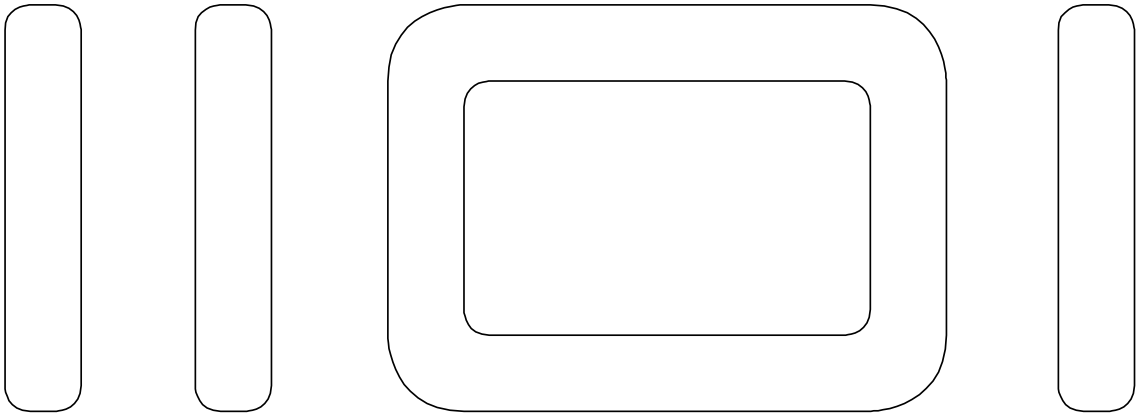
Rahmenanforderungen Systemarchitektur

Version 4.0



Dokumenteninformation	
Verantwortliche Stelle:	Dataport, TA 2
Datum:	31.05.2016
Status des Dokumentes:	Nach Befassung im Kooperationstag

Inhaltsverzeichnis

Dokumentenverwaltung

Ansprechpartner und Ort der Ablage

Ansprechpartner: Dataport, TA 2

Ort der Ablage:

Änderungsübersicht

Version	Datum	Veränderungen/ Bemerkungen	Autor(en)
V3.0	10.05.2012	Finalisiert	Dataport
V4.0	12.10.2015	Überarbeitung des gesamten Dokumentes	Dataport

Dokumentenverweise

Dokumentenname	Bemerkungen	Ort der Ablage

Hinweis zur Abnahme des Dokumentes

0 Vorwort

Im Rahmen einer Vergabe soll dieses Dokument Bietern eine valide Lösungsfindung und Kostenschätzung erleichtern. Es hat in diesem Rahmen ausschließlich informellen Charakter und wird unabhängig von den einzelnen Formulierungen nicht in die Vergabeentscheidung mit einbezogen. Insbesondere stellen die einzelnen Aspekte ausdrücklich keine Bewertungs- oder Ausschlusskriterien dar und haben insoweit keine vergaberechtliche Relevanz.

1 Allgemeine Anforderungen und Möglichkeiten durch die Rechenzentrumsinfrastruktur

Für den zentralen Betrieb von IT-Anwendungen betreibt Dataport ein Twin-Datacenter. Dabei handelt es sich um zwei identisch aufgebaute Rechenzentren, die jeweils über unabhängige Basisdienste verfügen. Dieses ermöglicht technisch den Aufbau einer georedundanten Ausfallsicherheit, die auf Verfahrensebene zwingend gesondert geprüft und beauftragt werden muss. Das Rechenzentrum ist jeweils in zwei Datacenter (DC) unterteilt, wobei nur ins Internet DC eine Verbindung aus dem Internet heraus besteht. Der Abruf von Informationen oder Diensten aus dem Internet erfolgt grundsätzlich über einen als Basisdienst bereitgestellten Proxy-Dienst. Auf das Intranet DC kann nur aus den Landesnetzen zugegriffen werden. Jeder Kunde besitzt in den beiden Datacentern eine eigene Mandantenzone, in die ausschließlich er aus seinem eigenen Landesnetz zugreifen kann. Ein Zugriff auf andere Bereiche als die eigene Mandantenzone ist wegen möglicher IP-Adressüberschneidungen in den Landesnetzen nicht möglich. Eine vom Internet DC zum Intranet DC aufgebaute Kommunikationsbeziehung ist nur über ein Application-Level Gateway (ALG) möglich. Bei länderübergreifenden Verfahren ist eine Two-Tier-Architektur vorzusehen, wobei die Frontend-Komponente jeweils in den zugehörigen Mandantenzonen platziert wird und die Backend-Komponente in einer gemeinsam genutzten Zone (Shared Backend) steht. Jedes Land benötigt dabei eine eigene Frontend-Komponente. Im Internet DC stehen ausschließlich die Dataport eigenen Verzeichnisdienste zur Verfügung.

1.1 Basisdienste

Das Rechenzentrum bietet diverse Basisdienste an, die bei Notwendigkeit der Nutzung der entsprechenden Funktionalität zwingend zu verwenden sind. Voraussetzung dafür ist eine Erfüllung der sicherheitstechnischen Mindestanforderungen (Umsetzung der ABC-Maßnahmen aus den BSI-Bausteinschichten 1 bis 5, wobei in den Schichten 1 und 5 auf die Mitwirkungspflicht des Kunden verzichtet wird sowie die Umsetzung der Z-Maßnahmen und benutzerdefinierten Maßnahmen, die aus der Risikoanalyse resultieren).

1.1.1 Admin Plattform

Sämtliche administrative Zugriffe auf Server erfolgen ausschließlich über die Admin-Plattform auf Basis einer Terminal-Server-Lösung. Einzelheiten zur Administration und den Voraussetzung sind unter 2.10 aufgeführt.

1.1.2 Antivirenmanagement

Sämtliche Server werden über ein zentrales Antivirenmanagement versorgt. Standardmäßig sind sämtliche Verzeichnisse in den Scan mit einbezogen. Software ist so zu gestalten, dass dabei keine Wechselwirkungen auftreten oder Ausnahmen generiert werden müssen.

1.1.3 Application-Level Gateway

Sämtliche Zugriffe aus dem Internet DC ins Intranet DC werden ausschließlich über ein Application-Level Gateway (ALG) geführt. Sollte eine solche Kommunikationsbeziehung notwendig sein, so sind entsprechende Filterregeln zu formulieren, die die notwendige Kommunikation möglichst exakt beschränken.

1.1.4 elektronische Archivierungssysteme

Dataport betreibt als Archivspeicher eine EMC²-Centera. Diese ist als objektorientierter Speicher in diverse Middleware-Komponenten eingebunden, die als Schnittstelle zwischen Fachverfahren und Archivspeicher dienen:

- Eldorado: Ist das zentrale System der FHH. Die Verbindung wird mittels HTTPS-Protokoll verschlüsselt und der Zugriff ist über ein Token gesichert. Die Ansprache erfolgt über einen Web-Service.
- Easy Enterprise
- Governikus LZA (nach TR-ESOR)
- VIS-Archivkonnektor: Diese Middleware ermöglicht die Übernahme von Dokumenten aus dem System „VISkompakt“ zur elektronischen Aktenführung in die Langzeitarchivierung.

Eine direkte Ansprache der EMC²-Centera über das Centera SDK ist nur in Ausnahmefällen möglich.

1.1.5 Datensicherung

Für die konsistente Sicherung der Datenbestände werden Standardverfahren angeboten. Die Sicherungsdaten werden an einen zweiten Standort repliziert.

1.1.6 DHCP

Im Rechenzentrum werden DHCP-Server zur Zuweisung der Netzwerkkonfiguration verwendet. Manuelle Konfigurationen von Netzwerkschnittstellen sind nicht vorzusehen.

1.1.7 DIVA

Bei „DIVA“ handelt es sich um die zentrale mandantenfähige Citrix-Infrastruktur, die bei der Nutzung von Server based Computing zu verwenden ist.

1.1.8 Job Scheduling

Die automatische Jobsteuerung wird im Rechenzentrum per Job Scheduling (Control-M) über ein zentrales System auf diversen Zielsystemen bereitgestellt und verwaltet. Lokale automatische Jobsteuerung auf einzelnen Servern ist nicht erwünscht.

1.1.9 Namensauflösung

Die Namensauflösung findet im Rechenzentrum mittels Domain Name System (DNS) statt. In Softwareanwendungen sind ausschließlich die entsprechenden Namen anstatt der IP-Adressen zu verwenden.

1.1.10 Proxy für Basisdienste

Es handelt sich dabei um die einzige Möglichkeit für Server aus dem Rechenzentrum heraus eine Kommunikation ins Internet aufzubauen. Direktverbindungen sind nicht möglich.

1.1.11 SMTP Relay

Zum Versenden von E-Mails durch Softwareanwendungen stehen im Rechenzentrum SMTP-Relays zur Verfügung. Das direkte Versenden von E-Mails über Anwendungsserver ist nicht möglich.

1.1.12 Softwareverteilung

Die Verteilung von Client-Software auf eine Vielzahl von Client-Arbeitsplätze sowie die Verteilung von Basiskomponenten auf Windows-Server erfolgt über eine zentrale Softwareverteilung per SCCM.

1.1.13 Storage Service (blockorientiert)

Dieser Service stellt Servern für blockorientierte Zugriffe (SCSI) Speicherplatz im Storage Area Network (SAN) zur Verfügung. Es werden zwei unterschiedliche Performanceklassen mit ca. 100 MB/s oder ca. 40 MB/s an Datendurchsatz unterschieden.

Eine Spiegelung (synchron, asynchron) kann gesondert beauftragt werden.

1.1.14 File-Service (dateiorientiert)

Dieser Service stellt für dateiorientierte Zugriffe (CIFS, NFS) einen File-Service als Network Attached Storage (NAS) mit einem Datendurchsatz von ca. 30 - 40 MB/s zur Verfügung.

Eine asynchrone Spiegelung kann gesondert beauftragt werden.

1.1.15 Überwachung

Sämtliche Server werden per SCOM und Universal Logging System (ULS) überwacht. Dabei werden Status- und Schwellwerte überwacht und Leistungsdaten ausgewertet. Anwendungssoftware soll hierzu eine entsprechende Kompatibilität aufweisen.

1.1.16 Verzeichnis- und Namensdienst

Es werden Domain Name System (DNS) und Active Directories (ADs) als zentrale Elemente im Rechenzentrum und den Landesnetzen verwendet. Dabei sind alle Verzeichnisdienstserver (Domain Controller) gleichzeitig auch Namensdienstserver. Es ist ferner zu berücksichtigen, dass es im Rechenzentrum mandantenspezifische ADs (z.B. für die Trägerländer) und mandantenübergreifende ADs (z.B. für RZ-Infrastrukturdienste) gibt.

Der Verzeichnisdienst (AD) ist für die Verteilung der Härtungs- und weiterer Konfigurationseinstellungen über AD-Gruppenrichtlinien sowie die Autorisierung und Authentifizierung zuständig.

Der Namensdienst (DNS) dient der Übersetzung zwischen Servername und IP-Adresse und ist zwingende Voraussetzung für die Funktionsfähigkeit eines ADs.

1.1.17 VPN-Concentrator

Bei dem VPN-Concentrator handelt es sich um einen zentral platzierten Terminierungspunkt für Fernzugriffe, die über unsichere Netze geführt werden. Die Nutzung umfasst dabei die Einwahl einzelner Software-Clients, Verbindungen zwischen Hardware-Clients (z.B. VPN-Router) sowie Zwecke der Netzkopplung.

1.1.18 Zeitdienst

Der zentrale Zeitdienst stellt eine synchronisierte Zeit auf allen integrierten Systemen sicher. Er ist Voraussetzung für weitere Basisdienste.

1.1.19 zentrales Patchmanagement

Dataport betreibt ein zentrales Patchmanagement, um so ein möglichst hohes Maß an Sicherheit zu gewährleisten. Das Einspielen von sicherheitsrelevanten Patches für Softwarekomponenten, die nicht vom Hersteller der Fachanwendung bereitgestellt werden und somit verfahrensunabhängig sind, soll unabhängig von der Fachanwendung jederzeit möglich sein.

1.1.20 Zertifikate

Dataport betreibt eine eigene Public-Key-Infrastruktur (PKI) zur Erstellung von Zertifikaten. Soweit möglich, sind diese Zertifikate zu nutzen.

2 Anforderungen an den technischen Betrieb

Für einen technischen Betrieb im Rechenzentrum von Dataport sind eine Reihe von technischen und organisatorischen Anforderungen zu berücksichtigen.

2.1 Unterstützte Plattformen und Komponenten

- Der technische Betrieb aller Anwendungskomponenten erfolgt über unterstützte Plattformen und Komponenten.
- Der technische Betrieb soll grundsätzlich über Hauptplattformen und -komponenten erfolgen.
- Der Betrieb über eine Nebenplattformen oder -komponente setzt voraus, dass es keine Freigabe der Software-Hersteller für die ausgewiesenen Hauptplattformen / -komponenten gibt.
- **Die derzeit unterstützten Versionen der unterstützten Plattformen und Komponenten werden detailliert in der Anlage 1 aufgelistet.**

  Dataport ist bestrebt, die Zahl seiner Betriebsplattformen zu reduzieren. Es ist ausdrücklich erwünscht, im Rahmen der bestehenden Möglichkeiten Lösungsalternativen für mehr als nur eine der genannten Plattformen und Komponenten vorzuschlagen.

  Die Plattform System z enthält die Betriebssysteme z/OS und z/VM mit Linux on z (Suse Linux Enterprise [SLES]) 64 Bit.

Serverplattformen ohne Redundanz / Lastverteilung	**Hauptplattform / -Komponente**	**Nebenplattform / -Komponente**
	Windows Server 64 Bit englisch über Intel x86	
	Linux (x86): Suse Linux Enterprise (SLES) 64 Bit über Intel x86	
	Linux on z: Suse Linux Enterprise (SLES) 64 Bit über IBM z/VM über IBM System z	

Serverplattformen	**Hauptplattform / -Komponente**	**Nebenplattform / -Komponente**

mit Redundanz / Last-verteilung	Windows Server 64 Bit englisch über Intel x86 über Failover Clustering	
	Linux (x86): Suse Linux Enterprise (SLES) 64 Bit über Intel x86 über SLES High Availability extension (SLES HAE)	
	Linux on z: Suse Linux Enterprise (SLES) 64 Bit über IBM z/VM über IBM System z („Linux on z“) über IBM z/VM LGR oder TSA (Tivoli System Automation)	
	z/OS: IBM z/OS über IBM System z über IBM Parallel Sysplex	

Datenbank-plattformen	**Hauptplattform / -Komponente**	**Nebenplattform / -Komponente**
	Microsoft SQL Server über Windows Server 64 Bit engl. über Intel x86	
	Oracle über Suse Linux Enterprise (SLES) 64 Bit über Intel x86	
	Oracle über Linux on z	
	MySQL über Suse Linux Enterprise (SLES) 64 Bit über Intel x86	
	DB2 über z/OS, ggf. DataSharing mode	
	Adabas über z/OS	

Webservices	**Hauptplattform / -Komponente**	**Nebenplattform / -Komponente**
	Microsoft Internet Information Server (IIS) über Windows Server 64 Bit englisch über Intel x86	
	Apache http über Suse Linux Enterprise (SLES) 64 Bit über Intel x86	
	Apache http Server über Linux on z	
	IBM http Server (Apache) über z/OS	
	Apache Tomcat über Suse Linux Enterprise (SLES) 64 Bit über Intel x86	
	Apache Tomcat über z/OS	
	Apache Tomcat über Linux on z	
	Apache http über Windows Server 64 Bit englisch über Intel x86	
	Apache Tomcat über Windows Server 64 Bit englisch über Intel x86	

Applikations-services	**Hauptplattform / -Komponente**	**Nebenplattform / -Komponente**
	.NET-Plattform über dem .NET-Framework über Microsoft Internet Information Server (IIS) über Windows Server 64 Bit englisch über Intel x86	
	Java JDK	
	Java EE	
	JBoss	

	über Linux on z	
	JBoss über Suse Linux Enterprise (SLES) 64 Bit über Intel x86	
	Oracle WebLogic Server (Oracle WLS) über Suse Linux Enterprise (SLES) 64 Bit über Intel x86	
	IBM Websphere über z/OS	
	SAG Natural/Adabas über z/OS	

Client-Plattformen	**Hauptplattform / -Komponente**	**Nebenplattform / -Komponente**
	Microsoft Windows Client-Betriebssysteme	
	Citrix XenApp **ohne** Microsoft Application Virtual-ization (kurz App-V)	Citrix XenApp mit Microsoft Application Virtualiza-tion (kurz App-V)

Verzeichnisdienste	**Hauptplattform / -Komponente**	**Nebenplattform / -Komponente**
	Microsoft Active Directory	

2.2 Anforderungen an einen zentralen Verfahrensbetrieb

Zentraler Verfahrensbetrieb

- BSI Konformer Betrieb muss möglich sein:

  Das Verfahren ist vom Hersteller zeitnah so anzupassen, dass es mit allen aktuellen Patchen des Betriebssystems und allen zusätzlichen Middlewarekomponenten, die es benötigt (z.B. IIS, Apache, Java, Adobe Produkten), betrieben werden kann.

- Es sollen mindestens zwei Betriebs-Instanzen des Verfahrens betrieben werden: ein Qualitätssicherungs- und ein Produktionssystem.

- In Produktionssystemen werden Dritten[1] keinerlei administrative Zugriffsrechte gewährt.

[1] Dritte: sämtliche Personen, die keine Dataport Mitarbeiter sind

- In Qualitätssicherungssystemen können Dritten unter den Rahmenbedingungen sicherer Administration nach Absprache grundsätzlich lesende Rechte bereitgestellt werden.
- Für ein Testsystem können Dritten unter den Rahmenbedingungen sicherer Administration nach Absprache grundsätzlich weitergehende Zugriffrechte bereitgestellt werden.
- Die Softwarebestandteile des Verfahrens sollen aus einzelnen logischen Komponenten bestehen, die auf getrennten Maschinen betrieben werden können (modularer Aufbau). Die Architektur soll sich dabei an einer dreischichtigen Architektur bestehend aus Benutzerebene, Applikationsebene und Datenbankebene orientieren.
- Das Verfahren soll Fehlerprotokolle über eine Administrationsoberfläche einsehbar machen.
- Das Verfahren soll keinerlei Abhängigkeiten zu bestimmten Prozessortypen oder sonstigen Hardwarekomponenten besitzen.
- Im Falle von Komponenten des Verfahrens, welche mit Java-Technologie implementiert wurden, soll die genutzte Java VM dediziert installiert werden, um Konflikte mit anderen Applikationen zu vermeiden.
- Das Verfahren soll keine Lizenzaktivierung über das Internet und nach Möglichkeit keine Lizenzierung durch Hardware-Token/-Dongle vorsehen.
- Das Prüfverfahren der Lizenzierung soll einen möglichen Austausch der Hardware berücksichtigen.
- Das Verfahren soll eine bestimmte Zeit einen Ausfall der Lizenzprüfung tolerieren (z.B. beim Einsatz eines Lizenzservers).
- Das Verfahren sollte unter VMware vSphere unterstützt werden.
- Verfahrensserver werden standardmäßig gehärtet. Die Anwendungssoftware soll unter typischen Härtungsmechanismen auf Basis von Best Practice Empfehlungen der Betriebssystem- und Middlewarehersteller betrieben werden können.
- Das Verfahren muss administrative Tätigkeiten protokollieren.

2.3 Anforderungen an zentrale Komponenten einer Anwendung

- Der Betrieb von zentralen Komponenten einer Anwendung soll über Server-Plattformen erfolgen, die im Abschnitt 2.1 “Unterstützte Plattformen und Komponenten“ und in Anlage 1 spezifiziert sind.
- Die Verfahrenskomponenten müssen automatisiert und ohne Benutzerinteraktion installiert und vollständig deinstalliert werden können.
- Die Installationspfade müssen frei wählbar sein und das Verfahren muss auch dann funktionieren, wenn die Software nicht in den vorgegebenen Verzeichnissen installiert wird.
- Der Ablageort der Nutzdaten der Anwendung muss konfigurierbar sein.

- Es dürfen keine Anwendungskomponenten in der Partition des Betriebssystems installiert werden.
- Das Monitoring der Anwendung soll für Windows soweit möglich mit dem Microsoft Systemcenter Operations Manager (SCOM) und für Linux mit dem Universal Logging System (ULS) erfolgen. Die Anwendung muss dafür ggf. Management Packs vorhalten.
- Anwendungskomponenten müssen ggf. als Daemon oder Windows Dienste implementierbar sein und dürfen keinen angemeldeten Benutzer voraussetzen.
- Für eine Hardware unabhängige Installation ist es wichtig, dass das Verfahren auch mit einem virtuellen Verfahrensnamen betrieben werden kann. Dabei muss es sich um eine Rechner unabhängige TCP/IP-Adresse mit entsprechendem DNS-Eintrag handeln (kein DNS-Alias).
- Zur Unterstützung des Supports und zur Fehlersuche muss ein Debug-Schalter gesetzt werden können, der aussagefähige Informationen in entsprechenden „Logbüchern“ ausgibt. Um den Betrieb möglichst wenig einzuschränken, sollten diese Schalter zur Laufzeit und ohne Neustart gesetzt werden können.
- Die Anwendungskomponenten müssen in der Lage sein, selbständig eine Lastverteilung auf mehrere CPUs vorzunehmen (Multiprozessorfähigkeit).
- Für eine Lastverteilung sollte die Anwendung nach Möglichkeit eine Skalierbarkeit über mehrere Knoten (= installierte Instanzen) unterstützen (Multi-Node-Fähigkeit). Dazu muss sichergestellt werden, dass die Informationen einer Benutzer-Sitzung Knoten unabhängig gespeichert werden oder keine besonderen Daten für eine Benutzersitzung benötigt werden.
- Wenn die Anwendung eine höhere Verfügbarkeit erreichen muss, sind die Anforderungen im Abschnitt 2.8 “Höhere Verfügbarkeiten / Lastverteilung“ zu berücksichtigen.

2.4 Anforderungen an die Datenbankkomponenten einer Anwendung

- Der Betrieb von Datenbank-Komponenten einer Anwendung soll über Datenbank-Plattformen erfolgen, die im Abschnitt 2.1 “Unterstützte Plattformen und Komponenten“ und in der Anlage 1 spezifiziert sind.
- Der Microsoft SQL-Server ab Version 2012 wird in der 64 Bit-Version auf Windows Servern der Enterprise Edition betrieben. Zum Einsatz kommen nur englische Sprachversionen der Datenbanksoftware. Ein Microsoft SQL-Server wird grundsätzlich als Named-Instance installiert. Nach Möglichkeit werden die Datenbanken zusammen mit Datenbanken anderer Verfahren zusammen in großen Cluster-Systemen betrieben.
- Nutzdaten werden grundsätzlich in einem Storage Area Network (SAN) abgelegt.
- Datenbank-Services werden auf den Serverplattformen dediziert betrieben. Es ist nicht möglich, auf diesen Serverplattformen zusätzliche Software oder Komponenten der Anwendung zu installieren.

2.5 Anforderungen an die Applicationservice-Komponenten einer Anwendung

- Der Betrieb von Applicationservice-Komponenten einer Anwendung soll über Applicationservice-Plattformen erfolgen, die im Abschnitt 2.1 “Unterstützte Plattformen und Komponenten“ und in der Anlage 1 spezifiziert sind.

2.6 Anforderungen an PC-Arbeitsplatz-Komponenten einer Anwendung

Die Installation und der Betrieb erfolgt ausschließlich auf standardisierten, zentral administrierten PC- Arbeitsplätzen („Clients“). Eine Installation von PC-Arbeitsplatz-Komponenten einer Anwendung kann nur im Rahmen und unter strikter Einhaltung der definierten Standards erfolgen.

- Der Betrieb von PC-Arbeitsplatzkomponenten (Client-Komponenten) der Anwendung sollen auf Plattformen und mit Komponenten erfolgen, die im Abschnitt 2.1 “Unterstützte Plattformen und Komponenten“ und in der Anlage 1 spezifiziert sind.
- Weitere einzuhaltende technische Details auf den standardisierten Arbeitsplätzen sind in der Anlage 2 beschrieben.
- Auf allen Arbeitsplätzen ist Microsoft Office installiert.
- Die auf den Arbeitsplätzen installierten Softwarekomponenten werden Warenkörben zugeordnet. Die auf allen Arbeitsplätzen installierten Softwarekomponenten finden sich im Standardwarenkorb, der bei Bedarf durch den optionalen Warenkorb ergänzt wird. Kunden-individuelle Komponenten befinden sich in Kundenwarenkörben.
  Die jeweils relevanten Warenkörbe können auf Nachfrage bereitgestellt werden.

Für die Installation und Konfiguration der Anwendungskomponenten, die auf dem PC-Arbeitsplatz betrieben werden müssen, gelten folgende Anforderungen:

- Das Verfahren soll nicht auf einzelne Clients lizenziert, sondern über eine Enterprise Lizenz angeboten werden. Ist dies nicht wirtschaftlich möglich, soll ein Lizenzserver zum Einsatz kommen.
- Im Falle einer Client-Installation soll die MSI-Technologie ohne manuelle Eingriffe durch das Verfahren unterstützt werden.
- In der Dokumentation des Verfahrens soll auf mögliche Konflikte und Abhängigkeiten zu dritten Softwarekomponenten (z.B. Microsoft Office, ActiveX-Komponenten, MDAC, JRE, .NET, IE-Plug-Ins) hingewiesen werden.
- Lokal ausgeführte Client-Komponenten des Verfahrens müssen vollständig im User-Kontext lauffähig sein. Es werden keinerlei Administrationsrechte gewährt.

2.7 Anforderungen an Arbeitsplatz-Komponenten einer Anwendung auf einem Terminalserver

- Der Betrieb von Arbeitsplatzkomponenten (Client-Komponenten) der Anwendung auf Terminalservern soll auf Plattformen und mit Komponenten erfolgen, die im Abschnitt 2.1 “Unterstützte Plattformen und Komponenten“ und in der Anlage 1 spezifiziert sind.

- Die Arbeitsplatz-Komponenten einer Anwendung sollen automatisiert installierbar sein, d.h. sie verfügen über eine Installationsroutine, sind über System Center Configuration Manager (SCCM) gleichzeitig auf mehrere Systeme installierbar oder sie sind über das Produkt Microsoft Application Virtualization (kurz App-V) paketierbar.
- Die Druckausgabe der Anwendung soll über „Universal Printing“ erfolgen.
- Bei nicht Windows-basierten ThinClients muss die Anwendung in der Lage sein, die Druckaufgaben über ThinPrint zu unterstützen.

2.8 Höhere Verfügbarkeiten / Lastverteilung

- Höhere Verfügbarkeiten und/oder eine Lastverteilung für Komponenten einer Anwendung sollen über Plattformen erfolgen, die im Abschnitt 2.1 “Unterstützte Plattformen und Komponenten“ und in der Anlage 1 spezifiziert sind.

2.9 Verzeichnisdienst

- Für die Trägerländer von Dataport wird jeweils ein Microsoft Active Directory (AD) betrieben. Die derzeit eingesetzten Versionen und Komponenten sind in der Anlage 1 aufgelistet.
- Darüber hinaus werden im Intranet Datacenter zwei mandantenübergreifende Microsoft Active Directories betrieben. Einmal für länderübergreifende Verfahren, die von mehreren Trägerländern genutzt werden und zum anderen Verbundverfahren wie Exchange und SharePoint (Ressourcen-AD‘s). Im Internet Datacenter werden ebenfalls mehrere Microsoft Active Directories betrieben.
- Windows basierte Server sind immer Mitglied in einem AD, da über die AD-Integration AVM, SCOM und SCCM genutzt wird. Alle anderen Standard-Server sind ebenfalls Mitglied in einem AD.
- Eine AD-integrierte Anwendung muss für die Authentifizierung das Kerberos-Protokoll unterstützen.

2.10 Anforderungen an die Administration von Verfahrens- und Systemkomponenten

- Die Administration von Verfahrens- und Systemkomponenten muss über die rollenbasierte Administration erfolgen. Administrative Tätigkeiten müssen nachvollziehbar und protokollierbar sein.
- Administrationswerkzeuge sollen auf einer Administrationsplattform über einem Citrix Terminal Service betreibbar und mittels Microsoft App-V virtualisierbar sein.
- Der Datenaustausch im Rahmen administrativer Tätigkeiten muss über die Administrationsplattform erfolgen. Dafür steht ein FTP-Server bereit.

2.10.1 Voraussetzungen für die Nutzung der Administrationsplattform

- Grundvoraussetzung für administrative Eingriffe ist eine Sicherheitsüberprüfung nach § 34 HmbSÜG.
- Die Clientsicherheit muss sichergestellt sein.
- Es ist Software für den Aufbau einer entsprechend gesicherten Terminalserver-Sitzung notwendig.
- Eine Zweifaktor-Authentisierung aus einer Kunden-Domäne heraus ist notwendig.

2.11 Anforderungen an den Betrieb im Netz

- Insbesondere zwischen zentralen Komponenten der Anwendung und den Client-Komponenten muss das transferierte Datenvolumen in einem sinnvollen und wirtschaftlichen Verhältnis zu üblichen Bandbreiten in Weitverkehrsnetzen stehen.
- Die Kommunikation insbesondere zwischen zentralen Komponenten der Anwendung und den Client-Komponenten muss „weitverkehrsfähig“ sein. Paketlaufzeiten von bis zu 100 ms (z.B. DSL Anschluss) müssen vom Verfahren toleriert werden und dürfen nicht zu Time-Outs oder Abbrüchen führen.
- Clients und Server kommunizieren über eine Layer 3 IP-Verbindung und befinden sich nicht im gleichen IP-Subnetz.
- Clients können nur die Server der Frontend Layer erreichen. Clientsoftware kann nicht auf Server zugreifen, die dem Applikation Layer oder dem Datenbank Layer zugeordnet sind.
- Zwischen Client und Server muss eine normgerechte TCP-Kommunikation erfolgen. IP-Pakete, die nicht für die TCP-Kommunikation vorgesehene Ports nutzen, werden geblockt.
- Die Anwendung sollte NAT (Network Address Translation) tauglich sein.
- In der Anwendung dürfen keine IP-Adressen fest kodiert werden.
- Die Anwendung muss für die Adressierung von Servern und Clients DNS-Namen verwenden, damit IP-Adressänderungen ohne Eingriffe in das Verfahren erfolgen können.
- Allen Servern und Endgeräten werden IP-Adressen mittels DHCP zugewiesen.
- Alle Kommunikationsbeziehungen zwischen allen Komponenten müssen dokumentiert sein.
- Die Anwendung soll Kommunikationsprotokolle verwenden, die nach IP-Adresse und Port gefiltert werden können.
- Es sollten möglichst keine dynamisch ausgehandelten Ports verwendet werden.
- Die Verwendung von Port-Ranges ist vorteilhaft, um die Verwaltung von Access-Filter-Listen überschaubar zu gestalten.

2.12 Anforderungen an einen Fernzugriff

Ein Fernzugriff liegt vor, wenn Personen auf ein IT-System zum Zwecke der Wartung, Reparatur, Bedienung oder Unterstützung aus der Ferne zugreifen und dieser Zugriff nicht ausschließlich der Nutzung der vertragsgemäß von Dataport bereitgestellten Dienstleistungen dient.

- Die Bereitstellung der jeweiligen Fernzugriffsinfrastruktur und die Verpflichtung zur Umsetzung der von Dataport vorgegebenen Sicherheitsmaßnahmen sind zwischen der Daten verarbeitenden Stelle und der Dienstleisterin / dem Dienstleister vertraglich zu regeln.
- Auf die Umsetzung von Maßnahmen zur Clientsicherheit ist die / der einzelne Nutzerin / Nutzer schriftlich zu verpflichten. Dies ist als Obliegenheit der Auftraggeberin / des Auftraggebers schriftlich mit Dataport zu vereinbaren, wenn Dataport nicht Auftraggeberin des Fernzugriffs ist.
- Für Fernzugriffe auf IT-Systeme, deren Betrieb ausschließlich in der Verantwortung der Auftraggeberin / des Auftraggebers liegt, gelten keine von Dataport geforderten Regelungen.

2.13 Anforderungen an Druck

2.13.1 Lokaler Druck

Die Druckausgaben für einen Einzeldruck der Applikationen über die Benutzerschnittstelle müssen die Standarddruckschnittstellen von Windows unterstützen. Es muss die Möglichkeit gegeben sein, zusätzliche Drucker (auch virtuelle) einzurichten, zu bedienen und deren Eigenschaften und Druckeinstellungen verändern zu können. Die Applikation sollte eine Voransicht des Ausdrucks am Bildschirm anbieten.

Für Seriendruckanwendungen mittlerer und großer Datenmengen ist auf eine ausreichende Hardwareausstattung (CPU, RAM) zu achten.

2.13.2 Massendruck durch Dataport

Das Druck- und Kuvertierzentrum von Dataport kann Dateien zum personalisierten Massendruck in den Formaten AFP (Advanced Function Presentation) oder PDF (Portable Document Format) verarbeiten.

AFP-Druckdateien:

AFP-Druckdaten können über folgende zwei Wege angenommen werden:

a) Erzeugung durch Kundenverfahren direkt im zOS/MVS

b) direkte Bereitstellung per File-Transfer vom Kunden

Bei den Daten muss es sich um Textdaten mit externen AFP-Ressourcen, eingestreuten AFP-Steuerbefehlen oder einen reinen AFP-Datenstrom handeln.

Als zusätzliche Aufbereitung können folgende Leistungen beauftragt werden:

i) Portoklassentrennung

ii) Einbinden unterschiedlicher Formulare (z.B. Zahlungsverkehrsvordrucke, Postzustellaufträge)

iii) Aufbringen von Kuvertiersteuerzeichen und Zuführen von Beilagen

Die Druckdaten können durch Druckaufträge mittels Control D (BMC Software) sortiert, gemischt und sortiert sowie mit Bearbeitungshinweisen auf Deck- und Trennblättern für die Weiterverarbeitung im Versand oder beim Kunden versehen werden.

PDF-Druckdateien:

Anzuliefern ist eine Datei im Format PDF/A (Version 1.2 - 1.4; andere Versionen nur auf Anfrage) mit eingebetteten Schriftarten, deren Inhalt nichts mehr hinzuzufügen ist. Nicht verarbeitet werden können CID-Fonts, asiatische Codierung sowie verschlüsselte oder mit Passwort geschützte PDF-Dateien. Für die Druckdatenübermittlung ist eine Übertragung auf einen openFT-Server vorzusehen.

Der Bereich der Empfängeradresse ist fest zu positionieren, insbesondere die Positionen von Postleitzahl und Ort dürfen nicht variieren. Das Anschriftenfeld ist nach DIN 5008 zu gestalten. Die erste Seite jedes Dokumentes muss über ein eindeutiges Ordnungsmerkmal an gleichbleibender Position verfügen. Zur Bestätigung der technischen Machbarkeit ist ein frühzeitiger Kontakt zum Druck- und Kuvertierzentrum von Dataport empfehlenswert.

3 Allgemeine Sicherheitsanforderungen

- Das Verfahren muss eine Verträglichkeit mit gängigen Virenschutzprodukten für Client- und Serversysteme gewährleisteten (siehe Anlage 1).
- Das Verfahren soll eine klare Trennung zwischen Systembereich und Datenbereich umsetzen. Die Datenablage darf nicht in Systempartitionen erfolgen.
- Das Verfahren muss jede Transaktion, auch die Vergabe von Rechten, protokollieren. Das Protokollierungsverfahren muss sicherstellen, dass die Protokolle nicht manipulierbar sind.
- Das Verfahren soll Sicherheit vor Zerstörung und/oder Verfälschung durch äußere/innere Angriffe auf den Datenbestand gewährleisten. Eingabe- und Bedienungsfehler sollen von der Software abgefangen werden und dürfen nicht zu undefinierten Zuständen oder Abstürzen des Systems führen.
- Für die zu betreibende Software sind sicherheitsspezifische Informationen wie beispielsweise Berechtigungskonzept (Rollen- und Rechtekonzept), Protokollierungskonzept, Mandantenkonzept (sofern erforderlich), Schnittstellenkonzept, Installations- und Betriebshandbuch bzw. Betriebsvorgaben des Herstellers sowie die Dokumentation von Sicherheitsfunktionen in der relevanten Fachanwendungssoftware bereitzustellen.
- Der Hersteller der Fachanwendungssoftware muss die Bereitstellung von Sicherheitsupdates, Patches und hierfür notwendige Installationsdokumentation sicherstellen sowie Support für seine Software liefern. Das Einspielen von sicherheitsrelevanten Updates für das zum Einsatz kommende Betriebssystem sowie von Software- oder Middlewarekomponenten, die nicht vom Hersteller der Fachanwendungssoftware bereitgestellt werden (beispielsweise .Net, Java, JBoss, Apache, Tomcat), sollen unabhängig vom Fachverfahren durch Dataport durchgeführt werden können. Die Fachanwendungssoftware muss dafür kurzfristig für den aktuellen Sicherheitspatchstand des zum Einsatz kommenden Betriebssystem sowie der Software- oder Middlewarekomponenten freigegeben oder angepasst werden. Das für den Betrieb der Anwendungssoftware erforderliche Betriebssystem als auch die erforderlichen Softwarekomponenten müssen in der zum Einsatz kommenden Version vom jeweiligen Hersteller des Betriebssystems bzw. der Softwarekomponenten supportet sein.
- Dataport richtet IT-Sicherheit am Standard BSI-Grundschutz aus. Alle Module des Verfahrens sollen den Grundschutzanforderungen nach IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genügen. Das gilt insbesondere für den Baustein B 1.9 (Hard- und Softwaremanagement) sowie Bausteine der Anwendungsschicht (wie Allgemeine Anwendung, Webanwendung oder WebServices). Der Betrieb nach Standard BSI-Grundschutz, mindestens Schutzbedarf „Normal“, muss nachweisbar sein.

4 Rahmenlizenzverträge

Dataport besitzt für sich und seine Trägerländer Rahmenlizenzverträge, über die kostenpflichtig Lizenzen bezogen werden können. Eine konkrete Auflistung der über einen Rahmenlizenzvertrag beziehbaren Lizenzen ist der Anlage 3 zu entnehmen.

5 Anlagen

Dieses Dokument besitzt folgende Anlagen, auf die innerhalb des Dokuments mit folgender Kurzbezeichnung referenziert wird:

- **Anlage 1:** Dokument „Rahmenanforderungen Systemarchitektur, Anlage Basissoftware“
- **Anlage 2:** Dokument „Rahmenanforderungen Systemarchitektur, Anlage Konformität zu durch Dataport supportete Arbeitsplatz-PCs“
- **Anlage 3:** Dokument „Rahmenanforderungen Systemarchitektur, Anlage Rahmenlizenzverträge“