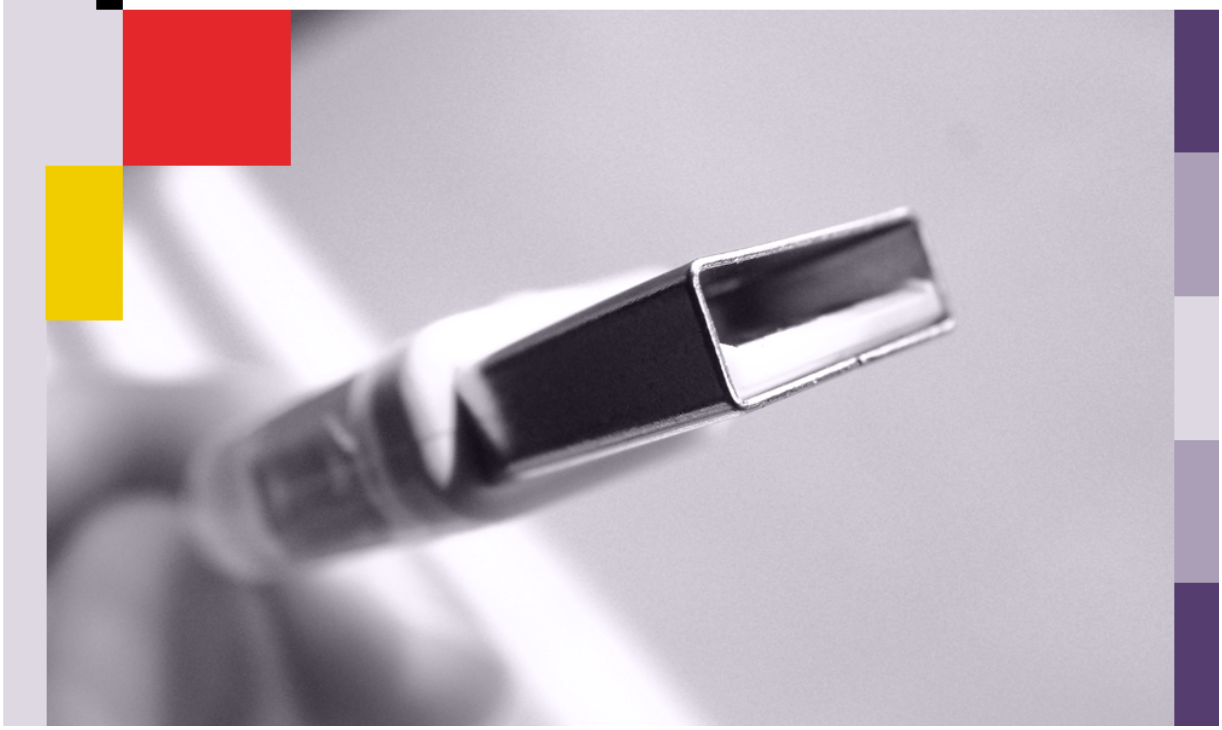
Bundesministerium
des Innern

SAGA

Version 4.0

Standards und Architekturen für
E-Government-Anwendungen



März 2008

Dieser Band wurde erstellt vom Bundesministerium des Innern
in Zusammenarbeit mit der]init[AG und
dem Fraunhofer-Institut für Software- und Systemtechnik (ISST).

Redaktion:]init[AG, Berlin

Homepage und Download der digitalen Version: http://www.kbst.bund.de/saga
mailto: IT2@bmi.bund.de

SAGA

Standards und Architekturen für E-Government-Anwendungen

Version 4.0

März 2008

Herausgegeben vom
Bundesministerium des Innern

Danksagung

Das Bundesministerium des Innern und das SAGA-Autoren-Team danken den Vertretern von Ländern und Kommunen in der KoopA-SAGA-Projektgruppe, den Vertretern zentraler IT-Dienstleister der Bundesverwaltung sowie allen Mitgliedern des SAGA-Expertenkreises für ihre fachliche Unterstützung bei der Erstellung der vorliegenden Version von SAGA.

Der Dank gilt weiterhin allen Nutzerinnen und Nutzern des SAGA-Forums und des SAGA-Kontaktformulars, die mit ihren engagierten Kommentaren einen maßgeblichen Beitrag zur Fortschreibung des Dokuments geleistet haben.

Vorbemerkung:

Dieses Dokument stellt in verdichteter Form verbreitete Standards, Verfahren und Methoden der modernen IT-Entwicklung für E-Government vor. Naturgemäß werden von den Experten auf diesem Gebiet sehr viele Abkürzungen und überwiegend englischsprachige Akronyme verwendet. Ein Teil dieser Namen sind urheberrechtlich beziehungsweise als Warenzeichen oder Produkt für bestimmte Hersteller oder Normungsorganisationen national und international geschützt.

Zur Erzielung einer einfachen Struktur wurde generell auf solche Urheberrechts- und Quellenverweise verzichtet. **Die Verwendung eines „Namens" oder einer Abkürzung in diesem Dokument bedeutet nicht, dass sie frei von Urheber- und Schutzrechten anderer sind.**

Ebenso können Herausgeber, Autoren und befragte Experten keine Verantwortung für die technische Funktionsfähigkeit, Kompatibilität oder Vollständigkeit der diskutierten Standards übernehmen. Die vorliegende Version 4.0 wurde im Oktober 2007 veröffentlicht; Kommentare, Ergänzungen, Berichtigungen werden vom Bundesministerium des Innern, Referat IT 2 erbeten und können im Forum unter http://www.kbst.bund.de/saga-forum eingestellt werden.

Versionsnummern sind dort aufgeführt, wo sie im diskutierten Zusammenhang relevant sind. Wenn für Standards keine Versionsnummern angegeben sind, sollte die aus Marktsicht stabilste Version verwendet werden, welche nicht immer die neueste Version ist.

Eine pauschale Forderung nach SAGA-Konformität trägt nicht zur Erreichung der Ziele von SAGA bei. Die pauschale Forderung lässt aufgrund der Komplexität des Dokuments immer Spielraum für Interpretationen und Missverständnisse. Dies erschwert es dem Auftragnehmer, die Anforderungen zu erfüllen, und dem Auftraggeber, die Erfüllung der Anforderungen zu kontrollieren. Für weitere Ausführungen zum korrekten Umgang mit dem Thema SAGA-Konformität siehe Abschnitt 2.4 auf Seite 25 und http://www.kbst.bund.de/saga-konformitaet für zusätzliche Hilfestellungen.

Inhaltsverzeichnis

0 Status, Änderungshistorie und Ausblick

0.1 Änderungen gegenüber Version 3.0

Dieses Dokument ist eine Überarbeitung von SAGA in der Version 3.0. Folgende Änderungen wurden vorgenommen:

In Kapitel 2 „Grundlagen von SAGA" wurden die englischsprachigen Namen der Listen zur erweiterten Klassifizierung von technischen Standards außerhalb des Dokuments (White List, Grey List, Black List) durch deutschsprachige Namen (Vorschlagsliste, Bestandsschutzliste, Negativliste) ersetzt[1].

Kapitel 4 „Enterprise Viewpoint: Grundlagen E-Government" wurde strukturell neu gegliedert. Die Begriffe „E-Government" und „Dienstleistung" werden klarer definiert[2]. Weiterhin wurde das Kapitel um die Themen „E-Government 2.0"[3], „Deutschland-Online"[4], „Deutschland als Mitglied der Europäischen Union"[5], „EU-Dienstleistungsrichtlinie"[6] und „Signatur-Projekte und -Initiativen des Bundes"[7] erweitert.

Das Kapitel 5 „Information Viewpoint: Standardisierung von Datenmodellen" wurde hinsichtlich des Deutschland-Online Vorhabens „Standardisierung"[8] inklusive der Themen XGenerator 2.0[9] und Kernkomponenten (Core Components)[10] überarbeitet.

Das Kapitel 6 „Computational Viewpoint: Referenz-Software-Architektur" wurde um Abschnitte zu Architekturentscheidungen[11] und um Hinweise zur Einführung diensteorientierter Architekturen[12] erweitert.

In Kapitel 7 „Engineering Viewpoint: IT-Service-Management und Referenzinfrastruktur" wird als Best Practice für IT-Service-Management die „IT Infrastructure Library" (ITIL) eingeführt[13]. Weiterhin wird das Deutsche Verwaltungsdiensteverzeichnis (DVDV) näher vorgestellt[14].

Die bisherigen Kapitel 8 „Technology Viewpoint (Teil I): Standards für die IT-Architektur" und Kapitel 9 „Technology Viewpoint (Teil II): Standards für die Datensicherheit" wurden in eine gemeinsame Struktur zu dem Kapitel 8 „Technology Viewpoint: Standards für IT-Architektur und Datensicherheit" zusammengeführt. Weiterhin wurden Produkte und Implementierungen konsequent durch die zugrunde liegenden Standards ersetzt. Die bisherige Positivliste von unterstützten Plug-Ins wurde durch eine Aufzählung von Anforderungen

1. siehe Abschnitt 2.3.2 „Erweiterte Klassifizierung von Standards" auf Seite 21
2. siehe Abschnitt 4.1 „Definitionen zum E-Government in Deutschland" auf Seite 37
3. siehe Abschnitt 4.3.1 „E-Government 2.0 – Das Programm des Bundes" auf Seite 39
4. siehe Abschnitt 4.3.2 „Deutschland-Online – Die gemeinsame E-Government-Strategie von Bund, Ländern und Kommunen" auf Seite 40
5. siehe Abschnitt „Deutschland als Mitglied der Europäischen Union" auf Seite 44
6. siehe Abschnitt 4.5.4 „EU-Dienstleistungsrichtlinie – Schaffung eines EU-Binnenmarkts" auf Seite 50
7. siehe Abschnitt „Initiativen und Projekte des Bundes im Bereich elektronischer Signaturen" auf Seite 48
8. siehe Abschnitt 5.3 „Das Deutschland-Online Vorhaben „Standardisierung"" auf Seite 59
9. siehe Abschnitt 5.4.3 „XGenerator 2.0" auf Seite 64
10. siehe Abschnitt 5.4.4 „Kernkomponenten" auf Seite 65
11. siehe Abschnitt 6.3.1 „Architekturentscheidungen" auf Seite 74
12. siehe Abschnitt 6.3.2 „Einführung einer diensteorientierten Architektur" auf Seite 75
13. siehe Abschnitt 7.1 „IT-Service-Management mittels ITIL" auf Seite 81
14. siehe Abschnitt 7.4.1 „Deutsches Verwaltungsdiensteverzeichnis" auf Seite 91

ersetzt, die von Plug-Ins in E-Government-Anwendungen der Bundesverwaltung eingehalten werden sollen. Inhaltlich wurden die Themen „IP-Telefonie“[15] und „Registrys“[16] neu eingeführt und das bereits in SAGA 3.0 vorhandene Thema „Smartcards“[17] weiter ausgebaut.

Für die Einer-für-Alle-Angebote (EfA-Angebote) der Bundesverwaltung gibt es in SAGA 4.0 keinen eigenständigen Anhang mehr. Die Beschreibung der EfA-Angebote erfolgt in Zukunft zeitnah und aktuell außerhalb von SAGA auf der Homepage der KBSt[18] beziehungsweise den Homepages der einzelnen EfA-Angebote. Die Definitionen von EfA-Dienst, EfA-System, Infrastruktur und EfA-Konzept wurden in das Kapitel 6[19] verschoben.

Außerdem wurde auf die Weiterentwicklung von Standards reagiert. Standards der Vorschlagsliste (ehemals White List) wurden übernommen, Klassifizierungen vorhandener Standards verändert und Standards aus dem Dokument auf die Bestandsschutzliste (ehemals Grey List) verschoben[20].

0.2 Zukünftige Themenbereiche

Folgende Themengebiete sollen für die nächste SAGA-Version weiter untersucht und detailliert werden:

a. Entwicklung und Standardisierung von Prozess- und Datenmodellen
b. IT-Service-Management anhand der „IT Infrastructure Library“ (ITIL) v3.0
c. Langzeitarchivierung von dynamischen Informationen aus Datenbanken und Web-Seiten
d. Kommunikation per Instant Messaging und Chat
e. Austausch und Visualisierung von 3D-Daten

Ergänzend zum SAGA-Dokument stellt das Bundesministerium des Innern im Web weitere Informationen, Links und Hilfsmittel zur Verfügung[21].

15. siehe Abschnitt 8.7.4 „IP-Telefonie“ auf Seite 129
16. siehe Abschnitt 8.8.1 „Verzeichnisdienste und Registrys“ auf Seite 135
17. siehe Abschnitt 8.11.2 „Kontaktlose Smartcards“ auf Seite 140 und Abschnitt 8.11.3 „Lesegeräte und Schnittstellen für Smartcards“ auf Seite 140
18. siehe http://www.kbst.bund.de/efa
19. siehe Abschnitt 6.3.6 „Wiederverwendung und Integration von EfA-Angeboten“ auf Seite 78
20. zur Definition von Vorschlagsliste und Bestandsschutzliste siehe Abschnitt 2.3.2 auf Seite 21
21. siehe http://www.kbst.bund.de/saga

1 Einleitung

1.1 Hintergrund

Mit dem Ziel, eine moderne und dienstleistungsorientierte Verwaltung zu schaffen, setzt die Bundesregierung immer mehr Verwaltungsprozesse elektronisch um. Durch den Einsatz von E-Government lassen sich die Anliegen von Bürgern, der Wirtschaft und innerhalb der Verwaltung schneller und effizienter erledigen. Um die vielfältigen Anwendungen zukunftsfähig und für alle zugänglich zu gestalten, sind Standards notwendig. Die Richtlinie Standards und Architekturen für E-Government-Anwendungen (SAGA) gewährleistet dies.

Kurz nach dem Start der bundesweiten Initiative BundOnline stellte die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) im Jahr 2002 das Dokument erstmalig zur Verfügung. Seitdem unterstützte SAGA die Behörden, das gesteckte Ziel der Initiative zu erreichen und über 400 internetfähige Dienstleistungen online anzubieten.

Aufbauend auf diesem Erfolg begleitet der SAGA-Expertenkreis kontinuierlich die Arbeit an den Richtlinien. Mit der Version 4.0 haben erstmals zentrale IT-Dienstleister der Bundesverwaltung an der Fortschreibung mitgewirkt. Durch die Diskussion im öffentlichen SAGA-Forum fließen ständig aktuelle Entwicklungen und Erfahrungen in das Dokument ein. In enger Zusammenarbeit mit einer KoopA-SAGA-Projektgruppe[22] werden auch konkrete Anforderungen der Länder und Kommunen einbezogen. Mit diesem Wissen verfasst das SAGA-Autoren-Team unter der inhaltlichen Verantwortung des Bundesministeriums des Innern regelmäßig eine aktualisierte Version.

Zahlreiche abgeschlossene Projekte haben sich mittlerweile an den von SAGA empfohlenen modernen und investitionssicheren Standards und Technologien orientiert. Viele Bundesbehörden nutzen bei der Planung und Umsetzung ihrer IT-Vorhaben SAGA, um die verschiedenen geplanten und vorhandenen Anwendungen untereinander interoperabel zu gestalten.

Diese große Akzeptanz und insbesondere das zunehmende Interesse der Länder und Kommunen zeigen, dass SAGA für deutsches E-Government weiter an Bedeutung gewinnt. Mit der vorliegenden Version 4.0 bietet SAGA erneut einen Leitfaden für die wirtschaftliche und zukunftsorientierte Realisierung von IT-Projekten in der Verwaltung.

1.2 Angesprochener Leserkreis

SAGA richtet sich in erster Linie an Entscheider aus den Bereichen Organisation, Informationstechnik und E-Government in der deutschen Verwaltung. Das Dokument gibt als Leitfaden eine Orientierungshilfe für die Konzeption technischer Architekturen und die technische Grobkonzeption einzelner IT-Anwendungen.

22. KoopA ADV = **Koop**erations**a**usschuss **a**utomatisierte **D**aten**v**erarbeitung Bund / Länder / Kommunaler Bereich

Entwickler von Anwendungen sind aufgefordert, im Detail nach weiteren Lösungen zu suchen, wenn die vorgestellten Standards und Lösungsvorschläge zur Umsetzung fachlicher Anforderungen nicht ausreichen.

Der Bund sieht seine Initiative als einen Beitrag zur Entwicklung von E-Government in Deutschland. Die im Rahmen der Initiative gesammelten Erfahrungen sollen flächendeckende und behördenübergreifende E-Government-Angebote fördern.

1.3 Ziele

SAGA verfolgt die Ziele:

a. **Interoperabilität** – Gewährleistung der Zusammenarbeit verschiedener E-Government-Anwendungen, um effizient Informationen zwischen Bund, Bürgern, Unternehmen und Partnern des Bundes auszutauschen
b. **Wiederverwendbarkeit** – mehrfache Nutzung von Prozess- und Datenmodellen, Systemen, Diensten und Komponenten in verschiedenen E-Government-Projekten, um Synergieeffekte zu erzeugen
c. **Offenheit** – Einbindung offener Standards in E-Government-Anwendungen, um deren langfristige Nutzbarkeit zu fördern[23]
d. **Reduktion von Kosten und Risiken** – Berücksichtigung investitionssicherer Entwicklungen am Markt und im Bereich der Standardisierung
e. **Skalierbarkeit** – Sicherstellung der Nutzbarkeit von Anwendungen bei sich ändernden Anforderungen hinsichtlich Volumen und Transaktionshäufigkeit

1.4 Aufgaben

SAGA verfolgt einen umfassenden Standardisierungsansatz für die deutsche Verwaltung, um die genannten Ziele zu erreichen.

Festlegung der technischen Normen, Standards und Architekturen für E-Government-Anwendungen

Die technischen Normen, Standards und Architekturen umfassen alle für das E-Government relevanten Ebenen und Elemente. Sie sind die Grundlage für die Interoperabilität und Kompatibilität der zu entwickelnden E-Government-Anwendungen.

Vereinheitlichung von Prozessen und Daten in Verwaltungen

Um die Interoperabilität und Kompatibilität der E-Government-Anwendungen zu erreichen, ist es notwendig, Grundlagen zur Vereinheitlichung von Prozessen und Daten in deutschen Verwaltungen zu schaffen. Um dies zu unterstützen, werden auf der Website der KBSt Dienste und Systeme beschrieben, die als Bausteine (Einer-für-Alle-Angebote[24]) in E-Government-Anwendungen eingesetzt werden können.

23. Abschnitt 2.2 „Mindestanforderungen bezüglich der Offenheit von Standards“ auf Seite 20
24. EfA-Angebot und Netze: http://www.kbst.bund.de/efa

1.5 Grundprinzipien für E-Government-Anwendungen

E-Government-Anwendungen haben den Anspruch, ihre Zielgruppen vollständig erreichen zu können. Deshalb sollen alle Funktionen unabhängig von der gewählten Plattform der Nutzer, von der Konfiguration der Nutzersysteme und den Fähigkeiten der Nutzer erreichbar sein. Die E-Government-Anwendungen müssen sich an den Anforderungen und Bedürfnissen der Zielgruppen orientieren.

Ausgehend von diesen Voraussetzungen werden die nachfolgenden Grundprinzipien für E-Government-Anwendungen festgelegt:

a. E-Government-Anwendungen nutzen als Frontend primär den Web-Browser, es sei denn, die umzusetzenden Dienstleistungen sind über Browser nicht sinnvoll abbildbar.
b. Sie verzichten auf aktive Inhalte, um den Benutzer nicht zu zwingen, die Sicherheitseinstellungen des Browsers herabzusetzen und so Beschädigungen durch unsichere Web-Seiten zu ermöglichen, oder verwenden zumindest nur signierte und qualitätsgesicherte Anwendungen nach Abschnitt 8.5.1 „Informationszugriff mit Computern“ auf Seite 104.
c. E-Government-Anwendungen legen keine Programmteile und Daten auf den Computern der Anwender ab, die sich deren Kontrolle entziehen[25].

1.6 Beziehung zu anderen E-Government-Dokumenten

Standards und Architekturen für E-Government werden bereits seit einigen Jahren in Deutschland und in anderen Ländern erprobt[26]. Die hier gewonnenen Erfahrungen und der internationale Austausch darüber tragen dazu bei, die Definition und Umsetzung von SAGA zu erleichtern.

SAGA erscheint innerhalb der KBSt-Schriftenreihe, wie beispielsweise auch das „V-Modell XT“, der „Migrationsleitfaden“ und das „DOMEA-Konzept“. Die Dokumente dieser Reihe werden bei Fortschreibungen aufeinander abgestimmt. Das bedeutet konkret, dass SAGA Aussagen älterer Dokumente „überschreibt“ und neuere Dokumente die Aussagen der letzten SAGA-Version berücksichtigen. Bei der Fortschreibung von SAGA wird durch einen breiten Abstimmungsprozess vermieden, dass Widersprüche zu aktuellen Dokumenten auftreten.

E-Government-Handbuch

Zur Förderung von E-Government-Initiativen des Bundes – wie z. B. der 2005 abgeschlossenen Initiative BundOnline 2005 – sowie zur Unterstützung der Landes- und Kommunalbehörden entstand unter Federführung des Bundesamts für Sicherheit in der Informationstechnik (BSI) das E-Government-Handbuch[27]. Das Handbuch ist als Nachschlagewerk und zentrale Informationsbörse zum Thema E-Government konzipiert.

25. Als ein Negativbeispiel für ungefragtes Ablegen von Programmen auf Computern sei die automatische Installation von Software beim Einlegen einiger Musik-CDs genannt.
26. siehe entsprechende Dokumente und Publikationen Großbritanniens [e-GIF], der Vereinigten Staaten von Amerika [FIPS-PUBS], Australiens [APEC] und Europas [IDABC]
27. siehe http://www.bsi.bund.de/fachthem/egov/3.htm

Das E-Government-Handbuch ist eine modularisierte Materialsammlung mit einem breiteren Themenspektrum als SAGA. Wo gleiche Themen behandelt werden, ist das E-Government-Handbuch konkreter. Deshalb werden aus SAGA heraus einige Module des E-Government-Handbuchs referenziert[28]. SAGA gibt Richtlinien vor, während das E-Government-Handbuch die Umsetzung dieser Richtlinien erläutert und praktische Ratschläge gibt.

Mitte Februar 2003 wurde SAGA in das E-Government-Handbuch aufgenommen. Es ist das verbindlichste Modul des Handbuchs. Alle anderen Module stellen die Konformität zu SAGA sicher.

Im Zuge der Betrachtung des Themenschwerpunkts „IT und IT-Sicherheit" ist die Studie „Sichere Integration von E-Government-Anwendungen (SIGA)"[29] erstellt worden. Ziel dieser Studie ist es, die in SAGA dargestellten Technologien für die Ebene der Geschäftslogik aufzuarbeiten, Zusammenhänge zu erschließen sowie entscheidende, neutrale Hilfestellungen für IT-Experten und -Entscheider zu geben.

IT-Grundschutz-Kataloge und -Standards

Zur Erstellung von IT-Sicherheitskonzepten für normalen Sicherheitsbedarf werden vom BSI mit dem IT-Grundschutz[30] Standardsicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und das als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.

Zum IT-Grundschutz gehören die BSI-Standards zum IT-Sicherheitsmanagement[31] und die IT-Grundschutz-Kataloge[32], die das bisherige IT-Grundschutzhandbuch ersetzen. Die BSI-Standards unterteilen sich in:

a. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)[33],
b. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise[34] und
c. BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz[35].

Die Anwendung des IT-Grundschutzes wird in SAGA durch Festlegung der BSI-Standards zum IT-Sicherheits-Management und der IT-Grundschutz-Kataloge als obligatorische Standards gefordert[36].

28. siehe z. B. Abschnitt 8.1.4 „Umsetzung der Sicherheitskonzeption" auf Seite 95 und Abschnitt 8.5.4 „Technologien zur Authentisierung" auf Seite 107
29. siehe [SIGA]
30. siehe http://www.it-grundschutz.de/
31. siehe http://www.bsi.de/literat/bsi_standard/
32. siehe http://www.bsi.de/gshb/deutsch/
33. siehe http://www.bsi.bund.de/literat/bsi_standard/standard_1001.pdf
34. siehe http://www.bsi.de/literat/bsi_standard/standard_1002.pdf
35. siehe http://www.bsi.de/literat/bsi_standard/standard_1003.pdf
36. siehe Kapitel 7 auf Seite 81 und Abschnitt 8.1 auf Seite 93

Barrierefreie Informationstechnik-Verordnung – BITV

Die Verordnung zur Schaffung barrierefreier Informationstechnik nach dem § 11 Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung – BITV)[37], die am 24. Juli 2002 in Kraft trat, wird in SAGA referenziert und in Bezug auf die Realisierung der Präsentations- und Client-Schicht als obligatorischer Standard festgelegt[38].

V-Modell XT

Das V-Modell XT[39] ist das für den gesamten Bereich der Bundesverwaltung verbindliche Vorgehensmodell zur Entwicklung von IT-Systemen der Bundesbehörden. Das V-Modell XT muss bei strategischer Planung und Projektmanagement sowie bei der Implementierung von E-Government-Anwendungen beachtet werden.

Als Leitfaden zum Planen und Durchführen von Entwicklungsprojekten definiert es unter Berücksichtigung des gesamten Systemlebenszyklus die in einem Projekt zu erstellenden Ergebnisse. Gleichzeitig beschreibt es die konkreten Vorgehensweisen, mit denen diese Ergebnisse erarbeitet werden. Darüber hinaus legt das V-Modell XT die Verantwortlichkeiten jedes Projektbeteiligten fest. Es dient somit als Vertragsgrundlage, Arbeitsanleitung und Kommunikationsbasis.

Das V-Modell XT wird im Rahmen von Releases ständig weiterentwickelt.

IT Infrastructure Library – ITIL

Zum effektiven und verlässlichen Management von IT-Prozessen hat sich die „IT Infrastructure Library" (ITIL) als Verfahrensbibliothek, die Best Practices liefert, inzwischen weltweit als akzeptierter Defacto-Standard etabliert. Von der KBSt wurden daher eine Reihe von Schriften zur Anwendung von ITIL herausgegeben[40].

In ITIL wird dabei mit dem Service Management ein Querschnittsthema behandelt, das vom Beginn des Lebenszyklusses einer IT-Anwendung berücksichtigt werden muss. Dabei entstehen Synergien zum Vorgehen nach den anderen Standards, die in einer KBSt-Studie dargestellt werden[41].

Während der Erstellung von SAGA 4.0 ist die weiterentwickelte Version ITIL 3.0 erschienen. Um auf ein erprobtes Vorgehen zu setzen und auf deutschsprachige Literatur verweisen zu können, wird im Engineering Viewpoint (Kapitel 7) die durch KBSt-Dokumente unterstützte Version ITIL 2.0 vorgestellt[42].

Migrationsleitfaden

Ziel des Leitfadens[43] ist es, sowohl strategisch-wirtschaftliche als auch detaillierte technische Entscheidungshilfen bei einer geplanten oder gerade vollzogenen Migration zu bie-

37. siehe http://bundesrecht.juris.de/bitv/
38. siehe Abschnitte 4.5.3 auf Seite 49 und 8.6.1 auf Seite 108
39. siehe http://www.kbst.bund.de/v-modell
40. siehe http://www.kbst.bund.de/itil
41. siehe „ITIL und Standards für IT-Prozesse", Version 1.0.1, KBSt-Brief 1/2006, Oktober 2006
42. siehe Abschnitt 7.1 „IT-Service-Management mittels ITIL" auf Seite 81
43. siehe http://www.kbst.bund.de/migrationsleitfaden

ten. Im Fokus steht die Ablösung von proprietären Produkten sowohl durch Open-Source-Software (OSS) als auch – wo notwendig – durch nachfolgende Generationen von proprietären Produkten. Es werden behördenspezifische Szenarien erstellt und verschiedene Migrationsalternativen diskutiert.

Zur Erstellung des Migrationsleitfadens wurde bei den relevanten Berührungspunkten SAGA in der Version 2.1 berücksichtigt. Die Fortschreibung von SAGA hat keine Auswirkungen auf die getroffenen Aussagen.

DOMEA-Konzept

DOMEA[44] steht für Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang. Ziel des Konzepts ist die Einführung der elektronischen Akte. An die Stelle der Papierakten sollen künftig behördliche Geschäftsprozesse treten, die medienbruchfrei und vollständig elektronisch realisiert werden können. Hierbei gelten die gleichen rechtlichen und funktionalen Anforderungen wie bei Papierdokumenten. Seit der Veröffentlichung des Konzepts 1999 hat sich DOMEA zu einem Standard in der elektronischen Vorgangsbearbeitung in Bundes-, Landes- und auch Kommunalbehörden etabliert. Für Produkthersteller stellt das DOMEA-Konzept eine wesentliche Informationsquelle zur Ermittlung der Anforderungen der öffentlichen Verwaltung dar, die in die Weiterentwicklung der Produkte einfließen.

Das modular aufgebaute Konzept enthält neben dem Organisationskonzept und dem sich hieraus ergebenden Anforderungskatalog Erweiterungsmodule, die spezielle Themen des Organisationskonzepts vertieft darstellen.

Der Anforderungskatalog des DOMEA-Konzepts setzt die organisatorischen Erfordernisse in funktionale Anforderungen um. Diese orientieren sich einerseits an den SAGA-Standards und beeinflussen andererseits die Fortschreibung des SAGA-Dokuments. Für Software-Produkte aus dem Bereich der elektronischen Vorgangsbearbeitung beschreibt das DOMEA-Konzept die maßgeblichen Anforderungen. Diese gehen in einigen Punkten über die Anforderungen von SAGA hinaus, gefährden also nicht die SAGA-Konformität.

1.7 Der Evolutionsprozess

Normen, Standards und Architekturen in SAGA durchlaufen einen festgelegten Prozess für ihre Aufnahme:

a. Vorschlag der Normen, Standards und Architekturen in dem öffentlich zugänglichen Diskussionsforum, über das Kontaktformular, aus dem SAGA-Expertenkreis, der KoopA-SAGA-Projektgruppe, von zentralen IT-Dienstleistern des Bundes oder durch das SAGA-Autoren-Team
b. Sichtung der Vorschläge durch das SAGA-Autoren-Team
c. Diskussion der Normen, Standards und Architekturen, die vom SAGA-Autoren-Team als geeignet bewertet wurden, im SAGA-Expertenkreis

44. siehe http://www.kbst.bund.de/domea

d. Annahme der Vorschläge durch Beschluss der KBSt auf Grundlage der Diskussion von SAGA-Autoren-Team und SAGA-Expertenkreis
e. Einarbeitung der angenommenen Normen, Standards und Architekturen in SAGA durch das SAGA-Autoren-Team, sobald der Beschluss der KBSt vorliegt

SAGA wird in regelmäßigen Abständen fortgeschrieben, an neueste Entwicklungen und Erkenntnisse angepasst und auf den Homepages von KBSt[45] und E-Government-Handbuch[46] publiziert.

Sollten Problemstellungen auftreten, die durch bekannte Standards nicht gelöst werden können, werden Aufforderungen zu Vorschlägen (Request for Proposals – RFP) an den SAGA-Expertenkreis versandt, um mögliche Lösungsvorschläge zu ermitteln.

Öffentliches Diskussionsforum

In einem öffentlich zugänglichen Forum unter http://www.kbst.bund.de/saga-forum können sich Internetnutzer registrieren und die Anwendung und Weiterentwicklung von SAGA diskutieren. Die Ergebnisse der Diskussionen werden ausgewertet und bei Eignung in der nächsten Version des SAGA-Dokuments berücksichtigt.

Kontaktformular

Auf der SAGA-Homepage befindet sich ein Kontaktformular[47] für die Anwender von SAGA. Dort können Anregungen und Fragen strukturiert direkt an das SAGA-Autoren-Team gerichtet werden.

SAGA-Expertenkreis

Die KBSt hat einen Expertenkreis[48] mit Vertretern aus Wirtschaft, Wissenschaft und Verwaltung eingerichtet und beruft dessen Mitglieder. In regelmäßigen Abständen oder bei begründeten Anlässen wird die Expertenrunde in die Fortschreibung einbezogen.

KoopA-SAGA-Projektgruppe und zentrale IT-Dienstleister des Bundes

Vom KoopA ADV werden Vertreter aus Ländern und Kommunen entsandt, um in Workshops die Weiterentwicklung von SAGA zu begleiten. Das SAGA-Autoren-Team erstellt Fragenkataloge zu geplanten Änderungen, die von den Teilnehmern beantwortet und um eigene Vorschläge ergänzt werden. Analog zu diesem Vorgehen werden in Workshops und schriftlichem Austausch die Anforderungen zentraler IT-Dienstleister des Bundes erfasst und bei der Fortschreibung des Dokuments berücksichtigt.

SAGA-Rechenschaftsbericht

Die Vorschläge an das SAGA-Autoren-Team, die im öffentlichen Forum, im Kontaktformular, im SAGA-Expertenkreis, in der KoopA-SAGA-Projektgruppe und von zentralen IT-Dienstleistern des Bundes gemacht wurden, werden in einem SAGA-Rechenschaftsbe-

45. siehe http://www.kbst.bund.de/saga
46. siehe http://www.bsi.bund.de/fachthem/egov/3.htm
47. siehe http://www.kbst.bund.de/saga-kontaktformular
48. siehe http://www.kbst.bund.de/saga-expertenkreis

richt[49] aufgelistet und das Ergebnis der Prüfung dokumentiert. Annahme oder Ablehnung der Vorschläge werden begründet.

1.8 Aufbau des Dokuments

Kapitel 2 trifft Aussagen zum Geltungsbereich und zur Verbindlichkeit von SAGA. Weiterhin werden die Mindestanforderungen zur Offenheit von Standards sowie die Definitionen der verschiedenen Klassifikationen von Standards vorgestellt. Ebenso wird die Thematik der SAGA-Konformität von E-Government-Anwendungen behandelt.

Im Kapitel 3 folgt die Darstellung des Architekturmodells für E-Government-Anwendungen. Das Modell wurde auch für die Beschreibung des deutschen E-Government angewendet. Dementsprechend enthalten die nachfolgenden Kapitel 4 bis 8 Sichten (Viewpoints) des Architekturmodells auf das E-Government in seiner Gesamtheit:

a. Kapitel 4 dokumentiert Ziele des deutschen E-Government, Akteure, Rollen, Rahmenbedingungen, Richtlinien, Interaktionsformen sowie die Zielsetzungen bezüglich einheitlicher Prozesse (Enterprise Viewpoint).
b. In Kapitel 5 werden die Aktivitäten zur Definition einheitlicher Datenmodelle und Hilfestellungen für Entwickler von Datenmodellen beschrieben (Information Viewpoint).
c. Das Kapitel 6 enthält eine Referenz-Software-Architektur, aus der Architekturen für konkrete E-Government-Anwendungen entwickelt werden können, und Informationen zur Integration von Bausteinen, wie den Einer-für-Alle-Angeboten (EfA-Angeboten), in die Software-Architektur (Computational Viewpoint).
d. In Kapitel 7 werden für den Betrieb von E-Government-Anwendungen IT-Service-Management und die Anforderungen an E-Government-Rechenzentren beschrieben sowie die Nutzung von Bausteinen wie den EfA-Angeboten in einer bestehenden Infrastruktur dargestellt (Engineering Viewpoint).
e. In Kapitel 8 werden die Standards, Technologien und Methoden für die IT-Architektur und zur Erreichung von Datensicherheit festgelegt (Technology Viewpoint).

Der Anhang A enthält ein Literaturverzeichnis und im Anhang B werden die klassifizierten Standards aus dem Kapitel 8 alphabetisch aufgelistet. Im Anhang C befindet sich schließlich ein Verzeichnis der in SAGA verwendeten Abkürzungen.

49. siehe http://www.kbst.bund.de/saga

2 Grundlagen von SAGA

2.1 Geltungsbereich und Verbindlichkeit von SAGA

Bislang wurden ca. 400 Dienstleistungen der verschiedenen Verwaltungen des Bundes identifiziert. Die Dienstleistungen lassen sich z. B. nach ihren Zielgruppen[50] gruppieren, siehe Abbildung 2-1.

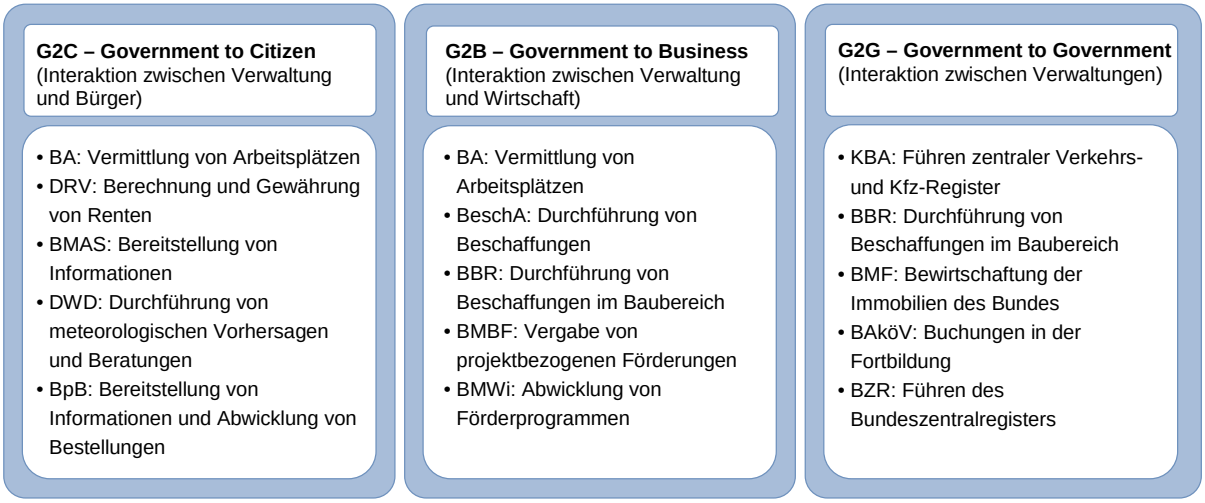


Abbildung 2-1: Ausgewählte Dienstleistungen des Bundes

Der Geltungsbereich von SAGA erstreckt sich auf die Bundesverwaltung und Software-Systeme mit Schnittstellen zwischen Bundesbehörden und Landes- beziehungsweise Kommunalbehörden, um die oben aufgezeigten Dienstleistungen zu unterstützen.

SAGA beinhaltet Empfehlungen zu Standards und Architekturen für E-Government-Anwendungen. Als E-Government-Anwendungen werden Software-Systeme bezeichnet, die zur Erfüllung von Dienstleistungen des Bundes eingesetzt werden oder die Erfüllung solcher Dienstleistungen aktiv unterstützen. Für Systeme, die keine direkten Schnittstellen zum E-Government haben, wird eine Migration empfohlen, wenn die Kosten-Nutzen-Betrachtung positiv ausfällt. Bei der Beschaffung von Standard-Software[51] sollten vorrangig Produkte oder Produktversionen gewählt werden, die zu den Empfehlungen von SAGA kompatibel sind. SAGA betrachtet hierbei nicht alle Elemente einer technischen Architektur, sondern nur Bereiche, die wesentlichen Einfluss auf die genannten Ziele[52] haben.

Das Bundesministerium des Innern empfiehlt, bei der Ausschreibung von E-Government-Anwendungen für die Bundesverwaltung SAGA so zu berücksichtigen, wie es in Abschnitt 2.4.1 „Definition der Konformität“ auf Seite 25 und Abschnitt 2.4.2 „SAGA-Konformität in der Ausschreibung“ auf Seite 26 beschrieben ist.

Die Bundesministerien regeln die Verbindlichkeit von SAGA in ihren Geschäftsbereichen.

50. siehe Abschnitt 4.6.2 „Beziehungen in Interaktionen“ auf Seite 52
51. Software, die lediglich installiert und konfiguriert wird
52. siehe Abschnitt 1.3 „Ziele“ auf Seite 12

2.2 Mindestanforderungen bezüglich der Offenheit von Standards

Ein Ziel von SAGA ist der Einsatz offener Standards in E-Government-Anwendungen, siehe Abschnitt 1.3 „Ziele“ auf Seite 12. Derzeit existieren eine Vielzahl von Definitionen für einen „Offenen Standard“, allerdings gibt es keine allgemein gültige, allseits akzeptierte Definition. Verschiedene Standardisierungsgremien haben Definitionen herausgegeben, die sich im Wesentlichen, was den Prozess der Entstehung eines Standards, dessen Dokumentation und Verwendung betrifft, gleichen. Umstritten sind jedoch Fragen zur Form der Standardisierungsorganisation und der Lizenzkostenregelung eines Standards. Diese werden in den verschiedenen Gremien (z. B. IDABC, ETSI, DIN, CEN, ISO) unterschiedlich bewertet. SAGA soll nicht zum Forum für diese Diskussionen werden, sondern eine praxisbezogene Empfehlung bleiben. Daher wurden „Mindestanforderungen“ an die Offenheit von Standards definiert, die auch künftig eine Bewertungsgrundlage für die Aufnahme oder Ablehnung eines Standards in SAGA darstellen.

Die Mindestanforderungen bezüglich der Offenheit von Standards zur Aufnahme in SAGA sind folgendermaßen definiert:

a. Der Standard wurde veröffentlicht und die Dokumentation der Standardspezifikation ist entweder kostenlos oder maximal gegen eine Schutzgebühr erhältlich.
b. Das geistige Eigentum (beispielsweise in Form von Patenten) am Standard oder an Teilen des Standards ist möglichst lizenzkostenfrei benutzbar.
c. Die Verwendung des Standards ist für die Bundesverwaltung und die Nutzer ihrer Dienstleistungen uneingeschränkt möglich.
d. Der Standard muss auch in Zukunft veröffentlicht und frei nutzbar bleiben.

2.3 Klassifizierung und Lebenszyklen von Standards

2.3.1 Klassifizierung in SAGA

Standards werden in drei Klassen eingeordnet. Konkurrierende Standards, die nicht aufgeführt sind, sollen nicht oder nur in Ausnahmefällen angewendet werden, siehe dazu auch Abschnitt 2.3.4 „Nicht-klassifizierte Standards“ auf Seite 25.

Unter Beobachtung:

Standards stehen unter Beobachtung, wenn sie der gewünschten Entwicklungsrichtung folgen, finalisiert sind und die Mindestanforderungen an die Offenheit von Standards erfüllen[53]. Gegebenenfalls haben sie sich aber noch nicht ausreichend in der Praxis bewährt oder erfüllen bislang nicht alle Ziele von SAGA, siehe Abschnitt 1.3 „Ziele“ auf Seite 12.

Wenn es neben den unter Beobachtung stehenden Standards keine konkurrierenden obligatorischen oder empfohlenen Standards gibt, können unter Beobachtung stehende Standards in E-Government-Anwendungen eingesetzt werden. Nur in begründeten Ausnah-

53. siehe Abschnitt 2.2 „Mindestanforderungen bezüglich der Offenheit von Standards“ auf Seite 20

men sind unter Beobachtung stehende Standards höher klassifizierten Alternativen vorzuziehen.

Empfohlen:

Standards werden empfohlen, wenn sie sich in der Praxis bewährt haben, es aber einen noch geeigneteren obligatorischen Standard gibt beziehungsweise sie nicht alle Ziele von SAGA erfüllen. Es müssen jedoch die Mindestanforderungen an die Offenheit von Standards erfüllt werden und Investitionssicherheit gegeben sein.

Wenn es neben empfohlenen Standards keine konkurrierenden obligatorischen Standards gibt, sollte von den empfohlenen Standards nur in begründeten Ausnahmen abgewichen werden.

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

Obligatorisch:

Standards sind obligatorisch, wenn sie sich in der Praxis bewährt haben und die bevorzugte Lösung darstellen. Sie sind am Markt etabliert und erfüllen alle Ziele von SAGA. Diese Standards sind vorrangig zu beachten und anzuwenden.

Konkurrierende Standards können nebeneinander obligatorisch sein, wenn sich die Anwendungsschwerpunkte deutlich unterscheiden. In solchen Fällen ist der für die jeweilige Anwendung am besten geeignete Standard zu verwenden.

Wenn obligatorische und empfohlene oder unter Beobachtung stehende Standards nebeneinander existieren, sollten die letztgenannten nur in begründeten Ausnahmefällen angewendet werden.

Eine obligatorische Klassifikation bedeutet nicht, dass der Standard in jeder E-Government-Anwendung einzusetzen ist. Nur wenn aus den Anforderungen der Anwendung heraus der Einsatz der mit dem Standard verbundenen Technologie oder Funktionalität erforderlich oder sinnvoll ist, sollte der jeweilige obligatorische Standard verwendet werden.

2.3.2 Erweiterte Klassifizierung von Standards

Auf der SAGA-Homepage unter http://www.kbst.bund.de/saga-standards wurden mit dem Erscheinen von SAGA 2.0 drei Listen zur erweiterten Klassifizierung von Standards eingeführt. Lediglich die Standards auf der Bestandsschutzliste (ehemals Grey List) dürfen den im SAGA-Dokument klassifizierten Standards (Obligatorisch, Empfohlen, Unter Beobachtung) vorgezogen werden – allerdings nur bei Erweiterungen bestehender Systeme, bei denen diese Standards bereits im Einsatz sind.

Vorschlagsliste

Die Vorschlagsliste (ehemals White List) wurde geschaffen, um zeitnah auf neue Entwicklungen reagieren und um diese zur Kenntnisnahme extern kommunizieren zu können. Bei der Weiterentwicklung des SAGA-Dokuments ist die Vorschlagsliste eine wichtige Grundlage zur Aufnahme von Standards in SAGA.

Standards werden in der Vorschlagsliste geführt, wenn sie als Anregungen und Ideen zur Aufnahme in SAGA an das SAGA-Autoren-Team herangetragen wurden, Potenzial für den Einsatz in E-Government-Anwendungen haben und noch nicht weitergehend klassifiziert wurden.

Standards in der Vorschlagsliste werden durch das SAGA-Autoren-Team und den SAGA-Expertenkreis beurteilt. Ergebnis der Beurteilung kann eine Aufnahme der Standards in der nächsten Version des SAGA-Dokuments, die Verschiebung auf die Negativliste (ehemals Black List) oder Bestandsschutzliste (ehemals Grey List) oder aber auch der Verbleib auf der Vorschlagsliste sein, um die weitere Entwicklung, z. B. bei noch nicht finalisierten Standards, zu beobachten. Die Standards auf der Vorschlagsliste werden vor der Veröffentlichung einer neuen SAGA-Version erneut bezüglich ihrer Eignung zur Aufnahme geprüft.

Bestandsschutzliste

Standards werden in die Bestandsschutzliste (ehemals Grey List) aufgenommen, wenn sie in der aktuellen SAGA-Version nicht mehr geführt, in einer vorangegangenen SAGA-Version aber mit dem Status „Empfohlen“ oder „Obligatorisch“ klassifiziert wurden beziehungsweise in der Vergangenheit am Markt eine große Verbreitung hatten. Bei der Erweiterung bestehender Systeme stehen diese Standards unter Bestandsschutz und können weiterhin eingesetzt werden. Für neue E-Government-Anwendungen sollen diese Standards jedoch nicht mehr zum Einsatz kommen.

Negativliste

Im Rahmen der Diskussion von SAGA werden bestimmte in der Vergangenheit bereits abgelehnte Standards immer wieder für die Aufnahme vorgeschlagen. Um die Ergebnisse dieser Diskussionen transparent zu machen und um zu informieren, für welche Standards eine Aufnahme in SAGA nicht mehr zu erwarten ist, wurde die Negativliste (ehemals Black List) eingerichtet.

Standards werden in der Negativliste geführt, wenn sie durch das SAGA-Autoren-Team und den SAGA-Expertenkreis erfasst und abgewiesen wurden. Die Standards sollten in neuen sowie in bestehenden E-Government-Anwendungen nicht eingesetzt werden. Der Einsatz ist nur dann zulässig, wenn eine parallele SAGA-konforme Lösung existiert. Zum Beispiel können Bilder im BMP-Format zur Verfügung gestellt werden, obwohl es auf der Negativliste steht, wenn gleichzeitig die Bilder auch in einem SAGA-konformen Format wie GIF angeboten werden.

Wenn ein in der Negativliste geführter Standard weiterentwickelt wird und sich in den kritisierten Punkten von der alten Version unterscheidet, muss die Versionsnummer des Standards angegeben werden, für die eine Aufnahme in die Negativliste erfolgt ist. Für die neu-

ere Version steht dann der Weg zur Aufnahme in SAGA über die Vorschlagsliste (ehemals White List) offen.

2.3.3 Lebenszyklen von Standards

Neben den in SAGA klassifizierten Standards, siehe Abschnitt 2.3.1 auf Seite 20, werden weitere Standards in drei verschiedenen Listen geführt, siehe Abschnitt 2.3.2 auf Seite 21. Während die Einordnung von Standards in die Klassifikationen „Obligatorisch", „Empfohlen" und „Unter Beobachtung" im SAGA-Dokument festgehalten und fortgeschrieben wird, erfolgt die Darstellung und laufende Pflege der Standards in den Listen auf der SAGA-Homepage unter http://www.kbst.bund.de/saga-standards.

Standards können in ihrem Lebenszyklus verschiedene Stadien durchlaufen. Diese werden im Überblick in Abbildung 2-2 auf Seite 24 dargestellt.

Die Übergänge eines Standards zwischen den Listen der SAGA-Homepage unter http://www.kbst.bund.de/saga-standards und den Klassen im SAGA-Dokument werden nachfolgend definiert.

1 Neue Standards werden vom SAGA-Autoren-Team, von Experten oder von Anwendern zur Klassifizierung eingebracht, siehe dazu auch Abschnitt 1.7 „Der Evolutionsprozess" auf Seite 16. Ohne eine vertiefte Prüfung werden diese Standards zunächst in der Vorschlagsliste gesammelt. Vor der Erstellung einer neuen SAGA-Version findet eine gründliche Prüfung statt. Neben dem Verschieben in das SAGA-Dokument, in die Bestandsschutzliste oder in die Negativliste kann auch der Verbleib in der Vorschlagsliste ein Prüfergebnis sein. Solche Standards erfüllen die Anforderungen für eine Aufnahme in SAGA noch nicht, z. B. weil sie noch nicht finalisiert sind. Für die nächste SAGA-Version wird ihre Aufnahme erneut geprüft. Vor der Fertigstellung einer neuen SAGA-Version können die Übergänge 1 und 2 beziehungsweise 1 und 3 auch in einem Schritt durchlaufen werden.

2 Standards, die nach erfolgter Prüfung keinen Eingang in SAGA erhalten, werden in der Negativliste als abgewiesene Standards geführt.

3 Standards der Vorschlagsliste, die nach eingehender Prüfung in neuen Projekten nicht eingesetzt werden sollten, jedoch in bestehenden Projekten noch genutzt werden könnten, werden in die Bestandsschutzliste verschoben.

4 Nach einer positiven Prüfung der entsprechenden Anforderungen, siehe dazu Abschnitt 2.3.1 „Klassifizierung in SAGA" auf Seite 20, werden Standards in SAGA mit der Klassifikation „Unter Beobachtung" aufgenommen. Werden die jeweiligen Anforderungen erfüllt, kann der Standard auch direkt einer der höheren Klassen „Empfohlen" oder „Obligatorisch" zugeordnet werden. Die Übergänge 4 und 5 beziehungsweise 4, 5 und 6 werden dann in einem Schritt durchlaufen.

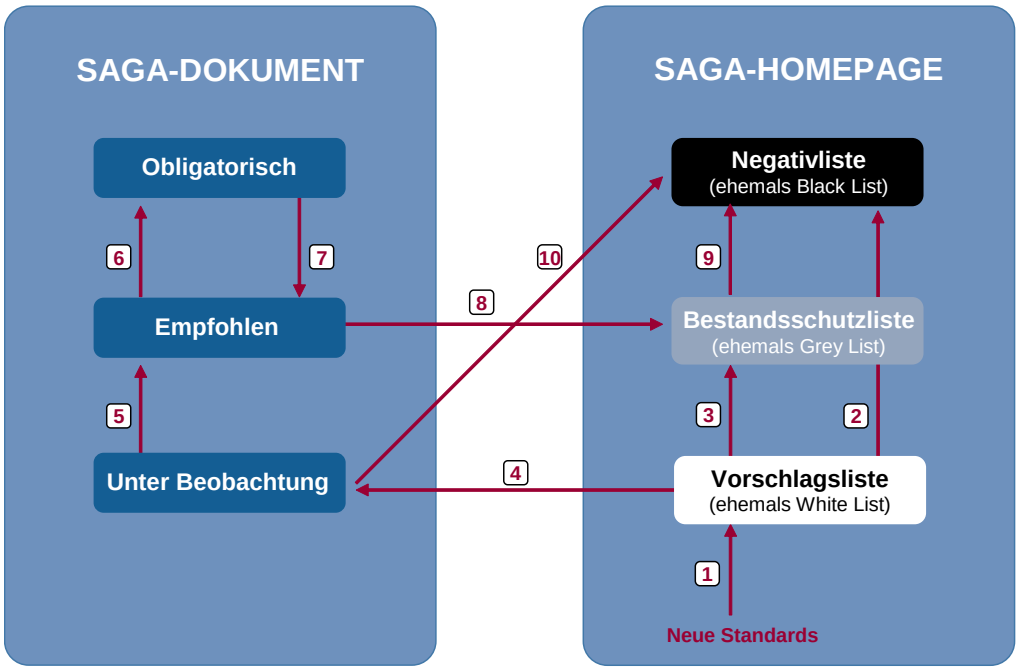


Abbildung 2-2: Lebenszyklen von SAGA-Standards

5 Standards mit dem Status „Unter Beobachtung“ werden nach einer erfolgreichen Prüfung der entsprechenden Anforderungen in SAGA als „Empfohlen“ klassifiziert. Werden die Voraussetzungen dafür erfüllt, kann der Standard auch direkt der höheren Klasse „Obligatorisch“ zugeordnet werden. Die Übergänge 5 und 6 werden dann in einem Schritt durchlaufen. Standards, die nach erfolgter Prüfung die Anforderungen für eine Höherklassifizierung in SAGA noch nicht erfüllen und nicht auf die Negativliste verschoben werden sollen, behalten die Klassifikation „Unter Beobachtung“ bei.

6 Standards mit dem Status „Empfohlen“ werden nach einer erfolgreichen Prüfung der entsprechenden Anforderungen in SAGA als „Obligatorisch“ klassifiziert. Standards, die nach erfolgter Prüfung die Anforderungen für eine Höherklassifizierung in SAGA noch nicht erfüllen und nicht auf die Bestandsschutzliste verschoben werden sollen, behalten die Klassifikation „Empfohlen“ bei.

7 Standards mit dem Status „Obligatorisch“ werden nach einer Prüfung und der entsprechenden Neubewertung in SAGA als „Empfohlen“ klassifiziert. Soll der Standard in neuen Projekten nicht mehr zum Einsatz kommen, kann er auch sofort in die Bestandsschutzliste verschoben werden. Die Übergänge 7 und 8 werden dann in einem Schritt durchlaufen. Standards, die nach erfolgter Prüfung die Anforderungen für die Klassifikation „Obligatorisch“ weiterhin erfüllen, behalten ihren Status bei.

8 Wenn Standards mit dem Status „Empfohlen“ nach eingehender Prüfung in neuen Projekten nicht mehr eingesetzt werden sollten, werden sie auf die Bestandsschutzliste verschoben.

9 Veraltete Standards, die ausreichend lange in der Bestandsschutzliste geführt wurden und keinen weiteren Bestandsschutz genießen sollen, werden in die Negativliste überführt.

10 Standards mit dem Status „Unter Beobachtung“, die keine Aussicht mehr haben, jemals eine höhere Klassifikation zu erhalten, werden direkt in die Negativliste verschoben.

Die Standards, die im Rahmen der Erstellung einer neuen SAGA-Version geprüft werden, können somit nicht nur einen Schritt des zuvor vorgestellten Lebenszyklus gehen, sondern auch in ihrem Status verharren oder gleich mehrere Übergänge absolvieren.

2.3.4 Nicht-klassifizierte Standards

In SAGA nicht aufgeführte Standards oder Architekturen sind

a. nicht spezifisch für E-Government- oder E-Commerce-Anwendungen,
b. auf eine andere Detailebene bezogen als die hier in SAGA aufgeführten Standards,
c. in genannten Standards inbegriffen oder werden durch genannte Standards referenziert,
d. zu neu oder zu umstritten, um verlässlich die baldige Etablierung als Standard voraussetzen zu können oder
e. nicht gewünscht, weil sie mit vorgestellten Standards oder Architekturen konkurrieren oder die Interoperabilität einschränken.

2.4 SAGA-Konformität

2.4.1 Definition der Konformität

Die SAGA-Konformität einer E-Government-Anwendung[54] wird anhand der in SAGA beschriebenen Modelle, Verfahren und Standards beurteilt:

a. Berücksichtigung standardisierter Prozessmodelle
b. Berücksichtigung standardisierter Datenmodelle
c. Einhaltung der in SAGA beschriebenen technischen Standards und Architekturen
d. Nutzung verwertbarer Einer-für-Alle-Angebote (EfA-Angebote)[55]

Um eine umfassende Aussage über die SAGA-Konformität einer E-Government-Anwendung insbesondere bei der Umsetzung komplexer Fachverfahren zu ermöglichen, sollte eine Anwendung für die Konformitätsaussage zunächst in einzelne Einheiten[56] untergliedert werden. Hier wird zwischen eigenentwickelten Software-Einheiten und nicht eigenentwickelten externen Einheiten (Produkte) unterschieden. Zur Beurteilung der SAGA-Kon-

54. E-Government-Anwendung wird als Überbegriff für jegliche IT-Systeme gebraucht, die E-Government-Dienstleistungen des Bundes erbringen. Für die Definition des Begriffs E-Government-Dienstleistung siehe Abschnitt 4.1.2 auf Seite 37.
55. siehe Abschnitt 6.3.6 „Wiederverwendung und Integration von EfA-Angeboten“ auf Seite 78
56. Nach dem V-Modell XT ist eine Einheit das in der Hierarchie am weitesten oben stehendes Systemelement, siehe http://www.v-modell-xt.de/.

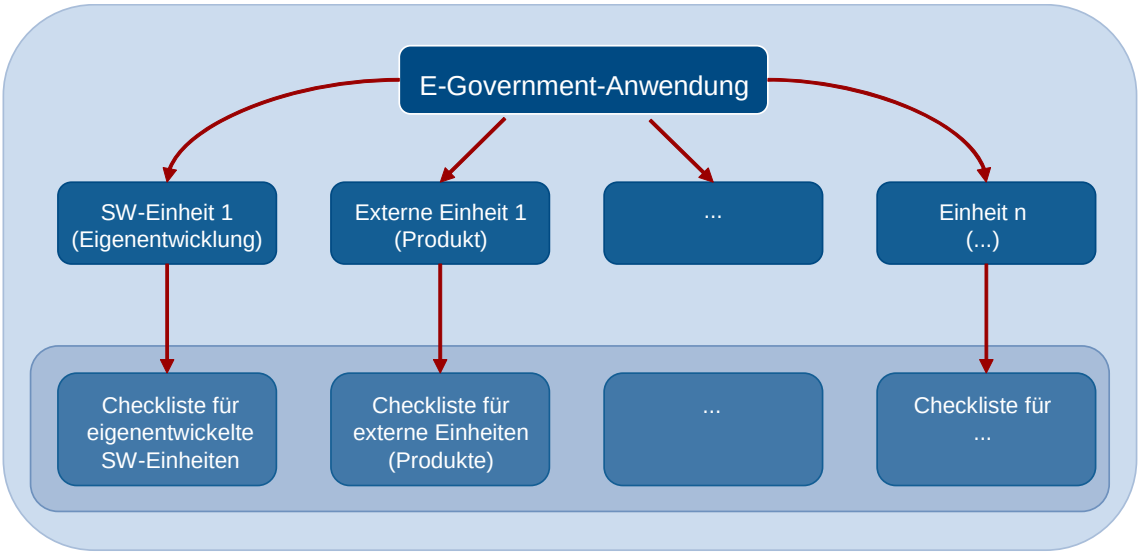


Abbildung 2-3: Aufbau SAGA-Konformitätserklärung und Checklisten

formität von Produkten wird vor allem Wert auf Kommunikationsschnittstellen, Datenaustauschformate und Sicherheit gelegt. Für Eigenentwicklungen sind zusätzlich die Technologien zur Modellierung und Implementierung der Anwendung sowie der Einsatz von EfA-Angeboten relevant.

Auf der SAGA-Homepage werden eine leere und eine beispielhaft ausgefüllte Konformitätserklärung mit Checklisten für Software-Einheiten und externe Einheiten zur Verfügung gestellt[57]. Die Checklisten enthalten die Themenbereiche, die jeweils für Eigenentwicklungen oder Produkte von Belang sind.

Welche konkreten Standards aus den relevanten Themenbereichen für die Erfüllung der SAGA-Konformität zum Einsatz kommen müssen, variiert je nach Einsatzgebiet und Funktionsumfang der Anwendung. Zum Beispiel spielen die Festlegungen, um Informationsangebote für Mobiltelefone beziehungsweise PDAs zu erstellen, nur dann für die SAGA-Konformität eine Rolle, wenn diese Endgeräte von der E-Government-Anwendung bedient werden sollen. SAGA-Konformität wird deshalb durch den Einsatz der Teilmenge aller SAGA-Standards erreicht, die für die jeweilige E-Government-Anwendung relevant ist.

2.4.2 SAGA-Konformität in der Ausschreibung

Um bei der Frage der SAGA-Konformität die konkreten Anforderungen des Auftraggebers nicht zu vernachlässigen und um nicht ausschließlich auf Aussagen des Auftragnehmers angewiesen zu sein, sollte der Auftraggeber eine Kriteriengruppe „SAGA-Konformität“ beziehungsweise SAGA-relevante Kriterien in seine Verdingungsunterlagen aufnehmen.

Eine pauschale Forderung nach SAGA-Konformität trägt nicht zur Erreichung der Ziele von SAGA bei. Die pauschale Forderung lässt aufgrund der Komplexität des Dokuments immer Spielraum für Interpretationen und Missverständnisse. Dies erschwert es dem Auftragnehmer, die Anforderungen zu erfüllen, und dem Auftraggeber, die Erfüllung der Anforderungen zu kontrollieren.

57. siehe http://www.kbst.bund.de/saga-konformitaet

Die pauschale Forderung nach SAGA-Konformität darf deshalb nicht gestellt werden.

Stattdessen sollte der im Folgenden erläuterte Prozess der Konformitätserklärung von Auftraggeber und Auftragnehmer durchlaufen werden, siehe Abbildung 2-4. Durch ihn werden Interpretationsspielräume eingeschränkt und Missverständnisse reduziert. Die konkreteren Forderungen sind überprüfbar und schaffen dadurch Vertragssicherheit zwischen Auftraggeber und Auftragnehmer. Durch die Konkretisierung der Anforderungen wird außerdem vermieden, dass Angebote ungewollt teuer ausfallen.

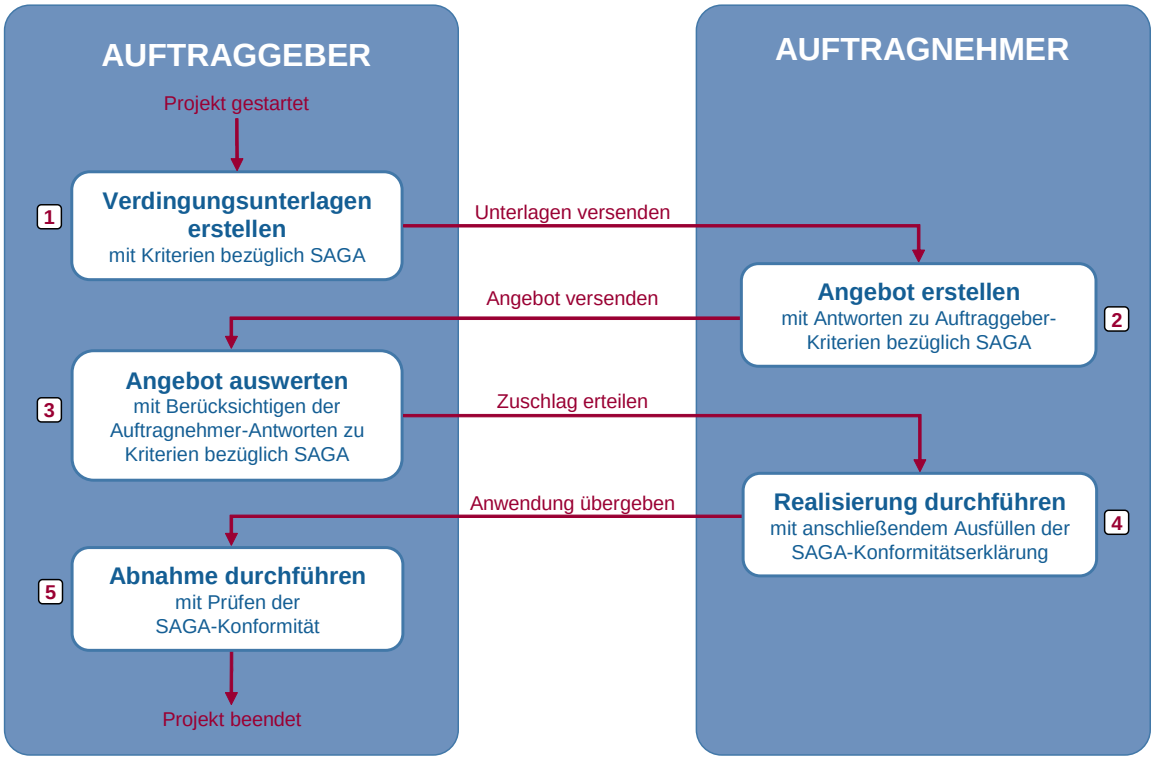


Abbildung 2-4: Prozess zur SAGA-Konformitätserklärung

Der Prozess besteht im Wesentlichen aus fünf Schritten, die nachfolgend kurz beschrieben werden:

Schritt 1: Aufnahme der SAGA-Konformitätsaspekte in die Verdingungsunterlagen einer Ausschreibung

Der Auftraggeber stellt eine Reihe von Ausschluss- und Bewertungskriterien zusammen, die alle relevanten Aspekte der gewünschten Anwendung abdecken. Als Vorlage kann die Beispiel-Kriteriengruppe dienen, die auf der SAGA-Homepage zum Download bereit steht[58]. Diese Beispiel-Kriteriengruppe enthält mögliche Kriterien, die sich aus der Anwendung von SAGA ergeben können. Der Auftraggeber muss daraus diejenigen Kriterien auswählen oder ergänzen, die für das Projekt relevant sind. Die Beispiel-Kriteriengruppe enthält erklärende Hinweise, die die Auswahl erleichtern.

Auch die Entscheidung, ob Kriterien als Ausschluss- oder Bewertungskriterien festgelegt werden, sind vom Auftraggeber zu treffen. Ausschlusskriterien sollten sehr zurückhaltend

58. siehe http://www.kbst.bund.de/saga-konformitaet

eingesetzt werden, da sie die Anzahl der Angebote reduzieren. Alternativ sollten hoch gewichtete Bewertungskriterien in Betracht gezogen werden.

Schritt 2: Beantwortung der Kriteriengruppe SAGA-Konformität durch den Auftragnehmer im Rahmen der Angebotserstellung

Der Auftragnehmer beantwortet im Rahmen seiner Angebotserstellung die Kriteriengruppe „SAGA-Konformität". Er kann sich an einer ausgefüllten Beispiel-Kriteriengruppe orientieren, die ebenfalls auf der SAGA-Homepage zum Download bereit steht[59]. Diese Kriteriengruppe ist beispielhaft ausgefüllt und enthält erklärende Kommentare, die beim Ausfüllen einer konkreten Kriteriengruppe helfen.

Schritt 3: Prüfung der Angaben zur SAGA-Konformität durch den Auftraggeber, Bewertung der entsprechenden Kriterien im Rahmen der Angebotsauswertung

Der Auftraggeber prüft die ausgefüllten Kriteriengruppen der eingegangenen Angebote. Angebote, die für die Kriteriengruppe „SAGA-Konformität" nicht die Anforderungen des Auftraggebers erfüllen, d. h. die SAGA-Konformität nicht zusichern können, werden entsprechend bewertet.

Schritt 4: Ausfüllen der Konformitätserklärung für die realisierte Anwendung durch den Auftragnehmer

Hat der Auftragnehmer die E-Government-Anwendung realisiert, erklärt er schriftlich deren SAGA-Konformität. Dazu füllt er die Konformitätserklärung für die Anwendung aus und fügt die Checklisten für die einzelnen Einheiten der Anwendung als Anlagen bei. Abweichungen von den Zusagen der ausgefüllten Kriteriengruppe „SAGA-Konformität" sollten frühzeitig mit dem Auftragnehmer abgestimmt werden und sind in der Konformitätserklärung zu begründen. Unterstützung erhält der Auftragnehmer durch die Beispiel-Konformitätserklärung, die auf der SAGA-Homepage zum Download bereit steht[60]. Auch leere Vorlagen einer Konformitätserklärung stehen dort zur Verfügung.

Schritt 5: Prüfung der SAGA-Konformität anhand von Angebot und Konformitätserklärung durch den Auftraggeber im Rahmen der Abnahme

Auf der Grundlage der vom Auftragnehmer im Angebot ausgefüllten Kriteriengruppe „SAGA-Konformität" und der nach der Realisierung erstellten Konformitätserklärung kann der Auftraggeber die SAGA-Konformität während der Abnahme beurteilen. Durch die konkreten Vorgaben des Angebots ist diese Beurteilung leicht möglich. Erkannte Abweichungen der Anwendung von den Zusagen des Angebots stellen gegebenenfalls einen Mangel dar, der bei der Abnahme zu berücksichtigen ist.

2.4.3 SAGA-Konformität trotz niedriger Klassifikation

Eine SAGA-konforme Anwendung muss nicht zwangsläufig nur mit Technologien realisiert worden sein, die in SAGA die Klassifikation „Obligatorisch" erhalten haben. Aus verschiede-

59. siehe http://www.kbst.bund.de/saga-konformitaet
60. siehe http://www.kbst.bund.de/saga-konformitaet

nen Gründen ist auch der Einsatz von Standards mit niedrigerer Klassifikation (oder auch ohne Klassifikation in SAGA) möglich, ohne die SAGA-Konformität zu verletzen[61].

Fehlende Alternativen

Der Einsatz empfohlener Standards ist SAGA-konform, wenn es keine obligatorische Alternative gibt. Ebenso können unter Beobachtung stehende Standards SAGA-konform eingesetzt werden, wenn für den jeweiligen Einsatzzweck keine obligatorischen oder empfohlenen Standards in SAGA geführt werden.

Spezielle Funktionen und Anwendungsgebiete

Werden in SAGA zu einem Einsatzgebiet neben höher klassifizierten Standards („Obligatorisch" oder „Empfohlen") Standards mit niedrigerer Klassifikation geführt („Empfohlen" oder „Unter Beobachtung"), ist der Beschreibung der Standards zu entnehmen, unter welchen Voraussetzungen die niedriger klassifizierten Standards vorgezogen werden können. Gründe dafür sind vor allem ein benötigter erweiterter Funktionsumfang[62] oder spezielle Anwendungsgebiete[63]. Der Einsatz von Standards „Unter Beobachtung" sollte besonders gründlich abgewogen werden, da für sie keine Investitionssicherheit festgestellt wurde und kein Bestandsschutz zugesichert wird. Bereits mit der nächsten SAGA-Version können solche Standards in der Negativliste (ehemals Black List) geführt werden.

Parallele Angebote

Wenn entsprechend der vorherigen Ausführungen SAGA-konforme Standards verwendet werden, können *zusätzlich* Standards beziehungsweise Formate eingesetzt werden, die SAGA nicht oder in geringerer Klassifikation aufführt. Werden beispielsweise Daten für Tabellenkalkulationen[64] im CSV-Format angeboten, können dieselben Daten zusätzlich auch in anderen Formaten, wie Microsoft Excel, zur Verfügung gestellt werden, ohne die SAGA-Konformität zu verletzen.

Einsatz von externen Einheiten (Produkten)

Für externe Einheiten (in Abgrenzung zu eigenentwickelten Software-Einheiten) wird der Schwerpunkt auf Kommunikationsschnittstellen, Datenaustauschformate und Sicherheit gelegt. Technologien zur Prozessmodellierung, Datenmodellierung, Applikationsarchitektur und die Verwendung von EfA-Angeboten[65] sind nicht Bestandteil der Checklisten zur SAGA-Konformitätserklärung. Für konkrete Einheiten sollten Auftraggeber prüfen, ob sie in Ausschreibungen gegebenenfalls trotzdem entsprechende Technologien fordern, um z. B. vorhandene Infrastrukturen für den Betrieb der Einheit zu nutzen und um Synergien mit anderen E-Government-Anwendungen zu erzielen.

61. siehe dazu auch die Definitionen der Klassifikationen und Listen im Web im Abschnitt 2.3 auf Seite 20
62. siehe z. B. die Beschreibungen zu den verschiedenen PDF-Version im Abschnitt 8.6.7.1 auf Seite 112
63. siehe z. B. die Beschreibungen der Unicode-Kodierungen im Abschnitt 8.6.2 „Zeichensätze" auf Seite 108
64. siehe Abschnitt 8.6.7.4 „Formate für Tabellenkalkulationen zur Weiterbearbeitung" auf Seite 114
65. siehe Abschnitt 6.3.6 „Wiederverwendung und Integration von EfA-Angeboten" auf Seite 78

Technologien außerhalb des Fokus von SAGA

Themen, zu denen SAGA (noch) keine Aussagen trifft, berühren selbstverständlich nicht die Beurteilung der SAGA-Konformität einer E-Government-Anwendung.

2.4.4 Verantwortung für Konformität

Die Verantwortung für die Konformität von E-Government-Anwendungen zu SAGA liegt bei der für eine E-Government-Anwendung fachlich zuständigen Behörde. Es obliegt auch den jeweiligen Behörden zu überprüfen, wie Fachanwendungen migriert werden können.

Die Bundesministerien regeln die Verantwortlichkeit in ihren Geschäftsbereichen.

Aufgrund der Komplexität von SAGA ist auch der Prozess zur Sicherstellung von SAGA-Konformität komplex. Daher wird angestrebt, die Anwender in Zukunft noch besser zu unterstützen. Informationen über aktuelle Entwicklungen in diesem Bereich werden über die SAGA-Homepage des Bundesministerium des Innern[66] zur Verfügung gestellt.

2.4.5 Migration zur Konformität

Übergangsphase

SAGA wird kontinuierlich weiterentwickelt und regelmäßig fortgeschrieben, um stets an neue Anforderungen angepasst werden zu können. Deshalb können einzelne E-Government-Anwendungen, die sich an einer älteren SAGA-Version[67] orientieren, vorübergehend nicht zur aktuellen SAGA-Version konform sein.

Für nicht konforme Anwendungen sollten Migrationspläne entwickelt werden, wenn eine Kosten-Nutzen-Betrachtung positiv ausfällt. Dies wird möglicherweise erst bei wesentlichen Weiterentwicklungen der Anwendungen der Fall sein.

Maßnahmen zur Erzielung von Konformität

Die Konformität zu SAGA wird durch folgende Maßnahmen gefördert:

a. SAGA wird frühzeitig in Projektplanungen einbezogen.
b. Die SAGA-Konformität wird bei der Genehmigung von Projekten gefordert und überprüft.
c. Bei Förderung von Projekten durch öffentliche Verwaltungen kann die Konformität zu SAGA verbindlich gefordert werden.
d. SAGA-Konformität wird bei der Vergabe von Aufträgen verbindlich gefordert.

2.4.6 Nicht-Konformität

E-Government-Anwendungen, die ganz oder in Teilen nicht konform zu SAGA sind, unterliegen folgenden Restriktionen:

a. Die Nutzung von Einer-für-Alle-Angeboten (EfA-Angeboten)[68] kann eingeschränkt sein.

66. siehe http://www.kbst.bund.de/saga-konformitaet
67. alte Versionen von SAGA sind im SAGA-Archiv unter http://www.kbst.bund.de/saga abrufbar

b. Die Beratung durch Kompetenzzentren ist eingeschränkt oder nicht möglich.
c. Schnittstellen zu diesem System können gegebenenfalls nicht bedient werden.
d. Eine Förderung durch öffentliche Verwaltungen ist in der Regel nicht möglich.

68. siehe Abschnitt 6.3.6 „Wiederverwendung und Integration von EfA-Angeboten“ auf Seite 78

3 Architekturmodell für E-Government-Anwendungen

3.1 Überblick

Mit dem Architekturmodell verbindet SAGA folgende Ziele:

a. Zur Erleichterung der Kommunikation soll ein gemeinsames Verständnis aktueller IT-Architekturen, IT-Technologien und E-Government-Strukturen erreicht werden.

b. Für E-Government verfügbare IT-Technologien sollen mit diesem Modell erfasst, verglichen, nach Relevanz bewertet und einheitlich strukturiert werden.

c. Bei der Realisierung von E-Government-Projekten soll auf einheitliche Standards zurückgegriffen werden können.

Um komplexe, verteilte E-Government-Anwendungen zu beschreiben, bietet sich das Referenzmodell für offene, verteilte Datenverarbeitung (RM-ODP[69]) an, das als ISO/IEC 10746-3:1996 normiert wurde. Die Betrachtung der Anwendung wird in verschiedene Sichtweisen (Viewpoints) zerlegt und so die Komplexität der Gesamtarchitektur reduziert, was die leichtere Verständlichkeit und Beherrschbarkeit einer Anwendung ermöglicht. Die Basis von RM-ODP ist das objektorientierte Paradigma[70]. Objektorientiertheit fördert klare Strukturen, Wiederverwendbarkeit und Wartbarkeit der geschaffenen Modelle und des Systems.

Das RM-ODP-Modell definiert fünf Sichtweisen auf ein System, siehe Abbildung 3-1:

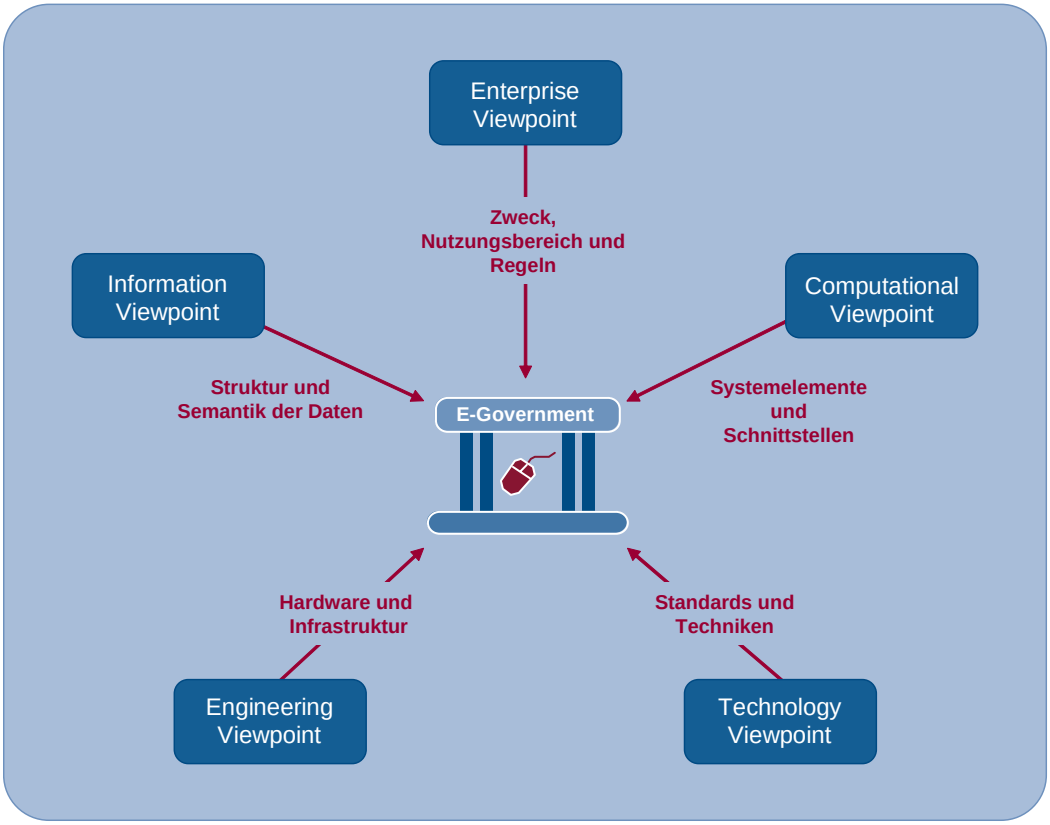


Abbildung 3-1: Viewpoints gemäß RM-ODP

69. Reference Model of Open Distributed Processing, siehe [ISO 1996]
70. siehe [KBSt 2007], Abschnitt 3.3.1

a. Der Enterprise Viewpoint spezifiziert Zweck, Nutzungsbereich und Regeln einer Anwendung.
b. Der Information Viewpoint beschreibt die Struktur und Semantik der zu verarbeitenden Daten, also das Datenmodell.
c. Der Computational Viewpoint stellt die Zerlegung einer Anwendung in funktionale Elemente und deren Interaktionsschnittstellen dar.
d. Der Engineering Viewpoint stellt die Verteilung der einzelnen Elemente des Systems auf physikalische Ressourcen sowie deren Verbindungen dar.
e. Der Technology Viewpoint beschreibt die zur Realisierung des Systems verwendeten Technologien.

Mit Hilfe der fünf Sichten können sowohl existierende Systeme beschrieben werden, als auch neue Systeme und Anwendungen modelliert werden. Der Einsatz von RM-ODP zur Beschreibung von E-Government-Anwendungen wird von SAGA nahe gelegt, jedoch nicht gefordert.

Darüber hinaus wird das SAGA-Dokument selbst nach dem RM-ODP-Modell strukturiert. So sind Kapitel entstanden, die jeweils einem Viewpoint zuzuordnen sind, siehe Abschnitt 1.8 „Aufbau des Dokuments“ auf Seite 18.

3.2 Enterprise Viewpoint

Der Enterprise Viewpoint für E-Government-Anwendungen beinhaltet zwei grundlegende Elemente: die organisatorische Struktur von E-Government allgemein und die organisatorischen Modelle der Anwendung. Hier wird die Gesamtumgebung für das System und sein Zweck beschrieben. Außerdem werden die Anforderungen an das System, zu erfüllende Rahmenbedingungen, ausführbare Aktionen und Richtlinien aus Sicht der Organisation oder des Unternehmens definiert. Dabei werden die Verfahren, deren Regeln und die an den Verfahren beteiligten Akteure in ihren Rollen festgelegt.

Die Effizienz der Informationstechnologie hängt wesentlich von einer ganzheitlichen Betrachtung ab. Das heißt, dass man nicht die Informationstechnologie in den Vordergrund stellt, sondern zuvorderst die fachliche Anwendung als Prozess betrachtet und beschreibt.

Dienstleistungen sind in Form von fachlichen Prozessmodellen zu beschreiben. Hierfür sollen von der Anfrage des „Kunden“ (Bürger, Wirtschaft, andere Behörde etc.) bis zur Leistungserbringung alle Arbeitsschritte betrachtet werden. Diese Prozessmodelle sollen in einer ersten Entwicklungsstufe auf einem relativ abstrakten Niveau verbleiben.

Neue Vorschläge zu Prozessdefinitionen sollen immer auf

a. Wiederverwendbarkeit,
b. Einfachheit und
c. Abbildbarkeit durch bereits vorhandene Prozessdefinitionen

überprüft werden. Zur Unterstützung der Verantwortlichen bei der Prozessmodellierung wird auf der Homepage der KBSt ein Leitfaden zur Prozess- und Datenmodellierung[71] bereitgestellt. Weiterhin kann z. B. das in der Bundesstelle für Informationstechnik (BIT)

angesiedelte Kompetenzzentrum Vorgangsbearbeitung, Prozesse und Organisation (CC VBPO)[72] Unterstützung leisten.

Das Kapitel 4 „Enterprise Viewpoint: Grundlagen E-Government“ auf Seite 37 beschreibt modellhaft den Enterprise Viewpoint auf das deutsche E-Government. SAGA stellt im Abschnitt 8.2 „Prozessmodelle“ auf Seite 97 Beschreibungsmittel zur Definition des Enterprise Viewpoint für konkrete E-Government-Anwendungen zur Verfügung.

3.3 Information Viewpoint

Dieser Viewpoint legt die Struktur und Semantik der Informationen des Systems fest. Darüber hinaus wird festgelegt, welche Aktivitäten (Statusänderungen) mit den Informationsobjekten durchgeführt werden können und welchen Einschränkungen diese Aktivitäten unterliegen.

Eine stringente Prozessdefinition erfordert die Verwendung von übergreifenden Datendefinitionen für wesentliche Datenentitäten (z. B. den Antrag) und für Daten, die zwischen Prozessen oder Anwendungen ausgetauscht werden.

Datenmodelle sollen immer auf

a. Wiederverwendbarkeit,
b. Einfachheit und
c. Abbildbarkeit auf bereits vorhandene Datenmodelle

überprüft werden. Zur Unterstützung der Verantwortlichen bei der Datenmodellierung wird auf der Homepage der KBSt ein Leitfaden zur Prozess- und Datenmodellierung[73] bereitgestellt.

Das Kapitel 5 „Information Viewpoint: Standardisierung von Datenmodellen“ auf Seite 57 entspricht dem Information Viewpoint auf das deutsche E-Government und sollte bei der Erstellung eigener Datenmodelle berücksichtigt werden. Im Abschnitt 8.3 „Datenmodelle“ auf Seite 98 werden die anzuwendenden Technologien klassifiziert.

3.4 Computational Viewpoint

In dieser Sicht wird eine Anwendung in logische, funktionale Elemente zerlegt, die für die Verteilung geeignet sind. Das Ergebnis sind Objekte, die Schnittstellen besitzen, über die sie ihre Funktionalität anbieten beziehungsweise die Funktionalität anderer Objekte nutzen.

Die Interaktion geschieht über lokale und entfernte Kommunikation zwischen den Elementen. Abhängig vom Schutzbedarf ist eine sichere Interaktion notwendig. Die Schutzziele sind im Abschnitt 8.1.2.1 „Schutzziele“ auf Seite 94 beschrieben.

71. siehe http://www.kbst.bund.de/modellierungsleitfaden
72. siehe http://www.kbst.bund.de/, „E-Government“ > „Vorgangsbearbeitung, Prozesse und Organisation“
73. siehe http://www.kbst.bund.de/modellierungsleitfaden

Die Anwendungen werden außerdem in Schichten unterteilt, in denen sich die einzelnen Elemente wiederfinden.

Das Kapitel 6 „Computational Viewpoint: Referenz-Software-Architektur“ auf Seite 67 ist die Beschreibung eines allgemeinen Computational Viewpoint auf E-Government-Anwendungen, der als eine Grundlage für die Erstellung dieser Sicht für eine konkrete Online-Dienstleistung verwendet werden kann. Weiterhin sind in dem Kapitel die Architekturen für verschiedene Anwendungsfälle von E-Government-Anwendungen – z. B. Systeme und Dienste – beschrieben. SAGA definiert im Kapitel 8 „Technology Viewpoint: Standards für IT-Architektur und Datensicherheit“ auf Seite 93 Standards und Technologien zur Realisierung des Computational Viewpoint sowie zur Schaffung von sicheren Interaktionen zwischen Systemelementen.

3.5 Engineering Viewpoint

Der Engineering Viewpoint beschreibt die erforderliche Systemunterstützung, um eine Verteilung der Objekte aus dem Computational Viewpoint zu erlauben. Dazu gehören Systemelemente zur Ausführung von Objekten, wie zum Beispiel Computer-Hardware und Kommunikationsinfrastruktur sowie alle Arten von Software-Plattformen für verteilte Systeme.

Das Kapitel 7 „Engineering Viewpoint: IT-Service-Management und Referenzinfrastruktur“ auf Seite 81 beschreibt allgemein den Engineering Viewpoint für E-Government-Anwendungen von Bundesbehörden. Daraus kann die entsprechende Sicht auf eine konkrete Online-Dienstleistung abgeleitet werden. Dem Kapitel 8 „Technology Viewpoint: Standards für IT-Architektur und Datensicherheit“ auf Seite 93 sind eine Reihe von Technologien zu entnehmen, mit denen die Sicherheit von Netzwerken unterstützt werden sollte.

3.6 Technology Viewpoint

Diese Sicht beschreibt die gewählten konkreten Technologien zur Implementierung und Realisierung des Systems.

SAGA beschreibt in Kapitel 8 auf Seite 93 die klassifizierten Standards, Technologien und Methoden für IT-Architektur und Datensicherheit.

4 Enterprise Viewpoint: Grundlagen E-Government

Entsprechend der Definition des Enterprise Viewpoint in Kapitel 3 „Architekturmodell für E-Government-Anwendungen“ werden im Folgenden als Gesamtumgebung für die standardisierte Einführung von E-Government-Anwendungen die Grundlagen für das E-Government in Deutschland beschrieben.

Neben dieser übergreifenden Betrachtung wird die prozessuale Ebene im E-Government näher betrachtet. Die Prozessmodelle bilden den Ausgangspunkt für die Ableitung von verwaltungsübergreifenden Bausteinen, die in E-Government-Anwendungen integriert werden.

4.1 Definitionen zum E-Government in Deutschland

4.1.1 Begriff des E-Government

Unter E-Government (Electronic Government) wird die Nutzung elektronischer Informations- und Kommunikationstechnologien zur Einbeziehung des Verwaltungskunden in das Handeln von Regierung und öffentlicher Verwaltung verstanden[74]. Ziel ist es, den Kunden des Verwaltungshandelns, also Bürgern, Wirtschaftsunternehmen und der Verwaltung selbst, Verwaltungsdienstleistungen und Informationen elektronisch zugänglich zu machen. Die Nutzungsmöglichkeiten dieser Technologien sind sehr vielfältig. Angefangen bei der Verwaltungsmodernisierung durch elektronische Vorgangsbearbeitung, reichen sie über die Bereitstellung von Verwaltungsinformationen auf Behördenportalen im Internet bis hin zu den komplexen Transaktionen und interaktiven elektronischen Bürgerdiensten im Netz.

E-Democracy-Aspekte werden hier nicht explizit aufgegriffen, da von einem unterschiedlichen Rollenverständnis ausgegangen wird, in denen der Staat den Bürgern gegenübertritt. Im Bereich von E-Government werden die Bürger und Unternehmen als Kunden der Verwaltung und des Staates gesehen. Im Bereich von E-Democracy sind die Bürger der Souverän, der die Grundlagen für die Ausübung von Staatsgewalt legt.

4.1.2 Begriff der Dienstleistung im E-Government

Im Rahmen von E-Government wird unter dem Begriff Dienstleistung die Ausführung beziehungsweise das Ergebnis einer Tätigkeit durch eine öffentliche Verwaltung verstanden, die dem Bürger, dem Unternehmen oder einer anderen öffentlichen Verwaltung dient[75]. Eine Dienstleistung umfasst Vorgänge, Verpflichtungen und Belastungen, wie z. B. die Anerkennung der Kriegsdienstverweigerung, die Beantragung von Arbeitslosengeld oder die Erteilung einer Zolleinfuhrgenehmigung.

74. siehe BSI: „Das E-Government-Glossar“, Version vom 4. Januar 2006, Abschnitt 1.1, Seite 3; http://www.bsi.bund.de/fachthem/egov/download/6_EGloss.pdf
75. siehe BSI: „Das E-Government-Glossar“, Version vom 4. Januar 2006, Abschnitt 1.2, Seite 4; http://www.bsi.bund.de/fachthem/egov/download/6_EGloss.pdf

4.2 Leitbilder des E-Government

Durch E-Government ergeben sich neue Möglichkeiten für die Modernisierung und Innovation der öffentlichen Verwaltung durch elektronische Dienstleistungen und Verfahren. Dies betrifft zum einen das Innenverhältnis der Verwaltung und zum anderen das Außenverhältnis zwischen der Verwaltung, den Bürgern und der Wirtschaft[76].

4.2.1 Orientierung an Bedürfnissen der Bürger

Das Internet und vernetzte Computersysteme bestimmen die Zukunft. Durch die zunehmende Internetdurchdringung vor allem in privaten Haushalten nimmt auch der Bedarf an elektronischen Dienstleistungen des Staates zu. Auf diesen Bedarf wird durch E-Government reagiert.

Für Bürger ist der Verwaltungskontakt zum Teil mit langen Wegen und Wartezeiten verbunden. Der Vorteil internetbasierter Kommunikation und Transaktion kann dem gegenüber zu maßgeblichen Zeit- und Kosteneinsparungen führen. So können Bürger zukünftig in einer Vielzahl von Fällen ihre Verwaltungskontakte elektronisch bequem von zu Hause abwickeln. Internetportale vereinfachen den Zugang zu den Informationen und Dienstleistungen der Verwaltung.

Um den Service der Verwaltungen bedarfsgerecht zu gestalten, muss es Bürgern auch in Zukunft freistehen, welchen Zugang zur Verwaltung sie wählen. Der Zugang zur Verwaltung muss persönlich, via Internet und E-Mail sowie per Telekommunikation möglich sein. Um das Verwaltungshandeln effizient zu gestalten, müssen diese Zugangskanäle in den Verwaltungen so früh und so weit möglich integriert sowie einheitlich bearbeitet werden. Zudem sind Internetbarrieren und eventuelle Ausgrenzungen durch das Internet abzubauen beziehungsweise zu vermeiden.

4.2.2 E-Government als Standortfaktor für die Wirtschaft

Wirtschaftsunternehmen haben in verschiedenen Bereichen regelmäßig Kontakt mit der Verwaltung, z. B. bei Zertifizierungs-, Zulassungs- oder Genehmigungsverfahren sowie Verfahren der Zoll- und Steuerverwaltung.

Weltweit haben alle führenden Industrienationen in den vergangenen Jahren leistungsstarke E-Government-Angebote geschaffen. E-Government ist heute ein Standortfaktor. Die nationalen und EU-weiten Planungen zum Ausbau der E-Government-Angebote in den kommenden Jahren richten sich folglich durchgängig auf die Erhöhung des Nutzens für Bürger und vor allem für Unternehmen sowie auf die Senkung der Kosten von Verwaltungsleistungen. In einigen Ländern wird vorrangig der bedarfsgerechte Ausbau der E-Government-Angebote und die Erhöhung der Nutzungszahlen betrieben. Die beginnende Integration der Verwaltungs- und Wirtschaftsprozesse entlang der Wertschöpfungsketten ermöglicht, Bürokratiekosten zum Vorteil der Unternehmen und des Staates zu reduzieren, z. B. im Bereich der Statistik oder der Ein- und Ausfuhr von Waren.

76. E-Government-Handbuch: http://www.bsi.bund.de/fachthem/egov/6.htm, Kapitel I, Modul „Chefsache E-Government – Leitfaden für Behördenleiter“

Die Verfügbarkeit und die Qualität elektronischer Verwaltungsdienstleistungen ist damit ein nicht zu unterschätzender Faktor im globalen Wettbewerb um die Ansiedlung von Firmen geworden. Rahmenbedingungen sind attraktiv zu gestalten und Barrieren für Unternehmen so niedrig wie möglich zu halten.

4.3 Strategische Vorgaben

Die im vorangegangenen Abschnitt betrachteten Leitbilder bilden die hauptsächliche Zielsetzung für die strategischen Vorgaben des E-Government von Europa und Deutschland. Zur Erreichung dieser Ziele ist eine Modernisierung der öffentlichen Verwaltung notwendig. Eine allgemeine Übersicht zu Programmen, Strategien und Maßnahmen des Bundes zu diesem Thema mit den Schwerpunkten Personal, Verwaltungssteuerung, Organisation und E-Government ist über die Web-Seite http://www.verwaltung-innovativ.de/ erreichbar. Im Folgenden werden die zentralen Programme und Strategien für den Bund vorgestellt, die für die weitere Entwicklung des E-Government in Bund, Ländern und Kommunen Deutschlands die Schwerpunkte für die nächsten Jahre setzen.

4.3.1 E-Government 2.0 – Das Programm des Bundes

Oberstes Ziel des Programms E-Government 2.0[77], das im September 2006 durch das Bundeskabinett verabschiedet wurde, ist die Ausrichtung der Bundesverwaltung auf eine service-orientierte Informationsgesellschaft. Die Bedürfnisse der Nutzer von E-Government-Anwendungen sollen in Zukunft noch stärker in den Mittelpunkt rücken – so sollen Nutzer beispielsweise mit Behörden ohne Angst vor Identitätsbetrug und elektronischer Belästigung kommunizieren können[78]. Dementsprechend soll das Internetangebot der Bundesverwaltung in Deutschland bis 2010 qualitativ und quantitativ weiter ausgebaut werden. Das Programm wird durch das BMI in Zusammenarbeit mit den einzelnen Bundesressorts koordiniert.

Die genannten Ziele werden in vier Handlungsfeldern mit Maßnahmen unterstützt:

a. Portfolio
   Bedarfsorientierter, qualitativer und quantitativer Ausbau des E-Government-Angebots des Bundes (z. B. Arbeitsagentur-Online[79])
b. Prozessketten
   Medienbruchfreie elektronische Prozessabwicklung zwischen Wirtschaft und Verwaltung durch integrierte Prozessketten sowie entsprechende Standards für Schnittstellen und Austauschformate (z. B. Sichere Lebensmittelkette[80])

77. siehe http://www.kbst.bund.de/e-government/
78. Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI): Bundesministerium des Innern, 2005; http://www.bmi.bund.de/, Navigationspunkte „Themen A-Z" > „Informationsgesellschaft" > „Sicherheit in der Informationstechnik" > Kasten „Links zum Thema"
79. siehe http://www.arbeitsagentur.de/
80. Forschungsverbund IT FoodTrace: http://www.itfoodtrace.de/

c. Identifizierung
   Einführung eines elektronischen Identitätsmanagement unter Verwendung der zukünftigen Funktionen und Anwendungen z. B. auf dem elektronischen Personalausweis (ePA)[81] sowie die Erarbeitung von E-Identity-Konzepten

d. Kommunikation
   Sichere Kommunikationsinfrastruktur in Form von Portalen für Bürger, Unternehmen und Verwaltungen (z. B. Bürgerportale[82])

4.3.2 Deutschland-Online – Die gemeinsame E-Government-Strategie von Bund, Ländern und Kommunen

Ziel von Deutschland-Online (DOL)[83] ist es, eine gemeinsame und vollständig integrierte E-Government-Landschaft in Deutschland zu schaffen und somit elektronisch erhobene Daten durchgängig und ebenenübergreifend zwischen Verwaltungen von Bund, Ländern und Kommunen austauschen zu können. Die Strategie beruht hierbei auf den folgenden Prinzipien:

a. Einer für Alle (EfA)
   Von einzelnen Beteiligten aus Bund, Ländern und Kommunen erfolgt die Entwicklung von Modelllösungen, die von den anderen Beteiligten genutzt werden.

b. Verantwortung der Federführer
   Die Hauptverantwortung eines DOL-Projekts liegt bei der vorschlagenden Behörde, die auch für die Entstehung eines tragfähigen Geschäftsmodells sowie die Umsetzung verantwortlich ist.

c. Transparenz der Standards – Konkurrenz der Produkte
   Durch transparente Standards und Prozessmodelle wird ein Rahmen festgelegt, für den verschiedene Produkte ausgewählt werden können, und somit die Interoperabilität zwischen verschiedenen Produkten gefördert.

Zur Umsetzung der strategischen Ziele haben die Regierungschefs von Bund und Ländern im Juni 2006 den Aktionsplan Deutschland-Online mit sechs priorisierten Vorhaben verabschiedet und im Juni 2007 um die IT-Umsetzung der EU-Dienstleistungsrichtlinie erweitert[84]:

Infrastruktur[85]

Derzeit existieren in Bund, Ländern und Kommunen unterschiedliche Netzinfrastrukturen, die nicht miteinander verbunden sind und somit Insellösungen darstellen. Für eine Vielzahl von Behörden besteht so keine oder nur vereinzelt die Möglichkeit, mit anderen Behörden Daten zuverlässig, einfach und sicher elektronisch auszutauschen. Mit dem Aufbau einer Kommunikationsinfrastruktur für die öffentliche Verwaltung Deutschlands soll ein einheitli-

81. siehe http://www.epass.de/
82. siehe http://www.kbst.bund.de/e-government/, Navigationspunkt „Bürgerportale“
83. siehe http://www.deutschland-online.de/
84. siehe http://www.deutschland-online.de/, Navigationspunkt „Strategie“ > Download „Aktionsplan Deutschland-Online vom 14.06.2007.pdf“
85. siehe http://www.deutschland-online.de/, Navigationspunkte „Vorhaben“ > „Priorisierte Vorhaben“ > „Infrastruktur“

ches Netz geschaffen sowie eine sichere elektronische Kommunikation zwischen Behörden von Bund, Ländern und Kommunen erreicht werden.

Standardisierung

Das DOL-Vorhaben „Standardisierung" soll die Entwicklung und Bereitstellung von fachlichen Standards für den elektronischen Datenaustausch (XÖV-Standards) unterstützen und koordinieren, sodass elektronische Verwaltungsprozesse effizient und in einheitlicher Weise umgesetzt werden können. Hierfür werden aufeinander abgestimmte Maßnahmen durch das Vorhaben zur Unterstützung der XÖV-Projekte der öffentlichen Verwaltung angeboten: Entwicklungsmethoden, standardisierte Datenmodelle, Werkzeuge und technische Infrastrukturen sowie Beratungsleistungen und Öffentlichkeitsarbeit.[86]

IT-Umsetzung der EU-Dienstleistungsrichtlinie[87]

Ziel des Vorhabens ist die Vereinfachung und Beschleunigung der elektronischen Verwaltungsverfahren in Deutschland im Rahmen der EU-Dienstleistungsrichtlinie[88]. Ab Ende 2009 soll es für Unternehmer der Europäischen Union möglich sein, ihre Angelegenheiten für die Aufnahme und die Durchführung ihrer Dienstleistungstätigkeit über einen einheitlichen Ansprechpartner online durchzuführen, unabhängig davon, welcher Nationalität sie angehören und in welchem Mitgliedsland sie sich momentan befinden. Als ein Meilenstein zu diesem Ziel wird bis Mitte 2008 ein Modell für die IT-Umsetzung der Richtlinie entwickelt und erprobt. Im Rahmen dieses Modells sollen die infrastrukturellen Anforderungen auf nationaler Ebene im europaweiten Kontext definiert, die erforderliche IT-Unterstützung für die medienbruchfreie Verfahrensabwicklung beschrieben, eine geeignete IT-Architektur entwickelt sowie Technologien mit Blick auf benötigte Schnittstellen vorgeschlagen werden.

Meldewesen[89]

Die Meldedaten von 82 Millionen Bürgern in Deutschland werden zurzeit in über 5.000 Meldebehörden dezentral elektronisch erfasst, registriert, verwaltet und in circa 114 Millionen Geschäftsvorfällen im Jahr – beispielsweise zur Auskunftserteilung – verwendet. Am 1. September 2006 wurde als Bestandteil der Föderalismusreform die ausschließliche Gesetzgebungskompetenz für das Meldewesen an den Bund übertragen. Ziel dessen ist die Schaffung eines Bundesmelderegisters (BMR) in Ergänzung der kommunalen Register, um das Meldeverfahren für die Bürger zu vereinfachen, die Melderegisternutzung für Wirtschaft und Verwaltung effizienter und kostengünstiger zu gestalten, die Qualität und Aktualität der Meldedaten zu verbessern sowie die Schaffung bundesweit einheitlicher Online-Dienste zu ermöglichen.

86. für eine ausführliche Darstellung siehe Abschnitt 5.3 „Das Deutschland-Online Vorhaben „Standardisierung"" auf Seite 59 und http://www.deutschland-online.de/, Navigationspunkte „Vorhaben" > „Priorisierte Vorhaben" > „Standardisierung"
87. siehe http://www.deutschland-online.de/, Navigationspunkt „Strategie" > Download „Aktionsplan Deutschland-Online vom 14.06.2007.pdf"
88. siehe Abschnitt 4.5.4 „EU-Dienstleistungsrichtlinie – Schaffung eines EU-Binnenmarkts" auf Seite 50
89. siehe http://www.deutschland-online.de/, Navigationspunkte „Vorhaben" > „Priorisierte Vorhaben" > „Meldewesen"

Kfz-Wesen[90]

Zurzeit ist es Bürgern und Wirtschaft möglich, einzelne Aufgaben im Rahmen der An-, Ab- und Ummeldung von Kraftfahrzeugen online durchzuführen (z. B.: Eintragen von Fahrzeugdaten zur Antragsvorbereitung, Reservieren von Wunschkennzeichen). Das eigentliche Verfahren selbst muss jedoch immer noch vor Ort in den Zulassungsbehörden von den Bürgern wahrgenommen werden. Ziel des Vorhabens ist es, eine organisatorische, rechtliche und technische Lösung zur Fahrzeugregistrierung zu finden, die Bürgern und Wirtschaft eine durchgängige Verfahrensabwicklung über das Internet ohne Medienbrüche bietet.

Personenstandswesen[91]

Am 23. Februar 2007 wurde das Gesetz zur Reform des Personenstandsrechts (PStRG) verabschiedet, das ab 1. Januar 2009 eine elektronische Registerführung möglich macht und diese ab 1. Januar 2014 verbindlich vorschreibt. Ziel des Vorhabens ist es, ein nach dem Gesetz ausgerichtetes elektronisches Verfahren für die Personenstandsregistrierung zu entwickeln und darauf aufbauend Pilotprojekte für das Personenstandswesen in einzelnen Bundesländern durchzuführen sowie den Bürgern eine Online-Registerauskunft und eine Online-Urkundenbeantragung zu ermöglichen. Bestandteil des Vorhabens ist auch die automatisierte Kommunikation zwischen dem Personenstandsregister und anderen Behörden im Rahmen der Auskunftsanforderung. Diesen Austausch soll das zu entwickelnde Datenformat XPersonenstand unterstützen.

Weitere Vorhaben von Deutschland-Online

Neben den zuvor beschriebenen priorisierten Vorhaben gibt es weitere Vorhaben, die im Rahmen von Deutschland-Online durchgeführt werden[92]:

a. Amtliche Statistik
b. BAföG (Bundesausbildungsförderungsgesetz)
c. Clearingstellen
d. Deutsches Signatur- und Kartenforum
e. Geodaten
f. Geschäftsmodelle
g. Gewerberegister
h. Justizregister
i. VEMAGS (Verfahrensmanagement Großraum- und Schwertransporte)
j. Verbund Internetportale / Zuständigkeitsfinder
k. XAusländer
l. XSozial

90. siehe http://www.deutschland-online.de/, Navigationspunkte „Vorhaben“ > „Priorisierte Vorhaben“ > „Kfz-Wesen“
91. siehe http://www.deutschland-online.de/, Navigationspunkte „Vorhaben“ > „Priorisierte Vorhaben“ > „Personenstandswesen“
92. siehe http://www.deutschland-online.de/, Navigationspunkte „Vorhaben“ > „Weitere Vorhaben“

4.4 Organisatorische Rahmenbedingungen

Die Umsetzung von E-Government in Deutschland ist an organisatorische Rahmenbedingungen gebunden, die berücksichtigt werden müssen. Die wichtigsten werden im Folgenden beschrieben.

4.4.1 Verwaltungsübergreifende Interaktionen

Föderalismus in Deutschland

Föderalistische Staaten wie Deutschland werden bei der Implementierung von E-Government mit den Problemen eines dezentralen Verwaltungsaufbaus konfrontiert, da die dezentralen Verwaltungseinheiten weitgehend autonom von der zentralen staatlichen Instanz agieren.

Während die Gesetzgebungskompetenz zum Großteil vom Bund wahrgenommen wird, liegt die Ausführung der Gesetze hauptsächlich bei den Ländern und Kommunen. Die unmittelbare Bundesverwaltung übernimmt gesamtstaatliche Aufgaben. Einen Verwaltungsunterbau besitzen nur die im Grundgesetz[93] (Art. 87-89) festgelegten Bereiche, wie z. B. Auswärtiger Dienst, Bundeswehr, Bundespolizei oder Bundesfinanzverwaltung. Daneben gibt es noch weitere gesamtstaatliche Aufgaben, die in der Regel von Sonderverwaltungsbehörden ohne Verwaltungsunterbau wahrgenommen werden (z. B. Bundeskriminalamt, Statistisches Bundesamt, Deutsches Patent- und Markenamt).

Die unmittelbare Bundesverwaltung gliedert sich in:

a. *Oberste Bundesbehörden*, wie z. B. die Bundesministerien, das Bundespräsidialamt und das Bundespresseamt
b. *Bundesoberbehörden*, die für ein spezielles Aufgabengebiet zentral für die gesamte Bundesrepublik zuständig sind (z. B. das Bundeskartellamt)
c. *Bundesmittelbehörden* mit regionalen Zuständigkeiten (z. B. die verschiedenen Oberfinanzdirektionen)
d. *Untere Bundesbehörden*, die örtlich beschränkt tätig sind (z. B. Hauptzollämter)

Im Rahmen bestimmter bundesstaatlicher Aufgaben für den Vollzug von Gesetzen bedient sich der Bund ausgegliederter Verwaltungsträger mit eigener Rechtspersönlichkeit. Diese rechtsfähigen Körperschaften, Anstalten und Stiftungen der mittelbaren Bundesverwaltung sind selbstständig für ihren Sachbereich im gesamten Bundesgebiet zuständig und unterstehen der Aufsicht eines Ministeriums.

Vergleichbare Strukturen finden sich in den einzelnen Bundesländern. Hinzu kommen die Städte, Kreise und Gemeinden, die als selbstverwaltete Gebietskörperschaften die dritte Verwaltungsebene bilden. Neben Bundes- und Landesaufgaben nehmen sie auch eigene Aufgaben wahr.

Die Nutzer von E-Government-Dienstleistungen differenzieren in der Regel nicht nach den Verwaltungsebenen Bund, Länder und Kommunen. Unternehmen und Bürger erwarten

93. Grundgesetz für die Bundesrepublik Deutschland (GG): http://www.gesetze-im-internet.de/bundesrecht/gg/

vielmehr ein einheitliches und durchgängiges E-Government-Angebot, siehe Abbildung 4-1.

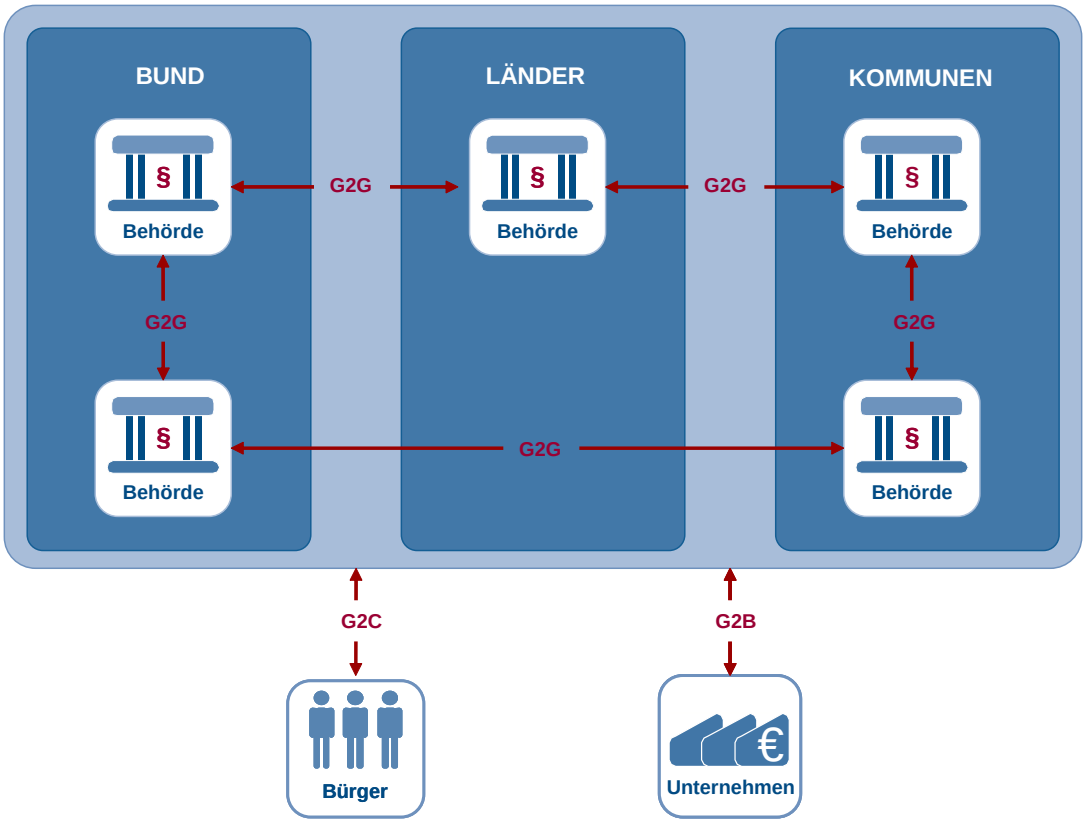


Abbildung 4-1: E-Government-Interaktionen in Deutschland

Insgesamt muss es Kooperation, Vernetzung und Abstimmung innerhalb und zwischen den Verwaltungsebenen geben. Ein erster Schritt war auf Bundesebene die Realisierung des Informationsverbunds Berlin-Bonn (IVBB)[94], mit dem ein Intranet für Oberste Bundesbehörden geschaffen wurde. Mit dem Ausbau zum Informationsverbund der Bundesverwaltung (IVBV)[95] sollen alle Bundesbehörden in einem sicheren, geschlossenen Netz vereint werden, was sowohl technisch als auch organisatorisch eine große Herausforderung darstellt[96].

Mit der gemeinsamen nationalen E-Government-Strategie von Bund, Ländern und Kommunen, Deutschland-Online, wurde im Juni 2007 ein erweiterter Aktionsplan vorgestellt[97].

Deutschland als Mitglied der Europäischen Union

Die Bundesrepublik Deutschland als Mitglied der Europäischen Union (EU) wird zunehmend vor die Aufgabe gestellt, grenzüberschreitende E-Government-Dienstleistungen, wie sie in der EU-Dienstleistungsrichtlinie gefordert werden, umzusetzen. Ziel ist es, einen ein-

94. siehe http://www.kbst.bund.de/ivbb
95. siehe http://www.kbst.bund.de/ivbv
96. E-Government-Handbuch: http://www.bsi.bund.de/fachthem/egov/6.htm, Kapitel V, Unterkapitel C, Modul „Netzplattform für E-Government“
97. siehe Abschnitt 4.3.2 „Deutschland-Online – Die gemeinsame E-Government-Strategie von Bund, Ländern und Kommunen“ auf Seite 40

heitlichen Binnenmarkt in der EU zu schaffen und allen Bürgern und Unternehmen die gleichen Chancen und Rechte einzuräumen.

Wie in Abbildung 4-2[98] dargestellt, müssen verstärkt nationale Dienstleistungen den Bürgern, Unternehmen und Behörden anderer Mitgliedsstaaten angeboten werden. Auch die Zusammenarbeit mit der EU-Verwaltung bekommt zukünftig eine größere Bedeutung.

Die Bürger und Unternehmen als Nutzer dieser grenzüberschreitenden E-Government-Anwendungen differenzieren in der Regel nicht nach den Verantwortungsbereichen der nationalen Verwaltungen, sondern erwarten vielmehr ein einheitliches, multilinguales und durchgängiges E-Government-Angebot zwischen den Mitgliedsstaaten. So muss es in Zukunft möglich sein, dass z. B. ein Bauunternehmer in Italien, der sich in Spanien niederlassen möchte, die dafür erforderlichen Behördengänge auf elektronischem Wege bereits aus Italien durchführen kann. Der Unternehmer tritt hierbei nur mit einem Ansprechpartner in Kontakt. Die notwendigen Interaktionen zwischen den unterschiedlichen Verwaltungen der Mitgliedsstaaten untereinander finden im Hintergrund als grenzüberschreitende E-Government-Anwendung statt, ohne dass der Unternehmer davon Kenntnis haben oder Kontakt zu den einzelnen Behörden aufnehmen muss.

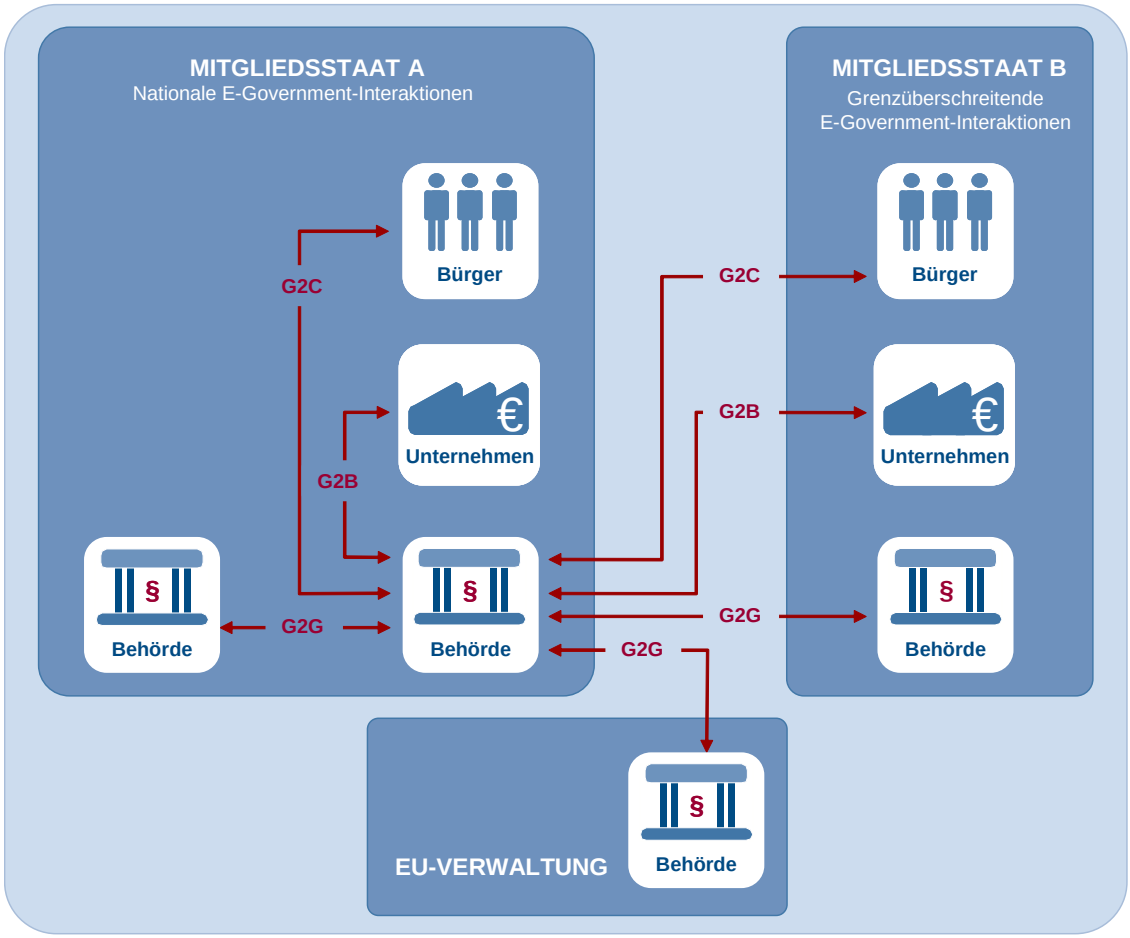


Abbildung 4-2: Nationale und grenzüberschreitende E-Government-Interaktionen

98. nach „European Interoperability Framework for Pan-European eGovernment Services“ (EIF) v1.0, IDABC, 2004; http://ec.europa.eu/idabc/servlets/Doc?id=19528, Seite 12, Abbildung 3

Neben der Anmeldung von Unternehmen wurden beispielsweise folgende Themenbereiche für grenzüberschreitende Anwendungen identifiziert: Steuererklärung, Beantragung von Arbeitslosenunterstützung, Kfz-Anmeldung. Die EU-Dienstleistungsrichtlinie[99] bildet für die Umsetzung dieser Anwendungen den entsprechenden Rahmen.

4.4.2 Optimierung der Verwaltungsprozesse

Eine erfolgreiche Einführung und Umsetzung von E-Government setzt im Vorfeld die Überprüfung gewachsener Prozesse voraus. Bestehende Regeln sowie die Ablauf- und Aufbauorganisation sollten in geeigneter Form unter Berücksichtigung technischer und rechtlicher Gegebenheiten angepasst und vereinfacht werden. Allein die elektronische Abbildung herkömmlicher Verfahren führt in der Regel nicht zur Optimierung.

Die bestehenden Verwaltungsabläufe sind teilweise historisch gewachsen und über Jahre hinweg durch viele Änderungen komplex geworden. Folgende Maßnahmen sind daher vor der elektronischen Umsetzung der Fachanwendungen empfehlenswert:

a. Vereinfachung von Verfahren
b. Deregulierung
c. Verkürzung von Prozessketten
d. Verringerung von Schnittstellen
e. Vermeidung von iterativen Durchläufen
f. Verkürzung von Durchlauf- und Liegezeiten[100]

Erste Schritte zum Bürokratieabbau zielten darauf ab, Prozesse und gesetzliche Regelungen bei Verwaltungsdienstleistungen zu vereinfachen. Deutschland-Online[101] erfasst deshalb Dienstleistungen, deren Bereitstellung mehrere Verwaltungsebenen betrifft. Mit dem Programm der Bundesregierung „Zukunftsorientierte Verwaltung durch Innovationen“[102] werden ebenenübergreifende Prozesse angestoßen, die zu einem offenen Dialog über eine gemeinsame Vision einer zukunftsfähigen, netzwerkorientierten Verwaltung in Deutschland führen.

4.4.3 Qualifizierung des Personals

Die Verwendung und Pflege von Standards sowie Entwicklung, Betrieb und der sachgerechte Umgang mit IT-gestützten Systemen erfordern einen kontinuierlichen Informationsaustausch und Schulungsprozess. Viele Mitarbeiter des öffentlichen Dienstes sind hochmotiviert, wenn es darum geht, E-Government zu unterstützen. Dieses wichtige Kapital muss für die Umsetzung von E-Government genutzt und vermehrt werden. Dazu sind intensive Schulungen von Mitarbeitern durchzuführen. Zudem muss die Attraktivität und Anziehungskraft der Verwaltungen für IT-Experten gesteigert werden.

---

99. siehe Abschnitt 4.5.4 „EU-Dienstleistungsrichtlinie – Schaffung eines EU-Binnenmarkts“ auf Seite 50
100. E-Government-Handbuch: http://www.bsi.bund.de/fachthem/egov/6.htm, Kapitel III, Modul „Phase 3 – Analyse“
101. siehe http://www.deutschland-online.de/
102. siehe http://www.verwaltung-innovativ.de/

4.4.4 Einbindung der Nutzer

Der Nutzen von E-Government hängt im Wesentlichen von der Kundenakzeptanz der angebotenen Dienstleistungen ab. Das Einsparpotenzial von E-Government kann nur dann voll ausgeschöpft werden, wenn die bereitgestellten Online-Dienstleistungen von den potenziellen Nutzern angenommen und genutzt werden. Wünsche von Bürgern, Unternehmen und Behörden müssen kontinuierlich zielgruppenspezifisch abgefragt werden. Das Dienstleistungsportfolio und der Prozess zur Erbringung der Leistung müssen sich diesen Anforderungen anpassen.

4.5 Rechtliche Rahmenbedingungen

Neben den strategischen Vorgaben und organisatorischen Rahmenbedingungen sind auch rechtliche Bedingungen zu beachten. Die wichtigsten werden im Folgenden mit den Rechtsanpassungen zur elektronischen Signatur, Gesetzen, Verordnungen und Hilfestellungen zu Datenschutz und Barrierefreiheit sowie der EU-Dienstleistungsrichtlinie beschrieben. Eine ausführliche Darstellung der vorgenommenen Rechtsanpassungen bietet das E-Government-Handbuch des Bundes[103].

4.5.1 Elektronische Signaturen

Elektronische Signaturen eröffnen eine Möglichkeit für Nutzer von E-Government-Anwendungen, sich authentifizieren zu lassen[104]. Durch sinnvolle, praktikable und zeitnahe Rechtsanpassungen wird die Möglichkeit für das E-Government gegeben, Verwaltungsprozesse medienbruchfrei und effizient gestalten zu können.

Rechtliche Anpassungen

Ein wesentlicher Erfolgsfaktor für die Umsetzung von E-Government ist die Rechtsverbindlichkeit von elektronischer Kommunikation. Nötig ist deshalb eine digitale Lösung für eine rechtsverbindliche Unterschrift: die qualifizierte elektronische Signatur. Sie stellt im Gegensatz zur einfachen elektronischen Signatur und zur fortgeschrittenen elektronischen Signatur den höchsten Grad zur elektronischen Nachbildung einer handschriftlichen Unterschrift dar. Die zum Einsatz von elektronischen Signaturen erforderlichen Rechtsanpassungen zur Gleichstellung mit der handschriftlichen Unterschrift sind in Deutschland abgeschlossen. Es ist neben der Anpassung des Signaturgesetzes an europäische Vorgaben auch eine Einbindung der elektronischen Signatur in die jeweiligen Generalklauseln im Verwaltungs- und Privatrecht erfolgt[105].

Verbreitung der elektronischen Signatur

Die Verbreitung und Akzeptanz qualifizierter elektronischer Signaturen erfolgt aufgrund des zurzeit noch anzutreffenden Missverhältnisses zwischen Nutzen und Kosten bisher nur

103. E-Government-Handbuch: http://www.bsi.bund.de/fachthem/egov/6.htm, Kapitel II, Modul „Rechtliche Rahmenbedingungen für E-Government"
104. siehe Abschnitt 8.5.4 „Technologien zur Authentisierung" auf Seite 107, Abschnitt 8.10 „Elektronische Signatur" auf Seite 137 und Abschnitt 8.11 „Smartcards" auf Seite 139
105. für Informationen zu den rechtlichen Grundlagen der elektronischen Signatur siehe http://www.bsi.de/esig/

langsam. So findet die qualifizierte elektronische Signatur bislang nur in einigen wenigen Massenverfahren und Verwaltungszweigen Anwendung, z. B. im Rechnungswesen.

Ursache dafür sind insbesondere Bedenken bezüglich der Sicherheit bei der Anwendung von Signaturen und Signaturkarten, die mangelnde Interoperabilität zwischen verschiedenen Signaturkartenanwendungen sowie die Einschränkung der rechtlichen Anerkennung auf einzelne Staaten.

Die Bundesnetzagentur (BNetzA) hat zur Überbrückung der sicherheitsrelevanten Bedenken bereits Produkte für qualifizierte elektronische Signaturen geprüft und zertifiziert[106]. Diese Produkte entsprechen den notwendigen hohen Anforderungen von Signaturgesetz[107] (SigG) und Signaturverordnung[108] (SigV).

Weiterhin stellen die Kosten für die Restrukturierung der verwaltungsinternen Abläufe, die Ausstattung mit Technik (Smartcard, Software, Kartenleser) und die laufende Nutzung (regelmäßig zu erneuernde Zertifizierung des Signaturschlüssels) für Verwaltungen einen Faktor dar, der im Verhältnis zum Nutzen noch relativ hoch ist und somit auch die schnellere Verbreitung verhindert.

In der Bevölkerung hingegen existiert vor allem Aufklärungsbedarf über den Einsatz und den Mehrwert elektronischer Signaturen. Erste realisierte Anwendungen zeigen, dass Smartcards für Bürger dann besonders attraktiv sind, wenn diese damit sowohl privatwirtschaftliche als auch staatliche Dienstleistungen in Anspruch nehmen können.

Initiativen und Projekte des Bundes im Bereich elektronischer Signaturen

Die Signaturinitiativen und -projekte der Bundesverwaltung sollen in der Zukunft enger aufeinander abgestimmt werden, um die Verbreitung und Akzeptanz insbesondere von Signaturkarten voranzutreiben. Beispiele für Projekte in der Bundesverwaltung, die sich mit dem Einsatz von Signaturen und Signaturkarten befassen, sind:

a. elektronische Gesundheitskarte[109]
   Die elektronische Gesundheitskarte umfasst das elektronische Rezept, die europäische Krankenversicherungskarte, die Daten für den Notfall, die Arzneimitteldokumentation sowie die elektronische Patientenakte. Weiterhin wird ein elektronischer Heilberufsausweis entwickelt, mit dessen Hilfe ein Arzt eine qualifizierte elektronische Signatur erzeugen kann, die die bisherige eigenständige Unterschrift ersetzt, beispielsweise zum „Unterschreiben" eines elektronischen Rezepts für den Patienten. Im Dezember 2006 begannen Feldtests zur Erprobung der elektronischen Gesundheitskarte.
b. elektronischer Personalausweis (ePA)[110]
   Die Funktion der elektronischen Signatur wird als Option ebenfalls in den elektronischen Personalausweis integriert werden. „Option" heißt, dass der elektronische Personalausweis für die Aufnahme eines qualifizierten Signaturzertifikates vorbereitet ist, das

106. Bundesnetzagentur (BNetzA): http://www.bundesnetzagentur.de/enid/Elektronische_Signatur/Produkte_pi.html
107. Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG): http://www.gesetze-im-internet.de/sigg_2001/
108. Verordnung zur elektronischen Signatur (SigV): http://bundesrecht.juris.de/sigv_2001/
109. siehe http://www.die-gesundheitskarte.de/
110. siehe http://www.epass.de/

Zertifikat selbst aber vom Inhaber des Ausweises in den Speicherchip nachgeladen werden muss. Diese Wahlfreiheit ermöglicht den Einsatz in Abhängigkeit von einem konkreten Bedarf. Die Integration biometrischer Informationen und einer Authentisierungsfunktion vervollkommt den künftigen elektronischen Personalausweis und macht ihn zum zuverlässigen Identitätsnachweis und zum universellen, zukunftsfähigen und sicheren Schlüssel für E-Government und E-Business.

c. elektronische Steuererklärung (ELSTER)[111]
   Im Rahmen der elektronischen Steuererklärung können Bürger und Unternehmen beispielsweise die Umsatzsteuer-Voranmeldung, die Lohnsteueranmeldung oder die Lohnsteuerbescheinigung online ausfüllen und abgeben. Weiterhin kann die elektronische Steuerkontoabfrage durchgeführt werden, zu der eine vom System unterstützte Signaturkarte benötigt wird. Auf der Website wird eine Übersicht solcher Signaturkarten dargestellt[112].

4.5.2 Datenschutz

E-Government bietet im Bereich der Datenverarbeitung vielfältige Möglichkeiten und Rationalisierungspotenziale. Im Idealfall werden Daten aus den unterschiedlichsten Zusammenhängen nur einmal zentral erfasst und könnten dann für beliebige Zwecke dezentral abgerufen und wiederverwendet werden.

Beim Austausch elektronischer Daten in und zwischen den Behörden müssen jedoch datenschutzrechtliche Anforderungen beachtet und durch geeignete technische und organisatorische Maßnahmen umgesetzt werden. Vor allem personenbezogene Daten dürfen nur im gesetzlich formulierten Rahmen erhoben, verarbeitet und weitergegeben werden.

Umfassende Informationen zum Thema datenschutzgerechtes E-Government sind im E-Government-Handbuch des Bundes in einem eigenen Modul[113] dargestellt. Vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit werden unter dem Thema „Technologischer Datenschutz" für bestimmte Anwendungsfälle Orientierungshilfen zur Verfügung gestellt[114], wie zum Beispiel zum Einsatz von Dokumentenmanagementsystemen oder kryptografischen Verfahren.

4.5.3 Barrierefreiheit

In Deutschland leben über acht Millionen behinderte Menschen, davon 6,6 Millionen mit einer Schwerbehinderung. Insbesondere Menschen mit Sehstörungen und körperbehinderte Menschen sind bei der Nutzung des Internets auf technische Hilfen angewiesen, wie zum Beispiel Großbildmonitor oder Lupenfunktion, Braillezeile, Sprachausgabe oder ähnliches. Damit E-Government-Anwendungen von diesen Geräten optimal erfasst werden können, müssen bei Programmierung, Gestaltung und redaktioneller Pflege eine Vielzahl von Regeln beachtet werden.

---

111. siehe http://www.elsteronline.de/
112. siehe https://www.elsteronline.de/eportal/Sicherheit.tax#sigkarte
113. E-Government-Handbuch: http://www.bsi.bund.de/fachthem/egov/6.htm, Kapitel II, Modul „Datenschutzgerechtes E-Government"
114. siehe http://www.bfdi.bund.de/, „Startseite Datenschutz" > „Themen" > „Technologischer Datenschutz"

Am 1. Mai 2002 trat das neue Behindertengleichstellungsgesetz[115] (BGG) mit dem Ziel in Kraft, die Benachteiligung von behinderten Menschen zu beseitigen sowie die gleichberechtigte Teilhabe von behinderten Menschen am Leben in der Gesellschaft zu gewährleisten und ihnen eine selbstbestimmte Lebensführung zu ermöglichen.

Dies gilt auch für die Nutzung des Internets. Die wesentlichen Kriterien und Hinweise finden sich in der Verordnung zur Schaffung barrierefreier Informationstechnik nach § 11 BGG (Barrierefreie Informationstechnik-Verordnung – BITV[116]), die am 24. Juli 2002 in Kraft trat. Die BITV wendet als technischen Standard die Web Content Accessibility Guidelines[117] 1.0 (WCAG 1) aus dem Jahr 1999 an. Die BITV gilt seit dem 1. Januar 2006 verbindlich für Behörden der Bundesverwaltung[118] und betrifft:

a. Internetauftritte und -angebote,
b. Intranetauftritte und -angebote, die öffentlich zugänglich sind,
c. mittels Informationstechnik realisierte grafische Programmoberflächen, die öffentlich zugänglich sind.

4.5.4 EU-Dienstleistungsrichtlinie – Schaffung eines EU-Binnenmarkts

Die EU-Dienstleistungsrichtlinie[119] wurde am 12. Dezember 2006 durch das Europäische Parlament und den Europäischen Rat beschlossen. Ziel der Richtlinie ist der Abbau von bürokratischen Hindernissen in der Europäischen Union (EU), die Förderung des grenzüberschreitenden Dienstleistungsverkehrs[120] und somit einhergehende Verwirklichung eines einheitlichen EU-Binnenmarkts. Die Richtlinie muss bis Ende 2009 umgesetzt sein. Sie umfasst im Rahmen der elektronischen Verfahrensabwicklung u. a. die Forderungen nach

a. Einheitlichen Ansprechpartnern
   „Die Mitgliedstaaten stellen sicher, dass Dienstleistungserbringer folgende Verfahren und Formalitäten über einheitliche Ansprechpartner abwickeln können:
   a) alle Verfahren und Formalitäten, die für die Aufnahme ihrer Dienstleistungstätigkeiten erforderlich sind, insbesondere Erklärungen, Anmeldungen oder die Beantragung von Genehmigungen bei den zuständigen Behörden, einschließlich der Beantragung der Eintragung in Register, Berufsrollen oder Datenbanken oder der Registrierung bei Berufsverbänden oder Berufsorganisationen;
   b) die Beantragung der für die Ausübung ihrer Dienstleistungstätigkeit erforderlichen Genehmigungen." (Artikel 6, Absatz 1)

115. Gesetz zur Gleichstellung behinderter Menschen (BGG): http://www.gesetze-im-internet.de/bundesrecht/bgg/
116. Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV): http://www.gesetze-im-internet.de/bitv/
117. siehe http://www.w3.org/TR/1999/WAI-WEBCONTENT-19990505/
118. E-Government-Handbuch: http://www.bsi.bund.de/fachthem/egov/6.htm, Kapitel IV, Modul „Barrierefreies E-Government"
119. Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt: http://ec.europa.eu/internal_market/services/services-dir/index_de.htm
120. im Gegensatz zur sonstigen Verwendung des Begriffs „Dienstleistung" mit Bezug zum E-Government (siehe Abschnitt 4.1.2 „Begriff der Dienstleistung im E-Government" auf Seite 37) wird in Zusammenhang mit der EU-Dienstleistungsrichtlinie folgende Definition einer Dienstleistung verwendet: „[...] jede [...] selbstständige Tätigkeit, die in der Regel gegen Entgelt erbracht wird" (Artikel 4, Abs. 1)

b. Sicherstellung der Aufnahme und Ausübung von Dienstleistungen
„Die Mitgliedstaaten stellen sicher, dass alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner oder bei der betreffenden zuständigen Behörde abgewickelt werden können." (Artikel 8, Absatz 1)

c. Berücksichtigung von gemeinsamen Standards
„Die Kommission erlässt nach dem in Artikel 40 Absatz 2 genannten Verfahren Durchführungsbestimmungen zu Absatz 1 des vorliegenden Artikels, um die Interoperabilität der Informationssysteme und die Nutzung der elektronischen Verfahren zwischen den Mitgliedstaaten zu erleichtern, wobei auf Gemeinschaftsebene entwickelte gemeinsame Standards berücksichtigt werden." (Artikel 8, Absatz 3)

4.6 Prozesse im E-Government

4.6.1 Stufen der Interaktion

Generell kann man E-Government-Dienstleistungen nach den Interaktionsstufen Information, Kommunikation und Transaktion unterscheiden[121].

Information umfasst die Bereitstellung von Informationen für Bevölkerung, Wirtschaft und andere Gesellschaftsteile. Auf dieser Stufe nimmt der Benutzer lediglich die Rolle eines Informationsempfängers ein. Dieser Bereich ist am weitesten entwickelt, nahezu alle öffentlichen Stellen sind im Internet durch umfangreiche Web-Angebote präsent.

Viele dieser Informationssysteme werden durch **Kommunikation**slösungen mit Dialog- und Partizipationsmöglichkeiten ergänzt, um den Austausch von Nachrichten zu ermöglichen. Diese reichen von Lösungen wie E-Mail oder web-basierten Diskussionsforen bis hin zu komplexen Anwendungen, wie z. B. Videokonferenzsystemen für Telekooperation. Auch hier ist der Entwicklungsstand in der deutschen Verwaltung als weit fortgeschritten zu bezeichnen.

Transaktion hat das höchste Interaktionsniveau. Dieser Bereich umfasst die eigentliche Erbringung von Dienstleistungen in der öffentlichen Verwaltung. Dazu gehören z. B. die elektronische Annahme und Bearbeitung von Anträgen oder Aufträgen sowie die Bereitstellung von Formularen, die direkt am Computer ausgefüllt und sofort an den zuständigen Empfänger versandt werden. Auch elektronische Zahlungs- oder Ausschreibungssysteme sind hier zuzuordnen.

Bisher sind Transaktionsdienstleistungen im Vergleich zu den anderen Interaktionsstufen in geringerem Maße realisiert worden. Um die Authentizität und Vertraulichkeit der zwischen den einzelnen Instanzen übermittelten Daten sicherzustellen, sind Public Key Infrastructures (PKIs) eine wichtige Voraussetzung. Vor allem der rechtsverbindliche elektronische Austausch von Dokumenten stellt die öffentliche Verwaltung nach wie vor sowohl vor technische als auch organisatorische Herausforderungen, die bisher nicht befriedigend gelöst

121. siehe [v. Lucke et al. 2000], Seite 3

werden konnten. Hinzu kommt die bisherige mangelnde Verbreitung der elektronischen Signatur in allen Gesellschaftsteilen.

4.6.2 Beziehungen in Interaktionen

Neben der Unterteilung nach Interaktionsstufen kann bei E-Government auch eine Unterteilung nach den beteiligten Partnern vorgenommen werden[122], siehe Abbildung 4-1 auf Seite 44:

a. Government-to-Citizen (G2C)
   Elektronische Interaktion zwischen Bürger und Verwaltung – dieser Bereich schließt auch gemeinnützige Organisationen ein
b. Government-to-Business (G2B)
   Elektronische Geschäftsbeziehung zwischen Verwaltung und Wirtschaft
c. Government-to-Government (G2G)
   Elektronische Beziehungen zwischen verschiedenen Behörden und Einrichtungen der öffentlichen Verwaltung

Verwaltungskunden sind somit Bürger, Wirtschaft und andere Verwaltungen. Der Fokus liegt hier auf den Interaktionsbeziehungen G2C und G2B. Abstimmungsbeziehungen zwischen Behörden (G2G) werden im Rahmen der jeweiligen Transaktionsdienstleistungen zwischen der Verwaltung und den Bürgern beziehungsweise der Wirtschaft behandelt. Kommunikationsbeziehungen innerhalb einer Behörde (Government-to-Employee, G2E) werden hier nicht explizit thematisiert.

4.6.3 Transaktionen im E-Government

Wie in Kapitel 4.6.1 bereits beschrieben, handelt es sich bei den Dienstleistungen der öffentlichen Verwaltung nicht nur um Leistungen, sondern auch um Rechte und Pflichten. Um die Handlungsformen der Verwaltung – und damit die möglichen Transaktionen – standardisieren zu können, ist eine funktionale Kategorisierung der Verwaltung notwendig. Dadurch lassen sich allgemeingültige Typen von transaktionalen Dienstleistungen ableiten.

Transaktionale Dienstleistungstypen

Die deutsche Verwaltung lässt sich anhand von Zuständigkeiten und Rechtsformen funktional in die Bereiche der Leistungs- und Eingriffsverwaltung kategorisieren. Aus den kategorisierten funktionalen Verwaltungszweigen lassen sich verschiedene Dienstleistungstypen ableiten und entsprechend in Leistungen und Eingriffe unterteilen.

Bei Leistungen fordern Bürger oder Wirtschaftsunternehmen von der Verwaltung eine Leistung oder Vergünstigung, d. h. sie sind die Initiatoren. Die Leistungen umfassen:

a. Antragsverfahren für staatliche Geldleistungen
b. Gewährung von Subventionen
c. Förderverfahren

122. siehe [v. Lucke et al. 2000], Seite 3

d. Genehmigungsverfahren

Eingriffe liegen vor, wenn die Verwaltung in die Rechtssphäre des Bürgers vordringt und dessen Freiheit oder Eigentum belastet beziehungsweise ihm Verpflichtungen auferlegt. In diesem Fall geht die Einleitung von bestimmten Maßnahmen von der Verwaltung aus. Eingriffe liegen vor bei:

a. Bußgeldverfahren
b. Strafverfolgungsverfahren
c. Gerichtsverfahren
d. Einzug von Steuern
e. Einzug von Zöllen
f. Meldepflichten

Einen weiteren Dienstleistungstyp stellt das öffentliche Beschaffungswesen dar. Hier tritt der Staat als Kunde von Wirtschaftsunternehmen auf. Die Beauftragung von Leistungen oder Gütern ist an bestimmte Verwaltungsverfahren gebunden.

Prozessualer Aufbau von Transaktionsleistungen

Die einzelnen Transaktionstypen lassen sich wiederum in verschiedene Teilschritte unterteilen. Die Teilschritte bestehen aus einer oder mehreren Aktionen, an denen unterschiedliche Rollenträger beteiligt sind. Im Folgenden werden für den Bereich der Leistungen exem-

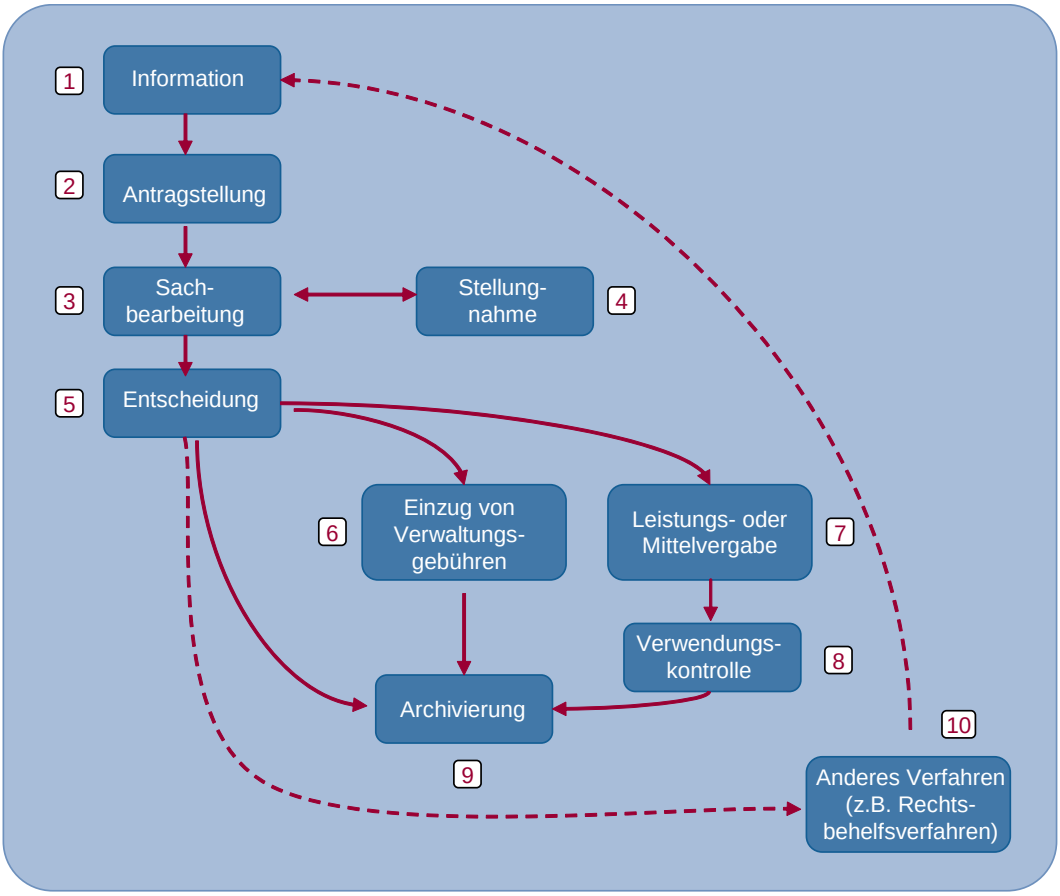


Abbildung 4-3: Teilschritte von Transaktionsleistungen

plarisch Teilschritte, Aktionen und Rollen aufgezeigt. Anhand dieser Methodik lassen sich für jeden anderen Transaktionstyp vergleichbare Prozessmodelle ableiten.

Entsprechend erfolgt für den Bereich der Leistungen die Definition jener Teilschritte, die in der Abbildung 4-3 auf Seite 53 und der Tabelle 4-1 in Beziehung gesetzt und näher erläutert werden. Jeder Teilschritt beinhaltet verschiedene Aktionen und Rollen, die von verschiedenen Akteuren ausgeübt werden. So beinhaltet beispielsweise der Teilschritt Antragstellung als Aktionen die Antragstellung an sich, die Antragsübermittlung sowie die Entgegennahme des Antrags. Die Rolle des Antragstellers wird im Normalfall von einem Bürger oder einem Wirtschaftsunternehmen wahrgenommen. Die Antragsentgegennahme in der Behörde und die Übermittlung an den jeweiligen Sachbearbeiter übernimmt die Poststelle – im Idealfall eine virtuelle.

Äquivalent beinhalten auch die übrigen Teilschritte Aktionen und Rollen, die in der Tabelle 4-1 genannt werden.

	Teilschritte	Aktionen	Rollen
1	Information	Informationsbereitstellung	Redaktion
		Informationsabruf	Interessent
2	Antragstellung	Antragstellung	Antragsteller
		Antragsübermittlung	(virtuelle) Poststelle
		Antragsentgegennahme	Bearbeiter
3	Sachbearbeitung	Sachverhaltsprüfung	Bearbeiter, vorgesetzter Bearbeiter, weitere Bearbeiter
		Informationsanforderung	Bearbeiter, vorgesetzter Bearbeiter, (virtuelle) Poststelle, weitere Bearbeiter
		Informationsabgabe	Antragsteller, (virtuelle) Poststelle
4	Stellungnahme	Informationsbewertung	Bearbeiter, vorgesetzter Bearbeiter, weitere Bearbeiter
5	Entscheidung	Bescheiderstellung	Bearbeiter, vorgesetzter Bearbeiter
		Bescheidzustellung	Antragsteller, (virtuelle) Poststelle
6	Einzug von Verwaltungsgebühren	Gebühreneinzug	Zahlungspflichtiger, (virtuelle) Kasse
7	Leistungs- oder Mittelvergabe	Auszahlung	Bezugsberechtigter, (virtuelle) Kasse

Tabelle 4-1: Teilschritte, Aktionen und Rollen bei Transaktionsleistungen

	Teilschritte	Aktionen	Rollen
8	Verwendungs-kontrolle	Sachverhaltsprüfung	Bearbeiter, vorgesetzter Bearbeiter, weitere Bearbeiter
		Informationsanforderung	Bearbeiter, vorgesetzter Bearbeiter, (virtuelle) Poststelle, weitere Bearbeiter
		Informationsabgabe	Bezugsberechtigter, (virtuelle) Poststelle
9	Archivierung	Archivierung	Bearbeiter, Registratur
10	Anknüpfung an andere Verfahren	Datenübergabe	Antragsteller, Bearbeiter, weitere Behörden, weitere Bearbeiter

Tabelle 4-1: Teilschritte, Aktionen und Rollen bei Transaktionsleistungen

Nicht jeder Dienstleistungstyp, der im Abschnitt „Transaktionale Dienstleistungstypen“ auf Seite 52 definiert ist, muss alle Teilschritte beinhalten. Je nach Vorgang können Teilschritte während der Bearbeitung mehrfach auftreten.

4.7 Bausteine zur Umsetzung von E-Government-Anwendungen

Aus der in Abschnitt 4.6 „Prozesse im E-Government“ auf Seite 51 dargestellten Analyse der Dienstleistungstypen mit der damit verbundenen Identifikation von Teilschritten, Aktionen und Rollen lassen sich funktionale Bausteine ableiten, die – mit entsprechenden Konfigurationsmöglichkeiten versehen – bei der informationstechnischen Abbildung unterschiedlicher Verfahren verwendet werden können. Die potenziellen Einsatzmöglichkeiten dieser Bausteine sind abhängig von der Qualität der Prozessanalyse und der gewählten Software-Architektur[123].

Bei Anwendung des beschriebenen Verfahrens lassen sich exemplarisch die folgenden Typen von Bausteinen definieren:

a. Benutzerschnittstelle
   Anhand der analysierten Rollen ergibt sich die Notwendigkeit, Bausteine zu entwickeln, die Funktionen für den Zugang zur E-Government-Anwendung bereitstellen. Hierzu gehört eine einheitliche, wiedererkennbare Benutzerschnittstelle einschließlich Funktionen zur Benutzer- und Rollenverwaltung sowie zur Authentifizierung der Anwender im System.
b. Prozessbausteine
   Die identifizierten Aktionen werden – z. B. nach Häufigkeit des möglichen Einsatzes bei der Abbildung der Geschäftslogik priorisiert – bei Bedarf standardisiert und als Dienst oder System implementiert.

123. siehe Kapitel 6 „Computational Viewpoint: Referenz-Software-Architektur“ auf Seite 67

c. Infrastrukturbausteine
   Weitere Bausteine vereinheitlichen und realisieren die Kommunikation zwischen den anderen Bestandteilen elektronischer Verfahren.

Die Einer-für-Alle-Angebote (EfA-Angebote) der deutschen Bundesverwaltung, die zum größten Teil im Rahmen der Initiative BundOnline[124] erstellt wurden, werden auf der Website der KBSt[125] als Beispiele für solche Bausteine näher beschrieben. Die Erstellung von Fachanwendungen unter Einsatz wiederverwendbarer Dienste und Systeme wird im Kapitel 6 „Computational Viewpoint: Referenz-Software-Architektur“ auf Seite 67 skizziert.

124. siehe http://www.bundonline2005.de/
125. siehe http://www.kbst.bund.de/efa

5 Information Viewpoint: Standardisierung von Datenmodellen

Dieses Kapitel beschreibt als Information Viewpoint nach RM-ODP[126], wie durch Standardisierung von Datenmodellen und geeignete Modellierungsmethoden die Interoperabilität von Anwendungen hergestellt beziehungsweise verbessert wird.

5.1 Ebenen der Interoperabilität

Ein wichtiges Ziel von SAGA ist die Sicherstellung der Interoperabilität von E-Government-Anwendungen, siehe Abschnitt 1.3 „Ziele“ auf Seite 12. Die Festlegung des Technology Viewpoint auf XML als Standard für den Datenaustausch[127] stellt hierfür lediglich eine technische Basis dar. XML ist zwar eine notwendige technische Grundlage, aber so wie eine Aneinanderreihung korrekter Wörter einer Sprache nicht zwangsläufig einen sinnvollen Satz ergibt, so reicht auch XML allein nicht aus, um Interoperabilität zwischen Anwendungen zu gewährleisten. Um sinnvoll Daten zwischen Systemen austauschen und ihre Weiterverarbeitung sicherstellen zu können, ist es wichtig, Interoperabilität sowohl auf technischer als auch auf organisatorischer und semantischer Ebene sicherzustellen.

Organisatorische Interoperabilität

Organisatorische Interoperabilität klärt vor allem, wann und warum bestimmte Daten ausgetauscht werden. Im Rahmen der organisatorischen Interoperabilität werden also insbesondere die Prozesse, die zum Datenaustausch führen, unter Beachtung rechtlicher Rahmenbedingungen (z. B. Gesetze und Verordnungen) aufeinander abgestimmt.

Technische Interoperabilität

Die reine Möglichkeit zum Datenaustausch wird hingegen als technische Interoperabilität bezeichnet. Zur technischen Interoperabilität gehört die Festlegung von Übertragungswegen und Protokollen (z. B. SOAP, HTTP, FTP, IP, SMTP). Die entsprechenden Standards werden im Technology Viewpoint beispielsweise in Abschnitt 8.7 „Kommunikation“ auf Seite 124 referenziert. Notwendige technische Voraussetzung für Interoperabilität ist auch eine gemeinsame Sprache für die Datenbeschreibung. Im Abschnitt 8.6.6 auf Seite 111 wird XML als obligatorischer Standard für den Datenaustausch benannt.

Semantische Interoperabilität

Semantische Interoperabilität ist gegeben, wenn zwei Systeme Daten so austauschen, dass die Daten von beiden Kommunikationspartnern in gleicher Weise interpretiert werden und Missverständnisse ausgeschlossen sind. Dies bezieht sich nicht nur auf die Form, sondern insbesondere auch auf den Inhalt der übermittelten Daten.

Diese semantische Interoperabilität erreicht man erst durch die Festlegung einer einheitlichen Darstellungsform und einer Semantik für die Elemente der ausgetauschten XML-

126. siehe Kapitel 3 „Architekturmodell für E-Government-Anwendungen“, Abschnitt 3.4 „Computational Viewpoint“ auf Seite 35
127. siehe Abschnitt 8.6.6 „Austauschformate für Daten“ auf Seite 111

Dateien. Diese Festlegung lässt sich beispielsweise durch die Vorgabe konkreter Datenmodelle in Form von XML-Schemata (XSD) oder Regular Language Description for XML New Generation (Relax NG) erreichen[128].

Weiterhin muss durch die Dokumentation der Schemata sichergestellt werden, dass die Bestandteile einheitlich interpretiert werden. Beispielsweise muss dokumentiert werden, ob ein Element „Straße" innerhalb einer Adresse auch die Hausnummer enthält oder ob ein Element „Vorname" mehrere Vornamen oder nur den Rufnamen beinhalten darf.

Die sinnvolle Weiterverarbeitung der Inhaltsdaten kann oft nur dann erfolgen, wenn über die Schemata hinaus weitere Festlegungen getroffen werden. Um zum Beispiel die Angaben von Berufen vergleichbar zu machen, ist eine Festlegung auf bestimmte Schreibweisen und Formulierungen nötig, da eine Software beim einfachen Vergleich der Berufe „Dolmetscher" und „Übersetzer" keine Übereinstimmung feststellen wird. Schreibt man aber die Verwendung des Berufsklassenschlüssels der Deutschen Rentenversicherung Bund vor, so würden alle Datensätze von Übersetzern als Beruf den Wert „8220" enthalten. Damit wäre die Vergleichbarkeit gegeben und semantische Interoperabilität hergestellt. Die Benutzung solcher einheitlicher Codelisten ist daher ein geeignetes Mittel für die Herstellung semantischer Interoperabilität. Darüberhinaus verbessert die Verwendung von Codelisten aber auch die Qualität der zu verarbeitenden Daten. So wird z. B. die Eingabe von Rechtschreibfehlern und unplausiblen Daten in Freitextfeldern durch die in Auswahllisten dargestellten Codes verhindert.

5.2 Gegenstand der Standardisierung von Datenmodellen

Wie bereits in Abschnitt 5.1 dargelegt, sichert die Festlegung von XML als Standard für die Datenbeschreibung in SAGA[129] lediglich die technische Interoperabilität beim Austausch von Daten zwischen Anwendungen. Aufgrund der hohen Flexibilität von XML ist aber allein mit dieser Festlegung keine Vereinheitlichung der Datenmodelle erreicht. Gerade bei Bestandteilen von Datenmodellen, wie z. B. Anschrift und Name einer natürlichen Person, die in verschiedensten E-Government-Anwendungen vorkommen, ist eine Vielzahl von Darstellungsvarianten entstanden. Da in jeder Anwendung das Datenmodell auf andere Weise in XML beschrieben werden kann, ist keine semantische Interoperabilität gegeben. Eine Standardisierung dieser Datenmodelle kann hier zur Vermeidung von Varianten beitragen und die Interoperabilität von Anwendungen, die auf die gleichen standardisierten Datenmodelle setzen, verbessern. Erste Ergebnisse zur Standardisierung von Datenmodellen sind bereits erreicht.

Standardisierungsvorhaben in der Wirtschaft haben gezeigt, dass der Versuch, eine vollständige Standardisierung von Datenmodellen durchzuführen, meist zum Scheitern verurteilt ist. Die Standardisierungsaktivitäten im Rahmen von Deutschland-Online konzentrieren sich daher auf Kommunikationsschnittstellen für den elektronischen Datenaustausch in zwei abgegrenzten Gebieten. Zum einen ist dies die Standardisierung von fachspezifischen

128. siehe Abschnitt 8.3.2 „Austauschformate für Datenmodelle" auf Seite 99
129. siehe Abschnitt 8.6.6 „Austauschformate für Daten" auf Seite 111

Datenmodellen, zum anderen die Standardisierung von fachübergreifenden Datenmodellen, so genannten Kernkomponenten (Core Components).

Fachspezifische Datenmodelle

Unter fachspezifischen Datenmodellen versteht man solche Datenmodelle, die einen starken Fachbezug haben und deren Wiederverwendung deshalb in der Regel auf einen Einsatzbereich beschränkt bleibt, auch wenn mehrere Behörden an dem Austausch der Fachdaten beteiligt sein können. Ein Beispiel für ein solches Datenmodell ist „XMeld" aus dem Meldewesen.

Fachübergreifende Datenmodelle

Im Gegensatz zu fachspezifischen Datenmodellen zeichnen sich fachübergreifende Datenmodelle – auch Kernkomponenten (Core Components[130]) genannt – dadurch aus, dass sie in verschiedenen fachlichen Einsatzbereichen verwendet werden. Beispiele für solche Datenmodelle sind „Name" und „Anschrift".

5.3 Das Deutschland-Online Vorhaben „Standardisierung"

5.3.1 Auftrag und Projektziel

Ziffer 2 des Aktionsplans Deutschland-Online[131] stellt fest, dass verbindliche einheitliche Standards für den Datenaustausch eine unverzichtbare Voraussetzung für durchgängige elektronische Geschäftsprozesse in der öffentlichen Verwaltung in Deutschland sind.

Vor diesem Hintergrund wurde das Deutschland-Online-Vorhaben „Standardisierung" als eines von sechs priorisierten Deutschland-Online-Vorhaben eingerichtet und dem Bund (vertreten durch das Bundesministerium des Innern[132]) und dem Land Bremen (vertreten durch die OSCI-Leitstelle[133]) als Federführer übergeben.

Das Vorhaben soll die Entwicklung und Bereitstellung von fachlichen Standards für den elektronischen Datenaustausch (XÖV-Standards) unterstützen und koordinieren, sodass elektronische Verwaltungsprozesse effizient und in einheitlicher Weise umgesetzt werden können.

Die Ergebnisse des Vorhabens „Standardisierung" sollen insbesondere in den XÖV-Projekten[134] genutzt werden. Für die XÖV-Projekte sollen gemeinsame Methoden, Werkzeuge und Infrastrukturen geschaffen werden. Beispiele solcher XÖV-Projekte sind:

a. „XMeld" (Meldewesen)
b. „XBau" (Bauwesen)

130. siehe Abschnitt 5.4.4 „Kernkomponenten" auf Seite 65
131. für eine ausführliche Darstellung siehe Abschnitt 4.3.2 „Deutschland-Online – Die gemeinsame E-Government-Strategie von Bund, Ländern und Kommunen" auf Seite 40 und siehe http://www.deutschland-online.de/
132. siehe Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung, http://www.kbst.bund.de/
133. siehe OSCI-Leitstelle, http://www.osci.de/
134. siehe http://www.osci.de/, Navigationspunkte „XÖV-Koordination" > „XÖV-Projekte"

c. „XJustiz“ (elektronischer Rechtsverkehr)

d. „XDomea“ (Vorgangsbearbeitung)

e. „XKfz“ (Kraftfahrzeugwesen)

f. „XFinanz“ (Finanzwesen)

5.3.2 XÖV-Arbeitsgruppen

Das Deutschland-Online-Vorhaben „Standardisierung“ teilt sich auf in vier Teilprojekte: „Bestandserhebung und Gesamtkonzept“, „Technische Infrastruktur für XÖV“, „XÖV-Koordination“ und „Kommunikation, Öffentlichkeitsarbeit und Vertretung in Gremien“. Eine ausführliche Darstellung des Gesamtvorhabens kann dem Projekthandbuch[135] entnommen werden.

Im Teilprojekt „XÖV-Koordination“ gibt es zwei Arbeitsgruppen für die Entwicklung einheitlicher Methoden und Konzepte zur Standardisierung der fachspezifischen XÖV-Standards und der fachübergreifenden XÖV-Kernkomponenten:

a. *Arbeitsgruppe „Datenkonferenz“*: In der Arbeitsgruppe arbeiten Experten – vor allem Behördenvertreter der einzelnen XÖV-Projekte (z. B. XMeld, XKfz) – an der Identifikation und Definition fachübergreifender Datenmodelle (XÖV-Kernkomponenten) mit. Auf diese Weise wird sichergestellt, dass die Anforderungen der schon bestehenden XÖV-Projekte in die Datenstandards einfließen und die erstellten Standards in den unterschiedlichen XÖV-Projekten wiederverwendet werden können. Weiterhin wurde im Rahmen der Arbeitsgruppe ein Vorgehen für die Beantragung und Abstimmung von XÖV-Kernkomponenten erarbeitet. Die Arbeit zu den einzelnen Themen wird in verschiedenen Unterarbeitsgruppen geleistet.

b. *Arbeitsgruppe „Auslieferung und Implementierung von XÖV-Standards“*: Die Arbeitsgruppe befasst sich mit dem praktischen Einsatz der fertig gestellten XÖV-Standards. Hierzu werden durch die Arbeitsgruppe u. a. festgelegt:

   i. allgemeine Regeln für die Beschreibung von Testfällen in XÖV-Projekten zur Überprüfung der Konformität von IT-Fachverfahren, die diesen XÖV-Standard implementieren,

   ii. die Namens- und Design-Regeln für XML-Schemata,

   iii. Konzepte für die Verwendung und Pflege von Codelisten sowie

   iv. das Vorgehen bei der Änderung von XÖV-Standards.

5.3.3 XÖV-Framework

Das XÖV-Framework[136] beschreibt ein auf dem V-Modell XT[137] basierendes Vorgehensmodell zur Durchführung von XÖV-Standardisierungsprojekten. Es werden die verschiedenen

135. siehe http://www.deutschland-online.de/, Navigationspunkte „Vorhaben“ > „Priorisierte Vorhaben“ > „Standardisierung“ > „Downloads & Informationen“ > Link „Projekthandbuch“

136. siehe XÖV-Framework v1.0 - Leitlinien für die XÖV-Standardisierung, Oktober 2006, Abbildung 1, http://www.deutschland-online.de/, Navigationspunkte „Vorhaben“ > „Priorisierte Vorhaben“ > „Standardisierung“ > „Downloads & Informationen“ > Link „XÖV-Framework“

137. siehe V-Modell XT, http://www.kbst.bund.de/v-modell und Abschnitt 1.6 „Beziehung zu anderen E-Government-Dokumenten“ auf Seite 13

Projektphasen, die ein XÖV-Projekt durchlaufen sollte, sowie Regeln für den erfolgreichen Abschluss dieser Phasen beschrieben, siehe Abbildung 5-1.

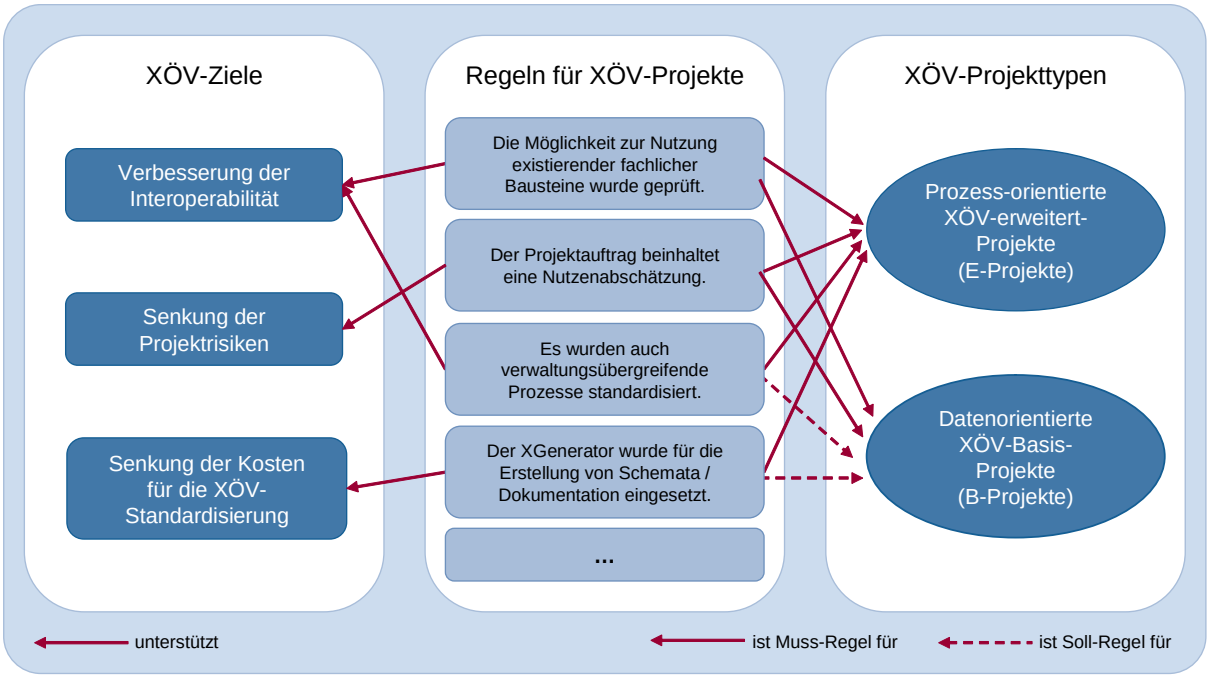


Abbildung 5-1: Ziele, Regeln und Projekttypen im XÖV-Framework

Ziel ist es, einheitliche Qualitäts- und Bewertungskriterien für den Status von laufenden und zukünftigen XÖV-Standardisierungsprojekten zur Verfügung zu stellen. Einheitliche Bewertungskriterien sind wiederum eine wichtige Voraussetzung für die verbindliche Empfehlung von XÖV-Standards und damit für die Anwendung der Projektergebnisse und den Erfolg von Standardisierungsprojekten.

Als Ziele verfolgt das XÖV-Framework insbesondere

a. die Verbesserung der Interoperabilität,
b. die Senkung der Kosten durch Wiederverwendbarkeit sowie
c. die Senkung der Projektrisiken durch Erfahrungsaustausch und Lernen aus Best Practices.

Das XÖV-Framework unterscheidet zwei Arten von XÖV-Projekten:

a. *XÖV-Basis-Projekte (B-Projekte)*: Ziel von B-Projekten ist die Erstellung eines standardisierten Datenmodells oder eines XML-Schemas.
b. *XÖV-erweitert-Projekte (E-Projekte)*: E-Projekte gehen über das Ziel von B-Projekten hinaus und streben die Verbesserung und Standardisierung von verwaltungsübergreifenden Prozessen an (XÖV-Standards für z. B. XMeld).

5.4 Unterstützung für Entwickler von Datenmodellen

Aufgrund der zunehmenden Vernetzung von Anwendungen wird die Sicherstellung der semantischen Interoperabilität durch geeignete Datenmodellierung immer wichtiger. Die

Datenmodellierung in komplexen E-Government-Projekten stellt die Projektverantwortlichen damit vor immer größere Herausforderungen. Das Bundesministerium des Innern unterstützt die Entwickler von Datenmodellen als ersten Schritt zu standardisierten Datenmodellen durch Maßnahmen, die im Folgenden beschrieben werden, siehe auch Abbildung 5-2.

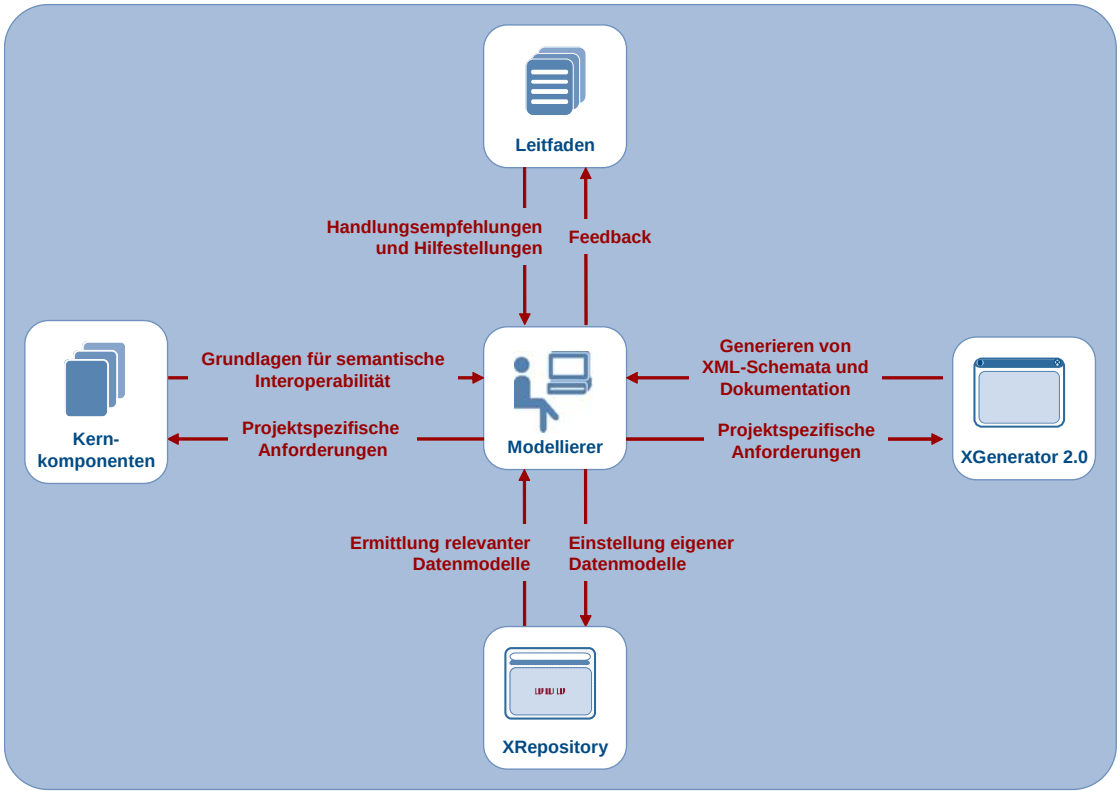


Abbildung 5-2: Unterstützung für Entwickler von Datenmodellen

5.4.1 Leitfaden für Entwickler von Prozess- und Datenmodellen

Die KBSt bietet auf ihrer Homepage einen Leitfaden für Entwickler von Prozess- und Datenmodellen[138] an. Dieser gibt den Projektverantwortlichen praktische Hilfestellungen und Handlungsempfehlungen bei der täglichen Arbeit und beschreibt, wie qualitativ hochwertige Datenmodelle entwickelt werden können.

Der Leitfadens ist so konzipiert, dass der gesamte Ablauf der Prozess- und Datenmodellierung behandelt wird. Er umfasst Ausführungen zur Vorbereitung der Modellierung, zur Modellierung selbst sowie zur Analyse und Optimierung bestehender Modelle. Alle Themenfelder werden vom Leitfaden behandelt und mit Beispielen illustriert.

138. siehe „Leitfaden für Entwickler von Prozess- und Datenmodellen“, KBSt, 2007, http://www.kbst.bund.de/modellierungsleitfaden

5.4.2 XML-Infopoint und XRepository

Eine weitere Hilfestellung stellt die KBSt mit dem XML-Infopoint[139] auf ihrer Homepage zur Verfügung. Hier werden Informationen zu geplanten, laufenden und abgeschlossenen Projekten mit XML-Bezug gesammelt. Durch Berücksichtigung öffentlich zugänglicher Informationen und Spezifikationen thematisch ähnlicher Projekte oder durch Kontaktaufnahme mit den Verantwortlichen anderer Projekte können Synergieeffekte erzielt und die eigenen Aufwände reduziert werden.

Im Frühjahr 2008 soll der XML-Infopoint durch das XRepository abgelöst werden.

Das Hauptziel des XRepository ist die öffentliche Bereitstellung von fachspezifischen und fachübergreifenden Datenmodellen[140], um durch deren Wiederverwendung in Projekten Einsparungen zu erzielen und die Interoperabilität zu verbessern. Ein besonderer Schwerpunkt wird auf standardisierte Datenmodelle (XÖV-Standards und Kernkomponenten) gelegt.

Um eine große Basis an Inhalten zu erhalten, werden die Hürden für die Aufnahme von Datenmodellen so gering wie möglich angesetzt. Dies kann allerdings der Forderung nach hoher Qualität entgegenstehen. Das XRepository wird aus diesem Grund mehrstufig aufgebaut, siehe Abbildung 5-3.

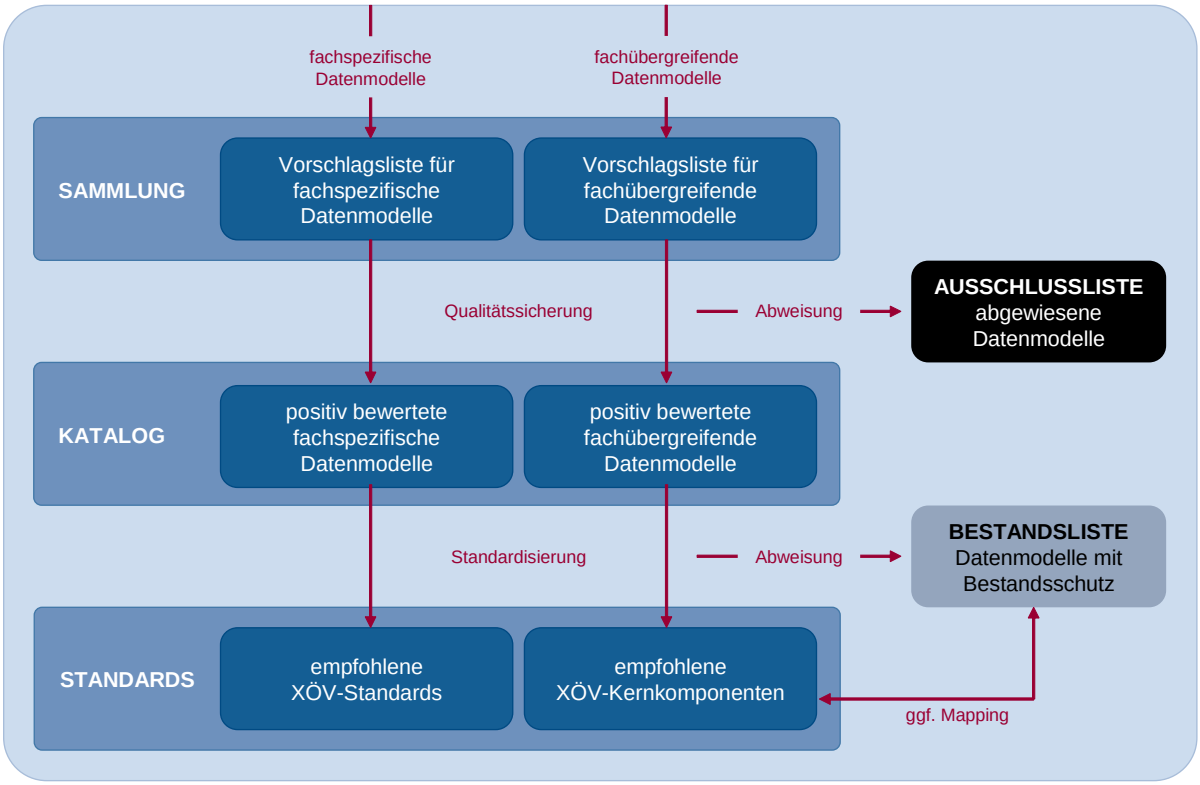


Abbildung 5-3: Standardisierungsprozess im XRepository

Die erste Stufe ist eine **Sammlung**, die die geforderte breite Basis an Datenmodellen aufnimmt. Modelle können hier von registrierten Nutzern ohne große Hürden eingestellt wer-

139. siehe XML-Infopoint, http://www.kbst.bund.de/xml-technologie
140. siehe Abschnitt 5.2 „Gegenstand der Standardisierung von Datenmodellen“ auf Seite 58

den. Lediglich eine kurze Vorprüfung soll die Einstellung irrelevanter und unpassender Inhalte verhindern. Die Nutzer des XRepository werden darauf hingewiesen, dass bei einer Verwendung dieser Modelle eine hohe Qualität und die Kompatibilität zu künftigen Standards nicht sichergestellt sind. Nichtsdestotrotz kann die Wiederverwendung von Modellen aus der Sammlung des XRepository zu Einsparungen durch die Vermeidung von Doppelarbeiten führen. Die Anwendung von Modellen aus der Sammlung ist insbesondere dort geeignet, wo keine Interoperabilität zu anderen Systemen hergestellt werden muss.

Um trotz niedriger Anforderungen an die Sammlung des XRepository eine hohe Qualität sicherstellen zu können, wird eine zweite Stufe eingeführt: ein **Katalog** qualitätsgesicherter Datenmodelle. In diesen Katalog werden nur Modelle aus der Sammlung aufgenommen, die festgelegte Qualitätsanforderungen erfüllen[141].

In die dritte Stufe des XRepository werden die **Standards**, also XÖV-Kernkomponenten (fachübergreifend) und XÖV-Standards (fachspezifisch), aufgenommen. Die standardisierten Datenmodelle erfüllen die Qualitätsanforderungen des Katalogs. Es wird darauf geachtet, dass zu den Standards keine konkurrierenden Datenmodelle im Katalog existieren. Für Modelle des Katalogs, die durch Standards ersetzt werden, wird deshalb eine Bestandsliste eingerichtet. Datenmodelle, die auf dieser Bestandsliste geführt werden, können weiterhin genutzt werden. Neue Projekte sollten aber die Standards verwenden. Um die Ablösung von etablierten Modellen des Katalogs durch Standards zu erleichtern, können im XRepository Migrationshinweise bereitgestellt werden, die die Überführung der etablierten Modelle in XÖV-Kernkomponenten beziehungsweise XÖV-Standards erleichtern. Mappings können die Verwendung der Standards für den Datenaustausch ermöglichen, ohne die etablierten Datenmodelle intern ablösen zu müssen.

Der Einsatz der im XRepository dargestellten Standards zur Datenmodellierung wird insbesondere in solchen E-Government-Anwendungen empfohlen, die einen verwaltungs- oder anwendungsübergreifenden Datenaustausch beinhalten.

Nicht nur in Deutschland, sondern auch auf internationaler Ebene wird die Standardisierung von Datenmodellen – insbesondere auch die Entwicklung von Kernkomponenten – vorangetrieben und es entstehen Repositorys zu ihrer Verbreitung. Auf internationaler Ebene ist das UN/CEFACT führend an der Entwicklung von Kernkomponenten beteiligt[142]. Sofern die deutschen Standards internationalen Datenverkehr berühren, wird frühzeitig ein Austausch mit internationalen Standardisierungsprojekten gesucht.

5.4.3 XGenerator 2.0

Der vom Bundesministerium des Innern bereitgestellte XGenerator 2.0[143] ist ein Werkzeug, mit dem aus UML-Modellen Spezifikationen für einen XML-basierten Datenaustausch automatisiert generiert werden können. Diese Spezifikationen können den Software-Implementationen in einer maschinenlesbaren Form zur Verfügung gestellt werden.

141. Die Qualitätsanforderungen werden nach Publikation des XRepository detailliert auf der Homepage beschrieben werden.
142. siehe Core Component Library, http://www.unece.org/cefact/codesfortrade/codes_index.htm#ccl
143. siehe XGenerator 2.0, http://www.kbst.bund.de/xgenerator

Eine Spezifikation besteht hierbei aus einer Menge von maschinenlesbaren XML-Schemata und einer dazu konsistenten Dokumentation für die Anwendungsentwickler. Durch die Nutzung des XGenerator 2.0 kann eine ansonsten notwendige und schwierige manuelle Pflege der Schemata und der Dokumentation vermieden werden. Bei Änderungen an dem Fachmodell können unter Einsatz des XGenerator 2.0 die neuen XML-Schemata sowie Dokumentationen automatisiert generiert werden.

Der XGenerator 2.0 bietet die folgenden Funktionalitäten, siehe Abbildung 5-4:

a. Validierung von UML-Modellen gegen das XÖV-UML-Profil[144]
b. automatische Generierung sowie Validierung von XML-Schema-Dateien aus UML-Modellen
c. automatische Generierung von DocBook-Dateien[145] aus UML-Modellen

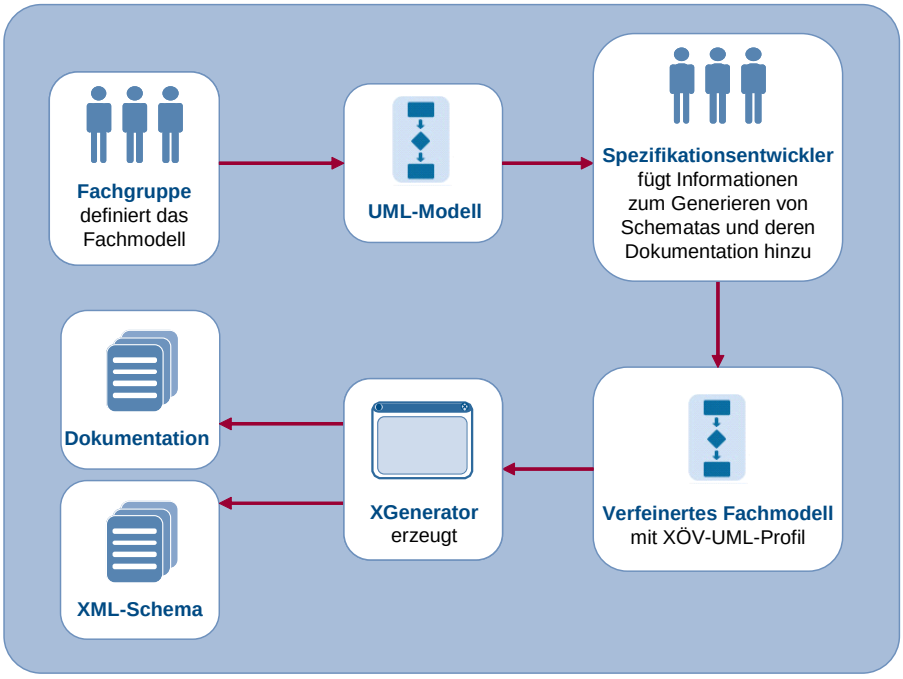


Abbildung 5-4: Arbeitsweise des XGenerator 2.0

5.4.4 Kernkomponenten

Für den medienbruchfreien elektronischen Austausch von Daten auch über verschiedene Fachgebiete hinweg werden fachübergreifende standardisierte Datenmodelle benötigt, z. B. wenn Personendaten zwischen Meldewesen und Kfz-Wesen ausgetauscht werden sollen. Vom United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) wurde zu diesem Zweck das Konzept der Kernkomponenten (Core Components) entwi-

144. Ein UML-Profil ist ein Standardmechanismus, um die UML-Spezifikation individuell zu erweitern. Das XÖV-UML-Profil definiert u. a. eine Menge von spezifischen Zusatzannotationen (Stereotypen), um die Generierung von XML-Schemata und deren Dokumentation zu steuern, siehe http://www.osci.de/, Navigationspunkte „XÖV-Koordination“ > „XÖV-UML-Profil“.

145. DocBook ist ein offenes Dokumentenformat, das von OASIS (Organization for the Advancement of Structured Information Standards) standardisiert wurde und gut geeignet ist, um daraus Druck- und Online-Formate zu generieren, wie z. B. PDF und HTML.

ckelt. Im Rahmen des Deutschland-Online-Vorhabens „Standardisierung“ wurden für eine Reihe von Kernkomponenten Entwürfe erstellt, die dem Kooperationsausschuss automatische Datenverarbeitung Bund / Länder / Kommunaler Bereich (KoopA ADV) zur Verabschiedung vorgelegt werden und dann der deutschen Verwaltung zur Verfügung stehen. Zu diesen Kernkomponenten gehören u. a.:

a. Natürliche Person
b. Name einer natürlichen Person
c. Organisation
d. Behörde
e. Anschrift
f. Geschlecht
g. Religion
h. Familienstand
i. Ausweisdokument
j. Sprache
k. Staat
l. Zeitraum

Entwickler von Datenmodellen können diese Kernkomponenten als Vorlage nehmen und durch das Weglassen von Attributen, die Einschränkung von Wertebereichen beziehungsweise der Kardinalitäten eine Fachkomponente erstellen, die den Anforderungen des jeweiligen Datenaustauschs entspricht. Durch die redundanzfreie Modellierung (eine Information kann nicht in verschiedenen Elementen untergebracht werden) und eindeutige Dokumentation der Kernkomponenten wird unterstützt, dass die Daten ohne menschlichen Eingriff ausgetauscht werden können. Zum Beispiel legt die Kernkomponente „Anschrift“ fest, dass die Hausnummer ein eigenes Attribut ist und nicht zusammen mit dem Namen der Straße gespeichert werden darf. Nur wenn alle Kommunikationspartner ihre Daten nach den gleichen Regeln modellieren, können Konflikte beim automatischen Datenaustausch vermieden werden.

Durch die Beteiligung der XÖV-Projekte an der Entwicklung der Kernkomponenten wird sichergestellt, dass sie deren Anforderungen erfüllen. Das DOL-Vorhaben „Standardisierung“ stellt sicher, dass neue Anforderungen bei der Pflege der Kernkomponenten berücksichtigt werden und entsprechend dem Bedarf weitere Kernkomponenten erstellt werden.

Finale Versionen und Entwürfe von Kernkomponenten und Fachkomponenten sollen zukünftig im so genannten XRepository gespeichert und allgemein verfügbar gemacht werden.

6 Computational Viewpoint: Referenz-Software-Architektur

Der Computational Viewpoint nach RM-ODP[146] beschreibt den architektonischen Aufbau von verteilten E-Government-Anwendungen in abstrakter Form und lässt Realisierungsdetails außer Betracht. In diesem Kapitel werden Architekturentscheidungen erläutert und die resultierende Referenz-Software-Architektur dargestellt. Des Weiteren werden Hilfestellungen bei der Konzeption und Entwicklung langfristig betreibbarer, wartbarer und weiterentwickelbarer E-Government-Anwendungen für die Bundesverwaltung gegeben.

Der Begriff „Referenz-Software-Architektur" bezeichnet hier eine idealtypische Architektur für die Bundesverwaltung. Er beschreibt den konzeptionellen Aufbau der E-Government-Anwendungen (konkret: Dienste[147] und Systeme[148]) einer Verwaltung oder – allgemeiner – einer Organisation.

Im Abschnitt 6.1 werden allgemeine nicht-funktionale Anforderungen an die Entwicklung von Anwendungen beschrieben, die losgelöst vom Einsatz im E-Government zu betrachten sind. Die Ausprägung dieser Anforderungen beeinflusst die zu treffenden Architekturentscheidungen.

Im Abschnitt 6.2 „Realisierungsoptionen und Architekturparadigmen" werden wesentliche Alternativen und Richtlinien zu Architekturentscheidungen vorgestellt. Die Optionen und Paradigmen spiegeln den heutigen Stand der Software-Architektur wider.

Abschließend wird im Abschnitt 6.3 aufbauend auf den Anforderungen und Lösungsalternativen aus den Abschnitten 6.1 und 6.2 eine Referenz-Software-Architektur für E-Government-Anwendungen entwickelt.

6.1 Allgemeine Anforderungen an Software-Anwendungen

Der Computational Viewpoint in SAGA gibt Hilfestellung beim Entwurf von E-Government-Anwendungen unter Beachtung der in SAGA deklarierten Ziele[149] und der im Rahmen der Betrachtungen des Enterprise Viewpoint in Kapitel 4 dargestellten Leitbilder und Anforderungen.

Neben den spezifischen funktionalen Anforderungen an die Entwicklung einer E-Government-Anwendung, wie sie sich beispielsweise aus der Fachspezifikation ableiten lassen, gibt es eine Reihe allgemeiner Anforderungen mit Relevanz für die Architektur. Die folgende Aufzählung solcher nicht-funktionalen Anforderungen erfolgt alphabetisch und spiegelt somit keine Gewichtung der einzelnen Anforderungen unter software-technischen

146. siehe Kapitel 3 „Architekturmodell für E-Government-Anwendungen", Abschnitt 3.4 „Computational Viewpoint" auf Seite 35
147. Dienste sind Entitäten, die Funktionalität für Anwendungen bereitstellen. Die Nutzung der Dienste kann es externen Anwendungen darüber hinaus ermöglichen, die vom Dienst bereitgestellten Ressourcen zu verwalten. Dienste werden über ihre Schnittstellen und die bereitgestellte Funktionalität spezifiziert.
148. Systeme sind Entitäten, die dem Anwender komplexe Funktionalitäten zur Verfügung stellen. Sie nutzen hierfür gegebenenfalls bereitgestellte Dienste.
149. siehe Abschnitt 1.3 „Ziele" auf Seite 12

Gesichtspunkten wider[150]. Insbesondere spielen jedoch die in SAGA festgeschriebenen Ziele Interoperabilität und Wiederverwendbarkeit eine herausragende Rolle.

a. Erweiterbarkeit
   Erweiterbarkeit bezeichnet die Fähigkeit, dem System wirtschaftlich neue Funktionalität hinzuzufügen oder die bestehende Funktionalität zu erweitern, ohne dass diese dadurch beeinträchtigt wird. Insbesondere, wenn E-Government-Anwendungen über einen langen Zeitraum betrieben werden, müssen sie bei sich ändernden gesetzlichen Regelungen erweiterbar sein.

b. Flexibilität
   Das Merkmal „Flexibilität" beschreibt allgemein die Fähigkeit, eine Architektur zu modifizieren, um neue, nicht-funktionale Anforderungen kostengünstig zu erfüllen. Eine änderbare Topologie erlaubt eine schnelle Modifikation einer verteilten Architektur und verbessert damit nicht-funktionale Anforderungen wie Verfügbarkeit, Zuverlässigkeit und Skalierbarkeit.

c. Interoperabilität
   Interoperabilität bezeichnet die medienbruchfreie Realisierung von Transaktionsdienstleistungen zwischen behördenübergreifenden Fachanwendungen. Eine organisatorische Voraussetzung dafür ist, dass die Verwaltungsprozesse aufeinander abgestimmt sind, damit die sie abbildenden E-Government-Anwendungen miteinander interagieren können.

d. Offenheit
   Das Merkmal „Offenheit" eines E-Government-Systems ist mitentscheidend für den erfolgreichen Einsatz. Damit bestehende und neue Systeme ohne größeren Aufwand in andere Systeme integriert werden können, müssen sie über wohl definierte und dokumentierte Schnittstellen verfügen oder so gekapselt werden, dass sie zumindest über Portale integriert werden können.

e. Performanz
   Das Merkmal „Performanz" (oder auch „Leistungsfähigkeit") eines Systems bezeichnet generell die Fähigkeit, Funktionalität schnell genug auszuführen, um die Nutzbarkeit des Systems zu gewährleisten.
   Ein Maß für die Leistungsfähigkeit ist die Kapazität eines Systems, d. h. die Fähigkeit, eine gegebene Anzahl von Aufträgen pro Zeiteinheit verarbeiten zu können.

f. Sicherheit
   Sicherheit beschreibt die Zusicherung, dass Informationen nur in Übereinstimmung mit der formulierten Sicherheitspolitik modifiziert oder publiziert werden können.
   Vertraulichkeit, Authentizität und Nachvollziehbarkeit sowie die Anwendung des Bundesdatenschutzgesetzes und die Beachtung der relevanten Kapitel des E-Government-Handbuchs zum Thema Sicherheit müssen beim Einsatz von Online-Dienstleistungen gewährleistet sein, siehe auch Kapitel 8.1 „IT-Sicherheitskonzeption" auf Seite 93.

g. Skalierbarkeit
   Skalierbarkeit beschreibt die Fähigkeit, auch bei steigender Nutzungslast einer Anwendung die gewünschte Effizienz und Performanz beim Betrieb zu gewährleisten. Eine

150. siehe [KBSt 2007]

Verteilung der Anwendung oder deren Bestandteile muss problemlos durchführbar sein.

h. Verfügbarkeit
   Verfügbarkeit ist ein Maß dafür, wie ausfallsicher eine Anwendung Funktionalität, Dienste oder Ressourcen zur Verfügung stellt.

i. Wartbarkeit
   Wartbare E-Government-Anwendungen zeichnen sich dadurch aus, dass Betrieb und Pflege wirtschaftlich erfolgen. Eine effiziente Wartung muss für externe Fachleute, die nicht an der Entwicklung des Systems beteiligt waren, ohne größere Einarbeitung möglich sein.

j. Wiederverwendbarkeit
   Wiederverwendbarkeit bezeichnet die mehrmalige Nutzung von Anwendungen oder ihrer Bestandteile bei gleichen oder ähnlichen Dienstleistungen. Eine redundante Entwicklung wird somit vermieden. Eine Wiederverwendung kann auf verschiedenen Abstraktionsebenen erfolgen, z. B. Erfahrungsaustausch zwischen Behörden sowie Nutzung gemeinsamer Daten- und Prozessmodelle, Architekturmuster und zentraler Dienste.

Eine konkrete Gewichtung der verschiedenen Anforderungen hängt von Faktoren ab, die im Rahmen des Fachkonzepts der einzelnen E-Government-Anwendungen erarbeitet und bewertet werden müssen. So ist beispielsweise bei Anwendungen, die über sehr hohe Zugriffszahlen verfügen, eher die Verfügbarkeit von Bedeutung, während bei umfangreichen Genehmigungsverfahren die Sicherheit stärker im Vordergrund stehen könnte.

Weitere Erläuterungen können dem „IT-Architekturkonzept für die Bundesverwaltung“ [KBSt 2007] entnommen werden.

6.2 Realisierungsoptionen und Architekturparadigmen

In den folgenden Abschnitten werden Realisierungsoptionen und Architekturparadigmen vorgestellt, die bei der Realisierung von E-Government-Anwendungen beachtet werden sollten beziehungsweise aus denen die geeigneten Optionen ausgewählt werden sollten. Die Optionen und Paradigmen spiegeln den heutigen Stand der Technik wider. Weitere Informationen können dem „IT-Architekturkonzept für die Bundesverwaltung“ [KBSt 2007] entnommen werden.

6.2.1 Komponentenbasierte Entwicklung

Unter einer Komponente versteht man eine Software-Entität, die ohne Änderung in Software-Anwendungen verwendet werden kann, die außerhalb der Kontrolle der Entwickler der Komponente liegen. Nutzer haben in der Regel keinen Zugriff auf den Quellcode einer Komponente, können deren Verhalten jedoch in der von den Entwicklern der Komponente vorgesehenen Art und Weise anpassen.

Komponenten bieten über Exportschnittstellen ihre Funktionalität an und verwenden für die Realisierung der angebotenen Funktionalität gegebenenfalls wieder von anderen Kom-

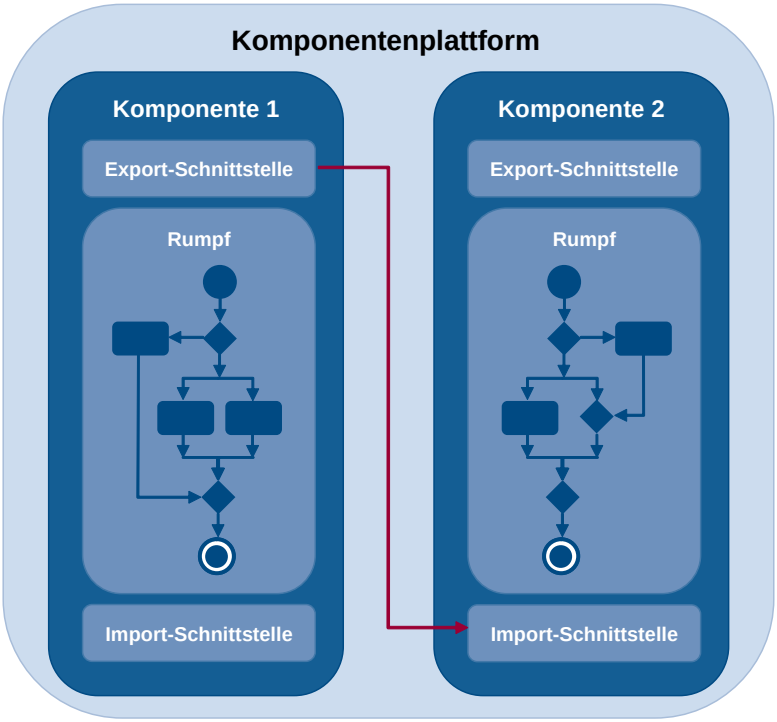


Abbildung 6-1: Komponentenbasierte Entwicklung

ponenten angebotene Funktionalitäten, deren Nutzung in der Importschnittstelle spezifiziert wird, siehe Abbildung 6-1. Da die Beschreibung der von einer Komponente angebotenen und konsumierten Funktionalitäten von der eigentlichen Realisierung entkoppelt ist, können die Realisierungen für die Nutzer unbemerkt ausgetauscht werden, was viele Möglichkeiten für eine Weiterentwicklung der Realisierung bietet.

Eine weitere wesentliche Verbesserung im Vergleich zu rein objektorientierten Konzepten bieten standardisierte Laufzeitumgebungen für Komponenten in Form von Applikations-Servern oder leichtgewichtigeren Frameworks, die die deklarative Nutzung spezieller fachunabhängiger Leistungen wie Autorisierung, Lokalisierung, Persistenz oder Transaktionsverwaltung für Komponenten anbieten. Da diese Funktionalitäten nicht mehr in den Komponenten selbst realisiert werden müssen, lässt sich die Software-Erstellung vereinfachen und beschleunigen. Weiterhin ist ein Austausch und eine einfache Wiederverwendung von Komponenten im Sinne des Paradigmas zur Trennung von Zuständigkeiten (separation of concerns) in anderen Anwendungskontexten möglich. Damit Komponenten die Funktionalität einer Plattform nutzen können, müssen spezielle Komponenten-Plattform-Kontrakte implementiert werden, d. h. Komponenten werden immer für genau einen Typ von Komponentenplattform realisiert.

6.2.2 Diensteorientierte Software-Architektur

Der Begriff „Dienst“ bezeichnet ein Konzept aus dem Kontext der Geschäftsprozessmodellierung, das für eine wiederholbare Ausführung von Geschäftsaktivitäten steht. Der im Folgenden zugrunde gelegte Ansatz fordert, dass Dienste zustandslos sind – im Gegensatz zur komponentenbasierten Entwicklung. Die Abbildung 6-2 „SOA-Referenzmodell“ auf Seite 71 visualisiert beispielhaft die Diensterbringung und Dienstnutzung in einer dienste-

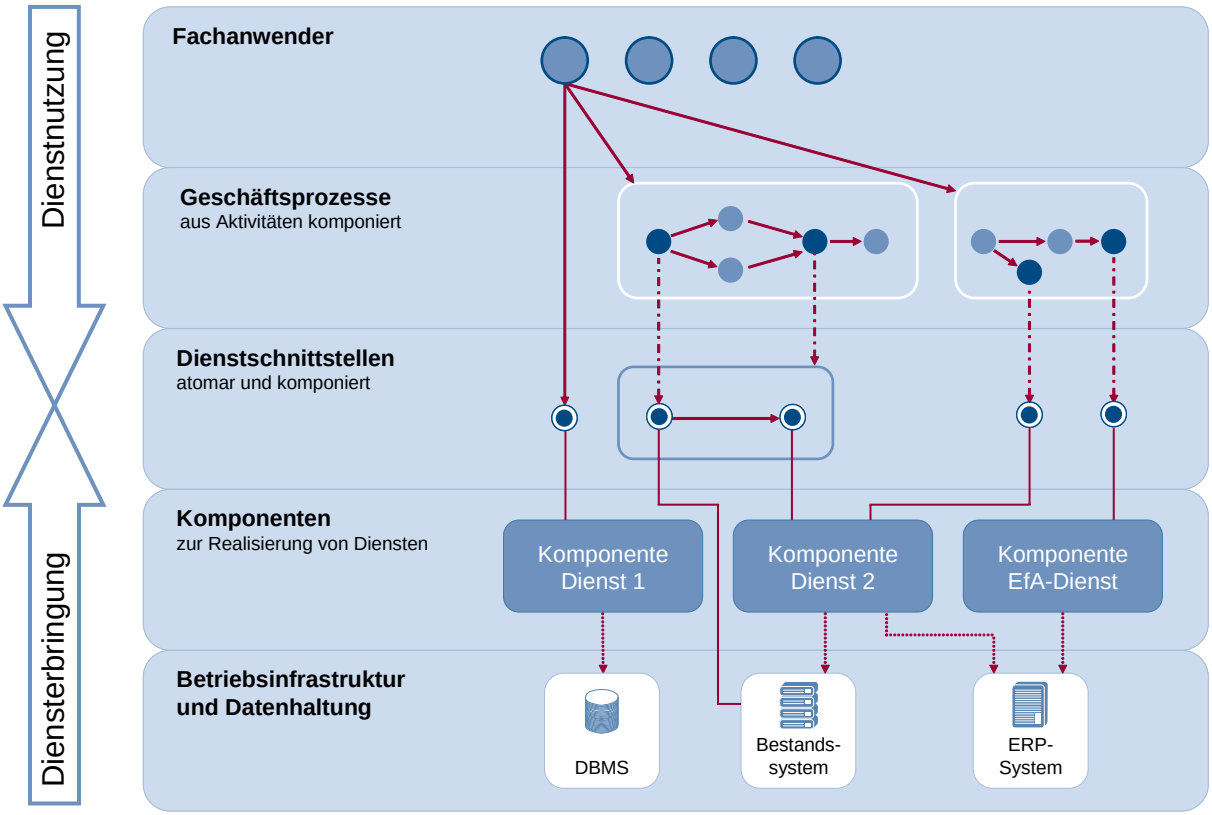


Abbildung 6-2: SOA-Referenzmodell

orientierten Architektur (Englisch: Service Oriented Architecture – SOA). Die einzelnen Ebenen in der Darstellung dienen nur der logischen Gliederung und stellen keine Schichten im Sinne eines Schichtenmodells dar.

Dienste stellen ihre Funktionalität über Schnittstellen (mittig in Abbildung 6-2 die dunklen Kreise mit hellem Rand) bereit. Wie die Funktionalität erbracht wird, ist für die Nutzer irrelevant. Die Funktionalität neu implementierter Dienste wird durch Komponenten realisiert. Mit Hilfe von Konnektoren kann die Funktionalität von Bestandssystemen modular gekapselt und als Dienste zur Verfügung gestellt werden.

Fachanwender (oben in Abbildung 6-2 die hellen Kreise mit dunklem Rand) nutzen die Dienste entweder direkt oder integrieren sie in ihre Geschäftsprozesse. Diese Prozesse (weiße Rahmen) entstehen durch die Komposition von einzelnen Aktivitäten (Kreise). Die Aktivitäten nutzen innerhalb einer Komposition andere Aktivitäten. Jede Aktivität erfordert entweder einen manuellen Eingriff (heller Kreis) oder kann auf Dienste abgebildet werden (dunkler Kreis). Diese Abbildung kann auf einen atomaren, also allein stehenden, Dienst oder eine Komposition, also einen Zusammenschluss, von Diensten (symbolisiert durch den Rahmen um zwei Dienstschnittstellen) erfolgen. Durch die Komposition bestehender Dienste wird den Geschäftsprozessen und Fachanwendern ein höherwertiger Dienst zur Verfügung gestellt.

Die technische Stärke einer diensteorientierten Architektur liegt darin, dass sie die Kombination bereits bestehender Funktionalität unabhängig von den zur Realisierung verwende-

ten Technologien ermöglicht. Eine diensteorientierte Architektur muss jedoch einige Voraussetzungen erfüllen:

a. Für die Interaktion zwischen Diensten und ihren Nutzern (die Pfeile in Abbildung 6-2 in Richtung Dienstschnittstellen und deren Kompositionen) muss eine Kommunikationsbasis festgelegt werden, die auf allgemein akzeptierten Standards basiert[151]. Der Dienst muss diese Standards beherrschen, um nutzbar zu sein.
b. Potenzielle Nutzer müssen Informationen über verfügbare Dienste erhalten können. Ein Repository kann diese Informationen zur Verfügung stellen und so einen einheitlichen Zugriff auf Dienste ermöglichen.

Aus wirtschaftlicher Sicht ermöglicht die diensteorientierte Architektur eine Kostenreduzierung bei der Entwicklung und dem Betrieb von Anwendungen, wenn eine größere Anzahl von Diensten zur Verfügung steht und diese von vielen Anwendungen genutzt werden. Dann können der Entwicklungsaufwand und die Entwicklungszeit für neue Anwendungen reduziert werden, da nur noch die Funktionalität realisiert werden muss, die nicht durch bereits vorhandene Dienste abgedeckt wird. Insbesondere der zentrale Betrieb von Diensten ermöglicht Kostenersparnisse durch sparsameren Ressourceneinsatz und reduzierten Personalbedarf.

Ein Verzeichnis für elektronische Dienste der öffentlichen Verwaltung wird durch das Deutsche Verwaltungsdiensteverzeichnis (DVDV) realisiert. Darin sind die zur Nutzung notwendigen Verbindungsparameter der Dienste gespeichert, siehe Abschnitt 7.4.1 auf Seite 91.

6.2.3 Mehrschichtenarchitektur

Im Folgenden wird erläutert, warum Mehrschichtenarchitekturen sowohl in einer komponentenbasierten als auch in einer diensteorientierten Ausprägung die Erfüllung der im Abschnitt 6.1 genannten Anforderungen unterstützen.

Trennung von Geschäfts- und Datenhaltungslogik

Die Trennung von Geschäfts- und Datenhaltungslogik minimiert die Abhängigkeiten von Systemen beziehungsweise Diensten vom Datenbankhersteller. Auf steigende Anforderungen, z. B. an die Performanz oder Verfügbarkeit, kann mit dem Austausch der Datenbank reagiert werden, ohne dass eine Änderung in der Geschäftslogik notwendig wird. Außerdem kann dieselbe Software einfacher mit anderen Datenbankprodukten wiederverwendet werden.

Trennung von Präsentations- und Geschäftslogik

Eine Trennung von Präsentations- und Geschäftslogik bietet eine technische Lösung zur optimalen Unterstützung mehrerer Präsentationskanäle, wie verschiedene Browser-Typen oder mobile Endgeräte, z. B. Personal Digital Assistants (PDAs). Neben diesem Aspekt führt die Trennung von Präsentations- und Geschäftslogik zu einer wesentlich besseren Strukturierung der Architektur, wodurch Wartbarkeit, Fehlerbehebung, Flexibilität, Wiederverwendbarkeit und Nachvollziehbarkeit deutlich verbessert und somit mittelfristig die Kosten

151. siehe Abschnitt 8.7.1.2 „Middleware-Kommunikation mit verwaltungsexternen Applikationen“ auf Seite 127

gesenkt werden. Außerdem unterstützt die Trennung eine potenzielle Verteilbarkeit der Anwendung auf mehrere Server, wobei ein Server die Präsentationsschicht und ein zweiter Server die Geschäftslogik bedient, von der aus die Dienste angesprochen werden, die wiederum auf anderen Servern laufen können. Damit wird der Betrieb in den Aspekten Sicherheit, Wartbarkeit und Skalierung positiv beeinflusst. Hierbei sollte besonderes Augenmerk auf die Kommunikation gelegt werden, da eine nicht optimale Verteilung die Performanz negativ beeinflusst.

Trennung von Client und Präsentationslogik

Um zu vermeiden, dass jede Anwendung die Installation einer eigenen Client-Software erfordert, wird der einheitliche Zugang über den Browser empfohlen, siehe Abschnitt 8.5.1 „Informationszugriff mit Computern“ auf Seite 104. Da aus Gründen der Barrierefreiheit und der Sicherheit E-Government-Anwendungen auch dann noch nutzbar sein sollen, wenn beim Client alle aktiven Inhalte deaktiviert wurden, müssen die Daten server-seitig in einer eigenen Präsentationsschicht aufbereitet werden. Für verschiedene Clients können zielgerichtet für die jeweiligen Anforderungen unterschiedliche Präsentationen generiert werden.

Mehrschichtenarchitektur

Die Trennung von Client, Präsentationslogik, Geschäftslogik und Datenhaltungslogik führt zu einer Mehrschichtenarchitektur:

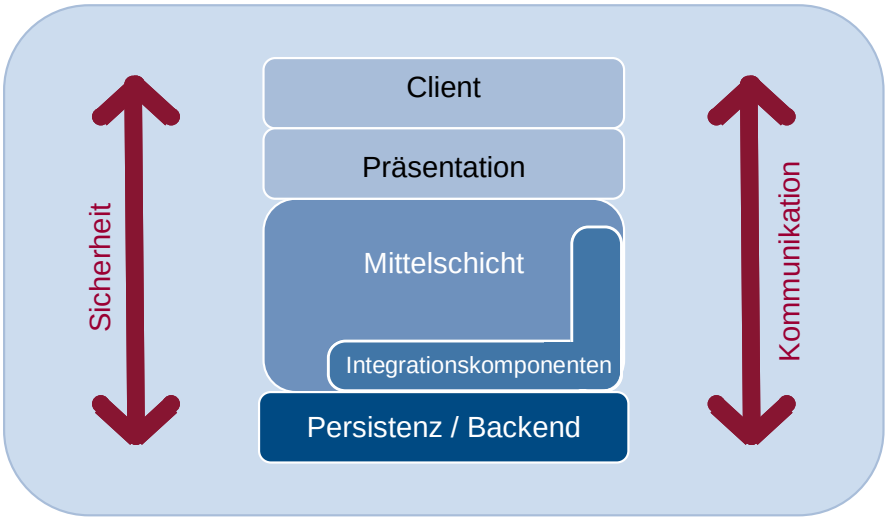


Abbildung 6-3: Strukturelle Sicht – Mehrschichtenarchitektur

a. In der **Client-Schicht** findet die Interaktion zwischen Benutzer und Software statt. Die von der Präsentationslogik aufbereiteten Daten sowie das User Interface werden visualisiert. Die Client-Schicht repräsentiert somit unterschiedliche Zugriffskanäle, die sich aufgrund unterschiedlicher Benutzer, Endgeräte, Übertragungswege, aber auch unterschiedlicher Anwendungszwecke ergeben, um mit den Fachanwendungen zu interagieren. Auf folgende Endgeräte wird in SAGA Bezug genommen:
   i. Web-Zugriff über Web-Browser oder spezielle Browser-Plug-Ins,

ii. Mobilfunktelefone und Personal Digital Assistants (PDAs),

iii. externe Anwendungen (z. B. ERP-Systeme)

b. Die **Präsentationsschicht** realisiert die Aufbereitung der Anwendungsdaten für den Client (z. B. als Web-Seite) und die Interaktion des Nutzers mit der Fachanwendung. Die Präsentationsschicht umfasst alle Standards zur Kommunikation mit den betrachteten Endgeräten der Client-Schicht.

c. Die **Mittelschicht**, auch Geschäftsschicht genannt, implementiert die Geschäftslogik, unabhängig von deren Präsentation, und verarbeitet die Daten aus der Persistenzschicht. Dies erfolgt auf Basis von Diensten und – soweit es nicht durch Dienste erbracht werden kann – durch Komponenten. Hier findet die Programmablaufkontrolle statt, die das Zusammenspiel der Dienste und Komponenten steuert.

d. Die **Persistenzschicht** ist für die Speicherung von Datenobjekten zuständig. Sie abstrahiert von der Datenbank. Das **Backend** steht als Sammelbegriff für Funktionalitäten des Betriebssystems, spezifische Datenbanken, aber auch bestehende gegebenenfalls nicht SAGA-konforme Anwendungen, wie Bestands- oder ERP-Systeme.

6.3 Referenz-Software-Architektur für E-Government-Anwendungen

Interoperabilität, Wiederverwendbarkeit, Wirtschaftlichkeit, Offenheit und Skalierbarkeit sind wesentliche Anforderungen an E-Government-Anwendungen[152]. Die hier beschriebene Referenz-Software-Architektur basiert auf den Realisierungsoptionen und Architekturparadigmen aus dem Abschnitt 6.2, die wiederum dazu dienen, die allgemeinen Anforderungen aus Abschnitt 6.1 zu erfüllen. Sie setzt auf Mehrschichtenarchitekturen und erlaubt sowohl den Einsatz von Diensten als auch direkt von Komponenten. Die Implementierung sollte objektorientiert erfolgen[153].

6.3.1 Architekturentscheidungen

Aufgrund der heterogenen Anforderungen der unterschiedlichen Behörden ist es nicht sinnvoll, eine auf nur einem Architekturparadigma basierende Referenz-Software-Architektur zu definieren, die für alle Anwendungen angewandt werden soll. Vielmehr ist es notwendig, von Fall zu Fall zu betrachten, welcher Ansatz der geeignete ist.

Die Möglichkeit eines diensteorientierten Ansatzes[154] sollte stets geprüft werden, da er hohe Flexibilität, Interoperabilität, Wiederverwendbarkeit und Offenheit ermöglicht. Führt eine Organisation eine diensteorientierte Architektur ein, ist in der Regel eine enge Zusammenarbeit zwischen IT- und Fachseite erforderlich, um bestehende Geschäftsprozesse zu dokumentieren und geeignete Dienste zu identifizieren. Die Vorteile des neuen Ansatzes kommen vor allem dann zum Tragen, wenn bestehende Prozesse im Hinblick auf die neue Architektur überarbeitet werden.

152. siehe Abschnitt 1.3 „Ziele“ auf Seite 12
153. siehe [KBSt 2007], Abschnitt 3.3.1
154. siehe Abschnitt 6.2.2 „Diensteorientierte Software-Architektur“ auf Seite 70

Diensteorientierte Architekturen erfordern im Vergleich zu komponentenbasierten Architekturen eine zusätzliche Abstraktionsebene. Diese Abstraktion wird durch Kommunikationsprotokolle erreicht, die von allen Komponentenplattformen unterstützt werden. Diese Protokolle haben dann meist eine eingeschränkte Funktionalität und sind weniger performant als spezielle plattformspezifische Kommunikationsprotokolle. Unter folgenden Bedingungen ist es ratsam, statt einer diensteorientierten Architektur eine komponentenbasierte Architektur zu realisieren:

a. Es werden Anforderungen an die Performanz der Anwendung gestellt, die im Rahmen einer diensteorientierten Architektur nicht realisiert werden können (z. B. Antwortzeiten).
b. Die zu unterstützenden Geschäftsprozesse sind so komplex, dass die einzelnen Aktivitäten nicht mehr auf zustandslose Dienste abgebildet werden können.
c. Die Flexibilität der diensteorientierten Architektur wird nicht benötigt.

Detailliertere Empfehlungen zur Auswahl des geeigneten Architekturparadigmas können den Abschnitten 3.4 „Architekturentscheidungen“ und 4 „Fallbezogene Architekturentscheidungen“ des „IT-Architekturkonzepts für die Bundesverwaltung“ [KBSt 2007] entnommen werden.

6.3.2 Einführung einer diensteorientierten Architektur

Im Folgenden werden organisatorische Herausforderungen sowie der Kostenaspekt bei der Einführung einer diensteorientierten Architektur betrachtet.

Wesentliche organisatorische Herausforderungen sind:

a. Der Einführungsprozess einer diensteorientierten Architektur ist komplex, da die Anwendungslandschaft durch eine Vielzahl bestehender Systeme geprägt ist und nur wenig Spielraum für Neuentwicklungen und Anpassungen besteht. Aus diesem Grund vollzieht sich eine solche Einführung über einen längeren Zeitraum. Die Einführung sollte schrittweise erfolgen und zunächst mit einem Pilotprojekt beginnen.
b. Eine Vielzahl wieder verwendbarer Dienste entsteht erst dann, wenn Dienste anwendungsübergreifend im Hinblick auf eine IT-Gesamtarchitektur im Sinne eines Bebauungsplans der gesamten Anwendungslandschaft und nicht anwendungsspezifisch entwickelt werden. Dies setzt ein IT-Architekturmanagement voraus, das für die Planung und Ausgestaltung der IT-Gesamtarchitektur verantwortlich ist, siehe „IT-Architekturkonzept für die Bundesverwaltung“ [KBSt 2007]. Das IT-Architekturmanagement ist ein kontinuierlicher Prozess, der sowohl strategische als auch operationale Elemente beinhaltet.
c. Diensteorientierte Architekturen haben im Vergleich zu herkömmlichen Architekturen beziehungsweise Architekturen mit weitgehend geschlossenen Einzelanwendungen andere, oft komplexere Anforderungen beziehungsweise Herausforderungen bezüglich der Sicherheit. In einer diensteorientierten Architektur ist nicht mehr die IT-Sicherheit einzelner Fachanwendungen, sondern aller an einem Fachverfahren beteiligten, möglicherweise verteilt betriebenen Dienste zu berücksichtigen. Diese Anforderungen

sind bereits im Entwicklungsprozess mit verteilten Verantwortlichkeiten und später im Betrieb abzustimmen.

d. Eine parallele Entwicklung von Diensten in verschiedenen Projekten, die in einer Anwendung zusammen zum Einsatz kommen sollen, macht ein projektübergreifendes Projektmanagement – d. h. ein Multi-Projekt-Management – erforderlich. Nur so können projektübergreifende Anforderungen erfüllt werden.
e. Die projektübergreifende Natur einer diensteorientierten Architektur hat Auswirkungen auf die Organisation und Durchführung des Testens, beispielsweise durch Versionswechsel von Diensten. Alle nutzenden Anwendungen sind dann von den Testaktivitäten betroffen.
f. Durch die unabhängig voneinander erfolgende Weiterentwicklung der Dienste durch unterschiedliche Lieferanten müssen Änderungen im Rahmen eines Änderungsmanagements für alle betroffenen Anwendungen abgestimmt werden. Es sind Regeln für neue Versionen der Dienste (Release Policy) wie Umfang und darauf abgestimmter Testaufwand für alle Lieferanten zu definieren.
g. Die verteilte Zuständigkeit für die Entwicklung und den Betrieb von Diensten erfordert ein Service Level Management für ein angemessenes und wirtschaftlich sinnvolles Niveau der IT-Dienstleistungen, wobei für konkrete Dienste jeweils SLAs (Service Level Agreements) zwischen Dienstnutzern und Dienstanbietern abgeschlossen werden müssen. Die Organisation des IT-Betriebs muss prozessorientiert und diensteorientiert erfolgen. Als Basis eignen sich dafür die Empfehlungen aus ITIL[155].
h. Diensteorientierung erfordert die Entwicklung neuer Abrechnungsmodelle, die der verteilten Entwicklung und dem verteilten Betrieb der Anwendungen beziehungsweise Dienste gerecht werden.

Die Einführung einer diensteorientierten Architektur führt insbesondere am Anfang zu erhöhten Investitionen, da z. B. durch den Einsatz neuer Prinzipien und Techniken Schulungsbedarf für Mitarbeiter entsteht und die zuvor genannten organisatorischen Herausforderungen zu bewältigen sind.

6.3.3 Dreischichtenarchitektur für Dienste

Bei der Realisierung eines Dienstes mit einer Mehrschichtenarchitektur nach Abschnitt 6.2.3 entfällt die Präsentationsschicht, siehe Abbildung 6-4 auf Seite 77. Dies liegt daran, dass Dienste ihre Funktionalität aus der Geschäftslogik, also der Mittelschicht, heraus erbringen. Der Nutzer des Dienstes ist eine andere Anwendung (Client), die gegebenfalls selbst für die Präsentation der Ergebnisse zuständig ist. Diensterbringung und Dienstnutzung erfolgen wie in Abbildung 6-2 „SOA-Referenzmodell“ auf Seite 71 beschrieben.

6.3.4 Vierschichtenarchitektur für E-Government-Systeme

Die Abbildung 6-5 auf Seite 78 veranschaulicht beispielhaft den Aufbau in einer konkreten Ausprägung für eine Mehrschichtenarchitektur eines E-Government-Systems entsprechend der allgemeinen Beschreibung im Abschnitt 6.2.3. Man erkennt, dass die Präsentati-

155. siehe Abschnitt 7.1 „IT-Service-Management mittels ITIL“ auf Seite 81

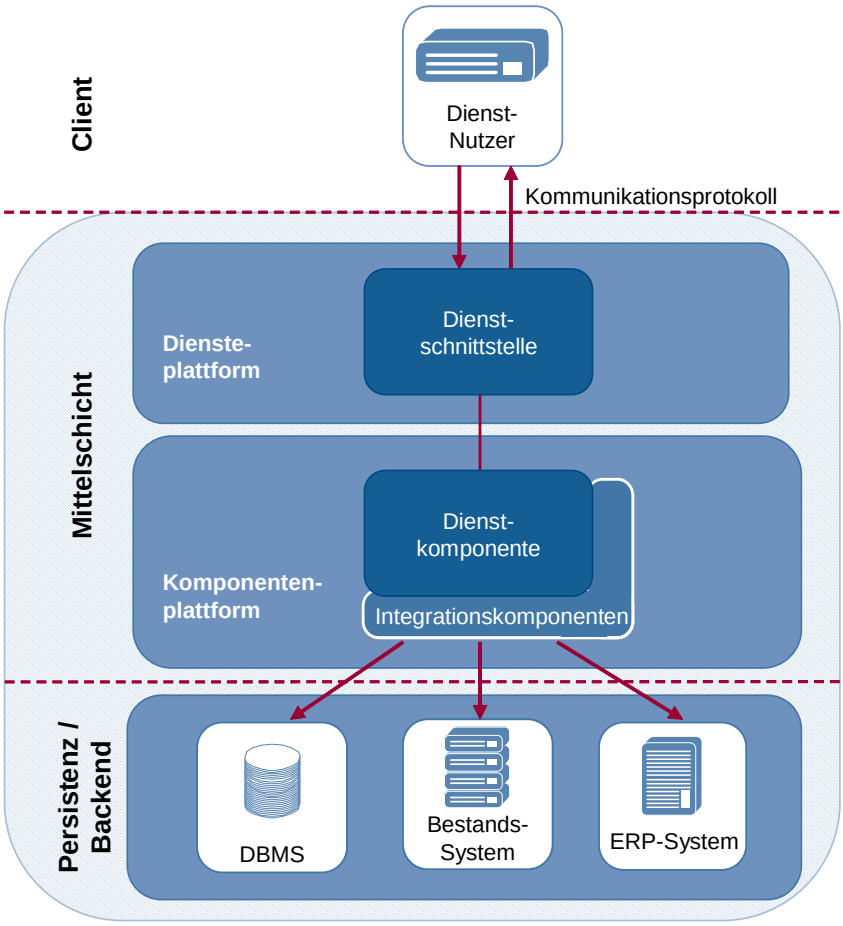


Abbildung 6-4: Modell einer Dreischichtarchitektur von Diensten

onsschicht aus einem Presentation Application Server besteht, der beispielsweise mit Java Server Pages HTML- und XML-Daten generiert. Der Business Application Server in der Mittelschicht bildet das Rückgrat der Anwendung und erbringt die Fachfunktionalität auf Basis von Diensten und Komponenten. Über Anwendungsschnittstellen (oder auch Dienstschnittstellen wie in Abbildung 6-4) kann externen Anwendungen und Diensten ein Zugriff auf das E-Government-System unter Umgehung der Präsentationsschicht ermöglicht werden.

Die Einbindung von Bestands- und ERP-Systemen erfolgt über entsprechende Integrationskomponenten. Die Systeme stellen ihre Funktionalität über Anwendungsschnittstellen oder Dienstschnittstellen bereit. Gegebenenfalls sind Konnektoren notwendig, um Bestandssysteme modular zu kapseln.

6.3.5 Sicherheit

Um die Anforderungen an die Sicherheit umzusetzen, sind die im E-Government-Handbuch beschriebenen Design-Empfehlungen zu berücksichtigen. Von besonderer Relevanz sind die Module „Sichere Integration von E-Government-Anwendungen – SIGA“[156] und „Sichere Architekturen für Client-Server-Architekturen für E-Government“ im Unterkapitel „IT und IT-Sicherheit“. Zwar auf komponentenbasierte Realisierung zugeschnitten, lassen

156. siehe [SIGA]

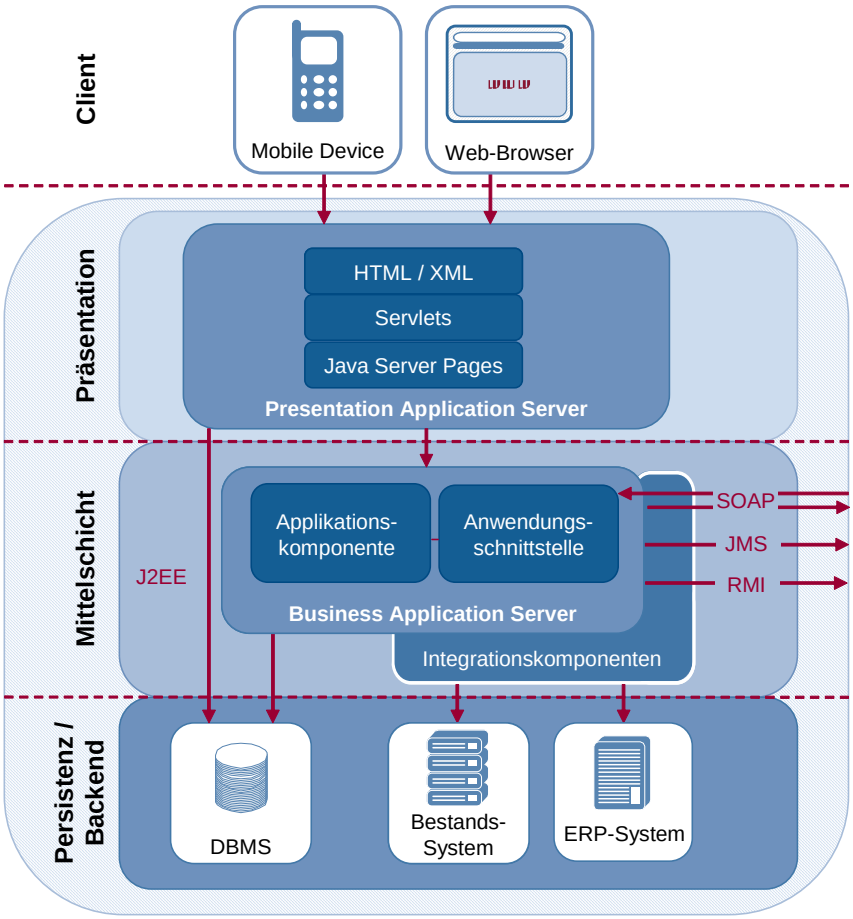


Abbildung 6-5: Beispielmodell einer Vierschichtenarchitektur von E-Government-Systemen

sich die angeführten Architekturprinzipien in der Regel eins-zu-eins auf diensteorientierte Architekturen übertragen.

6.3.6 Wiederverwendung und Integration von EfA-Angeboten

Beim Entwurf einer zu erstellenden E-Government-Anwendung wird geprüft, welche Dienste und Systeme neu entwickelt werden müssen und wo bestehende verwendet werden können. Insbesondere sind vorrangig die auf der KBSt-Website aufgeführten EfA-Dienste, EfA-Systeme, Infrastrukturen und EfA-Konzepte zu berücksichtigen[157].

Der Begriff „Dienst" bezeichnet ein Konzept aus dem Kontext der Geschäftsprozessmodellierung, das für eine wiederholbare Ausführung von Geschäftsaktivitäten steht. Die *EfA-Dienste* stellen ihre Funktionalität über Schnittstellen bereit. Von den Eigenschaften der Implementation wird vollständig abstrahiert. Beispiele für EfA-Dienste sind:

a. Zahlungsverkehrplattform (ePayment)
b. Verzeichnisdienst
c. GeoDatenZentrum (GDZ)

157. siehe „EfA-Angebot und Netze": http://www.kbst.bund.de/efa.

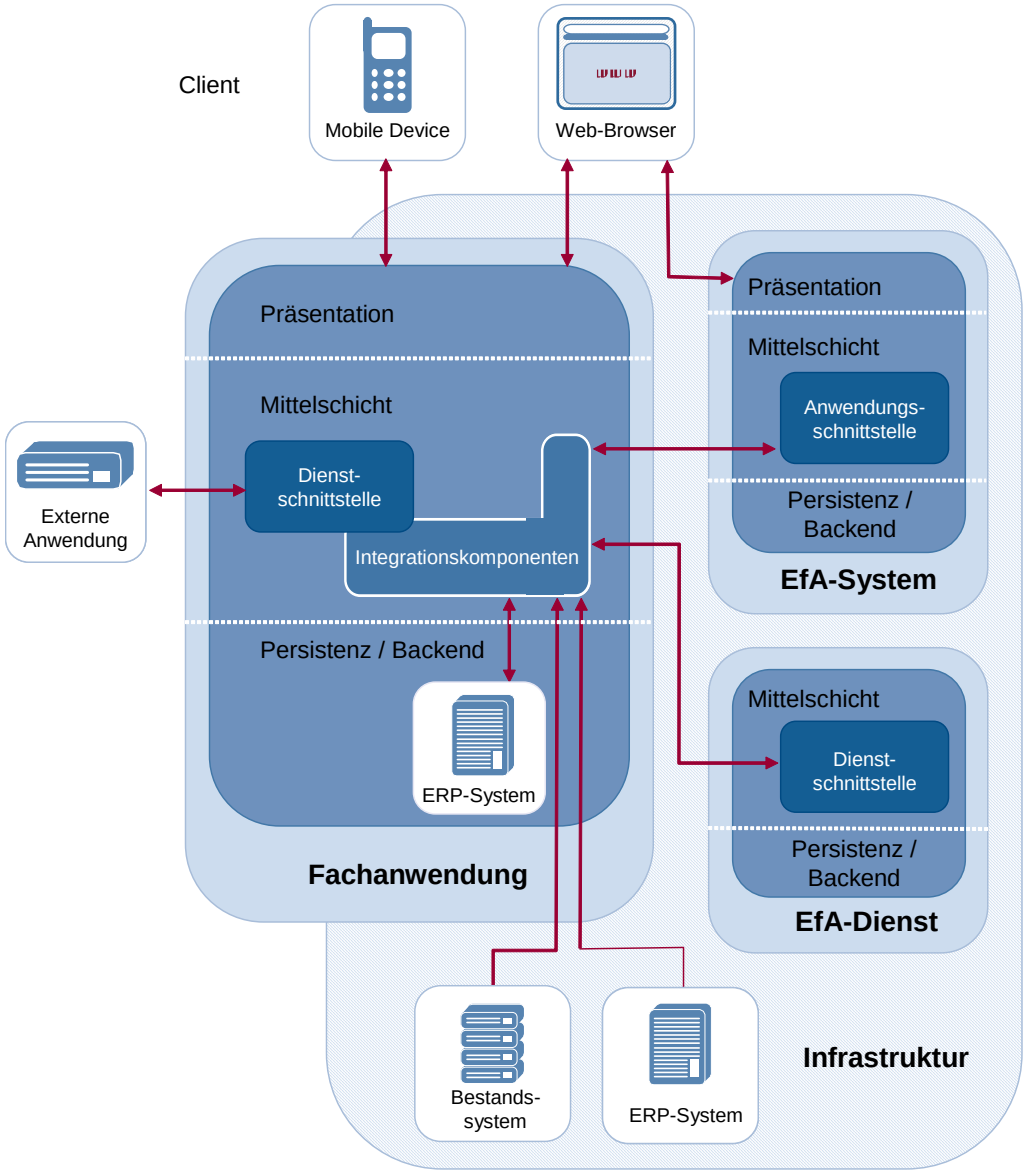


Abbildung 6-6: Integration von EfA-Angeboten

Ein *EfA-System* ist ein einheitliches Ganzes, eine Software-Entität, die ein komplexe Funktionalität zur Verfügung stellt. Zu den EfA-Systemen zählen beispielsweise:

a. Formular-Management-System (FMS)
b. Content-Management-System (CMS)
c. Travel-Management-System (TMS)

Die Leistungen von *Infrastrukturen* sind unabhängig von konkreten E-Government-Anwendungen, aber von grundlegender Bedeutung für eine behördenübergreifende elektronische Kommunikation. Als Infrastruktur stehen zum Beispiel zur Verfügung:

a. Informationsverbund der Bundesverwaltung (IVBV)
b. Deutsches Verwaltungsdiensteverzeichnis (DVDV)
c. Public-Key-Infrastruktur der Verwaltung (V-PKI)

Ein *EfA-Konzept* beschreibt ein allgemeines wiederverwendbares Vorgehen für die Realisierung konkreter Sachverhalte in E-Government-Anwendungen. Als Konzepte stehen beispielsweise zur Verfügung:

a. ArchiSafe
b. Online-Beratung

Wird das EfA-System Datensicherheit[158] eingesetzt, muss eine eigene Client-Anwendung (der OSCI-Client-Enabler) bei den Nutzern der Online-Dienstleistung installiert werden. Der Browser bleibt jedoch der bevorzugte Client für E-Government-Anwendungen, weshalb dieses Szenario keinen Eingang in die Referenz-Software-Architektur gefunden hat.

Komplexere E-Government-Anwendungen sind mit Integrationskomponenten ausgestattet, um existierende IT-Anwendungen wie die EfA-Angebote, Bestandssysteme und besonders nicht SAGA-konforme Anwendungen zu integrieren. Diese Integrationskomponenten, wie in Abbildung 6-6 auf Seite 79 gezeigt, sind direkt in der Mittelschicht angesiedelt. Sie bieten Kommunikationsmöglichkeiten zu Anwendungen, wie z. B. ERP-Lösungen, an, soweit diese nicht als Dienst bereitstehen und über eine Dienstschnittstelle angesprochen werden können. Im letzten Fall ist keine gesonderte Integrationskomponente erforderlich.

158. siehe EfA-System Datensicherheit („Virtuelle Poststelle"): http://www.kbst.bund.de/efa-vps

7 Engineering Viewpoint: IT-Service-Management und Referenzinfrastruktur

Dieses Kapitel beschreibt als Engineering Viewpoint nach RM-ODP[159] Betriebsprozesse und Aufbau einer effektiven und sicheren Infrastruktur. Aktuelle Anforderungen an Datenschutz, Datensicherheit, Leistungsfähigkeit und Verfügbarkeit von E-Government-Anwendungen setzen dabei hohe Maßstäbe an die Betreiber der Anwendungen und die technische Infrastruktur. Daher muss für die Anwendungen eine geeignete technische Infrastruktur aus den physikalischen Ressourcen aufgebaut und für die Nutzer durch die Netzwerkebene mit externen Diensten geeignet verbunden werden, die nur im Rahmen kontinuierlicher Prozesse des IT-Service-Managements erfolgreich und sicher betrieben werden kann.

7.1 IT-Service-Management mittels ITIL

Für die Gestaltung, die Implementierung und das Management wesentlicher Steuerungsprozesse in der IT bietet die „IT Infrastructure Library" (ITIL) als ein Best Practice eine etablierte Grundlage.

Während der Erstellung von SAGA 4.0 ist die weiterentwickelte Version ITIL 3.0 erschienen. Um auf ein erprobtes Vorgehen zu setzen und auf deutschsprachige Literatur verweisen zu können, wird im Engineering Viewpoint die durch KBSt-Dokumente unterstützte Version ITIL 2.0 vorgestellt.

7.1.1 Einführung in ITIL

ITIL ist kunden-, service- und prozessorientiert und besteht aus acht eng miteinander verzahnten Schwerpunktpublikationen, die sich mit der Unterstützung von Geschäftsprozessen durch IT-Prozesse beschäftigen. Das IT-Service-Management unterteilt sich in

a. taktische Prozesse zur Planung und Umsetzung von Service-Anforderungen (Service Delivery) sowie
b. operative Prozesse zur Unterstützung der Qualität und Wirtschaftlichkeit der Services im täglichen Betrieb (Service Support),

die einführend in einer Studie des BSI dargestellt und mit Synergien zur ebenfalls als kontinuierlicher Prozess betrieben IT-Sicherheit ergänzt werden[160].

Ein erfolgreiches IT-Service-Management erfordert das Zusammenwirken der einzelnen Prozesse, wobei auch eine gegenseitige Steuerung und Kontrolle stattfindet. In ITIL werden dazu die Aufgaben der Prozesse beschrieben, aber die konkrete Abgrenzung kann nach den speziellen Gegebenheiten gestaltet werden. Da die Prozesse ständig betrieben werden müssen, sind dafür konkrete Verantwortlichkeiten erforderlich. Nach ITIL werden daher zunächst Rollen für die jeweiligen Prozessmanager definiert, die dann mit Personen zu

159. siehe Kapitel 3 „Architekturmodell für E-Government-Anwendungen", Abschnitt 3.5 „Engineering Viewpoint" auf Seite 36
160. siehe [BSI 2005]

besetzen sind. Hierbei kann eine Person mehrere Rollen übernehmen, wenn sich dadurch keine Interessenkonflikte ergeben und die Vertretung gesichert ist. Bei der Einführung von ITIL muss daher mit der Abstimmung der Prozesse und Verantwortlichkeiten begonnen werden.

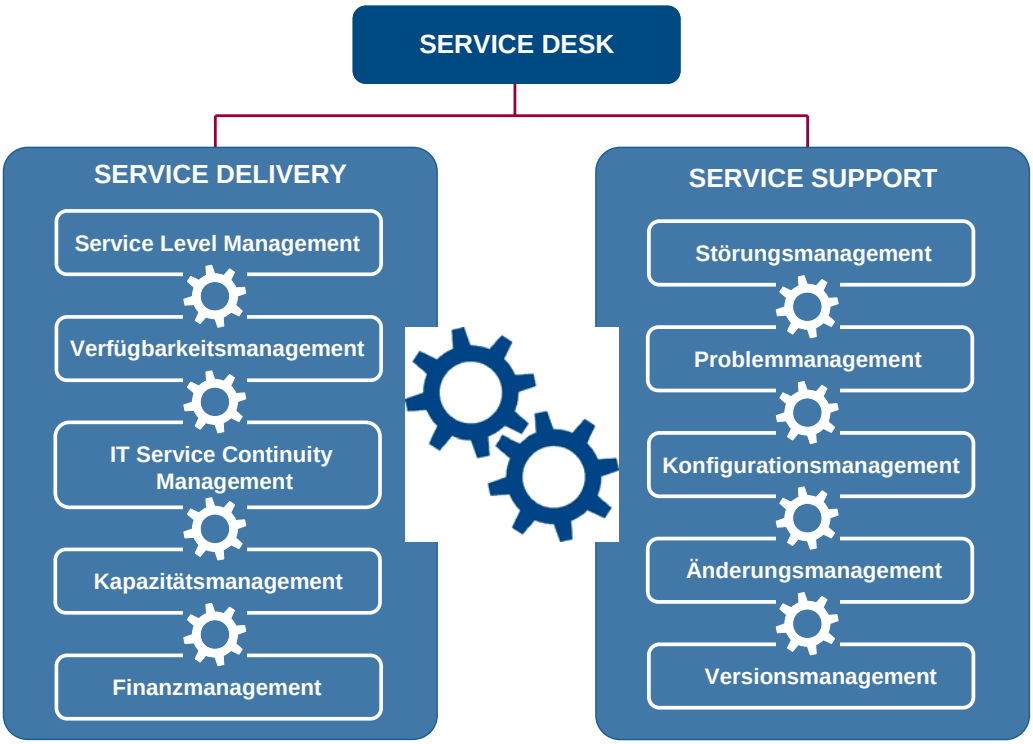


Abbildung 7-1: ITIL-Prozesse im Überblick

Die ITIL-Prozesse kommunizieren untereinander über gemeinsam genutzte Informationssammlungen. Wesentlich für die Kontrolle von Prozessen ist das Berichtswesen, welches in allen ITIL-Prozessen zur Qualitätssicherung integriert ist. Auch eine objektive Erfolgskontrolle wird in ITIL durch den Einsatz von so genannten Key-Performance-Indikatoren unterstützt.

7.1.2 Taktische IT-Service-Management-Prozesse (Service Delivery)

Für E-Government-Anwendungen als Dienstleistungen müssen die konkreten Service-Anforderungen der Kunden geplant und dauerhaft umgesetzt werden. Dazu müssen nach ITIL die Service Delivery Prozesse betrieben werden.

Service Level Management

Bei der Entwicklung einer neuen E-Government-Anwendung werden Kundenanforderungen als konkretes Service-Angebot in einer Service-Vereinbarung (Service Level Agreement, SLA) zwischen Dienstleister und Kunden ausgehandelt. Dabei werden die Funktionalität, aber auch nichtfunktionale Anforderungen wie Leistungsfähigkeit (nach der Anzahl gleichzeitig aktiver Nutzer) oder Verfügbarkeit (mit maximalen Ausfall- und Wiederherstellungszeiten) abgestimmt. Ziel ist die klare Definition der Erwartung beider Seiten an eine

neue Dienstleistung. Neben der erstmaligen Erstellung eines SLA werden auch spätere Kundenwünsche und die Überwachung der Einhaltung des SLA durch den Prozess Service Level Management geregelt. Dieser Prozess steuert und überwacht sowohl die Leistungsfähigkeit als auch die Qualität einer Dienstleistung.

Verfügbarkeitsmanagement (Availability Management)

Die funktionsfähige Bereitstellung von E-Government-Anwendungen in den erforderlichen Geschäftszeiten steuert das Verfügbarkeitsmanagement (Availability Management). Ziel ist die kosteneffektive Sicherung einer ununterbrochenen Verfügbarkeit entsprechend den Geschäftserfordernissen. Einzubeziehen sind auch die Abhängigkeiten von externen Dienstleistern, z. B. durch Wartungsverträge.

IT Service Continuity Management (ITSCM)

IT ist ein wichtiger Produktionsfaktor, dessen Weiterfunktionieren auch unter Auswirkungen von Katastrophen im ITIL-Prozess IT Service Continuity Management (ITSCM) geplant werden muss. Dies erfolgt im Rahmen des Business Continuity Managements (BCM), welches den Wiederanlauf der Geschäftsprozesse zur Sicherung der erforderlichen Mindestproduktionskapazitäten sicherstellt.

Kapazitätsmanagement (Capacity Management)

Der wirtschaftliche Umgang mit IT-Ressourcen soll für wettbewerbsfähige Dienstleistungen durch den ITIL-Prozess Kapazitätsmanagement (Capacity Management) langfristig gesteuert werden.

Finanzmanagement (Financial Management)

Die Steuerung der Kosten für E-Government-Anwendungen und damit die Plan- und Steuerbarkeit der Wirtschaftlichkeit, z. B. durch Budgetierung, erfolgt durch den ITIL-Prozess Finanzmanagement (Financial Management). Hierbei kann auch eine Verrechnung von Dienstleistungen mit Kunden geregelt werden.

7.1.3 Operative IT-Service-Management-Prozesse (Service Support)

Die Service-Qualität von E-Government-Anwendungen kann nur in Abhängigkeit vom operativen Betrieb gesteuert werden. Dazu werden durch die ITIL-Prozesse des Service Support alltäglich die IT-Dienstleistungen erbracht.

Service Desk

Die effektive Kommunikation mit Kunden ist eine wirksame Voraussetzung zum erfolgreichen Betrieb von E-Government-Anwendungen. Dazu muss den Kunden beziehungsweise Anwendern ein schneller und einfacher Kontakt zur IT bereitgestellt werden. Entsprechend ITIL ist dazu ein zentraler Anlaufpunkt, der Service Desk, einzurichten, der die Kommunikation wirtschaftlich bündelt und trotzdem kontinuierliche Anwenderbetreuung sichert. Bei E-Government-Anwendungen kann auch die Kommunikation mit dem Bürger im Rahmen des Service Desks erfolgen. Zur Erhöhung der Akzeptanz sollte ein Service Desk durch mög-

lichst viele Kommunikationswege, wie Telefon, E-Mail oder Web-Anwendungen, erreichbar sein.

Störungsmanagement (Incident Management)

Die Meldung von Störungen, aber auch allgemeine Anfragen müssen aufgenommen und zügig durchgängig bearbeitet werden. Der ITIL-Prozess Störungsmanagement (Incident Management) nimmt Meldungen von Anwendern auf, sichert reaktiv die durchgängige Bearbeitung bei geringstmöglicher Beeinträchtigung des Anwenders und informiert ihn über den Stand der Behebung. Um eine hohe Zufriedenheit der Anwender zu sichern, wird eine entsprechend dem SLA (siehe „Service Level Management" auf Seite 82) fristgerechte Behebung entsprechend der Support-Stufe überwacht und gegebenenfalls auch durch Eskalation beschleunigt. Das Störungsmanagement sollte durch Software, wie ein Ticketingsystem (auch als Trouble Ticket System bezeichnet), unterstützt werden, um Meldungen zu verwalten, an andere Prozesse zu kommunizieren und auch auswerten zu können. Das Störungsmanagement umfasst auch die Aufnahme von Meldungen über Sicherheitsvorfälle und hat daher eine hohe Bedeutung für die Informationssicherheit[161].

Problemmanagement (Problem Management)

Können bei Störungen die Ursachen nicht sofort eindeutig ermittelt und behoben werden, so kann das Störungsmanagement den Service für den Anwender mit einer Ausweichlösung schnell wiederherstellen, gleichzeitig aber den ITIL-Prozess Problemmanagement (Problem Management) mit der Fehlersuche beauftragen. Die Behebung der eigentlichen Ursachen von Störungen, die auch proaktiv erfolgen kann, verbessert die Zuverlässigkeit und Wirtschaftlichkeit von IT-Dienstleistungen.

Konfigurationsmanagement (Configuration Management)

Für den Betrieb von E-Government-Anwendungen wird eine Informationsgrundlage für alle IT-Service-Management-Prozesse benötigt. Der ITIL-Prozess Konfigurationsmanagement (Configuration Management) verwaltet Informationen über die Eigenschaften und Zusammenhänge aller Komponenten der IT-Infrastruktur. Dazu gehört auch die Archivierung von Master-Kopien der eingesetzten Software. Die anderen ITIL-Prozesse können diese Informationen nutzen, aber auch Konfigurationsänderungen anmelden.

Änderungsmanagement (Change Management)

Zur Weiterentwicklung von IT oder zur Behebung von Störungsursachen müssen verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozessen und Verfahren vorgenommen werden. Zur Steuerung und Kontrolle dieser Änderungen wird der ITIL-Prozess Änderungsmanagement (Change Management) eingesetzt. Wesentlich ist hierbei die Abstimmung aller Betroffenen über zu erwartende Auswirkungen der geplanten Änderungen in einem so genannten Änderungsfreigabe-Gremium (Change Advisory Board, CAB). Erst nach einer Freigabe im CAB besteht ein vertretbares Risiko, die Verfügbarkeit von IT-Dienstleistungen nicht durch Änderungskonflikte zu gefährden. Änderungen müssen

161. siehe [BSI 2005]

getestet und durch angemessene Rückfallverfahren abgesichert sein. Die Pflege eines Änderungskalenders vereinfacht die Koordinierung.

Versionsmanagement (Release Management)

Die Weiterentwicklung von Infrastrukturen erfolgt in neuen Versionen. Der ITIL-Prozess „Versionsmanagement (Release Management)" umfasst Planung, Gestaltung, Erzeugung, Konfiguration, Test, Abnahme und Inbetriebnahme einer Soft- oder Hardwareversion für eine Produktionsumgebung. Versionen müssen entsprechend einer Versionspolitik geplant, vor der Freigabe angemessen getestet und zur Sicherung des laufenden Betriebs unter der Kontrolle des Änderungsmanagements in Produktion genommen werden (Roll-out). Das Versionsmanagement hat Beziehungen zur IT-Beschaffung und zum Vertragsmanagement, wie sie in der KBSt-Schriftenreihe (z. B. „ITIL und IT-Beschaffung"[162]) beschrieben sind.

7.1.4 IT-Sicherheit

IT-Sicherheit ist eine wichtige Grundlage für erfolgreiche E-Government-Anwendungen. In ITIL wird dazu eine eigene Schwerpunktpublikation zum Sicherheitsmanagement (Security Management) herausgegeben, die auf eine weitestmögliche Verknüpfung des Prozesses Sicherheitsmanagement mit den IT-Service-Management-Prozessen verweist. Darüberhinaus wird in ITIL zum Sicherheitsmanagement auf den Standard BS 7799[163] der British Standard Institution verwiesen, deren Empfehlungen als internationaler Standard ISO/IEC 27001 vom IT-Grundschutz des BSI im BSI-Standard 100-1 berücksichtigt werden.

Generell sind die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Sicherheit von E-Government-Anwendungen[164] und zum IT-Grundschutz (das ehemalige IT-Grundschutzhandbuch)[165] des BSI zu berücksichtigen. IT-Sicherheit muss bei der Planung von E-Government-Anwendungen von Anfang an mit einbezogen werden[166]. Zur Wahrung der Wirtschaftlichkeit müssen IT-Sicherheitsmaßnahmen angemessen sein. Grundlage dafür ist die möglichst frühzeitig zu erstellende Schutzbedarfsfeststellung, wie sie im BSI-Standard 100-2[167] empfohlen wird. Eine solche Schutzbedarfsfeststellung stuft anhand der möglichen Schäden die IT-Infrastruktur in die Schutzbedarfskategorien normal, hoch und sehr hoch ein.

Bei der Feststellung eines normalen Schutzbedarfs für die E-Government-Anwendungen können die in den IT-Grundschutzkatalogen empfohlenen Standardmaßnahmen genutzt werden. Bei hohem oder sehr hohem Schutzbedarf sollte zusätzlich eine Risikoanalyse nach dem BSI-Standard 100-3[168] durchgeführt werden, wobei die IT-Grundschutzkataloge Unterstützung bieten. Daraus können sowohl die umfangreich gesammelten Gefährdun-

162. siehe http://www.kbst.bund.de/itil, Kasten „Produkte & Dokumente" > „ITIL und IT-Beschaffung"
163. siehe http://www.bsi-global.com/
164. siehe E-Government-Handbuch unter http://www.bsi.bund.de/fachthem/egov/3.htm
165. siehe IT-Grundschutz-Kataloge unter http://www.it-grundschutz.de/
166. siehe Abschnitt 8.1 „IT-Sicherheitskonzeption" auf Seite 93
167. siehe http://www.bsi.de/literat/bsi_standard/standard_1002.pdf
168. siehe http://www.bsi.de/literat/bsi_standard/standard_1003.pdf

gen ausgewertet und mit erweiterten Maßnahmen aus den IT-Grundschutzkatalogen oder zusätzlichen Maßnahmen aus dem E-Government-Handbuch[169] kompensiert werden.

Der Aufwand zum Betrieb einer sicheren Infrastruktur kann für kleinere Behörden nicht wirtschaftlich sein, sodass sich ein Outsourcing in die Rechenzentren externer IT-Dienstleister oder übergeordneter Behörden lohnen kann.

7.2 Aufbau einer E-Government-Infrastruktur

Die Einführung einer Referenzinfrastruktur in SAGA dient dem Ziel, die erforderlichen infrastrukturellen Voraussetzungen für den Betrieb von E-Government-Anwendungen und die dafür erforderliche Systemstruktur zu definieren. Folgende Ziele sollen entsprechend dem Schutzbedarf mit einer Festlegung von Parametern für eine Referenzinfrastruktur im Sinne einer Betriebsumgebung erreicht werden:

a. angemessener physikalischer Schutz der Systeme
b. angemessene Verfügbarkeit der Systeme
c. angemessene Sicherheit von Systemen und ihren Komponenten
d. Einordnung von Systemen und ihren Komponenten in getrennte Sicherheitszonen
e. Skalierbarkeit von Systemen und Infrastruktur
f. einfache Pflege, effektive Wartung komplexer Systeme und ihrer Komponenten durch das Betriebspersonal

In Abbildung 7-2 auf Seite 87 wird eine allgemeine Gesamtsicht einer verteilten E-Government-Anwendung auf die Bereiche Benutzer, Netzwerk und Infrastruktur dargestellt.

Sowohl der Bereich des Netzwerks als auch der des Benutzers liegen in der Regel außerhalb der Kontrolle des Betreibers einer E-Government-Anwendung und sind daher nicht Schwerpunkt dieser Betrachtung. Der Infrastrukturbereich hingegen wird durch den Betreiber kontrolliert und muss durch seine Systemstruktur den Betriebsanforderungen für E-Government-Anwendungen genügen.

Die folgenden Abschnitte beschreiben die Anforderungen an ein Rechenzentrum und seine IT-Infrastruktur.

7.2.1 Physikalische Infrastruktur

Der Schutz von Systemen gegen höhere Gewalt wie Blitz, Feuer, Wasser, unzulässige Temperatur und Luftfeuchte oder technische Ausfälle wie Ausfall der Stromversorgung sowie organisatorische Mängel wie unbefugten Zutritt zu schutzbedürftigen Räumen setzt die Einrichtung einer geeigneten Unterbringung für die Server und IT-Systeme voraus. Rechenzentren, die den Betrieb von E-Government-Anwendungen planen, sollten daher entsprechend der Schutzbedarfsfeststellung die notwendigen IT-Sicherheitsmaßnahmen gemäß IT-Grundschutz-Katalogen des BSI umsetzen. Dazu zählen u. a.:

a. die Aufstellung der IT-Systeme in geeigneten Räumen

169. siehe http://www.e-government-handbuch.de/

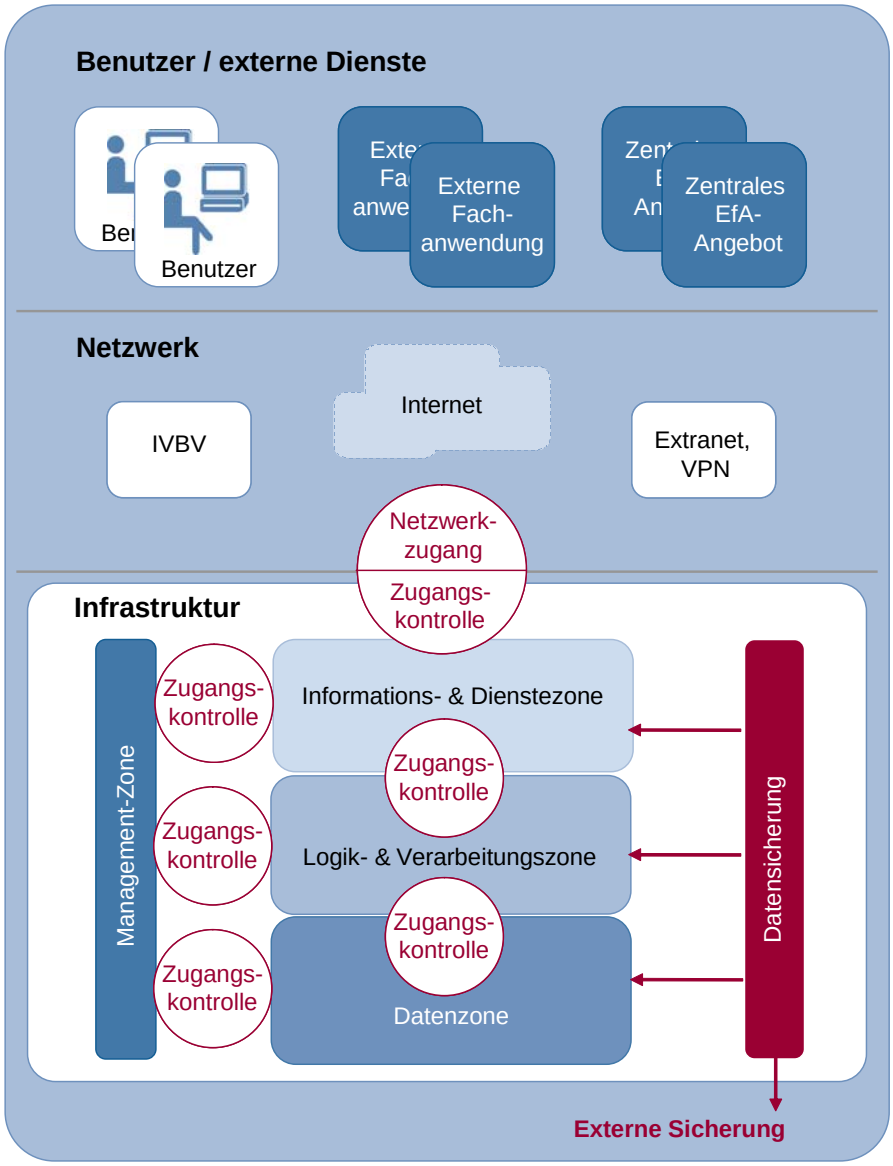


Abbildung 7-2: Engineering Viewpoint einer E-Government-Anwendung

b. eine Zutrittskontrolle zu diesen Räumen
c. geeignete Maßnahmen zur rechtzeitigen Feuererkennung und -bekämpfung
d. geeignete Maßnahmen zur Energieversorgung
e. geeignete Maßnahmen zur Klimatisierung
f. eine Datensicherung nach einem dazugehörigen Datensicherungskonzept

7.2.2 Zonenkonzept und Kommunikationsbeziehungen

Die Systeme innerhalb des Rechenzentrums werden in verschiedenen Zonen platziert, die anhand der Sicherheitsanforderungen für Dienste und Daten der jeweiligen Zone definiert werden. Um den grundsätzlichen Schutzbedarf von E-Government-Anwendungen durch das Zonenkonzept abdecken zu können, sollen mindestens die im Folgenden beschriebenen vier Zonen in der Infrastruktur eines Rechenzentrums implementiert werden. Für den Betrieb komplexer E-Government-Anwendungen können weitere Zonen erforderlich wer-

den. Dabei sollte auf eine angemessene Trennung der Zonen entsprechend den Grundstrukturen für Sicherheits-Gateways[170] geachtet werden, das bedeutet:

a. Eine Netzwerkkomponente (Router, Switch, Hub o.ä.) kann immer nur als Übergang von einer in eine zweite Zone genutzt werden, sodass in jeder Netzwerkkomponente nur Daten der beiden direkt angeschlossenen Zonen weitergeleitet werden. Eine Vermischung von Datenströmen im Falle eines Fehlers oder eines gezielten Angriffs wird somit verhindert.
b. Auf einem Server-System können nur Systeme einer Zone gehostet werden. Verteilte Anwendungen müssen daher auf Server-Systemen in verschiedenen Zonen betrieben werden.
c. Ein Server-System, dessen E-Government-Anwendungen Kommunikationsbeziehungen in mehrere Zonen benötigen, muss über eine entsprechende Anzahl physikalisch und logisch getrennter Netzwerkverbindungen (z. B. mehrere Netzwerkkarten) verfügen. Ein Übergang von einer Zone in die andere wird somit auf diesem System ausgeschlossen.

Informations- und Dienstezone

Die Informations- und Dienstezone umfasst den Bereich des Netzes, der zwischen dem Internet und den übrigen Zonen des Netzes steht. In dieser Zone befinden sich Server, auf die ein Zugriff aus externen Netzen erforderlich ist oder die ihrerseits Dienste aus externen Netzen nutzen. Sollen Systeme mit unterschiedlichen Sicherheitseinstufungen betrieben werden, empfiehlt sich die Einrichtung weiterer Informationszonen.

Die Kommunikationsbeziehungen zwischen Systemen in der Informations- und Dienstezone und Systemen in der Logik- und Verarbeitungszone sollten angemessen zum Schutzbedarf durch den Einsatz verschlüsselter Kommunikationskanäle geschützt werden.

Logik- und Verarbeitungszone

In dieser Zone werden Systeme untergebracht, die Daten aus der Datenzone verarbeiten und diese den Anwendern über Systeme in der Informations- und Dienstezone zur Verfügung stellen. Eine direkte Kommunikation zwischen externen Netzen, wie dem Internet, und der Logik- und Verarbeitungszone ist nicht erlaubt.

Datenzone

In der Datenzone stehen alle Systeme, auf denen Daten gespeichert und für längere Zeiträume vorgehalten werden. Zugriffe auf diese Zone sind nur aus der Verarbeitungszone und der Management-Zone erlaubt. Ein direkter Zugriff aus externen Netzen ist unter keinen Umständen erlaubt. Ebenso dürfen aus dieser Zone heraus keine aktiven Zugriffe auf weitere Zonen erfolgen. Eine Ausnahme stellt die Management-Zone dar.

170. IT-Grundschutzkataloge des BSI, Maßnahme M 2.73, Auswahl geeigneter Grundstrukturen für Sicherheitsgateways, http://www.bsi.de/gshb/deutsch/m/m02.htm

Management-Zone

In der Management-Zone werden alle Systeme untergebracht, die zu administrativen Zwecken oder der Überwachung von Systemen in den anderen Zonen benötigt werden. Weiterhin können zentrale Dienste zur Benutzerverwaltung oder Authentifizierung in dieser Zone untergebracht werden. Ein Zugriff aus der Management-Zone in andere Zonen und umgekehrt ist daher erlaubt.

Ein Zugriff aus externen Netzen auf die Management-Zone ist unter keinen Umständen zulässig.

Datensicherung

Die Datensicherung sollte in jeder Zone durch eigenständige Sicherungskomponenten erfolgen. Die Sicherung der Daten der Informationszone sollte hierbei wiederum über geschützte Kommunikationskanäle erfolgen.

7.2.3 Netzwerkzugang und Zugangskontrolle

Sicherheits-Gateways steuern die Trennung der einzelnen Zonen innerhalb des Rechenzentrums ebenso wie den Zugang von und zu externen Netzwerken. Dabei können verschiedene Technologien zum Einsatz kommen.

Der Übergang zwischen der Informations- und Dienstezone und externen Netzen ist der sicherheitskritischste Punkt und wird daher durch eine Kombination mehrerer Sicherheitsmechanismen geschützt. Zum einen erfolgt an dieser Stelle eine Trennung auf Netzwerkprotokollebene in verschiedene Netzwerksegmente und -adressbereiche. Interne Netzwerkadressen werden maskiert und somit in externen Netzwerken nicht publiziert. Für sehr kleine Netzwerke auf der Basis von IPv4 ohne hohen Schutzbedarf kann dies auch durch Network Address Translation (NAT) erfolgen.

Weiterhin wird durch Filtermechanismen sichergestellt, dass der Zugriff aus externen Netzen nur auf bestimmte Dienste in der Informations- und Dienstezone erlaubt ist. Die Filterregeln werden üblicherweise auf Firewalls oder Firewall-Routern implementiert, die auf Basis von Paketfiltern die Informationen in den Headern der eingehenden Datenpakete untersuchen und nicht erlaubte Zugriffe abweisen.

Darüber hinaus können Application Gateways eingesetzt werden, die die Kommunikation vollständig entkoppeln, indem sie Datenströme auf Anwendungsebene validieren und gegebenenfalls eine protokollkonforme Neugenerierung von Requests realisieren.

Die Kommunikationsbeziehungen zwischen den internen Zonen werden ebenfalls durch Sicherheits-Gateways geregelt. Für die Implementierung der Zugriffskontrolle zu den sensiblen Bereichen der Logik- und Verarbeitungszone sowie der Datenzone sollten aufgrund der umfassenderen Filtermöglichkeiten Firewalls zum Einsatz kommen, die auf Basis von dynamischen Paketfiltern (Stateful Inspection) arbeiten und in der Lage sind, nicht nur einzelne Pakete, sondern Kommunikationsströme über mehrere Pakete hinweg zu überwachen. Dynamische Paketfilter bieten die Möglichkeit, Netzwerkverbindungen nicht nur

nach fest eingetragenen Regeln, sondern darüber hinaus auch auf Basis von vorangegangenen Kommunikationsbeziehungen validieren zu können.

Der Einsatz von VLAN-Technologie bietet sich aufgrund seiner einfachen und flexiblen Administration für die Zugangskontrolle zu den Systemen in der Management-Zone an. Dazu werden alle Systeme, die Zugriff auf einen Dienst in der Management-Zone benötigen, in einem virtuellen Netzsegment (VLAN) zusammengefasst. Um eine ungewollte Kopplung der einzelnen Zonen über die VLANs der Management-Zone zu verhindern, werden alle Systeme mit einem zweiten Netzwerk-Interface ausgestattet, das ausschließlich für administrative Zugänge genutzt werden darf und mit einem Paketfilter ausgerüstet ist.

Von einem Einsatz der VLAN-Technologie zur Verbindung anderer Zonen als der Management-Zone ist aus Sicherheitsgründen abzuraten.

7.3 Netzwerke als Bindeglied einer Infrastruktur zu externen Diensten und Benutzern

Die Netzwerkebene ist das Verbindungsglied zwischen den Systemen in der Rechenzentrumsinfrastruktur und externen Diensten sowie den Benutzern von E-Government-Anwendungen, siehe Abbildung 7-2 „Engineering Viewpoint einer E-Government-Anwendung“ auf Seite 87. In dieser Ebene werden sowohl das Internet, TESTA (Trans-European Services for Telematics between Administrations), der Informationsverbund der Bundesverwaltung (IVBV), der Informationsverbund Berlin-Bonn (IVBB) als auch weitere VPN-basierte Netze oder Extranets zusammengefasst. Auch hauseigene Intranets fallen in den Bereich der Netzwerkebene. In den letzten Jahren haben sich deutliche Konsolidierungstendenzen im Bereich der Netzwerktechnologien gezeigt. Dennoch sind nach wie vor eine Vielzahl verschiedener Technologien im Einsatz. Durch eine Abstraktion auf höheren Protokoll- oder Anwendungsebenen kann jedoch eine Interoperabilität der Systeme erreicht werden, sodass in SAGA auf konkrete Technologieempfehlungen für den Bereich der Netzwerkebene verzichtet wird.

Aus Sicht des Engineering Viewpoint auf eine E-Government-Anwendung spielt die sichere und performante Anbindung an Internet, TESTA, IVBV, IVBB oder Extranets eine wichtige Rolle, um einen zuverlässigen Zugang zu Anwendern und externen Diensten zu gewährleisten. Bei der Konzeption von E-Government-Anwendungen müssen daher auf Basis einer Abschätzung des zu erwartenden Netzwerkverkehrs die erforderlichen Bandbreiten bereitgestellt und die im Abschnitt 7.2.3 beschriebenen Zugangskontrollen implementiert werden.

7.4 Zugriff auf externe Dienste

Externe Dienste nutzen über Netzwerke die Infrastruktur von E-Government-Anwendungen, siehe Abbildung 7-2 „Engineering Viewpoint einer E-Government-Anwendung“ auf Seite 87.

7.4.1 Deutsches Verwaltungsdiensteverzeichnis

Das Deutsche Verwaltungsdiensteverzeichnis (DVDV)[171] bildet eine fach- und ebenenübergreifende Infrastruktur für das E-Government in Deutschland. Dort sind im XML-Format Adressierungsparameter von Online-Diensten der öffentlichen Verwaltung hinterlegt. Dabei handelt es sich vorrangig um technische Beschreibungen der Dienste im WSDL-Format[172] sowie ergänzende URLs und kryptografische Zertifikate. Das DVDV ermöglicht damit das Auffinden aller für eine automatisierte Maschine-Maschine-Kommunikation benötigten Informationen in maschinenlesbarer Form. Hierdurch werden die Grundlagen geschaffen, um die Online-Dienste voll automatisiert zwischen Maschinen und dennoch sicher und rechtsverbindlich abzuwickeln.

Technische Grundlage ist der Verzeichnisdienststandard LDAP[173], der die Struktur zur Ablage und Auffindbarkeit der Informationen des DVDV definiert. Der Kern des DVDV ist der zentrale Bundesmaster, der durch die Bundesstelle für Informationstechnik (BIT) bereit gestellt wird, siehe Abbildung 7-3. Er ist die einzige Stelle, bei der ein schreibender Zugriff auf die Datenbestände erfolgen kann. Die Datenpflege erfolgt durch die angeschlossenen und berechtigten Stellen in den Ländern. Der Bundesmaster spiegelt seinen Datenbestand kontinuierlich auf dezentral (z. B. in den Bundesländern) aufgestellte DVDV-Landes-Server, die sich die Anfragelast der einzelnen Datenabrufe teilen. Die Pflege und Replikation der

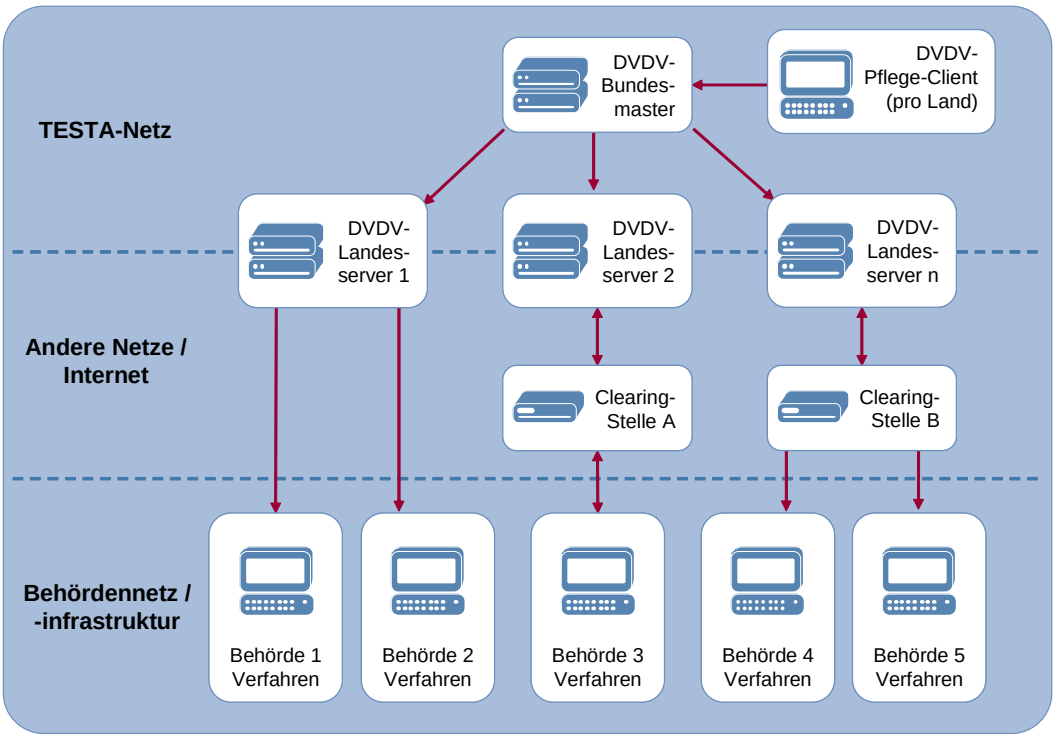


Abbildung 7-3: Aufbau des Deutschen Verwaltungsdiensteverzeichnisses

171. siehe http://www.dvdv.de/
172. Web Service Description Language; siehe Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124
173. Lightweight Directory Access Protocol, siehe Abschnitt 8.8.1 „Verzeichnisdienste und Registrys“ auf Seite 135; für das DVDV wird die Open-Source-Referenzimplementation OpenLDAP eingesetzt, siehe http://www.openldap.org/

WSDL-Dateien und ergänzenden Parameter wird durch den Einsatz von OSCI-Transport abgesichert.

Die erste Anwendung ist seit dem 1. Januar 2007 die Umsetzung des im Jahre 2002 novellierten Melderechtsrahmengesetzes, speziell der Teil der länderübergreifenden Datenübermittlungen. Damit kann auf papiergebundene Rückmeldungen und Fortschreibungen des Melderegisters verzichtet werden. Stattdessen werden die Daten zwischen den beteiligten Behörden ausschließlich elektronisch und automatisiert übermittelt. Weitere bereits integrierte Dienste (Stand: Mitte 2007) sind die Dienste zur Kommunikation des Bundeszentralamts für Steuern mit den Meldebehörden im Rahmen der Vergabe der einheitlichen Steueridentifikationsnummer und das Kommunale Kernmelderegister des Freistaats Sachsen. Das DVDV ist in seiner Architektur so angelegt, dass prinzipiell beliebige automatisierte Kommunikationsbeziehungen im E-Government seine Dienste nutzen können.

Die BIT betreibt die Koordinierende Stelle des DVDV. Diese stellt den Informationsfluss zu den Anwendern und Diensteanbietern sicher und steht über die Adresse dvdv@bva.bund.de für Anfragen zum DVDV zur Verfügung.

7.4.2 Nutzung von EfA-Angeboten

Im Rahmen der Einer-für-Alle-Angebote (EfA-Angebote)[174] der Bundesverwaltung werden – unterteilt in EfA-Dienste, EfA-Systeme, EfA-Konzepte und Infrastrukturen – sowohl im Internet als auch über den IVBV für die Behörden nutzbare Angebote für die Einbindung in ihre E-Government-Anwendungen bereitgestellt.

Dienste, wie z. B. der EfA-Dienst ePayment[175], können über Web-Service-Schnittstellen im Internet aufgerufen werden. Dazu werden vom EfA-Dienst zum einen die erforderlichen server-seitigen Web-Service-Schnittstellen und zum anderen eine Referenzimplementierung zum Aufruf der Web Services durch die jeweilige E-Government-Anwendung zur Verfügung gestellt. In ähnlicher Form erfolgt auch die Kommunikation mit externen Fachanwendungen von anderen Behörden oder Unternehmen, die ebenfalls über Middleware-Kommunikationsschnittstellen angebunden werden können.

Dezentrale EfA-Angebote hingegen, wie die EfA-Systeme Datensicherheit[176] und Formular-Management-System[177], werden innerhalb der Rechenzentrumsinfrastruktur der einzelnen Behörden implementiert. In diesem Fall sollten wiederum die bereits im Abschnitt 7.2 „Aufbau einer E-Government-Infrastruktur“ auf Seite 86 beschriebenen Regeln beachtet werden.

174. siehe Abschnitt 6.3.6 „Wiederverwendung und Integration von EfA-Angeboten“ auf Seite 78
175. siehe EfA-Dienst Zahlungsverkehrsplattform („ePayment“): http://www.kbst.bund.de/efa-zvp
176. siehe EfA-System Datensicherheit („Virtuelle Poststelle“): http://www.kbst.bund.de/efa-vps
177. siehe EfA-System Formular-Management-System: http://www.kbst.bund.de/efa-form

8 Technology Viewpoint: Standards für IT-Architektur und Datensicherheit

In diesem Kapitel werden den einzelnen Elementen des in Kapitel 3 vorgestellten Architekturmodells technische Standards zugeordnet und kurz beschrieben. Wenn für Standards keine Versionsnummern angegeben sind, ist die aus Marktsicht stabilste Version zu verwenden, welche nicht immer die neueste Version sein muss.

Die Bedeutungen der Klassen „Obligatorisch", „Empfohlen" und „Unter Beobachtung" werden im Abschnitt 2.3.1 „Klassifizierung in SAGA" auf Seite 20 näher beschrieben.

8.1 IT-Sicherheitskonzeption

Die vorgestellten Standards für IT-Sicherheit empfehlen ein systematisches Vorgehen zur Erreichung und Erhaltung eines angemessenen Niveaus der IT-Sicherheit. Dazu wird in einem nach seiner Initiierung kontinuierlich laufenden IT-Sicherheitsmanagementprozess eine IT-Sicherheitskonzeption erstellt und weiterentwickelt. Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) wird seit Dezember 2005 in mehreren BSI-Standards und den IT-Grundschutzkatalogen ein Vorgehen empfohlen und unterstützt, das vormals im IT-Grundschutzhandbuch (IT-GSHB) dargelegt war.

8.1.1 Managementsysteme für Informationssicherheit

Als ersten Schritt hin zu einer umfassenden IT-Sicherheitskonzeption ist die Schaffung eines Managementsystems für die Informationssicherheit notwendig.

Obligatorisch:	BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) v1.0

Der BSI-Standard 100-1[178] mit den allgemeinen Anforderungen an ein ISMS (Informationssicherheitsmanagementsystem) sollte im Rahmen der Sicherheitskonzeption angewendet werden. Der Standard ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO-Standards 13335 und 17799[179].

8.1.2 IT-Grundschutzvorgehensweise

Für die Wirtschaftlichkeit der IT-Sicherheitskonzeption sind für eine IT-Anwendung einschließlich der zu verarbeitenden Daten nur IT-Sicherheitsmaßnahmen zu ergreifen, die für den festgestellten Schutzbedarf angemessen sind. Die systematische Vorgehensweise für die IT-Konzeption umfasst Schritte wie die Schutzbedarfsanalyse.

178. siehe http://www.bsi.de/literat/bsi_standard/standard_1001.pdf
179. siehe http://www.iso.org/

Obligatorisch: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise v1.0

Im Dezember 2005 veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen Standard „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise“[180]. Der Standard beinhaltet eine Beschreibung, wie IT-Sicherheitsmanagement in der Praxis aufgebaut und betrieben werden kann. Es sollte im Rahmen der IT-Sicherheitskonzeption angewendet werden. Mit diesem Vorgehen lassen sich IT-Sicherheitskonzepte einfach und effizient erstellen und die IT-Sicherheit im laufenden Betrieb aufrechterhalten beziehungsweise verbessern.

8.1.2.1 Schutzziele

Schutzziele definieren die Sicherheitsinteressen der beteiligten Kommunikationspartner in allgemeiner Form:

a. *Vertraulichkeit* – Schutz vor unbefugter Kenntnisnahme:
   Daten werden Individuen, Entitäten oder Prozessen nicht unautorisiert zur Verfügung gestellt oder offenbart.
   Die Sicherung der Vertraulichkeit wird durch Verschlüsselung von Informationen (Kryptografie) erreicht.
b. *Integrität* – Schutz vor Manipulation:
   Daten können nicht unautorisiert verändert oder zerstört werden. Dazu gehören auch Angaben zur Herkunft oder zum Erstellungszeitpunkt.
   Die Sicherung der Integrität wird durch Verschlüsselung von Informationen (Kryptografie) beziehungsweise den Einsatz von Signaturen erreicht.
c. *Verfügbarkeit* – Schutz vor Ausfall der IT-Systeme*:*
   Die Eigenschaft einer Entität beziehungsweise Ressource ist zugänglich beziehungsweise nutzbar, wenn es durch eine autorisierte Entität gewünscht wird.
   Hohe Verfügbarkeit wird durch Vielfalt, Verteiltheit und Fehlertoleranz erreicht.

8.1.2.2 Schutzbedarfskategorien

Der Schutzbedarf muss für jede IT-Anwendung der verarbeiteten Daten ermittelt werden. Er orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen IT-Anwendung bezüglich der unter Abschnitt 8.1.2.1 definierten Schutzziele verbunden sind.

Um Anwendungen sicherheitstechnisch zu bewerten, wird jedem Schutzziel eine Schutzbedarfskategorie zugeordnet. In „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise“ wird dazu folgende Einteilung vorgenommen:

180. siehe http://www.bsi.de/literat/bsi_standard/standard_1002.pdf

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 8-1: Schutzbedarfsklassen

Bei der Schutzbedarfsfeststellung ist insbesondere auch eine mögliche Verarbeitung von personenbezogenen Daten zu betrachten, um die datenschutzrechtlichen Rahmenbedingungen einzuhalten. SAGA verzichtet auf die Erläuterung von Datenschutzmaßnahmen. Hinweise zum Datenschutz bezüglich Rahmenbedingungen, Herausforderungen und Handlungsempfehlungen findet man im E-Government-Handbuch (Modul: Datenschutzgerechtes E-Government[181]).

8.1.3 Risikoanalyse

Obligatorisch: BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz v2.0

Der BSI-Standard 100-3[182] zur ergänzenden Risikoanalyse im Anschluss an die IT-Grundschutz-Analyse sollte für Bereiche mit deutlich über das normale Maß hinausgehenden Sicherheitsanforderungen angewendet werden. Gründe für eine Risikoanalyse können in hohem oder sehr hohem Schutzbedarf, dem Einsatz von (noch) nicht in den IT-Grundschutz-Katalogen behandelten Anwendungen oder Komponenten sowie dem Betrieb in im IT-Grundschutz nicht berücksichtigten Einsatzszenarien (Umgebung, Anwendung) liegen.

8.1.4 Umsetzung der Sicherheitskonzeption

Obligatorisch: Industrial Signature Interoperability Specification - MailTrusT (ISIS-MTT) v1.1

Grundlagen, Standards und Profile für die Umsetzung von Sicherheitskonzeptionen sind in ISIS-MTT v1.1[183] vorgegeben. Die Spezifikation entstand durch die Zusammenführung von Industrial Signature Interoperability Specification (ISIS) und MailTrusT (MTT).

ISIS-MTT ist eine Delta-Spezifikation, die auf bestehenden, relevanten internationalen Standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ETSI) basiert und diese für den Einsatz in der Praxis konkretisiert. Schwerpunkt der Spezifikation sind Aussagen zu Konformitätsanforderungen, die von konformen PKI-Komponenten und -Anwendungen bei der Generierung

181. siehe E-Government-Handbuch (http://www.bsi.bund.de/fachthem/egov/6.htm), Kapitel II, Modul „Datenschutzgerechtes E-Government“
182. siehe http://www.bsi.de/literat/bsi_standard/standard_1003.pdf
183. siehe http://www.isis-mtt.org/

beziehungsweise Verarbeitung von bestimmten Datenobjekten, wie beispielsweise Zertifikaten, erfüllt werden müssen.

Die ISIS-MTT-Spezifikation besteht im Wesentlichen aus einem Kerndokument, das ausschließlich auf einer Profilierung (Einschränkung optionaler Merkmale) internationaler Standards beruht und somit internationale Interoperabilität gewährleisten soll. Diese Kernspezifikation ist für alle Hersteller und Anbieter obligatorisch und kann bei Bedarf um optionale Profile ergänzt werden. Die bereits vorliegenden Profile „SigG-Profile" und „Optional Enhancements to the SigG-Profile" beschreiben die aktuelle Ausprägung qualifizierter Signaturen in Deutschland.

Das Kerndokument der ISIS-MTT-Spezifikation besteht aus acht Teilen mit folgenden Inhalten:

1. Aufbau von Public-Key-Zertifikaten, Attribut-Zertifikaten und Zertifikats-Sperrlisten
2. Aufbau und Versand von Anfragen an die Zertifizierungs-Stelle (PKCS#10) und Antworten von der Zertifizierungs-Stelle (PKCS#7)
3. Aufbau von verschlüsselten und signierten Nachrichten
4. Abfrage von Public-Key-Zertifikaten, Attribut-Zertifikaten und Zertifikats-Sperrlisten mittels LDAP, OCSP[184], FTP oder HTTP; Aufbau von Anfragen und Antworten an beziehungsweise von Zeit-Stempel-Stellen
5. Gültigkeitsprüfung von Public-Key-Zertifikaten und Attribut-Zertifikaten
6. zugelassene Algorithmen für Hash-Funktionen, Signaturen, Verschlüsselung, Authentisierung von Nachrichten an die und von der Zertifizierungsstelle; zugelassene Algorithmen für XML Signature und XML Encryption
7. Beschreibung des „Cryptographic Token Interface" (PKCS#11) mit Datentypen und Funktionen
8. Profiling und Erweiterung von XML Signature und XML Encryption

Obligatorisch: BSI, IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge[185] des BSI sollten angewendet und die dort beschriebenen Standardsicherheitsmaßnahmen umgesetzt werden. Die Nutzung der Baustein-, Maßnahmen- und Gefährdungskataloge unterstützt eine komponentenorientierte Arbeitsweise, mit der sich IT-Sicherheitskonzepte einfach, effizient und effektiv realisieren lassen.

Empfohlen: KoopA ADV, Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung v1.1

Der Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung des KoopA ADV [186] soll dem Ziel dienen, die Lösung kryptografischer Problemstellungen für ausgewählte Projekte in der öffentlichen Verwaltung zu

184. OCSP = Online Certificate Status Protocol
185. siehe http://www.bsi.de/gshb/deutsch/
186. siehe http://www.koopa.de/projekte/pki.html

erleichtern und ist in erster Linie als Arbeitshilfe für die Behörden gedacht. Typische Problemstellungen werden in Form von Szenarien definiert, für die wiederum Lösungsmöglichkeiten aufgezeigt werden.

Empfohlen: BSI, E-Government-Handbuch

Das E-Government-Handbuch[187] des BSI umfasst organisatorische und technische Empfehlungen zum IT-Einsatz im E-Government. Für die Entwicklung einer E-Government-Anwendung im Sinne von SAGA sind insbesondere die sicherheitstechnischen Empfehlungen des Handbuchs relevant[188]. In dem Kapitel „IT und IT-Sicherheit" werden in den folgenden Modulen IT-sicherheitsrelevante Empfehlungen gegeben:

1. Allgemeine Informationen zu sicheren E-Government-Anwendungen
2. Authentisierung im E-Government
3. Optimierung der Auffindbarkeit von Web-Inhalten
4. Sichere Integration von E-Government-Anwendungen
5. Sichere Zahlungsverfahren für das E-Government
6. Sichere Kommunikation im E-Government
7. Sichere Client-Server-Architekturen für das E-Government
8. E-Government ohne aktive Inhalte

Die Empfehlungen des E-Government-Handbuchs sollten vor allem immer dann berücksichtigt werden, wenn eine Schutzbedarfsklasse „hoch" oder „sehr hoch" vorliegt[189] – also die Anforderungen an die IT-Sicherheit über den IT-Grundschutz hinausgehen. Das E-Government-Handbuch gibt diesbezüglich Empfehlungen zur Konzeption und zur Umsetzung einer entsprechenden IT-Sicherheit.

8.2 Prozessmodelle

8.2.1 Technologien zur Prozessmodellierung

Obligatorisch: Rollenmodelle und Flussdiagramme

Rollenmodelle und Flussdiagramme sollten zur Definition einfacher Prozesse eingesetzt werden. Dabei ist es wichtig, alle mit einem Prozess befassten Rollen und Systeme zu identifizieren und die Prozessschritte in Form von Flussdiagrammen zu beschreiben. Flussdiagramme sollten sich im weiteren Sinne nach DIN 66001 „Informationsverarbeitung; Sinnbilder und ihre Anwendung" richten.

187. siehe http://www.bsi.bund.de/fachthem/egov/3.htm
188. siehe http://www.bsi.bund.de/fachthem/egov/6.htm#Kapitel_IV, Unterkapitel IV B: „IT und IT-Sicherheit"
189. siehe Abschnitt 8.1 „IT-Sicherheitskonzeption" auf Seite 93

Obligatorisch: Unified Modeling Language (UML) v2.0

Zur Vorbereitung und Dokumentation von Großprojekten sollte die Unified Modeling Language (UML)[190] für objektorientierte Modellierung angewendet werden. Insbesondere Use Cases und Aktivitätsdiagramme haben sich im Einsatz bewährt und erlauben, transparente Spezifikationen zu erstellen und abzustimmen. Diese Spezifikationen können durch entsprechende Werkzeuge weiter verwendet werden.

8.2.2 Austauschformate für Prozessmodelle

Empfohlen: XML Metadata Interchange (XMI) v2.x

XML Metadata Interchange (XMI)[191] ist ein Standard der Object Management Group (OMG), der zur Notation und zum Austausch von Meta-Object-Facility(MOF)-basierten Modellen (Beispiel: UML) in XML eingesetzt werden sollte. Das Format ist offen und herstellerunabhängig. UML 2.0[192] lässt sich in XMI 2.0 und XMI 2.1 transformieren. XMI v2.0.1 wurde als ISO/IEC 19503:2005[193] standardisiert.

8.3 Datenmodelle

8.3.1 Technologien zur Datenmodellierung

Obligatorisch: Entity Relationship Diagramme (ERD)

Bei der Entwicklung von relationalen Datenbank-Schemata sollten Entity Relationship Diagramme eingesetzt werden. Auch funktionale Datenmodelle für eine fachliche Grobkonzeption sollten mit ER-Diagrammen dargestellt werden.

Obligatorisch: Unified Modeling Language (UML) v2.0

Bei der Datenmodellierung für objektorientierte Anwendungen sollte UML eingesetzt werden. Es bieten sich beispielsweise Klassendiagramme an, die wieder in anderen Anwendungen oder durch andere Werkzeuge genutzt werden können. Aus entsprechenden Spezifikationen können direkt XML-Datenstrukturen generiert werden.

190. siehe http://www.uml.org/
191. siehe http://www.omg.org/technology/documents/formal/xmi.htm
192. siehe Abschnitt 8.2.1 „Technologien zur Prozessmodellierung“ auf Seite 97
193. siehe http://www.iso.org/

8.3.2 Austauschformate für Datenmodelle

Obligatorisch: XML Schema Definition (XSD) v1.0

Zur strukturierten Beschreibung von Daten sollen XML-Schemata gemäß den Definitionen des World Wide Web Consortium (W3C)[194] mit der XML Schema Definition (XSD) erstellt werden.

Empfohlen: Regular Language Description for XML New Generation (Relax NG)

Der Standard (ISO/IEC 19757-2:2003[195]) Relax NG[196] kann, ebenso wie XML Schema Definition (XSD), zur strukturierten Beschreibung von Daten genutzt werden.

Relax NG ist weniger verbreitet als XSD und hat eine geringere Werkzeugunterstützung. Es ist jedoch einfacher, leichter lesbar und dennoch ausdrucksstärker.

Zwar ist für die strukturierte Beschreibung von Daten XSD obligatorisch, die Nutzung von Relax NG ist dennoch möglich, da Relax-NG-Schemata mit (Open Source) Werkzeugen in XML Schemata transformiert werden können[197].

Empfohlen: XML Metadata Interchange (XMI) v2.x

Analog zu Abschnitt 8.2.2 „Austauschformate für Prozessmodelle“ auf Seite 98.

8.3.3 Beschreibungssprachen für Metadaten von Dateien

Empfohlen: Resource Description Framework (RDF)

Das Resource Description Framework (RDF)[198] ist eine Sprache zur Repräsentation von Informationen über Ressourcen im Web, die vom W3C entwickelt wurde. RDF ist ausgerichtet auf die Beschreibung von Metadaten und Ontologien und ist somit ein wichtiger Bestandteil von Semantic Web. RDF ermöglicht es, Vokabulare zu deklarieren, d. h. Begriffe zu definieren, damit relevante Informationen über Ressourcen in einer solchen Art und Weise beschrieben werden, sodass sie gesammelt, integriert und wiederverwendet werden können. In RDF können auch einfache Vokabulare wie Dublin Core verwendet werden. RDF sollte zur Beschreibung von Metadaten für Web-Ressourcen eingesetzt werden.

194. siehe http://www.w3.org/XML/Schema
195. siehe http://www.iso.org/
196. siehe http://www.relaxng.org/
197. siehe http://www.thaiopensource.com/relaxng/trang.html
198. siehe http://www.w3.org/TR/rdf-primer/

Empfohlen: Dublin Core (DC)

Dublin Core (DCMI Metadata Terms)[199] ist ein weit verbreiteter Standard, der von ISO[200] und NISO[201] standardisiert wurde. Der Standard ist eine Entwicklung von der Dublin Core Metadata Initiative (DCMI). Die neuste Version wurde im Mai 2007 von der NISO genormt – die Überarbeitung basiert noch immer auf dem ISO-Standard 15836-2003 vom Februar 2003. Der Standard sollte zur Metadaten-Beschreibung von Web-Seiten, digitalen Objekten und Dokumenten eingesetzt werden.

Das zweite Kapitel der Spezifikation („The Dublin Core Metadata Element Set") enthält die 15 Kernelemente des Standards: contributor, coverage, creator, date, description, format, identifier, language, publisher, relation, rights, source, subject, title und type. Jedes Element entspricht jeweils einer Eigenschaft, der ein gewisser Wert zugeordnet werden kann. Sie sind optional und können beliebig oft zur Beschreibung eines Objekts verwendet werden. Für einige Elemente stehen weitere Unterelemente, die „Refinements" oder „Qualifiers" genannt werden, zur Verfügung, die genauere Beschreibungen von Ressourcen ermöglichen.

Die Elemente von Dublin Core können in HTML/XHTML- und RDF/XML-Dokumenten verwendet werden. In HTML-Dokumenten können Dublin-Core-Metadaten mit dem META-Element im Dokumentkopf angegeben werden.

8.4 Applikationsarchitektur

In diesem Abschnitt werden Programmiersprachen und Technologien zur Realisierung der Applikationsarchitektur festgelegt. Im ersten Teil werden die Standards für die Middleware des E-Government-Architekturmodells definiert, wobei vor allem auf den Aspekt der Applikationsintegration eingegangen wird. Im Anschluss erfolgt eine Erweiterung der Standards für Applikationen ohne beziehungsweise mit geringem Middleware-Anteil, d. h., dass die Middleware-Standards auch für einfachere Applikationen eingesetzt werden können.

Die Vorgaben und Empfehlungen folgen aus den Gestaltungsprinzipien Betriebssystemneutralität, Interoperabilität und Portabilität.

Middleware-Dienste, wie z. B. Replikation, verteiltes Transaktionsmanagement, Personalisierung, Internationalisierung, Messaging etc., werden in der aktuellen Version in Ansätzen referenziert.

In begründeten Fällen, z. B. bei erheblichen Wirtschaftlichkeitsvorteilen, kann von den zu bevorzugenden (obligatorischen, empfohlenen) Technologien abgewichen werden.

199. siehe http://dublincore.org/documents/dcmi-terms/
200. publiziert als ISO 15836:2003, siehe http://www.iso.org/
201. publiziert als ANSI/NISO Z39.85 - 2007, http://www.niso.org/standards/index.html

8.4.1 Applikationsarchitektur mit Middleware

Obligatorisch: Java Platform, Enterprise Edition (Java EE) v5

Zur Entwicklung und Integration folgender Anwendungen (Verbundanwendungen) in der Mittelschicht sollten Technologien der Java Platform, Enterprise Edition (Java EE)[202] angewendet werden:

a. Einer-für-Alle-Angebote (EfA-Angebote)[203],
b. Anwendungen, die EfA-Angebote oder dazu bereitgestellte Bibliotheken unmittelbar einbinden und
c. Anwendungen, die als Ganzes oder in Teilen (Komponenten) für eine Wiederverwendung (Portierung) vorgesehen sind.

Java EE ist eine Spezifikation, die eine Reihe von Programmierschnittstellen und einen Entwicklungsprozess definiert. In der Gesamtheit bildet Java EE eine Architektur, die wesentliche Aspekte von geschäftskritischen Anwendungen berücksichtigt und unterstützt. Java EE stellt wichtige Funktionsbausteine bereits zur Verfügung, die bei der Entwicklung von Anwendungen genutzt werden können. Dazu gehören seit der Version 1.4[204] als so genannte Core-Bibliotheken auch Standard-Programmierschnittstellen (APIs) und Technologien: Java Authentication and Authorization Service (JAAS), Java API for XML Parsing (JAXP) und Java Naming and Directory Interface (JNDI). Sämtliche Core-Bibliotheken sind alternativen Technologien vorzuziehen.

Java EE v5[205], das im Mai 2006 finalisiert wurde, zeichnet sich gegenüber der Vorgängerversion J2EE v1.4 insbesondere durch Verbesserungen in dem Bereich Wartbarkeit von Anwendungen sowie der Vereinfachung des Programmiermodells aus. Weiterentwicklungen wurden u. a. auch bei der Definition und Nutzung von Web Services und dem Mapping von Java-Klassen zu XML und Datenbanken vorgenommen.

Als so genannte optionale Bibliotheken bietet Java EE v5 gegenüber Java SE v5 u. a. folgende APIs und Technologien:

a. Java Message Service (JMS) v1.1,
b. J2EE Connector Architecture (JCA) v1.5,
c. Java Transaction API (JTA),
d. JavaMail API v1.4,
e. Java Management Extensions (JMX) v1.2,
f. Enterprise JavaBeans (EJB) v3.0[206],
g. Java Server Faces (JSF) v1.2[207],
h. Java Server Pages (JSP) v2.1 und

202. siehe http://java.sun.com/javaee/
203. siehe Abschnitt 6.3.6 „Wiederverwendung und Integration von EfA-Angeboten“ auf Seite 78
204. publiziert als JSR-000151, siehe http://www.jcp.org/en/jsr/detail?id=151
205. publiziert als JSR-000244, siehe http://www.jcp.org/en/jsr/detail?id=244 und http://java.sun.com/javaee/
206. Alternativ zum Einsatz von EJB kann auch ein anderes Application Framework verwendet werden, wie zum Beispiel das Spring Application Framework, siehe http://www.springframework.org/.
207. publiziert als JSR-000252, siehe http://www.jcp.org/en/jsr/detail?id=252

i. Java Servlet API v2.5.

Durch den Java Community Process[208] werden in naher Zukunft immer mehr anwendungsnahe Elemente die Funktionsvielfalt von Java EE bereichern. Die Definition neuer Elemente geschieht über so genannte Java Specification Requests (JSR).

Obligatorisch: Java Platform, Standard Edition (Java SE) v5

Soweit für eine Anwendung der Leistungsumfang von Java EE anfänglich oder dauerhaft nicht im vollen Umfang benötigt wird, sollten alternativ die Technologien von Java EE einzeln eingesetzt werden. Als Grundlage dient die Java Platform, Standard Edition (Java SE)[209]. Die einzelnen Technologien sollten entsprechend der Java EE Spezifikation 5[210] verwendet werden, um einen kompatiblen Migrationspfad zu Java EE zu bilden.

Unter Beobachtung: C# Language Specification/ Common Language Infrastructure (CLI)

Der Standard ECMA-334[211] „C# Language Specification" (ISO/IEC 23270:2006[212]) spezifiziert die Form und die Interpretation von Programmen, die mit der Sprache C# geschrieben wurden.

Der Standard ECMA-335[213] „Common Language Infrastructure (CLI)" (ISO/IEC 23271:2006 und ISO/IEC TR 23272:2006[214]) definiert eine Infrastruktur für verschiedene Systemumgebungen, in der Anwendungen, die in verschiedenen Programmiersprachen geschrieben wurden, ausgeführt werden können. Die Infrastruktur abstrahiert von spezifischen Eigenschaften der Systemumgebungen, sodass Anwendungen nicht verändert werden müssen, um sie auf verschiedenen Systemen zu betreiben.

Es gibt zwei Implementationen der ECMA-Standards. Das .NET-Framework von Microsoft läuft nur unter Windows. Die beiden ECMA-Standards basieren auf .NET v2.0 und sind dadurch auch Bestandteil von .NET v3.0. Die Verfügbarkeit für weitere Betriebssysteme wird nur durch eine weitere Implementierung, nämlich Mono[215], sichergestellt.

Die beiden ECMA-Standards bilden kein vollständiges Entwicklungs-Framework ab, da durch sie beispielsweise die Implementierung von Clients und Präsentationsschichten nicht unterstützt wird.

208. siehe http://www.jcp.org/
209. siehe http://java.sun.com/javase/
210. publiziert als JSR-000176, siehe http://www.jcp.org/en/jsr/detail?id=176
211. siehe http://www.ecma-international.org/publications/standards/Ecma-334.htm
212. siehe http://www.iso.org/
213. siehe http://www.ecma-international.org/publications/standards/Ecma-335.htm
214. siehe http://www.iso.org/
215. siehe http://www.mono-project.de/

Unter Beobachtung:	Business Process Execution Language for Web Services (BPEL4WS) v1.1

Zur Komposition von Geschäftsprozessen auf Basis von Web Services kann BPEL4WS[216] eingesetzt werden. Das unter der Schirmherrschaft von OASIS stehende BPEL4WS ist eine XML-basierte Beschreibungssprache, die Web Services und die damit verbundenen Standards (SOAP, WSDL, UDDI) um geschäftliche Transaktionen erweitert.

Große Infrastrukur- und Anwendungsanbieter unterstützen die Spezifikation und es stehen Werkzeuge, auch als Open-Source-Lösung[217], zur Verfügung. BPEL4WS wurde zum OASIS-Standard WS-BPEL 2.0 weiterentwickelt.

Unter Beobachtung:	Web Services Business Process Execution Language (WS-BPEL) v2.0

WS-BPEL[218] v2.0 wurde im April 2007 als Standard bei der OASIS verabschiedet. Der Standard dient der Komposition von Geschäftsprozessen auf Basis von Web Services. Werkzeuge zu WS-BPEL v2.0 sind am Markt vorhanden. WS-BPEL v2.0 ist zu seinem Vorgänger BPEL4WS v1.1 nicht kompatibel.

8.4.2 Applikationsarchitektur ohne Middleware

Für einfache E-Government-Anwendungen ohne Middleware steht ergänzend zu den Standards des vorigen Abschnitts die folgende Technologie zur Auswahl.

Empfohlen:	PHP: Hypertext Preprocessor (PHP) v5.x

Für Anwendungen ohne Integrationsbedarf, also nicht verteilte Stand-Alone-Anwendungen, die nicht mit Einer-für-Alle-Angeboten (EfA-Angeboten)[219], mit Legacy-Systemen oder anderen E-Government-Fachanwendungen kommunizieren, kann PHP[220] (rekursives Akronym für „PHP: Hypertext Preprocessor“) eingesetzt werden. PHP wird als Open-Source-Projekt von der PHP Group entwickelt und ist eine in HTML eingebettete Skriptsprache für die Entwicklung von Web-Applikationen.

In der Version 5 erfolgt eine umfassende Unterstützung von Konzepten objektorientierter Programmierung. Verfahren zur Datenkapselung, der Referenzierung von Variablen und Exception Handling (Ausnahmebehandlung) stellen wichtige Fortschritte im Rahmen der Weiterentwicklung dar.

216. siehe http://www-128.ibm.com/developerworks/library/specification/ws-bpel/
217. siehe http://www.bpelsource.com/products/
218. siehe http://www.oasis-open.org/specs/index.php#wsbpelv2.0
219. siehe Abschnitt 6.3.6 „Wiederverwendung und Integration von EfA-Angeboten“ auf Seite 78
220. siehe http://www.php.net/

8.5 Client

Der Client ist eine Software auf einem Endgerät, die einen von der Middleware angebotenen Dienst in Anspruch nimmt. Die Client-Schicht umfasst somit die klassische Benutzerseite mit allen Möglichkeiten der modernen Technologie, um mit der öffentlichen Verwaltung zu interagieren, wobei der Informationszugriff über unterschiedliche Medien erfolgen kann. In Deutschland haben bislang vor allem die folgenden Medien Verbreitung gefunden, sodass bei einem Informationsangebot für diese Endgeräte optimale Voraussetzungen für die breite Nutzung von E-Government-Anwendungen bestehen:

a. Computer (PC, Notebook)
b. Mobiltelefon / Personal Digital Assistant (PDA)
c. externe Systeme (z. B. ERP-Systeme von Industrieunternehmen)

Standardisierungsbemühungen für Spielkonsolen und insbesondere für digitales, interaktives Fernsehen sind noch nicht zu einheitlichen Empfehlungen gekommen. Größte Verbreitungschancen werden dem so genannten „Thin Client" eingeräumt, der nur geringe Anforderung an Hard- und Software-Ausstattung des Endgerätes stellt und voraussetzt, dass möglichst viel Funktionalität server-seitig zur Verfügung gestellt wird.

8.5.1 Informationszugriff mit Computern

Auf Computern[221] stehen prinzipiell zwei unterschiedliche Clients zur Verfügung, um auf Informationen zuzugreifen oder Informationen zu erhalten: Web-Browser und spezifische Client-Anwendungen (z. B. Java-Clients – auch Applets). Letztere ermöglichen u. a. einen direkten Zugriff auf internetbasierte Dienste, E-Mail-Server und – je nach Erlaubnis – auf das Betriebssystem zur Nutzung lokaler Ressourcen wie lokaler Datenträger. Bei der Verwendung aktiver Inhalte dürfen nur die in SAGA zugelassenen Client-Technologien zum Einsatz kommen. Der Einsatz von Active-X-Controls ist grundsätzlich nicht zugelassen. Bei Verwendung aktiver Inhalte sollte – soweit möglich – ein Parallelangebot ohne aktive Inhalte vorgehalten werden, siehe auch Abschnitt 1.5 „Grundprinzipien für E-Government-Anwendungen" auf Seite 13.

Obligatorisch: Java Network Launching Protocol (JNLP) v1.5

Die Auslieferung von Java-Client-Anwendungen über das Internet sollte über das Java Network Launching Protocol (JNLP)[222] erfolgen. Dafür kann die Referenzimplementierung „Java Web Start"[223] genutzt werden.

Der Einsatz von JNLP ermöglicht die einfache, plattformunabhängige Verteilung von Java-Applikationen und vermeidet Versionskonflikte der Java-Laufzeitumgebungen (Java Runtime Environment – JRE).

221. Von einem Computer wird in diesem Zusammenhang dann gesprochen, wenn das Endgerät kein kleines Display, keine geringe Bandbreite und eine Tastatur besitzt.
222. publiziert als JSR-000056 (Final Release), siehe http://www.jcp.org/en/jsr/detail?id=56
223. siehe http://java.sun.com/products/javawebstart/

8.5.1.1 Web-Browser

Um bei der Realisierung von E-Government-Anwendungen eine breite Nutzung zu ermöglichen, sollten als Frontend Web-Browser verwendet werden, die die Formate der Präsentationsebene verarbeiten und darstellen können, siehe Abschnitt 8.6. Hierbei sind folgende browser-basierte Client-Technologien zugelassen:

a. Die Nutzung von Cookies ist zugelassen, soweit
   i. diese nicht persistent sind und
   ii. Web-Seiten einer Domain keine Inhalte anderer Domains inkludieren, welche Cookies setzen.

   Hierbei sind die Empfehlungen zum HTTP-Protokoll gemäß Abschnitt 8.7.5 zu berücksichtigen.
b. Die Nutzung von Javascript ist zugelassen. Jedoch muss sichergestellt sein, dass die Web-Seiten auch dann verwendbar sind, wenn Javascript deaktiviert wurde. Diese Forderung deckt sich mit der als obligatorisch klassifizierten BITV[224]. Damit wird erreicht, dass Anwender nicht gezwungen werden, wegen E-Government-Anwendungen ihre Sicherheitseinstellungen zu lockern. Bei der Nutzung von Javascript ist der Abschnitt 8.6.4 „Aktive Inhalte“ auf Seite 111 zu berücksichtigen.
c. Die Nutzung von Java-Applets ist zugelassen, wenn diese vom Server signiert sind und damit als authentisch und integer beim Client erkannt werden können. Die Hersteller von Java-Applets müssen ihr Produkt vorzugsweise durch ein vom Hersteller unabhängiges Software-Unternehmen qualitätssichern lassen oder die Qualität zumindest in Form einer Erklärung zusichern.[225]
d. Die Nutzung von Plug-Ins erfolgt ausschließlich entsprechend den Anforderungen auf der Web-Seite http://www.kbst.bund.de/saga-plugins.
e. Für gängige Browser-Typen werden Beispielkonfigurationen erstellt und vom BSI über das Internet allgemein zur Verfügung gestellt.
f. Beim Versand von Formulardaten ist die Vertraulichkeit der Informationen durch Verwendung von TLS-verschlüsselten Kanälen unter Nutzung zugehöriger Server-Zertifikate sicherzustellen.
g. Auch bei der Nutzung der zugelassenen Client-Technologien ist die Rechtsverordnung zur Barrierefreiheit unverändert zu berücksichtigen.

8.5.1.2 Client-Anwendungen

Der Standard-Client für Anwendungen mit direktem Zugriff auf Web-Server ist der Web-Browser. Wenn direkter Zugriff auf internetbasierte Dienste nicht notwendig ist oder die Funktionalität eines Web-Browsers begründeterweise als unzureichend anzusehen ist, wie zum Beispiel im Fall komplexer Geschäftsvorfälle mit direktem Dateisystemzugriff oder Nutzung von Legacy-Software, dann können Client-Anwendungen verwendet werden.

224. siehe BITV, Abschnitt 6.3 „Es muss sichergestellt sein, dass mittels Markup-Sprachen geschaffene Dokumente verwendbar sind, wenn Scripts, Applets oder andere programmierte Objekte deaktiviert sind.“ (http://bundesrecht.juris.de/bitv/)

225. Nähere Informationen zu diesem Thema sind im Web unter der Adresse http://www.kbst.bund.de/saga-applets zu finden.

Diese Anwendungen werden auf dem Client-Rechner installiert und müssen bei Weiterentwicklungen mit den notwendigen Updates versorgt werden. Sie können entweder über CD-ROM oder über eine Download-Möglichkeit[226] auf einer Web-Seite als signierte Anwendungen zur Verfügung gestellt werden. Die Verwendung von Java-Anwendungen wird empfohlen (Vorteil der Plattformunabhängigkeit).

Client-Anwendungen müssen den folgenden Anforderungen genügen:

a. Alle personenbezogenen und sicherheitskritischen Daten sind auf dem lokalen Datenträger verschlüsselt abgelegt.
b. Bei direktem Zugriff auf internetbasierte Dienste wird eine sichere Datenübertragung zum Server unterstützt, siehe Abschnitt 8.7.5 „Anwendungsprotokolle“ auf Seite 130. Für die sonstige Client-Server-Kommunikation sind ausschließlich die im Abschnitt 8.7.1 „Middleware-Kommunikation“ auf Seite 124 definierten Protokolle zugelassen.
c. Die in SAGA dokumentierten Austauschformate für einen Austausch der Nutzerdaten mit anderen Anwendungen sollen unterstützt werden.
d. Es erfolgt eine Qualitätssicherung der Anwendung durch ein vom Hersteller unabhängiges Software-Unternehmen.
e. Die Anwendung wird mit einem Software-Zertifikat ausgeliefert, welches im Rahmen der Installation verifiziert wird.
f. Neben dem Download der Anwendung über das Internet wird auch die Distribution per CD-ROM angeboten.
g. Die Rechtsverordnung zur Barrierefreiheit ist zu berücksichtigen.

8.5.1.3 E-Mail-Client

Zum Empfangen, Senden und Bearbeiten von E-Mails sind E-Mail-Clients einzusetzen, die mindestens die technische Unterstützung der E-Mail-Standards aus Abschnitt 8.7.3 „E-Mail-Kommunikation“ gewährleisten. An dieser Stelle sei darauf hingewiesen, dass die Kommunikation dieser Clients nur im Hinblick auf die Kommunikation mit der Verwaltung standardisiert beziehungsweise auf obiges beschränkt ist. Bei der Verwendung externer, nicht mit dem Bund gekoppelter Mail-Server unterliegt der Client hinsichtlich der verwendeten Standards und Protokolle keiner Beschränkung.

8.5.2 Informationszugriff mit mobilen Endgeräten

Mobiltelefone, PDAs und andere mobile Endgeräte besitzen – in Abgrenzung zum Computer – entweder

a. ein kleines Display,
b. eine geringe Bandbreite oder
c. keine Standardtastatur

und müssen die von Servern angebotenen Standards für mobile Endgeräte der Präsentationsebene unterstützen[227]. Weiterhin sollten so umfassend wie möglich die Standards, die

226. siehe auch „Java Network Launching Protocol (JNLP) v1.5” auf Seite 104
227. siehe Abschnitt 8.6.13 „Technologien für die Präsentation auf mobilen Endgeräten“ auf Seite 123

zur Präsentation von Inhalten durch Computer im allgemeinen beschrieben werden, auch durch die mobilen Endgeräte dargestellt werden[228].

Weiterhin sind die in Abschnitt 8.5.1 „Informationszugriff mit Computern“ auf Seite 104 beschriebenen Anforderungen z. B. bezüglich aktiver Inhalte einzuhalten.

8.5.3 Informationszugriff durch externe Systeme

Die Kommunikation und Interaktion zwischen externen und internen Systemen sollte über eine Teilmenge der Standards abgewickelt werden, die für die Kommunikation und Interaktion zwischen internen Systemen definiert werden. So ist bei der Server-zu-Server-Kommunikation XML über SOAP gleichberechtigt zu RMI zu betrachten[229].

8.5.4 Technologien zur Authentisierung

Um die Schutzziele Vertraulichkeit und Integrität zu gewährleisten, ist die Identitätsfeststellung und Authentisierung von Kommunikationspartnern für bestimmte E-Government-Anwendungen erforderlich.

Obligatorisch: BSI, E-Government-Handbuch, Modul „Authentisierung im E-Government“

Verschiedene Mechanismen können für die Authentisierung verwendet werden, z. B. Nutzererkennung / Passwort, PIN / TAN oder Zertifikate. Eine sicherheitstechnische Betrachtung verschiedener Authentisierungsverfahren erfolgt im Modul „Authentisierung im E-Government“[230] des E-Government-Handbuchs, das vom BSI herausgegeben wird.

Empfohlen: Security Assertion Markup Language (SAML) v2.0

SAML[231] ist ein XML-basiertes Format zum Austausch von Authentisierungsinformationen. Durch den Austausch von Daten in einem einheitlichen Format fördert es insbesondere die Interoperabilität zwischen E-Government-Anwendungen. Die Publikation der Version 2.0 erfolgte im März 2005.

Unter Beobachtung: Kerberos v5

Kerberos[232] ist ein Protokoll zur Authentisierung in Rechnernetzen, das vom Massachusetts Institute of Technology (MIT) entwickelt wurde. Durch den einheitlichen Austausch von Authentisierungsdaten wird die Interoperabilität gefördert. Durch betriebssystemabhängige Erweiterungen kommt es allerdings teilweise zu Inkompatibilitäten zwischen verschiedenen Implementationen.

228. siehe Abschnitt 8.6 „Präsentation“ auf Seite 108
229. siehe dazu Abschnitt 8.6.6 „Austauschformate für Daten“ auf Seite 111, Abschnitt 8.4 „Applikationsarchitektur“ auf Seite 100, Abschnitt 8.7 „Kommunikation“ auf Seite 124 und Abschnitt 8.8 „Backend“ auf Seite 134
230. siehe E-Government-Handbuch (http://www.bsi.bund.de/fachthem/egov/6.htm), Kapitel IV B, Modul „Authentisierung im E-Government“
231. siehe http://www.oasis-open.org/specs/index.php#samlv2.0
232. publiziert als RFC 1510, siehe http://www.ietf.org/rfc/rfc1510.txt und http://web.mit.edu/kerberos/

8.6 Präsentation

Die Präsentationsschicht stellt den Clients Informationen zur Verfügung. Je nach Anwendungsfall müssen unterschiedliche Formate bereitgestellt werden, die in den folgenden Abschnitten aufgelistet werden. Die Verwendung offener Austauschformate, die über hinreichend viele Funktionen verfügen und auf unterschiedlichen Plattformen verfügbar sind, wird grundsätzlich gefordert.

Es ist zulässig, die Informationen zusätzlich – oder nach Vereinbarung zwischen allen Beteiligten auch alternativ – zu den obligatorischen und empfohlenen Formaten in Formaten anzubieten, die von SAGA nicht berücksichtigt wurden.

8.6.1 Barrierefreie Darstellung

Obligatorisch: Barrierefreie Informationstechnik Verordnung (BITV)

Um das Informationsmedium Internet auch behinderten Menschen zugänglich zu machen, wird die Vermeidung von Barrieren für Menschen mit Behinderungen gefordert. Um eine solche barrierefreie Darstellung sicherzustellen, sollen die Anforderungen der „Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik Verordnung – BITV)“[233] zugrunde gelegt werden. Diese Rechtsverordnung setzt §11 des Behindertengleichstellungsgesetzes um und berücksichtigt insbesondere die Web Content Accessibility Guidelines[234] des W3C in der Version 1.0. Zum Thema Barrierefreiheit siehe auch Abschnitt 4.5.3 auf Seite 49.

8.6.2 Zeichensätze

Obligatorisch: Unicode v4.x UTF-8

Um ausreichend Zeichen für die verschiedenen, weltweit existierenden Buchstaben, Ziffern und Symbole zur Verfügung zu haben, sollte als Zeichensatz für Dokumente ISO 10646:2003[235] (auch bekannt als Unicode v4.x) in der UTF-8 Kodierung verwendet werden[236].

Empfohlen: Unicode v4.x UTF-16

Soweit die Dokumente in nicht westeuropäischen Sprachen verfasst sind (z. B. Griechisch, Bulgarisch), kann ISO 10646:2003[237], auch bekannt als Unicode v4.x, in der UTF-16-Kodierung[238] verwendet werden.

233. siehe http://bundesrecht.juris.de/bitv/
234. siehe http://www.w3.org/TR/WCAG10/
235. siehe http://www.iso.org/
236. Diese Spezifikation ist unter http://www.unicode.org/ verfügbar.
237. siehe http://www.iso.org/
238. Diese Spezifikation ist unter http://www.unicode.org/ verfügbar.

8.6.3 Technologien zur Informationsaufbereitung

Obligatorisch: Hypertext Markup Language (HTML) v4.01

HTML ist die etablierte Sprache, um Hypertexte im World Wide Web zu publizieren. Neben den Text-, Multimedia- und Hyperlink-Funktionen früherer HTML-Versionen unterstützt HTML v4.01[239] mehr Multimedia-Optionen, Skript-Sprachen und bessere Formulare und Druckfunktionen. Für die technische Umsetzung des barrierefreien Zugangs durch Web Content Accessibility Guidelines Version 1.0 ist der Einsatz von HTML v4.01 erforderlich. Es wurde eine bessere Trennung zwischen Dokumentstruktur und Präsentation eingeführt. Dazu wird die Nutzung von Stylesheets anstelle von HTML-Präsentationselementen und -attributen forciert. HTML 4 macht auch große Schritte im Hinblick auf die Internationalisierung von Dokumenten, mit dem Ziel, das World Wide Web wirklich weltweit zu machen.

Obligatorisch: Multipurpose Internet Mail Extensions (MIME) v1.0

Zur standardisierten Angabe, welches Format eine Datei oder ein Teil davon hat, sollte das Format Multipurpose Internet Mail Extensions (MIME) verwendet werden. Es erlaubt dem E-Mail-Client oder dem Web-Browser die eindeutige Identifikation des Dateityps, siehe dazu RFC 2045 bis RFC 2049[240]. Die offizielle Liste der möglichen Ausprägungen von MIME-Typen ist bei der Internet Assigned Numbers Authority (IANA)[241] zu finden.

Obligatorisch: Java Servlet v2.5

Zur dynamischen Generierung von Web-Inhalten sollte Servlet v2.5[242] eingesetzt werden. Servlet v2.5 ermöglicht es Applikations-Servern auf Basis von Java EE 5, Anfragen von Clients entgegenzunehmen und dynamisch zu beantworten.

Obligatorisch: Java Server Pages (JSP) v2.1

Zur dynamischen, server-basierten Generierung von Web-Inhalten sollte JSP v2.1[243] verwendet werden. JSP v2.1 beinhaltet eine Expression Language (EL), die dazu dient, den Java Code von JSP Code zu trennen und in statische Fragmente (z. B. HTML) einzubetten. JSP v2.1 baut auf der Technologie Java Servlet v2.5 auf.

Empfohlen: Extensible Hypertext Markup Language (XHTML) v1.0

XHTML v1.0 Second Edition, eine W3C Recommendation[244] vom August 2002, ist als Neuformulierung von HTML v4.0 unter Wahrung der Konformität zu XML ein Austauschformat, welches zahlreiche Forderungen der Interoperabilität und der Barrierefreiheit erfüllt. Die

239. siehe http://www.w3.org/TR/html401/, standardisiert als ISO/IEC 15445:2000, siehe http://www.iso.org/
240. siehe http://www.ietf.org/rfc.html
241. siehe http://www.iana.org/assignments/media-types/
242. publiziert als JSR-000154 (Maintenance Release), siehe http://www.jcp.org/en/jsr/detail?id=154
243. publiziert als JSR-000245, siehe http://www.jcp.org/en/jsr/detail?id=245
244. siehe http://www.w3c.org/TR/xhtml1

Entwicklung von Web-Seiten wird durch die Benutzung von XHTML v1.0 beschleunigt, weil gegenüber HTML v4.01 zahlreiche vormals notwendige Browser-Optimierungen eingespart werden. Des Weiteren erhöhen klare syntaktische Vorgaben (Kleinschreibung der Elemente und Attribute, Wohlgeformtheit gemäß XML) wesentlich die Lesbarkeit des Quellcodes und damit die Kosten für deren Wartung und Weiterentwicklung. XHTML 1.0 wird von allen gängigen Browsern unterstützt.

Empfohlen: Cascading Style Sheets Language Level 2 (CSS2)

Zur Gestaltung von HTML-Seiten sollte die Cascading Style Sheets Language Level 2 (CSS2)[245] verwendet werden.

Empfohlen: Extensible Stylesheet Language (XSL) v1.0

Zur server-basierten, dynamischen Transformation und Darstellung von XML-Dokumenten beispielsweise in HTML-Dateien sollte die Extensible Stylesheet Language (XSL)[246] in der Version 1.0 eingesetzt werden.

Empfohlen: Extensible Stylesheet Language Transformations (XSLT) v1.0

Wenn Anwendungen unterschiedliche XML-Schemata verwenden, kann bei einem Datenaustausch die Konvertierung von einem Format in ein anderes notwendig werden. Diese Formatkonvertierung sollte über die vom W3C definierte Sprache XSLT[247] als Teil von XSL (Extensible Stylesheet Language) erfolgen.

Unter Beobachtung: Extensible Stylesheet Language (XSL) v1.1

XSL v1.1 ist seit dem 5. Dezember 2006 eine W3C Recommendation[248]. Mit dieser Version wurden einige Neuerungen eingeführt, wie z. B. die Referenzierung von Seitenzahlen, Lesezeichen (bookmarks) sowie Änderungsmarkierungen (change marks). Die Werkzeugunterstützung sowie die Relevanz in der praktischen Anwendung des Standards ist im Vergleich zur Vorversion XSL v1.0 noch nicht so weit fortgeschritten.

Unter Beobachtung: Extensible Stylesheet Language Transformations (XSLT) v2.0

Die Extensible Stylesheet Language v2.0 wurde im Januar 2007 als W3C Recommendation verabschiedet[249]. Sie bietet zahlreiche Neuerungen, wie etwa die Verwendung von XPath 2.0. Weitere Verbesserungen betreffen die Ausgabemethoden sowie die Sortier- und Gruppierungsmöglichkeiten. XSLT v2.0 ist nicht vollständig abwärts kompatibel. Außerdem stehen bisher wenige Prozessoren zur Verfügung.

245. siehe http://www.w3.org/TR/REC-CSS2/
246. siehe http://www.w3.org/TR/xsl/
247. siehe http://www.w3.org/TR/xslt
248. siehe http://www.w3.org/TR/xsl11/
249. siehe http://www.w3c.org/TR/xslt20/

8.6.4 Aktive Inhalte

Aktive Inhalte sind Computerprogramme, die in Web-Seiten enthalten sind (z. B. Javascript) oder beim Betrachten der Seite automatisiert nachgeladen werden (z. B. Java Applets, ActiveX Controls oder auch Flash-Animationen) und auf dem Client (vom Browser oder Betriebssystem) ausgeführt werden. Bei der Verwendung von aktiven Inhalten sind die Restriktionen gemäß Abschnitt 8.5 zu berücksichtigen.

Obligatorisch: ECMAScript Language Specification

Soweit gemäß Abschnitt 8.5.1.1 „Web-Browser" auf Seite 105 innerhalb von HTML-Seiten Javascript verwendet wird, sollte dieses der Spezifikation von ECMA-262 3rd Edition[250] vom Dezember 1999 genügen. Diese Spezifikation wurde unter der Bezeichnung ISO/IEC 16262[251] auch von ISO/IEC als Standard aufgenommen.

8.6.5 Formulare

Unter Beobachtung: XForms v1.0

XForms ist eine Spezifikation[252] für Web-Formulare. Die Intention der Spezifikation ist es, in Zukunft die in HTML oder XHTML abgebildeten Formulare abzulösen. XForms bietet einen größeren Funktionsumfang und führt bei client-seitiger Verarbeitung zu einer Reduzierung der Anzahl der Server-Zugriffe.

Zwar sind Implementierungen und auch Plug-Ins verfügbar, standardmäßig wird XForms jedoch nicht von allen Browsern unterstützt.

8.6.6 Austauschformate für Daten

Obligatorisch: Extensible Markup Language (XML) v1.0

XML v1.0[253] ist eine aus der Standard Generalized Markup Language (SGML) abgeleitete Sprache, mit der Daten strukturiert abgebildet werden sollten. Die Sprache bietet die Möglichkeit zur Erweiterung und Ergänzung von Tags. Die Darstellung der abgebildeten Daten erfolgt mit der Beschreibungssprache Extensible Stylesheet Language (XSL)[254].

XML sollte als der universelle und primäre Standard für den Datenaustausch aller verwaltungstechnisch relevanten Informationssysteme dienen.

Neu zu beschaffende Systeme sollten in der Lage sein, über XML Daten auszutauschen. Existierende Systeme müssen nicht zwingend XML-fähig sein – sie sollten jedoch anstreben, über Adapter (Integrationskomponenten) XML-Daten austauschen zu können.

250. siehe http://www.ecma-international.org/publications/standards/Ecma-262.htm
251. siehe http://www.iso.org/
252. siehe http://www.w3.org/TR/xforms/
253. siehe http://www.w3.org/XML/
254. siehe „Extensible Stylesheet Language (XSL) v1.0" auf Seite 110

Unter Beobachtung: Election Markup Language (EML) v4.0

Insbesondere beim Austausch von Daten im Umfeld von E-Voting-Prozessen kann der Standard Election Markup Language (EML)[255] eingesetzt werden.

EML v4.0 wurde im Februar 2006 als OASIS-Standard verabschiedet. Sie definiert eine Reihe von XML-Schemata, die geeignet sind, einen generischen Wahlprozess abzubilden. Zu diesen Wahlprozessen können öffentliche Wahlen (Bundestagswahl, Kommunalwahl) oder private Wahlen (Betriebsratswahlen, Urabstimmungen) gehören. Die EML kann an alle Szenarien angepasst werden und liefert auch Sicherheitsfunktionen zur Absicherung der Daten.

Unter Beobachtung: Extensible Markup Language (XML) v1.1

XML v1.1[256] ist eine überarbeitete Version zu XML v1.0 und wurde am 4. Februar 2004 im Status „Recommendation" veröffentlicht sowie am 15. April 2004 ergänzt. Die Unicode-Fähigkeiten wurden verbessert und Inkonsistenzen bei der Markierung des Zeilenendes behoben. Zurzeit gibt es kaum Parser für XML v1.1.

8.6.7 Austauschformate für Dokumente

8.6.7.1 Formate für Textdokumente zum Informationsaustausch

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

Obligatorisch: Portable Document Format (PDF) v1.4

Für nicht zur Weiterbearbeitung vorgesehene Textdokumente sowie zur Unterstützung von Formularen und barrierefreien Textdokumenten sollte das plattformunabhängige Portable Document Format von Adobe eingesetzt werden. Die PDF-Version 1.4[257] wird vom Acrobat-Reader[258] ab Version 5 unterstützt.

Beim Einsatz sind die Empfehlungen des Moduls „Sicherer Internet-Auftritt im E-Government" im E-Government-Handbuch in Bezug auf aktive Inhalte zu berücksichtigen[259]. Insbesondere beim Konvertieren von (teilweise) geschwärztem Text in das PDF-Format sollte sichergestellt werden, dass der Text tatsächlich nicht mehr kopierbar / suchbar im PDF vorhanden ist. Ebenso stellt die Passwortfunktion von PDF, gleich welche Schlüsselstärke die Kodierung hat, keine genügende Sicherheitsmaßnahme für Dokumente mit schutzwürdigem Inhalt dar, da sie mit entsprechenden Werkzeugen umgangen werden kann.

255. siehe http://www.oasis-open.org/specs/index.php#eml4.0
256. siehe http://www.w3.org/TR/xml11/
257. siehe http://www.adobe.com/devnet/pdf/pdfs/PDFReference.pdf
258. siehe http://www.adobe.de/products/acrobat/readermain.html
259. siehe http://www.bsi.bund.de/fachthem/egov/download/4_IntAuf.pdf

Obligatorisch: Hypertext Markup Language (HTML)

Hypertext-Dokumente, die für den Informationsaustausch vorgesehen sind, z. B. Newsletter, sollten im HTML[260]-Format zum Einsatz kommen, siehe Abschnitt 8.6.3 „Technologien zur Informationsaufbereitung“ auf Seite 109.

Empfohlen: Portable Document Format (PDF) v1.5

Die PDF-Version 1.5[261] ist der Nachfolger des als „Obligatorisch“ klassifizierten PDF v1.4. Für ältere Windows- und MacOS-Versionen sind teilweise keine Distributionen des Acrobat Readers für PDF v1.5 verfügbar. Die PDF-Version 1.5 wird vom Acrobat-Reader[262] ab Version 6 unterstützt. Die Version besitzt u. a. Erweiterungen in den Bereichen Kryptografie, Kompression und inhaltliches Tagging. Beim Einsatz sind die Empfehlungen des Moduls „Sicherer Internet-Auftritt im E-Government“ im E-Government-Handbuch in Bezug auf aktive Inhalte zu berücksichtigen[263].

Unter Beobachtung: Portable Document Format (PDF) v1.6

Die PDF-Version 1.6[264] ist momentan in einem sehr geringen Umfang verbreitet. Die Version ist der Nachfolger der als „Obligatorisch“ klassifizierten Version 1.4 sowie der als „Empfohlen“ klassifizierten Version 1.5. Sie weist Verbesserungen in den Bereichen Kryptografie und der Einbettung von Dateianhängen auf. Die PDF-Version 1.6 wird vom Acrobat-Reader[265] ab Version 7 unterstützt. Beim Einsatz sind die Empfehlungen des Moduls „Sicherer Internet-Auftritt im E-Government“ im E-Government-Handbuch in Bezug auf aktive Inhalte zu berücksichtigen[266].

8.6.7.2 Formate für Textdokumente zur Weiterbearbeitung

Textdokumente, die für eine weitere Bearbeitung vorgesehen sind, müssen veränderbar sein. Es wird zwischen einfachen Textdokumenten und komplexen Textdokumenten mit Layoutinformationen unterschieden.

Obligatorisch: Text

Einfache, weitgehend unstrukturierte und zur Weiterbearbeitung vorgesehene Textdokumente ohne Anforderungen an das Layout sollten im weit verbreiteten Text-Format (z. B. mit der Dateiendung .txt) ausgetauscht werden, um eine generelle Lesbarkeit sicherzustellen. Die anzuwendenden Zeichensätze werden im Abschnitt 8.6.2 festgelegt.

260. standardisiert als ISO/IEC 15445:2000, siehe http://www.iso.org/
261. siehe http://www.adobe.com/devnet/pdf/pdfs/PDFReference15_v6.pdf
262. siehe http://www.adobe.de/products/acrobat/readermain.html
263. siehe http://www.bsi.bund.de/fachthem/egov/download/4_IntAuf.pdf
264. siehe http://www.adobe.com/devnet/pdf/pdfs/PDFReference16.pdf
265. siehe http://www.adobe.de/products/acrobat/readermain.html
266. siehe http://www.bsi.bund.de/fachthem/egov/download/4_IntAuf.pdf

Empfohlen: Open Document Format for Office Applications (OpenDocument) v1.0

OpenDocument[267] wurde von OASIS als XML-basiertes Dokumentenformat für Texte, Tabellenkalkulationen, Präsentationen und andere Office-Dokumente standardisiert. Inhalt der Dokumente und Informationen über ihr Layout sind voneinander getrennt und können dadurch unabhängig verarbeitet werden. Es kann zum Austausch von komplexen Dokumenten eingesetzt werden, die zur Weiterbearbeitung vorgesehen sind. Im November 2006 erfolgte die Veröffentlichung von OpenDocument v1.0 unter dem Namen ISO/IEC 26300:2006[268] als Standard. OpenDocument wird u. a. durch das plattformunabhängige, lizenzfreie und offene Office-Paket von OpenOffice.org[269] unterstützt.

Unter Beobachtung: Office Open XML (OOXML)

Office Open XML[270] wurde von der ECMA im Dezember 2007 als XML-basiertes Dokumentenformat für Texte, Tabellenkalkulationen, Präsentationen und andere Office-Dokumente als Standard ECMA-376 veröffentlicht. Es kann zum Austausch von komplexen Dokumenten eingesetzt werden, die zur Weiterbearbeitung vorgesehen sind.

8.6.7.3 Formate für Tabellenkalkulationen zum Informationsaustausch

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

Obligatorisch: Portable Document Format (PDF) v1.4

Analog zu Abschnitt 8.6.7.1 auf Seite 112.

Empfohlen: Portable Document Format (PDF) v1.5

Analog zu Abschnitt 8.6.7.1 auf Seite 112.

Unter Beobachtung: Portable Document Format (PDF) v1.6

Analog zu Abschnitt 8.6.7.1 auf Seite 112.

8.6.7.4 Formate für Tabellenkalkulationen zur Weiterbearbeitung

Tabellenkalkulationen, die für eine weitere Bearbeitung vorgesehen sind, müssen veränderbar sein. Es wird zwischen einfach strukturierten Daten und komplexen Dokumenten, gegebenenfalls mit Layoutinformationen, unterschieden.

267. siehe http://www.oasis-open.org/committees/download.php/12572/OpenDocument-v1.0-os.pdf
268. siehe http://www.iso.org/
269. siehe http://de.openoffice.org/
270. siehe http://www.ecma-international.org/publications/standards/Ecma-376.htm

Obligatorisch: Comma-Separated Values (CSV)

Tabellen mit einfach strukturierten Daten ohne Anforderungen an das Layout sollten mittels Comma Separated Values[271] (Dateiendung .csv) ausgetauscht werden.

Unter Beobachtung: Open Document Format for Office Applications (OpenDocument) v1.0

Siehe Abschnitt 8.6.7.2 auf Seite 113. OpenDocument[272] unterstützt die Referenzierung von Formelsprachen, diese sind jedoch noch nicht Bestandteil des Standards. Ein Technical Committee von OASIS arbeitet an einer entsprechenden Spezifikation[273].

Unter Beobachtung: Office Open XML (OOXML)

Analog zu Abschnitt 8.6.7.2 auf Seite 113

8.6.7.5 Formate für Präsentationen zum Informationsaustausch

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

Obligatorisch: Portable Document Format (PDF) v1.4

Analog zu Abschnitt 8.6.7.1 auf Seite 112.

Obligatorisch: Hypertext Markup Language (HTML)

Nicht veränderbare Präsentationen in Form von Hypertext-Dokumenten sollten im HTML[274]-Format ausgetauscht werden, siehe Abschnitt 8.6.3 „Technologien zur Informationsaufbereitung“ auf Seite 109.

Empfohlen: Portable Document Format (PDF) v1.5

Analog zu Abschnitt 8.6.7.1 auf Seite 112.

Unter Beobachtung: Portable Document Format (PDF) v1.6

Analog zu Abschnitt 8.6.7.1 auf Seite 112.

271. publiziert als RFC 4810, siehe http://www.ietf.org/rfc/rfc4180.txt
272. standardisiert als ISO/IEC 26300:2006, siehe http://www.iso.org/
273. siehe http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office-formula
274. standardisiert als ISO 15445:2000, siehe http://www.iso.org/

Unter Beobachtung:	Synchronized Multimedia Integration Language (SMIL) v2.0

SMIL ist eine auf XML basierende, standardisierte Sprache zum Schreiben von interaktiven Multimediapräsentationen[275]. „Ein typisches Beispiel für eine solche Anwendung ist ein multimediales Nachrichtencenter, welches Audios und Videos zu einer Nachricht abspielt, während gleichzeitig Hintergrundinformationen auf HTML-Web-Seiten dargestellt werden."[276]

Es gibt eine Reihe von kostenlosen SMIL-Playern. Von den marktüblichen Browsern unterstützt aber bisher nur der Internet Explorer eine Teilmenge von SMIL[277].

8.6.7.6 Formate für Präsentationen zur Weiterbearbeitung

Präsentationen, die für eine weitere Bearbeitung vorgesehen sind, müssen veränderbar sein.

Unter Beobachtung:	Open Document Format for Office Applications (OpenDocument) v1.0

Analog zu Abschnitt 8.6.7.2 auf Seite 113.

Unter Beobachtung:	Office Open XML (OOXML)

Analog zu Abschnitt 8.6.7.2 auf Seite 113.

8.6.7.7 Gesicherter Dokumentenaustausch

Für die Interaktionsstufe Kommunikation ist der Austausch sicherer Dokumente erforderlich. Dies umfasst z. B. die Sicherung von Dokumenten als E-Mail-Anlagen und die Sicherung von Dokumenten für beliebige Kommunikationswege.

Bezüglich der Sicherung von E-Mail-Anlagen ist der Standard ISIS-MTT v1.1 relevant. Für den sicheren Austausch von XML-Dokumenten (z. B. für weiterverarbeitbare Formulare) haben die XML-spezifischen Standards XML Signature und XML Encryption Relevanz erlangt.

Obligatorisch:	Industrial Signature Interoperability Specification - MailTrusT (ISIS-MTT) v1.1, Teil 3

ISIS-MTT v1.1 definiert ein interoperables Datenaustauschformat für signierte und verschlüsselte Daten. Es berücksichtigt auch die Sicherung binärer Daten (insbesondere Part 3: Message Formats), sodass beliebige Dateien als E-Mail-Anlagen gesichert übertragen werden können.

275. siehe http://www.w3.org/TR/2005/REC-SMIL2-20050107/
276. siehe Pauen, Peter: „Zukunftsorientierte Ansätze – SMIL", http://www.informatik.fernuni-hagen.de/pi3/PDFs/SMIL.pdf
277. siehe http://www.w3.org/AudioVideo/#SMIL

Obligatorisch: XML Signature

Der gemeinsame W3C- und IETF-Standard XML Signature (XML-Signature Syntax and Processing, W3C Recommendation und IETF RFC 3275)[278] beschreibt digitale Signaturen für beliebige Daten (in der Regel jedoch XML), indem ein XML-Schema und ein Verarbeitungsregelwerk (für die Generierung und Validierung der Signatur) bereitgestellt werden. Die Signatur kann ein oder mehrere Dokumente beziehungsweise Daten unterschiedlicher Art (Bild, Text etc.) umfassen.

Ein zentrales Merkmal von XML Signature ist die Möglichkeit, anstelle des gesamten XML-Dokuments nur bestimmte Teile desselben zu signieren. Diese Flexibilität ermöglicht beispielsweise, die Integrität bestimmter Elemente eines XML-Dokuments zu sichern, während andere Teile verändert werden können: z. B. kann ein Benutzer in einem signierten XML-Formular bestimmte Felder ausfüllen, ohne dass die Integrität des Dokuments verletzt wird. Dies war mit herkömmlichen Signaturen nicht möglich, da immer das gesamte Dokument signiert wurde und somit jede Veränderung / Einfügung eine Integritätsverletzung bedeutete.

Obligatorisch: XML Encryption

Der W3C-Standard XML Encryption (XML Encryption Syntax and Processing, W3C Recommendation)[279] stellt ein XML-Schema und ein Verarbeitungsregelwerk bereit, das die Verschlüsselung / Entschlüsselung von ganzen Dokumenten, einschließlich XML-Dokumenten, XML-Elementen und Inhalten von XML-Elementen unterstützt.

Zusammen mit XML-Signature ist XML Encryption gesetzte Grundlage mehrerer von der Industrie angenommener Standards für den sicheren XML-basierten Dokumentenaustausch (Web Services Security, SAML, ISIS MTT, ebXML-Messaging, FinTS, OSCI-Transport).

Unter Beobachtung: XML Advanced Electronic Signatures (XAdES) v1.2

Der „XML Advanced Electronic Signatures (XAdES)"[280] Standard wurde vom European Telecommunications Standard Institute (ETSI) entwickelt. XAdES-Signaturen erfüllen nicht nur die Anforderungen der fortgeschrittenen elektronischen Signatur laut EU-Richtlinie, sondern gewährleisteten zusätzlich Nicht-Abstreitbarkeit (non-repudiation) und Langzeitgültigkeit (long-term validity). XAdES ist eine Erweiterung von XML Signature.

In Deutschland wird XAdES beispielsweise bei der Deutschen Post Signtrust eingesetzt. Es gibt mehrere kommerzielle Anbieter von Programmen, die Dokumente auf Basis von XAdES für eine Speicherung aufarbeiten.

278. siehe http://www.w3.org/TR/xmldsig-core/
279. siehe http://www.w3.org/TR/xmlenc-core/
280. siehe http://www.w3.org/TR/XAdES/

8.6.8 Austauschformate für Bilder

Obligatorisch: Graphics Interchange Format (GIF) v89a

Aufgrund der weiten Verbreitung sollte für den Austausch von Grafiken und Schaubildern das Format Graphics Interchange Format (GIF)[281] gewählt werden. GIF-Bilddateien werden mit einer Farbtiefe von 256 Farben (8 Bit pro Pixel) komprimiert.

Obligatorisch: Joint Photographic Experts Group (JPEG)

Für den Austausch von Bildern sollte das Format Joint Photographic Experts Group[282] (JPEG) verwendet werden, welches das Ändern des Komprimierungsgrades und die Angabe der Dichte derart unterstützt, dass ein Kompromiss zwischen Dateigröße, Qualität und Verwendung erleichtert wird. Mittels JPEG können Farb- und Grauwertbilder mit 16,7 Millionen Farben (24 Bit Farbinformationen) gespeichert werden. Eine Vielzahl von Grafik- und Präsentationsprogrammen unterstützen das Format. Die gebräuchliche Komprimierung in JPEG ist verlustbehaftet, erreicht aber hohe Kompressionsraten. Für Grafiken mit gleichfarbigen Flächen und kontrastreichen Farbübergängen (Beispiel: Schrift) ist JPEG ungeeignet.

Empfohlen: Portable Network Graphics (PNG) v1.2

Das Grafikformat Portable Network Graphics[283] (PNG) kann verwendet werden. Das Format ist lizenzfrei und unterstützt 16 Millionen Farben, Transparenz, verlustfreie Kompression, inkrementelle Anzeige der Grafik (erst Grobstruktur, bis Datei ganz übertragen ist) und das Erkennen beschädigter Dateien. Das Format wurde von der ISO standardisiert (ISO/IEC 15948:2003[284]).

Empfohlen: Tagged Image File Format (TIFF) v6.0

TIFF[285] kann zur Speicherung gerasteter Bilder eingesetzt werden. Unterstützt wird TIFF durch alle gängigen Grafik- und Präsentationsprogramme. Um maximale Interoperabilität zu erreichen, sind ausschließlich Eigenschaften aus der „Baseline TIFF“[286] einzusetzen. TIFF kann zum Einsatz kommen, wenn die Fähigkeit des Formats benötigt wird, mehrseitige Dokumente darzustellen. Für eingescannte Textdokumente (Graustufen- oder S/W-Grafiken) ist TIFF besonders geeignet.

281. siehe http://www.w3.org/Graphics/GIF/spec-gif89a.txt
282. siehe http://www.jpeg.org/index.html?langsel=de, standardisiert als ISO/IEC 10918-1:1994, siehe http://www.iso.org/, standardisiert als ITU-T.81, siehe http://www.itu.int/rec/T-REC-T.81/en
283. siehe http://www.w3.org/TR/PNG/
284. siehe http://www.iso.org/
285. siehe http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf
286. Unter „Baseline TIFF“ sind Eigenschaften von TIFF-Dateien zusammengefasst, die jedes TIFF-fähige Programm unterstützen sollte. Beispielsweise gehören zu „Baseline TIFF“ ausschließlich die beiden Komprimierungsverfahren „Huffman“ und „Packbits“, während „LZW“, „JPEG“, „ZIP“ und „CCITT“ optionale Erweiterungen sind, die nicht in jedem TIFF-fähigen Programm implementiert sind.

Empfohlen: Geo Tagged Image File Format (GeoTIFF)

GeoTIFF[287] ist eine Erweiterung von TIFF v6.0. Im Datei-Header ist zusätzlich eine Georeferenzierung enthalten, sodass im Gegensatz zu dem herkömmlichen TIFF die Georeferenzdatei *.tfw nicht erstellt werden muss. Das Format GeoTIFF wird durch die etablierten Geoinformationssysteme unterstützt.

Unter Beobachtung: Joint Photographic Experts Group 2000 (JPEG2000) / Part 1

JPEG 2000[288] ist der Nachfolger von JPEG und noch nicht weit verbreitet. Es liefert bei gleicher Qualität eine höhere Kompression als JPEG. Zusammen mit der Verwendung von Metadaten ist JPEG 2000 für die Aufnahme von Geodaten geeignet[289]. Eine Browser-Unterstützung für JPEG 2000 existiert nur über Plug-Ins. Die Klassifizierung von JPEG 2000 wird auf den ersten Teil des ISO-Standards[290] eingeschränkt, da dieser die Kernfunktionalität enthält und am gebräuchlichsten ist.

8.6.9 Animation

Obligatorisch: Animated Graphics Interchange Format (Animated GIF) v89a

Unter Animation ist hier die Bewegung in Grafiken zu verstehen, die auf einer Web-Seite angezeigt wird. Bevorzugt sollte Animated GIF als eine Variante des GIF-Grafikformats[291] zum Einsatz kommen. Mehrere GIF-Einzelbilder werden hierbei in einer Datei gespeichert; die Reihenfolge, Anzeigedauer und Anzahl der Wiederholungen kann vorgegeben werden.

8.6.10 Audio- und Videodaten

8.6.10.1 Austauschformate für Audio- und Videodateien

Empfohlen: Quicktime

Für den Austausch von Videosequenzen sollte das marktübliche Quicktime-Format[292] verwendet werden. Mit einem entsprechenden Plug-In ist ein Web-Browser in der Lage, solche Dateien „abzuspielen".

Empfohlen: MPEG-4 Part 14 (MP4)

MP4 ist das offizielle Container-Format zu MPEG-4, das von der Moving Picture Experts Group entwickelt und als ISO/IEC-14496[293] standardisiert wurde. MP4 ist als Part 14 Teil des

287. siehe http://www.remotesensing.org/geotiff/
288. siehe http://www.jpeg.org/jpeg2000/
289. siehe OGC: „GML in JPEG 2000 Interoperability Experiment (GMLJP2)", http://www.opengeospatial.org/standards/gmljp2
290. standardisiert als ISO/IEC 15444-1:2004, siehe http://www.iso.org/
291. siehe http://www.w3.org/Graphics/GIF/spec-gif89a.txt
292. siehe http://quicktime.apple.com/

MPEG-4 Standards. MP4 ist ein offener, herstellerunabhängiger Standard und zahlreiche Werkzeuge und Produkte auf verschiedenen Plattformen unterstützen das Format.

MP4 kann für den Austausch von Videodateien verwendet werden, wobei MPEG-4 als Codec verwendet werden sollte.

Empfohlen: Ogg Encapsulation Format (Ogg)

Ogg[294] ist ein offenes, herstellerunabhängiges Container-Format für Audio- und Videodateien. Es wird von der Xiph.org Foundation[295] entwickelt und von vielen Media-Playern unterstützt.

Mit dem Container-Format Ogg können je nach Anwendungsfall verschiedene Codecs verwendet werden. Für Videodaten kann Theora[296] eingesetzt werden. Bei Audiodateien mit niedrigen Qualitätsanforderungen, zum Beispiel Sprachaufzeichnungen, ist Speex[297] geeignet. Für Audiodateien mit normalen Qualitätsanforderungen bietet sich Vorbis[298] an, dessen Qualität mit MP3 vergleichbar ist. Für höchste Qualitätsansprüche kann der verlustfreie Audio-Codec FLAC[299] verwendet werden.

Unter Beobachtung: Windows Media Video (WMV) v9

Das Format Windows Media Video (WMV) ist dem Quicktime-Format qualitativ überlegen. Allerdings wird der Einsatz des WMV-Formats durch Patente für Open-Source-Entwickler erschwert.

Unter Beobachtung: RealMedia v10

RealMedia der Firma RealNetworks[300] ist das Container-Format für das Audioformat RealAudio und das Videoformat RealVideo. All diese Formate sind proprietär. RealVideo ist dem Quicktime-Format qualitativ überlegen. Der kostenlose Player steht für alle gängigen Plattformen einschließlich einiger Mobile Devices zur Verfügung. RealMedia sollte nur eingesetzt werden, wenn die Audio-Video-Daten nicht archiviert werden sollen. Es ist sichergestellt, dass die Dateien heute abgespielt werden können, für die Zukunft ist zu befürchten, dass für dann alte RealMedia-Formate keine Player mehr zur Verfügung stehen.

8.6.10.2 Austauschformate für Audio- und Video-Streaming

Im Gegensatz zu „normalen" Audio- und Videosequenzen bietet Audio- und Video-Streaming ein Format, das es ermöglicht, schon während der Übertragung abgespielt zu werden. Dadurch werden Live-Übertragungen von Videos möglich, wohingegen bei „norma-

293. siehe http://www.iso.org/
294. publiziert als RFC 3533, siehe http://www.ietf.org/rfc/rfc3533.txt
295. siehe http://www.xiph.org/ogg/
296. siehe http://www.theora.org/
297. siehe http://www.speex.org/
298. siehe http://www.vorbis.com/
299. siehe http://flac.sourceforge.net/
300. siehe http://www.realnetworks.com/

len“ Audio- und Videodateien die Datei zunächst komplett übertragen und dann gestartet wird. In diesem Bereich ist bisweilen eine etwas unübersichtliche Vermischung von Anbietern, Produkten, Container- und Inhalts-Formaten anzutreffen. Da SAGA keine Produktempfehlungen treffen will, sollen Empfehlungen nur für das Container-Format getroffen werden.

Wichtig ist, dass die getroffenen Empfehlungen – so weit möglich – mit den gängigen Streaming-Servern und Client-Produkten kompatibel sind. Aufgrund eines seit Jahren vorhandenen starken Wettbewerbs in diesem Bereich ist zurzeit eine hohe Kompatibilität zwischen den unterschiedlichen Produkten bezüglich der unterstützten Formate gegeben.

Obligatorisch: Hypertext Transfer Protocol (HTTP) v1.1

Um eine hohe Verbreitung an möglichst viele Bürger zu erreichen, sollte bei der Wahl des Server-Produkts darauf geachtet werden, dass der Transport der Streaming-Daten auf jeden Fall über HTTP[301] möglich ist.

Empfohlen: Quicktime

Um eine möglichst hohe Kompatibilität des Streaming-Signals mit gängigen Web-Browsern und Video-Clients beziehungsweise Plug-Ins zu erreichen, sollte das Quicktime-Format[302] eingesetzt werden, siehe auch Abschnitt 8.6.10.1 auf Seite 119.

Empfohlen: MPEG-4 Part 14 (MP4)

MP4 kann für das Streaming von Videosequenzen verwendet werden. Dabei sollte MPEG-4 als Codec verwendet werden, siehe auch Abschnitt 8.6.10.1 auf Seite 119.

Empfohlen: Ogg Encapsulation Format (Ogg)

Ogg[303] ist ein offenes, herstellerunabhängiges Container-Format, das für Streaming Audio und Video eingesetzt werden kann.

Für Informationen zu geeigneten Audio- und Video-Codecs siehe Abschnitt 8.6.10.1 „Austauschformate für Audio- und Videodateien“ auf Seite 119.

Unter Beobachtung: Windows Media Video (WMV) v9

Analog zu Abschnitt 8.6.10.1 auf Seite 119.

301. publiziert als RFC 2616, siehe http://www.ietf.org/rfc/rfc2616.txt, weitere Informationen auch unter „HTTP“ im Abschnitt 8.7.5 „Anwendungsprotokolle“ auf Seite 130
302. siehe http://quicktime.apple.com/
303. publiziert als RFC 3533, siehe http://www.ietf.org/rfc/rfc3533.txt

Unter Beobachtung: RealMedia v10

Analog zu Abschnitt 8.6.10.1 auf Seite 119.

Beim Einsatz von RealMeadia für Streaming-Anwendungen ist zusätzlich zu beachten, dass die Preise für die RealMedia Server, Helix Server genannt, im Vergleich zu Windows Media und Quicktime hoch sind. Allerdings unterstützen die Helix Universal Server auch Windows Media und Quicktime.

8.6.11 Austauschformate für Geoinformationen

Die nachfolgend aufgeführten Standards für den Austausch von Geoinformationen werden in den Geodiensten vom Abschnitt 8.7.6 auf Seite 133 angewendet.

Empfohlen: Geography Markup Language (GML) v3.1.1

GML[304] ist eine Auszeichnungssprache zum Austausch und zum Speichern von geografischen Informationen im Vektorformat, welche räumliche und nicht-räumliche Eigenschaften berücksichtigt. Die Spezifikation erfolgte durch das Open Geospatial Consortium (OGC)[305]. GML beinhaltet keine Aussagen über die Darstellung auf dem Bildschirm oder in einer Karte.

GML v3.1.1 sollte insbesondere in Zusammenhang mit der Nutzung des Web Feature Service (WFS) v1.1 eingesetzt werden, siehe Abschnitt 8.7.6 „Geodienste“ auf Seite 133.

Empfohlen: Geography Markup Language (GML) v2.1.2

GML v2.1.2 sollte insbesondere in Zusammenhang mit der Nutzung von Web Feature Service (WFS) v1.0 eingesetzt werden, siehe Abschnitt 8.7.6 „Geodienste“ auf Seite 133.

8.6.12 Datenkompression

Um den Austausch großer Dateien zu ermöglichen und die Netzbelastung zu minimieren, sollten Systeme zur Kompression eingesetzt werden.

Obligatorisch: ZIP v2.0

Die komprimierten Daten sollten im international verbreiteten Format ZIP[306] Version 2.0 ausgetauscht werden.

Empfohlen: Gnu ZIP (GZIP) v4.3 / Tape ARchive (TAR)

Zur Komprimierung von großen Dateiarchiven können auch die Formate GZIP (Dateiendung .gz) in der Version 4.3, spezifiziert im RFC 1952[307], und TAR eingesetzt werden. Die

304. siehe http://www.opengeospatial.org/specs/, publiziert als ISO/PRF 19136, siehe http://www.iso.org/
305. siehe http://www.opengeospatial.org/
306. siehe http://www.pkware.com/business_and_developers/developer/popups/appnote.txt

TAR-Header-Datei ist Bestandteil von POSIX.1-2001, das in dem ISO/IEC-Standard 9945[308] aufgegangen ist.

Um ein Dateiarchiv anzulegen, müssen zuerst alle Dateien mit TAR zu einer Archivdatei zusammengefasst werden. Die Archivdatei kann dann mit GZIP komprimiert werden (Dateiendung .tgz oder .tar.gz). Diese so genannte solide Kompression führt im Gegensatz zu ZIP-komprimierten Dateiarchiven zu geringeren Dateigrößen, da redundante Informationen über Dateigrenzen hinweg komprimiert werden.

8.6.13 Technologien für die Präsentation auf mobilen Endgeräten

Sofern ein Informationsangebot für Mobiltelefone beziehungsweise PDAs erstellt werden soll, ist der Aufbau von SMS-Diensten aufgrund der breiten Akzeptanz in der Bevölkerung zu bevorzugen. Die Darstellung von Web-Seiten für den Mobilfunk findet noch keine große Anwendung in Deutschland.

Über die folgenden Technologien hinaus sollten auch die Standards, die zur Präsentation von Inhalten durch Computer im allgemeinen beschrieben wurden, für mobile Endgeräte zum Einsatz kommen, siehe Abschnitte 8.6.1 bis 8.6.12.

Obligatorisch: Short Message Services (SMS)

Der Short Message Service (SMS)[309] ist Teil des GSM-Mobilfunk-Standards (Global System for Mobile communication), der vom 3rd Generation Partnership Project (3GPP) erarbeitet wird. Das 3GPP ist ein Zusammenschluss mehrerer Standardisierungsgremien (u. a. ETSI) mit dem Ziel der Erstellung von technischen Spezifikationen, die alle Aspekte der Mobilfunktechnik präzise beschreiben.

Unter Beobachtung: Wireless Application Protocol (WAP) v2.0

Das Wireless Application Protocol (WAP)[310] v2.0 ist eine Spezifikation zur Entwicklung von Anwendungen, die über drahtlose Kommunikationsnetzwerke operieren. Haupteinsatzgebiet ist der Mobilfunk. WAP umfasst die Wireless Markup Language (WML) v2.0. Die Darstellungsmöglichkeiten von WAP v2.0 haben sich gegenüber der Vorgängerversion denen im World Wide Web stark angenähert. Mit üblichen Web-Browsern sind WML-Seiten nicht lesbar. Somit müssen Angebote, die sowohl für mobiles als auch für das normale Internet angeboten werden sollen, zweifach publiziert werden.

WAP v2.0 enthält weiterhin das XHTML Mobile Profile (XHTMLMP)[311], das auf XHTML Basic basiert. Somit können Dokumente, die in XHTML Basic geschrieben wurden, mit WAP-2.0-Browsern gelesen werden. XHTMLMP unterstützt diverse Skriptsprachen, z. B. das ECMA-

307. siehe http://www.ietf.org/rfc/rfc1952.txt
308. siehe http://www.iso.org/
309. veröffentlicht als 3GPP TS 23.040, siehe http://www.3gpp.org/ftp/Specs/html-info/23040.htm, und veröffentlicht als ETSI TS 123 040 V7.0.1, siehe http://www.etsi.org/
310. siehe http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html
311. siehe http://www.openmobilealliance.org/tech/affiliates/wap/wap-277-xhtmlmp-20011029-a.pdf

Script Mobile Profile (ESMP), ein Subset von ECMA262[312] ohne rechen- und speicherintensive Skriptfunktionen.

Mittlerweile sind die meisten mobilen Endgeräte mit WAP-2.0-Browsern ausgestattet. Jedoch geht der Trend bei Handys und insbesondere bei PDAs hin zu Web-Browsern mit voller Funktionalität.

Unter Beobachtung: Extensible Hypertext Markup Language (XHTML) Basic v1.0

XHTML Basic v1.0[313] ist ein Standard zur Darstellung von auf XML umgesetzten HTML-Seiten für Anwendungen, die nicht die volle Darstellungsvielfalt von HTML unterstützen können (z. B. Mobilfunktelefone oder PDAs).

XHTML Basic wurde erweitert zum XHTML Mobile Profile (XHTMLMP)[314], das in WAP v2.0 enthalten ist. Somit können Dokumente, die in XHTML Basic geschrieben wurden, mit WAP-2.0-Browsern gelesen werden.

8.7 Kommunikation

Innerhalb des Elements Kommunikation wird zwischen Anwendungs-, Middleware- und Netzwerkprotokollen sowie Verzeichnisdiensten unterschieden.

8.7.1 Middleware-Kommunikation

Bei der Middleware-Kommunikation wird unterschieden, ob Server-Anwendungen innerhalb der Verwaltung untereinander kommunizieren, siehe Abschnitt 8.7.1.1, oder ob eine Client-Anwendung außerhalb der Verwaltung mit einem Server der Verwaltung kommuniziert, siehe Abschnitt 8.7.1.2.

Die Spezifikation der zu übertragenden Datenelemente sollte mittels der in Abschnitt 8.3 „Datenmodelle“ auf Seite 98 und Abschnitt 8.6.6 „Austauschformate für Daten“ auf Seite 111 benannten Technologien erfolgen.

8.7.1.1 Middleware-Kommunikation innerhalb der Verwaltung

Obligatorisch: Remote Method Invocation (RMI)

Für die interne Kommunikation zwischen Java-Objekten ist Java RMI[315] besonders geeignet. Über RMI kann ein Objekt auf einer Java Virtual Machine (VM) Methoden eines Objektes aufrufen, das in einer anderen Java VM existiert. Java Remote Method Invocation ist Bestandteil der Java Standard Edition (Java SE) und damit auch Bestandteil der Enterprise Edition (Java EE).

312. siehe Abschnitt 8.6.4 „Aktive Inhalte“ auf Seite 111
313. siehe http://www.w3.org/TR/2000/REC-xhtml-basic-20001219/
314. siehe http://www.openmobilealliance.org/tech/affiliates/wap/wap-277-xhtmlmp-20011029-a.pdf
315. siehe http://java.sun.com/rmi/

Obligatorisch: Simple Object Access Protocol (SOAP) v1.1

SOAP[316] sollte für die Kommunikation zwischen dem Erbringer und dem Nutzer eines Dienstes im Sinne des SOA-Referenzmodells[317] eingesetzt werden. Mittels SOAP können strukturierte Daten als XML-Objekte zwischen Anwendungen oder ihren Komponenten über ein Internetprotokoll (z. B. über HTTP) ausgetauscht werden.

Obligatorisch: Web Services Description Language (WSDL) v1.1

Zur Service-Definition sollte die Web Services Description Language (WSDL) eingesetzt werden. WSDL ist eine standardisierte Sprache[318], mit der Web Services so beschrieben werden, dass sie durch andere Applikationen genutzt werden können, ohne weitere Implementierungsdetails zu kennen oder die gleiche Programmiersprache einsetzen zu müssen.

Obligatorisch: Java Message Service (JMS) v1.1

Der JMS[319] wird zum Erzeugen, Senden, Empfangen und Lesen von Nachrichten (Messages) genutzt. Die JMS API definiert ein einheitliches Interface, um Java-Programmen die Kommunikation mit Messages zu anderen Messaging-Systemen zu ermöglichen. Die Kommunikation mit Messages hat den Vorteil der losen Kopplung. JMS sichert ab, dass die Nachrichten asynchron und verlässlich verschickt werden.

Der Einsatz von JMS sollte dann erfolgen, wenn die miteinander kommunizierenden Komponenten hinsichtlich ihrer Schnittstellen nicht offen gelegt werden sollen (leichtere Austauschbarkeit) und die Kommunikation zwischen den Komponenten generell asynchron und fehlertolerant verlaufen soll.

Obligatorisch: J2EE Connector Architecture (JCA) v1.5

JCA[320] sollte eingesetzt werden, um Bestandssysteme in Java-Anwendungen zu integrieren beziehungsweise mit ihnen zu kommunizieren. Dafür müssen die Systeme so genannte Ressource-Adapter bereitstellen. Für jedes Bestandssystem muss nur einmal ein Ressource-Adapter erstellt werden, er kann dann in allen Umgebungen für Java Enterprise Editionen (Java EE) wiederverwendet werden. Häufig benutzt der JCA Ressource-Adapter Messages, wie beispielsweise JMS, um mit den Bestandssystemen zu kommunizieren.

316. siehe http://www.w3.org/TR/soap11/
317. siehe Abbildung 6-2 auf Seite 71
318. siehe http://www.w3.org/TR/wsdl
319. publiziert als JSR-000914, siehe http://www.jcp.org/en/jsr/detail?id=914
320. publiziert als JSR-000112, siehe http://www.jcp.org/en/jsr/detail?id=112

Empfohlen: Java Language Mapping to OMG IDL

Die bekannteste Implementierung der Spezifikation Java Language Mapping to OMG IDL[321], die von der OMG veröffentlicht wurde, ist das Remote Method Invocation over Internet Inter ORB Protocol (RMI-IIOP) von Sun.

Java RMI-IIOP[322] ist integraler Bestandteil der Java Standard Edition (Java SE) und damit auch Bestandteil der Enterprise Edition (Java EE). Über RMI-IIOP können verteilte Java-Applikationen mit entfernten Anwendungen über CORBA kommunizieren. Eine RMI-IIOP-Kommunikation kann mit allen Object Request Brokern geführt werden, die der aktuellen CORBA Spezifikation 2.3.1[323] genügen. Die entfernten Anwendungen sind deshalb nicht auf die Sprache Java beschränkt.

Empfohlen: Web Services (WS)-Security v1.1

WS-Security[324] ist ein OASIS-Standard für sichere Web Services. Er definiert Erweiterungen des SOAP-Protokolls, um Vertraulichkeit, Integrität und Verbindlichkeit der SOAP-Nachrichten für die Sicherung von Web Services bereitzustellen. WS-Security unterstützt das Signieren und Verschlüsseln von SOAP-Nachrichten basierend auf XML Signature und XML Encryption. Unterschiedliche Sicherheitsmodelle und unterschiedliche kryptografische Verfahren sollen zugrunde liegen können.

Ebenfalls erlaubt WS-Security unterschiedliche „Sicherheits-Token", d. h. Datenformate, die bestimmte Identitäten oder Eigenschaften zusichern, z. B. X.509-Zertifikate, Kerberos Tickets, SAML-Token oder verschlüsselte Schlüssel.

Die Spezifikation von WS-Security besteht aus der „WS-Security Core Specification 1.1" und den Profilen:

a. Username Token Profile 1.1,
b. X.509 Token Profile 1.1,
c. SAML Token profile 1.1,
d. Kerberos Token Profile 1.1,
e. Rights Expression Language (REL) Token Profile 1.1 und
f. SOAP with Attachments (SWA) Profile 1.1.

Die Token Profile spezifizieren, wie die verschiedenen Token in SOAP genutzt werden können.

Unter Beobachtung: Universal Description, Discovery and Integration (UDDI) v2.0

Das UDDI-Protokoll ist die Basis für den Aufbau einer standardisierten, interoperablen Plattform, die das einfache, schnelle und dynamische Auffinden von Web Services erlaubt. Die

321. siehe http://www.omg.org/docs/ptc/00-01-06.pdf
322. siehe http://java.sun.com/products/rmi-iiop/
323. siehe http://omg.org/cgi-bin/doc?formal/99-10-07
324. siehe http://www.oasis-open.org/specs/index.php#wssv1.1

Weiterentwicklung von UDDI wird im Rahmen von OASIS vorangetrieben[325]. UDDI setzt auf Standards des W3C und der Internet Engineering Task Force (IETF) auf, wie z. B. XML, HTTP, DNS und SOAP.

8.7.1.2 Middleware-Kommunikation mit verwaltungsexternen Applikationen

Für den Zugriff von Client-Applikationen über das Internet auf Server-Applikationen bei der Verwaltung sollten Web Services verwendet werden.

Indem eine Web-Service-Schicht für eine existierende Server-Applikation zur Verfügung gestellt wird, ermöglicht sie es Client-Systemen, die Funktionen der Applikationen über das Hypertext Transfer Protocol (HTTP) aufzurufen. Ein Web Service ist ein Dienst, der aus Komponenten zusammengesetzt sein kann, und mit anderen Komponenten über das Standardprotokoll HTTP mittels SOAP kommuniziert. Für den Nachrichteninhalt selbst wird XML verwendet, das schon im Abschnitt 8.3 „Datenmodelle“ auf Seite 98 als universeller und primärer Standard für den Datenaustausch aller verwaltungstechnisch relevanten Informationssysteme beschrieben wurde.

Zur leichteren Zusammenstellung der benötigten Standards definiert die Web Service Interoperability Organization (WS-I) Profile aus bestehenden Standards. Das anzuwendende Profil ist WS-I-Basic v1.1[326] und umfasst u. a. XML Schema v1.0, SOAP v1.1, WSDL v1.1 und UDDI v2.0.

Obligatorisch: Simple Object Access Protocol (SOAP) v1.1

Analog zu Abschnitt 8.7.1.1 auf Seite 124.

Obligatorisch: Web Services Description Language (WSDL) v1.1

Analog zu Abschnitt 8.7.1.1 auf Seite 124.

Empfohlen: Web Services (WS)-Security v1.1

Analog zu Abschnitt 8.7.1.1 auf Seite 124.

Unter Beobachtung: Universal Description, Discovery and Integration (UDDI) v2.0

Analog zu Abschnitt 8.7.1.1 auf Seite 124.

325. siehe http://www.uddi.org/
326. siehe http://www.ws-i.org/Profiles/BasicProfile-1.1.html

8.7.2 Netzwerkprotokolle

Obligatorisch: Internet Protocol (IP) v4

Im IT-Umfeld der Bundesverwaltung sollte IP v4 (RFC 791[327], RFC 1700[328]) in Verbindung mit TCP (Transmission Control Protocol, RFC 793[329]) und UDP (User Datagram Protocol, RFC 768[330]) verwendet werden.

Bei der Neubeschaffung von Komponenten eines Systems sollten solche beschafft werden, die neben IP v4 auch IP v6 unterstützen, um eine zukünftige Migration zu ermöglichen.

Obligatorisch: Domain Name System (DNS)

Seit Mitte der 1980er Jahre ist das Domain Name System (DNS, RFC 1034[331], RFC 1035[332]) Standard im Internet. DNS bezeichnet einen hierarchischen Name-Server-Dienst an zentralen Stellen des Internets. Hier wird ein eingegebener Server-Name in die zugehörige IP-Adresse umgewandelt.

Unter Beobachtung: Internet Protocol (IP) v6

IP v6[333] ist die nächste Version des IP-Protokolls, die bisher noch keine weite Verbreitung gefunden hat. Eine der Änderungen gegenüber der aktuellen Version 4 ist die Vergrößerung der IP-Adresse auf 128 Bit, um zukünftig auch vielfältige eingebettete und mobile IP-basierte Systeme adressieren zu können.

IP v6 beinhaltet IPsec (IP-Security Protocol), das im Wesentlichen im Bereich VPN (Virtual Private Network) Anwendung findet und auch unabhängig von IP v6 eingesetzt werden kann. Durch den Einsatz von VPNs mit sicheren Verschlüsselungsverfahren wird der Transportkanal und die Authentisierung der Endsysteme sichergestellt, wie es z. B. für Funknetze (Wireless Local Area Network – WLAN), aber auch für Heimarbeitsplätze oder in der Standortvernetzung erforderlich ist. Informationen zu IPsec und VPN finden sich u. a. beim Bundesamt für Sicherheit in der Informationstechnik[334].

327. siehe http://www.ietf.org/rfc/rfc791.txt
328. siehe http://www.ietf.org/rfc/rfc1700.txt
329. siehe http://www.ietf.org/rfc/rfc793.txt
330. siehe http://www.ietf.org/rfc/rfc768.txt
331. siehe http://www.ietf.org/rfc/rfc1034.txt
332. siehe http://www.ietf.org/rfc/rfc1035.txt
333. siehe http://www.ietf.org/rfc/rfc2460.txt und http://www.ietf.org/rfc/rfc3041.txt
334. siehe http://www.bsi.de/, z. B. „Aufbau von Virtual Private Networks (VPN) und Integration in Sicherheitsgateways“ unter http://www.bsi.de/fachthem/sinet/loesungen_transport/VPN.pdf

8.7.3 E-Mail-Kommunikation

Obligatorisch:	Simple Mail Transfer Protocol (SMTP) / Multipurpose Internet Mail Extensions (MIME) v1.0

Für den E-Mail-Transport werden E-Mail-Protokolle vorausgesetzt, die den Spezifikationen von SMTP / MIME[335] für den Nachrichten-Austausch entsprechen (RFC 2821, RFC 2045 bis RFC 2049)[336]. E-Mail-Anhänge sollten den Dateiformaten entsprechen, die im Abschnitt 8.6 „Präsentation“ auf Seite 108 definiert wurden.

Obligatorisch:	Post Office Protocol (POP) v3 / Internet Message Access Protocol (IMAP) v4rev1

In Ausnahmefällen kann es vorkommen, dass elektronische Postfächer angeboten werden müssen. Dazu sollten POP3[337] oder IMAP[338] als weit verbreitete Standards eingesetzt werden.

Obligatorisch:	Industrial Signature Interoperability Specification - MailTrusT (ISIS-MTT) v1.1, Teile 1 bis 6

Für die Interaktionsstufe Kommunikation ist ein möglicher Anwendungsfall der sichere Austausch von E-Mails. Eine sichere E-Mail-Kommunikation umfasst die Sicherung von E-Mails während ihrer Übermittlung von einem Sender zu einem Empfänger. Dieser Anwendungsfall betrachtet E-Mails in ihrer Gesamtheit. Die Sicherung von Dokumenten, auch von E-Mail-Anlagen, wird in Abschnitt 8.6.7.7 „Gesicherter Dokumentenaustausch“ auf Seite 116 behandelt.

Die ISIS-MTT-Spezifikation berücksichtigt auf Basis der Grundfunktionen elektronische Signatur, Verschlüsselung und Authentisierung vielfältige Anwendungsfelder von Verfahren zur Sicherung des elektronischen Geschäftsverkehrs (z. B. Datei-, Mail-, Transaktions- und Zeit-Sicherung), siehe Abschnitt 8.1.4 „Umsetzung der Sicherheitskonzeption“ auf Seite 95.

Für die Sicherung von E-Mail-Kommunikation sind insbesondere die Teile 1 bis 6 relevant.

8.7.4 IP-Telefonie

Sprache beziehungsweise Telefonie ist ein wichtiger und etablierter Kommunikationskanal für Bürger, Unternehmen und Behörden. Auch Behörden betreiben bereits Callcenter und nutzen dafür teilweise Telefonanlagen mit Voice-over-IP (VoIP). Für diese Kommunikationsart sind im Bereich der Präsentation die Schnittstellen nach außen anzubieten und im Backend Schnittstellen zu E-Government-Anwendungen bereitzustellen (Computer Telephony Integration – CTI). So können den Kunden auf Web-Seiten kontextabhängig VoIP-Verbindungen zu den jeweils spezialisierten Bearbeitern oder Callcenter-Mitarbeitern

335. siehe auch Abschnitt 8.6.3 „Technologien zur Informationsaufbereitung“ auf Seite 109
336. siehe http://www.ietf.org/rfc.html
337. publiziert als RFC 1939, siehe http://www.ietf.org/rfc/rfc1939.txt
338. publiziert als RFC 3501, siehe http://www.ietf.org/rfc/rfc3501.txt

angeboten und beim Bearbeiter die bis dahin eingegebenen Daten medienbruchfrei angezeigt werden.

Empfohlen: H.323

Für IP-Telefonie soll das Protokoll zur Signalisierung nach dem Standard H.323[339] der ITU-T mit den zu dieser Familie gehörenden Protokollen zum Datentransport eingesetzt werden.

Unter Beobachtung: Session Initiation Protocol (SIP) v2.0

SIP ist ein von der IETF erarbeiteter Standard für die Signalisierung bei IP-Telefonie (RFC 3261[340]). Er kann zusammen mit den ergänzenden Protokollen zur Datenübertragung als Alternative zu H.323 eingesetzt werden.

8.7.5 Anwendungsprotokolle

Die Anbindung von sicherheitsbezogenen Infrastrukturen (z. B. Verzeichnisdienste für Zertifikate, Sperrlisten usw.) wird in Abschnitt 8.1.4 „Umsetzung der Sicherheitskonzeption“ auf Seite 95 behandelt.

Obligatorisch: File Transfer Protocol (FTP)

Für die Dateiübertragung gilt das File Transfer Protocol (FTP, RFC 959[341]) als Standard. FTP ist einer der ältesten Internetdienste. Ziele von FTP sind es, das Mitbenutzen von Dateien zu ermöglichen, dem Benutzer die einheitliche Bedienung von verschiedenen Dateisystemtypen bereitzustellen und Daten effizient und verlässlich zu transportieren. Der Download größerer Dateien gelingt über FTP meist etwas schneller als über HTTP.

Da FTP sämtliche Daten, inklusive Passwörter, unverschlüsselt versendet, sollte es nicht für Anwendungen mit erhöhtem Sicherheitsbedarf eingesetzt werden. In diesem Fall sind gesicherte Verfahren, wie z. B. SSH-2 und TLS, die ebenfalls in diesem Abschnitt beschrieben sind, zu verwenden.

Obligatorisch: Hypertext Transfer Protocol (HTTP) v1.1

Für die Kommunikation zwischen Client und Web-Server sollte HTTP v1.1 (RFC 2616[342]) eingesetzt werden. Web-Server sollten neben der Version 1.1 aber auch HTTP v1.0 (RFC 1945[343]) unterstützen. Beim Einsatz von HTTP Session Management und Cookies sollte der Standard HTTP State Management Mechanism (RFC 2965[344]) befolgt werden. HTTP v1.1 bietet gegenüber der Version 1.0 durch seine Upload- und Download-Funktionalität die

339. siehe http://www.itu.int/rec/T-REC-H.323/en
340. siehe http://www.ietf.org/rfc/rfc3261.txt
341. siehe http://www.ietf.org/rfc/rfc959.txt
342. siehe http://www.ietf.org/rfc/rfc2616.txt
343. siehe http://www.ietf.org/rfc/rfc1945.txt
344. siehe http://www.ietf.org/rfc/rfc2965.txt

Möglichkeit für so genannte „Web-Ordner“ (siehe WebDAV auf Seite 132). Chat-Systeme können mittels HTTP v1.1 das Neuladen der Web-Seite veranlassen.

Obligatorisch: Online Service Computer Interface (OSCI)-Transport v1.2

Das Online Service Computer Interface (OSCI)[345] wurde im Rahmen des Wettbewerbs MEDIA@Komm entworfen. OSCI umfasst eine Menge von Protokollen, die für die Anforderungen im E-Government geeignet sind und durch die OSCI-Leitstelle erstellt werden. Zielsetzung ist die Unterstützung von Transaktionen in Form von Web Services und deren vollständige Abwicklung über das Internet.

OSCI-Transport 1.2 ist der Teil von „OSCI“, der die Querschnittsaufgaben im Sicherheitsbereich löst. Die Existenz einer zentralen Vermittlungsstelle, des so genannten Intermediär, der Mehrwertdienstleistungen erbringen kann, ohne die Vertraulichkeit auf der Ebene der Daten zu Geschäftsvorfällen zu gefährden, ist für die sichere Umsetzung von Prozessen des E-Government mittels OSCI charakteristisch. Als sicheres Übertragungsprotokoll ermöglicht es verbindliche (auch SigG-konforme) Online-Transaktionen.

OSCI-Transport unterstützt die asynchrone Kommunikation per Intermediär und die Ende-zu-Ende-Verschlüsselung für die vertrauliche Übermittlung von Daten. OSCI-Transport standardisiert sowohl die Nachrichteninhalte als auch die Transport- und Sicherheitsfunktionen und basiert auf internationalen Standards (u. a. XML Signature, DES, AES, RSA und X.509), die in geeigneter Weise konkretisiert werden.

Wesentliche Designkriterien für OSCI-Transport in der Version 1.2 waren:

a. Aufsetzen auf offene Standards (SOAP, XML Signature, XML Encryption),
b. Technikunabhängigkeit, d. h. Übertragung mit einem beliebigen technischen Kommunikationsprotokoll ohne spezifische Anforderungen an Plattformen und Programmiersprachen,
c. Skalierbarkeit der Sicherheitsniveaus (fortgeschrittene Signaturen oder qualifizierte beziehungsweise akkreditierte elektronische Signaturen nach Bedarf der Anwendung).

Obligatorisch: Transport Layer Security (TLS) v1.0

TLS[346] ist ein kryptografisches Protokoll, das die Integrität und die Vertraulichkeit einer Kommunikationsverbindung im World Wide Web sichert. Es wurde aus dem Protokoll Secure Sockets Layer (SSL) entwickelt. Der bis einschließlich SAGA Version 2.1 obligatorische Standard SSL v3 wird in der Bestandsschutzliste (ehemals Grey List) geführt. Ältere SSL-Standards sollten aus Sicherheitsgründen auch für bestehende Anwendungen nicht mehr verwendet werden.

TLS setzt auf TCP/IP auf und sichert Kommunikationsprotokolle für Anwendungen, wie z. B. HTTP, IIOP, RMI etc., in transparenter Art und Weise. TLS-gesicherte Web-Seiten werden mit https:// statt mit http:// angesprochen.

345. siehe http://www.osci.de/
346. publiziert als RFC 2246, siehe http://www.ietf.org/rfc/rfc2246.txt

TLS unterstützt ebenfalls eine einseitige Authentisierung des Behörden-Servers gegenüber dem Client des Kommunikationspartners, damit sich dieser davon überzeugen kann, dass er tatsächlich mit dem Behörden-Server verbunden ist. Auch eine beidseitige Authentisierung von Client und Server kann durch TLS unterstützt werden.

TLS bietet folgende kryptografische Mechanismen:

a. asymmetrische Authentisierung der Kommunikationspartner (über X.509-Zertifikate),
b. sicherer Austausch von Sitzungsschlüsseln (über RSA-Verschlüsselung oder Diffie-Hellman-Schlüsseleinigung),
c. symmetrische Verschlüsselung der Kommunikationsinhalte,
d. symmetrische Nachrichtenauthentisierung (über MACs) und Schutz gegen Wiedereinspielen von Nachrichten.

Die genaue Funktionsweise von TLS ist im KoopA ADV Handlungsleitfaden[347] Abschnitt 5.2.2 beschrieben. Die Kombination verschiedener Verfahren wird in TLS als „Cipher Suite" bezeichnet. Eine TLS-Cipher-Suite enthält stets vier kryptografische Algorithmen: ein Signaturverfahren, ein Schlüsselaustauschverfahren, ein symmetrisches Verschlüsselungsverfahren sowie eine Hash-Funktion.

Empfohlen: Secure Shell v2 (SSH-2)

Das Protokoll SSH-2[348] ist die weiterentwickelte Version des seit 1995 existenten SSH. Es ermöglicht, durch einen standardisierten Authentisierungsvorgang einen verschlüsselten Kanal (Tunnel) zwischen Client- und Server-System zu öffnen und anschließend über die Transportschicht verschlüsselte Nutzdaten zu senden und zu empfangen. Die verschiedenen Open-Source- und kommerziellen Implementierungen des Protokolls bieten Möglichkeiten zur starken Verschlüsselung der Nutzdaten und lassen beispielsweise die Fernsteuerung entfernter Rechner und Dateitransfer (SSH-FTP) zu. Somit existiert eine sichere Alternative zu FTP.

Empfohlen: WWW Distributed Authoring and Versioning (WebDAV)

WebDAV[349] ist ein von der Internet Engineering Task Force (IETF) erarbeiteter Standard, der als Erweiterung von HTTP zum Schreiben und Verändern von Dateien in Netzwerken eingesetzt werden kann. Er stellt somit eine Alternative zu FTP dar. Im Gegensatz zu FTP muss bei der Dateiübertragung mittels WebDAV kein Port extra freigegeben werden, da WebDAV den HTTP Port 80 benutzt. Der schreibende Zugriff mittels Passwörtern sollte verschlüsselt erfolgen, z. B. über HTTPS oder TLS. Jedoch bieten nicht alle Anwendungen, die WebDAV unterstützen, einen Support für die genannten Verschlüsselungsmechanismen.

347. siehe http://www.koopa.de/projekte/pki.html
348. publiziert unter RFC 4251 - 4256, siehe http://www.ietf.org/rfc.html
349. publiziert als RFC 2518, siehe http://www.ietf.org/rfc/rfc2518.txt und http://www.webdav.org/

Unter Beobachtung: Transport Layer Security (TLS) v1.1

TLS v1.1[350] ist eine im April 2006 verabschiedete Weiterentwicklung von TLS v1.0, bei der die Sicherheit verbessert wurde. Die Unterstützung von TLS v1.1 ist für die nächste Generation von Web-Browsern geplant.

8.7.6 Geodienste

Alle Standards in diesem Abschnitt sind entweder Spezifikationen des Open Geospatial Consortium (OGC)[351] oder bauen auf diesen auf. Die Klassifikationen wurden mit der Geodateninfrastruktur Deutschland (GDI-DE)[352] abgestimmt und orientieren sich an [GDI-DE 2007]. Die Festlegung von Formaten für den Austausch von Geoinformationen erfolgt im Abschnitt 8.6.11 auf Seite 122.

Empfohlen: Catalogue Services Specification v2.0 – ISO Metadata Application Profile v1.0

Bei dem Catalogue Services Specification v2.0 – ISO Metadata Application Profile[353] handelt es sich um ein Applikationsprofil für Katalogdienste, das vom OGC angenommen wurde. Das Profil bezieht sich auf die CSW-Basisspezifikation des OGC und auf die Metadatenspezifikationen von der ISO (ISO 19115, ISO 19119). Es sollte zur Implementierung einer standardkonformen Metadatenrecherche genutzt werden.

Empfohlen: Web Map Service Deutschland (WMS-DE) v1.0

Ziel des Profils WMS-DE[354] ist es, die von der Geodateninfrastruktur Deutschland (GDI-DE) an einen Web Map Service (WMS) gestellten Anforderungen verbindlich zu definieren. Mit WMS-Diensten, die dieses Profil unterstützen, wird beim Anwender eine deutschlandweite Darstellung durch Kombination der digitalen Karten und Daten verschiedener WMS-Dienste möglich. Von den verbindlichen Randbedingungen im Rahmen der GDI-DE sollen sowohl die Anbieter beim Einrichten der Dienste, als auch die Nutzer bei der Abfrage profitieren.

Empfohlen: Web Coverage Service (WCS) v1.0

WCS[355] ermöglicht den Zugriff auf mehrdimensionale Rasterdaten. Dieser Dienst eignet sich insbesondere zur Abgabe von Rasterdaten z. B. in Shoplösungen, zur Bereitstellung von Messwerten in Form von Zeitreihen sowie für die Abgabe von digitalen Geländemodellen.

350. publiziert als RFC 4346, siehe http://www.ietf.org/rfc/rfc4346.txt
351. siehe http://www.opengeospatial.org/
352. siehe http://www.gdi-de.org/
353. siehe http://www.opengeospatial.org/standards/cat
354. siehe http://www.gdi-de.org/de/download/WMS_DE_Profil_V1.pdf
355. siehe http://www.opengeospatial.org/specs/

Empfohlen: Web Feature Service (WFS) v1.0

WFS v1.0.0[356] ermöglicht den Zugriff auf Geodatenobjekte (Features), in der Regel in Form von Vektordaten. Der Datenaustausch erfolgt in der Geography Markup Language (GML) v2.1.2, siehe Abschnitt 8.6.11 „Austauschformate für Geoinformationen“ auf Seite 122.

Empfohlen: Web Feature Service (WFS) v1.1

WFS v1.1.0[357] findet im Vergleich zu der Version 1.0.0 bislang eine nicht so breite Anwendung. Der Datenaustausch erfolgt in Geography Markup Language (GML) v3.1.1, siehe Abschnitt 8.6.11 „Austauschformate für Geoinformationen“ auf Seite 122.

Empfohlen: Simple Feature Access – Part 2: SQL option (SFA-2) v1.1.0

SFA-2[358] definiert Schnittstellen zum Zugriff auf Geodatenobjekte (Features). Der Standard wurde neben dem OGC auch von der ISO standardisiert und trägt deshalb auch den Namen ISO 19125-2[359].

8.8 Backend

In der deutschen Verwaltung werden verschiedene Bestands- oder Legacy-Systeme eingesetzt und mit einer hohen Wahrscheinlichkeit auch weiterhin betrieben (z. B. ERP, Mainframe-Transaktionsverarbeitung, Datenbanksysteme und andere Legacy-Applikationen). Diese Legacy-Systeme können je nach unterstützter Betriebsart in drei Klassen gruppiert werden:

a. transaktionsgesicherte Verarbeitung durch Endbenutzer mittels vorhandener Dialogsysteme,
b. asynchrone Verarbeitung von Daten mit Stapelverarbeitungsprozessen (Massendatenverarbeitung) und
c. Programm-Programm-Kommunikation auf der Basis proprietärer Protokolle.

Zur Integration von Bestandssystemen existieren zwei grundsätzliche Möglichkeiten:

a. direkte Integration über so genannte „Legacy-Schnittstellen“ oder
b. Integration über eine eigene Integrationsschicht, in welcher der eigentliche Zugriff auf die Bestandssysteme modular gekapselt wird.

Detaillierte Lösungskonzepte müssen in Anbetracht der zu erreichenden Ziele, der zur Verfügung stehenden Zeit, des vorhandenen Budgets und der Funktionen, die bei der Integration des Bestandssystems unterstützt werden sollen, bewertet und verglichen werden.

Die folgenden Abschnitte skizzieren unterschiedliche Lösungskonzepte, die sich bei den drei genannten Betriebsarten bewährt haben.

356. siehe http://www.opengeospatial.org/specs/
357. siehe http://www.opengeospatial.org/specs/
358. siehe http://www.opengeospatial.org/specs/
359. siehe http://www.iso.org/

Die Spezifikation der zu übertragenden Datenelemente sollte mittels der in Abschnitt 8.3 „Datenmodelle“ auf Seite 98 und Abschnitt 8.6.6 „Austauschformate für Daten“ auf Seite 111 benannten Technologien erfolgen.

8.8.1 Verzeichnisdienste und Registrys

Obligatorisch: Lightweight Directory Access Protocol (LDAP) v3

LDAP v3 (RFC 4510 - 4519[360]) ist ein auf hierarchisch geordnete Informationen optimiertes Protokoll des Internets, das auf X.500 basiert und für den Zugriff auf Verzeichnisdienste verwendet wird.

Unter Beobachtung: Universal Description, Discovery and Integration (UDDI) v2.0

Analog zu Abschnitt 8.7.1.2 „Middleware-Kommunikation mit verwaltungsexternen Applikationen“ auf Seite 127.

Unter Beobachtung: Directory Services Markup Language (DSML) v2

DSML[361] ist eine XML-basierte Sprache, um Daten mit Verzeichnisdiensten – z. B. im Zuge von Anfragen und Aktualisierungen – auszutauschen. Der Zugriff auf die Verzeichnisdienste wird durch die Verwendung der Spezifikation erleichtert. DSML v2 wurde 2001 als OASIS-Standard veröffentlicht.

Unter Beobachtung: ebXML Registry Services and Protocols (ebXML RS) v3.0/ ebXML Registry Information Model (ebXML RIM) v3.0

ebXML RS beschreibt die Dienste und Protokolle, die eine ebXML-konforme Registry bietet. Eine ebXML-Registry ist ein System, das beliebige Inhalte und zugehörige, standardisierte Metadaten sicher verwaltet. ebXML RIM beschreibt das zugehörige Informationsmodell. Die Anwendung der Technologien sollte zusammen erfolgen.

ebXML RS v3.0[362] und ebXML RIM v3.0[363] wurden von OASIS[364] am 1. Mai 2005 als OASIS-Standards verabschiedet. Die Version 3.0 ergänzt viele nützliche Features gegenüber der Version 2.0, z. B. Versionierung von Repository-Inhalten.

8.8.2 Zugriff auf Datenbanken

Obligatorisch: Java Database Connectivity (JDBC) v3.0

Für Zugriffe auf Datenbanken sollte JDBC[365] genutzt werden.

360. siehe http://www.ietf.org/rfc/rfc4510.txt
361. siehe http://www.oasis-open.org/specs/index.php#dsmlv2
362. siehe http://www.oasis-open.org/specs/index.php#ebxmlrsv3.0
363. siehe http://www.oasis-open.org/specs/index.php#ebxmlrimv3.0
364. siehe http://www.oasis-open.org/

8.8.3 Zugriff auf Bestandssysteme

Obligatorisch: Remote Method Invocation (RMI)

Analog zu Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124.

Obligatorisch: Simple Object Access Protocol (SOAP) v1.1

Analog zu Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124.

Obligatorisch: Web Services Description Language (WSDL) v1.1

Analog zu Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124.

Obligatorisch: Java Message Service (JMS) v1.1

Analog zu Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124.

Obligatorisch: J2EE Connector Architecture (JCA) v1.5

Analog zu Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124.

Empfohlen: Java Language Mapping to OMG IDL

Analog zu Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124.

Empfohlen: Web Services (WS)-Security v1.1

Analog zu Abschnitt 8.7.1.1 „Middleware-Kommunikation innerhalb der Verwaltung“ auf Seite 124.

8.9 Verschlüsselung

Kryptografische Algorithmen für die Verschlüsselung können auf Daten und / oder Schlüssel angewendet werden, um diese vertraulich zu übermitteln.

365. publiziert als JSR-000054, siehe http://www.jcp.org/en/jsr/detail?id=54

8.9.1 Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsverfahren sind z. B. notwendig, um einen so genannten Session-Key zwischen Kommunikationspartnern auszutauschen. Ein Session-Key ist ein symmetrischer Schlüssel, siehe Abschnitt 8.9.2 auf Seite 137.

Obligatorisch: RSA

Das RSA-Verfahren[366] ist das wichtigste asymmetrische Verfahren, auch Public-Key-Verfahren genannt. Beim Verschlüsseln wird die zu verschlüsselnde Bitfolge mit dem öffentlichen Schlüssel des Kommunikationspartners verschlüsselt. Danach kann der entstandene verschlüsselte Geheimtext nur noch vom Besitzer des privaten Schlüssels wieder in Klartext entschlüsselt werden. Die Sicherheit basiert auf der Schwierigkeit, große natürliche Zahlen zu faktorisieren. Übliche Schlüssellängen sind 2048 und 4096 Bit. 1024-Bit-Schlüssel werden von der Bundesnetzagentur nicht mehr empfohlen.

RSA wird beim Verschlüsseln äquivalent zum Signieren genutzt, siehe Abschnitt 8.10.2 auf Seite 138.

8.9.2 Symmetrische Verschlüsselungsverfahren

Werden symmetrische Verfahren verwendet, so benutzen diese den gleichen geheimen Schlüssel für die Verschlüsselung und Entschlüsselung. Diese Verfahren sind im Allgemeinen sehr performant.

Obligatorisch: Advanced Encryption Standard (AES)

AES[367] ist ein symmetrischer Blockchiffre, dessen Blocklänge auf 128 Bit festgelegt ist und dessen Schlüssellänge 128, 192 oder 256 Bits groß sein kann. AES wurde im Oktober 2000 vom National Institute of Standards and Technology (NIST)[368] veröffentlicht.

Der bis einschließlich SAGA Version 2.1 empfohlene Triple Data Encryption Standard (Triple-DES, auch 3DES) wird in der Bestandsschutzliste (ehemals Grey List) geführt.

8.10 Elektronische Signatur

Die Sicherheit einer elektronischen Signatur hängt primär von der Stärke der zugrunde liegenden Kryptoalgorithmen ab. Zum Thema „Elektronische Signatur“ siehe auch Abschnitt 4.5.1 auf Seite 47.

366. RSA wurde benannt nach den Erfindern Ronald L. **Ri**vest, Adi **S**hamir und Leonard **A**dleman
367. siehe http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, publiziert als FIPS 197
368. siehe http://csrc.nist.gov/

Obligatorisch: Kryptoalgorithmen nach Bundesnetzagentur für die elektronische Signatur

Die Bundesnetzagentur veröffentlicht im Bundesanzeiger jährlich die geeigneten Kryptoalgorithmen, die in Erfüllung der Anforderungen nach Signaturgesetz (SigG) und Signaturverordnung (SigV) als mindestens geeignet für die jeweils kommenden sechs Jahre anzusehen sind[369]. Dazu werden auch die für eine ausreichende Sicherheit notwendigen Mindestgrößen von Parametern wie Blockgrößen und Schlüssellängen angegeben. Das BSI kann die Eignung weiterer Verfahren feststellen.

Eine elektronische Signatur im Sinne des Gesetzes umfasst die folgenden Kryptoalgorithmen.

8.10.1 Hashen von Daten

Eine Hash-Funktion reduziert die zu signierenden Daten auf einen Hash-Wert, eine Bitfolge fester Länge. Signiert werden dann nicht die Daten selbst, sondern stattdessen jeweils ihr Hash-Wert.

Obligatorisch: Secure Hash Algorithm (SHA)-256

SHA-256 (Secure Hash Algorithm)[370] ist eine kryptografische Hash-Funktion, die als Weiterentwicklung von SHA-1 (160 Bit langer Hash-Wert) einen 256 Bit langen Hash-Wert generiert.

Empfohlen: Secure Hash Algorithm (SHA)-224 / Secure Hash Algorithm (SHA)-384 / Secure Hash Algorithm (SHA)-512

SHA-224, SHA-384 und SHA-512 (Secure Hash Algorithm)[371] sind kryptografische Hash-Funktionen, die als Weiterentwicklungen von SHA-1 (160 Bit langer Hash-Wert) längere Hash-Werte generieren (die Länge entspricht der angegebenen Nummer).

8.10.2 Asymmetrische Signaturverfahren

Ein asymmetrisches Signaturverfahren besteht aus einem Signier- und einem Verifizieralgorithmus. Das Signaturverfahren hängt von einem Schlüsselpaar ab, bestehend aus einem privaten (d. h. geheimen) Schlüssel zum Signieren (Erzeugen) und dem dazugehörigen öffentlichen Schlüssel zum Verifizieren (Prüfen) der Signatur.

Obligatorisch: RSA

Analog zu Abschnitt 8.9.1 „Asymmetrische Verschlüsselungsverfahren“ auf Seite 137 sollte RSA für das asymmetrische Signaturverfahren eingesetzt werden.

369. siehe http://www.bundesnetzagentur.de/enid/Veroeffentlichungen/Algorithmen_sw.html
370. publiziert als FIPS PUBS 180-2, siehe http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
371. publiziert als FIPS PUBS 180-2, siehe http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

Empfohlen: Digital Signature Algorithm (DSA)

Der Digital Signature Algorithm (DSA)[372] ist das Signaturverfahren, das im amerikanischen Digital Signature Standard (DSS) 1991 spezifiziert wurde. DSA ist ein reiner Signaturalgorithmus. Die US-Regierung hat DSS patentiert, die Benutzung ist jedoch frei. DSA ist weniger verbreitet als RSA. Der Algorithmenkatalog der Bundesnetzagentur sieht ab 2008 für qualifizierte elektronische Signaturen gegenüber dem Standard vergrößerte Parameterlängen vor. Übliche Schlüssellängen sind 2048 und 4096 Bit. 1024-Bit-Schlüssel werden von der Bundesnetzagentur nicht mehr empfohlen.

8.10.3 Key Management

Damit Anwendungen elektronische Signaturen einsetzen können, muss es die Möglichkeit geben, öffentliche elektronische Schlüssel (Public Keys) realen Personen oder Institutionen zuzuordnen. Um Interoperabilität zwischen verschiedenen Anwendungen zu erreichen, müssen die Formate für diese Daten übereinstimmen sowie einheitliche Mechanismen zum Lesen und Schreiben der Daten eingesetzt werden.

Empfohlen: XML Key Management Specification (XKMS) v2

XKMS[373] spezifiziert Protokolle zur Registrierung und Verteilung von Public Keys. Die Protokolle sind für das Zusammenspiel mit XML Signature und XML Encryption entworfen worden und finden ihr Anwendungsgebiet deshalb bei XML-basierter Kommunikation, wie z. B. bei Web Services. Die Spezifikation besteht aus zwei Teilen: die XML Key Registration Service Specification (X-KRSS) und die XML Key Information Service Specification (X-KISS).

Clients können vergleichsweise einfache XKMS-Anfragen zum Auffinden und Validieren von Public Keys einsetzen und Relay-Server greifen zur Beantwortung der Anfragen auf bestehende LDAP- und OCSP-Infrastrukturen zu. Mit nur einem Protokoll können so parallel verschiedene Verzeichnisdienste genutzt werden.

8.11 Smartcards

Smartcards sind Chipkarten mit integriertem Prozessor, die auch als Mikroprozessorkarten bezeichnet werden. Im Gegensatz zu Chipkarten, die nur der Speicherung von Daten dienen (Speicherkarten), können Smartcards auch Daten verarbeiten. Smartcards können als Personal Security Environment (PSE) dienen, um vertrauenswürdige Zertifikate und private Schlüssel sicher aufzubewahren und darüber hinaus auch als (sichere) Signaturerstellungseinheit fungieren.[374]

Nach der Art der Kontaktierung des Chips unterscheidet man kontaktbehaftete und kontaktlose Smartcards. Während kontaktbehaftete Smartcards über sichtbare, äußere Kon-

372. publiziert als FIPS 186-2, siehe http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
373. siehe http://www.w3.org/TR/xkms2/
374. siehe Bundesamt für Sicherheit in der Informationstechnik (BSI): „Grundlagen der elektronischen Signatur – Recht, Technik, Anwendung“, 2006, http://www.bsi.de/esig/esig.pdf

taktflächen verfügen, wird die Kommunikation mit den Lesegeräten bei kontaktlosen Smartcards über Funkkommunikation (Radio Frequency IDentification – RFID) hergestellt.

8.11.1 Kontaktbehaftete Smartcards

Obligatorisch: Identification Cards - Integrated circuit cards

Kontaktbehaftete Smartcards sollten der Norm ISO/IEC 7816[375] entsprechen. Der Standard beschreibt u. a. Abmessungen, Positionierung von Kontakten und Beschriftung, elektrische Eigenschaften sowie Übertragungsprotokolle.

8.11.2 Kontaktlose Smartcards

Obligatorisch: Identification Cards – Contactless integrated circuit cards

Kontaktlose Smartcards mit einer Übertragungsrate von bis zu ca. 847 kbit/s – das entspricht einer Reichweite bis zu 0,1 m – sollten der Norm ISO/IEC 14443[376] entsprechen. Der Standard beschreibt in vier Teilen Aufbau, Funktion und Betrieb dieser Smartcards. Der elektronische Reisepass[377] basiert auf diesem Standard. Der in Planung befindliche elektronische Personalausweis soll ebenfalls auf dem Standard beruhen.

8.11.3 Lesegeräte und Schnittstellen für Smartcards

Obligatorisch: Technische Richtlinie für die eCard-Projekte der Bundesregierung (BSI TR-03116) v1.0

Smartcard-Anwendungen, welche kryptografische Verfahren einsetzen, sollten die in der technischen Richtlinie BSI TR-03116[378] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschriebenen Sicherheitsanforderungen für den Einsatz kryptografischer Verfahren in eCard-Projekten der Bundesregierung berücksichtigen.

Obligatorisch: Industrial Signature Interoperability Specification - MailTrust (ISIS-MTT) v1.1, Teil 7

Komponenten, welche die universelle Krypto-Schnittstelle „Cryptographic Token Interface" (Cryptoki) unterstützen, sollten Konformität zu ISIS-MTT[379] v1.1, Teil 7 (Cryptographic Token Interface) aufweisen.

375. siehe http://www.iso.org/
376. siehe http://www.iso.org/
377. siehe http://www.epass.de/
378. siehe http://www.bsi.bund.de/literat/tr/tr03116/BSI-TR-03116.pdf
379. siehe http://www.isis-mtt.org/

Unter Beobachtung:	Interoperability Specification for ICCs and Personal Computer Systems (PC/SC) v2.0

PC/SC[380] spezifiziert eine Schnittstelle zwischen Kartenlesegeräten und den Anwendungen.

Unter Beobachtung:	OpenCard Framework (OCF) v1.2

OCF[381] spezifiziert eine Schnittstelle zwischen Kartenlesegeräten und den Anwendungen.

Unter Beobachtung:	Secure Interoperable ChipCard Terminal (SICCT) v1.10

SICCT[382] beschreibt ein Basiskonzept für applikationsunabhängige Terminals für Smartcards auf der Grundlage von ISO/IEC 7816 und ISO/IEC 14443[383]. Anwendungen mit hohen oder sehr hohen Sicherheitsanforderungen können Konformität zu SICCT anstreben.

8.12 Langzeitarchivierung

Mit der zunehmenden Verbreitung von elektronischen Dokumenten in Verwaltungen ist es für deren nachhaltige und langfristige Aufbewahrung notwendig, Standards für die Speicherung zu verwenden, welche die Authentizität und Vollständigkeit der Dokumente gewährleisten.

Empfohlen:	Tagged Image File Format (TIFF) v6.0

Für Grafiken und S/W-Bilder sollte TIFF v6.0 zur Langzeitarchivierung eingesetzt werden. In diesem Einsatzfeld ist maximale Interoperabilität besonders wichtig. Deshalb sind ausschließlich Eigenschaften aus der „Baseline TIFF" einzusetzen sind, siehe auch Abschnitt 8.6.8 auf Seite 118.

Empfohlen:	Joint Photographic Experts Group (JPEG)

Analog zu Abschnitt 8.6.8 „Austauschformate für Bilder" auf Seite 118 sollte JPEG für die Langzeitarchivierung von Bildern, insbesondere für Fotos, eingesetzt werden.

Empfohlen:	Extensible Markup Language (XML) v1.0

XML ist für die Langzeitarchivierung geeignet, dazugehörige Schemata und XSL-Dateien müssen jedoch auch archiviert werden, siehe auch Abschnitt 8.6.6 „Austauschformate für Daten" auf Seite 111. Beispiele für XML-basierte Sprachen zur Langzeitarchivierung sind

380. siehe http://www.pcscworkgroup.com/specifications/specdownload.php
381. siehe http://www.opencard.org/index-downloads.shtml
382. siehe http://www.teletrust.de/fileadmin/files/publikationen/Spezifikationen/SICCT_Spezifikation_1.10.pdf
383. siehe http://www.iso.org/

Encoded Archival Description (EAD)[384], Encoded Archival Context (EAC)[385] und Metadata Encoding and Transmission Standard (METS)[386].

Empfohlen: ArchiSig, Grundsätze für die beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente

Das Projekt ArchiSig[387] wurde von verschiedenen Teilnehmern aus Wissenschaft und Industrie sowie Anwendern unter Federführung des Informatikzentrums Niedersachsen und der Staatlichen Archivverwaltung Niedersachsen durchgeführt. Es legt Grundsätze[388] zur Langzeitsicherung elektronisch signierter Dokumente fest, die beachtet werden sollten.[389]

Empfohlen: Portable Document Format Archive - 1 (PDF/A-1)

Der Standard PDF/A-1[390] (ISO 19005-1:2005[391]) basiert auf PDF v1.4, siehe Abschnitt 8.6.7.1, mit den Einschränkungen, dass eine Einbettung der Schriften sowie die Erfassung von Metadaten erfolgt und keine Kennwörter, ausführbarer Code oder Audio- und Videodaten verwendet werden.

Die Konformität zu ISO 19005-1:2005 kann mittels zwei unterschiedlicher Grade beschrieben werden:

1. PDF/A-1b (auch Level B Conformance genannt) bildet die minimale Konformität mit der Forderung, dass das generierte Erscheinungsbild der PDF-Datei langfristig reproduzierbar ist.
2. PDF/A-1a (auch Level A Conformance genannt) baut auf Level B auf und verlangt zusätzlich noch, dass die PDF-Datei durchsuchbar ist (Textextraktion). PDF/A-1a erfüllt komplett die Forderungen des ISO-Standards (full conformance).

Der Standard sollte zur Langzeitarchivierung von Texten und Präsentationen eingesetzt werden. Durch den von der ISO anerkannten Standard lassen sich Dokumentinhalt, Dokumentform und Metadaten zum Dokument in einer archivierten Datei erfassen. Die Anzeige der Datei ist auch ohne die Ursprungsanwendung möglich. Ebenso findet eine barrierefreie Darstellung von Inhalten statt.

Unter Beobachtung: Extensible Markup Language (XML) v1.1

Analog zu Abschnitt 8.6.6 „Austauschformate für Daten“ auf Seite 111.

384. siehe http://www.loc.gov/ead/
385. siehe http://jefferson.village.virginia.edu/eac/
386. siehe http://www.loc.gov/standards/mets/
387. siehe http://www.archisig.de/
388. siehe http://www.archisig.de/grundsaetze.pdf
389. eingesetzt wird ArchiSig z. B. im Rahmen des Projekts „ArchiSafe“, siehe http://www.archisafe.de/
390. siehe http://www.adobe.de/products/acrobat/pdfs/pdfarchiving.pdf
391. siehe http://www.iso.org/

Anhang A Literaturverzeichnis

[APEC]

National Office for the Information Economy / CSIRO: *APEC e-Business: What do Users need?*, 2002
http://nla.gov.au/nla.arc-25067
http://www1.cmis.csiro.au/Reports/APEC_E-commerce.pdf

[BOL]

Bundesministerium des Innern (Hrsg.): *BundOnline 2005: Umsetzungsplan 2004 – Status und Ausblick*, Dresden 2004
http://www.kbst.bund.de/ (im Bereich > E-Government > Initiativen > BundOnline 2005 > Umsetzungsplan und Abschlussbericht > 2004 - Umsetzungsplan)

[BSI 2005]

Bundesamt für Sicherheit in der Informationstechnik: *ITIL und Informationssicherheit – Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management*, Berlin, 2005
http://www.bsi.de/literat/studien/ITinf/itil.pdf

[e-GIF]

Office of the e-Envoy: *e-Government Interoperability Framework Version 6.0*, 2004
http://www.govtalk.gov.uk/schemasstandards/egif.asp
http://www.govtalk.gov.uk/documents/e-gif-v6-0(1).pdf
Office of the e_Envoy: *Technical Standards Catalogue Version 6.1*, 2004
http://www.govtalk.gov.uk/documents/TSCv6-1_2004-11-15.pdf

[FIPS-PUBS]

National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL): *Federal Information Processing Standards Publications,* 2005
http://www.itl.nist.gov/fipspubs/

[GDI-DE 2007]

Geodateninfrastruktur Deutschland: *Architektur der Geodateninfrastruktur Deutschland*, Konzept zur fach- und ebenenübergreifenden Bereitstellung von Geodaten im Rahmen des E-Government in Deutschland, Version 1.0, 2007
http://www.gdi-de.org/de/download/GDI_ArchitekturKonzept_V1.pdf

[IDABC]

European Commission: *Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*, 2005
http://europa.eu.int/idabc/

[IEEE 2000]

Institute of Electrical and Electronics Engineers (IEEE): *IEEE-Standard 1471-2000: Recommended Practice for Architectural Description of Software-Intensive Systems*, 2000

[ISO 1996]
ISO/IEC 10746-3: *Information technology – Open Distributed Processing – Reference Model: Architecture*, Genf 1996

[ITG 2000]
Informationstechnische Gesellschaft (ITG) im VDE: *Electronic Government als Schlüssel der Modernisierung von Staat und Verwaltung*. Ein Memorandum des Fachausschusses für Verwaltungsinformatik der Gesellschaft für Informatik e.V. (GI) und des Fachbereichs 1 der Informationstechnischen Gesellschaft (ITG) im Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE), Bonn / Frankfurt 2000
http://mediakomm.difu.de/documents/memorandum.pdf

[KBSt 2007]
KBSt: *IT-Architekturkonzept für die Bundesverwaltung*, 2007
http://www.kbst.bund.de/architekturkonzept

[Kudraß 1999]
Kudraß, Thomas: *Describing Architectures Using RM-ODP*, Online-Publikation, 1999
http://www.imn.htwk-leipzig.de/~kudrass/Publikationen/OOPSLA99.pdf

[Lenk et al. 2000]
Lenk, Klaus / Klee-Kruse, Gudrun: *Multifunktionale Serviceläden*, Berlin 2000

[Lenk 2001]
Lenk, Klaus: *Über Electronic Government hinaus Verwaltungspolitik mit neuen Konturen,* Vortrag auf der 4. Fachtagung Verwaltungsinformatik in der Fachhochschule des Bundes für öffentliche Verwaltung am 5. September 2001

[v. Lucke et al. 2000]
Lucke, Jörn von / Reinermann, Heinrich: *Speyerer Definition von Electronic Government*. Ergebnisse des Forschungsprojektes Regieren und Verwalten im Informationszeitalter, Online-Publikation, 2000
http://foev.dhv-speyer.de/ruvii/Sp-EGov.pdf

[Neuseeland]
State Services Commission, New Zealand: *E-government in New Zealand*, 2007
http://www.e-government.govt.nz/

[Schedler et al. 2001]
Schedler, Kuno / Proeller, Isabella: *NPM*, Bern / Stuttgart / Wien 2001

[Schreiber 2000]
Schreiber, Lutz: *Verwaltung going digit@l. Ausgewählte Rechtsfragen der Online-Verwaltung*, in: Digitale Signaturen, in: Kommunikation & Recht Beilage 2 zu Heft 10/2000

[Schweiz]
Schweizerische Bundeskanzlei: *Sektion elektronischer Behördenverkehr*, Homepage der Beratungs-, Dienstleistungs- und Betriebsorganisation für den elektronischen Behördenverkehr (E-Government), 2007
http://www.bk.admin.ch/org/bk/00346/00348/index.html?lang=de

[SIGA]
Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik (BSI): *Sichere Integration von E-Government-Anwendungen*, Modul des E-Government-Handbuch, 2003
http://www.bsi.bund.de/fachthem/egov/4_siga.htm

Anhang B Übersicht der klassifizierten Standards

Symbole

A

B

C

D

E

F

G

H

I

J

K

L

M

O

P

Q

R

S

T

U

W

X

Z

Anhang C Abkürzungsverzeichnis

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AG	Aktiengesellschaft
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
ArchiSig	Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente
BGG	Behindertengleichstellungsgesetz
BIT	Bundesstelle für Informationstechnik
BITV	Barrierefreie Informationstechnik-Verordnung
BMI	Bundesministerium des Innern
BMP	Windows Bitmap
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BOL	Initiative BundOnline 2005
BPEL4WS	Business Process Execution Language for Web Services
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CC VBPO	Kompetenzzentrum Vorgangsbearbeitung, Prozesse und Organisation
CEN	Comité Européen de Normalisation
CMS	Content Management System
CORBA	Common Object Request Broker Architecture
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CSS	Cascading Style Sheets Language
CSV	Character Separated Value
CSW	Web Catalogue Service
CTI	Computer Telephony Integration
DCMI	Dublin Core Metadata Initiative
DES	Data Encryption Standard
DIN	Deutsches Institut für Normung e. V.
DNS	Domain Name System

DOMEA	Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang
DRV	Deutsche Rentenversicherung Bund
DSA	Digital Signature Algorithm
DSML	Directory Services Markup Language
DSS	Digital Signature Standard
DV	Datenverarbeitung
DVDV	Deutsches Verwaltungsdiensteverzeichnis
ebXML	Electronic Business using XML
ECMA	European Computer Manufacturers Association
EfA	Einer für Alle
e-GIF	E-Government Interoperability Framework
EJB	Enterprise JavaBeans
EML	Election Markup Language
ER	Entity Relationship
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
FinTS	Financial Transaction Services
FIPS-PUBS	Federal Information Processing Standards Publications
FLAC	Free Lossless Audio Codec
FMS	Formular Management System
FTP	File Transfer Protocol
G2B	Government to Business
G2C	Government to Citizen
G2E	Government to Employee
G2G	Government to Government
GDI-DE	Geodateninfrastruktur Deutschland
GI	Gesellschaft für Informatik e.V.
GIF	Graphics Interchange Format
GML	Geography Markup Language
GSM	Global System for Mobile Communications
HTML	Hypertext Markup Language

HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
ISIS	Industrial Signature Interoperability Specification
ISIS-MTT	Industrial Signature Interoperability Specification - MailTrusT
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
ITG	Informationstechnische Gesellschaft im VDE
ITIL	IT Infrastructure Library
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IVBB	Informationsverbund Berlin-Bonn
IVBV	Informationsverbund der Bundesverwaltung
J2EE	Java 2 Platform, Enterprise Edition
JAAS	Java Authentication and Authorization Service
Java EE	Java Platform, Enterprise Edition
Java SE	Java Platform, Standard Edition
JAXP	Java API for XML Parsing
JCA	J2EE Connector Architecture
JDBC	Java Database Connectivity
JMS	Java Message Service
JMX	Java Management Extensions
JNDI	Java Naming and Directory Interface
JNLP	Java Network Launching Protocol

JPEG	Joint Photographic Experts Group
JRE	Java Runtime Environment
JSP	Java Server Pages
JSR	Java Specification Requests
JTA	Java Transaction API
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern
KoopA ADV	Kooperationsausschuss automatische Datenverarbeitung Bund / Länder / Kommunaler Bereich
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MIME	Multipurpose Internet Mail Extensions
MIT	Massachusetts Institute of Technology
MOF	Meta Object Facility
MPEG	Moving Picture Experts Group
MTT	MailTrusT
NAT	Network Address Translation
NISO	National Information Standards Organization
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
ODF	OpenDocument Format
OGC	Open Geospatial Consortium
OMG	Object Management Group
OOXML	Office Open XML
OSCI	Online Services Computer Interface
OSS	Open Source Software
PC	Personal Computer
PDA	Personal Digital Assistant
PDF	Portable Document Format
PDF/A	PDF Archive
PHP	PHP: Hypertext Preprocessor
PIN	Persönliche Identifikationsnummer

PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	IETF Working Group „Public-Key Infrastructure (X.509)“
PNG	Portable Network Graphics
POP	Post Office Protocol
PSE	Personal Security Environment
RDF	Resource Description Framework
Relax NG	Regular Language Description for XML New Generation
REL	Rights Expression Language
RFC	Request for Comments
RFP	Request for Proposals
RFID	Radio Frequency Identification
RIPE	RACE Integrity Primitives Evaluation
RIPEMD	RIPE (RACE Integrity Primitives Evaluation) Message Digest
RMI	Remote Method Invocation
RMI-IIOP	Remote Method Invocation over Internet Inter-ORB Protocol
RM-ODP	Reference Model of Open Distributed Processing
RSA	Rivest, Shamir, Adleman Public Key Encryption
SAGA	Standards und Architekturen für E-Government-Anwendungen
SAML	Security Assertion Markup Language
SC	Service Center
SFA	Simple Feature Access
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SIGA	Sichere Integration von E-Government-Anwendungen
SigG	Signaturgesetz
SigV	Signaturverordnung
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMIL	Synchronized Multimedia Integration Language
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service

SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TAN	Transaktionsnummer
TAR	Tape Archive
TCP/IP	Transmission Control Protocol / Internet Protocol
TESTA	Trans-European Services for Telematics between Administrations
TIFF	Tagged Image File Format
TLS	Transport Layer Security
TMS	Travel Management System
Triple-DES	Triple Data Encryption Standard
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP (IP-Telefonie)
V-PKI	Public Key Infrastruktur der Verwaltung (Verwaltungs-PKI)
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WCAG	Web Content Accessibility Guidelines
WCS	Web Coverage Service
WebDAV	WWW Distributed Authoring and Versioning
WFS	Web Feature Service

WML	Wireless Markup Language
WMS	Web Map Service
WMV	Windows Media Video
WS	Web Service
WS-BPEL	Web Services Business Process Execution Language
WSDL	Web Services Description Language
WS-I	Web Service Interoperability Organization
WS-Security	Web Services Security
WWW	World Wide Web
XAdES	XML Advanced Electronic Signatures
XHTML	Extensible Hypertext Markup Language
X-KISS	XML Key Information Service Specification
XKMS	XML Key Management Specification
X-KRSS	XML Key Registration Service Specification
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XÖV	XML-basierte fachliche Standards für den elektronischen Datenaustausch innerhalb und mit der öffentlichen Verwaltung
XSD	Extensible Markup Language Schema Definition
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformations