



# Technische Mindestanforderung

## Bereich: Serversysteme

Verantwortlich:

Robert Gladewitz

Kevin Glück

DBFZ Leipzig

Stand: 22.03.2023

Nächste Überprüfung: 03.2024

Gültigkeit: 03.2024



## Inhaltsverzeichnis

1	Allgemeines .....	3
1.1	Ziel des Dokuments und allgemeine Vorgaben.....	3
1.2	Verwendete Abkürzungen .....	3
1.3	Gültigkeit und Einschränkungen .....	4
1.4	Grundlegende Anforderungen .....	4
2	Vorgaben.....	5
2.1	Grundlegende Hardwarekonfiguration.....	5
2.2	Anforderungen für Serverhardware.....	6
2.3	Anforderungen Betriebssysteme .....	8
2.3.1	Windows Betriebssysteme.....	8
2.3.2	Anforderungen für Linux Systeme.....	9
2.3.3	Andere Systeme (Blackbox Systeme, Hardwaresysteme) .....	10
2.4	Einrichtung.....	12
3	Herstellung der Betriebsbereitschaft, Schulung.....	12
4	Service und Maintenance, fakultativ: Garantie .....	13
5	Bereitstellung eines Pflichtenheftes.....	14

## 1 Allgemeines

### 1.1 Ziel des Dokuments und allgemeine Vorgaben

Dieses Dokument legt die technischen Mindestanforderungen für Serversysteme in Ausschreibungen und Verträgen fest. Abweichungen sind vertraglich festzulegen und im Vorfeld mit der IT des DBFZ abzusprechen.

Diese Mindestanforderungen gelten auch für Projektbeschaffungen und Beschaffungen im Rahmen von Baumaßnahmen, wenn ein Betrieb in den Netzen des DBFZ vorgesehen ist.

Grundsätzlich definieren alle gesetzten Vorgaben eine Minimalanforderung. Nachweislich höherwertige Komponenten können verwendet werden und können je nach Ausschreibung und Vertrag zu einer Höherwertung führen.

### 1.2 Verwendete Abkürzungen

AES	Advanced Encryption Standard
AG	Auftraggeber (DBFZ)
IPMI	Intelligent Platform Management Interface
KVM	Kernel-based Virtual Machine
NBD	Next Business Day
SAN	Storage Area Network
SMTP	Simple Mail Transport Protocol
SNMP	Simple Management Transport Protocol
SSL	Secure Socket Layer
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
OS	Operating System (Betriebssystem)
LACP	Link Aggregation Control Protocol

### 1.3 Gültigkeit und Einschränkungen

Alle Vorgaben in diesem Dokument sind spezieller zu werten, als die durch Standardformulare gesetzten Vorgaben. Die Definitionen in diesem Dokument ersetzen hiermit Definitionen und Anforderungen aus Vergabeformularen.

Dieses Dokument besitzt eine zeitlich eingeschränkte Gültigkeit, angegeben durch „Nächste Überprüfung“ im Deckblatt. Bei Ausschreibungen oder Verträgen ist nach Ablauf dieses Datums zu überprüfen, ob eine aktualisierte Version bereitgestellt wurde. Wenn keine neuere Version verfügbar ist, bleiben die Vorgaben aus der letzten verfügbaren Version gültig.

Alle technischen Mindestanforderungen des DBFZ sind unter <https://www.dbfz.de/tma> verfügbar.

### 1.4 Grundlegende Anforderungen

Die aktuelle Systemlandschaft der Auftraggeberin, im Folgenden DBFZ genannt, besitzt grundlegende Anforderungen an Server- und Infrastrukturkomponenten:

- Redundante Ausstattung,
- Hohe Ausfallsicherheit,
- Erfüllung der BSI Grundschutzanforderungen für Rechentechnik,
- Datensicherheit,
- Erreichbarkeit (Hochverfügbarkeit),
- Kosteneffizienz,
- Fünf Jahre Support/Wartung Reaktionszeit 4h Mission Critical (Betriebsverhindernder Mangel 24h Wiederherstellungszeit),
- Hardware Supportleistungsgarantie min. bis 5 Jahre nach Auslieferung

Dieses Dokument beinhaltet die minimalen Vorgaben für eine Erweiterung auf Basis der geforderten Gesichtspunkte.

## 2 Vorgaben

### 2.1 Grundlegende Hardwarekonfiguration

Alle angebotenen Komponenten müssen als 19 Zoll Rack-Lösung geliefert werden. Je nach Lösung müssen notwendige Softwarekomponenten und dazugehörige Lizenzen mitgeliefert werden. Alle in diesem Dokument gesetzten Vorgaben sind als Mindestvoraussetzung zu werten.

Der Auftraggeber muss bei Angebotsabgabe über die verwendeten 19 Zoll Höheneinheiten (HE) aller Komponenten informiert werden. Hierbei müssen zusätzlich die notwendigen Anschlüsse für Netzwerk, Stromversorgung und andere Infrastrukturkomponenten aufgeschlüsselt werden.

Für Angaben zu Vorraussetzungen von Komponenten dürfen nur solche berücksichtigt werden, die aktuell verfügbar sind. Ankündigungen zukünftiger Produkte dürfen nicht zu Grunde gelegt werden.

## 2.2 Anforderungen für Serverhardware

Seitens des Auftraggebers wird die Infrastruktur für 19 Zoll Komponenten bereitgestellt. Ebenfalls wird die unterbrechungsfreie Stromversorgung durch die IT des DBFZ sichergestellt.

In der folgenden Tabelle werden alle Vorgaben an die Serverausstattung zusammengefasst.

Vorgabe	Wert	Bemerkung
Prozessor	Aktuell verfügbare Version des Intel Xeon E5m AMD EPYC	Je nach System Anforderungen, können höhere CPU Anforderungen definiert werden
Raid	Hardware Raid-Controller Raid 1 / Raid 5 / Raid 10	Alternativ können begründet Software-Raids eingesetzt oder Dateisystemorganisierte Raid-Systeme eingesetzt werden
Festplatten	SAS SSD / SSD	Bei Verwendung von SSDs ist darauf zu achten, dass diese als schreibintensive Enterprise Version verwendet wird
Netzteile	Redundante Auslegung	
Netzwerk	2x 10 GBit Kupfer LACP	LACP muss kompatibel mit Cisco
KVM / Managed Module	Netzwerk Remoteconsole, Überwachung und Hardwarekontrolle.	Vergleichsweise HP iLO oder Dell DRAC
SNMP/IPMI	Überwachung der Hardwarekomponenten.	Hierbei muss beim Ausfall einzelner Komponenten eine Warnung auslesbar sein.

Tabelle 1: Vorgaben Serverhardwareausstattung

Für die Speicherung der Daten sind für alle Serversysteme und Systeme mit zentralgespeicherten Nutzerdaten Raid-Systeme zu verwenden.

Raid	HW/System/Software	Serversystem	Betriebssystem	Nutzerdaten niedriger Klassifizierung	Nutzerdaten hohe Klassifizierung	Daten Versuchsanlagen	Daten für dedizierte Anwendungen
Raid 1	Hardware	Serversysteme	X	X		X	X
Raid 5	Hardware	Serversysteme		X		X	X
Raid6	Hardware	Serversysteme			X		
Raid 10	Hardware	Serversysteme			X		
Raid 1	Software	Serversysteme/ technische Systeme	X			X	
Raid 5	Software	technische Systeme				X	X
Raid 1	System BTRFS	Serversysteme	X	X		X	X
RAID- Z1	System ZFS RAID-Z1	Serversysteme	X	X		X	X
RAID- Z2	System ZFS RAID-Z2	Serversysteme	X	X			X

Tabelle 2: Vorgaben Raid-Systeme

## 2.3 Anforderungen Betriebssysteme

### 2.3.1 Windows Betriebssysteme

Bei der Verwendung von Microsoft Betriebssystemen für Serverkomponenten ist im DBFZ die Verwendung der Microsoft Serverbetriebssysteme (Windows Server) vorgeschrieben. Die Lizenzen für die Serversysteme müssen durch den Auftragnehmer mitgeliefert werden. Einzelnachweise für den Erwerb und die Weitergabe der Lizenz muss Bestandteil der Lieferung sein.

Der Betrieb aller erforderlichen Dienste muss ohne eine zusätzliche Daueranmeldung eines Benutzers möglich sein. Konfigurationen, bei denen ein Benutzer generell angemeldet ist, um eine Software im Autostart zu starten, sind nicht zulässig.

Zusätzlich müssen folgende Anforderungen erfüllt werden:

Vorgabe	Wert	Bemerkung
Windows Server Version	Windows Server Standard 2019	Es kann auch eine höherwertige Version lizenziert werden
HyperV Technologien zulässig	Ja	Aber nur, wenn dies notwendig ist.
Firewall	Muss aktiviert sein	Firewallregeln müssen vorher mit der IT des DBFZ abgesprochen und dokumentiert werden
IPv4/IPv6	Eine DUAL Stack Konfiguration von IPv4 und IPv6 ist für den Einsatz neuer Server vorgeschrieben.	Globale Adressen werden durch das DBFZ zur Verfügung gestellt
Dienste	Dokumentation der zusätzlichen Dienste und Komponenten	

Tabelle 3: Betriebssysteme



### 2.3.2 Anforderungen für Linux Systeme

Für die Verwendung von Linux Systemen ist zu beachten, dass die Aktualität der Komponenten durch den Hersteller oder den Auftragnehmer gewährleistet sein muss. Folgende Linux Distributionen sind für Serversysteme am DBFZ zulässig:

- Linux Debian (Version > 10)
- Red Hat Enterprise (aktuelle Version)
- Ubuntu aktuelle LTS
- Suse Enterprise (aktuelle Version)

Bei der jeweiligen Version muss ein Support von mindesten 3 Jahren ohne Versionswechsel möglich sein. Dies bedeutet, dass die jeweils aktuellste LTS Version zum Einsatz kommen muss.

Für einen Versionswechsel des Linux Systems muss von Hersteller die Lauffähigkeit der angebotenen Anwendungen über einen Zeitraum von fünf Jahren unentgeltlich garantiert werden. Auch bei Veränderungen durch Updates der Systeme muss die Lauffähigkeit der angebotenen Komponenten und Anwendungen für mindesten fünf Jahre garantiert werden.

Weitere Anforderungen für die Verwendung von Linux Systemen sind in der folgenden Tabelle aufgeführt:

Vorgabe	Wert	Bemerkung
Updates	Manuelle Updates müssen für fünf Jahre garantiert werden	
Virtualisierung	Ja	
Firewalls	Muss aktiviert sein.	
root Zugriff	notwendig	
IPv4/IPv6	Eine DUAL Stack Konfiguration von IPv4 und IPv6 ist für den Einsatz neuer Server vorgeschrieben.	Globale Adressen werden durch das DBFZ zur Verfügung gestellt
Dienste	Dokumentation der zusätzlichen Dienste und Komponenten	

Tabelle 4: Vorgaben Linux

### 2.3.3 Andere Systeme (Blackbox Systeme, Hardwaresysteme)

Für alle anderen Systeme wie Blackbox Systeme, muss mit der IT Abteilung des DBFZ im Vorfeld der Einsatz und die Absicherung des Systems abgesprochen werden.

Systeme wie Blackbox Systeme sind **nur** zulässig, wenn folgende Kriterien **nicht** anwendbar sind:

- Datenspeicherung von Forschungsdaten oder Verwaltungsdaten ohne zusätzliche Sicherung im Netz,
- Datenhaltung von Labordaten,
- Anwendungsentwicklungen und Dateien ohne weitere Sicherung (siehe 2021.03.Softwareentwicklung),
- Speicherung von Benutzerdaten,
- Speicherung von Projektdaten

Sicherheitskritische Systeme müssen zusätzlich für den Einsatz entsprechende Zertifizierungen nachweisen. Die Aktualität dieser Zertifizierungen muss bei jeder Beschaffung durch die IT des DBFZ geprüft und bestätigt werden und muss für die aktuell angebotenen Systeme zur Verfügung stehen. Generelle Zertifikate, beispielsweise für eine Technologie, sind hier nicht ausreichend.

Bei geschlossenen Systemen müssen vorhandene Versions- und Patchstände der verwendeten Software und Systemdateien offengelegt werden. Das DBFZ behält sich vor, Penetrationstest durchzuführen und deren Ergebnisse zu veröffentlichen.

Der Hersteller muss mindestens über einen Zeitraum von fünf Jahren oder wenn abweichend gefordert, während der geplanten Laufzeit, Updates und Upgrade ohne weitere Kosten zur Verfügung stellen. Hierbei müssen auch neue Technologien, wenn diese für einen weiteren Betrieb notwendig sind, kostenfrei während der geforderten Laufzeit zur Verfügung gestellt werden. Alternativ ist die Absicherung einer Updatebereitstellung über den in Kapitel 4 beschriebenen Wartungsvertrag abdeckbar.

Grundlegende Vorgaben für solche Systeme sind in der folgenden Tabelle aufgeführt.

Vorgabe	Wert	Bemerkung
Updates	Updates für Fehler und Sicherheitsrisiken müssen für fünf Jahre garantiert werden	
Raid	Für Daten und System: Raid 1/Raid5	Software Raid ist zulässig, muss aber vorher dokumentiert werden
Netzteile	Redundant	
Netzwerk	2x 1GBit	LACP, Cisco kompatibel

SNMP/IPMI	Notwendig	Auslesen des Systemzustand muss möglich sein.
Firewall	aktiviert	Regeln müssen vom Auftragnehmer oder Hersteller dokumentiert werden.
IPv4/IPv6	Eine DUAL Stack Konfiguration von IPv4 und IPv6 ist für den Einsatz neuer Server vorgeschrieben.	Globale Adressen werden durch das DBFZ zur Verfügung gestellt.
8021x	Muss unterstützt werden	Aktuell werden am DBFZ nur TLS und MD5 für die Authentifizierung unterstützt.

Tabelle 5: Vorgaben andere Systeme

Am DBFZ werden regelmäßig Penetrationstests durchgeführt. Bei Feststellung von Sicherheitsrisiken muss der Auftragnehmer oder der Hersteller umgehend Updates oder Workarounds bereitstellen.

Zusätzlich verpflichtet sich der Auftragnehmer, dass Informationen zu Sicherheitslücken zeitnah zur Verfügung gestellt werden. Hierbei kann beispielsweise die Möglichkeit von Mails mit den Informationen zu Sicherheitslücken zur Abhilfe verwendet werden. Auch wäre eine Informationsverteilung über DFN-Cert Meldungen, die seitens des DBFZ geprüft werden, möglich.

Aktuell nicht gepflegte und supportete Betriebssysteme dürfen ausdrücklich nicht verwendet werden. Dies gilt auch für Komponenten, die nicht in produktiven Bereichen eingesetzt werden.

Bei der Verwendung von Blackbox-Systemen sind dem Auftraggeber folgende Informationen zur Verfügung zu stellen:

- Verwendetes Betriebssystem und Version
- Verwendete Softwarekomponenten und deren Versionen
- Verwendete Komponenten
- Möglichkeiten der Konfiguration
- Bekannte Zugriffsmöglichkeiten (WEB-Interface, Telnet, SSH etc.)

## 2.4 Einrichtung

Die Komponenten müssen durch den Auftragnehmer nach den oben genannten Vorgaben installiert werden. Die Installation muss nicht vor Ort durchgeführt werden. Die Abschlussarbeiten und die Inbetriebnahme müssen vor Ort zusammen mit der IT des DBFZ durchgeführt werden. Eventuell zusätzliche Herstellervorgaben müssen im Vorfeld mit dem DBFZ abgesprochen werden.

Entsprechende Kabel-Infrastruktur ist bereits vorhanden. Material zur Installation (Netzwerkkabel, Module) muss durch den Auftragnehmer geliefert werden.

Zur Übernahme müssen folgende Dokumente an den Auftraggeber übergeben werden:

- Lizenzunterlagen
- Schulungsunterlagen
- Dokumentation über den Aufbau des Systems
- Dokumentation über zusätzliche Firewallregeln
- Dokumentation über zusätzliche Windowsdienste und -features
- Ansprechpartner und Supportinformationen

## 3 Herstellung der Betriebsbereitschaft, Schulung

Die Herstellung der Betriebsbereitschaft der Hard- und Software erfolgt beim Auftraggeber durch den Auftragnehmer. Die Demonstration der Betriebsbereitschaft des Systems umfasst neben der Vorführung der Ablauffähigkeit insbesondere die unter Punkt 2 dargestellten Funktionalitäten. Alle angebotenen Komponenten müssen entsprechend der Vorgaben miteinander kompatibel sein.

Im Zuge der Herstellung der Betriebsbereitschaft müssen alle Komponenten nach Vorgaben des DBFZ eingerichtet werden. Der Auftrag ist erst abgeschlossen, wenn die Systemlieferung aller erforderlichen Hard- und Softwarekomponenten abschließend bewirkt ist. Dies muss innerhalb von maximal acht Wochen nach Zuschlagserteilung erfolgt sein.

Bei der Einrichtung der Komponenten müssen die Mitarbeiter vor Ort entsprechend geschult werden. Die Schulung findet am Tag der Herstellung der Betriebsbereitschaft statt und ist für zwei Mitarbeiter vorzusehen. Die Mitarbeiter müssen nach Abschluss der Systemlieferung der Geräte und der Software selbstständig in der Lage sein, diese zu bedienen und zu konfigurieren.

#### 4 Service und Maintenance, fakultativ: Garantie

Für alle Aufträge und Ausschreibungen muss ein fünfjähriger Servicevertrag angeboten werden. Folgende Voraussetzungen müssen in einem Servicefall erfüllt werden:

- Maximal 24 Stunden Erstreaktionszeit,
- Wiederherstellungszeiten
  - Betriebsverhindernder Mangel: 24 Stunden
  - Betriebsbehindernder Mangel: 48 Stunden
  - Leichter Mangel: 7 Tage/5 Arbeitstage,
- die Serviceunterstützung bei Hardwarefehlern muss vor Ort ausgeführt werden

Je nach Anforderungen an das System, können geringere Reaktions- und Wiederherstellungszeiten festgelegt werden.

Software-Updates, Sicherheitsupdates und neue Feature-Packs während des gesamten Zeitraums (fünf Jahre) sind in einem Pauschalpreis festzulegen. Das Gleiche gilt für die Anpassungen an neue Technologien, wie zum Beispiel an neue Verschlüsselungs- oder Authentifizierungstechnologien.

Sollten Sicherheitslücken durch den Hersteller oder anderer Institute wie das DFN-CERT bekannt werden und diese aktiv ausgenutzt werden, müssen diese zeitnah, spätestens nach 2 Tagen, geschlossen werden.

Alle angebotenen Komponenten sollten eine unselbständige Garantie mit Vorort austausch für einen Zeitraum von fünf Jahren beinhalten. Deshalb wird über die Mängelhaftung nach Ziffer 13 EVB-IT Systemlieferungs-AGB hinausgehend der Abschluss einer individuellen Garantievereinbarung in der folgenden Form angestrebt:

Alternativ kann für alle Komponenten ein Wartungsvertrag inklusive kostenlosem Hardwaretausch angeboten werden. Dieser muss ebenfalls den kostenlosen Austausch aller Komponenten ermöglichen und notwendige Softwareupdates / -upgrades während des Wartungszeitraums beinhalten.

Der Auftragnehmer garantiert für die Dauer von fünf Jahren, dass die Sache frei von jeglichen Sachmängeln im Sinne des § 434 BGB ist. Dies gilt auch für solche Mängel, die erst nach Gefahrübergang auftreten (unselbständige Garantie). Er steht also unbedingt und vorbehaltlos dafür ein, dass innerhalb dieses Zeitraums ab Gefahrübergang der Gegenstand mangelfrei ist und bleibt.

Grundsätzlich ist ein Remote Support für die Beseitigung von Mängeln möglich. Seitens des DBFZ wird hierbei auf die Lösung BOMGAR gesetzt, die basierend auf HTTPS eine Remoteunterstützung ermöglicht. Diese zeichnet alle Tätigkeiten während einer Sitzung auf und speichert diese auf Servern des DBFZ. Eine nachträgliche Auswertung ist somit jederzeit gewährleistet.

## 5 Bereitstellung eines Pflichtenheftes

Für Ausschreibungen und Verträge mit Bestellungen von Serverkomponenten muss ein Pflichtenheft bereitgestellt werden. Die Aufschlüsselung der angebotenen Komponenten und Dienstleistungen muss einzeln ausgewiesen werden.

Eine Wertung muss grundsätzlich durch die IT des DBFZ durchgeführt werden. Bei Nichterfüllung der Vorgaben behält sich das DBFZ vor, die Hardware für einen produktiven Betrieb am DBFZ auszuschließen.