Anlage 2
zur IT-Standardisierungsrichtlinie

IT-Standards Land Brandenburg

1 Vorbemerkung

Die IT-Standards werden entsprechend der IT-Standardisierungsrichtlinie definiert und jährlich fortgeschrieben. Ziel ist es, schrittweise einheitliche Standards zu erreichen, das heißt, es soll je Aufgabenbereich nur einen verbindlichen Standard geben, der gezielt bei Migrationen anzustreben ist. Grundsätzlich sollte die Festlegung von Standards auf der Ebene offener Protokolle, Schnittstellen und Austauschformate stattfinden. Die Festlegung konkreter Produkte als Ersatz eines einheitlichen Standards darf nur dann erfolgen, wenn sich für die jeweilige Querschnittsaufgabe trotz intensiver Marktuntersuchung kein geeigneter Standard auf der Ebene von Protokollen, Schnittstellen und Austauschformaten finden lässt. Dabei sind auch die vergaberechtlichen Rahmenbedingungen zu beachten.

Diese Ziele können aufgrund der Ausgangslage nur über einen schrittweisen Prozess der Evaluation, der Betrachtung der Funktionalität und Wirtschaftlichkeit zukünftiger Standards erreicht werden.

Die IT-Standards sind im Sinne der E-Government- und IT-Organisationsrichtlinie verbindlich einzuhalten. Abweichungen von den hier definierten IT-Standards unterliegen dem Genehmigungsvorbehalt gemäß Ziffer 3.1.2 e der E-Government und IT-Organisationsrichtlinie.

In Abstimmung mit der E-Government- und IT-Leitstelle ist im Zusammenhang mit Pilotierungen beziehungsweise Kompetenzerwerb ein gezielter Einsatz und eine damit verbundene Evaluation anderer Schnittstellen, Protokolle, Austauschformate und Produkte möglich.

2 Standards in Bezug auf Protokolle, Schnittstellen und Austauschformate

Für den Regelungsbereich der Protokolle und Schnittstellen werden die Festlegungen des Technology Viewpoint (Teil I): Standards für die IT-Architektur (Kapitel 8) der „Standards und Architekturen für E-Government - SAGA“ der Beauftragten der Bundesregierung für Informationstechnik in der jeweils aktuellen Fassung[1] (zurzeit Version 4) als verbindlich festgelegt.

Entsprechend der SAGA-Klassifizierung von Standards werden diese in „obligatorisch“, „empfohlen“ und „unter Beobachtung“ unterteilt.

2.1 Verzeichnisdienst

Obligatorisch

Grundsätzlich stellt der ZIT-BB des Landes einen einheitlichen Verzeichnisdienst MetaDIR bereit. 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 und das zentrale Adressbuch anschlussfähig sein.

Die Rahmenbedingungen für die Teilnahme am MetaDIR (zum Beispiel Namenskonventionen) werden vom ZIT-BB festgelegt.

2.2 Netzwerkprotokolle

Obligatorisch

Für den Aufbau lokaler Netzwerke ist TCP/IP (IPv4) zu verwenden.

Unter Beobachtung

Die Protokollversion IPv6 wird evaluiert.

Bei neuen Beschaffungen müssen alle Komponenten IPv6 fähig sein.

[1] http://www.cio.bund.de/DE/Standards/SAGA/saga_node.html

2.3 Standards für den Dokumentenaustausch

Elektronischer Dokumentenaustausch zwischen den Behörden und nach außen soll 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 Ministerien sind die folgenden über SAGA hinausgehenden Festlegungen für bearbeitbare Dokumentenaustauschformate verbindlich für die Landesverwaltung.

2.3.1 Austausch von nicht bearbeitbaren Textdokumenten

Obligatorisch

Für Dokumente, die beim Empfänger nicht bearbeitet werden sollen, ist das Portable Document Format (PDF) mindestens in der Version 1.4 zu verwenden.

Empfohlen

Auf die Einschränkung von Nutzer-Rechten (zum Beispiel Drucken, Markieren und Kopieren) sollte verzichtet werden.

2.3.2 Austausch von bearbeitbaren Textdokumenten

Obligatorisch

Innerhalb der Landesverwaltung wird für den Austausch von bearbeitbaren Textdokumenten das Word-Format (DOC) in der Version 2000 verwendet, welches auch von verschiedenen Open Source Software (OSS) Produkten bedient werden kann.

Empfohlen

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

Unter Beobachtung

ODT (ODF) und DOCX (OOXML) werden in verschiedenen Bereichen getestet. Die Ergebnisse sollen in die nächste Fortschreibung einfließen.

2.3.3 Austausch von bearbeitbaren Tabellendokumenten

Obligatorisch

Innerhalb der Landesverwaltung wird für den Austausch von bearbeitbaren Tabellendokumenten das Excel-Format (XLS) in der Version 2000 verwendet, welches auch von verschiedenen Open Source Software (OSS) Produkten bedient werden kann.

Empfohlen

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

Unter Beobachtung

ODS (ODF) und XLSX (OOXML) werden in verschiedenen Bereichen getestet. Die Ergebnisse sollen in die nächste Fortschreibung einfließen.

2.3.4 Komprimierung großer Dokumente beziehungsweise einer Vielzahl von kleineren, zusammengehörenden Dokumenten

Obligatorisch

Für Komprimierung ist das Format ZIP Version 2.0 ohne Verschlüsselung zu verwenden.

2.3.5 Sonstiger Datenaustausch

Obligatorisch

Soweit für den Zweck ein XÖV-Standard im XRepository[2] definiert wurde, ist dieser obligatorisch anzuwenden.

Für Modellierungen im Rahmen von Standardisierungsprojekten ist die vom XÖV vorgesehene UML (Unified Modelling Language) in der Version 2.2 zu nutzen.

Empfohlen

Falls für den Datenaustausch mit anderen Systemen innerhalb oder außerhalb der Landesverwaltung keine festen Formatvorgaben bestehen, wird für die Beschrei-bung der auszutauschenden Daten die Extended Markup Language (XML) verwendet.

2.3.6 Datenaustausch mit Brandenburgisches Landeshauptarchiv (BLHA)

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

Mit dem BLHA ist abzustimmen, ob und in welcher Form (Schnittstelle) die Daten aus dem IT-Verfahren dem BLHA zur Langzeitarchivierung zu übermitteln sind (§ 4 Absatz 7 BbgArchivG).

Bei neuen Projekten ist die Planung, Ausführung und Finanzierung aus dem Projekt heraus durchzuführen.

2.4 Gesicherte Transaktionen

Obligatorisch

Für gesicherte Transaktionen im Zusammenhang mit E-Government-Lösungen wird das Protokoll Online Service Computer Interface (OSCI)-Transport obligatorisch festgelegt. Für die Zustellung von OSCI-Nachrichten ist der im Rahmen der virtuellen Poststelle (VPS) vom ZIT-BB zentral bereit gestellter OSCI-Intermediär zu nutzen.

3 E-Government Basiskomponenten

3.1 Content Management System

Als Content Management System ist für den Webauftritt des Landes Brandenburg[3] landeseinheitlich SixCMS eingesetzt.

Empfohlen

Auch für hauseigene Webauftritte wird SixCMS empfohlen.

3.2 VPS

Obligatorisch

Für die sichere, vertrauliche, rechtsverbindliche und elektronische Kommunikation zwischen Bürgern, den Verwaltungen und der Wirtschaft ist die vom ZIT-BB bereitgestellte VPS zu nutzen. 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).

3.3 Signaturkomponente

Obligatorisch

[2] https://www.xrepository.deutschland-online.de/xrepository/
[3] brandenburg.de sowie BB.intern

Für die Realisierung von elektronischen Signaturfunktionalitäten ist diejenige Signaturkomponente obligatorisch zu verwenden, die der ZIT-BB zur Verfügung stellt.

3.4 Formularserver/-Service

Obligatorisch

Als Formularservice ist der vom ZIT-BB angebotene Service zu nutzen.

Empfohlen

Die Formulare sind so anzubieten, dass sie online befüllt und eingereicht werden können. Der Prozess der Datenübernahme ist medienbruchfrei zu gestalten.

3.5 Bezahlplattform

Obligatorisch

Die Realisierung von Bezahlfunktionalitäten erfolgt mit der vom ZIT-BB bereitgestellten Bezahlplattform.

3.6 Portalserver und BPM

Obligatorisch

Für die Ausgestaltung von E-Government-Prozessen mit Außenwirkung und deren Ausstattung mit Portalfunktionalitäten ist die vom ZIT-BB bereitgestellte Umgebung zu nutzen.

4 Standardsysteme und Querschnittsverfahren

Im Land werden die folgenden Softwareprodukte eingesetzt.

4.1 Arbeitsplatzsysteme (Clients)

4.1.1 Client-Betriebssystem

Obligatorisch

Für den Betrieb der Clients kommt grundsätzlich als Betriebssystem Microsoft Windows ab Version XP zum Einsatz. Bei neuen Installationen ist Windows 7 einzusetzen. Die Clients sind mit dem jeweils aktuellen Servicepack und alle Sicherheitspatches zu betreiben.

In Abstimmung mit dem ZIT-BB erfolgt eine ständige Evaluierung auch im realen Einsatz von alternativen (zum Beispiel Open Source) Betriebssystemen.

4.1.2 Einsatz von Web-Browsern

Obligatorisch

Auf den Clients kommen Web-Browser zum Einsatz, die folgende W3C-Standards unterstützen: HTML 4.01, XHTML 1.1, XSLT, CSS Level 2 und P3P.

Einzusetzen sind der Internet Explorer (zurzeit Version 8) und/oder Firefox (zurzeit Version 3.6). Grundsätzlich sind alle Sicherheitspatches und Updates zu installieren.

Auf die Einbindung Browser-abhängiger Mechanismen (Plug-In-Lösungen, Active-X, Visual Basic, und so weiter) sollte verzichtet werden. Browser-basierte neue Anwendungen müssen auf allen genannten Alternativen laufen.

4.1.3 Büroanwendungen

Empfohlen

Für die Büroanwendungen Textverarbeitung, Tabellenkalkulation, Präsentation und Grafik wird grundsätzlich das Softwareprodukt Microsoft Office ab Version 2007 eingesetzt.

In Abstimmung mit dem ZIT-BB erfolgt eine ständige Evaluierung auch im realen Einsatz von alternativen (zum Beispiel Open Source) Office-Produkten.

4.1.4 Datenbanken

Der Einsatz von Client-Datenbanken wird nicht empfohlen.

4.1.5 Lesen von PDF-Dateien

Empfohlen

Zum Lesen von PDF-Dateien wird Acrobat Reader (zurzeit Version 9.3) eingesetzt. Grundsätzlich sind alle Sicherheitspatches und Updates zu installieren.

4.2 Server und Netze

4.2.1 Serverbetriebssysteme

Mit Hinblick auf die durchzuführende Konsolidierung der Server-Landschaft erfolgt die Auswahl der Serverbetriebssysteme gemeinsam mit dem ZIT-BB.

4.2.2 Datenbankmanagementsysteme

Mit Hinblick auf die durchzuführende Konsolidierung der Datenbankmanagementsysteme erfolgt die Auswahl gemeinsam mit dem ZIT-BB.

4.2.3 Landesverwaltungsnetz (LVN)

Obligatorisch

Die Vernetzung der Behörden ist mit dem LVN zu realisieren.

Für die Anbindung externer Netze sind die durch den ZIT-BB bereitgestellten Gateways zu nutzen.

4.3 IT-Querschnittsverfahren

4.3.1 Groupware und Kommunikationsverbund

Obligatorisch

Zum Senden und Empfangen von E-Mails sind E-Mail-Clients einzusetzen, die zumindest den Austausch von unformatiertem Text gewährleisten und das Post Office Protocol 3 (POP3) beziehungsweise das Internet Mail Access Protocol (IMAP) unterstützen. Hierfür ist der Standard Simple Mail Transfer Protocol (SMTP) in Verbindung mit dem Standard Multipurpose Internet Mail Extensions (MIME) einzuhalten.

Für E-Mail-Anlagen sind die Dokumentenaustauschformate (siehe 2.3) einzuhalten. E-Mail-Inhalte sind im Format „nur Text“ zu verfassen und zu verschicken. Die Empfehlungen des KoopA/ADV zu E-Mails in elektronischen Akten[4] sind einzuhalten.

Der ZIT-BB betreibt hierfür künftig eine zentrale Groupware-Lösung. Mailboxen werden grundsätzlich dabei zentral im ZIT-BB gehostet, ohne dass dezentrale Server zum Einsatz kommen.

4.3.2 System für Personal- und Stellenverwaltung

Obligatorisch

Für die Personal- und Stellenverwaltung in der Landesverwaltung ist mit Ausnahme der Schulverwaltung das vom ZIT-BB betriebene landesweit einheitliche System PerIS zu nutzen.

4.3.3 System für Haushalts-Kassen-Rechnungswesen und Kosten- und Leistungsrechnung

Obligatorisch

[4] http://www.lvnbb.de/media_fast/2134/Grundsatzpapier-E-Mails_in_elektronischen_Akten-Version_1.pdf

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

4.3.4 Haushaltsaufstellungsverfahren

Obligatorisch

Als Produkt für die Haushaltsaufstellung wird HAVWeb eingesetzt.

4.3.5 Reisekostenrechnung

Obligatorisch

Für die dezentrale Reisekostenrechnung wird die Software SMS eingesetzt.

Für die zentrale Reisekostenabrechnung in der ZBB wird Reiko verwendet.

4.3.6 Wirtschaftlichkeitsberechnungen

Obligatorisch

Für Wirtschaftlichkeitsberechnungen wird das vom Bund kostenlos zur Verfügung gestellte Programm WiBe Kalkulator 1.0.1 eingesetzt.

4.3.7 Projektmanagement

IT-Projekte sind gemäß Nummer 4.2.5 der IT-Strategie anhand einheitlicher Projektmanagementmethoden durchzuführen.

Unter Beobachtung

Als Methodik ist der Projektmanagementleitfaden einzusetzen.

4.3.8 Webbasierte Kommunikations- und Dokumentenplattform

Obligatorisch

Als subsidiäre Internet-basierte Informations- und Kommunikationsplattform sowie für den Dokumentenaustausch kommt landesweit das Open Source Produkt CIRCA in der jeweils aktuellen Version zum Einsatz.

4.3.9 Brandenburgisches Vorschriftensystem (BRAVORS)

Obligatorisch

Zur Sammlung, Veröffentlichung und Recherche aller im Land Brandenburg erlassenen und gültigen Gesetze, Rechtsverordnungen und Verwaltungsvorschriften (inklusive ihrer Genese) wird die webbasierte Lösung BRAVORS eingesetzt. BRAVORS wird vom ZIT-BB im LVN bereitgestellt.[5]

4.3.10 Zentrales Verzeichnis der Personen und Ressourcen (PeRLa)

Der ZIT-BB betreibt ein webbasiertes PeRLa[6] der Landesverwaltung.

4.3.11 Vorgangsbearbeitung und Aktenhaltung

Für die elektronische Vorgangsbearbeitung und Aktenhaltung, soweit sie nicht durch spezifische Fachverfahren abgedeckt wird, ist das vom ZIT-BB betriebene landesweit einheitliche System EL.DOK-BB zu benutzen.

Die Ausnahmen gemäß KV 734/08 bleiben hiervon unberührt.

4.3.12 Kabinettinformationssystem

Unter Beobachtung

[5] BRAVORS ist unter http://bravors.lvnbb.de/) und im Internet (http://www.landesrecht.brandenburg.de/zu erreichen.
[6] PeRLa ist unter http://x500-gw.lvnbb.de/vd/oulist.php im Landesverwaltungsnetz zu erreichen.

EL.KIS als Mandant von EL.DOK-BB wird zur Vor- und Nachbereitung sowie Dokumentation von Kabinettsitzungen eingeführt.

4.3.13 Elektronische Normenverkündung

Zur elektronischen Ausfertigung und Verkündung von Verordnungen und Gesetzen sowie deren Verkündung in dem elektronischen Gesetz- und Verordnungsblatt für Brandenburg kommt landesweit EL.Norm zum Einsatz.

4.3.14 eNorm

Zur Einhaltung rechtsförmlicher und redaktioneller Vorgaben während der schriftlichen Erarbeitung von Gesetz- und Verordnungsentwürfen in der Landesverwaltung sowie der elektronischen Normverkündung kommt landesweit eNorm zum Einsatz.

5 Standards in Bezug auf Datenschutz und Datensicherheit

5.1 Sicherheit

Obligatorisch

In Bezug auf die Gewährleistung der IT-Sicherheit ist der IT-Grundschutz auf Basis der Sicherheitsmaßnahmen gemäß den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuellen Fassung zu gewährleisten.

Für das Erstellen von Sicherheitskonzepten sind die methodischen Vorgaben des BSI (BSI-Standards 100x) zu beachten.

5.2 Verschlüsselung/elektronische Signaturen

Obligatorisch

Die Übertragung verschlüsselter Daten ist mittels Verfahren herzustellen, die vom Bundesamt für Sicherheit in der Informationstechnik als sicher eingestufte Methoden und Schlüssellängen verwenden.

Für den Austausch vertraulicher beziehungsweise personenbezogener Daten zwischen Behörden der öffentlichen Verwaltung ist die Public-Key-Infrastruktur für die öffentliche Verwaltung (PKI-1-Verwaltung) zu nutzen. Die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik, welche unter anderem für die Verwendung von signaturgestützten Produkten den Standard „ISIS-MTT“ (inklusive Verschlüsselung mit Mail-Trust-Standard: MTT) vorsehen, sind zu beachten.

Für elektronische Signaturen, die nicht rechtlichen Ansprüchen genügen müssen und vor allem zur sicheren Authentifizierung des Absenders dienen, sind Zertifikate der PKI-1-Verwaltung zu nutzen. Für qualifizierte Signaturen sind qualifizierte Signaturzertifikate auf multifunktionalen Signaturkarten entsprechend SigG/SigV zur rechtssicheren Signatur zu verwenden.

Empfohlen

Bei der Datenübermittlung im Weitverkehrsbereich sind personenbezogenen Daten normalen Schutzbedarfs nach Schutzstufenkonzept der LDA Brandenburg mit einer Leitungsverschlüsselung (das heißt Verschlüsselung am Ausgangspunkt des lokalen Quellnetzes zum Eingangspunkt des lokalen Zielnetzes) zu verschlüsseln, bei darüber liegendem Schutzbedarf mit einer Applikationsverschlüsselung auszustatten.

Falls im bilateralen E-Mail-Verkehr mit Stellen innerhalb und außerhalb der Landesverwaltung die Verschlüsselung der übertragenen Daten im Einzelfall aus Vertraulichkeitsgründen geboten ist und eine ausreichende Verschlüsselung nicht über die austauschenden Systeme hergestellt werden kann, sind möglichst SMIME-Implementierungen, die Zertifikate (X.509) unterstützen, zu nutzen.

Vertrauliche Inhalte, insbesondere beim Austausch über HTTP und FTP, sollen nur über gesicherte Kommunikationsverbindungen zwischen Clients und Servern übermittelt werden, die sich des Secure Socket Layers/Transport Layer Security (SSL/TLS) beziehungsweise der Secure Shell (SSH) bedienen.

Für geschlossene Nutzergruppen können auch andere Sicherheitsmechanismen zum Einsatz kommen, die individuellen Sicherheitskonzepten genügen.

5.3 VPN

Obligatorisch

Für VPN sind die in den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) niedergelegten Grundsätze und Standards einzuhalten.

Empfohlen

Sofern bei der Datenübermittlung im LVN eine Leitungsverschlüsselung (siehe Nummer 5.2) erforderlich ist, sind die vom LVN bereitgestellten Sicherheitsmerkmale (Verschlüsselung auf IPSEC-Basis) zu nutzen.

Für weitergehenden Schutzbedarf ist die VPN-Lösung StrongSWAN unter Verwendung von Zertifikaten der PKI-1-Verwaltung (siehe Nummer 5.2) zu nutzen.

Für geschlossene Nutzergruppen können auch andere Sicherheitsmechanismen zum Einsatz kommen, die individuellen Sicherheitskonzepten genügen.

5.4 Firewalls

Obligatorisch

Für den Einsatz von Firewalls sind die in den Grundschutzkatalogen des BSI niedergelegten Grundsätze und Standards einzuhalten.

Kommunikationsverbindungen von Netzen der Landesverwaltung zu Fremdnetzen sind über die zentralen Zugänge der LVN-Fachnetzbetreiber zu führen. Zentrale Zugänge von Netzen der Landesverwaltung zu anderen Verwaltungsnetzen sind mittels separater Firewalltechnik, zu öffentlichen Netzen mittels Firewalls auf Application-Level-Gateway-Niveau abzusichern.

Empfohlen

Werden in lokalen Netzen personenbezogene Daten hohen oder sehr hohen Schutzbedarfs nach Schutzstufenkonzept der LDA verarbeitet, ist der Einsatz einer separaten Firewall erforderlich. Bei darunter liegendem Schutzniveau ist der Einsatz von Paketfiltern ausreichend.

5.5 Virenschutz

Obligatorisch

Für den Virenschutz sind die in den Grundschutzkatalogen des BSI niedergelegten Grundsätze und Standards einzuhalten.

Der Virenschutz erfolgt über Schutzprogramme. Die Verantwortung für die Organisation des Virenschutzes liegt bei den lokalen Einrichtungen beziehungsweise im Falle der Auftragsdatenverarbeitung beim Dienstleister.

Empfohlen

Zur Gewährleistung des Virenschutzes können sich die lokalen Einrichtungen zentral bereitgestellter Virenschutzmechanismen im LVN bedienen.

Um eine umfassende Virenschutzvorsorge zu erreichen, sollten die Schutzprogramme zum Virenschutz sowohl zentral als auch dezentral installiert sein.

5.6 Hardware-Schnittstellen

Obligatorisch

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

Organisatorische Maßnahmen kommen zur Ergänzung technischer Sicherheitsmaßnahmen in Betracht (zum Beispiel durch Einrichtung von USB-Schleusen).

5.7 Kontaktbehaftete Chipkarten

Obligatorisch

Für kontaktbehaftete Chipkarten für Identitätsprüfungen, zum Beispiel für Dienstausweise entsprechend der „Richtlinie über die Einführung einheitlicher Dienstausweise für die obersten Landesbehörden des Landes Brandenburg“ (ABl. 30/09) vom 2. Juli 2009, ist als Mindestvoraussetzung ein Chip in EEPROM-Technologie mit einer Speicherkapazität von mindestens 16 Kilobyte sowie einfacher Sicherheitslogik (PIN) zu verwenden.

Er hat der ISO-Normen 7816-3 für den Befehlsatz und die Übertragungsprotokolle, ISO 7816-2 für Belegung der Kontakte sowie den ISO-Normen 8824 und 8825 für die Zeichencodierung zu entsprechen.

Als Schnittstelle zur Applikation ist zusätzlich zur Kommunikation mittels kartenspezifischer Befehle eine Unterstützung von CSP beziehungsweise PKCS#11 vorzusehen.

Der ZIT-BB ist als Registrierungsstelle für die Erstellung der notwendigen Zertifikate für Authentisierungs- und Signaturzwecke zu nutzen. Weitere Festlegungen zum Verfahren trifft der ZIT-BB.

6 Geoinformationen

6.1 Raumbezug der Geodaten

Obligatorisch

Geodaten sind im einheitlichen Bezugssystem gemäß Runderlass III Nr. 13/1996 des Ministeriums des Innern vom 10. Mai 1996 zu referenzieren. Das Lagebezugssystem ist das europäische System ETRS 89 mit UTM-Abbildung (33. UTM-Zone). Das Höhenbezugssystem ist das System des DHHN 92.

Die durch den Aufbau der Geodateninfrastruktur Berlin/Brandenburg geforderten Koordinatenreferenzsysteme und Projektionen sollen von den webbasierten Geodiensten so unterstützt werden, dass Anfragen und Antworten in den geforderten Koordinatenreferenzsystemen und Projektionen erfolgen können, auch wenn die Daten intern in einem anderen Koordinatenreferenzsystem oder in einer anderen Projektion gespeichert sind.[7]

Die GDI-konformen webbasierten Geodienste müssen in der Lage sein, folgende geografischen Koordinatenreferenzsysteme zu unterstützen (siehe Architekturkonzept der GDI-DE, Version 2.x):
- WGS84 (EPSG 4326)
- ETRS89 (EPSG 4258)

Die GDI-konformen webbasierten Geodienste müssen in der Lage sein, folgende Projektionen zu unterstützen (siehe Architekturkonzept der GDI-DE, Version 2.x):
- ETRS89/ETRS-TM32 (EPSG 3044)
- ETRS89/UTM Zone 32N (EPSG 25832)

Darüber hinaus müssen die webbasierten Geodienste der GDI BE/BB folgende Projektion unterstützen:
- ETRS89/UTM Zone33N (EPSG 25833)

Empfohlen

Für webbasierte Geodienste der GDI BE/BB sollte folgende Projektion unterstützt werden:
- Berliner Soldner Koordinaten (EPSG 3068)

6.2 Metadaten

Obligatorisch

Metadaten für Geodaten, Geodatendienste und Geoanwendungen sind entsprechend der ISO 19115, und Metadaten über Geodienste sind entsprechend der ISO 19115/19119 bereitzustellen. Jede Bereitstellung von Geodaten für Dritte sollte durch die gleichzeitige Abgabe der dazugehörigen Metadaten qualifiziert werden. Dabei sind mindestens die Mandatory Elemente des Berlin/Brandenburgischen Profils in der aktuellen Fassung anzugeben. Metadatenbereitsteller von INSPIRE-relevanten Geodaten, Geodatendiensten und Geoanwendungen verpflichten sich ihre Metadaten über das GeoMIS BE/BB bereitzustellen und zu veröffentlichen.

[7] Architekturkonzept der GDI-DE Version 2.x

6.3 Geodatenaustausch

Obligatorisch

Für den Austausch von Geodaten zwischen Geoinformationssystemen gibt es die Vorgabe, nachfolgende Datenformate primär für den lesenden und schreibenden Zugriff mindestens zu unterstützen. Für den Austausch von Vektordaten sind die Formate NAS, ESRI-Shape und EDBS, für Rasterdaten TIFF Format 5.0 mit Georeferenzierungsdatei zu verwenden. Die Rasterdatenkompression von farbigen Geodaten ist im Format TIFF-LZW, die Rasterdatenkompression von schwarz/weißen Geodaten (1Bit Farbtiefe) ist im Format CCITT, Gruppe 4 vorzunehmen.

Die Georeferenzierung ist mittels Datei im tfw-Format (je TIFF-Datei) durchzuführen.

Empfohlen

Für den Austausch von Vektordaten werden zusätzlich die Formate Geography Markup Language (GML) und ESRI-Coverage sowie für Rasterdaten die Formate GeoTIFF und ECW empfohlen.

Geodaten werden über Geodienste bereitgestellt.

Unter Beobachtung

Zukünftig ist für den ressourcenschonenden Umgang mit Rasterdaten die Einführung des verlustbehafteten Komprimierungsformates MrSID vorgesehen. Für den Datenaustausch unter ESRI-Nutzern ist das Format ArcGIS-XML vorzusehen.

6.4 Einrichtung von Webservices

Die Bereitstellung der Geodaten innerhalb einer Geodateninfrastruktur erfolgt grundsätzlich über webbasierte Geodienste. Die Nutzbarkeit der Dienste wird durch vereinbarte Schnittstellen, das heißt Standards oder Implementierungsspezifikationen sichergestellt. Die Schnittstellen definieren das Kommunikationsformat und das Verhalten des Dienstes. Anwendungen oder andere Dienste müssen neben Kenntnissen über die Schnittstellen wissen, dass der Dienst zur Verfügung steht und die geforderte Serviceleistung liefert.[8]

Bei der Bereitstellung von webbasierten Geodiensten müssen folgende Standards unterstützt werden:

6.4.1 Darstellungsdienste

Obligatorisch

Web Map Service (WMS) - stellt Karten- oder Othophotodarstellungen in Bildformaten dar. Optional können auch Sachinformationen zu einem Bildpunkt abgefragt werden. Ein GDI-konformer WMS muss in der Lage sein, mindestens eine der beiden folgenden Schnittstellen zu unterstützen (siehe Architekturkonzept der GDI-DE, Version 2.x):

- OGC-WMS Version 1.3, OpenGIS® Web Map Service Implementation Specification
- WMS-DE-Profil Version 1.0 (basierend auf OGC-WMS 1.1.1)

6.4.2 Downloaddienste

Obligatorisch

Web Feature Service (WFS) - ermöglicht einen webbasierten Zugriff auf vektorbasierte Objekte. Ein GDI-konformer WFS muss in der Lage sein, mindestens eine der beiden folgenden Schnittstellen zu unterstützen (siehe Architekturkonzept der GDI-DE, Version 2.x):

- OGC-WFS Version 2.0, OpenGIS® Web Feature Service Implementation Specification
- OGC-WFS Version 1.0, OpenGIS® Web Feature Service Implementation Specification

Gazetteer Service - ermöglicht die Suche nach geografischen Objekten, zum Beispiel Adressen. Der Gazetteer Service wird nach folgendem Standard implementiert:

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

6.4.3 Suchdienste

Obligatorisch

[8] Architekturkonzept der GDI-DE Version 2.x

Der Katalogdienst ermöglicht den webbasierten Zugriff auf Metadaten über Geodaten, Geodienste und Anwendungen. Ein GDI-konformer Web Catalog Service (CSW) muss folgende Schnittstelle unterstützen:

- OGC-CSW OpenGIS® Catalog Service Specification 2.0.2 - ISO Metadata Application Profile, Version 1.0[9]

Weitere webbasierte Geodienste sowie die Aussagen zur Performanz-, Verfügbarkeit und Kapazität der Dienste sind im Architekturkonzept der GDI-DE geregelt und zu berücksichtigen.

6.4.4 Weitere Dienste gemäß Architekturkonzept der GDI-DE, Version 2.x

Empfohlen

Die Spezifikationen gemäß Nummer 8 des Architekturkonzeptes der GDI-DE, Version 2.x sollen eingehalten werden.

6.5 Veröffentlichung der webbasierten Geodienste

Empfohlen

Die der GDI-BE/BB zur Verfügung gestellten webbasierten Geodienste sollen im Geoportal der GDI-BE/BB registriert werden.

7 Sonstiges

7.1 Migrationen

Für Weiterentwicklungen der IT-Infrastruktur beziehungsweise bei geplanten Migrationen ist der „Migrationsleitfaden“ des IT-Beauftragten des Bundes (Version 3 vom April 2008)[10] zu beachten.

[9] Architekturkonzept der GDI-DE Version 2.x
[10] http://www.cio.bund.de/cae/servlet/contentblob/294268/publicationFile/4678/migrationsleitfaden_download.pdf