

SAGA

Standards und Architekturen für
eGovernment-Anwendungen

Version 1.1

Schriftenreihe der KBSt

Band 56

ISSN 0179 - 7263

Nachdruck, auch auszugsweise, ist genehmigungspflichtig

Dieser Band wurde erstellt von der KBSt im Bundesministerium des Innern in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der]init[AG, Booz Allen Hamilton und der Fraunhofer Gesellschaft.

Redaktion:]init[AG, Berlin

Ansprechpartner:

Bundesministerium des Innern

Referat IT2 (KBSt)

11014 Berlin

E-Mail: IT2@bmi.bund.de

Telefon: +49-1888/681-0

Fax: +49-1888/681-2782

Homepage und Download der digitalen Version: <http://www.kbst.bund.de/saga>

SAGA

**Standards und Architekturen für eGovernment-Anwendungen
Version 1.1**

Februar 2003

Herausgegeben vom
Bundesminister des Innern

Danksagung

Die KBSt und das Autoren-Team danken allen Mitgliedern des SAGA-Expertenkreises für ihre fachliche Unterstützung bei der Erstellung der vorliegenden Version von SAGA.

Der Dank gilt weiterhin allen Teilnehmerinnen und Teilnehmern am SAGA-Forum, die mit ihren engagierten Kommentaren einen maßgeblichen Beitrag zur Fortschreibung des Dokuments geleistet haben.

Vorbemerkung:

Dieses Dokument stellt in verdichteter Form verbreitete Standards, Verfahren, Methoden und auch Produkte der modernen IT-Entwicklung für eGovernment vor. Naturgemäß werden von den Experten auf diesem Gebiet sehr viele Abkürzungen und überwiegend englischsprachige Akronyme verwendet. Ein Teil dieser Namen sind urheberrechtlich bzw. 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 1.1 wurde am 12. Februar 2003 veröffentlicht; Kommentare, Ergänzungen, Berichtigungen werden erbeten an das Bundesministerium des Innern, Referat IT2 (KBSt) und über das Forum unter <http://www.kbst.bund.de/saga>.

Teilweise sind diskutierte Standards zwingend mit lizenzpflichtigen Produkten verbunden. Unsere Empfehlung ist rein technisch zu verstehen, ob und in welcher Form (Einzel-/Sammellizenz) ein Produkt wirtschaftlich einsetzbar ist, ist im Einzelfall zu prüfen.

Versionsnummern sind dort aufgeführt, wo sie im diskutierten Zusammenhang relevant sind; die Nichterwähnung impliziert aber keine Konformität. Wenn für Standards keine Versionsnummern angegeben sind, ist die aus Marktsicht stabilste Version zu verwenden, welche nicht immer die neueste Version ist.

Die Autoren gestatten die Weiterverwendung des Dokumentes – auch in Teilen – unter Angabe der Quelle.

Inhaltsverzeichnis

0	Änderungshistorie und Status	5
0.1	Änderungen gegenüber Version 0.9	5
0.2	Zukünftige Themenbereiche	5
1	Einleitung	7
1.1	Hintergrund	7
1.2	Angesprochener Leserkreis	7
1.3	Ziel und Aufbau des Dokumentes	8
1.4	Abzubildende Dienstleistungen	10
1.5	Erfolgsfaktoren für die Standardisierung	11
2	Die Evolution von SAGA	13
2.1	Aufgaben	13
2.2	Der Evolutionsprozess	14
3	Verbindlichkeit und Konformität der Anwendungen	16
3.1	Geltungsbereich und Verbindlichkeit von SAGA	16
3.2	Verantwortung für Konformität	17
3.3	Migration zur Konformität	18
3.4	Nicht-Konformität	18
4	Architekturbaukasten für eGovernment-Anwendungen	19
4.1	Ziele und Prinzipien des Baukastens	19
4.2	Modellierung von Fachanwendungen in den Sichten	20
5	Standards für die IT-Architektur	26
5.1	Client	26
5.2	Präsentation	29
5.3	Fachliche Prozess- und Datenmodelle	40
5.4	Datenintegration	42
5.5	Middleware Architektur	43
5.6	Kommunikation	45
5.7	Anbindung an das Backend	50
6	Standards für Datensicherheit	53
6.1	Ziele und Prinzipien der Datensicherheit	53
6.2	Sicherheitsstandards für die Ermittlung des Schutzbedarfs	57
6.3	Standards für bestimmte Anwendungsfälle	57

6.4	Übergreifende Datensicherheitsstandards	65
7	Basiskomponenten und Kompetenzzentren	69
7.1	Basiskomponenten	69
7.2	Kompetenzzentren	72
8	Anhang	74
8.1	Tabellarische Übersicht der Standards für die IT-Architektur	74
8.2	Tabellarische Übersicht der Standards für Datensicherheit	79
8.3	Glossar	81

Obligatorische Standards

Standards sind obligatorisch, wenn sie sich bewährt haben und sie die bevorzugte Lösung darstellen. Diese Standards sind verbindlich und damit vorrangig zu beachten und anzuwenden.

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

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

Barrierefreie Informationstechnik Verordnung BITV	29
Hypertext Markup Language (HTML)	30,32,33,34
ISO 10646-1:2000/Unicode v3.0 UTF-8	31
ECMA-262 – ECMAScript Language Specification	32
Text (.txt)	32
Portable Document Format (PDF) Version 4	33, 34
Multipurpose Internet Mail Extensions (MIME)	33
Comma Separated Value (CSV).....	33
Graphics Interchange Format (GIF)	34
Joint Photographic Experts Group (JPEG)	34
MPEG-1 Layer 3 (MP3)	36
Quicktime (.qt, .mov)	36, 37
HTTP	37, 49
Animated GIF	38
ZIP v2.0	38
Short Message Services (SMS)	38
Rollenmodelle und Flussdiagramme	41
Entity Relationship Diagramme	42
Extensible Markup Language Schema Definition (XSD) v1.0.....	42, 43, 47
Extensible Markup Language (XML)	42
J2EE v1.3	44
J2SE	44
JAAS v1.0.....	44
JDBC v2.0	44

JAXP v1.1.....	44
JMS, J2EE Connector Architecture	45
JNDI v1.1.2.....	45
Remote Method Invocation (RMI).....	46
Web Services Description Language (WSDL) v1.1	47
SOAP v1.1	47
IP v4	48
DNS	48
File Transfer Protocol (FTP).....	48
SMTP/MIME	49
POP3/IMAP	49
LDAP v3	49
BSI, IT-Grundschutzhandbuch	57
SSL/TLS	58
MTT Version 2/SPHINX/PKI-1-Verwaltung.....	60, 61
ISIS-MTT	60, 62, 66
OSCI-Transport v1.2	63
ISO/IEC 7816	66
Kryptoalgorithmen nach RegTP für die elektronische Signatur	67
Triple-DES	68
IDEA	68
Basiskomponente Zahlungsverkehrsplattform („ePayment“).....	69
Basiskomponente Portal www.bund.de	70
Basiskomponente Formularserver.....	71

Empfohlene Standards

Standards werden empfohlen, wenn sie sich bewährt haben, sie aber entweder nicht zwingend erforderlich sind bzw. nicht die bevorzugte Lösung darstellen oder eine Einstufung als obligatorisch noch weiterer Abstimmung bedarf. Wenn es neben empfohlenen Standards keine konkurrierenden obligatorischen Standards gibt, so darf von den empfohlenen Standards nur in begründeten Ausnahmen abgewichen werden.

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

Wenn empfohlene und unter Beobachtung stehende Standards nebeneinander existieren, so sollen die letztgenannten nur in begründeten Ausnahmen angewandt werden.

Hypertext Markup Language (HTML) v4.01	30
Cascading Style Sheets Language Level 2 (CSS2)	31
Extensible Stylesheet Language (XSL) v1.0	31
ISO 10646-1:2000/Unicode v3.0 UTF-16	31
ISO 8859-1	31
ISO 8859-15	31
Servlets und Java Server Pages oder XSL	32
Extensible Markup Language (XML)	33, 51
Portable Network Graphics (PNG).....	35
Tagged Image File Format (TIFF)	35
Enhanced Compressed Wavelet (ECW)	35
GZIP v4.3	38
Unified Modeling Language (UML)	41
Extensible Stylesheet Language Transformation (XSLT) v1.0	43
RMI-IIOP	46
J2EE Connectors, Java Message Service.....	51
Web Services	52
UN/EDIFACT	52
KoopA, Handlungsleitfaden für die Einführung der elektronischen Signatur und der Verschlüsselung in der Verwaltung.....	57
BSI, E-Government-Handbuch.....	57
XML Signature	62
XML Encryption	63
Basiskomponente Datensicherheit („Virtuelle Poststelle“)	70
Basiskomponente Content Management System.....	71

Standards unter Beobachtung

Standards stehen unter Beobachtung, wenn sie der gewünschten Entwicklungsrichtung folgen, aber noch nicht ausgereift sind oder sie sich noch nicht ausreichend am Markt bewährt haben. Wenn es neben unter Beobachtung stehenden Standards kei-

ne konkurrierenden obligatorischen oder empfohlenen Standards gibt, so können unter Beobachtung stehende Standards eine Orientierungshilfe geben.

Extensible Hypertext Markup Language (XHTML) v1.0.....	30
Portable Document Format (PDF) Version 5.....	33, 34
Geography Markup Language (GML).....	35
Scalable Vector Graphic (SVG).....	36
Vector Markup Language (VML)	36
Ogg	37
WML v1.x	39
WAP v1.x	39
XHTML Basic	39
Unified Modeling Language (UML).....	42
Microsoft Windows .NET Framework	45
UDDI	47, 49
IP v6	48
DSML v2	50
WS-Security	64
Basiskomponente Call Center	72

0 Änderungshistorie und Status

Das vorliegende Dokument in der Version 1.1 ist die erste freigegebene Veröffentlichung von SAGA (Standards und Architekturen für eGovernment-Anwendungen) und hat verbindlichen Charakter.

0.1 Änderungen gegenüber Version 0.9

Dieses Dokument basiert auf der bereits veröffentlichten Version SAGA 0.9, die intensiv mit Experten aus Bund, Ländern, Kommunen und der Wirtschaft diskutiert worden ist. Über 150 Kommentare wurden bearbeitet, von denen ca. 95 in Änderungen des Dokumentes resultierten.

Die Änderungen beziehen sich hauptsächlich auf die

- a. klarere Darstellung von Standards zur verbesserten Lesbarkeit und Handhabbarkeit
- b. Überarbeitung des Architekturbaukasten unter Verwendung von RM-ODP (Zerlegung von Anwendungen in Sichten)
- c. Überarbeitung der Kapitel Präsentation, Middleware, Kommunikation und Datensicherheit

Im Bereich der Client-Technologie wurden mit Einschränkungen auch aktive Inhalte, wie Javascript und Plug-Ins, sowie der Einsatz von Cookies zugelassen.

Ein Kapitel über Basiskomponenten und Kompetenzzentren wurde eingefügt. Die Basiskomponenten sind Kernbestandteile der eGovernment-Architektur von BundOnline 2005. Ihre Einsatzgebiete zur Realisierung von eGovernment-Anwendungen werden von SAGA festgelegt.

0.2 Zukünftige Themenbereiche

SAGA wird in regelmäßigen Abständen fortgeschrieben, neuesten Entwicklungen und Erkenntnissen angepasst und unter der Adresse <http://www.kbst.bund.de/saga> sowie im E-Government-Handbuch unter <http://www.e-government-handbuch.de> publiziert.

Folgende Themengebiete sollen weiter untersucht und detailliert werden:

- a. Weitere Zugriffskanäle wie digitales Fernsehen, Spielkonsolen etc.
- b. Methoden, Verfahren und Werkzeuge (inklusive Tests der Konformität zu SAGA)
- c. Fachliche Prozess- und Datenmodelle
- d. Basiskomponenten und deren Anbindung an das Backend
- e. Einarbeiten der ersten praktischen Erfahrungen mit der Anwendung von SAGA

Insbesondere das Kapitel Basiskomponenten wird zur nächsten Version umfangreiche Erweiterungen erfahren. Dies ergibt sich aus dem Projektfortschritt der einzelnen Basiskomponenten und den detaillierteren Anforderungen an diese.

1 Einleitung

1.1 Hintergrund

Mit den Standards und Architekturen für eGovernment-Anwendungen (SAGA) erbringt die Bundesregierung eine weitere wichtige Voraussetzung für eine moderne und dienstleistungsorientierte Verwaltung.

Bundeskanzler Gerhard Schröder hat im September 2000 die eGovernment-Initiative BundOnline 2005 gestartet und die Bundesverwaltung verpflichtet, ihre über 350 internetfähigen Dienstleistungen bis zum Jahr 2005 online bereit zu stellen. Die Bundesbehörden haben mit der Umsetzung begonnen. Seit Ende 2002 werden bereits mehr als 160 Dienstleistungen der Verwaltung online angeboten.

Unter Koordination des Bundesministeriums des Innern (BMI) wurden ein Umsetzungsplan erstellt und Basiskomponenten definiert. Diese Basiskomponenten sowie Anwendungen, die nach dem Prinzip „Einer für alle“ entwickelt wurden, und die in den nächsten Jahren neu zu schaffenden eGovernment-Anwendungen sollen nahtlos miteinander kommunizieren können. Dem Benutzer soll eine einheitliche Bedienlogik („look and feel“) zur Verfügung gestellt werden. Nach der Erstellung des Umsetzungsplanes richtete das Bundesministerium des Innern eine Projektgruppe ein, die diesen Umsetzungsplan technisch konkretisiert.

Unter Einbindung von acht Industrieexperten sowie weiteren sechs Experten aus Bundes-, Länder- und Kommunalverwaltung erfolgte zunächst eine Bestandsaufnahme existierender Standards.

Auf dieser Basis entstand der nachfolgende Vorschlag für Standards und Architekturen für eGovernment-Anwendungen (SAGA).

Der Beschluss der Bundesregierung zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung vom 16. Januar 2002 wurde ebenso wie die "Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik Verordnung BITV)" berücksichtigt.

1.2 Angesprochener Leserkreis

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

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

Die definierten Standards und Architekturen sollen kostenintensive Doppelentwicklungen innerhalb der öffentlichen Verwaltung vermeiden und Synergien, die durch das Internet möglich werden, offensiv nutzen. Der Bund sieht seine Initiative auch als seinen Beitrag zur Entwicklung von eGovernment in Deutschland. Hier gesammelte Erfahrungen und die im Rahmen von BundOnline 2005 entwickelten Basiskomponenten sollen allen Anwendern die Orientierung in der Verwaltung erleichtern und flächendeckende eGovernment-Angebote fördern.

1.3 Ziel und Aufbau des Dokumentes

1.3.1 Grundprinzipien

Modernes eGovernment erfordert interoperable Informations- und Kommunikationssysteme, die (idealerweise) reibungslos zusammenwirken. Durch einfache und klare Standards und Spezifikationen kann die Interoperabilität von Informations- und Kommunikationssystemen erreicht werden. SAGA identifiziert erforderliche Standards, Formate und Spezifikationen, legt dafür Konformitätsregeln fest und schreibt diese entsprechend den technologischen Entwicklungen fort.

eGovernment-Anwendungen werden nach folgenden Grundprinzipien entwickelt:

- a. eGovernment-Anwendungen nutzen als Frontend primär den 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 Internet-Seiten zu ermöglichen, oder verwenden zumindest nur signierte und qualitätsgesicherte Anwendungen gemäß Kapitel 5.2.
- c. eGovernment-Anwendungen legen keine Programmteile und Daten auf den Computern der Anwender ab, die sich deren Kontrolle entziehen.

1.3.2 Zielsetzung

SAGA verfolgt das Ziel

- a. stetige Informationsflüsse zwischen Bürgern, dem Bund und Partnern des Bundes zu gewährleisten (Interoperabilität),
- b. ähnliche Vorgehensweisen bei der Bereitstellung von Dienstleistungen und bei der Definition von Datenmodellen zu etablieren (Wiederverwendbarkeit). Ländern und Kommunen wird angeboten, Entwicklungsergebnisse der Initiative Bund-Online 2005 zu verwenden.

- c. auf Spezifikationen in Form öffentlich zugänglicher Dokumentationen zurückgreifen zu können (Offenheit),
- d. Entwicklungen am Markt und im Bereich der Standardisierung zu berücksichtigen (Reduktion von Kosten und Risiken),
- e. die Anwendbarkeit der Lösungen bei sich ändernden Anforderungen hinsichtlich Volumen und Transaktionshäufigkeit sicherzustellen (Skalierbarkeit).

1.3.3 Umfang

SAGA versteht sich als Standardisierung mit einem ganzheitlichen Ansatz, der alle erforderlichen Aspekte erläutert, um die genannten Ziele zu erreichen. Nicht aufgeführte Standards oder Architekturen sind

- a. nicht spezifisch für eGovernment- oder eCommerce-Anwendungen,
- b. bezogen auf eine andere Detailebene 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,
- e. nicht gewünscht, weil sie mit vorgestellten Standards oder Architekturen konkurrieren oder die Interoperabilität einschränken.

Des Weiteren betrachtet SAGA nicht alle Elemente einer technischen Architektur, sondern nur Bereiche, die wesentlichen Einfluss auf die genannten Ziele haben (siehe Kapitel 4).

Das Dokument beschreibt Standards im Wesentlichen in zwei Teilen:

- a. Die Kapitel 4 – 6 beschreiben den Architekturbaukasten und seine Elemente.
- b. Kapitel 7 beschreibt Standards für die im Rahmen von BundOnline 2005 definierten Basiskomponenten.

1.4 Abzubildende Dienstleistungen

Das Dokument definiert drei Zielgruppen, an die sich die Dienstleistungen der Bundesverwaltung (siehe eine Auswahl in Abbildung 1-1) richten:

- Government to Citizens: Dienstleistungen, die der Bund Bürgern direkt anbietet,
- Government to Business: Dienstleistungen, die der Bund Unternehmen anbietet,
- Government to Government: Dienstleistungen des Bundes für die Verwaltung.

Über 350 Dienstleistungen der verschiedenen Verwaltungen des Bundes wurden identifiziert. Durch die Betrachtung der Dienstleistungen entlang der Wertschöpfungskette konnten acht Dienstleistungstypen (siehe www.bundonline2005.de) abgeleitet werden. Bereits 73 Prozent der heute nachgefragten Dienstleistungen lassen sich den folgenden drei Typen zuordnen:

- Erfassen, Aufbereiten und Bereitstellen von Informationen,
- Bearbeiten von Anträgen, die an die Verwaltung gerichtet werden,
- Abwickeln von Förderungen.

G2C Government to Citizens	G2B Government to Business	G2G Government to Government
<ul style="list-style-type: none">• BA: Vermittlung von Arbeitsplätzen• BA: Gewährung von Geldleistungen• BfA: Berechnung und Gewährung von Renten• BMA: Bereitstellung von Informationen• BA: Durchführung von Beratungen• BfA: Durchführung von Beratungen• DWD: Durchführung von meteorologischen Vorhersagen und Beratungen• BfA: Einzug von Rentenversicherungsbeiträgen• BEV: Erstattung von Kosten im Rahmen der Krankenversorgung und Pflegeversicherung der Beamten• BZgA: Bereitstellung von Fachinformationen (zur gesundheitlichen Aufklärung)• BpB: Bereitstellung von Informationen und Abwicklung von Bestellungen• BAFA: Förderung erneuerbarer Energien	<ul style="list-style-type: none">• BA: Vermittlung von Arbeitsplätzen• KBA: Führen zentraler Verkehrs- und Kfz-Register• BeschA: Durchführung von Beschaffungen• BBR: Durchführung von Beschaffungen im Baubereich• BZV: Zollbehandlungen Aus- und Einfuhr• StBA: Durchführung zentraler Statistiken• BMBF: Vergabe von projektbezogenen Förderungen• BMWi: Abwicklung von Förderprogrammen• BaKred: Informationsangebot zu bankenaufsichtlich relevanten Themen• BfF: Vergabe der Umsatzsteuer-identifikationsnummer• EBA: Vergabeverfahren nach VOL/A, VOB/A, VOF• RegTP: Vergabe von Rufnummern• BA: Bereitstellung von Informationen	<ul style="list-style-type: none">• BeschA: Beschaffungen• BfF: Zentrale Kassenführung des Bundes• BBR: Durchführung von Beschaffungen im Baubereich• BMF: Bewirtschaftung der Immobilien des Bundes• BAKöV: Buchungen in der Fortbildung• StBA: Durchführung zentraler Statistiken• BZR: Führen des Bundeszentralregisters• BZR: Erteilung von Auskünften aus dem Gewerbezentralregister

Abbildung 1-1: Ausgewählte Dienstleistungen des Bundes

1.5 Erfolgsfaktoren für die Standardisierung

Standards und Architekturen für eGovernment werden bereits seit einigen Jahren in Deutschland und in anderen Ländern erprobt¹. Die hier gewonnenen Erfahrungen und der internationale Austausch tragen dazu bei, die Definition und Umsetzung von SAGA zu erleichtern. Allgemein akzeptierte Faktoren für den Erfolg von eGovernment sind:

Gesetzliche Rahmenbedingungen

Die gesetzlichen Rahmenbedingungen müssen eine komfortable und effiziente Abbildung von Dienstleistungen im Internet ermöglichen.

So ist zum Beispiel die begrenzte elektronische Speicherung von Kundendaten (Bürger, Unternehmen oder Behörden) erforderlich, um Nutzern eine sinnvolle Bedienung zu ermöglichen und um mehr als Informationsdienstleistungen erbringen zu können.

Wünsche der Kunden

Der Nutzen von eGovernment hängt im Wesentlichen von der Kundenakzeptanz der angebotenen Dienstleistungen ab. Wünsche von Bürgern, Unternehmen und Behörden müssen kontinuierlich abgefragt werden. Das Dienstleistungsportfolio und der Prozess zur Erbringung der Leistung müssen sich diesen Anforderungen anpassen.

Prozessdefinitionen und Metadaten

Eine einheitliche Prozess- und Datendefinition ist Voraussetzung für die Vereinheitlichung von Technik, Anwendungen und Schnittstellen.

Schulungen

Die Verwendung und Pflege von Standards bedeutet einen kontinuierlichen Informationsaustausch und Schulungsprozess. Über das BMI bzw. die Projektgruppe Bund-Online 2005 werden entsprechende Aktivitäten organisiert.

¹ Siehe entsprechende Dokumente Großbritanniens (eGIF: eGovernment Interoperability Framework), der Vereinigten Staaten von Amerika (GOSIP: Open System Interconnection Profile), Australiens (APEC e-Business: What do Users need?) und Europas (IDA: Interchange of Data between Administrations)

Einbindung von Partnern und Outsourcing

Durch enge Kooperation mit Partnern und durch Outsourcing von Aktivitäten, die keine Hoheitsaufgabe darstellen, können Kosten gespart und die Effizienz von eGovernment-Leistungen erhöht werden.

2 Die Evolution von SAGA

2.1 Aufgaben

SAGA ist ein umfassender Standardisierungsansatz für die Initiative BundOnline 2005, der sich auf vier Entwicklungsrichtungen (Aufgaben) konzentriert:

- a. Festlegung der technischen Normen, Standards und Architekturen,
- b. Prozessmodellierung,
- c. Datenmodellierung sowie
- d. Entwicklung von Basiskomponenten.

Festlegung der technischen Normen, Standards und Architekturen

Die technischen Standards und Architekturen umfassen alle für das eGovernment relevanten Ebenen und Komponenten (siehe Kapitel 4). Sie sind die Grundlage für die Interoperabilität und Kompatibilität bei der Entwicklung der eGovernment-Anwendungen und der Basiskomponenten der Initiative BundOnline 2005.

Prozessmodellierung

Prozessmodellierung umfasst die methodische Beschreibung der eGovernment-Prozesse im Ganzen oder in Teilschritten (siehe Kapitel 5.3), um

- a. die verschiedenen Fachanwendungen ähnlich zu gestalten,
- b. die Wiederverwendbarkeit von Prozessen und Systemen zu einem hohen Grad zu gewährleisten.

Datenmodellierung

Datenmodellierung umfasst die methodisch standardisierte Beschreibung der Daten, die in den eGovernment-Prozessen (-Anwendungen) kommuniziert werden, im Ganzen oder in Teilen (siehe Kapitel 5.3), um

- a. die Interoperabilität von verschiedenen, auch von zukünftigen Anwendungen sicherzustellen,
- b. die Wiederverwendbarkeit von Prozessen und Systemen zu einem hohen Grad zu gewährleisten.

Entwicklung von Basiskomponenten

Basiskomponenten werden auf Grundlage von oft verwendeten, übergreifenden Prozessmodellen von BundOnline 2005 ausgewählt, spezifiziert und umgesetzt. Bereits sechs Basiskomponenten befinden sich in der Umsetzungsphase (siehe Kapitel 7).

2.2 Der Evolutionsprozess

Das Bundesministerium des Innern schlägt die Standards und Architekturen vor, die übergreifend für das eGovernment des Bundes gelten sollen. Dieser Vorschlag geht aus den Hinweisen und Anmerkungen aus den Foren zu SAGA, der Bewertung durch die Expertenkommission und der schlussendlichen Formulierung durch die Autoren hervor. Das Bundesministerium stellt im Weiteren die Abstimmung mit den Bundesressorts sicher.

Die Prozess- und Datenmodellierung erfolgt aus den einzelnen eGovernment-Projekten der Behörden heraus. Prozessmodelle von übergreifender Bedeutung werden durch das für Prozesse und Organisation zuständige Kompetenzzentrum beim Bundesverwaltungsamt (BVA) standardisiert. Die Standardisierung der Datenmodelle soll durch eine noch näher zu bestimmende Leitstelle geschehen. Das Bundesministerium des Innern koordiniert die Entwicklung.

Über die Entwicklung von Basiskomponenten entscheidet das Bundesministerium des Innern in Abstimmung mit den Bundesressorts.

SAGA wird in regelmäßigen Abständen fortgeschrieben, neuesten Entwicklungen und Erkenntnissen angepasst und unter der Adresse <http://www.kbst.bund.de/saga> sowie im E-Government-Handbuch unter <http://www.e-government-handbuch.de> publiziert.

2.2.1 Öffentliches Diskussionsforum

In einem öffentlich zugänglichen Forum (<http://foren.kbst.bund.de>) können sich Internet-Nutzerinnen und Internet-Nutzer registrieren und zu Themen von SAGA diskutieren.

2.2.2 Aufforderung zu Kommentaren, Request for Comments (RFC)

Zeitgleich zur Publikation von neuen Dokumenten oder von neuen Dokumentversionen sind alle Interessierten aufgefordert, die aktuellen Inhalte zu kommentieren. Auf der SAGA-Homepage (<http://www.kbst.bund.de/saga>) wird dafür ein Kontaktformular bereitgestellt. Übermittelte Kommentare werden in der nächsten Version des entsprechenden Dokumentes berücksichtigt.

2.2.3 Expertenkreis

Das Bundesministerium des Innern richtet einen Expertenkreis mit Vertretern aus Industrie und Behörden ein und beruft deren Mitglieder. In regelmäßigen Abständen oder bei begründeten Anlässen wird die Expertenrunde in die Fortschreibung einbezogen.

2.2.4 Aufforderung zu Vorschlägen, Request for Proposals (RFP)

Wenn Problemstellungen auftreten, die durch bekannte Techniken nicht gelöst werden können, werden Aufforderungen zu Vorschlägen (RFP – Request for Proposals) an den autorisierten Expertenkreis versandt, um Lösungsmöglichkeiten zu eruieren. Die Vorschläge werden unter <http://foren.kbst.bund.de> in einem geschlossenen Forum eingestellt und diskutiert.

3 Verbindlichkeit und Konformität der Anwendungen

3.1 Geltungsbereich und Verbindlichkeit von SAGA

SAGA beschreibt die empfohlenen technischen Rahmenbedingungen für die Entwicklung, Kommunikation und Interaktion von IT-Systemen der Bundesbehörden. Die Konformität mit SAGA ist grundsätzlich verbindlich für alle Prozesse und Systeme, die eGovernment-Dienstleistungen des Bundes erbringen. Für Systeme, die keine direkten Schnittstellen zum eGovernment haben, wird eine Migration empfohlen, wenn die Kosten-Nutzen-Betrachtung positiv ausfällt. Bei der Beschaffung von Standard-Software² sollten vorrangig Produkte oder Produktversionen gewählt werden, die zu der in SAGA empfohlenen Architektur kompatibel sind.

Die Bundesministerien regeln die Verbindlichkeit von SAGA in ihren Geschäftsbereichen.

3.1.1 Klassifizierung von Standards

Standards werden in drei Klassen eingeordnet. Konkurrierende Standards, die nicht aufgeführt sind, sollen nicht oder nur in zwingenden Ausnahmen angewandt werden.

Obligatorisch:

Standards sind obligatorisch, wenn sie sich bewährt haben und sie die bevorzugte Lösung darstellen. Diese Standards sind verbindlich und damit vorrangig zu beachten und anzuwenden.

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

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

Empfohlen:

Standards werden empfohlen, wenn sie sich bewährt haben, sie aber entweder nicht zwingend erforderlich sind bzw. nicht die bevorzugte Lösung darstellen oder eine Einstufung als obligatorisch noch weiterer Abstimmung bedarf. Wenn es neben emp-

² Software, die lediglich installiert und konfiguriert wird

fohlenen Standards keine konkurrierenden obligatorischen Standards gibt, so darf von den empfohlenen Standards nur in begründeten Ausnahmen abgewichen werden.

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

Wenn empfohlene und unter Beobachtung stehende Standards nebeneinander existieren, so sollen die letztgenannten nur in begründeten Ausnahmen angewandt werden.

Unter Beobachtung:

Standards stehen unter Beobachtung, wenn sie der gewünschten Entwicklungsrichtung folgen, sie aber noch nicht ausgereift sind oder sie sich noch nicht ausreichend am Markt bewährt haben. Wenn es neben unter Beobachtung stehenden Standards keine konkurrierenden obligatorischen oder empfohlenen Standards gibt, so können unter Beobachtung stehende Standards eine Orientierungshilfe geben.

3.1.2 Definition der Konformität

Die Konformität eines IT-Systems zu SAGA ist erreicht, wenn

- a. die beschriebenen technischen Standards und Architekturen eingehalten werden,
- b. Prozessmodelle, die bereits standardisiert sind, angewandt werden,
- c. Datenmodelle, die bereits standardisiert sind, berücksichtigt werden und
- d. auf vorhandenen Basiskomponenten aufgesetzt wird.

3.2 Verantwortung für Konformität

Die Verantwortung für die Konformität von eGovernment-Anwendungen zu SAGA liegt bei der für einen Prozess oder ein System fachlich zuständigen Behörde. Es obliegt auch den jeweiligen Behörden zu überprüfen, wie Fachanwendungen migriert werden können.

Die Bundesministerien regeln die Verantwortlichkeit in ihren Geschäftsbereichen.

Die Bereitstellung von Konformitätstests ist Teil der zukünftigen Entwicklung von SAGA (siehe Kapitel 0.2).

3.3 Migration zur Konformität

3.3.1 Übergangsphase

SAGA ist relativ neu und wird kontinuierlich weiterentwickelt und neuen Anforderungen angepasst. Deshalb können einzelne Prozesse und Systeme vorübergehend nicht zu SAGA konform sein.

Für nicht konforme Prozesse und Systeme sollen Migrationspläne entwickelt werden, wenn eine Kosten-Nutzen-Betrachtung positiv ausfällt. Dies kann erst bei einer wesentlichen Fortschreibung oder Erneuerung der Fall sein.

Ein pragmatisches Vorgehen wird empfohlen, um die Konformität zu SAGA zu gewährleisten.

3.3.2 Maßnahmen zur Erzielung von Konformität

Die Konformität zu SAGA wird durch folgende Maßnahmen gefördert:

- a. SAGA wird frühzeitig in Projektplanungen einbezogen.
- b. Die Konformität zu SAGA wird bei der Genehmigung von Projekten gefordert und überprüft.
- c. Bei Förderung, insbesondere aus Mitteln für die Initiative BundOnline 2005, wird die Konformität zu SAGA verbindlich gefordert.
- d. SAGA wird bei der Vergabe von Aufträgen verbindlich gefordert.

3.4 Nicht-Konformität

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

- a. Die Nutzung von Basiskomponenten kann eingeschränkt sein.
- b. Die Beratung durch Kompetenzzentren ist eingeschränkt oder nicht möglich.
- c. Schnittstellen zu diesem System können nicht bedient werden.
- d. Eine Förderung, insbesondere aus Mitteln für die Initiative BundOnline 2005, ist in der Regel nicht möglich.
- e. Das System kann ggf. nicht in das Dienstleistungsportal www.bund.de integriert werden.

4 Architekturbaukasten für eGovernment-Anwendungen

4.1 Ziele und Prinzipien des Baukastens

Mit dem Modell eines Architekturbaukastens verbindet SAGA folgende Ziele:

- a. Zur Erleichterung der Kommunikation soll ein gemeinsames Verständnis aktueller IT-Architekturen und -Technologien und eGovernment-Strukturen erreicht werden.
- b. Für eGovernment verfügbare IT-Technologien sollen mit diesem Modell erfasst, verglichen, nach Relevanz bewertet und einheitlich strukturiert werden.
- c. Bei der Realisierung von eGovernment-Projekten soll auf Standards zurückgegriffen werden können.

Um komplexe, verteilte eGovernment-Anwendungen zu beschreiben, ist eine Betrachtung der Anwendung unter verschiedenen Sichtweisen sinnvoll. Die Zerlegung in Sichten reduziert die Komplexität der einzelnen Sichten.

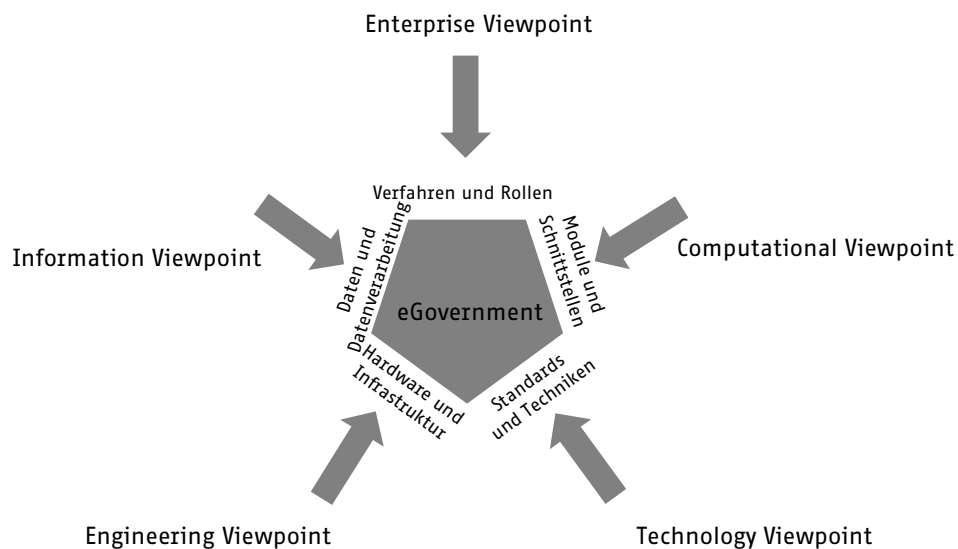


Abbildung 4-1: Viewpoints gemäß RM ODP

Der Architekturbaukasten stellt daher die Grundstruktur von eGovernment-Anwendungen in den unterschiedlichen Sichten dar und gibt Modelle, Standards und Technologien an die Hand, um die Anwendungen zu modellieren und realisieren.

Das Referenzmodell für offene verteilte Datenverarbeitung (RM ODP³) schlägt fünf Sichtweisen auf ein System vor, die für SAGA übernommen werden:

- Der Enterprise Viewpoint spezifiziert Zielsetzung, Anwendungsbereich, Verfahren und Regeln einer Anwendung.
- Der Information Viewpoint beschreibt die Ausprägung und Semantik der verarbeiteten Daten, sowie die detaillierten Prozesse zur Datenverarbeitung.
- Der Computational Viewpoint stellt die Zerlegung einer Anwendung in funktionale Module und deren Interaktionsschnittstellen dar.
- Der Engineering Viewpoint stellt die Verteilung der einzelnen Elemente des Systems auf physikalische Ressourcen sowie deren Verbindung dar.
- 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.

4.2 Modellierung von Fachanwendungen in den Sichten

Der Enterprise Viewpoint für eGovernment-Anwendungen beinhaltet zwei grundlegende Elemente: die organisatorische Struktur von eGovernment allgemein und die organisatorischen Modelle der Anwendung.

³ ITU-T Rec. X.903 ISO/IEC 10746-3: Reference Model of Open Distributed Processing

4.2.1 Grundlagen eGovernment

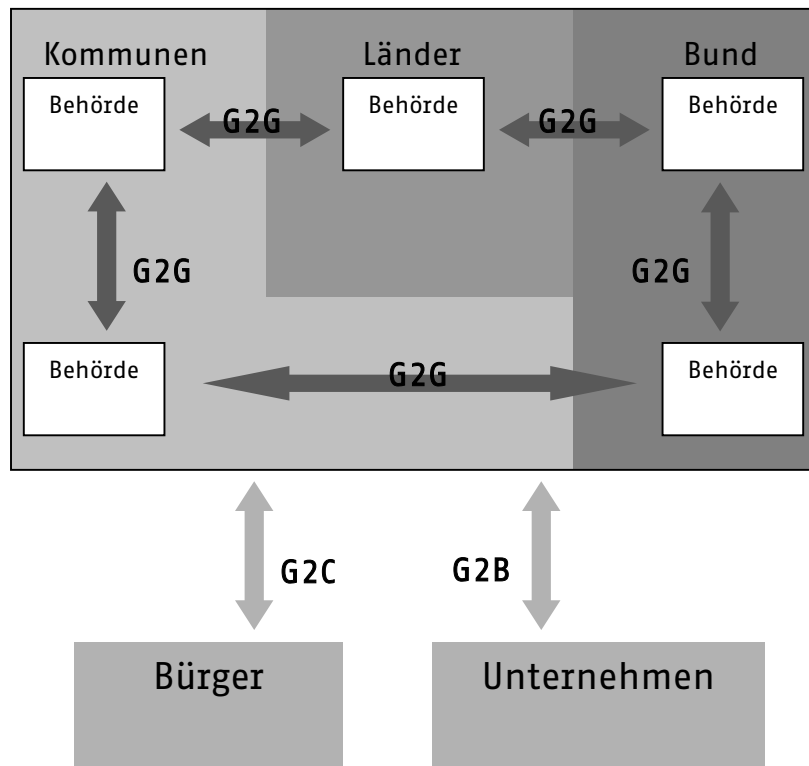


Abbildung 4-2: eGovernment-Interaktionen im Überblick

eGovernment-Interaktionen lassen sich in drei Kategorien teilen (siehe auch Abbildung 4-2):

1. Behörden interagieren untereinander, um Prozesse zu realisieren. Dies wird als Government-to-Government-Interaktion (G2G) bezeichnet.
2. Die Interaktion von Bürgern mit Behörden wird als Government-to-Citizen (G2C) bezeichnet.
3. Die Schnittstelle von Unternehmen zu Behörden sind Government-to-Business-Interaktionen (G2B).

Der Architekturbaukasten ist für alle drei Schnittstellen gültig. Derzeit nicht Gegenstand ist die interne Bedienung der Verfahren durch die Mitarbeiter der Behörden:

4. Die Bedienung der Anwendung innerhalb einer Verwaltung ist Teil der Government-to-Employee-Interaktion (G2E).

SAGA unterscheidet für jede Interaktionsschnittstelle drei wesentliche Kommunikationsszenarien nach ihrer Stellung in der Wertschöpfungskette (siehe auch E-Government-Handbuch):

- a. *Information*: Informationen werden zur Verfügung gestellt und bei Bedarf abgerufen.
- b. *Kommunikation/Interaktion*: bilaterale Kommunikation für einfache allgemeine Geschäftsvorfälle, z.B. Beratung oder Zusammenarbeit.
- c. *Transaktion/Integration*: komplexe, fachbezogene Geschäftsvorfälle mit einer mehrstufigen Wertschöpfungskette zwischen beteiligten Kommunikationspartnern, deren Zielsetzung die Ausführung einer individuellen Dienstleistung ist, z.B. Antragsverfahren, Beschaffungsvorhaben und Aufsichtsmaßnahmen. Transaktionen können sowohl online als auch offline ausgeführt werden.

4.2.2 Enterprise Viewpoint (Unternehmens- und Organisationsspezifische Sicht)

Hier wird die Gesamtumgebung für das System und sein Zweck beschrieben. Außerdem werden die Anforderungen (requirements) an das System, zu erfüllende Bedingungen (constraints), ausführbare Aktionen (actions) und DV-Zielvorgaben (policies) aus Sicht der Organisation oder des Unternehmens definiert. Dabei werden die Verfahren, deren Regeln, und die an den Verfahren beteiligten Akteure in ihren Rollen definiert.

SAGA stellt in Kapitel 5.3 die notwendigen Beschreibungsmittel und Vorgehensmodelle zur Definition des Enterprise Viewpoint zur Verfügung.

4.2.3 Information Viewpoint (Sicht auf die Informationen und Informationsverarbeitung)

Dieser Viewpoint legt die Struktur und Semantik der Informationen des Systems fest. Weitere Punkte sind die Definition von Quellen und Senken von Information sowie die Verarbeitung und Transformation von Information durch das System. Hierzu gibt es Integritätsregeln und Invarianten. Zur Definition der Datenmodelle stellt SAGA in Kapitel 5.3 die notwendigen Mittel bereit. Die Interoperabilität der Fachanwendungen und Integrierbarkeit werden durch die in Kapitel 7 beschriebenen Basiskomponenten sichergestellt. Diese Basiskomponenten definieren die zu verwendenden Datenmodelle und stellen eine gemeinsame Datenbasis bereit.

4.2.4 Computational Viewpoint (Sicht auf strukturelle und modulare Aufteilung des Systems)

Hier wird ein System in logische, funktionale Komponenten zerlegt, die für die Verteilung geeignet sind. Das Ergebnis sind Objekte, die Schnittstellen besitzen, an denen sie Dienste anbieten bzw. nutzen.

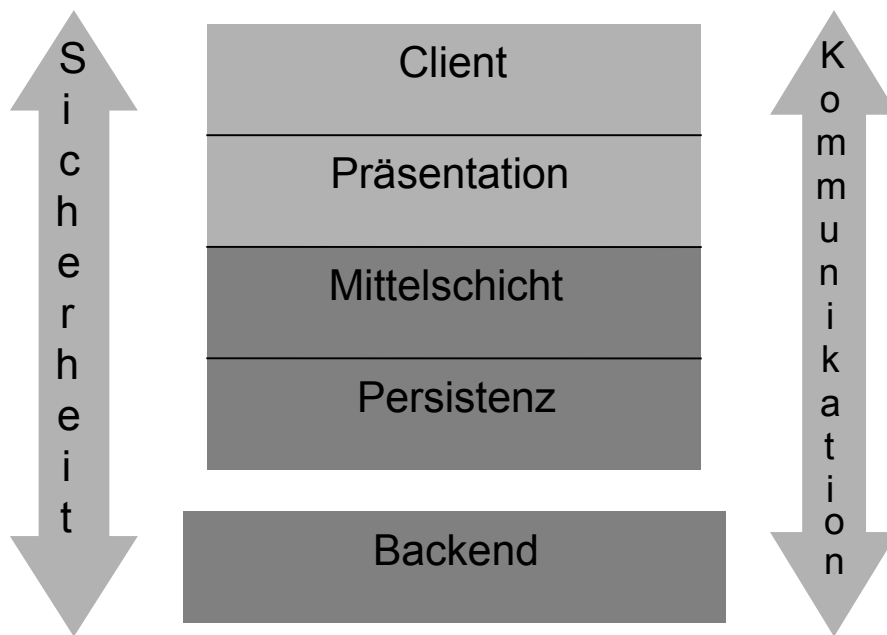


Abbildung 4-3: Strukturelle Sicht – Schichtenmodell

Eine eGovernment-Fachanwendung wird dabei prinzipiell in vier Schichten (siehe Abbildung 4-3) zerlegt:

1. Die Client-Schicht repräsentiert 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 1.1 Bezug genommen:
 - a. Webzugriff über Web-Browser oder spezielle Browser-Plug-Ins,
 - b. Mobilfunktelefone und Personal Digital Assistants (PDAs),
 - c. externe Systeme (z.B. ERP-Systeme von Industrieunternehmen).
2. Die Präsentation beschreibt die Informationsaufbereitung im Client und Interaktion des Nutzers mit der Fachanwendung. Die Präsentations-Komponente umfasst alle Standards zur Kommunikation mit den betrachteten Endgeräten des Client-Tiers.
3. Die Mittelschicht umfasst vor allem Neuentwicklungen für eGovernment und bildet meist den Kern eGovernment-spezifischer Anwendungen. In der Mittelschicht werden die spezifischen Geschäftslogiken der Fachanwendungen verknüpft. Die Darstellung der technischen Komponenten konzentriert sich auf die Abbildung und Diskussion von Standards für die Mittelschicht und ihrer Schnittstellen, da hier die größte Integration im Rahmen von eGovernment-

Lösungen erwartet wird. Die Mittelschicht verarbeitet die Daten aus dem Backend oder der Persistenzschicht.

- Die Persistenzschicht stellt die Datenspeicherung sicher. Dies wird meist mittels Datenbanken gelöst.

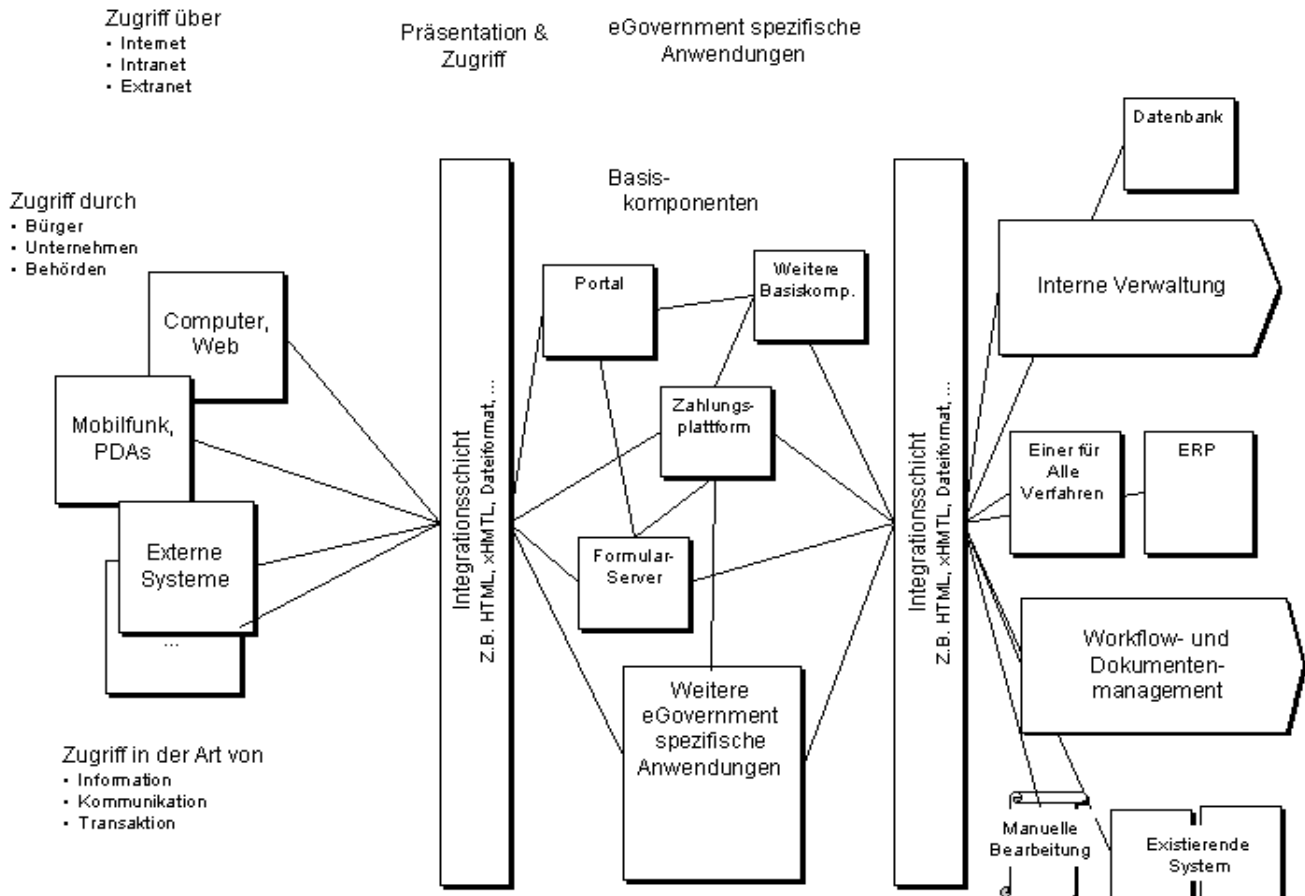


Abbildung 4-4: Das Architekturmodell abstrahiert Endgeräte, Systeme zur Datensicherheit sowie Methoden, Verfahren, Werkzeuge

Das Backend bezeichnet vorwiegend die „alte“ Welt (so genannte Legacy-Systeme). Diese Systeme bilden Fachanwendungen ab und werden meist nicht nur für eGovernment-Zwecke benötigt.

Innerhalb dieser Schichten wird eine Fachanwendung in Module aufgeteilt, die über definierte Schnittstellen interagieren. Die Interaktion geschieht über lokale und entfernte Kommunikation zwischen den Modulen.

Die in Kapitel 7 definierten Basiskomponenten stellen funktionale Module zur Realisierung von eGovernment-Anwendungen zur Verfügung.

Durch Endgeräte, Benutzer, Kommunikationsszenarien und Übertragungsmedien ergeben sich eine Vielzahl möglicher Anwendungsfälle. SAGA bezieht sich immer auf alle Anwendungsfälle, auf Ausnahmen wird entsprechend hingewiesen.

Zwischen sämtlichen Modulen ist eine sichere Interaktion notwendig. Diese Sicherheitsanforderungen umfassen:

- a. die Authentifizierung der beteiligten Personen und Systeme, um sicherzustellen, dass allen im System präsentierten Identitäten vertraut werden kann,
- b. die Autorisierung der Akteure, um sicherzustellen, dass die Akteure berechtigt sind, die jeweiligen Interaktionen auszuführen,
- c. die Integrität der Daten und Prozesse, um sicherzustellen, dass bei der Kommunikation die Daten unverändert übertragen werden und alle Prozesse korrekt ausgeführt werden,
- d. die Vertraulichkeit der Daten, um sicherzustellen, dass nur die Kommunikationspartner Zugriff auf die Daten haben. Vor allem ein unbefugtes Abhören der Kommunikation muss dabei ausgeschlossen werden.

SAGA definiert in Kapitel 6 Standards und Modelle, um die Interaktionen sicher zu gestalten.

4.2.5 Engineering Viewpoint (Sicht auf die physikalische Verteilung des Systems)

Diese Sicht beschreibt die erforderliche Systemunterstützung, um eine Verteilung der Objekte aus dem Computational Viewpoint zu erlauben. Dazu gehören Ausführungseinheiten für die Objekte, wie zum Beispiel Rechner und Kommunikationsinfrastruktur wie zum Beispiel Netzwerke, sowie alle Arten von Software-Plattformen für verteilte Systeme.

4.2.6 Technology Viewpoint (Technologische Sicht)

Dieser Punkt beschreibt die Wahl konkreter Technologien zur Implementierung und Realisierung des Systems.

SAGA beschreibt in Kapitel 5 die obligatorischen und empfohlenen Standards, gliedert nach den Schichten des Computational Viewpoints. Sicherheitsrelevante und –unterstützende Modelle und Standards sind mit allen anderen Modellen und Standards verknüpft und werden deshalb in Kapitel 6 übergreifend für alle Bereiche des Architekturbaukastens spezifiziert.

5 Standards für die IT-Architektur

In diesem Kapitel werden den einzelnen Elementen des in Kapitel 4 vorgestellten Architekturbaukastens 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.

5.1 Client

Der Client ist eine Software auf einem Endgerät, die einen vom Middle-Tier angebotenen Dienst in Anspruch nimmt. Der Client-Tier umfasst somit die klassische Benutzeroberfläche 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, so dass bei einem Informationsangebot für diese Endgeräte optimale Voraussetzungen für die breite Nutzung von eGovernment-Anwendungen bestehen:

- a. Computer (PC, Laptop)
- 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 serverseitig zur Verfügung gestellt wird.

5.1.1 *Web-/Computerbasierter Informationszugriff*

Auf Computern 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), die u.a. einen direkten Zugriff auf internetbasierte Dienste, E-Mail-Clients und je nach Erlaubnis auf das Betriebssystem ermöglichen. 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 soll soweit möglich ein Parallelangebot ohne aktive Inhalte vorgehalten werden (siehe auch Kapitel 1.3.1).

5.1.1.1 Web-Browser

Um bei der Realisierung von eGovernment-Anwendungen eine breite Nutzung zu ermöglichen, sollen als Frontend Web-Browser verwendet werden, die die Formate der Präsentationsebene (siehe Kapitel 5.2) verarbeiten und darstellen können. Hierbei sind folgende browserbasierte Client-Technologien zugelassen:

- 1) Die Nutzung von Cookies ist zugelassen, soweit diese
 - a) nicht persistent und
 - b) an die ausstellende Domain gebunden sind.Hierbei sind die Empfehlungen zum HTTP-Protokoll gemäß Kapitel 5.6.3 zu berücksichtigen.
- 2) Die Nutzung von Javascript ist zugelassen, wenn dieses durch Einsatz eines Server-Zertifikats und Nutzung einer SSL-Verbindung (siehe Kapitel 6.3.1) als authentisch und integer beim Client erkannt werden kann. Bei der Nutzung von Javascript ist das Kapitel 5.2.1.5 zu berücksichtigen.
- 3) Die Nutzung von Java-Applets ist zugelassen, wenn diese vom Server signiert sind und damit als authentisch und integer beim Client erkannt werden können und wenn eine Qualitätssicherung durch ein vom Hersteller unabhängiges Software-Unternehmen erfolgt ist.
- 4) Es wird eine Positivliste von unterstützten Plug-Ins geführt und unter der Adresse <http://www.kbst.bund.de/saga-plugins> veröffentlicht.
- 5) Für gängige Browser-Typen werden Beispielkonfigurationen erstellt und vom BSI über das Internet allgemein zur Verfügung gestellt.
- 6) Beim Versand von Formulardaten ist die Vertraulichkeit der Informationen durch Verwendung von SSL-verschlüsselten Kanälen unter Nutzung zugehöriger Server-Zertifikate sicherzustellen.
- 7) Auch bei der Nutzung der zugelassenen Client-Technologien ist die Rechtsverordnung zur Barrierefreiheit unverändert zu berücksichtigen.

5.1.1.2 Client-Anwendungen mit direktem Zugriff auf internetbasierte Dienste

Der Standard-Client für Anwendungen mit direktem Zugriff auf Web-Server ist der Web-Browser. Wenn die Funktionalität eines Web-Browsers begründeter Weise 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. Diese Anwendungen werden auf dem Client installiert und müssen bei Weiterentwicklungen mit den notwendigen Updates versorgt werden. Sie können entweder über CD-ROM oder über eine Download-Möglichkeit auf einer Internet-Seite als signierte Anwendungen zur Verfügung gestellt

werden. Dabei wird die Verwendung von Java-Anwendungen empfohlen (Vorteil der Plattformunabhängigkeit).

Client-Anwendungen müssen den folgenden Anforderungen genügen:

- 1) Alle personenbezogenen und sicherheitskritischen Daten sind auf dem lokalen Datenträger verschlüsselt abgelegt.
- 2) Eine sichere Datenübertragung zum Server, zum Beispiel gemäß den Spezifikationen von OSCl-Transport, wird unterstützt. Für die sonstige Client-Server Kommunikation sind ausschließlich die in Kapitel 5.6.1.2 definierten Protokolle zugelassen.
- 3) Die in SAGA dokumentierten Austauschformate für einen Austausch der Nutzerdaten mit anderen Anwendungen sollen unterstützt werden.
- 4) Es erfolgt eine Qualitätssicherung der Anwendung durch ein vom Hersteller unabhängiges Software-Unternehmen.
- 5) Die Anwendung wird mit einem Software-Zertifikat ausgeliefert, welches im Rahmen der Installation verifiziert wird.
- 6) Neben dem Download der Anwendung über das Internet wird auch die Distribution per CD-ROM angeboten.
- 7) Die Rechtsverordnung zur Barrierefreiheit ist zu berücksichtigen.

5.1.1.3 E-Mail-Client

Zum Empfangen, Senden und Bearbeiten von E-Mails sind E-Mail-Clients einzusetzen, die zumindest die technische Unterstützung der folgenden beiden E-Mail-Standards gewährleisten.

- SMTP: zum Empfang und zum Versenden von E-Mails
- MIME: als E-Mail Format Beschreibung

An dieser Stelle sei darauf hingewiesen, dass die Kommunikation dieser Clients nur im Hinblick auf die Kommunikation mit der Verwaltung standardisiert bzw. 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.

In Ausnahmefällen kann es vorkommen, dass elektronische Postfächer angeboten werden müssen. Es sind die Standards in Kapitel 5.6.3 zu verwenden.

5.1.2 Informationszugriff via Mobiltelefon/PDA

Um über Mobiltelefone oder PDAs das Angebot der Präsentationsebene nutzen zu können, sind derzeit Protokolle notwendig, die serverseitig bedient werden (siehe Kapitel 5.2.2). Anwendungen auf solchen Engeräten sind in Deutschland noch nicht verbreitet.

5.1.3 Informationszugriff über externe Systeme

Die Kommunikation und Interaktion zwischen externen und internen Systemen soll 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.

Siehe die Kapitel Datenintegration, Middleware, Kommunikation und Anbindung an das Backend (Kapitel 5.4 bis 5.7).

5.2 Präsentation

Das Element Präsentation stellt dem Client-Tier Informationen zur Verfügung. Je nach Anwendungsfall müssen unterschiedliche Formate bereitgestellt werden, die in den folgenden Unterkapiteln aufgelistet werden. Dabei wird die Verwendung offener Austauschformate, die über hinreichend viele Funktionen verfügen und auf unterschiedlichen Plattformen verfügbar sind, 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.

5.2.1 Informationsverarbeitung – Computer/Web

5.2.1.1 Behindertengerechte 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)", siehe http://www.bmi.bund.de/Annex/de_22681/BITV.pdf, zu Grunde gelegt werden. Diese Rechtsverordnung setzt §11 des Behindertengleichstellungsgesetzes um und

berücksichtigt dabei insbesondere die Web Content Accessibility Guidelines des W3C in der Version 1.0, die unter <http://www.w3.org/TR/WCAG10> zugänglich ist.

5.2.1.2 Austauschformate für Hypertext

Obligatorisch: Hypertext Markup Language (HTML) v3.2

Um die Unterstützung von älteren Browser-Generationen zu gewährleisten, muss das Format HTML v3.2 (<http://www.w3.org/TR/REC-html32>) unterstützt werden.

Empfohlen: Hypertext Markup Language (HTML) v4.01

Heute sind bereits weitflächig Browser-Typen im Einsatz, die das Nachfolgeformat von HTML v3.2 unterstützen. W3C empfiehlt einerseits, dass Autoren HTML v4.01 (<http://www.w3.org/TR/html401/>) verwenden, und andererseits, dass Browser, die HTML v4.01 unterstützen, abwärtskompatibel sind. Auch ist HTML v4.01 gefordert für die technische Umsetzung des barrierefreien Zuganges durch Web Content Accessibility Guidelines Version 1.0.

Dennoch kann es vorkommen, dass Browser HTML v4.01 nicht in vollem Umfang unterstützen. Deshalb ist die funktionale Kompatibilität der Anwendung zu HTML v.3.2 zu gewährleisten. Damit ist gemeint, dass a) Informationen vollständig dargestellt und b) Funktionen vollständig genutzt werden können, aber in der Darstellung auf der HTML-Seite im Bereich Gestaltung Einschränkungen in Kauf genommen werden können.

Unter Beobachtung: Extensible Hypertext Markup Language (XHTML) v1.0

XHTML v1.0 (<http://www.w3.org/TR/xhtml1/>) formuliert HTML v4.01 als XML-Anwendung. Mit der weiteren Entwicklung und Verbreitung neuerer Browser-Generationen soll XHTML v1.0 zum Einsatz kommen. Anwendungen sollen dabei die funktionale Kompatibilität zu HTML v.3.2 gewährleisten.

5.2.1.3 Style Sheets

Um angebotene Informationen für unterschiedliche Browser-Typen einheitlich darzustellen, können Style Sheets Verwendung finden. Style Sheets sind Formatvorlagen für beliebige Daten, in denen beschrieben wird, wie Auszeichnungen in SGML-konformen Sprachen darzustellen sind. Je nach Anwendungszweck können einer oder beide der folgenden durch das W3C etablierten Typen von Style Sheets verwendet werden:

Empfohlen: Cascading Style Sheets Language Level 2 (CSS2)

Zur Gestaltung von HTML-Seiten soll die Cascading Style Sheets Language Level 2 (CSS2) (<http://www.w3.org/TR/REC-CSS2/>) verwendet werden.

Empfohlen: Extensible Stylesheet Language (XSL) v1.0

Zur Transformation und Darstellung von XML-Dokumenten in HTML Dateien soll die Extensible Stylesheet Language (XSL) in der Version 1.0 (<http://www.w3.org/TR/xsl/>) eingesetzt werden.

5.2.1.4 Zeichensätze

Obligatorisch: ISO 10646-1:2000/Unicode v3.0 UTF-8

Um ausreichend Zeichen für die verschiedenen, weltweit existierenden Buchstaben, Ziffern und Symbole zur Verfügung zu haben, soll als Zeichensatz für Dokumente im HTML-Format ISO 10646-1:2000/Unicode V3.0 in der UTF-8 Kodierung verwendet werden. Diese Spezifikation ist unter www.unicode.org verfügbar.

Empfohlen: ISO 10646-1:2000/Unicode v3.0 UTF-16

Soweit die Dokumente in griechischer Sprache oder in anderen nicht west-europäischen Sprachen verfasst sind, soll die UTF-16-Kodierung verwendet werden.

Empfohlen: ISO 8859-1

Derzeit findet der Zeichensatz ISO 8859-1 noch immer Verbreitung und kann weiterhin verwendet werden.

Empfohlen: ISO 8859-15

Die Kodierung gemäß ISO 8859-15 ist derzeit noch verbreitet und wird in diesem Rahmen weiterhin zugelassen.

5.2.1.5 Statische und dynamische, passive und aktive Inhalte

Statische Inhalte sind (HTML-)Dateien, die von einem Web-Server nicht zur Laufzeit generiert, sondern in der Regel aus dem Dateisystem ausgelesen und geliefert werden. **Dynamische Inhalte** sind HTML Dateien, die zur Laufzeit – z.B. mittels Abfragen aus Datenbanken – auf dem Server generiert und dann ausgeliefert werden.

Passive Inhalte sind HTML Dateien, die keinen Programm-Code und keine Computerprogramme enthalten oder zur Laufzeit nachladen. **Aktive Inhalte** sind Computerprogramme, die in Internet-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 Kapitel 5.1 zu berücksichtigen.

Obligatorisch: HTML-Format

Für die Bereitstellung von *Informationen* sollen HTML-Seiten mit Hilfe der in Abschnitt 5.2.1.2 definierten Austauschformate für Hypertext eingesetzt werden. Die Unterstützung aktiver Inhalte und von Plug-Ins darf nur in dem in Kapitel 5.1 definierten Umfang vorausgesetzt werden.

Obligatorisch: ECMA-262 – ECMAScript Language Specification

Soweit gemäß Kapitel 5.1.1.1 innerhalb von HTML Seiten Javascript verwendet wird, soll dieses der Spezifikation von ECMA 262 (siehe www.ecma.ch) genügen.

Empfohlen: Servlets und Java Server Pages oder XSL

Für die serverbasierte dynamische Erzeugung von HTML Seiten sollen Servlets und Java Server Pages (JSP, siehe <http://java.sun.com/products/jsp/>) oder Servlets und XSL (siehe <http://www.w3.org/TR/xsl/>) eingesetzt werden.

5.2.1.6 Dateitypen und Typerkennung für Textdokumente

Je nach Verwendungszweck sind unterschiedliche Dateitypen für Textdokumente zu verwenden:

Obligatorisch: Text (.txt)

Einfache, veränderbare Textdokumente werden im weit verbreiteten Format (.txt) ausgetauscht, was eine generelle Lesbarkeit sicherstellen soll. Der anzuwendende Zeichensatz ist in der Norm ISO 8859-1 beschrieben und bezeichnet ASCII plus Umlaute.

Obligatorisch: Hypertext Markup Language (HTML)

Hypertext Dokumente werden im HTML-Format als (.html)-Dateien zum Einsatz kommen (siehe Kapitel 5.2.1.2).

Obligatorisch: Portable Document Format (PDF) Version 4

Unveränderbare Textdokumente sollen im plattformunabhängigen Portable Document Format von Adobe Acrobat als (.pdf) in der Acrobat Viewer Version 4 zur Verfügung gestellt werden (www.adobe.de).

Empfohlen: Extensible Markup Language (XML)

Weiterhin kann auch XML zur Beschreibung von Dokumenten eingesetzt werden, welches hierfür mehr gestalterische Möglichkeiten bietet als HTML. Eine genaue Spezifikation findet sich unter <http://www.w3.org/TR/2000/REC-xml-20001006>.

Unter Beobachtung: Portable Document Format (PDF) Version 5

Zur Unterstützung von Formularen und barrierefreien Textdokumenten ist der Einsatz der noch nicht so verbreiteten Version 5 des Portable Document Formats von Adobe Acrobat als (.pdf) möglich. Beim Einsatz für Formulare sind die Empfehlungen des Moduls "Sicherer Internet-Auftritt" im E-Government-Handbuch in Bezug auf aktive Inhalte zu berücksichtigen (siehe Kapitel 5.2.1.5).

Obligatorisch: Multipurpose Internet Mail Extensions (MIME)

Zur standardisierten Angabe, welches Format eine Datei oder ein Teil davon hat, ist das Format Multipurpose Internet Mail Extensions (MIME) zu verwenden. Es erlaubt dem E-Mail-Client oder dem Web-Browser die eindeutige Identifikation des Dateityps. Siehe dazu RFC 2045 bis RFC 2049.

5.2.1.7 Dateitypen für Tabellenkalkulationen

Für Tabellenkalkulationen sind je nach Anforderung an die Veränderbarkeit des Dokuments unterschiedliche Formate für den Datenaustausch einzusetzen:

Obligatorisch: Comma Separated Value (CSV)

Abgegrenzte (delimited), kommaseparierte Tabellen sind als (.csv)-Dateien zu speichern und auszutauschen.

Obligatorisch: Portable Document Format (PDF) Version 4

Analog zu 5.2.1.6.

Unter Beobachtung: Portable Document Format (PDF) Version 5

Analog zu 5.2.1.6.

5.2.1.8 Dateitypen für Präsentationen

Präsentationen sollen je nach Anforderung an die Veränderbarkeit des Dokuments in unterschiedlichen Formaten ausgetauscht werden:

Obligatorisch: Hypertext Markup Language (HTML)

Veränderbare Präsentationen sollen als Hypertext Dokumente im HTML-Format als (.html)-Dateien ausgetauscht werden (siehe Kapitel 5.2.1.2 *Austauschformate für Hypertext*).

Obligatorisch: Portable Document Format (PDF) Version 4

Analog zu 5.2.1.6.

Unter Beobachtung: Portable Document Format (PDF) Version 5

Analog zu 5.2.1.6.

5.2.1.9 Austauschformate für Bilder

Obligatorisch: Graphics Interchange Format (GIF)

Aufgrund der weiten Verbreitung ist für den Austausch von Grafiken und Schaubildern das Format Graphics Interchange Format (.gif) zu wählen, wobei (.gif) Bilddateien mit einer Farbtiefe von 256 Farben (8 Bit pro Pixel) komprimiert werden.

Obligatorisch: Joint Photographic Experts Group (JPEG)

Für den Austausch von Bildern ist das Format Joint Photographic Experts Group (.jpg) zu wählen, das das Ändern des Komprimierungsgrades und die Angabe der Dichte unterstützt, so dass ein Kompromiss zwischen Dateigröße, Qualität und Ver-

wendung erleichtert wird. Es werden 16,7 Mio. Farben (24 Bits Farbinformationen) unterstützt.

Empfohlen: Portable Network Graphics (PNG)

Wenn möglich, soll das Grafikformat Portable Network Graphics (.png, <http://www.w3.org/TR/REC-png>) verwendet werden. Das Format (.png) kann lizenzfrei angewendet werden, unterstützt 16 Mio. Farben, Transparenz, verlustfreie Kompression, inkrementelle Anzeige der Grafik (erst Grobstruktur, bis Datei ganz übertragen ist) und das Erkennen beschädigter Dateien.

(.png) wird anstelle von (.gif) obligatorisch, wenn sich neuere Browser der fünften Generation vollständig etabliert haben.

Empfohlen: Tagged Image File Format (TIFF)

Für Grafikinformatoren, die keinerlei Informationsverlust erlauben, soll das Tagged Image File Format (.tif) verwendet werden. (.tif) ist ein Dateiformat für Rastergrafiken, wobei verschiedene Formatierungen es Anwendungen erlauben, Teile der Grafik zu verarbeiten oder zu ignorieren.

Empfohlen: Enhanced Compressed Wavelet (ECW)

Falls höchstmögliche Kompression benötigt wird, soll das Rastergrafikformat Enhanced Compressed Wavelet (.ecw) zum Einsatz kommen.

5.2.1.10 Austauschformate für Geoinformationen (Rasterdaten, Vektordaten)

Die Bereitstellung von Geoinformationen über das Internet („Geodatenkiosk“) sowie deren kartographische Darstellung (WebGIS) im Internet beginnt sich zunehmend zu verbreiten. Die Darstellung von geographischen Informationen in Form thematischer Karten über Internet-Portale kann entweder über Rasterdaten oder als Vektorgrafik auf Präsentationsebene erfolgen. Eine Vektorgrafik beschreibt ein Bild als Folge geometrischer Objekte. Diese Objekte (z.B. Linie, Kreis, Spline, Overlay) haben die Eigenschaften Position, Farbe und Anordnung.

Unter Beobachtung: Geography Markup Language (GML)

GML (Geography Markup Language) ist eine Auszeichnungssprache zum Transport und zur Speicherung geographischer Informationen, welche räumliche und nicht-räumliche Eigenschaften berücksichtigt. GML wurde durch das Open GIS Consortium (OGC) definiert. GML beinhaltet keine Aussage über die Darstellung auf dem

Bildschirm oder in einer Karte. Die Geometrien werden durch Simple Features repräsentiert, welche ebenfalls durch das OGC definiert wurden.

Seit der Version 2.0 erfolgt die Spezifikation nicht mehr durch Dokumenttyp-Definitionen (DTD) sondern mittels XML Schema.

Unter Beobachtung: Scalable Vector Graphic (SVG)

Das W3C definiert SVG als Sprache, die zweidimensionale Grafiken in XML beschreibt. SVG unterstützt dabei drei Arten von grafischen Objekten:

- Vektorgrafiken (beispielsweise Linien, Kurven, Polygone, Pfade)
- Pixelbilder
- Text

SVG ermöglicht, dass grafische Objekte gruppiert, verändert oder in andere vorher gerenderte Objekte transformiert werden. Beschneidungspfade, Alphakanäle oder Filtereffekte sind dabei besondere Features. In SVG erstellte Grafiken können zudem interaktive und dynamische Eigenschaften besitzen.

Unter Beobachtung: Vector Markup Language (VML)

Die Darstellung von Vektorgrafiken kann durch das Dateiformat Vector Markup Language (.vml) unterstützt werden. (.vml) ist eine auf XML basierende Auszeichnungssprache für 2-dimensionale Grafiken, eingebettet in HTML. Sie benutzt dabei die von CSS bekannten Strukturen.

5.2.1.11 Austauschformate für Audio- und Video-Dateien

Obligatorisch: MPEG-1 Layer 3 (MP3)

Für den Austausch von Audio-Sequenzen soll das marktübliche Format (.mp3) verwendet werden, wobei (.mp3) für MPEG-1 Layer 3 (MPEG = Motion Picture Experts Group) steht. (.mp3) ist ein Verfahren, um Audio-Daten bei höchster Qualität extrem zu komprimieren. Mit einem entsprechenden Plug-In ist ein Browser in der Lage, solche Dateien "abzuspielen". Mehr Informationen zu (.mp3) sind unter www.iis.fhg.de verfügbar.

Obligatorisch: Quicktime (.qt, .mov)

Für den Austausch von Videosequenzen soll das marktübliche Quicktime-Format verwendet werden. Mit einem entsprechenden Plug-In ist ein Browser in der Lage,

solche Dateien "abzuspielen". Mehr Informationen zu Quicktime sind unter quicktime.apple.com verfügbar.

5.2.1.12 *Austauschformate für Audio- und Video-Streaming*

Im Gegensatz zu „normalen“ Audio- und Video-Sequenzen 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 "normalen" 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 dabei 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: HTTP

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

Obligatorisch: Quicktime (.qt, .mov)

Um eine möglichst hohe Kompatibilität des Streaming-Signals mit gängigen Browsern, Audio- und Video-Clients, bzw. Plug-Ins zu erreichen, wird der Einsatz des Quicktime-Formats empfohlen, das derzeit von allen gängigen Produkten unterstützt wird. Mehr Informationen zu Quicktime sind unter quicktime.apple.com verfügbar.

Unter Beobachtung: Ogg

Ogg ist ein derzeit unter Open Source entwickeltes, herstellerunabhängiges Container-Format für Streaming Audio (Ogg Vorbis) und Video (Ogg Theora, Ogg Tarkin). Es gibt bereits Ankündigen von führenden Streaming-Server-Herstellern, dieses Format in Kürze zu unterstützen. Es wird erwartet, dass dieses Format in naher Zukunft eine größere Verbreitung finden wird. Weitere Informationen zu Ogg finden sich unter www.ogg.org.

5.2.1.13 *Animation*

Obligatorisch: Animated GIF

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

5.2.1.14 *Datenkompression*

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

Obligatorisch: ZIP v2.0

Die komprimierten Daten sollen im international verbreiteten Format ZIP Version 2.0 als (.zip) Dateien ausgetauscht werden.

Empfohlen: GZIP v4.3

Ersatzweise ist auch das Format GZIP in der Version 4.3, spezifiziert in RFC 1952 (www.ietf.org), als (.gz)-Dateien möglich.

5.2.2 Informationsverarbeitung – Mobiltelefon/PDA

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

Obligatorisch: Short Message Services (SMS)

Für die Realisierung von Short Message Services soll die Spezifikationen des SMS-Forums, zugänglich unter www.smsforum.net, Anwendung finden. Das SMS-Forum ist ein internationales Forum aller großen Informationstechnologieunternehmen.

Unter Beobachtung: WML v1.x

Die Wireless Markup Language (<http://www.wapforum.org/what/technical.htm>) wurde definiert zur Benutzung in schmalbandigen Umgebungen, besonders dem Mobilfunk, und ist die zu WAP gehörige Markup Language. Alle Mobilfunkbetreiber in Deutschland unterstützen WML 1.x.

In Deutschland wird seit kurzem der sehr erfolgreiche Dienst i-mode der japanischen Telekommunikationsgesellschaft NTT DoCoMo für Mobiltelefone in Lizenz angeboten. Die Lizenzvereinbarung sieht vor, dass Endgeräte in Deutschland mit dual Browser Systemen ausgeliefert werden, die sowohl das proprietäre Format iHTML als auch das in Europa verbreitete WML v1.x unterstützen, so dass WML v1.x für die Zwecke von SAGA genügt.

Unter Beobachtung: WAP v1.x

Das Wireless Application Protocol (WAP) v1.x (www.wapforum.org) ist eine Spezifikation zur Entwicklung von Anwendungen, die über drahtlose Kommunikationsnetzwerke operieren. Haupteinsatzgebiet ist der Mobilfunk.

Unter Beobachtung: XHTML Basic

XHTML Basic (<http://www.w3.org/TR/xhtml-basic/>) 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). Derzeit werden wiederum Subsets von HTML Basic für verschiedene Endgeräte definiert.

WML 2.0 basiert wie WML 1.0 auf XML, ist jedoch ein Subset der XHTML Mobile Profile Spezifikation, welches wiederum ein Subset von XHTML Basic ist.

5.2.3 Informationsverarbeitung – externe Systeme

Siehe die Kapitel Datenintegration, Middleware, Kommunikation und Anbindung an das Backend (Kapitel 5.4 bis 5.7). Von den im Bereich Middleware benannten Standards ist jedoch nur eine Untermenge für die Kommunikation mit externen Systemen relevant. Im Zentrum der Kommunikation mit externen Systemen stehen XML und Web-Service-Technologie. Bestehende Schnittstellen, basierend auf OSI-Technologie, werden schrittweise migriert.

5.3 Fachliche Prozess- und Datenmodelle

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 und benötigte Daten definiert. Ein Beispiel für dieses Vorgehen ist XMeld, das vom Land Bremen entwickelt wurde.

5.3.1 Fachliche Prozessmodelle

Dienstleistungen sind in Form von fachlichen Prozessmodellen zu beschreiben. Hierfür sollen von der Anfrage des Kunden bis zur Leistungserbringung alle Arbeitsschritte Ende-zu-Ende betrachtet werden. Diese Prozessmodelle sollen in einer ersten Entwicklungsstufe auf einem relativ hohen Niveau verbleiben und in der Regel aus nicht mehr als 20 Arbeitsschritten bestehen.

Neue Vorschläge zu Prozessdefinitionen sollen immer auf

- a. Wiederverwendbarkeit,
- b. Einfachheit und
- c. Abbildbarkeit mit bereits vorhanden Prozessdefinitionen

überprüft werden. Hierbei soll das für Prozesse und Organisation zuständige Kompetenzzentrum unterstützen. Dieses Kompetenzzentrum soll auch mit Hilfe von Arbeitsgruppen die Definition der im Folgenden genannten Prozessarten a und b übernehmen.

Grundsätzlich werden drei Prozessvarianten unterschieden:

- a. Referenzmodelle definieren Vorlagen für Arbeitsabläufe, die nicht spezifisch für eine Dienstleistung sind. Sie sollen nicht behördenspezifisch aufgebaut sein, sondern allgemein den Prozess zwischen Kunden und einem Dienstleister beschreiben.
- b. Übergreifende Prozesse sind Arbeitsabläufe, die für alle oder für einen Großteil der Dienstleistungen gleich sind (beispielsweise Navigation, Login, Basiskomponenten und Schlüsselanwendungen).
- c. Spezifische Prozesse sind Arbeitsabläufe, die je nach Dienstleistung unterschiedlich sind. Diese sollen auf Referenzmodellen aufbauen. Unterschiede sind im Zweifel zu begründen.

Obligatorisch: Rollenmodelle und Flussdiagramme

Rollenmodelle und Flussdiagramme können 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 sollen sich im weiteren Sinne nach DIN 66001 Informationsverarbeitung, Sinnbilder und ihre Anwendung, richten.

Empfohlen: Unified Modeling Language (UML)
--

Zur Vorbereitung und Dokumentation von Großprojekten soll die Unified Modeling Language (UML, siehe www.omg.org) für objektorientierte Modellierung angewendet werden. Insbesondere Use Cases haben sich im Einsatz bewährt und erlauben transparente Spezifikationen zu erstellen und abzustimmen. Die Anwendung von UML ist jedoch aufwendig und setzt entsprechende Kenntnisse sowie gegebenenfalls den Einsatz spezieller Werkzeuge voraus. Andererseits können aus entsprechenden Spezifikationen direkt XML-Datenstrukturen oder Java-Programmteile generiert werden.

5.3.2 Fachliche Datenmodelle

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

Datenmodelle sollen immer auf

- a. Wiederverwendbarkeit,
- b. Einfachheit,
- c. Abbildbarkeit mit bereits vorhandenen Datendefinitionen

überprüft werden. Hierbei soll das für Prozesse und Organisation zuständige Kompetenzzentrum unterstützen. Die Standardisierung der Datenmodelle soll durch eine noch näher zu bestimmende Leitstelle und durch von dieser gesteuerte Arbeitsgruppen geschehen (siehe Kapitel 2.2). Vor dem Beginn der Formulierung von Datenmodellen soll überprüft werden, ob ähnliche Modelle in Deutschland oder auf europäischer Ebene bereits vorliegen.

Drei Ebenen der Detaillierung werden unterschieden:

- a. Funktionale Datenmodelle beschreiben wesentliche Datenentitäten und deren Beziehung zueinander, ohne auf Spezifika einzugehen. Diese Darstellung wird für die fachliche Grobkonzeption empfohlen.

- b. Objektorientierte Referenzklassen definieren die grundsätzlichen Datenelemente der eGovernment-Anwendungen und beinhalten die verallgemeinerbaren Elemente.
- c. Abgeleitete Klassen oder Objekte erben alle Datenelemente der Referenzklassen und addieren weitere spezifische Merkmale.

Obligatorisch: Entity Relationship Diagramme

Funktionale Datenmodelle der oben genannten Detaillierungsebene a. bedürfen der Darstellung mit Entity Relationship Diagrammen.

Obligatorisch: Extensible Markup Language Schema Definition (XSD) v1.0

Die Datenspezifikation der beschriebenen Detaillierungsebenen b. und c. soll als XML-Schema erfolgen (siehe Kapitel 5.4).

Unter Beobachtung: Unified Modeling Language (UML)

Zur Vorbereitung und Dokumentation von Großprojekten kann die Unified Modeling Language (UML, siehe www.omg.org) für objektorientierte Modellierung angewendet werden. Aus entsprechenden Spezifikationen können direkt XML-Schemata generiert werden.

5.4 Datenintegration

5.4.1 Datenbeschreibung

Obligatorisch: Extensible Markup Language (XML)

XML (Extensible Markup Language) soll als der universelle und primäre Standard für den Datenaustausch aller verwaltungstechnisch relevanten Informationssysteme dienen (<http://www.w3.org/XML>).

Neu zu beschaffende Systeme sollen in der Lage sein, über XML Daten auszutauschen. Existierende Systeme müssen nicht zwingend XML-fähig sein.

Wo nötig kann auch Middleware eingesetzt werden, die eingehende XML-Informationen interpretiert und in die benötigten Datenformate der Alt- bzw. Fremdsysteme transformiert bzw. konvertiert. Dieser Prozess kann in beide Richtungen erfolgen; über Workflow- und Transaktionsmechanismen kann die Durch- bzw. Ausführung eines Geschäftsprozesses überwacht werden.

Obligatorisch: Extensible Markup Language Schema Definition (XSD) v1.0

Zur strukturierten Beschreibung von Daten sollen XML-Schemata gemäß den W3C-Definitionen (www.w3.org) mit der Extensible Markup Language Schema Definition (XSD) erstellt werden.

5.4.2 Datentransformation

Empfohlen: Extensible Stylesheet Language Transformation (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 erfolgt über die durch die W3C definierte Sprache XSLT (<http://www.w3.org/TR/xslt>) als Teil von XSL (Extensible Stylesheet Language).

5.4.3 Zeichensätze

Beim Austausch von Daten gelten für die zu verwendenden Zeichensätze die Standards, die auch schon im Kapitel 5.2 *Präsentation* definiert wurden. Dabei können individuelle Teile von XML-Schemata weiter im Zeichensatz eingeschränkt werden.

5.5 Middleware Architektur

In diesem Kapitel werden die Standards in dem Element Middleware des eGovernment-Architekturbaustens definiert, wobei vor allem auf den Aspekt Applikationsintegration eingegangen wird. Die Vorgaben und Empfehlungen in diesem Bereich folgen aus den Gestaltungsprinzipien, die im Umsetzungsplan der BundOnline-2005-Initiative festgelegt wurden, namentlich Betriebssystemneutralität, Interoperabilität und Portabilität.

Andere 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.

Obligatorisch: J2EE v1.3

Zur Entwicklung und Integration folgender Anwendungen (Verbundanwendungen) auf dem Middle-Tier, nämlich

- Basiskomponenten,
- Anwendungen, die Basiskomponenten oder dazu bereitgestellte Bibliotheken unmittelbar einbinden, und
- Anwendungen, die als Ganzes oder in Teilen (Komponenten) für eine Wiederverwendung (Portierung) vorgesehen sind,

wird die Anwendung von Java 2 Platform Enterprise Edition (J2EE) Technologien vorausgesetzt. J2EE ist eine Spezifikation, die eine Reihe von Programmierschnittstellen und einen Entwicklungsprozess definiert. In der Gesamtheit bildet J2EE eine Architektur, die wesentliche Aspekte von geschäftskritischen Anwendungen berücksichtigt und unterstützt. Die Systemarchitektur von J2EE umfasst verschiedene Java- und Java-Middleware-Technologien (Servlets, JavaBeans, Enterprise JavaBeans u.a.), welche die Basis für verbreitete eBusiness-Frameworks bilden. Teil des J2EE Software Developer Kits sind Standard-Programmierschnittstellen (APIs) und Technologien, z.B. JDBC 2.0 API, JMS 1.0, JTA 1.0, JAXP 1.1, J2EE Connector API 1.0, JAAS 1.0, JavaMail API 1.2, JAXR. Detaillierte Informationen zu J2EE in der aktuellen Version 1.3 finden sich unter <http://java.sun.com/j2ee>.

Obligatorisch: J2SE

Soweit für eine Anwendung der Leistungsumfang von J2EE anfänglich oder dauerhaft nicht im vollem Umfang benötigt wird, sollen alternativ die Technologien von J2EE einzeln eingesetzt werden. Als Grundlage dient dabei die Java 2 Platform Standard Edition (J2SE). Die einzelnen Technologien sollten entsprechend der J2EE Spezifikation 1.3 verwendet werden, um einen kompatiblen Migrationspfad zu J2EE zu bilden.

JAAS v1.0

Authentifizierung und Autorisierung soll mit Hilfe des Java Authentication and Authorization Service (JAAS) implementiert werden. JAAS bietet Module zur Integration in die Authentifizierung von Unix, Windows NT und Kerberos. JAAS ist Bestandteil der Java 2 Platform Standard Edition (J2SE).

JDBC v2.0

Für Zugriffe auf Datenbanken soll JDBC genutzt werden.

JAXP v1.1

Für die Verarbeitung von XML-Dokumenten soll die Java API for XML Parsing (JAXP) verwendet werden.

JMS, J2EE Connector Architecture

Für die Integration von externen Systemen sollte entweder der Java Message Service (JMS) oder die J2EE Connector Architecture genutzt werden.

JNDI v1.1.2

Für den Zugriff und die Erstellung von Verzeichnisdiensten sollte JNDI genutzt werden. JNDI bietet Zugriffsmöglichkeiten auf LDAP und andere Verzeichnisdienste.

Unter Beobachtung: Microsoft Windows .NET Framework

Das .NET Framework ist eine Middleware Technologie, die von Microsoft entwickelt wurde. Die Systemarchitektur von .NET umfasst eine Laufzeitumgebung für unterschiedliche Programmiersprachen und eine Entwicklungsumgebung. Sie unterstützt wesentliche Webstandards (darunter SOAP, WSDL, UDDI, XML).

Kernkomponenten der .NET Middleware sind durch internationale Standardisierungsgremien standardisiert worden. Zurzeit werden Projekte durchgeführt, die die Implementierung von Kernkomponenten der .NET Middleware auf Nicht-Windows-Betriebssystemen zum Ziel haben.

Derzeit erfüllt die .NET-Architektur die Anforderungen an die Portabilität noch nicht betriebssystemunabhängig. Es wird erwartet, dass Microsoft die .NET-Technologie zu einem offenen Standard weiterentwickelt und dabei auch die Konformität zu den in SAGA vorgesehenen Standards gewährleistet.

5.6 Kommunikation

Innerhalb des Elements Kommunikation wird zwischen Anwendungs-, Middleware- und Netzwerkprotokollen sowie Verzeichnisdiensten unterschieden.

5.6.1 Middleware-Protokolle

Bei den Middleware-Protokollen wird unterschieden, ob Server-Anwendungen innerhalb der Verwaltung untereinander kommunizieren (Kapitel 5.6.1.1), oder ob eine Client-Anwendung außerhalb der Verwaltung mit einem Server der Verwaltung kommuniziert (siehe Kapitel 5.6.1.2).

5.6.1.1 Server-Server Kommunikation innerhalb der Verwaltung

Obligatorisch: Remote Method Invocation (RMI)

Für die Kommunikation von Anwendungen oder Anwendungskomponenten, die auf einer J2EE-Architektur basieren, ist Remote Method Invocation (RMI) besonders geeignet. Über RMI kann ein Objekt auf einer Java Virtual Machine (VM) Methoden eines Objektes aufrufen, das auf einer anderen Java VM läuft. Weitere Informationen zu RMI finden sich auf <http://java.sun.com>.

Obligatorisch: SOAP v1.1

Für die Kommunikation von Anwendungen oder Anwendungskomponenten, die auf einer J2EE-Architektur basieren, kann SOAP (Simple Object Access Protocol) eingesetzt werden, wenn die Anforderungen an den Protokollumfang es zulassen. Bei einer Kommunikation zwischen Servern, die nicht auf J2EE basieren, ist SOAP besonders geeignet. Mittels SOAP können strukturierte Daten als XML-Objekte zwischen Anwendungen oder Anwendungskomponenten über ein Internet-Protokoll (z.B. über HTTP) ausgetauscht werden. Für weitere Information zu SOAP siehe www.w3.org.

Obligatorisch: Web Services Description Language (WSDL) v1.1

Zur Servicedefinition soll die Web Services Description Language (WSDL) eingesetzt werden. WSDL ist eine standardisierte Sprache, mit der Web Services so beschrieben werden, dass sie durch andere Applikationen genutzt werden können, ohne weitere Implementierungsdetails kennen oder die gleiche Programmiersprache einsetzen zu müssen.

Obligatorisch: Extensible Markup Language Schema Definition (XSD)

Die Spezifikation der zu übertragenden Datenelemente soll mittels XML Schema erfolgen.

Empfohlen: RMI-IIOP

RMI-IIOP ist integraler Bestandteil von J2EE. Über RMI-IIOP können J2EE Applikationen oder Applikationskomponenten mit CORBA-Komponenten kommunizieren, falls auf den zugehörigen Applikations-Servern die geeigneten Object Request Broker zur Verfügung stehen.

5.6.1.2 Client-Server Kommunikation

Für den Zugriff von Client-Applikationen über das Internet auf Server-Applikationen bei der Verwaltung sollen 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 eine Software-Komponente, die mit anderen Komponenten über das Standardprotokoll HTTP mittels SOAP kommuniziert. Für den Nachrichteninhalte selbst wird XML verwendet, das schon im Kapitel 5.4 *Datenintegration* 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 Profile aus bestehenden Standards. Das anzuwendende Profil ist WS-I-Basic und umfasst XML Schema 1.0, SOAP 1.1, WSDL 1.1, und UDDI 1.0.

Obligatorisch: Web Services Description Language (WSDL) v1.1
--

Zur Servicedefinition soll die Web Services Description Language (WSDL) eingesetzt werden. WSDL ist eine standardisierte Sprache, mit der Web Services so beschrieben werden, dass sie durch andere Applikationen genutzt werden können, ohne weitere Implementierungsdetails kennen oder die gleiche Programmiersprache einsetzen zu müssen.

Obligatorisch: Extensible Markup Language Schema Definition (XSD) v1.0
--

Die Spezifikation der zu übertragenden Datenelemente soll mittels XML Schema erfolgen.

Obligatorisch: SOAP v1.1

Mittels SOAP (Simple Object Access Protocol) können strukturierte Daten als XML-Objekte zwischen Anwendungen über ein Internet-Protokoll (z.B. über HTTP) ausgetauscht werden. Für weitere Informationen zu SOAP siehe www.w3.org.

Unter Beobachtung: UDDI v2.0

Das Projekt UDDI (Universal Description, Discovery and Integration, aktuelle Version 2.0, www.uddi.org) ist eine XML-basierte Technologieinitiative von Unternehmen aus allen Wirtschaftszweigen mit dem Ziel, Web Services zu publizieren, strukturiert zu verwalten und dem Nutzer verfügbar zu machen. UDDI setzt dabei auf Standards

des World Wide Web Consortium (W3C) und der Internet Engineering Task Force (IETF) auf, wie z.B. XML, HTTP, DNS-Protokollen und SOAP.

5.6.2 Netzwerkprotokolle

Obligatorisch: IP v4

Aktuell wird im IT-Umfeld der Bundesverwaltung IP v4 (Internet Protocol, RFC 0791, RFC 1700) in Verbindung mit TCP (Transmission Control Protocol, RFC 793) und UDP (User Datagram Protocol, RFC 768) verwendet.

Unter Beobachtung: IP v6

IP v6 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/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. Informationen zum Thema finden sich u.a. im Internet-Angebot der Aktion "Sicherheit im Internet" (www.sicherheit-im-internet.de) oder beim Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de).

Obligatorisch: DNS

Seit Mitte der 1980er Jahre sind Domain Name Services (DNS, RFC 1034, RFC 1035, RFC 1591) 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.

5.6.3 Anwendungsprotokolle

Die Anbindung von sicherheitsbezogenen Infrastrukturkomponenten (z.B. Verzeichnisdienste für Zertifikate, Sperrlisten usw.) wird in Kapitel 6.4.2 behandelt.

Obligatorisch: File Transfer Protocol (FTP)

Für die Dateiübertragung gilt das File Transfer Protocol (FTP, RFC 959, RFC 1123, RFC 2228, RFC 2640) als Standard. FTP ist mit der älteste Internet-Dienst. 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. Im Gegensatz zu HTTP sieht FTP den Wiederstart und die Wiederherstellung bei einer Unterbrechung vor.

Obligatorisch: HTTP v1.0

Für die Kommunikation zwischen Client und Web-Server soll HTTP v1.0 (RFC 1945) eingesetzt werden. Web-Server sollen sowohl HTTP v1.0 als auch die Version 1.1 (RFC 2616) unterstützen. Beim Einsatz von HTTP Session Management und Cookies soll der Standard HTTP State Management Mechanism (RFC 2965) befolgt werden.

Obligatorisch: SMTP/MIME

Für den E-Mail-Transport werden E-Mail-Protokolle vorausgesetzt, die den Spezifikationen von SMTP/MIME für den Nachrichten-Austausch entsprechen (RFC 821, RFC 822, RFC 2045, RFC 2046, RFC 2047, RFC 2048, RFC 2049). E-Mail-Anhänge sollen dabei den Dateiformaten entsprechen, die im Kapitel 5.2 definiert wurden.

Obligatorisch: POP3/IMAP

In Ausnahmefällen kann es vorkommen, dass elektronische Postfächer angeboten werden müssen. Dazu sollen POP3 oder IMAP als weit verbreitete Standards eingesetzt werden.

5.6.4 Verzeichnisdienste

Obligatorisch: LDAP v3

LDAP v3 (Lightweighted Directory Access Protocol, RFC 2251) 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: UDDI v1.0

Das Projekt UDDI (Universal Description, Discovery and Integration, www.uddi.org) ist eine XML-basierte Technologie von Unternehmen aus allen Wirtschaftszweigen mit dem Ziel, Web Services zu publizieren, strukturiert zu verwalten und dem Nutzer verfügbar zu machen. UDDI setzt auf Standards des World Wide Web Consortium (W3C) und der Internet Engineering Task Force (IETF) auf, wie z.B. XML, HTTP, DNS-Protokollen und SOAP.

Directory Services Markup Language (DSML, www.oasis-open.org) ist eine Definition in XML, mit der auf Verzeichnisdienste zugegriffen werden kann. Sie ist so entwickelt, dass verschiedene Verzeichnisse zusammen bearbeitet werden können.

5.7 Anbindung an das Backend

In der deutschen Verwaltung werden verschiedene Bestands- oder Legacy-Systeme eingesetzt und mit einer hohen Wahrscheinlichkeit auch weiterhin betrieben werden (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 sogenannte "Legacy-Schnittstellen" oder
- b. Integration über eine eigene Integrationsschicht, in der 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 Unterkapitel skizzieren unterschiedliche Lösungskonzepte, die sich bei den drei genannten Betriebsarten bewährt haben.

5.7.1 Dialogsysteme

Solche Bestandssysteme können mit oder ohne Integrationsschicht in eGovernment-Lösungen der deutschen Verwaltung integriert werden:

- a. mit Integrationsschicht
Neuentwicklung der Oberflächen für eine Darstellung im Browser. Die Verarbeitung der Bestandsdaten soll dann in einer eigenen Integrationsschicht erfolgen.

- b. ohne Integrationsschicht
Umsetzung der vorhandenen Dialoge mittels eines Produktes auf Oberflächen, die in einem Browser ablaufen können.

5.7.2 Stapelverarbeitung

Viele große Kommunikationssysteme verarbeiten ihre Daten in Stapelverarbeitungsprozessen, insbesondere wenn es um die Verarbeitung großer Datenmengen geht. Die Daten werden entweder auf Datenträgern angeliefert oder per File Transfer übermittelt.

Empfohlen: Extensible Markup Language (XML)

Bei dieser Betriebsart soll in Zukunft auch die Übermittlung der Daten über XML-Dokumente unterstützt werden, siehe Kapitel 5.4 Datenintegration. Dies eröffnet neue Möglichkeiten und macht die Schnittstellen flexibler.

5.7.3 Programm-Programm-Kommunikation

Im Bereich der Bundesverwaltungen existieren weit verbreitete Schnittstellen, wie zum Beispiel die in Kapitel 7.3 beschriebene F15-Schnittstelle. Solche weit verbreiteten Schnittstellen sollten angewendet und modernisiert werden.

Empfohlen: Extensible Markup Language (XML)

Für die Umstellung derartiger noch auf proprietären Protokollen basierender Verarbeitungsschnittstellen zu modernen Technologien hat sich der Informationsaustausch über XML-Dokumente etabliert. Mittlerweile bieten viele Hersteller die erforderlichen Schnittstellen zur Konversion der Daten in XML-Formate an, so dass sich der Entwicklungsaufwand reduziert und gegebenenfalls die Entwicklung einer eigenständigen Connector-Funktionalität entfallen kann.

Empfohlen: J2EE Connectors, Java Message Service

Um eine nahtlose Integration in die J2EE-Plattform zu gewährleisten wird empfohlen die Integration über J2EE-Connectors oder den Java Message Service zu realisieren.

Empfohlen: Web Services

Für die Übertragung der Daten bieten sich vor allem Web Services an.

Auch in der Industrie sind manche Standards sehr weit verbreitet. Sie sollten weiter angewendet und modernisiert werden. Als Beispiel:

Empfohlen: UN/EDIFACT

Die vorwiegend im B2B-Umfeld verbreitete Methode des elektronischen Datenaustauschs (EDI) ist weiterhin möglich. Der internationale Standard für den elektronischen Datenaustausch ist seit 1987 „UN Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT)“. Dieser Standard ist bei dem Aufbau von EDI-Verbindungen einzuhalten, sofern nicht auf moderne Technologie nach SAGA umgestellt werden kann.

6 Standards für Datensicherheit

Ein wesentlicher Aspekt für die erfolgreiche Umsetzung und Durchführung von Dienstleistungen im Rahmen von BundOnline 2005 ist die Gewährleistung der Datensicherheit. Datensicherheit repräsentiert und fördert die vertrauenswürdige und sichere Kommunikation von Bürgern, Behörden und Wirtschaft.

Der eGovernment-Architekturbaukasten (siehe Kapitel 4) identifiziert Datensicherheit als eine durchgängige Komponente, die je nach Bedarf bzw. Anforderung in jedem Element und jeder Säule des Baukastens durch entsprechende Verfahren, Methoden und Datenformate unterstützt werden kann. Der Einsatz der technischen Mittel muss so gestaltet werden, dass Vertrauen zwischen den kommunizierenden Instanzen gebildet wird, der Grundschutz gewährleistet ist und die klassischen Schutzziele erfüllt werden.

Da die Relevanz von Sicherheitsmaßnahmen in den letzten Jahren durch die zunehmende Nutzung des Internets extrem gestiegen ist, kann man auch einen Anstieg von Normungsbestrebungen in diesem Bereich verzeichnen. So ist eine Vielzahl von Sicherheitsstandards, -richtlinien und -empfehlungen entstanden.

Dieses Kapitel stellt die relevanten Sicherheitsstandards und -empfehlungen für eGovernment-Dienstleistungen vor.

6.1 Ziele und Prinzipien der Datensicherheit

Die vorgestellten Standards für Datensicherheit helfen zu ermitteln, ob für eine Dienstleistung ein Schutzbedarf vorliegt oder nicht. Nur wenn Schutzbedarf ermittelt wurde, müssen auch Schutzmaßnahmen ergriffen werden.

6.1.1 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.
- b. *Integrität* – Schutz vor Manipulation:
Daten können nicht unautorisiert verändert oder zerstört werden.
- c. *Authentizität* – Schutz vor gefälschter Identität/Herkunft:
Es wird sichergestellt, dass die Identität einer Entität bzw. Ressource (z.B. Mensch, Prozess, System, Dokument, Information) die ist, die sie zu sein vorgibt.

d. *Verfügbarkeit* – Schutz vor Ausfall der IT-Systeme:

Die Eigenschaft einer Entität bzw. Ressource ist zugänglich bzw. nutzbar, wenn es durch eine autorisierte Entität gewünscht wird.

Die Verschlüsselung von Informationen (Kryptographie) ist ein wichtiges Hilfsmittel bei der Sicherung der Vertraulichkeit, Integrität und Authentizität.

Hohe Verfügbarkeit wird durch Vielfalt, Verteiltheit und Fehlertoleranz erreicht.

6.1.2 Schutzbedarf

Der Schutzbedarf muss für jede IT-Anwendung ermittelt werden. Er orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen IT-Anwendung verbunden sind.

Die Ermittlung des Schutzbedarfs wird im IT-Grundschutzhandbuch (Kapitel 2.2 Schutzbedarfsfeststellung, www.it-grundschutzhandbuch.de) erläutert und im E-Government-Handbuch (Modul: Phasenplan E-Government – Phase 3 „Analyse“, www.e-government-handbuch.de) in Anlehnung an das IT-Grundschutzhandbuch in vier Kategorien unterteilt:

Kategorie	Schadensauswirkung
„kein“	Ein besonderer Schutz ist nicht notwendig, da keine Schadensauswirkungen zu erwarten sind.
„niedrig bis mittel“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Abbildung 6-1: Schutzbedarfskategorien

Um Anwendungen sicherheitstechnisch zu bewerten, kann jedem Schutzziel eine Schutzbedarfskategorie zugeordnet werden. Beispiele für die Schutzbedarfsfeststellung findet man im E-Government-Handbuch (Modul: Phasenplan E-Government – Phase 3 „Analyse“).

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 vom Bundesbeauftragten für den Datenschutz bezüglich Gefährdungen und Maßnahmeempfehlungen findet man in dem Vorschlag für ein Datenschutzkapitel zum IT-Grundschutzhandbuch des BSI

(<http://www.bfd.bund.de/technik/DS-KAP/35.htm>); zukünftig (voraussichtlich 1. Quartal 2003) wird auch das E-Government-Handbuch um ein Datenschutzkapitel ergänzt.

6.1.3 Strukturmodell für Datensicherheit

Um Sicherheitsstandards einfacher zu verstehen und anwenden zu können, wurde der eGovernment-Architekturbaukasten aus Kapitel 4 sicherheitsspezifisch in einem Strukturmodell (siehe Abbildung 6-2) verfeinert.

Das Strukturmodell ist kein Schichtenmodell, sondern veranschaulicht verschiedene Spezifikationsprozesse zum Erreichen der gewünschten Sicherheitsziele. Es dient der Verständnisbildung für die Komplexität von IT-Sicherheit.

Ein Datensicherheitsstandard umfasst im allgemeinen mehr als eine Strukturebene, daher wird auf eine gezielte Einordnung verzichtet. Jeder Standard kann jedoch aus Sicht der einzelnen Strukturebenen betrachtet werden.

Das Strukturmodell und die aufgeführten Datensicherheitsstandards entbinden nicht von der eingehenden Analyse der Fachanwendung hinsichtlich Gesetzeskonformität und der Einhaltung der Datenschutzbestimmungen durch die entsprechenden Spezialisten sowie von der Überprüfung und Einhaltung des Sicherheitsniveaus in allen Instanzen und Prozessen der Kommunikationskette. Eine anwendungsspezifische Risikoanalyse, die Schutzbedarfsfeststellung sowie ein Sicherheitskonzept sollen erstellt werden.

Schutzziele, Schutzbedarf und Anwendungsfälle (siehe Kapitel 4) definieren die Zielsetzung von Sicherheitsmaßnahmen.

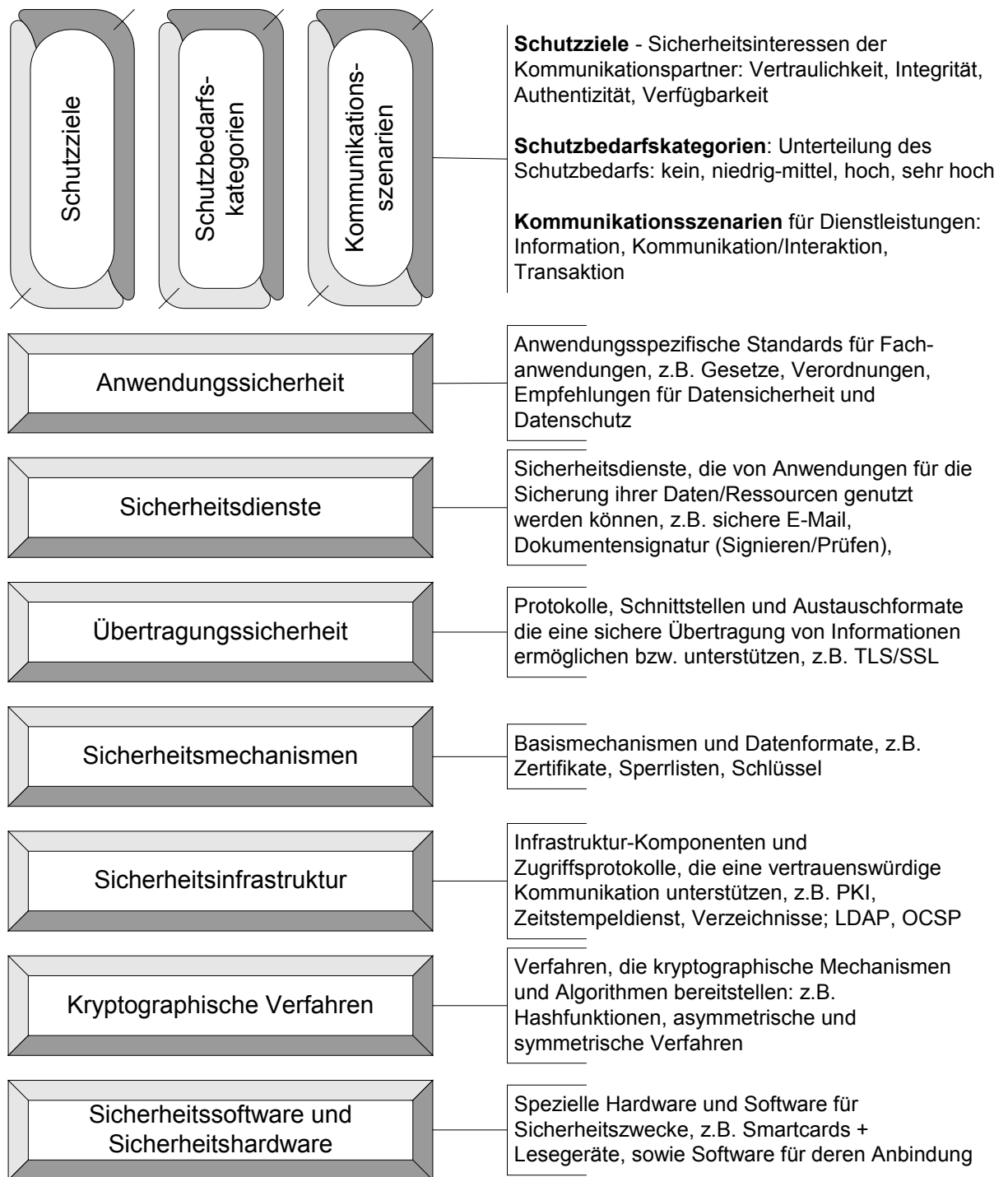


Abbildung 6-2: Strukturmodell für Sicherheitsstandards

6.2 Sicherheitsstandards für die Ermittlung des Schutzbedarfs

Generell sind die Gesetze und Beschlüsse des Bundes als obligatorisch anzusehen. Diese werden durch Empfehlungen und Anleitungen für die IT-Sicherheit ergänzt.

Für die Ermittlung des Schutzbedarfs sollen die nachfolgend aufgeführten Empfehlungen und Anleitungen des BSI und KoopA verwendet werden. Sofern ein Schutzbedarf für die IT-Anwendung bzw. Komponente ermittelt wurde, ist die Anwendung dieser Empfehlungen und Anleitungen obligatorisch.

Obligatorisch: BSI, IT-Grundschutzhandbuch

Die Anwendung des IT-Grundschutzhandbuchs des BSI (Handbuch zur Erstellung von IT-Sicherheitsrichtlinien für niedrigen und mittleren Sicherheitsbedarf, siehe www.it-grundschutzhandbuch.de) wird gefordert. Mit Hilfe des IT-Grundschutzhandbuchs lassen sich IT-Sicherheitskonzepte einfach und arbeitsökonomisch realisieren. Die Struktur des IT-Grundschutzhandbuchs unterstützt eine komponentenorientierte Arbeitsweise.

Empfohlen: KoopA, Handlungsleitfaden für die Einführung der elektronischen Signatur und der Verschlüsselung in der Verwaltung

Der Handlungsleitfaden für die Einführung der elektronischen Signatur und der Verschlüsselung in der Verwaltung des KoopA ADV (www.koopa.de) soll dem Ziel dienen, die Lösung kryptographischer Problemstellungen für ausgewählte Projekte in der öffentlichen Verwaltung zu 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 des BSI (www.e-government-handbuch.de) wurde zur Unterstützung der Initiative BundOnline 2005 erstellt. Das Handbuch umfasst Empfehlungen zur Organisation und zum IT-Einsatz im eGovernment. Insbesondere werden auch sicherheitstechnische Empfehlungen zur Verfügung gestellt.

6.3 Standards für bestimmte Anwendungsfälle

Um eine anwendungsnahe Zuordnung von Sicherheitsstandards zu ermöglichen, werden häufige Anwendungsfälle aus sicherheitsspezifischer Sicht formuliert (siehe Abbildung 6-3 und auch Kapitel 4).

	Information	Kommunikation/ Interaktion	Transaktion/ Integration
Sichere Übertragung von Web-Inhalten (Integrität und Vertraulichkeit)	▶ SSL/TLS		
Web-Server-Authentizität			
Sicherung von E-Mail-Kommunikation		▶ MTT Version 2 ▶ ISIS-MTT	
Gesicherter Dokumentenaustausch (Authentizität, Integrität und Vertraulichkeit)		▶ MTT Version 2 ▶ ISIS-MTT ▶ XML Signature und XML Encryption	
Transaktionen			▶ OSCI-Transport v1.2
Web Services			▶ WS-Security

Abbildung 6-3: Sicherheitsstandards für bestimmte Anwendungsfälle

6.3.1 Sichere Übertragung von Web-Inhalten und Web-Server-Authentizität

Kommuniziert ein Client mit dem Web-Server einer Behörde, so muss sichergestellt sein, dass es sich tatsächlich um den Server der Behörde handelt (Web-Server Authentizität). Der Abruf von Informationen, d.h. die Übermittlung von Web-Inhalten, die Integrität und/oder Vertraulichkeit erfordern, muss während der Übertragung im Internet gesichert erfolgen.

Obligatorisch: SSL/TLS

Das Protokoll SSL (Secure Sockets Layer) ist ein kryptographisches Protokoll, das die Integrität, Vertraulichkeit und Authentizität im World Wide Web sichert. SSL wurde zum Protokoll TLS (Transport Layer Security) weiterentwickelt (<http://www.ietf.org/rfc/rfc2246.txt>).

SSL/TLS setzen auf TCP/IP auf und sichern Kommunikationsprotokolle für Anwendungen wie z.B. HTTP, FTP, IIOIP etc. in transparenter Art und Weise. SSL/TLS-gesicherte WWW-Seiten werden mit https:// statt mit http:// angesprochen.

Die Verwendung von HTTP über SSL-gesicherte Verbindungen wird oft als HTTPS bezeichnet.

SSL/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.

SSL/TLS bietet folgende kryptographische 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 SSL/TLS ist im KoopA Handlungsleitfaden Kapitel 5.2.2 beschrieben. Die Kombination verschiedener Verfahren wird in SSL/TLS als „Cipher Suite“ bezeichnet. Eine SSL/TLS-Cipher Suite enthält stets vier kryptographische Algorithmen: ein Signaturverfahren, ein Schlüsselaustauschverfahren, ein symmetrisches Verschlüsselungsverfahren sowie eine Hash-Funktion.

Folgende Empfehlungen werden im Handlungsleitfaden des KoopA vorgegeben:

- a. Für symmetrische Verfahren soll eine maximale Schlüssellänge gewählt werden, d.h. derzeit 128 Bit oder 112 Bit 3-DES; von Einfach-DES und RC2 wird abgeraten.
- b. Als Hash-Funktion soll SHA-1 eingesetzt werden.
- c. RSA-Modulo soll mindestens 1024 Bit haben.

6.3.2 Sicherung von E-Mail-Kommunikation

Für das Kommunikationsszenario Kommunikation/Interaktion 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 Kapitel 6.3.3 „Gesicherter Dokumentenaustausch“ behandelt.

Obligatorisch: MTT Version 2/SPHINX/PKI-1-Verwaltung
--

MTT Version 2

Die MTT-Spezifikation Version 2 (www.teletrust.de) ist eine deutsche Entwicklung von TeleTrust e.V.. Der Standard umfasst:

- a. X.509v3-Zertifikate und X.509-CRLv2-Sperrlistenformate,
- b. S/MIME-v3 Dokumentenformat,
- c. PKCS und PKIX-Managementnachrichten.

Dieser Standard wird als obligatorisch eingestuft, da er sowohl die Basis für das Projekt SPHINX als auch für die Verwaltungs-PKI bildet. Zukünftig wird dieser Standard durch ISIS-MTT (siehe unten) abgelöst werden.

SPHINX

Die in SPHINX eingesetzten starken Kryptoverfahren sind Teil der MTT-Spezifikation. Im Pilotversuch "SPHINX – sichere E-Mail" wurde die Ende-zu-Ende-Sicherheit von E-Mail mittels Public-Key-Kryptographie herstellerübergreifend erprobt. Das Gesamtkonzept wurde auf Basis der MailTrust-Spezifikation (MTT Version 2) erstellt und umfasst den zugrunde gelegten Standard für die elektronische Signatur und zur Verschlüsselung sowie die zur Einführung von Sicherheitstechnik notwendigen Infrastrukturmaßnahmen und organisatorischen Regelungen. Aufgrund dieses Konzepts wurde für die beteiligten Behörden und Organisationen eine Sicherheitsinfrastruktur aufgebaut, die es den Teilnehmern ermöglicht, Dokumente sicher auszutauschen.

PKI-1-Verwaltung – Public-Key-Infrastruktur für den Behördenbereich

Aufbauend auf den Erfahrungen des Pilotprojekts SPHINX hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Errichtung einer Public-Key-Infrastruktur (PKI) für den Bereich der Verwaltung (PKI-1-Verwaltung) realisiert. Die Wurzelzertifizierungsstelle (Policy Certification Authority: PCA) der PKI-1-Verwaltung ist zu nutzen. Von Landesbehörden, Kommunen und weiteren öffentlichen Institutionen werden eigene, von der PCA-1-Verwaltung zertifizierte Zertifizierungsstellen betrieben. Für den Einsatz von SPHINX im Kontext der PKI-1-Verwaltung hält das BSI Unterlagen unter www.bsi.de abrufbereit.

Obligatorisch: ISIS-MTT

Die ISIS-MTT-Spezifikation berücksichtigt auf Basis der Grundfunktionen elektronische Signatur, Verschlüsselung und Authentifizierung vielfältige Anwendungsfelder von Verfahren zur Sicherung des elektronischen Geschäftsverkehrs (z.B. Mail-, Datei-, Transaktions- und Zeit-„Sicherheit“).

ISIS-MTT ist eine Delta-Spezifikation, die auf bestehenden, relevanten internationalen Standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ETSI) basiert. Schwerpunkt der Spezifikation sind Aussagen zu Konformitätsanforderungen, die von konformen PKI-Komponenten und -Anwendungen bei der Generierung bzw. Verarbeitung von bestimmten Datenobjekten wie beispielsweise Zertifikaten erfüllt werden müssen.

Der Umfang der ISIS-MTT-Spezifikation wurde bestimmt durch die Zusammenführung und Vereinheitlichung der MailTrust- (Version 2, März 1999, TeleTrust e.V.) und der ISIS-Spezifikation (Industrial Signature Interoperability Specification: Version 1.2, Dezember 1999, T7 e.V.).

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. Die Basis von ISIS-MTT ist eine für alle Hersteller und Anbieter obligatorische Kernspezifikation, die bei Bedarf um optionale Profile ergänzt werden kann. Die bereits vorliegenden Profile „SigG-conforming Systems and Applications“ und „Optional Enhancements to the SigG-Profile“ beschreiben die aktuelle Ausprägung qualifizierter Signaturen in Deutschland.

Aktuelle Versionen der Spezifikation können von den Webseiten www.teletrust.de und www.t7-isis.de geladen werden.

ISIS-MTT wird als obligatorisch eingestuft, da ISIS-MTT der Nachfolger von MTT v2 ist, wobei MTT v2 vollständig in ISIS-MTT integriert wurde. Sobald ISIS-MTT durch geeignete Produkte unterstützt wird (ca. ab 2003), wird ISIS-MTT den MTT v2 Standard ersetzen.

6.3.3 Gesicherter Dokumentenaustausch

Für das Kommunikationsszenario Kommunikation/Interaktion 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 sind die Standards MTTv2 und ISIS-MTT relevant. Für den sicheren Austausch von XML-Dokumenten (z.B. für weiterverarbeitbare Formulare) erlangen die XML-spezifischen Standards XML Signature und XML Encryption zunehmend Relevanz.

Obligatorisch: MTT Version 2/SPHINX/PKI-1-Verwaltung
--

Die MTT-Version-2-Spezifikation (siehe Kapitel 6.3.2 *Sicherung von E-Mail-Kommunikation*) definiert ebenfalls ein interoperables Datenaustauschformat für signierte und verschlüsselte Daten. Insbesondere berücksichtigt MTT die Sicherung

binärer Daten, so dass beliebige Dateien als E-Mail-Anlagen gesichert übertragen werden können.

MTT Version 2, das Projekt SPHINX und die Verwaltungs-PKI unterstützen einen sicheren Ende-zu-Ende Dokumentenaustausch. Zukünftig wird MTTv2 durch ISIS-MTT (siehe Kapitel 6.3.2) abgelöst werden.

Obligatorisch: ISIS-MTT

ISIS-MTT (siehe Kapitel 6.3.2 *Sicherung von E-Mail-Kommunikation*) integriert MTT Version 2 vollständig und wird diesen Standard zukünftig ablösen.

Empfohlen: XML Signature

XML Signature ist ein gemeinsamer Standard von W3C und IETF (W3C, XML-Signature Syntax and Processing, W3C Recommendation und IETF RFC 3275, März 2002, <http://www.ietf.org/rfc/rfc3275.txt>).

Dieser Standard 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 dabei ein oder mehrere Dokumente bzw. Daten unterschiedlicher Art (Bild, Text etc.) umfassen.

Für die Platzierung der XML Signature gibt es drei Möglichkeiten:

- a. Einbettung (enveloped): Die Signatur kann eingebettet sein, d.h. in das signierte Dokument wird das XML-Fragment, das die Signatur darstellt, eingefügt.
- b. Umschlag (enveloping): Die Signatur kann als Umschlag fungieren, d.h. sie wird auf ein Dokument angewandt, auf das innerhalb der Signatur verwiesen wird.
- c. Unabhängigkeit (detached): Die Signatur kann unabhängig vorliegen (detached), d.h. sie wird separat von der Quelle aufbewahrt, entweder in demselben oder in einem anderen XML-Dokument.

Ein zentrales Merkmal von XML Signature ist die Möglichkeit, anstelle des gesamten XML-Dokuments nur bestimmte Teile desselben zu signieren. Es können sowohl asymmetrische Kryptoalgorithmen als auch symmetrische Verfahren eingesetzt werden, die in Abhängigkeit vom Schutzziel gewählt werden müssen.

Diese Flexibilität ermöglicht beispielsweise, die Integrität bestimmter Elemente eines XML-Dokuments zu sichern, während andere Teile verändert werden können: z.B. ein signiertes XML-Formular, das an einen Benutzer geschickt wird. Hier kann der Benutzer bestimmte Felder ausfüllen, ohne dass die Integrität des Dokuments verletzt wird. Dies war in herkömmlichen Signaturen nicht möglich, da immer das ganze Dokument signiert wurde und somit jede Veränderung/Einfügung eine Integritätsverletzung bedeutet hätte.

Folgende Kryptoalgorithmen werden benannt:

- a. Hash-Funktion: SHA1
- b. Kodierung: base64
- c. MAC: HMAC-SHA1 (symmetrische Schlüssel); (HMAC RFC 2104)
- d. Signatur: DSA-SHA1 (DSS); empfohlen zusätzlich RSA-SHA1

Eine Spezialisierung der kryptographischen Präferenzen für bestimmte Kommunikationsszenarien ist noch nicht erfolgt.

Empfohlen: XML Encryption

XML Encryption ist ein W3C Standard, jedoch im Gegensatz zu XML Signature noch kein RFC (XML Encryption Syntax and Processing, W3C Candidate Recommendation, 4. März 2002, <http://www.w3.org/TR/xmlenc-core/>).

XML Encryption stellt ein XML-Schema und ein Verarbeitungsregelwerk (für die Verschlüsselung/Entschlüsselung) bereit, das die Verschlüsselung/Entschlüsselung von ganzen Dokumenten, Dokumentteilen (Dokumentelementen) oder von Elementinhalten unterstützt.

Die Verschlüsselung kann mit einem symmetrischen oder einem asymmetrischen Schlüssel erfolgen.

Folgende Kryptoalgorithmen werden benannt:

- a. Blockverschlüsselung: 3DES, AES
- b. Schlüsseltransport: RSA (RSAES-PKCS1-v1_5 algorithm, RFC 2437)
- c. Schlüsseleinigung: Diffie-Hellman (optional)
- d. Hash-Funktion: SHA1, RIPEMD-160
- e. Kodierung: base64

XML Encryption wird als Ergänzung zu XML Signature empfohlen. Die Akzeptanz dieses Standards ist jedoch noch nicht der von XML Signature gleichwertig.

6.3.4 Transaktionen

Transaktionen umfassen die komplexen, fachbezogenen Geschäftsvorfälle mit einer mehrstufigen Wertschöpfungskette zwischen beteiligten Kommunikationspartnern.

Obligatorisch: OSCI-Transport v1.2

OSCI (Online Service Computer Interface) wurde im Rahmen des Wettbewerbs MEDIA@Komm entworfen. OSCI umfasst eine Menge von Protokollen, die für die

Anforderungen im eGovernment geeignet sind und durch die OSCI-Leitstelle erstellt werden. Zielsetzung ist dabei 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 Geschäftsvorfalldaten zu gefährden, ist für die sichere Umsetzung von Prozessen des eGovernment 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 bzw. akkreditierte elektronische Signaturen nach Bedarf der Anwendung).

6.3.5 Web Services

Die zunehmende Wichtigkeit von XML als Datenaustausch- und Spezifikationsformat auch im Sicherheitsbereich sowie die Einführung von Web Services als integrative Middleware bewirkt eine aktive Standardisierung von XML Sicherheitsstandards in den Gremien des W3C und OASIS. Die Relevanz und der finale Umfang der Entwürfe sind derzeit noch nicht vollständig abschätzbar.

Unter Beobachtung: WS-Security

WS-Security ist ein neuer Industriestandard für Web Services Sicherheit. WS-Security definiert Erweiterungen des SOAP-Protokolls, um Vertraulichkeit, Integrität und Verbindlichkeit der SOAP-Nachrichten für die Sicherung von Web Services bereitzustellen. Unterschiedliche Sicherheitsmodelle und unterschiedliche kryptographische 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 oder verschlüsselte Schlüssel.

WS-Security wird als eine Art Gründungsdokument für Web Services Sicherheit betrachtet, dem zukünftig weitere Dokumente (WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation und WS-Authorization) folgen sollen.

WS-Security wurde gemeinsam von IBM, Microsoft und Verisign entworfen und besitzt daher eine starke Herstellerunterstützung. Die Relevanz dieses Standards kann noch nicht endgültig eingeschätzt werden, könnte sich jedoch als wesentlich für die SOAP-Kommunikation der zukünftig eingesetzten Web Services erweisen.

6.4 Übergreifende Datensicherheitsstandards

Übergreifende Sicherheitsstandards umfassen die Standards, die nicht bestimmten Anwendungsfällen bzw. Kommunikationsszenarien zuzuordnen sind.

	Information	Kommunikation/ Interaktion	Transaktion/ Integration
Anbindung Sicherheitsinfrastruktur		▶ ISIS-MTT	
Anbindung Smartcards	▶ ISO/IEC 7816		
Kryptoalgorithmen für die elektronische Signatur	▶ Veröffentlichung durch RegTP ▶ (Hash-Funktionen: RIPEMD-160, SHA-1; Signaturalgorithmen: RSA, DSA, DSA-Varianten)		
Symmetrische Kryptoalgorithmen	▶ Triple-DES, IDEA, AES		

Abbildung 6-4: Übergreifende Sicherheitsstandards

6.4.1 Authentisierung

Um das Schutzziel Authentizität zu gewährleisten, ist die Identitätsfeststellung und Authentisierung von Kommunikationspartnern für bestimmte eGovernment-Anwendungen erforderlich. Verschiedene Mechanismen können für die Authentisierung verwendet werden, z.B. Nutzerkennung/Passwort, PIN/TAN oder Zertifikate. Die sicherheitstechnische Betrachtung der verschiedenen Authentisierungsmöglichkeiten wird zukünftig durch ein separates Modul des E-Government-Handbuchs behandelt (voraussichtlich Ende 2002).

6.4.2 Anbindung Sicherheitsinfrastruktur

Die Sicherheitsinfrastruktur umfasst Verzeichnis-, Zertifizierungs- und Zeitstempelkomponenten, die die Verteilung und Handhabung von Zertifikaten, Sperrlisten und Zeitstempeln sowohl für E-Mail als auch für Web-Umgebungen unterstützen. Der Zugang zu diesen Komponenten erfolgt durch operationale Protokolle.

Obligatorisch: ISIS-MTT

ISIS-MTT (siehe Kapitel 6.3.2 *Sicherung von E-Mail-Kommunikation*) beschreibt im Teil 4 „Operational Protocols“ Protokolle bzw. Profile für die Anbindung von Sicherheitsinfrastrukturen. Diese umfassen den Zugang zu Verzeichnissen mittels LDAP V.3, Online Certificate Status Protocol (OCSP), FTP und HTTP sowie das Time Stamp Protocol (TSP).

6.4.3 Anbindung Smartcards

Die Integration von Smartcards, Smartcard-Lesern und deren Treiberarchitekturen bzw. von kompletten, multifunktionalen „Smartcard/Leser Bundles“ ist für die Client-Infrastruktur unter anderem für den Einsatz von qualifizierten elektronischen Signaturen erforderlich.

Die Initiative D21 (www.initiaved21.de) bearbeitet diese Thematik in der Arbeitsgruppe 5 – Projekt Smartcards. Die Ergebnisse dieser Projektgruppe werden die aufgeführten Standards für die Anbindung von Smartcards ergänzen.

Obligatorisch: ISO/IEC 7816

Smartcards (Chipkarten) müssen der Norm ISO/IEC 7816 entsprechen. Komponenten, die die universelle Krypto-Schnittstelle „Cryptographic Token Interface (Cryptoki)“ unterstützen, müssen Konformität zu ISIS-MTT Teil 7 (Cryptographic Token Interface) aufweisen.

6.4.4 Kryptoalgorithmen für die elektronische Signatur

Die Sicherheit einer elektronischen Signatur hängt primär von der Stärke der zugrunde liegenden Kryptoalgorithmen ab.

Obligatorisch: Kryptoalgorithmen nach RegTP für die elektronische Signatur
--

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) veröffentlicht im Bundesanzeiger jährlich die geeigneten Kryptoalgorithmen in Erfüllung der Anforderungen nach SigG und SigV für die kommenden 6 Jahre (www.regtp.de). Das BSI kann die Eignung weiterer Verfahren feststellen.

Eine elektronische Signatur im Sinne des Gesetzes umfasst die folgenden Kryptoalgorithmen:

- a. Ein Algorithmus zum Hashen von Daten (eine Hash-Funktion), der die zu signierenden Daten auf einen Hash-Wert, d.h. eine Bitfolge fester Länge, reduziert. Signiert werden dann nicht die Daten selbst, sondern stattdessen jeweils ihr Hash-Wert.
- b. Ein asymmetrisches Signaturverfahren, das aus einem Signier- und einem Verifizieralgorithmus besteht. Das Signaturverfahren hängt ab von einem Schlüsselpaar, bestehend aus einem privaten (d.h. geheimen) Schlüssel zum Signieren (Erzeugen der Signatur) und dem dazugehörigen öffentlichen Schlüssel zum Verifizieren (Prüfen) der Signatur.
- c. Ein Verfahren zur Erzeugung von Schlüsselpaaren für die einzelnen Teilnehmer.

Geeignete Hash-Funktionen

- a. RIPEMD-160
RIPEMD-160 ist eine kryptographische Hash-Funktion, die wie SHA-1 Hash-Werte mit 160 Bit Länge generiert.
- b. SHA-1
SHA-1 (Secure Hash Algorithm) ist eine kryptographische Hash-Funktion, die sehr häufig verwendet wird. SHA-1 verarbeitet Blöcke mit 512 Bit Länge und generiert Hash-Werte mit 160 Bit Länge.

Geeignete Signaturalgorithmen

- a. RSA
RSA wurde von Rivest, Shamir und Adleman entwickelt. Das RSA-Verfahren ist das wichtigste asymmetrische Verfahren, auch Public Key Verfahren genannt. Die Sicherheit basiert auf der Schwierigkeit, große natürliche Zahlen zu faktorisieren. Übliche Längen für den Modulus sind 512, 1024 und 2048 Bit, wobei 512 Bit Schlüssel nicht mehr empfohlen werden.
- b. DSA
Der Digital Signature Algorithm (DSA) ist das Signaturverfahren, das im amerikanischen Digital Signature Standard (DSS) 1991 entwickelt und spezifiziert wurde. DSA ist ein reiner Signaturalgorithmus (im Gegensatz dazu ermöglicht RSA sowohl die elektronische Signatur als auch den Schlüsselaustausch). Die US-Regierung hat DSS patentiert, die Benutzung ist jedoch frei.

c. DSA-Varianten basierend auf elliptischen Kurven (EC-DSA, EC-KDSA, EC-GDSA, Nyberg-Rueppel-Signaturen).

Die Eignung bzw. Ausprägung der anzuwendenden Algorithmen kann durch die geltenden Standards beeinflusst werden, z.B. spezifiziert ISIS-MTT Teil 6 die für ISIS-MTT gültigen kryptographischen Algorithmen.

6.4.5 Symmetrische Kryptoalgorithmen für die Verschlüsselung

Kryptographische Algorithmen für die Verschlüsselung können auf Daten und/oder Schlüssel angewandt werden, um diese vertraulich zu übermitteln.

Werden symmetrische Verfahren verwendet, so benutzen diese den gleichen geheimen Schlüssel für die Verschlüsselung und Entschlüsselung. Diese Verfahren sind im allgemeinen sehr performant.

RegTP schreibt keine Verschlüsselungsalgorithmen vor, jedoch werden hier die in ISIS-MTT Teil 6 (Cryptographic Algorithms) festgelegten Algorithmen übernommen. Im Zweifelsfalle besitzen die Spezifikationen im ISIS-MTT-Standard Gültigkeit. Für die Ausprägung (Mode/Padding) des jeweiligen Algorithmus' wird auf ISIS-MTT Teil 6 verwiesen.

Obligatorisch: Triple-DES

Triple-DES, auch als 3DES bezeichnet, ist eine dreifache DES (Data Encryption Algorithm) Variante, d.h. ein symmetrischer Verschlüsselungsalgorithmus mit 168 Bit effektiver Schlüssellänge. 3DES benutzt drei DES-Schlüssel mit je 56 Bit. Das Verfahren gilt als sicher, ist aber nicht besonders performant.

Obligatorisch: IDEA

IDEA (International Data Encryption Algorithm) wurde in Europa entwickelt und arbeitet mit einer Schlüssellänge von 128 Bit.

7 Basiskomponenten und Kompetenzzentren

Die Realisierung der im Rahmen von BundOnline 2005 identifizierten ca. 400 internetfähigen Dienstleistungen wird durch sogenannte **Basiskomponenten** unterstützt. Die Basiskomponenten bieten zentral technische Funktionalitäten an, die durch unterschiedliche Dienstleistungen und Behörden genutzt werden können. Sie liefern Technologieplattformen, die – einmal entwickelt – teils identisch oder bedarfsgerecht konfiguriert zur breiten Anwendung in der Bundesverwaltung kommen.

Als Ergänzung zu den Basiskomponenten wurden sogenannte **Kompetenzzentren** eingerichtet. Die Aufgabe der Kompetenzzentren besteht vornehmlich in der Begleitung der Behörden bei der Einführung der entsprechenden Basiskomponenten.

7.1 Basiskomponenten

Die Basiskomponenten stellen Funktionalitätsblöcke zur Verfügung, die Bestandteil sehr vieler Dienstleistungen sind und als Dienste oder Module in die eGovernment-Anwendungen eingebunden werden.

Die Basiskomponenten unterscheiden sich hinsichtlich ihres Entwicklungsstandes: Während die Basiskomponente „Portal www.bund.de“ in einer ersten Version bereits im 1. Quartal 2001 in Betrieb genommen wurde, befindet sich die Basiskomponente „Call Center“ derzeit noch im Stadium der Bedarfsanalyse.

Die Basiskomponenten werden in mehreren Stufen realisiert. Somit werden im Laufe der Zeit immer wieder neue Versionen der Basiskomponenten mit jeweils erweitertem Funktionsumfang zur Verfügung gestellt.

Die als obligatorisch gekennzeichneten Basiskomponenten sind bei der Realisierung von eGovernment-Anwendungen grundsätzlich einzusetzen. Die vorübergehende Nutzung alternativer Realisierungswege für durch die Basiskomponenten realisierte Funktionalitätsblöcke soll nur in begründeten Ausnahmefällen erfolgen, wenn dadurch nachträgliche Migrationskosten vermieden werden können.

Obligatorisch: Basiskomponente Zahlungsverkehrsplattform („ePayment“)

Die Realisierung zahlreicher Online-Dienstleistungen setzt die Möglichkeit voraus, Gebühren für kostenpflichtige Leistungen der Verwaltung auf elektronischem Weg einzuziehen bzw. begleichen zu können. Auf diese Weise können bei der Digitalisierung von Verwaltungsdienstleistungen die Effizienzvorteile elektronischer Zahlungsvorgänge ausgeschöpft werden.

Die **Basiskomponente Zahlungsverkehrsplattform** ist ein ePayment-Service, der in unterschiedlichste eGovernment-Verfahren eingebunden werden kann. Durch die

zentrale Bereitstellung sollen vielfältige Eigenentwicklungen vermieden und ein kostengünstiger Betrieb gewährleistet werden.

Die notwendige Anbindung an das Haushalts-, Kassen- und Rechnungswesen des Bundes (HKR) ist Bestandteil der Zahlungsverkehrsplattform und muss somit nicht von jedem eShop separat realisiert werden. Als Kernfunktionalitäten soll die Zahlungsverkehrsplattform

- a. einen Service zum Inkasso der Geldbeträge anbieten,
- b. den Einzug der Beträge sicherstellen,
- c. den Erfolg oder auch Misserfolg der Transaktion mitteilen und
- d. die Einnahmen dem HKR-System zur Verbuchung übergeben.

Empfohlen: Basiskomponente Datensicherheit („Virtuelle Poststelle“)

Die **Basiskomponente Datensicherheit** („Virtuelle Poststelle“) dient der Abwicklung einer sicheren, nachvollziehbaren und vertraulichen Kommunikation zwischen Behörden und verwaltungsexternen Kommunikationspartnern im Rahmen von eGovernment-Dienstleistungen. Sie soll u.a. zu einer wesentlichen Entlastung aller Beteiligten von Routinearbeiten führen, die mit einer durch elektronische Signaturen und Verschlüsselungen gesicherten Kommunikation häufig noch verbunden sind.

Bei Nutzung elektronischer Kommunikationskanäle soll die Virtuelle Poststelle weitgehend automatisch als zentrales Security-Gateway fungieren und die Funktionen Authentifizierung, Signaturprüfung und Signaturerstellung sowie Ent- und Verschlüsselung bereitstellen. Obwohl die virtuelle Poststelle grundsätzlich als zentraler Dienstleister (zentrale Anlaufstelle) in einer Behörde fungiert und in erster Linie eine indirekte Kommunikation mit der Behörde unterstützt, wird im Bereich der E-Mail-Kommunikation daneben auch weiterhin eine direkte sichere Kommunikation mit einzelnen Sachbearbeitern möglich sein.

Als Input bzw. Output der virtuellen Poststelle werden sowohl E-Mails, E-Mail-Attachments als auch Datenstrukturen für eine Web-Schnittstelle angesehen. Sie wird bei Bedarf darüber hinaus weitere Sicherheitsprüfungen zur Verfügung stellen.

Solange die Basiskomponente Datensicherheit nicht verfügbar ist, berät das Kompetenzzentrum Datensicherheit, wie Übergangslösungen etabliert werden können, die einen späteren Wechsel zur Basiskomponente vereinfachen.

Obligatorisch: Basiskomponente Portal www.bund.de
--

Die **Basiskomponente Portal www.bund.de** ist der zentrale Einstiegspunkt zu den Online-Dienstleistungen und Informationsangeboten des Bundes. Somit fällt dem Portal die Aufgabe zu, den Bürgerinnen und Bürgern, Wirtschaft und Verwaltung die schnelle und komfortable Erschließung der elektronischen Dienstleistungsangebote

des Bundes zu ermöglichen. Dabei übernimmt das Portal die Funktion eines Information Guides, der adressatenspezifische Informationen und Dienstleistungen bereitstellt und damit die Kommunikationsmöglichkeiten mit der Bundesverwaltung nachhaltig verbessert.

Die Startseite von www.bund.de wurde in Anlehnung an kommerzielle Seiten mit Suchfenstern und einem Themenkatalog gestaltet. Behördendaten, darunter Adressverzeichnis werden über die verteilte Redaktion durch die Behörden selbst im Portal gepflegt.

Obligatorisch: Basiskomponente Formularserver

Die **Basiskomponente Formularserver** ist ein Kataster der Formulare des Bundes für die Zielgruppen Bürger, Wirtschaft und Verwaltung und wird über das Portal www.bund.de als Formular-Center zur Verfügung gestellt. Formulare können über das verteilte Content Management System des Portals dezentral eingestellt bzw. verlinkt werden.

Zielsetzung ist es, die Kommunikation zwischen Verwaltung und Bürgern teilweise oder vollständig in digitaler Form zu ermöglichen. Durch den Einsatz digitaler Formulare sowie die digitale Übertragung von Formularen über das Internet können laufende Kosten reduziert und die Verarbeitung auf beiden Seiten vereinfacht und beschleunigt werden.

Mittelfristig wird die vollständige und medienbruchfreie Bearbeitung der jeweiligen Formularinhalte über das Internet angestrebt.

Empfohlen: Basiskomponente Content Management System
--

Die **Basiskomponente Content Management System (CMS)** wird allen Behörden der Bundesverwaltung für ihre Internet-, Intranet- sowie Extranet-Anwendungen bereitgestellt. Das System wird unter Berücksichtigung der vom Presse- und Informationsamt der Bundesregierung veröffentlichten Gestaltungsrichtlinien (Internet-Styleguide der Bundesregierung) sowie der behindertenfreundlichen Vorgaben für das „barrierefreie“ Internet erstellt.

Die Basiskomponente CMS wird auf der Basis des Content Management Systems CAP 4.0 der Firma CoreMedia aufgebaut und gezielt auf die Anforderungen der Behördenlandschaft abgestimmt. Das vorkonfigurierte System kann den einzelnen Bundesbehörden sowohl zentral (durch Hosting) als auch dezentral (durch die spätere Weitergabe der angepassten Applikation) zur Verfügung gestellt werden.

Unter Beobachtung: Basiskomponente Call Center
--

Bei komplexen eGovernment-Dienstleistungen reichen häufig die üblichen Hilfestellungen zur Bedienung (Informationsseiten, Hilfe-Assistenten etc.) nicht aus. In diesen Fällen kann ein Call Center eine zusätzliche wertvolle Unterstützung für die Nutzer darstellen. Derzeit wird der Bedarf der potenziellen Nutzer an Call-Center-Leistungen erhoben.

7.2 Kompetenzzentren

Zur Unterstützung der eGovernment-Initiative BundOnline 2005 wurden vier Kompetenzzentren eingerichtet. Vorrangige Aufgabe der Kompetenzzentren ist die Bereitstellung von Know-how für die dezentrale Umsetzung der Online-Dienstleistungen. Dies umfasst insbesondere die Beratung bei der Implementierung der Basiskomponenten und der Online-Dienstleistungen.

Das **Kompetenzzentrum Datensicherheit** im Bundesamt für Sicherheit in der Informationstechnik (BSI) berät die Behörden in Fragen der Sicherheit von eGovernment-Verfahren und beim Einsatz der digitalen Signatur. Für die Übertragung sensibler Daten über das Internet gilt es, vertrauenswürdige Infrastrukturen zu schaffen, Verwaltungsprozesse neu zu strukturieren und vorhandene Anwendungen der Behörden mit geeigneten Sicherheitslösungen auszustatten. Hierdurch wird eine reibungslose, rechtsverbindliche und vertrauliche Online-Kommunikation der externen Umwelt mit der Bundesverwaltung ermöglicht und eine sichere innerbehördliche Kommunikation gewährleistet.

Das **Kompetenzzentrum Zahlungsverkehrsplattform** wird für die gesamte Bundesverwaltung Methoden und Konzepte zum Aufbau und für den Betrieb von ePayment-Anwendungen zur Verfügung stellen. Zusätzlich wird es technisches Know-how zur Anbindung von eShops an die zentrale Zahlungsverkehrsplattform sammeln und aufbereiten, Beratungen durchführen sowie Markt-Know-how für andere ePayment-Systeme (Anbieter, Produkte, Services, Preismodelle, Trends etc.) bereitstellen. Das Kompetenzzentrum Zahlungsverkehrsplattform wird seine Arbeit mit der Bereitstellung der ersten Stufe der Zahlungsverkehrsplattform im Frühjahr 2003 aufnehmen.

Das **Kompetenzzentrum Content Management System (CMS)** berät Behörden der Bundesverwaltung, die für die Online-Bereitstellung ihrer Dienstleistungen die Basiskomponente CMS nutzen wollen, bei der Implementierung. Zudem wirkt es konzeptionell an der bedarfsgerechten Realisierung der Basiskomponente CMS mit und wird nach der Fertigstellung der Basiskomponente CMS als Ansprechpartner für Optimierungsvorschläge und individuelle Bedarfsanpassung zur Verfügung stehen.

Das **Kompetenzzentrum Vorgangsbearbeitung, Prozesse und Organisation** wird die Behörden dabei unterstützen, vor der Realisierung von Online-Dienstleistungen eine Optimierung der betroffenen Geschäftsprozesse durchzuführen. Darin wird eine

zwingende organisatorische Voraussetzung gesehen, um die vorhandenen Optimierungspotenziale nutzen zu können. Die Hauptaufgabe des Kompetenzzentrums besteht darin, die Bundesbehörden zur eigenverantwortlichen und wirtschaftlichen Umsetzung ihrer Dienstleistungen zu befähigen. Den Bundesbehörden soll die fachliche und methodische Unterstützung zur Anpassung der Aufbau- und Ablauforganisation sowie der Verwaltungsabläufe angeboten werden.

8 Anhang

8.1 Tabellarische Übersicht der Standards für die IT-Architektur

8.1.1 Präsentation

8.1.1.1 Informationsverarbeitung – Computer/Web

Kap.	Komponente	Technische Spezifikation
5.2.1	Behindertengerechte Darstellung	<ul style="list-style-type: none"> ▶ Barrierefreie Informationstechnik Verordnung BITV
5.2.1	Austauschformate für Hypertext	<ul style="list-style-type: none"> ▶ HTML v3.2, http://www.w3.org/TR/REC-html32 ▶ HTML v4.01, http://www.w3.org/TR/html401/ ▶ XHTML v1.0, http://www.w3.org/TR/xhtml1/
5.2.1	Style Sheets	<ul style="list-style-type: none"> ▶ CSS2 (Cascading Style Sheets) als Ergänzungssprache zu HTML, http://www.w3.org/TR/REC-CSS2 ▶ XSL v1.0, http://www.w3.org/TR/xsl/
5.2.1	Zeichensätze	<ul style="list-style-type: none"> ▶ ISO 10646-1:2000/Unicode V3.0 in UTF 8 bzw. UTF 16 Codierung, www.unicode.org ▶ ISO 8859-1 ▶ ISO 8859-15
5.2.1	Statische und dynamische, passive und aktive Inhalte	<ul style="list-style-type: none"> ▶ HTML-Format ▶ ECMA-262 – ECMAScript Language Specification ▶ Servlets und Java Server Pages oder XSL
5.2.1	Dateitypen und Typerkennung für Textdokumente	<ul style="list-style-type: none"> ▶ Text (.txt) ▶ Hypertext Markup Language (HTML) ▶ Portable Document Format (PDF) Version 4 ▶ Extensible Markup Language (XML) ▶ Portable Document Format (PDF) Version 5 ▶ Multipurpose Internet Mail Extensions (MIME)
5.2.1	Dateitypen für Tabellenkalkulationen	<ul style="list-style-type: none"> ▶ Comma Separated Value (CSV) ▶ Adobe Acrobat als (PDF)-Datei Version 4 ▶ Adobe Acrobat als (PDF)-Datei Version 5

5.2.1	Dateitypen für Präsentationen	<ul style="list-style-type: none"> ▶ Hypertext Markup Language (HTML) ▶ Portable Document Format (PDF) Version 4 ▶ Portable Document Format (PDF) Version 5
5.2.1	Austauschformate für Bilder	<ul style="list-style-type: none"> ▶ Graphics Interchange Format (GIF) ▶ Joint Photographic Experts Group (JPEG) ▶ Portable Network Graphic (PNG) ▶ Tag Image File Format (TIFF) ▶ Enhanced Compressed Wavelet (ECW)
5.2.1	Austauschformate für Geoinformationsdaten (Rasterdaten, Vektordaten)	<ul style="list-style-type: none"> ▶ Geography Markup Language (GML) ▶ Scalable Vector Graphic (SVG) ▶ Vector Markup Language (VML)
5.2.1	Austauschformate für Audio- und Video-Dateien	<ul style="list-style-type: none"> ▶ MPEG-1 Layer 3 (MP3) ▶ Quicktime (.qt, .mov)
5.2.1	Austauschformate für Audio- und Video-Streaming	<ul style="list-style-type: none"> ▶ HTTP als Transportprotokoll ▶ Quicktime (.qt, .mov) ▶ Ogg
5.2.1	Animation	<ul style="list-style-type: none"> ▶ Animated GIF
5.2.1	Datenkompression	<ul style="list-style-type: none"> ▶ ZIP v2.0 ▶ GZIP v4.3 (.gz)

8.1.1.2 Informationsverarbeitung – Mobiltelefon/PDA

Kap.	Komponente	Technische Spezifikation
5.2.2	SMS	<ul style="list-style-type: none"> ▶ Spezifikation, wie definiert vom SMS-Forum, http://www.smsforum.net/doc/public/Spec/
5.2.2	WML 1.x	<ul style="list-style-type: none"> ▶ www.wapform.org
5.2.2	WAP 1.x	<ul style="list-style-type: none"> ▶ Spezifikation wie definiert vom WAP-Forum, www.wapforum.org
5.2.2	XHTML-BASIC	<ul style="list-style-type: none"> ▶ http://www.w3.org/tr/xhtml-basic/

8.1.2 Fachliche Prozess- und Datenmodelle

Kap.	Komponente	Technische Spezifikation
5.3.1	Prozessmodelle	<ul style="list-style-type: none">▶ Rollenmodelle und Flussdiagramme (DIN 66001)▶ UML
5.3.2	Datenmodelle	<ul style="list-style-type: none">▶ Entity Relationship Diagramme▶ Extensible Markup Language Schema Definition 1.0 (XSD)▶ Unified Modeling Language (UML)

8.1.3 Datenintegration

Kap.	Komponente	Technische Spezifikation
5.4.1	Datenbeschreibung	<ul style="list-style-type: none">▶ Extensible Markup Language (XML)▶ Extensible Markup Language Schema Definition 1.0 (XSD)
5.4.2	Datentransformation	<ul style="list-style-type: none">▶ Extensible Stylesheet Language Transformation 1.0 (XSLT)
5.4.3	Zeichensätze	<ul style="list-style-type: none">▶ Die Standards der aus Kapitel 5.2 Präsentation werden verwendet▶ Individuelle Teile des XML-Schemas können im Zeichensatz weiter eingeschränkt werden

8.1.4 Middleware

Kap.	Komponente	Technische Spezifikation
5.5	Middleware Architektur	<ul style="list-style-type: none">▶ J2EE v1.3▶ J2SE▶ Microsoft .NET Framework

8.1.5 Kommunikation

8.1.5.1 Middleware-Protokolle

Kap.	Komponente	Technische Spezifikation
5.6.1	Middleware Protokolle zur Server-Server Kommunikation	<ul style="list-style-type: none">▶ Remote Method Invocation (RMI)▶ SOAP▶ WSDL 1.1 (Web Services Description Language)▶ Extensible Markup Language Schema Definition (XSD)▶ RMI-IIOP
5.6.1	Middleware Protokolle zur Client-Server Kommunikation	<ul style="list-style-type: none">▶ WSDL 1.1 (Web Services Description Language)▶ Extensible Markup Language Schema Definition 1.0 (XSD)▶ SOAP 1.1▶ UDDI 2.0

8.1.5.2 Netzwerkprotokolle

Kap.	Komponente	Technische Spezifikation
5.6.2	Internet Protocol	<ul style="list-style-type: none">▶ IP v4 (RFC 791) mit TCP und UDP▶ IP v6
5.6.2	Name Services/ Naming Policy	<ul style="list-style-type: none">▶ DNS (RFC 1034, RFC 1035, RFC 1591)

8.1.5.3 Anwendungsprotokolle

Kap.	Komponente	Technische Spezifikation
5.6.3	Dateiübertragung	<ul style="list-style-type: none">▶ FTP (RFC 959, RFC 1123, RFC 2228, RFC 2640) File Transfer Protocol▶ HTTP v1.0 (RFC 1945) und v1.1 (RFC 2616)
5.6.3	E-Mail Transport	<ul style="list-style-type: none">▶ E-Mail-Protokolle, die den Spezifikationen von SMTP/MIME für den Nachrichtenaustausch entsprechen▶ POP3/IMAP für elektronische Postfächer

8.1.5.4 Verzeichnisdienste

Kap.	Komponente	Technische Spezifikation
5.6.4	Directory	▶ LDAP V3 (Lightweighted Access Protocol) für den allgemeinen Zugriff auf Adressbuchressourcen (nach X.500) (RFC 2251, 2252, 2253, 2256, 2798, 1777, 1823)
5.6.4	Web Service Request Registry	▶ UDDI v1.0 (Universal Description, Discovery and Integration, www.uddi.org)
5.6.4	Directory Services	▶ DSML V2

8.1.6 Anbindung an das Backend

8.1.6.1 Stapelverarbeitung

Kap.	Komponente	Technische Spezifikation
5.7.2	Stapelverarbeitung	▶ Extensible Markup Language (XML)

8.1.6.2 Programm-Programm-Kommunikation

Kap.	Komponente	Technische Spezifikation
5.7.3	Informationsaustausch	▶ Extensible Markup Language (XML)
5.7.3	J2EE Integration	▶ J2EE Connectors, Java Message Service
5.7.3	Datenaustausch	▶ Web Services
5.7.3	Datenaustausch	▶ UN/EDIFACT

8.2 Tabellarische Übersicht der Standards für Datensicherheit

Kap.	Komponente	Technische Spezifikation
6.2	Sicherheitsstandards für die Ermittlung des Schutzbedarfs	<ul style="list-style-type: none"> ▶ BSI, IT-Grundschutzhandbuch, www.it-grundschutzhandbuch.de ▶ KoopA ADV, "Handlungsleitfaden für die Einführung der elektronische Signatur und der Verschlüsselung" in der Verwaltung, neue Version in Vorbereitung ▶ BSI, Sicheres E-Government: E-Government-Handbuch, www.e-government-handbuch.de
6.3.1	Sichere Übertragung von Web-Inhalten und Web-Server Authentizität	<ul style="list-style-type: none"> ▶ SSL und TLS ▶ TLS: T. Dierks, C. Allen: The TLS Protocol, Version 1.0, Januar 1999, RFC 2246, http://www.ietf.org/rfc/rfc2246.txt
6.3.2	Sicherung von E-Mail Kommunikation	<ul style="list-style-type: none"> ▶ MTT v.2/SPHINX/PKI-1-Verwaltung ▶ TeleTrust: "MailTrust", Version 2, März 1999, www.teletrust.de ▶ BSI: Sphinx Schriftenreihe, Projekt hinsichtlich Verfahren zur digitalen Signatur und zur Verschlüsselung http://www.bsi.de/aufgaben/projekte/sphinx/dokument.htm ▶ ISIS-MTT: T7 & Teletrust; Common ISIS-MTT Specification for PKI Applications, Version 1.0.1, 15. November 2001, http://www.t7-isis.de/ISIS-MTT/isis-mtt.html <ul style="list-style-type: none"> • Part 1: Certificate and CRL Profiles • Part 2: PKI Management, in Bearbeitung • Part 3 Message Formats • Part 4 Operational Protocols (LDAP, OCSP, TSP) • Part 5 Certificate Path Validation • Part 6 Cryptographic Algorithms • Part 7 Cryptographic Token Interface

6.3.3	Gesicherter Dokumentenaustausch	<ul style="list-style-type: none"> ▶ MTT v.2/SPHINX/PKI-1-Verwaltung ▶ ISIS-MTT ▶ XML Signature: IETF und W3C, RFC 3275, XML-Signature Syntax and Processing, W3C Recommendation, 12. Februar 2002, http://www.w3.org/TR/xmlsig-core/ und http://www.ietf.org/rfc/rfc3275.txt ▶ XML Encryption: W3C XML Encryption Syntax and Processing., W3C Candidate Recommendation, 04. 03. 2002, http://www.w3.org/TR/xmlenc-core/
6.3.4	Transaktionen	<ul style="list-style-type: none"> ▶ OSCI-Transport v1.2: OSCI-Leitstelle, Spezifikation, 07.06.2002, www.osci.de
6.3.5	Web Services	<ul style="list-style-type: none"> ▶ WS-Security: IBM, Microsoft, Verisign: Web Services Security (WS-Security), v1.0, 5. April 2002, http://www-106.ibm.com/developerworks/library/ws-secure/
6.4.2	Anbindung Sicherheitsinfrastruktur	<ul style="list-style-type: none"> ▶ ISIS-MTT Teil 4 (LDAP, OCSP, TSP)
6.4.3	Anbindung Smartcards	<ul style="list-style-type: none"> ▶ ISO/IEC 7816: ISO/IEC, Information Technology - "Identification Cards - Integrated Circuit(s) Cards with Contacts" ▶ Initiative D21 Arbeitsgruppe 5
6.4.4	RegTP Kryptoalgorithmen	<ul style="list-style-type: none"> ▶ RegTP, Geeignete Kryptoalgorithmen, http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/03/
6.4.5	Symmetrische Kryptoalgorithmen	<ul style="list-style-type: none"> ▶ Triple-DES: FIPS 46-3, Data Encryption Standard, Oktober 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf ▶ IDEA: International Data Encryption Algorithm ▶ AES: Federal Information Processing Standards (FIPS PUB) 197: Advanced Encryption Standard (AES), November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

8.3 Glossar

AES	Advanced Encryption Standard
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVA	Bundesverwaltungsamt
CEN	Comité Européen de Normalisation
CORBA	Common Object Request Broker Architecture
CRL	Certificate Revocation List
CSS	Cascading Style Sheets Language
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Services
DSA	Digital Signature Algorithm
DSML	Directory Services Markup Language
DSS	Digital Signature Standard
ECW	Enhanced Compressed Wavelet
EDI	Electronic Data Interchange
e-GIF	e-Government Interoperability Framework
EIS	Enterprise Information System
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
GML	Geography Markup Language
GOSIP	Government Open Systems Interconnection Profile
HMAC	Keyed-Hash Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IDA	Interchange of Data between Administrations

IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IIOB	Internet Inter-ORB Protocol
IMKA	Interministerielle Koordinierungsausschuss für die Informationstechnik in der Bundesverwaltung
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
J2EE	Java 2 Enterprise Edition
JAAS	Java Authentication and Authorization Service
JAXP	Java API for XML
JAXR	Java API for XML Registries
JDBC	Java Database Connectivity
JMS	Java Message Service
JTA	Java Transaction API
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern
KoopA	Kooperationsausschuss ADV Bund/Länder/Kommunaler Bereich
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MTT	MailTrusT
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OSCI	Online Services Computer Interface
PCA	Policy Certification Authority
PDA	Personal Digital Assistant
PDF	Portable Document Format
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	IETF Working Group „Public-Key Infrastructure (X.509)“

PNG	Portable Network Graphics
RegTP	Regulierungsbehörde für Telekommunikation und Post
RFC	Request for Comments
RFP	Request for Proposals
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RSA	Rivest, Shamir, Adleman Public Key Encryption
SAGA	Standards und Architekturen für eGovernment-Anwendungen
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
SVG	Scalable Vector Graphic
TCP/IP	Transmission Control Protocol/Internet Protocol
TIF	Tag Image File Format
TLS	Transport Layer Security
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VML	Vector Markup Language
W3C	World-Wide-Web Consortium
WAP	Wireless Application Protocol
WSDL	Web Services Description Language
WWW	World Wide Web
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language
XSD	Extensible Markup Language Schema Definition

XSL Extensible Stylesheet Language
XSLT Extensible Stylesheet Language Transformation