Software- und Kriterienkatalog zu RAfEG*– Referenzarchitektur für E-Government

D. Beer, S. Höhne, G. Rünger, M. Voigt
Fakultät für Informatik
Technische Universität Chemnitz
Straße der Nationen 62, 09111 Chemnitz

E-Mail: dbeer@cs.tu-chemnitz.de, s.hoehne@nhconsult.de
ruenger@cs.tu-chemnitz.de, mvoigt@viosys.com

Zusammenfassung

Das RAfEG-Projekt (Referenzarchitektur für E-Government) hat eine Softwarearchitektur zur Unterstützung der elektronischen Abbildung von öffentlichen Verwaltungsdienstleistungen zum Ziel, wobei insbesondere auch interne Verwaltungsprozessabläufe einbezogen werden. Schwerpunkt ist dabei die Konzeption und Umsetzung einer Referenzimplementierung, die die Erstellung von Anwendungssoftware für eine breite Klasse von E-Government-Anwendungen ermöglicht. Die Architektur als auch die Implementierung selbst ist für heterogene, (räumlich) verteilte Plattformen mit verteilten Prozessabläufen konzipiert. Der vorliegende Informatik-Bericht erstellt dazu einen Systemkatalog, welcher die aktuell in Frage kommenden Systeme, Technologien und Charakteristika mit dem Ziel der Definition und Gewichtung der jeweils zugrunde zu legenden Anforderungskriterien in Form eines Kriterienkataloges zusammenfasst.

*Das diesem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (bmb+f) im Rahmen der Forschungsoffensive „Software Engineering 2006“ unter dem Förderkennzeichen 01 IS C07 B gefördert.

Inhaltsverzeichnis

1 Einleitung

In Deutschland stehen die öffentlichen Verwaltungen vor einer Herausforderung: Trotz stetig abnehmender finanzieller Mittel und Personalabbau steigen die Anforderungen hinsichtlich der Bearbeitungsdauer und –qualität sowie Flexibilität. Die Ursachen sind hier in einem zunehmenden — mit der EU-Osterweiterung deutlich zu spürenden — globalen Standortwettbewerb, einem steigenden Kostendruck durch eine schwach wachsende Wirtschaft und Überalterung sowie einem wachsenden politischen Druck auf die Modernisierung der Verwaltungen zu suchen.

Die Lösung dieser Herausforderung verspricht E-Government, die breite Nutzung von Informationstechnologie zur Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung und der Leistungserstellung. In der ersten Phase der E-Government Realisierung bestand das Ziel in einer möglichst umfassenden Information und teilweise Kommunikation mit dem Bürger (Formularserver, Bürgerinformation, E-Mail). Daneben wurden E-Procurement-Portale geschaffen, welche die Beschaffungsprozesse der Verwaltungen effizienter gestalten.

Das volle Potential des E-Government erschöpft sich hingegen erst mit der — oft erst durch die Informationstechnologie ermöglichten — Optimierung der Verwaltungsprozesse. Dies fordert die öffentliche Verwaltung nicht nur in technischer sondern auch im verstärktem Maße in organisatorischer Sicht. Dies schließt letztlich alle am Verwaltungsprozess beteiligten Partner (Verwaltungen, Unternehmen, Vereine, Bürger, etc.) ein. Voraussetzung dafür ist die Integration verteilter, heterogener Systeme über die organisatorischen Grenzen einer einzelnen Verwaltung hinaus.

Die Herausforderung des RAfEG Verbundprojektes besteht in der Entwicklung einer Referenzsoftwarearchitektur, welche die Erstellung, Anpassung oder Integration von Anwendungssoftware zur Unterstützung solcher organisationsübergreifender, moderner Verwaltungsprozesse in einer standardisierten Form ermöglicht. Dies schließt die Entwicklung eines Modulsystems mit notwendigen Modellen, Methoden, Schnittstellen und Protokollen sowie flexibel einsetzbarer Komponenten prozessunterstützender Vorgangssteuerungssoftware ein. Dabei werden neben den rein fachlichen, aufgabenbezogenen Aspekten insbesondere Sicherheitsaspekte sowie technische und organisatorische Schnittstellen ausführlich betrachtet. Mit Hilfe der in RAfEG festgeschriebenen Standards können auch bisherige E-Government-Insellösungen miteinander technologisch verbunden werden, so dass eine medienbruchfreie, IT-gestützte Ausführung von Verwaltungsabläufen ohne die Kosten einer kompletten Neuentwicklung ermöglicht wird.

Im Vorfeld der Erstellung des dazu notwendigen Software– und Kriterienkataloges erfolgte eine Analyse der realen IuK-technischen Rahmenbedingungen mit dem Ziel, die Realisierungsumgebung für die Softwarearchitektur und eine erste Referenzimplementierung zu ermitteln und die Ergebnisse des Projektes zeitnah in der Praxis umzusetzen. Vorrangiges Ziel war dabei die nahtlose Integration der RAfEG-Systemarchitektur in bestehende IuK-Systemumgebungen unter Nutzung etablierter Standards. Der vorliegende Software– und Kriterienkatalog betrachtet dazu Standards und Softwaresysteme in den Kategorien:

- Bürokommunikationssysteme (BKS),
- Geografische Informationssysteme (GIS),
- Dokumentenmanagementsysteme (DMS),
- Sicherheitssoftware und –komponenten und
- Präsentationskomponenten.

Die folgenden Kapitel geben einen Überblick zu den in den Kategorien betrachteten Systemen, Technologien und Standards. In der Zusammenfassung jedes Kapitels werden die wichtigsten Bewertungskriterien hervorgehoben und — sofern sinnvoll — in Bezug auf deren Gewichtung unter Berücksichtigung typischer Verwaltungsprozesse dargestellt.

In der abschließenden Zusammenfassung wird eine allgemeine Bewertungsmatrix dargestellt, anhand derer die Gewichtung einzelner Bewertungskriterien für die verschiedenen Kategorien deutlich wird.

2 System– und Kriterienkatalog Dokumentenmanagementsysteme

2.1 Einleitung

Das Dokumentenmanagement befasst sich mit der Erfassung/Erstellung, Bearbeitung, Speicherung, Weitergabe und Archivierung von elektronischen Dokumenten. Diese Dokumenten können einerseits nicht-kodierte Informationen (Non Coded Information, NCI, bspw. Bilddateien) und von einer Software interpretierbare Informationen (Coded Information, CI, bspw. ein Text) enthalten.

Dokumentenmanagementsysteme (DMS) sind historisch aus elektronischen Archivsystemen entstanden, welche elektronische Dokumente speicherten. Heute zählen DMS zu den Groupware-Produkten, d. h. sie lassen die gemeinsame Bearbeitung eines Vorganges auf Dokumentenbasis durch mehrere Personen, zu gleichen oder verschiedenen Zeitpunkten, ortsunabhängig und organisationsübergreifend zu. Der Unterschied zu Transaktionssystemen (bspw. ein Buchungssystem) besteht in der Bearbeitung komplexer Vorgänge auf Basis von Dokumenten (vgl. [1], S. 455).

Wesentliches Merkmal von Dokumentenmanagementsystemen ist, dass diese Dokumente in Dokumentengruppen (Containern) zusammenfassen, über ein Konfigurationsmanagement verfügen und Dokumentenobjekten Metainformationen zuordnen (Selfcontained Object) können.

2.2 Grundanforderungen an DMS

DMS müssen den Anwender bei der Erstellung/Erfassung, Änderung, Prüfung, Verteilung, Dokumentenverwendung und Archivierung von Dokumenten unterstützen.

Erstellung/Erfassung CI– (strukturierte Daten) und NCI-Dokumente (unformatierte Daten) müssen von einem DMS erstellt oder erfasst werden können. Neben dem eigentlichen Dokument müssen zusätzliche Informationen erfassbar sein. In der Regel sind dies Dokumententyp, –kategorie, –status, Zugriffs–/Bearbeitungsrechte, Querverweise (auf relevante Dokumente), Notizen und weitere Informationen.

Änderung Zur Bearbeitung eines Dokumentes muss dieses mit Hilfe einer Suchfunktion und anhand diverser Merkmale vom Benutzer auffindbar sein. Die Bearbeitung eines Dokumentes darf nur nach einer entsprechenden Autorisierung des Benutzers und einer Sicherung der Integrität (bspw. einer Sperrung des Dokumentes für Bearbeitungen anderer Benutzer) erfolgen.

Prüfung Nach Bearbeitung eines Dokumentes erfolgt eine Prüfung. Dies kann manuell durch einen entsprechend definierten Benutzer und/oder automatisch durch das DMS erfolgen. Je nach Ergebnis der Prüfung wird der Status des bearbeiteten Dokumentes geändert. Mit Speicherung der neuen Dokumentenversion erfolgt ein entsprechender Eintrag in der Historie. Hier kann auch eine Fristenüberwachung stattfinden, welche Benutzer bei der Erledigung zeitkritischer Vorgänge unterstützt.

Verteilung Nach Freigabe eines Dokumentes wird dieses an definierten Orten in jeweils spezifizierten Formaten anderen Benutzern bereitgestellt. Mitunter werden zu diesem Zeitpunkt Benutzer über die neue Dokumentenversion informiert (Benachrichtigungsfunktion).

Dokumentenverwendung Benutzer des DMS, welche mit Dokumenten arbeiten möchten, diese aber nicht bearbeiten bzw. modifizieren, erhalten über oft umfangreiche Suchfunktionen die Möglichkeit nach relevanten Dokumenten zu suchen. Sie erhalten das entsprechend der Versionierung treffende Dokument. In der Dokumentenverwendung werden alle für die Anwendung irrelevanten Informationen gegenüber dem Benutzer herausgefiltert.

Archivierung Verfallende Dokumentenversionen werden von DMS archiviert. Zu einem späteren Zeitpunkt können die Dokumente dann wiederhergestellt werden, um bspw. für eine Revisionsprüfung bereitzustehen oder eine fälschlicherweise neuere Version des Dokumentes zu ersetzen.

Die Entscheidungskriterien für ein konkretes DMS sind neben den jeweils erforderlichen Ausprägungen der Grundfunktionalitäten von der Menge der zu archivierenden Dokumente, der Zugriffshäufigkeit und der Häufigkeit und dem Umfang der Dokumentenänderungen abhängig. Weiterhin sollte sich das DMS nahtlos in die bestehende Softwareinfrastruktur, insbesondere. die Bürokommunikationssoftware, einbetten lassen.

2.3 Einbettung DMS in bestehende Softwareinfrastruktur

Im Rahmen der RAfEG Referenzarchitektur besteht die Anforderung, Dokumentenmanagementsysteme in die bestehende Softwareinfrastruktur — insbesondere. Bürokommunikations– und Workflowsteuerungssoftware — einzubetten. Diese Integration erfolgt üblicherweise über Schnittstellen, welche in den Phasen der Dokumentenerfassung, –bearbeitung, –prüfung, –verteilung, –verwendung und –archivierung die Kommunikation mit anderer Software, Hardware und Netzwerken ermöglichen.

Schnittstelle	Beschreibung
ODMA	ODMA ist ein von der Open Document Management Alliance entwickelter Standard. Produkte der Bürokommunikationssoftware können mit Hilfe dieses Standards transparent, hersteller– und produktübergreifend ein Dokumentenmanagementsystem nutzen. Der Standard wird vorallem von DMS auf MS Windows Basis unterstützt.

TWAIN	TWAIN ist eine standardisierte Softwareschnittstelle für Scanner, Digitalkameras, etc. über die sich alle Hardwarefunktionen per Software steuern lassen. Geräte, die dem TWAIN-Standard entsprechen, lassen sich aus jedem TWAIN-kompatiblen DMS heraus steuern und dienen hier vorallem der Dokumentenerfassung von NCI-Dokumenten.
OCR	Mit Hilfe von OCR-Software („optische Zeichenerkennung“) können NCI-Dokumente in CI-Dokumente gewandelt werden. Besonders bei der Erfassung von standardisierten Formularen wird OCR-Software eingesetzt.
LDAP	Das Lightweight Directory Access Protokoll (LDAP) entstand als Frontend für den X.500 Verzeichnisdienst. LDAP speichert diverse Informationen in einer Baumhierarchie und wird vorallem zur Speicherung von Benutzer– und Gruppeninformationen genutzt.
WebDAV	Die Erweiterung „Web Distributed Authoring and Versioning“ des HTTP-Protokoll ist als offener Standard (RFC2518) definiert und erlaubt die dokumentenorientierte Teamarbeit im Internet. WebDAV vereinfacht damit die Zusammenarbeit räumlich getrennter Teams über das Internet. Gängige Bürokommunikationssoftware (bspw. MS Office) unterstützt WebDAV.
MAPI	Das von Microsoft entwickelte Messaging API (MAPI) ermöglicht dem DMS Dokumente via E-Mail über den MAPI-fähigen E-Mail-Client zu empfangen und zu verschicken. Der Standard wird vor allem vom kommerziellen, MS Windows basierten Lösungen unterstützt.
XML	In XML (offener W3C Standard) werden die Struktur und die Inhalte von verschiedensten Dokumenten beschrieben. Damit wird eine medienneutrale Verarbeitung von Texten ermöglicht.
PDF	Das Portable Document Format (PDF) ist ein universelles Dateiformat. PDF-Dokumente können unabhängig von dem Programm und dem Betriebssystem, mit dem sie erstellt wurden betrachtet werden. Dazu wird der kostenlos verfügbare Adobe Acrobat Reader oder ein entsprechendes Browser-PlugIn benötigt. PDF-Dokumente eignen sich daher insbesondere zur Dokumentenverteilung und –verwendung, da PDF Dokumente i. d. R. nicht weiter modifiziert werden und entsprechend geschützt werden können.

Tabelle 2.1: Übliche DMS Schnittstellen

Neben der Integration in die bestehende Applikationslandschaft ist die Integration des DMS in das Betriebssystem zu beachten. Eine tiefe Integration in das Betriebssystem besitzt den Vorteil einer automatischen Einbindung aller Applikationen in das DMS, da sämtliche Dokumente, welche mit irgendeiner Applikation geöffnet oder geschrieben werden sollen, über das DMS bereitgestellt und kontrolliert werden können. Nachteil ist eine starke Abhängigkeit vom Betriebssystem.

Einbindung	Beschreibung
Direkt in Betriebssystem	Integration des DMS direkt in Filesystem des Betriebssystems. Vorteile: • direkte Kontrolle aller Dokumentenaktivitäten durch DMS möglich • Nahtlose Integration in Softwareinfrastruktur • Fremdsoftware muss nur bedingt Schnittstellen bereitstellen Nachteile: • Abhängigkeit von Betriebssystem und –version • Updates aufwendig, da in Abhängigkeit von Betriebssystemversion • tangiert systembedingt alle Softwaresysteme
Applikation auf Arbeitsplatzrechner	DMS existiert als separate Applikation oder Systemdienst auf Arbeitsplatzrechner. Vorteile: • beeinflusst Funktionen anderer Software nicht • unabhängig von Betriebssystemversion Nachteile: • Applikation muss separat gestartet werden • Applikation muss aktiv genutzt werden • Updates auf jedem Arbeitsplatz nötig
Webbasierte Applikation	DMS stellt als Webapplikation seine Dienste über Webbrowseroberfläche zur Verfügung. Vorteile: • Updates zentral möglich • Unabhängig von Betriebssystem des Arbeitsplatzrechners Nachteile: • Webapplikation muss aktiv genutzt werden

Tabelle 2.2: DMS Integrationsoptionen

2.4 Systemübersicht

Die Zahl der Hersteller und Anbieter von DMS beträgt heute weltweit schätzungsweise 300; in Deutschland allein ca. 100. Die Gestaltung einer Übersicht ist hier sehr schwierig, da eine Reihe von Anbietern dieselben Produkte unter eigenen Namen vertreiben oder Komponenten verschiedener Produkte miteinander kombinieren (vgl. [2] und eigene Recherche).

Auf Grund der unübersichtlichen Marktlage wurde hier auf eine Nennung aller DMS-Produkte verzichtet und dafür eine Unterteilung in OpenSource– und kommerzielle Produkte getroffen. Kommerzielle DMS sind oft als geschlossene Systeme konzipiert, besitzen dafür aber einen großen Funktionsumfang. Mitunter sind die DMS Bestandteil integrierter Lösungen, welche weitere die Gruppenarbeit unterstützende Softwaresysteme beinhalten.

OpenSource Produkte sind i. d. R. als Webapplikationen entwickelte Systeme und nutzen offene Standards zum Austausch mit anderen Softwaresystemen.

2.4.1 OpenSource

Der Einsatz von OpenSource DMS ist mit folgenden Vorteilen verbunden:

- Software ist lizenzkostenfrei erhältlich und
- Individuelle Zusatzentwicklungen oder Modifikation des Quellcodes sind möglich.

Die hier vorgestellten DMS sind webbasierte Systeme, welche im Unterschied zu den kommerziellen Produkten oft nur einen Teil der möglichen DMS-Funktionalität abbilden.

Knowledge Tree Das PHP basierte Produkt Knowledge Tree wird von dem südafrikanischen Unternehmen „Jam Warehouse“ hergestellt und ist unter der GNU Public Licence (GPL) downloadbar. Die Software wurde ursprünglich für das South African Medical Research Council entwickelt und ist vollständig webbasiert. Es deckt die Grundanforderung an ein DMS ab und bietet zusätzlich einige Workflow– und Sicherheitsfunktionen.

Jakarta Slide Slide ist ein Framework für Content Management, welches durch seine gute WebDAV Unterstützung und optionaler Ablage der Dokumente in einer Datenbank, für die Entwicklung von DMS genutzt werden kann. Slide stellt eine Client API zur Verfügung, welche zur individuellen Implementierung genutzt werden kann. Das Framework eignet sich ausschließlich zur Entwicklung individueller DMS und stellt kein komplettes Softwaresystem dar. Durch die Eingliederung von Slide in die Gruppe der Apache Jakarta Produkte, ist eine weiterführende Entwicklung des Frameworks zu erwarten.

OpenCMS Das auf Java basierende Produkt ist als Content Management System entwickelt, ist aber durch Nutzung eines virtuellen Filesystem (VFS) und diverser — zumindest angekündigter Features — genauso als webbasiertes Dokumenten Management System zu nutzen.

2.4.2 Kommerzielle Anbieter

Die hier vorgestellten DMS kommerzieller Anbieter zeichnen sich oft durch eine sehr gute Integration in bestehende Softwareinfrastrukturen aus und bieten unter einer einheitlichen Oberfläche eine Reihe von Funktionalitäten. Der Umfang von über 300 DMS Produkten erlaubt hier keinen vollständigen Überblick. Daher sind hier vorrangig Systeme berücksichtigt, welche als Speziallösung für die öffentliche Verwaltung beworben werden oder über nennenswerte Eigenschaften verfügen.

e-komm Office Das von der n-komm GmbH hergestellte, aktenplanbasierte DMS „e-komm Office“ ist zentraler Bestandteil der sog. „e-komm Suite“. Die Suite enthält eine Reihe von Anwendungen für die öffentliche Verwaltung. Das Paket basiert auf Lotus Notes (vgl. Abschnitt 3.5.1 auf Seite 32).

Merkmal des Systems ist, dass der komplette Schriftverkehr immer unter einem Aktenzeichen abgelegt wird. Zur Verteilung und Dokumentenverwendung kann E-Mail und Fax (ein– und ausgehend) integriert werden. Dokumente können elektronisch signiert und in frei definierbare Workflows eingebunden werden.

EASY ENTERPRISE.+ Das Produkt der EASY Software AG stellt eine umfassende Lösung für den Einsatz in verschiedenen Arbeitsumgebungen wie mySAP, Lotus Notes oder Navision dar. Die webbasierte Applikation ist nach dem J2EE-Standard in Java implementiert und erlaubt damit den Einsatz beliebiger J2EE-konformer Applikationsserver (bspw. Jboss, IBM WebSphere und Bea WebLogic). Vorteilhaft für große Organisationen ist die damit verbundene Fähigkeit zur Verteilung der Anwendung auf verschiedene (ggf. auch heterogene) Rechnersysteme. Das DMS unterstützt frei definierbare Workflows (Anbindung an MS VISIO möglich) und bietet einen XML Server[1].

windream DMS Im Gegensatz zu den webbasierten Lösungen setzt das DMS der windream GmbH aus ein in das Produkt integrierte virtuelles Filesystem, welches das Filesystem der Microsoft Windows Betriebssysteme ergänzt. Damit kann das DMS automatisch alle vom Benutzer angeforderten oder zu speichernden Dokumente prüfen und indizieren. Zusätzlich wird die Suche nach Dokumenten über eine Erweiterung der MS Windows Suchfunktion erleichtert[2].

cc DMS In Kommunen unterschiedlicher Größenordnungen wird das DMS des Unternehmens CC e-gov GmbH eingesetzt. Die Software setzt sich aus Applikationen für den elektronischen Aktenordner (Kern-DMS), elektronische Archivierung und geordnete Schriftgutverwaltung zusammen. Das System verspricht eine gute Integration in vorhandene Office-Umgebungen und nahezu beliebige Fachanwendungen. Eine den gesetzlichen Bestimmungen entsprechende revisionssichere Ablage ist gewährleistet[3].

SAPERION Das DMS der SAPERION AG befindet sich bei mehreren öffentlichen Verwaltungen im Einsatz und bietet eine gute Integration für Groupware– und ERP-Systeme (Lotus Notes, SAP, MS Exchange, Navision). Die serverbasierte Applikation ist über webbasierte oder wahlweise native Clients basierend auf MS Windows zu nutzen. Das System unterstützt mehrere Standardschnittstellen. Hervorzuheben ist die Möglichkeit, EDM-Systeme (Engineering Data Management) wie AutoCAD, MegaCAD, etc. anzubinden.

Hyperwave IS/6 Die Hyperwave AG bietet mit Hyperwave IS/6 eine Content Management Plattform, welche durch ihre Architektur alle Grundanforderungen an ein DMS erfüllt. Die webbasierte Applikation unterstützt über 200 Dokumentenformate und nutzt offene Standards wie Java, HTML, SSL, XML, CSS und WebDAV. Das System lässt — wie fast alle webbasierten Lösungen — eine verteilte Installation auf mehrere Server zu. Hyperwave IS/6 wird von der Bundesagentur für Arbeit, der US Regierung sowie eine Reihe weiterer öffentlicher Verwaltungen im In– und Ausland genutzt.

[1] Quelle: `http://www.easy.de/dyn/epctrl/mod/easy000445/cat/easy000445/pri/easy`
[2] Quelle: `http://www.windream.com`
[3] Quelle: `http://www.cc-egov.de`

2.5 Anforderungen

Zu den Grundanforderungen an ein DMS gehört die nahtlose Integration in die bestehende EDV-Umgebung (vgl. [3], S. 129). Dazu ist aus organisatorischer Sicht die Einbindung in beliebige Geschäftsprozesse und aus technischer Sicht die Unterstützung relevanter Schnittstellen notwendig. Speziell öffentliche Verwaltungen aber auch Unternehmen müssen diversen gesetzlichen Anforderungen nachkommen. Dabei sollten Dokumentenmanagementsysteme unterstützend wirken.

2.5.1 Gesetzliche Anforderungen

Revisionssicherheit Seit dem Jahr 2002 haben Finanzbehörden gemäß § 147 Abs. 6 AO ein Datenzugriffsrecht auf elektronisch gespeicherte Unternehmensdaten. Dies erfordert ein revisionssicheres Archivsystem für alle in den Bereichen der Finanz–, Anlagen– und Lohnbuchhaltung[4] anfallenden Dokumente. Die Finanzbehörden sind dazu mit Software ausgestattet wurden, welche diverse Analysemöglichkeiten zulässt und die Dokumentenformate von MS Excel und Plaintext (ASCII) versteht und auf MS Access, dBASE, SAP/AIS sowie ODBC-fähige Datenbanken zugreifen kann.

Innerhalb von E-Government-Anwendungen sind verantwortliche Stellen in der öffentlichen Verwaltung verpflichtet, technisch-organisatorische Maßnahmen zur Revisionssicherheit (insb. in Hinblick auf personenbezogene Daten) zu erbringen (vgl. [4], S. 17, 58f). Dies schließt primär auch DMS ein. Die Anforderung der Revisionssicherung hat zur Folge, das bei Dokumentenformatkonvertierungen keine Informationen verloren gehen dürfen, Dokumente vor Veränderungen geschützt werden und zum Zeitpunkt der Prüfung wieder reproduziert werden kann.

Zertifizierung nach ISO9000 Die Verwaltung von Dokumenten, welche Richtlinien, Geschäftsprozesse und Arbeitsergebnisse, etc. beinhalten, nimmt innerhalb der ISO9000 Zertifizierung und Compliance eine zentrale Rolle ein[5]. Auch wenn sich die Zertifizierung nurbeschränkt auf Bereiche der öffentlichen Verwaltung anwenden lässt, nehmen viele Verwaltungen im Sinne einer verbesserten Organisation, Kundenorientierung und Wirtschaftlichkeit eine entsprechende Zertifizierung vor (vgl. [5]). DMS müssen zertifizierte Verwaltungen vorallem hinsichtlich der Dokumentenprüfung, –verwendung und –verteilung unterstützen.

Anforderung	Beschreibung
Revisionssichere Archivierung	Schutz von Dokumenten vor Veränderung und Reproduktion eines Dokumentes zu einem bestimmten Zeitpunkt.

Tabelle 2.3: DMS Anforderungen zur revisionssicheren Archivierung

[4] u. a. gemäß 257 HGB

[5] Quelle: `http://www.aixonix.de/cms.php?id=140`

2.5.2 Benutzerverwaltung

DMS müssen über ein Berechtigungssystem auf die Zugriffsschutzebenen Archiv, Klassen/Ordner, Dokumente und Komponenten (des DMS) verfügen. Die Benutzerverwaltung muss (im Idealfall) Autorisierung und Authentifizierung des DMS-Benutzers sicherstellen und elektronische Unterschriften ermöglichen. Die Verwaltung stellt damit sicher, das ein Benutzer Dokumente eines für ihn freigegebenen Status in einem sog. Check-Out-Prozess erhalten und bearbeiten sowie in einem Check-In-Prozess in das DMS einstellen können.

Anforderung	Beschreibung
Benutzer(-gruppen)	• Autorisierung des DMS Benutzers • Nutzung bereits vorhandener Benutzer(-gruppen) innerhalb der IT-Infrastruktur einer Organisation → Nutzung von LDAP
Elektronische Unterschrift	• Authentifikation von Dokumentenbearbeitungen • Nutzung entsprechender Standards
Check-In/–Out	• Gleichzeitige Bearbeitung eines Dokumentes ist nur zulässig, wenn Änderungen wieder zusammengeführt werden können.

Tabelle 2.4: DMS Anforderungen zur Benutzerverwaltung

2.5.3 Dokumente und Versionen

NCI–/CI-Dokumente DMS sollten mit NCI-Dokumenten arbeiten können und eine Unterstützung für CI-Dokumente bestimmter Formate bieten. CI-Dokumente sollten in den Formaten der MS Office Pakete, XML und PDF verarbeitet werden können — PDF hier insb. im Rahmen der Dokumentenverwendung.

Zu diesen Dokumenten werden zusätzliche Informationen gespeichert (Bearbeitungsstati, Annotationen, Indizes, etc.). Die Indizierung kann dabei manuell oder automatisch (bzw. in einer Mischform) erfolgen. NCI-Dokumente können mit Hilfe von Texterkennung und/oder Barcodelesern indiziert werden. Die Anzeige von Dokumenten wird von DMS im Nur-lesen-Modus sowie Bearbeitenmodus erlaubt.

Die Ablagestruktur des DMS sollte Klassen, Ordner und eine Mehrfachablage (durch Referenzierung/Links) zulassen. Das Teilen und Zusammensetzen von Dokumenten (in entsprechend unterstützten Dokumentenformaten) ist in diversen Anwendungsfällen eine nützliche Funktion.

Anforderung	Beschreibung
Dokumentenformate	• Unterstützung De-facto-Standard → MS Office Formate • Unterstützung plattformunabhängiger, offener Standards: → HTML, XML, PDF
NCI-Dokumente	• Verwaltung von NCI-Dokumenten
Bearbeitungsstatus	• Status der Bearbeitung durch einen Benutzer
Annotationen	• ergänzende Informationen zu Dokumenten(-versionen)
Indizierung	• manuell und/oder automatische Indizierung von Dokumenten

Klassifizierung	• Klassifizierung von Dokumenten
Referenzierung	• Verknüpfung von Dokumenten und/oder Dokumententeilen
Dokumentenanzeige	• Anzeige verschiedener Dokumententypen durch entsprechende Viewer
Internationalisierung	• Unterstützung von Unicode-Zeichensätzen, Codierung in → UTF

Tabelle 2.5: DMS Anforderungen an NCI-Dokumente

Konfigurationsmanagement Dokumente sollten — vorallem im Sinne der Revisionssicherheit — in allen Versionen vorgehalten werden. Die dazu notwendige Änderungs– und Releaseverwaltung verwaltet dabei alle Änderungen inkl. Informationen zu der Änderungen (Zeitpunkt, Bearbeiter, etc.) sowie die eigentliche Version des Dokumentes. In der entstehenden Historie zu einem Dokument muss jede Änderung nachvollziehbar dargestellt werden (Darstellung des Audit Trail). An das Linkmanagement innerhalb verknüpfter Dokumente werden in Bezug auf die Versionierung erhöhte Anforderungen gestellt, da die Verknüpfung des Dokumentes in einer bestimmten Version zu allen zu diesem Zeitpunkt aktuellen Versionen verlinkter Dokumente sichergestellt werden muss.

Anforderung	Beschreibung
Versionierung	• Speicherung aller Änderungen und Releases • Informationen zum Benutzer, Releaseinformationen • Sicherung des Audit Trail
Linkmanagement	• Verwaltung aller Dokumentenverknüpfungen in den entsprechenden Versionierungen

Tabelle 2.6: DMS Anforderungen Konfigurationsmanagement

Import/Export und Datenhaltung Die Verwaltung der Dokumente und Informationen zu den Dokumenten kann in Form einzelner Dokumentendateien oder innerhalb einer Datenbank erfolgen. Sinnvoll erscheint oft aus Performancegründen die Sicherung der Dokumente als Dateien und aller zusätzlicher Informationen in einer separaten Datenbank. Hier werden in der Regel SQL-Datenbanken genutzt. Beim Import und Export von diversen Dokumentenformaten unterstützen die meisten DMS die zum De-facto-Standard zählenden Formate der MS Office Pakete, HTML (vorallem webbasierte DMS), XML, TIFF (eingescannte Dokumente) und PDF. Besondere Aufmerksamkeit verdient XML, da über diesen offenen Standard das DMS in fast beliebige EDV-technische Umgebungen zu integrieren sind. PDF hat sich als universelles Dokumentenformat als Standard für die Dokumentenverteilung und –verwendung etabliert.

Anforderung	Beschreibung
Datenbank	• Speicherung der Daten in einer oder mehreren verteilten Datenbanken
Dokumentenimport	• Unterstützung der MS Office Dokumentenformate, XML-Dokumente

Dokumentenexport	• Export von Dokumenten in einem XML-Format zur Weiterverarbeitung • Export als PDF-Dokument

Tabelle 2.7: DMS Anforderungen Datenhaltung

Archivierung Die Sicherung von Dokumenten nach ihrer Klassifizierung, Dokumentenalter und –benutzer(-gruppen) in Form einer Teil– und Vollsicherung ist Aufgabe der Dokumentenarchivierung. Dazu sind vom DMS Speichersysteme wie CD-R(W)–, DVD–, WORM– und COLD-Systeme anzusteuern. Die Archivierung hat revisionssicher zu erfolgen. Zur Sicherung sind dabei Dokumentenformate zu nutzen, welche auch in Zukunft — mit einer gewissen Sicherheit — lesbar sind bzw. entsprechende Anzeigevorrichtungen sind vorzuhalten.

Anforderung	Beschreibung
Vollsicherung	• Sicherung aller Dokumente in allen (aktuellen) Versionen • Revisionssicheres Dokumentenformat → XML, PDF, TIFF • Sicherung auf externen Speichermedien • Einspielen von Vollsicherungen
Teilsicherung	• Sicherung von Änderungen • Wiedereinspielen von Änderungen
Speichermedien	• Ansteuerung externer Speichermedien → DVD, WORM, COLD • Unterstützung von Jukeboxes

Tabelle 2.8: DMS Anforderungen Archivierung

Suche Zur Suche über die vom DMS verwalteten Dokumente steht standardseitig eine Volltextsuche (für NCI-Dokumente oft mit Unterstützung von OCR-Komponenten) zur Verfügung. Die Suche kann boolsche Operatoren enthalten und kann schrittweise verfeinert werden. Darüber hinaus ist eine Suche über Indizes, Dokumentenklassen, Annotationen, etc. sowie zeit– und benutzerabhängigen Faktoren möglich.

Anforderung	Beschreibung
Volltextsuche	• Unterstützung boolscher Operatoren • Unicodesuche
Integration externer Suchmaschinen	• Zugriff auf vom DMS verwaltete Dokumente über Filesystem, WebDAV oder Datenbank (→ ODBC, JDBC). • externe Volltextsuchmaschinen (bspw. Verity, Autonomy, etc.) müssen Dokumentenformat kennen → XML, PDF, MS Office Formate
Integration von OCR-Komponenten	• Zugriff auf vom DMS verwaltete Dokumente über Filesystem oder Datenbank (→ ODBC, JDBC). • OCR-Komponenten muss Dokumentenformat kennen → TIFF

Render-Server	• Bereitstellung von Dokumentenabschnitten ohne das komplette Dokument zu übertragen

Tabelle 2.9: DMS Anforderungen Suche

2.5.4 Schnittstellen

In den Phasen der Erstellung/Erfassung, Änderung, Prüfung, Verteilung, Dokumentenverwendung und Archivierung von Dokumenten müssen DMS Informationen über definierte Schnittstellen erhalten und freigeben können. Im Vordergrund sollte dabei die Nutzung offener Standards stehen, da sich die Eigenschaften der Interoperabilität und Portabilität vorteilhaft auf den Einsatz eines DMS innerhalb einer heterogenen Systemlandschaft auswirken. Über XML-basierte Datenaustauschformate ist ein von der ursprünglichen Applikation unabhängiger Zugriff auf Dokumenteninhalte möglich und die Offenlegung des inneren Aufbaus über eine DTD sorgt für die nötige Offenheit des Standards. Die Verteilung von Dokumenten muss in einem universellen Dateiformat erfolgen, welches die Dokumentennutzung unabhängig von der verwendeten Hardware und Betriebssystem zulässt.

Dokumentenablage

Schnittstelle	Beschreibung
WebDAV	Mit WebDAV („Web Distributed Authoring and Versioning“) [6], einer Erweiterung des HTTP-Protokolls, können über das Internet/Intranet Dokumente im Team erstellt und bearbeitet werden. WebDAV ist ein offener Standard (RFC2518) und nutzt XML-codierte Daten zur Verwaltung der Dokumente. **Erweiterungen:** • DeltaV [7], IETF DeltaV Arbeitsgruppe[6] ermöglicht Konfigurationsmanagement • DASL[7] (DAV Searching and Locating) ermöglicht die Suche über Dokumente • WebDAV Access Control Protocol [8] definiert eine Syntax zur Beschreibung von Zugriffsberechtigungen Die Autorisierung eines Benutzers erfolgt über die im HTTP-Standard definierten Methoden.
ODMA	Der von der Open Document Management Alliance entwickelte Standard erlaubt es Produkten der Bürokommunikationssoftware eine transparente, hersteller– und produktübergreifende Integration in Dokumentenmanagementsysteme.

[6] „IETF DeltaV Working Group“, `http://www.webdav.org/deltav/`
[7] `http://www.webdav.org/dasl/`

ODBC	Unabhängig von Betriebssystem und Applikation kann über eine „Open DataBase Connectivity“ (ODBC-)Schnittstelle auf die Datenbank des DMS zugegriffen werden. ODBC basiert auf dem X/OPEN SQL-Call-Level-Interface.

Tabelle 2.10: DMS Schnittstelle Dokumentenablage

Erfassung/Erstellung

Schnittstelle	Beschreibung
TWAIN	Mit Hilfe der TWAIN-Schnittstelle können interne oder externe Erfassungskomponenten der DMS entsprechend kompatible Scanner, Digitalkameras, etc. steuern.
Faxeingang	Telefaxe können von DMS automatisch erfasst und ggf. mit Hilfe von OCR-Software geprüft werden. Eingehende Faxe werden dabei vom System i. d. R. als Pixelbild-Dokumente im TIFF-Format gespeichert.
E-Mail-Eingang	Eingehende E-Mails mit ggf. anhängenden Dokumenten können von DMS automatisch erfasst werden. Dazu muss das DMS entweder einen integrierten E-Mail-Client enthalten oder einen innerhalb der Bürokommunikationssoftware eingesetzten Client nutzen können. Unter MS Windows Plattformen existiert dazu das von Microsoft entwickelte MAPI-Protokoll (Steuerung MAPI-fähiger E-Mail-Clients).

Tabelle 2.11: DMS Schnittstelle Erfassung/Erstellung

Verteilung

Schnittstelle	Beschreibung
PDF	Das Portable Document Format (PDF) ist ein universelles Dateiformat. PDF-Dokumente können unabhängig von dem Programm und dem Betriebssystem, mit dem sie erstellt wurden betrachtet werden. Dazu wird der kostenlos verfügbare Adobe Acrobat Reader oder ein entsprechendes Browser-PlugIn benötigt. PDF-Dokumente eignen sich daher insbesondere zur Dokumentenverteilung und –verwendung, da PDF Dokumente i. d. R. nicht weiter modifiziert werden und entsprechend geschützt (Verschlüsselung) werden können.
Faxausgang	Telefaxe können von DMS automatisch versendet werden. Das Faxsystem stellt dazu i. d. R. einen entsprechenden Druckertreiber bereit.

E-Mail-Ausgang	Ausgehende E-Mails mit ggf. anhängenden Dokumenten können von DMS automatisch versendet werden. Dazu muss das DMS entweder einen integrierten E-Mail-Client enthalten oder einen innerhalb der Bürokommunikationssoftware eingesetzten Client nutzen können. Unter MS Windows Plattformen existiert dazu das von Microsoft entwickelte MAPI-Protokoll (Steuerung MAPI-fähiger E-Mail-Clients).

Tabelle 2.12: DMS Schnittstelle Verteilung

Benutzerverwaltung

Schnittstelle	Beschreibung
LDAP	Das Lightweight Directory Access Protokoll (LDAP) entstand als Frontend für den X.500 Verzeichnisdienst. LDAP speichert diverse Informationen in einer Baumhierarchie und wird vorallem zur Speicherung von Benutzer– und Gruppeninformationen genutzt. Innerhalb größerer Organisationen werden damit Benutzerinformationen zentral gepflegt. LDAP ist Bestandteil vieler anderer Verzeichnisdienste zur Benutzerverwaltung und bildet damit i. d. R. die zentrale Schnittstelle zum Zugriff auf Benutzerinformationen zur Autorisierung und Authentifikation.
Active Directory (Microsoft)	Active Directory ist ein Verzeichnisdienst für Microsoft Windows Netzwerke (Win2k), welcher Nutzerinformationen speichert und den Zugriff auf Netzwerkressourcen steuert. Active Directory enthält das LDAP und kann damit zur Benutzerverwaltung in DMS genutzt werden.
NDS (Novell)	Der Novell Directory Service (NDS) wurde von der Firma Novell für das Betriebssystem Novell NetWare eingeführt. Der NDS bildet eine hierarchische Struktur ab. Der Nachfolger eDirectory integriert das LDAP und kann damit alle hier möglichen Verzeichnisdienste abzubilden.
YP/NIS (Sun)	Der Network Information Service (NIS, früher Yellow Pages YP) wurde von der Firma Sun Microsystems als Verzeichnisdienst für Benutzerkonten, Computer und andere Netzwerkressourcen innerhalb der UNIX-Welt entwickelt.

Tabelle 2.13: DMS Schnittstelle Benutzerverwaltung

2.5.5 Anwendung

DMS Anwendungen stellen dem Benutzer einen Client zur Verfügung mit dessen Hilfe dieser auf die Funktionen und Komponenten des DMS zugreifen kann. Dieser Client kann als Fat-Client (im LAN– und WAN-Bereich), Applet (Intranet-Bereich) und XML/HTML-basiertes Browserfrontend (Internet–/Intranet-Bereich) bereitgestellt werden. Sinnvoll ist die Bereitstellung mehrerer Clienttypen für die unterschiedlichen Anwendungsfälle inner-

halb einer Organisation bzw. für das organisationsübergreifende Arbeiten. Neben den Funktionalitäten und deren Einbettung in die bestehende Softwareinfrastruktur über entsprechende Schnittstellen, ist der Einsatz vom unterstützten Betriebssystem (auf Client– und Serverseite), notwendiger Zusatzsoftware (Applikationsserver, etc.) und zusätzliche notwendiger Datenbanksysteme abhängig. Lizenzrechtlich kann zwischen kommerziellen Softwarelizenzen und ASP-Lizenzen (Application Service Providing) sowie OpenSource-Lizenzen unterschieden werden.

2.5.6 Workflow

Im Bereich der Workflowunterstützung bieten viele DMS leistungsfähige und flexible Komponenten zur Definition von Prozessen, Regeln und Bedingungen an. Damit sollten Tätigkeiten sequentiell, parallel und selektiv ausführbar sein. Für standardisierbare, wiederkehrende Aufgaben muss eine Stapelverarbeitung zu definierten Zeiten und Bedingungen möglich sein. Workflowkomponenten von DMS unterstützen i. d. R. die Priorisierung von Prozessen sowie Wiedervorlage– und Freigabefunktionen. Unabhängig von der zu einem DMS gehörigen Workflowkomponente (oft vom Hersteller des DMS oder fest in das DMS integriert) ist die Initiierung von DMS-Funktionen durch externe Workflowsteuerungssysteme wünschenswert.

2.6 Kriterienkatalog

Bei der Erstellung von Bewertungskriterien für DMS ist zu berücksichtigen, dass es sich i. d. R. um fertige Softwarepakete handelt. Damit steht die Erweiterung oder Modifikation des DMS im Vergleich zur nahtlosen Integration in die bestehende IuK-Systemumgebung im Hintergrund.

Kriterium	Beschreibung
Kategorie: Hersteller/ Entwickler	
Lizenztyp	Die konkrete Lizenzierung von DMS ist irrelevant.
Verbreitung	DMS tauschen i. d. R. keine Informationen oder Dokumente mit anderen DMS aus. Der Einsatz eines weit verbreiteten DMS ist daher nicht zwingend notwendig.
Weiterentwicklung	Die aktive Weiterentwicklung eines DMS spricht für eine laufende Fehlerbeseitigung und ist zu begrüßen. Im Gegensatz zu anderen Systemen ist das ständige „Auf dem aktuellen Stand halten“ eines DMS allerdings nicht notwendig.
Modifizierbarkeit	Die Modifizierbarkeit eines DMS — im Sinne von Quellcodeänderungen — ist in der Praxis i. d. R. nicht notwendig und würde das Versionsmanagement unnötig erschweren.
Kategorie: Systemumgebung	
Betriebssystem	DMS werden i. d. R. auf gesonderten Servern installiert und stellen ihre Dienste über Schnittstellen (LDAP, ODMA, etc.) zur Verfügung bzw. greifen über definierte Schnittstellen (LDAP, etc.) auf benötigte Dienste zurück. Die Integration eines DMS ist damit weniger eine Frage des Betriebssystems.

Typ	DMS werden als Applikationen angeboten.
Schnittstellen	• zu BKS: ODMA, WebDAV • zu GIS: WebDAV • zu Content-Frameworks: WebDAV • zu Sicherheitslösungen: API zur Ergänzung von Lösungen zur elektronischen Signatur und Dokumentenverschlüsselung
Kategorie: Standards	
BGG §7	DMS sollten vor allem hinsichtlich der Steuerung und Visualisierung von behinderten Personen benutzt werden können. In Abhängigkeit von Betriebssystem können hier verschiedene Standards existieren (bspw. Microsoft Active Accessibility (MSAA)).
XML	Die Konfiguration und Verhaltenssteuerung eines DMS sollte auf Grundlage XML-basierter Dokumente durchgeführt werden können. Damit wird es externen Applikationen ermöglicht das DMS besser zu integrieren.
Flexibilität	Bis auf wenige Standardmodifikationen sind i. d. R. keine Änderungen in der Steuerung des Applikationsverhaltens notwendig.
Dokumentenformate	Zur Bildung von Indizes und anderen Funktionen müssen DMS in der Lage sein, verwaltete Dokumente zu lesen. Innerhalb einer Organisation genutzte Dokumentenformate müssen vom eingesetzten DMS erkannt und verarbeitet werden können.
Kategorie: Sicherheit	
IT-Integration	DMS sind — sofern sie innerhalb einer IT-Umgebung eingesetzt werden — integraler Bestandteil der IuK-Systemumgebung.
Nutzerautorisation/ Nutzerauthentifikation	Die Autorisation und Authentifikation des DMS-Nutzers (Benutzerverwaltung) sollte innerhalb der IuK-Systemumgebung auf Grundlage eines zentralen Verzeichnisdienstes (Schnittstellen LDAP, Active-Directory, YP/NIS) erfolgen.
Verschlüsselung	Die verschlüsselte Speicherung innerhalb des DMS verwalteter Dokumente ist nicht zwingend erforderlich. DMS sollten aber eine verschlüsselte Übertragung der Dokumente unterstützen. Zur Dokumentenverteilung sollten Dokumente mit den jeweils Dokumentenformattypischen Verschlüsselungsverfahren geschützt werden können.
Signatur	Die Signatur einzelner Dokumente sollte lediglich hinsichtlich der Dokumentenverteilung (bspw. PDF, E-Mail, ...) unterstützt werden.
Kategorie: Features	
Internationalisierung	Insbesondere zur Suche und Indizierung der vom DMS verwalteten Dokumente müssen Unicode-kodierte Dokumente verarbeitet werden können.
Archivierung	Die Archivierung der vom DMS verwalteten Dokumente ist eine DMS-Kernfunktion und ist damit zwingend erforderlich.
Austauschbarkeit von Komponenten	Der Austausch einzelner Komponenten (Archivierung, Indizierung, Suche, Render-Server, etc.) eines DMS ist nicht zwingend notwendig, kann aber in Hinblick auf die Erweiterung oder Verbesserung einzelner DMS-Komponenten sinnvoll sein.

Tabelle 2.14: Kriterien für DMS

3 System– und Kriterienkatalog Bürokommunikationssysteme

3.1 Einleitung

Innerhalb der im Rahmen des RAfEG Verbundprojektes zu entwickelnden Referenzarchitektur ist die Einbindung von Bürokommunikationssoftware (BKS) zu beachten. Unter Bürokommunikationssoftware wird hier Software verstanden, welche einen Bearbeiter bei seiner Aufgabenerledigung in einem Büro durch verschiedene, kontextunabhängige, dialogorientierte Produkte unterstützt (vgl. [9]).

Dieser Systemkatalog wurde unter besonderer Beachtung der Nutzung von Standards zum Austausch von Dokumenten, der Kommunikation aller Prozessbeteiligten und dem Zugriff auf bzw. Interaktion mit einer Prozesssteuerungssoftware erstellt. Ziel ist die Erarbeitung eines Kriterienkataloges anhand dessen die Eignung der verschiedenen am Markt verfügbaren BKS-Systeme ermöglicht wird.

3.2 Grundanforderungen an Bürokommunikationssoftware

Bürokommunikationssoftware besteht i. d. R. aus mehreren Produkten, welche nicht zwingend vom selben Hersteller/Anbieter stammen müssen. Sie sind viel eher als Bausteine eines Gesamtsystems zu sehen, dessen Aufgabe es ist, den Benutzer durch ihre reibungslose Zusammenarbeit eine effiziente Erledigung der ihm gestellten Aufgaben zu ermöglichen. Aus diesem Grund enthalten die sog. „Office-Pakete“ der verschiedenen Hersteller oft mehrere Produkte, so das deren Zusammenarbeit sichergestellt ist.

Im folgenden sind die am meisten genutzten BKS-Produkte aufgeführt. Im Regelfall wird vom einzelnen Bearbeiter nur ein Teil der hier aufgeführten Produkte genutzt. Für alle Produkte gilt, das zur Verarbeitung der von ihnen erzeugten Dokumente, die strukturierte Speicherung derer Inhalte erforderlich ist. Die Ergebnisse der verschiedenen Produkte müssen innerhalb eines integrierten Bürosystems zusammengeführt werden können, um ein endgültiges Dokument zu erstellen, welches bspw. Text, Tabellen und Bilder enthält (vgl. [10], S. 72).

3.2.1 Textverarbeitung

Dialogorientierte Textverarbeitungen ermöglichen den Textentwurf, Textumformung, Speicherung und unterstützen die Textverwendung. Hinsichtlich des Textentwurfs unterstützt die Textverarbeitung bei der Festlegung des inhaltlichen Konzeptes und der

sprachlichen Gestaltung, bei der Textumformung bei der Modifikation des Inhaltes, der Form, der Struktur und Sprache eines Dokumentes. Zur Textverwendung werden Funktionen zum Druck, Archivierung, Übermittlung an andere Bearbeiter, etc. angeboten (vgl. [11]). Die Arbeitsweise bei der Texterstellung orientierte sich heute fast ausschließlich am Layout, an der Formatierung und an der Darstellung des Textes. Das Konzept des „What you see is what you get“ (WYSIWYG), welches die weitgehend identische Darstellung von Ausdruck und Bildschirmdarstellung ermöglicht, wirkt hier allerdings oft einer strukturierten Erfassung von Texten entgegen, so das moderne Textverarbeitungen den Benutzer bei dieser Aufgabe oft unterstützen (bspw. durch Vorlagen, Erkennung von Überschriften, etc.).

Zusätzlich zu den Grundfunktion einer Textverarbeitung wird von heutigen Produkten die Arbeit mit Zeichnungen, Tabellen und Webinhalten genauso wie die Arbeit mit Indizes, Fußnoten und Kommentaren bzw. Bearbeitungsversionen erwartet. Rechtschreibkontrolle, Serienbrief und weitere Zusatzfunktionen können heute von jeder gängigen Textverarbeitung erwartet werden. Neben dialogorientierten existieren stapelverarbeitende Textverarbeitungen (bspw. LaTeX), welche die Prozesse des Textentwurf, –umformung, –speicherung und –verwendung automatisiert abarbeiten und nicht in den Dialog mit dem Benutzer treten. Stapelverarbeitende Textverarbeitungen werden hier nicht zum Bereich Bürokommunikationssoftware gezählt.

3.2.2 Tabellenkalkulation

Mit Hilfe einer Tabellenkalkulation können umfangreiche Berechnungen durchführt werden. Dazu kann der Benutzer in jedes Feld einer angezeigten Tabelle Zahlen, Texte oder Formeln hinterlegen. Formeln können dabei auch Werte aus anderen Feldern referenzieren.

Die eingegebenen Zahlen, Texte und Ergebnisse diverser Berechnungen können grafisch aufbereitet werden, indem sie in Form verschiedenartiger Diagramme dargestellt werden. Diagramme können damit bspw. als visuelle Hilfen bei der Darstellung quantitativer Informationen über Trends und Statistiken dienen. Genauso lassen sich die Tabellen und Diagramme im Layout verändern und ausdrucken. Mit Hilfe einer Tabellenkalkulation lässt sich die Verarbeitung größerer Datenmengen automatisieren.

3.2.3 Zeichenprogramm

Zur Erstellung von einfachen Grafiken zur Illustration von Dokumenten, Kalkulationen oder Präsentationen werden Zeichenprogramme genutzt. Im Rahmen der Nutzung als Bestandteil einer Bürokommunikationssoftware geht es hier weniger um die Erstellung oder Manipulation von Pixelgrafiken, sondern um die Erstellung von Schaubildern und die Skalierung von Photos oder Cliparts[1]. Grundsätzlich kann zwischen Grafik– (Vektorgrafiken) und Bildbearbeitungssoftware (Pixelbilder) unterschieden werden. Mitunter sind die Funktionalitäten des Zeichenprogramms fest im Funktionsumfang der Textverarbeitung, Tabellenkalkulation oder Präsentationssoftware enthalten, so das Hersteller von Office-Paketen kein gesondertes Zeichenprogramm beifügen.

[1] Als Cliparts bezeichnet man gezeichnete Bilder (Symbole, Comics, etc.), die in Dokumente eingebaut werden können.

Eine Sonderfunktion erfüllen Bildbearbeitungsprogramme beim Erfassen, Bearbeiten und Speichern von Bildern, welche am Arbeitsplatz des Benutzers digitalisiert werden (bspw. mit Hilfe eines Scanners, Digitalkamera, etc.). In einer Büroumgebung dienen sie als Schnittstelle zur Erfassung nicht-elektronischer Informationen als Bild und deren Weiterverarbeitung im Bürokommunikationssystem.

3.2.4 Präsentationssoftware

Präsentationssoftware dient zur Erzeugung von multimedialen Präsentationen. Dazu werden Texte, Grafiken und ggf. multimediale oder interaktive Objekte auf einzelnen Folien platziert. Das heißt insbesondere die Ergebnisse von Textverarbeitungen, Tabellenkalkulationen und Zeichenprogrammen werden hier zusammengeführt und aufbereitet. Die meisten Präsentationsprogramme bieten dazu die Möglichkeit eingebundene Dokumente (bspw. Texte) zu modifizieren, um diese für eine Präsentation aufzubereiten.

3.2.5 (elektronische) Post

Zum Empfangen und Versenden von Textnachrichten und Dokumenten werden sog. E-Mail-Clients, d. h. Softwareprodukte welche dem Benutzer die Kommunikation mit einem E-Mail-Server erlauben, eingesetzt. Sender und Empfänger der Nachrichten können dabei an verschiedenen Rechnernetzen angeschlossen sein. Der Internet-E-Mail-Standard stellt sicher, das plattformübergreifend Texte und binärcodierte Daten übertragen werden können. Die Aufgabe der korrekten Darstellung empfangener Nachrichten obliegt dem E-Mail-Client (konkret der Unterstützung des Clients bezüglich des übermittelten Inhaltstyps und –codierung). Je nach E-Mail-Client bzw. dessen Einstellungen können bestimmte Dokumententypen direkt innerhalb der E-Mail-Client-Umgebung betrachtet und bearbeitet werden bzw. gesichert werden. E-Mail-Clients bestehen aus einem Mail Transfer Agent (MTA), welcher das Versenden und Empfangen der E-Mails, und einem Mail User Agent (MUA), welcher die Kommunikation mit dem Benutzer erledigt. Hinsichtlich des Datenschutzes, der Datensicherheit und Authentizität bietet das Internet-E-Mail-System keine Lösung, so das diese Anforderungen durch Zusatzsoftware oder im E-Mail-Client bereits integrierte Funktionen sichergestellt werden muss.

3.2.6 Ablage

Ein Bürokommunikationssystem muss in der Lage sein, mit ihm erstellte bzw. verwaltete Dokumente in einer strukturierten und sicheren Art und Weise zu sichern und ggf. zu archivieren. Sofern diese Funktion nicht von einem Dokumentenmanagementsystem erfüllt wird — hier erfolgt der Zugriff über entsprechende Schnittstellen —, erfolgt die Ablage in den meisten Office-Paketen innerhalb eines bestimmten Speicherortes auf dem Filesystem nach Dokumententypen getrennt. Diese Dokumentenordner sind i. d. R. durchsuchbar und können in festgelegten Zeitabständen archiviert werden. Hinsichtlich der Dokumentenarchivierung unterscheiden sich die Produkte eines integrierten Bürokommunikationssystems oft erheblich.

3.2.7 Kalender

Terminplanungen für einzelne Personen, Gruppen oder Organisationen erfolgen innerhalb eines Bürokommunikationssystems über eine entsprechende Kalendersoftware. Mitunter ist diese bereits Bestandteil der E-Mail-Lösung, da das Versenden und Empfangen von Dokumenten zu Terminplanungen, –abstimmungen, –festlegungen und –freigaben zu den Standardaufgaben elektronischer Kalender gehört. Neben der Abstimmung mit anderen Kalenderprodukten der Bürokommunikationssoftware anderer Benutzer ist eine Synchronisation des Kalenders mit mobilen Endgeräten (Laptop, PDA, Mobiltelefon, etc.) des Benutzers möglich.

3.2.8 Browser

Webbrowser ermöglichen die Darstellung Webseiten und erlauben darüber hinaus die Interaktion mit einem Webserver im Intranet oder Internet. Der Benutzer wird — sofern dies für seine Arbeit notwendig ist — den Browser vorrangig zur Informationsrecherche nutzen und kann komplette Webseiten(-dokumente) oder Teile davon in seine Office-Komponenten (bspw. Textverarbeitung oder Präsentationsprogramm) übernehmen.

Da Webbrowser auf allen gängigen Systemumgebungen verfügbar sind und inzwischen zum De-facto-Standard eines auslieferungsfähigen Betriebssystems gehören, eignet sich der Browser als Präsentationsoberfläche von Anwendungen in verteilten, heterogenen Umgebungen.

3.3 Einbettung in bestehende Softwareinfrastruktur

Im Rahmen der hier behandelten Architektur besteht zwingend die Anforderung, das BKS-Systeme Dokumente untereinander und mit anderen Anwendungen (Dokumentenmanagement, Workflowsysteme, etc.) austauschen können.

3.3.1 Dokumentenmanagement

Die Sicherung und Archivierung der mittels eines Bürokommunikationssystem erzeugten Dokumente kann mit Hilfe eines Dokumentenmanagementsystems (DMS) erfolgen. Diese Systeme indizieren und strukturieren Dokumente und ermöglichen darüber hinaus die Verwaltung und Archivierung mehrerer Versionen eines Dokumentes, so das letztlich alle Schritte von der Erzeugung bis zur endgültigen Fassung des Dokumentes transparent werden. Gleichzeitig findet eine ständige Überwachung des Dokumentenzugriffs statt, um unberechtigten oder gleichzeitigen (Gefahr von Inkonsistenzen) Zugriff auf ein Dokument zu verhindern.

Viele DMS bieten darüber hinaus automatische Nachrichtenfunktionen bei Änderungen eines Dokumentes (ggf. durch Anbindung des E-Mail-Client der Bürokommunikationssoftware) und können verschiedene Versionen eines Dokumentes vergleichen und Unterschiede hervorheben. Damit können bspw. Unterschiede in verschiedenen Versionen einer technischen Zeichnung, Geländeplänen, etc. einfach erkannt werden. Die Güte eines DMS ergibt sich aus der nötigen Zeit, um auf gesuchte Informationen zuzugreifen und der Vollständigkeit des Dokumentenpools.

3.3.2 Workflow-Managementsysteme

Die Aufgabe eines Workflowmanagement-Systems (WfMS) besteht darin, einen beschriebenen und definierten Workflow zu interpretieren. Die Beschreibung des Workflow erfolgt dabei oft mit Hilfe externer Programme. Workflow-Managementsysteme ermöglichen damit die Automatisierung eines Geschäftsprozesses, indem es die durchzuführenden Aktivitäten entsprechend der hinterlegten Workflowbeschreibung abarbeitet.

Neben der Modellierung und Definition von Arbeitsabläufen und deren Aktivitäten besteht die Aufgabe von WfMS in der Verwaltung aller gerade notwendigen Instanzen definierter Workflow. Innerhalb einer Instanz erfolgt eine Steuerung der einzelnen Aktivitäten auch über Interaktion mit dem Benutzer oder externen Applikationen.

3.3.3 Fachanwendungen

Zur Erledigung genau definierter, kontextbezogener Aufgaben existieren Fachanwendungen (Berichtssysteme [z. B. UIS], GIS–, CRM–, CAD-Anwendungen, etc.). Hier handelt es sich i. d. R. um Spezialanwendungen oder Individualsoftware, welche von speziell dafür geschulten Bearbeitern bedient wird. Fachanwendungen erzeugen oft spezifische Dokumente oder legen ihre Daten in einer Datenbank ab. Sofern die damit erzeugten Daten in Form eines Dokumentes gespeichert oder exportiert werden können, ist eine Weiterverarbeitung mit Produkten der Bürokommunikationssoftware möglich (bspw. Versand per E-Mail, etc.). Wird der Dokumententyp von einem Produkt des Bürokommunikationssystems unterstützt, ist die Einbindung des Dokumentes der Fachanwendung in andere Dokumente (bspw. Präsentation, Berichte, etc.) möglich.

3.3.4 Allgemeine Schnittstellen

Bürokommunikationssysteme kommunizieren i. d. R. über die von ihnen erzeugten und gespeicherten bzw. versandten Dokumenten mit ihrer Umwelt. Produkte, welche auf Dokumente dieser Systeme zugreifen möchten, müssen auf die Dokumente als solche und — sofern sie diese modifizieren oder indizieren möchten — ihren Inhalt zugreifen können. Dazu ist zwingend die Kenntnis zur Dokumentenstruktur (Dateiformat) nötig.

Hier existieren proprietäre Formate, welche allerdings teilweise als De-facto-Standard gelten, und standardisierten, offenen Formaten. Ein Versuch, einen offenen Standard zu etablieren fand 1995 mit Definition der ISO 8613 ODA statt. Auf Grund mangelnder Unterstützung durch die führenden Hersteller von Bürokommunikationssoftware ist dieser Versuch als gescheitert zu betrachten. Inzwischen unterstützen allerdings weitgehend alle bedeutenden Hersteller den Import und Export über XML basierte Dokumente und unterstützen damit einen offenen Standard, um Dokumente getrennt nach Inhalt, Form und Struktur auszutauschen.

3.3.5 Anwendungsspezifische Standards

Die einzelnen Produkte innerhalb einer Office-Lösung nutzen oft spezifische Standards zur Ablage der mit ihnen erzeugten Dokumente oder entsprechende Schnittstellen, welche

auch Fremdsystemen (Workflow-Managementsysteme, Fachanwendungen, etc.) den Zugriff ermöglichen. Die hier vorgestellten Standards werden von den meisten Anwendungen im Bereich der Bürokommunikationssoftware genutzt.

Produkt	Standard	Beschreibung
Textverarbeitung, teilw. Zeichenprogramme, Tabellenkalkulation	ISO 8612 ODA	Die ISO 8613 definiert den Open Document Architecture (ODA) Standard zum Dokumentenaustausch in offenen Systemen (vgl. [12]).
Textverarbeitung, Tabellenkalkulation, Browser	XML	In XML (offener W3C Standard) werden die Struktur und die Inhalte von verschiedensten Dokumenten beschrieben. Damit wird eine medienneutrale Verarbeitung von Texten ermöglicht.
Textverarbeitung	RTF	Rich Text Format (RTF) Dokumente (vgl. [13]) dienen zum Datenaustausch zwischen Textverarbeitungsprogrammen verschiedener Hersteller. Das textbasierte Format wurde von Microsoft eingeführt.
Tabellenkalkulation	CSV	Character Separated Values (CSV) Dokumente dienen zum Datenaustausch zwischen Tabellenkalkulationen verschiedener Hersteller. Das textbasierte Format nutzt ein (frei definierbares) Trennzeichen zur Abgrenzung der Spalten und den Zeilenumbruch zur Abgrenzung der Tabellenzeilen.
Textverarbeitung, Tabellenkalkulation, Zeichenprogramm, Präsentationssoftware	PDF	Das Portable Document Format (PDF) ist ein universelles Dateiformat, das innerhalb der Textverwendung genutzt wird. PDF-Dokumente können unabhängig von dem Programm und dem Betriebssystem, mit dem sie erstellt wurden betrachtet werden. Dazu wird der kostenlos verfügbare Adobe Acrobat Reader oder ein entsprechendes Browser-PlugIn benötigt. PDF-Dokumente eignen sich daher insbesondere zum Austausch mit anderen Benutzern, welche Dokumente nicht weiter modifizieren.
Zeichenprogramm	TWAIN	TWAIN ist eine standardisierte Softwareschnittstelle für Scanner, Digitalkameras, etc. über die sich alle Hardwarefunktionen per Software steuern lassen. Geräte, die dem TWAIN-Standard entsprechen, lassen sich aus jedem TWAIN-kompatiblen Office-Programm heraus steuern.
Zeichenprogramm, Präsentationsprogramm	SMIL, SVG	SVG: Scalable Vector Graphics (zweidimensionale Vektorgrafik) und SMIL: Synchronized Multimedia Integration Language (Multimediapräsentationen) sind XML basierte Formate zum Austausch von Grafiken und Multimediapräsentationen.

Kalender	SyncML	SyncML Data Sync ist ein auf XML basierender offener Standard zur Synchronisation von Daten (insb. Adressen, Kalender, etc.) zwischen verschiedenen Rechnern (insb. mobilen Endgeräten und Servern).
E-Mail-Client	MAPI	Das von Microsoft entwickelte Messaging API (MAPI) ermöglicht diversen Fachanwendungen Nachrichten über den MAPI-fähigen E-Mail-Client zu empfangen und zu verschicken. Der Standard wird vor allem vom kommerziellen, MS Windows basierten Lösungen unterstützt.
E-Mail-Client	IMAP	Das Internet Message Access Protocol (IMAP4, RFC 2060) ermöglicht die strukturierte Ablage von E-Mails auf einem Server. Auf diesen Server können zeitgleich mehrere Benutzer mit ihren IMAP-fähigen E-Mail-Clients zugreifen. Da E-Mails erst auf Anforderung übertragen werden eignet sich der IMAP-Standard insb. für den E-Mail Zugriff von mobilen Endgeräten aus.
Textverarbeitung, E-Mail-Client, Browser	Unicode (UTF-8, UTF-16 UCS-2, UTF-32 UCS-4)	Mit Hilfe von Unicode-Zeichencodierungen ist bzw. kann für jedes graphische Zeichen oder Element aller bekannten Schriftkulturen und Zeichensysteme ein Code festgelegt werden. Damit werden Zeichendekodierungen zwischen verschiedenen Systemen unnötig und der entsprechende Konvertierungsaufwand entfällt. Vorteil der UTF-8 Kodierung ist, das normale auf dem ASCII-Standardzeichensatz basierende Nachrichten unverändert gültig sind. Unicode fähige Produkte können problemlos im internationalen Geschäftsverkehr genutzt werden.
Browser	HTML 4.0, XHTML	HTML ist eine SGML (ISO 8879) basierte Auszeichnungssprache für hypertextbasierte Dokumente. Mit dem W3C Standard HTML 4.0 und XHTML können ansprechende, barrierefreie Webseiten entwickelt werden.
Browser	CSS 2.0	Zur ansprechenden Darstellung von HTML/XHTML/XML-Dokumenten werden Cascading Style Sheets genutzt (W3C Standard). In diesen kann medienabhängig definiert werden, wo und wie Bereiche eines Dokumentes dargestellt werden (Position, Ausrichtung, Schriftart, etc.).
Browser	HTTP 1.1	Browser können über das Hypertext Transfer Protokoll Dokumente von einem Webserver anfordern und zu einem Webserver schicken.

Dokumenten-management	ODMA	ODMA ist ein von der Open Document Management Alliance entwickelter Standard. Produkte der Bürokommunikationssoftware können mit Hilfe dieses Standards transparent, hersteller– und produktübergreifend ein Dokumentenmanagementsystem nutzen. Der Standard wird allerdings hauptsächlich von DMS auf Basis des Betriebssystems MS Windows unterstützt.

Tabelle 3.1: BKS Standards

3.4 Anforderungskatalog

Der im folgenden aufgestellte Anforderungskatalog enthält alle Bereiche, welche innerhalb des RAfEG-Konzeptes bzgl. einzubindender Bürokommunikationssoftware relevant sind.

3.4.1 Offene Systeme

Eigenschaft offener Systeme ist, das diese über eine offene Spezifikation hinsichtlich des Informationszugangs, der genutzten Verfahren und der Einsatzfähigkeit in heterogenen Umgebungen besitzen. Sie besitzen die Eigenschaften der Interoperabilität und Portabilität. Grundsätzlich ist der Einsatz offener Systeme zu empfehlen, da diese die von ihnen produzierten Inhalte öffentlich zugänglich halten (oft durch Einsatz eines standardisierten Formates und einer entsprechenden Dokumentation), sowie Interoperabilität und Portabilität sicherstellen.

Hinsichtlich der Einpassung in die zu erstellende RAfEG-Softwarearchitektur sollte Bürokommunikationssoftware (und ihre Komponenten) vor allem über standardisierte Schnittstellen und Formate kommunizieren können. Produkte, welche dieser Anforderung nur ungenügend entsprechen, können weder Dokumente aus vorherigen Prozessschritten verarbeiten noch Dokumente in einem weiterverarbeitbaren Format an ein Workflow-Managementsystem übergeben.

3.4.2 Betriebssysteme

Die eingesetzte Office-Software sollte innerhalb einer Organisationseinheit für alle dort eingesetzten Betriebssysteme (natürlich nur im Rahmen der Bürokommunikation eingesetzter OS) verfügbar sein. Da der Dokumentenaustausch innerhalb einer Organisationseinheit oft in einem erheblich größeren Umfang stattfindet, als zwischen den Organisationseinheiten sollten hier Konvertierungsprobleme zwischen inkompatiblen Dokumentenformaten vermieden werden. Innerhalb eines Office-Paketes treten i. d. R. selbst auf verschiedenen Betriebssystemen keine Konvertierungsprobleme auf, so das der Einsatz eines Office-Paketes innerhalb einer Organisationseinheit zu empfehlen ist.

3.4.3 Lizenzpolitik

Für das RAfEG-Konzept spielt die Lizenzpolitik eines Anbieters von Bürokommunikationssoftware eine untergeordnete Rolle. Eine sehr individuelle Anpassung der Bürokommunikationssoftware an die Bedürfnisse einer Institution können jedoch Änderungen oder Ergänzungen bestimmter Softwareteile erzwingen. Für diesen Fall ist die freie Verfügbarkeit und (auch rechtlich einwandfreie) Modifizierbarkeit von Quellcode wichtig. Der Sourcecode sollte dann idealerweise einer General Public Licence (GPL) unterliegen. Zu beachten ist, das einige Lizenzierungen in diesem Bereich auch den modifizierten Code grundsätzlich unter eine offene Lizenz legen.

3.4.4 Softwarearchitektur

Im Normalfall werden Office-Softwarepakete als Stand-alone Applikation auf dem PC des Benutzers oder auf einem zentralen Server installiert. In beiden Fällen wird allerdings der eigentliche Applikationscode auf den Rechner des Benutzers kopiert und dort ausgeführt. Damit ergibt sich die Problematik, Updates der Softwarepakete möglichst zeitgleich auf allen Benutzer-PCs zu installieren und ggf. vorher auf ihre gewünschte Funktionsweise zu prüfen. Im Gegensatz zu Stand-alone-Applikationen können ASP-fähige Anwendungen von einem ASP (Application Service Provider) IT-Dienstleister über das Internet oder Intranet bereitgestellt werden. Die ASP-fähige Software befindet sich auf einem vom Client durch ein Netzwerk erreichbaren Server. Der Client überträgt nur Eingabe– und Ausgabeinformationen an den Server, welcher diese an die Applikation leitet bzw. von dieser erhält. Damit können einzelne Komponenten der Bürokommunikationssoftware sehr einfach für einzelne Benutzer verfügbar gemacht werden, Updateprozesse können zentral auf dem Server abgearbeitet werden. In Verbindung mit einem Workflow-Managementsystem ist damit eine sehr enge Verzahnung von Workflowsteuerung und Bürokommunikationssoftware möglich.

3.4.5 Office-Funktionalitäten (Programmpakete)

Welche der oben skizzierten Produkte für einen konkreten Benutzer der Bürokommunikationssoftware notwendig, sinnvoll oder vernachlässigbar sind, ist vom konkreten Anwendungsfall abhängig. Sofern die Präsentationsschicht eines eingesetzten Workflow-Managementsystem den Browser als Interaktionsmedium nutzt, ist diese Komponente das einzig zwingend notwendige Produkt.

3.4.6 Sicherheit

Grundsätzlich sind Dokumente der Bürokommunikationssoftware vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung zu bewahren. Für die Verwendung von einigen Dokumenten ist Sicherheit hinsichtlich der Authentizität erforderlich. Während der Verlust von Dokumenten oft über integrierte (rudimentäre) Backuplösungen oder ein integriertes Dokumentenmanagement gelöst wird, sind alle anderen Anforderungen oft nur über zusätzliche Programme erfüllbar. Sicherheit bieten

hier Verfahren der Kryptografie (Verschlüsselung von Dokumenten und digitale Unterschriften), welche offengelegt sind und damit von hinreichend genügend Personen auf ihre Verlässlichkeit getestet werden konnten.

3.4.7 Datenaustauschformate

Um Dokumente mit anderen Anwendungen oder Bürokommunikationssystemen innerhalb und auch außerhalb der eigenen Organisation auszutauschen, müssen sich alle am Datenaustausch beteiligten Partner auf ein Datenaustauschformat einigen. Diese sollte idealtypisch als offener Standard („Offener Standard für Dokumentenaustausch“) vorliegen und von allen am Markt befindlichen Office-Paketen unterstützt werden.

XML basierte Dokumentenformate bieten sich hier an, da unter Einsatz der durch das W3C verabschiedeten Empfehlungen über ein XML-basiertes Datenaustauschformat ein von der ursprünglichen Applikation unabhängiger Zugriff auf die Dokumenteninhalte möglich ist. Der innere Aufbau einer XML Dokumentendatei ist über eine Document Type Definition (DTD) offengelegt. Dokumente sind damit von jeder Software vollständig validierbar und sie können auf semantische Strukturinformationen zugreifen, um diese gezielt zu ändern, zu ergänzen, zu löschen oder zu lesen. Bereits existierende Standards zur Verschlüsselung und Authentifizierung (XML Encryption, OASIS SAML, XML Signature) bieten auch die geforderte Sicherheit[2].

In der Praxis werden XML basierte Datenaustauschformate erst seit wenigen Jahren unterstützt, so das vor allem in den älteren kommerziellen Office-Paketen keine hinreichende oder keine XML Unterstützung beim Import und Export von Dokumenten geboten wird. Die Dominanz des Office-Paketes „Microsoft Office“ des US-amerikanischen Herstellers Microsoft Corp. hat dazu geführt, das die meisten verfügbaren Bürokommunikationssysteme die MS Office Dateiformate verarbeiten können. Damit sind diese proprietären Dateiformate als De-facto-Standard zu betrachten.

Unabhängig von den Microsoft Office Dokumentenformaten für Textverarbeitung und Tabellenkalkulation haben sich die teilweise selbst von Microsoft entwickelten De-facto-Standards RTF und CVS etabliert. Diese Dokumentenformate dienen vorallem dem Datenaustausch über Systemgrenzen hinweg können allerdings oft nur einen Teilbereich der Dokumenteninhalte aufnehmen (CSV kann bspw. keine mit der Tabellenkalkulation erstellen Diagramme enthalten). Für die Zukunft zeichnet sich hier ein Trend zur Nutzung rein XML-basierter Dokumentenformate ab.

3.4.8 Schnittstellenunterstützung

Zur Integration des Bürokommunikationssystems in andere Umgebungen (Workflow-Managementsystem, Dokumentenmanagement, etc.) bzw. der Integration von Fachanwendungen sollten verschiedene Standardschnittstellen unterstützt werden.

[2]Das Open Office XML Format Technical Committee, welches neu eingesetzt wurde, soll ein auf XML basierendes Format entwickeln, in welches sich Dokumente aus Textverarbeitungen, Tabellenkalkulationen und Präsentations-Tools speichern lassen.

3.5 Systemkatalog

3.5.1 Verbreitete Officepakete

Mit seinem Produkt MS Office und 80 % Marktanteil ist Microsoft Marktführer im Bereich von Bürokommunikationssoftware (Office-Pakete). Den verbleibenden Anteil teilen sich die Anbieter Corel, Lotus und Sun. Die Pakete unterscheiden sich nicht außerordentlich im Funktionsumfang, so dass sich die Marktführerschaft von Microsoft vor allem auf seine Dominanz im Betriebssystemmarkt zurückführen lässt (Quelle: [14], Kapitel 3.3 „Officepakete und sonstige Anwendungen“).

Sun StarOffice Suns StarOffice verfügt über schätzungsweise 7 % Marktanteil. Wohl mit aus diesem Grund ist dem Hersteller eine weitgehende Kompatibilität zum De-facto-Standard der MS Office Dateiformate sehr wichtig. Positiv fällt auf, das sich die Funktionalität von StarOffice über ein angebotenes Software-Development-Kit (SDK) erweitern lässt[3].

OpenOffice OpenOffice ist ein offenes, frei verfügbares Office-Paket, welches für die wichtigsten Desktop Betriebssysteme verfügbar ist. Die einzelnen Produkte der Bürokommunikationssoftware bilden allerdings nur den Kernbereich (Textverarbeitung, Tabellenkalkulation und Präsentation) ab.

Corel WordPerfect Trotz des fehlenden E-Mail-Clients ist Corel WordPerfect eine preiswerte Alternative zu den bekannten Office-Paketen. Durch die angebotene ODMA Schnittstelle ist eine nahtlose Anbindung an Dokumentenmanagementsysteme möglich. Als Besonderheit besitzt WordPerfect bereits eine integrierte Dokumenten-Versionsverwaltung.

Koffice Koffice wurde zum Betrieb unter Linux/KDE (K Desktop Environment) entwickelt und stellt hier das Standard-Office-Paket dar. Das System verfügt eine Vielzahl von Produkten, die teilweise weit über den Funktionsumfang kommerzieller Anbieter hinausgeht. Das Besondere an Koffice ist die komponentenbasierte Architektur auf Basis das Kparts Komponenten-Modells. Damit sind alle Komponenten untereinander kombinierbar. Die Dateiformate basieren auf XML und sind vollständig dokumentiert. Genauso wie Koffice existieren auch für KDE entwickelte Kalender, E-Mail-Clients, etc., so dass die fehlende Integration dieser Pakete (bspw. Korganizer) eher wundert.

Microsoft Office Das Beratungsunternehmen Giga Information Group ermittelte für 2003 folgende Verteilung der Softwareversionen: MS Office XP 12 %, MS Office 2000 53 % und MS Office 97 35 %[4]. Zu bemerken ist hier, dass die in der Übersicht aufgezeigte XML-Unterstützung erst ab der (recht neuen) Version MS Office 2003 Professional (zum Zeitpunkt der Studie noch nicht berücksichtigt) verfügbar ist.

[3] Quelle: CHIP Testbericht StarOffice, `http://www.chip.de/artikel/c_artikelunterseite_11078701.html?tid1=19495&tid2=19778`

[4] Quelle: eigene Berechnung auf Grundlage: `http://www.kefk.net/Software/Anwendungen/MS.Office/index.asp`, 2003

Microsoft Works Mit MS Works bietet Microsoft ein preiswertes, stark eingeschränktes Office-Paket. Die (je nach Version) enthaltene Tabellenkalkulation ist in ihrem Funktionsumfang stark eingeschränkt und E-Mail-Client ist MS Outlook. Insgesamt eignet sich MS Works eher für den Home Office Bereich.

AppleWorks AppleWorks zählt zu den Standard-Office-Paketen unter Apple Macintosh und ist ausschließlich für Apple Computer verfügbar.

3.5.2 Vergleich

In der folgenden Übersicht werden die verbreitetsten Office-Pakete hinsichtlich ihrer Unterstützung verschiedener Standards und Schnittstellen verglichen. Bei der Angabe zu den wichtigsten Import– und Exportfiltern wurde folgender Schlüssel verwendet:

Schlüssel	Dateiformate des Office-Paketes	Schlüssel	Dateiformate des Office-Paketes
1	MS Office	5	PDF
2	WordPerfect	6	MS Works
3	AmiPro	7	Rich Text Format (RTF)
4	StarOffice	8	Character Separated Values (CSV)

Tabelle 3.2: Dokumentenformate mit Schlüsselzuordnung

	StarOffice	OpenOffice	WordPerfect Office Suite	Koffice	MS Office	Lotus SmartSuite	MS Works	AppleWorks
Hersteller	Sun Microsystems	Sun Microsystems	Corel Corp.	KDE e.V.	Microsoft Corp.	IBM Corp.	Microsoft Corp.	Apple Computer Inc.
Betriebssystem								
MS Windows	×	×	×		×	×	×	
Linux	×	×		×				
Macintosh		×			×			×
andere	Solaris (SPARC, x86)					OS/2		
Lizenz								
Modell	kommerziell	GNU	kommerziell	GPL/LGPL	kommerziell	kommerziell	kommerziell	kommerziell
Programmcode	OpenSource	OpenSource	geschützt	OpenSource	geschützt	geschützt	geschützt	geschützt
Architektur								
Stand-alone Applikation	×	×	×	×	×	×	×	×
ASP	angekündigt (StarPortal)				×			
Standards								
Austauschformat	XML	XML	proprietär	XML	proprietär	proprietär	proprietär	proprietär
XML Import/Export	×	×	×	×	×	×		
XML Schema offen	×	×	×	×	×	Unbekannt		
Unicode / Internationalisierung	×	×	×	×	×	×	×	
HTML 4.0 / XHTML	×	×	×	×	×	×		×
CSS	×	×	×	×	×	×		×
Office								
Textverarbeitung	×	×	×	×	×	×	×	×
Tabellenkalkulation	×	×	×	×	×	×	×	×
Präsentationsprogramm	×	×	×	×	×	×		×
Zeichenprogramm	×	×	(×)	×	×	×		×
Post (E-Mail)	×				×	×		
Ablage					(×) nur E-Mail			
Kalender	×		×		×	×		
Import	1,2,3,7,8	1,4,7,8	1,7,8	1,2,3,7,8	1,2,3,6,7,8	1,7,8	1,7,8	1,7,8
Export	1,2,3,5,7,8	1,4,5,7,8	1,5,7,8	1,2,3,7,8	1,2,3,6,7,8	1,7,8	1,7,8	1,5,7,8
Schnittstellen								
ODMA			×		×	×		
ODA/OpenDocument		angekündigt		angekündigt				
MAPI	×	×			×	×	×	
IMAP	×				×	×		
HTTP 1.1	×	×	×		×	×		×
SyncML								
Umfrage Regierungspräsidium Leipzig								
Anzahl Nutzer	1	0	1	0	62	7	0	0

Tabelle 3.3: Vergleich des Funktionsumfangs von Officepaketen

3.6 Bürokommunikationssoftware in der öffentlichen Verwaltung

3.6.1 Anforderungen des Bundes

Mit dem Ziel die einseitige Abhängigkeit von einzelnen Herstellern zu lösen, wird der Einsatz von OpenSource-Software durch Beschlüsse des Bundestages und dem Bundesamt für Sicherheit in der Informationstechnik gefördert. Hinzu kommen Überlegungen durch die zu erwartenden Kostenvorteile, Sicherheitsaspekte (die sicherheitskritische Bewertung offener Systeme ist grundsätzlich besser möglich, als in geschlossenen Systemen), Verfügbarkeit und Wartung.

3.6.2 Anforderungen der Partner des RP Leipzig

Nach einer Umfrage des Regierungspräsidium Leipzig unter 71 grundsätzlich an Planfeststellungsverfahren beteiligten Institutionen nutzen 87 % der Befragten MS Office Pakete, 10 % Lotus SmartSuite und der Rest Sun StarOffice sowie Corel WordPerfect. Es ist anzunehmen, das hier auch vor allem ältere Programmversionen genutzt werden, so dass die in neueren Versionen teilweise gegebenen Möglichkeiten hinsichtlich des XML-Import und –Export nicht gegeben sind. Die — zumindest für den Prototyp zu schaffende Softwarearchitektur — hat dem insofern Rechnung zu tragen, das zumindest Teilnehmer mit dergleichen und/oder abwärtskompatiblem Programmversion Dokumente von anderen Teilnehmern erhalten und weiter verschicken können. Da die MS Office Formate von allen untersuchten Office-Paketen hinreichend gut unterstützt werden, sollten diese entsprechend genutzt werden.

3.7 Fazit

Die auf dem Markt befindlichen kommerziellen Office-Pakete bieten einen großen Funktionsumfang hinsichtlich der enthaltenen Programmpakete und Features. In der Praxis geht mit der Entscheidung für ein bestimmtes Office Paket auch die Entscheidung für ein bestimmtes Dokumentenformat einher. Die Nutzung plattformübergreifend nutzbarer Austauschformate (bspw. RTF und CSV) wird mit teilweise erheblichen Datenverlusten (insbesondere bei Formatierungen, Seitengestaltung, eingebetteten Objekten, etc.) erkauft. Die Etablierung offener Standards (bspw. ODA) kann als gescheitert betrachtet werden.

Die Nutzung XML-basierter Dokumentenformate erlaubt gegenüber den bisherigen, proprietären Dokumentenaustauschformaten die Speicherung aller Informationen zu einem Dokument. Ob diese Informationen von einem anderen Office Paket ausgewertet und korrekt interpretiert werden liegt primär an der Unterstützung der entsprechenden Funktionalität. Weiterhin müssen von einem Office Paket nicht verarbeitbare Informationen bei der Speicherung des Dokumentes nicht zwingend verloren gehen. Die aktive Unterstützung des XML Standard durch den Marktführer Microsoft Corp. lässt so eine Empfehlung zu Gunsten XML-basierter Dokumente zu. Zur Verteilung erstellter Dokumente ist das Portable Document Format (PDF) Dokumentenformat zu empfehlen, da entsprechende

Anzeigeprogramme für sehr viele Plattformen verfügbar sind und die direkte Erzeugung und Verteilung von PDF-Dokumenten direkt aus der Office-Umgebung möglich ist.

3.8 Kriterienkatalog

Bei der Erstellung von Bewertungskriterien für BKS ist zu berücksichtigen, dass es sich i. d. R. um fertige Softwarepakete handelt, welche zur täglichen Arbeit genutzt werden. Damit steht die Erweiterung oder Modifikation des BKS im Vergleich zur nahtlosen Integration in die bestehende IuK-Systemumgebung im Hintergrund.

Kriterium	Beschreibung
Kategorie: Hersteller/ Entwickler	
Lizenztyp	Office-Pakete werden i. d. R. als kommerzielle Produkte vertrieben. Dies hat allerdings keinen Einfluss auf dessen Einsatz innerhalb einer Verwaltung.
Verbreitung	Dokumenteninkompatibilitäten zwischen den verschiedenen Systemen und Probleme bei der Dokumentenkonvertierung legen den Einsatz eines möglichst weit verbreiteten BKS nahe.
Weiterentwicklung	Verschiedene BKS-Komponenten wie Browser und E-Mail-Client sind häufigen Änderungen unterworfen, Dokumentenkonvertierungskomponenten müssen beim organisationsübergreifenden Dokumentenaustausch aktuell gehalten werden. Daher sollte auf eine aktive Weiterentwicklung des BKS geachtet werden.
Modifizierbarkeit	Die Modifizierbarkeit eines BKS — im Sinne von Quellcodeänderungen — ist in der Praxis i. d. R. nicht notwendig und würde das Versionsmanagement unnötig erschweren.
Kategorie: Systemumgebung	
Betriebssystem	BKS sind i. d. R. nur für bestimmte Betriebssysteme verfügbar. Beim geplanten Einsatz eines BKS ist darauf zu achten, das in den jeweiligen BKS-Versionen alle benötigten Komponenten in der geforderten Versionierung für die im Einsatz befindlichen Betriebssysteme verfügbar sind.
Typ	BKS werden als Applikationen angeboten.
Schnittstellen	• zu BKS: Nutzung plattformübergreifend nutzbarer Austauschformate (bspw. RTF und CSV) • zu DMS: ODMA, WebDAV (siehe Kapitel DMS) • zu Sicherheitslösungen: API zur Ergänzung von Lösungen zur elektronischen Signatur und Dokumentenverschlüsselung (insb. E-Mail-Client)
Verteilung (Systemarchitektur)	Hinsichtlich der Integration der BKS in eine IuK-Systemumgebung sowie aus ggf. lizenzrechtlichen Fragen ist die Entscheidung für oder gegen den BKS-Einsatz im Rahmen des Application Service Providing entscheidend.

Kategorie: Standards	
BGG §7	BKS sollten vor allem hinsichtlich der Steuerung und Visualisierung von behinderten Personen benutzt werden können. In Abhängigkeit von Betriebssystem können hier verschiedene Standards existieren (bspw. Microsoft Active Accessibility (MSAA)).
XML	Moderne BKS unterstützen standardmäßig XML-basierte Dokumentenformate, welche mit Hilfe eines Transformators in andere Dokumentenformate transformierbar sind. Der Unterstützung XML-basierter Dokumentenformate sollte daher hohen Wert eingeräumt werden.
Flexibilität	Bis auf wenige Standardmodifikationen sind i. d. R. keine Änderungen in der Steuerung des Applikationsverhaltens notwendig. Office Pakete müssen hier grundsätzlich keine granularen Steuerungsmöglichkeiten besitzen.
Dokumentenformate	BKS müssen die innerhalb einer Organisation verwendeten Dokumentenformate verarbeiten können. Hier empfiehlt sich die Nutzung plattformübergreifend nutzbarer Austauschformate (bspw. RTF und CSV) oder grundsätzlich XML-basierter Dokumentenformate (bspw. OpenDocument, MS Word XML).
IT-Integration	BKS werden i. d. R. als fertige, vorkonfigurierte Softwarepakete ausgeliefert. Die Integration in eine bestehende IuK-Systemarchitektur muss daher ohne Modifikation des Softwarepaketes möglich sein.
Nutzerautorisation/ Nutzerauthentifikation	Die Anmeldung eines Nutzers und Prüfung der Zugriffsrechte erfolgt i. d. R. nicht innerhalb eines BKS, sondern mit Hilfe eines Dokumentenmanagementsystem und/oder des Betriebssystems.
Verschlüsselung	Die von BKS gebotenen Verschlüsselungsverfahren (siehe Kapitel Sicherheit) zur Dokumentenverschlüsselung sind oft als unsicher einzustufen und sollten nicht genutzt werden. Zur sicheren Ablage von Dokumenten sind Kryptografiefunktionen von Dokumentenmanagementsystemen zu nutzen. Ausnahme bilden Standardverschlüsselungsverfahren für Webbrowser und E-Mail.
Signatur	BKS unterstützen i. d. R. keine elektronische Signatur für Dokumente. Ausnahme bilden E-Mail-Clients, welche oft auf Grundlage gültig zertifizierter Schlüssel eine Signatur ausgehender E-Mails vornehmen können.
Kategorie: Features	
Internationalisierung	Eingesetzte Office-Pakete müssen in allen Komponenten gängige Unicode-Unterstützung bieten.
Archivierung	Archivierungsfunktionen werden i. d. R. von Dokumentenmanagementsystemen wahrgenommen. BKS benötigen diese Funktion daher — bis auf die Archivierung von ein– und ausgehender E-Mail — nicht.
Austauschbarkeit von Komponenten	Der Austausch einzelner Komponenten (Textverarbeitung, Tabellenkalkulation, etc.) eines BKS ist nicht notwendig und wird von keinem bekannten BKS unterstützt.

Tabelle 3.4: Kriterien für BKS

4 System– und Kriterienkatalog Geografische Informationssysteme

4.1 Einleitung

4.1.1 Was versteht man ganz generell unter GIS?

Geographische Informationssysteme (GIS) bilden ein wesentliches Hilfsmittel für die Erfassung, Modellierung, Analyse und Visualisierung raumbezogener Daten und bestehen aus Hard– und Softwareanwendungen, deren Funktion von der zugrunde liegenden Fachanwendung abhängig ist. Zu den Komponenten eines GIS gehören:

- das Datenmodell zur Speicherung der raumbezogenen Daten,
- die Geodaten (i.d.R in Form digitalisierter Raumdaten),
- Datenaustauschschnittstellen von und zu externen (Fach-)Anwendungen sowie
- Funktionen zur Modellierung, Analyse und Visualisierung der Geodaten.

Zu den wichtigsten Komponenten gehören die Geodaten, da diese in zeit– oder kostenintensiver Arbeit übertragen werden müssen. Daher lässt sich ein Geographisches Informationssystem auch als Menge sämtlicher in einem betrachteten Raum ermittelten Daten, die so strukturiert werden, dass aus ihnen auf bequeme Weise geeignete Zusammenstellungen zum Treffen von Entscheidungen erstellt werden können, definieren (vgl. [15]).

4.1.2 Drei Sichten eines GIS

Ein Geographisches Informationssystem bietet mehrere Sichten für die Arbeit mit geographischen Informationen:

Geodatenbank-Sicht Ein GIS ist eine raumbezogene Datenbank, deren Datensätze geographische Informationen bezüglich eines allgemeinen Datenmodells verkörpern (z. B. Eigenschaften, Rasterbilder, Topologien, usw.)

Visualisierungs-Sicht Ein GIS besteht aus einer Menge von „intelligenten“ Karten, welche Eigenschaften und deren Beziehungen zueinander auf der Erdoberfläche darstellen. Eine Vielzahl von Kartenansichten kann aus den zugrunde liegenden geographischen Informationen erzeugt werden, welche man als „Fenster in die Datenbank“ bezeichnen kann und die der Unterstützung von Abfragen, Analysen und Bearbeitungen dienen.

Verarbeitungs-Sicht Ein GIS besteht aus einer Anzahl von Werkzeugen zur Datentransformation welche neue geographische Daten aus den bereits existierenden Daten ableiten. Diese Geo-Verarbeitungsfunktionen entnehmen den vorhandenen Datensätzen Informationen, wenden darauf analytische Funktionen an und schreiben die Ergebnisse in neue Datensätze hinein.

4.1.3 Open GIS Consortium

Das „Open GIS Consortium“ (OGC)[1] ist eine international agierende, gemeinnützige Organisation, welche die Entwicklung von Standards für raumbezogene Dienstleistungen anführt. Das OGC arbeitet mit Regierungen, privaten Unternehmen und Hochschulen zusammen, um offene und erweiterbare Schnittstellen zur Softwareentwicklung für geographische Informationssysteme (GIS) und andere etablierte Technologien zu entwerfen. Anerkannte Spezifikationen[2] stellt das OGC der Öffentlichkeit kostenlos zur Verfügung.

4.1.4 Amtliches Topographisch-Kartographisches Informationssystem (ATKIS)

Die Vermessungsverwaltungen der Länder der Bundesrepublik Deutschland haben den gesetzlichen Auftrag, die Topographie des Landesgebietes zeitnah zu erfassen und nach einheitlichen Grundsätzen nachzuweisen und darzustellen. Mit dem Amtlichen Topographischen Informationssystem (ATKIS)[3], einem bundesweit einheitlichen Projekt der Arbeitsgemeinschaft der Vermessungsverwaltungen der Länder der Bundesrepublik Deutschland (AdV), wird die Topographie der Bundesrepublik Deutschland in einer geotopographischen Datenbasis beschrieben und in Form nutzungsorientierter digitaler Erdoberflächenmodelle bereitgestellt. Damit ist ATKIS die öffentlich-rechtliche Datenbasis für rechnergestützte digitale Verarbeitungstechnologien und die geotopographische Raumbezugsbasis für die Anbindung und Verknüpfung mit geothematischen Fachdaten. Es trägt den Charakter eines Geobasis-Informationssystems[4].

Zur einheitlichen topographischen Beschreibung des Gebietes der Bundesrepublik Deutschland stehen drei Modelle zur Verfügung:

- Die *Digitalen Landschaftsmodelle (DLM)* beschreiben die topographischen Objekte der Landschaft und das Relief der Erdoberfläche im Vektorformat. Die Objekte werden einer bestimmten Objektart zugeordnet und durch ihre räumliche Lage, ihren geometrischen Typ, beschreibende Attribute und Beziehungen zu anderen Objekten (Relationen) definiert. Jedes Objekt besitzt deutschlandweit eine eindeutige Identifikationsnummer (Identifikator).

  Dieses Modell wird in den Informationsdichten Basis-DLM, DLM50 (1:50.000), DLM250 (1:250.000) und DLM1000 (1:1.000.000) angeboten.

[1] `http://www.opengis.org/`
[2] `http://www.opengis.org/specs/`
[3] `http://www.atkis.de`
[4] `http://www.adv-online.de`

- *Digitale Topographische Karten (DTK)* sind Rasterdaten der vorliegenden Topographischen Kartenwerke. Die Rasterdaten sind nach kartographischen Inhaltselementen in verschiedene Ebenen gegliedert und können als einfarbige Einzelebenen sowie als einfarbige und farbige Kombinationsausgabe abgegeben werden.

  Hier gibt es die Karten in den Maßstäben DTK10, DTK25, DTK50, DTK100, DTK250 und DTK1000.

- *Digitale Geländemodelle (DGM)* sind in regelmäßigen Gittern oder unregelmäßig oder linienförmig angeordnete, in Lage und Höhe geokodierte Punktmengen, welche die Geländeformen der Erdoberfläche (Relief) beschreiben. Digitale Geländemodelle können außerdem ergänzende Angaben (z. B. Geländekanten, Gerippelinien, einzelne Geländehöhenpunkte) enthalten.

  Diese stehen in den Qualitätsstufen DGM5, DGM25, DGM50, DGM250 und DGM1000 zur Verfügung.

Allerdings wurde noch nicht die gesamte Fläche von Deutschland in jedem Maßstab digitalisiert. Während in den neuen Bundesländern bereits flächendeckend Digitale Topographische Karten im Maßstab 1:10.000 vorhanden sind, wird in den alten Bundesländern noch daran gearbeitet.

4.2 Grundanforderungen an GIS

4.2.1 Datenerfassung/Erstellung

Normalerweise ist es nicht mehr nötig, Karten in Papierform einzuscannen und zu digitalisieren, da dies bereits durch das ATKIS-Projekt vorgenommen wurde bzw. noch vorgenommen wird. Diese Daten können von den Vermessungsverwaltungen der Länder im Maßstab 1:5.000 bis 1: 100.000 oder vom Geodatenzentrum des Bundesamtes für Kartographie und Geodäsie[5] im Maßstab 1:250.000 bis 1:1.000.000 bezogen werden.

Ein relevanter Punkt ist dagegen, die Möglichkeit einzuräumen, Änderungen an bereits fertiggestellten Projektierungsdaten vornehmen zu können, bzw. Markierungen und Beschriftungen der Karte hinzuzufügen. In Hinsicht auf die spätere Verwendung des Systems ist dies insbesondere für Träger öffentlicher Belange von großer Bedeutung, falls in der jeweiligen Institution nicht bereits ein GIS installiert ist.

4.2.2 Analyse

Analysefunktionen bilden den Kern eines GIS. Erst durch die Möglichkeit aus den gegebenen Informationen neue Daten zu erzeugen und auszuwerten, entsteht ein vollwertiges und praktisch nutzbares System. Einfachste Analysefunktionen sind beispielsweise Filter– und Suchfunktionen, Entfernungsberechnungen, Adresssuche und ähnliches. Aber auch komplexere Berechnungen sind denkbar, z. B. Berechnung von Schallemissionen, Bestimmung von Überflutungsbereichen, Einteilung in Zuständigkeitsgebiete für Einsatzkräfte, Ermittlung von Staugefahrzonen und weitere.

[5] `http://www.geodatenzentrum.de/`

4.2.3 Visualisierung

Das Anzeigen der Daten gehört sicherlich zu den wichtigsten Anforderungen. Dabei muss es möglich sein, die Informationen entsprechend der benötigten Bedürfnisse zu filtern. Üblicherweise sind unterschiedliche Aspekte der Karte in verschiedenen Schichten (sog. Layern) untergebracht, die einzeln zu– und abgeschaltet werden können. Durch das Übereinanderlegen der einzelnen Schichten (vergleichbar mit transparenten Folien), erhält man einen Eindruck über die räumlich korrespondierenden Eigenschaften. Farbliche Kontraste unterstützen diesen Effekt.

4.2.4 Ausgabe/Verbreitung

Um die berechneten Daten auch Personen zur Verfügung zu stellen, die nicht über entsprechende Software zum Anzeigen der internen Datenformate verfügen, sollte es möglich sein von einem Webbrowser auf die von Servern bereitgestellten Karten zuzugreifen. Dabei muss der Inhalt nicht statisch hinterlegt sein, sondern kann von einem Server entsprechend der Spezifika einer Anfrage dynamisch und individuell erstellt werden. Eine andere Möglichkeit der Verteilung der Informationen ist das Abspeichern der Karten als Rasterbild und Versenden über die üblichen Kommunikationswege.

4.2.5 Datenkonvertierung

Üblicherweise werden geographische Daten, insbesondere während der Planung von Bauvorhaben, von mehreren verschiedenen Instanzen erzeugt und weiterverarbeitet. Je nach Anforderung an die durchzuführende Aufgabe, werden jeweils verschiedene Werkzeuge von unterschiedlichen Softwareherstellern verwendet. Dadurch bedingt fallen Daten in verschiedensten Formaten an, die nicht von jeder verwendeten Software universell verstanden werden. Es kann also notwendig sein, über einen Zwischenschritt, die Daten in ein zur Weiterverarbeitung lesbares Format zu konvertieren.

4.3 Systemkatalog

Die betrachteten GIS-Anwendungen und –werkzeuge können in Kategorien eingeteilt werden. Diese Einteilung ist nicht immer eindeutig, da einige Produkte vielseitig einsetzbar sind. Eine genaue Differenzierung der Anwendungen ist damit nicht immer sicher möglich. Zusätzlich ist zwischen Programmen unterscheiden, die reine, in sich geschlossene Anwendungen darstellen und solchen, die eine Entwicklerschnittstelle anbieten, und somit direkt in das eigene Projekte einbezogen werden können, sofern die verwendete Schnittstelle mit selbst genutzten Schnittstellen übereinstimmt. Die meisten hier dargestellten Bibliotheken wurden in Java geschrieben. Es gibt aber auch einige C/C++ Implementierungen.

Alle hier aufgeführten Produkte sind Open Source und stehen unter der GNU Public Licence. Die folgende Tabelle dient der groben Übersicht und Einordnung der Produkte:

Produkt	Einordnung	API	Sprache	Version	Datum
GDAL	Bibliothek: Raster Konverter	ja	C++	1.2.1	Jun 2004
Geocoder	Adresssuche	nein			ca. 2002
GeoServer	Map–/Feature-Server	ja	Java	1.2.0-rc2	Jun 2004
GeoTools	Developer Kit	ja	Java	2.0.RCO	Jul 2004
GisToolKit	Developer Kit	ja	Java	2.8.1	Jul 2003
GisToolKit Editor	Bearbeiten / Anzeigen	(ja)	Java	–	–
GisToolKit Server	Server	(ja)	Java	–	–
GML4J	Bibliothek: GML-Verarbeitung	ja	Java	1.03beta	Apr 2002
GRASS	Bearbeiten / Anzeigen	ja	C++	5.7.0	Jun 2004
JTS Topology Suite	Bibliothek: 2D-Algorithmen	ja	Java	1.4	Nov 2003
JUMP	Bearbeiten / Anzeigen	ja	Java	1.1.1	Dez 2003
Lx-Viewer	Anzeigen / Konvertieren	nein		2.01	Nov 2003
MapServer	Map-Server	Script	C++	4.2.1	Jul 2004
MySQL Spatial	Datenbankerweiterung	–	–		
NetMaps	Anzeigen (Client)	nein	Applet	2.0	1999/2000
OGR	Bibliothek: Vektor Konverter	ja	C++		
OpenSVGMapserver	Map-Server	Script	PHP	1.01	
PostGIS	Datenbankerweiterung	–	–	0.8.2	Mai 2004
PROJ.4	Bibliothek: Projektion	ja		4.4.8	Mai 2004
vec2web	Konvertieren	nein		0.1.5	Sep 2003

Tabelle 4.1: Übersicht: GIS Software

4.3.1 Serverlösungen

Serverprogramme dienen der Bereitstellung raumbezogener Daten, die zum Beispiel von einem netzwerkfähigen Browser abgerufen werden können. Dazu zählen neben den eigentlichen Kartendaten (Rasterbild des Kartenausschnitts) auch damit verknüpfte Attribute. Um auf Daten jeglicher Art zugreifen zu können, müssen Server Zugriff auf eine oder mehrere, unter Umständen auch unterschiedliche, Datenbanken haben, die eventuell auch verteilt organisiert sind. Datenbankzugriffe laufen für den Client (Browser) transparent ab.

Entsprechend der Spezifikation des OpenGIS Consortium hat ein Map Server drei Aufgaben:

1. Erzeugen einer Karte (als Rasterbild, als eine Folge grafischer Elemente oder als eine Menge von „geographic feature data“),
2. Beantworten einfacher Abfragen zum Inhalt der Karte,
3. Auskunft darüber geben, welche Art von Karten es erzeugen kann und für welche davon weitere Anfragen gestellt werden können.

Ein Standard-Webbrowser kann in erster Linie mit Hilfe von URLs (Uniform Resource Locator) entsprechende Anfragen an den Map Server richten. Der Inhalt einer solchen URL hängt davon ab, welche der drei Aufgaben benötigt werden. Alle URLs enthalten eine Versionsnummer der „Web Mapping Technology specification“ und einen Parameter mit dem Anfragetyp.

Zusätzlich gilt:

- Um eine Karte zu erzeugen, müssen die übergebenen Parameter Auskunft geben über: den abzubildenden Ausschnitt der Erde, das verwendete Koordinatensystem, die Typen von Informationen, die angezeigt werden sollen, das gewünschte Ausgabeformat und eventuell die Ausgabegröße, der Zeichenstil und anderes mehr.
- Um den Inhalt einer Karte abzufragen, enthalten die URL-Parameter die Position auf der Karte, welche von Interesse ist.
- Um den „Bestand“ des Map Servers abzufragen, müssen die URL-Parameter einen „capabilities“ Requesttyp enthalten.

Der OGC „Web Map Service“ erlaubt es Klienten Kartenbilder zu überlagern, die von verschiedenen Map Servern im Internet angeboten werden. In einer ähnlichen Weise erlaubt der OGC „Web Feature Service“ (WFS) einem Klienten raumbezogene Daten, die in GML (Geography Markup Language) kodiert sind, von unterschiedlichen Servern zu beziehen.

Die Anforderungen an einen „Web Feature Service“ sehen wie folgt aus:

- Schnittstellen müssen in XML definiert sein.
- GML muss verwendet werden, um Eigenschaften (features) innerhalb des Interfaces zu beschreiben.
- Ein WFS muss in der Lage sein, Eigenschaften mit Hilfe von GML darzustellen.
- Die Datenspeicherung der geographischen Eigenschaften muss für den Klienten transparent ablaufen. Die einzige Zugriffsmöglichkeit ist über das WFS-Interface.
- Die Benutzung einer Teilmenge der XPath-Ausdrücke für „referencing properties“.

GeoServer Der GeoServer[6] bietet eine vollständige transaktionsorientierte, unter der GPL veröffentlichte, Java-Implementierung (J2EE) der „Web Feature Server Specification“ des Open-GIS Consortiums inklusive einer integrierten Unterstützung für Web Map Service (WMS).

[6] `http://geoserver.sourceforge.net`

GISToolKit Server Der GISToolKit Server[7] ist ein einfacher Web Map Server (WMS) basierend auf der OGC „Web Map Service Specification“ und ist Bestandteil der GISToolKit Entwicklerbibliotheken. Datenquellen (ESRI Shape File, PostGIS Database, DB2 Spatial Extender Database, ImageFile for image layers) können dynamisch hinzugefügt werden. Der Server ist unter der LGPL veröffentlicht. Die Administration des Servers erfolgt über ein webbasiertes Interface.

MapServer Der MapServer[8] stellt eine komplette Entwicklungsumgebung in der Programmiersprache C/C++ zur Erstellung von internetbasierten Anwendungen in Bezug auf die Behandlung raumbezogener Daten zur Verfügung. Die Anwendungen können bspw. zur dynamischen Kartenerzeugung, der Abbildung von Browserfunktionalitäten in geographischen Karten und Informationsabruf dienen. Zur Anbindung von Skriptsprachen wie PHP, Perl und Python (Java in Kürze) an die servereigene C-API enthält der Server die Skriptsprache MapScript. MapServer ist ohne lizenzrechtliche Einschränkungen nutzbar. Verfügbare Geodaten lassen sich über (fast) beliebige Datenbanken einbinden (bspw. Oracle, Sybase, MySQL). MapServer unterstützt eine Reihe Vektorformate (ESRI shapefiles, PostGIS, ESRI ArcSDE, viele andere über OGR) und Rasterformate (TIFF/GeoTIFF, EPPL7, viele andere über GDAL).

OpenSVGMapserver Der OpenSVGMapserver[9] besteht aus einer Anzahl in der Skriptsprache PHP entwickelten Komponenten (lauffähig auf allen Webservern, welche eine PHP-Unterstützung bieten), welche aus raumbezogenen Daten in einer MySQL-Datenbank dynamisch Karten im Dokumentenformat SVG generieren. Die vom Server erzeugten SVG-Dokumente können mit einem beliebigen SVG-Viewer (bspw. als PlugIn innerhalb des Webbrowsers) betrachtet werden. OpenSVGMapserver ist unter der GPL veröffentlicht. Da bis zum aktuellen Zeitpunkt keine stabile Version des Servers verfügbar ist, wird der produktive Einsatz von OpenSVGMapserver nicht empfohlen.

4.3.2 Entwicklerbibliotheken

Die hier vorgestellten Bibliotheken bieten eine große Vielfalt an Funktionen, angefangen vom Einlesen von raumbezogenen Daten aus verschiedensten Datenquellen, über Transformationen der Daten bis hin zum Darstellen relevanter Aspekte der eingelesenen Quellen.

GeoTools Das GeoTools Toolkit[10] erlaubt die Entwicklung OpenGIS-konformer Softwarelösungen in Java. Die Standards des OpenGIS Consortiums (OGC) werden entsprechend umgesetzt. Als Datenformate werden Shapefile, ArcGrid, ArcSDE, Postgis, Oracle Spatial, MySQL unterstützt. Neben Funktionen zum Laden und Speichern von Daten, steht auch ein großer Funktionsumfang für die Darstellung der Daten zur Verfügung.

[7] `http://gistoolkit.sourceforge.net/Server.html`
[8] `http://mapserver.gis.umn.edu/index.html`
[9] `http://www.carto.net/projects/open_svg_mapserver/`
[10] `http://www.geotools.org`

GISToolKit Das auf Java basierende GISToolKit[11] enthält einen Server und einen Editor. GISToolKit liest geographische Daten aus beliebigen Quellen (DB2 Spatial Extender, ESRI SDE, Terraserver, 1.0.0 OGC Web Map Services, ESRI Shapefiles, POSTGIS database) und stellt diese dar. Mit Hilfe des Editors können die Geodaten auch direkt in der Datenquelle geändert werden.

GML4J GML4J[12] stellt eine Java-API zum Lesen von GML-Dokumenten (Geography Markup Language) zur Verfügung. GML ist ein offener Standard zur XML-basierten Speicherung von Geodaten. GML4J erlaubt die Auswertung der innerhalb von GML-Dokumenten verwendeten XML-Elemente.

PROJ.4 PROJ.4[13] enthält eine Bibliothek mit Funktionen für kartographische Projektionen (Koordinatentansformation). Es existieren fertige Bibliotheken für MS Windows (DLL) und Linux. PROJ.4 wird unter anderem in GRASS, MapServer, PostGIS, Thuban, OGDI und OGRCoordinateTransformation eingesetzt.

JTS Topology Suite Die JTS Topology Suite[14] bietet eine vollständige, einheitliche und robuste Implementierung von grundlegenden 2D-Algorithmen in Java und richtet sich nach der „Simple Features Specification for SQL“ veröffentlicht vom OpenGIS Consortium. Hervorzuheben ist die hohe Performance und Stabilität als Kriterien für den Einsatz in Produktivsystemen.

GDAL Die GDAL[15] C++-Konverter-Bibliothek für geographische Raster-Datenformate bietet ein abstraktes Datenmodell für die aufrufende Applikation. Anwendungen können damit in einer standardisierten Form auf Geodaten in den unterschiedlichsten Datenformaten zugreifen. GDAL unterstützt inkl. Einiger Rasterbild-Formate über 40 Dokumentenformate.

OGR Die C++-Bibliothek OGR[16] bietet Lese– und teilweise Schreibzugriff auf verschiedene Vector-Datei-Formate wie bspw. ESRI Shapefiles, S-57, SDTS, Post-GIS, Oracle Spatial und Mapinfo mid/mif und TAB Formate. OGR ist Teil der GDAL Konverter-Bibliothek.

4.3.3 Anzeige– und Bearbeitungssoftware

GISToolKit Editor Der GISToolKit Editor[17] erlaubt die Visualisierung von Geodaten und die Anwendung von einfachen Operationen. Der Editor ist Bestandteil der GISToolKit Entwicklerbibliotheken und erlaubt daher das Lesen und Schreiben aus bzw. in eine Vielzahl von Datenbanken und Dokumentenformaten.

[11] http://gistoolkit.sourceforge.net/
[12] http://gml4j.sourceforge.net/
[13] http://www.remotesensing.org/proj/
[14] http://www.vividsolutions.com/JTS/jts_frame.htm
[15] http://www.remotesensing.org/gdal/
[16] http://www.remotesensing.org/gdal/ogr
[17] http://gistoolkit.sourceforge.net/Editor.html

JUMP Ähnlich dem GISToolKit Editor ist JUMP[18] Bestandteil der JTS Topology Suite und bietet eine interaktive Arbeitsoberfläche zum Betrachten, Editieren und Verarbeiten von raumbezogenen Daten. JUMP bietet gleichzeitig eine API für Entwickler mit vollem Zugriff auf alle Funktionen des Editors, welcher darüber hinaus modular erweiterbar ist. Die in Java entwickelte Anwendung unterstützt wichtige Industriestandards wie die GML und das OpenGIS Consortium spatial object model.

LX-Viewer Der LX-Viewer[19] ermöglicht das Anzeigen, Drucken (Postscript) und Speichern von DWG– und DXF-Dokumenten sowie die Dokumentenkonvertierung in die Bilddateiformate BMP, SVG und PNG. Zur besseren Visualisierung können 3D-Modelle verschoben, vergrößert und gedreht werden.

NetMaps NetMaps[20] ist ein JavaApplet zur Visualisierung von vektorbasierten Karten in einem Webbrowser. Es werden die Datenformate ArcInfo shape-Dateien (SHP/DBF) und MapInfo MIF/MID unterstützt.

4.3.4 Konverter

Konverter eignen sich sehr gut, um Daten aus verschiedenen Quellen in unterschiedlichen Formaten in ein einheitliches Format umzuwandeln, welches dann weiterverarbeitet werden kann. Konverter können so als Mittler fungieren, wenn die datenverarbeitende Software nicht alle benötigten Eingabeformate lesen kann.

vec2web Das Tool vec2web[21] (vector to web) ermöglicht die Konvertierung von DXF-Dokumenten in die Bilddokumentenformate (Rasterformate) BMP, GIF, JPEG, PNG, XPM, XBM, PBM, PGM, PPM, Postscript und DXML.

GRASS (Geographic Resources Analysis Support System) GRASS[22] ist ein Geographisches Informationssystem zur Verarbeitung von Raster– und Vektordaten, welches eine umfangreiche GIS-Bibliothek bietet. Die Rasterformate ASCII, ARC/GRID, E00, GIF, GMT, TIF, PNG, ERDAS LAN, Vis5D, SURFER und die Vektorformate ASCII, ARC/INFO ungenerate, ARC/INFO E00, ArcView SHAPE, BIL, DLG (U.S.), DXF, DXF3D, GMT, GPS-ASCII, USGS-DEM, IDRISI, MOSS, MapInfo MIF, TIGER, VRML können gelesen und geschrieben werden. Neben diesen umfangreichen Möglichkeiten im Bereich der Dokumentenkonvertierung ist eine Geodatenvisualisierung auf verschiedensten Plattformen möglich und Funktionen zur räumlichen Analyse, Kartengenerierung, Datenmodellierung und –speicherung (Datenbankschnittstelle) enthalten.

[18] `http://www.vividsolutions.com/jump/`
[19] `http://lx-viewer.sourceforge.net/`
[20] `http://www.sitex.ro/netmaps/`
[21] `http://www.ribbonsoft.com/vec2web.html`
[22] `http://grass.itc.it/`

4.3.5 Sonstiges

MySQL Spatial Entsprechend der „OpenGIS Simple Features Specifications For SQL“ [16] stellt MySQL Spatial[23] eine Erweiterung der Datenbank MySQL zur Erzeugung, Ablage und Analyse geographischer Daten dar. Die Erweiterung ist innerhalb des MySQL-Paketes ab Version 4.1 enthalten. Zum Datenaustausch mit anderen Systemen werden die Text– und Binärdokumentenformate WKT und WKB bzgl. des Datenimport und –export unterstützt.

PostGIS Entsprechend der „OpenGIS Simple Features Specifications For SQL“ stellt PostGIS[24] eine Erweiterung der Datenbank PostgreSQL zur Erzeugung, Ablage und Analyse geographischer Daten dar.

4.4 Kriterien

Bei der Erarbeitung von Kriterien zur Auswahl zu nutzender GIS-Software bzw. entsprechender Basistechnologien und Werkzeuge sind folgende Gesichtspunkte zu beachten:

- Existierende Richtlinien oder Empfehlungen zur Auswahl der Systeme
- Nutzung möglichst weit verbreiteter, offener Systeme
- Einsatz von freier Software
- Soll fertiges GIS-System oder offenes GIS-Framework genutzt werden

Zur konkreten Entscheidung sind folgende Kriterien zu berücksichtigen:

- System/Framework: Welche Dokumentenformate/Datenbanken/Datenformate sollen genutzt werden?
- System/Framework: Welche Betriebssysteme müssen unterstützt werden?
- Framework: Sind die Bibliotheken/APIs in der gewünschten Programmiersprache nutzbar?
- System/Framework: Ist der Funktionsumfang ausreichend?
- System/Framework: Weiterentwicklung des Produktes und Stabilität der Implementierung?

Kriterium	Beschreibung
Kategorie: Hersteller/ Entwickler	
Lizenztyp	Der konkrete Lizenztyp eines GIS ist lediglich unter kaufmännisch-rechtlichen Gesichtspunkten sowie dem Aspekt der Verbreitung und Weiterentwicklung / Modifizierbarkeit zu betrachten. Werden Frameworks genutzt, ist zu berücksichtigen, welchen Einfluss die Lizenz des Frameworks auf die Nutzung und Verwendung der daraus hergestellten Applikation besitzt.

[23] `http://www.mysql.com/doc/en/Spatial_extensions_in_MySQL.html`
[24] `http://postgis.refractions.net/`

Verbreitung	Der Einsatz weit verbreiteter, offener Systeme ist unter dem Gesichtspunkt der Kompatibilität der Dokumentenformate beim Dokumentenaustausch bzw. der verteilten Bearbeitung zwischen GIS-Nutzern stark hervorzuheben.
Weiterentwicklung	Zum Dokumentenaustausch mit anderen, ggf. organisationsfremden GIS-Nutzen muss der Dokumentenimport und –export mit den aktuellen Dokumentenformaten anderer GIS arbeiten können. Der ständigen Weiterentwicklung des eingesetzten GIS ist daher ein hoher Stellenwert zuzuordnen.
Modifizierbarkeit	Die Gewichtung der Modifizierbarkeit eines GIS ist davon abhängig, ob ein fertiges GIS-System oder ein offenes GIS-Framework genutzt werden soll. Fertige Systeme müssen und dürfen i. d. R. nicht modifiziert werden, offene Frameworks bilden i. d. R. nur bestimmte Teilbereiche eines GIS ab und sind speziell für die Ergänzung / Modifikation gedacht.
Kategorie: Systemumgebung	
Betriebssystem	GIS werden als Serverlösungen betrieben oder sind aus Entwicklerbibliotheken für einen individuellen Anwendungszweck zusammengestellt wurden. Hinsichtlich des Betriebssystems ist auf die Verfügbarkeit von Frontends für das von den potentiellen Nutzern genutzte Betriebssystem zu achten.
Typ	Die Entscheidung zwischen einem fertigen GIS-System und einem offenen GIS-Framework ist davon abhängig zu machen, in welchem Maße Individualisierungen des GIS notwendig sind oder nur spezielle Funktionen/Teilbereiche eines GIS genutzt werden.
Schnittstellen	GIS sollten über ein definiertes API zu steuern sein.
Verteilung (Systemarchitektur)	GIS werden i. d. R. als Serverlösungen betrieben, welche Ihre Dienste über ein proprietäres API oder Skriptsprache zur Verfügung stellen.
Kategorie: Standards	
BGG §7	Sofern GIS über Clientapplikationen verfügen, sollten diese hinsichtlich der Steuerung und Visualisierung von behinderten Personen benutzt werden können. In Abhängigkeit von Betriebssystem können hier verschiedene Standards existieren (bspw. Microsoft Active Accessibility (MSAA)). GIS Serverlösungen, welche für andere Komponenten einer IuK-Systemlandschaft Dienste erbringen (bspw. Kartendaten visualisieren), sind davon nicht betroffen. Es ist Aufgabe der aufrufenden Komponente die erhaltenen Daten ggf. so aufzubereiten, dass diese von behinderten Personen genutzt werden können.
Ergonomie	Ergonomische Anforderungen treffen lediglich auf GIS-Clientapplikationen zu.
XML	GIS sollten die Dokumentenformate VRML und SVG unterstützen.

Dokumenten-formate	GIS müssen die innerhalb einer Organisation verwendeten Dokumentenformate verarbeiten können. Hier empfiehlt sich die Nutzung plattformübergreifend nutzbarer Austauschformate (bspw. DXF) oder grundsätzlich XML-basierter Dokumentenformate (bspw. SVG) sofern in ihnen alle zur Weiterbearbeitung notwendigen Informationen integriert werden können.
Kategorie: Sicherheit	
IT-Integration	GIS Serverlösungen sollten ihre Dienste allen Beteiligten transparent zur Verfügung stellen und über die gebotene API alle benötigten Funktionen bereitstellen. Über die individuelle Entwicklung eigener Softwarekomponenten kann damit eine nahtlose Integration in bestehende IuK-Systemlandschaften sichergestellt werden.
Nutzerauto-risation/ Nutzerauthen-tifikation	GIS bieten i. d. R. keine Möglichkeit zur Autorisation und Authentifikation einzelner Nutzer sowie einer darauf basierenden Freischaltung bzw. Sperrung von Diensten und Dokumenten oder die Generierung nutzerspezifischer Sichten auf Kartenmaterial. Trotzdessen ist diese Anforderung innerhalb öffentlicher Verwaltungen bei der Bearbeitung organisationsübergreifender Verwaltungsprozesse zu berücksichtigen und bspw. Durch eine Kapselung der GIS-Funktionalitäten sicherzustellen.
Verschlüsselung	Die verschlüsselte Speicherung von Kartendaten muss von einem GIS nicht unterstützt werden, da die Verschlüsselung und Signatur von GIS-Dokumenten mit Hilfe entsprechender Komponenten innerhalb der verwendeten Bürokommunikationssoftware erfolgen kann. Bietet das GIS einen Map-Server, welcher visualisierte Kartendaten innerhalb des Intra–/Internet bereitstellt, sollte die verschlüsselte Übertragung unter Nutzung des HTTPS unterstützt werden.
Signatur	Zur Signatur von GIS-Dokumenten können Komponenten der Bürokommunikationssoftware (bspw. E-Mail) oder innerhalb eines integrierten Systems enthaltene Sicherheitskomponenten (bspw. Virtuelle Poststelle mit Signierdiensten) genutzt werden.

Tabelle 4.2: Kriterien für GIS

5 System– und Kriterienkatalog Sicherheitskomponenten

5.1 Einleitung

Die elektronische Umsetzung von Verwaltungsvorgängen innerhalb der IuK-Infrastruktur der öffentlichen Verwaltung erfordert die Beachtung verschiedener datenschutzrechtlicher Vorgaben unter Berücksichtigung der jeweiligen Kommunikationsweg-spezifischen Anforderungen. Dies bedingt einerseits die Berücksichtigung von Aspekten der Datensicherheit (Verfügbarkeit, Datenintegrität, Verbindlichkeit und Vertraulichkeit) und des eigentlichen Datenschutzes (i.S. des Schutzes von Daten vor Missbrauch).

Innerhalb von Verwaltungsverfahren müssen zum einen Teile der Daten eines in Bearbeitung befindlichen Verfahrens öffentlich zugänglich gemacht werden. Des Weiteren ist eine standardisierte Kommunikationsplattform notwendig, über die, trotz der Heterogenität der verwendeten Systeme, eine vertrauliche Kommunikation mit den ggf. räumlich verteilten Institutionen möglich ist. Dies gilt insbesondere dann, wenn Daten innerhalb eines räumlich verteilt zu bearbeitenden Verwaltungsprozesses zu verarbeiten sind. Die bisherigen Annahmen einer sicheren Übermittlung von Dokumenten auf postalischem Weg lassen sich nicht auf Computernetzwerke als Pendant zur Post übertragen. Durch den Aufbau und die Funktionsweise der elektronischen Nachrichtenübertragung einiger Netze (insb. des Internet) lassen sich keine sicheren Transportwege und Zwischenstationen garantieren. Um dennoch auf die weit ausgebaute Infrastruktur des Internet als Übertragungsmedium für sensible Daten zurückgreifen zu können, ist ein Transport in verschlüsselter Form notwendig.

Die folgenden Abschnitte beschränken sich auf die ausschließliche Betrachtung TCP/IP-basierter Netzwerke, weil:

- innerhalb der öffentlichen Verwaltungen i. d. R. die dafür notwendigen, technischen Voraussetzungen gegeben sind und
- die Einbindung räumlich verteilter und teilweise ausschließlich über öffentliche Netze einzubindende Teilnehmer von Verwaltungsverfahren eine Nutzung des Internet nahe legen.

5.2 Aspekte der Datensicherheit

5.2.1 Verfügbarkeit

Aufgabe der Datensicherheit ist es, eine möglichst hohe Verfügbarkeit aller zur Arbeit notwendigen sowie auf Anfrage bereitzustellenden Daten (bspw. im Rahmen von technisch-organisatorischen Maßnahmen zur Revisionssicherheit) innerhalb einer Institution (bspw.

Behörde, Verwaltung, etc.) zu garantieren. Hardwareseitig erfordert dies eine möglichst räumlich getrennte und entsprechend gesicherte (Zugangs–, Brand–, Wasserschutz) Bereitstellung von Rechentechnik zur Datenspeicherung, eine schnelle, möglichst im laufenden Betrieb austauschbare Speicherhardware und ausfallsichere Speicherung der Daten (bspw. mit Hilfe eines RAID Systems [17]) sowie der Einsatz von Backupsystemen. Unabhängig von der ggf. konkreten physischen oder logischen Verteilung von Daten auf mehrere Speicherorte muss ein transparenter Zugriff auf die Daten und Dokumente seitens der Benutzer erfolgen können.

5.2.2 Integrität

Die Sicherung der Datenintegrität dient dem Schutz der Daten vor ungewollten Modifikationen. Dazu zählen Veränderungen der Daten durch Fehler in Hard– und Softwaresystemen, gezielte Datenlöschung oder –veränderung durch Schadroutinen (Computerviren, –würmer) und Angriffe (Hackerangriffe, gezielte Nutzung von Fehlern in Clientsoftware) sowie Modifikationen durch bewusste oder unbewusste Aktionen des Benutzers. Für jede Klasse der möglichen Datenintegritätsverletzungen können geeignete Maßnahmen zum Schutz der Datenintegrität getroffen werden:

Verletzung der Datenintegrität durch	Maßnahmen zum Schutz der Datenintegrität
Hardwarefehler	• (Physisch) Redundante Speicherung der Daten Einsatz von Backupsystemen
Softwarefehler	• Einspielen von laufenden Softwareupdates Einsatz von Backupsystemen
Computerviren und Computerwürmer	• Einsatz von Antivirensoftware und laufende Aktualisierung der Virendatenbank
Hackerangriffe, Nutzung von Fehlern in Browsersoftware	• Laufendes (wenn möglich automatisiertes) Einspielen von Betriebssystem– und Browsersoftwareupdates • Einsatz eines Firewalls oder komplette physische Trennung des Intranet von anderen, externen Netzen • Einsatz digitaler Signaturen und von Message Authentication Codes (MACs), d. h. elektronischer Zeitstempel einer vertrauenswürdigen Instanz
Benutzer	• Zentrale Benutzerverwaltung und Zugriffssteuerung mit möglichst granular zu vergebenden Rechten

Tabelle 5.1: Datenintegritätsverletzungen und Schutzmaßnahmen

5.2.3 Verbindlichkeit

Mit der Verbindlichkeit wird die Authentizität, d. h. die Echtheit des Urhebers, und die Dokumentenintegrität, d. h. die Unverfälschtheit eines elektronischen Dokumentes gegenüber seinem Original, sichergestellt. Beide Ziele lassen sich durch Einsatz digitaler Signaturen, d. h. dem Nachweis, dass nur eine bestimmte Person einen Datenblock verschlüsselt haben kann, erreichen. Mit dem Signaturgesetz (SigG) und der Signaturverordnung (SigV) wurden in der Bundesrepublik die notwendigen gesetzlichen Voraussetzungen zur Gleich-

stellung der (qualifizierten) elektronischen Signatur und der handschriftlichen Unterschrift geschaffen. Die Sicherstellung der Verbindlichkeit darf dabei die Integrität des Dokumentes nicht verletzen, was beim Einsatz der oben genannten Verfahren sichergestellt ist.

5.2.4 Vertraulichkeit

Das Vertrauen in die elektronische Kommunikation setzt neben dem Schutz der Verbindlichkeit durch Dokumentenintegrität den Schutz vor unberechtigter Kenntnisnahme und Vervielfältigung voraus. Diese Anforderungen bedingen einerseits den Schutz der kabelgebundenen und drahtlosen Netzwerkkommunikation vor unzulässigem Zugriff sowie die Verschlüsselung der Kommunikation auf Netzwerk– und Dokumentenebene.

Die Netzwerkkommunikation kann dazu mit Hilfe einer Stromverschlüsselung (sog. Online-Algorithmen) oder Blockchiffrierung (hier i. d. R. relativ kleine Datenblöcke) kodiert werden. Der zu übertragende Klartext wird dabei zeichen– oder bitweise verschlüsselt. Genauso können elektronische Dokumente mit Hilfe eines Blockchiffre kodiert werden. Bei den dazu eingesetzten Verfahren kann unterschieden werden zwischen:

- *symmetrischen Kryptosystemen (Secret-Key-Kryptosystemen)*
  Verwendung eines Schlüssels zur Ver– und Entschlüsselung der chiffrierten Daten. Dieser Schlüssel muss allen Kommunikationspartnern bekannt sein.
- *asymmetrischen Kryptosystemen (Public-Key-Kryptosysteme)*
  Verwendung eines Schlüsselpaares zur Ver– und Entschlüsselung von Daten. Mit Kenntnis eines Schlüssels ist in keinem (momentan) vertretbaren Aufwand der zum Schlüsselpaar gehörige zweite Schlüssel berechenbar.
- *Hybridverfahren*
  Kombination von symmetrischen und asymmetrischen Kryptosystemen

Die Sicherheit eines gewählten kryptografischen Verfahrens sollte dabei zwingend

- von der Geheimhaltung der gewählten Schlüssel und nicht des verwendeten Verfahrens abhängen,
- einfach zu bedienen sein und sich möglichst nahtlos in die technisch-organisatorischen Gegebenheiten des Arbeitsplatzes einfügen und
- mit einfach zu merkenden oder einzusetzenden Schlüsseln (bspw. PIN, Cryptocard, etc.) arbeiten.

In der Regel sind diese Bedingungen mit Einhaltung des sog. Kerckhoff-Prinzips[1] erfüllt.

5.3 Kommunikationsnetzwerke

Bei der Betrachtung von elektronischen Kommunikationsnetzwerken im öffentlichen Sektor lassen sich drei verschiedene Klassen unterscheiden:

1. die Kommunikation innerhalb einer Verwaltung *(internes Netzwerk)*

[1] Als Designkriterium für kryptografische Verfahren nach Auguste Kerckhoff von Nieuwenhof (*1835, †1903) in „La Cryptographie militaire“, 1883

2. die Kommunikation mit anderen Verwaltungen *(behördenübergreifende Netzwerke)*
3. die Kommunikation mit Trägern öffentlicher Belange sowie Bürgern bzw. externen Institutionen *(externe Netzwerke)*

Internes Netzwerk Unter einem internen Netzwerk soll das Intranet einer jeden einzelnen Verwaltung verstanden werden. Da es sich hier oft um komplexe, zum Teil langfristig aufgebaute, Infrastrukturen handelt, sollten Änderungen nur dann vorgenommen werden, wenn diese wichtige Voraussetzungen für notwendige Ziele sind oder entscheidende Verbesserungen mit sich bringen. Zur Absicherung der Kommunikation webbasierter Dienst der Bearbeiter mit einem Server können verschlüsselte Verbindungen (bspw. über eine optionale Sicherheitsschicht im Protokoll-Stack von HTTP → HTTPS, WAP → WTLS[2], etc.) genutzt werden. Dies bietet eine einfache Möglichkeit, die einzelnen Verbindungen vor unzulässiger Modifikation und Kenntnisnahme zu schützen. Die dazu notwendige Verteilung eines lokalen Server-Zertifikates auf den Rechnern von Verwaltungen kann als mit einem vertretbaren Aufwand verbunden angesehen werden. Zur Abtrennung und zum Schutz der Schnittstellen zu externen Netzwerken kann eine sog. Firewall Einsatz finden. Damit kann die Gefahr einer missbräuchlichen externen Nutzung falsch konfigurierter Dienste reduziert werden.

Behördenübergreifende Netzwerke Die zweite Gruppe der Netzwerke, oft auch als G2G (government to government) bezeichnet, erfordert einen höheren Sicherungsaufwand. Existieren zwischen den kommunizierenden Verwaltungen bereits Netzwerke, die schon den Anforderungen an die Sicherheit genügen, stellt dies den einfachsten Fall dar. Beispiele für derartige Behördennetze, die eine sichere Kommunikation ermöglichen, sind TESTA[3] (Trans-European Services for Telematics between Administrations) sowie IVBV[4] (Informationsverbund der Bundesverwaltung).

Besteht kein solches sicheres Netzwerk, erfolgt die Kommunikation über die existierende Internetanbindung der Behörden. In diesem Fall empfiehlt es sich, die Daten auf ihrem Weg durch die öffentlichen Netze zu verschlüsseln. Für diesen Einsatzzweck steht bereits das offene und weit verbreitete Protokoll IPSec zur Verfügung, wofür Implementierungen auf allen gängigen Betriebssystemen existieren. Für die Verschlüsselung benötigen die kommunizierenden Rechner der Behörden jeweils ein Schlüsselzertifikat der Kommunikationspartner. Die händische Verteilung dieser Schlüsselzertifikate wird jedoch mit der Zunahme beteiligten Behörden schnell unpraktikabel. In diesem Fall empfiehlt sich eine hierarchische Verwaltung der Zertifikate. Eine vertrauenswürdige, zentrale Instanz wäre sowohl für die Erstellung, als auch für die Bereitstellung der Zertifikate verantwortlich. Die Verwendung standardisierter Techniken erleichtert eine eventuelle Integration in andere landes– oder bundesweite Schlüsselhierarchien.

Externe Netzwerke Die externen Netzwerke, also jene, in denen eine Verwaltung mit anderen öffentlichen und privatwirtschaftlichen Institutionen und Bürgern kommuniziert, stellen die dritte Klasse der Kommunikationsnetzwerke. Für diese werden auch die Begriffe G2C (government to citizen) und G2B (government to business) verwendet. Da nicht mit

[2] Wireless Transport Layer Security
[3] `http://www.koopa.de/produkte/testa.html`
[4] `http://www.kbst.bund.de/Behoerdennetze/-,66/IVBV.htm`

jeder Institution bzw. jedem Bürger auf elektronischen Weg kommuniziert werden kann bzw. aus service– und gesetzesorientierter Sicht kein Zwang zur Nutzung elektronischer Angebote ausgeübt werden soll, kann es hier zu notwendigen Medienbrüchen kommen. Maßnahmen zum Schutz elektronischer Dokumente können hier zwangsläufig nicht mehr greifen.

Sollen Daten in externen Netzwerken ausgetauscht werden, so ist zu bedenken, dass sie in den öffentlichen Netzen vielen Angriffsmöglichkeiten ausgesetzt sind. Um die Authentizität (Echtheit des Absenders) und die Integrität (Unverfälschtheit) der Daten zuzusichern, können digitale Signaturen eingesetzt werden. Bei der Übertragung vertraulicher Daten sollte zusätzlich noch eine Verschlüsselung zum Einsatz kommen. Durch den elektronischen Datenaustausch sowie die Bereitstellung elektronischer Dienste durch die Behörden ergeben sich jedoch auch neue Gefahren. Die Infrastruktur ist nun zusätzlich vor Viren, Würmern und anderen „Schädlingen“ sowie Angriffen aus externen Netzen zu schützen.

Für die Begrenzung der zulässigen Kommunikation zwischen internem und externem Netz empfiehlt sich der Einsatz einer sog. Firewall, die eine Filterung der Verbindungen basierend auf vordefinierten Regeln realisiert. Sollen in einer Behörde Server betrieben werden, die externe Dienste anbieten, stellen diese ein mögliches Ziel für Angriffe dar, die die Sicherheit des internen Netzes gefährden. Aus diesem Grund empfiehlt es sich, derartige Server in eine gesonderte, auch zum internen Netz gefilterte Umgebung zu stellen, wodurch das Risiko minimiert wird. Für diese gesonderten Netze wird häufig der aus dem militärischen Sprachgebrauch geborgte Begriff „Demilitarisierte Zone“, kurz DMZ, verwendet.

5.4 Dokumentensignierung und –verschlüsselung

Während der Schutz der Kommunikationsnetzwerke durch physische Trennung von öffentlichen Netzwerken und Kommunikationsverschlüsselung dem Schutz einer Gruppe von einzelnen Institution garantiert, dient die Signierung und Verschlüsselung einzelner Dokumente dem Vertrauen und dem Schutz vor unberechtigter Einsichtnahme und Modifikation durch Mitglieder der Institutionen.

5.4.1 Webdokumente

Der Schutz von Webdokumenten im weiteren Sinne, d. h. Dokumentenanforderungen und –übermittlungen für stationäre und mobile Endgeräte, erfolgt i. d. R. auf Ebene der Kommunikationsnetzwerke. Dazu wird eine Sicherheitsschicht im Protokoll-Stack des primär verwendeten Netzwerkprotokolls genutzt. Diese Sicherheitsschicht nutzt ein geeignetes kryptographisches Verfahren, um alle zu übertragenden Dokumente und Metadaten zu verschlüsseln. Als Standard wird hier eine SSL/TLS-Verschlüsselung [18], unter Verwendung eines Diffie-Hellman-Schlüsselaustausches, genutzt. Mit Hilfe von X.509 Zertifikaten erlaubt SSL/TLS die Authentifikation des Servers und (optional) des Client. Das Zertifikat des Servers muss dabei von einer Stelle innerhalb eines hierarchischen Systems von Zertifizierungsstellen (en: certificate authority – CA) erstellt wurden sein und die betreffende Zertifizierungsstelle vom Clients als vertrauenswürdig akzeptiert werden.

Werden zur Kommunikation mehrere Gateways genutzt, muss bedacht werden, dass die zu übertragenden Nutzdaten auf dem Gateway im Klartext vorliegen. Die scheinbar sichere Anforderung eines WML-Dokumentes auf einem Webserver über das WAP (bspw. von einem mobilen Endgerät) veranlasst das WAP-Gateway (üblicherweise des Mobilfunkbetreibers) das angeforderte Dokument von einem Webserver (bspw. unter Nutzung des HTTPS) zu holen. Auf dem WAP-Gateway wird das Dokument entschlüsselt (HTTPS → Klartext) und erneut für die Nutzung innerhalb des WAP verschlüsselt (Klartext → WTLS (vgl. [19])). Ist der Einsatz von Gateways zwingend nötig, wird daher der Einsatz eines physisch geschützten Gateways innerhalb der Institution bzw. Institutionsgruppe empfohlen.

Durch die mögliche Verschlüsselung auf Ebene des Kommunikationsnetzwerkes ist eine direkte Verschlüsselung der übertragenen Dokumente nicht notwendig. Die Verschlüsselung sichert allerdings nicht die Authentizität eines Dokumentes sondern lediglich die Authentizität des Webservers, die Vertraulichkeit und Integrität des übertragenen Dokumentes. Die Modifikation von übertragenen Dokumenten (ohne Sicherheitsschicht innerhalb des Netzwerkprotokolls) kann mit Hilfe einer Hashfunktion (innerhalb des HTTP(S) standardmäßig ein 128 Bit langer MD5-Hash [20]) entdeckt werden. Der MD5-Hash gibt dazu eine „Checksumme“ des zu übertragenden Dokumentes wieder. Als Wert wird ein berechneter MD5-Digest [21] in einer Base64-kodierten Form verwendet.

5.4.2 E-Mail / virtuelle Poststelle

E-Mail ist ein Dienst in Computernetzwerken, mit dessen Hilfe elektronische Nachrichten und Dokumente zwischen einem Sender und einem oder mehreren Empfängern ausgetauscht werden können. Neben dem weit verbreiteten Internet-E-Mail-Dienst existieren weitere E-Mail-Dienste, welche allerdings aufgrund ihrer schwachen Verbreitung hier nicht näher betrachtet werden sollen. Eine einzelne Internet-E-Mail wird dabei mit Hilfe des Standards SMTP (Simple Mail Transfer Protokoll) [22, 23] im Klartext über mehrere Stationen vom Sender zum Empfänger verschickt. Ähnlich den Webdokumenten kann auch zur Übermittlung von E-Mails eine Sicherheitsschicht innerhalb des Protokoll-Stack zur verschlüsselten Übertragung eingesetzt werden. Die „SMTP Service Extension for Secure SMTP over TLS“ [24] ist hier ein anerkannter Standard zur sicheren Übertragung von Internet-E-Mail und kann innerhalb des Standards ESMTP [25] genutzt werden.

Dies setzt allerdings die Unterstützung des Secure SMTP auf allen Stationen (Mail Transfer Agents – MTAs) der E-Mail-Übertragung voraus, was innerhalb öffentlicher Netze nicht garantiert werden kann. Dies ist insofern kritisch, als das der RFC 2487 Standard direkt fordert, dass ein MTA nicht auf einer verschlüsselten Übertragung (über das Transport–Layer-Security-Protokoll (TLS) oder Secure Sockets Layer [SSL]) bestehen darf und die Zustellung an den Empfänger auf Grundlage eines als unsicher (weil leicht zu fälschenden) zu betrachtenden MX-Eintrags[5] des Domain Name Service (DNS) erfolgt. Der Einsatz des SSL/TLS-Protokolls ist damit lediglich innerhalb einer Umgebung sinnvoll, in welcher die Zustellung von E-Mail fest konfiguriert, d. h. ohne Nutzung öffentlicher MX-Einträge, und die SSL/TLS-Nutzung vorgeschrieben ist sowie grundsätzlich kein Zugriff aus öffentlichen Netzen auf MTAs ermöglicht wird. Um trotz dessen eine sichere Übertragung und Signierung von Internet-E-Mails zu garantieren, können die E-Mail-Dokumente selbst — also

[5] Der Mail Exchange Resource Record (MX-RR) legt fest, zu welchem Internet-E-Mail-Server eine E-Mail geschickt werden soll.

unabhängig von den genutzten Übertragungsprotokollen — mittels kryptografischer Verfahren kodiert und signiert werden oder mittels Hashwert– und Zeitstempelbildung hinsichtlich ihrer Integrität gesichert werden. Dazu können grundsätzlich symmetrische als auch asymmetrische Kryptoverfahren genutzt werden. Die Kommunikation über i. d. R. unsichere, öffentliche Netze legt an dieser Stelle die Nutzung asymmetrischer Verfahren nahe.

Innerhalb größerer Institutionen wie bspw. Verwaltungen, können diese Aufgaben von einem zentralen Dienst wahrgenommen werden. Damit sind kryptografische Funktionen nicht vom einzelnen Mitarbeiter durchzuführen sondern werden zentral gesteuert. Darüber hinaus können ein– und ausgehende E-Mails hinsichtlich ihrer Authentizität geprüft bzw. modifiziert sowie durch angebundene Workflowmanagementsysteme (WfMS) weiter verarbeitet werden. Das E-Government-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ([26], Modul „Verschlüsselung und Signatur“) empfiehlt für öffentliche Verwaltungen die Einrichtung einer sog. „virtuellen Poststelle“, welche diese Aufgaben wahrnehmen soll. Vorteil dieses zentralen Hintergrunddienstes ist die für den Mitarbeiter transparente Bereitstellung verschiedener Dienste (Empfangsquittungen, Posteingangs– und Postausgangsbuch, Virenschutz, Signierung, Verschlüsselung, zentrale Schlüsselverwaltung, Archivierung, Kopplung von WfMS, usw.). Zeitgleich setzt dies allerdings hohe Anforderungen an den (auch physischen) Schutz und die Vertrauenswürdigkeit des internen Kommunikationsnetzwerkes, da bspw. automatisch durchgeführte Signaturen nicht direkt vom betreffenden Mitarbeiter durchgeführt werden und damit die Nicht-Abstreitbarkeit einer E-Mail zwar ab der virtuellen Poststelle aber nicht zwingend zweifelsfrei bis zum Arbeitsplatz des Mitarbeiters gegeben ist.

Die virtuelle Poststelle (VPS) wurde im Zuge der Initiative BundOnline2005 in einem Fachkonzept behandelt. Neben diesem Fachkonzept existieren bereits fertige Produkte, die eine VPS realisieren. Dazu gehören neben Governikus, einem Projekt das in Public-Private-Partnership entstand, auch GEAM (GEAM Encrypts All Mail) als kommerziellem Vertreter.

5.4.3 Sonstige Dokumente

Elektronische Dokumente können unabhängig vom Übertragungsweg innerhalb von Kommunikationsnetzwerken verschlüsselt werden, um eine Kenntnisnahme oder Modifikation des Inhaltes wirksam zu verhindern. Dazu unterstützen einige Dokumentenformate bereits entsprechende kryptografische (i. d. R. symmetrische) Verfahren. Unabhängig davon können beliebige Dokumente mit Hilfe entsprechender Kryptosoftware verschlüsselt werden.

Dokumentenformate, welche direkt eine Verschlüsselung oder Signatur unterstützen, bieten oft in diesem Zusammenhang weitere Konfigurationsmöglichkeiten in Bezug auf die Dokumentenverwendung. So können bspw. die Ausdrucksmöglichkeit, die Weitergabe, Modifikationsoptionen, etc. modifiziert werden. Die Nutzung dieser Features ist aber grundsätzlich an die korrekte Interpretation und Beachtung der Optionen in der zur Dokumentenverarbeitung oder –ansicht genutzten Applikation gebunden und damit nicht als sicher einzustufen. Sofern das Dokumentenformat eine Verschlüsselung nach einem als allgemein sicher geltenden Chiffrieralgorithmus unter Beachtung des Kerckhoff-Prinzips (Veröffentlichung des Verfahrens, Abhängigkeit der Chiffrierstärke von Schlüssel, etc.) durchführt ist die Verschlüsselung als sicher anzunehmen.

Unterstützt ein Dokumentenformat die Verschlüsselung und Signatur nicht, können Kryptoapplikationen das gesamte elektronische Dokument verschlüsseln bzw. signieren. Notwendige Voraussetzung ist, dass der bzw. die Empfänger des Dokumentes dieselbe Applikation (oder eine auf denselben Standard beruhende Applikation) nutzen.

In beiden Anwendungsfällen obliegt dem Benutzer die Verwaltung der zur Ver– und Entschlüsselung bzw. Signatur notwendigen Passworte und/oder Schlüsselpaare.

Übersicht zu üblichen Dokumentenformaten und Unterstützung hinsichtlich Verschlüsselung und Signatur

Dokumentenformat	Verschlüsselungsverfahren	Signaturverfahren
Bürokommunikationssoftware		
MS Office Formate	• Office 97/2000 kompatible Verfahren • RC4[6] → beide Verfahren gelten als unsicher, RC4 in Abhängigkeit der Schlüssellänge	–
Rich Text Format	–	–
StarOffice und OpenOffice Formate	• Blowfish[7] (Cipher-Feedback-Modus)	–
Adobe PDF	• RC4 → nur Verschlüsselung einzelner Objekte innerhalb der PDF-Datei	• RSA 1024 Bit, 2048 Bit
E-Mail (S/MIME)	• RSA • DES • TripleDES	• RSA
Geografische Informationssysteme (GIS Software)		
DXF	–	–
Sonstige offene Dokumentenformate		
XML	XML Encryption [27] (Schlüsselaustausch über RSA) • TripleDES • AES 128Bit, 256 Bit • Optional: AES 192Bit	XML-DSIG [28] • DSA • RSA
PNG	–	–

Tabelle 5.2: Dokumentenverschlüsselung und –signierung

5.4.4 Zertifikate

Zertifikate sind innerhalb asymmetrischer Verschlüsselungsverfahren zur Bestätigung elektronischer Unterschriften notwendig. Sie stellen sicher, dass sich hinter dem bekannten

[6]RC4 (Ron's Cipher 4) ist eine Stromverschlüsselung (Online-Algorithmus), welcher ursprünglich für RSA Security entwickelt wurde. RC4 gilt inzwischen als gebrochen. Von der Verwendung wird abgeraten!

[7]Blowfish ist ein sehr schneller, nicht patentierter Verschlüsselungsalgorithmus, welcher bis heute als sicher gilt. Quelle: `http://www.schneier.com/`

öffentlichen Schlüssel eines Senders auch tatsächlich die angegebene Person befindet. Das Zertifikat enthält dazu die öffentlichen Schlüssel, Namen, Seriennummer und Gültigkeitsdauer einer Person und ist mit dem privaten Schlüssel eines Zertifizierungsdiensteanbieters (engl. CA) signiert. Der Empfänger einer Nachricht kann den ihm vorliegenden öffentlichen Schlüssel eines Senders damit auf Echtheit prüfen. Voraussetzung dazu ist allerdings das Vertrauen des Empfängers in den Zertifizierungsdiensteanbieter selbst, welches wiederum durch ein Zertifikat eines höheren Zertifizierungsdiensteanbieters erreicht werden kann. Dieser im Standard S/MIME genutzte hierarchische Aufbau erzwingt letztlich die Existenz einer obersten Zertifizierungsdiensteanbieters (engl. Root CA), welcher uneingeschränktes Vertrauen bei allen potentiellen Empfängern signierter Nachrichten genießt. In Deutschland wird diese Aufgabe von der Regulierungsbehörde für Telekommunikation und Post (RegTP) wahrgenommen. Eine Implementierung dieser hierarchischen Public-Key-Infrastruktur, d. h. einer Struktur zur Hinterlegung öffentlicher Schlüssel, erfolgt innerhalb des offenen Standards X.509 [29]. Vorteil des S/MIME-Standards ist, das eine geringe Nutzerinteraktion und keine fachliches Know-how im Bereich der Kryptografie vom Nutzer erwartet werden.

Alternativ können Zertifikate innerhalb eines „Web of Trust“ (OpenPGP) vergeben werden. Dabei können Zertifikate für öffentliche Schlüssel von beliebigen Personen ausgestellt werden. Das Vertrauen in einen öffentlichen Schlüssel wird hier anhand der Anzahl der für ihn ausgestellten Zertifikate und dem eigenen Vertrauen in diese Zertifikate bemessen. Auf dieser Grundlage sind mit OpenPGP erzeugte Signaturen nicht mit dem deutschen Signaturgesetz konform.

Zur Prüfung einer elektronischen Signatur wird zuerst die Signatur selbst mit Hilfe kryptographischer Verfahren auf Korrektheit geprüft. Danach erfolgt die Prüfung des öffentlichen Schlüssels des Senders auf korrekte Zuordnung zu der angegebenen Person anhand eines Zertifikates. Dieses Zertifikat wird anschließend hinsichtlich seiner Vertrauenswürdigkeit entlang des hierarchischen Zertifizierungspfades bzw. anhand alternativer Vertrauensmerkmale geprüft. Die dazu notwendige Vorhaltung mehrerer öffentlicher Schlüssel und Zertifikate sowie Sperrlisten für widerrufene Zertifikate erfolgt i. d. R. durch einen innerhalb einer Institution erreichbaren Verzeichnisdienst, welcher diese Informationen allen angeschlossenen Arbeitsplätzen zur Verfügung stellt. Im Idealfall wird dazu ein existierender Verzeichnisdienst genutzt, da die ansonsten notwendige mehrfache Datenhaltung aufwendig ist und die potentielle Gefahr von Inkonsistenzen gegeben ist.

Verzeichnissdienst	Bemerkung
LDAP	Das Lightweight Directory Access Protokoll (LDAP, RFC2251) entstand als Frontend für den X.500 Verzeichnisdienst und stellt eine vereinfachte Form des Directory Access Protokoll (DAP) dar. LDAP speichert diverse Informationen in einer Baumhierarchie und wird vor allem zur Speicherung von Benutzer– und Gruppeninformationen genutzt. In diesem Zusammenhang kann der Standard zur Speicherung von Schlüsseln und Zertifikaten genutzt werden.

OCSP	Das Online Certificate Status Protocol (OCSP, RFC2560) entstand als Frontend für den X.509 Verzeichnisdienst (Standard zur Speicherung digitaler Zertifikate) und dient zur Speicherung von Zertifikaten und ihres jeweiligen Status. Anfragende Clients haben damit die Möglichkeit, Zertifikatsinformationen zeitnah abzurufen und sind nicht auf intervallgesteuerte Aktualisierungen von Zertifikatsinformationen angewiesen!
Active Directory (Microsoft)	Active Directory ist ein Verzeichnisdienst für Microsoft Windows Netzwerke (Win2k), welcher Nutzerinformationen speichert und den Zugriff auf Netzwerkressourcen steuert. Active Directory enthält das LDAP und kann damit zur Speicherung von Schlüsseln und Zertifikaten genutzt werden.
NDS (Novell)	Der Novell Directory Service (NDS) wurde von der Firma Novell für das Betriebssystem Novell NetWare eingeführt. Der NDS bildet eine hierarchische Struktur ab. Der Nachfolger eDirectory integriert das LDAP und kann damit alle hier möglichen Verzeichnisdienste abzubilden.
YP/NIS (Sun)	Der Network Information Service (NIS, früher Yellow Pages YP) wurde von der Firma Sun Microsystems als Verzeichnisdienst für Benutzerkonten, Computer und andere Netzwerkressourcen innerhalb der UNIX-Welt entwickelt. Auf Grund von Sicherheitsmängeln, schlechter Skalierbarkeit und der Beschränkung auf Unix-Betriebssysteme eignet sich NIS nicht als Verzeichnisdienst für Schlüssel und Zertifikate.
HTTP-Keyserver	Innerhalb des „Web of Trust“ kommen diese öffentlich zugänglichen Keyserver zum Einsatz, welche sich allerdings auf die Bereitstellung von Schnittstellen zur Abfrage öffentlicher Schlüssel beschränken.

Tabelle 5.3: Übersicht: Verzeichnisdienste

5.4.5 Interoperabilität der Signaturen

Grundsätzlich ist die Interoperabilität digitaler Signaturen zwischen S/MIME- und OpenPGP-Welten nicht gegeben. Dies ist einerseits mit den inkompatiblen Dokumentenformaten und Protokollen, andererseits mit den verschiedenen Vertrauensmodellen zu begründen.

Um die Interoperabilität der digitalen Signaturen verschiedener Systeme zu gewährleisten, wurde ein Standard definiert, der die Vorgaben bisheriger Richtlinien genauer eingrenzt. Die neue Spezifikation „ISIS-MTT“, als Vereinigung des Industrial Signature Interoperability Standard und der MailTrusT-Standards, definiert deshalb, basierend auf existiernden Standards, interoperable Datenformate und Protokolle für den sicheren Austausch von Daten. Dies umfasst nicht nur sichere e-Mail-Kommunikation, sondern unter anderem auch die Sicherung von XML-Dokumenten. Die ISIS-MTT Profil für digitale Signaturen in XML ist dabei konform zu den — für den deutschen E-Government-Bereich bindenden — Spezifikationen des Online Services Computer Interface (OSCI).

5.5 Sicherheitssoftware

5.5.1 Grundanforderungen an die Sicherheit

Als Grundanforderungen an die sichere elektronische Datenübertragung können drei Punkte genannt werden:

1. die Vertraulichkeit der Information, also der Geheimhaltung der übertragenen Nachricht,
2. die Integrität einer Nachricht, womit der Schutz vor unbemerkter Veränderung des Inhaltes gemeint ist,
3. die Authentizität, als Synonym für die überprüfbare Echtheit der Absenderidentität.

Den Schutz vor dem Mitlesen unbeteiligter Personen, den ein Brief bisher (in beschränktem Maße) bot, kann ein über öffentliche Datennetze übertragenes Dokument nicht gewährleisten. Es ist daher notwendig, eine Verschlüsselung der Kommunikation zu verwenden.

Im bisherigen postalischen Dokumentenverkehr diente die handschriftliche Unterschrift zum Nachweis der Authentizität einer Person. War gleichzeitig die Integrität der Dokumente gewährleistet, so zum Beispiel durch persönliche Übergabe, oder durch den Briefversand, wurde daraus auch die Nicht-Abstreitbarkeit des Dokumenteninhaltes abgeleitet.

Bei der Unterzeichnung von elektronischen Dokumenten im E-Government ist daher ein Verfahren anzuwenden, das der handschriftlichen Unterschrift rechtlich gleichgestellt ist. Aus der digitalen Unterschrift muss sich auch weiterhin ableiten lassen, dass das vorliegende Dokument unverändert ist und von der unterschreibenden Person stammt. Sind in dem Verwaltungsprozess Fristen gesetzt, so müssen auch diese im elektronischen Dokumentenverkehr abgebildet werden.

5.5.2 Anforderungen an die zu verwendende Sicherheitssoftware

Zur Schaffung einer hersteller– und systemunabhängigen Lösung, deren Akzeptanz durch Unterstützung des Produkteinsatzes in heterogenen Systemumgebungen unterstützt wird, sollte eingesetzte Sicherheitssoftware verfügbare offene Standards unterstützen. Damit können Insellösungen verhindert und beim Einsatz komponentenbasierter Software einzelne Komponenten zu späteren Zeitpunkten ausgetauscht werden. Durch Nutzung von rollenbasierten Verzeichnisdiensten zum zeitnahen Abruf von öffentlichen Schlüsseln und Zertifikaten werden Benutzer und Administratoren weitestgehend von den Aufgaben des Zertifikatsmanagements entlastet.

Sicherheitssoftware sollte sich möglichst transparent in bereits eingesetzte Standardsoftware (bspw. Bürokommunikationssysteme) integrieren lassen und keine weitgehenden Nutzerinteraktionen erfordern, um den nötigen Schulungsaufwand und Probleme durch Fehlbedienung und –konfiguration zu minimieren. Ein wichtiges Kriterium für die Akzeptanz ist die Usability der Sicherheitssoftware. Von den Anwendern sollten keine Kenntnisse über Kryptographie bzw. interne Funktionsweisen für die Verwendung der Software verlangt werden. Sofern auf die konkrete Sicherheitsproblematik anwendbar, muss auf eine Einhaltung des Kerckhoff-Prinzips geachtet werden (dies ist i. d. R. bei der Nutzung offener

Standards der Fall). Notwendige Schlüssel sind derart zu wählen, dass diese eine sichere Verschlüsselung von Dokumenten erlauben, d. h. Dokumente nicht mit vertretbarem Aufwand ohne Kenntnis eines entsprechenden Schlüssels dekodiert werden können.

Anforderungen an Sicherheitssoftware

- Nutzung offener Standards
- komponentenbasierte Softwarearchitektur
- Nutzung vorhandener Verzeichnisdienste (LDAP, OCSP, etc.)
- Transparente Integration in bestehende IT-Infrastruktur
- Kryptografie: Einhaltung des Kerckhoff-Prinzips

Kryptoverfahren	Schlüssellänge (in Bit)	Bemerkung
Symmetrische Verschlüsselungsverfahren		
AES	128, 192, 256	Advanced Encryption Standard: Standard-Verschlüsselungsverfahren innerhalb des e-Government-Bereiches der USA für vertrauliche (nicht geheime) Kommunikation.
Blowfish	32–448 (variabel)	Blowfish gilt allgemein als sehr sicher und bietet eine hervorragende Performance. Vorteil ist die variable Schlüssellänge.
CAST, CAST-256	40–128, 256 (CAST-256)	CAST unterstützt variable Schlüssellängen und gilt allgemein als sicher. Die bekannte Kryptosoftware PGP setzt CAST ein.
Cobra 128	576	Der Cobra Kryptoalgorithmus zeichnet sich durch seine offene Architektur (variable Blocklängen) aus und gilt als Mutation des Blowfish-Verfahren.
DES	56	Data Encryption Standard: In der Vergangenheit im e-Government-Bereich der USA eingesetztes Kryptoverfahren, welches inzwischen kompromittiert wurde und damit nicht mehr verwendet werden sollte.
IDEA	128	IDEA nutzt ein ähnliches Verschlüsselungsverfahren wie DES, arbeitet aber mit einem längeren Schlüssel und ist um ein Vielfaches schneller. Trotz der Ähnlichkeit zu DES gilt IDEA trotz einer Reihe bekannter schwacher Schlüssel als sicher.
RC4, RC5, RC6	bis 2048	Die von dem amerikanischen Unternehmen RSA patentierten Verfahren können mit variabler Schlüssellänge operieren. RC4 gibt allgemein als unsicher und sollte nicht mehr verwendet werden. Die Nachfolger RC5 und RC6 gelten als sicher.
Twofish	128, 192, 256	Twofish gilt als effizient zu implementierendes Verfahren mit einer hohen kryptografischen Sicherheit.

Triple-DES	168	Triple-DES stellt eine Erweiterung des DES-Verfahrens dar, welche im wesentlichen lediglich die Verdreifachung der ursprünglichen Schlüssellänge von 56 Bit betrifft.
Asymmetrische Verschlüsselungsverfahren		
DSS / DSA	1024	Digital Signature Standard / Digital Signature Algorithm: Vom „National Institute of Standards and Technology“ (NIST) zum Standard erhobenes Kryptoverfahren für digitale Signaturen. Gegenüber RSA, dem De-Facto-Standard der Industrie, besitzt DAS vor allem hinsichtlich der Geschwindigkeit und der Schlüssellänge von 1024 Bit Nachteile. Zur Ermittlung von Hashwerten nutzt DSA den Hashalgorithmus SHA-1. Hinweis: DSA unterstützt lediglich die digitale Signatur, keine Verschlüsselung
ECC	256	Elliptic Curve Cryptosystem: Das ECC ermöglicht trotz relativ geringer Schlüsselgröße eine gegenüber DSA oder RSA wesentlich schneller und hinsichtlich der Sicherheit vergleichbare Ergebnisse. Auf Grund der geringen CPU– und Speicherbelastung findet ECC vor allem auf Smart-Card Anwendung.
RSA	Variabel (1024 Bit gilt als sicher)	RSA (nach den Erfindern Rivest, Shamir und Adleman) ist der De-Facto-Standard bei asymmetrischen Verschlüsselungsverfahren. Trotz relativ hoher CPU– und Speicherbelastung ist die grundsätzlich nicht beschränkte, variable Schlüssellänge die größte Stärke des als sicher einzuschätzenden Verfahrens.
Hashfunktionen		
MD4/ MPPE	–	Message-Digest 4 (MD4) erzeugt einen Hashwert mit einer Länge von 128Bit und gilt inzwischen als unsicher, da nachgewiesen werden konnte, dass fast identische Nachrichten mit gleichem Hashwert generiert werden können. Das in MS Windows integrierte Verschlüsselungsprotokoll „Microsoft Point-to-Point-Encrytion“ (MPPE) basiert auf MD4.
MD5	–	Message-Digest 5 (MD5) erzeugt wie sein Vorgänger MD4 einen Hashwert mit einer Länge von 128Bit. Wie MD4 gilt MD5 inzwischen als unsicher.
SHA	–	Secure Hash Algorithm (SHA): Ein von dem National Institute of Standards and Technology (NIST) entwickelter Standard, welcher auf dem MD4 Verfahrend beruht aber auf Grund eines 160 Bit langen Hashwertes wesentlich robuster auf Angriffe reagiert. Bisher sind keine erfolgreichen Angriffe auf SHA bekannt. Das NIST veröffentlichte weitere Verfahren (SHA-224, SHA-256, SHA-384 und SHA-512), welche teilweise Dokumente mit einer Größe von bis zu 2128 Bit verarbeiten können.

Tabelle 5.4: Vergleich gängiger Verschlüsselungsverfahren

5.5.3 Gesetzliche und normative Vorgaben Verschlüsselung

Innerhalb des IT-Grundschutzhandbuches des BSI ([30], S. 95f.), dessen Beachtung zur Erteilung eines Zertifikats bzw. einer Selbsterklärung erforderlich ist, wird der Einsatz kryptografischer Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit empfohlen. Die Zertifizierung des BSI ist nicht gesetzlich vorgeschrieben. Das BSI empfiehlt hier die Entwicklung eines Kryptokonzeptes und die darauf aufbauende Anforderungsermittlung und Auswahl eines geeigneten Verfahrens. Hinsichtlich des Kryptoalgorithmus werden beim Einsatz symmetrischer Verschlüsselung Triple-DES, IDEA, RC 5 (mind. 80Bit Schlüssellänge) und beim Einsatz asymmetrische Verschlüsselung RSA oder auf Elliptischen Kurven basierende Verschlüsselungsverfahren (ECC) empfohlen. Das BSI empfiehlt den Einsatz von Produkten, welche hinsichtlich der

- Funktionalität und Interoperabilität die gewünschten kryptographischen Verfahren und Schlüsselstärken unterstützen, in die IT-Infrastruktur (Netzwerk, Performance, etc.) passen sowie gängige offene Standards unterstützen,
- Wirtschaftlichkeit die Kosten– und Ressourcenaufwände für Anschaffung und Betrieb sowie mögliche Einsparungen berücksichtigt werden und
- Zertifizierung den Einsatz nach der ITSEC (Information Technology Security Evaluation Criteria) zertifizierter Produkte.

Im Gegensatz zu anderen europäischen, asiatischen und amerikanischen Staaten, existiert in der Bundesrepublik Deutschland kein Verbot oder Einschränkung (bspw. hinsichtlich bestimmter Kryptoverfahren oder Schlüssellängen) hinsichtlich des Einsatzes kryptographischer Verfahren.

Signatur und Zeitstempel Für die Bundesrepublik Deutschland sind die notwendigen rechtlichen Rahmenbedingungen für die Erstellung und Verwendung elektronischer Signaturen, qualifizierten Zeitstempeln sowie für die Erbringung von Signatur– und Zertifizierungsdiensten vom Gesetzgeber im Signaturgesetz (SigG) sowie der Verordnung zur elektronischen Signatur (SigV) festgelegt wurden. Damit ist auch eine rechtliche Sicherheit für die Gleichstellung der zu verwendenden elektronischen Unterschrift zur bisher verwendeten und akzeptierten handschriftlichen Unterschrift gewährleistet. Dokumente, die mit einer qualifizierten digitalen Signatur (§2, Nr.3 SigG) signiert wurden, sind für eine Kommunikation, in der gesetzlich die Schriftform gefordert wird, zulässig, sofern die elektronische Form nicht ausgeschlossen wurde (vgl. [26], Abschnitt 4.1.2 „Rechtliche Rahmenbedingungen für E-Government“).

Das Gesetz über Rahmenbedingungen für elektronische Signaturen (§2 SigG) unterscheidet hinsichtlich

- *elektronischen Signaturen*
  Ausschließlich zur einfachen Authentifizierung
- *fortgeschrittenen elektronischen Signaturen*
  Identifizierung und eindeutige Zuordnung des Signaturschlüsselinhabers
- *qualifizierten elektronischen Signaturen*
  Signaturen auf Basis eines qualifizierten Zertifikates (anerkannte Zertifizierungsstelle)

Hinsichtlich des Produkteinsatzes zur Erzeugung, Sicherung und Anwendung qualifizierter elektronischer Signaturen schreibt der Gesetzgeber folgende Rahmenbedingungen vor:

- Signaturfälschungen und Modifikationen signierter Daten müssen zuverlässig erkennbar sein,
- die unberechtigte Nutzung von Signaturschlüsseln ist zu verhindern,
- bei der elektronischen Signatur von Daten ist darzustellen, auf welche Daten sich die Signatur bezieht,
- bei der Prüfung einer elektronischen Signatur muss dargestellt werden können, auf welche Daten sich die Signatur bezieht, ob die Daten unverändert vorliegen, der Signaturschlüsselinhaber eindeutig zuordenbar ist und welche Inhalte das zur Signaturzertifizierung verwendete Zertifikat aufweist und
- eine hinreichend geheime Sicherung eines Signaturschlüssels muss gewährleistet sein.

Der Gesetzgeber gibt eine konkreten kryptographischen Algorithmen vor, fordert aber indirekt den Einsatz asymmetrischer Verfahren, da symmetrische Verfahren die Kenntnis des Signaturschlüssels bei allen beteiligten Personen voraussetzen. Bei der Auswahl eines asymmetrischen, kryptographischen Verfahrens muss sichergestellt werden, das dieses keine Modifikationen signierter Daten zulässt, was die laufende Kontrolle eingesetzter Verfahren hinsichtlich ihrer Sicherheit erforderlich macht.

Innerhalb des IT-Grundschutzhandbuches des BSI werden als geeignete Algorithmen für Signaturen RSA und DSA benannt ([30] S. 1121).

Öffentliche Hand Zur Standardisierung von E-Government-Anwendungen wurden von einem Expertenkreis die „SAGA – Standards und Architekturen für E-Government-Anwendungen“ erarbeitet. Sie liegen seit August 2003 vor und empfehlen „...technische Rahmenbedingungen für die Entwicklung, Kommunikation und Interaktion von IT-Systemen der Bundesbehörden. Für Prozesse und Systeme, die E-Government-Dienstleistungen des Bundes erbringen, ist die Konformität mit SAGA verbindlich.“ (Quelle: [31]). Im Rahmen der Initiative BundOnline 2005[8] wird die Nutzung des Online Services Computer Interface (OSCI) empfohlen bzw. als obligatorischer Standard vorgeschrieben [32]. Koordiniert von der OSCI-Leitstelle[9] beinhaltet OSCI Protokollstandards für die Kommunalwirtschaft, um Dokumente verschlüsselt und signiert sicher auszutauschen. Gleichwohl unterstützt der OSCI-Protokollstandard auch den unverschlüsselten und unsignierten Austausch von Dokumenten.

5.5.4 Schnittstellen für Sicherheitslösungen

Neben kompletten, oft in sich geschlossenen Sicherheitslösungen existieren eine Reihe von Frameworks bzw. offenen Schnittstellen, welche die Integration von Kryptofunktionalität in individuell zu entwickelnde Software oder existierende Standardsoftware ermöglichen. Hinsichtlich ihrer Funktionalität kann folgende Gruppierung genutzt werden:

- Ver– und Entschlüsselung von Daten bzw. Dokumenten

[8] http://www.bundonline-2005.de/
[9] http://www.osci.de/

- Signatur(-prüfung)
- Anmelde– bzw. Berechtigungsfunktionen / Authentifizierung und Autorisierung
- Sicherer Daten– und Dokumententransport über Netzwerke
- Unterstützung sicherheitsrelevanter Hardware (Kartenterminals, USB-Token, Systeme zur Erfassung biometrischer Merkmale, etc.)

Die Nutzung offener Standards verspricht im Grunde ein größeres Vertrauen in eine Softwarelösung, da die betreffenden sensiblen Bereiche nicht individuell programmiert werden müssen oder der korrekten Implementierung einer Sicherheitsfunktion eines unbekannten Herstellers vertraut werden muss. Voraussetzung dafür ist, dass die genutzte Implementierung der Sicherheitsfunktionen ausreichend gut getestet und keine kompromittierenden Angriffe auf die Komponente bekannt sind.

Produkte

Bezeichnung	Lösung für *	Lizenz	Betriebssystem	Kryptoverfahren	Schnittstellen / PlugIns
PGP	C, S	Bis 2.3 GPL, dann kommerziell	Windows, Unix, MacOS, OS/2, viele mehr	RSA, DSA	MS Outlook, Lotus Notes, Eudora, Pegasus Mail 3.0, Netscape Messenger und Claris E-Mailer (Mac)
GnuPG	C, S	GNU GPL	Windows, Linux, MacOS[10]	RSA, DSA	MS Outlook
Steganos Security Suite	C	kommerziell	MS Windows	AES	
Steganos Crypt&Go	C	kommerziell	MS Windows	AES 128Bit	MS Outlook

Tabelle 5.5: Übersicht: Verschlüsselungsprodukte

API / Frameworks

Bezeichnung	Typ	Lösung für *	Lizenz	Betriebssystem	Kryptoverfahren	Schnittstellen / PlugIns
CryptoAPI	API (C/C++, VB)	C, S	kommerziell	MS Windows	RC2, RC4, DES, TripleDES, RSA	COM (CAPICOM)
NSDPGP 3.0	API (C/C++)	C, S	frei nutzbar	MS Windows	RSA, DSA	DLL / COM
CT-API	Framework zum Zugriff auf Speicher– und Prozessorchipkarten	H	kommerziell	MS Windows, Linux, andere	–	Funktionsbibliothek
OCF (Open Card Framework)	Java-Framework	N, H	Open Card Consortium Licence	alle	–	OCF (muss von Chipkarte und Terminal unterstützt werden)
PC/SC (Personal Computer/Smart Card)	Standard für Zugriff auf Chipkarten, keine Festlegung auf Sprache	N, H	kommerziell	MS Windows (bereits enthalten), Linux (MUSCLE)	–	Kartentreiber
OSCI[11]	Java-API, .NET	C, S, N	LGPL	alle	Siehe Bouncycastle, Apache XML Security	
Bouncycastle	Java-API	C, S	frei nutzbar	alle	RSA, DSA, AES, CAST, DES, IDEA, PGP, RC2, RC5, RC6, SHA, MD5	
Apache XML Security	API (Java, C/C++)	C, S	ASL	alle	AES, RSA, TripleDES, DAS, SHA	

Tabelle 5.6: Übersicht: Sicherheitsframeworks

* C – Dokumentenverschlüsselung, S – Signatur, N – Datentransport, H – Hardwareunterstützung

[10] `http://macgpg.sourceforge.net/de/`

[11] Hier im Bezug auf die Implementierung von OSCI Transport 1.2 des Vereins MediaKomm Esslingen, `http://www.osci.mediakomm.esslingen.de`

In Bezug auf die Nutzung innerhalb des E-Government ist die Nutzung des OSCI-Protokollstandards hervorzuheben. Ziel der OSCI-Kommunikation ist ein verlässlicher, vertraulicher und nachweisbarer Austausch elektronischer Dokumente auf Grundlage anerkannter, offener Standards (OSCI Transport, Teil A) sowie die Standardisierung der Dokumente unter fachlichen Gesichtspunkten auf Grundlage der XML (OSCI, Teil B). Zu diesen Standards gehören HTTP, SOAP[12], MIME und XML (insb. XML Encryption und XML DSIG). Die — bisher einzige — Implementierung des OSCI Transport Standards (Teil A) des Vereins MediaKomm Esslingen setzt diesen Standard um. Inhalts– und Nutzungsdaten werden während eines OSCI-konformen Dokumentenaustausches strikt getrennt und sofern erforderlich getrennt verschlüsselt und signiert. Die verfügbare Implementierung bietet unter Nutzung anderer Schnittstellen (JCE/Bouncycastle, JNDI/LDAP)[13], eine einfache Schnittstelle zur Implementierung derartiger Funktionen.

Authentifizierung über Webinterfaces Zum Feststellen der Authentizität eines Benutzers über ein Webinterface kann eine Prüfung auf Ebene der Anwendungsschicht (TCP/IP-Anwendungsschicht) und/oder der Dokumentenebene erfolgen.

Standard	Beschreibung
Prüfung auf Anwendungsschicht	
HTTP-Basic	Client-Authentifizierung, bei welcher Login und Passwort im Klartext übertragen werden. Bei Einsatz des HTTPS werden auch Authentifizierungsdaten verschlüsselt. Trotzdessen liegen diese an den Endpunkten der HTTP-Verbindung in entschlüsselter Form vor. Der Nutzer wird einmalig zur Eingabe von Login und Passwort aufgefordert.
HTTP-Digest	Client-Authentifizierung, bei welcher das Passwort als Hashwert (MD5) übertragen wird. Der Nutzer wird einmalig zur Eingabe von Login und Passwort aufgefordert.
HTTP-NTLM	NTLM ist das innerhalb des Betriebssystems MS Windows gebräuchliche Protokoll zur Authentifizierung in Windows-Netzwerken und –Domänen. Das Passwort wird verschlüsselt übertragen. Sofern der Nutzer ordnungsgemäß unter MS Windows angemeldet ist, müssen Login und Passwort nicht eingegeben werden.
HTTPS-Client-Certificates	Mit Hilfe des HTTPS können sich auch Clients mit Hilfe eines Zertifikates gegenüber einem Server autorisieren. Voraussetzung dazu ist die Installation eines Clientzertifikates auf dem PC des Nutzers.
WAP/WTLS-Client-Authentification	Analog des Einsatzes von HTTPS-Client Zertifikaten zur Nutzerauthentifikation können mobile Endgeräte eine Authentifizierung auf Ebene des WTLS durchführen.
Prüfung auf Dokumentenebene	
WML-FORM	Analog der Nutzung von HTML-Formularen zur Nutzerauthentifizierung, können mobile Endgeräte Logindaten über ein Formular erfassen.

[12]Simple Object Access Protocol: Auf dem XML-Standard basierendes Protokoll zum Austausch von Daten zwischen zwei Systemen und dem Aufruf entfernter Funktionen.

[13]`http://www.osci.mediakomm.esslingen.de/documents/es_osci_manual_2004-04-07.pdf`

HTML-FORM	Nutzung eines HTML-Formulars zur Abfrage und Übermittlung von Authentifizierungsdaten. Die eingetragenen Daten werden dabei grundsätzlich unverschlüsselt übertragen. Eine Verschlüsselung über HTTPS ist zu empfehlen! ***Hinweis:*** *Formulardaten sollten mit Hilfe der POST-Methode übertragen werden, da mittels GET-Methode übertragende Daten unverschlüsselt in der Adresszeile des Browsers stehen bleiben und ggf. im Logfile des Servers archiviert werden.*
Prüfung über externe Hardware	Mit Hilfe externer Komponenten, welche auf dem PC des Nutzers ausgeführt werden (bspw. JavaApplets, ActiveX-Controls, ...), können Authentifizierungsdaten abgefragt werden (bspw. über ein Formular) und dann mittels individuell wählbarer Verschlüsselungsmethode übertragen und geprüft werden. Zertifizierte Komponenten können auf diverse Schnittstellen des Nutzer PCs (bspw. Chipkarten APIs) zugreifen. Damit können auf Chipkarten, USB-Token oder biometrischen Merkmalen basierende Authentifizierungsmethoden hinreichend gut unterstützt werden.

Tabelle 5.7: Authentifizierungsstandards für Webinterfaces

5.6 Kriterienkatalog

Bei der Betrachtung verschiedener Komponenten zur Sicherstellung datenschutzrechtlicher und datensicherheitsrelevanter Vorgaben sind verschiedene Kriterien zu prüfen. Dazu gehören Grundsatzfragen zum unterstützten Systemumgebung, dem Lizenzmodell und der Softwareweiterentwicklung, welche kosten– und wartungsseitig Einfluss auf eine Entscheidung nehmen. In Bezug auf Sicherheitskomponenten sind folgende Kriterien zu berücksichtigen:

Aspekt: Features

- *Notwendige Features*
  Existieren Anforderungen, welche die Nutzung eines speziellen Features erzwingen, sollte dieses im Produkt enthalten sein oder individuell dazu programmiert werden können.
- *Erhaltung der Flexibilität*
  Eingesetzte Features dürfen die Flexibilität (bspw. beim Einsatz bestimmter Komponenten) nicht beeinträchtigen.

Aspekt: Normative Vorgaben

- *Konformität zum SigG und der SigV*
  Einsatz möglichst qualifizierter elektronischer Signaturen unter Einsatz eines hierarchischen Zertifizierungssystems. Nutzung eines asymmetrischen Kryptoverfahrens.
- *Einsatz OSCI-konformer Protokollstandards*
  Beachtung der im OSCI Transport, Teil A spezifizierten Protokollstandards zum sicheren Austausch elektronischer Dokumente.

Kriterium	Beschreibung
Kategorie: Hersteller/ Entwickler	
Lizenztyp	Handelt es sich um freie Software oder eine kommerzielle Version eines Produktes. Können bei Fehlfunktionen (hier i. d. R. durch Datenverlust) einer Komponente Haftungsrisiken auf den Hersteller verlagert werden? Die Kompromittierung des eingesetzten Kryptoverfahrens kann dem Hersteller i. d. R. nicht angelastet werden.
Verbreitung	Die Verbreitung eines konkreten Produktes ist hinsichtlich des verwendeten Kryptoverfahrens und ggf. eingesetzter Dokumentenformate von Belang.
Weiterentwicklung	Die ständige Weiterentwicklung von Sicherheitssoftware oder –komponenten spricht dafür, dass der Hersteller bzw. die Entwickler an einer ständigen Aktualität (bspw. hier auch in Bezug auf Virensignaturen) und auch Sicherheit des eingesetzten Kryptoverfahrens interessiert sind. Die Maßgabe zur Veröffentlichung des Sourcecodes bzw. Bekanntgabe des verwendeten Kryptoalgorithmus ist nicht gleichbedeutend mit der tatsächlichen Sicherheit des gewählten Verfahrens, so dass einer ständigen Weiterentwicklung bzw. Betreuung und die Bekanntgabe von Angriffsversuchen auf das Kryptoverfahren eine hohe Bedeutung zukommt.
Modifizierbarkeit	Der Quellcode muss (zur Einhaltung des Kerckhoff-Prinzips) verfügbar und gut dokumentiert sein. I.d.R. muss die (auch rechtliche Zulässigkeit) von Ergänzungen und Modifikationen nicht gegeben sein.
Kategorie: Systemumgebung	
Betriebssystem	In Abhängigkeit des Einsatzzweckes ist die Verfügbarkeit des Produktes für spezielle Betriebssysteme oder Ablaufumgebung (z. B. Java-Environment) zu betrachten.
Laufzeitumgebur	Beim Einsatz einer Komponente innerhalb einer Ablaufumgebung, ist die Verfügbarkeit der Komponente in der spezifischen Sprache zu prüfen.
Typ	Sicherheitskomponenten sollten, für den Benutzer transparent, im Hintergrund laufen. Daher ist deren Einsatz als Framework oder Komponenten mit definiertem API gegenüber eigenständigen, i. d. R. mit Nutzerdialogen versehenen, Applikationen zu bevorzugen.
Schnittstellen	Die Software unterstützt alle notwendigen Schnittstellen und Dienste (Input/Output, bspw. HTTP, LDAP, PC/SC, etc.) sowie — sofern das Produkt aus mehreren Komponenten besteht — interne Schnittstellen, welche einen Austausch von Komponenten ermöglichen.
Kategorie: Standards	
BGG §7, Ergonomie	Sicherheitskomponenten sollten nach Möglichkeit nur in Ausnahmefällen mit dem Benutzer interagieren. Da von einem Standardanwender keine Hintergund– und Vorkenntnisse im Bereich Verschlüsselung, digitale Signatur, etc. vorauszusetzen sind, müssen Dialoge und damit verknüpfte Optionen hohe ergonomische Anforderungen im Bereich der Selbsterklärungsfähigkeit und Erwartungskonformität besitzen.
XML	Der Einsatz von XML zur Konfiguration und Steuerung der Sicherheitskomponenten ist zu empfehlen.

Flexibilität	Die eingesetzten Kryptoverfahren müssen nach aktuellem Stand als sicher eingestuft sein, d. h. es sind bisher keine erfolgreichen kompromittierenden Angriffe auf das Verfahren gelungen. Für den Fall einer Kompromittierung muss ein einfacher Wechsel des Verfahrens möglich sein.
Dokumentenform	Das System sollte offene, gut dokumentierte und möglichst weit verbreitete Standards nutzen, um eine hohe Interoperabilität zu erreichen.
Kategorie: Sicherheit	
IT-Integration	Die Software/Komponente muss einfach zu bedienen/zu integrieren und sich nahtlos in die technisch-organisatorischen Gegebenheiten der Umgebung einfügen. Die Nutzerinteraktion ist auf ein Minimum zu beschränken. Die eingesetzte Software erfüllt alle Bedingungen des Kerckhoff-Prinzips
Nutzerautorisation/ Nutzerauthentifikation	Die Nutzung von Verschlüsselungs– und Signierfunktionen erfordert eine eindeutige und sichere Erkennung des Benutzers. Sicherheitskomponenten sollten dazu den Einsatz technischer Hilfsmittel wie Chipkarten, Geräte zur Erkennung biometrischer Merkmale, etc. bzw. die hier verwendeten Standards (CT-API, PC/SC).
Verschlüsselung	Komponenten zur Verschlüsselung mittels kryptografischer Verfahren sollten im Bereich der asymmetrischen Verschlüsselung RSA (auf Grund der weiten Verbreitung als Quasi-Standard zu betrachten) und im Bereich der symmetrischen Verschlüsselung Verfahren wie Triple-DES, Blowfish oder Twofish unterstützen.
Signatur	Der Einsatz der elektronischen Signatur muss — um den Anforderungen des SigG zu genügen — auf Grundlage einer hierarchischen Zertifizierung (Standards: S/MIME, RSA) erfolgen.
Kategorie: Features	
Austauschbarkeit von Komponenten	Die eingesetzten Komponenten müssen in der Lage sein, das verwendete Kryptoverfahren zu wechseln. Dies kann bspw. bei Kompromittierung eines spezifischen Verfahren notwendig werden.

Tabelle 5.8: Kriterien für Sicherheitskomponenten

6 System– und Kriterienkatalog Webinterfaces

6.1 Einleitung

Innerhalb der im Rahmen des RAfEG Verbundprojektes zu entwickelnden Referenzarchitektur muss die Einbindung von Arbeitsplatzrechnern (im folgenden Clients) in ein organisationsübergreifendes Workflowsteuerungssystem berücksichtigt werden (Abbildung der Präsentationsschicht). Der hier dargestellte Systemkatalog stellt alle dafür in Betracht kommenden Technologien und Systeme dar. Bei der Katalogerstellung wurden vorrangig offene Systeme aus dem OpenSource Bereich berücksichtigt, da das RAfEG Projekt hier einen entsprechenden Schwerpunkt setzt[1].

6.2 Verfahren

Zur Einbindung von Arbeitsplatzrechnern in ein Workflowsteuerungssystem kann ein Webbrowser als Präsentationsapplikation genutzt werden. Webbrowser sind für alle gängigen Betriebssysteme verfügbar und inzwischen so weit verbreitet, dass ein geringer Schulungsaufwand pro Benutzer zu erwarten ist. Alternativ kann eine eigene Präsentationsapplikationen entwickelt werden, welche die Interaktion des Benutzers mit dem Workflowsteuerungssystem zulässt.

Vorteile	Nachteile
Webbrowser als Präsentationsapplikation	
• für alle gängigen Arbeitsplatzumgebungen verfügbar • geringer Schulungsaufwand • Nutzung offener Standards für Präsentation (HTTP, (X)HTML, CSS)	• Einschränkungen in Präsentation durch unabhängigen Standard → Usability • Teilweise fehlerhafte Implementierung der Standards
Individuelle Präsentationsapplikation	
• direkte Integration in Betriebssystem des Benutzers → bessere Kontrollmöglichkeiten • Usability → durch Verlagerung von Applikationsfunktionen auf die Präsentationsschicht	• Individuelle Entwicklung nötig • Updates schwer verteilbar, Nutzung von Installation abhängig • Schulungsaufwand • proprietärer Standard

Tabelle 6.1: Vor– und Nachteile versch. Präsentationsapplikationen

[1] vgl. RAfEG-Projektantrag, S. 15

Ziel der zu erstellenden Referenzarchitektur soll die Nutzung offener Standards sein, da diese die Interoperabilität und Portabilität sicherstellen. Aus diesem Grund kann die Entwicklung individueller Präsentationsapplikationen — unabhängig von dem zusätzlichen Entwicklungsaufwand und den damit verbundenen Kosten — hier nicht empfohlen werden.

Bei der Nutzung des Webbrowsers zur Interaktion mit einem Benutzer muss das Webinterface in der Lage sein, eine Oberfläche in einem der gängigen Standards bzw. im Idealfall einem beliebigen Ausgabeformat zu generieren sowie Eingaben des Benutzers an die Komponenten einer Applikation zu übermitteln, welche für die Bearbeitung der Eingaben zuständig sind. Eine darzustellende Arbeitsoberfläche kann aus mehreren Bearbeitungsfeldern bzw. Komponenten bestehen, deren Darstellung und Verarbeitung von spezifisch dafür entwickelten Funktionsbausteinen einer Applikation durchgeführt wird.

Mit dem Ziel der Wiederverwendbarkeit und Kapselung wird damit jede Funktion als eigenständige Komponente innerhalb eines Frameworks abgebildet. Diese Komponente soll — vorerst unabhängig vom später auszugebenden Format (HTML, XHTML, XML, PDF, WML, etc.) — nur den Teil der Arbeitsoberfläche generieren, für den sie zuständig ist. Dazu muss die Komponente ggf. notwendige Eingaben des Benutzers direkt erhalten können.

Zur Erfüllung dieser Anforderungen bietet Java bereits fertige Konzepte in Form von Servlets und Portlets an. Grundsätzlich lassen sich die darin beschriebenen Verfahren aber auch in anderen Sprachen umsetzen.

6.2.1 Servlets

Servlets stellen (programmtechnisch) Klassen dar, welche Anforderungen einer Webseite von einem Clients (allg. HTTP-Request) verarbeiten und eine dynamisch erzeugte Antwort (allg. HTTP-Response) zurücksenden können. Dazu stellt ein Servlet Container (bspw. Tomcat) den Request an das betreffende Servlet durch und sendet dessen Ausgabe an den Client. Das Servlet besitzt dabei die Aufgabe, die komplette Ausgabe selbst zu erzeugen. Im einfachsten Fall wird das zu erzeugende Dokument (bspw. XHTML-Dokument) direkt in den Standard-Ausgabestrom geschrieben.

Ein Nachteil dieses Konzeptes ist, das das Ausgabeformat direkt im Quellcode des Servlets kodiert wird und das Servlet die komplette Arbeitsoberfläche generiert. Eine Modifikation des Ausgabeformates erzwingt damit immer auch eine Änderung am Programmcode. Als Ausweg bietet sich hier die Generierung einer vorformatierten Ausgabe an, welche dann je nach Request in ein beliebiges Ausgabeformat umgeformt werden kann. In der Praxis kommen dazu XSL-Prozessoren und –Formatierer zum Einsatz.

Innerhalb des Java-Umfeldes ist die Java Servlet Specification[2] als offener Standard definiert und garantiert damit die Interoperabilität zwischen Servlets unterschiedlicher Hersteller.

[2] vgl. JSR-000154 JavaTM Servlet 2.4 Specification, `http://www.jcp.org/aboutJava/communityprocess/final/jsr154/`

6.2.2 Portlets

Ein Portlet bildet einen bestimmten, anwendungsspezifischen Teil einer Arbeitsoberfläche (bspw. einer Portal-Webseite) hinsichtlich seiner Präsentation und seiner Funktionalität ab (sog. Fragment). Die Anforderung (Request) eines Benutzers wird innerhalb des Portlet-Konzeptes von einem Portlet-Container entgegengenommen und dann in Abhängigkeit vom Request an das entsprechende Portlet weitergereicht. Dieses Portlet verarbeitet den Request und generiert die von ihm verwaltete Komponente der Arbeitsoberfläche. Der Portal-Server stellt daraus die komplette Arbeitsoberfläche (bspw. HTML-Dokument) her und kann damit auch entsprechende Caching-Mechanismen nutzen.

In einem Portlet können ebenfalls mehrere Anwendungen zusammengefasst (im Sinne einer integrierten Funktion) werden. Durch Kommunikation zwischen verschiedenen Portlets können auch Funktionen und Ausgaben anderer Portlets genutzt bzw. initiiert werden.

Die entsprechende API zur Entwicklung von Portlets im Java-Umfeld ist als offener Standard, der Portlet Specification[3], definiert. Damit ist eine Interoperabilität zwischen Portlets unterschiedlicher Hersteller garantiert. Portlets können mit verschiedenen Entwicklungsumgebungen erstellt werden und existieren für viele Standardanwendungen bereits als vordefinierte Portlets.

WSRP Der Web Services for Remote Portlets (WSRP), deren Standardisierung von OASIS verwaltet und koordiniert wird, ermöglicht auf Grundlage von XML und der WebService-Standards SOAP[4] und WSDL[5] die Einbindung der Ausgabe externer Portlets in die eigene Arbeitsoberfläche[6]. WSRP beinhaltet gegenüber klassischen, datenorientierten WebServices eine Benutzerschnittstelle zur einfachen Integration in fremde Portlets und kann damit ggf. die eigene grafische Darstellung selbst bestimmen. Da die Kommunikation auf Basis der XML stattfindet, ist die Implementierung eines entsprechenden WSRP-Dienstes in einer beliebigen Sprache möglich.

WSRP unterstützt die Verteilung der Generierung der Arbeitsoberfläche innerhalb einer heterogenen Umgebung durch Definition eines offenen Standards.

SAP iViews SAP iView ist eine proprietäre Schnittstellendefinition zur Einbindung von Anwendungen als Fragmente einer Arbeitsoberfläche für das mySAP Enterprise Portal. Konzeptionell unterscheiden sich iViews damit nicht wesentlich von Portlets. IViews können mit Hilfe des SAP Portal Development Kit innerhalb verschiedener Umgebungen (Java, .NET, etc.) implementiert werden[7]. Die Ausgabe erfolgt auf Basis der XML.

6.2.3 Zusammenfassung

Servlets wie auch Portlets sind in der Lage, einen Request über einen entsprechenden Container entgegenzunehmen und an die entsprechende Komponente weiterzureichen. Damit

[3] vgl. JSR-000168 Portlet Specification, `http://www.jcp.org/aboutJava/communityprocess/review/jsr168/`
[4] vgl. XML Protocol Working Group, `http://www.w3.org/2000/xp/Group/`
[5] vgl. Web Services Description Language (WSDL) 1.1, `http://www.w3.org/TR/wsdl`
[6] vgl. Web Services for Remote Portlets Specification, `http://www.oasis-open.org/committees/wsrp`
[7] vgl. `http://www.iviewstudio.com`

ist eine weit reichende Modularisierung möglich, welche dem Ziel der Bildung von „Softwarebausteinen“ bzw. Komponenten entgegenkommt. Bei der Generierung der Arbeitsoberfläche unterscheiden sich beide Konzepte. Während Servlets die komplette Oberfläche generieren, behandeln Portlets in der Regel nur das ihnen zugeordnete Fragment. Der Portal-Server sorgt für die komplette Erzeugung der Arbeitsoberfläche. In Bezug auf das Ausgabeformat existieren in Servlets keine Einschränkungen, innerhalb von Portlets müssen lediglich die gewünschten Formate registriert werden und entsprechende Templates zur Generierung des auszugebenden Dokumenten(-teils) bereitstehen.

Um den Eingriff in Programmquellcode bei Änderungen der Ausgabeformate komplett zu vermeiden, empfiehlt sich der Einsatz von Widget-Klassen. Widget-Klassen bieten dem Anwendungsentwickler ein (mehr oder weniger flexibles) Set von visuellen Komponenten (Textfelder, Formulare, etc.), aus denen die Arbeitsoberfläche (oder Teile davon) generiert wird. Soll das Erscheinungsbild, die Position oder andere Parameter einer solchen visuellen Komponente modifiziert werden, ist lediglich ein Eingriff in eine entsprechende Vorlage aber kein Eingriff in den Quellcode nötig. Weiterhin können bei einem fest definierten Set von Komponenten Gestaltungsänderungen unabhängig von der konkreten Anwendung vorgenommen werden.

6.3 Frameworks

6.3.1 Portal-Frameworks

Portal-Frameworks unterstützen den Entwickler bei der Implementierung von Portalen. Sie bieten dazu eine Schnittstelle um Requests entgegenzunehmen, zu verarbeiten und die Ausgabe zu erstellen. Aufeinander aufbauend werden hier bekannte (i. d. R. OpenSource) Frameworks kurz vorgestellt.

Entscheidungsrelevante Faktoren sind:

- System Requirements, Installation
- Welche Voraussetzungen werden an die (Software-)Umgebung gestellt (bspw. J2EE Application Server, Sprachen) und sind bei der Installation Besonderheiten zu berücksichtigen?
- Dokumentation
- In welcher Sprache, Qualität und für welche Zwecke existieren Dokumentationen?
- Anpassungsfähigkeit / Customizing
- Können Anpassungen und Ergänzungen selbst vorgenommen werden?

Frameworks zur Content-Publication

Frameworks zur Content-Publication bieten Schnittstellen zur Erfassung von Requests und Generierung von Dokumenten verschiedener Formate (i. d. R. HTML-Seiten).

Cocoon Cocoon ist ein auf J2EE basierendes, modular aufgebautes OpenSource Publishing Framework welches i. d. R. als Servlet genutzt wird, sich aber auch innerhalb eines Portlet Frameworks nutzen lässt. Mittels eines modularen Konzeptes kann ein XML-Quelldokument in ein beliebiges Zielformat transformiert werden. Das Framework nutzt dazu die Komponenten:

1. *Producer*
   Übergibt notwendige, strukturierte Informationen in Form eines DOM[8] an den Reaktor. Im Kern enthält der „Producer“ dazu einen XML-Parser.

2. *Reaktor*
   Bestimmt anhand von Parametern, welcher Prozessor und Formatierer zur Generierung des endgültigen Dokumentes verwendet werden soll.

3. *Prozessor*
   Der Prozessor führt eine XSL-Transformation der Seite durch und erweitert damit das DOM des Producers.

4. *Formatierer*
   Bereitet das Dokument zur Auslieferung vor bzw. erstellt dieses in der gewünschten Formatierung (bspw. WML, PDF, Microsoft Office Dateiformate, etc.)

Für jede dieser Komponenten (mit Ausnahme des Reaktors) bietet Cocoon Standards an, welche aber problemlos durch eigene Komponenten ausgetauscht werden können. Cocoon nutzt standardseitig Xerces als Producer, Xalan als XSLT-Prozessor und FOP als XSLT-Formatierer. Cocoon ist sehr gut dokumentiert und es existieren mehrere Projekte, welche das Cocoon-Framework nutzen.

Struts Struts unterstützt die komponentenbasierte Softwareentwicklung von Webanwendungen mit JSP/Servlets und ist als OpenSource verfügbar. Das Framework stellt momentan den De-facto-Standard für aktionsgesteuerte Frameworks dar. Vom Benutzer initiierte Requests werden in sog. Action-Klassen und in zugeordneten ActionForms weiter verarbeitet.

Sämtliche Aktionen werden in einer oder mehreren zentral gehaltenen XML-basierten Konfigurationsdateien definiert. Die Präsentation erfolgt standardseitig mit Hilfe von Java Server Pages (JSP). Anpassungen für andere Verfahren (auch über XSLT) sind auch möglich. Im Backend ermöglicht Struts den einfachen Datenaustausch auf Basis von JDBC und EJB. Für Struts existieren mehrere Entwicklungswerkzeuge, welche die Implementierung von Struts-Anwendungen erleichtern.

Turbine Turbine stellt dem Entwickler webbasierter Applikationen eine Reihe von Servicekomponenten zur Verfügung, welche bspw. für Datenhaltung, Caching, Logging, etc. genutzt werden können[9]. Mit diesem Ansatz ist Turbine eher als Baukastensystem zu sehen, mit dem nicht nur Web-Applikationen entwickelt werden können. Die Struktur des Frameworks besteht aus fünf Modulen: Action, Layout, Navigation, Screen und Page.

[8] DOM: Document Object Model, Vom W3C erarbeitetes Modell für Objekte eines Dokuments.
[9] vgl. `http://jakarta.apache.org/turbine/index.html`

Letzteres entscheidet anhand der Anforderungen (Request) des Benutzers, welche Aktion (Action) durchgeführt werden soll und erstellt mit Hilfe der restlichen Module die gewünschte Ausgabe. Dabei wird davon ausgegangen, dass das zu erzeugende Dokument (Page) aus einer oberen und unteren Navigation und einem Inhaltsbereich (Screen) besteht.

Expresso Expresso ermöglicht die komponentenbasierte Entwicklung verteilter Web-Applikationen. Das Framework stellt dazu Komponenten zur Sicherheit, Datenhaltung, Protokollierung (Logging), Cachemechanismen, etc. zur Verfügung[10]. Das Open Source Projekt nutzt dazu das Struts Framework und den XML Parser Xerces.

Vergleich

Kriterium	Cocoon	Struts	Turbine	Expresso
Lizenz	ASL[11]	ASL	ASL	Jcorporate Apache Style Software License
OpenSource	×	×	×	×
Komponentenbasiert / Komponentenaustausch	×/ ×	×/ ×	×/ ×	×/ ×
Einbindung beliebiger Avalon[12]-kompatibler Komponenten möglich	×	–	×	–
Programmiersprache	Java	Java	Java	Java
Verhalten über Konfiguration steuerbar	×	×	×	×
Verteilung auf mehrere Server	×	×	×	×
Backend-Funktionalitäten	Logging	Nicht explizit enthalten	Datenhaltung, Logging	Caching, Datenhaltung, E-Mail, Logging, Login, Sicherheit, Workflow, etc.

Tabelle 6.2: Vergleich: Frameworks zur Content-Publication

Portal Frameworks

Diese Frameworks bieten die nötige Grundfunktionalität zur Implementierung von Portalen auf Basis bzw. unter Nutzung des Portlet-Konzeptes. Portal-Frameworks sollten über eine Komponenten-Schnittstelle zur Integration der Portlet-Komponenten verfügen.

Pluto Pluto enthält eine Referenzimplementierung der Java Portlet Specification JSR-168 und stellt lediglich einen Portlet-Container zur Instanzierung und Nutzung von Portlets dar. Die eigentlichen Portlets sind selbst zu implementieren.

[10] vgl. `http://www.jcorporate.com/html/products/expresso.html`
[11] Apache Software Licence
[12] vgl. `http://avalon.apache.org/`

Jetspeed Das Jetspeed-Framework bietet die Grundfunktionalität zur Implementierung von Portalen und wird im Rahmen des Jakarta-Projektes der Apache Foundation als OpenSource Framework angeboten. Jetspeed generiert Portalseiten mit Hilfe einer hinterlegten Seitenbeschreibung und nutzt durchgängig eine XML konforme Sprache zur Beschreibung von Portalseiten. Die Präsentation erfolgt standardseitig über eine Kombination aus Java Server Pages (JSP) und HTML, kann aber auch unabhängig vom Datenformat erfolgen[13].

Zur Abbildung aller enthaltenen Funktionalitäten setzt Jetspeed auf verschiedene zusätzliche OpenSource Projekte. Dazu gehören Turbine (als Servlet-Schnittstelle), ECS, Castor, Cocoon (inkl. der Standardkomponenten) und Velocity. Jetspeed bietet darüber hinaus die Möglichkeit, Portlets zu integrieren.

Die sehr gute Dokumentation, welche auch viele Beispiele enthält, erleichtert die Implementierung auf Grundlage dieses Frameworks. Die Nutzung mehrerer anderer Projekte erschwert allerdings die individuelle Anpassung des Frameworks erheblich, da hier neben dem Wissen um die J2EE Programmierkonzepte auch alle anderen Projekte hinreichend gut genug bekannt sein müssen.

Liferay Liferay ist eine J2EE Applikation — und damit im engeren Sinne nicht als Framework zu nutzen —, basiert auf Enterprise Java Beans (EJBs) und baut auf das Struts-Framework auf. Auf Liferay basierende Portale können Requests auf Basis von HTTP (HTML/WML → Verarbeitung durch Struts Servlet), WebServices sowie SOAP und RMI entgegennehmen. Die eigentliche Geschäftslogik, welche den Request verarbeitet, ist in Stateless Session EJBs enthalten[14].

Die Lösung zeichnet sich durch eine gute Dokumentation aus. Da Liferay eine eigene Applikation darstellt, sind Portale damit schnell umsetzbar. Unterstützt wird dies durch bereits fertige Portlets für diverse Funktionalitäten. Nachteil dieses Konzeptes ist, das ein Customizing (im Quellcode) so gut wie unmöglich ist.

Jahia Der kommerzielle Portalserver Jahia, welcher zusätzlich Funktionen des Content Management enthält, beinhaltet ein unter der GPL veröffentlichtes Framework zur Entwicklung bzw. Erweiterung von Web-Applikationen. Jahia baut auf Struts, Turbine und andere existierende Frameworks auf. Neben Jahia spezifischen Schnittstellen stehen Servlets, WebServices, Portlet (JSR-168) und zukünftig weitere offene Schnittstellen zur Verfügung. Damit können bereits existierende Servlets ohne erheblichen Zusatzaufwand in das Jahia Framework integriert werden.

jPorta jPorta ist eine J2EE Applikation — und damit im engeren Sinne nicht als Framework zu nutzen — und basiert auf dem Jeenius Framework[15]. Das Jeenius Framework unterstützt die Entwicklung von webbasierten J2EE Applikationen mit Schwerpunkten auf der Benutzerauthentifikation und –autorisation sowie der Entwicklung von Web-Frontends inkl. Caching und XML Transformation. Zur Generierung des Web-Frontends setzt jPorta verstärkt auf Java Server Pages (JSPs). Wie Liferay lassen sich mit jPorta in kurzen

[13]Quelle: `http://www.intranetjournal.com/articles/200304/pij_04_04_03a.html`
[14]Quelle: `http://www.liferay.com/products/index.jsp`
[15]vgl. `http://jeenius.sourceforge.net`

Entwicklungszeiten kleinere Portale realisieren. Dafür ist für individuelle Modifizierungen oder Ergänzungen Know-how im Umgang mit dem Jeenius Framework notwendig.

jPortlet jPortlet ist die Open Source Implementierung eines Portlet-Container, welcher stark der IBM WebSphere Portlet API nachempfunden wurde. Im Gegensatz zu anderen Frameworks entspricht die Implementierung allerdings nicht der JSR-168 Schnittstellenspezifikation.

Zur Abbildung aller enthaltenen Funktionalitäten setzt jPortlet auf verschiedene zusätzliche OpenSource Projekte. Dazu gehören Velocity und Hibernate. JPortlet unterstützt eine rollenbasierte Userverwaltung und Cachemechanismen.

6.3.2 Web-Frameworks

Servlet– und Portlet-Frameworks bilden die Grundlage zur Entwicklung von Portalen, lassen allerdings i. d. R. die Ausgabe beliebiger (oft dem DOM entsprechende) Inhalte zu, d.h. der Entwickler kann festlegen, welche Komponenten (Textfelder, Formulare, etc.) erzeugt werden sollen. Um einen „Wildwuchs“ der individuell hinzugefügten Komponenten zu verhindern, bietet es sich an, dem Entwickler nur ein festes Set an visuellen Komponenten zur Verfügung zu stellen.

Millstone UserInterfaceLibrary Das als OpenSource Implementierung angebotene Millstone API[16], hinter dem ein eigenes Widget-Modell steht, wird durchgängig in der XML-basierten User Interface Markup Language (UIML, offener Standard) beschrieben. Damit kann dieses Framework mittels Adaptern für verschiedene Ausgabeformate (HTML, WML, ...) erweitert werden. Die Adapter werden auf Basis von XSLT Stylesheets erstellt, welche die Transformation von UIML in das gewünschte Ausgabeformat übernehmen.

Damit ergibt sich eine sehr gute Integrationsmöglichkeit in XML-basierten Portal-Frameworks. Portlets können auf dieser Grundlage in dem ihnen zugeordneten Fragment definierte Objekte (Tabellen, Texte, Formulare, etc.) anlegen. Millstone sorgt dann für die Generierung der Ausgabe für verschiedene Ausgabemedien.

Echo Angelehnt an das Swing API, welche die Entwicklung grafischer Nutzeroberflächen für Java Applikationen ermöglicht, können mit Echo ereignisgesteuerte Webapplikationen entwickelt werden. Damit werden vom Entwickler nur grundlegende Kenntnisse bzgl. HTML, HTTP, etc. abverlangt. Echo ist OpenSource Software und wird unter der GPL Lizenz vertrieben[17].

Nachteil des Frameworks ist, dass das Rendering des (standardseitig ausschließlich HTML-)Codes über den Programmcode erfolgt und damit von Haus aus relativ unflexibel ist. Ein Rendering mit Hilfe externer XSLT-Stylesheets oder ähnlicher Verfahren ist nicht vorgesehen. Das Framework kann allerdings um beliebige Rendering Komponenten erweitert werden, welche beliebige Ausgabeformate unterstützen können.

[16] vgl. `http://millstone.sourceforge.net/`
[17] vgl. `http://www.nextapp.com/products/echo/doc/cat/renderedcomponents.html`

WingS Ähnlich dem Echo-Framework, lehnt sich WingS an die Swing API an und erlaubt damit die schnelle — letztlich vom Ausgabeformat unabhängige — Generierung von grafischen Oberflächen. WingS eignet sich damit für die Portierung von Swing– zu Web-Oberflächen. WingS ist OpenSource und wird unter der GPL vertrieben.

Analog zu Echo dient WingS standardseitig zur Generierung von HTML-Code in einem vorgegebenen Style. Für jede visuelle Komponente (Text, Button, etc.) steht dazu ein Codegenerator zur Verfügung, welcher in Abhängigkeit vom Request verschiedene Ausgabeformate erzeugen kann. Werden die Codegeneratoren entsprechend modifiziert bzw. erweitert, ist damit auch die Erzeugung von beliebigen Ausgabeformaten möglich. Leider ist diese Möglichkeit wenig dokumentiert. Das dahinter stehende Konzept erzwingt die Codegenerierung (des auszugebenden Dokumentes) über den Programmcode.

ECS Das Element Construction Set (ECS) ist ein Java API zur Generierung von Elementen und zugehörigen Attributen für diverse SGML-konforme Dokumente (bspw. XML, XHTML, WML). Die Elemente können direkt mit Hilfe von Java Objekten erzeugt werden — die Entwicklung ist damit unabhängig von der konkreten Ausprägung des zu erzeugenden Datenformates möglich. ECS unterliegt der GPL und ist damit als OpenSource Software frei verfügbar.

In Bezug auf die Oberflächengenerierung eignet sich ECS zur Erzeugung von vom Ausgabeformat unabhängigen XML Dokumenten, welche dann über eine entsprechende XSLT-Transformation in das gewünschte Ausgabeformat umgewandelt werden können. Änderungen der Oberfläche, d.h. Modifikation der visuellen Komponenten oder des Ausgabeformates, müssen dann nicht direkt im Programmcode erfolgen — dazu muss lediglich das XSLT Dokument verändert werden.

6.4 Darstellung des Interface im Browser

6.4.1 Gesetzliche Anforderungen

Zur Darstellung von Arbeitsoberflächen existieren in der BR Deutschland verschiedene gesetzliche Vorgaben, welche vorrangig dem gesundheitlichen Schutz der Benutzer dienen. Für öffentliche Verwaltungen können im Einzelfall erweiterte Anforderungen gelten.

Barrierefreiheit

Sind von Menschen gestaltete Lebensbereiche (Verkehrsmittel, Gebäude, IuK-Systeme, etc.) für behinderte Menschen grundsätzlich und ohne besondere Erschwernis oder fremde Hilfe nutzbar, sind diese „barrierefrei“. In Bezug auf Informations– und Kommunikationssysteme wird unter dem Begriff der „Barrierefreiheit“ der den ungehinderten Zugang zu Informationen im Internet in erster Linie für körperlich behinderte Benutzer (insb. seh–, hör– und motorisch behinderte Menschen) verstanden.

Speziell zur Schaffung webbasierter Benutzeroberflächen wurde die Web Accessibility Initiative (WAI) gegründet, welche entsprechende Richtlinien veröffentlichte. Diese Richtlinien [33] enthalten verschiedene Kriterien und Checklisten, welche in drei verschiedene Prioritätsstufen eingeteilt sind. In der BR Deutschland regelt die Barrierefreie

Informationstechnik-Verordnung (BITV) und §7 Behindertengleichstellungsgesetz (BGG) die wesentlichen Kriterien zur Schaffung webbasierter Benutzeroberflächen. Diese Richtlinien laufen letztlich auf die WAI-Richtlinien hinaus.

Hinsichtlich der dargestellten Inhalte ist eine klare, einfache Sprache zu verwenden, Polyseme sind zu vermeiden und Text sollte nur dann mit multimedialen Inhalten ergänzt werden, wenn dies das Verständnis fördert. Alle Nicht-Text-Komponenten (Formulare, Bilder, etc.) müssen beschrieben werden. Benutzer müssen Informationen zu Kontext und Orientierung bereitgestellt bekommen.

Ergonomie

In Bezug auf die Ergonomie sind in erster Linie die Regelungen des Bundesarbeitsschutzgesetzes und die Bildschirmarbeitsverordnung bindend. Nach §4 Bildschirmarbeitsverordnung (Umsetzung der EU-Richtlinie 90/270 EWG) ist zu beachten, das Oberflächen, welche zur Erledigung „fremdbestimmter Aufgaben“ zur Erreichung von Zielen einer Organisation (d.h. Verwaltungen, Unternehmen, etc.) bestimmt sind, Angaben zu Dialogabläufen und die Beschreibung von Fehlern anbieten müssen.

Neben den Gesetzen befassen sich mehrere internationale, europäische und deutsche Normen mit der Ergonomie:

- *DIN 29241*
  Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten
- *DIN 66234 Teil 8*
  Aufgabenangemessenheit, Selbstbeschreibungsfähigkeit, Steuerbarkeit, Erwartungskonformität, Fehlerrobustheit
- *ISO 9241 Part 10*
  Suitability for the task, Self-descriptiveness, Controllability, Conformity with user expectations, Error tolerance, Suitability for individualization, Suitability for learning

Zu den wichtigsten Festlegungen gehören hier:

- *Aufgabeangemessenheit*
  Dialoge sollen bei der Erledigung einer Arbeitsaufgabe unterstützen und durch spezifische Eigenschaften des Systems den Benutzer nicht belasten. Aufgaben, welche nicht zwingend die Interaktion mit dem Benutzer erfordern, werden vom System selbsttätig durchgeführt. Das System kann das spezifische Prozesswissen beim Benutzer voraussetzen.
- *Selbstbeschreibungsfähigkeit*
  Der Benutzer muss auf Wunsch Informationen zum Einsatzzweck, Leistungsumfang und einzelnen Dialogschritten erhalten. Damit müssen (unter Umständen auch situationsabhängige) Systemzusammenhänge erkannt werden können.
- *Steuerbarkeit*
  Eine Arbeitsoberfläche muss dem Benutzer die Möglichkeit geben: Die Geschwindigkeit der Bearbeitung, Auswahl und Reihenfolge der Arbeitsmittel sowie Art und Umfang der Ein– und Ausgaben zu beeinflussen. D.h. unter anderem, dass kein vorgegebener Arbeitstakt existiert und Dialoge unterbrochen werden können.

- *Erwartungskonformität*
  Die Interaktion muss für den Benutzer in einer aus seinen Erfahrungen im Arbeitsablauf erwartungskonformen Art und Weise erfolgen. Das erzwingt ein einheitliches Dialogverhalten, Rückmeldungen des Systems, möglichst gleich bleibende Antwortzeiten und die Ausgabe eines erkennbaren Bearbeitungsstandes von Arbeitsprozessen.
- *Fehlerrobustheit*
  Selbst bei erkennbar fehlerhaften Eingaben muss das gewünschte Arbeitsgebnis mit möglichst geringem Arbeitsaufwand erreicht werden. Dazu gehört, dass Fehler dem Benutzer verständlich angezeigt und Korrekturmöglichkeiten angeboten werden bzw. der Fehler automatisch behoben wird. Das System darf durch Fehleingaben nicht in einen undefinierten Zustand gelangen.

6.4.2 Anforderungen an Portale

Portale sollen einen einfachen und schnellen Zugriff auf interne und externe Informationen und Anwendungen ermöglichen. Sie dienen der Unterstützung von Transaktionen und dem Management vom Workflowprozessen sowie der Kommunikation von Benutzern untereinander.

Sie integrieren damit Teile des Dokumentenmanagement, der Bürokommunikation, Knowledge– und von Workflowmanagementsystemen. Sie müssen damit sowohl strukturiert formatierte als auch unstrukturierte Informationen integrieren und kategorisieren können. Dazu müssen die entsprechenden Schnittstellen der angesprochenen Systeme genutzt werden (Filesysteme, Schnittstellen der Mail– und Groupware– und Dokumentenmanagementsysteme).

Der Zugriff auf ein Portal erfolgt im Normalfall über einen Webbrowser, ist aber auch über mobile oder sonstige Endgeräte (PDA, Smartphone, etc.) möglich. Erreicht wird diese weite Integration verschiedener Endgeräte über die strikte Nutzung offener Standards und Schnittstellen (z. B. Portlets, WebServices, http, XML, etc.). Portale sind skalierbar, beeinträchtigen durch ihre Antwortzeit die Arbeit der Benutzer nicht und bieten die notwendige Sicherheit durch Verschlüsselung des Datenaustausches.

6.4.3 Standards

Übertragung

Zur Übertragung der darzustellenden Dokumente an das Endgerät des Benutzers (bspw. PC mit Webbrowser) existieren endgerätespezifische Übertragungsprotokolle. Das genutzte Übertragungsprotokoll sollte folgenden Anforderungen genügen:

- Offener Standard
- Breite Verfügbarkeit von Server– und Clientapplikationen für alle genutzten Netze, Hardware– und Betriebssysteme
- Aktive Nutzung des Standards
- Eignung des Standard für webbasierte Portale

Da webbasierte Portale, welche hier Betrachtungsgegenstand sind, auf dem TCP/IP-Referenzmodell basieren, erfolgt im Folgenden lediglich eine Betrachtung oberhalb der Netzwerkebene. Zum Versenden von Daten zwischen zwei Netzwerkteilnehmern (Server und Client) existieren innerhalb der Transportschicht folgende Protokolle:

- *TCP*
  Transmission Control Protocol — verbindungsorientierte, sichere Datenübertragung
- *UDP*
  User Datagram Protocol — verbindungslose, unsichere Datenübertragung

Die Nutzung des UDP erfüllt nicht die Voraussetzungen, welche hinsichtlich der Ergonomie an einen Bildschirmarbeitsplatz gestellt werden, da UDP nicht sicherstellt, dass alle vom Client (Arbeitsplatz) angeforderten Daten vollständig und in der korrekten Reihenfolge empfangen werden können.

Die Anwendungsschicht umfasst alle Protokolle, die mit Applikationen (bspw. einem Webbrowser) zusammenarbeiten und anwendungsspezifische Daten zwischen Client und Server austauschen. In Bezug auf webbasierte Portale sind folgende Protokolle relevant:

HTTP Das Hypertext Transfer Protocol (HTTP) ist ein Client–/Serverprotokoll zum Zugriff auf Informationen im Web und stellt die oberste der Protokollschichten des ISO/OSI-Schichtenmodells dar. Mit Hilfe des HTTP-Protokolls können beliebige Dokumententypen transportiert werden. Primär wird das Protokoll allerdings zur Übertragung von HTML-Seiten genutzt. Das HTTP enthält neben dem eigentlichen Dokument einen Header, welcher Metainformationen enthält und das Dokument sowie die verarbeitende Applikation näher beschreibt. Innerhalb eines Vorganges kann http immer maximal ein Dokument enthalten. Zur Sicherung des Datentransfers können mit Hilfe von HTTPS (Hypertext Transfer Protocol Secure) alle übertragenen Daten verschlüsselt werden. HTTP wird vorrangig für die Kommunikation mit stationären Bildschirmarbeitsplätzen genutzt.

WAP Ähnlich dem HTTP regelt das Wireless Application Protocol (WAP) die Kommunikation zwischen einem Server und mobilen Endgeräten (bspw. Mobiltelefone, PDA, etc.). Die WAP-Architektur umfasst dabei ein komplettes, verbindungsorientiertes (WTP) Fünf-Schichtenmodell:

- *Transport* – Wireless Datagram Protocol (WDP)
  Kommunikation zwischen WAP und physikalischen Netzen wie GSM– oder TCP/IP-Netzen
- *Sicherungsschicht* – Funktion Wireless Transport Layer Security (WTLS)
  Sicherung der Datenintegrität, Privatsphäre und Authentifizierung
- *Transaktionsschicht* – Wireless Transaction Protocol (WTP)
  Ausführung von Transaktionen
- *Session-Schicht* – Wireless Transaction Protocol (WSP)
  Abbildung eines verbindungsorientierten und verbindungslosen Service
- *Anwendungsschicht* – Wireless Application Environment (WAE)
  WAE unterstützt Wireless Markup Language (WML), WML-Script und Wireless Telephony Applications (WTA)

WAP wird vor allem in der BR Deutschland und Europa unterstützt, wird allerdings nicht in der erwarteten Häufigkeit genutzt.

iMode Der aus Japan kommende Standard zur Kommunikation von mobilen Endgeräten mit einem Server dient vor allem dazu, in der Anwendungsschicht mit Hilfe von cHTML kodierten Inhalten zu empfangen. Im Gegensatz zu WAP wird iMode in Japan stark genutzt. Der iMode Dienst basiert auf einem paketvermittelten Netz, in dem alle Datenpakete unabhängig von einer separaten Verbindung verschickt werden können. Ein gesonderter Verbindungsaufbau kann hier entfallen. Imode nutzt folgende Schichten:

- *PDC-P*
  Paketvermittlung innerhalb des Mobilfunknetzes
- *Transportschicht* – Transport Layer Protokoll (TLP)
  Hoher Datenpaketdurchsatz
- *Anwendungsschicht* – Application-Layer-Protocol (ALP)
  Ermöglicht die direkte HTTP-Kommunikation zwischen Mobiltelefon und iMode-Server

Über die Konzentration auf cHTML, einer Untermenge des vom W3C standardisierten HTML, setzt die Entwicklung von iMode Applikationen kein gesondertes Know-how voraus.

Darstellung

Die Darstellung der an ein Endgerät des Benutzers (bspw. PC mit Webbrowser) übertragenen Dokumente erfolgt mit Hilfe einer Präsentationsapplikation. Das verwendete Dokumentenformat muss dazu einem von der Applikation unterstützten Format entsprechen. Je nach Endgerät (oft in Hinblick auf die Datenmenge und den beschränkten Darstellungsbereich) und Anwendungszweck (Interaktion oder Präsentation) sind verschiedene Dokumentenformate zu empfehlen. Die Dokumentenformate sollten folgenden Anforderungen entsprechen:

- Offener Standard
- Breite Verfügbarkeit von Präsentationsapplikationen (Browser, etc.) für alle genutzten Betriebssysteme
- Aktive Nutzung des Standards
- Eignung des Standard für webbasierte Portale

HTML-Familie und CSS Zur Darstellung von Webseiten wird die 1992 von Tim Berner-Lee und Robert Cailliau entwickelte Hypertext Markup Language (HTML) verwendet. Alle heute am Markt befindlichen Webbrowser unterstützen die Darstellung von in HTML kodierten Dokumenten.

HTML ist eine als offener Standard definierte, textorientierte Auszeichnungssprache, welche auf Grundlage der Standard Generalized Markup Language (SGML)[18] entwickelt

[18]Die Festschreibung der SGML Spezifikation erfolgt in ISO-Norm 8879

wurde. Innerhalb eines HTML-Dokumentes werden alle logischen Komponenten des Dokumentes beschrieben und hierarchisch gegliedert. Darüber hinaus werden in Textdokumenten oft genutzte Elemente wie Überschriften, Tabellen, Grafiken, etc. direkt als solche ausgezeichnet. Das W3C[19] entwickelt den HTML-Standard ständig weiter und sorgt für eine transparente Darstellung des Standards.

Zum aktuellen Zeitpunkt stellen der Standard HTML 4.01 und die daraus abgeleitete XHTML 1.1 (XML-konforme Kodierung eines HTML-Dokumentes) den Stand der Entwicklung dar. HTML 4.01 legt viel Wert auf eine durchgängige logische Beschreibung aller Komponenten, der Auslagerung aller Formatierungen in die Ergänzungssprache Cascading Stylesheets (CSS), welche mit der CSS 2.1 Spezifikation[20] von den verbreitetsten Browsern weitgehend unterstützt wird, sowie der Einbindung von Skriptsprachen und der Internationalisierung. Im Gegensatz zu vorherigen HTML-Spezifikationen legt die konsequente Nutzung des HTML 4.01 bzw. XHTML-Standards die Grundlage zur Generierung barrierefreier Webseiten. Die Unterstützung der ISO/IEC 10646 (Unicode-System) erlaubt die Notation von Webseiten in allen hier definierten Schriften.

cHTML Zur Beschreibung von Dokumenten für mobile Endgeräte auf Basis des iMode Übertragungsstandards wurde vom japanischen Telefonkonzern NTT 1998 der cHTML-Standard entwickelt und beim W3C zur Diskussion eingereicht[21]. Compact HTML (cHTML) bildet nur eine Teilmenge des HTML-Standard ab, um auf den oft mit wenig Hauptspeicher und niedrig getakteten CPUs ausgestatteten und geringer Bandbreite angebundenen Endgeräten die Darstellung von HTML-Dokumenten zu ermöglichen. Dazu schließt cHTML einige Teile des HTML-Standards aus (Tabellen, Frames, Zeichensätze/Internationalisierung, CSS, etc.), übernimmt ansonsten aber die jeweilige Spezifikation.

Im Gegensatz zu WML müssen HTML-Dokumente zur Auslieferung an mobile Endgeräte allerdings nicht komplett umgeschrieben werden und der cHTML-Standard profitiert automatisch von allen Erweiterungen des normalen HTML-Standards.

WML Ebenfalls zur Dokumentenbeschreibung für mobile Endgeräte wurde in Europa von verschiedenen Netzbetreibern (darunter auch die Deutsche Telekom) auf Basis der WAP-Übertragung die Wireless Markup Language (WML) entwickelt. Ähnlich dem iMode-Standard soll mit Hilfe vom WML den Spezifika mobiler Endgeräte begegnet werden. Ein WML-Dokument („Deck“) kann dazu mehrere sog. „Cards“ enthalten, von denen immer genau eine Card im Display des Endgeräts dargestellt werden kann. Die WML basiert im Gegensatz zu HTML und cHTML (nicht XHTML) auf dem XML-Standard.

Neben der Dokumentenbeschreibung mittels WML können zusätzlich WML-Skripte (WMLScript) eingebunden werden, welche — ähnlich der Einbindung von bspw. JavaScript in HTML — die Abarbeitung von Funktionalitäten auf dem Endgerät zulassen. Die Formatierung der in den WML-Cards enthaltenen Inhalte (Text, Überschriften, Tabellen, etc.) erfolgt vom WML-Browser und kann nicht bzw. nur in sehr begrenztem Maße (bspw. Ausrichtung, Hervorhebungen) gesteuert werden.

[19] `http://www.w3c.org/`
[20] `http://www.w3.org/TR/CSS21/`
[21] `http://www.w3.org/TR/1998/NOTE-compactHTML-19980209/`

PDF Das Portable Document Format (PDF) ist ein universelles Dateiformat. PDF-Dokumente können unabhängig von dem Programm und dem Betriebssystem, mit dem sie erstellt wurden, betrachtet werden. Dazu wird der kostenlos verfügbare Adobe Acrobat Reader oder ein entsprechendes Browser-PlugIn benötigt. PDF-Dokumente eignen sich daher insbesondere zur Dokumentenverteilung und –verwendung, da PDF Dokumente i. d. R. nicht weiter modifiziert werden und entsprechend geschützt werden können.

Die Nutzung von PDF beschränkt sich momentan auf stationäre Endgeräte, da für deren Übertragung i. d. R. eine große Bandbreite bzw. Übertragungsgeschwindigkeit und für die Darstellung teilweise erheblicher Hauptspeicherbedarf und CPU-Leistung erforderlich ist. Ähnlich HTML– oder WML-Dokumenten können PDF-Dokumente Querverweise (innerhalb aber auch außerhalb des Dokumentes) sowie interaktive Elemente (Formulare) enthalten.

Zusammenfassung

Dokumentenformat	HTML-Familie	cHTML	WML	PDF
Anwendungsziel	Webseiten/ –browser	Mobiltelefone	Mobiltelefone	Dokumenten-verwendung, –ausdruck
Format	textbasiert	textbasiert	textbasiert	binär
Interaktion / Formulare	möglich	möglich	möglich	möglich
Scripteinbettung	möglich	nicht möglich	extern	Acrobat Script[22]
Formatierung der Darstellung	über CSS	bedingt möglich	bedingt möglich	möglich

Tabelle 6.3: Standardisierte Dokumentenformate zur Content-Darstellung

Kodierung

Die Kodierung von beliebigen Zeichen anderer Sprachen als Deutsch kann aus verschiedenen Gründen notwendig sein. Dazu zählen unter anderem:

- Wiedergabe von Zitaten oder komplett fremdsprachiger Dokumente
- Ansprache/Information ausländischer Bürger
- Ansprache/Information nicht deutsch sprechender Deutscher (bspw. Spätaussiedler, Sorben, etc.)

Zur Darstellung der Schriften können entweder spezifische oder vollständige Zeichensätze verwendet werden. Der Einsatz spezifischer Zeichensätze empfiehlt sich vor allem auf mobilen Endgeräten, da diese i. d. R. nur die zwingend notwendigen Zeichensätze enthalten. Dazu beinhaltet die von der European Computer Manufacturer's Association (ECMA) entwickelte ISO-8859-Zeichensatzfamilie ein Set von standardisierten Zeichensätzen

[22] Acrobat Script ist eine in Acrobat und Acrobat Reader ausführbare Scriptsprache, welche Javascript um eigene Objekte erweitert.

für alphabetische Schriften (d.h. keine fernöstlichen Zeichen). Alle Zeichensätze enthalten den wichtigsten Teil des ASCII-Zeichensatzes (Werte 0 bis 127) und können damit weitestgehend alle Standard-ASCII-Texte darstellen.

Im Gegensatz zur ISO-Kodierung strebt die Unicode-Kodierung eine (möglichst) vollständige Erfassung aller bekannten Zeichen an. Jedes Zeichen ist dazu klassifiziert und mit einem eindeutigen, für den Standard verbindlichen Zeichenwert versehen. Zusätzlich enthält jedes Zeichen diverse Eigenschaften wie bspw. die Schreibrichtung. Das Unicode-Standardisierungskonsortium wurde 1991 gegründet und bestimmt die aufzunehmenden Zeichen. Unicode 2.0 ist mit der ISO/IEC 10646 synchronisiert und wird damit vom HTML 4.01 bzw. XHTML-Standard unterstützt. In der Regel wird hier eine Unicode UTF-8 Kodierung eingesetzt, da damit kodierte Dokumente hinsichtlich des ASCII-Standardzeichensatzes (Code 0–127) unverändert gültig sind und nicht in der Zwei-Byte-Notation des Unicode BMP-Teil kodiert werden müssen[23].

Neben der Kodierung sind weitere Unterschiede in der Schreibkultur zu beachten. Dazu zählt u. a. die Schreibrichtung (bspw. die arabische, hebräische Schrift oder fernöstliche Schriften). Die Abbildung dieser Schreibkultur erfordert hinsichtlich der Texteingabe eine entsprechende Unterstützung durch das Betriebssystem und die Präsentationssoftware (Webbrowser).

Kodierung	ASCII	ISO-8859-x	ISO-10646 (Unicode)
Max. Zeichenzahl	256	jeweils 128 zusätzlich zu ASCII-Basiszeichensatz	2^{32}
Schreibkultur insb. Schreibrichtung	nicht unterstützt	nicht unterstützt	unterstützt

Tabelle 6.4: Vergleich: Textkodierungen

6.4.4 Werkzeuge

Liegen die auf einer Arbeitsoberfläche darzustellenden Inhalte in XML-Notation vor, müssen diese mit Hilfe eines XSLT-Prozessors für die Ausgabe vorbereitet und mit Hilfe eines XSLT-Formatierers in das gewünschte Ausgabeformat gebracht werden. Die meisten Frameworks zur Content-Publication bringen diese Werkzeuge bereits mit, lassen aber i. d. R. einen Austausch der Komponenten zu. XSLT-Prozessor

XSLT-Prozessor XSLT-Prozessoren können XML-Dokumente im Kontext ihrer logischen Baumstruktur mit Hilfe eines XSLT-Stylesheets transformieren. Innerhalb dieses Prozesses entsteht ein neues Dokument, welches von einem XSLT-Formatierer in das endgültige Ausgabeformat gebracht wird. Entscheidungskriterien für XSLT-Prozessoren sind[24]:

- Konformität zu den offenen Standards XSLT und XPATH

[23] Dies verringert bei der sporadischen Nutzung von Nicht-ASCII-Zeichen zusätzlich die Dokumentengröße gegenüber einer durchgängigen Unicode.

[24] vgl. XSLT-Prozessoren im Überblick: http://www.oio.de/public/xml/xslt-prozessoren.html

- Schnittstellen zur Einbindung in das genutzte Framework (inkl. genutzte Programmiersprache)
- Lizenzpolitik des Hersteller
- Performance
- Verbreitung des Prozessors und Stabilität der Entwicklergemeinde bzw. des Herstellers

Eine Übersicht über gängige XSLT-Prozessoren ist in Tabelle 6.5 dargestellt (s. nächste Seite).

XSLT-Formatierer XSLT-Formatierer erzeugen auf Grundlage des von einem XSLT-Prozessor erzeugten Dokumentes das letztlich an den Benutzer auszuliefernde Dokument (bspw. PDF, Postscript, MS Office kompatible Dokumentenformate). In der Regel erwarten XSLT-Formatierer dazu ein nach dem XSL-FO-Standard [34] formatiertes XML-Dokument, welches dann in einem sog. Rendering-Prozess in das Ausgabeformat überführt wird. Bewertungskriterien für XSLT-Formatierer sind:

- Konformität bei der Unterstützung des XSL-FO-Standard
- Unterstützte Ausgabeformate
- API Verfügbarkeit (insb. für welche Sprachen)
- Lizenzpolitik des Herstellers
- Performance
- Verbreitung des Prozessors und Stabilität der Entwicklergemeinde bzw. des Herstellers

Tabelle 6.6 zeigt eine Übersicht über einige ausgewählte XSLT-Formatierer (s. nächste Seite).

Zur Generierung HTML–, XML–, WML– und Plaintext-konformer Dokumente ist i. d. R. kein XSLT-Formatierer nötig, da dies bereits von den meisten XSLT-Prozessoren erledigt wird. Bei der Generierung von PDF-Dokumenten ist zu beachten, das momentan kein XSLT-Formatierer bekannt ist, welcher Formulare (und damit Interaktionsmöglichkeiten) innerhalb des PDF-Dokumentes zulässt. Bei den verschiedenen Herstellern/Entwicklern existieren allerdings bereits entsprechende Bemühungen.

Prozessor/Merkmal	Xalan-J / Xalan-C++	Saxon-B, Saxon-SA	XT	Sablotron	MSXML
Lizenz	ASF	B: MPL, SA: Kommerziell	OpenSource	GPL	kommerziell
API für Sprachen	Java, C++	Java	Java	C++, PHP, Perl	C/C++
Betriebssystem	Java: alle, C++: Windows, Linux (RedHat und SuSE), Solaris, AIX, HP-UX	alle	alle	Windows, Linux, Solaris, FreeBSD, OpenBSD, HP-UX, MacOS	Windows
XSLT Standard	1.0	2.0	1.0	1.0	1.0
XPATH Standard	1.0	2.0	1.0[25]	1.0	1.0
URL / Hersteller	http://xml.apache.org/xalan-j/	http://saxon.sourceforge.net/	http://www.blnz.com/xt/	http://www.gingerall.com/charlie/ga/xml/p_sab.xml	http://msdn.microsoft.com/xml/

Tabelle 6.5: Übersicht: XSLT-Prozessoren

Formatierer/Merkmal	FOP	XEP	XSL Formatter	PassiveTex	ScripturaXBOS
Lizenz	ASF	kommerziell	kommerziell	OpenSource	kommerziell
API für Sprachen	Java	Java, .NET	Java, .NET, C++ (angekündigt)	Makros für TeX System	Java, C++, Cobol, SOAP
Betriebsystem	alle	Java: alle, .NET: Windows	alle	alle	alle
Quellformat	XSL-FO 1.0	XSL-FO 1.0	XSL-FO 1.0, eigene Erweiterungen	XSL-FO 1.0	Scriptura Document, XSLT, XSL-FO
Zielformate	PDF (inkl. Verschlüsselung), PCL, PS, RTF, SVG, XML, Print, AWT, MIF, TXT	PDF, PS	PDF, MathML, WordML (MS Office 2003), EMF/WMF, TIFF	PDF, TEX	PDF (inkl. Verschlüsselung), XHTML, XSL-FO, PCL, AFP, RTF, XML
URL / Hersteller	http://xml.apache.org/fop/	http://www.renderx.com/	http://www.antennahouse.com/	http://www.tei-c.org.uk/Software/passivetex/	http://www.inventivedesigners.com/scriptura

Tabelle 6.6: Übersicht: XSLT-Formatierer

[25]Hier konnte die konkrete Unterstützung nicht ermittelt werden.

6.5 Kriterienkatalog

Bei der Erarbeitung von Kriterien zur Auswahl eines passenden Frameworks und entsprechender Basistechnologien und Werkzeuge wurden folgende Gesichtspunkte beachtet:

- Existierende Richtlinien oder Empfehlungen zur Auswahl der Systeme
- Nutzung möglichst weit verbreiteter, offener Systeme
- Einsatz von freier Software

Die ausgearbeiteten Kriterien stellen eine unverbindliche Empfehlung dar, welche die Grundlage bei der Entwicklung der RAfEG-Referenzarchitektur bildet.

6.5.1 SAGA-Richtlinien

Zur Standardisierung von E-Government-Anwendungen wurden von einem Expertenkreis die „SAGA – Standards und Architekturen für E-Government-Anwendungen“ erarbeitet. Sie liegen seit August 2003 vor und empfehlen „... technische Rahmenbedingungen für die Entwicklung, Kommunikation und Interaktion von IT-Systemen der Bundesbehörden. Für Prozesse und Systeme, die E-Government-Dienstleistungen des Bundes erbringen, ist die Konformität mit SAGA verbindlich.“ (Quelle: [31]).

Basiskomponente CMS

Zur Abbildung von (Informations-)Portalen wird innerhalb Intranet– und Internetumgebungen der Bundesbehörden die Nutzung des CoreMedia Enterprise Portal Server Integration Package empfohlen (vgl. [32], S. 136f). Damit soll die Verwaltung und Pflege der Portale vereinheitlicht und vereinfacht werden. Zur Einbindung von Fachanwendungen kommen die Kommunikationsprotokolle SOAP (WebServices), CORBA, RMI und direkte Interprozesskommunikation zum Einsatz.

Im Frontend wird hier ein Portlet-Framework auf Basis des IBM Websphere Portal Server genutzt. Die Portletspezifikation entspricht dem JSR-168. Im Backend wird eine auf Systinet WASP basierenden Web Services Schnittstelle angeboten.

SAGA Grundanforderungen

Hinsichtlich der Anforderungen an eine Softwarearchitektur für die Entwicklung von Applikationen im E-Government-Bereich stellen die SAGA-Richtlinien verschiedene Anforderungen (vgl. [32], S. 58f). In Bezug auf die Entwicklung der Präsentationsschicht eines Workflowsteuerungssystems ergeben sich folgende Anforderungen:

- *Sicherheit*
  Sicherstellung der Autorisierung eines Benutzers und (optional) die Verschlüsselung des Datenverkehrs.
- *Wiederverwendbarkeit*
  Einsatz von Komponenten (in Bezug auf Darstellung [hier Designkomponenten], Werkzeuge, Frameworks), welche entweder bereits existieren und genutzt werden

können bzw. Entwicklung eigener Komponenten unter dem Aspekt der Wiederverwendbarkeit.

- *Flexibilität*
  Anpassungsfähigkeit und Portierbarkeit muss gewährleistet sein. D.h. das bspw. die Generierung des darzustellenden Dokumentes (inkl. dessen Formates) frei konfigurierbar sein sollte und nicht fest kodiert wird.
- *Offenheit*
  Das System hat weitestgehend offene Standards zu nutzen. Die Grundlage des Systems sollte ausschließlich auf offene Standards setzen, Schnittstellen zum Import/Export von Daten oder Dokumenten müssen ggf. auch proprietäre Standards nutzen.
- *Skalierbarkeit*
  Die Generierung des Frontend und Verarbeitung von Nutzereingaben muss auf mehrere Rechner verteilbar sein, d.h. das eingesetzte Framework und die konkrete Implementierung muss eine Verteilung auf mehrere Cluster unterstützen.
- *Performance*
  Im Sinne einer guten Ergonomie müssen Antwortzeiten des Systems den Erwartungen des Benutzers entsprechen oder ein entsprechender Bearbeitungsstatus angezeigt werden.
- *Verfügbarkeit*
  Die Zugriff auf die Applikation muss berechtigten Personen zu den entsprechenden Arbeitszeiten oder durchgängig (je nach Zielgruppe) möglich sein.
- *Fehlertoleranz*
  Fehleingaben oder der Versuch das System absichtlich zu verändern (bspw. über Cross-Site Request Forgeries) müssen von System verhindert oder entsprechend korrigiert werden.
- *Wartbarkeit*
  Die Einarbeitung externer Fachleute sollte über die Verwendung möglichst weit verbreiteter, gut dokumentierter Systeme erfolgen. Das Verhalten und die Ausgaben des Systems sollten weitestgehend über Konfigurationen und nicht Änderungen am Quellcode erfolgen können.

6.5.2 Kriterienauswahl

Bei der Auswahl der Bewertungskriterien wurde hier eine Gruppierung nach verschiedenen Aspekten vorgenommen.

Aspekt: Präsentation

- *Übertragungsprotokoll*
  Werden stationäre Endgeräte angesprochen ist die Nutzung von HTTP als De-facto-Standard unumgänglich. Mobile Endgeräte sollten je nach verwendetem Netz über WAP oder iMode angesprochen werden. Das eingesetzte System hat die notwendigen Übertragungsprotokolle zu unterstützen.
- *Fragmente*
  Eine funktionale Komponente des Systems sollte — wie innerhalb des Portlet-

Konzeptes beschrieben — nur die Fragmente eines Dokumentes ändern, für welche es die entsprechenden Rechte besitzt.

- *Rendering*
  Das Rendering des auszugebenden Dokumentes sollte ohne Eingriff in den Quellcode frei konfigurierbar sein. Der Einsatz von XML/XSLT bietet die einfachste Möglichkeit, das Layout der Anwendung anzupassen und außerhalb des Anwendungspfades zu speichern, was beim Update der Anwendung verhindert, dass das spezifische Layout überschrieben wird. Beim Einsatz von JSP ist es zwingend erforderlich, dass diese Dateien mit im Anwendungsverzeichnis liegen.

Kriterium	Beschreibung
Kategorie: Hersteller/ Entwickler	
Lizenztyp	Systeme zur Generierung von webbasierten Arbeitsoberflächen für verschiedene Geräteklassen sind kommerziell und als OpenSource, teilweise auch als Mischformen erhältlich. Neben Fragestellungen zur Haftung bei Fehlfunktionen (die Präsentationskomponente ist der Bereich, welcher ggf. die Verbindung zu öffentlichen Netzen herstellt) ist bei kommerziellen Lizenzen zu hinterfragen, ob Beschränkungen hinsichtlich der serverseitigen Verteilung (Serverlizenzen) und clientseitigen Verteilung (Clientlizenzen) exisitieren.
Verbreitung	Eine große Verbreitung spricht für eine bessere Wartbarkeit der Software. Hersteller kommerzieller Software können dazu zu Verkaufszahlen (sofern diese veröffentlicht werden) bzw. Marktanteil, Entwickler freier Software zu Downloads/bekannten Projekten und/oder Veröffentlichungen befragt werden.
Weiterentwicklung	Findet eine laufende Weiterentwicklung des Produktes statt? Das kann u. a. aus der Versionierung, Historie der stabilen Versionen (insb. in OpenSource Projekten), dem Datum des letzten Release, den Releaseabständen, der Anzahl der Entwickler bzw. Unternehmensgröße des Herstellers sowie Aktivitäten von Anwendern in Mailinglisten, Foren oder unabhängigen Veröffentlichungen bestimmt werden.
Modifizierbarkeit	Sind Modifizierungen am Quellcode zulässig? Dazu muss der Quellcode verfügbar und gut dokumentiert sein.
Kategorie: Systemumgebung	
Betriebssystem	Für welche Betriebssysteme ist das Produkt verfügbar oder nutzt es eine Ablaufumgebung, welche für das gewünschte Betriebssystem verfügbar ist? Die hier vorgestellten Frameworks nutzen i. d. R. Java-Technologie, so dass der Einsatz geläufiger Serverbetriebssysteme problemlos möglich ist.
Laufzeitumgebung	In welcher Programmiersprache in das Produkt entwickelt. Bei der Nutzung von Enterprise Java Beans (EJB) ist bspw. als Plattform ein J2EE Application Server (z. B. JBoss, JOnAS) notwendig, der mehr Ressourcen benötigt als ein J2EE Web Container (z. B. Tomcat, Jetty).

Typ	Präsentationskomponenten sollten auf Grundlage eines Framework erstellt werden, da dies die nötige Flexibilität hinsichtlich des Produkteinsatzes, der Austauschbarkeit von Komponenten und in der Betriebsphase notwendiger Modifizierungen und Ergänzungen einzelner Komponenten (bspw. zur Unterstützung neuer Endgeräte, etc.) sichert.
Schnittstellen	Über welche Schnittstellen kann das Produkt genutzt werden? Dies betrifft externe Schnittstellen (Input/Output) sowie — sofern das Produkt aus mehreren Komponenten besteht — interne Schnittstellen, welche einen Austausch von Komponenten ermöglichen.
Verteilung (Systemarchitektur)	Die Präsentationskomponente bzw. einige ihrer Subkomponenten sollte über mehrere Server verteilt werden, damit Ergebnisse rechenintensiver Arbeiten wie bspw. das Rendern diverser Dokumentenformate (PDF, RTF, ...) zeitnah bereitgestellt werden können. Um Load-Balancing zu ermöglichen, muss eine Verteilung auf mehrere Server zwingend möglich sein.
Kategorie: Standards	
BGG §7	Der Aufbau und die Gestaltung eines Dokumentes muss auf Grundlage der WAI-Richtlinien (zumindest Umsetzung der WAI-A-Kriterien) erfolgen. Dialoge und Ausgaben sind anhand der Ergonomierichtlinien zu erstellen. Das Dokumentenformat muss dazu vollkommen flexibel konfigurierbar sein, d.h. eingesetzte Software bzw. Komponenten (bspw. XSLT-Formatierer) dürfen keine eigenen, fest kodierten Annahmen über das Erscheinungsbild des auszugebenden Dokumentes treffen.
Ergonomie	Zur Einhaltung der Richtlinien/Normen zur Ergonomie muss die Gestaltung und die Abfolge sowie Prüfung und Bearbeitung von Arbeitsschritten flexibel definierbar und für verschiedene Endgeräte und Nutzergruppen anpassbar sein.
XML	Das System sollte offene, gut dokumentierte und möglichst weit verbreitete Standards nutzen, um eine hohe Interoperabilität zu erreichen. Die Nutzung XML-basierter Dokumente ist im beschriebenen Umfeld unumgänglich, da diese unabhängig von der eigentlichen Anwendung verarbeitet werden können und einen De-facto-Standard darstellen.
Flexibilität	Die Steuerung der Software muss weitestgehend über eine entsprechende Konfiguration möglich sein (bspw. auf Basis von XML– oder XSL-Dokumenten), um häufige Änderungen am Quellcode zu vermeiden. Eingesetzte Features dürfen die Flexibilität (bspw. beim Einsatz bestimmter Komponenten) nicht beeinträchtigen.
Dokumentenformate	Dokumente sollten vom System in den allg. gebräuchlichen Formaten HTML 4.01, XHTML und PDF generierbar sein. Ältere HTML-Formate sind auf Grund der fehlenden Unicode-Unterstützung nicht zu empfehlen. Zur Formatierung von HTML-Dokumenten muss konsequent auf Style Sheets gesetzt werden, da sich darüber — unabhängig vom HTML-Quellcode — das Erscheinungsbild für diverse Ausgabemedien (Bildschirm, Drucker, Screenreader, etc.) steuern lässt.

Kategorie: Sicherheit	
IT-Integration	Die gewählten Präsentationskomponenten müssen sich hinsichtlich der Anbindung an Backendsysteme (Verzeichnisdienste, Datenbanken, DMS, GIS/Mapserver, etc.) in die bestehende IT-Infrastruktur einfügen sowie Sicherheitskomponenten (bspw. Autorisation und Authentifikation) ggf. integrieren können. Dazu müssen die hier jeweils eingesetzten Protokolle und Schnittstellen unterstützt werden (bspw. LDAP, JDBC, WebDAV, etc.).
Nutzerautorisation/ Nutzerauthentifikation	Die Nutzerautorisation und –authentifikation erfolgt nicht primär in den Präsentationskomponenten sondern sollte über eine separate, einen Verzeichnisdienst nutzende Sicherheitskomponente erfolgen. Sofern diese Komponente eine Autorisierung auf Protokollebene (http, WAP/WTLS-Client-Authenfication, etc.) durchführen, muss dies von der Präsentationskomponente unterstützt werden.
Verschlüsselung	Eine Verschlüsselung sollte auf Ebene der Anwendungsschicht (HTTPS, etc.) sowie innerhalb generierter Dokumente (bspw. PDF → RC4) möglich sein. Dies kann entweder innerhalb der genutzten Präsentationskomponenten oder unter Nutzung externer Sicherheitskomponenten erfolgen. Zur Verschlüsselung sollten offene, weit verbreitete Standards zum Einsatz kommen, da diese nach allgemeiner Erfahrung den größten Schutz bieten.
Signatur	Die elektronische Signatur einzelner Dokumente (insb. PDF → RSA 1024 Bit, 2048 Bit) kann für einzelne Anwendungsfälle relevant sein. Die Signatur zur Autorisation von Servern ist über die Nutzung von serverseitigen, zertifizierten Signaturen möglich und sollte zum Standardfunktionsumfang der Präsentationskomponente gehören.
Kategorie: Features	
Internationalisierung	Die Unterstützung des Unicode-Zeichensatzes sowie diverser Schreibkulturen gehört zum Standardumfang von Präsentationskomponenten.
Austauschbarkeit von Komponenten	Existieren Anforderungen, welche die Nutzung eines speziellen Features erzwingen, sollte dieses im Produkt enthalten sein, zusätzlich integriert oder individuell dazu programmiert werden können. Speziell bei der Anforderung zur Generierung verschiedenster Dokumentenformate (bspw. HTML, WML, PDF, SVG, etc.) sollte die Präsentationskomponente über die nötige Flexibilität zur Integration zusätzlicher Subkomponenten verfügen.

Tabelle 6.7: Kriterien für Webinterfaces

7 Zusammenfassung

Der Software– und Kriterienkatalog gibt einen Überblick über die aktuell in Frage kommenden Systeme, Technologien und deren Charakteristika. Die übergeordnete Zielsetzung bestand in der Erarbeitung von Bewertungskriterien und –gewichtungen, welche:

- die Erstellung der RAfEG-Systemarchitektur mit dem Ziel der nahtlosen Integration von Softwaresystemen und –komponenten ermöglichen und
- den möglichen Einsatz bestehender oder neu zu erwerbender Softwaresysteme und –komponenten erleichtern.

Neben den jeweils spezifischen Kriterien konnten allgemeingültige Bewertungsmerkmale erarbeitet werden, welche unter Berücksichtigung der spezifischen Gewichtung innerhalb einer Software–/Systemkategorie für alle betrachteten Systeme relevant sind. Die folgende Matrix gibt dazu einen Überblick (s. Tabelle 7.1 und 7.2).

Kriterium	Ausprägung	Relevanz für				
		BKS	DMS	GIS	Präsentation	Sicherheit
A – Hersteller/Entwickler						
Lizenztyp	A1-1 Kommerziell A1-2-0 Freeware (kein Code) A1-2-1 GPL A1-2-2 LGPL	Irrelevant, da nur Schnittstellen wichtig	Irrelevant, da nur Schnittstellen wichtig	Irrelevant, da nur Schnittstellen wichtig	Niedrig: Beschränkungen hinsichtlich Clientanzahl beachten	Niedrig: Sofern Kerckhoff-Prinzip erfüllt, keine Einschränkung
Verbreitung	A2-1 Anzahl Installationen	Sehr hoch	Niedrig	Sehr hoch	Hoch	Irrelevant: Sofern Kryptoverfahren verbreitet ist
Weiterentwicklung	A3-1 Updates/Upgrades pro Jahr	Hoch	Niedrig	Hoch	Hoch	Sehr hoch
Sourcecode/ Modifizierbarkeit	A4-1 Nicht zulässig A4-2-1 Zulässig, nicht praktikabel A4-2-2 Zulässig, praktikabel	Irrelevant	Irrelevant	Irrelevant	Niedrig	Niedrig
B – Systemumgebung						
Betriebssystem	B1-1-0 MS Windows 95/98 B1-1-1 MS Windows NT B1-1-2 MS Windows 2000/XP/2003 B1-2 Linux B1-3 Mac OS X B1-4 IBM OS/2	Sehr hoch	Niedrig	Niedrig	Niedrig	Niedrig
Laufzeitumgebung	B2-1 Java B2-2 PHP	Irrelevant	Irrelevant	Irrelevant	Frameworks: Hoch	Frameworks: Hoch
Typ	B3-1 Applikation B3-2 API B3-3 Framework	Hoch	Hoch	Hoch	Sehr hoch	Hoch
Schnittstellen	B4-1 zu (anderen) BKS B4-2 zu (anderen) DMS B4-3 zu (anderen) GIS B4-4 zu Content-Frameworks B4-5 zu Sicherheitslösungen	Sehr hoch	Hoch	Hoch	Niedrig	Sehr hoch
Verteilung	B5-1 Stand-alone B5-2 ASP B5-3 Client/Server	Irrelevant	Irrelevant	Irrelevant	Hoch	Irrelevant

Tabelle 7.1: Kriterienmatrix zu Hersteller/Entwickler und Systemumgebung

Kriterium	Ausprägung	Relevanz für				
		BKS	DMS	GIS	Präsentation	Sicherheit
C – Standards						
BGG §7	C1-1 WAI-A C1-2 WAI-AA C1-3 WAI-AAA	Hoch	Niedrig	Niedrig	Sehr hoch	Irrelevant
Ergonomie	C2-1 DIN 29241 C2-2 DIN 66234/8	Sehr hoch	Hoch	Hoch	Hoch	Hoch
XML	C3-1 XML Dokumente C3-2 XML Konfiguration C3-3 XML Kommunikation	Hoch	Hoch	Hoch	Sehr hoch	Hoch
Flexibilität/ Steuerung des Applikations-verhaltens	C4-1 innerhalb Applikation C4-2 außerhalb Applikation	Niedrig	Niedrig	Niedrig	Sehr hoch	Hoch
Dokumenten-formate	C5-1 proprietär C5-2 offener Standard C5-3 Industriestandard	Sehr hoch	Hoch	Sehr hoch	Sehr hoch	Sehr hoch
D – Sicherheit						
Integration in bestehendes IT-Konzept	D1-1 keine Anpassung nötig D1-2 Anpassung nötig	Hoch	Hoch	Hoch	Hoch	Sehr hoch
Prüfung der Nutzerautori-sation und –authentifikation	D2-1 Integriert D2-2 Nutzung Fremddienste	Niedrig (wenn durch DMS geschützt)	Sehr hoch	Sehr hoch	Hoch	Sehr hoch
Verschlüsselung	D3-1 keine Verschlüsselung D3-2-1 proprietäres Verfahren D3-2-2 Standardverfahren	Niedrig	Niedrig	Niedrig	Hoch	Sehr hoch
Signatur	D4-1 keine Signatur D4-2-1 proprietäres Verfahren D4-2-2 Standardverfahren	Niedrig (wenn virtuelle Poststelle)	Niedrig	Irrelevant	Niedrig	Sehr hoch
E – Features						
Internationali-sierung	E1-1 Unicode-Unterstützung E1-2 Schriftkulturen	Sehr hoch	Sehr hoch	Hoch	Sehr hoch	Irrelevant
Archivierung	E2-1 Vollsicherung E2-2 Teilsicherung E2-3 Rückspielen	Niedrig (wenn DMS ge-nutzt)	Sehr hoch	Niedrig (wenn DMS ge-nutzt)	Irrelevant	Irrelevant
Austausch-barkeit von Komponenten	E3-1 nicht möglich E3-2 innerhalb des Systems E3-3 außerhalb des Systems	Niedrig, oft Irrelevant	Niedrig, oft Irrelevant	Niedrig	Hoch	Sehr hoch

Tabelle 7.2: Kriterienmatrix zu Standards, Sicherheit und Features

Literaturverzeichnis

[1] Stahlknecht, P. ; Hasenkamp, U.: *Einführung in die Wirtschaftsinformatik*. 9. Auflage. Berlin : Springer Verlag, 1999

[2] Kontacts IT-solutions GmbH (Hrsg.): *Dokumenten Management System (DMS) / Produktauswahl*. Version: 2003. `http://www.kontacts.de/1_Unternehmen/Downloads/Kontacts_Arb-Papier_DRT.%pdf`. – Online–Ressource, Abruf: 8. Mär. 2005. – DRT Arbeitspapier

[3] Bernau, G.: *Mit der richtigen Informationsverarbeitung auf Erfolgskurs*. Wiesbaden : Gabler Verlag, 1997

[4] Datenschutzinstitut Niedersachen (Hrsg.): *Datenschutzgerechtes eGovernment*. Version: Nov. 2002. `http://cdl.niedersachsen.de/blob/images/C1358174_L20.pdf`. – Online–Ressource, Abruf: 8. Mär. 2005

[5] Krems, Burkhardt: *Qualitätsmanagement*. Version: Mär. 2004. `http://www.olev.de/q/qm.htm`. – Online–Ressource, Abruf: 8. Mär. 2005

[6] Goland, Y. ; Whitehead, E. ; Faizi, A. ; Carter, S. R. ; Jensen, D.: *RFC 2518: HTTP Extensions for Distributed Authoring – WEBDAV*. `http://webdav.org/specs/rfc2518.html`. Version: Feb. 1999

[7] Clemm, G. ; Amsden, J. ; Ellison, T. ; Kaler, C. ; Whitehead, J.: *RFC 3253: Versioning Extensions to WebDAV*. `http://www.webdav.org/deltav/protocol/rfc3253.html`. Version: Mär. 2002

[8] Clemm, G. ; Reschke, J. F. ; Sedlar, E. ; Whitehead, J.: *RFC 3744: WebDAV Access Control Protocol*. `http://webdav.org/specs/rfc3744.html`. Version: Mai 2004

[9] Mayer-Föll, R. (Hrsg.) ; Pätzold, J. (Hrsg.): *Umweltinformationssystem Baden-Württemberg als Teil des Landessystemkonzepts, Rahmenkonzeption 1998, RK UIS '98*. Ministerium für Umwelt und Verkehr Baden-Württemberg, Stuttgart : Universitätsverlag Ulm GmbH, 1998

[10] Lierhaus, Gerd: *Computerlexikon*. 1. Auflage. Düsseldorf : Sybex-Verlag, 1991

[11] Engesser, Hermann (Hrsg.): *DUDEN Informatik*. 2. Auflage. Mannheim, Leipzig, Wien, Zürich : Dudenverlag, 1993

[12] Appelt, Wolfgang: *Dokumentenaustausch in offenen Systemen: Einführung in ISO-Norm 8613*. Berlin, etc. : Springer Verlag, 1990

[13] Microsoft Corporation (Hrsg.): *Rich Text Format (RTF) Specification*. Version: Mai 1999. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnrtfs%pec/html/rtfspec.asp. – Online–Ressource, Abruf: 8. Mär. 2005. – Version 1.6

[14] Braun, Fabian: *Standard- und Individualsoftware: Einsatzmöglichkeiten, Vor- und Nachteile*. Version: Jan. 2004. http://www.iwi.uni-hannover.de/lv/seminar_ws03_04/www/Braun/seminar.htm%. – Online–Ressource, Abruf: 8. Mär. 2005. – Seminar

[15] Schilcher, Matthäus: *GIS – Begriffe und Definitionen*. Version: Feb. 2002. http://www.gis1.bv.tum.de/Aktuelles/Infos/Dokumente/Geoinformationssyst%eme.htm. – Online–Ressource, Abruf: 8. Mär. 2005

[16] Open GIS Consortium (OGC) (Hrsg.): *OpenGIS Simple Features Specifications For SQL*. Version: Mai 1999. http://www.opengeospatial.org/docs/99-049.pdf. – Online–Ressource, Abruf: 8. Mär. 2005. – Revision 1.1

[17] Patterson, D. A. ; Gibson, G. A. ; Katz, R. H.: A Case for Redundant Arrays of Inexpensive Disks (RAID). In: *Proceedings of the International Conference on Management of Data (SIGMOD)*, ACM, 109–116

[18] Dierks, T. ; Allen, C.: *RFC 2246: The TLS Protocol Version 1.0*. http://www.faqs.org/rfcs/rfc2246.html. Version: Jan. 1999

[19] Wireless Application Forum, Ltd. (Hrsg.): *WAP WTLS Spezifikation*. http://www.wmlclub.com/docs/especwap1.2/SPEC-WTLS-19991105.pdf. Version: Nov. 1999

[20] Rivest, R.: *RFC 1321: The MD5 Message-Digest Algorithm*. http://www.faqs.org/rfcs/rfc1321.html. Version: Apr. 1992

[21] Myers, J. ; Mellon, C. ; Rose, M.: *RFC 1864: The Content-MD5 Header Field*. http://www.faqs.org/rfcs/rfc1864.html. Version: Okt. 1995

[22] Postel, J.: *RFC 821: Simple Mail Transfer Protocol*. http://www.faqs.org/rfcs/rfc821.html. Version: Aug. 1982

[23] Klensin, J.: *RFC 2821: Simple Mail Transfer Protocol*. http://www.faqs.org/rfcs/rfc2821.html. Version: Apr. 2001

[24] Hoffman, P.: *RFC 2487: SMTP Service Extension for Secure SMTP over TLS*. http://www.faqs.org/rfcs/rfc2487.html. Version: Jan. 1999

[25] Klensin, J. ; Rose, M. ; Stefferud, E. ; Crocker, D.: *RFC 1869: SMTP Server Extensions*. http://www.faqs.org/rfcs/rfc1869.html. Version: Nov. 1995

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.): *E-Government-Handbuch*. Version: 2004. http://www.e-government-handbuch.de/. – Online–Ressource, Abruf: 8. Mär. 2005

[27] Imamura, T. ; Dillaway, B. ; Simon, E.: *XML Encryption Syntax and Processing*. Version: Dez. 2002. http://www.w3.org/TR/xmlenc-core/. – Online–Ressource, Abruf: 8. Mär. 2005. – W3C Recommendation

[28] Bartel, M. ; Boyer, J. ; Fox, B. ; LaMacchia, B. ; Simon, E.: *XML-Signature Syntax and Processing*. Version: Feb. 2002. http://www.w3.org/TR/xmldsig-core/. – Online–Ressource, Abruf: 8. Mär. 2005. – W3C Recommendation

[29] Housley, R. ; Polk, W. ; Ford, W. ; Solo, D.: *RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. http://www.faqs.org/rfcs/rfc3280.html. Version: Apr. 2002

[30] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.): *IT-Grundschutzhandbuch: 6. EL*. Version: 2004. http://www.bsi.bund.de/gshb/deutsch/download/GSHB2004.pdf. – Online–Ressource, Abruf: 8. Mär. 2005

[31] Koordinierung- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (Hrsg.): *SAGA-Standards / Lifecycle*. Version: Aug. 2003. http://www.kbst.bund.de/E-Government/SAGA-,229/Standards-Life-Cycle.htm%. – Online–Ressource, Abruf: 8. Mär. 2005

[32] Bundesministerium des Inneren (Hrsg.): *SAGA – Standards und Architekturen für E-Government-Anwendungen*. Version: 2003. http://www.kbst.bund.de/saga. – Online–Ressource, Abruf: 8. Mär. 2005

[33] World Wide Web Consortium (W3C) (Hrsg.): *Web Content Accessibility Guidelines 1.0*. Version: Jan. 2000. http://www.w3c.de/Trans/WAI/checkpunkt-liste.html. – Online–Ressource, Abruf: 8. Mär. 2005

[34] Adler, S. ; Berglund, A. ; Caruso, J. ; Deach, S. ; Graham, T. ; Grosso, P. ; Gutentag, E. ; Milowski, A. ; Parnell, S. ; Richman, J. ; Zilles, S.: *Extensible Stylesheet Language (XSL) Version 1.0*. Version: Okt. 2001. http://www.w3.org/TR/xsl/. – Online–Ressource, Abruf: 8. Mär. 2005. – W3C Recommendation

Tabellenverzeichnis