



BIT August 2026

Technischer Abschlussbericht Proof of Concept BOSS

Betrieb von openDesk auf der BIT-Infrastruktur
Beilage 1 zur Machbarkeitsstudie



Hinweis: Dieser Bericht dokumentiert die im Proof of Concept (PoC) erhobenen technischen und betrieblichen Beobachtungen. Strategische Bewertungen und eine wirtschaftliche Beurteilung erfolgen durch den Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (BK-DTI) in einem separaten Bericht. Das Bundesamt für Informatik und Telekommunikation (BIT) hat diesen PoC im Auftrag von BK-DTI durchgeführt.

Inhalt

1	Zusammenfassung	3
1.1	Auftrag und Zielsetzung	3
1.2	Vorgehen	3
1.3	Wesentliche Beobachtungen	3
2	Einleitung	4
2.1	Ausgangslage und Auftrag	4
2.2	Ziele des PoC	4
2.3	Abgrenzungen	4
3	PoC-Setup	5
3.1	Prüfgegenstand	5
3.2	Erfolgskriterien gemäss Projektauftrag	6
3.3	Zeitraum	6
3.4	Methodisches Vorgehen	6
3.5	Zeitplan und wichtigste Etappen	6
4	Architektur und Infrastruktur	8
4.1	Zielarchitektur (geplant)	8
4.2	Tatsächlich realisierte Architektur: Backend	8
4.3	Tatsächlich realisierte Architektur: Client	8
4.4	Netzzonen und Zugriffskonzept	8
4.5	Identitäts- und Zugriffsmanagement	8
4.6	Sicherheitsaspekte	8
5	Durchgeführte Tests und Beobachtungen	9
5.1	User Acceptance Test – Browserlösung	9
5.2	Beobachtungen Linux-Clients	9
5.3	Skalierung und Performance	9
5.4	Sicherheits- und Compliance-Befunde	10
5.5	Schnittstellen zu Umsystemen	10
5.6	Community Edition vs. Enterprise Edition	10
6	Ergebnisse	11
6.1	Erfüllung der PoC-Ziele	11
6.2	Befunde	11
6.3	Offene Punkte	12
7	Mögliche Folgeszenarien	13
7.1	Szenario A – Notfall-BA	13
7.2	Szenario B – Koexistenz und gezielte Substitution	13
7.3	Szenario C – Vollsubstitution	13
7.4	Faktenbezug	13
8	Abkürzungen und Glossar	14

1 Zusammenfassung

1.1 Auftrag und Zielsetzung

Der Proof of Concept (PoC) BOSS hatte zum Ziel, die technische und betriebliche Eignung von openDesk als Alternative und Open-Source-basierte Workplace-Suite für die Bundesverwaltung zu prüfen. Geprüft wurden die funktionale Abdeckung, die technische Integrierbarkeit in die BIT-Infrastruktur sowie betriebliche Aspekte. Der PoC liefert Faktengrundlagen für zukünftige Architektur- und Sourcing-Entscheide durch den Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (BK-DTI).

1.2 Vorgehen

Im PoC BOSS hat das BIT eine openDesk-Umgebung auf der «Red Hat Open Shift»-Plattform (RHOS) aufgebaut. Auf dieser Umgebung wurden drei Client-Varianten geprüft: Browser-Zugang über den Standard Büroautomations-Client (BA-Client), ein Linux-Fat-Client sowie ein virtueller Linux-Client in Hyper-V. Weiter wurden User Acceptance Tests mit 172 Teilnehmenden aus mehreren Departementen durchgeführt. Auch konzeptionelle Abklärungen zur Anbindung an eIAM, GEVER, SAP und die M365-Datenübernahme waren Teil des PoC.

1.3 Wesentliche Beobachtungen

- User Acceptance Tests: Über alle Verwaltungseinheiten bewerteten die Testbenutzenden die Browserlösung mit durchschnittlich 5,4 von 6 Punkten. Die getestete Browserlösung wurde auf der Enterprise Edition getestet und deckt Basisprozesse (Dokumentenbearbeitung, Dateiablage, Kollaboration sowie grundlegende Mail- und Kalenderfunktionen) ab.
- openDesk ist gemäss Hersteller nicht für OpenShift optimiert. Rund 100 Container-Images mussten erstellt und mehrere Plattform-Ausnahmen bewilligt werden.
- Mehrere Ereignisse beeinflussten den Projektverlauf: So war ein Wechsel auf dedizierte Bare-Metal-Nodes (SSF-Cluster) nötig. Nach dem Sicherheitsvorfall XWiki im August 2025 musste zudem der Internet-Zugriff gesperrt werden. Das Versionsupgrade 1.4 auf 1.8 mit vorgängigem Wechsel von der Community auf die Enterprise Edition ging mit einem Datenverlust einher.
- Eine echte Ende-zu-Ende-Verschlüsselung in Jitsi ist auf Kleingruppen (≤ 20 Teilnehmende) begrenzt, die Transportverschlüsselung skaliert höher.
- Der Linux-Fat-Client (Kubuntu) wurde von Testpersonen als flüssiger empfunden als die Browser-Variante. Eine zentrale Linux-Management-Infrastruktur existiert beim BIT aktuell jedoch nicht.
- Eine Datenübernahme aus M365 ist mit nativen Microsoft-Backup-Funktionen nicht möglich. Mögliche alternative Pfade wären: Graph-API-basierte Pipelines oder etablierte Drittprodukte. Diese wurden im PoC konzeptionell beschrieben, jedoch nicht produktiv umgesetzt.

2 Einleitung

2.1 Ausgangslage und Auftrag

Das BIT stellt für BK-DTI eine Open-Source-basierte Office- und Kollaborations-Lösung bereit. Die Lösung soll auf den Vorarbeiten von BK-DTI sowie auf den von ZenDiS publizierten Open-Source-Komponenten aufsetzen. Backend-seitig wird auf der bestehenden RHOS-Plattform des BIT aufgebaut; client-seitig werden Browser-, Fat-Client- und virtuelle Varianten geprüft.

Als Referenzprodukt wurde openDesk eingesetzt – eine modulare Office- und Kollaborations-Suite, die im Auftrag des deutschen Bundesministeriums des Innern durch das Zentrum für Digitale Souveränität (ZenDiS) für die öffentliche Verwaltung entwickelt wird.

PoC BOSS - Architektur Uebersicht

openDesk-Backend betrieben im BIT - Drei Client-Zugriffsarten vom Arbeitsplatz

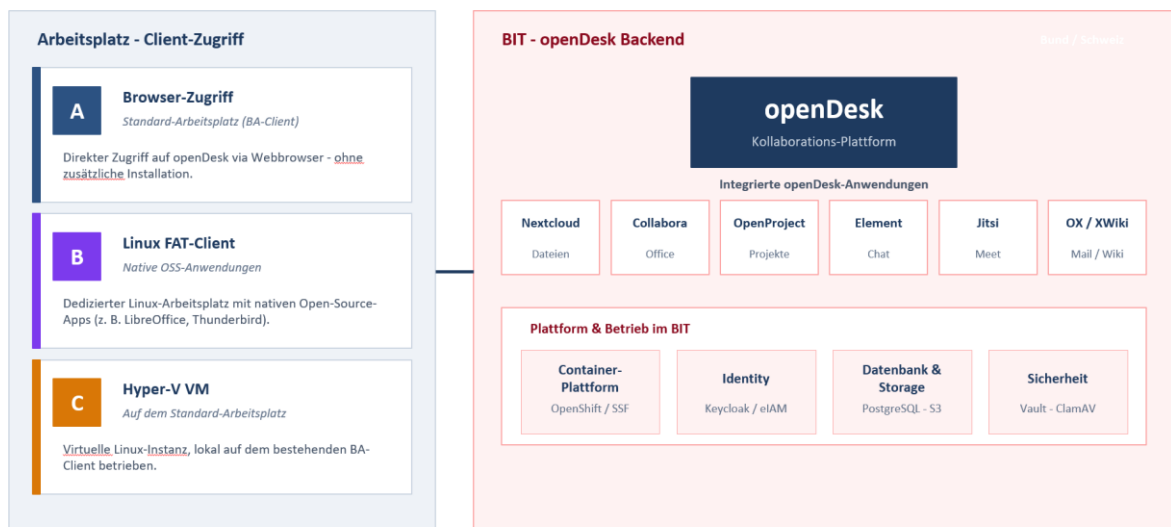


Abbildung 1: Architektur-Übersicht PoC Boss.

2.2 Ziele des PoC

Drei Zielebenen wurden adressiert:

- **Fachlich:** Abdeckung zentraler Kollaborations-Geschäftsfälle (Zusammenarbeit, Kommunikation, Dokumenten- und Informationsmanagement)
- **Technisch:** Integrierbarkeit in IAM-, Netzwerk-, Sicherheits- und Client-Infrastrukturen sowie Erfassung von Sicherheits-, Skalierungs- und Wartbarkeitsaspekten
- **Betrieb:** Erfassung der für einen Betrieb relevanten Aspekte unter den regulatorischen und organisatorischen Rahmenbedingungen der Bundesverwaltung

2.3 Abgrenzungen

- Backend nur deploybar, sofern Container-Images / Helm-Charts CVE-Level ≤ 7 erreichen und mit BIT-Vorgaben kompatibel sind.
- Drei Client-Varianten: BA-Standardclient (Browser), Linux-Fat-Client, virtueller Linux-Client. Smart Devices nur als BYOD via Browser.
- Schutzbedarf: Ausgangsbasis Grundschutz.
- Datenmigration aus M365 konzeptionell beschrieben, nicht produktiv umgesetzt.
- Betrieb und Support des Backends erfolgte während der PoC-Dauer auf Best-Effort-Basis.
- Performance- und Skalierungsmessungen erfolgten nur exemplarisch.
- Strategische Bewertungen und eine Wirtschaftlichkeitsbetrachtung sind nicht Bestandteil dieses Berichts.

3 PoC-Setup

3.1 Prüfgegenstand

Eingesetzt wurde openDesk im Projektverlauf in zwei Editionen:

- **Community Edition:** Der Bezug erfolgte über opencode.de, und wurde für den Aufbau und initiale Inbetriebnahme der Plattform auf der BIT-RHOS-Infrastruktur genutzt.
- **Enterprise Edition:** Diese wurde durch ZenDiS bereitgestellt und kam nach dem fehlgeschlagenen Versionsupgrade 1.4 auf 1.8 der Community Edition (vgl. Kap. 3.5 und 5.4) zum Einsatz. Mit der Enterprise Edition wurde der User Acceptance Test durchgeführt.

openDesk ist eine Sammlung von zwölf bewährten Open-Source-Anwendungen, die unter einer gemeinsamen Oberfläche zu einem vollständigen Büro-Arbeitsplatz zusammengeführt werden. Entwickelt wurde die Suite vom Zentrum für Digitale Souveränität (ZenDiS), einer Gesellschaft der deutschen Bundesregierung, im Auftrag des Bundesministeriums des Innern. Das Ziel: eine vollwertige Alternative zu kommerziellen Office-Paketen, bei der die öffentliche Verwaltung die volle Kontrolle über Daten und Betrieb behält.

Die zwölf Anwendungen decken alles ab, was im Verwaltungsalltag gebraucht wird – von E-Mail, Kalender und Kontakten (Open-Xchange) über Chat und Videokonferenzen (Element auf Basis des Matrix-Standards, Nordeck mit Jitsi) bis hin zur Dateiablage (Nextcloud) und zum gemeinsamen Bearbeiten von Office-Dokumenten im Browser (Collabora). Hinzu kommen ein Wiki für die Wissensablage (XWiki), strukturierte Notizen, sowie umfassendes Projekt- und Aufgabenmanagement (OpenProject). Den Rahmen bildet ein zentrales Identity- und Zugriffsmanagement (Univention Nubus), das Anmeldung und Berechtigungen für alle Anwendungen einheitlich regelt.

Das Besondere an openDesk ist nicht ein einzelnes Produkt, sondern das Zusammenspiel: Eine E-Mail mit Termin-Einladung landet automatisch im Kalender, ein im Chat geteilter Link öffnet die Datei direkt in der Online-Office-Suite, und eine Aufgabe aus OpenProject kann mit Notizen, Dokumenten und Videomeetings verknüpft werden – alles über eine einheitliche Anmeldung und in einer konsistenten Benutzeroberfläche. Anwenderinnen und Anwender müssen sich nicht zwölf Werkzeuge merken, sondern arbeiten in einer integrierten Umgebung.

Weil alle Komponenten quelloffen sind und über offene Schnittstellen kommunizieren, lassen sich einzelne Bausteine bei Bedarf austauschen oder ergänzen, ohne das Gesamtsystem in Frage zu stellen. Genau diese Modularität macht openDesk zur tragfähigen Grundlage für einen digital souveränen Arbeitsplatz in der öffentlichen Verwaltung.

openDesk – Anwendungen und Komponenten

12 integrierte Open-Source-Anwendungen für die digitale Zusammenarbeit der öffentlichen Verwaltung



Quelle: opendesk.eu/de/produkt · Herausgeber: ZenDiS GmbH im Auftrag des BMI

Stand: November 2025

Abbildung 2: Übersicht der Anwendungen und Komponenten von openDesk.

OpenDesk ist gemäss dem Hersteller ZenDiS für Kubernetes optimiert. Das BIT bietet diese Infrastruktur im Zuge der Standardisierung des BIT-Angebots nicht mehr als Marktleistung an und hat OpenDesk für die OpenShift-Infrastruktur angepasst. Aufgrund des quelloffenen Codes ist eine solche Anpassung möglich.

Aufgrund des fehlgeschlagenen Versions-Upgrades bei der Community Edition beziehen sich die im PoC erhobenen Anwender- und Betriebserfahrungen auf die Enterprise Edition. Aussagen zur Nutzbarkeit oder Reife der Community Edition lassen sich aus dem PoC nicht ableiten.

3.2 Erfolgskriterien gemäss Projektauftrag

Die Erfolgskriterien für den PoC wurden folgendermassen definiert.

- Die getestete, Open-Source-basierte Lösung deckt wesentliche Büroautomations-Kernfunktionalitäten wie Dokumentenbearbeitung, Dateiablage, Kollaboration, Audio- / Video-Konferenzen sowie grundlegende Mail- und Kalenderfunktionen ab.
- Die Büroautomations-Kernfunktionalitäten können vollständig mit Open-Source-Komponenten abgedeckt werden.
- Im PoC wird die Machbarkeit einer Integration von GEVER und SAP nachgewiesen.

3.3 Zeitraum

Das Projekt ist mit der Unterzeichnung der Dienstleistungsvereinbarung zwischen BK-DTI und dem BIT im November 2024 gestartet. Der User Acceptance Test (UAT) fand im vierten Quartal 2025 statt. Der Abschluss bzw. Rückbau der im PoC aufgebauten Infrastruktur ist per 01.12.2026 geplant.

3.4 Methodisches Vorgehen

Die Architekturarbeiten waren angelehnt an das Open Group Architecture Framework (TOGAF) – ein herstellerunabhängiger Standard für Unternehmensarchitektur. Die Modellierung erfolgte in Innovator, der folgende Aufbau auf der BIT-Container-Plattform (CAE / RHOS). Die Architektur wurde in einem iterativen Prozess und in Reaktion auf Sicherheits- und Plattformvorgaben angepasst.

3.5 Zeitplan und wichtigste Etappen

Die folgende Abbildung zeigt die wichtigsten Etappen und den Zeitplan des PoC BOSS auf. Diese Ereignisse und Entscheide im Projektverlauf hatten auch Einfluss auf die tatsächlich realisierte Architektur im PoC BOSS.

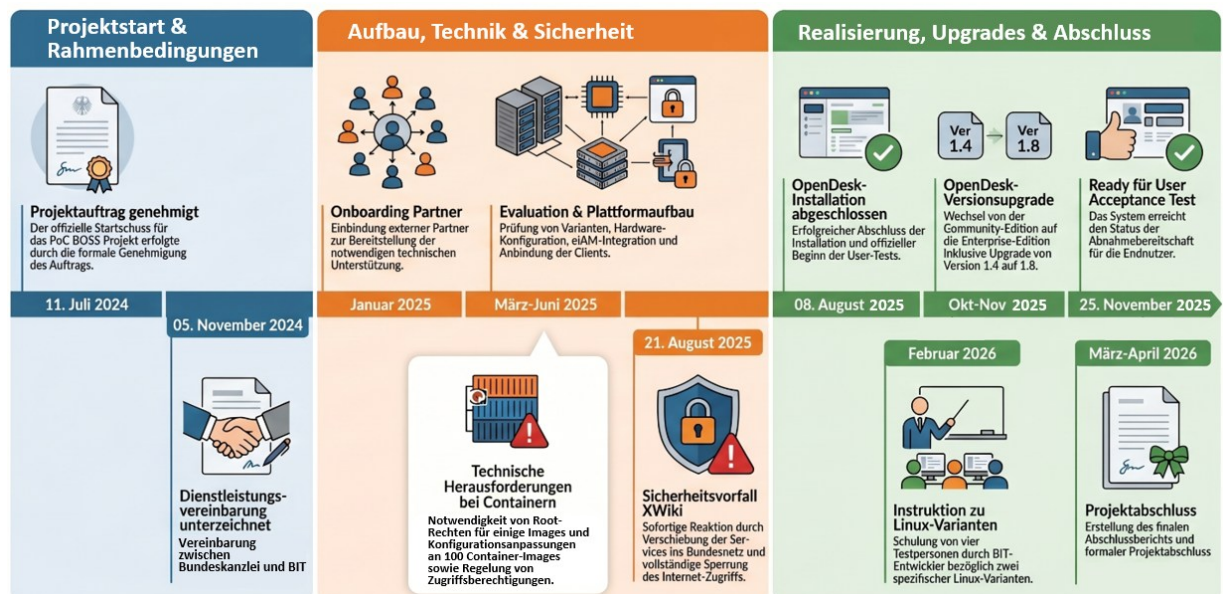


Abbildung 3: Zeitplan und wichtigste Etappen des PoC BOSS

#	Datum	Ereignis / Entscheid	Auswirkung
1	11.2024	DLV unterschrieben	Projektstart
2	02.2025	Onboarding des Projektteams	Start technische Umsetzung
3	02.2025	BIT-Shared-Cluster nicht nutzbar (Root-Privilegien einzelner Container)	Wechsel der Plattform notwendig
4	04 -05.2025	Aufbau zwei dedizierter Nodes auf Bare-Metal SSF-Cluster (V3c)	Verzögerung, Architekturanpassung, Kostenfolge
5	08.2025	Sicherheitsvorfall XWiki nach Öffnung des UDP-Ports (User Data Protocol) für Internet-Zugriff	Kompromittierungsrisiko; ISBO BIT untersagt Internet-Zugriff
6	09.2025	Ausnahmeantrag Variante A (BA- Standardclient mit Browserzugang) bewilligt (mit Auflage: kein Internet- Zugang)	Client-Architektur musste neu konzipiert werden
7	Q4 2025	Einsatz der Enterprise Edition; Versionswechsel von 1.4 auf 1.8 führte zu Datenverlust	Wiederaufbau erforderlich
8	12.2025	Ausnahmeantrag Variante C (virtueller Linux-Client in Hyper-V auf Windows-PC) bewilligt (mit Auflage: kein Internet-Zugang)	Bestätigung der bestehenden Einschränkung

4 Architektur und Infrastruktur

4.1 Zielarchitektur (geplant)

Ursprünglich war vorgesehen, ein modulares Backend auf der BIT-Shared-RHOS-Plattform mit Internet-Erreichbarkeit, durchgängige SSO-Anbindung an agov.ch / eIAM sowie drei Client-Varianten aufzubauen. Die wesentlichen Anforderungen waren dabei

- der Einsatz von Open-Source-Code,
- eine container-basierte, skalierbare Lösung,
- eine modulare Architektur,
- die Einhaltung des IT-Grundschutzes
- sowie eine lückenlose Dokumentation.

4.2 Tatsächlich realisierte Architektur: Backend

Deployment auf RHOS in der CAE des BIT. Die wesentlichen, bezogenen Platfformdienste umfassen:

- PostgreSQL: 10 Datenbank-Instanzen plus pgAdmin
- Object Storage: 500 GB für openDesk-Komponenten
- Vault / Managed Application Vault (MAV) für Secret-Management
- CI/CD: GitOps via Bitbucket, ArgoCD und Tekton im Cluster
- ClamAV: Cloud-Service nicht nutzbar (HTTPS-API statt Socket); ClamAV als Pod im Cluster betrieben

Open-Xchange benötigt eine eigene MariaDB, alle anderen Komponenten nutzen die externe PostgreSQL. Rund 100 Container-Images wurden für den Betrieb auf OpenShift konfiguriert (User-IDs, Capabilities, Root-Privilegien).

4.3 Tatsächlich realisierte Architektur: Client

Drei Client-Varianten wurden aufgebaut:

- **Variante A** – BA-Standardclient mit Browser-Zugang (primär getestete Variante im UAT).
- **Variante B** – Linux-Fat-Client (Kubuntu 24.04 LTS, KDE Plasma): vollständig neuer Arbeitsplatzrechner mit Open-Source-Stack. Installation in zwei Phasen via eigene Skripte; lokale Konten, keine zentrale Verwaltung im PoC.
- **Variante C** – Virtueller Linux-Client in Hyper-V auf Windows-PC: Funktional identisch zu Variante B.

Smart Devices: Der Zugang erfolgte ausschliesslich über den Browser, keine Geräteverwaltung.

4.4 Netzzonen und Zugriffskonzept

Der Zugriff auf openDesk erfolgt aus der Client-Zone (APS) über die Policy-Enforcement-Zone in die Server-Zone des BIT. Der Zugriff aus dem Internet ist seit September 2025 nicht zugelassen.

4.5 Identitäts- und Zugriffsmanagement

eIAM wurde als Login-Methode in openDesk integriert, die Anbindung erfolgte über das Referenzsystem (myaccount-r.eiam.admin.ch). Benutzer müssen vor dem ersten Login vorprovisioniert sein; in Keycloak ist ein User-ID-Mapping konfiguriert.

Beobachtung: Thunderbird- und WebDAV-Zugriffe erfordern aktuell App-Passwörter, da OAuth2/OIDC nicht durchgängig integriert ist.

4.6 Sicherheitsaspekte

- Ausnahmeanträge: (Variante A, September 2025, mit Auflage); zusätzlicher Antrag für Variante C (Dezember 2025).
- Container-Image-Scans: Diese sind bei jedem Update zwingend erforderlich, der gemessene Aufwand beläuft sich auf ca. 12 Stunden pro Update-Zyklus.
- OpenShift-Härtung: Es sind Ausnahmen für vordefinierte User-IDs und einzelne Capabilities erforderlich, damit die meisten Workloads lauffähig sind.
- Authentisierung: eIAM (Browser); App-Passwörter für Mail-/WebDAV-Clients.

5 Durchgeführte Tests und Beobachtungen

5.1 User Acceptance Test – Browserlösung

Der User Acceptance Test (UAT) prüfte die Browserlösung auf der Enterprise Edition unter realitätsnahen Bedingungen für zentrale Büroarbeitsprozesse. Ein detaillierterer Ergebnisbericht findet sich in der Beilage 1 Ergebnisbericht User Acceptance Test (UAT) zum Proof of Concept BOSS der BK-DTI.

Kennzahl	Wert
Eingeladene Testpersonen	172
Aktiv Teilnehmende	73
Teilnahmequote	42.4 %
Durchschnittsbewertung	5,4 / 6,0

Beobachtungen: Bei der getesteten Browserlösung haben die Teilnehmenden die Dokumentenbearbeitung, Dateiablage, Kollaboration sowie Mail- und Kalender-Grundfunktionen konsistent über alle Verwaltungseinheiten hinweg positiv beurteilt.

Chats und Meetings wurden mit dem Produkt Element verschlüsselt. Die Schlüssel werden geräteweise erzeugt und über einen Recovery Key bzw. eine Sicherheitsphrase gesichert. Im PoC zeigte sich, dass das Schlüsselhandling bei den Benutzenden fehleranfällig ist. Dies lässt sich jedoch durch eine Integration in die Client-Landschaft des BIT (Produktion) mitigieren – etwa durch zentrales Hinterlegen eines Recovery-Keys im Passwortmanager und automatisierte Geräteverifizierung via Single Sign on (SSO).

5.2 Beobachtungen Linux-Clients

Linux-Fat-Client (Kubuntu): Diese Client-Variante wurde von den Testpersonen flüssiger empfunden als die getestete Browser-Variante. Sie bietet Offline-Fähigkeit, GPU-beschleunigte A/V-Konferenzen und Zugriff auf Funktionstasten. Eine zentrale Linux-Management-Infrastruktur (MDM/UEM, Patch-Management, Zertifikatsverteilung) existiert beim BIT aktuell nicht.

Wichtig für die Interpretation: Der beobachtete Unterschied ist nicht auf das Betriebssystem Linux zurückzuführen, sondern auf die Ausführungsart als FAT-Client also auf den Einsatz nativ installierter Anwendungen (z. B. LibreOffice, Thunderbird, native Chat- und Konferenz-Clients) anstelle browserbasierter Web-Oberflächen. Die lokale Verarbeitung, der direkte Zugriff auf Systemressourcen und die entkoppelten UI-Threads erklären den Effekt nicht der Kernel darunter.

Virtueller Linux-Client in Hyper-V: Im Test zeigten sich Einschränkungen bei der GPU-Beschleunigung und Videokonferenz-Stabilität gegenüber dem physischen Linux-Fat-Client.

5.3 Skalierung und Performance

Es wurden keine systematischen Lasttests durchgeführt. Die Aussagen basieren auf der Architekturanalyse und Erfahrungswerten der eingesetzten Komponenten:

- Jitsi mit Transportverschlüsselung (DTLS-SRTP): ca. 100 – 150 gleichzeitige Nutzende pro Videobridge; horizontale Skalierung über mehrere JVB-Pods möglich.
- Jitsi mit echter Ende-zu-Ende-Verschlüsselung (E2EE): ab 20 Teilnehmenden faktisch nicht einsetzbar. Eine Server-Skalierung kompensiert die Einschränkung nicht.
- Collabora Online: typisch 10 – 20 gleichzeitige Editoren je Dokument. Dazu sind mehrere COOL-Pods hinter dem Load-Balancer plus RWX-Shared-Storage erforderlich.
- Nextcloud, Element/Matrix, OpenProject: skalieren mit horizontalem Pod-Autoscaling, Cluster-DB und Caching (Redis).
- Die Skalierung ist primär eine Frage des Cluster-Designs (RWX-Storage, Cluster-DB, HPA), nicht von openDesk selbst.

5.4 Sicherheits- und Compliance-Befunde

- Sicherheitsvorfall XWiki (08.2025): Schwachstelle nach Öffnung des UDP-Ports für Internet-Zugriff. Folge: Sperrung des Internet-Zugriffs.
- Datenverlust beim Versionsupgrade 1.4 auf 1.8, weshalb ein Wiederaufbau erforderlich war. In diesem Kontext wurde auf die Enterprise Edition gewechselt. Alle nachfolgenden Tests basierten auf der Enterprise Edition.
- Patch-Dynamik: Monatliche Releases; Container-Image-Scan und -Freigabe sind nötig, das führt zu ca. 12 Stunden Aufwand pro Update. Der Gesamtaufwand inkl. Vorbereitung beträgt ca. 3 Arbeitstage pro Update.

5.5 Schnittstellen zu Umsystemen

Die Schnittstellen zu Umsystemen wurden im PoC nicht durchgängig getestet.

Der aktuelle Stand der Abklärungen:

- **SAP:** Der Zugriff via SAP WebGUI (Browser) ist konzeptionell möglich. Die Voraussetzungen sind SICF/ITS, HTTPS, SSO im SAP-Backend. Diese Voraussetzungen wurden im PoC nicht verifiziert. Ein konkretes SAP-Endsystem wurde nicht festgelegt.
- **GEVER (Acta Nova):** Unter Linux nicht vollständig funktionsfähig, weshalb Anpassungen erforderlich wären. Aktuell gibt es keine Linux-Roadmap-Zusage des Herstellers. Acta Nova kann zwar im Browser aufgerufen werden, aber die produktivitätsentscheidenden Features (Office-Integration, Outlook-Übernahme) sind ohne die Windows-Client-Komponente nicht oder nur eingeschränkt verfügbar.
- **M365-Datenübernahme:** Die native M365-Backup-Funktion ist ungeeignet (Sicherungen verbleiben in der Microsoft-Cloud, kein Export-Artefakt). Mögliche Lösungspfade: Microsoft Graph API, eDiscovery-Export, OneDrive-Sync oder konsolidierende Drittprodukte. Das Konzept ist beschrieben, jedoch nicht produktiv umgesetzt.

5.6 Community Edition vs. Enterprise Edition

Im PoC wurde zuerst die Community Edition eingesetzt. Nach dem fehlgeschlagenen Versionsupgrade (vgl. Kap. 5.4) erfolgte der Wechsel auf die Enterprise Edition. Die wesentlichen Unterschiede umfassen:

Kriterium	Community Edition	Enterprise Edition
Lizenzkosten	kostenfrei	kostenpflichtig, Staffelpreise ab 500 Nutzern
Komponenten-Versionen	Community-Versionen	Enterprise-Versionen u. a. von Nextcloud, Element, OX, Nubus mit zusätzlichen Funktionen und LTS-Sicherheitspatches
Update/Upgrade	monatliche Patches	monatliche Patches
Support	Community-Forum	professioneller Support, skalierbar bis 24/7
SLA	keine Garantie	garantierte Verfügbarkeit gemäss Vertrag
Betriebsmodelle	Self-Hosting	Self-Hosting, SaaS, Confidential Cloud

Die Eignung der Community Edition für eine Bundesverwaltungs-Zielgrösse wurde im PoC nicht systematisch verifiziert.

6 Ergebnisse

6.1 Erfüllung der PoC-Ziele

Ziel	Status	Bemerkung
BA-Kernfunktionalität verfügbar	erfüllt	Die Browserlösung wurde im UAT mit 5.4/6 bewertet (Enterprise Edition)
openDesk auf BIT-RHOS lauffähig	erfüllt mit Auflagen	Mehrere Konfigurationen an ca. 100 Container-Images, Plattform-Ausnahmen erforderlich
Integration eIAM	erfüllt (Browser-Version)	Thunderbird/WebDAV nur via App-Passwort; OAuth2/OIDC nicht durchgängig
Machbarkeit GEVER-Integration	konzeptionell	Unter Linux nicht funktionsfähig, müsste als PlugIn erweitert werden
Machbarkeit SAP-Integration	konzeptionell	WebGUI plausibel; im PoC nicht verifiziert
M365-Datenübernahme	konzeptionell	Pipeline beschrieben, nicht umgesetzt
Skalierungs- und Lasttests	teilweise	Architekturanalyse, keine systematischen Messungen

6.2 Befunde

Die folgende Liste fasst die im PoC erhobenen Befunde zusammen, ohne diese zu bewerten:

- Es handelt sich um eine funktional konsistente, modulare Suite. Die Browserlösung wurde von den Teilnehmenden des UAT als gut bewertet.
- Der Browserzugang erfolgt stabil, ohne dass zusätzliche Client-Infrastruktur nötig ist.
- Die Lösung ist auf der BIT-RHOS-Infrastruktur trotz fehlender offizieller OpenShift-Unterstützung lauffähig. Dazu sind Konfigurationen an ca. 100 Container-Images erforderlich.
- Der Linux-Fat-Client wurde von Testpersonen positiv beurteilt. Die Offline-Fähigkeit ist gegeben. Es ist zu beachten, dass die Linux-Fat-Clients «standalone» getestet wurden, d. h. es existiert zurzeit kein Management-System für die Verwaltung von Linux-Fat-Clients.
- Die Lösung bedarf einer hohen, monatlichen Update-Frequenz. Im PoC gab es keine etablierten Backup-/Restore-Prozesse, es kam zu einem Datenverlust beim Upgrade der Community Edition von Version 1.4 auf 1.8.
- Konfigurations-Aufwand pro Update-Zyklus (Container-Image-Scans und Freigabe) liegt bei ca. 12 Stunden, der Gesamtaufwand inkl. Vorbereitung bei ca. 3 Arbeitstagen.
- Die Eignung der Community Edition für die Zielgrösse Bundesverwaltung konnte im PoC nicht verifiziert werden.
- E2EE-Videokonferenzen mit Jitsi sind technisch auf Kleingruppen bis ca. 20 Teilnehmende begrenzt.
- Videokonferenz-Lobby: Ein Moderator muss als erstes beitreten und die weiteren Teilnehmenden freischalten. Dabei handelt es sich um ein bewusstes Sicherheits-Feature, jedoch mit eingeschränkter Usability.
- Die Fachanwendungs-Integration (GEVER, SAP) ist nicht abgesichert.
- Die eIAM-Integration für die Browser-Variante funktioniert. OAuth2/OIDC funktioniert nicht durchgängig für Mail-/WebDAV-Clients.
- RWX-fähiger Shared Storage ist Voraussetzung für Collabora und mehrere weitere Komponenten.
- Migration von Community Edition zu Enterprise Edition für E-Mail-Speicher (Dovecot 2.x → Dovecot Pro) ist nicht direkt unterstützt.

6.3 Offene Punkte

- Ein systematischer Vergleich, welche Anwendungen und Services von M365 mit openDesk abgedeckt werden können, wurde nicht durchgeführt.
- Wahl des M365-Backup-/Export-Produkts im BIT-Umfeld
- Linux-Device-Management-Lösung (Beschaffung und Betrieb)
- Integrationstests zu mindestens einem konkreten SAP-Endsystem und einem GEVER-Anwendungsfall
- Behandlung der UAT-Daten beim Rückbau per 01.12.2026
- openDesk nutzt «ingress-nginx annotations» (Support-Ende März 2026). Unter OpenShift nicht nativ unterstützt – auf Kubernetes als eigener Service aktivierbar.
- Eignungsnachweis Community Edition für eine produktive Zielgrösse.

7 Mögliche Folgeszenarien

Aus den im PoC erhobenen Erkenntnissen lassen sich verschiedene Folgeszenarien ableiten. Eine Bewertung, Priorisierung oder Empfehlung dieser Szenarien ist nicht Bestandteil dieses technischen Berichts.

7.1 Szenario A – Notfall-BA

Die openDesk Enterprise Edition wird als Ausweichplattform vorgehalten, ohne produktive Rolle im Alltag. Beispielsweise als SaaS bezogen, ergänzt durch eine regelmässig synchronisierte M365-Datenkopie. Die Linux-Client-Blueprints werden vorgehalten, aber nicht produktiv ausgerollt.

7.2 Szenario B – Koexistenz und gezielte Substitution

Die openDesk Enterprise Edition wird parallel zu M365 für definierte Einsatzzwecke betrieben (z. B. sichere Bearbeitung, ausgewählte Organisationseinheiten, externe Kollaboration). M365 bleibt dabei die Hauptplattform. Es wird ein verwalteter Linux-Client für Spezialprofile bereitgestellt.

7.3 Szenario C – Vollsubstitution

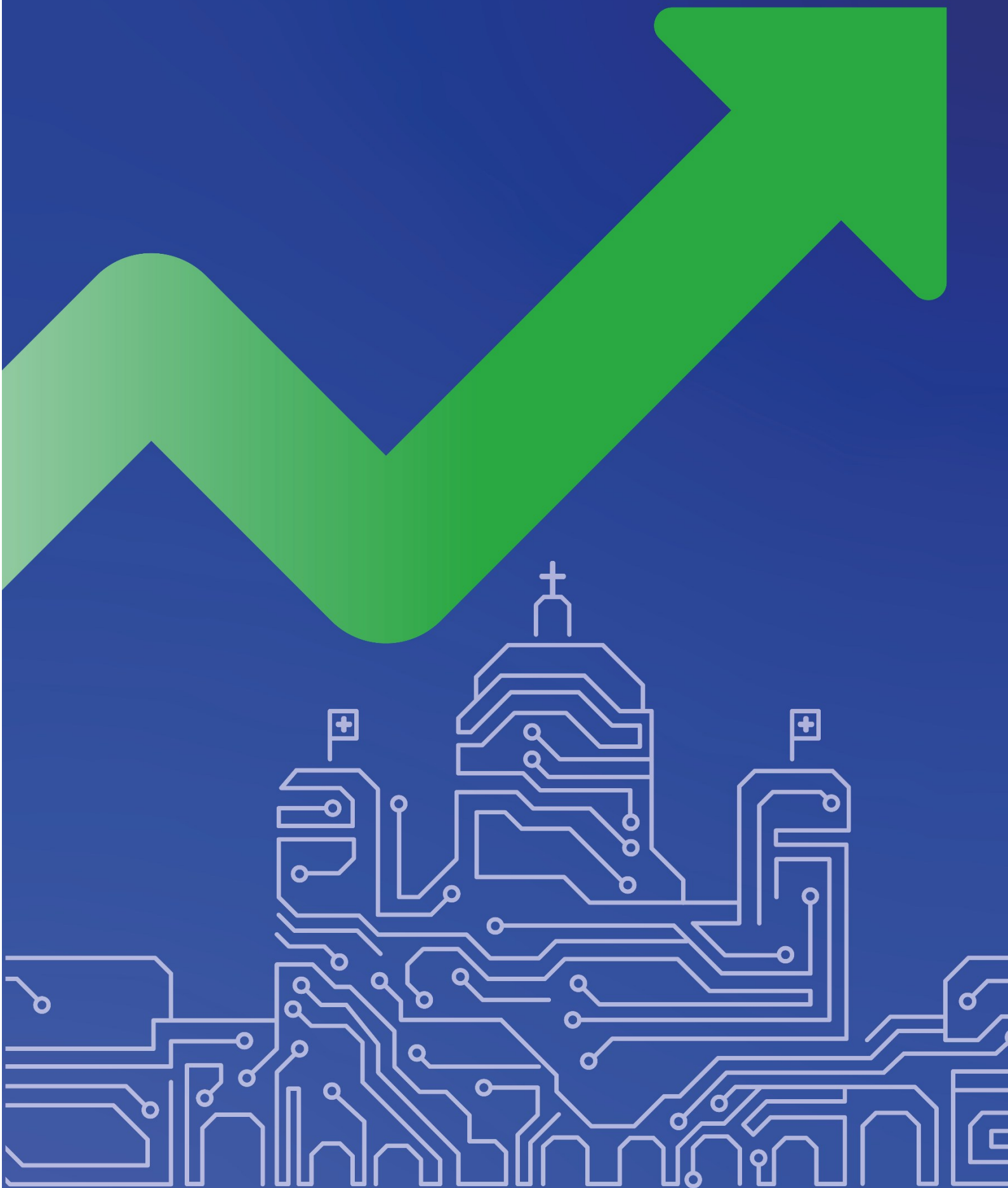
openDesk wird als Primärplattform etabliert, M365 wird über einen mehrjährigen Transformationszeitraum abgelöst. Dieses Szenario erfordert Investitionen in Plattformbetrieb, Client-Management, Fachanwendungs-Portierungen und Change-Management.

7.4 Faktenbezug

Alle drei Szenarien setzen die Enterprise Edition voraus, da die Eignung der Community Edition für eine Bundesverwaltungs-Zielgrösse im PoC nicht verifiziert wurde. Für jedes Szenario sind die in Kap. 6.3 genannten offenen Punkte zu klären – insbesondere Linux-Client-Management, M365-Datenextraktion, GEVER- und SAP-Integration.

8 Abkürzungen und Glossar

Begriff	Bedeutung
agov.ch	Zentraler Login-Dienst des Bundes
APS	Arbeitsplatz-System
BA	Büroautomation
BA-Client	Standard-Arbeitsplatzgerät der Bundesverwaltung
BIT	Bundesamt für Informatik und Telekommunikation
BK DTI	Bundeskanzlei, Bereich Digitale Transformation und IKT-Lenkung
CAE	Container Application Environment des BIT
CE / EE	Community Edition / Enterprise Edition
CEBA	Cloud-Enabling-Büroautomation (Programm zu Einführung von M365 in der BV)
CI/CD	Continuous Integration / Continuous Delivery
CVE	Common Vulnerabilities and Exposures (Sicherheitslücken-Klassifizierung)
DLV	Dienstleistungsvereinbarung
E2EE	Ende-zu-Ende-Verschlüsselung
eIAM	Identitäts- und Zugriffsmanagement-Dienst des Bundes
GEVER	Geschäftsverwaltung (z. B. Acta Nova) der Bundesverwaltung
govdigital	Genossenschaft für vergabefreien Bezug digitaler Leistungen
HPA	Horizontal Pod Autoscaler (Kubernetes)
ISBO	Informatiksicherheitsbeauftragter Organisation
JVB	Jitsi Videobridge
M365	Microsoft 365
MAV	Managed Application Vault
MDM/UEM	Mobile Device Management / Unified Endpoint Management
OAuth2/OIDC	Standardprotokolle für Authentisierung und Autorisierung
openDesk	Open-Source-Workplace-Suite, Produkt von ZenDiS
PoC	Proof of Concept
RHOS	Red Hat OpenShift
RWX	Storage-Modus mit gleichzeitigem Lese- und Schreibzugriff durch mehrere Knoten
SD BA	Standarddienst Büroautomation
SLA	Service Level Agreement
SSF / V3c	Bezeichnung interner BIT-Cluster-Umgebungen
SSO	Single Sign-On
UAT	User Acceptance Test
UDP	User Datagram Protocol
WebDAV	Protokoll für entfernten Datei-Zugriff
ZenDiS	Zentrum für Digitale Souveränität (Anbieter openDesk)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Informatik und Telekommunikation BIT
Domestic Services