

**IT-Standards Land Brandenburg  
in der Fassung vom 5. Juni 2019**

Runderlass der Landesregierung  
Az.: 1793/04 vom 15. Juni 2004  
Fortschreibung durch den RIO-Ausschuss am 5. Juni 2019

Bekanntmachung des Ausschusses  
der Ressort Information Officer

**SAGA de.bb 5.3.0 Modul Standards**

**Inhaltsverzeichnis**

**1 Einleitung**

- 1.1 Anwendung des Klassifikationssystems

**2 Management-Methoden**

- 2.1 Projektmanagement
- 2.2 Wirtschaftlichkeitsbetrachtungen
- 2.3 Software- und Systemtests
- 2.4 Einführung, Betrieb sowie Außerbetriebnahme von IT-Verfahren

**3 Informationssicherheit**

- 3.1 Zertifizierte Produkte und Dienstleistungen

**4 Prozessmodelle**

**5 Datenmodelle**

**6 Backend-Architektur (Server)**

- 6.1 Server-Betriebssysteme
- 6.2 Datenbanksysteme
- 6.3 Cluster Suite
- 6.4 Hypervisor

**7 Client**

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

**8 Präsentation**

- 8.1 Barrierefreie Darstellung
- 8.2 Zeichensätze und -kodierungen
- 8.3 Informationsaufbereitung
- 8.4 Austauschformate für Daten
- 8.5 Austauschformate für Dokumente
  - 8.5.1 Dokumente zum Informationsaustausch
  - 8.5.2 Textdokumente zur Weiterbearbeitung
  - 8.5.3 Tabellendokumente zur Weiterbearbeitung
  - 8.5.4 Gesicherter Dokumentenaustausch
- 8.6 Austauschformate für Bilder
- 8.7 Geoinformationen
  - 8.7.1 Raumbezug der Geodaten

- 8.7.2 Metadaten für Geoinformationen
- 8.7.3 Geodaten austausch
- 8.8 Datenkompression

## **9 Kommunikation**

- 9.1 Netzwerk
- 9.2 Firewall
- 9.3 Virenschutz
- 9.4 E-Mail
- 9.5 Telefonie
- 9.6 Anwendungsprotokolle
- 9.7 Verzeichnisdienste
- 9.8 Webbasierte Geodienste
  - 9.8.1 Koordinatensysteme und Projektionen
  - 9.8.2 Darstellungsdienste
  - 9.8.3 Downloaddienste
  - 9.8.4 Suchdienste
  - 9.8.5 Sonstige Geodienste
  - 9.8.6 Veröffentlichung der webbasierten Geodienste

## **10 Backend**

## **11 Verschlüsselung/Elektronische Signatur**

## **12 Chipkarten**

- 12.1 Kontaktbehaftete Chipkarten
- 12.2 Kontaktlose Chipkarten
- 12.3 Schnittstellen für Chipkarten

## **13 Langzeitspeicherung**

- 13.1 [entfällt]
- 13.2 Langzeitspeicherung von Bildern
- 13.3 Langzeitspeicherung von Daten
- 13.4 Langzeitspeicherung von Dokumenten
- 13.5 Beweiswerterhaltung digital signierter Dokumente

## **14 Migrationen**

### **A E-Government Basiskomponenten**

- A.1 Content Management System
- A.2 Virtuelle Poststelle (VPS)
- A.3 Signaturkomponente
- A.4 Formularservice
- A.5 Portalservice
- A.6 Webkartenkomponente
- A.7 Multikanal-Zugang

### **B IT-Querschnittsverfahren**

- B.1 Personal- und Stellenverwaltung
- B.2 Haushalts-Kassen-Rechnungswesen (HKR) und Kosten- und Leistungsrechnung (KLR)
- B.3 Haushaltsaufstellungsverfahren
- B.4 Reisekostenrechnung
- B.5 Wirtschaftlichkeitsberechnungen
- B.6 Webbasierte Kommunikations- und Dokumentenplattform
- B.7 Vorschriftensystem
- B.8 Vorgangsbearbeitung und Aktenhaltung
- B.9 Kabinetttinformationssystem
- B.10 Elektronische Normenverkündung
- B.11 Stellenportal im Internet

### **C Abkürzungsverzeichnis**

## 1 Einleitung

SAGA<sup>1</sup> de.bb ist die Fortschreibung der IT-Standards des Landes Brandenburg entsprechend der IT-Standardisierungsrichtlinie<sup>2</sup>. 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<sup>3</sup>.

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<sup>4</sup> 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<sup>5</sup> 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“<sup>6</sup> 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<sup>7</sup> 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.

#### 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.

<sup>1</sup> SAGA ist ein Eigenname, der ursprünglich als Abkürzung von „Standards und Architekturen für eGovernment-Anwendungen“ eingeführt wurde.

<sup>2</sup> <http://bravors.brandenburg.de/de/verwaltungsvorschriften-221628>

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

<sup>4</sup> <http://www.bravors.brandenburg.de/>

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

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

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

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.

#### 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

Verworfen Standards **KÖNNEN** dann eingesetzt werden, wenn parallel eine SAGA-konforme Lösung zur Verfügung gestellt wird.<sup>8</sup> 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 Funktionsumfangs, 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** gemäß Nummer 4.2.5 der IT-Strategie<sup>9</sup> anhand einheitlicher Projektmanagementmethoden durchgeführt werden.

Empfohlene Spezifikation: Projektmanagementleitfaden

Als Methodik **SOLLTE** der Leitfaden Projektmanagement<sup>10</sup> 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<sup>11</sup> genutzt werden.

<sup>8</sup> 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.

<sup>9</sup> [http://bravors.brandenburg.de/br2/sixcms/media.php/66/Amtsblatt%2030\\_04%20%28S.%20567-581%29.pdf](http://bravors.brandenburg.de/br2/sixcms/media.php/66/Amtsblatt%2030_04%20%28S.%20567-581%29.pdf)

<sup>10</sup> Nur im Intranet der Landesverwaltung:  
[http://www.lvnbb.de/media\\_fast/2134/Leitfaden\\_Projektmanagement.pdf](http://www.lvnbb.de/media_fast/2134/Leitfaden_Projektmanagement.pdf)

<sup>11</sup> <http://www.cio.bund.de/wibe>

Für die Implementation siehe B.5 „Wirtschaftlichkeitsberechnungen“.

### 2.3 Software- und Systemtests

Beobachtete Spezifikation: IEEE 829

Im Bereich der Polizei werden Software- und Systemtests in länderübergreifenden Verbänden 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.

## 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<sup>12</sup> gewährleistet werden.

Verbindliche Spezifikation: BSI-Standard 200-1: Managementsysteme für Informationssicherheit

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

Verbindliche Spezifikation: BSI-Standard 200-3 Risikomanagement

Verbindliche Spezifikation: BSI-Standard 100-4: Notfallmanagement

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<sup>13</sup> erfolgen.

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

<sup>12</sup> Das BSI modernisiert zurzeit seine Dokumente zum IT-Grundschutz. Dadurch kann es zu kurzfristigen Änderungen kommen.

<sup>13</sup> Nur im Intranet der Landesverwaltung:  
[http://www.lvnbb.de/media\\_fast/2134/Anlage\\_2\\_Leitlinie%20zur%20Gew%C3%A4hrleistung%20der%20Informationssicherheit%20%28Inform....pdf](http://www.lvnbb.de/media_fast/2134/Anlage_2_Leitlinie%20zur%20Gew%C3%A4hrleistung%20der%20Informationssicherheit%20%28Inform....pdf)

<sup>14</sup> 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<sup>15</sup> durchgeführt werden.

Verbindliche Implementation: Elektronische Erstellung und Fortschreibung von Sicherheitskonzepten

Für die zentrale elektronische Erstellung und Fortschreibung von Sicherheitskonzepten MUSS die zentral bereitgestellte Lösung<sup>16</sup> genutzt werden. Behörden und Einrichtungen der Justiz, die nicht dem Kontrahierungszwang unterliegen, sind hiervon ausgenommen.

Länderübergreifende Verbände 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 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.

## 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 Implementierungen, welche im ZIT-BB eingesetzt werden, der Vorzug gegeben werden.

<sup>15</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden\\_IS-Revision-v2\\_pdf.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf)

<sup>16</sup> Derzeit das beim ZIT-BB betriebene Produkt Verinice

Die Server SOLLTEN mit dem jeweils aktuellen Servicepack und allen Sicherheits-Patches betrieben werden. Der ZIT-BB behält sich vor Systeme, die nicht auf dem neuesten Stand sind, in einer Quarantäne-Umgebung zu betreiben.

Empfohlene Implementation: Red Hat Enterprise Linux ab Version 6.10

Empfohlene Implementation: Suse Linux Enterprise Server ab Version 12.x

Empfohlene Implementation: Windows Server 2016

Bestandsgeschützte Implementation: Red Hat Enterprise Linux ab Version 6.x (bis 11/2020)

Der Status dieses Standards wechselt ab November 2020 auf „verworfen“.

Verworfen Implementation: Suse Linux Enterprise Server ab Version 11.x

Der Status dieses Standards ist seit März 2019 auf „verworfen“, da es kein Support mehr für diese Version gibt.

Bestandsgeschützte Implementation: Windows Server 2012 R2

Empfohlene Implementation: HP Unix Version 11.31

Bestandsgeschützte Implementation: HP Unix Version 11.11 und 11.23

Beobachtete Implementation: Windows Server 2019

## 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 allen Sicherheits-Patches betrieben werden.

Empfohlene Implementation: MySQL

Das Datenbanksystem MySQL SOLLTE entweder in den Versionen 5.6 oder 5.7 als Enterprise oder Community Edition (jeweils die neueste Stable Release) eingesetzt werden.

Empfohlene Implementation: Microsoft SQL (ab Version 2008)

Das Datenbanksystem Microsoft SQL Server SOLLTE entweder in den Versionen 2012, 2014 oder 2016 als Standard oder Enterprise Edition eingesetzt werden.

Unter Beobachtung: Microsoft SQL 2017

Bestandsgeschützte Implementation: Microsoft SQL Server 2008 R2

Der Status dieses Standards wechselt ab dem 9. Juli 2019 auf „verworfen“.

Empfohlene Implementation: Informix

Das Datenbanksystem Informix SOLLTE entweder in den Versionen 11.70 oder 12.10 als Workgroup oder Enterprise Version eingesetzt werden.

Empfohlene Implementation: Oracle Enterprise Edition

Das Datenbanksystem Oracle SOLLTE in der Version 12.2 Enterprise Edition eingesetzt werden.

Bestandsgeschützte Implementation: Oracle Database 12.1.x Enterprise Edition

Der Status dieses Standards wechselt ab dem 31. Juli 2019 auf „verworfen“.

Verworfen Implementation: Oracle Database 11.2.x Enterprise Edition

Seit dem Support-Ende von Oracle Database 11.2.x Enterprise Edition am 31. Dezember 2018 sollte diese Version nicht mehr eingesetzt werden.

Empfohlene Implementation: PostgreSQL

Das Datenbanksystem PostgreSQL SOLLTE in den Versionen 9.6 oder 10 eingesetzt werden.

Bestandsgeschützte Implementation: PostgreSQL 9.5

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

Bestandsgeschützte Implementation: PostgreSQL 9.4

Der Status dieses Standards wechselt ab Dezember 2019 auf „verworfen“.

### 6.3 Cluster Suite

Empfohlene Implementation: HP Serviceguard for Linux ab Version 12.20

Empfohlene Implementation: Microsoft Failover Cluster auf Basis Windows Server 2012 R2 (und höher)

Bestandsgeschützte Implementation: HP Serviceguard for Linux Version 11.20



Bestandsgeschützte Implementation: Red Hat Cluster Suite

#### 6.4 Hypervisor

Empfohlene Implementation: VMware vSphere ab Version 6.x (Enterprise)

Empfohlene Implementation: Microsoft Hyper-V ab Windows Server 2016

Empfohlene Implementation: Citrix XEN Server ab Version 7.1

Beobachtete Implementation: Citrix XEN Server Version 7.5

Bestandsgeschützte Implementation: Citrix XEN Server Version 6.2

### 7 Client

Der ZIT-BB betreibt die Clients gemäß Brandenburg Client 2.0. Diese Standards stellen eine Teilmenge des Standard-Clients dar.

#### 7.1 Client-Betriebssysteme

Der ZIT-BB prüft Alternativen zur Microsoft-Umgebung.

Verbindliche Implementation: Microsoft Windows 10

Bei Installationen neuer Fat-Clients MUSS als Betriebssystem Windows 10 64-bit Version 1803 eingesetzt werden. Die Clients MÜSSEN mit dem jeweils aktuellen Servicepack und allen Sicherheits-Patches betrieben werden.

Bestandsgeschützte Implementation: Thin-Clients vom ZIT-BB

Für den Betrieb von Thin-Clients MUSS die zentral bereitgestellte Lösung des ZIT-BB (siehe Servicekatalog Kapitel 5) genutzt werden.

Als Betriebssystem auf den Thin-Clients kommt IGLE 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 Arbeitsplätzen in der Landesverwaltung (mobile wie auch Fat-Clients) MÜSSEN mit Microsoft Bitlocker gegen den unberechtigten Zugriff verschlüsselt werden.

## 7.2 Web-Browser

Verbindliche Implementation: Internet Edge und Mozilla Firefox

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

Es MÜSSEN Microsoft Edge 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.

Bestandgeschützte Implementation: Internet Explorer auf Thin Clients

Aufgrund der fehlenden Implementation von Microsoft Edge auf Windows Server wird bei Thin Clients weiterhin Microsoft Internet Explorer Version 11 eingesetzt.

## 7.3 PDF-Reader

Verbindliche Implementation: Adobe Acrobat Reader DC

Zum Lesen von PDF-Dateien MUSS der Adobe Acrobat Reader DC in der aktuell verfügbaren und vom ZIT-BB freigegebenen Version installiert sein. Alle Sicherheits-Patches und Updates MÜSSEN installiert werden.

## 7.4 Büroanwendungen

Der ZIT-BB prüft Alternativen zur Microsoft-Umgebung.

Verbindliche Implementation: Microsoft Office 2016 Professional

Für die Büroanwendungen Textverarbeitung, Tabellenkalkulation, Präsentation und Grafik<sup>17</sup> MUSS das Software-Produkt Microsoft Office 2016 Professional eingesetzt werden.

Bestandgeschützte Implementation: Microsoft Office 2010

Der Status dieses Standards wechselt am 13. Oktober 2020 auf „verworfen“.

## 7.5 Groupware-Anwendung

Verbindliche Implementation: Microsoft Outlook 2016

<sup>17</sup> Grafiken in diesem Sinne sind 2D-Objekt-Grafiken, wie zum Beispiel Organigramme, Datagramme, Flussdiagramme, nicht jedoch Rastergrafiken wie Bilder oder Fotos beziehungsweise 3D-Grafiken (hierfür gibt es keine klassifizierte Implementation).

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

Beobachtete Implementation: Microsoft Outlook 2019

Der Einsatz von Outlook 2019 wird unter dem Blickwinkel der Ablösung von Windows 7 im ZIT-BB projiziert.

Bestandsgeschützte Implementation: Microsoft Outlook 2010

Der Status dieses Standards wechselt am 13. Oktober 2020 auf „verworfen“.

#### 7.6 Client-Datenbanken

Client-Datenbanken sollten nach Möglichkeit nicht zum Einsatz kommen. Wenn diese 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 eine Ressource zu speichern, die in eine zentrale Datensicherung eingebunden ist.

Bestandsgeschützte Implementation: Microsoft Access 2010

Der Status dieses Standards wechselt am 13. Oktober 2020 auf „verworfen“.

#### 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 (zum Beispiel durch Einrichtung von USB-Schleusen).

#### 7.8 Weitere Implementierungen beim Standard-Client

Diese Implementierungen 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 2.40

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 Manipulieren von Archivdateien aller Art MUSS an allen PC-Arbeitsplätzen das Programm 7-Zip eingesetzt werden.

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

## 8 Präsentation

### 8.1 Barrierefreie Darstellung

Verbindliche Spezifikation: Brandenburgische Barrierefreie Informationstechnik-Verordnung (BbgBITV)

Die BbgBITV<sup>18</sup> konkretisiert als Rechtsverordnung das Brandenburgische Behindertengleichstellungsgesetz (BbgBGG) in Bezug auf die Berücksichtigung von Barrierefreiheit in der Informationstechnik und beschreibt die technischen Anforderungen an Layout, Design und Benutzerführung, die zu erfüllen sind, wenn eine Website für alle Benutzer zugänglich gestaltet sein soll. Insbesondere die Gruppe der behinderten Menschen wird in dieser Verordnung berücksichtigt.

Die BbgBITV MUSS bei der Erstellung öffentlich zugänglicher Web-Seiten und IT-Systeme beachtet werden.

### 8.2 Zeichensätze und -kodierungen

Verbindliche Spezifikation: Unicode/UTF-8

Bei der Erstellung von Web-Seiten 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)

<sup>18</sup> <http://bravors.brandenburg.de/de/verordnungen-212053>

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

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<sup>19</sup> 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.

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 weitestgehend in einem formatgetreuen und inhaltlich unveränderbaren Format erfolgen. Bearbeitbare Formate sollen 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 2.0 (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.

<sup>19</sup> <https://www.xrepository.de/>

### 8.5.2 Textdokumente zur Weiterbearbeitung

Verbindliche Spezifikation: Office Open XML (OOXML)

Innerhalb der Landesverwaltung MUSS für den Austausch von bearbeitbaren Textdokumenten das Office Open XML Format (unter anderem .docx) verwendet werden, welches auch von verschiedenen Open Source Software (OSS)-Produkten verarbeitet werden kann.

Eingebettete Makros und Objekte DÜRFEN NICHT verwendet werden.

Bestandsgeschützte Spezifikation: Word (.doc) Binary File Format

Innerhalb der Landesverwaltung KANN für den Austausch von bearbeitbaren Textdokumenten das Word-Format (.doc) in der Version 97-2003 verwendet werden.

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

### 8.5.3 Tabellendokumente zur Weiterbearbeitung

Verbindliche Spezifikation: Office Open XML (OOXML)

Innerhalb der Landesverwaltung MUSS für den Austausch von bearbeitbaren Tabellendokumenten das OOXML-Format für Tabellendokumente (unter anderem .xlsx) verwendet werden, welches auch von verschiedenen Open Source Software (OSS)-Produkten verarbeitet werden kann.

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

Bestandsgeschützte Spezifikation: Excel Binary File Format (.xls) Structure Specification

Innerhalb der Landesverwaltung KANN für den Austausch von bearbeitbaren Tabellendokumenten das Excel-Format (.xls) in der Version 97-2003 verwendet werden, welches auch von verschiedenen Open Source Software (OSS)-Produkten verarbeitet werden kann.

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

### 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 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 „Geodaten austausch“.

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 mithilfe von Alpha-Kanälen erreicht werden.

Beobachtete Spezifikation: Scalable Vector Graphics (SVG)

SVG KANN insbesondere für Vektorgrafiken benutzt werden. Damit ist es möglich, Bilder in Web-Seiten 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 9.8 „Webbasierte Geodienste“.

### 8.7.1 Raumbezug der Geodaten

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

Als Lagebezugssystem MUSS das europäische System ETRS89 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. Dabei MÜSSEN mindestens die Mandatory-Elemente des Berlin/Brandenburgischen Profils in der aktuellen Fassung angegeben werden.

Verbindliche Implementation: GeoMIS BE/BB

Metadatenbereitsteller von Geodaten, Geodatendiensten und Geoanwendungen MÜSSEN ihre Metadaten über das GeoMIS BE/BB bereitstellen und veröffentlichen.

### 8.7.3 Geodaten austausch

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.



## 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.

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 in die Landesnetze

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

Bestandsgeschützte Implementation: VPN-Zugang des ZIT-BB vom Internet in die Landesnetze

Für den Netzzugang vom Internet sollte durch die IT-Leitstelle geprüft werden, ob eine Migration zur vom ZIT-BB angebotenen Terminalserver-Lösung möglich ist.

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.

Bestandsgeschützte Spezifikation: Windows Internet Naming Service (WINS)

Windows Internet Naming Service KANN genutzt 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 Clients und Server eingesetzt werden, die den Standard SMTP einhalten.

Verbindliche Spezifikation: RPC over HTTP mit SSL

Zur Kommunikation zwischen Outlook und Exchange ab Version 2016 MUSS RPC over http mit SSL eingesetzt werden.

Bestandsgeschützte Spezifikation: MAPI

Zur Kommunikation zwischen Outlook und Exchange bis Version 2010 KANN weiterhin MAPI 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 Telefonie

Verbindliche Implementierung: Dienst 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<sup>20</sup> genannten Ausnahmen greifen entsprechend.

#### 9.6 Anwendungsprotokolle

Empfohlene Spezifikation: Transport Layer Security (TLS) 1.2

Falls die Datenübertragung in Weitverkehrsnetzen auf Anwendungsebene abzusichern ist, sind TLS beziehungsweise SSH empfohlen. SSLv3 DARF NICHT mehr verwendet werden. Der Einsatz der Version 1.3 wird evaluiert.

Beobachtete Spezifikation: Transport Layer Security (TLS) 1.3

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

Verworfen Spezifikation: Secure Shell, Version 1 (SSH-1)

Verworfen Spezifikation: Secure Sockets Layer (SSL) 3.0

Empfohlene Spezifikation: Online Service Computer Interface (OSCI)-Transport 1.2

Für gesicherte Transaktionen im Zusammenhang mit E-Government-Lösungen SOLLTE das Protokoll Online Service Computer Interface OSCI-Transport 1.2 verwendet werden.

Beobachtete Spezifikation: Online Service Computer Interface (OSCI)-Transport 2.0

Im Unterschied zu Version 1.2 übernimmt OSCI-Transport 2.0 mittlerweile verfügbare Protokolle des Web-Service-Stack. Daher ist OSCI-Transport 2.0 nicht abwärtskompatibel zur Version 1.2.

OSCI-Transport 2.0 wurde im April 2010 durch den KoopA ADV veröffentlicht und KANN in IT-Systemen verwendet werden, wenn die genutzten Funktionalitäten nicht in OSCI-Transport 1.2 existieren.

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

#### 9.7 Verzeichnisdienste

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

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

<sup>20</sup> <http://bravors.brandenburg.de/de/verwaltungsvorschriften-221216>

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)<sup>21</sup> in BB.intern, der in den Projekten eingesetzt werden KANN.

## 9.8 Webbasierte Geodienste

### 9.8.1 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.<sup>22</sup>

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

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

### 9.8.2 Darstellungsdienste

Verbindliche Spezifikation: OGC-WMS 1.3/WMS-DE-Profil 1.0

GDI DE-konforme Web Map Services (WMS) MÜSSEN mindestens eine der beiden folgenden Schnittstellen unterstützen<sup>23</sup>:

- OGC-WMS Version 1.3.0, OpenGIS® Web Map Service Implementation Specification
- WMS-DE-Profil Version 1.0 (basierend auf OGC-WMS 1.1.1)

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 9.8.1 alle genannten Projektionen unterstützen.

Verworfen Spezifikation: Berliner Soldner Koordinaten (EPSG 3068)

<sup>21</sup> PeRLa ist unter <http://perla.lvnbb.de> im Landesverwaltungsnetz zu erreichen.

<sup>22</sup> Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.0, [http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage\\_Beschlussvorlage\\_25\\_Sitzung\\_Architektur\\_GDI\\_DE\\_Technik3.3.0.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage_Beschlussvorlage_25_Sitzung_Architektur_GDI_DE_Technik3.3.0.pdf?__blob=publicationFile)

<sup>23</sup> Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.0, [http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage\\_Beschlussvorlage\\_25\\_Sitzung\\_Architektur\\_GDI\\_DE\\_Technik3.3.0.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage_Beschlussvorlage_25_Sitzung_Architektur_GDI_DE_Technik3.3.0.pdf?__blob=publicationFile)

Verbindliche Spezifikation: Technical Guidance/Handlungsempfehlungen

INSPIRE-konforme Darstellungsdienste MÜSSEN folgende Anforderungen erfüllen:

- Technical Guidance for the implementation of INSPIRE View Services<sup>24</sup>
- Verordnung zu INSPIRE-Netzdiensten<sup>25</sup>
- Handlungsempfehlungen der GDI DE für die Bereitstellung INSPIRE-konformer Darstellungsdienste<sup>26</sup>

### 9.8.3 Downloaddienste

Verbindliche Spezifikation: OGC-WFS Version 2.0

GDI DE-konforme Web Feature Services (WFS) MÜSSEN die folgende Schnittstelle unterstützen<sup>27</sup>:

- 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<sup>28</sup>:

- 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<sup>29</sup>
- Verordnung zu INSPIRE-Netzdiensten<sup>30</sup>
- Handlungsempfehlungen der GDI DE für die Bereitstellung INSPIRE-konformer Downloaddienste<sup>31</sup>

<sup>24</sup> Siehe Technical Guidance for the implementation of INSPIRE View Services  
[http://inspire.ec.europa.eu/documents/Network\\_Services/Technical\\_Guidance\\_ViewServices\\_v3.11.pdf](http://inspire.ec.europa.eu/documents/Network_Services/Technical_Guidance_ViewServices_v3.11.pdf)

<sup>25</sup> Siehe Verordnung (EG) Nr. 976/2009 hinsichtlich der Netzdienste  
<http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009R0976&from=EN>

<sup>26</sup> Siehe Handlungsempfehlungen für die Bereitstellung von INSPIRE-konformen Darstellungsdiensten (INSPIRE View Services)  
[http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Handlungsempfehlungen\\_INSPIRE\\_Darstellungsdienste.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Handlungsempfehlungen_INSPIRE_Darstellungsdienste.pdf?__blob=publicationFile)

<sup>27</sup> Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.0,  
[http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage\\_Beschlussvorlage\\_25\\_Sitzung\\_Architektur\\_GDI\\_DE\\_Technik3.3.0.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage_Beschlussvorlage_25_Sitzung_Architektur_GDI_DE_Technik3.3.0.pdf?__blob=publicationFile)

<sup>28</sup> Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.0,  
[http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage\\_Beschlussvorlage\\_25\\_Sitzung\\_Architektur\\_GDI\\_DE\\_Technik3.3.0.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage_Beschlussvorlage_25_Sitzung_Architektur_GDI_DE_Technik3.3.0.pdf?__blob=publicationFile)

<sup>29</sup> 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](http://inspire.ec.europa.eu/documents/Network_Services/Technical_Guidance_Download_Services_v3.1.pdf)

<sup>30</sup> Siehe Verordnung (EU) Nr. 1088/2010 zur Änderung der Verordnung (EG) Nr. 976/2009 hinsichtlich Downloaddiensten und Transformationsdiensten  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:323:0001:0010:DE:PDF>

<sup>31</sup> Siehe Handlungsempfehlungen für die Bereitstellung von INSPIRE-konformen Downloaddiensten (INSPIRE Download Services)  
[http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Handlungsempfehlungen\\_AK\\_Geodienste\\_Inspire\\_Downloadservices1\\_3\\_0.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Handlungsempfehlungen_AK_Geodienste_Inspire_Downloadservices1_3_0.pdf?__blob=publicationFile)

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.

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

#### 9.8.4 Suchdienste

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

GDI DE-konforme Web Catalogue Services (CSW) MÜSSEN folgende Schnittstelle unterstützen:

- OGC-CSW OpenGIS® Catalogue Service Specification 2.0.2 - ISO Metadata Application Profile, Version 1.0<sup>32</sup>

Verbindliche Spezifikation: Technical Guidance/Handlungsempfehlungen

INSPIRE-konforme Suchdienste MÜSSEN folgende Anforderungen erfüllen:

- Technical Guidance for the implementation of INSPIRE Discovery Services<sup>33</sup>
- Verordnung zu INSPIRE-Netzdiensten<sup>34</sup>

#### 9.8.5 Sonstige Geodienste

Empfohlene Spezifikation: Architekturkonzept der GDI-DE, Version 3.0 - Technik, Kapitel 6

Für sonstige Geodienste SOLLTEN die Spezifikationen gemäß Architekturkonzept der GDI-DE, Version 3.0 eingehalten werden.<sup>35</sup>

#### 9.8.6 Veröffentlichung der webbasierten Geodienste

Verbindliche Implementation: Geoportal Brandenburg

<sup>32</sup> Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.0, [http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage\\_Beschlussvorlage\\_25\\_Sitzung\\_Architektur\\_GDI\\_DE\\_Technik3.3.0.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage_Beschlussvorlage_25_Sitzung_Architektur_GDI_DE_Technik3.3.0.pdf?__blob=publicationFile)

<sup>33</sup> Siehe Technical Guidance for the implementation of INSPIRE Discovery Services [http://inspire.ec.europa.eu/documents/Network\\_Services/Technical\\_Guidance\\_DiscoveryServices\\_v3.1.pdf](http://inspire.ec.europa.eu/documents/Network_Services/Technical_Guidance_DiscoveryServices_v3.1.pdf)

<sup>34</sup> Siehe Verordnung (EG) Nr. 976/2009 hinsichtlich der Netzdienste <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009R0976&from=EN>

<sup>35</sup> Siehe Architektur der Geodateninfrastruktur Deutschland Version 3.0, [http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage\\_Beschlussvorlage\\_25\\_Sitzung\\_Architektur\\_GDI\\_DE\\_Technik3.3.0.pdf?\\_\\_blob=publicationFile](http://www.geoportal.de/SharedDocs/Downloads/DE/GDI-DE/Dokumente/Anlage_Beschlussvorlage_25_Sitzung_Architektur_GDI_DE_Technik3.3.0.pdf?__blob=publicationFile)

GDI BE/BB-konforme webbasierte Geodienste MÜSSEN im Geoportal 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<sup>36</sup> 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.

## 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 9.6 „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 9.6 „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

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 Algorithmenkatalog der Bundesnetzagentur in der jeweils aktuellen Version angewendet werden. Er wird regelmäßig im Bundesanzeiger veröffentlicht.

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.

<sup>36</sup> [http://www.geobasis-bb.de/GeoPortal1/produkte/web\\_geodienste.htm](http://www.geobasis-bb.de/GeoPortal1/produkte/web_geodienste.htm)

Verbindliche Spezifikation: Vertrauensdienstegesetz

Für qualifizierte Signaturen MÜSSEN qualifizierte Signaturzertifikate auf multifunktionalen Signaturkarten entsprechend dem Vertrauensdienstegesetz (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<sup>37</sup> berücksichtigen.

## 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 Bezahlungssystemen zum Einsatz.

<sup>37</sup> Nur im Intranet der Landesverwaltung:  
[http://www.lvnbb.de/media\\_fast/2134/De-Mail\\_Namenskonzept\\_des\\_Landes\\_Brandenburg.pdf](http://www.lvnbb.de/media_fast/2134/De-Mail_Namenskonzept_des_Landes_Brandenburg.pdf)



### 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 Langzeitspeicherung

Im Interesse einer effizienten und kostengünstigen Speichernutzung MUSS bei der Einführung von IT-Verfahren festgelegt werden, wann die Daten ausgesondert werden können beziehungsweise wie lange sie vorgehalten werden müssen (Aufbewahrungsfrist).

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 des Brandenburgischen Archivgesetzes - 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.

Bei neuen Projekten sind die Planung, die Ausführung und die Finanzierung der Langzeitspeicherung aus dem Projekt heraus durchzuführen.

Verbindliche Spezifikation: Open Archival Information System (OAIS)

Die Langzeitspeicherung/Langzeitarchivierung MUSS gemäß ISO-Standard 14721:2012 OAIS erfolgen.

#### 13.1 [entfällt]

#### 13.2 Langzeitspeicherung von Bildern

Empfohlene Spezifikation: Tagged Image File Format (TIFF) 6.0

Empfohlene Spezifikation: Joint Photographic Experts Group 2000 (JPEG2000)

Bei der Verwendung von JPEG2000 zur Langzeitspeicherung SOLLTE die verlustfreie Komprimierung gewählt werden.

#### 13.3 Langzeitspeicherung von Daten

Empfohlene Spezifikation: Extensible Markup Language (XML) v1.1

#### 13.4 Langzeitspeicherung von Dokumenten

Empfohlene Spezifikation: PDF Archive 2 (PDF/A-2)

#### 13.5 Beweiswerterhaltung digital signierter Dokumente

Empfohlene Spezifikation: ArchiSig

## 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)<sup>38</sup> 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 Content Management System

Verbindliche Implementation: SixCMS

Als Content Management System MUSS für den Webauftritt des Landes Brandenburg<sup>39</sup> landeseinheitlich SixCMS eingesetzt werden.

Empfohlene Implementation: SixCMS

Für haus eigene Webauftritte SOLL SixCMS verwendet werden.

Empfohlene Implementation: WordPress

WordPress KANN verwendet werden. Diese Instanzen dürfen nicht im LVN betrieben werden und können nicht durch den ZIT-BB administriert werden.

#### A.2 Virtuelle Poststelle (VPS)

Verbindliche Implementation: Virtuelle Poststelle (VPS) des Landes Brandenburg

Für die sichere, vertrauliche, rechtsverbindliche und elektronische Kommunikation zwischen Bürgern, den Verwaltungen und der Wirtschaft MUSS die vom ZIT-BB bereitgestellte VPS genutzt werden. Dies gilt besonders für folgende Schwerpunkte:

- Zustellung und Prüfung von OSCI-Nachrichten,
- Prüfung elektronischer Signaturen von Dokumenten,
- zentrale Signatur und Verschlüsselung von E-Mails ins Internet,
- Erstellung und Prüfung von elektronischen Zeitstempeln (Quittungen).

#### A.3 Signaturkomponente

Verbindliche Implementation: Signaturkomponente des Landes Brandenburg

Für die Realisierung von elektronischen Signaturfunktionalitäten MUSS diejenige Signaturkomponente verwendet werden, die der ZIT-BB zur Verfügung stellt.

<sup>38</sup> [http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/migrationsleitfaden\\_4\\_0\\_download.pdf?\\_\\_blob=publicationFile](http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/migrationsleitfaden_4_0_download.pdf?__blob=publicationFile)

<sup>39</sup> brandenburg.de sowie BB.intern

#### A.4 Formularservice

Verbindliche Implementation: Formularservice des Landes Brandenburg

Als Formularservice MUSS bei Daten des normalen Schutzbedarfs bezüglich der Grundbedrohung Vertraulichkeit (entsprechend den landeseinheitlichen Schutzbedarfskategorien) der vom ZIT-BB angebotene Service genutzt werden; darüber hinaus wird die Anwendung in Abhängigkeit des Ergebnisses einer Risikoanalyse empfohlen.

Die Formulare SOLLTEN so angeboten werden, dass sie online befüllt und eingereicht werden können. Der Prozess der Datenübernahme SOLLTE medienbruchfrei gestaltet werden.

#### A.5 Portalservice

Empfohlene Implementation: Portalservice im ZIT-BB

Für einen portalgestützten Zugang zu Anwendungen SOLLTE der vom ZIT-BB bereitgestellte Portalservice genutzt werden.

Dieses Angebot wird zurzeit mit dem Produkt Liferay bereitgestellt.

#### A.6 Webkartenkomponente

Empfohlene Implementation: Kartennavigator BRANDENBURGVIEWER-API

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

#### A.7 Multikanal-Zugang

Beobachtete Implementation: Dienstleistung des ZIT-BB

Das Land Brandenburg ist der Verwaltungsvereinbarung Governikus Multimessenger (GMM) mit dem Land Rheinland-Pfalz beigetreten. Ziel ist der Aufbau eines Multikanal-Nachrichtensammel- und -protokollierungsdienstes, mit dem elektronische Nachrichten gegebenenfalls verschlüsselt und signiert auf verschiedenen Kanälen an die Landesverwaltung gerichtet werden können.

### 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 1.2

Für Wirtschaftlichkeitsberechnungen SOLLTE das vom Bund kostenlos zur Verfügung gestellte Programm WiBe Kalkulator 1.2 eingesetzt werden.

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

#### B.6 Webbasierte Kommunikations- und Dokumentenplattform

Verbindliche Implementation: DialogBB

Im ZIT-BB wurde DialogBB auf Basis des Portalservers (A.5) als Nachfolger von CIRCA eingeführt und MUSS entsprechend den Einsatzgebieten von CIRCA genutzt werden.

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.<sup>40</sup>

#### B.8 Vorgangsbearbeitung und Aktenhaltung

Die Vorgangsbearbeitung und Aktenhaltung MUSS am „Organisationskonzept elektronische Verwaltungsarbeit“<sup>41</sup> ausgerichtet werden.

<sup>40</sup> BRAVORS ist im Landesverwaltungsnetz unter <http://bravors.lvnbb.de/> und im Internet unter <http://www.landesrecht.brandenburg.de/> zu erreichen.

<sup>41</sup> [http://www.verwaltung-innovativ.de/DE/E\\_Government/orgkonzept\\_everwaltung/orgkonzept\\_everwaltung\\_artikel.html](http://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_artikel.html)

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 Kabinetttinformationssystem

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.

#### 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 soll. Sollte eine Behörde den Einsatz eines Stellenportals prüfen, sollte der Kontakt mit diesem Projekt aufgenommen werden.

### 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   |
| EEPROM    | Electrically Erasable Programmable Read-Only Memory  |
| ESR       | Extended Support Release   |
| ESRI      | Environmental Systems Research Institute   |
| ETRS      | European Terrestrial Reference System  |
| 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  |
| 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   |
| PSP       | Platform for Privacy Preferences Project   |
| RIO       | Ressort Information Officer  |
| SAGA      | ein Eigenname (ursprünglich: Standards und Architekturen für eGovernment-Anwendungen)              |
| SigG      | Signaturgesetz   |
| SP2       | Service Pack 2   |
| SSH       | Secure Shell   |
| SSL       | Secure Sockets Layer   |
| SVG       | Scalable Vector Graphics   |
| TCP       | Transmission Control Protocol  |
| TIFF      | Tagged Image File Format   |

|            |  |
|------------|--|
| TLS        | Transport Layer Security                       |
| UCS        | Univention Corporate Server                    |
| 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.“           |