PoC-Konzept: Outlook/Exchange ablösen – europäische Groupware unter Linux

Proof of Concept (PoC) zur Auswahl, Pilotierung und Betriebsbewertung einer EU-basierten Groupware-Plattform
mit Linux-Client-Strategie (Mail, Kalender, Kontakte, Delegation, Mobile Sync)

Inhalt

1. Zielbild und Executive Summary

Ziel dieses PoC ist es, eine praxistaugliche Alternative zu Outlook/Exchange zu evaluieren und unter realistischen Betriebsbedingungen zu pilotieren. Der Fokus liegt auf europäischen Betriebs- und Vertragsmodellen, einer Linux-kompatiblen Client-Strategie sowie auf Standards (IMAP/SMTP, CalDAV/CardDAV; optional ActiveSync), um Lock-in zu reduzieren und Souveränitäts- und Compliance-Anforderungen belastbar abzubilden.

Der PoC soll nicht beweisen, dass eine Lösung "100% deckungsgleich" zu Microsoft ist. Er soll zeigen, ob die kritischen Use Cases zuverlässig funktionieren, wie hoch der Migrations- und Betriebsaufwand ist und welche Anpassungen (Prozesse/Schulung) realistisch einzuplanen sind – ohne am Ende ein fragiles Flickwerk zu betreiben.

2. Ausgangslage und Treiber

In vielen Organisationen ist Outlook das Nutzer-Frontend, während Exchange (bzw. Exchange Online) die eigentliche Groupware-Logik bereitstellt. Der administrative Komfort entsteht vor allem durch die tiefe Verzahnung mit Identity/Directory (klassisch Active Directory): Nutzeranlage, Postfach, Berechtigungen/Delegationen und Lifecycle-Prozesse (Joiner/Mover/Leaver) sind stark integriert.

Parallel steigen Anforderungen an Datenresidenz, Drittlandtransfers, Subprozessor-Transparenz und Zugriffskontrolle (Remote-Support, Admin-Zugriffe, Telemetrie). Begriffe wie "EU-Cloud" sind dabei nur dann belastbar, wenn Datenflüsse, Vertragspartner, Betriebsmodell und Schlüssel-/Zugriffshoheit sauber dokumentiert sind.

3. PoC-Umfang

3.1 Im Scope

Der PoC umfasst bewusst sowohl die Endnutzer-Perspektive (Alltagstauglichkeit der Clients unter Linux) als auch die Admin- und Betriebs-Perspektive (Provisioning, Delegation, Monitoring, Backup). Ziel ist kein "Feature-Bingo", sondern ein belastbarer Nachweis, welche Exchange-Kernprozesse im Zielmodell ohne Workarounds funktionieren und wo Prozessanpassungen nötig sind.

Funktionaler Umfang (zu verifizieren in realistischen Use Cases):

1. Mail-Flow Ende-zu-Ende (Ein-/Ausgang, Verteiler, Alias, serverseitige Regeln, Abwesenheiten).
2. Kalender inkl. Einladungen, Delegation (Assistenz-Szenario), Ressourcenbuchung (Raum/Equipment) und Free/Busy.
3. Kontakte inkl. zentralem Adressbuch/GAL-Äquivalent, CardDAV-Sync und Rechte-/Freigabekonzept.
4. Shared Mailboxes bzw. funktionale Entsprechung (Team-Postfächer, gemeinsame Ordner, Berechtigungen).

5. Mobile Sync: iOS/Android mit Standard-Mailclients sowie optional EAS, wenn erforderlich; Prüfung von Remote-Wipe/Policy-Fähigkeiten im Zusammenspiel mit vorhandenem MDM.

Client-Umfang (Linux):

Getestet werden mindestens zwei Nutzungswege: (1) Desktop-Client unter Linux (Thunderbird/Betterbird oder Evolution) und (2) Web-UI/PWA des Groupware-Backends als Fallback bzw. Standard in Web-first-Szenarien. Bewertet werden Bedienbarkeit, Performance, Offline-Verhalten, Suchfunktionen, sowie typische Support-Anfragen (Profil, Zertifikate, Konto-Setup).

Identity, Provisioning und Zugriffsverwaltung:

Der PoC bildet den "Joiner/Mover/Leaver"-Prozess ab: Anlage/Änderung/Deaktivierung von Accounts, automatische Postfachbereitstellung, sowie Zuweisung und Entzug von Berechtigungen (z.B. Stellvertretung, Zugriff auf Team-Postfächer). Dabei werden die gängigen Enterprise-Mechanismen geprüft: SSO (SAML/OIDC), Verzeichnisanbindung (LDAP/AD-Read), sowie automatisiertes Provisioning über SCIM oder definierte Sync-Mechanismen des Produkts.

Betrieb und Wartbarkeit:

Im Scope sind Basisthemen, die in großen Umgebungen über Erfolg oder "Montag brennt's" entscheiden: Patch-/Update-Prozesse (inkl. Rollback-Plan), Monitoring/Alerting (Dienste, Queue, Storage), Log-Aggregation und Audit-Trails, Backup/Restore-Tests (Einzelpostfach, Kalenderobjekte, Konfig), sowie ein Minimal-Runbook für Incident- und Restore-Fälle.

Souveränität, Datenschutz und Compliance:

Der PoC prüft das konkrete Betriebsmodell: Datenresidenz in der EU, AVV/DPA, Subprozessorenliste, Support- und Admin-Zugriffe (Remote Access), sowie technische und organisatorische Maßnahmen. Zusätzlich wird eine pragmatische Drittland-/CLOUD-Act-Risikoabschätzung vorgenommen, basierend auf Vertragspartner, Konzernstruktur und Zugriffspfaden. Ergebnis ist keine Rechtsmeinung, sondern eine dokumentierte Entscheidungsgrundlage für Datenschutz und Security.

Migration (PoC-Teilmenge):

Es wird eine repräsentative Datenstichprobe migriert (z.B. 10-20 Postfächer inkl. Delegation/Shared Mailbox, 3-5 Ressourcen, Kontakte und Kalenderhistorie in definierter Tiefe). Ziel ist, Migrationswerkzeuge und -aufwand zu bewerten, Datenqualität zu prüfen (Einladungen/Serientermine), sowie die notwendigen Cutover-Schritte und Kommunikationsmaßnahmen abzuleiten.

3.2 PoC-Setup, Zielgruppen und Skalierungsannahmen

Der PoC wird in einer isolierten Testumgebung (separates DNS/TLS, Test-Domäne oder Subdomäne) aufgebaut. Als Pilotgruppe werden typischerweise 30-80 Nutzer abgebildet, darunter bewusst "schwierige" Rollen: Assistenz/Delegation, Shared Mailbox-Teams, Viel-Planer (Serientermine), sowie Mobile-heavy User. Für Skalierungsthemen werden nicht 20.000 Nutzer

simuliert, sondern die relevanten Engpässe: Provisioning-Latenz, Storage/IO, Mail-Queue, Backup-Fenster, sowie Admin-Aufwände pro 1.000 Nutzer (hochgerechnet).

3.3 Abnahmekriterien und Messgrößen

Die Abnahme erfolgt anhand messbarer Kriterien statt Bauchgefühl. Dazu zählen: Erfolgsquote der Kern-Use-Cases (Mail/Kalender/Kontakte/Delegation), Anzahl und Schwere von Workarounds, Admin-Aufwand für Joiner/Mover/Leaver und Berechtigungen, Stabilität (Incidents), sowie Wiederherstellbarkeit (Restore-Nachweis). Ergänzend werden Nutzerfeedback und Support-Ticketmuster dokumentiert, um Trainingsbedarf realistisch zu quantifizieren.

3.4 Deliverables

Der PoC liefert: Architektur- und Betriebsdokumentation (Soll/IST), Ergebnisprotokolle je Testfall, Risiko- und Gap-Liste (funktional, betrieblich, compliance), sowie eine Empfehlung für das weitere Vorgehen (Standards-first vs. Exchange-nah vs. Managed EU). Für Enterprise-Szenarien enthält die Empfehlung eine grobe Programmstruktur (Wellen, Co-Existence, Change/Training), damit die Diskussion nicht bei "geht/geht nicht" stehen bleibt.

3.5 Out of Scope (für diesen PoC)

Ersetzung des gesamten Office-Stacks (z.B. MS Office vs. LibreOffice), Teams/Chat/Telefonie, komplexe DLP-Suiten sowie vollständige globale Rollouts. Der PoC liefert jedoch belastbare Input-Daten für ein späteres Programm (20k+ Nutzer).

4. Lösungsansätze (Longlist) und Bewertungslogik

Aus der Diskussion ergeben sich drei robuste Architekturpfade. Der PoC bewertet mindestens zwei davon, um echte Alternativen vergleichen zu können.

4.1 Pfad A – Standards-first Groupware (IMAP/SMTP + CalDAV/CardDAV)

Stärken: geringerer Lock-in, klare Protokolle, gute Linux-Client-Unterstützung. Risiko: einzelne Exchange-spezifische Workflows müssen ggf. angepasst werden.

Beispiele (je nach EU-Betriebsmodell): SOGo, Nextcloud-basierte Kalender/Kontakte-Setups (als Bestandteil), sowie andere DAV-fähige Groupware-Server.

4.2 Pfad B – Exchange-nahe Alternativen aus Europa

Stärken: geringere Nutzerumstellung, oft bessere Abbildung von Delegation/Shared Mailbox/Mobile-Sync nahe am Exchange-Erlebnis. Risiko: höhere Betriebs- und Kompatibilitätskomplexität.

Beispiele: grommunio, Kopano.

4.3 Pfad C – EU-gehostete Groupware-Suite (Managed Service)

Stärken: schneller produktiv, weniger Eigenbetriebsaufwand, Web-UI als stabiler Standardclient. Risiko: Abhängigkeit vom Provider-Operating-Model; vertragliche/technische Souveränität muss geprüft werden.

Beispiele: OX-basierte Anbieter/Services (u.a. mailbox.org als Referenz aus der Diskussion).

4.4 Auswahlkriterien (Kurzfassung)

Die Entscheidung erfolgt nicht über Feature-Listen, sondern über messbare Kriterien:

- Kern-Use-Cases: Mail/Kalender/Kontakte, Delegation/Freigaben, Ressourcen, Shared Mailbox-Äquivalente
- Identity-Integration: SSO (SAML/OIDC), Provisioning (LDAP/SCIM), Gruppen/Rollenmodell
- Betriebsreife: Updates, Monitoring, Backup/Restore (inkl. Test-Restore), Auditing/Logs
- Souveränität: EU-Datenresidenz, EU-Vertragspartner, Subprozessoren, Supportzugriffe, Schlüsselhoheit
- Security: MFA, Admin-Härtung, TLS, SPF/DKIM/DMARC, Rollen-/Rechtekonzept, Incident-Prozesse
- Change/Enablement: Schulungsaufwand, Dokumentation, Supporttickets im Pilot

4.5 Bewertungslogik (Gates + Scoring)

Für eine belastbare Entscheidung wird die Longlist in zwei Stufen bewertet: (1) harte Ausschlusskriterien (Gates) und (2) ein gewichtetes Scoring. Damit wird vermieden, dass einzelne Komfort-Features schwache Souveränität oder Betriebsrisiken „überstimmen“.

Stufe 1 – Gates (Mindestanforderungen):

- EU-Datenresidenz und EU-Vertragspartner sind vertraglich und technisch nachvollziehbar (inkl. Subprozessorenliste, Support-/Remote-Zugriffe, Betriebsorte).
- Kein zwingender US-Anknüpfungspunkt im Betrieb (z. B. US-Support als Standardpfad oder US-Subprozessoren für Kernfunktionen). Falls vorhanden: dokumentierte Risikoabwägung, TOMs und Transfermechanismen.
- Identity und Zugriffsschutz: SSO (SAML oder OIDC) und MFA für Admins; Rollen- und Rechtemodell ist prüfbar.
- Transport- und Speicherschutz: TLS, saubere Cipher-Policies, nachvollziehbare Verschlüsselungsoptionen; Schlüsselmanagement/Schlüsselhoheit ist geklärt.
- Betriebsfähigkeit: Update- und Patchprozess, Backup/Restore inklusive Test-Restore, Logging/Auditing und Monitoring sind vorgesehen und im PoC validierbar.
- Linux-Client-Tauglichkeit: IMAP/SMTP sowie CalDAV/CardDAV (oder gleichwertige Standards) sind funktionsfähig; mobile Nutzung ist im Zielbild abgedeckt.

Stufe 2 – Gewichtetes Scoring:

Bewertet wird auf einer Skala von 0 bis 5 (0 = nicht vorhanden, 3 = erfüllt, 5 = sehr gut/übertrifft). Die Punkte werden mit Gewichten multipliziert. Quellen sind PoC-Tests, Doku-/Vertragsprüfung, Admin-Workshops und Anbieterfragebogen.

Kategorie	Gewicht	Messpunkte/Belege (Auszug)	Mindestniveau im PoC
Funktionale Groupware-Coverage	25%	Mail, Kalender, Kontakte; Delegation/Freigaben; Ressourcen; Shared Mailbox-Äquivalente; Einladungen/Free-Busy	>= 3
Identity & Provisioning	15%	SSO (SAML/OIDC), Gruppen/Rollen, (LDAP/SCIM) Provisioning, Joiner/Mover/Leaver-Abläufe	>= 3
Linux-Client & UX	10%	Thunderbird/Evolution/Web-UI; Kalender/Kontakte-Sync; Offline/Cache; Suchfunktion; Usability im Pilot	>= 3
Mobile & Außendienst	10%	iOS/Android Sync (DAV oder EAS), Richtlinien/MDM-Anbindung, Remote-Wipe/Container (falls relevant)	>= 3
Betrieb & Wartbarkeit	15%	Updates/Upgrades, Backup/Restore, Monitoring, Automatisierung, HA-Optionen, Admin-UI/API	>= 3
Security Controls	15%	MFA/Admin-Härtung, TLS/DMARC/SPF/DKIM, Logging/Audit, RBAC, Incident-Prozesse, Schlüsselmanagement	>= 3
Souveränität & Compliance	10%	EU-Residenz, Subprozessoren, Supportzugriffe, Datenflüsse, Export/Portabilität, Exit-Strategie	>= 4

Hinweis: Die Kategorie „Souveränität & Compliance“ wird bewusst streng bewertet. Ein gutes Ergebnis ist nur möglich, wenn Datenflüsse, Zugriffsmodelle und Vertragsbeziehungen transparent und auditierbar sind.

4.6 Longlist (Produkte/Ansätze) mit Einordnung

Die Longlist ist bewusst heterogen: Sie enthält sowohl standards-basierte Groupware-Stacks als auch exchange-nahe Plattformen und Managed Services. Im PoC werden daraus in der Regel zwei bis drei Kandidaten als Shortlist getestet.

4.6.1 Standards-first Groupware (Pfad A)

SOGo: Standards-orientierte Groupware mit Fokus auf CalDAV/CardDAV und klassische Groupware-Funktionen. Geeignet, wenn offene Protokolle und klare Interoperabilität Vorrang haben. Wichtig im PoC: Delegation/Freigaben, Ressourcen und Mobile-Sync im Zielbetrieb.

Nextcloud als Baustein: In vielen Zielbildern dient Nextcloud als Plattformkomponente (Kalender/Kontakte/Files), nicht zwingend als vollständiger Exchange-Ersatz. Im PoC wird

geprüft, ob die Groupware-Use-Cases ohne Medienbrüche abbildbar sind (z. B. DAV-Sync, Einladungen, Freigaben).

Tine Groupware: Europäische Groupware-Option mit klassischem Groupware-Ansatz. Im PoC ist insbesondere die Integration in Identity/Provisioning und die Alltagstauglichkeit mit Linux-Clients relevant.

4.6.2 Exchange-nahe Alternativen aus Europa (Pfad B)

grommunio: Zielrichtung ist eine exchange-nahe Groupware mit stärkerer Abbildung von Shared Mailboxes/Delegation/Mobile-Sync. Im PoC liegt der Schwerpunkt auf Admin-Aufwand (Provisioning, Rechte), Client-Kompatibilität unter Linux (Standards/Web) und Betriebsreife (Updates, Backup/Restore).

Kopano: Ebenfalls exchange-nahe Groupware mit Fokus auf Collaboration und Outlook-nahe Szenarien. Im PoC werden insbesondere Freigaben/Delegation, mobile Nutzung und Integrations-/Betriebsaspekte bewertet.

4.6.3 EU-gehostete Groupware-Suite (Managed Service, Pfad C)

Open-Xchange-basierte Managed Services: Sinnvoll, wenn ein Provider-Betriebsmodell gewünscht ist und Web-UI als Standardclient akzeptiert wird. Im PoC wird der Schwerpunkt auf Vertrag/AVV, Subprozessoren, Supportzugriffe, Exit-Optionen, sowie Identity-Integration (SSO/Provisioning) gelegt.

mailbox.org (als Referenz): Beispiel für einen EU-Provider-Ansatz aus der Diskussion. Für den PoC ist nicht der Markenname entscheidend, sondern ob das Betriebsmodell die Souveränitätsanforderungen (Residenz, Zugriff, Transparenz, Exit) erfüllt.

4.6.4 Weitere Optionen (Kontext/Benchmark)

Zimbra: Leistungsfähige Groupware, in der Praxis stabil, aber eher „betreiben“ als „Click & Go“. Als Benchmark kann Zimbra hilfreich sein, wenn man Funktions- und Betriebsreife vergleichen möchte. Für EU-Souveränitätsziele ist im Einzelfall die Anbieter-/Betriebsstruktur zu prüfen.

Hinweis: Die Longlist kann je nach Organisation um Appliances, Container-Stacks oder dedizierte EU-Sovereign-Cloud-Angebote erweitert werden. Wichtig ist, dass zusätzliche Kandidaten die Gates erfüllen und in der PoC-Zeit realistisch testbar sind.

4.7 Auswahl- und Entscheidungsprozess im PoC

Die Shortlist wird nach einem transparenten Ablauf gebildet:

6. Longlist-Sichtung und Gate-Prüfung (Datenresidenz, Vertragspartner, Subprozessoren, Supportzugriffe, Identity-Fit).
7. Shortlist von 2–3 Kandidaten mit klarer Hypothese (z. B. „Standards-first mit geringem Lock-in“ vs. „Exchange-nah mit geringer Nutzerumstellung“).
8. PoC-Tests entlang definierter Use Cases (inkl. Assistenz-/Delegationsrollen und Mobile-heavy User) und dokumentierter Testfälle.
9. Scoring und Zusammenfassung der Ergebnisse (inkl. Risiken, Betriebsaufwand, Change-Aufwand, Exit-Strategie).

10. Empfehlung mit Zielbild (Architektur + Betrieb) und Migrationspfad (Pilot/Wellen/Coexistence).

Das Ergebnis ist bewusst mehr als „Tool A gewinnt“. Es umfasst eine begründete Empfehlung, welche Kombination aus Produkt und Betriebsmodell die Anforderungen an Alltagstauglichkeit, Betriebsreife und Souveränität am besten erfüllt.

5. Zielarchitektur für den PoC

Die Zielarchitektur im PoC ist bewusst als modularer Bauplan definiert: Identity bleibt die führende Quelle, Groupware wird als klar abgegrenzter Backbone betrieben und Clients greifen über standardisierte Protokolle zu. So vermeiden wir das typische „Flickwerk“-Gefühl, weil Änderungen an einer Schicht nicht ungeplant Nebenwirkungen in einer anderen Schicht erzeugen – zumindest nicht ohne sichtbare Schnittstelle und Change-Prozess.

5.1 Referenz-Bausteine

5.1.1 Identity & Access (Single Source of Truth)

Identity ist der zentrale Integrationspunkt. Im PoC wird daher festgelegt, dass Benutzer, Gruppen und Rollen nicht in der Mailplattform gepflegt werden, sondern im führenden Verzeichnisdienst. Für bestehende Umgebungen ist das meist Active Directory; alternativ sind EU-konforme Identity-Stacks denkbar. Entscheidend ist: Eine Stelle ist zuständig, und alles andere wird automatisiert nachgezogen.

SSO erfolgt über SAML/OIDC (je nach Lösung und Client/Web-UI). Für Lifecycle-Prozesse (Joiner/Mover/Leaver) wird Provisioning im PoC als eigenes Arbeitspaket getestet: idealerweise SCIM; falls nicht verfügbar, über LDAP-Sync oder Script-/API-gestütztes Provisioning. Ziel ist, dass ein neuer Nutzer nach Freigabe in der Identity innerhalb definierter Zeit automatisch ein Postfach, Standardgruppen und ggf. Default-Policies erhält.

5.1.2 Groupware-Backbone (Mail, Kalender, Kontakte)

Der Groupware-Backbone wird im PoC in drei möglichen Pfaden aufgebaut (Standards-first, Exchange-nah, Managed EU). Unabhängig vom Pfad gelten dieselben Architekturprinzipien: klare Zuständigkeit für Mailbox-Daten, definierte Schnittstellen (IMAP/SMTP sowie CalDAV/CardDAV) und optional ein Mobile-Sync-Mechanismus (DAV oder ActiveSync), wenn dies für die Zielgruppe erforderlich ist.

Für Exchange-typische Funktionen (Shared Mailboxes, Delegation, Ressourcen, Free/Busy) wird je Lösung konkret festgehalten, wie diese abgebildet werden: über native Groupware-Funktionen, über Rollen/Gruppen aus Identity oder über die Web-UI. Die Architektur dokumentiert pro Use Case den „Source of Truth“ und die technische Umsetzung, damit später nachvollziehbar bleibt, wo etwas konfiguriert wird.

5.1.3 Client-Schicht unter Linux & Mobile

Auf Linux wird bewusst nicht versucht, Outlook 1:1 zu kopieren, sondern die produktiven Workflows abzubilden. Im PoC werden zwei Desktop-Client-Profile definiert: (1) Standard-Profil

via IMAP + CalDAV/CardDAV (z. B. Thunderbird/Betterbird oder Evolution) und (2) Web-UI/PWA als Referenz, um Funktionslücken der Desktop-Clients abzufedern (z. B. Delegations-Workflows oder Ressourcenverwaltung, falls clientseitig eingeschränkt).

Für Mobilgeräte wird das Sync-Modell je Pfad festgelegt: DAV-first (CalDAV/CardDAV) oder – falls nötig – ActiveSync. Im PoC wird geprüft, welche Policies (z. B. Geräteverschlüsselung, App-PIN, Remote Wipe) über ein vorhandenes MDM durchgesetzt werden müssen und ob das Zielsystem die erforderlichen Kontrollpunkte bietet.

5.1.4 Mailflow, Edge Security & DNS

Der Mailflow wird im PoC so aufgebaut, dass er später ohne grundlegende Änderungen skalierbar ist: Inbound/Outbound über definierte SMTP-Endpoints, klare Trennung zwischen Transport (MTA/Edge) und Mailbox-Backend (IMAP/Groupware). Optional kann ein vorgeschaltetes Security-Gateway (Spam/Phishing/Malware) genutzt werden, sofern bereits vorhanden oder im Zielbild vorgesehen.

DNS-Konfiguration ist Teil der Zielarchitektur: SPF/DKIM/DMARC werden im PoC aktiv gesetzt und überwacht. Das reduziert Deliverability-Risiken und liefert messbare Ergebnisse (DMARC-Reports, Fehlkonfigurationen, Spoofing-Schutz).

5.1.5 Betrieb: Monitoring, Backup, Updates

Damit der PoC nicht zur „Bastellösung“ wird, ist Betrieb Teil der Architektur. Im PoC werden mindestens Health-Checks, Metriken (CPU/RAM/Storage, Queue-Längen, IMAP/SMTP-Verfügbarkeit), Log-Aggregation und Alerting definiert. Ebenso wird ein Update-Pfad festgelegt (Patchfenster, Rollback, Testinstanz), um zu zeigen, dass die Lösung nicht nur installierbar, sondern nachhaltig betreibbar ist.

Backups erfolgen täglich (Mailbox + Kalender + Kontakte) mit mindestens einem Restore-Test im PoC. Wichtig ist nicht nur „es gibt ein Backup“, sondern: Wiederherstellung einzelner Objekte (z. B. gelöschter Termin), Mailbox-Restore für einen Nutzer und Recovery-Zeit (RTO/RPO) werden zumindest grob validiert.

5.2 Sicherheitsbaseline (PoC muss dies erfüllen)

Die Sicherheitsbaseline ist als Mindestanforderung definiert. Lösungen, die diese Punkte nicht erfüllen, können im PoC zwar technisch getestet werden, gelten aber als nicht zielbildfähig. Damit vermeiden wir, dass am Ende ein funktionales System übrig bleibt, das später aus Compliance-Gründen doch verworfen werden muss.

- Transportverschlüsselung: TLS wird für alle relevanten Schnittstellen erzwungen (SMTP, IMAP, DAV, Web), inklusive moderner Cipher Suites und sauberer Zertifikatskette. Optional: MTA-STS/TLS-RPT, wenn im Zielbild vorgesehen.
- Authentisierung: MFA für Benutzerzugänge und für Admin-Zugänge verpflichtend. Admin-Konten sind getrennt (kein Daily-Driver-Admin). Break-Glass ist definiert und streng protokolliert.

- Domain-Schutz: SPF, DKIM und DMARC werden umgesetzt und im PoC anhand von Reports überwacht. Ziel ist messbar bessere Deliverability und reduzierter Spoofing-Spielraum.
- Protokollierung & Audit: Admin-Aktionen (Konfiguration, Rechte, Delegationen, Rollen) werden nachvollziehbar geloggt; Security-relevante Ereignisse (Login-Anomalien, Policy-Verstöße) sind auswertbar.
- Datenschutz & Zugriffsmodell: Supportzugriffe sind dokumentiert (wer, wann, warum), idealerweise zeitlich begrenzt und nachvollziehbar. Falls Managed Service: Subprozessorenliste, Support-Standorte und Zugriffspfade werden geprüft.
- Backup & Recovery: tägliche Backups inklusive Kalender/Kontakte. Im PoC werden Restore-Szenarien praktisch getestet (Mailbox wiederherstellen, einzelnen Termin zurückholen) und dokumentiert.

5.3 Architekturvarianten je Pfad (PoC-spezifisch)

Da die Longlist verschiedene Ansätze umfasst, dokumentiert der PoC pro Kandidat eine konkrete Referenz-Topologie (z. B. Container-Stack vs. Appliance-Installer vs. Managed Service). Für jede Variante werden mindestens Komponenten, Datenflüsse, Ports/Firewall-Regeln, Identity-Anbindung, Backup-Mechanik und Monitoring-Punkte festgehalten. Das ist bewusst Teil des PoC, weil sich Enterprise-Tauglichkeit häufig genau hier entscheidet.

6. PoC-Plan (Phasen, Deliverables, Zeitbox)

Dieses Kapitel beschreibt einen praxistauglichen PoC-Plan, der sowohl für Managed-EU-Hosting als auch für Self-hosted/Private-Cloud-Varianten funktioniert. Der Fokus liegt auf reproduzierbaren Ergebnissen: messbare Erfolgskriterien, dokumentierte Datenflüsse und ein belastbarer Betriebsnachweis (Monitoring, Backup/Restore, Patch-Prozess).

Empfohlene Zeitbox: 4–6 Wochen (Managed) bzw. 6–10 Wochen (Self-hosted), abhängig von Identity-Integration (SSO/Provisioning), Anzahl der Pilotnutzer, Migrationsumfang (Mail/Kalender/Kontakte) und Mobile-Device-Anforderungen. Kritische Arbeitspakete laufen parallel in Workstreams (Technik, Betrieb, Security/Compliance, Enablement).

Übersicht der Phasen, Deliverables und Exit-Kriterien:

Phase	Zeitbox	Kernaktivitäten (Auszug)	Deliverables	Exit-/Go-No-Go-Kriterien
0 – Initiierung & Scope Freeze	2–5 AT	PoC-Ziele/Use-Cases fixieren, Pilotgruppe benennen, Kandidaten (min. 2) auswählen, Kommunikations- und Supportkanal definieren	PoC-Charter, Erfolgskriterien, Pilotliste, Risiko-Register (initial)	Ziele messbar, Stakeholder benannt, PoC-Umfang abgestimmt
1 – Architektur & Compliance Pre-Check	3–7 AT	Datenflüsse/Unterauftragnehmer, EU-Residenz, Supportzugriffe, Schlüssel-/Krypto-Konzept, Logging-Anforderungen, TOMs-Abgleich	Datenflussdiagramm, AVV/DPA-Checkliste, Threat-/Abuse-Model (leichtgewichtig), Hardening-Baseline (v1)	Keine roten Flags (z.B. ungeklärte Drittlandzugriffe), Mindestanforderungen erfüllt
2 – Build & Integrationen	5–10 AT	Bereitstellung Groupware, DNS/Mailflow (Testdomäne), SSO	Install-/Konfig-Doku, IaC/Config-Snippets	Grundfunktionen laufen stabil,

		(SAML/OIDC), Provisioning (SCIM/LDAP-Sync), Rollen/Delegationen, Mobile-Sync (optional)	(wo möglich), Runbooks (Start/Stop/Backup/Patch), Monitoring-Dashboards (v1)	Admin-Prozesse reproduzierbar
3 – Pilotbetrieb & Migration	10–15 AT	Onboarding Pilotnutzer, Linux-Client Setup (Thunderbird/Betterbird/Evolution/Web), Migration (Mail + optional Kalender/Kontakte), Ticket-Auswertung, UX-Reibungspunkte	Pilot-Guide, Schulungs-Minis (1–2 Seiten), Migrationsprotokoll, Ticket-Report (Top Issues)	Akzeptanzkriterien erreicht, keine Showstopper in Kern-Use-Cases
4 – Betrieb, Security & BCDR Tests	5–10 AT	Patch-/Update-Test, Backup/Restore (objektiv gemessen), Rechte-/Audit-Checks, Last-/Stabilitätsbeobachtung, Abuse/Spam-Szenarien	Restore-Nachweis (RTO/RPO), Security-Testprotokolle, Audit-Log-Review, Betriebsbericht (SLA/SLO Vorschlag)	Recovery und Betrieb nachweisbar, Risiken bewertet und mitigierbar
5 – Auswertung & Entscheidungsvorlage	2–5 AT	Scoring/Benchmark, TCO-Annäherung, Rollout-Roadmap, Migrationsstrategie (Wellen), Entscheidungsvorlage für Steering	Ergebnisbericht, Entscheidungsvorlage, Rollout-Plan (High Level), Backout-/Coexistence-Konzept	Go/No-Go Entscheidung, nächste Schritte freigegeben

6.1 Arbeitsorganisation und Rollen

Für den PoC werden vier Workstreams empfohlen, die in kurzen Zyklen (z.B. tägliches 15-Minuten-Stand-up, wöchentliches Steering) arbeiten: (1) Plattform/Integration, (2) Betrieb/Monitoring/Backup, (3) Security/Compliance, (4) Enablement/Support. Damit wird vermieden, dass technische Fortschritte durch ungeklärte Compliance-Fragen oder fehlende Betriebsprozesse blockiert werden.

Minimal-Rollenmodell: PoC-Lead (gesamt), Plattform-Admin, Identity-Admin, Mailflow/DNS, Security/DSB-Vertretung, ServiceDesk-Lead sowie je Fachbereich 1–2 Pilot-Champions. Für Enterprise-ähnliche Szenarien sollte zudem ein Change-/Kommunikationsverantwortlicher eingeplant werden.

6.2 Phase 0 – Initiierung & Scope Freeze

In dieser Phase werden Zielbild und Messbarkeit festgezurrt. Entscheidend ist, dass nicht "Outlook ersetzen" getestet wird, sondern konkrete Use Cases: z.B. Shared Mailbox + Delegation, Ressourcenbuchung, mobiles Arbeiten, Archiv/Retention, Admin-Prozesse (Joiner/Mover/Leaver).

Deliverables: PoC-Charter (Ziele, Nicht-Ziele, Kandidaten), Erfolgskriterien/Abnahmekriterien, Pilot-Teilnehmerliste inkl. Rollen (Assistenz, Power User, Mobile-heavy), Kommunikationsplan (wie werden Änderungen angekündigt), Supportkanal (Ticket-Queue, SLAs für den PoC) sowie initiales Risiko-Register.

6.3 Phase 1 – Architektur & Compliance Pre-Check

Hier werden die typischen Souveränitätsfragen vor dem technischen Aufbau geklärt: Wo liegen Daten (Residenz), wer hat administrativen Zugriff (Support/Remote), welche Unterauftragnehmer sind beteiligt, wie werden Logs und Backups behandelt, und wer hält welche Schlüssel (wenn Verschlüsselung eingesetzt wird).

Deliverables: Datenflussdiagramm (inkl. Telemetrie/Supportpfade), Checkliste AVV/DPA + Subprozessoren, Definition Logging/Audit-Anforderungen, Hardening-Baseline (MFA, Admin-Rollen, Netzwerksegmentierung), sowie eine kurze Bedrohungsbetrachtung (Abuse/Spam, Account Takeover, Insider/Admin). Exit-Kriterium ist ein "No red flags"-Ergebnis oder dokumentierte Mitigations.

6.4 Phase 2 – Build & Integrationen

Aufbau der Zielumgebung für den PoC: Bereitstellung der Groupware (Managed oder Self-hosted), Einrichtung von Mailflow (MX/Relay, ggf. Testdomäne), SSO via SAML/OIDC, Provisioning (SCIM oder LDAP-Sync), Rollen/Delegationsmodell, Ressourcenpostfächer und ggf. ActiveSync für Mobilgeräte. Parallel werden Monitoring, Backup und Patch-Prozess bereits "PoC-fähig" umgesetzt, nicht erst am Ende.

Deliverables: Konfigurationsdokumentation (inkl. DNS und Mailrouting), Runbooks (Start/Stop, User anlegen/ändern, Delegationen, Backup/Restore, Patch), Monitoring-Dashboards/Alerts (Baseline), sowie ein technischer Betriebssteckbrief (Ports, Abhängigkeiten, Kapazitätsannahmen). Exit: Kern-Use-Cases in einem Admin-Test erfolgreich.

6.5 Phase 3 – Pilotbetrieb & Migration

Onboarding der Pilotnutzer in Wellen (z.B. 10/20/50): Client-Setup unter Linux (Thunderbird/Betterbird/Evolution oder Web), Einrichtung von Kalender/Kontakten (CalDAV/CardDAV), Shared Mailboxes/Delegationen, Ressourcenbuchung und – falls im Scope – Mobile Sync. Die Migration sollte bewusst begrenzt werden (z.B. 3–6 Monate Mailhistorie), um Probleme sichtbar zu machen, ohne den PoC in Datenvolumen zu ertränken.

Deliverables: Pilot-Guide ("Top 10 Aufgaben"), Kurztrainings (15–30 Minuten), Ticket-Report (Kategorien, Zeit bis Lösung, wiederkehrende Ursachen), UX-Reibungspunkte inkl. Workarounds/Policy-Entscheidungen. Exit: definierte Akzeptanzquote (z.B. 80% Kernaufgaben ohne Workaround) und keine offenen Showstopper.

6.6 Phase 4 – Betrieb, Security & BCDR Tests

Nachweis der Betriebsreife: Patch/Update in kontrolliertem Fenster, Backup und Restore mit Zeitmessung (RTO/RPO), Log-Review (Admin-Aktionen, Auth-Events), Rechte-/Delegationsprüfungen sowie Stabilitätsbeobachtung unter realistischer Last (z.B. 50–200 Postfächer im PoC). Zusätzlich sollten Abuse-Szenarien getestet werden (Spam/Phishing, Rate Limits, kompromittierter Account).

Deliverables: Restore-Protokolle, Security-Testprotokolle, Betriebsbericht (Monitoring, Kapazität, Wartungsfenster), aktualisiertes Risiko-Register mit Mitigations. Exit: Recovery ist nachweisbar, Betrieb ist standardisierbar.

6.7 Phase 5 – Auswertung, Entscheidungsvorlage und nächste Schritte

Abschluss mit strukturierter Bewertung: gewichtetes Scoring gemäß Kapitel 4, TCO-Annäherung (Lizenzen, Hosting, Betrieb, Support), Migrations- und Rollout-Roadmap (Wellen, Coexistence), sowie eine klare Entscheidungsempfehlung je Pfad (Standards-first vs. exchange-nahe Alternative vs. Managed).

Deliverables: Ergebnisbericht (PoC-Scorecards, Lessons Learned), Entscheidungsvorlage für Steering (Go/No-Go), sowie ein High-Level-Rolloutplan inkl. Change/Training-Ansatz und Backout-Konzept (z.B. Mailrouting zurück, Datenexport).

7. Testkatalog

Der Testkatalog dient als gemeinsame, nachvollziehbare Prüfliste zwischen IT, Security/Compliance, Betrieb und Pilotnutzer*innen. Er ist so aufgebaut, dass die Ergebnisse pro Lösung (Kandidat A/B) vergleichbar sind und am Ende direkt in das gewichtete Scoring (Kapitel 4) sowie die Go/No-Go-Entscheidung einfließen.

Für jeden Testfall werden mindestens festgehalten: Testumgebung/Version, Tester*in, Datum, Ergebnis (Pass/Fail), Abweichung, Workaround/Restriction und der Nachweis (Screenshot, Log, Export). Kritische Findings werden als Tickets erfasst und priorisiert (Showstopper / High / Medium / Low).

7.1 Testorganisation und Bewertungsregeln

Der PoC bewertet nicht nur Funktionalität, sondern vor allem Reproduzierbarkeit und Betriebsfähigkeit. Ein Test gilt erst dann als bestanden, wenn er mindestens zweimal reproduzierbar ist (z. B. an zwei Tagen oder nach einem Restart), und der Nachweis dokumentiert wurde.

Priorisierung: Must (M) = zwingend für produktiven Betrieb bzw. Risikoakzeptanz; Should (S) = wichtig für Akzeptanz/Komfort; Could (C) = optional, kann in späteren Wellen nachgezogen werden. Showstopper sind insbesondere: ungeklärte Drittlandzugriffe, fehlende Auditierbarkeit, nicht beherrschbarer Admin-Aufwand, instabile Mail-/Kalender-Funktion oder fehlender Restore-Nachweis.

7.2 Testbereiche

Der Testkatalog ist in Bereiche gegliedert: (1) Mailflow und Zustellung, (2) Kalender/Ressourcen, (3) Kontakte/Adressbuch, (4) Identity/Provisioning, (5) Client-Schicht (Linux/Web/Mobile), (6) Security & Compliance, (7) Betrieb/BCDR und (8) Performance. Je nach Lösungspfad (Standards-first, exchange-nah, Managed EU) können einzelne Tests abweichen; Abweichungen werden explizit markiert.

7.3 Master-Testkatalog (PoC)

Die folgende Tabelle bildet den Mindestumfang für einen belastbaren Vergleich. Ergänzend werden projektspezifische Tests (z. B. Archiv/Retention, DLP, Journaling, spezifische MDM-Policies) aufgenommen, wenn sie im Scope liegen.

ID	Bereich	Testfall / Setup (Kurz)	Passkriterium	Nachweis	Prio
F-01	Mailflow	Intern/extern senden & empfangen inkl. 10 MB Anhang; Reply/Forward; MIME/UTF-8	Zustellung < 2 Min, keine Encoding-Fehler, TLS aktiv	Header-Check + Server-Logs	M
F-02	Mailflow	SMTP AUTH/Submission; SPF/DKIM/DMARC Validierung (outbound)	SPF/DKIM pass, DMARC aligned; TLS enforced	Mail-Header + DNS Records	M

F-03	Mailflow	Serverseitige Regeln/Filter (Folder, Weiterleitung intern)	Regeln greifen reproduzierbar, keine Schleifen	Screenshots + Log	S
F-04	Mailflow	Shared Mailbox: Zugriff, Send-as & Send-on-behalf	Rechte wirken innerhalb 5 Min; korrekter From/On-behalf Header	Rechte-Matrix + Testmails	M
F-05	Mailflow	Quotas/Limit-Verhalten (Warnung, Hard limit)	Warnungen/Reject wie definiert; User-Feedback verständlich	Log + Client-Message	S
C-01	Kalender	Einladungen intern/extern, Zu-/Absage, Updates	RFC-konform; Updates überschreiben korrekt; TZ korrekt	Client-Screenshot + ICS	M
C-02	Kalender	Free/Busy und Verfügbarkeiten (Org-intern)	Free/Busy abrufbar, keine Leaks außerhalb Policy	Screenshot + Log	M
C-03	Kalender	Delegation: Assistenz verwaltet Kalender/Einladungen	Lesen/Schreiben/Einladen wie Rollenmodell	Rechte-Matrix + Testprotokoll	M
C-04	Ressourcen	Raum-/Ressourcenbuchung mit Konflikten und Regeln	Auto-accept/deny wie Policy; Konflikte nachvollziehbar	Kalender-Log + Einladung	M
C-05	Kalender	Serientermine, Ausnahmen, Verschiebungen	Keine Dubletten; Exceptions bleiben konsistent	Screenshot + Export	S
K-01	Kontakte	CardDAV Sync (Desktop + Mobile), Kontaktgruppen falls unterstützt	Sync < 5 Min; keine Dubletten; Felder korrekt	Screenshots + DAV-Logs	M
K-02	Adressbuch	Zentrales Verzeichnis (GAL-Äquivalent) / LDAP Lookup	Suche schnell; Rollen/Privacy beachtet	Suche-Screenshot + Config	M
I-01	Identity	SSO (SAML/OIDC) Web-UI; MFA/Conditional Access	SSO stabil; MFA enforced; Session policies wirken	IdP-Logs + Screenshot	M
I-02	Provisioning	Joiner: User anlegen -> Postfach, Gruppen, Default-Policies	Automatisch innerhalb Zielzeit; kein manueller Nacharbeitsschritt	Audit-Log + Provisioning-Report	M
I-03	Provisioning	Mover: Namensänderung/Gruppe/Rolle -> Rechte & Alias	Änderungen propagieren ohne Rechteverlust	Audit-Log + Testmail	S
I-04	Provisioning	Leaver: Deaktivierung, Forward/Archive, Zugriff entziehen	Zugriff entzogen; Mailbox Handling wie Policy	Audit-Log + Admin-Protokoll	M
L-01	Linux Client	Thunderbird/Betterbird Profil: IMAP + DAV; Autodiscovery falls möglich	Setup dokumentiert; Stable sync; keine Datenverluste	Setup-Guide + Screenshot	M
L-02	Linux Client	Evolution Profil: IMAP + DAV oder EWS (falls genutzt)	Kalender/Kontakte nutzbar; Einladungen korrekt	Screenshot + Testprotokoll	S
L-03	Web UI	Web-UI/PWA als Fallback für Delegation/Ressourcen	Kernworkflows ohne Desktop-Client möglich	Testprotokoll	S
M-01	Mobile	iOS/Android: DAV oder EAS; Mail/Kal/Kontakte	Sync stabil; Policies (PIN/Encrypt) umsetzbar	MDM Policy + Test	M
M-02	Mobile	Remote Wipe / Account Removal über MDM	Wipe erfolgreich; Audit nachvollziehbar	MDM Log + Gerätetest	S
S-01	Security	TLS 1.2+ erzwungen; Cipher/Cert-Kette; HSTS (Web)	Keine weak ciphers; gültige Zertifikate	ssllabs/openssl Output + Screenshot	M
S-02	Security	Admin-Interfaces: MFA, IP-Restriktion, RBAC	Adminzugriff gehärtet; least privilege	Config + Audit-Log	M
S-03	Security	Audit-Logs: Admin Aktionen, Login, Zugriff auf Shared	Logs vollständig, manipulationsgeschützt, exportierbar	Log-Auszug + Retention Config	M
S-04	Compliance	Datenflüsse/Subprozessoren/Supportzugriffe dokumentiert	EU-Residenz belegbar; Supportpfade kontrolliert	DPA/AVV Auszug +	M

				Datenflussdiagramm	
O-01	Betrieb	Monitoring: SMTP/IMAP/DAV, Queue, Disk, CPU, Zertifikate	Alarme/Thresholds definiert; Dashboard vorhanden	Monitoring Dashboard	M
O-02	Betrieb	Backup & Restore: Single Mailbox, Kalender, Punkt-in-Zeit	Restore erfolgreich; RTO/RPO gemessen	Restore-Report + Zeiten	M
O-03	Betrieb	Patch/Update-Prozess (Staging -> Prod)	Update ohne Downtime-Überraschung; Rollback möglich	Patch-Protokoll	S
P-01	Performance	Lasttest: 50–200 Postfächer (PoC), Peak Send/Recv, DAV Sync	Antwortzeiten akzeptabel; keine Timeouts	Load-Test Report	S

7.4 Ergänzende Detailtests und typische Stolperstellen

Erfahrungsgemäß entstehen die meisten Probleme nicht bei 'Senden/Empfangen', sondern an den Rändern: Delegation, Shared Mailboxes, Serientermine, Ressourcenregeln, mobile Policies und Admin-Lifecycle. Deshalb werden im PoC zusätzlich folgende Detailtests empfohlen:

- Delegation-Workflows end-to-end: Assistenz lädt extern ein, verschiebt Serie, verarbeitet Updates, sendet als/ im Auftrag.
- Shared Mailbox Governance: Wer darf was, wie werden Rechte zugewiesen (IdP/Gruppe vs. GUI), wie wird das auditiert.
- Zeit-/Zeitzonen-Konsistenz: Sommerzeitwechsel, 'floating' events, mobile vs. desktop Inkonsistenzen.
- Abuse-Szenarien: kompromittierter Account, Rate Limits, Brute-Force Schutz, Quarantäne/Spam-Handling.
- Failure Modes: Was passiert bei IdP-Ausfall, DAV-Timeouts, vollem Disk, Zertifikatsablauf, DNS-Fehlern.

7.5 Abnahme und Ergebnisdokumentation

Am Ende des PoC wird pro Kandidat ein Testprotokoll mit Scorecard erstellt: Anteil bestandener Must/Should-Tests, offene Findings mit Risikobewertung, Workarounds/Restriktionen sowie eine Einschätzung zu Admin-Aufwand und Betriebsreife. Nur wenn alle Must-Tests bestanden sind und kein Showstopper vorliegt, kann ein Kandidat in eine Rollout-Planung überführt werden.

8. Risiken und Gegenmaßnahmen

Dieses Kapitel bündelt die zentralen Risiken für einen PoC zur Ablösung von Outlook/Exchange durch europäische Groupware-Alternativen in einem Linux-Client-Setup – inklusive konkreter Gegenmaßnahmen, PoC-Checks und Abnahmekriterien. Ziel ist, Risiken nicht zu „diskutieren“, sondern im PoC messbar zu machen und Entscheidungsreife herzustellen.

8.1 Bewertungsmodell und Risikokategorien

Für den PoC werden Risiken entlang von Eintrittswahrscheinlichkeit und Auswirkung bewertet (Skala 1–5). Zusätzlich wird vermerkt, ob ein Risiko im PoC direkt getestet oder entkräftet werden kann („PoC-validierbar“) oder erst in der Rollout-Phase adressiert werden muss.

Typische Kategorien sind: Recht/Compliance (z.B. Drittlandzugriffe), Identity und Provisioning, Funktionalität (Delegation/Shared Mailboxes/Ressourcen), Mobile und Clients, Migration und Koexistenz, Betrieb (Updates/Monitoring/Backup), Sicherheit (Hardening/Logging/Incident Response), Skalierung/Performance sowie Change und Enablement.

8.2 Risiko-Register mit Gegenmaßnahmen

Risiko	Beschreibung	Eintritt	Auswirkung	Gegenmaßnahmen im PoC	Nachweis/Abnahme
Drittlandzugriffe/Cloud Act-Relevanz	US-Anknüpfungspunkte (Mutterkonzern, Subprozessoren, Supportzugriffe, Telemetrie) können Zugriffsrisiko und Transfer-Themen auslösen.	Mittel	Hoch	Vendor- und Subprozessorenprüfung, Support-Access-Policy, technische Zugriffspfade (Jump-Host, MFA, Session Recording) definieren; Datenflüsse dokumentieren.	AVV/DPA + Subprozessorenliste geprüft; Zugriffsmatrix + Data-Flow-Diagramm; PoC-Report mit Findings.
Unzureichende AD/IdM-Integration	Fehlende oder fragile Kopplung an AD/IdM führt zu manueller Nutzerverwaltung und erhöhtem Betriebsaufwand.	Mittel	Hoch	SSO (SAML/OIDC) aktivieren; Provisioning via SCIM/LDAP-Sync automatisieren; Joiner/Mover/Leaver-End-to-End testen.	Automatisierte Anlage/Deprovisioning im Test; Rollen/Berechtigungen reproduzierbar; Runbook dokumentiert.
Delegation/Shared Mailboxes nicht gleichwertig	Assistenzszenarien, Zugriffsdelegationen und Team-Postfächer funktionieren anders als in Exchange – Risiko für Akzeptanz.	Mittel	Hoch	Kern-Use-Cases definieren (Lesen/Senden/Antworten, Kalenderpflege, Vertreterregel); mit Pilotrollen testen; Workarounds bewerten.	Testprotokolle mit Erfolgsquote; Gap-Liste + akzeptierte Workarounds/No-Gos.
Ressourcen und Free/Busy inkonsistent	Raum-/Equipmentbuchung und Free/Busy-Abfrage ist je nach Suite/Client unterschiedlich umgesetzt.	Niedrig-Mittel	Mittel-Hoch	Ressourcenobjekte einrichten; Einladungsfluss (intern/extern) testen; Konfliktregeln dokumentieren.	Ressourcenbuchung reproduzierbar; Einladungen/Antworten korrekt; definierte Konfliktregeln.
Mobile Sync / MDM-Policies	Smartphone-Anbindung (EAS/DAV) oder Policy-Umsetzung (PIN, Remote Wipe, Container) kann eingeschränkt sein.	Mittel	Hoch	Mindestsatz an MDM-Policies definieren; iOS/Android-Tests; ggf. EAS vs. DAV vergleichen; Client-Standard festlegen.	MDM-Policy-Tests bestanden; dokumentierte Supported Clients; Risiko-/Restliste.
Migration: Datenqualität und Vollständigkeit	PST/Archivdaten, Kalenderhistorie, Kontakte, Aufgaben und Berechtigungen migrieren nicht vollständig oder	Mittel	Mittel-Hoch	Migrationsscope priorisieren; Stichprobenmigration + Count-Checks; kritische Artefakte (Delegationen) separat verproben.	Migrationsreport (Counts, Stichproben); definierte Nicht-Migrationsobjekte; Restore-Test.

	sind inkonsistent.				
Mail-Deliverability und DNS	SPF/DKIM/DMARC, Reverse DNS und Reputation beeinflussen Zustellbarkeit – besonders beim Providerwechsel.	Niedrig-Mittel	Hoch	DNS-Plan erstellen; DKIM-Signing testen; DMARC-Policy stufenweise; Pilot-Domain/Subdomain für PoC nutzen.	DMARC-Reports; Testmails zu großen Providern; dokumentierter Cutover-Plan.
Betrieb: Patchen/Upgrades brechen Integrationen	Updates/Upgrades können Clients, Plugins oder SSO/Provisioning beeinträchtigen; ohne Prozess droht Stillstand.	Mittel	Hoch	Staging-Updateprozess im PoC; Rollback-Strategie; Version-Pinning; Changefenster und Rollout-Runbook.	Update-Test erfolgreich; Rollback geprobt; Runbook + Wartungsfensterdefinition.
Monitoring/Logging unzureichend	Fehlende Metriken/Logs erschweren Incident Response und Betrieb (Mailflow, Auth, Sync, Queue, Storage).	Mittel	Mittel	Zentrale Logs (SIEM) anbinden; Service-Metriken definieren; Alarmierungsregeln; Synthetic Checks (Login, Send/Receive).	Dashboard/Alerts vorhanden; Beispiel-Incident durchgespielt; Logfelder dokumentiert.
Security Baseline nicht erfüllt	MFA/SSO, Admin-Härtung, TLS-Policy, Least Privilege oder Secrets-Handling werden nicht konsistent umgesetzt.	Niedrig-Mittel	Hoch	Hardening-Checklist; Adminrollen minimieren; Break-glass-Prozess; TLS/Cipher Policy; Secrets-Management.	Baseline-Checklist abgehakt; Konfigurationsreview; Break-glass getestet.
Skalierung/Performance (20k+)	PoC ist klein, Rollout groß: Storage, IOPS, Indexing, Sync-Last, Backupfenster und Supportlast können kippen.	Mittel	Hoch	Lastannahmen + Capacity-Modell; synthetische Tests (Mailboxgrößen, Parallel-Login, Sync); HA/Scale-out-Variante definieren.	Capacity-Sheet; Performance-Report; Skalierungsplan + Grenzwerte.
Enablement und Akzeptanz	Nutzer sind an Outlook gewöhnt; Abweichungen erzeugen Supporttickets und Produktivitätsverlust.	Mittel	Mittel-Hoch	Pilot mit Champions; Fokus-Training auf Top-Workflows; Quick-Guides; Ticket-Kategorisierung; klare Supportpfade.	Ticket-Auswertung; Trainingsmaterial; Abnahme durch Pilotgruppe (Survey).

8.3 PoC-spezifische Exit-Kriterien je Risikogruppe

Damit der PoC nicht in einer reinen Feature-Diskussion endet, werden pro Risikogruppe konkrete Exit-Kriterien definiert. Beispiele: Identity/Provisioning: Joiner/Mover/Leaver vollautomatisiert und dokumentiert. Delegation: die vereinbarten Assistenz-Workflows in mindestens 90% der Testfälle erfolgreich. Betrieb: mindestens ein Update plus Rollback erfolgreich geprobt; Backup/Restore nachweislich möglich. Compliance: Datenflüsse und Zugriffspfade vollständig dokumentiert; vertragliche Prüfungen abgeschlossen. Akzeptanz: Pilotgruppe bestätigt Alltagstauglichkeit; Ticketvolumen im erwarteten Rahmen.

Offene Punkte werden als Rest-Risiken mit Owner, Zieltermin und Maßnahme in die Entscheidungsvorlage übernommen. So ist transparent, was im PoC abschließend geklärt wurde und was bewusst in die Rollout-Planung überführt wird.

9. PoC-Ergebnisartefakte

Dieses Kapitel beschreibt die konkreten Ergebnisartefakte, die nach Abschluss des PoC vorliegen müssen, damit eine belastbare Go/No-Go-Entscheidung sowie eine anschließende Skalierung (Pilot → Rollout) möglich ist. Die Artefakte sind so strukturiert, dass sie sowohl die fachliche Nutzbarkeit als auch den Betrieb (Security, Compliance, Supportfähigkeit) nachvollziehbar belegen.

9.1 Management Summary & Entscheidungsvorlage

Eine kompakte Entscheidungsvorlage (max. 10–15 Seiten) fasst Zielbild, geprüfte Optionen, Ergebnisse und Empfehlung zusammen. Sie enthält ein Kriterien-basiertes Scoring (inkl. Gewichtung), eine klare Risikoeinschätzung (inkl. Restrisiko/akzeptierte Abweichungen), sowie eine Empfehlung für den nächsten Schritt (z. B. erweiterter Pilot, produktiver Rollout oder Abbruch). Wichtig: Die Vorlage benennt explizit, welche Exchange/Outlook-Funktionen im PoC nicht oder nur eingeschränkt abgebildet wurden und welche Maßnahmen für Enterprise-Skalierung erforderlich wären.

9.2 Architekturpaket (Zielbild + Varianten)

Das Architekturpaket dokumentiert die PoC-Zielarchitektur in einer Tiefe, die ein späteres Engineering ermöglicht. Dazu gehören mindestens: (a) logisches Architekturdiagramm (Identity/SSO/Provisioning, Groupware, Client-Schicht, Mailflow, DNS), (b) Datenflussdiagramme inkl. Trust Boundaries, (c) Rollen- und Berechtigungsmodell (Admin-Rollen, Delegation, Shared Mailboxes), (d) Schnittstellenübersicht (Protokolle/APIs, Ports, Abhängigkeiten) und (e) Architekturvarianten je Lösungsansatz (Standards-first vs. Exchange-nahe Variante) mit expliziten Trade-offs.

9.3 Security- & Compliance-Nachweise

Für Datenschutz und Informationssicherheit werden prüffähige Nachweise gesammelt. Das umfasst u. a.: TIA/Transfer-Bewertung (inkl. Subprozessoren, Support-/Remotezugriffe), TOM-Mapping auf interne Richtlinien und ISO/BSI-Kontrollen (sofern anwendbar), Verschlüsselungskonzept (Transport/At-Rest, Schlüsselverwaltung), Logging/Auditing (Welche Events? Aufbewahrung? Manipulationsschutz?), sowie Nachweise zu Data Residency und Mandantentrennung (bei EU-Hosting). Ergänzend sollten Export-/Konfigurationsbelege und Screenshots des Hardening-Status als Appendix bereitgestellt werden.

9.4 Test- und Qualitätsnachweise

Alle relevanten Tests werden nachvollziehbar dokumentiert: Testplan, ausgeführte Testfälle (inkl. Ergebnis/Belege), Defect-Log mit Priorisierung und Status, sowie eine Kurzbewertung der Nutzerakzeptanz (z. B. strukturierte Feedback-Auswertung aus Pilotgruppe). Zusätzlich: Performance-/Stabilitätsmetriken (Login-Zeiten, Sync-Verhalten, Zustellzeiten,

Kalender-Free/Busy), Wiederherstellungstests (RTO/RPO-Nachweis) und – falls relevant – Mobile-Sync-Validierung (iOS/Android).

9.5 Betriebs- und Supportpaket

Das Betriebspaket stellt sicher, dass die Lösung nicht nur „geht“, sondern auch betreibbar ist. Es umfasst Runbooks für Standardprozesse (User Lifecycle, Delegation/Shared Mailboxes, Ressourcen), Monitoring- & Alerting-Konzept (Dashboards, Schwellenwerte, Ticket-Integration), Patch-/Upgrade-Prozess (inkl. Rollback), Backup-/Restore-Playbook, sowie Break-glass-Prozeduren. Ergänzend: Betriebsgrenzen (max. Nutzer je Node, Storage/IO-Bedarf, HA-Konzept) und Support-Schnittstellen (1st/2nd/3rd-Level, Hersteller/Provider).

9.6 Migration & Rollout-Paket

Für die Skalierung wird eine Rollout-Roadmap inklusive Wellenansatz dokumentiert. Dazu gehören eine Migrationsstrategie (Cutover vs. Co-Existence, DNS/MX-Wechsel, Übergangsregeln), Datenmigrationskonzept (Mail, Kalender, Kontakte, ggf. Aufgaben), ein Kommunikations- und Enablement-Plan (Quick Guides, FAQ, Champions-Netzwerk) sowie ein Plan für spezielle Nutzergruppen (Assistenzrollen, Shared Mailboxes, Ressourcenbuchung, mobile Heavy-User).

9.7 Kosten-, Aufwand- und Sizing-Unterlagen

Abschließend werden Sizing und Kosten transparent gemacht: Infrastrukturbedarf (Compute/Storage/Backup), Lizenz-/Subskriptionskosten (falls kommerziell), Betriebsaufwand (FTE-Schätzung nach Rollout-Stufe), sowie ein Vergleich „as-is vs. to-be“ (z. B. Einsparungen durch EU-Hosting, aber zusätzlicher Aufwand für Eigenbetrieb). Diese Unterlagen sind essenziell, um die Diskussion von „Gefühl“ auf „planbar“ zu drehen.

9.8 Artefaktübersicht und Abnahmekriterien

Die folgende Übersicht definiert die Mindest-Artefakte inklusive Abnahmekriterien. Organisationen können die Liste je nach Scope (KMU vs. Enterprise) erweitern.

Artefakt	Inhalt (Kurz)	Format/Ort	Abnahme (Beleg)
Entscheidungsvorlage	Scoring, Empfehlung, Restrisiko, Go/No-Go	DOCX/PDF	Freigabe Steering/IT+DSB
Architekturpaket	Diagramme, Datenflüsse, Rollen, Schnittstellen, Varianten	DOCX + Diagrammdateien	Architekturreview
Testdokumentation	Testfälle, Protokolle, Defects, KPIs, Nutzerfeedback	Testbericht + Tickets	QA/PoC-Leitung
Security & Compliance Pack	TIA/TOMs, Data Residency, Hardening, Logs, Schlüsselkonzept	Appendix + Exporte	ISB/DSB-Freigabe
Betriebshandbuch	Runbooks, Monitoring, Patch, Backup/Restore, Break-glass	Wiki/DOCX	Ops-Abnahme
Rollout- & Enablement-Paket	Wellenplan, Migration, Kommunikation, Trainingsmaterial	DOCX + Inhalte	Change/HR/IT
Kosten & Sizing	BoM, Opex/Capex, FTE, Skalierungsannahmen	XLSX/DOCX	Controlling/IT

10. Anhang: Begriffe

Dieser Anhang erläutert zentrale Begriffe, Abkürzungen und Konzepte aus dem PoC. Die Definitionen sind praxisorientiert und fokussieren auf Relevanz für Auswahl, Betrieb und Compliance der Zielplattform.

10.1 Protokolle & Client-Schnittstellen

Begriff	Kurzbeschreibung	Relevanz im PoC
IMAP	Standardprotokoll zum Abruf und zur Verwaltung von E-Mails auf dem Server.	Basis für Desktop- und Mobile-Clients; vereinfacht Anbieterwechsel.
SMTP	Standardprotokoll zum Versand von E-Mails.	Wichtig für Mailflow, Relays, Auth und Transportverschlüsselung.
CalDAV	HTTP-basiertes Protokoll für Kalender (RFC 4791).	Kalendersync unter Linux (Thunderbird/Evolution) und in vielen Mobile-Apps.
CardDAV	HTTP-basiertes Protokoll für Kontakte (RFC 6352).	Kontaktsync/GAL-ähnliche Szenarien über Adressbücher.
ActiveSync (EAS)	Protokoll für Push-Sync von Mail/Kalender/Kontakten auf Mobilgeräten.	Relevant, wenn native Smartphone-Integration ohne Zusatz-App gefordert ist.
EWS	Exchange Web Services – API für Exchange/Outlook-Integrationen.	Viele Clients/Connectoren nutzen EWS; als Dauerstrategie kritisch (Deprecation-Risiko).
MAPI/MAPI over HTTP	Outlook-typische Schnittstelle für Exchange-Funktionen.	Nur für Exchange-nahe Alternativen relevant; erhöht Komplexität/Lock-in.
JMAP	Modernes JSON-basiertes Mail-API (RFC 8620).	Option für zukünftige Clients; heute noch nicht überall Standard.
Sieve	Serverseitige Filterregeln für E-Mails.	Ersatz für Outlook-Regeln; wichtig für Governance und Nutzerkomfort.
DAV (WebDAV)	Allgemeiner HTTP-Standard für Datei/Objektzugriff.	Manche Groupware nutzt DAV-Mechanismen für Inhalte/Anhänge.

10.2 Identity, SSO & Provisioning

Begriff	Kurzbeschreibung	Relevanz im PoC
AD (Active Directory)	Microsoft-Verzeichnisdienst für Identitäten, Gruppen, Geräte, Policies.	Oft die zentrale Quelle für Benutzer/Gruppen; Integration entscheidet Admin-Aufwand.
LDAP	Verzeichnisprotokoll zur Abfrage/Verwaltung von Identitäten.	Häufige Integrationsschicht für Groupware und Adressbuch/GAL.
SSO	Single Sign-On: einmal anmelden, mehrere Systeme nutzen.	Reduziert Supportaufwand; wichtig für Akzeptanz im Rollout.
SAML 2.0	SSO-Standard für Webanwendungen (Assertions).	Typisch für Browser-basierte Groupware/Webmail.
OpenID Connect (OIDC)	SSO-Standard auf OAuth2-Basis (Tokens).	Modern und verbreitet; gut für Apps/APIs.
OAuth 2.0	Autorisierungsframework für Token-basierte Zugriffe.	Wichtig für moderne Clients und API-Zugriffe.
SCIM	Standard zur automatisierten Nutzer-/Gruppen-Provisionierung.	Ersetzt manuelle Benutzeranlage; reduziert „Flickwerk“-Risiko.
Joiner/Mover/Leaver	Lifecycle-Prozess: Eintritt, Rollenwechsel, Austritt.	PoC prüft, ob Provisioning/Deprovisioning robust und auditierbar ist.
Rollen- und Gruppenmodell	Abbildung von Berechtigungen über Rollen/Gruppen.	Entscheidend für Delegation, Shared Mailboxes, Ressourcen und Policies.

MFA	Multi-Factor Authentication.	Baseline für Cloud/Remote-Zugriffe; im PoC verpflichtend zu testen.

10.3 Mail-Security & Zustellqualität

Begriff	Kurzbeschreibung	Relevanz im PoC
SPF	DNS-Eintrag zur Autorisierung sendender Mailserver.	Reduziert Spoofing; Muss-Kriterium in produktiven Setups.
DKIM	Signaturverfahren für E-Mails mittels Domain-Schlüssel.	Integrität/Authentizität; wichtig für Zustellrate und Anti-Phishing.
DMARC	Policy- und Reporting-Standard auf SPF/DKIM-Basis.	Steuert Quarantine/Reject und liefert Reports; zentral für Governance.
STARTTLS	Aushandlung von TLS über SMTP (opportunistisch).	Standard im Mailtransport; PoC prüft Mindestversionen/Cipher.
MTA-STS	Policy für erzwungene TLS-Zustellung zu einer Domain.	Härtet Transport; relevant für vertrauliche Kommunikation.
TLS-RPT	Reporting für MTA-STS/TLS-Fehler.	Hilft beim Betrieb/Fehleranalyse im PoC.
DANE	DNSSEC-basierte Bindung von TLS-Zertifikaten.	Option für stark gehärtete Umgebungen; abhängig von DNSSEC.
Anti-Spam/Anti-Malware	Filterung und Erkennung schädlicher Inhalte.	PoC bewertet Wirksamkeit, False Positives und Betriebskonzept.
Quarantäne	Isolierung verdächtiger Mails zur Prüfung/Freigabe.	Wichtig für Security und Supportprozesse.
Journaling	Regelbasierte Kopie von Mails zu Compliance-Zwecken.	Relevant für Legal Hold/Regulatorik; im PoC als Option bewerten.

10.4 Datenschutz, Compliance & Souveränität

Begriff	Kurzbeschreibung	Relevanz im PoC
DSGVO	EU-Datenschutzgrundverordnung.	Rahmen für Verarbeitung, TOMs, Betroffenenrechte.
AVV/DPA	Auftragsverarbeitungsvertrag/ Data Processing Agreement.	Pflicht bei Dienstleistern; PoC fordert vollständige Unterlagen.
TOMs	Technische und organisatorische Maßnahmen.	Müssen konkret, prüfbar und passend zum Risiko sein.
DPIA/DSFA	Datenschutz-Folgenabschätzung.	Je nach Risiko/Umfang erforderlich; PoC liefert Input.
RoPA/VVT	Verzeichnis von Verarbeitungstätigkeiten.	Dokumentationspflicht; PoC definiert notwendige Einträge.
Drittlandtransfer	Übermittlung in Länder außerhalb EWR.	Kernrisiko; PoC betrachtet Datenflüsse und Zugriffsmöglichkeiten.
Schrems II	EuGH-Urteil zu Datentransfers (u.a. Anforderungen an SCC/TIA).	Grundlage für Transfer Impact Assessments und Maßnahmenpakete.
CLOUD Act	US-Gesetz mit Zugriffsmöglichkeiten auf Daten US-bezogener Anbieter.	PoC prüft US-Anknüpfungspunkte (Konzern, Support, Subprozessoren).
Datenresidenz	Physische Speicherung/Verarbeitung in einer Region (z. B. EU).	Allein nicht ausreichend; muss mit Kontrolle/Vertragspartner zusammenpassen.
Digitale Souveränität	Fähigkeit, IT unabhängig, kontrollierbar und auditierbar zu betreiben.	PoC bewertet Abhängigkeiten, Exit-Fähigkeit und Transparenz.
Subprozessor	Unterauftragnehmer eines	PoC verlangt Liste, Standorte,

	Dienstleisters.	Zwecke, Kontrollmechanismen.
Schlüsselhoheit	Wer kontrolliert kryptografische Schlüssel.	Relevanz bei Verschlüsselung/Backups; beeinflusst Zugriffsszenarien.

10.5 Betrieb, Architektur & Delivery

Begriff	Kurzbeschreibung	Relevanz im PoC
Managed Service	Betriebsmodell mit ausgelagertem Betrieb durch Provider/MSP.	Reduziert internen Aufwand; PoC prüft SLAs und Zugriffsmodelle.
Self-hosted	Betrieb in eigener Verantwortung (on-prem oder IaaS).	Mehr Kontrolle, mehr Verantwortung; PoC bewertet Betriebsreife.
Appliance	Vorkonfigurierte Lösung (virtuell/physisch) mit Installer/Updates.	Kann Komplexität senken; PoC prüft Update- und Backup-Prozess.
Container (Docker/Kubernetes)	Betrieb über Container-Stacks und Orchestrierung.	Standard in modernen Plattformen; PoC prüft Observability und Patching.
IaC	Infrastructure as Code (z. B. Terraform/Ansible).	Reproduzierbarkeit, Audit, schnelle Wiederherstellung.
Observability	Monitoring/Logging/Tracing als Betriebsgrundlage.	PoC fordert Metriken, Logs, Dashboards, Alerting.
SIEM	Security Information and Event Management.	Anbindung für Korrelation/Detection; PoC prüft Log-Qualität.
Backup/Restore	Sicherung und Wiederherstellung inkl. Tests.	Pflicht: Restore-Test im PoC als Abnahmebedingung.
RTO/RPO	Recovery Time/Point Objective.	Zielwerte für Wiederanlauf und Datenverlust; PoC quantifiziert.
Hardening	Sicherheits-Härtung (Konfig, Dienste, Berechtigungen).	PoC dokumentiert Baseline (TLS, MFA, Adminzugriffe).

10.6 Exchange- und Groupware-Konzepte

Begriff	Kurzbeschreibung	Relevanz im PoC
Groupware	Plattform für Mail/Kalender/Kontakte plus Sharing/Workflows.	Ziel: Exchange-Funktionen funktional ersetzen.
Shared Mailbox	Gemeinsames Postfach für Teams/Funktionen.	PoC testet Rechte, Zugriff, Archivierung und Audit.
Delegation	Berechtigung, für andere zu handeln (z. B. Kalender verwalten).	Kritischer Use Case (Assistenz/Management).
Free/Busy	Verfügbarkeitsanzeige für Terminplanung.	Muss unter Clients/Plattformen konsistent sein.
Ressourcenpostfach	Kalenderobjekt für Raum/Equipment-Buchung.	PoC prüft Buchungsregeln, Konflikte, Moderation.
GAL	Global Address List – zentrales Adressbuch in Exchange.	PoC definiert Ersatz (LDAP/CardDAV/Directory).
Retention	Aufbewahrungsregeln für Inhalte über Zeit.	Governance-Anforderung; PoC bewertet Umsetzbarkeit.
Legal Hold	Sperre gegen Löschung für eDiscovery/Compliance.	Relevanz je Branche; im PoC als Option bewerten.
Client-Standardisierung	Festlegung unterstützter Clients/Versionen.	Schlüssel zur Skalierung (Supportkosten, Stabilität).