN die vorhandenen und definierten Objekte vom lokalen Active Directory in das Entra ID synchronisiert. Die Synchronisation erfolgt in regelmässigen Abständen.
   a. Mit Entra Connect Sync DÜRFEN NUR persönliche Benutzerkonten ohne privilegierte Berechtigungen (z.B. Administratoren) synchronisiert werden (Konto Typ U- und X- der LE).
   b. Weitere Accounttypen (Bsp. Testkonto, Schulungskosten) DÜRFEN nur gemäss entsprechendem Konzept des LE synchronisiert werden. Die Freigabe erfolgt durch das zuständige Gremium gemäss Geschäftsorganisationskonzept des LE.
   c. Lokale Servicekonten (aka Serviceaccount) im SD/BA DÜRFEN NICHT nach Entra ID synchronisiert werden.

1.3.1.2.1 Authentifizierungsmethoden

1. Entra Connect bietet verschiedene Authentifizierungsmethoden.

Mode	Beschreibung	Soll-Architektur
Entra Password Hash Synchronization (PHS)	Passwort Hashes werden in die Cloud synchronisiert, Entra ID löst Anmeldeanfragen direkt in der Cloud auf.	Nein
Entra Pass-through Authentication (PTA)	Light-weight Agents werden On-Premises installiert und Anmeldeanfragen an lokales AD weitergeleitet ohne AD FS.	Ja
Federation Integration (Authentisierung über AD FS)	Mit Verwendung von AD FS werden Anmeldeanfragen an lokales AD weitergeleitet.	Nein
Föderation mit eIAM FED-Login	OIDC-/SAML-basierte Föderation zum eIAM-IdP FED-Login zur Nutzung der FED-Login Access App für Zugriffe auf den Tenant von ausserhalb des Bundesnetzes	Ja

Tabelle 3: Authentifizierungsmethoden

1.3.2 Exchange Hybrid

1. Die lokal installierte Exchange Organisation wird mit Exchange Online hybrid erweitert. Hierfür MUSS folgende Variante verwendet werden:
   a. Es MUSS die Hybrid Variante «Classic Hybrid» im Setup «Voll» verwendet werden.
   b. Sobald der funktionale Umfang auch mit «Modern Hybrid» im Setup «Voll» sichergestellt werden kann, MUSS diese Variante geprüft und nach Rücksprache mit dem zuständigen Gremium umgesetzt werden.

Hybrid Variante	Setup	Beschreibung	Soll-Architektur
Classic Hybrid	Voll	Vollwertige, klassische Hybrid-Konfiguration mit direkter Veröffentlichung der Exchange Organisation im Internet. Diese Variante erlaubt eine vollumfängliche Exchange Hybrid Erfahrung. Die Exchange Server (On-Premises) müssen über das Internet erreichbar sein. Diese Variante ist erforderlich, wenn Teams Funktionen (Kalender) vollumfänglich zur Verfügung stehen müssen. z.B. Zugriff auf die On-Premises Mailbox. Zugriffe von M365 können über die EWS Policy gesteuert werden.	Ja
Modern Hybrid	Voll	Vollwertige Hybrid-Konfiguration unter Anwendung des Exchange Hybrid-Agenten. Diese Variante erfordert keine eingehende Verbindung zum Exchange Server (On-Premises). Die Kommunikation erfolgt über den Hybrid Agent im Zusammenspiel mit Azure App Proxy (Azure Service). Einschränkungen (nicht abschliessend) - Hybrid Modern Authentication wird nicht unterstützt - Der Hybrid-Agent unterstützt eine einzelne Exchange-Organisation. Mehrere Exchange-Organisationen werden nicht unterstützt - Teams-Kalenderfunktionen, die Zugriff auf lokale Postfächer erfordern, funktioniert nicht - Der Hybrid-Agent unterstützt einen einzelnen Migrationsendpunkt mit den Standardgrenzwerten des Diensts. Mehrere Migrationsendpunkte mit benutzerdefinierten Endpunkten oder URLs werden nicht unterstützt.	Bevorzugt

Tabelle 4: Exchange Hybrid

1.3.3 SharePoint Hybrid

1. Mit der lokalen SharePoint Plattform ist der Aufbau einer hybriden Umgebung für unterschiedliche Szenarien denkbar. Eine Hybridisierung DARF NUR dann vorgenommen werden, wenn folgende Vorgaben eingehalten werden können.
   a. Es DÜRFEN KEINE Daten von On-Premises nach SharePoint Online übermittelt werden (z.B. Indexinformationen zur SharePoint Suche, sensitive Benutzerinhalte (MySite)). Massgebend dazu ist die [E031].

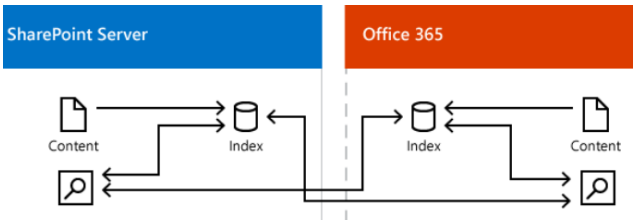
Hybridfunktion	Beschreibung	Soll-Architektur
Hybride Self-Service Site Erstellung	Die hybride Self-Service Site Erstellung leitet die Erstellungsseite im SharePoint Server auf die Microsoft 365 Group Creation um. Durch die Konfiguration können die Anwender ihre Websites in SharePoint Online anstelle von SharePoint Server erstellen.	Nein Sites in SharePoint Online sind über das Self-Service-Portal zu bestellen.
Hybride Federated Search	Mit der hybriden föderierten Suche wird der Index in SharePoint Server als auch den Index in SharePoint Online abgefragt. Die Indexe bleiben auf der jeweiligen Plattform.  	Ja, es DÜRFEN KEINE Indexe in die Cloud übertragen werden.
Hybride Profile	Mit hybriden Profilen hat der Anwender ein einziges Profil in Microsoft 365, in dem alle Profilinformationen gepflegt werden	Ja, es DÜRFEN KEINE sensitiven Inhalte übertragen werden.
Hybrider Terminologie Speicher	Die hybride SharePoint-Taxonomie ermöglicht eine einzige Taxonomie, die sich über SharePoint Server und SharePoint Online erstreckt. Dadurch gibt es eine einzige konsistente Taxonomie, unabhängig wo sich die Websites befindet.	Nein
Hybrides OneDrive for Business	Im SharePoint Server wird das OneDrive for Business nach SharePoint Online umgeleitet. Es bietet sich an die Daten in der Cloud zu speichern, zu teilen und zusammenzuarbeiten.	Ja, OneDrive for Business wird nur Online angeboten.

Tabelle 5: SharePoint Hybrid

1.3.4 Skype for Business mit Teams

1.3.4.1 Coexistence Modes

1. Für die Integration von Teams gibt es verschiedene Coexistence Modes. Der Coexistence Mode kann pro Benutzer konfiguriert werden. Es werden die folgenden Coexistence Modes bereitgestellt:
   a. Standard für Hybride Benutzer: Island Mode
   b. Standard für klassische Benutzer: Skype for Business only

c. Teams only: Wenn das Konto die Telefonie Dienste über Teams bezieht.

Coexistence Modes	Beschreibung	Soll-Architektur
Islands Mode	Beide Welten eine Insel, die fast nichts miteinander zu tun haben. Jeder Benutzer muss beide Clients (Skype for Business und Teams) parallel starten. Telefonie Dienste stehen nur in Skype for Business zur Verfügung. Externe SIP-Kontaktierungen erfolgen über den Skype for Business Edge Server und können nur in Skype for Business bearbeitet werden.	Ja
Skype for Business only	Die Benutzer verwenden weiterhin Skype for Business. Teams kann im «Skype for Business only» nicht benutzt werden.	Nein
Teams Only	Damit steht ausschliesslich Teams dem Benutzer zur Verfügung. Auch die Telefonie Dienste werden mit Teams bereitgestellt. Skype for Business wird nicht mehr verwendet.	Ja; frühestens möglich, wenn Teams Telefonie Anbindung realisiert ist (separate Migrationsplanung)

Tabelle 6: Coexistence Mode

1.3.4.2 Telefonie Anbindung

1. Die Anbindung mit Teams an das öffentliche Telefonnetz (PSTN) in der Schweiz MUSS über die Infrastruktur der Bundesverwaltung erfolgen (Variante Direct Routing).
2. Die Anbindung an das öffentliche Telefonnetz (PSTN) ausserhalb der Schweiz erfolgt nach spezifischen Standortkonzept.

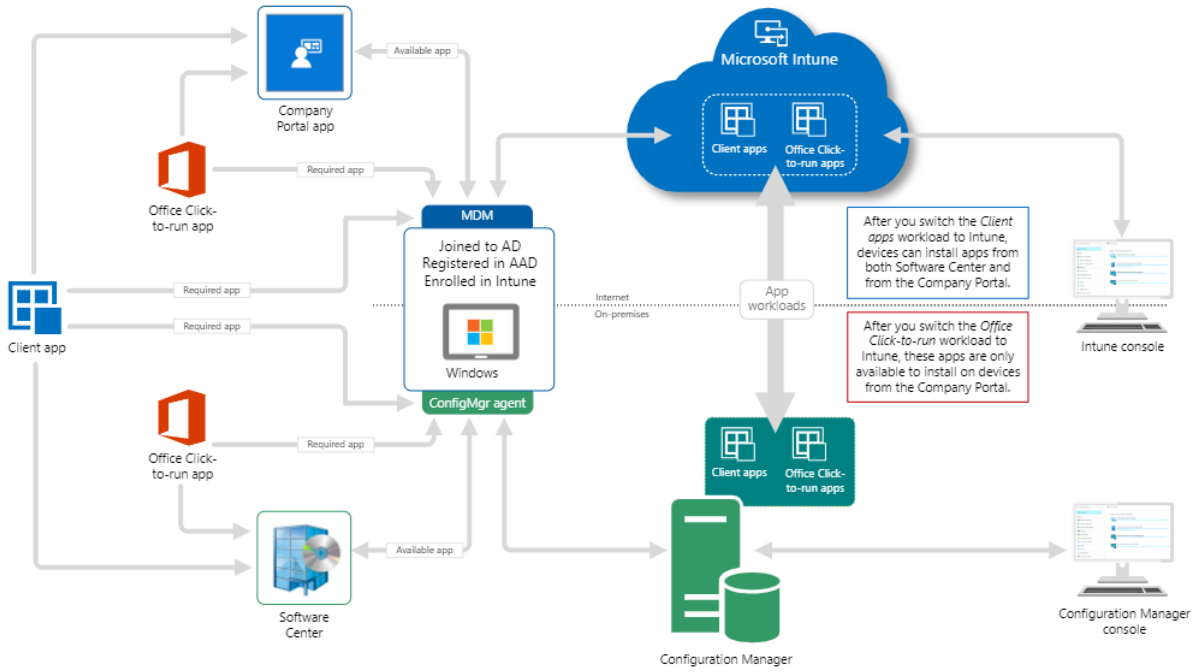
Variante	Beschreibung	Soll-Architektur
Calling Plan	Calling Plan (Anrufplan) ermöglicht die Anbindung an das öffentliche Telefonnetz ohne lokal installierte Infrastruktur. Diese Variante ist nicht in jedem Land und Region verfügbar.	Nach Bedarf und Verfügbarkeit an ausländischen Standorten
Direct Routing	Direct Routing ermöglicht es, die lokale SBC-Infrastruktur anzubinden und den bestehenden Nummern-Block zu verwenden (ohne Operator Connect).	MUSS (Schweiz), nach Bedarf und Verfügbarkeit an ausländischen Standorten
Operator Connect	Operator Connect ist eine weitere Option für die Bereitstellung von PSTN-Konnektivität (Public Switched Telephone Network) mit Teams und Telefonanlagen. Allerdings unterstützt Operator Connect nur «Teams Only» Mode.	Nach Bedarf an ausländischen Standorten

Tabelle 7: Telefonie Anbindung

1.4 Einbindung der Endgeräte

1.4.1 Co-Management

1. Die Backend-Infrastruktur (lokale System Center Configuration Management Platform) MUSS mit Intune erweitert werden (Co-Management).



Quelle: [Co-Verwaltungsworkloads - Configuration Manager | Microsoft Learn]

2. Im Co-Management KANN der Co-Verwaltungsworkload (in der Art eines Schiebereglers) konfiguriert werden, woher der Client die Konfiguration/Software erhält (Microsoft Endpoint Configuration Manager (MECM) vs. Intune):
   a. Compliance-Richtlinien
   b. Windows Update-Richtlinien
   c. Ressourcenzugriffsrichtlinien
   d. Endpunktschutz
   e. Gerätekonfiguration
   f. Office Click-to-Run apps
   g. Client-Apps
3. Microsoft Intune DARF NUR eingesetzt werden, wenn es technisch notwendig ist. Der Co-Verwaltungsworkload Schieberegler SOLL weiterhin auf System Center Configuration Manager (oder MECM) konfiguriert werden. Davon ausgenommen sind Endgeräte die nur in Microsoft Intune verwaltet werden (Bsp. SmartDevices).
4. Die Softwareverteilung SOLL analog heute erfolgen, ausser wenn es technisch notwendig ist, KANN die Software auch über Microsoft Intune verteilt werden.
5. Das Unternehmensportal-App SOLL nur eingesetzt werden, wenn dies technisch notwendig ist.

1.4.2 Geräteidentität

1. In M365 gibt es verschiedene Geräte Modi, wie das Endgerät in M365 integriert werden kann. Zum Benutzerkonto in Entra ID gibt es auch noch eine Geräteidentität. Dabei MUSS ein Computerobjekt in Entra ID erstellt werden.
2. Folgende Geräte Modi DÜRFEN verwendet werden:

Mode	Beschreibung	Soll-Architektur
Entra ID join	Geräte mit Windows 11 oder neuer, die sich im Besitz der Organisation befinden. Windows Server 2019 oder neuer in der Organisation (Option, aber nicht vorgesehen). Verwaltung der Geräte über Mobile Device Management (z.B. Intune) möglich. Anmeldung am Gerät mit Entra ID-Identität.	DARF NICHT Neue Use Cases müssen zuerst konzipiert und freigegeben werden.
Entra ID registered	Typischerweise mobiles Gerät (Mobiltelefon oder Tablet) Bring Your Own Device (BYOD), privates Gerät vom Benutzer Verwaltung der Geräte über Mobile Device Management (z.B. Intune) möglich Anmeldung am Gerät mit lokaler Identität	KANN, sobald der Einsatz definiert ist.
Hybrid Entra ID join	Zwischenschritt zu Entra ID join Gerät ist OnP AD joined und Entra ID joined und teilweise angewiesen auf eine Verbindung mit einem Domain Controller Verwaltung der Geräte über SCCM und GPOs möglich Verwaltung der Geräte über Mobile Device Management (z.B. Intune) mit Zusatz möglich Anmeldung am Gerät mit Domänen- resp. Entra ID-Identität	MUSS für BA-Client. Davon ausgenommen sind Legacy oder Cloud only Geräte.

Tabelle 8: Geräteidentität

1.4.3 Authentifizierungsmethoden

1. Einige Authentifizierungsmethoden können als primärer Faktor verwendet werden, wenn damit eine Anmeldung an einer Anwendung oder einem Gerät erfolgt, z.B. mit einem FIDO2-Sicherheitsschlüssel oder einem Kennwort. Andere Authentifizierungsmethoden sind nur als sekundärer Faktor verfügbar, wenn sie die Multi-Faktor-Authentifizierung mit Microsoft Entra verwenden.
2. Gäste MÜSSEN sich mit einer Authenticator App Authentifizieren.
3. Folgende Authentifizierungsmethoden DÜRFEN für Bundesmitarbeiter verwendet werden. Für privilegierte Zugriffe und Break Glass Accounts gelten die Vorgaben gemäss AR015.

Methode	Erster Anmeldungsvorgang	Einsatz als MFA-Mittel	Soll-Architektur
Windows Hello for Business	Ja	n/a	DARF NICHT
Microsoft Authenticator App (Push)	Nein	Ja, mit Code Eingabe	DARF NICHT

Methode	Erster Anmeldungs-vorgang	Einsatz als MFA-Mittel	Soll-Architektur
Microsoft Authenticator App (kennwortlos)	Ja	Ja, mit Code Eingabe	KANN
Authenticator Lite	Nein	Ja	DARF NICHT
FIDO2-Sicherheitsschlüssel	Ja	Ja	KANN, sobald der Einsatz definiert ist.
Zertifikatbasierte Authentifizierung (CBA)	Ja	Ja	MUSS für BA-Client
OATH-Hardwaretoken (Vorschau)	Nein	Ja	DARF NICHT
OATH-Softwaretoken	Nein	Ja	DARF NICHT
Befristeter Zugriffspass (TAP)	Ja	Ja	DARF NICHT, ausgenommen technische notwendig für die Registrierung des MFA-Mittel
SMS	Nein	Ja	DARF NICHT
Anruf	Nein	Ja	DARF NICHT
Kennwort	Ja	Nein	DARF NICHT, temporär ausgenommen, wenn SmartCard Anmeldung mit BA-Client nicht möglich ist.

Tabelle 9: Authentifizierungsmethode

1.4.4 Zugriffsmatrix

1. Die Abbildung zeigt die Zugriffe auf M365.

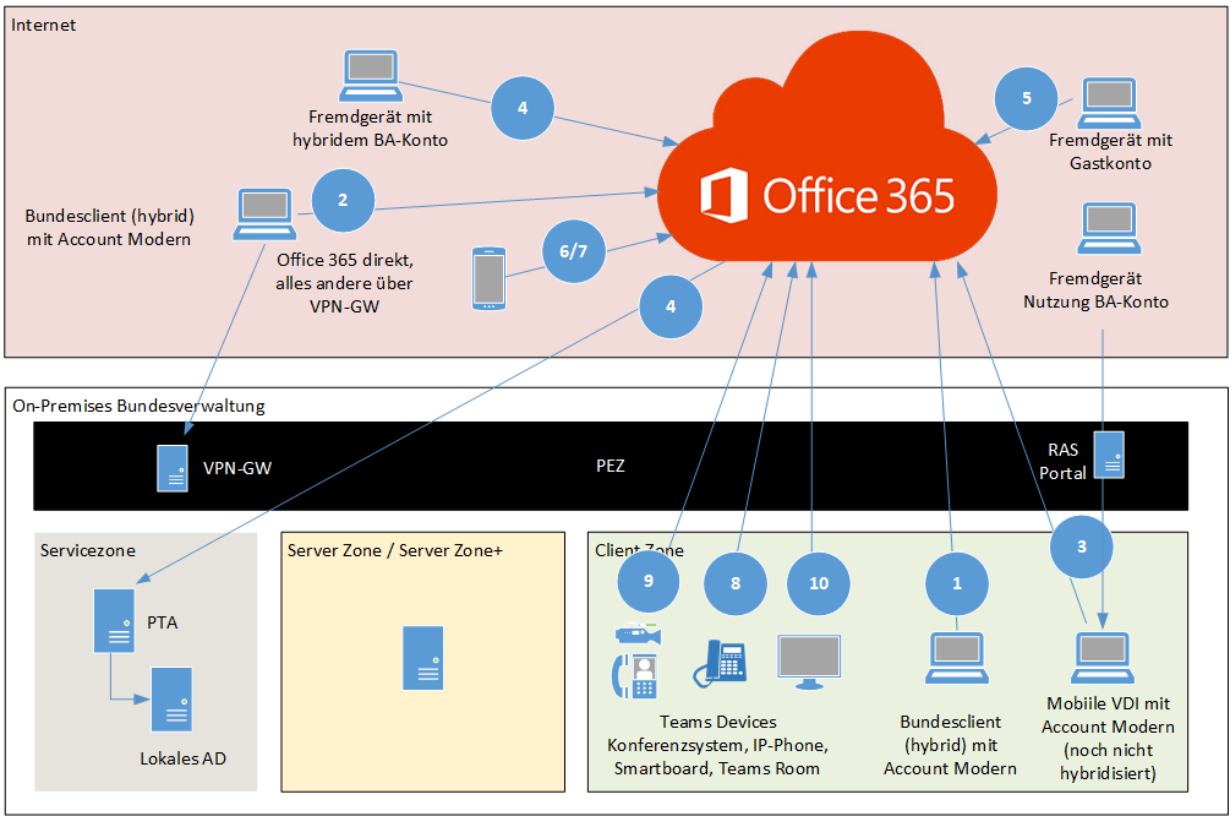


Abbildung 2: Zugriffe auf M365

2. Ausschliesslich die nachfolgenden Zugriffe auf M365 DÜRFEN verwendet werden.

#	Endgerät	Client-Verwaltung	Benutzerkonto	Anmeldung Endgerät	Sicherheitsstufe Endgerät	Anmeldung M365	Sicherheitsstufe M365[4]	Ressourcen	Bearbeitung M365 Daten
1	Bundesclient (hybrid)	Hybrid Entra ID join	Account Modern (U-/X-)	SmartCard (On-Prem AD, SSO M365)	Hoch	Seamless Single-Sign-On (SSSO)	Hoch	M365, On-Prem BA-Dienste, FA	lokales Office, Online
2	Bundesclient (hybrid)	Hybrid Entra ID join	Account Modern (U-/X-)	SmartCard (On-Prem AD, SSSO M365)	Hoch	Seamless Single-Sign-On (SSSO)	Hoch	M365, On-Prem BA-Dienste, FA	lokales Office, Online
3	Mobile VDI	SCCM/AD/Citrix Profil Manager	Account Modern (U-/X-)	UN/PW und SMS OTP (via RAS Portal)	Mittel	User ID und Authenticator (ohne Kennwort) aus Bundesnetz	Mittel	M365, On-Prem BA-Dienste, FA	lokales Office, Online
4	Fremdgerät	N/A	Account Modern (U-/X-)	N/A	N/A	User ID und Authenticator (ohne Kennwort [Passwordless])	Mittel	M365, EXO via OWA	Online

[4] Sicherheitsstufen entsprechen der Si001 – IKT-Grundschutz in der Bundesverwaltung

#	Endgerät	Client-Verwaltung	Benutzerkonto	Anmeldung Endgerät	Sicher-heitsstufe Endgerät	Anmeldung M365	Sicherheits-stufe M365[4]	Ressourcen	Bearbei-tung M365 Da-ten
5	Fremdgerät	N/A	Gastkonto	N/A	N/A	User ID und Authenti-cator (ohne Kennwort [Passwordless])	Mittel	Zugriff nur auf be-rechtigte Ressour-cen	Online
6	Managed SmartDevice	MDM (Intune) Citrix Endpoint Management, sofern Device als Managed Device in M365 erkannt wird	Account Mo-dern (U-/X-)	Mindestens gemäss MDM Vorgabe	Mittel	User ID und Authenti-cator (ohne Kennwort [Passwordless])	Mittel	M365	Lokales managed Office (MAM), Online
7	IP-Phone	Teams und Verwaltungs-software vom Hersteller	**Persönliches IP-Phone:** Account Mo-dern (U-/X-) **Unpersönli-ches IP-Phone:** Account Mo-dern (R-)	Wird noch ab-schliessend definiert (noch in Bearbeitung aufgrund WTO-Aus-schreibung UCC Devices)	Mittel	Registrierung Device mit verwendetem Konto	Gering	Teams Anruf, Teams Meeting	Nein

#	Endgerät	Client-Verwaltung	Benutzerkonto	Anmeldung Endgerät	Sicher-heitsstufe Endgerät	Anmeldung M365	Sicherheits-stufe M365[4]	Ressourcen	Bearbei-tung M365 Da-ten
8	Konferenz System	Teams und Verwaltungs-software vom Hersteller	Account Mo-dern (R-)	Wird noch ab-schliessend definiert (noch in Bearbeitung aufgrund WTO-Aus-schreibung UCC Devices)	Mittel	Registrierung Device mit Ressource Konto	Gering	Teams Anruf, Teams Meeting	Nein
9	Smartboard (Bsp. Surface-Hub)	Teams und Verwaltungs-software vom Hersteller	Account Mo-dern (R-)	Automatische Anmeldung aufgrund Re-gistrierung	Mittel	Registrierung Device mit verwendetem Res-source Konto	Gering	Teams Anruf, Teams Meeting mit Whiteboard und Of-fice Produkte	Teams Meetingin-halte
10	Teams Rooms	Teams und Verwaltungs-software vom Hersteller	Account Mo-dern (R-)	Automatische Anmeldung aufgrund Re-gistrierung	Mittel	Registrierung Device mit verwendetem Res-source Konto	Gering	Teams Anruf, Teams Meeting mit Whiteboard und Of-fice Produkte	Teams Meetingin-halte

Tabelle 10: Zugriffsmatrix

1.5 Stufen der Zusammenarbeit

Konzept	Definition	Prozess	Verwendung	M365 Ressourcen	Soll-Architektur
B2B Collaboration	Zusammenarbeit zwischen Unternehmen.	Einladen externer Benutzer über Azure AD B2B, wobei Gäste ihre Anmeldeinformationen von ihrer Heimorganisation verwenden. Für Zusammenarbeit ist eine Kollaborationsvereinbarung erforderlich [AR009, Kapitel 2.6].	Zusammenarbeit in SharePoint, Teams, Exchange und anderen M365-Diensten und Applikationen.	M365 Apps for Enterprise Exchange Online (E-Mail und Kalender) Power BI Azure DevOps Microsoft Power Platform M365 Groups (Enterprise Apps)	MUSS
B2B Direct Connect (cross-tenant-access)	Direkte, dedizierte Verbindung zwischen Unternehmen.	B2B Direct Connect erfordern eine gegenseitige Vertrauensstellung zwischen zwei Microsoft Entra-Organisationen, um Zugriff auf die Ressourcen der jeweils anderen zu ermöglichen.	Mit der direkten B2B-Verbindung können Benutzer beider Organisationen mit ihren eigenen Anmeldeinformationen zusammenarbeiten, ohne dass sie der Organisation des jeweils anderen als Gäste hinzugefügt werden müssen.	Alle Tenant Ressourcen. Einschränkung der Zugriffe mittels Gruppenmitgliedschaften.	DARF NICHT
B2B – Cross-Tenant Sync	Automatische Synchronisierung von Benutzeridentitäten (Entra ID) zwischen mehreren Tenants.	Durch die Erstellung einer **Cross-Tenant Access Policy** wird festgelegt, welche Tenants ihre Benutzer gegenseitig synchronisieren dürfen. Nachdem der Cross Tenant Sync Zugriff im Quell- und Ziel-Tenant eingerichtet wurde, können zusätzliche Sicherheitsrichtlinien wie Conditional Access	Ein Unternehmen kann Partnerorganisationen Zugriff auf M365-Dienste gewähren, z. B. für Projekte oder Support.	Ein synchronisierter Benutzer hat nicht automatisch Zugriff auf alle Ressourcen im Ziel-Tenant. Der Zugriff muss durch den Ziel-Tenant-Administrator explizit gewährt werden. Conditional Access Policies, Gruppenmitgliedschaften und Rollenbasierte Zugriffssteuerung (RBAC) spielen eine zentrale	DARF beantragt werden

Konzept	Definition	Prozess	Verwendung	M365 Ressourcen	Soll-Architektur
		Policies, MFA und andere Anforderungen konfiguriert werden. Nach der Einrichtung werden Benutzer (Member oder Gast) gemäss Attributemapping im Ziel-Tenant angelegt.		Rolle bei der Bestimmung, auf welche Ressourcen der Benutzer zugreifen kann.	
External Access	Bundesmitarbeiter können Personen aus einer anderen Organisation, anrufen und mit ihnen chatten.	Aktivierung von Einstellungen für externen Zugriff für bestimmte Dienste, z. B. Teams, um externen Benutzern die Teilnahme an Besprechungen zu ermöglichen.	Externe Benutzer nehmen an Teams-Besprechungen teil oder arbeiten in bestimmten Diensten z. B. Chat zusammen.	Microsoft Teams	DARF
Anonymer Zugriff	Teilnahme an Teams Meeting ohne Konto.	Die anonyme Teilnahme an Meetings wird in Teams verwaltet. Die Teilnahme an Meetings ist für nicht erlaubte Domains weiterhin möglich.	Zugang zu öffentlichen Meetings.	Microsoft Forms Microsoft Teams Meetings Microsoft Teams Webinar	Ja

Tabelle 11: Stufen der Zusammenarbeit

Weitere Ankündigungen von Microsoft zur verbesserten Zusammenarbeit wie «Entra ID multi-tenant organization» MÜSSEN nach Verfügbarkeit berücksichtigt werden.

1.5.1 Konfiguration mit B2B-Collaboration

1. Es gelten die übergreifenden Architekturrichtlinien aus der [AR015] gemäss der «Nutzung von EntraID Accounts in Kollaboration und Föderation».
2. Die Benutzer (Members) können externe Personen einladen (eingehender Datenverkehr). Im Gegenzug könnten Benutzer (Members) als Gäste in externe Organisationen (Tenants) eingeladen werden (ausgehender Datenverkehr). Die Gastkonten haben limitierten Zugriff auf die M365 Ressourcen.
3. Für eine Teilnahme eines Gastes im Typ-1 Tenant aus einem Typ-4 Tenant gelten folgende Kollaborationsregulationen:
   a. Die Gastkonten unterliegen der Verantwortung des SD/BA.
   b. Mitglieder des SD/BA Tenants (Members) können Gastbenutzer einladen.
   c. Der Life Cycle solcher Gastkonten MUSS über das ORA in den SD/BA Tenants erfolgen.
   d. Das Gastkonto authentifiziert sich mit MFA (vgl. 1.3.1.2.1).
   e. Der Gastbenutzerzugriff ist auf seine eigenen Eigenschaften beschränkt.
   f. Die Gastkonten haben nur auf das M365 Portfolio Bund Zugriff, welcher der SD/BA verantwortet. Von der Regelung ausgenommen sind die Services für den «persönlichen Gebrauchs zur individuellen Arbeitsoptimierung und -orchestrierung»[5]. Der Zugriff auf FA MUSS vom SD/BA LE unterbunden werden.
   g. Es DÜRFEN KEINE Gäste mit einer Mailadresse wie *@*.onmicrosoft.com zur Zusammenarbeit eingeladen werden.
4. Zur Teilnahme an einem MS Teams Meeting DARF ein anonymer Zugriff via Einladungslink erfolgen.
5. Der Einladende MUSS für die Collaboration mit Dritten sicherstellen, dass nur Personen eingeladen (Gastkonto) werden, wenn es sich um einen geschäftlichen Kontext handelt. Die Collaboration im privaten Kontext ist untersagt. Der Life Cycle der Gastkonten erfolgt wie in Kap. 3 Abs. c beschrieben inkl. der prozessualen Verantwortung des Einladenden.
6. Für die Teilnahme als Gast im Typ-4 Tenant gelten folgende Kollaborationsregulationen:
   a. Es besteht ein bewilligter Antrag zur Teilnahme als Gast im Typ-4 Tenant gemäss IAMV Art. 17.
   b. Der SD/BA LE MUSS hier entsprechende Prozesse implementieren, um dem gerecht zu werden. Es genügt nicht, durch Bestätigung des Benutzers, dass Personendaten an Dritte übermittelt werden. Daher ist eine generelle offene Collaboration mit Dritten untersagt, wenn Personendaten übermittelt werden, um den Kontrollverlust zu wahren.

[5] Hier sind Services aus der Power Plattform gemeint

Anhänge

A. Referenzen

ID	Referenz[6]
AR015	AR015 - Architekturvorgaben bei Nutzung von Cloud Ressourcen des Microsoft Ökosystems
IAMV	Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes
VDTI	Verordnung über die digitale Transformation und die Informatik, VDTI vom 25. November 2020; SR 172.010.58

B. Abkürzungen

Kürzel	Bedeutung
SD/BA	Standarddienst Büroautomation
M365	Microsoft 365
ORA	Orchestrierungsframework

[6] Erlasse auf Bundesstufe werden gemäss der «Systematischen Rechtssammlung» referenziert. Bei einer referenzierten Weisung zur Bundesinformatik wird die zum Ausgabedatum dieser Beilage gültige Version angegeben.