

Geschäftsdokument

Leistungsbeschreibung Vg-26-001 – Neuausrichtung der ALDB Kommunikationstechnik

Version 1.0

Stand: 05.11.2026

Inhaltsverzeichnis

1 Ziel 5
1.1 Zeitplanung 6
1.2 Abgrenzung des Leistungsgegenstands 6

2 Ausgangssituation und Rahmenbedingungen 7
2.1 IT-Infrastruktur – Bestand 7
2.1.1 KEIN Internetzugang 7
2.1.2 Betriebssysteme und Virtualisierung 8
2.1.3 Netzwerk 8
2.1.4 Datenbanken 9
2.1.5 Schnittstellen zu Bestandssystemen 10
2.1.6 Monitoring-System und Logging-Infrastruktur 10
2.1.7 Identitäts- und Zugriffsverwaltung 11
2.1.8 Client-Umgebung 11
2.1.9 Weiterentwicklung der Bestandsinfrastruktur 11
2.1.10 Ausstattung der bestehenden Arbeitsplätze 12
2.2 Externe Erreichbarkeit (Telefonie, Nebenstellen) 12
2.3 Mengengerüste/ Anzahl der User 12
2.4 Personaleinsatz und Qualifikation 13
2.5 Zutritt zu Standorten 13
2.6 Fehlerbehebung und Support, Zusätzliche Rahmenbedingungen 14

3 Funktionale Anforderungen 14
3.1 Sprache & Telefonie 14
3.2 ACD (Automatic Call Distribution) 15
3.2.1 Routing & Anrufverteilung 15
3.2.2 IVR und Self-Service 16
3.2.3 Agenten und Supervisoren Ansichten 16
3.2.4 Ticket- und E-Mail-Integration 17
3.3 Wallboard und Reporting 17
3.3.1 Echtzeit-Monitoring & Wallboard 17
3.3.2 Alarmierung & Eskalation 17
3.3.3 Anrufdaten-Schnittstelle & Auswertung 18
3.4 Unified Communication 18
3.4.1 Chats & Messaging 18
3.4.2 Conferencing 18
3.5 Anforderungen an Client Interface und Endgeräte 19
3.6 Endgeräte / Hardphones 20
3.6.1 Lieferung 21

© ALDB 2026

4 Nichtfunktionale Anforderungen 21
4.1 IT-Architekturvorgaben 21
4.2 Software Delivery 22
4.2.1 Allgemeine Anforderungen 22
4.3 Informationssicherheit 23
4.3.1 Software-Bereitstellung 23
4.3.2 Anwendungssicherheit 25
4.3.3 Sichere Kommunikation 25
4.3.4 Nachweis 25
4.3.5 VoIP und TK-Anlagen 26
4.3.6 Webanwendungen/-services/-server 26
4.3.7 Monitoring und Integration mit SIEM 26
4.3.8 Passwortverwaltung 27
4.3.9 Rollen- und Berechtigungskonzept 27
4.3.10 Datensicherung 27
4.4 IT-Betrieb 29
4.4.1 Administration und Konfiguration 29
4.4.2 Notfallbetrieb 30
4.4.3 Notfallübungen 30

5 Leistungsumfang Projektphase 31
5.1 Projektvorbereitung und Konzeption 31
5.2 Implementierung, Testing und Inbetriebnahme 32
5.2.1 Testinstallation (Referenz-IT) 32
5.2.2 Implementierung, Integration und Konfiguration in der Produktiv-Umgebung 33
5.2.3 Migration und Übergangsbetrieb 33
5.3 Abnahme 33
5.3.1 Grundsätze 33
5.3.2 Test- und Abnahmeplan 34
5.3.3 Abnahmestufen 34
5.3.4 Prüfinhalte der Funktionsprüfung 34
5.3.5 Probebetrieb 35
5.3.6 Mängelklassen und Abnahmekriterien 35
5.3.7 Abnahmeprotokoll und Mängelbeseitigung 36
5.4 Erstellung der Betriebsdokumentation 36
5.5 Schulung und Einweisung 37
5.6 Ansprechpartner über die Vertragslaufzeit 38
5.6.1 Projektkoordinator für Installation und Implementierung 38
5.6.2 Kommunikation 39

6 Leistungsumfang Betriebsphase 39
6.1 Softwarewartung und Updates 39
6.1.1 Standard-Releases 39

© ALDB 2026

6.1.2 Sicherheits-Patches 39
6.1.3 Release-Notes, Release-Dokumentation 40
6.2 Service- und Supportleistungen 40
6.2.1 1st Level Support: Hotline und E-Mail-Kontakt für Serviceanfragen und Störungsmeldungen 40
6.2.2 2nd Level Support: Unterstützung durch vorab vereinbarte Mitarbeitende 41
6.2.3 Vor-Ort-Unterstützung: durch vorab vereinbarte Mitarbeitende 41
6.2.4 SLAs: Reaktionszeiten, Lösungszeiten und Prioritäten 41
6.2.5 Eskalationsprozess (technisch/managementseitig) 43
6.3 Weitere Unterstützungsleistungen während der Vertragslaufzeit 43
6.4 Vertragsende und Übergang 44
A. Abkürzungen & Glossar 45

© ALDB 2026

1 Ziel

Die ALDB mit ihren ca. 500 Mitarbeitern betreibt ein Mobilfunknetz im KRITIS-Umfeld, welches Hochverfügbarkeit und erhöhte Sicherheitsmaßnahmen erfordert. Die Kunden des Netzes sind Behörden und Organisation mit Sicherheitsaufgaben, die Erreichbarkeit ist ganzjährig 24/7 zu gewährleisten.

Im Rahmen einer Modernisierungsmaßnahme und aufgrund des auslaufenden Support-Vertrages sollen die bestehende TK-Anlage und ACD ersetzt werden. Gleichzeitig sollen mit dieser Maßnahme bestehende Betriebsaufwände reduziert werden.

Gegenstand des Auftrags ist eine Telekommunikationsanlage (TK) und eine automatische Anrufverteilung (ACD) für die Standorte Berlin und Hannover (Georedundanz) und der Anschluss von vier weiteren Bürostandorten in Berlin, Hannover und Bonn daran und einer eigenständigen Referenz-Anlage.

TK-Anlage und ACD müssen als technisch aufeinander abgestimmte Gesamtlösung betrieben werden können. Die Integration muss über standardisierte, herstellerseitig unterstützte Schnittstellen erfolgen und darf kein kundenspezifisches Customizing oder komplexe Individualschnittstellen erfordern.

Ziel ist die Ablösung der bestehenden TK-/ACD-Landschaft durch eine standortübergreifend hochverfügbare Lösung, die im Active/Active-Betrieb geführt wird, vollständig On-Premise ohne Internetzugang in der bestehenden Infrastruktur der ALDB betrieben wird und den Betrieb rund um die Uhr trägt.

Der Funktionsumfang erstreckt sich über die normale Telefonie mit Chef/Sekretariat- sowie Agent-/ Supervisor Funktionen und Routings im Callcenter, konfigurierbaren Wallboard-Ansichten und Schnittstellen zum Ticketsystem und dem bestehenden Reporting. Im Zuge der Erneuerung kommen Funktionen wie Chat & Messaging sowie Konferenzen & Collaboration hinzu.

Im Rahmen des Auftrags werden folgende Leistungen erbracht:

- Lieferung eines Systems von Softwarekomponenten zur Erbringung der Funktionen, der dafür erforderlichen Lizenzen und der für den Betrieb notwendigen Komponenten
- Erbringung von Projektleistungen (Konzeption, Planung)
- Installation, Erst-Konfiguration und Herstellung der Betriebsbereitschaft innerhalb der Referenz-IT (Testing)
- Installation und Erstkonfiguration an beiden Produktiv-Standorten bis zur Herstellung der Betriebsbereitschaft, d.h. Integration in die bestehende Infrastruktur (Virtualisierung, Betriebssysteme, Datenbanken, Verzeichnisdienste, IAM, Netzwerk)
- Durchführung der Migration nach dem Migrationskonzept der ALDB einschließlich Übergangsbetrieb
- Schulungen für Administratoren und Nutzer inkl. Schulungsmaterial
- Dokumentation für den IT-Betrieb: nach der Beauftragung sind die in dieser Leistungsbeschreibung und den Anforderungskatalogen (Anlagen 2 und 3) genannten Unterlagen zu erstellen bzw. einzureichen.

© ALDB 2026

- Softwarewartung und -updates
- Service und Support-Leistungen
- Weitere Unterstützungs-Leistungen
- Unterstützung bei Vertragsende und Übergang

1.1 Zeitplanung

- Kickoff und Start des Projektes innerhalb von 14 Tagen nach Zuschlag
- Anforderungen an das Voice-Netz und erster Nachweis der Umsetzung der Sicherheitsanforderungen spätestens 4 Wochen nach Zuschlag (Kap. 2.1.3, 4.3.4)
- Feinkonzept einschließlich der Nachweise zu allen MUSS-Anforderungen spätestens 6 Wochen nach dem Kickoff; Freigabe durch die ALDB spätestens 2 Wochen nach Vorlage (Kap. 5.1)
- Betriebsbereitschaft der Referenzumgebung spätestens 2 Wochen nach Freigabe des Feinkonzepts; Teilabnahme 1 spätestens 2 Wochen nach Erklärung der Betriebsbereitschaft
- Umsetzung und Installation vor Ort: Betriebsbereitschaftserklärung für die Produktivumgebung spätestens 4 Monate nach Zuschlag
- Teilabnahme 2 (Produktivumgebung und Migration) spätestens 2 Wochen nach Erklärung der Betriebsbereitschaft der Produktivumgebung; anschließend Probebetrieb über mindestens 14 Kalendertage (Kap. 5.3.3, 5.3.5)
- Ziel ist, nach einer Projektierungsphase und Testinstallation die Installation, Konfiguration und Inbetriebnahme in den Produktivsystemen sowie die Migration von den Bestandssystemen so abzuschließen, dass die Gesamtabnahme nach Ende des Probebetriebs und der Funktionsprüfung spätestens am 30.06.2027 erfolgt.
- Hinweis zur abgeschlossenen Sicherheitsüberprüfung SÜ2: Diese ist aus Zeitgründen sofort nach Zuschlag in die Wege zu leiten. Sollte zum Zeitpunkt der Installation die SÜ2-Überprüfung der entsprechenden Mitarbeitenden des Auftragnehmers noch nicht abgeschlossen sein, müssen sie vollständig durch ALDB-Mitarbeiter begleitet werden, dürfen nicht selbständig im geschlossenen System der ALDB arbeiten, sondern müssen ALDB-Mitarbeiter durch die Installation führen. Die SÜ2 ist aufgrund vertraglicher Vorgaben der Auftraggeberin der ALDB für das Personal im 2nd-Level-Support sowie für Personal, das vor Ort Zugang zu den IT-Systemen benötigt, erforderlich; für den 1st-Level-Support ist sie nicht erforderlich. Hersteller erhalten ausschließlich vorgeprüfte, bereinigte Protokolldaten und benötigen keine SÜ2.

1.2 Abgrenzung des Leistungsgegenstands

Nicht Gegenstand dieses Auftrags sind die Lieferung und der Betrieb der Server-, Virtualisierungs-, Betriebssystem- und Datenbankplattformen; diese werden von der ALDB gemäß Kap. 2.1 beigestellt. Ebenfalls nicht Gegenstand sind die Session Border Controller und die Anschlüsse des Service Providers (Kap. 2.2), die Netzwerk-, Citrix- und Arbeitsplatzinfrastruktur mit Ausnahme der Tischtelefone (Kap. 3.6), die Anpassung der Bestandssysteme (Ticketsystem, Monitoring, SIEM, Datensicherung) über die Bereitstellung und Konfiguration der Schnittstellen der Lösung hinaus sowie Cloud- oder internetbasierte Dienste jeglicher Art.

Der laufende Betrieb der Lösung nach Abnahme erfolgt durch die ALDB. Der Auftragnehmer unterstützt den Betrieb mit den in Kap. 6 beschriebenen Leistungen.

© ALDB 2026

Ebenfalls nicht Gegenstand sind der Rückbau und die Außerbetriebnahme der Bestandssysteme (OXE, Genesys); diese erfolgen durch die ALDB. Eine Migration historischer Reporting- und Anrufdaten ist nicht erforderlich, da diese Daten in einem unabhängigen Rohdatenspeicher der ALDB vorliegen.

2 Ausgangssituation und Rahmenbedingungen

Die TK-Anlage und die ACD werden im KRITIS-Umfeld (kritische Infrastruktur) eingesetzt. Die Systeme sind als hochverfügbare On-Premise Lösung in einer produktiven Umgebung in vollständiger Georedundanz (an zwei Standorten) und Betriebs-Redundanz ausgelegt. Zusätzlich sind noch vier abgesetzte Büro-Standorte an die Anlage angebunden.

Weiterhin sind sie auf einer nichtproduktiven Referenz-Umgebung installiert.

Die bestehende Kommunikationsplattform basiert auf einer Alcatel-Lucent Enterprise OmniPCX Enterprise (OXE), die on-premise im Rechenzentrum der ALDB betrieben wird. Sie stellt die Telefonie-Dienste einschließlich Rufnummernmanagement, Endgeräteanbindung, standortübergreifender Kommunikation und Gruppenfunktionen bereit. Ergänzend ist eine on-premise betriebene Contact-Center-Lösung des Herstellers Genesys (Routing, Warteschlangenmanagement, Reporting, Agenten- und Supervisor-Arbeitsplätze) im Einsatz.

Die bestehende Lösung ist redundant aufgebaut (TK- und Contact-Center-Komponenten, SBC-Infrastruktur, Netzwerkverbindungen, Server- und Virtualisierungsplattformen, Datenspeicher- und Backup-Systeme). Vorhandene Rufnummernkonzepte, Routinglogiken, Contact-Center-Prozesse, Sicherheitsanforderungen sowie Schnittstellen zu Fachverfahren und Drittsystemen sind dabei zu berücksichtigen und ihre Funktionen nach Möglichkeit in die Zielarchitektur zu überführen.

Das System wird den drei Standorten (Hauptstandort, Nebenstandort, Referenzanlage) installiert. Vor einem Rollout auf die Produktiv-Umgebung wird die Funktionalität in der Referenz-Umgebung durch die ALDB geprüft.

Die Client-Lösung muss in der Citrix-Umgebung der ALDB funktionsfähig sein. Die User arbeiten über Citrix in einer geschützten Umgebung OHNE Zugang zum Internet.

2.1 IT-Infrastruktur – Bestand

Die Lösung ist in die nachstehend beschriebene Bestandsinfrastruktur einzupassen. Die genannten Plattformen sind gesetzt. Eine Erweiterung oder Veränderung der Bestandssysteme ist nur im Ausnahmefall und nach vorheriger Abstimmung mit der ALDB zulässig.

2.1.1 KEIN Internetzugang

Die Systeme der ALDB verfügen über keinen direkten Internetzugang. Diese Rahmenbedingung gilt uneingeschränkt für den Produktivbetrieb und die Referenz-IT.

© ALDB 2026

Daraus ergeben sich insbesondere folgende Festlegungen:

- Lizenzen und Softwarepakete müssen lokal eingespielt werden
- Lizenzprüfungen gegen Dienste des Herstellers im Internet sind nicht möglich, weshalb eine Lizensierung ohne Internetverbindung möglich sein muss
- Containerabbilder werden ausschließlich aus internen Quellen bezogen

2.1.2 Betriebssysteme und Virtualisierung

Die Lösung wird auf virtuellen Maschinen betrieben, die durch die ALDB bereitgestellt werden. Der Auftragnehmer gibt den Ressourcenbedarf je Komponente und Standort in der Projektphase (Feinkonzept) an. Die ALDB stellt die virtuellen Maschinen für die Referenzumgebung spätestens 1 Woche nach Freigabe des Feinkonzepts bereit, für die Produktivumgebung nach Abstimmung im Feinkonzept. Liefert der Auftragnehmer eine Appliance mit eigenem Betriebssystem, übernimmt er auch das Patchen dieses Betriebssystems.

Betriebssystem- und Softwarepakete werden ausschließlich über interne Quellen bezogen. Sofern die Lösung Containertechnologie verwendet, ist Podman bevorzugt und Docker alternativ zulässig. Eine Orchestrierung erfolgt über OpenShift. Für die Automatisierung von Installation und Konfiguration wird Ansible eingesetzt.

Das Sicherungsverfahren der ALDB setzt voraus, dass virtuelle Maschinen im laufenden Betrieb gesichert werden können.

Die Plattform ist folgendermaßen aufgebaut:

- **Betriebssystem:** Red Hat Enterprise Linux ab Version 9 (Bereitstellung einschließlich Lizenzen durch die ALDB), höhere Versionen abwärtskompatibel
- **Virtualisierungsplattform:** VMware vSphere 8 mit Standard-Cluster-Management
- **Container-Umgebung:** Podman, alternativ auch Docker
- **Container-Orchestrierung:** OpenShift
- **Konfigurationsmanagement:** Ansible
- **Datensicherung:** Veritas NetBackup ab Version 10.3.0.1
- **Quorum:** Im Falle notwendiger Quorum Devices steht für jeden Hauptstandort ein dritter Standort zur Verfügung. Dieser ist örtlich und netzwerktechnisch getrennt. Quorumserver müssen hier ebenfalls auf einem ESX-Cluster virtualisiert werden.

2.1.3 Netzwerk

Im Rahmen der Einführung wird ein Voice-Netzwerk aufgebaut. Die Anforderungen der Lösung an dieses Netz sind spätestens 4 Wochen nach Zuschlag zu definieren. Notwendige Routingeinstellungen für die Erstinstallation und für einen möglichen Standortausfall notwendige Anpassungen müssen konzipiert werden.

Die Erstellung und Beschreibung von notwendigen Kommunikationsbeziehungen aller Komponenten muss in einer bereitgestellten Kommunikationsmatrix erfolgen.

© ALDB 2026

Die Adressierung erfolgt derzeit über IPv4. Die Lösung muss unter IPv4 betreibbar sein und soll IPv6- und Dual-Stack-fähig sein, so dass eine spätere Umstellung ohne Systemwechsel möglich ist.

Die Zeitsynchronisation innerhalb der Zonen erfolgt über einen internen NTP-Dienst. Öffentliche Zeitserver sind nicht erreichbar.

2.1.4 Datenbanken

Die ALDB betreibt für alle drei zugelassenen Datenbanksysteme (Microsoft SQL Server, Oracle Database und PostgreSQL, siehe unten) hochverfügbare, georedundante Cluster über beide Standorte. Die beauftragte Lösung nutzt eines dieser Cluster. Die führende und dauerhafte Datenhaltung erfolgt ausschließlich in diesem Cluster. Eine lokale oder eingebettete Datenhaltung ist nur zur Zwischenspeicherung und für Konfigurationen der Call Control zulässig, wenn sie deklariert und in Datensicherung, Monitoring und Redundanzkonzept einbezogen ist.

Die Software muss die aktuellen Datenbankversionen unterstützen. Es muss eine Anbindung an die HA-Cluster der ALDB möglich sein, je nach Datenbanksystem Always-On-Cluster, RAC-Cluster oder vergleichbare Verfahren. Die Software muss einen Datenbankschwenk oder Failover transparent unterstützen. Es darf kein Neustart von Komponenten der Lösung wegen eines Datenbankschwenks notwendig sein.

Die Instanzen werden von mehreren Applikationen gemeinsam genutzt (Shared Instance). Der Datenbankbetrieb obliegt ausschließlich dem Fachbereich Datenbanken der ALDB. Dauerhafte Administrationsrechte auf Instanz- oder Serverebene werden dem Auftragnehmer nicht eingeräumt. Erhöhte Rechte für Installation, Update oder Migration werden auf Antrag zeitlich begrenzt erteilt.

2.1.4.1 Hochverfügbarkeit und Standortredundanz

Die Cluster erstrecken sich über beide Standorte, die in getrennten IP-Subnetzen liegen. Der logische Zugriffspfad eines Clusters löst daher auf mehrere Netzadressen auf, von denen zu jedem Zeitpunkt nur eine antwortet. Die vom Auftragnehmer gelieferte Software muss daher ihrerseits multi-subnet-fähig sein.

Die Datenbanken sind zu jedem Zeitpunkt nur an einem Standort aktiv. Applikationskomponenten am jeweils anderen Standort greifen daher über die Standortverbindung zu und unterliegen der dortigen Laufzeit. Zusätzlich erhöht der synchrone Commit die Schreiblatenz. Die Replikation erfolgt synchron. Ein Datenverlust tritt im Failover-Fall nicht ein.

Ein automatisches Failover erfolgt zwischen den Replikaten innerhalb eines Standorts. Der Schwenk auf den zweiten Standort erfolgt ausschließlich manuell, perspektivisch active-active.

2.1.4.2 Wartung und Backup

Die Sicherung der Datenbanken erfolgt zentral durch die ALDB über die nativen Mechanismen des jeweiligen Datenbanksystems, eingebunden in Veritas NetBackup ab Version 10.3.0.1.

© ALDB 2026

Notwendige Replikationsmechanismen, die nicht durch standardisierte Datenbankprozesse wie Export/Import von Datenbanken abgedeckt werden, müssen beschrieben und eingeführt werden.

2.1.4.3 Eingesetzte Datensysteme und Versionen

Folgende Datenbanksystem werden bei der ALDB eingesetzt:

- **Microsoft SQL Server 2019 Enterprise Edition**, Zielversionen 2022 und 2025. Betrieb in Always On Availability Groups mit synchronem Commit, mit automatischem Failover innerhalb eines Standorts und manuellem Schwenk zwischen den Standorten. Zugriff ausschließlich über den DNS-Namen des AG-Listeners
- **PostgreSQL**, Hauptversion 18. Betrieb als HA-Cluster mit Patroni, Zugriffe über HAProxy
- **Oracle Database 19c**. Betrieb mit Oracle Real Application Clusters und Oracle Data Guard

Die produktspezifischen Anforderungen an die Datenbanknutzung sind im Anforderungskatalog nach Datenbanksystem getrennt dargestellt.

2.1.5 Schnittstellen zu Bestandssystemen

Es besteht eine Kopplung an das bestehende Ticketsystem (Remedy Version 4.4.2+28041) über eine REST-Schnittstelle und eine Übergabe aller relevanten Callcenter-Daten an einen bestehenden Rohdatenspeicher. Der Übergabeweg an den Rohdatenspeicher wird in der Projektphase gemeinsam mit dem Auftragnehmer festgelegt, mit dem Ziel eines optimalen Zusammenspiels zwischen der Lösung und den Systemen der ALDB.

2.1.6 Monitoring-System und Logging-Infrastruktur

Die ALDB nutzt Icinga 2 und zukünftig Zabbix als zentrale Anwendung zur System- und Netzüberwachung. Sämtliche installierte Komponenten, Tools und Prozesse müssen in Icinga 2 integriert werden und sollen in Zabbix integrierbar sein. Vom Auftragnehmer sind deshalb die entsprechenden Konnektoren und APIs zu berücksichtigen bzw. bereitzustellen. Ein Alarmbehandlungsplan ist zu erstellen.

Überwachbar sein sollen mindestens:

- Verfügbarkeit jeder Systemkomponente je Standort
- aktiver Standort und Failover-Zustand
- Auslastung der Sprachkanäle
- Anzahl angemeldeter Agenten
- Zustand der Schnittstellen zu Bestandssystemen
- Zustand der Endgeräte
- Datenbankreplikation
- Laufzeiten eingesetzter Zertifikate

Die zentrale Protokollierung der ALDB soll angebunden werden.

© ALDB 2026

2.1.7 Identitäts- und Zugriffsverwaltung

Benutzerkonten werden zentral verwaltet. Die Lösung muss sich in die bestehende Verzeichnis- und Identitätsverwaltung einfügen. Eine eigenständige, getrennte Benutzerverwaltung ist nicht gewünscht. Das Active Directory ist führend. Zulässig sind lokale Notfallkonten für den Fall, dass das AD nicht verfügbar ist (vgl. Kap. 4.3.8 und 4.3.9), sowie die Pflege ACD-spezifischer Profile (z. B. Skills, Routing- und Agentenprofile) in der Applikation.

Konkret wird als Verzeichnisdienst das Microsoft Active Directory verwendet; für Windows-Komponenten sollen (Group-) Managed Service Accounts verwendet werden. Die Verzeichnisdienste sind über beide Standorte verteilt.

Zertifikate werden ausschließlich durch die interne Zertifizierungsstelle der ALDB ausgestellt. Verfahren, die öffentlich vertrauenswürdige Zertifikate, den Abruf von Sperrlisten oder Statusabfragen über das Internet voraussetzen, sind nicht einsetzbar.

LDAP über eine TLS-gesicherte Verbindung (LDAPS) und Single Sign-on (Kerberos) müssen unterstützt werden.

2.1.8 Client-Umgebung

Die Nutzer arbeiten überwiegend in einer virtualisierten Arbeitsplatzumgebung. Eingesetzt wird Citrix Virtual Apps and Desktops.

Der Zugriff auf die virtuellen Arbeitsplätze erfolgt über die Citrix Workspace App auf zentral verwalteten Thin Clients sowie bootfähige USB-Systeme der Firma ECOS. Diese Geräte werden über eine eigene zentrale Verwaltung des jeweiligen Geräteherstellers administriert. Die Installation zusätzlicher Software durch den Auftragnehmer ist nicht vorgesehen. Headsets werden lokal am Zugangsgerät betrieben. Unterstützt werden nur kabelgebundene Geräte. HDX-/Virtual-Channel-Plugins auf den IGEL-Clients sind nicht zulässig; die Audioverarbeitung erfolgt vollständig im Citrix-Server. Dies ist beim Ressourcenbedarf (Kap. 2.1.2) zu berücksichtigen.

Die Client-Umgebung ist folgendermaßen aufgebaut und von der Lösung zu unterstützen:

- **Endgeräte:** ThinClient ab IGEL OS Version 11.150.10 (Eine lokale Installation von Clients ist nicht möglich; die Nutzung erfolgt über den Web-Client in der Citrix-Umgebung)
- **Browser:** Firefox Version 140.11.0esr (64-Bit), Microsoft Edge Version 146.0.3856.62 (64-Bit)

2.1.9 Weiterentwicklung der Bestandsinfrastruktur

Des Weiteren unterliegt die in diesem Abschnitt beschriebene Infrastruktur der laufenden Pflege und Weiterentwicklung durch die ALDB. Der Auftragnehmer sichert den Betrieb der Lösung auch bei Änderungen an dieser Infrastruktur: Patches und Minor-Versionen im Rahmen der Wartung, größere Änderungen über das Abrufkontingent (Kap. 6.3).

Sicherheits- und Fehlerbehebungs-Patches sowie Minor-Versionswechsel der eingesetzten Betriebssysteme, der Virtualisierungsplattform, der Datenbanksysteme, der Verzeichnisdienste,

© ALDB 2026

der Arbeitsplatzvirtualisierung und der Browser dürfen den Betrieb der Lösung nicht beeinträchtigen. Ein gesonderter Vergütungsanspruch entsteht hierdurch nicht.

2.1.10 Ausstattung der bestehenden Arbeitsplätze

Arbeitsplatz Mitarbeiter Standard:

- IGEL, Thin Client (Betriebssystem Linux) oder Ecos Stick (Home-Office) für VPN in das interne ALDB-Sicherheitsnetz und Start eines Citrix Desktops
- Dell UltraSharp 49“ Monitor,
- Teilweise noch Telefon, Alcatel IP Desk Phone, 8086s
- Kabelgebundenes Headset

Arbeitsplatz Mitarbeiter Technischer Betrieb, Callcenter:

- 2 x IGEL, Thin Client (Betriebssystem Linux),
- Dell UltraSharp 49“ Monitor,
- 2. und 3. Monitor,
- Telefon, Alcatel IP Desk Phone, 8086s
- Kabelgebundenes Headset

2.2 Externe Erreichbarkeit (Telefonie, Nebenstellen)

Die externe Erreichbarkeit ist über zwei Anschlüsse des Service Providers Deutsche Telekom realisiert. Der Endpunkt des Serviceproviders liegt jeweils in einer DMZ, die TK-Systeme sind durch eine PAP-Struktur abgesichert.

Pro Standort werden zur Absicherung der Telekom Anbindung jeweils 2 Session Border Controller (SBC) der Firma secunet eingesetzt. Diese sind in eine PAP-Struktur eingebunden. Beide SBCs sind aktiv/aktiv konfiguriert.

Die Lösung muss mit der bestehenden SBC-Infrastruktur einschließlich deren Redundanzkonzept interoperabel sein. Eine Zertifizierung der Interoperabilität ist nicht erforderlich. Die SBC werden durch die ALDB konfiguriert.

2.3 Mengengerüste/ Anzahl der User

Der Auftragnehmer liefert sämtliche für den bestimmungsgemäßen Betrieb erforderlichen Softwarekomponenten und Lizenzen für das beschriebene Mengengerüst. Das Lizenzmodell muss eine mengenmäßige Erweiterung ohne Systemwechsel ermöglichen.

Produktiv-Umgebung: Anzahl der Business User (Nebenstellentelefonie, UC) Anzahl der ACD-Agents (Telefonie, UC und zusätzlich Callcenter-Aufgaben)	mind. 200

© ALDB 2026

Anzahl der maximal gleichzeitig angemeldeten Agents	100
Anzahl der Supervisoren	90
Anzahl der Administratoren	20
Anzahl der Arbeitsplätze mit Hardphone	5
Parallele externe Gespräche (aus der Kapazität der Carrier-Anbindung)	80
	> 60
Referenzumgebung (vollständige Funktionsfähigkeit):	
Business User	15
ACD-Agents	5
Supervisoren	3
Administratoren	2
Parallele externe Gespräche	5

2.4 Personaleinsatz und Qualifikation

Der Auftragnehmer erbringt die Leistungen mit dem Personal, das mindestens über die Qualifikationsanforderungen verfügt, die zum Nachweis der Eignung zu „Techniker oder technische Stellen“ im Rahmen der Prüfung der technischen und beruflichen Leistungsfähigkeit angegeben wurden.

Die personelle Leistungsfähigkeit muss insbesondere die folgenden Leistungsbereiche abdecken:

- tiefgehende technische Expertise
- Supportleistungen,
- Dienstleistungen und Beratungsleistungen.

Der Auftragnehmer legt der ALDB spätestens zwei Wochen vor Beginn der tatsächlichen Leistungserbringung die Namen und die konkreten Qualifikationsnachweisen der tatsächlich eingesetzten Personen vor. Die ALDB kann den Einsatz von Personen ablehnen, wenn diese das erklärte Qualifikationsniveau unterschreiten.

2.5 Zutritt zu Standorten

Der Zutritt zu den Standorten ist nur nach vorheriger Anmeldung möglich, im Regelfall muss diese vier Arbeitstage vorher erfolgen, im Fall von Störungen mit hoher Priorität kann dieser Zeitraum entsprechend gekürzt werden.

© ALDB 2026

2.6 Fehlerbehebung und Support, Zusätzliche Rahmenbedingungen

Aufgrund des Schutzbedarfes der Anwendung werden folgende Anforderungen an den Support und die Problembearbeitung gestellt.

- Die Leistungen zu Support und Fehlerbehebung, inkl. der Hotline, müssen aus Deutschland heraus und in deutscher Sprache erfolgen, wobei Rückfragen bei Herstellern zulässig sind.
- Es dürfen im Rahmen der Support- und Fehlerbearbeitung keine Nutzdaten aus den Systemen an den Auftragnehmer oder Hersteller übermittelt werden. Lediglich die Übermittlung vorgeprüfter und bereinigter Protokolldaten ist möglich. Die Supporterbringung darf von einer vollständigen Datenübermittlung nicht abhängig gemacht werden.
- Es muss gewährleistet sein, dass von der ALDB zum Zwecke einer Fehler-Analyse zur Verfügung gestellte Daten gemäß BSI-Grundschutz in Deutschland oder mindestens nicht außerhalb des Wirtschaftsraumes der Europäischen Union in sogenannten Drittländern gespeichert werden. Dies gilt auch für bereinigte oder anonymisierte Protokolldaten; eine Eskalation an Support-Organisationen außerhalb der Europäischen Union ist ausgeschlossen.

3 Funktionale Anforderungen

Die nachfolgenden Aufzählungen beschreiben den fachlichen Funktionsumfang. Die Verbindlichkeit der einzelnen Funktionen ergibt sich aus dem Anforderungskatalog TK/ACD (Anlage 2).

3.1 Sprache & Telefonie

Die Anlage muss die grundlegende Sprachtelefonie für alle Nutzer standort- und geräteunabhängig sicherstellen. Der Funktionsumfang umfasst klassische Telefonie-Leistungsmerkmale sowie erweiterte Steuerungs-, Verwaltungs- und Kontaktverwaltungsfunktionen:

- Anbindung an das öffentliche Telefonnetz inkl. Verwaltung von zwei getrennten Amtsleitungen. Erreichbarkeit aller Nutzer über externe Rufnummern (ein- und ausgehend), zentrale Service-Rufnummern über die ACD-Lösung
- Übernahme bestehender Rufnummernkonzepte (Amtsrufnummern, Durchwahlblöcke/DDI, Service- und Sonderrufnummern) in einen unternehmensweiten, standortübergreifenden Rufnummernplan inkl. Gruppen-, Funktions- und Notrufnummern
- SIP-Trunking mit Unterstützung mehrerer bzw. redundanter Carrier-Anbindungen, Alternativ- und Überlaufrouting sowie zeitabhängigem Routing
- Klassische Telefonie-Leistungsmerkmale: Anruflisten (personenbezogen, gerätunabhängig, Admin-löschbar), Rückruf bei Besetzt/Nichtmelden, Anklopfen, Halten/Makeln, Dreierkonferenz, Anrufweiterschaltung, Pick-up, Wahlwiederholung, Anrufschutz gegen Spam-Rufnummern.
- Gesprächsvermittlung: Aufbau/Steuerung/Beendigung von Gesprächen, interne Verbindungen, Weiterleitung mit kalter/warmer Übergabe, Rufumleitung, komfortable Wahlmöglichkeiten.
- Notruf-Routing 112/110 mit standortgerechter Zustellung an die zuständige Leitstelle für alle Standorte der ALDB (Berlin, Hannover, Bonn); für Homeoffice-Nutzer anhand einer

© ALDB 2026

Notfalladresse. Die Anlage bietet die Möglichkeit, Notfalladressen zentral zu verwalten bzw. dem Nutzer die Möglichkeit zu geben, diese eigenverantwortlich zu hinterlegen.

- Zusatzfunktionen: Rufnummernanzeige/-unterdrückung, Anrufbeantworter/Voicemail, Warteschleifen mit Musik/Ansage,
- Integriertes Kontaktverzeichnis (interne und externe Kontakte, Teams, Funktionskontakte), Import/Export (CSV, LDAP), für Namenssuche/Kurzwahl nutzbar
- Chef-/Sekretariatsfunktion inkl. Vertretungsregelung bei Abwesenheit der und definierter Überlaufregel.
- Sammelgruppen (standortübergreifend oder lokal), mit An-/Abmeldemöglichkeit, definiertem Berechtigtenkreis und konfigurierbarem Überlauf (use cases: als Türklingel nutzbar bzw. eine zentral administrierbare Rufbereitschaftsnummer),
- Verteilverfahren für Sammelanschlüsse: linear, zyklisch, parallel (gleichzeitiges Klingeln) und priorisiert, inkl. Nachtschaltung, Weiterschaltung bei Nichtmelden und Warteschlange
- Einheitliche Präsenzanzeige (verfügbar, beschäftigt, abwesend, DND, …) über alle Kanäle und Endgeräte hinweg mit Möglichkeit einer Kalendersynchronisation
- Erweiterte Leistungsmerkmale: Rückfrage, Vermitteln, Rufnummernanzeige des Gerufenen (COLP/COLR), Mehrfachrufnummern je Teilnehmer, Abweisen anonymer Anrufe; Rufumleitung sofort, bei Besetzt, bei Nichtmelden, bei Nichterreichbarkeit, zeitgesteuert sowie fernaktivierbar
- Pick-up-Varianten: Gruppen-Pickup, gezielter Pickup einzelner Teilnehmer und abteilungsübergreifender Pickup
- Teamfunktionen: Anzeige des Telefonstatus anderer Teammitglieder, Signalisierung und Übernahme eingehender Anrufe, individuelle Gruppenkonfiguration
- Erreichbarkeit unter einer Rufnummer über mehrere Endgeräte (Tischtelefon, Web-Client, Mobiltelefon, Heimarbeitsplatz) mit parallelem oder seriellem Rufen
- Hot Desking und User Mobility: Anmeldung eines Nutzers an beliebigen Endgeräten mit persönlichem Profil
- Voicemail: persönliche und Gruppen-Mailboxen, mehrere persönliche Ansagen, Nachrichtensignalisierung (MWI), Weiterleitung von Sprachnachrichten an das E-Mail-Postfach
- Erzeugung von Gesprächsdatensätzen (CDR) inkl. Dienstgüte-(QoS-)Daten sowie CTI-Schnittstelle nach einem offenen, dokumentierten Standard (z. B. CSTA, TAPI/JTAPI oder REST)
- Einhaltung der Anforderungen des deutschen Telekommunikationsrechts (u. a. TKG, gesetzliche Notrufanforderungen, Rufnummernübermittlung)

3.2 ACD (Automatic Call Distribution)

Die ACD-Anforderungen regeln die intelligente Verteilung eingehender Kontakte der Agenten über die Service-Nummern sowie die dafür benötigten Steuerungsfunktionen

3.2.1 Routing & Anrufverteilung

- Flexibles Call-Routing über mehrere Servicenummern und Standorte, mit zeit-/wochentags-abhängigen Szenarien; Priorisierung und Schichtung von Service-Rufnummern

© ALDB 2026

- Warteschlangensteuerung: zeit-/lastabhängige Regeln, personalisierte Ansagen, Übernahme bestehender Ansagen, konfigurierbarer Lastüberlauf; Suchkreis-Erweiterung auf weitere Gruppen.
- Agenten erhalten eine feste, standortunabhängige User-ID, Zuordnung zu mehreren Gruppen möglich mit unterschiedlichen Skill-Leveln
- Konfigurierbare, kombinierbare Routing-Mechanismen: Skill-/Competence-based, zeit- und standortabhängig, Same-Agent-Routing, Longest-/Most-Idle, Priorisierung nach Kunde/Anliegen/Wartezeit/SLA.
- Routing auf Basis der Anrufer- und der gewählten Rufnummer (ANI/DNIS) sowie Service-Level-basiertes Routing
- Kalenderbasierte Steuerung mit Tagestypen und Feiertagsprofilen (bundeslandspezifisch)
- Überlauf- und Interflow-Mechanismen bei Wartezeitüberschreitung; gleichzeitiges Einreihen in mehrere Gruppen; virtuelle Warteschlangen
- Callflows und Workflows ohne Programmierkenntnisse; Datenbankabfragen im Callflow
- Standortübergreifende Verteilung (Multi-Site) mit gemeinsamer Warteschlangensicht
- Filterlisten mit Black- und Whitelisting: gezieltes Sperren oder ausschließliches Freigeben definierter Rufnummern, Rufnummernbereiche oder Identifikatoren; die Listen sind administrativ konfigurierbar, revisionssicher dokumentierbar und rollenbasiert steuerbar

3.2.2 IVR und Self-Service

- IVR mit paralleler Sprach- (ASR) und DTMF-Steuerung,
- Import bestehender Ansagen/Audiodateien für Callflows; kurzfristig aktivierbare dynamische Text-to-Speech-Ansage vor Servicenummern, einfach administrierbar
- Automatische Vermittlung (Auto Attendant) bzw. sprachbasierter Vermittlungsdienst; webbasierte Konfiguration der IVR
- Deutschsprachige Text-to-Speech- und Spracherkennungsfunktionen (ASR)
- Anbindung der IVR über standardisierte, dokumentierte, gesicherte und konfigurierbare Schnittstellen (REST) an Backend-Systeme (Ticketsystem Remedy, Workflow-Systeme wie Camunda oder vergleichbare Systeme)
- Outbound-Kampagnenmanagement (Progressive/Preview Dialing, Zielgruppen-Import/-Segmentierung, Anrufzeiten, Sperrlisten) und Dialer-Funktionen (Auto-Dial, AMD-Erkennung, Retry-Logik)
- Automatisierte Anrufer-Authentifizierung (PIN/Kennwort, Namensabfrage)

3.2.3 Agenten und Supervisoren Ansichten

- Informationen zum eingehenden Call: Service-Nummer, Wartezeit, Anrufer-Informationen/ zugehörige Kontaktinformationen
- Persönliche und Team-Statistiken im Frontend (Gesprächsanzahl/-dauer, Status, Team-Belegung, wartende Calls) ohne unautorisierte Offenlegung personenbezogener Details; konsistent zu Wallboard-Daten
- Übersicht der Agentenverfügbarkeit zur betrieblichen Entscheidungsunterstützung
- Hilferuf-Funktion des Agenten an die Supervisoren
- Supervisor-Ansicht je Ressourcengruppe/Agent (Status, Gesprächsstatus, Hilfeanfragen)

© ALDB 2026

- An- und Abmeldung von Agents an einzelnen Warteschlangen; Nicht-verfügbar- und Pausenstatus mit Grundcodes (Reason Codes)
- Automatische Abmeldung bzw. Nicht-erreichbar-Status des Agenten nach Nicht-Annahme eines Anrufs sowie nach Sperren des Bildschirms; konfigurierbar, ob die Wiederfreischaltung durch den Supervisor bestätigt werden muss
- Flexible, gruppenspezifisch konfigurierbare Nachbearbeitungszeit sowie Erfassung von Abschlusscodes (Wrap-up-/Call-Codes)
- Konfigurierbarer Screen-Pop mit Anruferdaten (ANI, DNIS, IVR-Eingaben) und vorheriger Kontakthistorie; Click-to-Dial
- Steuerung von Agentenstatus und Anrufen sowohl im Web-Client als auch am Tischtelefon (CTI-Steuerung)
- Hotdesking und ortsunabhängiges Arbeiten der Agents (z. B. Homeoffice)
- farbcodierte, akustische oder E-Mail-Benachrichtigungen bei Schwellwertverletzungen

3.2.4 Ticket- und E-Mail-Integration

- ACD-TTS-Kopplung (Remedy): automatischer Ticketaufruf aus dem Anrufkontext
- ACD-gestützte E-Mail-Bearbeitung aus Funktionspostfächern: automatische Verteilung, regelbasierte Priorisierung, transparente Pool-/Queue-Sicht

3.3 Wallboard und Reporting

Die Anforderungen an Wallboard & Reporting beschreiben die Echtzeit-Sichtbarkeit des Betriebsgeschehens, die automatisierte Alarmierung bei Schwellwerten sowie die zeitnahe und historisch auswertbare Bereitstellung von Anrufdaten.

3.3.1 Echtzeit-Monitoring & Wallboard

- Für die Supervisoren: frei konfigurierbare Supervisor-Ansichten (Spalten/Sortierung/Filter/Zeitraum)
- Echtzeit-Monitoring für Warteschlangen, angemeldete Agenten, Status, Servicelevel und Auslastung
- Skalierbares Wallboard für Großbildschirme mit anpassbaren, positionierbaren Widgets; Statistiken zu ein-/angenommenen/verlorenen Anrufen je Servicenummer und Agentenstatusübersicht (datenschutzkonform konfigurierbar); darin integriert ist ein konfigurierbarer News-Ticker
- Die Konfiguration des öffentlichen Wallboards/News-Tickers erfolgt durch berechtigte Supervisoren/Administratoren, über eine einfach bedienbare Oberfläche

3.3.2 Alarmierung & Eskalation

- Automatisierte Ad-hoc-Benachrichtigungen (z. B. E-Mail, rot blinkendes Wallboard) bei SLA-Verletzungen (10sec Rufannahme), fehlender Agentenverfügbarkeit oder Unterbesetzung, gesteuert über eine konfigurierbare Eskalations-/Event-Strategie im Callflow (Ereignistyp, Zeitpunkt, betroffene Servicenummer/Gruppen)

© ALDB 2026

- Konfigurierbare akustische Alarmierung bei Schwellwertverletzungen (Unterbesetzung, Anrufannahmeverletzungen) sowie spezifisch für die vereinbarten SLA-Fristen
- Konfigurierbare Ampel-/Schwellwertlogik (z. B. Calls vs. angemeldete Agenten)

3.3.3 Anrufdaten-Schnittstelle & Auswertung

- Über die Schnittstelle zum Rohdatenspeicher werden alle Gespräche im vereinbarten Scope geliefert: eingehende (über Servicenummern und direkt gewählt), ausgehende und interne Gespräche, jeweils einschließlich abgebrochener, weitergeleiteter und übergelaufener Rufe, ohne Rückverfolgbarkeit auf einzelne Agenten.
- Pflicht-Zeitstempel je Ruf (Eingang, Beginn Agentensuche, Annahme, Ende), soweit für die Gesprächsart zutreffend, in Millisekunden-Auflösung ohne Rundung, mit dokumentierter Zeitbasis; Verfügbarkeit spätestens 5 Minuten nach Rufende, persistiert und historisch auswertbar.
- Konfigurierbare Service-Level-Ziele mit Echtzeit-Auswertung; Berücksichtigung aller Medienereignisse (Chat/Mail) in Reports und Echtzeit-Views.
- Direkter SQL-Datenbankzugriff für eigene BI-Auswertungen (inkl. verdichteter Views); Call-Lookup/Einzel-Call-Analyse mit vollständigem Trace (SIP, Gruppe, IVR); konfigurierbare Aufbewahrungsdauer der Reportingdaten.
- Historische Berichte auf Agenten-, Team-, Warteschlangen- und Organisationsebene (agentenbezogene Auswertungen gemäß Gesamtbetriebsvereinbarung), individuell konfigurierbar; Standardberichte u. a. zu Anrufverteilung, Warteschlangen-Performance, abgebrochenen Anrufen und Abschlusscodes
- Automatische, zeitgesteuerte Erstellung und Verteilung von Berichten (z. B. per E-Mail); Export mindestens in den Formaten XLSX und PDF
- Lückenlose Verfolgung eines Kontakts über alle Stationen (Cradle-to-Grave) sowie standortübergreifend konsolidiertes Reporting

3.4 Unified Communication

Die UC-Anforderungen regeln die Bereitstellung von dienstlichen Chat-, Konferenz- und Collaboration-Funktionen innerhalb der gesicherten Umgebung.

3.4.1 Chats & Messaging

- 1:1-Chats sowie administrativ steuerbare Gruppenchats
- Nachvollziehbare, auffindbare Chat-Verläufe
- Kontrollierter Wechsel aus einem Chat in Sprach-/Konferenzkommunikation
- Dateianhänge und Hyperlinks im Chat; durchsuchbare Chat-Historie
- Übernahme von Kalender- und Abwesenheitsinformationen in den Präsenzstatus

3.4.2 Conferencing

- Konferenzlösung für Sprache/Chat/Dokumentenfreigabe mit bis zu 500 Teilnehmern, Collaboration-Funktionen wie Screen-Sharing, Teilen von Dokumenten, Videokonferenz

© ALDB 2026

- Hinzufügen weiterer Teilnehmer zu laufenden Gesprächen, Möglichkeit einer kontrollierten Erweiterung laufender Einzelgespräche, stabiler Konferenzbetrieb bei Teilnehmerzugang oder -abgang
- Rollen- und Moderationskonzept (Initiator/Moderator, Teilnehmer) mit klar geregelten Steuerungsrechten (Stummschalten, Zulassen/Entfernen, Freigaben)
- Möglichkeit der Konfiguration für Start/Beendigung von Konferenzen nur durch berechtigte Nutzer;
- Warteraumfunktion zur kontrollierten Zulassung;
- Steuerung von Bildschirm-/Dokumenten-/Medienfreigaben
- Vollständige Teilnehmerübersicht während der Konferenz (Name, Rolle, Status)
- Geplante und Ad-hoc-Konferenzen, Meet-Me-Konferenzen mit PIN-Einwahl, mehrere Moderatoren, Sperren von Konferenzen, Anzeige des aktiven Sprechers
- Browserbasierte Teilnahme ohne Clientinstallation (WebRTC) sowie telefonische Einwahl in Web- und Videokonferenzen
- Whiteboard, Umfragen/Abstimmungen mit anonymer Auswertung, Konferenz-Chat und Dateifreigabe

3.5 Anforderungen an Client Interface und Endgeräte

Die Client-Lösung muss in der Citrix-Umgebung der ALDB funktionsfähig sein. Die User arbeiten über Citrix in einer geschützten Umgebung OHNE Zugang zum Internet. Lokal zu installierende Desktop-Anwendungen sind ausgeschlossen.

Die Anlage muss in der Citrix-Umgebung externe und soll interne Sprachkommunikation (VoIP/Telefonie) über Nebenstellen-Nummern oder ACD ermöglichen, über die Nutzung von Hardphones bzw. über eine Web-Applikation.

Ziel ist, allen Usern (Business und ACD) eine gemeinsame Kommunikationsplattform bereitzustellen, über die sie intern und extern telefonieren können, Konferenzen und Video-Konferenzen sowie Chat und Messaging nutzen können.

Es sollen neben den Hardphones folgende Möglichkeiten genutzt werden können:

- Browser-basiert (WEB-Client)
- Mobile Endgeräte sollen als bevorzugtes Endgerät („preferred device“) eingebunden werden können. Vorgesehen sind ausschließlich dienstliche Mobiltelefone; private Endgeräte werden nicht eingebunden.

Die Anlage soll ermöglichen, dass alle Nutzer (ACD-Agenten, Supervisoren/Teamleiter, Business-User) sich über die unterschiedlichen Endgeräte/Clients anmelden und erreichbar sein können, sowie selbst entscheiden, über welches Endgerät sie ein Gespräch führen wollen. (z. B. Tischtelefon, Web-Client). Die Funktionalität darf dabei nicht wesentlich vom Endgerät abhängen. Ziel ist eine flexible, aber konsistente Nutzung im dienstlichen Kontext

Der Web-Client muss über Single-Sign-On (SSO) eingebunden werden und innerhalb der vorhandenen Citrix-Umgebung nutzbar sein.

© ALDB 2026

Der Web-Client soll die Arbeit ohne physisches Telefon vollständig ermöglichen (Audio, Video, Präsenz, Kontakte, Anruflisten/Journal mit Filterfunktionen).

Das User-Frontend muss die Grundsätze der Dialoggestaltung nach DIN EN ISO 9241-110 berücksichtigen und eine deutschsprachige Oberfläche besitzen. Die Kernfunktionen (Anmelden, Statuswechsel, Anruf annehmen, übergeben, beenden) müssen auch per Tastatur bedienbar sein; aktive Sitzungen müssen ohne erzwungenen Neustart, erneute Anmeldung oder Leistungseinbruch laufen. Es soll intuitiv bedienbar und benutzerfreundlich sein, anpassbare Dashboards beinhalten und barrierefrei gemäß EN 301 549 / WCAG 2.1 AA sein.

Die Oberfläche soll schnelle Reaktionszeiten (Reaktionszeit bei Statuswechsel max. 2 Sek.) und eine Echtzeitaktualisierung von Status- und Warteschlangeninformationen bieten.

Die Anlage muss den persönlichen Status für alle angemeldeten Nutzer bereitstellen (z. B. frei, im Gespräch, Abwesend, hält Präsentation) und eine eindeutige Signalisierung, die mindestens folgende Aspekte umfasst:

- visuelle Signalisierung (z. B. Anzeige eingehender Anrufe, aktiver Gespräche, Sicherheits- und Verbindungsstatus)
- akustische Signalisierung (z. B. Klingeltöne, Hinweistöne, sicherheitsrelevante Warnsignale)

3.6 Endgeräte / Hardphones

Die 80 Arbeitsplätze, die ein Hardphone benötigen, sind aktuell mit Telefonen Alcatel IP Desk Phone 8086s ausgestattet, sollte diese Hardware für eine Nutzung der erforderlichen Funktionen im Callcenter nicht ausreichend geeignet sein werden beim Auftragnehmer entsprechende Endgeräte/Hardphones angefragt. In der Referenzumgebung werden Hardphones wie in der Produktivumgebung eingesetzt.

Hardphones sollen mindestens folgende Funktionen bereitstellen:

- Unterstützung der von der Anlage verwendeten Protokolle (VoIP/SIP)
- HD Voice für gute Sprachqualität
- Unterstützung kabelgebundener Headsets mit Noise Cancelling
- mehrere Leitungen und Rufzustände
- Funktionstasten
- Anzeige von Präsenz- und Statusinformation
- Headset-Schnittstelle inkl. elektronischem Hook-Switch (z. B. DHSG/EHS) für kabelgebundene Headsets
- frei programmierbare Funktionstasten mit mehrfarbiger LED-Signalisierung; Erweiterbarkeit über Tasten-/Erweiterungsmodule
- Lauthören/Freisprechen im Vollduplex
- integrierter Gigabit-Ethernet-Switch (10/100/1000 Base-T) zum Anschluss des Arbeitsplatzgeräts
- Stromversorgung über Power over Ethernet (IEEE 802.3af) und Energy Efficient Ethernet (IEEE 802.3az)
- grafisches Display, Tisch- und Wandmontage möglich

© ALDB 2026

3.6.1 Lieferung

Mit jeder Lieferung von Geräten gemäß Anforderungskatalog wird eine Datei (Excel/CSV) übersandt indem mindestens folgende Informationen vorhanden sind.

- S/N des Gerätes
- Typ-/Modellnummer
- 4k Hashwert / Device ID
- ggf. Lizenz Key sofern Liefergegenstand
- MAC-Adresse

Lieferungen sollen per Mail mindestens zwei Werktage vorher angekündigt werden. Die Lieferankündigung umfasst alle Arten der Lieferwege (Spedition, Post, usw.)

Die Anlieferung von Geräten in größeren Mengen (größer gleich 30 Geräte) erfolgt nach Absprache auf Palette.

4 Nichtfunktionale Anforderungen

Dieses Kapitel beschreibt die technischen, sicherheitsbezogenen und betrieblichen Anforderungen an die Lösung, die unabhängig von einzelnen Fachfunktionen gelten.

4.1 IT-Architekturvorgaben

Die Zielarchitektur sieht einen standortübergreifenden Active/Active-Betrieb der TK-Anlage und der ACD vor. Die Last liegt im Regelbetrieb auf beiden Standorten. Fällt ein Standort aus, übernimmt der verbleibende Standort automatisch den vollständigen Betrieb, ohne dass sich Service-Rufnummern, externe Erreichbarkeiten oder das Routingverhalten für Anrufer ändern.

Redundanz ist auf zwei Ebenen herzustellen:

- innerhalb eines Rechenzentrums durch Redundanz von Server-Komponenten, Diensten und Netzwerkpfaden (Call-Control- und Medienkomponenten sind je Standort redundant und über zwei Brandabschnitte des Rechenzentrums verteilt.)
- zwischen den Standorten (Geo-Redundanz)
- Integration von Softwareclustern inklusive der Anbindung eines der vorhandenen zentralen Datenbankcluster gemäß Kap. 2.1.4

Die Verfügbarkeit des Gesamtsystems der TK-Anlage darf 99,99% nicht unterschreiten. Die Erreichbarkeit der Service-Nummern beträgt > 99,5 %. Die Werte sind ganzjährig 24/7 zu gewährleisten und beziehen sich auf die Systemverfügbarkeit; Systemgrenze sind die vom Auftragnehmer gelieferten Komponenten. Die Werte gelten für das System, nicht für die von der ALDB beigestellte Umgebung. Messzeitraum ist das Kalenderjahr; die Ermittlung erfolgt über das Monitoring der ALDB.

Bei Ausfall eines Systemknotens übernimmt der verbleibende Knoten ohne manuelle Intervention 100 % der Anruflast. Beim Wechsel in den Einzelknotenbetrieb sowie bei der Wiederherstellung

© ALDB 2026

des redundanten Betriebs (automatischer Failback) dürfen bestehende Gespräche nicht abbrechen. Die Anrufverarbeitung muss auch während eines Upgrades aufrechterhalten werden.

Durch die redundante Architektur des Systems wird erreicht, dass Patches, Updates und Upgrades keine Downtime der Erreichbarkeit der Service-Nummern verursachen. Bei Ausfall einer einzelnen vom Auftragnehmer gelieferten Komponente bleibt die Telefonie einschließlich Anrufverteilung ohne Einschränkung verfügbar; für beigestellte Komponenten gelten die Vorgaben zum Notfallbetrieb einschließlich der zulässigen Einschränkungen bei Nichtverfügbarkeit der Datenbank (Kap. 4.4.2). In der Projektphase muss der Auftragnehmer die Updateprozedur für alle Komponenten vollständig beschreiben. Bei gelieferten Updates ist eine entsprechende Beschreibung des Releases und die Einbringung zu beschreiben.

4.2 Software Delivery

Der Auftragnehmer liefert Softwarekomponenten bzw. ein System für eine hochverfügbare, georedundant ausgelegte TK-Anlage und ACD inkl. zugehöriger Datenbank mit Webclient, Präsenzstatus, Supervisor-Ansicht, Echtzeit-Wallboard und betrieblichen Reports, einschließlich der dafür erforderlichen Lizenzen, die für den Aufbau, Betrieb, Sicherheit und Verfügbarkeit dieser georedundanten Hochverfügbarkeitslösung notwendig sind.

4.2.1 Allgemeine Anforderungen

Die Softwarekomponenten müssen in Summe mindestens die in den Anforderungskatalogen (Anlagen 2 und 3) beschriebenen und mit MUSS klassifizierten Anforderungen für TK-Anlage und ACD abdecken. Dies betrifft die funktionalen Anforderungen als auch die technische und sicherheitsorientierte Perspektive.

Die Softwarekomponenten ermöglichen die aktuell marktüblichen und zeitgemäßen Funktionen von Systemen dieser Art und bieten eine intuitive und ohne Programmierung je nach Zielgruppe anpassbare Benutzeroberfläche.

Die Lösung muss als native, auf offenen SIP-Standards basierende VoIP-Plattform ausgeführt sein und die herstellerunabhängige Anbindung von SIP-Trunks, SIP-Endgeräten, Web-Clients, Session Border Controllern und Drittanwendungen ermöglichen. Sie muss ohne grundlegenden Architekturwechsel mengenmäßig erweiterbar sein.

Die Erfüllung sämtlicher MUSS-Kriterien ist durch Herstellerdokumentation, technische Datenblätter oder vergleichbare Nachweise eindeutig mit Seitenverweis zu belegen. Die Nachweise legt der Auftragnehmer in der Projektphase vor, spätestens mit dem Feinkonzept (Kap. 5.1). Technisch gleichwertige Lösungen sind zulässig; die Gleichwertigkeit ist vom Auftragnehmer nachvollziehbar nachzuweisen.

Für die interne Bürokommunikation werden UC-Komponenten wie Chat, Messaging, Conferencing (Audio und Video) über die Clients bzw. die Nutzer-Interfaces bereitgestellt.

© ALDB 2026

4.3 Informationssicherheit

Die spezifizierten Anforderungen umfassen sowohl Anforderungen an die Software als auch Anforderungen an die Betriebsumgebung der Lösung. Hierzu zählen insbesondere Anforderungen an die zugrundeliegende IT-Infrastruktur, bereitgestellte Plattformdienste, Sicherheitskomponenten, Kommunikationsverbindungen sowie angebundene Umsysteme.

Die ALDB betreibt ein nach ISO/IEC 27001 und ISO/IEC 27019 zertifiziertes Informationssicherheitsmanagementsystem (ISMS) gemäß den Anforderungen des IT-Sicherheitskatalogs der Bundesnetzagentur. Der Auftragnehmer ist verpflichtet, sämtliche für die Leistungserbringung relevanten Vorgaben, Richtlinien, Prozesse und Verfahren dieses ISMS einzuhalten, an erforderlichen Sicherheits- und Compliance-Maßnahmen über die gesamte Vertragslaufzeit mitzuwirken und die Einhaltung auf Anforderung nachzuweisen.

Die Lösung ist für den Einsatz in VS-NfD-Umgebungen geeignet durch den Schutz von Sprach-, Video-, Chat- und Metadaten vor unbefugtem Zugriff sowie die Verschlüsselung von Signalisierung, Medien und gespeicherten Daten nach BSI TR-02102 (Stand der Technik). Der Auftragnehmer beschreibt in der Projektphase, wie die Lösung die Vorgaben der VSA im geschützten Netz der ALDB unterstützt.

Die ALDB erhält Audit- und Auskunftsrechte beim Auftragnehmer (Audits nach Ankündigung). Der Auftragnehmer unterstützt interne und externe Audits und stellt aktuelle Zertifikate und Prüfberichte bereit.

Der Anforderungskatalog Sicherheit (Anlage 3) beschreibt die weitergehenden konkreten Anforderungen zu

- VoIP und TK-Anlagen
- Web-Servern, -Services und –Anwendungen
- Passwortverwaltung
- Container
- Virtualisierung
- Rollen- und Rechtekonzept

4.3.1 Software-Bereitstellung

4.3.1.1 BSI IT Grundschutz

Der Auftragnehmer nutzt Tools und Erweiterungen zur Erfüllung von Anforderungen aus BSI IT-Grundschutz, u.a.:

- Auditing / Nachvollziehbarkeit
- Verschlüsselung (Transport und/oder ruhende Daten, gemäß Zielarchitektur der ALDB)
- Unterstützung bei Härtungsmaßnahmen (z. B. sichere Default-Konfigurationen, Rollen-/Rechtekonzepte)

© ALDB 2026

Vor der Übergabe der Software-Pakete sind alle dafür relevanten Grundschutz-Bausteine anzuwenden, bzw. -sofern notwendig- in Absprache mit der ALDB daran mitzuwirken vor allem

- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung (Umsetzung gemäß Anforderungskatalog Sicherheit, S-016)
- OPS.1.1.6 Software-Tests und -Freigaben
- APP.4.3 Relationale Datenbanksysteme

Ein Audit bzw. Zertifizierung durch das BSI wird hier nicht verlangt.

Die Lösung soll auf nach CIS-Benchmarks gehärteten Systemen betreibbar sein und deren Einsatz unterstützen.

4.3.1.2 Schwachstellenanalyse

Vor der Bereitstellung der Software müssen sämtliche Software-Komponenten vom Auftragnehmer einer Schwachstellenanalyse unterzogen worden sein.

Diese Schachstellen-Analyse sollte vor allem folgendes beinhalten:

- Identifizierung: Scannen auf Schad-Software und bekannte Sicherheitslücken im Sinne der geltenden BSI-Grundschutzanforderungen
- Bewertung & Klassifizierung: Die gefundenen Schwachstellen werden vom Auftragnehmer analysiert, nach Risiko bewertet (z. B. kritisch, hoch, mittel, niedrig) und deren Auswirkungen auf das Unternehmen eingeschätzt.
- Maßnahmenplanung: Der Auftragnehmer gibt auf Grundlage der Risiko-Analyse eine Handlungsempfehlung ab, und unterstützt bei der Maßnahmenumsetzung und deren Priorisierung. (Risikomanagement).

4.3.1.3 Regression-Tests

Vor der Bereitstellung neuer Software muss sichergestellt werden, dass bestehende Funktionalitäten weiterhin einwandfrei funktionieren und keine neuen Fehler entstanden sind. Dies schließt ebenfalls die Kompatibilität der Software zur ALDB-Plattform und den Toolschnittstellen ein.

Die Funktionalität / Kompatibilität ist durch entsprechende Regression-Tests nachzuweisen und zu dokumentieren sowie der ALDB zu übergeben.

4.3.1.4 Download-Plattform

Der Auftragnehmer muss die Software-Komponenten über eine von ihm betriebene Download-Plattform (z. B. SharePoint) bereitstellen, auf das die ALDB zum Zwecke des Software-Downloads zugreifen kann.

© ALDB 2026

Ebenso soll es der ALDB ermöglicht werden, Daten (z.B. Logs, oder Configs) für den Auftragnehmer zur Analyse abzulegen. Die Download-Plattform ist Bestandteil der IT-Infrastruktur des Auftragnehmers und unterliegt deshalb auch den allgemeinen Anforderungen an die IT-Infrastruktur des Auftragnehmers.

Anforderungen:

- Authentifizierung/Autorisierung für den Zugriff auf die Download-Plattform: Die Authentifizierung muss den aktuell gültigen Richtlinien des BSI entsprechen. Eine 2FA wird gefordert.
- Integritätsnachweise für Software-Pakete: Dies können z. B. Signaturen und/oder Checksummen sein

4.3.2 Anwendungssicherheit

Die Webanwendung ist nach dem Stand der Technik unter Berücksichtigung der jeweils aktuellen OWASP Top 10 – Web Application Security Risks zu entwickeln, zu testen und zu betreiben. Insbesondere sind geeignete Maßnahmen gegen Injection, fehlerhafte Zugriffskontrollen, unzureichende Authentisierung, Cross-Site-Scripting sowie unsichere Abhängigkeiten und Konfigurationen umzusetzen.

4.3.3 Sichere Kommunikation

Die Kommunikation der Applikation sowie ihrer Komponenten soll gegen unbefugtes Mitlesen und Manipulation abgesichert werden. Es sollen sichere Protokolle verwendet werden. Für den Einsatz von TLS sollen die Empfehlungen der BSI TR-02102-2 „Kryptographische Verfahren: Verwendung von TLS“ in der jeweils gültigen Fassung eingehalten werden. Unsichere bzw. nicht mehr empfohlene Protokollversionen, Algorithmen und Cipher Suites sollen nicht eingesetzt werden.

Signalisierung und Medienströme sollen verschlüsselt übertragen werden (SIP über TLS, SRTP). Die Verschlüsselung soll neben Signalisierung und Medien auch Service- und Administrationszugänge umfassen. TLS 1.3 soll unterstützt werden. Die Lösung soll ein Zertifikatsmanagement bereitstellen, das mit der internen Zertifizierungsstelle der ALDB betrieben werden kann.

4.3.4 Nachweis

Der Auftragnehmer soll die Umsetzung der Sicherheitsanforderungen erstmals spätestens 4 Wochen nach Zuschlag und während der Vertragslaufzeit auf Verlangen durch geeignete Nachweise, insbesondere Sicherheitsprüfungen bzw. Schwachstellenanalysen und eine Dokumentation der TLS-Konfiguration, belegen. Festgestellte kritische Sicherheitslücken sollen vor der produktiven Inbetriebnahme behoben werden. Der Auftragnehmer soll sich verpflichten, die Webanwendung nach OWASP Application Security Verification Standard (ASVS), Level 2, in der zum Zeitpunkt der Leistungserbringung aktuellen Fassung umzusetzen.

© ALDB 2026

4.3.5 VoIP und TK-Anlagen

Den Anforderungen für den Betrieb aller TK-Anlagen und VoIP-Systeme innerhalb der ALDB GmbH (ALDB) liegen die folgenden Bausteine des BSI-Grundschutzkompendiums zugrunde:

- NET.4.1 TK-Anlagen
- NET.4.2 VoIP

4.3.6 Webanwendungen/-services/-server

Eine Abgrenzung zwischen Webanwendungen, Webservices und Webserver lässt sich wie folgt durchführen:

„**Webanwendungen** stellen Funktionen und dynamische Inhalte zur Verfügung. Sie nutzen dazu das Internetprotokoll HTTP (Hypertext Transfer Protocol) bzw. HTTPS. Bei HTTPS wird die Verbindung durch die Protokolle SSL (Secure Socket Layer) oder TLS (Transport Layer Security) verschlüsselt und zusätzlich gesichert. Webanwendungen erstellen auf einem Server Dokumente und Benutzeroberflächen, z. B. Eingabemasken, und liefern diese an entsprechende Clientprogramme, wie etwa Webbrowser.“ (Quelle: Baustein APP.3.1)

„**Webservices** sind Anwendungen, die das http(S)-Protokoll verwenden, um Daten für andere Anwendungen bereitzustellen. In der Regel werden sie nicht unmittelbar durch Benutzer angesteuert.“ (Quelle: Baustein APP.3.1)

„Der **Webserver** ist die Kernkomponente jedes Webangebotes, er nimmt Anfragen der Clients entgegen und liefert die entsprechenden Inhalte zurück. Die Daten werden in der Regel über HTTP oder dessen mit TLS verschlüsselte Variante HTTPS transportiert.“ (Quelle: Baustein APP.3.2)

4.3.7 Monitoring und Integration mit SIEM

4.3.7.1 Meldungen und Monitoring

Grundsätzlich sollen alle sicherheitsrelevanten Logfiles an die zentrale Sicherheits-Log-Management-Lösung gesendet werden, welche die Logfiles von definierten Systemen (Quellen) empfängt (Ablage) und verwaltet. Innerhalb der Logdaten erfolgt eine stetige Suche nach sicherheitsrelevanten Ereignissen und Mustern, welche bei Auffälligkeiten und Abweichungen Alarme auslösen. Die zentrale Sicherheits-Log-Management-Lösung wird mit einem Security Information and Event Management Produkt (SIEM) implementiert und daher kurz mit dem Begriff SIEM-System bezeichnet.

Die Lösung soll eine lückenlose Protokollierung administrativer und sicherheitsrelevanter Aktivitäten (Activity Logging, Ereignisverfolgung, System-Historie) bereitstellen. Zur Fehleranalyse soll ein integriertes oder mitgeliefertes Werkzeug zur Aufzeichnung, Sammlung und Verwaltung von Diagnose- und Protokolldaten (Traces) zur Verfügung stehen.

© ALDB 2026

4.3.7.2 Überwachung der Integrität

Die ALDB setzt zur Überwachung der Integrität der Systeme des Informationsverbundes eine Software ein, die Veränderungen an kritischen Systemdateien und Systemeinstellungen überwacht. Hierzu wird auf den Systemen das Produkt HCL Bigfix (ehemals: IBM Tivoli Endpoint Manager) eingesetzt. Die Software soll eine Integration mit HCL Bigfix unterstützen. Dies gilt sowohl für Software die direkt auf der Hardware installiert wie auch für Software, die in einem Container läuft.

4.3.8 Passwortverwaltung

Die Anforderungen an Webanwendungen werden ergänzt durch Anforderungen an die Erzeugung, Aufbewahrung und den Umgang mit Passwörtern für Administratoren und Nutzer.

Im Regelbetrieb werden die Vorgaben für die Passwörter automatisch durch die Passwort-Policy im Active Directory umgesetzt. Die Applikation soll die im Anforderungskatalog Sicherheit gelisteten Anforderungen unterstützen.

Für den Fall, dass der Active Directory Dienst nicht verfügbar ist, soll eine Verwaltung für lokale Benutzer in der Applikation verfügbar sein. Die lokale Verwaltung soll die gleichen Vorgaben und Richtlinien erfüllen und unterschiedliche Policies für unterschiedliche Benutzertypen (z.B. Standardbenutzer, Notfallbenutzer, Administrator) unterstützen.

4.3.9 Rollen- und Berechtigungskonzept

Die Applikation muss an das bestehende MS Active Directory (AD) angebunden werden; das AD ist führend (vgl. Kap. 2.1.7). Die Authentifizierung soll ausschließlich über das Active Directory erfolgen. Administrative Rollen müssen über Verzeichnisgruppen vergeben werden. Nach erfolgreicher Anmeldung sollen die dem Benutzer im AD zugeordneten Gruppen- oder Rolleninformationen ausgelesen und automatisch den entsprechenden Profilen bzw. Berechtigungsrollen innerhalb der Applikation zugeordnet werden. ACD-spezifische Profile (z. B. Skills, Routing- und Agentenprofile) werden in der Applikation gepflegt.

Für den Fall, dass der Active Directory Dienst nicht verfügbar ist, soll eine Verwaltung für lokale Benutzer und Rollen in der Applikation verfügbar sein. Die lokale Verwaltung soll die gleichen Vorgaben und Richtlinien erfüllen.

4.3.10 Datensicherung

Notwendige Replikationsmechanismen, die nicht durch standardisierte Datenbankprozesse wie Export Import von Datenbanken abgedeckt werden, müssen beschrieben und eingeführt werden.

Bei einem Ausfall eines Servers oder Systems soll dieser durch notwendige Wiederherstellungsprozeduren ohne Datenverlust wiederhergestellt werden. Hierzu soll eine Backup- und Recovery-Prozedur erstellt werden. Auch menschliche Fehler wie Datenlöschung sollen abgefangen werden.

© ALDB 2026

Die Software soll eine vollständige Backup-Recovery-Funktion besitzen. Wenn nicht anders vermerkt, soll jeweils separat zwischen Software- und Daten-Backup unterschieden werden.

Die ALDB setzt auf ihren Servern Virtualisierung ein. Die Applikation soll bevorzugt über die Backup-Mechanismen der Virtualisierungssoftware gesichert werden.

Der Auftragnehmer soll darstellen inwieweit die Applikation unabhängig von/parallel zu der Datenbank gesichert werden kann und die Prozedur beschreiben für die folgenden Fälle:

- Ausfall und Wiederherstellung der Applikation ohne Ausfall der DB
- Ausfall und Wiederherstellung der DB ohne Ausfall der Applikation
- Ausfall und Wiederherstellung der Applikation und der DB

4.3.10.1 Unterstützung einer Sicherung im Rahmen der HW/VM Plattform

Aktuell kommen bei der ALDB verstärkt virtualisierte Umgebungen zum Einsatz. Die Software soll ein Szenario unterstützen in dem die Applikation evtl. unabhängig von der DB als Teil einer oder mehrerer VM(s) gesichert/eingespielt wird.

4.3.10.2 Prozedurbeschreibung

Die Backup-/Recovery-Prozedur soll durch den Auftragnehmer ausführlich beschrieben werden. Dabei soll die Möglichkeit des Backups im Rahmen der virtualisierten Umgebung berücksichtigt werden.

Notwendige Snapshots und Wiederherstellungsprozesse sollen beschrieben werden.

4.3.10.3 Vollständigkeit des Backups

Bei einem Backup sollen alle Informationen gesichert werden, vor allem:

- Sämtliche Software-Konfigurationen
- Sämtliche Regeln

4.3.10.4 Automatisches und manuelles Backup

Es soll ein automatisches Backup auf ein externes Medium nach einem definierten Zeitplan (zeitbasiert, z.B. tägliches Backup) möglich sein.

Ebenso soll die Möglichkeit bestehen, ein manuelles Backup durchzuführen.

In der Projektphase legt der Auftragnehmer ein Sicherungskonzept vor und beschreibt die Prozeduren dafür, inkl. Beistellungen durch die ALDB (Server-Ausstattung, Speicher-Eigenschaften…).

© ALDB 2026

4.3.10.5 Backup-Varianten (inkrementell, vollständig, pro Modul)

Es sollte auch die Möglichkeit geben, dass ein Backup von nur einem Software-Modul durchgeführt wird bzw. nur ein Backup von Software-Modulen durchgeführt wird, die sich geändert haben.

Es soll auch ein Backup von Änderungen möglich sein (inkrementelles Backup). Es sollte jedoch mindestens einmal pro Woche ein vollständiges Backup erstellt werden.

Es sollte möglich sein, die letzten 5 erstellen Backups bzw. individuell erstellte Backups wiederherzustellen.

Im Standard-Fall soll das letzte Backup für die Wiederherstellung genutzt werden.

4.3.10.6 Überwachung, Dokumentation des Backups

Die Software soll den Backup-Prozess überwachen und sicherstellen, dass ein Backup vollständig und fehlerfrei erfolgt ist.

Sollte ein Backup fehlerhaft bzw. unvollständig erfolgt sein, so soll die Software einen entsprechenden Alarm erzeugen, idealerweise mit der Ursache (z.B. nicht genügend Speicher, Ziel-Host nicht erreichbar, etc.).

Für alle (automatisierten) Backups soll ein Log-Eintrag erstellt werden (z.B. inkrementelles Backup wurde erfolgreich durchgeführt).

4.3.10.7 Recovery

Eine Wiederherstellung soll so erfolgen, dass die vollständige Funktionalität wiedergegeben ist und keine manuellen Nacharbeiten notwendig sind.

4.4 IT-Betrieb

4.4.1 Administration und Konfiguration

Die Anlage muss grundlegende Aufgaben für die Verwaltung und Organisation bereitstellen:

- zentrale Verwaltung von Benutzern und Rufnummern
- Vergabe von Nebenstellen und Berechtigungen
- Sperr- und Freigaberegeln (z. B. Auslandsgespräche)
- Interne Rufnummernverwaltung
- Zeitsteuerung (Tag-/Nachtbetrieb)

Es muss ein einheitlicher, standortunabhängiger Rufnummernplan gelten, wobei externe Servicenummern von der Deutschen Telekom übernommen werden müssen.

© ALDB 2026

Die Lösung muss eine zentrale und standortübergreifende Administration von Nutzern, Rufnummern, Nebenstellen sowie Service- und Skill-Zuordnungen ermöglichen. Benutzer und Konfigurationen werden nur einmal zentral angelegt und gepflegt und sind an allen Standorten wirksam. Alle Zuordnungen müssen administrativ konfigurierbar und dokumentiert sein.

Die Administration muss über eine webbasierte Administrationsoberfläche erfolgen; Standardänderungen dürfen keinen Neustart von Diensten erfordern. Sie muss Massenänderungen über Upload-/Download-Funktionen unterstützen. Die ALDB muss befähigt werden, die Systeme im laufenden Betrieb selbst zu administrieren, ohne auf zusätzlichen Herstellersupport angewiesen zu sein, idealerweise über bestehende Verzeichnisdienste wie Microsoft AD inklusive Unterstützung von Group Managed Service Accounts.

Der Auftragnehmer muss ein Rollen-/Nutzergruppen-Modell unterstützen, das mindestens die Nutzergruppen Agent, Supervisor/Teamleiter, Administrator und Business-User abbilden kann.

Jeder Nutzer erhält eine eindeutige User-ID mit zugehöriger Nebenstellen-Rufnummer, für Callcenter-Agenten erfolgt zusätzlich eine Zuordnung zu (mehreren) Services und Skills.

Die Administration von Routings (User-IDs und der einzelnen Skills und zugehörigen Standorte, und Konfiguration der zu den Service-Nummern zugehörigen Call-Routing Szenarien bzw. Sonder-Funktionen wie Rufbereitschaft, Sammelrufnummer oder Chef/Sekretariat) erfolgen über eine intuitive Oberfläche sowie Listenfunktionen mit Upload/Download für Massenänderungen.

4.4.2 Notfallbetrieb

Betrieb und Notfallbetrieb müssen ohne Rufnummernbruch funktionieren. Erreichbarkeit und Routing bleiben für Anrufer konsistent, unabhängig davon, welcher Standort gerade aktiv ist. Die Datenbank und ihre Replikation stellt die ALDB bereit und betreibt sie (Kap. 2.1.4); die synchrone Replikation stellt sicher, dass historisierte Daten im Failover-Fall vollständig erhalten bleiben. Call Control und Anrufverteilung arbeiten bei Nichtverfügbarkeit der Datenbank ohne Unterbrechung weiter; laufende Gespräche brechen nicht ab. Bis zur Wiederverfügbarkeit der Datenbank sind folgende Einschränkungen zulässig: keine Konfigurationsänderungen, keine historischen Auswertungen, keine Neuanmeldung von Benutzern und Endgeräten. Nicht eingeschränkt werden dürfen Routing, IVR-Grundfunktion und Statuswechsel angemeldeter Agents; gepufferte Daten gehen nicht verloren. Mögliche Ausfallszenarien sind zu beschreiben.

Alle notwendigen Schritte für Notfallübungen, wie Schwenk, Stromabschaltung oder Ausfall einzelner Systeme sind in einem Ausfall- und Schwenkkonzept zu beschreiben und zu testen. Bei Software-Anpassungen oder Systemveränderungen ist diese mit Unterstützung des Auftragnehmers zu aktualisieren.

4.4.3 Notfallübungen

Die ALDB führt regelmäßige Notfallübungen durch, insbesondere jährliche Standortumschaltungen und Testszenarien. Die Lösung muss diese Übungen ohne produktionskritische Einschränkungen und ohne Ausfallzeit technisch unterstützen.

© ALDB 2026

5 Leistungsumfang Projektphase

Dieses Kapitel beschreibt die Leistungen des Auftragnehmers vom Zuschlag bis zur Gesamtabnahme und Übergabe der Lösung in den Betrieb der ALDB.

5.1 Projektvorbereitung und Konzeption

Für die Erbringung dieser Leistungen ist ein Zeitplan zu erstellen inklusive Skizzierung von Arbeitspaketen sowie eines Projektplans.

Im Rahmen der Projektphase erfolgen alle Arbeiten von der Feinspezifikation, Installation, Konfiguration, Tests bis hin zur Abnahme und betriebsbereiten Übergabe des Systems.

Dokumentation von technischen Voraussetzungen: die angebotenen Betriebsarten (Web-Client) sind so dokumentieren, dass klar erkennbar und prüfbar ist, welche technischen Voraussetzungen (Browser, Policies, Ports, Security) gelten.

Der Auftragnehmer erstellt in Abstimmung mit der ALDB ein Feinkonzept, welches mindestens die Systemarchitektur, die Verteilung der Komponenten auf beide Standorte, das Redundanz- und Failover-Konzept, das Netzwerk- und Sicherheitskonzept, das Datenbank- und Datenhaltungskonzept sowie das Schnittstellenkonzept umfasst. Der Auftragnehmer legt das Feinkonzept spätestens 6 Wochen nach dem Kickoff vor; die ALDB gibt es spätestens 2 Wochen nach Vorlage frei. Zu den Leistungen gehören:

- Konzepterstellung einer Lösung für den standortredundanten und georedundanten Betrieb inkl. der Entwicklung möglicher Netzwerkkonzepte, die für den ausfallsicheren Betrieb notwendig sind.
- Entwicklung einer Feinspezifikation für die Implementierung des Systems (Installationen, Konfiguration, Integration in die Systemumgebung, Schnittstellen, Rollen- und Rechtekonzept, Datenmodell, Umsetzungsplanung, etc.).
- Vorbereitung, Durchführung und Dokumentation von Abstimmungen mit der ALDB zur Abstimmung offener Fragen bezüglich Implementierung, Inbetriebnahme und Migration
- Erstellung einer individuellen Installationsanleitung und -Dokumentation für die Installation „from Scratch“ auf Basis des bereitgestellten Betriebssystems, inkl. Anforderungen an die zugrunde liegende VM-Konfiguration sowie das Betriebssystem (z.B. benötigte Software-Pakete, Installationsoptionen).
- Erarbeitung eines Test- und Abnahmeplans inkl. Testfällen zum Nachweis der Erfüllung der Produktkriterien, ggf. iteratives Vorgehen mit der ALDB abzustimmen
- Erstellung eines Failover-Konzeptes, Backup und notwendigen Wiederherstellungskonzept sowie Desaster Recovery
- Ziel ist, die Migration durch geeignete Ablaufs-Szenarien (z. Bsp. Parallelbetrieb altes und neues System, Schrittweisem Schwenk der Standorte) gemeinsam mit der ALDB so zu planen und umzusetzen, dass der Geschäftsbetrieb ohne Unterbrechungen fortgeführt wird.
- Durchführung der Migration und Datenübernahme der bestehenden Rufnummern- und Teilnehmerkonzepte, Routinglogiken und ACD-Prozesse in die Zielarchitektur nach dem Migrationskonzept der ALDB

© ALDB 2026

Die erstellten Dokumente müssen grundsätzlich in deutscher Sprache verfasst werden.

Bei der Erstellung der Konzepte ist darauf zu achten, dass sie keine als „VS - Nur für den Dienstgebrauch“ eingestuften Inhalte beinhalten, da sie ansonsten beim Auftragnehmer in einer entsprechend zugelassenen IT-Umgebung erstellt und entsprechend geschützt werden müssen.

Der Auftragnehmer muss der ALDB das Recht zur Nutzung und Fortschreibung der für die Implementierung und Konfiguration des Systems erstellten Dokumente einräumen.

5.2 Implementierung, Testing und Inbetriebnahme

Installations- und Konfigurationsleistungen sowie die Begleitung der Abnahmetests sind an den Standorten der ALDB durchzuführen, da die Systeme in abgeschotteten Umgebungen ohne Internetzugang installiert werden.

Es dürfen im Rahmen der Implementierung und Konfiguration keine Nutzdaten und keine eingestuften Inhalte aus dem System an den Auftragnehmer oder Hersteller übermittelt werden. Lediglich die Übermittlung vorgeprüfter und bereinigter Protokolldaten ist möglich.

Die Installation und Konfiguration umfassen

- zwei produktive Systeme (Hauptstandort und Nebenstandort),
- vier daran angeschlossene Satelliten-Standorte
- ein Referenzsystem

Die Standorte befinden sich in Berlin, Hannover und Bonn.

Der Auftragnehmer übernimmt, in Abstimmung mit der Projektleitung der ALDB, die Installation, Erst-Konfiguration und Inbetriebnahme sowie Tests und Abnahme bis zur Herstellung der Betriebsbereitschaft und sorgt für die termingerechte Umsetzung gemäß der abgestimmten Runbooks und Projektplanung, einschließlich der Migration von den Altsystemen:

- Installation des Produkts und Basiskonfiguration gemäß der o.g. Feinspezifikation
- Anbindung der umliegenden Systeme an das System, Anbindung des Active Directory, die Integration der IVR in die Backend-Systeme sowie die Bereitstellung der Reporting-Schnittstelle
- (Beschreibung der) Einbindung in das IT-Monitoring inkl. Erstellung eines Alarmbehandlungsplans
- Einrichtung der Benutzer gem. Rollen- und Rechtekonzept sowie Erst-Einrichtung der Routings
- Begleitung der Abnahmetests gemäß Test- und Abnahmeplan
- Betriebsbereite Übergabe des Systems an die ALDB
- Erstellung eines Berechtigungskonzepts/ Rollenmodell

5.2.1 Testinstallation (Referenz-IT)

Die Installation und Konfiguration erfolgt zuerst als Testinstallation in der Referenzumgebung und anschließend an den zwei Produktivstandorten. Vor Produktivsetzung ist die Lösung in einer

© ALDB 2026

Testumgebung nachzuweisen. Die ALDB stellt hierfür bestehende Test- und Referenz-Umgebung sowie -Arbeitsplätze bereit; die Lösung muss deren Nutzung ermöglichen. Tests müssen sowohl rein webbasiert, ohne Tischtelefone, als auch mit Tischtelefonen möglich sein. Die Abnahme erfolgt auf Grundlage eines gemeinsam abgestimmten Testkatalogs.

5.2.2 Implementierung, Integration und Konfiguration in der Produktiv-Umgebung

Der Auftragnehmer implementiert die Lösung an beiden Standorten und integriert sie in die bestehende Infrastruktur. Dies umfasst insbesondere die Anbindung an die vorhandenen Einwahlknoten, an Active Directory, die Integration der IVR in die Backend-Systeme sowie die Bereitstellung der Reporting-Schnittstelle. Dabei erfolgt die Erstkonfiguration der Systeme, Routings und User.

5.2.3 Migration und Übergangsbetrieb

Die Migration soll ohne Unterbrechung der Erreichbarkeit erfolgen. Während des Übergangsbetriebs sollen die bestehenden ACD- und Reporting-Funktionen weiter nutzbar sein oder gleichwertig ersetzt werden. Das Migrationskonzept erstellt die ALDB. Der Auftragnehmer muss die ALDB in der Projektphase bei der Erstellung des Migrationskonzepts unterstützen, insbesondere durch fachliche und technische Beiträge zu Migrationsschritten, Rückfallszenarien und technischen Abhängigkeiten. Der Auftragnehmer führt die Migration nach dem Migrationskonzept der ALDB durch.

Zu übernehmen sind aus dem Bestandssystem:

- 2 Standorte mit je 500 Rufnummern
- ca. 50 Servicenummern
- 2 Callflows (Durchstellung direkt an freie Agenten; Ticketabfrage)
- ca. 10 vorhandene Ansagen
- ca. 15 Warteschlangen
- ca. 20 Mitarbeiter-Skills (Ressourcengruppen)
- 1 Chef-Sekretariats-Konstellation (2 Chefs mit 2 Sekretariaten)
- ca. 10 Sammelgruppen

Für die Analyse stellt die ALDB in der Projektphase einen CSV-Export der Daten aus der OXE sowie die Konfigurationsdateien der Genesys-Lösung zur Verfügung.

5.3 Abnahme

5.3.1 Grundsätze

Die Abnahme erfolgt auf Grundlage eines Test- und Abnahmeplans, den Auftragnehmer und ALDB in der Projektphase gemeinsam festlegen, einschließlich seiner Umsetzung. Voraussetzung jeder Abnahmestufe ist die schriftliche Erklärung der Betriebsbereitschaft durch den Auftragnehmer.

© ALDB 2026

Die Regelungen dieses Kapitels konkretisieren die Abnahmeregelungen. Die Mitwirkungsleistungen der ALDB (z. B. Bereitstellung von Testarbeitsplätzen, Fachtestern, Testrufnummern und Zugängen zu Bestandssystemen) benennt der Auftragnehmer im Test- und Abnahmeplan.

5.3.2 Test- und Abnahmeplan

Der Auftragnehmer erstellt im Rahmen der Projektvorbereitung und Konzeption (Kap. 5.1) einen Entwurf des Test- und Abnahmeplans, der gemeinsam mit der ALDB festgelegt wird, und legt ihn der ALDB spätestens zwei Wochen vor Beginn der ersten Funktionsprüfung zur Freigabe vor. Der Plan muss mindestens enthalten: Testumfang und Testobjekte, Testfälle mit Vorbedingungen, Testschritten und erwarteten Ergebnissen, die Zuordnung jedes Testfalls zu den Kapiteln dieser Leistungsbeschreibung und des Anforderungskatalogs (Rückverfolgbarkeit), Testdaten und Testumgebung, den Zeitplan, die erforderliche Mitwirkung der ALDB sowie Abbruch- und Wiederaufnahmekriterien. Die ALDB kann eigene Testfälle ergänzen.

5.3.3 Abnahmestufen

Die Abnahme erfolgt in den folgenden Stufen. Jede Stufe setzt die erfolgreiche Abnahme der vorangehenden Stufe voraus.

- Teilabnahme 1 – Referenzumgebung: Funktionsprüfung der funktionalen und nichtfunktionalen Anforderungen in der Referenz-IT (Kap. 5.2.1) als Voraussetzung für die Installation in der Produktivumgebung
- Teilabnahme 2 – Produktivumgebung und Migration: Funktionsprüfung an beiden Produktivstandorten und den angeschlossenen Bürostandorten einschließlich Integrations-, Redundanz-, Last- und Sicherheitstests sowie Nachweis der vollständigen und fehlerfreien Übernahme von Rufnummern, Teilnehmern, Routings, Ansagen und Konfigurationen je Migrationsschritt gemäß Migrationskonzept der ALDB (Kap. 5.2.3), das der Auftragnehmer umsetzt
- Gesamtabnahme: nach bestandenem Probebetrieb (Kap. 5.3.5) unter Einbeziehung aller Teilleistungen und ihres Zusammenwirkens

Die Dauer jeder Funktionsprüfung wird im Kick-off-Meeting besprochen und im Test- und Abnahmeplan dokumentiert

5.3.4 Prüfinhalte der Funktionsprüfung

Die Funktionsprüfungen umfassen, bezogen auf die jeweilige Abnahmestufe, mindestens die folgenden Prüfungen:

- Funktionstests aller Leistungsmerkmale gemäß Kap. 3 (Telefonie, ACD, IVR, Reporting, UC, Clients und Endgeräte), einschließlich der Notrufe 110/112 mit korrekter Standortzuordnung
- Plattform- und Installationsprüfung: Installation auf den von der ALDB bereitgestellten Systemen (VMware vSphere, Red Hat Enterprise Linux) bzw. auf den deklarierten Appliances und ggf. in der Container-Umgebung, Lizenzierung und Betrieb ohne Internetzugang, Netzanbindung gemäß Kommunikationsmatrix im IPv4-Betrieb, Sicherung der virtuellen

© ALDB 2026

Maschinen im laufenden Betrieb über Veritas NetBackup sowie Verträglichkeit mit Patches und Minor-Versionswechseln der Bestandsplattformen

- Arbeitsplatz- und Clientprüfung: Nutzung des Web-Clients in der Citrix-Umgebung auf IGEL Thin Clients und ECOS-Sticks (Homeoffice), mit den freigegebenen Browserversionen ohne lokale Komponenten, mit den eingesetzten kabelgebundenen Headsets
- Administrationsprüfung: Rollen- und Nutzergruppenmodell, zentrale Verwaltung von Benutzern, Rufnummern, Nebenstellen und Skills, einheitlicher standortübergreifender Rufnummernplan sowie Massenänderungen über Upload-/Download-Funktionen
- Schnittstellen- und Integrationstests, insbesondere Active Directory und Single-Sign-On, Ticketsystem, Reporting-Schnittstelle, Datenbankcluster, Monitoring, SIEM und Datensicherung
- Redundanz- und Failover-Tests: Ausfall einzelner Systemknoten, Ausfall eines Standorts, Ausfall eines SBC bzw. Provideranschlusses sowie Rückschwenk; jeweils mit dem Nachweis, dass bestehende Gespräche erhalten bleiben, die vereinbarten Umschaltzeiten eingehalten werden und kein Rufnummernbruch entsteht
- Last- und Performancetests mit simulierter Spitzenlast auf Basis des Mengengerüsts (Kap. 2.3), mindestens für gleichzeitige externe Gespräche und gleichzeitig angemeldete Agents sowie für IVR-Sitzungen gemäß der vom Auftragnehmer angegebenen Dimensionierung, einschließlich Prüfung der Sprach- und Ansagequalität sowie der Reaktionszeiten der Oberflächen (Kap. 3.5)
- Sicherheitstests: Nachweis der Verschlüsselung von Signalisierung und Medien, Prüfung der Systemhärtung, Schwachstellenscan sowie Prüfung des Rollen- und Berechtigungskonzepts; die ALDB behält sich einen eigenen Penetrationstest vor
- Datensicherungs- und Wiederherstellungstest einschließlich vollständiger Wiederherstellung eines Standorts
- Update-Test: Einspielen eines Updates bzw. Patches gemäß beschriebener Updateprozedur ohne Unterbrechung des Betriebs
- Nachweis der Einbindung in Monitoring und Alarmbehandlung durch Auslösen und Quittieren definierter Alarme
- Prüfung der Betriebsdokumentation (Kap. 5.4) auf Vollständigkeit und Richtigkeit sowie Nachweis der durchgeführten Schulungen (Kap. 5.5)

5.3.5 Probebetrieb

Nach erfolgreicher Teilabnahme 2 folgt ein Probebetrieb unter Realbedingungen über mindestens 14 Kalendertage. Der Probebetrieb ist bestanden, wenn in seinem Verlauf kein betriebsverhindernder Mangel aufgetreten ist, die Verfügbarkeit gemäß Kap. 4.1 eingehalten wurde, kein sicherheitsrelevanter Vorfall auf die Lösung zurückzuführen ist und alle gemeldeten betriebsbehindernden Mängel innerhalb der Fristen gemäß Kap. 6.2 beseitigt wurden. Tritt ein betriebsverhindernder Mangel auf, beginnt der Probebetrieb nach dessen Beseitigung erneut.

5.3.6 Mängelklassen und Abnahmekriterien

Während der Funktionsprüfungen und des Probebetriebs festgestellte Mängel werden wie folgt klassifiziert:

© ALDB 2026

- Betriebsverhindernder Mangel: Die Nutzung der Lösung oder wesentlicher Teile ist unmöglich oder unzumutbar eingeschränkt, z. B. fehlende Erreichbarkeit der Servicenummern, Ausfall der Notruffunktion, Versagen des Failovers, Verletzung von Sicherheitsanforderungen oder Datenverlust
- Betriebsbehindernder Mangel: Die Nutzung ist erheblich eingeschränkt, ein zumutbarer Workaround besteht jedoch, z. B. Ausfall einzelner Leistungsmerkmale, fehlerhafte Berichte oder Ausfall einzelner Schnittstellen mit manueller Ersatzlösung
- Leichter Mangel: Die Nutzung ist nur unwesentlich eingeschränkt, z. B. Darstellungsfehler oder Dokumentationslücken ohne Betriebsrelevanz

Die Mängelklassen entsprechen für die Mängelbeseitigung den Prioritäten gemäß Kap. 6.2: betriebsverhindernd der Priorität P1, betriebsbehindernd der Priorität P2, leicht den Prioritäten P3 bzw. P4.

Eine Abnahmestufe wird erklärt, wenn sämtliche Testfälle des freigegebenen Test- und Abnahmeplans durchgeführt wurden, alle Mindestanforderungen nachweislich erfüllt sind, kein betriebsverhindernder und kein betriebsbehindernder Mangel vorliegt und höchstens fünf leichte Mängel offen sind. Die Gesamtabnahme setzt zusätzlich den bestandenen Probebetrieb, die abgenommene Betriebsdokumentation, die durchgeführten Schulungen, den Nachweis der Lizenzen gemäß Kap. 2.3 sowie die Übergabe sämtlicher Zugangsdaten, Konfigurationsstände und Installationsmedien an die ALDB voraus.

Die ALDB kann eine Funktionsprüfung abbrechen, wenn ein betriebsverhindernder Mangel auftritt oder betriebsbehindernde Mängel eine sinnvolle Fortsetzung nicht zulassen. Nach Mängelbeseitigung ist die Funktionsprüfung in den betroffenen Teilen, bei Bedarf vollständig, zu wiederholen. Dies schließt Regressionstests der bereits geprüften Funktionen ein.

5.3.7 Abnahmeprotokoll und Mängelbeseitigung

Über jede Funktionsprüfung wird ein von beiden Parteien zu unterzeichnendes Protokoll erstellt. Es enthält mindestens die geprüften Leistungen mit Software- und Konfigurationsstand, die durchgeführten Testfälle mit Ergebnis, die festgestellten Mängel mit Klassifizierung und vereinbarter Beseitigungsfrist, Abweichungen vom Test- und Abnahmeplan sowie die Entscheidung über Erklärung oder Verweigerung der Abnahme. Der Auftragnehmer stellt der ALDB die Testberichte und Nachweise vollständig zur Verfügung.

Bei Abnahme offene leichte Mängel beseitigt der Auftragnehmer innerhalb von 30 Kalendertagen, soweit im Protokoll keine andere Frist vereinbart ist. Der Aufwand für Wiederholungen von Funktionsprüfungen, die durch Mängel der Leistung des Auftragnehmers erforderlich werden, trägt der Auftragnehmer.

5.4 Erstellung der Betriebsdokumentation

Der Auftragnehmer erstellt und überlässt im Rahmen des Einführungsprojektes eine deutschsprachige Dokumentation in elektronischer Form, die die folgenden Aspekte beinhaltet:

- Betriebsdokumentation mit Bezug auf die konkrete Installation

© ALDB 2026

- Benutzerdokumentation mit Beschreibung für alle implementierten Funktionen und deren Konfiguration
- Bereitstellung von erforderlichen systemseitigen Unterlagen für das erforderliche Notfall- und Wiederanlaufkonzept, die Umsetzung der Redundanz- und Hochverfügbarkeitsanforderungen, sowie das Backup- und Restore Verfahren
- Anwendungsübersicht
- Datenmodell
- Technische Dokumentation für die Datenbank-, Netzwerk- und Applikationsadministration
- Vollständige Angaben zur Installation und Deinstallation (inkl. Versionen und Patches)
- Vollständige Angaben zu Betriebsumgebungen, Parametrisierung, Konfiguration, Freischaltung, Fehlerbehebung)
- vollständige Schnittstellen- und Datenmodell-Dokumentation liefern, mindestens bestehend aus:
    - Beschreibung der Schnittstelle (Zugriffsart, Authentifizierung, Formate)
    - Datenobjekte/Felder inkl. Datentypen
    - Semantik jedes Feldes
    - Beispiel-Datensätze
    - Versionierungs- und Änderungsregeln, Programmdokumentation inkl. möglicher kundenspezifischer Anpassungen)
- Dokumentation der Datensicherungsmaßnahmen
- Dokumentation zum Datenschutz und IT-Sicherheit (Konfiguration gemäß DSGVO)
- Dokumentation für die Fachadministration zum Einrichten von Benutzern, Vergabe von Benutzerrechten, Parametrierung und Konfiguration
- Herstellerdokumentation, üblicherweise:
    - Benutzerhandbuch zum System (in der installierten Version)
    - Administrationshandbuch zum System (in der installierten Version)

Bei der Erstellung der Dokumentationen ist darauf zu achten, dass sie keine als „VS - Nur für den Dienstgebrauch“ eingestufte Inhalte beinhalten, da sie ansonsten beim Auftragnehmer in einer entsprechend zugelassenen IT-Umgebung erstellt und entsprechend geschützt werden müssen. Sofern der Auftragnehmer nicht über eine gehärtete Umgebung verfügt, sind sie sind so zu erstellen, dass die Einstufung erst nach dem Zusammenfügen innerhalb der geschützten Umgebung der ALDB erfolgt, alternativ sind sie innerhalb der geschützten ALDB-Umgebung zu erzeugen.

Die erstellten Dokumente müssen grundsätzlich in deutscher Sprache verfasst werden.

Der Auftragnehmer muss zudem der ALDB das Recht zur Nutzung und Fortschreibung der für die Implementierung und Konfiguration des SYSTEMS erstellten Dokumente einräumen.

5.5 Schulung und Einweisung

Die Leistung beinhaltet die Erstellung eines Schulungskonzeptes, die Bereitstellung von Schulungsunterlagen für die Schulung von Benutzern (Business User, Agents und Supervisoren) in Vorbereitung der Migration und die persönliche Schulung und Einweisung der Administratoren im Rahmen der Testinstallation.

© ALDB 2026

Zusätzlich soll die Erstellung bzw. Bereitstellung eines Webinars/ einer Video-Anleitung zum nachträglichen Anlernen neuer Benutzer angeboten werden.

Ergänzend ist eine Key-User-Schulung vorzusehen, die ausgewählte Mitarbeitende der ALDB befähigt, als Multiplikatoren für Business User, Agents und Supervisoren zu wirken. Schulungen können virtuell oder vor Ort stattfinden; die Einweisung der Administratoren und die Schulung der Multiplikatoren (Key User) finden vor Ort statt.

Das Schulungsvolumen beträgt: Administratoren 5, Business User 200, Call Center Agents 100, Supervisoren 20, Key User nach Abstimmung mit der ALDB, höchstens 10.

Ziel: Die Schulungsteilnehmer sind nach Durchlaufen der Schulung gemäß ihrer Rolle in der Lage, ohne weitere Unterstützung ihre Aufgaben wahrzunehmen. Aufgaben sind u.a. die fachliche Nutzung des Systems, Durchführung von administrativen Tätigkeiten wie Durchführung von Konfiguration, Einrichten von Benutzern und Berechtigungen, Erstellen von Berichten.

Die Schulungen/ Einweisungen müssen in deutscher Sprache stattfinden.

Schulungsunterlagen und Materialien werden in elektronischer Form, jedoch in einem druckfähigen Format, bereitgestellt und zur weiteren Nutzung überlassen.

5.6 Ansprechpartner über die Vertragslaufzeit

Der Auftragnehmer muss der ALDB über die gesamte Vertragslaufzeit hinweg einen Ansprechpartner benennen, der über die notwendige Entscheidungsbefugnis verfügt, um alle Aktivitäten im Zusammenhang mit der Leistungserbringung zu koordinieren und kurzfristig den Vertrag betreffende Entscheidungen herbeiführen können. Ein Ansprechpartner für die Projektphase wurde mit dem Angebot benannt, der Ansprechpartner für die gesamte Vertragslaufzeit ist nach dem Zuschlag zu benennen.

Auch für den Fall von gesetzlichen Änderungen oder Änderungen und Erweiterungen am Produkt während der Laufzeit des Vertrages sorgt der Ansprechpartner für die Koordination mit der System-Produktentwicklung und sorgt für entsprechende Integration.

5.6.1 Projektkoordinator für Installation und Implementierung

Für die termingerechte Umsetzung der Arbeiten bis zur Übergabe an den Betrieb wird vom Auftragnehmer zusätzlich der Einsatz eines Projektleiters erwartet, der über das erforderliche fachliche und methodische Knowhow sowie die notwendige Erfahrung in Implementierungsprojekten vergleichbarer Größe und Komplexität verfügt.

Zu den Aufgaben des Projektkoordinators zählen insbesondere die

- Planung der notwendigen Aktivitäten und Ressourcen für die Umsetzung der Projektphase
- Erstellung und Abstimmung einer Meilensteinplanung mit der Projektleitung der ALDB
- Steuerung der Umsetzung inkl. Personaleinsatz sowie regelmäßige Synchronisation mit der ALDB über den Projektfortschritt inkl. Dokumentation (Statusbericht)

© ALDB 2026

- Umgehende Information der ALDB über identifizierte Risiken sowie Erarbeitung von Maßnahmenvorschlägen zur Risikobewältigung

5.6.2 Kommunikation

Die Kommunikation muss grundsätzlich in deutscher Sprache erfolgen.

6 Leistungsumfang Betriebsphase

Dieses Kapitel beschreibt die Leistungen des Auftragnehmers nach erfolgter Gesamtabnahme über die gesamte Vertragslaufzeit.

6.1 Softwarewartung und Updates

Diese Leistung umfasst die regelmäßige Lieferung von neuen Software-Releases, Updates und Patches/Hotfixes (inkl. Sicherheitspatche) über die gesamte Vertragslaufzeit. Die Herstellerwartung von der Lieferung der Lizenzen bis zur Gesamtabnahme ist Bestandteil der Lieferleistung (Anlage 4, Pos. A1).

Der Wartungsvertrag muss der ALDB die Möglichkeit einräumen, eigenständig Releases, Updates, Patche herunterzuladen. Der Auftragnehmer stellt sie hierzu über seine Download-Plattform (z. B. SharePoint, Kap. 4.3.1.4) zur Verfügung; die Installation in den Systemen der ALDB erfolgt offline.

Durch den Auftragnehmer sind Handlungsanleitungen bereitzustellen zu den jeweiligen Updates, die die ALDB in die Lage versetzen, die Updates eigenständig zu testen und einzuspielen.

Durch die redundante Architektur des Systems wird erreicht, dass Patches, Updates und Upgrades keine Downtime der Erreichbarkeit der Service-Nummern verursachen (Kap. 4.1).

Vor jeder Software-Auslieferung sind vom Auftragnehmer eine Schwachstellenanalyse sowie Regression-Tests durchzuführen.

Test und Einspielen der Updates auf den IT-Systemen der ALDB durch den Auftragnehmer ist nicht Bestandteil, sondern es soll bei konkretem Unterstützungsbedarf auf Leistungen des Service und Support zurückgegriffen werden können.

6.1.1 Standard-Releases

Die vom Auftragnehmer zur Verfügung gestellten Versionen der Software-Komponenten sollen möglichst der aktuellen Hauptversion des Herstellers entsprechen, mindestens jedoch das Kriterium n-1 erfüllen (aktuelle oder vorhergehende Hauptversion).

6.1.2 Sicherheits-Patches

Der Auftragnehmer muss

© ALDB 2026

- proaktiv nach bekanntwerdenden Schwachstellen und Sicherheitslücken suchen. (z.B. Sicherheitsmitteilungen vom BSI / Cert-bund.de, durch Medien und IT-Fachportale, Community-Mitteilungen)
- diese unverzüglich, spätestens innerhalb von 24 Stunden an die ALDB melden
- gemeinsam mit der ALDB eine Bewertung dieser Schwachstelle vornehmen
- abhängig von dem Schadensrisiko sofort entsprechende Gegenmaßnahmen einleiten, (i.d.R. durch Bereitstellung von Security-Patches)

SLAs für Sicherheitslücken (Frist für die gemeinsame Bewertung mit der ALDB und die risikoabhängige Umsetzung von Workaround/Mitigation; der Patch wird unverzüglich nach Verfügbarkeit beim Hersteller bereitgestellt):

- S1: Kritische Sicherheitslücke (Eine Sicherheitslücke, die nach Bewertung von Basiswert, Zeitparameter und Umgebungsparameter einen Schweregrad zwischen 9,0 und 10,0 gem. Common Vulnerabilty Scoring System (CVSS) aufweist): 24h
- S2: weniger kritische Sicherheitslücke (Eine Sicherheitslücke, die nach Bewertung von Basiswert, Zeitparameter und Umgebungsparameter einen Schweregrad zwischen 7,0 und 8,9 gem. CVSS aufweist.): 72h
- S3: Unkritische Sicherheitslücke (Eine Sicherheitslücke, die nach Bewertung von Basiswert, Zeitparameter und Umgebungsparameter einen Schweregrad kleiner 7,0 gem. CVSS aufweist.): 120h

6.1.3 Release-Notes, Release-Dokumentation

Zusätzlich soll je Release bereitgestellt werden:

- Release Notes / Change Log
- CVE-Bezug inkl. kurzer Einordnung (sofern zutreffend)
- Upgrade-Hinweise und Upgrade-Pfade

6.2 Service- und Supportleistungen

Die Bereitstellung von Service- und Supportleistungen (inkl. deutschsprachiger Support-Hotline) dient der Aufrechterhaltung des Betriebs aller bereitgestellter Komponenten und der Störungs- und Problembehebung über die komplette Vertragslaufzeit, sofern diese Leistungen nicht bereits in „Software Wartung und Updates“ enthalten sind, insbesondere die strukturierte Analyse, Qualifizierung, Priorisierung und Behebung von Störungen zur schnellstmöglichen Wiederherstellung innerhalb des vereinbarten Servicelevels.

Unterstützung soll unter Einhaltung definierter Reaktionszeiten, und je nach Problemfall auch vor Ort bei der ALDB erfolgen. Dies beinhaltet die folgenden Einzelleistungen durch den Auftragnehmer:

6.2.1 1st Level Support: Hotline und E-Mail-Kontakt für Serviceanfragen und Störungsmeldungen

Bereitstellen eines einheitlichen deutschsprachigen Kontakts (Point of Contact) zur Entgegennahme von Supportanfragen und Fehlermeldungen über folgende Eingangstore:

© ALDB 2026

- Telefonische Hotline (24/7/365)
- E-Mail
- Erstunterstützung der ALDB bei der Fehlersuche und Fehlerbehebung sowie Initiierung und Koordination rückwärtiger Support- und Eskalationsanfragen (2nd, 3rd Level, Hersteller, …) bei Konfigurationsproblemen und Softwarefehlern, Unterstützung bei Sicherheitsvorfällen und kritischen Systemstörungen, unter Einhaltung festgelegter Reaktionszeiten
- Ggf. Bereitstellung eines Kundenportals zur Ticketaufgabe sowie zur Einsicht in aktive und abgeschlossene Meldungen
- Status-Überwachung und Dokumentation aller Meldungen bis zum Abschluss

6.2.2 2nd Level Support: Unterstützung durch vorab vereinbarte Mitarbeitende

- Nach Bedarf / je nach Problemfall telefonische Unterstützung durch zuvor benannte Mitarbeitende, welche die Zugangs- und Zutrittsvoraussetzungen der ALDB erfüllen (vorab vereinbarte Personen, nachgewiesene Fachexpertise, deutschsprachig, Sicherheitsüberprüfung SÜ2) und in die konkreten Gegebenheiten des System-Einsatzes bei der ALDB eingewiesen sind.
- Für kritische Störungen (P1 und P2) ist eine Rufbereitschaft bereitzustellen.

Die Störungsbehebung muss folgendes abdecken können:

- Fehleranalyse und Fehlerbehebung inkl. strukturierter Root-Cause-Analyse entsprechend in den folgenden Kapiteln beschriebenen SLAs und Rahmenbedingungen
- Unterstützung bei Desaster-Recovery-Ereignissen (Restore, Wiederanlauf, Datenkonsistenz)
- Zeitnahe Bereitstellung von Patches bei betriebskritischen Fehlern z.B. Hotfix/Workaround/Backport, abhängig vom Schweregrad
- Bereithalten von ausgebildetem Fachpersonal sowie von Mess-, Prüf- und Diagnosewerkzeugen

6.2.3 Vor-Ort-Unterstützung: durch vorab vereinbarte Mitarbeitende

Nach Bedarf / je nach Problemfall Unterstützung vor Ort bei der ALDB durch zuvor benannte Mitarbeitende, welche die Zugangs- und Zutrittsvoraussetzungen der ALDB erfüllen (vorab vereinbarte Personen, nachgewiesene Fachexpertise, deutschsprachig, Sicherheitsüberprüfung SÜ2 bei Zugang zu den IT-Systemen) und in die konkreten Gegebenheiten des Einsatzes bei der ALDB eingewiesen sind.

Die Anfahrt eines Experten zu einem Standort der ALDB erfordert eine vorherige explizite Anforderung und soll innerhalb von 48 Stunden nach Anforderung möglich sein. Die Anforderung erfolgt über den vereinbarten Point of Contact.

6.2.4 SLAs: Reaktionszeiten, Lösungszeiten und Prioritäten

Definitionen:

- **Reaktionszeit:** Die Reaktionszeit ist die Zeitspanne zwischen dem Eingang der Störungsmeldung beim Auftragnehmer und einer qualifizierten Rückmeldung bei der ALDB.

© ALDB 2026

Innerhalb dieser Zeit wird bereits aktiv mit der Entstörung durch die Fachexperten des Auftragnehmers begonnen.

- **Lösungsbeginn:** Zeitpunkt, an dem die aktive Bearbeitung zur Wiederherstellung des Service beginnt
- **Lösungszeit:** Die Lösungszeit ist die Zeit zwischen dem Eingang der Störungsmeldung beim Auftragnehmer und der Wiederherstellung der Betriebsbereitschaft oder einem wirksamen Workaround.
- **Prioritäten:** Mit welcher Priorität eine Störung eingestuft wird, hängt von der Dringlichkeit und den Auswirkungen ab und ist der folgenden Tabelle zu entnehmen:

Priorität		Auswirkungen			
		Sehr hoch (betrifft die ganze Organisation oder kritische Geschäftsprozesse)	Hoch (betrifft eine Abteilung oder wichtige Services)	Mittel (betrifft wenige Nutzer oder nicht essentielle Funktionen)	Niedrig (betrifft einen einzelnen Nutzer)
Dringlichkeit	kritisch (Totalausfall)	P1	P1	P1	P2
	hoch (Ausfall wesentlicher Funktionen, Verlust wichtiger Daten)	P1	P2	P2	P2
	mittel (Einschränkungen mit Workaround, durch Redundanz kompensiert)	P2	P3	P3	P3
	niedrig (Einschränkung im Bedienungskomfort, Konfigurationsfragen)	P3	P4	P4	P4

Die folgenden Reaktions- und Lösungszeiten sollen eingehalten werden; sie gehen als Bewertungskriterium in die Wertung ein (vgl. Anforderungskatalog TK/ACD):

Priorität	Reaktionszeit	Lösungsbeginn	Lösungszeit

© ALDB 2026

P1 – kritisch	< 30 Minuten	sofort	Workaround/Wiederherstellung < 4 Stunden
P2 – hoch	< 1 Stunde	sofort	<8 Stunden
P3 – mittel	< 4 Stunden	Gleicher bzw. Nächster Werktag	< 4 Werktage
P4 – niedrig	<1 Werktag	nach Vereinbarung	nach Vereinbarung, in der Regel spätestens nach 10 Werktagen

6.2.5 Eskalationsprozess (technisch/managementseitig)

Der Auftragnehmer verfügt während des Vertragszeitraums über einen Eskalationsprozess, stellt ihn in der Projektphase dar und benennt Ansprechpartner entsprechend der Eskalationsstufen.

Die Eskalationsstufen werden wie folgt eingeleitet:

Eskalationsstufe	**Auslöser / Trigger**
Stufe 1 (Operativ)	Eingang eines Incidents / SLA-Abweichung
Stufe 2 (Erweitert)	Keine Lösung innerhalb SLA / wiederkehrende Störung
Stufe 3 (Management)	Eskalation bei SLA-Verletzung / kritische Betriebsbeeinträchtigung
Stufe 4 (Leitungsebene)	Anhaltender schwerer Verstoß / geschäftskritischer Ausfall

Wird bei der Priorisierung eine kritische Störung (Major Incident) erkannt, ist ein gesonderter Eskalationsprozess einzuleiten: Die Störung wird unmittelbar an einen benannten Incident Manager des Auftragnehmers eskaliert. Dieser stellt in Abstimmung mit der ALDB ein technisches Notfallteam zusammen und koordiniert bei Bedarf die Einberufung eines Krisenstabs zur Lagebewertung. Dies gilt rund um die Uhr.

6.3 Weitere Unterstützungsleistungen während der Vertragslaufzeit

Die ALDB geht zum jetzigen Zeitpunkt davon aus, dass alle geforderten Leistungsanforderungen für einen produktiven Betrieb mit den vorigen Leistungen abgebildet werden und nach deren Abnahme bzw. Migration das System produktiv eingesetzt wird.

Der Auftragnehmer unterstützt die ALDB (auf Abruf) durch weitere Unterstützungsleistungen bei Maßnahmen, der laufenden Pflege und Wartung der eingesetzten Systeme sowie bei der kontinuierlichen Weiterentwicklung der Betriebsumgebung, die nach Inbetriebnahme und Abnahme während der Vertragslaufzeit durch den Auftragnehmer oder durch einen zertifizierten

© ALDB 2026

Partner erbracht werden. Dazu gehören zum Beispiel die Unterstützungsleistungen und Beratung bei

- Maßnahmen zur Weiterentwicklung, Performance Analyse und Optimierung, mit dem Ziel, die Stabilität, Verfügbarkeit und Leistungsfähigkeit der Services dauerhaft sicherzustellen
- Anpassung, Nutzung und Integration der Anwendung, z.B. Konfigurationsänderungen, Erstellung von Übersichten/Dashboards/Berichten, Anbinden von Datenquellen etc.
- Rollen und Berechtigungen für Anwender im System/Policies,
- Entwicklung/Anpassung von Skripten,
- Ggf. Integration verschiedener Systeme

Für diese Leistungen steht ein Abrufkontingent von 24 Personentagen je Vertragsjahr zur Verfügung, das tageweise und ohne Abrufverpflichtung zum Tagessatz gemäß Anlage 4, Pos. B2 abgerufen wird.

- Automatisierung, Nutzung von APIs des Produkts,
- Ggf. Beratung zum Gesamteinsatz des Systems bei der ALDB.

Die Unterstützung kann virtuell oder als Vor-Ort-Einsatz bei der ALDB erfolgen.

6.4 Vertragsende und Übergang

Zum Ende der Vertragslaufzeit oder nach einer Kündigung unterstützt der Auftragnehmer den geordneten Übergang auf eine Nachfolgelösung:

- Übergabeplan: Auf Anforderung der ALDB, spätestens 6 Monate vor Vertragsende bzw. innerhalb von 4 Wochen nach einer Kündigung, muss der Auftragnehmer einen Übergabeplan mit Ablauf, Terminen, Ansprechpartnern und der erforderlichen Mitwirkung der ALDB vorlegen.
- Datenexport: Der Auftragnehmer muss sämtliche Konfigurations- und Inhaltsdaten in dokumentierten, offenen Formaten (z. B. CSV, XML, JSON; Audio als WAV) bereitstellen, insbesondere Benutzer, Rufnummernplan, Routings, IVR-Callflows, Ansagen, Skills, Berichtsdefinitionen, Voicemails. Anruf- und Reportingdaten liegen im Rohdatenspeicher der ALDB vor und sind nicht Gegenstand der Rückgabe.
- Unterstützung beim Anbieterwechsel: Bis zu 6 Monate nach Vertragsende soll der Auftragnehmer die ALDB und einen nachfolgenden Anbieter unterstützen, insbesondere durch Auskünfte zu Schnittstellen und Datenstrukturen. Die Abrechnung erfolgt über das Abrufkontingent des letzten Vertragsjahres (24 Personentage je Vertragsjahr) zum Tagessatz gemäß Anlage 4, Pos. B2. Ein Zurückbehaltungsrecht an Daten oder Unterlagen besteht nicht.
- Weiterbetrieb: Erworbene Lizenzen sollen von der ALDB zeitlich unbegrenzt weiter genutzt werden können, auch ohne Wartungsvertrag. Bei Subskriptions- oder Mietmodellen soll der Auftragnehmer einen Übergangsbetrieb von bis zu 12 Monaten zu den bisherigen Konditionen zusichern.
- Übergabe und Löschung: Bei Vertragsende muss der Auftragnehmer sämtliche Zugangsdaten, administrativen Rechte und die aktuelle Betriebsdokumentation übergeben. Beim Auftragnehmer vorhandene Daten der ALDB müssen gelöscht und die Löschung schriftlich bestätigt werden (unter Beachtung von DSGVO und VS-NfD).

© ALDB 2026

A. Abkürzungen & Glossar

Abkürzung	Bedeutung
2FA	Zwei-Faktor-Authentifizierung
ACD	Automatic Call Distribution / automatische Anrufverteilung
AD	Active Directory (Verzeichnisdienst von Microsoft)
AG	Availability Group / Verfügbarkeitsgruppe (Microsoft SQL Server Always On)
ALDB	ALDB GmbH, ehemals Alcatel-Lucent Digitalfunk Betriebsgesellschaft mbH
ANI	Automatic Number Identification / Übermittlung der Rufnummer des Anrufers
APP	Bausteingruppe „Anwendungen“ des BSI-IT-Grundschutz-Kompendiums
ASR	Automatic Speech Recognition / automatische Spracherkennung
ASVS	Application Security Verification Standard (OWASP)
BI	Business Intelligence
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDR	Call Detail Record / Gesprächsdatensatz
CIS	Center for Internet Security (Herausgeber der CIS-Benchmarks zur Systemhärtung)
COLP / COLR	Connected Line Identification Presentation / Restriction – Anzeige bzw. Unterdrückung der Rufnummer des Angerufenen
CSTA	Computer Supported Telecommunications Applications (Standard für CTI-Schnittstellen)
CSV	Comma-Separated Values / Dateiformat für tabellarische Daten
CTI	Computer Telephony Integration / Rechnergestützte Telefonie
CVE	Common Vulnerabilities and Exposures / Kennung öffentlich bekannter Sicherheitslücken
CVSS	Common Vulnerability Scoring System / Bewertungssystem für den Schweregrad von Sicherheitslücken
DB	Datenbank
DBMS	Datenbankmanagementsystem
DDI	Direct Dial-In / Durchwahl(-block)
DHSG / EHS	Standards für elektronische Hook-Switch-Headsetschnittstellen
DMZ	Demilitarized Zone / Pufferzone
DND	Do Not Disturb / Bitte nicht stören (Präsenzstatus)
DNIS	Dialed Number Identification Service / Übermittlung der gewählten Rufnummer
DNS	Domain Name System
DSGVO	Datenschutz-Grundverordnung
DTMF	Dual-Tone Multi-Frequency / Mehrfrequenzwahlverfahren (Tonwahl)
EN	Europäische Norm

© ALDB 2026

Abkürzung	Bedeutung
ESX	VMware ESX(i), Hypervisor zur Servervirtualisierung
HA	High Availability / Hochverfügbarkeit
HD	High Definition (hier: HD Voice, Sprachübertragung in Breitbandqualität)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure (verschlüsseltes HTTP)
HW	Hardware
IAM	Identity and Access Management / Identitäts- und Zugriffsverwaltung
ID	Identifier / Kennung
IEEE	Institute of Electrical and Electronics Engineers (Normungsgremium)
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
IVR	Interactive Voice Response / interaktives Sprachdialogsystem
JTAPI	Java Telephony API (Programmierschnittstelle für CTI)
KRITIS	Kritische Infrastrukturen
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP über TLS (verschlüsselte Verzeichnisdienst-Kommunikation)
MAC	Media Access Control (hier: MAC-Adresse, Hardware-Adresse einer Netzwerkschnittstelle)
MS	Microsoft
MWI	Message Waiting Indication / Signalisierung neuer Nachrichten
NET	Bausteingruppe „Netze und Kommunikation“ des BSI-IT-Grundschutz-Kompendiums
NTP	Network Time Protocol / Protokoll zur Zeitsynchronisation
OPS	Bausteingruppe „Betrieb“ des BSI-IT-Grundschutz-Kompendiums
OS	Operating System / Betriebssystem
OWASP	Open Worldwide Application Security Project
OXE	Alcatel-Lucent Enterprise OmniPCX Enterprise (bestehende TK-Anlage)
P1 – P4	Prioritätsstufen für Störungen (P1 = höchste, P4 = niedrigste Priorität)
PAP	Paketfilter – Application-Level Gateway – Paketfilter / Architekturmodell
PIN	Persönliche Identifikationsnummer
Q	Quartal (z. B. Q4/2026 = 4. Quartal 2026)

© ALDB 2026

Abkürzung	Bedeutung
QoS	Quality of Service / Dienstgüte
RAC	Real Application Clusters (Cluster-Lösung für Oracle-Datenbanken)
REST	Representational State Transfer (Architekturstil für Web-Schnittstellen)
S/N	Serial Number / Seriennummer
S1 – S3	Schweregradklassen für Sicherheitslücken auf Basis des CVSS (S1 = kritisch, S3 = unkritisch)
SBC	Session Border Controller
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement / Dienstgütevereinbarung
SQL	Structured Query Language / Datenbankabfragesprache
SRTP	Secure Real-Time Transport Protocol (verschlüsselte Medienübertragung)
SSL	Secure Sockets Layer (Vorgängerprotokoll von TLS)
SSO	Single Sign-On / Einmalanmeldung
SÜ2	Erweiterte Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz
SÜG	Sicherheitsüberprüfungsgesetz
TAPI	Telephony Application Programming Interface (Programmierschnittstelle für CTI)
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TR	Technische Richtlinie (des BSI)
TTS	Trouble-Ticket-System (hier: Remedy)
UC	Unified Communications
USB	Universal Serial Bus
VM	Virtuelle Maschine
VoIP	Voice over IP / Internettelefonie
VPN	Virtual Private Network
VS	Verschlusssache
VSA	Verschlusssachenanweisung (Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz)
VS-NfD	Verschlusssache – Nur für den Dienstgebrauch
WCAG	Web Content Accessibility Guidelines / Richtlinien für barrierefreie Webinhalte
WebRTC	Web Real-Time Communication (Echtzeitkommunikation im Browser)

Tabelle 1: Abkürzungen & Glossar

© ALDB 2026