Anlage 2
zur IT-Standardisierungsrichtlinie

IT-Standards Land Brandenburg

Runderlass der Landesregierung
Az: 1793/04 vom 15. Juni 2004
Fortschreibung durch Beschluss des RIO-Ausschusses
am 28. September 2021

SAGA-Modul Standards
Version de.bb 5.4.0

Inhaltsverzeichnis

1 Einleitung 3
1.1 Anwendung des Klassifikationssystems 3

2 Management-Methoden 4
2.1 Projektmanagement 4
2.2 Wirtschaftlichkeitsbetrachtungen 4
2.3 Software- und Systemtests 5
2.4 Einführung, Betrieb sowie Außerbetriebnahme von IT-Verfahren 5
2.5 Green IT 5

3 Informationssicherheit 6
3.1 Zertifizierte Produkte und Dienstleistungen 6

4 Prozessmodelle 6

5 Datenmodelle 6

6 Backend-Architektur (Server) 7
6.1 Server-Betriebssysteme 7
6.1.1 Red Hat Linux 7
6.1.2 Suse Linux 7
6.1.3 Windows Server 7
6.1.4 HP Unix 7
6.1.5 Ubuntu Server 7
6.2 Datenbanksysteme 7
6.2.1 MySQL 7
6.2.2 Microsoft SQL 8
6.2.3 Informix 8
6.2.4 Oracle 8
6.2.5 PostgreSQL 8
6.3 Cluster Suite 9
6.4 Hypervisor 9
6.5 Container Laufzeitumgebungen 9

7 Client 10
7.1 Client-Betriebssysteme 10
7.2 Web-Browser 10
7.3 PDF-Reader 11
7.4 Büroanwendungen 11
7.5 Groupware-Anwendung 11
7.6 Client-Datenbanken 11
7.7 Hardware-Schnittstellen 11
7.8 Weitere Implementationen beim Standard-Client 11

8 Präsentation 12
8.1 Barrierefreie Darstellung 12
8.2 Zeichensätze und -kodierungen 12
8.3 Informationsaufbereitung 12

8.4 Austauschformate für Daten 13
8.5 Austauschformate für Dokumente 13
8.5.1 Dokumente zum Informationsaustausch 13
8.5.2 Textdokumente zur Weiterbearbeitung 13
8.5.3 Tabellendokumente zur Weiterbearbeitung 14
8.5.4 Gesicherter Dokumentenaustausch 14
8.6 Austauschformate für Bilder 14
8.7 Geoinformationen 15
8.7.1 Raumbezug der Geodaten 15
8.7.2 Metadaten für Geoinformationen 15
8.7.3 Geodatenaustausch 15
8.8 Datenkompression 16
8.9 Open-Government-Data 16
8.9.1 Metadaten für Open-Government-Data 16
8.9.2 Austausch der Metadaten für Open-Government-Data 16

9 Kommunikation 16
9.1 Netzwerk 16
9.2 Firewall 17
9.3 Virenschutz 17
9.4 E-Mail 17
9.5 Anwendungsprotokolle 18
9.6 Verzeichnisdienste 18
9.7 Webbasierte Geodienste 19
9.7.1 Koordinatensysteme und Projektionen 19
9.7.2 Darstellungsdienste 19
9.7.3 Downloaddienste 20
9.7.4 Suchdienste 21
9.7.5 Sonstige Geodienste 21
9.7.6 Veröffentlichung der webbasierten Geodienste 21

10 Backend 21

11 Verschlüsselung/Elektronische Signatur 22

12 Chipkarten 23
12.1 Kontaktbehaftete Chipkarten 23
12.2 Kontaktlose Chipkarten 23
12.3 Schnittstellen für Chipkarten 23

13 Archivierung 23

14 Migrationen 23

A E-Government Basiskomponenten 24
A.1 Basiskomponenten gemäß § 11 BbgEGovG 24
A.2 Content Management System 24
A.3 Webkartenkomponente 24

B IT-Querschnittsverfahren 25
B.1 Personal- und Stellenverwaltung 25
B.2 Haushalts-Kassen-Rechnungswesen (HKR) und Kosten- und Leistungsrechnung (KLR) 25
B.3 Haushaltsaufstellungsverfahren 25
B.4 Reisekostenrechnung 25
B.5 Wirtschaftlichkeitsberechnungen 25
B.6 Webbasierte Kommunikations- und Dokumentenplattform 25
B.7 Vorschriftensystem 26
B.8 Vorgangsbearbeitung und Aktenhaltung 26
B.9 Kabinettinformationssystem 26
B.10 Elektronische Normenverkündung 26
B.11 Stellenportal im Internet 27
B.12 Monitoring 27
B.13 Wissensmanagement 27
B.14 Projekt-Management Software 27

B.15 Telefonie 27
B.16 Videokonferenzen 27

C Abkürzungsverzeichnis 27

D* Alphabetische Übersicht klassifizierter verbindlicher Standards

1 Einleitung

SAGA[1] de.bb ist die Fortschreibung der IT-Standards des Landes Brandenburg entsprechend der IT-Standardisierungsrichtlinie[2]. Es ist eine Zusammenstellung von Referenzen auf Spezifikationen (Protokolle, Schnittstellen, Datenformate und Methoden) und Implementationen (Produkte und Verfahren) für IT-Systeme des Landes Brandenburg. SAGA de.bb orientiert sich an SAGA de.bund[3].

SAGA de.bb ist modular aufgebaut. Die SAGA-Module können zeitlich und weitgehend inhaltlich unabhängig voneinander publiziert werden. Jedes SAGA-Modul wird separat versioniert. Die aktuelle Gesamtversion von SAGA de.bb setzt sich aus den neuesten Versionen aller SAGA-Module zusammen. Alle verfügbaren SAGA-Module sind auf BRAVORS[4] zu finden.

Dieses SAGA-Modul klassifiziert die technischen Spezifikationen und Implementationen, mit denen die IT-Systeme der Landesverwaltung realisiert werden müssen. Es werden die Themengebiete betrachtet, bei denen der Einsatz einheitlicher Standards die Erreichung der Ziele von SAGA de.bb[5] am meisten befördert.

Dieses Modul wird entsprechend der IT-Standardisierungsrichtlinie regelmäßig fortgeschrieben.

Wenn für Standards keine Versionsnummern angegeben sind, ist die aus Marktsicht stabilste, finalisierte Version zu verwenden, welche nicht immer die neueste Version sein muss.

Zur Vereinfachung der Notation ist der Begriff „SAGA“ in diesem Dokument, sofern nicht anders angegeben, immer mit SAGA de.bb gleichzusetzen.

1.1 Anwendung des Klassifikationssystems

Das System zur Klassifikation von Standards (Spezifikationen und Implementationen) durch SAGA de.bb wird im SAGA-Modul „Grundlagen“[6] näher beschrieben. In diesem Modul befinden sich technische Standards mit den Klassifikationen „Verbindlich“, „Empfohlen“, „Beobachtet“ und „Bestandsgeschützt“. Die technischen Standards mit den Klassifikationen „Vorgeschlagen“ und „Verworfen“ können von der E-Government- und IT-Leitstelle im Ministerium des Innern und für Kommunales (MIK) des Landes Brandenburg erfragt werden. In den folgenden Ausführungen werden die sechs Klassen hinsichtlich ihrer Anwendung betrachtet.

Vorgeschlagen

Es ist nicht SAGA-konform, vorgeschlagene Standards einzusetzen, wenn es konkurrierende Standards[7] gibt, die bestandsgeschützt, beobachtet, empfohlen oder verbindlich sind. Wenn es keine konkurrierenden Standards gibt, die höher klassifiziert wurden, befindet sich das Themenfeld noch außerhalb der Festlegungen von SAGA de.bb und ist für die Betrachtung der SAGA-Konformität nicht relevant.

Beobachtet

Wenn es neben den beobachteten Standards keine konkurrierenden empfohlenen oder verbindlichen Standards gibt, SOLLTEN beobachtete Standards in IT-Systemen eingesetzt werden. Nur in begründeten Ausnahmen KÖNNEN beobachtete Standards empfohlenen Alternativen vorgezogen werden.

1* Teil D wird hier nicht veröffentlicht.
SAGA ist ein Eigenname, der ursprünglich als Abkürzung von „Standards und Architekturen für eGovernment-Anwendungen“ eingeführt wurde.

2 http://bravors.brandenburg.de/de/verwaltungsvorschriften-221628

3 Die Beauftragte der Bundesregierung für Informationstechnik: *SAGA*; 2011; http://www.cio.bund.de/saga

4 http://www.bravors.brandenburg.de/

5 Siehe SAGA-Modul Grundlagen de.bb 5.0.0,
http://bravors.brandenburg.de/br2/sixcms/media.php/66/Anlage%202%20IT-Standardisierungsrichtlinie%20%28Grundlagen%29.pdf

6 Siehe SAGA-Modul Grundlagen de.bb 5.0.0,
http://bravors.brandenburg.de/br2/sixcms/media.php/66/Anlage%202%20IT-Standardisierungsrichtlinie%20%28Grundlagen%29.pdf

7 Zwei Standards konkurrieren, wenn beide zur Erfüllung der Anforderungen eines Projekts geeignet sind.

Empfohlen

Konkurrierende Standards können nebeneinander empfohlen sein, wenn sich ihre Anwendungsschwerpunkte deutlich unterscheiden. In solchen Fällen SOLLTE der für die jeweilige Anwendung am besten geeignete Standard angewendet werden.

Von den empfohlenen Standards KANN in begründeten Ausnahmen abgewichen werden. Zu einem empfohlenen Standard gibt es keine verbindliche Alternative, da eine Empfehlung neben einem verbindlich einzusetzenden Standard keinen Sinn hat.

Verbindlich

Konkurrierende Standards können nebeneinander verbindlich sein, wenn sich die Anwendungsschwerpunkte deutlich unterscheiden. In solchen Fällen MUSS der für die jeweilige Anwendung am besten geeignete Standard verwendet werden.

Standards dieser Klassifikation sind im eigentlichen Sinne des Wortes verbindlich, MÜSSEN also bei der Einführung eines neuen IT-Systems jeder Alternative vorgezogen werden. Abweichungen gefährden die Ziele von SAGA de.bb in hohem Maße und sind deshalb nicht zugelassen.

Bei der funktionalen Änderung oder Erweiterung eines IT-Systems KÖNNEN als „Bestandsgeschützt“ klassifizierte Standards weiterhin genutzt werden. Es MUSS jedoch geprüft werden, ob die Migration zum verbindlichen Standard vorteilhaft ist.

Über Ausnahmen entscheidet die IT-Leitstelle.

Bestandsgeschützt

Bei der funktionalen Änderung oder Erweiterung eines IT-Systems stehen diese Standards unter Bestandsschutz und KÖNNEN auch weiterhin eingesetzt werden. Es SOLLTE geprüft werden, ob eine Migration zu den in SAGA de.bb als „Beobachtet“ oder „Empfohlen“ klassifizierten Standards Vorteile gegenüber dem Festhalten an als „Bestandsgeschützt“ klassifizierte Standards bringt. Gibt es eine als „Verbindlich“ klassifizierte Alternative, MUSS diese Überprüfung durchgeführt werden.

Verworfen

Verworfene Standards KÖNNEN dann eingesetzt werden, wenn parallel eine SAGA-konforme Lösung zur Verfügung gestellt wird.[8] Allein DÜRFEN diese Standards in neuen sowie in bestehenden IT-Systemen NICHT eingesetzt werden. Spätestens bei funktionalen Änderungen oder Erweiterungen MÜSSEN sie ausgetauscht werden. Dazu MUSS für die Erweiterung des Funktionsumfanges, gegebenenfalls unter Einsatz von Kapselung, von verworfenen Standards weg migriert oder eine SAGA-konforme Alternative geschaffen werden. Es SOLLTE jedoch für das gesamte bestehende IT-System geprüft werden, ob eine Migration oder Erweiterung vorteilhaft ist.

2 Management-Methoden

2.1 Projektmanagement

IT-Projekte MÜSSEN anhand einheitlicher Projektmanagementmethoden durchgeführt werden.

Empfohlene Spezifikation: Projektmanagementleitfaden

Als Methodik SOLLTE der Leitfaden Projektmanagement[9] in seiner jeweils geltenden Version eingesetzt werden.

2.2 Wirtschaftlichkeitsbetrachtungen

Verbindliche Spezifikation: WiBe 5.0 Kriterienkatalog

Für Wirtschaftlichkeitsbetrachtungen MUSS der Kriterienkatalog des WiBe-Fachkonzeptes 5.0[10] genutzt werden.

Für die Implementation siehe B.5 „Wirtschaftlichkeitsberechnungen“.

---

[8] Zum Beispiel dürfen Bilder im BMP-Format zur Verfügung gestellt werden, obwohl diese Spezifikation verworfen wurde, wenn gleichzeitig die Bilder auch in einem SAGA-konformen Format wie GIF angeboten werden.

[9] Nur im Intranet der Landesverwaltung: http://www.lynbb.de/media_fast/2134/Leitfaden_Projektmanagement.pdf

[10] http://www.cio.bund.de/wibe

2.3 Software- und Systemtests

Beobachtete Spezifikation: IEEE 829

Im Bereich der Polizei werden Software- und Systemtests in länderübergreifenden Verbünden angelehnt an den Standard IEEE 829 entsprechend erstellt und durchgeführt.

2.4 Einführung, Betrieb sowie Außerbetriebnahme von IT-Verfahren

Verbindliche Spezifikation: Richtlinie Verfahrensbetrieb

Für die Einführung, den Betrieb sowie die Außerbetriebnahme von IT-Verfahren MUSS bei IT-Verfahren, für deren Betrieb der ZIT-BB zuständig ist, die Richtlinie für die Einführung, den Betrieb sowie die Außerbetriebnahme von IT-Verfahren (Richtlinie Verfahrensbetrieb) angewendet werden.

2.5 Green IT

Die Bedeutung von Umweltschutz und ressourcenschonendes Verhalten ist wichtiger denn je. Das Land Brandenburg strebt einen verantwortungsbewussten und effizienten Umgang mit natürlichen Ressourcen an. Weil vor allem die IT ein großer Ressourcen-Verbraucher ist, besteht hier ein besonderes Potenzial. Aus diesem Grund ist es empfehlenswert die Ziele von Green IT anzustreben. Sie verfolgt das Ziel, Herstellung, Nutzung und Entsorgung von Geräten der IT über den gesamten Lebenszyklus hinweg umwelt- und ressourcenschonend zu gestalten.

Aus diesem Grund SOLLTE Green IT in Bezug auf Herstellung, Nutzung und Entsorgung von IT berücksichtigt werden.[11]

3 Informationssicherheit

In Bezug auf die Gewährleistung der IT-Sicherheit MUSS der IT-Grundschutz auf Basis der Sicherheitsmaßnahmen gemäß den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dem BSI-Grundschutzkompendium in der jeweils aktuellen Fassung[12] gewährleistet werden.

Verbindliche Spezifikation: BSI-Standard 200-1: Managementsysteme

Verbindliche Spezifikation: BSI-Standard 200-2: IT-Grundschutz-Methodik

Verbindliche Spezifikation: BSI-Standard 200-3: Risikomanagement

Verbindliche Spezifikation: BSI-Standard 100-4: Notfallmanagement

Beobachtete Spezifikation: BSI-Standard 200-4: Business Continuity Management (Community Draft)

Verbindliche Spezifikation: BSI IT-Grundschutz-Kompendium

Verbindliche Spezifikation: Landeseinheitliche Schutzbedarfskategorien

Der Betrieb des landesweiten Managementsystems für Informationssicherheit MUSS auf Grundlage der Informationssicherheitsleitlinie der Landesverwaltung Brandenburg[13] erfolgen.

Für das Erstellen von Sicherheitskonzepten MÜSSEN die methodischen Vorgaben des BSI (BSI-Standards) beachtet werden. Dabei MUSS die Schutzbedarfsfeststellung[14] auf Grundlage festgelegter, landesweit einheitlicher Schutzbedarfskategorien erfolgen.

---

11 https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2021/Sitzung_34.html?pos=11

12 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

13 Nur im Intranet der Landesverwaltung: http://www.lvnbb.de/media_fast/2134/Anlage_2_Leitlinie%20zur%20Gew%C3%A4hrleistung%20der%20Informationssicherheit%20%28Inform....pdf

14 Nur im Intranet der Landesverwaltung: http://www.lvnbb.de/sixcms/detail.php?id=611933&&bbi.itsm

Nach Veröffentlichung einer neuen Ergänzungslieferung durch das BSI KANN diese oder einzelne Bausteine daraus bei der Erstellung von Sicherheitskonzepten Verwendung finden. Ergänzungslieferungen KÖNNEN bei der Erstellung von Sicherheitskonzepten Verwendung finden, solange sie als Prüfgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz zugelassen sind.

Zur Prüfung des erreichten Sicherheitsniveaus gegebenenfalls durchzuführende Revisionen MÜSSEN auf Grundlage des entsprechenden BSI-Leitfadens[15] durchgeführt werden.

Verbindliche Implementation: Produkt verinice Version 1.22.2

Für die zentrale elektronische Erstellung und Fortschreibung von Sicherheitskonzepten MUSS bei der Standard-Absicherung die zentral bereitgestellte Lösung genutzt werden. Behörden und Einrichtungen der Justiz, die nicht dem Kontrahierungszwang unterliegen, sowie die Polizei Brandenburg sind hiervon ausgenommen.

Länderübergreifende Verbünde auf Grundlage von Staatsverträgen oder Verwaltungsabkommen (zum Beispiel der polizeiliche Informationsverbund) sind von diesen Regelungen ausgenommen, soweit die Gewährleistung der IT-Sicherheit im entsprechenden Verbund geregelt wird. Die im Verbund erzielten Sicherheitsniveaus (zum Beispiel verwendete Schutzbedarfskategorien) DÜRFEN aber NICHT hinter das landesweite Sicherheitsniveau (zum Beispiel die festgelegten, landesweit einheitlichen Schutzbedarfskategorien) zurückfallen.

3.1 Zertifizierte Produkte und Dienstleistungen

Vom BSI zertifizierte Produkte und Dienstleistungen MÜSSEN bei gleicher Eignung bevorzugt werden.

4 Prozessmodelle

Verbindliche Spezifikation: Unified Modeling Language (UML) 2.x

Für Prozessmodellierungen im Rahmen von Projekten zur Spezifikation, Konstruktion und Dokumentation von Softwareteilen und anderen Systemen MUSS die Unified Modeling Language (UML) in der Version 2.x genutzt werden.

Empfohlene Spezifikation: Business Process Model and Notation (BPMN) 2.x

Für Modellierung im Rahmen von Projekten zur Spezifikation kompletter Geschäftsprozesse und Arbeitsabläufe SOLLTE die Business Process Model and Notation (BPMN) in der Version 2.x genutzt werden.

5 Datenmodelle

Verbindliche Spezifikation: Unified Modeling Language (UML) 2.x

Für Datenmodellierungen im Rahmen von Projekten MUSS die Unified Modeling Language (UML) in der Version 2.x genutzt werden.

Verbindliche Spezifikation: Entity Relationship (ER) Modell

Für Datenmodellierungen datenbankgestützter Verfahren beziehungsweise in Relationalen Datenbanken MUSS das ER-Modell verwendet werden.

[15] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf

6 Backend-Architektur (Server)

6.1 Server-Betriebssysteme

Bei der Einführung eines neuen Systems oder der Migration eines vorhandenen Systems auf eine neue technische Basis SOLLTE den hier aufgeführten Implementationen, welche im ZIT-BB eingesetzt werden, der Vorzug geben werden. Eine Abweichung von den Betriebsstandards des ZIT-BB befreit nicht vom Kontrahierungszwang. Die Server SOLLTEN mit dem jeweils aktuellen Servicepack und MÜSSEN mit allen Sicherheits-Patches betrieben werden. Der ZIT-BB behält sich vor Systeme, die nicht auf dem neusten Stand sind, in einer Quarantäne-Umgebung zu betreiben oder außer Betrieb zu nehmen.

6.1.1 Red Hat Linux

Empfohlene Implementation: Red Hat Enterprise Linux ab Version 8.x

Bestandsgeschützte Implementation: Red Hat Enterprise Linux ab Version 7

6.1.2 Suse Linux

Empfohlene Implementation: Suse Linux Enterprise Server ab Version 15 SP

Bestandsgeschützte Implementation: Suse Linux Enterprise Server ab Version 12

6.1.3 Windows Server

Empfohlene Implementation: Windows Server 2016

Beobachtete Implementation: Windows Server 2019

Bestandsgeschützte Implementation: Windows Server 2012 R2

Der Status dieses Standards wechselt Ende 2022 auf „verworfen“.

6.1.4 HP Unix

Empfohlene Implementation: HP Unix Version 11.31

Bestandsgeschützte Implementation: HP Unix Version 11.11 und 11.23

6.1.5 Ubuntu Server

Beobachtete Implementation: Ubuntu Server 20.04 LTS

6.2 Datenbanksysteme

Bei der Einführung eines neuen Systems oder der Migration eines vorhandenen Systems auf eine neue technische Basis SOLLTE den hier aufgeführten Implementationen, welche im ZIT-BB (beziehungsweise dem jeweils zuständigen landeseigenen IT-Dienstleister) eingesetzt werden, der Vorzug gegeben werden.

Die Systeme SOLLTEN mit dem jeweils aktuellen Servicepack und MÜSSEN mit allen Sicherheits-Patches betrieben werden.

6.2.1 MySQL

Empfohlene Implementation: MySQL 8.x EE / CE

Das Datenbanksystem MySQL SOLLTE in der Version 8 als Enterprise oder Community Edition (jeweils die neueste Stable Release) eingesetzt werden.

Als Hochverfügbarkeitslösung MUSS Percona XtraDB-Cluster eingesetzt werden.

Bestandsgeschützte Implementation: MySQL 5.7

Der Status dieses Standards wechselt ab Oktober 2023 auf „verworfen“.

Verworfene Implementation: MySQL 5.6

Der Support für dieses Produkt endete im Februar 2021.

Seit dem Support-Ende (Premier Support) von MySQL (in den Versionen 5.6 und 5.7) dürfen diese Versionen nicht mehr neu implementiert werden.

6.2.2 Microsoft SQL

Empfohlene Implementation: Microsoft SQL

Das Datenbanksystem Microsoft SQL Server MUSS entweder in den Versionen 2014, 2016 oder 2019 als Standard oder Enterprise Edition eingesetzt werden.

Das bisher unter Beobachtung stehende Microsoft SQL 2017 wird nicht eingesetzt.

Bestandsgeschützte Implementation: Microsoft SQL 2012

Der Status dieses Standards wechselt Mitte 2022 auf „verworfen“.

6.2.3 Informix

Empfohlene Implementation: Informix 12.10

Das Datenbanksystem Informix SOLLTE in der Version 12.10 als Workgroup oder Enterprise Version eingesetzt werden.

Beobachtete Implementation: Informix 14.10

6.2.4 Oracle

Empfohlene Implementation: Oracle Enterprise Edition 19c (12.2.0.3)

Das Datenbanksystem Oracle MUSS in der Version 19c (12.2.0.3) Enterprise Edition eingesetzt werden.

Als Hochverfügbarkeitslösung MUSS Oracle Real Application Cluster (RAC) eingesetzt werden.

Bestandsgeschützte Implementation: Oracle Database 12.2.0.1 Enterprise Edition

Der Status dieses Standards wechselt ab Ende April 2022 auf „verworfen“.

6.2.5 PostgreSQL

Empfohlene Implementation: PostgreSQL 10.x, 11.x, 12.x

Das Datenbanksystem PostgreSQL IST in den Versionen 10, 11 oder 12 einzusetzen.

Bestandsgeschützter Betrieb: PostgreSQL 9.6

Der Status dieses Standards wechselt ab November 2021 auf „verworfen“.

6.3 Cluster Suite

Empfohlene Implementation: Red Hat High Availability Add-On ab Version RHEL 7.9 und RHEL 8.x

Empfohlene Implementation: Suse High Availability Extension ab Version SLES 12SP5 und 15SP2

Empfohlene Implementation: Microsoft Failover Cluster auf Basis Windows Server 2016 (und höher)

Der Status des bisherigen Standards „Microsoft Failover Cluster auf Basis Windows Server 2012 R2“ wechselt Ende 2022 auf „verworfen“.

Bestandsgeschützter Betrieb: HP Serviceguard for Linux Version 11.20

Bestandsgeschützter Betrieb: Red Hat Cluster Suite

6.4 Hypervisor

Empfohlene Implementation: VMware vSphere ab Version 6.5 (Enterprise)

Empfohlene Implementation: VMware vSphere ab Version 7.x

Bestandsgeschützter Betrieb: VMware vSphere ab Version 6.x

Bestandsgeschützter Betrieb: VMware vSphere ab Version 5.5 bis Q1/2021

Empfohlene Implementation: Microsoft Hyper-V ab Windows Server 2016 (und höher)

Empfohlene Implementation: Citrix Hypervisor Version 8.x

Bestandsgeschützte Implementation: Citrix XEN Server ab Version 7.1 CU2

Bestandsgeschützter Betrieb: Citrix XEN Server Version 6.2

6.5 Container-Laufzeitumgebungen

Bei der Einführung eines neuen Systems oder der Migration eines vorhandenen Systems auf eine neue technische Basis SOLLTEN die hier aufgeführten Implementationen verwendet werden.

Empfohlene Implementation: Podman ab Version 1.9

Die Container-Laufzeitumgebung Podman SOLLTE entweder in Verbindung mit den Betriebssystemversionen ab RHEL 8.2 oder ab SLES 15SP2 eingesetzt werden.

Empfohlene Implementation: Docker-Community Edition (CE) ab Version 19.03

Die Container-Laufzeitumgebung Docker-CE SOLLTE entweder in Verbindung mit den Betriebssystemversionen ab RHEL 8.2 oder ab SLES 15 SP2 eingesetzt werden.

7 Client

Der ZIT-BB betreibt die Clients gemäß Brandenburg-Client 2.0. Der Brandenburg-Client definiert die Installation eines Standard-Clients innerhalb der allgemeinen Verwaltung, wie sie vom ZIT-BB installiert und betrieben wird. Die nachfolgenden Standards stellen eine Teilmenge des Brandenburg-Clients da.

7.1 Client-Betriebssysteme

Verbindliche Implementation Fat-Client: Microsoft Windows 10

Bei Installationen neuer Fat-Clients MUSS als Betriebssystem Windows 10 64-bit eingesetzt werden. Die Clients MÜSSEN mit dem jeweils aktuellen Servicepack und allen Sicherheits-Patches betrieben werden.

Beobachtete Client-Implementation: Open Source als Alternative zu Microsoft

Verbindliche Implementation: ECOS-Bootstick als Produkt des ZIT-BB

Für den Betrieb von Thin-Client-Systemen auf Fremdgeräten MUSS das vom ZIT-BB angebotene Produkt ECOS-Bootstick verwendet werden.

Bestandsgeschützter Betrieb: Thin-Clients IGEL-Linux

Für den Betrieb von Thin-Clients (Hardware und Software) MUSS die zentral bereitgestellte Lösung des ZIT-BB genutzt werden.

Als Betriebssystem auf den Thin-Clients kommt IGEL-Linux zum Einsatz.

Als Desktopbetriebssystem für Terminal-Arbeitsplätze (Design des Desktops für Telearbeit und am Arbeitsplatz) kommt Windows 10 Design unter Windows Server 2016 zum Einsatz.

Verbindliche Implementation: Mobile Device Management System (MDM) vom ZIT-BB

Für alle anderen Endgeräte im Informationsverbund des ZIT-BB mit Datenanbindung an das LVN (Smartphones und Tablets unabhängig vom Betriebssystem) MUSS das Mobile Device Management System des ZIT-BB genutzt werden. Dieser Dienst wird zurzeit mit dem Black Berry Enterprise System (BES 12) realisiert. Näheres regelt eine Sicherheitsrichtlinie.

Verbindliche Implementation: Microsoft Bitlocker

Die Speichermedien von allen mobilen Arbeitsplätzen in der Landesverwaltung MÜSSEN mit Microsoft Bitlocker gegen den unberechtigten Zugriff verschlüsselt werden. Die Überwachung/Administration SOLLTE über MBAM-Konten erfolgen.

7.2 Web-Browser

Verbindliche Implementation: Microsoft Edge Chromium und Mozilla Firefox

Das Land Brandenburg verfolgt für APC, die Kontakt mit dem Internet haben, eine Zwei-Browser-Strategie.

Es MÜSSEN Microsoft Edge Chromium und Mozilla Firefox (das jeweils aktuelle Extended Support Release [ESR] SOLLTE bevorzugt werden) installiert sein. Es MÜSSEN alle Sicherheits-Patches und Updates installiert werden.

Browser-abhängige Mechanismen (Plug-In-Lösungen, Active-X, Visual Basic und so weiter) SOLLTEN NICHT eingebunden werden.

Browser-basierte neue Anwendungen MÜSSEN auf allen klassifizierten Alternativen laufen.

Bestandsgeschützter Betrieb: Internet Explorer 11

Der Status dieses Standards wechselt am 15. Juni 2022 auf „verworfen“.

Der Internet Explorer ist in Abhängigkeit zu Fachverfahren auch im Brandenburg-Client enthalten.

7.3 PDF-Reader

Verbindliche Implementation: Adobe Acrobat Reader DC

Beobachtete Implementation: Open Source als Alternative zum Adobe Acrobat Reader

7.4 Büroanwendungen

Verbindliche Implementation: Microsoft Office 2016 Professional

Beobachtete Implementation: Open Source als Alternative zu Microsoft Office

7.5 Groupware-Anwendung

Verbindliche Implementation: Microsoft Outlook 2016

Als Standard-Mail-Client für Kalender, E-Mail und Kontakte MUSS Outlook 2016 eingesetzt werden.

Beobachtete Implementation: Open Source als Alternative zu Microsoft Outlook

7.6 Client-Datenbanken

Client-Datenbanken SOLLTEN nach Möglichkeit nicht zum Einsatz kommen. Wenn sie jedoch zum Einsatz kommen, gelten die nachfolgenden Standards.

Verbindliche Implementation: Microsoft Access 2016

Falls die Nutzung einer serverbasierten Datenbank wirtschaftlich oder fachlich nicht möglich ist, MUSS als Client-Datenbank Microsoft Access 2016 eingesetzt werden.

Da für Endgeräte beziehungsweise lokale Dateien kein Sicherungskonzept existiert, ist bei Defekt, Fehlverhalten oder Ähnlichem eine Wiederherstellung nicht möglich. Es wird deswegen empfohlen, die Datenbank auf einer Ressource zu speichern, die in eine zentrale Datensicherung eingebunden ist.

7.7 Hardware-Schnittstellen

Die Sicherheitsgefährdungen durch kabelgebundene und kabellose Medien (wie zum Beispiel USB, Firewire, IrDA, Bluetooth und so weiter) MÜSSEN über technische Sicherheitsmaßnahmen beherrschbar gestaltet werden (zum Beispiel BIOS-Sperrung, Deaktivierung von USB-Treibern, Einsatz spezieller Sicherheitssoftware, Verschlüsselung).

Der Erlass einer lokalen organisatorischen Regelung KANN zur Ergänzung technischer Sicherheitsmaßnahmen in Betracht kommen.

7.8 Weitere Implementationen beim Standard-Client

Diese Implementationen stellen die Produkte dar, welche durch individuelle Beschlüsse des RIO-Ausschusses entstanden sind und damit Bestandteil des Brandenburg-Clients 2.0 wurden.

Verbindliche Implementation: KeePass 2.x

Wegen der Vielzahl der Passwörter besteht die Gefahr, dass diese aufgeschrieben und an offensichtlichen Stellen hinterlegt werden. Um dies zu vermeiden, MUSS ein Passwort-Manager angeboten werden.

Verbindliche Implementation: Gym-o-Fizz

Für die Ausgleichsgymnastik an PC-Arbeitsplätzen im Rahmen des Behördlichen Gesundheitsmanagements MUSS das Programm Gym-o-Fizz (gesprochen Gym-Office) eingesetzt werden.

Verbindliche Implementation: 7-Zip

Zum Öffnen und Ändern von Archivdateien aller Art MUSS an allen PC-Arbeitsplätzen das Programm 7-Zip eingesetzt werden.

Für die Erstellung eigener Archivdateien ist Kapitel 8.8 (Datenkompression) zu beachten.

8 Präsentation

8.1 Barrierefreie Darstellung

Verbindliche Spezifikation: Brandenburgische Barrierefreie Informationstechnik-Verordnung (BbgBITV)

Die Brandenburgische Barrierefreie Informationstechnik-Verordnung (BbgBITV) vom 17. September 2019[16] überführt die Richtlinie (EU) 2016/2102 in Landesrecht. Sie legt fest, dass Websites und mobile Anwendungen öffentlicher Stellen die 50 Erfolgskriterien der Web Content Accessibility Guidelines (WCAG) V. 2.1 der Konformitätsstufe AA erfüllen MÜSSEN.

8.2 Zeichensätze und -kodierungen

Verbindliche Spezifikation: Unicode/UTF-8

Bei der Erstellung von Webseiten und Verfahren sowie der Einrichtung von Clients MUSS als Zeichensatz Unicode in der Kodierung UTF-8 eingesetzt werden.

Verbindliche Spezifikation: Lateinische Zeichen in Unicode

Kann ein Verfahren nicht den gesamten Umfang von Unicode verarbeiten, so MUSS als Mindeststandard die Untermenge „Lateinische Zeichen“ in Unicode gemäß Beschluss des IT-PLR (IT-Planungsrat) 2014/04 unterstützt werden.

Beobachtete Spezifikation: DIN SPEC 91379

Die DIN SPEC 91379 wird als Nachfolger des Standards des IT-Planungsrates „Lateinische Zeichen in Unicode“ entwickelt.

Bestandsgeschützte Spezifikationen: ISO 8859-1 und ISO 8859-15

Wo eine Portierung nicht angebracht und angezeigt ist, KANN ISO 8859-1 oder ISO 8859-15 weiterhin eingesetzt werden.

8.3 Informationsaufbereitung

Verbindliche Spezifikation: Hypertext Markup Language (HTML) 5/Extensible Hypertext Markup Language (XHTML) 1.0

Browser-basierte neue Anwendungen MÜSSEN HTML 5 oder XHTML 1.0 nutzen.

Auf den Clients MÜSSEN Web-Browser installiert sein, die HTML 4.01, HTML 5 und XHTML 1.0 anzeigen können.

Verbindliche Spezifikation: Cascading Style Sheets (CSS 3)

Layout und Design von Web-Seiten MÜSSEN mittels CSS 3 umgesetzt werden.

[16] https://bravors.brandenburg.de/verordnungen/bbgbitv

Auf den Clients MÜSSEN Web-Browser installiert sein, die CSS 2.1 und CSS 3 unterstützen.

Empfohlene Spezifikation: Extensible Stylesheet Language Transformations (XSLT)

Neue Anwendungen SOLLTEN Umformungen von XML-Dateien auf dem Server oder dem Client mittels XSL Transformations (XSLT) umsetzen.

Auf den Clients SOLLTEN Web-Browser installiert sein, die XSLT unterstützen.

8.4 Austauschformate für Daten

Verbindliche Spezifikation: XÖV-Standard

Soweit für den Zweck des Datenaustauschs ein XÖV-Standard im XRepository[17] definiert wurde, MUSS dieser genutzt werden. Insbesondere MUSS gemäß den Beschlüssen des IT-Planungsrates (IT-PLR) die Standards XVergabe (elektronische Vergabe), XRechnung (elektronische Rechnungsstellung), XBau und XPlanung (Bau- und Planungsbereich), XDomea (Austausch von Akten und Dokumenten), XFall (einheitliche Datenstruktur bei der elektronischen Antragstellung), XZuFi (Zuständigkeitsfinder) sowie XDatenfelder und XProzess (Föderales Informationsmanagement FIM) genutzt werden.

Für polizeiliche Fachverfahren MÜSSEN für den Datenaustausch in neuen Anwendungen existente spezifische Ableitungen des XÖV-Standards eingesetzt werden (XPolizei, XWaffe, XMeld, …).

Empfohlene Spezifikation: Extensible Markup Language (XML) 1.0

Falls für den Datenaustausch mit anderen Systemen innerhalb oder außerhalb der Landesverwaltung keine festen Formatvorgaben bestehen, SOLLTE als Austauschformat die Extensible Markup Language (XML) verwendet werden.

8.5 Austauschformate für Dokumente

Elektronischer Dokumentenaustausch zwischen den Behörden und nach außen SOLLTE in einem formatgetreuen und inhaltlich unveränderbaren Format erfolgen. Bearbeitbare Formate SOLLTEN die Ausnahme für innerbehördlichen Dokumentenaustausch beziehungsweise für Arbeitsgruppen sein.

Der Versender eines elektronischen Dokumentes ist für die Einhaltung des Dokumentenaustausch-Standards verantwortlich und kann nur bei Einhaltung des Standards von einer Übermittlung des Dokumentes beziehungsweise der Informationen ausgehen.

Im Sinne eines einheitlichen Vorgangsverbundes der Ressorts sind die folgenden Festlegungen für bearbeitbare und nicht bearbeitbare Dokumentenaustauschformate verbindlich für die Landesverwaltung.

8.5.1 Dokumente zum Informationsaustausch

Dokumente, die dem Austausch von Informationen dienen, sollen von der Zielgruppe ausschließlich gelesen und nicht verändert werden. Eine weitere Bearbeitung ist deshalb nicht vorgesehen.

Verbindliche Spezifikation: Portable Document Format (PDF) 2.0

Für Dokumente, die beim Empfänger nicht bearbeitet werden sollen, MUSS das Portable Document Format (PDF) in der Version 1.5 (entsprechend ISO 32000-2) verwendet werden.

Die Einschränkung von Nutzer-Rechten (zum Beispiel bezüglich Drucken, Markieren und Kopieren) und proprietäre Erweiterungen SOLLTEN NICHT verwendet werden.

8.5.2 Textdokumente zur Weiterbearbeitung

Verbindliche Spezifikation: Office Open XML (OOXML)

Auf die Verwendung von eingebetteten Makros und Objekten MUSS verzichtet werden.

[17] https://www.xrepository.de/

Beobachtete Spezifikation: Open Document Format (ODF)

8.5.3 Tabellendokumente zur Weiterbearbeitung

Verbindliche Spezifikation: Office Open XML (OOXML)

Auf die Verwendung von eingebetteten Makros und Objekten MUSS verzichtet werden.

Beobachtete Spezifikation: Open Document Format (ODF)

8.5.4 Gesicherter Dokumentenaustausch

Für allgemeine Spezifikationen siehe Kapitel 11 „Verschlüsselung/Elektronische Signatur“.

Empfohlene Spezifikation: Common PKI Specifications for Interoperable Applications (Common PKI) 2.0

Für die Verwendung von signaturgestützten Produkten SOLLTE der Standard Common PKI 2.0 beachtet werden. Bei der Umsetzung MÜSSEN die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beachtet werden.

Bestandsgeschützte Spezifikation: Industrial Signature Interoperability and Mailtrust Specification (ISIS-MTT)

ISIS-MTT KANN weiterhin für Bestandssysteme verwendet werden.

8.6 Austauschformate für Bilder

Bildformate für den Austausch von Geodaten befinden sich im Abschnitt 8.7.3 „Geodatenaustausch“.

Verbindliche Spezifikation: Joint Photographic Experts Group (JPEG)

JPEG MUSS für die Speicherung und den Austausch von Fotos und Grafiken mit Farbverläufen, bei denen die verlustbehaftete Kompression dieses Formates unschädlich ist, verwendet werden. JPEG-Dateien bieten für derartige Bilder eine hohe Kompressionsrate.

Empfohlene Spezifikation: Portable Network Graphics (PNG)

PNG SOLLTE für den Austausch von gerasterten Grafiken und Schaubildern verwendet werden. Es ist ein Grafikformat, welches 16 Millionen Farben, verlustfreie Kompression, inkrementelle Anzeige der Grafik (erst Grobstruktur, bis Datei ganz übertragen ist) und das Erkennen beschädigter Dateien unterstützt. Transparenz kann mit Hilfe von Alpha-Kanälen erreicht werden.

Beobachtete Spezifikation: Scalable Vector Graphics (SVG)

SVG KANN insbesondere für Vektorgrafiken benutzt werden. Damit ist es möglich, Bilder in Webseiten einzubetten, die sich ohne Verpixelung auf beliebige Größen skalieren lassen.

Bestandsgeschützte Spezifikation: Graphics Interchange Format (GIF) v89a

GIF v89a KANN in Bestandssystemen als Austauschformat für nicht-fotografische Bilder, wie Strichzeichnungen, verwendet werden. Es ist jedoch nur für Bilder mit geringer Farbtiefe (256 Farben) geeignet.

8.7 Geoinformationen

Geodaten werden über Geodienste bereitgestellt, siehe Abschnitt 9.7 „Webbasierte Geodienste“.

8.7.1 Raumbezug der Geodaten

Verbindliche Spezifikation: ETRS89/UTM Zone 33N (EPSG 25833)

Als Lagebezugssystem MUSS das europäische System ETRS 89 mit UTM-Abbildung (33. UTM-Zone) verwendet werden.

Verbindliche Spezifikation: DHHN2016

Das DHHN2016 wurde am 30. Juni 2017 bundesweit eingeführt. Neu erhobene Geodaten SOLLEN im System DHHN2016 erfasst werden, vorhandene Geodaten SOLLEN in das DHHN2016 überführt werden. Zur Vermeidung von Verwechslungen MUSS stets die Bezeichnung „Höhen über NHN im DHHN2016“ beziehungsweise der EPSG-Code 7837 verwendet werden.

Bestandsgeschützte Spezifikation: DHHN92

Das DHHN92 wurde am 30. Juni 2017 durch das DHHN2016 abgelöst. Geodaten können im alten Höhensystem verbleiben, wenn sie lediglich Zustände in der Vergangenheit beschreiben. Zur Vermeidung von Verwechslungen MUSS stets die Bezeichnung „Höhen über NHN im DHHN92“ beziehungsweise der EPSG-Code 5783 verwendet werden.

8.7.2 Metadaten für Geoinformationen

Verbindliche Spezifikation: ISO 19115/19119

Metadaten für Geodaten und Geoanwendungen MÜSSEN entsprechend der ISO 19115 und Metadaten für Geodatendienste MÜSSEN entsprechend der ISO 19115 und 19119 bereitgestellt werden. Jede Bereitstellung von Geodaten für Dritte SOLLTE durch die gleichzeitige Abgabe der dazugehörigen Metadaten qualifiziert werden.

Verbindliche Implementation: CSW-GDI-BB

Metadatenbereitsteller von Geodaten, Geodatendiensten und Geoanwendungen, die noch in Verwendung stehen, MÜSSEN ihre Metadaten über das CSW-GDI-BB bereitstellen und veröffentlichen.

8.7.3 Geodatenaustausch

Für den Austausch von Geodaten zwischen Geoinformationssystemen MÜSSEN nachfolgende Datenformate primär für den lesenden und den schreibenden Zugriff mindestens unterstützt werden.

Verbindliche Spezifikation: Tagged Image File Format (TIFF) 5.0

Für den Austausch von Rasterdaten MUSS das TIFF Format 5.0 mit Georeferenzierungsdatei TFW verwendet werden. Die Rasterdatenkompression von farbigen Geodaten (8-Bit-Palette) MUSS im Format TIFF-LZW, die Rasterdatenkompression von schwarz/weißen Geodaten (1-Bit-Farbtiefe) MUSS im Format CCITT, Gruppe 4 vorgenommen werden.

Verbindliche Spezifikation: JPEG/JPEG2000

Für den Austausch von komprimierten beziehungsweise verlustbehafteten Rasterdaten MÜSSEN die Formate JPEG und JPEG2000 verwendet werden.

Die Georeferenzierung ist mittels Datei im JGW-Format (je JPEG-Datei) durchzuführen.

Verbindliche Spezifikation: NAS

Für den Austausch von Vektordaten in AFIS, ALKIS und ATKIS MUSS das Format NAS verwendet werden.

Empfohlene Spezifikation: GML

Für den Austausch anderer Vektordaten SOLLTE das Format „Geography Markup Language“ (GML) verwendet werden. GML ist in der ISO-Norm 19136 standardisiert.

Beobachtete Spezifikation: GeoPackage

Zum Transport größerer Datenmengen wird GeoPackage evaluiert.

Bestandsgeschützte Spezifikation: ESRI-Shape

Für den Austausch von Vektordaten KANN ESRI-Shape in Bestandssystemen vorerst weiterverwendet werden.

8.8 Datenkompression

Verbindliche Spezifikation: ZIP

Für die Komprimierung großer Dokumente beziehungsweise einer Vielzahl von kleineren, zusammengehörenden Dokumenten MUSS das Format ZIP verwendet werden.

8.9 Open-Government-Data

8.9.1 Metadaten für Open-Government-Data

Verbindliche Spezifikation: DCAT-AP.de

Metadaten für Open-Government-Data MÜSSEN entsprechend der DCAT-AP.de bereitgestellt werden. Jede Bereitstellung von Open-Government-Data für Dritte SOLLTE durch die gleichzeitige Abgabe der dazugehörigen Metadaten qualifiziert werden. Dabei MÜSSEN mindestens die Pflicht-Elemente angegeben werden.

Verbindliche Spezifikation: „Data Catalogue Application Profile“ deutsche Adaption (DCAT-AP.de) 1.1

Der „Data Catalogue Application Profile“ deutsche Adaption (DCAT-AP.de) 1.1[18] MUSS unterstützt werden.

8.9.2 Austausch der Metadaten für Open-Government-Data

Verbindliche Spezifikation: Resource Description Framework (RDF) 1.1

Für den Austausch von OGD-Metadaten MUSS zumindest das RDF-Format (nach Resource Description Framework [RDF] 1.1[19]) unterstützt werden.

9 Kommunikation

9.1 Netzwerk

Verbindliche Spezifikation: Internet Protocol Version 4 (IPv4)/Version 6 (IPv6)

Für den Aufbau von Netzwerken MUSS TCP/IP (IPv4) verwendet werden.

Der ZIT-BB bereitet die Migration auf IPv6 vor. Bei neuen Beschaffungen MÜSSEN deswegen alle Komponenten IPv6-fähig sein.

[18] https://www.dcat-ap.de/def/

[19] https://www.w3.org/RDF/

Verbindliche Implementation: Landesverwaltungsnetz (LVN)

Die Vernetzung der Behörden MUSS mit dem LVN, welches eine Netzverschlüsselung beinhaltet, realisiert werden.

Für die Anbindung externer Netze MÜSSEN die durch den ZIT-BB bereitgestellten Gateways genutzt werden.

Verbindliche Implementation: Netzzugang des ZIT-BB vom Internet

Für den Netzzugang vom Internet MUSS der vom ZIT-BB angebotene Terminalserver-Zugang genutzt werden.

Bestandsgeschützte Implementation: VPN-Zugang des ZIT-BB vom Internet

Der Status dieses Standards wechselt am 30. Juni 2022 auf „verworfen". Danach wird für den Netzzugang vom Internet durch die IT-Leitstelle geprüft, ob eine Migration zur vom ZIT-BB angebotenen Terminalserver-Lösung möglich ist oder die Ausnahmegenehmigung zu verlängern wäre.

Verbindliche Spezifikation: Domain Name System (DNS)

DNS MUSS für die Namensauflösung in IP-Adressen („forward lookup") und die umgekehrte Auflösung von IP-Adressen in Namen („reverse lookup") verwendet werden.

Verworfene Spezifikation: Windows Internet Naming Service (WINS)

Windows Internet Naming Service SOLLTE nicht mehr eingesetzt werden.

9.2 Firewall

Der Zugang vom Kernnetz der Landesverwaltung (alle vom ZIT-BB betriebenen IP-Netze) zu Fremdnetzen MUSS über Firewall-Technik abgesichert werden. Die Unterscheidung der Fremdnetze erfolgt nach Benutzergruppen. Die Absicherung erfolgt dann durch Firewall-Technik mit steigender Sicherheitswirkung. Näheres regelt eine landesweite Sicherheitsrichtlinie.

Werden in Sicherheitsdomänen Daten mit hohem oder sehr hohem Schutzbedarf nach den landeseinheitlichen Schutzbedarfskategorien verarbeitet, MUSS eine separate Firewall eingesetzt werden.

9.3 Virenschutz

Der Virenschutz MUSS über Schutzprogramme erfolgen. Um eine umfassende Virenschutzvorsorge zu erreichen, MÜSSEN die Programme zum Virenschutz sowohl zentral als auch dezentral installiert sein. Zentraler Virenschutz wird im Auftrag seiner Kunden durch den ZIT-BB realisiert.

Näheres regelt eine Sicherheitsrichtlinie.

9.4 E-Mail

Für E-Mail-Anlagen sind die Dokumentenaustauschformate (siehe Abschnitt Austauschformate für Dokumente) einzuhalten. E-Mail-Inhalte MÜSSEN im Format „nur Text" oder „HTML" verfasst und verschickt werden. Bei der Einstellung „HTML" sind Clients und Server so zu konfigurieren, dass die E-Mail als Mime-Type Multipart/Alternative verwendet und somit die Nachricht sowohl als HTML als auch als Text verschickt wird.

Der ZIT-BB betreibt hierfür einen zentralen Exchange-Cluster. Diese Mailboxen werden dabei zentral im ZIT-BB gehostet. Behörden und Einrichtungen der Justiz, die nicht an den ZIT-BB überführt werden, sowie Behörden und Einrichtungen der Polizei, die im getrennten Netz arbeiten, sind von dieser Regelung ausgenommen.

Verbindliche Spezifikation: Multipurpose Internet Mail Extensions (MIME) 1.0

E-Mail-Clients und -Server MÜSSEN den Standard MIME einhalten.

Verbindliche Spezifikation: Simple Mail Transfer Protocol (SMTP)

Zum Senden von E-Mails MÜSSEN IT-Systeme eingesetzt werden, die den Standard SMTP unterstützen.

Verbindliche Spezifikation: MAPI over HTTP

Zur Kommunikation zwischen Outlook und Exchange ab Ver-sion 2016 MUSS MAPI over HTTP eingesetzt werden.

Bestandsgeschützte Spezifikation: Post Office Protocol, Version 3 (POP3)/Internet Message Access Protocol, Version 4rev1 (IMAP4rev1)

Zum Empfangen von E-Mails SOLLTEN Clients eingesetzt werden, die POP3 oder IMAP unterstützen. E-Mail-Server SOLLTEN POP3 und IMAP zur Verfügung stellen. Dies kann nur innerhalb des LVN verwendet werden.

Empfohlene Spezifikation: SMIME/X.509

Falls im bilateralen E-Mail-Verkehr mit Stellen innerhalb und außerhalb der Landesverwaltung die Verschlüsselung der übertragenen Daten mit hohem oder sehr hohem Schutzbedarf bezüglich der Grundbedrohung Vertraulichkeit (entsprechend den landeseinheitlichen Schutzbedarfskategorien) im Einzelfall geboten ist und eine ausreichende Verschlüsselung nicht über die austauschenden Systeme hergestellt werden kann, SOLLTEN SMIME-Implementierungen, die Zertifikate (X.509) unterstützen, genutzt werden.

Dabei SOLLTE pro Ressort mindestens eine Lösung zur verschlüsselten Kommunikation mit Externen (Bürger, Wirtschaft und Verwaltung) angeboten werden.

9.5 Anwendungsprotokolle

Empfohlene Spezifikation: Transport Layer Security (TLS) 1.2 oder Transport Layer Security (TLS) 1.3

Falls die Datenübertragung in Weitverkehrsnetzen auf Anwendungsebene abzusichern ist, sind TLS beziehungsweise SSH empfohlen. SSLv3 DARF NICHT mehr verwendet werden.

Empfohlene Spezifikation: Secure Shell, Version 2 (SSH-2)

Verworfene Spezifikation: Transport Layer Security (TLS) 1.0/1.1

9.6 Verzeichnisdienste

Verbindliche Spezifikation: Lightweight Directory Access Protocol, Version 3 (LDAPv3)

Neuimplementierungen von Verzeichniszugriffen via LDAP SOLLTEN ausschließlich mit der gesicherten Version LDAPS erfolgen.

Sollte in Ausnahmefällen die dezentrale Einrichtung eines Verzeichnisdienstes erforderlich sein, MUSS dieser das Lightweight Directory Access Protocol (LDAP) Version 3 unterstützen und an den zentralen Verzeichnisdienst (MetaDIR) und das zentrale Adressbuch (Microsoft Active Directory) anschlussfähig sein.

Bestandsgeschützte Implementation: MetaDIR

Der ZIT-BB stellt einen einheitlichen übergeordneten Verzeichnisdienst MetaDIR bereit, der als zentraler Verzeichnisdienst eingesetzt werden MUSS.

Verbindliche Implementation: Active Directory des ZIT-BB

Der ZIT-BB stellt den Active Directory Domain Services (Active-Directory-Domain-Verzeichnisdienst, ADDS) bereit, der für die MS Windows Domain- und Ressourcenverwaltung eingesetzt werden MUSS. Behörden und Einrichtungen der Justiz, die nicht an den ZIT-BB überführt werden, sind von dieser Regelung ausgenommen.

Bestandsgeschützte Implementation: PeRLa

Der ZIT-BB betreibt für die webbasierte Suche ein zentrales Verzeichnis der Personen und Ressourcen der Landesverwaltung (PeRLa)[20] in BB.intern, der in den Projekten eingesetzt werden KANN.

9.7 Webbasierte Geodienste

9.7.1 Koordinatensysteme und Projektionen

Verbindliche Spezifikation: WGS84 (EPSG 4326)/ETRS89 (EPSG 4258)

GDI-DE-konforme webbasierte Geodienste MÜSSEN die geografischen Koordinatenreferenzsysteme EPSG 4326 und EPSG 4258 unterstützen.[21]

Verbindliche Spezifikation: ETRS89/UTM Zone 33N (EPSG 25833)

GDI-BB-konforme webbasierte Geodienste MÜSSEN die Projektion EPSG 25833 unterstützen.

9.7.2 Darstellungsdienste

Verbindliche Spezifikation: OGC-WMS 1.3

GDI-DE-konforme Web Map Services (WMS) MÜSSEN mindestens folgende Schnittstellen unterstützen[22]:

- OGC-WMS Version 1.3.0, OpenGIS® Web Map Service Implementation Specification

Beobachtete Spezifikation: Vorgaben der GDI-DE zur Bereitstellung von Darstellungsdiensten

Die Vorgaben der GDI-DE zur Bereitstellung von Darstellungsdiensten lösen die veraltete WMS-DE-Profil Version 1.0 ab.

Verbindliche Spezifikation: ETRS89/LCC (EPSG 3034)/ETRS89/LAEA (EPSG 3035)/ETRS89/TM32 (EPSG 3044)/ETRS89/TM33 (EPSG 3045)/ETRS89/UTM Zone 32N (EPSG 25832)

GDI-DE-konforme webbasierte Web Map Services (WMS) MÜSSEN zusätzlich zu den Standards in Abschnitt 9.7.1 alle genannten Projektionen unterstützen.

[20] PeRLa ist unter http://perla.lvnbb.de im Landesverwaltungsnetz zu erreichen.

[21] Siehe Architektur der Geodateninfrastruktur Deutschland - Technik Version 3.4.1, https://www.gdi-de.org/sites/default/files/2020-03/AK_Architektur_GDI-DE_Technik_V_3_4_1_0.pdf

[22] Siehe Architektur der Geodateninfrastruktur Deutschland - Technik Version 3.4.1, https://www.gdi-de.org/sites/default/files/2020-03/AK_Architektur_GDI-DE_Technik_V_3_4_1_0.pdf

Verbindliche Spezifikation: Technical Guidance/Handlungsempfehlungen

INSPIRE konforme Darstellungsdienste MÜSSEN folgende Anforderungen erfüllen:

- Technical Guidance for the implementation of INSPIRE View Services[23]
- Verordnung zu INSPIRE Netzdiensten[24]
- Handlungsempfehlungen der GDI-DE für die Bereitstellung INSPIRE konformer Darstellungsdienste[25]

9.7.3 Downloaddienste

Verbindliche Spezifikation: OGC-WFS Version/2.0

GDI DE-konforme Web Feature Services (WFS) MÜSSEN die folgende Schnittstelle unterstützen[26]:

- OGC-WFS Version 2.0, OpenGIS® Web Feature Service Implementation Specification

Gazetteer-Services (WFS-G) MÜSSEN nach einem der folgenden Standards implementiert sein:

- OGC-WFS Version 2.0, OpenGIS® Web Feature Service Implementation Specification

Für WFS und WFS-G KANN zusätzlich folgende Schnittstelle unterstützt werden[27]:

- OGC-WFS Version 1.1.0, OpenGIS® Web Feature Service Implementation Specification

Verbindliche Spezifikation: Technical Guidance/Handlungsempfehlungen

INSPIRE konforme Downloaddienste MÜSSEN folgende Anforderungen erfüllen:

- Technical Guidance for the implementation of INSPIRE Download Services[28]
- Verordnung zu INSPIRE Netzdiensten[29]
- Handlungsempfehlungen der GDI DE für die Bereitstellung INSPIRE konformer Downloaddienste[30]

Empfohlene Spezifikation: OGC-WCS Version 2.0.1

Für Anwendungen von Web Coverage Service innerhalb der GDI DE SOLL die Version 2.0.1 verwendet werden.

Empfohlene Spezifikation: ETRS89/UTM Zone 32N (EPSG 25832)

Für Anwendungen von Downloaddiensten innerhalb der GDI DE SOLLTE das Koordinatenreferenzsystem EPSG: 25832 (UTM Zone 32N) unterstützt werden.

---

23 Siehe Technical Guidance for the implementation of INSPIRE View Services
http://inspire.ec.europa.eu/documents/Network_Services/Technical_Guidance_ViewServices_v3.11.pdf

24 Siehe Verordnung (EG) 976/2009 hinsichtlich der Netzdienste
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009R0976&from=EN

25 Siehe Handlungsempfehlungen für die Bereitstellung von INSPIRE konformen Darstellungsdiensten (INSPIRE View Services)
https://www.gdi-de.org/sites/default/files/2020-03/Handlungsempfehlungen_INSPIRE_Darstellungsdienste.pdf

26 Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.1.4
https://www.gdi-de.org/sites/default/files/2020-03/AK_Architektur_GDI-DE_Technik_V_3_4_1_0.pdf

27 Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.1.4
https://www.gdi-de.org/sites/default/files/2020-03/AK_Architektur_GDI-DE_Technik_V_3_4_1_0.pdf

28 Siehe Technical Guidance for the implementation of INSPIRE Download Services
http://inspire.ec.europa.eu/documents/Network_Services/Technical_Guidance_Download_Services_v3.1.pdf

29 Siehe Verordnung (EU) Nr. 1088/2010 zur Änderung der Verordnung (EG) 976/2009 hinsichtlich Downloaddiensten und Transformationsdiensten
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:323:0001:0010:DE:PDF

30 Siehe Handlungsempfehlungen für die Bereitstellung von INSPIRE konformen Downloaddiensten (INSPIRE Download Services)
https://www.gdi-de.org/sites/default/files/2020-03/Handlungsempfehlungen_AK_Geodienste_Inspire_Downloadservices1_3_0.pdf

Beobachtete Spezifikation: OGC API - Features als Schnittstellen für den Zugriff auf Vektordaten

Beobachtete Spezifikation: Downloaddienste für vordefinierte Datensätze auf Basis von ATOM (The Atom Syndication Format, RFC 4287, IETF 200)

9.7.4 Suchdienste

Verbindliche Spezifikation: OpenGIS Catalogue Services Specification 2.0.2 - ISO Metadata Application Profile 1.0

GDI-DE-konforme Web Catalog Service (CSW) MÜSSEN folgende Schnittstelle unterstützen:

- OGC-CSW OpenGIS® Catalog Service Specification 2.0.2 - ISO Metadata Application Profile, Version 1.0[31]

Verbindliche Spezifikation: Technical Guidance/Handlungsempfehlungen

INSPIRE konforme Suchdienste MÜSSEN folgende Anforderungen erfüllen:

- Technical Guidance for the implementation of INSPIRE Discovery Services[32]
- Verordnung zu INSPIRE Netzdiensten[33]

9.7.5 Sonstige Geodienste

Empfohlene Spezifikation: Architekturkonzept der GDI-DE, Version 3.4.1 - Technik, Kapitel 6

Für sonstige Geodienste SOLLTEN die Spezifikationen gemäß Architekturkonzept der GDI-DE, Version 3.4.1 eingehalten werden.[34]

9.7.6 Veröffentlichung der webbasierten Geodienste

Verbindliche Implementation: Geoportal Brandenburg

GDI-BB-konforme webbasierte Geodienste MÜSSEN im Geo-portal Brandenburg über eine automatisierte Verknüpfung der Metadaten mit dem Geoportal veröffentlicht werden.

Verbindliche Spezifikation: Webbasierte Geobasisdienste der LGB

Bei einer Veröffentlichung der Fachdaten über webbasierte Geodienste in Geoanwendungen MÜSSEN als Basiskarten (Kartengrundlage) die Geobasisdienste[35] der LGB verwendet werden.

10 Backend

Mit Hinblick auf die Konsolidierung des Backends im ZIT-BB und die Zielstellung der Überleitung MÜSSEN alle Entscheidungen zum Backend gemeinsam mit dem ZIT-BB erfolgen.

---

31 Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.4.1 https://www.gdi-de.org/sites/default/files/2020-03/AK_Architektur_GDI-DE_Technik_V_3_4_1_0.pdf

32 Siehe Technical Guidance for the implementation of INSPIRE Discovery Services http://inspire.ec.europa.eu/documents/Network_Services/TechnicalGuidance_DiscoveryServices_v3.1.pdf

33 Siehe Verordnung (EG) 976/2009 hinsichtlich der Netzdienste http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009R0976&from=EN

34 Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.4.1 https://www.gdi-de.org/sites/default/files/2020-03/AK_Architektur_GDI-DE_Technik_V_3_4_1_0.pdf

35 https://geobasis-bb.de/lgb/de/geodaten/

11 Verschlüsselung/Elektronische Signatur

Für spezielle Anwendungsfälle siehe auch Abschnitt 8.5.4 „Gesicherter Dokumentenaustausch“, Abschnitt 9.1 „Netzwerk“, Abschnitt 9.4 „E-Mail“ und Abschnitt 9.5 „Anwendungsprotokolle“.

Die Übertragung verschlüsselter Daten MUSS mittels Verfahren hergestellt werden, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als sicher eingestufte Methoden und Schlüssellängen verwenden.

Für geschlossene Nutzergruppen KÖNNEN Sicherheitsmechanismen zum Einsatz kommen, die individuellen Sicherheitskonzepten genügen.

Bei der landesinternen Datenübermittlung im Weitverkehrsbereich (zum Beispiel LVN) MÜSSEN Daten normalen Schutzbedarfs bezüglich der Grundbedrohung Vertraulichkeit (entsprechend den landeseinheitlichen Schutzbedarfskategorien) mit einer Netzverschlüsselung (das heißt Verschlüsselung am Ausgangspunkt des lokalen Quellnetzes zum Eingangspunkt des lokalen Zielnetzes) verschlüsselt werden.

Bei der Datenübermittlung im Internet in E-Government Verfahren zwischen Bürgern und Verwaltung sowie Wirtschaft und Verwaltung MÜSSEN Daten normalen Schutzbedarfs bezüglich der Grundbedrohung Vertraulichkeit (entsprechend den landeseinheitlichen Schutzbedarfskategorien) mit einer Leitungsverschlüsselung (siehe Abschnitt 9.5 „Anwendungsprotokolle“) versehen werden.

Bei Daten mit hohem oder sehr hohem Schutzbedarf bezüglich der Grundbedrohung Vertraulichkeit und Integrität (entsprechend den landeseinheitlichen Schutzbedarfskategorien) MUSS eine Ende-zu-Ende-Verschlüsselung vorgesehen werden. Ausgenommen davon sind nur die Verfahren, deren Risikoanalyse ergeben hat, dass eine Ende-zu-Ende-Verschlüsselung entbehrlich ist.

Verbindliche Spezifikation: Kryptoalgorithmen nach Bundesnetzagentur für die elektronische Signatur gemäß eIDAS VO

Bei der Auswahl der Algorithmen und zugehörigen Parameter zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen MUSS der Kryptokatalog gemäß des Beschlusses der eIDAS-Expert Group SOG-IS in der jeweils aktuellen Version angewendet werden.[36]

Verbindliche Implementation: PKI-1-Verwaltung

Für den Austausch von Daten mit hohem oder sehr hohem Schutzbedarf zwischen Behörden der öffentlichen Verwaltung MUSS die Public-Key-Infrastruktur für die öffentliche Verwaltung (PKI-1-Verwaltung) genutzt werden.

Für elektronische Signaturen, die nicht rechtlichen Ansprüchen genügen müssen und vor allem zur sicheren Authentifizierung des Absenders dienen, MÜSSEN Zertifikate der PKI-1-Verwaltung genutzt werden.

Verbindliche Spezifikation: Vertrauensdienstegesetz

Für qualifizierte Signaturen MÜSSEN qualifizierte Signaturzertifikate auf multifunktionalen Signaturkarten entsprechend des Vertrauensdienstegesetzes (früher Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) und Verordnung zur elektronischen Signatur (SigV) zur rechtssicheren Signatur) verwendet werden.

Beobachtete Spezifikation: Online-Ausweisfunktion des neuen Personalausweises (eID)

Zum sicheren Identitätsnachweis KANN die Online-Ausweisfunktion des neuen Personalausweises (eID) entsprechend Personalausweis-Gesetz beim Ausfüllen von Formularen erfolgen.

Beobachtete Spezifikation: De-Mail

Alternativ KANN auch ein Dokument per De-Mail übermittelt werden. Die Übermittlung MUSS dann nach den Vorschriften des De-Mail-Gesetzes erfolgen und das De-Mail Namenskonzept des Landes Brandenburg[37] berücksichtigen.

---

[36] Version 1.2, Januar 2020: https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

[37] Nur im Intranet der Landesverwaltung: http://www.lvnbb.de/media_fast/2134/De-Mail_Namenskonzept_des_Landes_Brandenburg.pdf

12 Chipkarten

Für die Erstellung der notwendigen Zertifikate für Authentisierungs- und Signaturzwecke SOLLTE der ZIT-BB als Registrierungsstelle genutzt werden.

12.1 Kontaktbehaftete Chipkarten

Verbindliche Spezifikation: Electrically Erasable Programmable Read-Only Memory (EEPROM)

Für kontaktbehaftete Chipkarten für Identitätsprüfungen MUSS als Mindestvoraussetzung ein Chip in EEPROM-Technologie mit einer Speicherkapazität von mindestens 16 Kilobyte sowie einfacher Sicherheitslogik (PIN) verwendet werden.

Verbindliche Spezifikation: Identification Cards - Integrated circuit cards (ISO 7816)

Der Chip MUSS der ISO-Norm 7816-3 für den Befehlssatz und die Übertragungsprotokolle und ISO 7816-2 für die Belegung der Kontakte entsprechen.

Bei Einsatz von Chipkarten für zertifikatsbasierte Authentisierung und Signatur MUSS gesichert sein, dass Kryptoalgorithmen in diesen Fällen auf der Karte selbst ausgeführt werden.

Verbindliche Spezifikation: ISO 8824/ISO 8825

Der Chip MUSS den ISO-Normen 8824 und 8825 für die Zeichenkodierung entsprechen.

12.2 Kontaktlose Chipkarten

Beobachtete Spezifikation: Identification Cards - Contactless integrated circuit cards

Die physikalischen und elektrischen Eigenschaften sowie die von kontaktlosen Smartcards verwendeten Protokolle werden in der Norm ISO 14443 spezifiziert. Solche Smartcards kommen bei Identifikationssystemen, Zugangskontrollen und Bezahlsystemen zum Einsatz.

12.3 Schnittstellen für Chipkarten

Verbindliche Spezifikation: Microsoft Cryptography API (MS-CryptoAPI)/Public Key Cryptography Standard #11 (PKCS#11)

Als Schnittstelle zur Applikation MUSS zusätzlich zur Kommunikation mittels kartenspezifischer Befehle eine Unterstützung von Cryptographic Service Provider (CSP), einer Implementation der Microsoft Cryptography API (MS-CryptoAPI) oder von PKCS#11 vorgesehen werden.

13 Archivierung

Zur Gewährleistung einer nachhaltigen Aufbewahrung elektronischer Dokumente im Sinne von Vertrauenswürdigkeit und Sicherung des Beweiswertes in öffentlichen Verwaltungen sind Formate zu verwenden, die mit dem Brandenburgischen Landeshauptarchiv (BLHA) abzustimmen sind (§ 4 Absatz 7 Brandenburgisches Archivgesetz - BbgArchivG).

Das BLHA legt fest, welche Formate die Authentizität und Integrität der Objekte gewährleistet und informiert rechtzeitig, wenn Formate obsolet geworden sind beziehungsweise Migrationen auf neue Formate erforderlich sind.

14 Migrationen

Verbindliche Spezifikation: Migrationsleitfaden

Für Weiterentwicklungen der IT-Infrastruktur beziehungsweise bei geplanten Migrationen MUSS der „Migrationsleitfaden - Leitfaden für die Migration von Software“ der Beauftragten der Bundesregierung für Informationstechnik (aktuell: Version 4.0 vom März 2012)[38] beachtet werden.

Ferner MUSS das BLHA immer dann über geplante Migrationen rechtzeitig informiert werden, wenn Daten aus den betroffenen Fachverfahren der Anbietungspflicht unterliegen.

A E-Government Basiskomponenten

A.1 Basiskomponenten gemäß § 11 BbgEGovG

Verbindliche Implementation: Basiskomponenten gemäß § 11 BbgEGovG

Die im Gesetz über die elektronische Verwaltung im Land Brandenburg (Brandenburgisches E-Government-Gesetz - BbgEGovG) unter § 11 aufgeführten IT-Basiskomponenten sind gemäß der im Gesetz definierten Verpflichtungen einzusetzen.[39]

Zur Stärkung des vom IT-Planungsrat beschlossenen Nachnutzungsmodells ‚Einer für Alle‘ (EfA-Prinzip) zur Umsetzung des Onlinezugangsgesetzes beziehungsweise Entwicklung entsprechender IT-Basiskomponenten SOLLTE auf die Verwendung von Open Source-Lizenzen für im Land zu entwickelnde Software geachtet werden.

A.2 Content Management System

Verbindliche Implementation: SixCMS

Als Content Management System MUSS für den Webauftritt des Landes Brandenburg[40] landeseinheitlich SixCMS eingesetzt werden.

Empfohlene Implementation: MAIS 2.0

Als Mandantenanwendung SOLL für den Webauftritt des Landes Brandenburg[41] landeseinheitlich MAIS 2.0 eingesetzt werden.

Für hauseigene Webauftritte SOLL MAIS 2.0 Intranet verwendet werden.

A.3 Webkartenkomponente

Empfohlene Implementation: Kartennavigator BRANDENBURGVIEWER-API

Die Darstellung der webbasierten Geodienste in den Internetportalen der Landesverwaltung SOLLTE mit dem Darstellungswerkzeug (BRANDENBURGVIEWER-API) erfolgen.

Empfohlene Implementation: Kartenviewer-API

Die Kartenviewer-API löst zukünftig die BRANDENBURGVIEWER-API ab.

---

38 http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/migrationsleitfaden_4_0_download.pdf?__blob=publicationFile

39 Für die Vergabe von öffentlichen Aufträgen ist die webbasierte Lösung Vergabemarktplatz Brandenburg zu nutzen. https://bravors.brandenburg.de/verwaltungsvorschriften/vergabe2016

40 brandenburg.de sowie BB.intern

41 brandenburg.de sowie BB.intern

Nach der produktiven Bereitstellung dieser Schnittstelle SOLLTE die Darstellung der webbasierten Geodienste in den Internetportalen der Landesverwaltung mit dem Darstellungswerkzeug Kartenviewer-API erfolgen.

Beobachtete Implementierung: ArcGIS Enterprise - im Speziellen hier Portal for ArcGIS

B IT-Querschnittsverfahren

B.1 Personal- und Stellenverwaltung

Verbindliche Implementation: Landesbasislösung PerIS

Für die Personal- und Stellenverwaltung in der Landesverwaltung MUSS mit Ausnahme der Schulverwaltung die vom ZIT-BB betriebene landesweite einheitliche Landesbasislösung PerIS genutzt werden.

B.2 Haushalts-Kassen-Rechnungswesen (HKR) und Kosten- und Leistungsrechnung (KLR)

Verbindliche Implementation: SAP

Für das neue Finanzmanagement (insbesondere Haushalts-Kassen-Rechnungswesen, Kosten- und Leistungsrechnung und Anlagenbuchhaltung) MUSS in den Behörden und Einrichtungen der Landesverwaltung SAP eingesetzt werden.

B.3 Haushaltsaufstellungsverfahren

Verbindliche Implementation: HAVWeb

Als Produkt für die Haushaltsaufstellung MUSS HAVWeb eingesetzt werden.

B.4 Reisekostenrechnung

Verbindliche Implementation: PTravel Web

Für die zentrale Reisekostenabrechnung in der Zentralen Bezügestelle (ZBB) MUSS PTravel Web (ehemals Reiko) als Intranet-Lösung verwendet werden.

Bestandsgeschützte Implementation: SMS Reise

Für die dezentrale Reisekostenrechnung KANN die Software SMS Reise eingesetzt werden.

B.5 Wirtschaftlichkeitsberechnungen

Empfohlene Implementation: WiBe Kalkulator 1.3

Für Wirtschaftlichkeitsberechnungen SOLLTE das vom Bund kostenlos zur Verfügung gestellte Programm WiBe Kalkulator 1.3 eingesetzt werden.

Für den Kriterienkatalog zu Wirtschaftlichkeitsberechnungen siehe Abschnitt 2.2 „Wirtschaftlichkeitsbetrachtungen“.

B.6 Webbasierte Kommunikations- und Dokumentenplattform

Verbindliche Implementation: DialogBB

Als webbasierte Kommunikations- und Dokumentenplattform ist DialogBB zu nutzen.

Beobachtete Implementation: Microsoft SharePoint

Für die Integration von MS-Office und MS-SQL-Anwendungen auf eine webbasierte Plattform KANN Microsoft SharePoint eingesetzt werden.

B.7 Vorschriftensystem

Verbindliche Implementation: BRAVORS

Zur Sammlung, Veröffentlichung und Recherche aller im Land Brandenburg erlassenen und gültigen Gesetze, Rechtsverordnungen und Verwaltungsvorschriften (inklusive ihrer Genese) MUSS die webbasierte Lösung BRAVORS eingesetzt werden. BRAVORS wird vom ZIT-BB im LVN bereitgestellt.[42]

B.8 Vorgangsbearbeitung und Aktenhaltung

Die Vorgangsbearbeitung und Aktenhaltung MUSS am „Organisationskonzept elektronische Verwaltungsarbeit“[43] ausgerichtet werden.

Verbindliche Implementation: EL.DOK-BB

Für die elektronische Vorgangsbearbeitung und/oder Aktenhaltung, soweit sie nicht durch spezifische Fachverfahren abgedeckt wird beziehungsweise Vorgaben durch Fachverfahren bestehen, MUSS das vom ZIT-BB betriebene landesweit einheitliche System EL.DOK-BB genutzt werden.

Bestandsgeschützte Implementation: VIS

Für die Bereiche gemäß den Ausnahmeregelungen in KV 734/08 DARF VIS eingesetzt werden.

Die Ausnahmen gemäß KV 734/08 bleiben hiervon unberührt.

B.9 Kabinettinformationssystem

Verbindliche Implementation: EL.KIS

EL.KIS als Mandant von EL.DOK-BB MUSS zur Vor- und Nachbereitung sowie Dokumentation von Kabinettsitzungen genutzt werden.

B.10 Elektronische Normenverkündung

Verbindliche Implementation: EL.Norm

Zur elektronischen Ausfertigung von Gesetzen und Verordnungen sowie deren Verkündung in dem elektronischen Gesetz- und Verordnungsblatt für Brandenburg MUSS landesweit EL.Norm eingesetzt werden.

Verbindliche Implementation: eNorm

Zur Einhaltung rechtsförmlicher und redaktioneller Vorgaben während der schriftlichen Erarbeitung von Gesetz- und Verordnungsentwürfen in der Landesverwaltung sowie der elektronischen Normenverkündung MUSS landesweit eNorm eingesetzt werden.

[42] BRAVORS ist im Landesverwaltungsnetz unter http://bravors.lvnbb.de/ und im Internet unter http://www.landesrecht.brandenburg.de/ zu erreichen.

[43] https://www.verwaltung-innovativ.de/DE/Verwaltungsdigitalisierung/orgkonzept_everwaltung/orgkonzept_everwaltung_artikel.html;jsessionid=18BC158502D92E38D8AB20E03867E487.1_cid340

B.11 Stellenportal im Internet

Beobachtete Implementation: Interamt

INTERAMT ist ein Stellenportal im Internet für den öffentlichen Dienst, das bereits bei mehreren Ministerien eingeführt ist beziehungsweise eingeführt werden SOLLTE. Sollte eine Behörde den Einsatz eines Stellenportals prüfen, SOLLTE der Kontakt mit diesem Projekt aufgenommen werden.

Empfohlene Implementation: Karriereportal der Landesverwaltung

Stellenangebote und Ausbildungsplätze SOLLTEN - mit Ausnahme der Angebote von Referendarplätzen für Lehrkräfte und Juristen - in der Stellenbörse im Karriereportal der Landesverwaltung Brandenburg veröffentlicht werden. Dafür ist die Eingabeplattform im LVN mit SixCMS zu nutzen.

B.12 Monitoring

Beobachtete Implementation: checkmk ab Version 1.5.0p25

Das Monitoring-System checkmk SOLLTE entweder in der RAW (OpenSource) oder Enterprise-Edition (Subskription) eingesetzt werden. Für die Spezifikation: Monitoring-Server mit einem Agent-basierten Zugriff ohne SNMP.

B.13 Wissensmanagement

Beobachtete Implementation: BlueSpice MediaWiki 3.10

BlueSpice MediaWiki KANN in der kostenlosen oder Pro-Version eingesetzt werden. Der Versionseinsatz richtet sich nach den erforderlichen Use Cases.

B.14 Projekt-Management Software

Empfohlene Implementation: MS-Project 2016

B.15 Telefonie

Verbindliche Implementierung: IP-Telefoniedienst des ZIT-BB

Der ZIT-BB betreibt eine zentrale IP-Telefonie-Lösung für die Landesverwaltung (siehe Servicekatalog 6.2). Diese MUSS bei der Neuinstallation oder dem Ersatz vorhandener Telefonie-Lösungen verwendet werden.

Die in der allgemeinen Verwaltungsvorschrift über die Einrichtung und Nutzung dienstlicher Telekommunikationsanlagen[44] genannten Ausnahmen greifen entsprechend.

B.16 Videokonferenzen

Verbindliche Implementation: Videokonferenzdienst des ZIT-BB

C Abkürzungsverzeichnis

BB	Brandenburg
BbgBITV	Brandenburgische Barrierefreie Informationstechnik-Verordnung
BGG	Behindertengleichstellungsgesetz
BIOS	Basic Input Output System
BLHA	Brandenburgisches Landeshauptarchiv
BRAVORS	Brandenburgisches Vorschriftensystem
BSI	Bundesamt für Sicherheit in der Informationstechnik
CSS	Cascading Style Sheets

[44] https://bravors.brandenburg.de/verwaltungsvorschriften/dav_2017#4

EEPROM	Electrically Erasable Programmable Read-Only Memory
ESR	Extended Support Release
GDI-DE	Geodateninfrastruktur Deutschland
GIF	Graphics Interchange Format
HTML	HyperText Markup Language
IMAG	Interministerielle Arbeitsgruppe
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IrDA	Infrared Data Association
ISIS	Industrial Signature Interoperability Specification
ISO	International Organization for Standardization
IT	Informationstechnologie
JPEG	Joint Photographic Experts Group
KoopA ADV	Kooperationsausschuss Automatisierte Datenverarbeitung Vorläuferorganisation des IT-Planungsrates
LDAP	Lightweight Directory Access Protocol
LVN	Landesverwaltungsnetz
MBAM	Microsoft BitLocker-Verwaltung und -Überwachung
MIME	Multipurpose Internet Mail Extensions
MTT	Mailtrust
OAIS	Open Archival Information System
OGC-WMS	OpenGIS® Web Map Service Interface Standard
OOXML	Office Open XML
OSCI	Online Service Computer Interface
OSS	Open Source Software
PAP	Paketfilter-Application Layer Gateway-Paketfilter
PDF	Portable Document Format
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
POP3	Post Office Protocol Version 3
RIO	Ressort Information Officer
SAGA	ein Eigenname (ursprünglich: Standards und Architekturen für eGovernment-Anwendungen)
SigG	Signaturgesetz
SSH	Secure Shell
SSL	Secure Sockets Layer
SVG	Scalable Vector Graphics
TCP	Transmission Control Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
ULA	Oracle Unlimited License Agreement
UML	Unified Modeling Language
USB	Universal Serial Bus
UTF	Unicode Transformation Formats
VPN	Virtual Private Network
VPS	Virtuelle Poststelle
W3C	World Wide Web Consortium
WiBe	Wirtschaftlichkeitsbetrachtung
Windows XP	Windows eXPerience
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language
XÖV	XML in der öffentlichen Verwaltung
XSLT	Extensible Stylesheet Language Transformations
ZIP	kurz für Zipper, Reißverschluss
ZIT-BB	Brandenburgischer IT-Dienstleister.