eCH-0014 SAGA.ch

Name	SAGA.ch
Standard-Nummer	eCH-0014
Kategorie	Interoperabilitätsstandard
Reifegrad	Implementiert
Version	6.00
Status	Genehmigt
Genehmigt am	2012-09-06
Ausgabedatum	2012-09-12
Ersetzt Standard	5.00
Sprachen	Deutsch, Französisch
Autoren	Fachgruppe Technologie Josef Schmid, Leitung FG; Informatiksteuerungsorgan des Bundes Peter Kiowski, Microsoft Schweiz GmbH Daniel S.Muster Daniel Gabi, Schweizerische Bundeskanzlei Erich Vogt, Symantec Corp. Eric Dubuis, Berner Fachhochschule Anne Possoz, EPFL Thomas Teske, Oracle Software (Schweiz) GmbH Norbert Bollow, Swiss Open Systems User Group /ch/open Gregoire Hernan, Schweizerische Informatikkonferenz (SIK) Reto Gantenbein, Soreco AG
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Das Dokument SAGA.ch (Standards und Architekturen für eGovernment Anwendungen Schweiz) stellt in verdichteter Form die technischen Richtlinien für die Umsetzung von eGovernment Anwendungen in der Schweiz dar. Es werden hier verbreitete Standards für die Entwicklung von eGovernment Systemen vorgestellt. Standards bewirken kostengünstigere Lösungen, indem eGovernment Systeme nicht von Grund auf entwickelt werden müssen, sondern indem man beim Aufbau von eGovernment Systemen auf bewährte Basiskomponenten der ICT Industrie zurückgreifen kann. So werden Doppelentwicklungen und Insel-

lösungen innerhalb der Behörden vermieden. Durch die Standardisierung sollte weiter der Aufwand für das Engineering möglichst minimal gehalten werden.

SAGA.ch versteht sich als Standardisierung mit einem ganzheitlichen Ansatz, welcher die wichtigsten Aspekte erläutert, um die oben genannten Ziele zu erreichen. Das Dokument richtet sich in erster Linie an Entscheidungsträger aus den Bereichen Organisation und Informationstechnik (eGovernment Teams) der Behörden.

SAGA.ch ist in Anlehnung an die Dokumente SAGA.de Versionen 1.1 bis 4.0 entstanden, welche vom KBSt im Deutschen Bundesministerium des Innern und in Zusammenarbeit mit dem Deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) hergestellt worden sind. Weiter sind die zu SAGA entsprechenden, französischen[1], britischen[2] und globalen relevanten Standards (u.a. SAGA Indien, e-Gif Neuseeland, EIF) konsultiert worden.

Bemerkung

In Anlehnung an die Schriftenreihe KBSt; mit spezieller Bewilligung des KBSt-D

Dieser Vorschlag für einen Standard wurde von der ***eCH*** Fachgruppe Technologie erstellt; in Anlehnung an SAGA.de (vom KBSt im Deutschen Bundesministerium des Innern in Zusammenarbeit mit dem Deutschen Bundesamt für Sicherheit in der Informationstechnik, kurz BSI).

Redaktion: ***eCH*** Fachgruppe Technologie

Ansprechpartner: ***eCH***-Geschäftsstelle

E-Mail: info@eCH.ch

Homepage und Download der digitalen Version: www.eCH.ch

[1] Le cadre commun d´interoperabilité des systemes d'information publics

[2] eGIF eGovernment Interoperability Framework

Inhaltsverzeichnis

1 Status des Dokuments

Das vorliegende Dokument wurde vom Expertenausschuss ***genehmigt.*** Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

1.1 Änderungen von SAGA 5.0 zu 6.0

SAGA.ch Version 6.0 zeichnet sich durch folgende Änderungen zur der bisherigen von eCH und dem Informatikrat Bund verabschiedeten Version 5.0 aus:

Kapitel (v.5)	Name	Klassierung v.5	Klassierung v.6
	Aktualisierung der Versionen aller Standards		
4.2.x	Anwendung SAGA in Ausschreibungen/Abnahmen	--	Dringend empfohlen
4.3	Vorgehen bei SAGA Inkopatibilitäten (ISO/ITIL)	--	Dringend empfohlen
6.4.1	FTP Ergänzungen von Port und IETF RFC's	Empfohlen	Empfohlen
6.4.2	HTTP Ergänzungen Ports und IETF RFC's	Dringend empfohlen	Dringend empfohlen
6.4.3	SMTP Ergänzungen RFC's	Dringend empfohlen	Dringend empfohlen
6.8.	Überarbeitung/Kürzung des Kap.Webservices (WS)		
6.8.5	MTOM	--	Empfohlen
6.8.7	WS-Adressing	--	Dringend empfohlen
6.8.9.6	Sedex	--	Empfohlen
6.8.9.5	OSCI Neue Texte	Empfohlen	Empfohlen
6.8.10	WSRF	--	Unter Beobachtung
6.9	REST/RESTful HTTP	Unter Beobachtung	Empfohlen
6.10	SPML	--	Unter Beobachtung
6.11	ebXML Security Neue Texte	Unter Beobachtung	Unter Beobachtung
6.12.2	BPMN Textergänzungen	Empfohlen	Empfohlen
7.2.1	UTF-8	--	Dringend empfohlen
7.2.1	ISO-8859-15	--	Dringend empfohlen

7.2.2	CSS Neue Texte	Dringend empfohlen	Dringend empfohlen
7.2.4	SIARD	--	Empfohlen
7.2.7	HTML v.5	--	Unter Beobachtung
7.2.8	Interlis Neue Texte	Dringend empfohlen	Dringend empfohlen
7.2.13	Office Open XML Formats Neue Texte, Version	Empfohlen	Empfohlen
7.2.14 bis 7.2.18	PDF Formate A-1/A-2/ UA/VT/H/E/X Neue Texte	Empfohlen	Empfohlen/Unter Beobachtung
7.2.19	ATOM	--	Unter Beobachtung
7.2.19	RSS1.0/AtomPub 1.0	--	Empfohlen/Unter Beobachtung
7.2.20	RTF neuer Text	Empfohlen	Empfohlen
7.2.25	DSDL	--	Empfohlen
7.2.26	XBRL	--	Empfohlen
6.4.1	XForms	--	Empfohlen
7.4.7	SWF file format (Adobe)	--	Nicht empfohlen
7.6.1	JavaScript	Nicht Empfohlen	Empfohlen
7.6.5	AJAX Files	Nicht Empfohlen	Empfohlen
8.4	ISO/IEC 27001, 27002	--	Empfohlen
8.4	ISO/IEC 19770-1	--	Unter Beobachtung
8.5.2	AES (ISO 18033-3)	Empfohlen	Dringend empfohlen
8.5.2	IDEA Lizenz/Patentprüfung	Empfohlen	Empfohlen
8.5.4	SHA-1 Neue Texte	Empfohlen	Nicht empfohlen
8.8.3	Kerberos	Nicht Empfohlen	Empfohlen
8.8.5	IPSEC V.1.X Neue Texte	Dringend empfohlen	Dringend empfohlen
8.8.10.2	WS-SecureConversation	--	Empfohlen
8.8.10.5	Web Services Policy Attachment	--	Empfohlen
8.8.10.6	WS-Security Policy	--	Empfohlen
8.8.10.7	XACML	Unter Beobachtung	Empfohlen
8.8.10.8	XKMS	Nicht Empfohlen	Empfohlen
8.8.10.11	WS Coordination	--	Empfohlen
8.8.10.12	WS Transaction	--	Empfohlen
	WSS Profiles	Empfohlen Kap.8.7.10.8	gestrichen
8.9.1	ISO/IEC 14443 1-4	--	Unter Beobachtung
8.9.1	ISO/IEC 15693 1-3	--	Unter Beobachtung
8.9.1	ISO/IEC 18092 (NFC Suite)	--	Unter Beobachtung

8.9.1	MS Crypto API	Empfohlen	gestrichen
8.11.6	ISO/IEC 11770 1-4 Schlüs-seltransport	--	Unter Beobachtung

- Dokumentenkürzungen u.a. Verwendungsbeschriebe bei Empfehlungen gestrichen
- Review vom Glossar und Abkürzungen mit gegenseitigem Abgleich (u.a. Verweise adaptiert mit den relevanten Links)
- Erfinder und deren URL zusammengelegt
- Empfehlungsquerprüfungen mit anderen SAGA Dokumenten wie SAGA.de u.a. auch mit eGif Neuseeland und SAGA Indien.

2 Einleitung

2.1 Vorbemerkung

Dieses Dokument stellt in verdichteter Form verbreitete, technische Standards für die Entwicklung von eGovernment[3]-Systemen vor, nicht jedoch Abläufe, Prozesse, Methoden oder Produkte.

Erfahrungsgemäss werden von den Experten auf diesem Gebiet sehr viele Abkürzungen und überwiegend englische Akronyme verwendet. Ein Teil dieser Namen ist urheberrechtlich bzw. als Warenzeichen oder Produkt für bestimmte Hersteller oder Normierungsorganisationen national und international geschützt. Zur Erzielung einer einfachen Struktur wurde generell auf etwelche Urheberrechts- und Quellenverweise verzichtet. Die Verwendung eines „Namens“ oder einer Abkürzung in diesem Dokument bedeutet nicht, dass sie frei von Urheber- und Schutzrechten anderer sind.

Weiter können Herausgeber, Autoren und befragte Experten keine Verantwortung für die technische Funktionsfähigkeit, Kompatibilität oder Vollständigkeit der diskutierten Standards übernehmen. Kommentare, Ergänzungen, Berichtigungen werden bevorzugt an den auf Seite 2 erwähnten, offiziellen Ansprechpartner erbeten.

Versionsnummern sind dort aufgeführt, wo sie im diskutierten Zusammenhang relevant sind. Die Versionsnummern sind auch implizit über die Version oder über die Nummer des Standards angegeben worden; die Nichterwähnung einer Versionsnummer impliziert aber keine Konformität. Wenn für Standards gar keine Versionsnummern angegeben sind, ist die aus Marktsicht stabilste Version gemeint, welche nicht immer die neueste ist. Ab SAGA.ch Version 2.1 sind die entsprechenden Versionen der Standards, soweit vernünftig und notwendig, für alle aufgeführten Technologien berücksichtigt und festgelegt worden.

Wir verwenden, wenn möglich, geschlechtsneutrale Begriffe. Wo das nicht sinnvoll scheint, beschränken wir uns auf die männliche Form. Die männliche Form steht aber stets für beide Geschlechter.

2.2 Hintergrund

Mit der eGovernment-Strategie des Bundes vom 13. Februar 2002 hat der Bundesrat strategische Stossrichtungen aufgezeigt, an denen sich die Bundesverwaltung, aber auch die Kantone und die Gemeinden orientieren können. Er verpflichtet darin, die Bundesverwaltung, ihre internetfähigen Dienstleistungen so schnell wie möglich online bereit zu stellen.

[3] Unterstützung der Beziehungen, Prozesse und der politischen Partizipation innerhalb allen staatlichen Ebenen sowie gegenüber allen Anspruchsgruppen durch Bereitstellung von Interaktionsmöglichkeiten mittels elektronischer Medien.

2.3 Nutzen von Standards

Die Verfügbarkeit von e-Dienstleistungen der Verwaltung alleine genügt nicht. Die Systeme der Behörden auf Stufe Bund, Kanton und Gemeinde müssen sowohl untereinander als auch mit den entsprechenden Systemen in den Unternehmen interoperabel sein. Damit dies überhaupt möglich ist, sind technische Standards unter anderem aus folgenden Gründen eine absolute Notwendigkeit.

- Standards bewirken kostengünstigere Lösungen, weil Systeme nicht von Grund auf entwickelt werden müssen sondern auf *bewährte* Basiskomponenten der ICT-Industrie zurückgegriffen werden kann. So werden Doppelentwicklungen und auch Insellösungen innerhalb der Behörden vermieden. Der Aufwand für das Engineering sollte dabei möglichst minimal gehalten werden.
- Erst die Einigung auf Standards schafft die Voraussetzung für eine flächendeckende Interoperabilität und für den mit der technischen Einführung angestrebten Nutzen der elektronischen Kommunikation.
- Inkompatible Lösungen verursachen nebst Kosten infolge zusätzlicher Beschaffung und technischer Implementierung weitere (unnötige) Betriebsaufwände. Durch Standards können entsprechend Kosten gesenkt werden.
- Der bezüglich Aufwand optimierte Ausbau (Modularität) der bestehenden Lösungen wird erst durch die Einigung auf Standards ermöglicht.
- Die Einigung auf Standards erleichtert den bestehenden Anbieter auszuwechseln und verhindert dadurch mögliche Monopole.

Fazit: Standards bewirken die Erweiterbarkeit, die Flexibilität und die Interoperabilität von neuen und bestehenden Lösungen.

2.4 Angesprochener Leserkreis

SAGA.ch richtet sich in erster Linie an Entscheidungsträger aus den Bereichen Organisation und Informationstechnik (eGovernment-Teams) der Behörden. Das Dokument gibt ihnen eine Orientierungshilfe für die Konzeption technischer Architekturen und die technische Grobkonzeption einzelner eGovernment-Anwendungen.

SAGA.ch richtet sich aber auch an die Entwickler und Produktmanager von eGovernment-Systemen in der ICT-Industrie. Die ICT-Industrie ist aufgefordert, sich an der Diskussion und der Festlegung der ***eCH***-Standards zu beteiligen und Lösungen oder Alternativen vorzuschlagen, wenn die vorgestellten Standards zur Umsetzung fachlich nicht ausreichen.

2.5 Ziel und Aufbau des Dokuments

2.5.1 Grundprinzipien

Modernes eGovernment erfordert interoperable Informations-, Kommunikations- und Transaktionssysteme, die (im Idealfall) reibungslos zusammenwirken. Durch einfache und klare Standards und Spezifikationen können die Interoperabilität solcher Systeme optimiert oder

sogar erreicht werden. SAGA.ch identifiziert erforderliche Standards, Formate und Spezifikationen, legt dafür Konformitätsregeln fest und passt diese entsprechend den technologischen Entwicklungen in Zukunft weiter an.

2.5.2 Zielsetzung

SAGA.ch verfolgt die folgenden Ziele:

- Es legt die grundlegenden Formate und Protokolle der Technologie fest, welche den elektronischen Austausch von Informationen und die elektronische Abwicklung von Transaktionen zwischen Behörden und von Behörden mit Bürgern, Unternehmen und Organisationen ermöglichen.
- Die vorgegebenen, vorwiegend technischen Standards definieren eine stabile und verlässliche Basisarchitektur, auf welcher eGovernment-Lösungen der Schweiz aufsetzen sollen.
- SAGA.ch baut soweit wie möglich auf internationale Standards, welche im Markt verfügbar sind und sich dort bewährt haben.
- Die Entwickler lokaler Komponenten sollen bei der Wahl der Lösungstechnologie so frei wie möglich bleiben.
- SAGA.ch kann als Teil der Anforderungsspezifikation bei Ausschreibungen der öffentlichen Hand für eGovernment-Projekte eingesetzt werden.

In diesem Dokument sollen primär Standards zur Informationstechnologie (IT) aufgeführt werden, nicht aber Standards zur Organisation oder zur Projektabwicklung (in der IT). In den Kapiteln, wo ein Bezug zur Organisation und den Prozessen gemacht worden ist, ist dies nur erfolgt, weil man die technischen Ausführungen zum besseren Verständnis in einen Kontext (Zusammenhang) stellen wollte.

2.5.3 Umfang

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

- nicht relevant oder sinnvoll für eGovernment-Anwendungen,
- in genannten Standards inbegriffen oder werden durch genannte Standards referenziert.
- zu neu oder zu umstritten, so dass man sich auf eine baldige, allgemeine Anerkennung dieser Standards auf dem Markt nicht verlassen kann.

Des Weiteren betrachtet SAGA.ch nicht alle Elemente einer technischen Architektur, sondern nur Bereiche, welche einen wesentlichen Einfluss auf die zu verfolgenden Ziele haben. Das Dokument beschreibt Standards hauptsächlich in folgenden zwei Teilen:

- Kapitel 5 beschreibt in groben Zügen ein Schnittstellen- und Architekturmodell
- Die Kapitel 6 bis 8 beschreiben die zum Schnittstellenmodell passenden Standards

Dass gewisse Technologien in diesem Dokument ausführlicher als andere erläutert worden ist, will prinzipiell nichts über den jeweiligen Stellenwert der Technologie aussagen.

2.6 Abzubildende Dienstleistungen

Dienstleistungen der Behörden können sich an die folgenden vier Zielgruppen richten:

- **Privatpersonen** (G2C Government to Citizen)
- **Unternehmen** (G2B Government to Business)
- **Organisationen** (G2O Government to Organisations), z.B. Nichtregierungs-Organisationen (NGO)
- **Behörden** (G2G Government to Government)

Viele Dienstleistungen der verschiedenen Behörden (Bund, Kantone, Gemeinden) sind bekannt. Dabei unterscheidet man normalerweise zwischen den folgenden Dienstleistungstypen:

- **Informationsdienste.** Informationen der Behörden für die Benutzer, d.h. der Informationsfluss ist einseitig
- **Kommunikationsdienste.** Zwischen Behörden und Benutzern sowie unter den Benutzern, d.h. der Informationsfluss ist beidseitig
- **Transaktionsdienste.** Die Abwicklung von Geschäftsprozessen zwischen Behörden und Benutzern.

3 Die Evolution von SAGA.ch

3.1 Aufgabe

SAGA.ch ist ein umfassender Standardisierungsansatz der ***eCH*** Fachgruppe Technologie, welche Normen/Standards der Informationstechnologie, aber nur ansatzweise IKT-Architekturen für eGovernment-Projekte empfiehlt.

3.2 Entstehung

Der Inhalt von SAGA.ch basiert auf den Erfahrungen anderer Länder, insbesondere Deutschland, Frankreich, England, Neuseeland und Indien, sowie auf den persönlichen Erfahrungen und den Kenntnissen der einzelnen Expertenmitglieder der Fachgruppe. SAGA.ch wird in regelmässigen Abständen fortgeführt und aktualisiert, den neuesten Entwicklungen und Erkenntnissen angepasst und unter der Adresse www.eCH.ch publiziert.

3.3 Stellungnahmen und Kommentare

Alle Interessierten aus Behörden, Forschung und Industrie sind gebeten, den hier vorliegenden Inhalt zu kommentieren. Die Kommentare und Anmerkungen können direkt bei der offiziellen Ansprechstelle (s. Seite 2) eingebracht werden. Diese Kommentare werden dann in der Fachgruppe beurteilt und nach Möglichkeit und wo sinnvoll berücksichtigt.

4 Anwendung von SAGA

*4.*1 Klassifizierungen von Standards

eCH teilt Standards in folgende vier Klassen ein:

- Dringend empfohlen
- Empfohlen
- Unter Beobachtung
- Nicht empfohlen

Dringend empfohlen

Standards sind als „dringend empfohlen“ deklariert worden, wenn sie sich aus der Sicht von ***eCH*** bewährt haben und sie die bevorzugte Lösung darstellen. Diese Standards sind vorrangig zu beachten und anzuwenden. Konkurrierende Standards können nebeneinander dringend empfohlen sein, wenn es üblich ist, beide zu nutzen, und diese Nutzung zu keinen Kompatibilitätsproblemen führt. In solchen Fällen ist der für die jeweilige Anwendung am besten geeignete Standard anzuwenden.

Wenn dringend empfohlene und empfohlene oder unter Beobachtung stehende Standards miteinander existieren, so sollen die zwei letzteren nur in begründeten Ausnahmefällen angewandt werden.

Empfohlen

Standards werden als „empfohlen“ deklariert, wenn sie sich bewährt haben, sie aber entweder nicht zwingend erforderlich sind, oder nicht die bevorzugte Lösung darstellen oder für die Einstufung „dringend empfohlen“ noch der weiteren Abstimmung bedürfen. Wenn es neben empfohlenen Standards keine konkurrierenden dringend empfohlenen Standards gibt, so soll von den empfohlenen Standards nur in begründeten Ausnahmen abgewichen werden.

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

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

Unter Beobachtung

Standards werden als „unter Beobachtung“ deklariert, wenn sie der gewünschten Entwicklungsrichtung folgen, sie aber noch nicht ausgereift sind oder sie sich noch nicht ausreichend am Markt bewährt haben.

Wenn es neben „unter Beobachtung“ stehenden Standards keine konkurrierenden dringend empfohlenen oder empfohlenen Standards gibt, so können unter Beobachtung stehende Standards eine Orientierungshilfe sein.

Nicht empfohlen

Standards werden explizit als „nicht empfohlen“ bezeichnet, wenn sie veraltet sind und in früheren SAGA Versionen empfohlen wurden, oder deren Einsatz aus anderen Gründen zu Problemen mit der Interoperabilität führen können.

Die Wahl der jeweiligen Empfehlungen zu den entsprechenden Technologien basierte unter anderem auf den folgenden Kriterien:

- Allgemeine Akzeptanz, was Wirtschaftlichkeit bei der Implementation zur Folge hat.
- Die Technologie ist vielfach eingesetzt oder hat ein grosses Potenzial, dass sie in naher Zukunft in vielen Bereichen eingesetzt wird.
- In Anlehnung an SAGA.de und weiteren eGovernment Empfehlungen.
- Sicherheit

Die Begründung, warum einem Standard diese und nicht eine andere Empfehlung zugesprochen wurde, wird in diesem Dokument in der Regel nicht abgegeben.

4.2 Anwendung von SAGA in Ausschreibungen

Die Erfüllung der Empfehlungen von SAGA kann qualitativ in verschiedenen Stufen erfolgen:

4.2.1. SAGA-Anwendungserklärung (in der Ausschreibung)

Der Auftraggeber nimmt in den Unterlagen zur (WTO-)Ausschreibung eines Software-Systems den Hinweis auf SAGA.ch auf. Er wählt, inwiefern er die Erfüllung der Empfehlungen von SAGA.ch bewerten will: Wählt er es als MUSS-Kriterium bzw. Eignungskriterium, so muss ein Auftragnehmer, um überhaupt in die Auswahlrunde zu gelangen, bestätigen, dass er willens und fähig ist, das zu erstellende System entsprechend den SAGA-Empfehlungen zu erstellen. Der Auftraggeber hat auch die Möglichkeit, die Erfüllungsabsicht von SAGA-Empfehlungen durch den Auftragnehmer in der Bewertung mit zusätzlichen Punkten zu belohnen. Inwiefern die fertige Software am Ende SAGA-konform – d.h. interoperabel, etc. – ist, bleibt vorerst offen.

Dringend empfohlen

4.2.2. SAGA-Konformitätsklausel (für die Abnahme)

Nach der Realisierung erstellt der Auftragnehmer eine SAGA-Konformitätserklärung, weil er die Zusicherung der Erfüllung der Anforderungen von SAGA zum Bestandteil seines Angebotes gemacht hatte. Diese Erklärung wird zusammen mit dem ursprünglichen Angebot vom Auftraggeber geprüft. Eine erfolgreiche Prüfung ist Voraussetzung für die Abnahme des IKT Softwaresystems. Damit das Ergebnis messbar ist, müssen allerdings an einigen Stellen im Pflichtenheft präzisere Angaben gemacht werden, als in SAGA. Beispielsweise betreffend der geforderten Versionen von Standards, dem Grad der Behindertentauglichkeit von

Websites sowie deren Browserkompatibilität oder Qualität des Programmcodes (siehe u.a OWASP-Top-10 https://www.owasp.org/index.php/Top_10_2010-Main), usw.

[ähnlich: «Konzept für SAGA 5.0», beschlossen vom Rat der IT-Beauftragten am 05.06.2009; Version 1.1, Kap. 3.7]

	Dringend empfohlen

4.3 Vorgehen bei SAGA Inkompatibilitäten

Die Anbieter einer E-Government-Applikation sollten über ein professionelles IT-Service-Management gemäss ISO/IEC 20000 verfügen. Dazu werden die notwendigen Mindestanforderungen an Prozesse spezifiziert und dargestellt, die eine Organisation etablieren sollte, um IT-Services in definierter Qualität bereitstellen und managen zu können. Die ISO/IEC 20000 ist ausgerichtet an den Prozessbeschreibungen, wie sie durch die IT Infrastructure Library (ITIL) des Office of Government Commerce (OGC) beschrieben sind, und ergänzt diese komplementär. Die ITIL-Bibliothek unterteilt die Anforderungen an Prozesse und Management in: Strategie, Design, Umsetzung, Betrieb und Verbesserung.

Ein Ereignis («Incident», z.B. ein ungeplantes, unerwartetes Test- oder Auditergebnis, Terminablauf, Beschluss über eine Funktionalität oder dessen Budget usw.), welches die im Dienstleistungsvertrag oder der internen Policy aufgestellten Regeln und Vorgaben bezüglich Funktionalität, Benutz- und Verfügbarkeit, Interoperabilität, Vertraulichkeit und Sicherheit einer Applikation oder einer Schnittstelle beeinträchtigt, ist festzustellen und entsprechend der internen oder vertraglichen Organisation sowie den vorgesehenen Prozessen weiterzuleiten. In der Regel hängen der weitere Verlauf der Abarbeitung und das Ergreifen von Massnahmen bei einem solchen «Incident» vom Ausmass seiner Auswirkungen ab.

Die in den Standards beschriebenen Vorgehensweisen gelten für alle Ereignisse, nicht nur für SAGA-Inkompatibilitäten.

ISO/IEC 20000	Dringend empfohlen

Standards: www.snv.ch, www.ISO.org, www.IEC.org

ITIL V.3/4	Dringend empfohlen

Standards: www.itil.org

5 Systemgrenzen und Schnittstellen

5.1 Komponenten

Aus Sicht des Anwenders ist eine Unterteilung der eGovernment-Applikationen nach der Zielgruppe (Privatpersonen, Unternehmen, Organisationen, Behörden) sinnvoll. Aus technischer Sicht ist aber eine Unterteilung in die folgenden Komponenten sinnvoller:

- Endgerät
- System
- Clearingstelle

Ein **Endgerät** ermöglicht einem Benutzer den Zugriff auf ein System. Beispiele für Endgeräte sind ein Personalcomputer (PC), ein Personal Digital Assistant (PDA) und ein Handy (Mobilphon).

Ein **System** ist eine eGovernment-Anwendung.

Eine **Clearingstelle** ist eine Vermittlungsstelle (Broker), welche zwei oder mehrere Systeme verbindet, um Meldungen (z.B. XML-Dokumente) weiterzuleiten und zu vermitteln, Datenänderungen zu überwachen, zu koordinieren und die Datenkonsistenz zu schützen. Die Clearingstelle arbeitet ohne Interaktion eines Benutzers und wird vielfach in einer DMZ (Demilitarised Zone siehe Anhang C Glossar) betrieben.

Wir unterscheiden zwischen einer aktiven und einer passiven Clearingstelle.

- Die aktive Clearingstelle nimmt Meldungen von Systemen entgegen, entnimmt den Meldungen die Zieldestination und leitet die Meldungen an die entsprechenden Ziel-Systeme weiter.
- Die passive Clearingstelle nimmt Meldungen von Systemen entgegen und wartet, bis diese von den Zielsystemen abgeholt werden. Die passive Clearingstelle wird häufig in Hochsicherheitsbereichen eingesetzt.

Eine Clearingstelle hat generell den Vorteil, dass neue Teilnehmersysteme relativ schnell partizipieren können, weil die Interfaces nur gegen die standardisierte Schnittstelle der Clearingstelle entwickelt werden müssen.

Bemerkung: Anstatt des Begriffs „Clearingstelle“ werden im Bereich Web Services auch die englischen Begriffe „Transaction Manager“ oder „Coordinator“ verwendet. Beispiele für Clearingstelle oder Transaction Manager sind oder könnten sein:

- Sega Intersettle für das Abwickeln des Aktienverkaufs und für die Handänderung der Aktien
- Telekurs AG für den Zahlungsverkehr zwischen den Banken in der Schweiz
- Die Post

5.2 Schnittstellen

Wenn wir davon ausgehen, dass ein Endgerät nicht direkt mit einer Clearingstelle interagiert, ergeben sich drei verschiedene Schnittstellen zwischen den drei Komponenten (vergleiche folgende Abbildung):

- **S1:** Endgerät-System
- **S2:** System-System
- **S3:** System-Clearingstelle

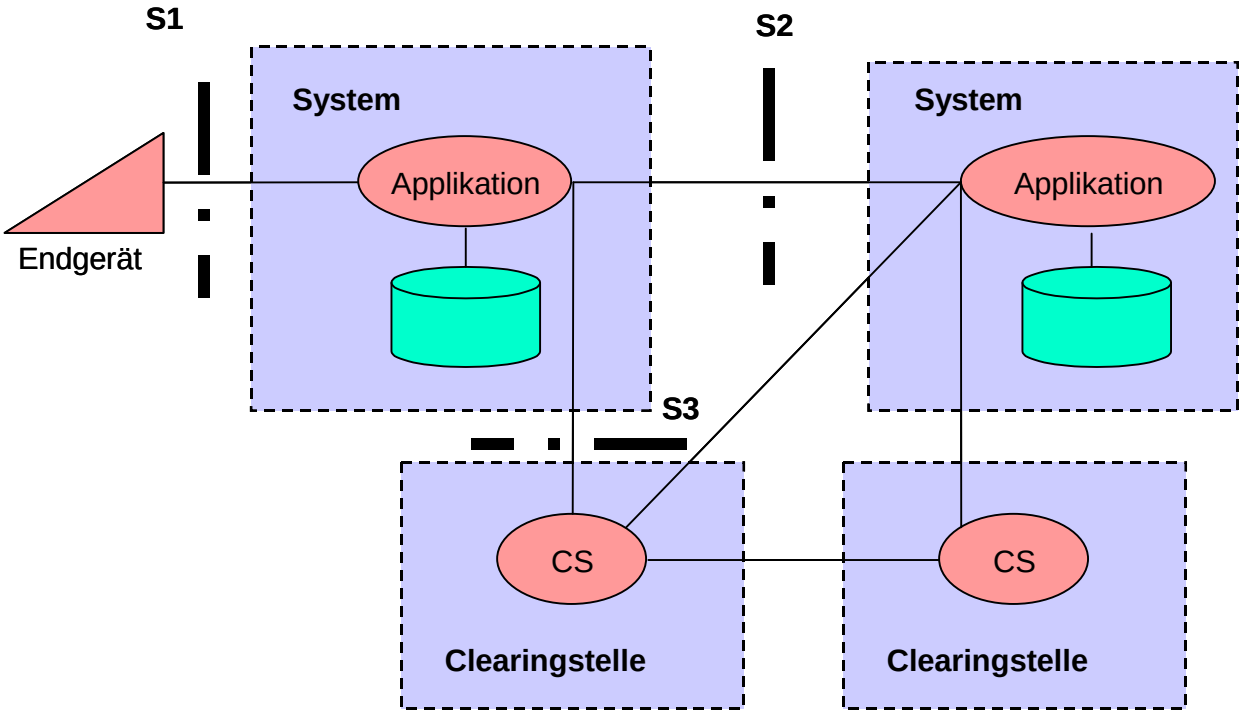

Abbildung 5-1 Schnittstellen

Weiter muss es möglich sein, dass zwischen den jeweiligen Clearingstellen kommuniziert werden kann und Daten ausgetauscht werden können, ähnlich wie bei der Schnittstelle S3.

Wichtig: Die nun folgenden Empfehlungen für die Realisierung von eGovernment Anwendungen beschränken sich vorerst (in dieser Version von SAGA.ch) hauptsächlich auf die Empfehlungen der Technologien, welche die Kommunikation und den Datenaustausch an den hier aufgeführten Schnittstellen S1, S2, S3 ermöglichen sollen. Deshalb werden hauptsächlich nur Datenformate, Kommunikationsprotokolle und Sicherheitsmechanismen empfohlen, welche bei diesen Schnittstellen eingesetzt werden können/sollen. Folglich wird auch in dieser Version von SAGA.ch weiterhin keine Aussage darüber gemacht, wie Datenbanksysteme aufzubauen, zu konfigurieren und abzusichern sind. Deswegen werden auch keine Empfehlungen zu Datenbank-Protokollen wie SQL und Xquery gemacht.

Die Schnittstelle zwischen den Clearingstellen erscheint in der Praxis nur selten und wird folglich in diesem Dokument zurzeit nicht weiter behandelt.

5.3 Abgrenzung

Um die hier vorgenommenen Empfehlungen abzugrenzen und die Zielsetzung des Dokuments besser zu verstehen, wird hier ein Informationsmodell vorgestellt und dabei erläutert, welche Komponenten in diesem Dokument standardisiert werden sollen und welche nicht.

5.3.1 Informationsmodell

Die Informationsbearbeitung in der IT lassen sich schematisch und grob in folgende 4 Kategorien (Schichten, engl. Layer) aufteilen, s. auch [GuA] S. 16.

- Client Plattform. Definiert die Zugangskanäle und Client Plattformen.
- Präsentation. Definiert die Darstellungsformate und Protokolle für den Client
- Middleware und Applikationslogik. Definiert die Funktionalität, welche für die Auslieferung der Inhalte und Formate notwendig sind, welche die Präsentation benötigt.
- Daten, Ressourcemanagement, Datenhaltung oder Persistenzschicht. Definiert die Datenquellen und –haltung, welche von der Applikationslogik benötigt wird.

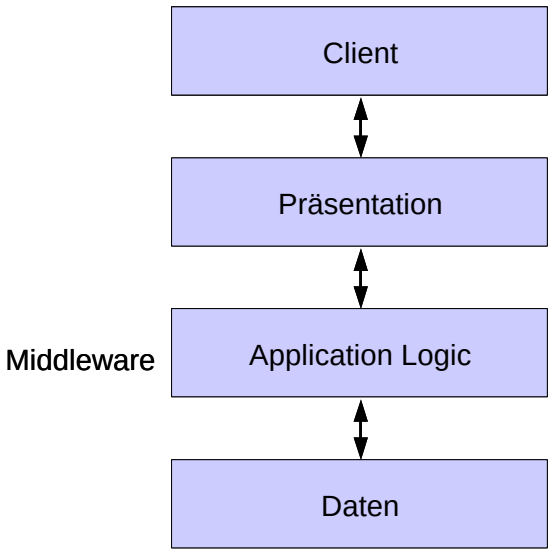

Abbildung 5-2 Informationsbearbeitungsschichten

Dieses Dokument empfiehlt, welche Kommunikationsprotokolle und Dateninhalte/-formate zwischen Client und Präsentation, Präsentation und Application Logic eingesetzt werden sollen. Bewusst werden hier keine Empfehlungen dazu abgegeben, wie die Kommunikation zwischen der Datenschicht und der Applikationslogik vonstatten gehen und welche Datenformate ausgetauscht werden sollen, weil dies unter anderem vom zu Grunde liegenden Betriebssystem und von den eingesetzten Datenbanken und Informationsverwaltungssystemen abhängt.

Etwas vereinfacht ausgedrückt: „Z.B. funktioniert das Internet auch alleine dadurch, dass die Kommunikationsprotokolle und die Dateninhalte definiert werden. Es wird dabei keine Aussage darüber gemacht, welches Betriebssystem oder welche Datenbanken eingesetzt werden soll.“

In der folgenden Abbildung sind die verschiedenen Kommunikationsmöglichkeiten dargestellt, wobei die mit einer gestrichelten („-----„) Linie dargestellten Kommunikationswege nicht Bestandteil dieses Standards sind.

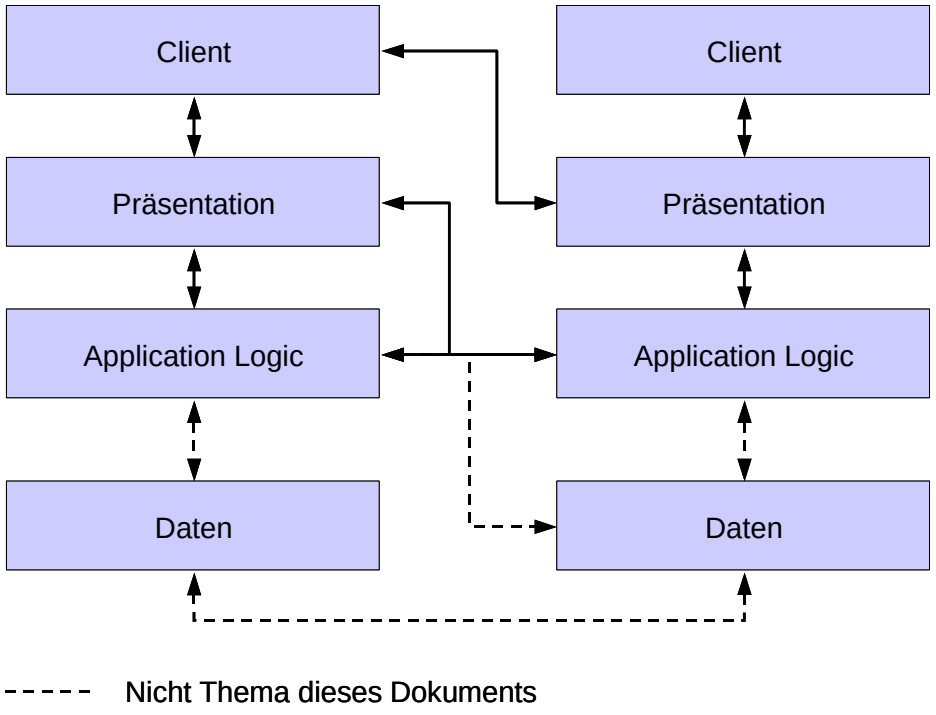

Abbildung 5-3 Mögliche Kommunikationswege

Ausnahme: Im Kapitel 6.6.4 „Directory Server-Protokolle nach X.500“ sind Empfehlungen zur Kommunikation zwischen der Datenschicht gemacht worden; dies aber nur um das Abgleichen der Personendaten und deren Zertifikate zu standardisieren.

5.3.2 Beispiel 3 Tier Architektur

Das vorangehende Informationsbearbeitungsmodell sieht bei einer 3Tier-Architektur wie folgt aus:

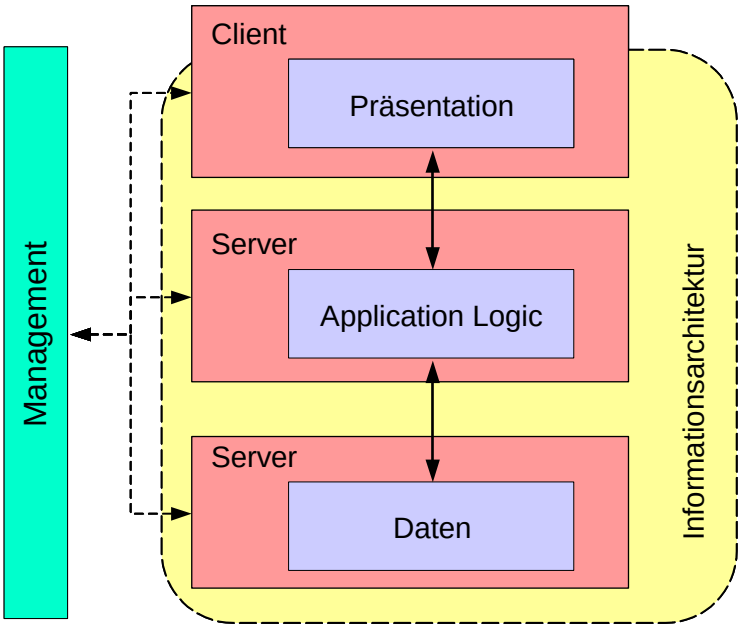

Abbildung 5-4 3Tier Architektur

Anmerkung: Die 3Tier Architektur tritt bei vielen Client Server Applikationen auf. Dabei residiert die Präsentationsschicht auf der Plattform beim Client.

Bei der letzten Abbildung sind noch die Verwaltung(Management)schnittstellen zu den verschiedenen Plattformen und Schichten dargestellt worden. Das Management der einzelnen Komponenten kann nicht einheitlich standardisiert werden, weil die Verwaltung und die Konfiguration der verschiedenen Komponenten bei verschiedenen Behörden, Institutionen oder juristischen und natürlichen Personen vorgenommen werden und zudem von dem zu Grunde liegenden Betriebssystem und von den jeweiligen Sicherheitsanforderungen abhängen. Deshalb werden hier fast keine Empfehlungen zur Managementschnittstelle, resp. zu Managementprotokollen abgegeben.

Die Kommunikation der Managementinformationen kann/sollte/muss abgesichert werden. Da, wie bereits erwähnt, das Management und somit auch die Sicherheit der Komponenten von verschiedenen Institutionen wahrgenommen wird, werden in diesem Bereich keine Empfehlungen zu den Sicherheitsmechanismen und –protokollen, wie z.B. SSH (Secure Shell), abgegeben.

5.3.3 Beispiel Ntier Architektur mit Web-Schnittstelle

In folgender Abbildung ist eine Ntier Architektur dargestellt. Dabei findet der Zugang zur Client Plattform über das HTTP-Protokoll und weitere statt. (Die Zeichnung stammt aus [GuA] und wurde leicht modifiziert.) Diese Architektur oder Aufteilung der Informationsverarbeitung wird u.a. bei Datenbankanfragen über das Web angewandt.

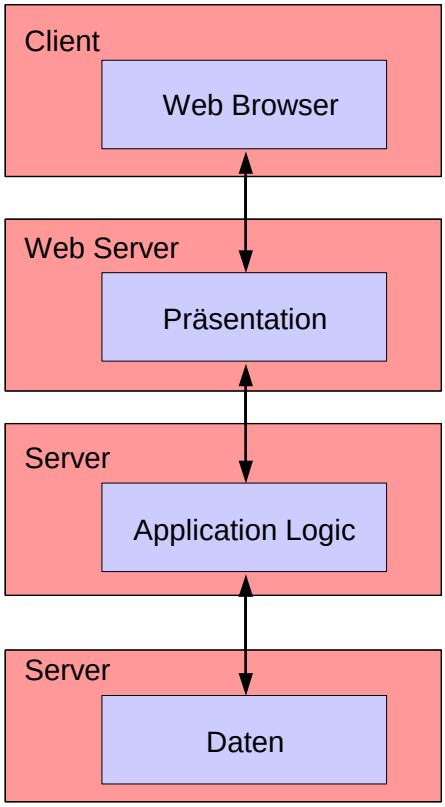

Abbildung 5-5 NTier Architektur

5.3.4 Anmerkung zu Service-Oriented Architecture (SOA)

Service-Oriented Architecture, kurz SOA, bedeutet oder drückt ein Konzept für eine Software Architektur aus, welches die Benutzung von Dienstleistungen definiert. Diese Dienstleistungen sollen die Anforderungen der Benutzer dieser Software erfüllen.

Im SOA Umfeld stellen Knoten in einem Netzwerk Ressourcen anderen Beteiligten in einer standardisierten (definierten) Art und Weise zur Verfügung. Die meisten Definitionen oder Konzepte von SOA beziehen sich auf die Nutzung von Web Services (zum Beispiel SOAP). Jedoch können auch andere auf Service basierende Technologien zur Realisierung von SOA eingesetzt werden.

Die in SAGA aufgeführten Technologien, insbesondere im Kontext von Web Services, erlauben eine Service-Oriented Architecture.

6 Kommunikationsprotokolle

Innerhalb dieses Kapitels wird zwischen folgenden Protokollen unterschieden:

- Netz- und Transportprotokolle, s. Kapitel 6.3 „Netz- und Transport-Protokolle“
- Anwendungsprotokolle, s. Kapitel 6.4 „Anwendungsprotokolle“
- Protokolle für die Mobilkommunikation, s. Kapitel 6.5 „Mobilkommunikation“
- Protokolle für den Zugriff auf Verzeichnisdienste, s. Kapitel 6.6 „Verzeichnisdienste“
- Protokolle oder Datenaustausch im Bereich Middleware, s. Kapitel 6.8 „Web Services (WS)“

Dabei wird angegeben, bei welchen Schnittstellen S1, S2, S3 (s. Kapitel 5.2 „Schnittstellen“) die Kommunikationsprotokolle eingesetzt und die dazu passenden Standards eingehalten werden sollen. Ist die Schnittstelle nicht aufgeführt oder erwähnt, so soll das Protokoll dort nicht unterstützt, resp. eingesetzt werden. Beispiel:

> Beim Protokoll XY wird folgende Angabe gemacht.
>
> **S2 S3**
>
> Das Protokoll XY soll gemäss den dort aufgeführten Empfehlungen bei der Schnittstelle S2 (System-System) und S3 (System-Clearingstelle) eingesetzt werden, aber nicht an der Schnittstelle S1 (Endgerät-System).

Die hier aufgeführten Definitionen sind in Anlehnung an die IETF (www.ietf.org) bzw. an die W3C (www.w3C.org) und weiteren vorgenommen worden. Spezifische Profile für die jeweiligen Protokolle oder Anwendungen sind unter Umständen noch zusätzlich zu erstellen und zu verabschieden.

6.1 Bemerkung zur Sicherheit

Viele der in diesem Kapitel aufgeführten Protokolle besitzen keine Sicherheitsmassnahmen. Werden sensitive Daten mit diesen Protokollen ausgetauscht, dann sollten zusätzlich die entsprechenden Sicherheitsmassnahmen und -technologien, welche im Kapitel 8 aufgeführt sind, eingesetzt werden.

6.2 Link Layer Protokolle

Die Link Layer Protokolle (Schicht 1/2 des Internetmodells) sind nicht Thema dieses Dokuments, weil die Netzwerkanbindungen der einzelnen Systeme in die Verwaltung der jeweiligen Institutionen und Telecomunternehmen (gemeint sind z.B. die WAN/LAN Industriestandards u.a. IEEE 802.X) fallen. Deshalb werden hierzu keine Empfehlungen abgegeben.

6.3 Netz- und Transport-Protokolle

Informationen zu den jeweiligen Netz-, Transportprotokollen und zu gewissen Anwendungsprotokollen findet der Leser bei [Hem].

6.3.1 Internet Protocol Stack

Der Internet Protocol Stack impliziert IP, TCP und UDP sowie die auf TCP bzw. UDP basierenden Anwendungsprotokolle.

S1	S2	S3	
Internet Protocol Stack gemäss IETF Standards			Dringend empfohlen

Tutorial: RFC 1180 TCP/IP

6.3.2 IPv6

Neue Netze, Netzmigrationen und Netzerweiterungen sollen mit IPv6 realisiert werden.

S1	S2	S3	
IPv6			Dringend empfohlen

Standards: RFC 2460 und zugehörige RFC 4294, RFC 5095 und weitere relevante.

6.3.3 IPv4

Aktuell wird im Umfeld IPv4 in Verbindung mit TCP (Transmission Control Protocol), und UDP (User Datagram Protocol) verwendet.

S1	S2	S3	
IPv4			Empfohlen

Standards: IPv4 (RFC 791, RFC 3232 und zugehörige), TCP RFC 793, UDP RFC 768

6.4 Anwendungsprotokolle

Anwendungsprotokolle, auch Applikationsprotokolle genannt, sind Protokolle, welche auf der Ebene 4 des Internetmodells (IETF) ausgetauscht werden.

6.4.1 File Transfer Protocol, FTP

Für die Dateiübertragung wurde früher ungesichertes FTP (Port 21) verwendet. Grundsätzlich sind keine Passworte unverschlüsselt zu übertragen. Um die Verschlüsselung und Authentifizierung zu nutzen, kann Transport Layer Security eingesetzt werden (FTP über SSL, kurz FTPS; zu SSL oder TLS gemäss Kapitel 8.8.1 SSL/TLS), oder FTP kann über SSH (Secure File Transfer Protocol) getunnelt werden (sFTP zu SSH gemäss Kapitel 0).

S1	S2	S3	
File Transfer Protocol (sFTP Port 22)			Empfohlen

Standards: RFC 2228, RFC 2428, RFC 2640 , RFC 3659, RFC 5797

Anmerkung: Alternativ kann u.a. auch Kapitel 6.4.2 HTTP oder Kapitel 6.4.8 WebDAV verwendet werden.

6.4.2 Hyper Text Transfer Protocol, HTTP

Für die Web-Kommunikation muss HTTP (mit Port 80 bzw. HTTPS mit Port 443) eingesetzt werden. Beim Einsatz von HTTP Session Management und Cookies soll der entsprechende Standard HTTP State Management Mechanism (RFC 2965) befolgt werden.

S1	S2	S3	
Hyper Text Transfer Protocol (HTTP v.1.1)			Dringend empfohlen

Standards: HTTP RFC 1945 bzw. RFC 2616, RFC 2965, RFC 5785 mit TLS

Anmerkung: Die Sicherung des HTTP-Protokolls über SSL oder TLS wird auch als HTTPS bezeichnet. Zu SSL oder TLS gemäss Kapitel 8.8.1 SSL/TLS. Die Sicherung des HTTP-Protokolls über S-HTTP (RFC 2660) wird aber nicht empfohlen, s. Kapitel 8.8.7 Secure HTTP.

6.4.3 Simple Mail Transfer Protocol und Format, SMTP

Für den E-Mail-Transport werden E-Mail-Protokolle vorausgesetzt, welche den Spezifikationen von SMTP und MIME für den Nachrichtenaustausch entsprechen. 1995 wurde das Protokoll erweitert zu ESMTP. E-Mail-Anhänge sollen dabei den Dateiformaten entsprechen, die von SAGA.ch vorgegeben werden.

S1	S2	S3	
Simple Mail Transfer Protocol / Format (SMTP mit Port 25 und MIME)			Dringend empfohlen

Standards: RFC 2822, RFC 2046, RFC 2049, RFC 2231, RFC 4288, RFC 4289, RFC 5321, RFC 5322

6.4.4 Mail-Zugangsprotokolle

Es kann vorkommen, dass elektronische Postfächer angeboten werden. Dazu sollen POP3, IMAP4 oder HTTP als Zugang zu E-Mails standardmässig eingesetzt werden. Die Authentifizierung zum Mailserver muss über einen gesicherten Kanal erfolgen.

S1			
POP3, IMAP4, HTTP für E-Mail			Dringend empfohlen

Standards: POP3 RFC 1939 aktualisiert durch RFC1957, RFC2449, IMAP4 RFC 2061, HTTP für E-Mail RFC 1945 v.1.0 und RFC 2616 v.1.1 und 2817

6.4.5 Telnet

Telnet soll durch eine bedienerfreundlichere, auf Web basierte, interaktive Bedienerführung ersetzt werden.

Telnet			Nicht empfohlen

6.4.6 Remote Procedure Call (RPC)

RPC dient unter anderem dem Aufruf von Befehlen auf einem entfernten Rechner.

	S2	S3
Remote Procedure Call (RPC) mit dynamischen Ports		Nicht empfohlen

	S2	S3
Authentisierte Remote Procedure Call (RPC) mit fixen Ports		Empfohlen

Standards: RFC 1050, RFC 1831

6.4.7 Terminal Service und Thin Client-Protokolle

Ein Einsatz von Terminal Service und Thin Client Protokollen ist, wenn überhaupt, nur an der Schnittstelle S1 möglich. Terminal Service und Thin Client Protokolle setzen aber voraus, dass die beiden Systeme an den Schnittstellen S1 von der gleichen Institution konfiguriert, verwaltet und gesichert werden. Der Einsatz von Terminal Service und Thin Client Protokollen wird deshalb nicht empfohlen.

	S1	S2	S3
Terminal Service und Thin Client Protokolle			Nicht empfohlen

Es wird durchaus der Fall sein, dass Thin Client und Terminal Service Protokolle innerhalb einer Organisation eingesetzt werden. Doch die Client Funktionalität an der linken Seite der Schnittstelle S1 wird dann vom Terminal Server wahrgenommen.

6.4.8 WebDAV

Das Web Distributed Authoring and Versioning (WebDAV) Protokoll ist im ursprünglichen RFC 2518 definiert und erweitert das HTTP/1.1-Protokoll gemäss RFC 2616. Dieses Protokoll erlaubt zusätzlich Methoden und Möglichkeiten, Inhalte oder Dokumente auf dem (WebDAV) Server zu publizieren, zu manipulieren, zu „locken“ oder nach erweiterten Attributen zu suchen.

	S1	S2	S3
WebDAV			Empfohlen

Standard: RFC 3744, 4918

6.5 Mobilkommunikation

Falls einmal Dienste via Mobilephone (Handy) angeboten würden, dann sollte der Austausch der Informationen mit dem Wireless Access Protocol (WAP) erfolgen. WAP wurde früher vom WAP Forum (www.wapforum.org) und wird heute von deren Nachfolgeorganisation Open Mobile Alliance (www.openmobilealliance.org), kurz OMA, standardisiert.

	S1
Wireless Access Protocol	Unter Beobachtung

Standards: Zu den Protokollen und anverwandten Diensten rund um WAP sind eine Reihe von Standards geschrieben worden, wie das Wireless Application Protocol Architecture (s. auch Anhang A „Referenzen & Bibliography“). Bei den Standards, welche von der OMA erarbeitet und publiziert worden sind, wird unter anderem auch festgehalten, wie XML-Dokumente über WAP transportiert werden können.

6.6 Verzeichnisdienste

6.6.1 LDAPv.3

LDAPv.3 (Lightweight Directory Access Protocol) ist ein auf hierarchisch geordnete Informationen optimiertes Protokoll des Internets, das für den Zugriff auf X.500 oder auf ähnliche Verzeichnisdienste verwendet wird. Frühere Versionen werden nicht empfohlen.

	S1	S2	S3
LDAPv.3			Dringend empfohlen

Standards: RFC 4511 und zugehörige RFC 4510

6.6.2 LDAP Replication

Hier wird eine Methode vorgeschlagen, wie LDAP Directories untereinander die Daten replizieren können.

	S2	S3
LDAP (Version 3) Replication Requirements		Unter Beobachtung

Standard: RFC 3384

6.6.3 DSML

Directory Services Markup Language (DSML) ist ein Standard von OASIS (www.oasis-open.org), wie Informationen über ein Verzeichnis (Directory) im XML-Format ausgedrückt werden können. Version 2 des Standards definiert, wie Anfragen an ein Directory oder wie Änderungen in einem Directory vorgenommen werden können, wobei die Befehle auf XML basieren.

	S1	S2	S3
Directory Services Markup Language (DSMLv.2.0)			Empfohlen

Standard: Directory Services Markup Language (DSML) v.2.0, January 2002, von OASIS (www.oasis-open.org).

6.6.4 Directory Server-Protokolle nach X.500

Folgende Directory-Protokolle zur Replikation, zur Anfrage von Daten und zum Abgleich der Daten gibt es gemäss dem Standard X.519:

- DSP Directory System Protocol
- DISP Directory Information Shadowing Protocol
- DOP Directory Operation Binding Management Protocol

	S2	S3
Directory Server-Protokolle nach X.500		Empfohlen

Standards: X.519, X520 Selected Attribute Types ,X521 Selected Object Classes und weitere zugehörige von der ITU (www.itu.org)

6.6.5 OCSP

Das Online Certificate Status Protocol (OCSP) ermöglicht, den aktuellen Status eines Zertifikats zu ermitteln, ohne auf eine CRL zuzugreifen. OCSP setzt auf HTTP auf.

	S1	S2	S3
Online Certificate Status Protocol (OCSP)			Empfohlen

Standard: RFC 2560

Bemerkung: Inwieweit OCSP dringend empfohlen oder nur empfohlen ist, sollte auch noch im Rahmen der PKI Anbindung untersucht werden.

6.7 Protokolle für Realtime Informationsaustausch

6.7.1 SIP

Das Session Initiation Protocol (SIP) für Voice über IP ist von der IETF standardisiert worden und umfasst mehrere RFC Standards und Best Practices.

S1	S2	S3

Session Initiation Protocol (SIP)	Empfohlen

Standard: Der Grundstandard RFC 3261 (und RFC 3265, RFC 3853, RFC 4320, RFC 4916, RFC 5367, RFC 5727, RFC 5393, RFC 5621, RFC 5626, RFC 5630, RFC 5922, RFC 5994, RFC 6026) ist in durch die in der Klammer erwähnten Standards erweitert und aktualisiert worden.

6.7.2 H.323 Protokollfamilie

Die H.323 Protokollfamilie ist von der ITU für Voice über IP entwickelt worden.

S1	S2	S3

H.323 Protokollfamilie	Empfohlen

Standard: H.323 ist ein ITU Standard zu Voice über IP. Doch weitere technische Aspekte sind in verschiedenen weiteren Standards aktualisiert worden, wie H.224, 225, 245, 246, 281, 283, 325, 328, 341oder H.450/460/500 Serien.

6.7.3 Skype

Skype ist ein proprietäres Voice über IP (Internet Telefonie) Protokoll, welches bisher noch nicht standardisiert worden ist.

S1	S2	S3

Skype	Nicht empfohlen

Standard: Kein Standard, proprietär

6.8 Web Services (WS)

6.8.1 Definition

Die Standardisierungsorganisationen in diesem Bereich (etwa OASIS, WS-I, W3C) und deren Mitglieder verwenden verschiedene Definitionen zum Begriff „Web Services“, s. auch [GuA]. Für uns gilt folgende Definition gemäss W3C[4]:

> Web Services ist ein System bestehend aus mehreren einzelnen Diensten im Netzwerk. Diese Dienste sind lose gekoppelt, erweiterbar und interoperabel. Die Schnittstellen und Funktionalitäten der Dienste sind in einem maschinenlesbaren Format definiert (Web Services Definition Language). Die Maschinen kommunizieren mittels Botschaften in der Regel im XML-Formaten untereinander.

6.8.2 Abhängigkeiten

Folgende Abbildung[5] fasst die Abhängigkeiten zwischen SOAP, WSDL, UDDI zusammen:

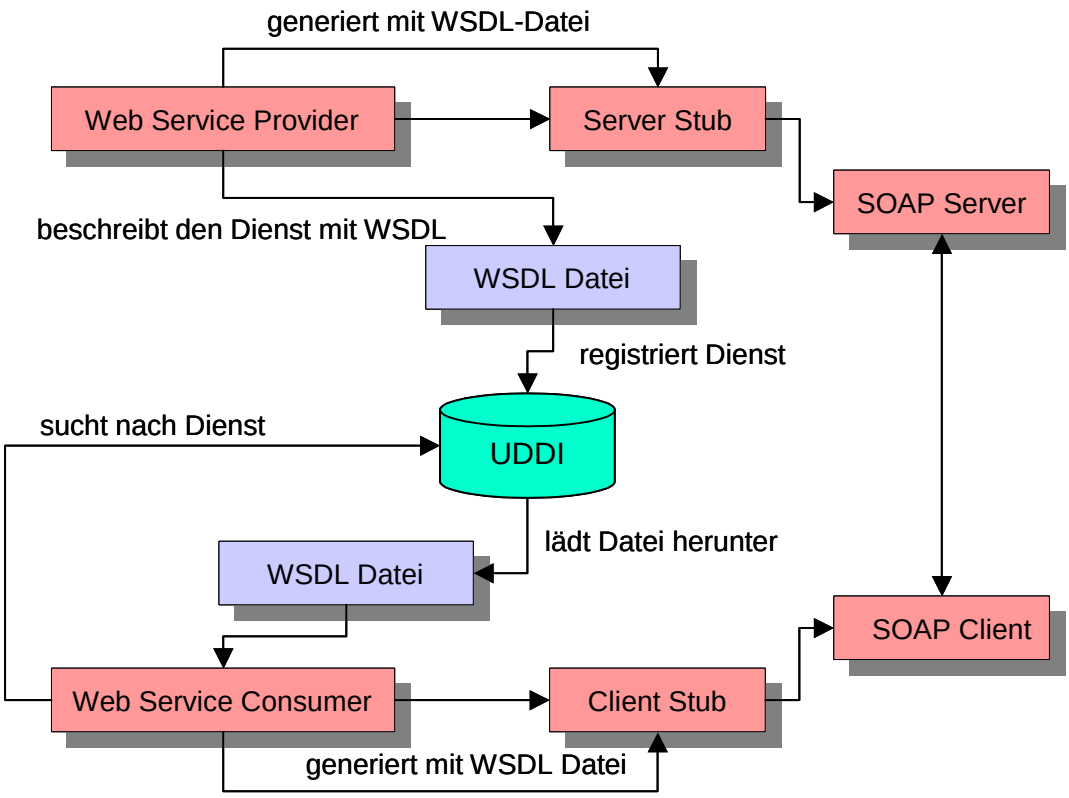

Abbildung 6-1 Abhängigkeiten bei Web Services

[4] Nicht wörtliche Übersetzung aus dem Web Services Glossary: http://www.w3.org/TR/ws-gloss/ .

[5] Die Informationen und die folgenden Zeichnungen stammen unter anderem aus [GuA]. Der an Web Services interessierte, aber darin nicht bewanderte Leser möge dieses Buch konsultieren, der technisch versierte Leser mit XML-Grundkenntnissen auch noch [ZoT].

6.8.3 Web Services Architektur

Die Architektur der Web Services lässt sich schematisch wie folgt darstellen:

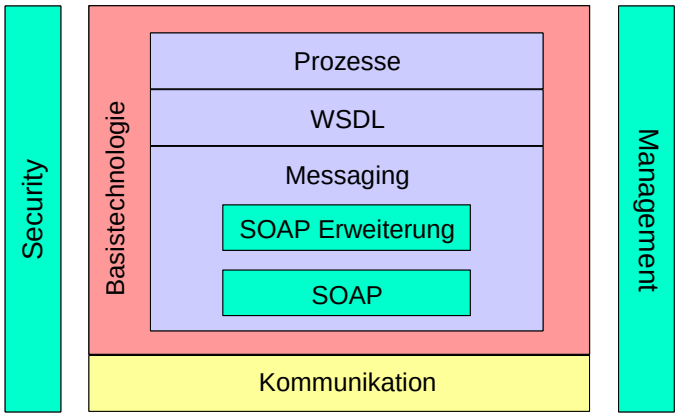

Abbildung 6-2 Architekturmodell Web Services

Die Sicherheit (Security) ist ein integraler Bestandteil über alle die hier aufgeführten Bereiche. Aspekte wie die geschützte Kommunikation, das gesicherte Messaging, authentisierte WSDL-Dokumente und verlässliche Prozesse oder Transaktionen sind in den nachfolgende Spezifikationen und im Kapitel 8 „Sicherheit“ aufgeführt.

6.8.4 SOAP

SOAP ist ein Protokoll und Meldungsformat. Das Meldungsformat selber ist eine XML-Anwendung und besitzt folgende 3 Komponenten: Die Hülle (engl. Envelope), bestehend aus Kopf (engl. Header; hier können zusätzliche Informationen über den Prozessablauf und die Kontrolle des Protokollablaufs enthalten sein, sowie Angaben zur Authentisierung oder der Dienstqualität) und dem Rumpf (engl. Body) – der eigentlichen Meldung.

SOAP wiederum setzt auf einem TCP Anwendungsprotokoll auf (z.B. HTTP, SMTP, usw.):

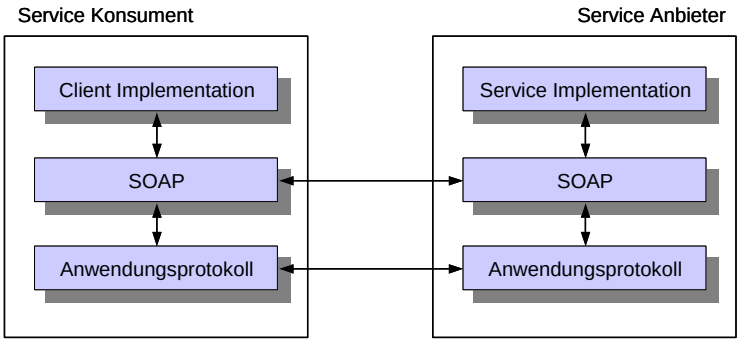

Abbildung 6-3 Protokollstack der SOAP-Meldungen

S1 S2 S3

SOAP v.1.2	Dringend empfohlen

Standard: SOAP v.1.2, June 2003, von W3C (www.w3C.org)

SOAP v.1.1	Empfohlen

6.8.5 Message Transmission Optimization Mechanism (MTOM)

MTOM ist ein vom W3C bereitgestellter Standard, um bei einer SOAP-Meldung binäre Daten zu transportieren. Dabei werden die binären Daten nicht als Text codiert und in die SOAP-Meldung eingebettet, sondern sie werden gemäss dem Standard „*XML-binary Optimized Packaging (XOP)*“ verpackt, zusammen mit der SOAP-Meldung. Die verpackte SOAP-Meldung wird mit Verweisen versehen, welche auf die Teile mit den verpackten binären Daten zeigen.

S1 S2 S3

Message Transmission Optimization Mechanism (MTOM)	Empfohlen

Standard: MTOM, W3C Recommendation, 25 January 2005, von W3C (www.w3c.org), XOP, W3C Recommendation, 25 January 2005, von W3C (www.w3c.org).

6.8.6 Web Service Description Language (WSDL)

Web Services werden mit Web Service Description Language (WSDL) beschrieben. WSDL ist eine auf XML basierende Sprache (XML Schema) und definiert unter anderem die Kommunikationsendpunkte und die auszutauschenden Nachrichten (Messages). Zum Austausch der Nachrichten ist kein spezielles Anwendungsprotokoll festgelegt. Doch können in der aktuellen Version lediglich für SOAP v.1.1 das Anwendungsprotokoll HTTP oder der Container MIME verwendet werden.

S1 S2 S3

Web Service Description Language (WSDL v.1.1)	Dringend empfohlen

Standard: WSDL Web Services Description Language v.1.1, 15 March 2001 von W3C (www.w3C.org)

Web Service Description Language (WSDL v.2.0)	Unter Beobachtung

Standard: WSDL Web Services Description Language Version 2.0 Part 1: Core Language, W3C Recommendation 26 June 2007 von W3C und weitere, (www.w3C.org)

6.8.7 WS-Addressing

WS-Addressing erlaubt es Webservices, Adressinformationen auszutauschen und erleichtert die Verwendung asynchroner Webserviceaufrufe, indem jede SOAP-Nachricht in ihrem Header zusätzliche Metainformationen über den Absender und den Empfänger der Antwort sowie den Empfänger von Fehlermeldungen enthält.

S1 S2 S3

Web Services Addressing (v.1.0)	Dringend empfohlen

Standard: Web Services Addressing (Core, SOAP Binding, Metadata) v.1.0, May 2006 / Sept. 2007 von W3C (www.w3C.org)

6.8.8 Universal Description, Discovery and Integration (UDDI)

Universal Description, Discovery and Integration (UDDI) standardisiert die Publikation der Dienste im Bereich Web Services.

S1	S2	S3

Universal Description, Discovery and Integration (UDDI v.2)	Empfohlen

Standard: Universal Description, Discovery and Integration (UDDI) v.2.0, February 2003 von OASIS (www.oasis-open.org)

6.8.9 Transaktionsprotokolle

SOAP alleine genügt nicht, damit komplexe Geschäftsprozesse abgewickelt werden können. Deshalb sind folgende Transaktionsprotokolle bereits konzipiert und spezifiziert worden:

- Web Services Reliable Messaging
- Web Services Coordination
- Web Services Atomic Transactions
- Business Activity
- OSCI Transport

6.8.9.1 WS Reliable Messaging

WS Reliable Messaging wurde zum zuverlässigen Austausch von Meldungen komzipiert.

S1	S2	S3

WS-Reliable Messaging V1.1 + Errata	Empfohlen

Standard: OASIS, Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.1, 7.Januar 2008, Standard

WS-Reliable Messaging V1.2	Unter Beobachtung

Standard: OASIS, Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.2, 28. Februar 2008

6.8.9.2 WS Coordination

WS Coordination wurde von OASIS (www.oasis-open.org) konzipiert und definiert ein gemeinsames Framework für die Koordination verteilter Aktivitäten. Die Standards WS-AtomicTransaction und WS-BusinessActivity bauen auf diesem Framework auf.

S1	S2	S3

WS-Coordination V1.1 + Errata	Empfohlen

Standard: OASIS, Web Services Coordination (WS-Coordination) Version 1.1.

6.8.9.3 WS Atomic Transaction

WS-Atomic Transaction setzt auf dem WS Coordination Protocol auf und ist vor allem für kurzzeitige Transaktionen gemeinsam von IBM, Microsoft und Bea Systems (www.bea.com) konzipiert und spezifiziert worden. Dabei werden 3 verschiedene Möglichkeiten spezifiziert, wie eine konsistente kurzlebige Transaktion ablaufen kann. WS Atomic Transaction ist zurzeit bei OASIS (www.oasis-open.org) in der Vernehmlassung.

S1	S2	S3

WS-Transaction V1.1 + Errata	Empfohlen

Standard: OASIS, Web Services Transaction (WS-Transaction) Version 1.1.

6.8.9.4 WS Business Activity

Die Web Services Business Activity (WS Business Activity) wurde von OASIS (www.oasis-open.org) konzipiert und setzt auf dem WS Coordination Protocol auf. Die Entwickler können dieses Protokoll nutzen, wenn sie Web Service Applikationen bauen, welche konsistente Vereinbarungen enthalten und während langer Zeit über verteilte Systeme ablaufen sollen.

S1	S2	S3

WS-BusinessActivity 1.1 + Errata	Empfohlen

Standard: OASIS, Web Services Business Activity (WS-BusinessActivity) Version 1.1 + Errata, 12. Juli 2007

6.8.9.5 OSCI-Transport

Online Service Computer Interface (OSCI) umfasst eine Menge von Protokollen, welche für die Anforderungen im eGovernment geeignet sind und durch die OSCI-Leitstelle erstellt werden. Zielsetzung ist dabei die Unterstützung von Transaktionen in Form von Web Services und von deren vollständigen Abwicklung. Sedex verwendet OSCI.

S1	S2	S3

OSCI-Transport V.1.2/2	Empfohlen

Standard: OSCI wurde in Deutschland im Rahmen des Wettbewerbs MEDIA@Komm entworfen.

6.8.9.6 Sedex

Der Bund stellt im Rahmen der Harmonisierung der Personenregister des Bundes und der kantonalen bzw. kommunalen Einwohnerregister seit Anfang 2008 eine Plattform für den sicheren Datenaustausch zwischen den Teilnehmern zur Verfügung: genannt Sedex (steht für: Secure Data Exchange).

Die Kommunikation erfolgt asynchron, erlaubt aber im Gegensatz zu herkömmlichen Mailing Systemen den Austausch sehr grosser und vieler gleichzeitiger Meldungen.

Sedex kann für weitere Bereiche genutzt werden, wobei primär e-Government Anwendungen im Fokus stehen. Für den Anschluss an Sedex ist ein Adapter in die partizipierende An-

wendung zu integrieren, und die geforderten Sicherheitsforderungen müssen erfüllt werden (Authentifizierung des Teilnehmers, ggf. Zertifizierung der Anwendung).

Ab Version 2.0 enthält der Sedex Adapter auch einen Webservice-Proxy, welcher die Authentifizierung eines Sedex Teilnehmers gegenüber Webservices aufgrund des Organisationszertifikates vornimmt, wodurch für die Webservices die Benutzerverwaltung entfällt.

S1	S2	S3

Sedex (Secure Data Exchange)	Empfohlen

Standards: Sedex , V.2.x , 2007–2010

Spezifikationen : http://www.bfs.admin.ch/bfs/portal/de/index/news/00/00/12/01.html

6.8.10 Web Services Resource Framework (WSRF)

WSRF ist eine Familie von Web Service-Standards zwecks der Erweiterung des im Grunde zustandslosen Kommunikationsmodells der Web Services zum zustandsbehafteten Kommunikationsmodell. Den Kommunikationspartnern wird in einer Session ein Konversationszustand in Form von Ressourcen zugeordnet. Die Ressourcen und ihre Eigenschaften (Lebenszyklus, Fehlerbehandlung, Gruppenzugehörigkeit), werden von einem speziellen Web Service zur Verfügung gestellt und verwaltet. Ein Web Service-Client schickt dem Web Service-Provider eine Meldung und referenziert dabei eine Ressource mittels einem URI.

S1	S2	S3

WS-Resource Framework V.1.2	Unter Beobachtung

Standard: Web Services Resource 1.2 (WS-Resource), OASIS (www.oasis-open.org), 1 April 2006; Web Services Resource Properties 1.2 (WS-ResourceProperties), OASIS (www.oasis-open.org), 1 April 2006; Web Services Resource Lifetime 1.2 (WS-ResourceLifetime), OASIS (www.oasis-open.org), 1 April 2006; Web Services Service Group 1.2 (WS-ServiceGroup), OASIS (www.oasis-open.org), 1 April 2006; Web Services Base Faults 1.2 (WS-BaseFaults), OASIS (www.oasis-open.org), April 1 2006.

6.9 REST bzw. RESTful HTTP

REST steht für den englischen Ausdruck "Representational State Transfer" und bezeichnet einen Architekturstil für verteilte Systeme, der direkt auf HTTP basiert, wobei die Verwendung eines komplexen Webservice Protokoll Stacks vermieden wird. Wesentliche Status-Informationen werden dabei in dynamischen URIs ausgedrückt.

S1	S2	S3

Representational State Transfer (REST bzw. RESTful HTTP)	Empfohlen

Standard: IETF RFC 2616 (HTTP)

6.10 Service Provisioning Markup Language (SPML)

«Provisioning» ist die Automatisierung aller erforderlichen Schritte für die Verwaltung (Einrichtung, Änderung und Widerruf) von Daten und Zugangsberechtigungen der Benutzer oder anderer Systeme in Bezug auf elektronisch veröffentlichte Dienste («Services»). Verwaltung und Austausch von Authorisierungsdaten erfolgen über SAML (s. Kapitel 8.8.10.3).

S1	S2	S3

Service Provisioning Markup Language V.2.0	Unter Beobachtung

Standard: Service Provisioning Markup Language (SPML), v.2.0, April 2006 von OASIS (http://www.oasis-open.org)

6.11 ebXML

Zu Electronic Business XML (ebXML) ist eine Serie von Standards vorhanden, welche von der OASIS (www.oasis-open.org) und von UN/CEFACT gemeinsam hergestellt worden sind, darunter auch ein Transaktionsprotokoll CPPA (Collaborative Partner Profile Agreement). Das Ziel der verschiedenen Standards ist es, eine Infrastruktur zu normieren, welche den globalen Nutzen von Electronic Business und deren Interoperabilität ermöglichen soll.

Dabei sind verschiedene Standards näher spezifiziert und standardisiert worden.

S1	S2	S3

electronic business using XML (ebXML)	Unter Beobachtung

Es sind auch verschiedene Standards ebXML Security erarbeitet worden bzw. sind noch in Arbeit. Welchen Stellenwert diese Sicherheitsstandards im Rahmen von ***eCH*** in Zukunft haben werden, hängt davon ab:

- Wie sich ebXML entwickelt.
- Wie sicher und sinnvoll und/oder verbreitet die Standards sind.

ebXML Security	Unter Beobachtung

Standards: Die Standards zu ebXML können bei der OASIS (www.oasis-open.org) bezogen werden.

6.12 Business Process Beschreibungssprachen

Ein Business Prozess kann aus verschiedenen Diensten bestehen, und die dabei vorgenommenen Transaktionen können komplex sein. Deswegen muss es Modelle geben, wie Dienste dargestellt werden sollen, so dass sie allgemein verstanden werden. Es gibt verschiedene Formen, wie der Ablauf des Prozesses zusammengestellt werden kann, u.a. folgende zwei Modelle[6]:

- Kompositionsmodell (engl. composition model). Hier werden die Charaktere der einzelnen Elemente definiert, aus welchen der Business Prozess und die Transaktion besteht.
- Orchestration model (zu Deutsch Orchestrierungsmodell). Hier wird die Abstraktion und Sprache definiert, welche dazu benötigt wird, den Ablauf der im Business Prozess involvierten Dienste zu beschreiben.

6.12.1 BPEL

Business Process Execution Language (BPEL) ist eine XML basierte Sprache zur Beschreibung, Modellierung und “Komposition“ von Geschäftsprozessen auf der Basis von Webservices.

BPEL ist mit WSDL abgestimmt.

Business Process Execution Language (BPEL) v.1.1	Empfohlen

Standard: Business Process Execution Language for Web Service (BPEL 4WS) v.1.1, December 2003 von OASIS (www.oasis-open.org)

6.12.2 BPMN

Business Process Model and Notation (BPMN) ist ein offener Beschreibungsstandard und eignet sich zur grafischen Darstellung (Notation) sowohl von internen als auch organisationsübergreifenden Prozessen. BPMN enthält ein umfangreiches Set an grafischen Symbolen.

Business Process Modeling Notation (BPMN)	Empfohlen

Standard: BPMN Version 2.0 gemäss eCH0140, siehe auch Object Management Group (www.omg.org; www.bpmn.org)

6.12.3 UML

Unified Modeling Language (UML) ist eine Sprache oder eine Darstellungsweise, wie der Prozess gemäss dem orchestration model beschrieben werden kann. Dabei werden die möglichen Zustände im Ablauf mittels Blockdiagrammen (engl. state charts) beschrieben und angegeben, ob und wie die einzelnen Zustände in andere übergehen können.

Unified Modeling Language (UML) v.1.5	Empfohlen

[6] Weitere Modelle sind bei [GuA] aufgelistet.

Unified Modeling Language (UML) v. 2.0	Empfohlen

Standard: Unified Modeling Language von Object Management Group (www.omg.org). Im Zweifelsfalle soll v.2.0 eingesetzt werden

6.12.4 XPDL

XML Process Definition Language (XPDL) ist eine XML-Anwendung zur Definition von Prozessen und Workflows. Der Standard zu XPDL wurde von der Workflow Management Coalition (WFMC, www.wfmc.org) definiert.

XML Process Definition Language (XPDL) v.2.X	Unter Beobachtung

Standard: XML Process Definition Language (XPDL) von WFMC (www.wfmc.org)

6.13 CORBA

CORBA steht für Common Object Request Broker Architecture und ist, wie Web Services, eine Middleware Plattform.

CORBA	Nicht Empfohlen

CORBA und dessen Protokolle (IIOP) haben den Status nicht empfohlen erhalten, weil:

- Das dabei verwendete IIOP-Protokoll (Internet Inter-ORB Protocol) bezüglich Sicherheit zu problematisch ist, weil der Server unter anderem ein Call Back zum Client aufbaut (s. dazu [ZeCs]) und die Portnummer des TCP-Protokolls je nach Anwendung dynamisch zugeteilt werden.
- Web Services standardisierte Datenformate und –inhalte verwendet und besonders für die Middleware Kommunikation zwischen verschiedenen Organisationen geeignet ist.
- Wir glauben, dass Web Services in Zukunft mehr eingesetzt und von mehr führenden SW Unternehmen unterstützt und angeboten werden wird.
- Zwei Middleware Architekturen aufzubauen, zu warten und abzugleichen zu kostspielig ist.

7 Datei- und Datenbeschreibungsformate

In diesem Kapitel „Datei- und Datenbeschreibungsformate“ werden die für den Datenaustausch zu verwendenden Datei- und Datenbeschreibungsformate definiert. Dabei wird in einer Tabelle angegeben, an welcher Schnittstelle S1, S2, S3 die entsprechenden Formate eingesetzt werden sollen. (Zur Definition von S1, S2, S3 s. Kapitel 5.2 „Schnittstellen“, Seite 22.) Beispiel:

> Beim Dateiformat XZ wird folgende Angabe gemacht.
>
> **S1 S3**
>
> Das Dateiformat XZ soll gemäss den dort gemachten Empfehlungen bei der Schnittstelle S1 (Endgerät-System) und S3 (System-Clearingstelle) eingesetzt werden, aber nicht an der Schnittstelle S2 (System-System).

In diesem Kapitel wird zwischen folgenden Datei- und Dateibeschreibungsformaten unterschieden:

- Dokumente und zugehörige Dokumentbeschreibungen, s. Kapitel 7.1
- Bilder und Grafiken (in Dokumenten), Kapitel 7.3
- Mulimedia, s. Kapitel 7.4
- Sonstige, s. Kapitel 7.4.7 und weitere

7.1 Bemerkung zur Sicherheit

Viele der in diesem Kapitel aufgeführten Dateiformate besitzen meist keine Sicherheitsmassnahmen. Werden sensitive Daten mit diesen Datenformaten ausgetauscht, dann sollten zusätzlich die entsprechenden Sicherheitsmassnahmen und -technologien, welche im Kapitel 8 aufgeführt sind, eingesetzt werden.

7.2 Dokumente und zugehörige Dokumentbeschreibungen

7.2.1 Zeichensätze und Kodierung

Zeichenkodierung: Um die Kompatibilität und Interoperabilität von Applikationen und Dokumenten zu erhöhen, müssen die Informationen zu den verwendeten Zeichensätzen an den geeigneten Stellen vermerkt werden, damit sie von jeder Software korrekt gelesen werden können.

Wir empfehlen, generell das Unicode-Format UTF-8 zu verwenden und auch Sonderzeichen damit abzubilden. Wenn dies Probleme bereitet oder nicht unterstützt wird, so sollte stattdessen der Zeichensatz ISO-8859-**15** (so in: Art. 80 der Zivilstandsverordnung) verwendet werden, da dieser im Gegensatz zu ISO-8859-**1** auch das €-Zeichen und die Sonderzeichen des Französischen korrekt abdeckt.

S1 S2 S3

UTF-8 (8-bit UCS Transformation Format)	Dringend empfohlen

Standards (gleichwertig): RFC 3629 / STD 63 (2003); The Unicode Standard, Version 4.0, §3.9–§3.10 (2003); ISO/IEC 10646-1:2000 Annex D (2000)

ISO-8859-15	Empfohlen

Standard: ISO-8859, diese Normenfamilie wird nicht mehr weiterentwickelt und soll durch die UTF / ISO UCS-Familie abgelöst werden.

7.2.2 CSS (Cascading Stylesheet)

Erfinder URL Håkon Wium Lie, Bert Bos Version 1, W3C Version 2 , www.w3C.org

Cascading Stylesheet (CSS) Version 2 stellt die von W3C überarbeitete Version von Cascading Stylesheet dar und wird wie bei der Version 1 zur Definition der Darstellung von Inhalten verwendet. Sowohl für Formatierung von Inhalten in XML als auch für HTML und XHTML kann CSS verwendet werden.

Verwendung

Definition der Darstellung von Informationen in XML, HTML und XHTML

S1

CSS (Cascading Stylesheet) Level 2 (CSS 2 und CSS 2.1)	Dringend empfohlen

Standard:
Cascading Style Sheets Level 2 (CSS 2) Specification, May 1998 von W3C
Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification, Candidate Recommendation Sept. 2009 (www.w3C.org)

S1 **S2** **S3**

CSS (Cascading Stylesheet) Level 3	Unter Beobachtung

Bemerkung zu den Versionen: Zwar ist CSS 2.1 vorerst nur ein Standard-Kandidat, steht aber nur einen Schritt vor der definitiven Verabschiedung. CSS 2.1 stellt die Revision 1 des veralteten 2.0-Standards dar und geht in der Regel bei Konfliktfällen vor. Aktuelle Browser unterstützen den Standard CSS 2.1 im Kernanwendungsbereich weitgehend.

7.2.3 CSV (Comma Separated Value List)

Erfinder URL Borland, www.borland.com

Comma Separated Value List Dateien, kurz CSV-Dateien, sind ASCII-Dateien, welche häufig benötigt werden, um den Inhalt einer Datenbank (z.B. dBASE, ACCESS, SQL-Datenbank) zu extrahieren und in eine andere Datenbank wieder einzulesen. Dabei entspricht häufig ein Datensatz (Datenblatt) einer Zeile. Die Zellen werden durch ein Separationszeichen getrennt, siehe dazu auch RFC 4180.

Verwendung

Produkte- und plattformübergreifender Datenaustausch

	S1	S2	S3	
Comma Separated Value List (CSV)				Empfohlen

7.2.4 SIARD

SIARD ist ein Format, mit welchem relationale Datenbanken (basierend auf SQL Standards) in einem statischen Datenbankmodel archiviert werden können. Das SIARD-Format basiert auf Standards u.a. auf den ISO-Normen Unicode, XML, SQL1999 und dem Industriestandard ZIP. Zurzeit wird SIARD im Schweizerischen Bundesarchiv sowie in mehreren Schweizer Bundesämtern eingesetzt. Im Mai 2008 wurde es als das offizielle Format des europäischen PLANETS-Projekts für die Archivierung von relationalen Datenbanken akzeptiert.

	S2	S3	
SIARD			Empfohlen

URL: http://www.bar.admin.ch/dienstleistungen/00823/00825/

7.2.5 EPS (Encapsulated Post Script)

Erfinder URL Adobe Systems, www.adobe.com

EPS ist das Akronym für "Encapsulated Post Script" (File). Die EPS Datei ist mit einem Post Script-fähigen Programm erstellt worden und kann in einem anderen Programm weiterverarbeitet werden. Der englische Ausdruck „Encapsulated“ (zu Deutsch eingeschlossen, eingewickelt) stammt daher, dass dem Post Script-Teil der Datei ein Vor- und Nachspann mit wichtigen Informationen zur Datei angefügt worden ist.

Verwendung

Datenaustausch von Vektordaten inkl. Schriften vornehmlich im graphischen Gewerbe.

	S1	S2	S3	
Encapsulated Post Script (EPS)				Nicht empfohlen

EPS wurde in der Praxis durch PDF ersetzt und hat deswegen an Bedeutung verloren.

7.2.6 Geography Markup Language

Erfinder URL Open Geospatial Consortium, www.opengeospatial.org

Die Geography Markup Language (GML) ist ein XML-Anwendung für den Austausch und die Archivierung Raum bezogener Informationen, einschliesslich der Geometrie und der Eigenschaften geografischer Objekte.

Verwendung

Beschreibung (auf der Basis von XML-Schema) und Austausch (in XML) von Geoinformationen.

	S1	S2	S3	
GML 3.0/3.1/3.1.1				Unter Beobachtung

7.2.7 HTML (Hypertext Markup Language)

Erfinder URL Tim Berners-Lee, www.w3c.org

Hypertext Markup Language (HTML) ist eine standardisierte Seitenbeschreibungssprache und ein Fundament für WWW im Internet bzw. Intranet.

Verwendung

Definiert sowohl die Gestaltung, den Inhalt und die Grafik der Seite als auch die Links (Hyperlinks, Verbindungen) zu eigenen oder fremden Seiten.

S1	S2	S3	
Hypertext Markup Language (HTML) v.4.01 (strict)			Dringend empfohlen
Hypertext Markup Language (HTML) v.4.01 (transitional)			Empfohlen
HTML v.5			Unter Beobachtung

.

Anmerkung: Aus Interoperabilitätsgründen soll in jedem HTML Dokument das Encoding angegeben werden.

7.2.8 Interlis

Erfinder URL Werner Messmer, Josef Dorfschmid, www.interlis.ch

Das Interlis Datenformat wird für die Erfassung von Geodaten und deren Austausch in der Schweiz verwendet. Es gibt zwei verschiedene, in der Schweiz verwendete Versionen. Version 1 (SN 612030), Version 2 (SN 612031) sind Standard der Schweizerischen Normenvereinigung (www.snv.ch) und siehe auch zusätzlich eGovernment Schweiz Standards von www.ech.ch eCH0056 (siehe u.a. WMS, WFS, WCS).

Verwendung

Modellierung mit einer Datenbeschreibungssprache und Austausch von Informationen mit Raumbezug (Geoinformationen), z.B. aus den Bereichen Vermessung, Raumplanung, Umwelt, Verkehr.

S1	S2	S3	
Interlis Version 1			Empfohlen

Interlis Version 1 sollte durch Interlis Version 2 ersetzt werden.

S1	S2	S3	
Interlis Version 2			Dringend empfohlen

7.2.9 LDIF

Das **Format** der Daten, welche mit LDAP publiziert werden, ist oft LDAP Data Interchange Format (LDIF).

S1	S2	S3	
LDIF			Empfohlen

Standard: RFC 2849

7.2.10 MIME (Multipurpose Internet Mail Extension)

Erfinder URL IETF (N. Borenstein, T. Rose), www.ietf.org

Multipurpose Internet Mail Extension (MIME) ist ein IETF Standard (www.ietf.org) für Dateiformate und für die Angabe der darin enthaltenen Dateitypen. Im Zusammenhang mit multimedialen Elementen auf WWW-Seiten werden diese Angaben in Zukunft immer wichtiger. MIME-Typen werden bei der Kommunikation zwischen WWW-Server und WWW-Browser eingesetzt. Sowohl der WWW-Server als auch der WWW-Browser unterhalten eine Liste mit den ihnen bekannten Dateitypen. In vielen Browser (z.B. bei Netscape) befindet sich diese Liste in den so genannten "Helper Applications". Beim Übertragen vom Server zum Browser wird über das HTTP-Protokoll der MIME-Type mitgeliefert. Auf Grund seiner Liste mit MIME-Typen weiss der WWW-Browser, wie er die Datei zu behandeln hat. (RFC 2045, 2046 und zugehörige).

Verwendung

Dieses ursprünglich für E-Mail - sie wird folglich auch Multi-Part Mail genannt - entwickelte Dateiaustauschformat wird inzwischen auch bei anderen Anwendungen des Internet benutzt. So werden in einer HTML-Datei ab dem Standard 4.0 oder einer XHTML-Datei Einträge von Javascript und CSS mit einer Option type="text/javascript" bzw. type="text/css" eingebaut. Damit wird auf den Einschluss eines anderen Dateiformates hingewiesen. Anwendung findet dies auch bei der Einbettung von Multimedia-Dateien.

S1	S2	S3	
Multipurpose Internet Mail (MIME)			Dringend empfohlen

Standards: RFC 2045, RFC2046, RFC 4288 (aktualisiert und erweitert durch RFC 2646, RFC 3798, RFC 5147) und zugehörige von der IETF (www.ietf.org).

7.2.11 Microsoft Office XML Format

Erfinder URL Microsoft, www.microsoft.com

Microsoft hat das XML-Dateiformat für Word, Excel, Visio und InfoPath offen gelegt. Die Spezifikationen dazu sind **für jeden lizenzpflichtig, jedoch gebührenfrei** zugänglich und erlauben die Nutzung der Formate in eigenen Applikationen auf beliebigen Zielplattformen. Dies umfasst auch zukünftige Änderungen an diesen Formaten. Trotz der hohen Verbreitung von Microsoft Office wird dieses Format nicht empfohlen, weil Microsoft selber ein anderes Datenformat bevorzugt.

Verwendung

Austausch von Daten (Texte, Tabellen, Formulare oder Diagramme).

S1	S2	S3

Microsoft Office 2003 XML-Format	Nicht empfohlen

7.2.12 ODF

Erfinder URL OASIS, www.oasis-open.org und www.openoffice.org

Das OpenDocument Format (ODF) ist ein XML-basiertes Dateiformat für Office-Anwendungen zum Austausch von Dokumenten, welche Text, Tabellen, Diagramme und grafische Elemente enthalten können. Das Dokumentformat ermöglicht die Umwandlung in alternative Formate, da es weitgehend existierende Standards einbindet.

Verwendung

Applikation unabhängiger Austausch von Dokumenten wie Texte, Tabellen, Formulare, Diagramme oder Grafiken

S1 S2 S3

ODF v.1.0	Nicht empfohlen

Standards: ISO/IEC 26300 oder bei OASIS(www.oasis-open.org)

ODF v.1.1	Empfohlen

Bei OASIS.

ODF v.1.2	Unter Beobachtung

Bei OASIS.

7.2.13 Office Open XML File Formats

Erfinder URL ecma, www.ecma-international.org

Office Open XML File Formats basiert auf XML und ist ein von Microsoft vorgeschlagenes und von der ECMA weiter entwickeltes Format, welches frei in verschiedenen Applikationen und Plattformen implementiert werden kann.

Verwendung

Applikation unabhängiger Austausch von Dokumenten wie Texte, Tabellen, Formulare, Diagramme oder Grafiken. Dieses Format war von Beginn weg so konzipiert, dass deren Codierung mit MS Office kompatibel ist

S1 S2 S3

Office Open XML File Formats	Empfohlen

Standards: ISO/IEC 29500

7.2.14 PDF (Portable Document Format)

Erfinder URL Adobe Systems, www.adobe.com

Das Portable Document Format (PDF) ist ein Dateiformat zur Darstellung von Dokumenten, welches die Schriften, die Formatierungen, die Farben und Grafiken eines beliebigen Quell-

dokuments (weitgehend) beibehält, unabhängig vom Betriebssystem und vom Programm, mit welchem es erstellt wurde. PDF ist eine seitenorientierte Darstellung von Dokumenten, im Gegensatz zu HTML, bei welcher kein festes Seitenlayout zu Grunde liegt.

S1	S2	S3	
Portable Document Format (PDF) v.1.7 (gemäss ISO)			Dringend empfohlen

Standards: ISO 32000-1:2008. PDF v.1.7 kann mit dem Acrobat Reader ab Version 8.0 gelesen werden. Es sind nur Features, welche im genannten ISO Standard spezifiziert sind, zu verwenden.

Portable Document Format (PDF) v.1.4 , 1.5 , 1.6			Empfohlen

PDF v.1.4/ 1.5/ 1.6 kann mit dem Acrobat Reader ab Version 5.0/6.0/7.0 gelesen werden.

7.2.15 PDF/A-1

PDF/A ist eine durch die ISO genormte Version des Portable Document Formats. PDF/A besitzt nur ein Teil der Möglichkeiten von PDF, ist aber speziell u.a. für die Anforderungen der Langzeitarchivierung und der Barrierefreiheit für behinderte Menschen sowie für die Wiedergabe auf mobilen Endgeräten wie PDAs zugeschnitten. Diese Norm ist eine Untermenge von PDF 1.4, welche in ISO 19005-1:2005 (PDF/A-1) spezifiziert ist.

Die Norm spezifiziert zwei Ebenen von Übereinstimmungsgraden:

- PDF/A-1b - Level B (Basic) visuelle Reproduzierbarkeit
- PDF/A-1a - Level A (Accessible) zusätzlich zu Level B, Unicode unterstützung und strukturierte Inhalte zur korrekten Darstellung durch Screenreader.

S1		S3	
Portable Document Format (PDF)/A-1			Empfohlen

Standards: ISO 19005-1:2005

7.2.16 PDF/A-2

Wesentliche Erweiterungen gegenüber PDF/A-1 sind : PDF/A-2 basiert auf PDF 1.7 (ISO 32000-1), JPEG 2000 Kompression erlaubt, Transparenzen erlaubt, Ebenen erlaubt, OpenType-Fonts können eingebettet werden, digitale Signaturen in Übereinstimmung mit den PAdES (PDF Advanced Electronic Signatures, ETSI TS 102 778), Container: PDF/A-1 Dateien können in PDF/A-2 Dateien eingebettet werden.

Die Norm spezifiziert drei Ebenen von Übereinstimmungsgraden:

- PDF/A-2b: Mindestanforderung an eine PDF/A-2 Datei, garantiert das richtige Erscheinungsbild des Dokuments für eine Langzeitarchivierung
- PDF/A-2a: realisiert vollständig allen Anforderungen der ISO 19005-2, insbesondere alle strukturellen und semantischen Eigenschaften

PDF/A-2a wie 2b, der gesamte Text ist in Unicode abgebildet, so dass der gesamte Text indexiert dargestellt werden kann.

S1	S3	
Portable Document Format (PDF)/A-2		Dringend empfohlen

Standards: ISO 19005-2:2011

7.2.17 PDF/UA/VT/H/E

S1	S2	S3	
Portable Document Format (PDF) UA/VT/H/E			Unter Beobachtung

Standards: ISO 32000-1:2008, ISO 14291-1 für PDF/UA (=Universal Access), ISO 16612-2 für PDF/VT (= Variable and Transactional Printing, Outputmanagment), für PDF/H (= Health care) ist der ISO noch offen, ISO 24517 für PDF/E (=Engineering, CAD/CAM).

7.2.18 PDF/X

PDF/X ist eine genormte Version des Portable Document Formats, soll aber den Anforderungen an die Druckvorlagen der Druckindustrie gerecht werden. PDF/X besitzt deshalb selber nur eine Untermenge der technischen Merkmale von PDF. Es werden PDF-Inhalte, welche die Vorhersehbarkeit des Druckergebnisses beeinträchtigen können (Transferfunktionen, Transparenzen) oder sich nicht sinnvoll drucken lassen (Video, Audio), untersagt und Angaben vorgeschrieben, welche für die präzise Kommunikation mit dem Druckdienstleister erforderlich sind (Anschnitt, Farbbezeichnungen usw.).

PDF/X ist in den folgenden ISO-Standards genormt:

- ISO 15929 definiert den PDF/X-Ansatz insgesamt.
- ISO 15930 definiert konkrete Normteile. ISO 15390 ist wiederum in verschiedene Unternormen gegliedert, wobei die Norm ISO 15930-3: PDF/X-3: 2002 in Europa hauptsächlich verwendet wird.

Verwendung

Zum Austausch von Anzeigendaten im Zeitungs- und Zeitschriftengeschäft oder zur Übermittlung von Vorlagen für Druckaufträge

Portable Document Format (PDF) X/3	Empfohlen

Standard: ISO 15930 Serie

Portable Document Format (PDF) X/4-5	Unter Beobachtung

Standards: ISO 15930-7 und -8:2008

Bemerkung zu den Versionen: Weiterhin wird auch auf die Vorgabe PDF-X/A-1 zurückgegriffen. Welche Version in einem Auftrag verwendet werden soll, wird zwischen dem Erzeuger der Druckvorlagen und dem Druckdienstleister vereinbart.

7.2.19 PS (Post Script)

Erfinder URL Adobe Systems, www.adobe.com

Post Script (PS) ist eine von Adobe System Inc. 1984 auf den Markt gebrachte Seitenbeschreibungssprache für das seitenweise Ausdrucken und Speichern von Grafiken und Texten. Die Software arbeitet system-, grössen- und auflösungsunabhängig. Die Qualität des Ausdrucks richtet sich einzig nach den technischen Möglichkeiten des Ausgabegerätes.

Verwendung

Seitenbeschreibungssprache für Drucker oder Filmbelichter.

S1	S2	S3	
Post Script (PS) Level 1-2-3 (als Format für den Dokumentenaustausch)			Nicht empfohlen

7.2.20 RDF (Resource Description Framework)

Erfinder URL W3C, www.w3C.org

RDF steht für den englischen Ausdruck „Resource Description Framework“ und stellt eine XML-Anwendung dar, mit welcher Ressourcen wie Texte, Bilder, SW, etc. beschrieben werden können. Die Informationen in RDF sind Metadaten, nämlich Informationen über eine Information, wie Quellenangaben, Autor, Copyright, Adressen.

Verwendung

Dient der zusätzlichen Bezeichnung von Dateien, wie Quelle, Autor, ISBN Nr., etc.

S1	S2	S3	
RDF (Resource Description Framework)			Empfohlen

Standard: Resource Description Framework Model und Syntax Specification Recommendation, 22 February 1999, Standard von W3C (www.w3C.org)

7.2.21 Newsfeeds (ATOM, RSS)

Portale, welche Neuigkeiten schnell aufschalten und diesen Service in einem Abonnement anbieten wollen (publish and suscribe), verwenden eines der Datenformate für Newsfeeds. Damit wird eine Information nicht wie im Internet üblich aufgrund der Aktion des Lesers (Pull), sondern nach Aufschaltung durch den Verfasser automatisch empfangen (Push). Diese Formate basieren auf XML und bieten unterschiedlichen Umfang an Tags. Zur Zeit werden in der Regel diese drei Formate von entsprechender Software unterstützt:

S1	
RSS 2.0	Dringend empfohlen

Spezifikation: RSS 2.0, RSS Advisory Board, http://www.rssboard.org/rss-specification

RSS 1.0 und andere Versionen	Empfohlen

Spezifikation: W3C, http://web.resource.org/rss/1.0/spec

Atom Publishing Protocol, AtomPub 1.0	Unter Beobachtung

Spezifikation: Atom 1.0, RFC 4287; AtomEnabled.org, http://www.atomenabled.org/developers/syndication/

7.2.22 RTF (Rich Text Format)

Erfinder URL Microsoft, www.microsoft.com

Rich Text Format (RTF) wurde für den Daten- und Grafikaustausch formatierter Texte zwischen verschiedenen Textverarbeitungsprogrammen entwickelt. Nachteil des RTF-Formates: Nicht alle Formatierungsmöglichkeiten komplexer Textverarbeitungen werden berücksichtigt.

Verwendung

Format zum Austausch von formatierten Texten.

S1 S2 S3

Rich Text Format (RTF) Version 1.6	Empfohlen

Die Spezifikation kann bei Microsoft bezogen werden (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnrtfspec/html/rtfspec.asp)

7.2.23 WML (Wireless Markup Language)

Erfinder URL OMA, www.openmobilealliance.org

Wireless Markup Language, kurz WML, basiert auf XML.

Verwendung

Zur effizienten Übermittlung von Daten und Bildern auf und von Mobilen Geräten.

S1 S2 S3

WML (Wireless Markup Language) 2.0	Unter Beobachtung

WML Version 2 enthält im Gegensatz zur Version 1 XHTML Mobile Systeme als Subset und hat CSS integriert.

7.2.24 XHTML (eXtensible Hypertext Markup Language)

Erfinder URL W3C, www.w3C.org

eXtensible Hypertext Markup Language (XHTML) ist eine Auszeichnungssprache für das World Wide Web basierend auf XML. XHTML ist die Anpassung von HTML 4.0 in XML 1.0. Damit können Web-Seiten als strukturierte Dateien im XML-Format kodiert werden. Ange-

dacht ist, dass XHTML HTML als Darstellungs- oder Dokumentenformat für Web-Seiten ersetzen soll.

Verwendung

Darstellung von Inhalten im World Wide Web.

	S1	S2	S3
eXtensible Hypertext Markup Language (XHTML) v.1.0 strict			Dringend empfohlen
eXtensible Hypertext Markup Language (XHTML) v.1.0 transitional			Unter Beobachtung
eXtensible Hypertext Markup Language (XHTML) v.1.1/v.2.0			Unter Beobachtung

Standard: XHTML 1.0 und 1.1, Extensible Hypertext Markup Language Recommendation 1.1, May 2001 von W3C (www.w3C.org).

7.2.25 XML (eXtensible Markup Language)

Erfinder URL W3C, www.w3C.org

Die eXtensible Markup Language (XML) ist eine generische plattformunabhängige Datenbeschreibungssprache. Seit Februar 1998 ist XML ein W3C-Standard. XML ist ebenfalls in RFC 3470 standardisiert.

Das XML-Dokument besitzt eine inhaltliche Struktur, jedoch ohne definierte Formatierung (Layout). Die Inhaltselemente werden durch eine Dokument Typ Definition (DTD) oder durch eine neuere und umfassendere Deklarationssprache (wie etwa XML-Schema) definiert. XML basiert auf diesen hier in SAGA.ch nicht weiter beschriebenen Basis-Standards: Unicode-Zeichensätze, URI für Namensräume und zur Adressierung sowie ISO-Standards etwa zur Benennung von Ländern und Sprachen.

Zu XML und zu XML Namespaces, sei auch auf die Dokumente eCH-0018 (XML Best Practices) und eCH-0033 (Beschreibung von XML Namespaces) von eCH verwiesen.

Verwendung

XML definiert Daten- und Dokumentformate.

	S1	S2	S3
eXtensible Markup Language (XML) v.1.0			Dringend empfohlen
eXtensible Markup Language (XML) v.1.1			Empfohlen

Standard: Extensible Markup Language (XML) Recommendation von W3C (www.w3C.org). Siehe zur Empfehlung der Versionen das Dokument eCH-0018, Kapitel 4

7.2.26 XML-Schema

Erfinder URL W3C, www.w3C.org

XML-Schema ist auch eine Anwendung von XML und dient der Beschreibung des Inhaltsmodells und der Deklaration der Elemente, wie Bestellungen, Zahlungsaufträge etc. oder von einfachen Datensätze wie Adressen.

XML-Schema ist bei W3C in folgende drei Standards unterteilt:

- XML-Schema Part 0: Primer
- XML-Schema Part 1: Structures
- XML-Schema Part 2: Datatypes

XML Part 0 beabsichtigt eine leicht lesbare Beschreibung der XML-Schema Eigenschaften und ist so ausgelegt, dass man schnell versteht, wie XML-Schema zu bilden sind. XML-Schema Part 1 und 2 definiert, wie die Merkmale und Eigenschaften der Struktur und Datentypen im XML-Schema zu beschreiben sind.

Verwendung

XML-Schema dient der Deklaration von XML-Inhalten und -Datentypen.

	S1	S2	S3
XML-Schema Part 0,1,2			Dringend empfohlen

Zu den Standards und Versionen siehe Dokument eCH-0036 – der FG XML.

7.2.27 Document Schema Definition Languages (DSDL)

In einigen XML-Applikationen werden einzelne der 11 Teile dieses Rahmenwerks (insbesondere RELAX NG, Schematron sowie Namespace-fähige DTDs) zur Datenmodellierung und Validierung verwendet. Meist wird jedoch für diese Aufgaben XML Schema verwendet.

	S1	S2	S3
Document Schema Definition Languages (DSDL)			Empfohlen

Standards: ISO/IEC 19757

7.2.28 XBRL (eXtensible Business Reporting Language)

Erfinder URL XBRL International, http://www.xbrl.org/ """"

XBRL ist eine XML-basierte Sprache, um Geschäfts- und Finanzinformationen auszudrücken. Um branchenspezifische Bedürfnisse, unterschiedliche Anwendungsbiete oder unterschiedliche Buchhaltungsstandards abzudecken, werden verschiedene "Taxonomien" verwendet. Für die ergänzende Definition von zusätzlichen Taxonomien gemäss lokalen oder nationalen Bedürfnissen sind sogenannte "nationale Jusrisdiktionen" zuständig, in der Schweiz der Verein XBRL CH; http://xbrl-ch.ch/.

	S1	S2	S3
eXtensible Business Reporting Language (XBRL) v. 2.1			Empfohlen

7.2.29 XSL (eXtensible Stylesheet Language)

Erfinder URL W3C, www.w3C.org

eXtensible Stylesheet Language (XSL) legt die Darstellung oder das Erscheinungsbild einer Klasse von XML-Dokumenten fest. Die Standardisierung der Darstellung der XML-Dokumenten besteht im Wesentlichen aus:

- XSL Transformations (XSLT). Eine Sprache zum Transformieren von XML-Dokumenten in andere XML-Formate oder reinen Text.
- XML Path Language (XPath). Eine Sprache zur Adressierung von Teilen von XML-Dokumenten (Knoten oder Sets von Knoten) referenziert oder wie Teile davon erreicht werden können.
- XSL Formatting Objects (XSL-FO). Beschreibt, wie die XML-Seiten aussehen, wenn sie dem Leser präsentiert werden.

Alle drei soeben erwähnten Standards sind separate XSL Standards. Verwendung

XSL dient einerseits der Umwandlung von XML-Dokumenten in andere Zielformate wie andere XML-Formate oder HTML-Dokumente sowie zur formatierten Ausgabe (mittels XSL-FO) z.B. in PDF- oder RTF-Dokumente.

	S1	S2	S3
eXtensible Stylesheet Language (XSL) 1.0 (XSL-FO)			Nicht empfohlen

Standards: Extensible Stylesheet Language (XSL), W3C Recommendation Version 1.0, 15 October 2001 (www.w3C.org).

	S1	S2	S3
eXtensible Stylesheet Language (XSL) 1.1 (XSL-FO)			Dringend empfohlen

Standards: Extensible Stylesheet Language (XSL) Version 1.1, W3C Recommendation, 05 December 2006 (www.w3C.org).

	S1	S2	S3
XSL Transformations (XSLT) 1.0 (mit XPath 1.0)			Dringend empfohlen

Standards: XSL Transformations (XSLT) Version 1.0, W3C Recommendation, 16 November 1999;
XML Path Language (XPath) Version 1.0, W3C Recommendation, 16 November 1999 (www.w3C.org).

	S1	S2	S3
XSL Transformations (XSLT) 2.0 (mit XPath 2.0)			Unter Beobachtung

Standards: XSL Transformations (XSLT) Version 2.0, W3C Recommendation, 23 January 2007, XML Path Language (XPath) 2.0, W3C Recommendation, 23 January 2007 (www.w3C.org)

Anmerkung: Zu XML generell gibt es bei eCH eine Reihe von Dokumenten (Standards und Best Practices). Die aktuellsten Dokumente können bei www.ech.ch heruntergeladen werden.

7.2.30 XForms

Erfinder URL W3C, www.w3C.org

XForms ist ein W3C-Standard für elektronische Formulare und interaktive Elemente einer Benutzeroberfläche. XForms ist nach Prinzip Model-View-Controller (MVC) aufgebaut und trennt daher die Datenfelder (z.B. XML Schema), die Darstellung (z.B. HTML) und die Ausführung (z.B. ECMA Script). XForms kann XML-Daten an den Server schicken. XForms können mit XML-Werkzeugen generiert und bearbeitet werden. Beim empfohlenen Einsatz von XForms server-side, werden die Formulare in HTML konvertiert und so zum Browser geschickt. Nicht empfohlen wird der direkte Einsatz, welcher beim Anwender die Installation einer Browser-Erweiterung erfordert.

Verwendung

Aufnahme, Verarbeitung, Ablage und Darstellung von Informationseinheiten in Formularfeldern

S1	S2	S3	
XForms v1.1 (Einsatz server-side)			Empfohlen

Standard:XForms 1.1, W3C Recommendation, 20 October 2009, von W3C (www.w3C.org).

7.3 Bilder und Grafiken

7.3.1 GIF (Graphics Interchange Format)

Erfinder URL Compuserve, www.compuserve.com

GIF ist die Abkürzung von "Graphics Interchange Format" – zu Deutsch Grafik-Austauschformat. Neben JPEG ist GIF das wichtigste Format, um Bilder browserkonform zu speichern. GIF-Bilder können maximal 256 verschiedene Farben enthalten, und eignen sich vor allem für Grafiken, Logos oder Schriftzüge. (JPEG unterstützt dagegen das Farbformat „True Color“ und eignet sich besser für Fotos!). Weiter ermöglicht dieses Bildformat eine verlustfreie Kompression und eine Farbe als transparent zu setzen.

S1	S2	S3	
Graphics Interchange Format (GIF) 89a			Dringend empfohlen
Graphics Interchange Format (GIF) 87a			Nicht empfohlen

7.3.2 JPEG (Joint Photographic Expert Group)

Erfinder URL JPEG (Joint Photographic Expert Group), www.jpeg.org

Joint Photographic Expert Group (JPEG) ist eine Kommission, welche das Verfahren zum Komprimieren und Speichern von Bild- und Videodaten festlegt. JPEG ermöglicht zudem eine verlustfreie Kompression und die Darstellung von mehr als 16 Millionen Farben.

S1	S2	S3
Joint Photographic Expert Group (JPEG / JPG)		Dringend empfohlen

Standards: ISO/IEC 10918-1. JPEG XR zukünftig in Anlehnung an ISO/IEC 29199-2.

7.3.3 PNG (Portable Network Graphics)

Erfinder URL W3C, www.w3C.org

Portable Network Graphics (PNG) ist ein vom World Wide Web Consortium (W3C) entwickeltes und als Standard verabschiedetes Dateiformat.

S1	S2	S3
Portable Network Graphics (PNG)		Dringend empfohlen

Standard: Portable Network Graphics (PNG) Recommendation 10 November 2003, von W3C (www.w3C.org).

7.3.4 SVG (Scalable Vector Graphics)

Erfinder URL W3C, www.w3C.org

Scalable Vector Graphics (SVG) ist eine vom World Wide Web Consortium (www.w3C.org) als "Recommendation" freigegebene XML-Anwendung zur Beschreibung von Vektorgrafiken und Animationen, die in Webseiten eingebunden werden können. SVG berücksichtigt drei Arten von Grafiken:

- Vektorbasierende Geometrie (z.B. Linien und Kurven)
- Pixelbilder und
- Text

S1	S2	S3
Scalable Vector Graphics (SVG) v.1.1		Empfohlen

Standard: Scalable Vector Graphics (SVG) 1.1 Recommendation, 14 January 2003 von W3C (www.w3C.org)

7.3.5 TIFF (Tagged Image File Format)

Erfinder URL aldus/adobe, www.adobe.com

Tagged Image File Format (TIFF) ist ein Dateiformat und Standard für Pixelgrafiken. Dieser Standard wurde von Aldus, Hewlett Packard und Microsoft als Ausgabeformat von Scannern ins Leben gerufen. Die meisten Grafikprogramme, die mit Pixelgrafiken umgehen können, unterstützen dieses Format. TIFF wird hauptsächlich in der digitalen Archivierung verwendet, manchmal auch zum verlustfreien Bilddatenaustausch (Bitmap).

S1	S2	S3
Tagged Image File Format (TIFF) v.5.0		Nicht empfohlen

Tagged Image File Format (TIFF) v.6.0	Empfohlen

Hinweis auf Standard: http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf

7.4 Multimedia

7.4.1 MPEG (Motion Pictures Expert Group)

Erfinder URL MPEG (Motion Pictures Expert Group), www.mpeg.org

Motion Picture Expert Group (MPEG) legte bzw. legt Dateiformate und Verfahren zum Komprimieren und Speichern von Video- bzw. Multimediadaten (Video, Bild- und Tondaten) in hoher Qualität fest. Es gibt verschiedene MPEG Standards.

7.4.1.1 MPEG-1

MPEG-1 erlaubt Kompressionsraten um die 1,5 Megabits pro Sekunde (Mbps) und wird vor allem für Video-CD Kodierung benutzt. MPEG-1 Audio Layer III ist der volle Name für das MP3 Audio Format. **MP3 ist lizenz- und gebührenpflichtig** sowohl für En- und Decodierung als auch für die reine Inhaltsweitergabe (Streaming, Dateiweitergabe).

MPEG-1	Empfohlen

7.4.1.2 MPEG-2

MPEG-2 ist der Standard für digitales Fernsehen, Set-top Boxen und DVDs. **MPEG-2 ist lizenz- und gebührenpflichtig** für En- und Decodierung als auch für die Inhaltsweitergabe!

MPEG-2	Empfohlen

7.4.1.3 MPEG-4

MPEG-4 kann vereinfacht als technische Erweiterung (für Durchsatzraten ab 64 kBit/sec.) von MPEG 1 und 2 aufgefasst werden und erlaubt neue, optimierte Methoden zur Komprimierung von Video und Audio Inhalten. **MPEG-4 ist lizenz- und gebührenpflichtig** für En- und Decodierung als auch für die Inhaltswiedergabe. MPEG-4 wurde in mehreren Versionen veröffentlicht, welche abwärtskompatibel sind, d.h. Version 2 (aus dem Jahre 1999) umfasst Version 1 (1998) etc. Die aktuelle Version ist 3. Wichtiger als die Versionen ist jedoch, wie bei allen anderen Mediaformaten, das verwendete Profil, welches den benutzten (Kompressions-) Algorithmus definiert.

Verwendung

Austausch von Filmen und Animationen.

S1 **S2** **S3**

MPEG-4 v.3	Empfohlen

Standard: ISO/IEC 14496

7.4.2 MP3

Siehe Kapitel 7.4.1.1

7.4.3 OGG

Erfinder URL Xiph.org Foundation, www.xiph.org

Ogg ist eine Familie von Datenformaten (besser Bitstream Formaten), welche von der Xiph.org Foundation vorangetrieben wird. Das bekannteste Format ist Ogg Vorbis, ein offenes und patentfreies Audio Format. Dieses Format wurde entwickelt, um mit MP3 zu konkurrenzieren. Ein weiteres Format ist Ogg Theora, ein offenes und patenfreies Video Format, entwickelt, um mit den kostenpflichtigen Formaten MPEG-4, RealVideo und Windows Media Video zu konkurrenzieren. Das Ogg Bitstream Format ist im RFC3534 standardisiert.

Verwendung

Austausch von Audio und Video Daten.

	S1	S2	S3
OGG Theora			Unter Beobachtung
OGG Vorbis/FLAC			Empfohlen

7.4.4 QT (QuickTime)

Erfinder URL Apple Macintosh, www.apple.com

QuickTime, kurz QT, ist ein Multimedia Datenformat, von Apple entwickelt, fähig, verschiedene Formate, wie Video, Audio, zu speichern. QuickTime ist **in der Regel lizenz-, aber nicht gebührenpflichtig** für En- und Decodierung als auch für die Inhaltsweitergabe. QuickTime ist verfügbar für die Betriebssysteme Macintosh OS, Windows und mit Einschränkungen Linux.

Verwendung

Zum Speichern und Austausch von Video und Audio Daten.

	S1	S2	S3
QT (QuickTime) v.6.5			Nicht empfohlen

7.4.5 WAV (WAVEform audio format)

Erfinder URL Microsoft, www.microsoft.com

WAVEform audio format WAV ist eine Variante des RIFF Bitstream Formats zum Speichern von Audiodaten unter Nutzung verschiedener Algorithmen. Am meisten verwendet ist das unkomprimierte, verlustfreie PCM, welches als de facto Standard für Audiodaten gelten kann und auf nahezu jeglicher Plattform unterstützt wird. WAV ist lizenz- und gebührenfrei.

Verwendung

Zur Speicherung von Audio Daten.

S1	S2	S3	
WAV (WAVEform audio format)			Empfohlen

Standard: http://www.tactilemedia.com/info/MCI_Control_Info.html

7.4.6 WMV/A (Windows Media Video/Audio)

Erfinder URL Microsoft, www.microsoft.com

Windows Media Video/Audio (WMV/A) ist der Name für eine Reihe von Video/Audio Technologien, welche von Microsoft entwickelt worden und Teil des Windows Media Framework sind. WMV/A wurde als neuer Industriestandard für Highdefinition (HD) DVDs ausgewählt. WMV/A ist **lizenz-,** in der Regel **aber nicht gebührenpflichtig** für En- und Decodierung als auch für die Inhaltsweitergabe. WMV/A ist verfügbar für die Betriebssysteme Macintosh OS, Windows, Solaris und Linux.

Verwendung

Zur Übermittlung und Speicherung von Video Daten.

S1	S2	S3	
WMV/A (Windows Media Video/Audio) v.9			Empfohlen

URL auf Standard: http://msdn.microsoft.com/en-us/library/bb331849(VS.85).aspx

7.4.7 SWF file format (Adobe Flash Player)

SWF ist ein Dateiformat zur Übermittlung von Vektorgrafik, Text, Video und Audio über das Internet zum Abspielen mit dem Browser-Plugin der Firma Adobe, wobei auch eine Skript-Sprache unterstützt wird, so dass interaktive Anwendungen möglich sind.

Im Zusammenhang dieses Browser-Plugins sind immer wieder Sicherheitsprobleme bekannt geworden, die sich vermeiden lassen, indem man das Plugin nicht installiert.

Das Format ist öffentlich dokumentiert, aber kein offener Standard: Es gibt ausser dem Browser-Plugin der Firma Adobe keine weitere vollständige Implementierung in einem Browser-Plugin. Ausserdem wird die Weiterentwicklung des Formats von einer einzelnen Firma bestimmt.

S1			
SWF file format			Nicht empfohlen

7.5 Sonstige

7.5.1 Kompression

7.5.1.1 GZIP (Gnu ZIP)

Erfinder Abraham Lempel, Jacob Ziv, Terry Welch

GZIP dient der verlustfreien Kompression von Daten und ist eine open source Version, welche bei den UNIX Betriebssystemen enthalten ist. GZIP basiert auf den gleichen Verfahren wie ZIP und wurde im RFC 1952 standardisiert.

Verwendung

Verlustfreie Kompression von Daten.

S1	S2	S3	
GZIP (Gnu Zigzag Inline Package) v.4.3			Empfohlen

7.5.1.2 ZIP

Erfinder A. Lempel, J. Ziv

Zigzag Inline Package (ZIP) ist eine verlustfreie Komprimierungsmethode, bei der die Originaldaten erhalten werden - was für Programme, Texte oder Tabellen unumgänglich ist. Packer wie Winzip arbeiten mit dieser Methode.

Verwendung

Datenaustausch in komprimierter Form.

S1	S2	S3	
Zigzag Inline Package (ZIP) v.2.0			Dringend empfohlen

Hinweis auf Standard: www.pkware.com

7.5.2 SMS (Short Message Service)

Erfinder URL ETSI / SMS Forum, www.ETSI.org / www.smsforum.net

SMS steht für Short Message Service und wurde vom ETSI und SMS Forum für den Austausch von Daten an und von Mobiltelefonen spezifiziert. Grundsätzlich bietet SMS keine Sicherheit. Folglich sollte der Austausch von SMS Nachrichten nur erfolgen, wenn die Bekanntgabe, die Veränderung oder der Verlust deren Inhalts risikolos ist.

Verwendung

Vorwiegend zur Übermittlung von Daten zu und von Mobilephones.

S1	S2	S3	
SMS (Short Message Service)			Empfohlen

Hinweis auf Standard: www.3gpp.org

7.6 Ausführbare Komponenten in Dateien

In bestimmte Dateien wie HTML können auch Programme wie JavaScript eingebunden werden, welche erst beim Empfänger (Client) der Daten ausgeführt werden. Solche Programme werden als ausführbare Komponenten bezeichnet. Die unkontrollierte Nutzung von Daten mit ausführbaren Komponenten kann zu gravierenden Sicherheitsproblemen führen, s. dazu auch [Nem]. Deswegen sollten nur signierte ausführbare Komponenten akzeptiert werden,

wobei das Zertifikat für die Verifikation der Signatur von einem vertrauenswürdigen Zertifizierungsdienst ausgestellt worden ist.

Unsignierte ausführbare Komponenten, wie ActiveX, Applets, nicht empfohlen

7.6.1 Java Script

Erfinder URL Brendan Eich, Netscape Communication, www.netscape.com

Verwendung

JavaScript ist eine plattformunabhängige Programmiersprache. JavaScript Programme werden hauptsächlich in HTML oder XML integriert, um beim Client entsprechende Abläufe oder Datenaufbereitungen auszulösen.

S1

JavaScript	Empfohlen

Der Einsatz von Javascript ist gestattet, mit dem Einsatz verbunden sind jedoch Sicherheitsrisiken ! Diese können zum Teil durch geeigneten eingeschränkten Einsatz verhindert werden. Die Websites sollten auch verwendbar sein, wenn Javascript im Browser nicht aktiviert ist.

Hinweis auf Standard: http://www.ecma-international.org/ . Dazu gibt es auch ISO 16262.

7.6.2 ActiveX

Erfinder URL Microsoft, www.microsoft.com

Verwendung

Zur Einbindung von Multimedia Daten und Programmen in Web-Applikationen oder Dateien. ActiveX wird bei der Kommunikation von „Cross-Application“ eingesetzt.

S1

Signierte ActiveX	Unter Beobachtung

URL auf Standard: http://msdn.microsoft.com/en-us/library/aa751972(VS.85).aspx

7.6.3 Java Applets

Erfinder URL Sun Microsystems, www.sun.com

Verwendung

Java ist eine plattformunabhängige Programmiersprache. Java Programme können auch in Web-Seiten oder anderen Applikationen integriert werden.

S1

Signierte Java Applets V.1.6	Empfohlen

Empfehlung: Wenn die Ausführung von aktiven Komponenten beim Empfänger erlaubt ist, sollte eine aktuelle Content Security Prüfung bei Empfänger aktiviert sein, welche den empfangenen Datenstrom auf gefährliche Inhalte (Komponenten) untersucht.

7.6.4 . Net Assembly

Erfinder URL Microsoft, www.microsoft.com

Verwendung

Im Microsoft .NET Framework (oder Mono) ist ein Assembly eine teilweise kompilierte Programm Bibliothek. In den Microsoft Windows Implementationen von .NET ist ein Assembly eine versendbare (engl. portable) und ausführbare Datei.

S1

Signierte .Net Assembly	Unter Beobachtung

7.6.5 AJAX

Erfinder Jesse James Garrett

Verwendung

AJAX, engl. Kürzel für Asynchronous JavaScript and XML, ist eine Web-Entwicklungstechnik, um interaktive Web-Applikationen zu entwickeln. Die Absicht dabei ist, die Web-Seite so zu gestalten, dass Veränderungen auf der Seite kein Neuladen der Seiten erfordern. Die soll u.a. die vermeintliche Übertragungsgeschwindigkeit und die möglichen Interaktionen erhöhen.

S1

AJAX Files	Empfohlen

Der Einsatz von AJAX ist anderen, insbesondere herstellerspezifischen Alternativen, vorzuziehen. Javascript ist eine Voraussetzung, dafür siehe dort (Sicherheitsrisiken !).

8 Sicherheit

Ein wesentlicher Aspekt für die erfolgreiche Umsetzung und Durchführung von Dienstleistungen (z.B. Web Services) im Rahmen von eGovernment Anwendungen ist die Datensicherheit. Datensicherheit repräsentiert und fördert die gesicherte Kommunikation zwischen den sich vertrauenden Instanzen, wie zwischen den Bürgern, zwischen den Behörden und den Bürgern als auch der Wirtschaft und den Behörden untereinander. Das Vertrauen wird unter anderem dadurch erschüttert, wenn Pannen auftreten, die Rechtskräftigkeit der Transaktion angezweifelt werden kann oder die Vorgänge nicht zuverlässig und nicht transparent[7] für die Beteiligten abgewickelt werden.

Datensicherheit wird als eine durchgängige Komponente identifiziert, welche je nach Bedarf und Anforderung in jedem Kommunikationsabschnitt durch entsprechende Verfahren und Methoden unterstützt werden kann oder muss. Der Einsatz der technischen und organisatorischen Mittel muss so gestaltet werden, dass:

- eine gesicherte Kommunikation zwischen den sich vertrauenden Instanzen gebildet werden kann.
- der minimale Grundschutz ermöglicht wird.
- die klassischen Schutzbedürfnisse befriedigt werden.
- die rechtlichen Rahmenbedingungen erfüllt werden.

Da die Bedeutung der Sicherheitsmassnahmen in den letzten Jahren durch die zunehmende Nutzung des Internets und durch die globale Kommunikation extrem gestiegen ist, kann man auch einen Anstieg von Normierungsbestrebungen im Bereich Sicherheit verzeichnen. So ist eine Vielzahl von Sicherheitsstandards, -richtlinien und -empfehlungen entstanden.

Dieses Kapitel stellt die relevanten Sicherheitsstandards und -empfehlungen für eGovernment-Dienstleistungen in knapper Form vor. Wie bereits zuvor werden hier hauptsächlich Technologien und Standards zur Absicherung der Schnittstellen S1, S2, S3 empfohlen. Nicht behandelt wird hier, wie Systeme abgesichert (gehärtet) und wie die Rechte verteilt werden sollen.

Aus folgenden Gründen sind neben den Empfehlungen noch zusätzliche Erläuterungen eingebaut worden:

- Zwecks besseren Verständnisses sind die hier aufgeführten Technologien in einen Kontext eingebunden worden.
- Weiter soll sich bei den hier gemachten Ausführungen herauskristallisieren, welche zusätzlichen Empfehlungen neben der IT Sicherheitsstrategie von ***eCH*** und SAGA.ch noch zu formulieren sind[8].

[7] Zur Transparenz und Rechtskräftigkeit von Prozessen siehe SNR CWA 14842-1

[8] Zu einem späteren Zeitpunkt können dann die entsprechenden Kapitel entsprechend gekürzt werden und sich eventuell nur noch auf einen Literaturhinweis beschränken.

8.1 Strukturmodell für Datensicherheit

Um die Sicherheitsstandards einfacher zu präsentieren und verstehen zu können, wurde das folgende Strukturmodell (s. folgende Abbildung) entworfen. Das Strukturmodell ist kein Schichtenmodell, sondern veranschaulicht die verschiedenen Spezifikationsbereiche in Form von Blöcken. Es dient dazu, die IT-Sicherheit trotz ihrer Komplexität besser zu kategorisieren und somit hoffentlich besser zu verstehen.

Ein Datensicherheitsstandard zur Sicherheitstechnologie umfasst im Allgemeinen mehr als einen hier gezeigten Strukturblock. Deshalb wird darauf verzichtet, die Standards den verschiedenen Blöcken zuzuordnen.

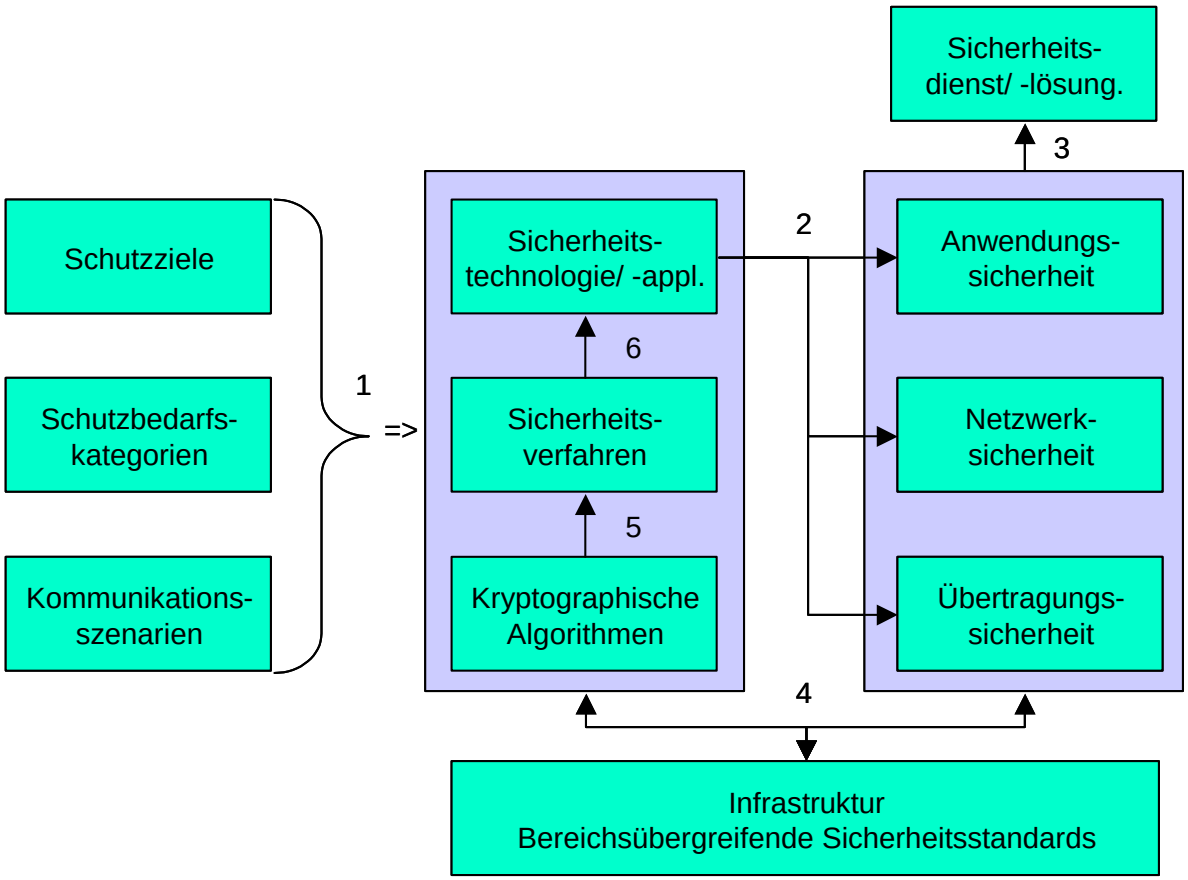

Abbildung 8-1 Strukturmodell für Sicherheitsstandards

Bilderklärung

Schutzziele. Hier wird pro Use Case oder pro angebotenen Dienst definiert, welchen Schutzbedarf der jeweilige Use Case oder Dienst hat.

Schutzbedarfskategorien. Hier werden die Schutzbedürfnisse und Risiken u.a. bezüglich folgender Kategorien festgehalten:

- Authentizität
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Kommunikationsszenarien. Hier werden der Kommunikationsprozess und –abläufe für die verschiedenen möglichen Szenarien beschrieben.

Kryptographische Algorithmen. In diesem Block werden die zu unterstützenden kryptographischen Algorithmen festgelegt.

Sicherheitsverfahren. Die verschiedenen kryptographischen Algorithmen können miteinander kombiniert werden, so dass sie eine bestimmte Schutzkategorie schützen können. Z.B. schützt die digitale Signatur die Authentizität und Integrität.

Sicherheitstechnologie/ -applikation. Eine Sicherheitstechnologie ist ein Standard, welcher in ein Produkt umgesetzt werden kann oder eine abgeschlossene Komponente eines Produkts bilden könnte (Halbfertigware)[9]. Eine Sicherheitstechnologie/ -applikation besteht aus einer Vielzahl von Sicherheitsverfahren, wie z.B. SSL/TLS, so dass gewisse Protokolle, Netzwerkabschnitte geschützt werden. Welche Sicherheitstechnologien/ -applikationen zum Einsatz kommen sollen, wird hier definiert.
Dem Bereich Sicherheitstechnologie/ -applikation werden auch die geschützte Ablage von Dokumenten und der Schutz von Datenbanken zugeordnet.

Übertragungssicherheit: Bei der Übertragungssicherheit werden die Daten und Informationen auf der Übertragungsstrecke gesichert. Diese Methode ist z.B. zur Sicherung von Daten geeignet, welche synchron übertragen werden, wie der Inhalt eines Telefongesprächs. Weiter ist hier die Link Layer Chiffrierung von Daten angesiedelt.

Netzwerksicherheit: Bei der Netzwerksicherheit werden die Informationen auf der Ebene des Netzwerks abgesichert und dort geschützt. Auf dieser Ebene werden die IP Pakete mit Nutzinformationen als ganzes und die Informationen zum Routing, wie RIP, OSPF oder BGP abgesichert, wobei die Nutzinformationen unter Umständen anders (auf einer anderen Ebene) als die Informationen zum Routing geschützt werden.

Anwendungssicherheit: Bei der Anwendungssicherheit werden die Informationen direkt unterhalb der Ebene 4 (z.B. SSL/TLS) des Internetmodells (IETF) Architekturmodells oder die Applikationsdaten selber (z.B. S/MIME) geschützt.

Infrastruktur und bereichsübergreifende Sicherheitsstandards. Das Arbeiten mit Public Key Verfahren benötigt bei einer grossen Anzahl von beteiligten Kommunikationspartnern Zertifikate und eine Infrastruktur, welche die Zertifikate handhabt und welche eventuell Aufgaben des Schlüsselmanagements übernimmt. Zu den bereichsübergreifenden Sicher-

[9] Mehr zur Abgrenzung zu den Sicherheitsverfahren im Kapitel 8.8.

heitsstandards zählen wir hier auch die Anbindung von Smart Cards oder die Schnittstellen zum Directory Service.

Sicherheitslösung: Eine Sicherheitslösung sichert einen Anwendungsfall (Use Case) und kann aus einer oder mehreren Komponenten der Übertragungs-, Netzwerk- oder Anwendungssicherheit bestehen. Doch im allgemeinen Fall kommen noch weitere Komponenten hinzu, wie

- Systemsicherheit (Härten eines Servers)
- Einbindung einer Firewall
- Massnahmen zur Sicherung der Verfügbarkeit
- UDDI Directory Sicherung
- Gesicherte Ablage und gesicherter Transport von WSDL Dateien
- Authentische WSDL Dateien
- usw.

Sicherheitslösungen als solche können nicht standardisiert werden, sondern es können nur Anleitungen, Tipps oder „best practices“ vermittelt werden. Deswegen werden in diesem Kontext keine Standards empfohlen oder für dringend empfohlen erklärt.

Für die Erarbeitung, Konzeption von Sicherheitslösungen und das Ergreifen von Massnahmen empfehlen wir, u.a. das Grundschutzhandbuch [GSHB] des Deutschen Bundesamtes für Sicherheit (BSI) zu konsultieren; für das Führen und Abwickeln von IT Projekten das Buch [Hermes] vom ISB. Ein Kurzüberblick, was beim Web-Auftritt in punkto Sicherheit zu beachten ist, ist im Dokument SNR CWA 14842-3 des SNV enthalten.

1. Die Schutzziele, Schutzbedarfskategorien und Kommunikationsszenarien beeinflussen die kryptographischen Algorithmen, die einzusetzenden Sicherheitsverfahren und die zu verwendenden Sicherheitstechnologien.
2. Die gewählte Sicherheitstechnologie hat einen Einfluss darauf, welche Abschnitte oder Teile der Kommunikation abgesichert werden. Z. B. ermöglicht S/MIME (Sicherheit in den Applikationsdaten), die Daten vom Absender bis zum Empfänger zu sichern, während IPSEC die Sicherheit der Daten auf Ebene des Netzwerks sichert und selten einen Schutz der Daten vom Sender bis zum Empfänger der Daten ermöglicht.
3. Die geschützten Kommunikationsabschnitte sind Bestandteile der Sicherheitslösung.
4. Definiert die Schnittstelle zur Infrastruktur und zu den gemeinsam genutzten Ressourcen, wie Smart Cards, Directory Service oder UDDI Verzeichnisse.
5. Die kryptographischen Algorithmen bestimmen die zu verwendenden Sicherheitsverfahren.
6. Die Sicherheitsverfahren legen die Ausprägung und Nutzung der Sicherheitstechnologien/ -applikationen fest.

Bemerkung: Das hier gezeigte Strukturmodell und die nun aufgeführten Datensicherheitsstandards entbinden nicht

- von der eingehenden Analyse der jeweiligen Fachanwendung hinsichtlich Gesetzeskonformität durch die entsprechenden Spezialisten,
- von der Einhaltung der Gesetze,
- sowie von der Überprüfung und Einhaltung des Sicherheitsniveaus in allen Instanzen und Prozessen der Kommunikationskette.

Eine anwendungsspezifische Risikoanalyse, die Schutzbedarfsfeststellung sowie ein Sicherheitskonzept müssen erstellt werden. Schutzziele, Schutzbedarf und Anwendungsfälle definieren die Zielsetzung der zu treffenden Sicherheitsmassnahmen.

8.2 Schutzziele

Schutzziele definieren die Sicherheitsinteressen oder -bedürfnisse der beteiligten Kommunikationspartner und werden in allgemeiner Form bezüglich der folgenden, verschiedenen Bedrohungen beschrieben:

- **Vertraulichkeit** – Schutz vor Kenntnisnahme durch Unberechtigte
  Bedrohung: Daten werden nicht autorisierten oder nicht berechtigten Individuen, Entitäten oder Prozessen zur Verfügung gestellt oder offenbart.
  Definition 1 von Vertraulichkeit: Eine Information liegt **vertraulich** vor, wenn ein bestimmter Personenkreis glaubt[10], dass nur er die Information lesen oder nur er Einsicht in die Information nehmen kann.
  Definition 2 von Vertraulichkeit: Absicherung, dass die Information nur einem bestimmten, autorisierten Personenkreis zugänglich ist [SNR CWA 14842-3].
- **Integrität** – Schutz vor ungewollter Manipulation
  Bedrohung: Daten können aus Sicht des Dateneigentümers oder -besitzers ungewollt oder unberechtigterweise verändert oder zerstört werden.
  Definition 1 von Integrität: Daten liegen **integer** vor, wenn man glaubt, dass man aus Sicht des Dateneigentümers unberechtigte oder ungewollte Veränderungen wahrnehmen kann, oder wenn man glaubt, sie vor Veränderung Unberechtigter oder vor ungewollter Veränderung schützen zu können.
  Definition 2 von Integrität: Schutz der Genauigkeit und Vollständigkeit der Information und Prozessmethoden.
- **Authentizität** – Schutz vor gefälschter Identität/Herkunft
  Bedrohung: Eine Entität bzw. Ressource (z.B. Mensch, Prozess, System) gibt vor, jemand anderes zu sein. Dadurch wird ihr unter Umständen unberechtigterweise Zutritt zu sensiblen Daten gewährt, oder es wird angenommen, dass die vorliegende und zu prüfende Information von jemand anderem stammt.

[10] Hier wurde bewusst das Wort „glauben“ verwendet, damit klar zum Ausdruck kommt, dass es keine 100% Sicherheit gibt. Man hätte auch das Wort „annehmen“ im Sinne von „vermuten“ verwenden können. Bewusst wurde der Ausdruck „gewährleisten“ in diesem Zusammenhang vermieden.

Definition 1von Authentizität: Die Daten oder Informationen liegen **authentisch** vor, wenn man glaubt, zu wissen, von welcher Entität die Daten oder Informationen stammen.
Definition 2von Authentizität: Die Authentizität ist die Bestätigung, dass die Daten von einer Entität stammen, wie von dieser angegeben oder behauptet (s. ISO 7498-2).

- **Verfügbarkeit** – Schutz vor Ausfall der IT-Systeme oder der Kommunikationswege
  Bedrohung: Dringend benötigte Informationen sind nicht mehr zugänglich, verfügbar oder lassen sich nur mit viel Aufwand oder nach einer gewissen Zeitspanne wieder einsehen und bearbeiten.
  Definition von Verfügbarkeit: Die Entität, bzw. Ressource A ist **verfügbar**, wenn sie einer autorisierten Entität in gewünschter Form und innerhalb einer zuvor definierten Zeit zugänglich und einsehbar ist.

Die oben genannten Sicherheitsdienste sind nicht vollständig (s. ISO 7498-2), doch sind dies grundsätzlich die wichtigsten. Weitere Sicherheitsdienste ergeben sich aus der Kombination oder aus einer Folge der oben genannten Sicherheitsdienste.

- **Nichtabstreitbarkeit** – Schutz vor Abstreitbarkeit des Empfangs oder Versands einer Nachricht.
  Bedrohung: Falls der Versand oder Erhalt der Informationen abgestritten werden kann, so kann kein verbindlicher Austausch von Informationen stattfinden .
  Definition von Nichtabstreitbarkeit des Senders: Der Empfänger erhält einen Beweis dafür, dass die Daten vom besagten Sender stammen. Dieser kann dann den Versand nicht bestreiten.
  Definition von Nichtabstreitbarkeit des Empfängers: Der Sender erhält einen Beweis dafür, dass die Daten beim Empfänger eingetroffen sind. Dieser kann dann den Erhalt nicht bestreiten.
- **Autorisierung** – Schutz vor der Zuteilung zu vieler und zu wenig Rechten.
  Bedrohung: Bei der Zuteilung zu vieler Rechte (Privilegien) erhält eine Entität unberechtigt Zugriff auf Daten, während bei der Zuteilung zu wenig Rechten die gewünschten Funktionen nicht vollumfänglich oder gar nicht genutzt werden können, obwohl die Entität dazu berechtigt ist.
  Definition von Autorisierung: Das korrekte Zuteilen der zuvor definierten Rechte (Privilegien) an eine Entität, nachdem diese authentisiert worden ist.

Die Verschlüsselung von Informationen (Kryptographie) ist unter anderem ein wichtiges Hilfsmittel zum Schutz der Vertraulichkeit, doch müssen infolge der Aufbewahrungsvorschriften und allfälliger Haftungsansprüche sowie der Bestimmung der Verantwortlichkeit auch die Authentizität, die Integrität und die Verfügbarkeit in hohem Masse mit anderen und den dazu notwendigen technischen Mitteln geschützt werden. Hohe Verfügbarkeit wird unter anderem durch Vielfalt, Zugriffsschutz, Verteiltheit oder/und Redundanz erreicht.

8.3 Schutzbedarf

Der Schutzbedarf muss für jede IT-Anwendung oder Dienst (Use Case) ermittelt werden. Er orientiert sich an den möglichen Schäden, welche aus der Beeinträchtigung der betroffenen IT-Anwendung resultieren können sowie der Eintrittswahrscheinlichkeit.

Die Ermittlung des Schutzbedarfs wird im zivilen Teil des Bundes gemäss der Bundesinformatikverordnung (BinfV, SR 172.010.58) und der darauf basierenden Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung (WIsB) und deren Anhänge abgewickelt. Ist ein erhöhter Schutzbedarf ausgewiesen, muss in Zusammenarbeit zwischen dem Leistungsbezüger und dem Leistungserbringer ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellt werden. Beurteilt werden die Risiken anhand des Produkts aus Eintrittswahrscheinlichkeit, Schadensausmass und einer Gewichtung. Folgende Kategorien werden unterteilt:

Stufe	Bemerkung	Beschreibung
1	Unwahrscheinlich	Möglich aber eher unwahrscheinlich
2	Selten	Tritt selten ein, aber man muss mit Eintritt rechnen
3	Gelegentlich	Tritt gelegentlich ein
4	Wahrscheinlich	Kommt oft vor
5	Häufig	Kommt laufend vor

Tabelle 8-1 Eintretenswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit in der IT zu bestimmen ist in Anbetracht der sich fast täglich ändernden Bedrohungslage schwierig oder nicht wirtschaftlich und zweckmässig. Deshalb ist darauf verzichtet worden, quantitative Angaben zu machen.

Anmerkung: In der folgenden Tabelle ist bewusst darauf verzichtet worden, absolute Zahlen zum Schadensausmass anzugeben, weil für die Privaten oder die Verwaltung auf kantonaler oder kommunaler Ebene Schadensbeträge unterschiedlicher Höhe bereits als kritisch oder katastrophal gelten.

Stufe	Auswirkung	Beurteilungskriterien
1	Vernachlässigbar	Die Einhaltung gesetzlicher und vertraglicher Pflichten ist nicht gefährdet. Die Aufgabenerfüllung wird höchstens geringfügig beeinträchtigt. Persönlichkeitsrechte sind nicht gefährdet Umweltschäden sind minimal Unfälle oder Krankheiten ohne Arbeitsabwesenheiten Kein Imageschaden für die Bundesverwaltung
2	Marginal	Die Einhaltung gesetzlicher und vertraglicher Pflichten ist gefährdet oder die Erfüllung wesentlicher Aufgaben ist beeinträchtigt. Persönlichkeitsrechte sind gefährdet Umweltschäden, welche wieder gut gemacht werden können. Unfälle oder Krankheiten mit mehreren verlorenen Arbeitstagen aber ohne bleibende Schäden sind möglich. Imageschaden für die Bundesverwaltung ist klein und von kurzer Dauer (kein Fernsehen und höchstens Kurzmeldung in der Presse).
3	Kritisch	Die Einhaltung gesetzlicher und vertraglicher Pflichten stark eingeschränkt oder die Erfüllung wesentlicher Aufgaben verunmöglicht. Persönlichkeitsrechte sind in hohem Masse gefährdet. Umweltschäden, welche wieder gut gemacht werden können Unfälle oder Krankheiten mit Hospitalisierung und bleibenden Schäden (Teil-Invalidität). Grösserer Imageschaden für die Bundesverwaltung (Artikel in Presse, aber nicht Seite 1 - kein Fernsehen).
4	Katastrophal	Einhaltung gesetzlicher und vertraglicher Pflichten bzw. die Erfüllung wesentlicher Aufgaben verunmöglicht. Verletzung der Persönlichkeitsrechte Leib und Leben sind gefährdet. Bleibende Umweltschäden entstehen. Grosser Imageschaden für Bundesverwaltung (Seite 1-Meldung in Presse und Fernsehen).

Tabelle 8-2 Schadensausmass

Um die jeweiligen Anwendungen (Use Cases) sicherheitstechnisch zu bewerten, muss den verschiedenen Schutzzielen (gemäss Art. 3 Abs. 5 BinfV die Integrität, Verfügbarkeit, Vertraulichkeit und Nachweisbarkeit) je eine Schutzbedarfskategorie zugeordnet werden. (Dieser Vorgang wird auch als Klassifikation bezeichnet.). Analog zum Deutschen Grundschutzhandbuch (IT-Grundschutzhandbuch des BSI; http://www.bsi.bund.de/gshb/) sind hier die

Schutzbedarfskategorie um die Authentizität und die Nachvollziehbarkeit erweitert worden, im Bewusstsein, dass Integrität und Authentizität unterschiedliche Begriffe enthalten und es Sicherheitsdienste gibt, welche wohl einen erhöhten Bedarf an Integrität nicht aber an Authentizität benötigen.

Weiter ist es empfehlenswert, auch den Zeitfaktor des Schutzbedarfs einer jeweiligen Kategorie zuzuordnen. Z.B. müssen gewisse Daten nur über eine kurze Zeitspanne bezüglich der Vertraulichkeit geschützt sein, während andere Informationen, wie private Schlüssel oder Geheimelemente, über Jahre bezüglich der Vertraulichkeit geschützt werden müssen.

Anmerkung: Einen hohen Schutz der Vertraulichkeit setzt einen hohen Schutz an Authentizität voraus, denn es ist notwendig zu wissen, an wen man die vertrauliche Nachricht sendet oder von wem man eine vertrauliche Nachricht bekommt. Dass Vertraulichkeit im Allgemeinen Authentizität voraussetzt, geht aus der Definition von [SNR CWA 14842-3] hervor. Der Schutz vor unautorisiertem Zugang setzt eine Autorisierung voraus, welche wiederum nur vorgenommen werden kann, wenn die autorisierende Entität authentisiert worden ist.

8.3.1 Sicherheitsstandards für die Ermittlung des Schutzbedarfs

Der Schutzbedarf darf nicht alleine an den möglichen materiellen Schäden bemessen werden, sondern muss auch die möglichen immateriellen Schäden berücksichtigen. Dies ist u.a. bei der Verarbeitung von personenbezogenen Daten besonders zu berücksichtigen. Die gesetzlichen, namentlich die datenschutzrechtlichen Rahmenbedingungen und die strafrechtlichen Geheimhaltungspflichten, sind deshalb einzuhalten. SAGA.ch verzichtet auf die Erläuterung von Datenschutzmassnahmen. Hinweise zum Datenschutz von Bundesbeauftragten sind von den Datenschutzbeauftragten des Bundes und der Kantone geregelt. Deutschland hat für den Datenschutz bezüglich Gefährdungen und Massnahmeempfehlungen einen Vorschlag für ein Datenschutzkapitel in SAGA.de ausgearbeitet.

Für den jeweiligen Use Case muss der Schutzbedarf für die einzelnen Prozesse, die jeweiligen Kommunikationsabschnitte und –szenarien definiert werden. Bei der Ermittlung oder Festlegung des Schutzbedarfs sollten unter anderem folgende Punkte berücksichtigt werden:

- Materielle Schäden (unmittelbare und mittelbare)
- Immaterielle Schäden (unmittelbare und mittelbare) wie Ruf oder Ansehen
- Gesetzliche Bestimmungen
- Wirtschaftlichkeit, wie Kosten, Praktikabilität und Akzeptanz

Eine konkrete Anleitung zur Ermittlung des Schutzbedarfs muss noch ermittelt und in Form eines Standards oder einer Empfehlung festgehalten werden.

8.3.2 Massnahmen

Nachdem der Schutzbedarf pro Sicherheitsziel definiert worden ist, muss festgelegt werden, mit welchen kryptographischen und technischen Mitteln das jeweilige Schutzziel (Authentizität, Vertraulichkeit, usw.) zu schützen ist. Die konkreten Sicherheitsmassnahmen orientieren sich an den jeweils aktuellen internationalen Standards wie ISO/IEC 17799/27001 oder

den IT-Grundschutz-Katalogen des BSI (Bundesamt für Sicherheit in der Informationstechnik).

Beispiel: In der ersten Kolonne der folgenden Tabelle sind die jeweiligen Kategorien von Schutzbedürfnissen für die Authentizität aufgelistet. In der zweiten Kolonne ist aufgeführt, mit welchen Massnahmen der jeweilige Schutzbedarf geschützt wird.

Auswirkung (Risiko) Authentizität	Massnahmen
Vernachlässigbar	Keine Massnahme erforderlich
Marginal	Username und Passwort, Einmalpasswort
Kritisch	MAC, HMAC, Digitale Unterschriften, Schlüsseltransport mit kurzen Schlüsseln
Katastrophal	MAC, HMAC, Digitale Unterschriften, Schlüsseltransport mit Schlüsseln einer bestimmten Mindestlänge, wobei die Erzeugung der Schlüssel gewissen Kriterien genügt.

Tabelle 8-3 Schutzbedarfskategorien und Massnahmen

Es handelt sich hier um ein Beispiel und nicht um eine Empfehlung. Die Zuordnung Schutzkategorie zu den entsprechenden Massnahmen muss noch ermittelt und in Form eines Standards oder Empfehlung festgehalten werden.

8.4 Systemmanagement als Voraussetzung der Systemsicherheit

Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für die Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems.

Die internationale Norm ISO/IEC 27002 enthält einen Leitfaden für das Informationssicherheits-Management.

ISO/IEC 27001, 27002	Empfohlen

Standards: www.snv.ch, www.iso.org

Die internationale Norm ISO/IEC 19770-1 definiert ein Prozess-Framework für die Verwaltung von Software wie insbesondere ausführbare Software (wie Betriebssystem, Anwendungsaprogramme und Hilfsprogramme), aber auch nicht-ausführbare Software (wie Fonts, Grafiken, Audio- und Video-Aufzeichnungen, Dokumente und Daten). Dabei geht es nicht nur um lizenzrechtliche Aspekte: Auch für das Management der Systemsicherheit sind zuverlässige Informationen darüber, welche Programme wo installiert sind, eine wichtige Voraussetzung.

ISO/IEC 19770-1	Unter Beobachtung

Standards: www.snv.ch, www.iso.org

8.5 Kryptographische Algorithmen

In diesem Unterkapitel werden die kryptographischen Algorithmen definiert, welche im Rahmen von ***eCH*** zum Einsatz kommen dürfen. Nicht aufgeführte Algorithmen gelten als nicht empfohlen. Dabei werden die Verfahren in folgende Kategorien unterteilt:

- Public Key Kryptographie (basiert auf asymmetrischen Verschlüsselungsverfahren)
- Symmetrische Kryptographie
- Steganographie
- Hashfunktionen
- Zufallszahlengeneratoren

Bei den kryptographischen Verfahren gibt es zu bestimmende Sicherheitsparameters u.a. Keylängen, Gruppengrössen und weitere siehe ECRYT II (www.ecrypt.eu.org ; Report on Algorithms and Keysizes 2011) *und auch www.NIST.org, www.BSI.de, www.rsa.com, NESSI (* Networked European Software and Services Initiative).

Im ISO/IEC JTC1/Sc27 Standardswerk sind Sicherheitsmechanismen (versus Sicherheitsalgorithmen) beschrieben.

8.5.1 Public Key Kryptographie

RSA	Dringend empfohlen

Je nach Anwendung (Use Case) und Schutzbedürfnis gilt das RSA Verfahren nur als „Unter Beobachtung“.

Standards: ISO/IEC 14888 (1-2), 18033-2, IETF RFC 3447, PKCS#1 v.2.1, IEEE P1363. Wie das Verfahren funktioniert, ist in [Sch] und [Stw] beschrieben.

Diffie-Hellman	Empfohlen

Je nach Anwendung (Use Case) und Schutzbedürfnis gilt das Diffie-Hellman Verfahren nur als „Unter Beobachtung“.

Standards: IEEE P1363. Wie das Verfahren funktioniert, ist in [Sch] und [Stw] beschrieben.

Elliptische Kurven	Empfohlen

Je nach Anwendung (Use Case) und Schutzbedürfnis gelten Elliptische Kurven nur als „Unter Beobachtung“.

Standards: ISO/IEC 15946 (all parts), 14888-3, 18033-2, IETF RFC 5639: IEEE P1363. Eine Einführung zu Elliptischen Kurven findet der Leser bei [Sad] und [Mud].

Bei den Technischen und Administrativen Vorschriften des Bakom [TAV] wird über den ETSI Standard TS 101 456 auf den Standard ETSI TS 102 176 verwiesen. Darin oder im Dokument [Bek] der RegTP (www.regtp.de) sind die Parameter und die Schlüssellängen für die Public Key Algorithmen (für den Einsatz von elektronischen Signaturen) definiert. Für RSA ist im ETSI TS 102 176 u.a. angegeben worden, nach welcher Methode die Primzahlen zu generieren sind.

8.5.2 Symmetrische Kryptographien

Bei den Verfahren sollten die Daten vor der Verschlüsselung noch komprimiert werden.

IDEA	Empfohlen

Standards: IDEA wird in vielen Standards wie SSL und TLS erwähnt, ohne selbst ein Standard zu sein. Wie das Verfahren funktioniert, findet der Leser in [Sch] und [Stw]. Der Einsatz von IDEA war lizenz- und gebührenpflichtig. Die entsprechenden Patente sind im 2010 in USA und 2011 in Europa abgelaufen.

DES mit 56 Bit Schlüssel	Nicht empfohlen

3DES mit 112 Bit Schlüssel	Empfohlen

Standards: ISO/IEC 18033-3

3DES mit 168 Bit Schlüssel	Dringend empfohlen

Standards: ISO/IEC 18033-3; Wie 3DES funktioniert, findet der Leser in [Sch] und [Stw].

AES	Empfohlen

Standards: ISO/IEC 18033-3; “ MISTY, CAST, HIGHT, Camellia, SEED “ sind im ISO/IEC 18033-3 beschrieben.

Bei AES besteht die Möglichkeiten, Schlüssel mit 128,192,256 Länge einzusetzen. Aufgrund einer Schwäche des Verfahrens mit 256 Bitschlüssellänge ist dies nicht unbedingt sicherer als mit kürzeren Schlüsseln.

Wenn möglich, sollte die Verschlüsselung im CBC Mode erfolgen, und das Padding minimal gehalten werden, (s. [Vau]).	Empfohlen

Standards: Modes of Operation (inkl.CBC Mode) ISO/IEC 10116, 18033-4 (die Anwendung auf Blockchiffren). Der Counter Mode ist „ähnlich sicher“ wie CBC. Bezüglich Padding; kritisch ist die Kombination von Chiffrierung, Padding und MACing ; siehe auch CCM (NIST Special Publication 800-38C), oder eine Auswahl solcher Verfahren.

Kompression	Empfohlen

Die Kompression als solche ist keine Verschlüsselungstechnik, aber eine Kompression vor der Chiffrierung steigert den Schutz der Vertraulichkeit, s. dazu [Mau].

Für die Generierung der Zufallszahlen für die Schlüssel sei den ETSI Standard ETSI TS 102 176 verwiesen (s. dazu auch Kapitel 8.5.5 „Zufallszahlengeneratoren“).

8.5.3 Steganographie

Steganographie als Mittel zur unerkannten (vertraulichen) Übermittlung vertraulicher Nachrichten wird sich im eGovernment kaum durchsetzen, weil die Übermittlung im eGovernment Umfeld standardisiert und das dabei verwendete Verfahren allgemein zugänglich sein muss. Ist allgemein bekannt, dass Steganographie eingesetzt wird, so ist Steganographie nicht mehr unerkannt, sondern allgemein bekannt. (Mehr zu Steganographie s. u.a. [Sad]).

Für die Hinterlegung von Informationen zum Schutz der Urheberrechte könnte es aber in Zukunft von Bedeutung sein, doch sind die Verfahren noch nicht sehr sicher und robust. Der Bereich der Steganographie, welche sich mit der Einbindung von Urheberinformationen beschäftigt, wird als Digital Watermarking bezeichnet.

Steganographie zum Schutz von Urheberrechten	Unter Beobachtung

8.5.4 Hashfunktion

SHA-1	Nicht empfohlen

Die Sicherheit ist nicht mehr gewährt.

Standards: Hashfunktionen siehe ISO/IEC 10018, FIPS 180-1, IETF RFC 4634

MD5	Empfohlen

Nicht empfohlen, wenn die **Daten über längere Zeit geschützt** werden sollten, wie etwa bei der Signatur für ein Zertifikat oder für einen Vertrag.

Standards: RFC 1321

SHA-2 224/256/384/512	Dringend Empfohlen

Standards: FIPS 180-3/4

SHA-2 224/256/384/512 wurde aus folgenden Gründen so klassifiziert: Bei den Public Key Kryptosystemen Elliptische Kurven und Diffie-Hellmann ist die Untergruppenstruktur q für die Signatur in verschiedenen Standards auf 160 Bit festgelegt worden ist. Damit es aber zu keinen Kollisionen und folglich zu keiner Minderung der Sicherheit der Hashfunktion kommt, muss q in Anzahl Bits grösser als die Länge des Hashwertes sein. Hier besteht noch ein Abgleichungsbedarf. Falls man SHA 224/256/384/512 einsetzt und die Untergruppenstruktur q auf 160 Bit belässt, gewinnt man nicht mehr an Sicherheit als beim Einsatz mit SHA-1.

RIPEMD-160	Empfohlen

8.5.5 Zufallszahlengeneratoren

Die Zufallszahlengeneratoren müssen modular eingebaut sein, so dass sie ersetzt werden können. Zufallszahlengeneratoren sind im ISO/IEC 18031 spezifiziert.

Im Standard ETSI TS 102 176 ist definiert oder wird auf Fachliteratur und Standards verwiesen, wie Zufallszahlen zu generieren sind. Eine Übersicht zu Zufallszahlengeneratoren und entsprechende Literaturhinweise findet der Leser auch bei [MOV].

8.6 Sicherheitsverfahren

8.6.1 Online Authentisierung

8.6.1.1 User Name und Passwort, Einmal-Passwort

User Name und Passwort über eine bezüglich der Vertraulichkeit ungeschützte Leitung bietet wenig bis keinen Schutz. Einmal-Passwörter bieten ebenfalls kaum ausreichenden Schutz, weil die Verbindung nach erfolgter Authentisierung durch einen unberechtigten Dritten übernommen werden kann oder wie bei der Authentisierung mit Passwort die gesandten Informationen verändert, gelöscht und/oder abgehört werden können.

Name und Passwort, Einmal-Passwort über eine ungeschützte Leitung für den Zugang von schützenswerte Daten.	Nicht empfohlen

User Name und Passwort oder Einmal-Passwort über eine bezüglich der Vertraulichkeit und Integrität geschützte Leitung (z.B. in Verbindung mit SSL/TLS) bieten einen relativ guten Schutz bezüglich der Authentizität. IPSEC ermöglicht auch einen Verbindungsaufbau mit Hilfe eines beidseitig bekannten Geheimelements. Dies kann auch ein Passwort sein. Siehe dazu auch Kapitel 8.6.1.5 „MAC/HMAC“.

Name und Passwort, Einmal-Passwort über eine geschützte Leitung (z.B. SSL/TLS) oder zum Aufbau einer IPSEC Verbindung	Empfohlen

8.6.1.2 Challenge Response

Das Challenge Response ist ein Verfahren zur Authentisierung eines Teilnehmers oder einer Instanz. Dabei muss die zu authentisierende Person oder Instanz die Gegenpartei davon überzeugen (Challenge), dass sie ein Geheimnis kennt, ohne dabei das Geheimnis der Gegenpartei mitteilen zu müssen.

Bei den Challenge Response Verfahren gilt es zu unterscheiden, ob im Verfahren ein Session Key zum Schutz der Verbindung vereinbart wird oder nicht. Verfahren, welche die Einigung eines Session Key beinhalten, sind u.a.:

- SSL/TLS
- IPSEC

Für Challenge Response Verfahren, welche keinen Session Key zum Schutz der Verbindung vereinbaren, gelten analog die Empfehlungen aus Kapitel 8.6.1.1.

Challenge Response Verfahren, welche keinen Session Key zum Schutz einer Verbindung vereinbaren, über eine ungeschützte Verbindung.	Nicht empfohlen

Challenge Response Verfahren, welche keinen Session Key zum Schutz einer Verbindung vereinbaren, über eine geschützte Verbindung.	Empfohlen

Empfehlungen zu Challenge Response Verfahren, welche einen Session Key vereinbaren und damit die Verbindung schützen, sind in den Kapiteln 8.8.1 bis 8.8.3 aufgeführt.

8.6.1.3 Digitale Unterschrift

Die Authentizität erfolgt durch eine digitale Unterschrift. Für die digitale Unterschrift werden ein Hashverfahren und ein Public Key Verfahren benötigt. Als Hashfunktion können die im Kapitel 6.3 „Kryptographische Algorithmen“ definierten Verfahren eingesetzt werden. Für die Public Key Verfahren können RSA, Diffie-Hellman oder Elliptische Kurven verwendet werden.

RSA	Dringend empfohlen

Standards: PKCS#7 1.5, RFC 3852, IEEE P1363

Elliptische Kurven und Diffie-Hellman für digitale Unterschriften	Empfohlen

Standards: IEEE P1363, FIPS 186-2.

Bemerkung: Das Verfahren zur Bildung von digitalen Unterschriften mit Diffie-Hellman Public Key Kryptosystem wird als Digital Signature Algorithm, kurz DSA, bezeichnet; mit dem Elliptic Curve Kryptosystem als Elliptic Curve DAS, kurz ECDSA.

8.6.1.4 Schlüsseltransport (nur Session Key)

Beim Schlüsseltransport von Session Keys soll RSA verwendet werden.

RSA	Dringend empfohlen

Standards: Dieses Verfahren ist in SSL/TLS, WTLS zur Server Authentisierung und in IPSEC zur Authentisierung der Kommunikationsteilnehmer implementiert.

Diffie-Hellman und Elliptische Kurven kommen für diesen Bereich in der Praxis nicht zum Einsatz.	Unter Beobachtung

8.6.1.5 MAC/HMAC

Hier werden die Integrität und Authentizität mittels eines Schlüssels (Passwort, Passphrase oder Bitfolge) und einem Hashverfahren gesichert. Dieses Verfahren bezeichnet man auch als MAC (Message Authentication Code). Wird die MAC Anwendung in einer bestimmten und definierten Weise modifiziert, dann spricht man auch vom HMAC Verfahren.

HMAC/MAC	Dringend empfohlen

Standards: HMAC IETF RFC 2104. Zu MAC selber gibt es keinen Standard, wird aber in der Praxis zur Sicherung der Routing-Protokolle eingesetzt.

8.6.2 Biometrische Verfahren

Die biometrischen Verfahren sind noch wenig standardisiert und werden im IT Umfeld zur Authentisierung noch selten eingesetzt.

Biometrische Verfahren	Unter Beobachtung

Standards: siehe ISO/IEC JTC1/Sc37

8.6.3 Langfristig gültige Signatur

Eine langfristig gültige Signatur, wie bei einer Vertragsunterzeichnung oder bei der Herstellung von Zertifikaten, muss mit Hilfe einer Hashfunktion erzeugt werden, welche eine Prüfsumme mit mindestens 160 Bit Länge erzeugt. (Zu den Problemen der langfristigen Aufbewahrung digitaler Signaturen, s. auch [Mud].)

Langfristig gültige Signatur	Empfohlen

Standard: RFC 5126. Der RFC ist technisch äquivalent zum ETSI-Standard TS 101 733 V.1.7.4. Deswegen wurde er hier aufgeführt, obwohl er nur den Status „Informational“ hat.

8.6.4 Online Vereinbarung eines Session Key

Bei den meisten Authentisierverfahren authentisieren sich die Parteien nicht nur, sondern vereinbaren dabei auch noch einen Session Key. Soll die Verbindung nachhaltig bezüglich der Vertraulichkeit geschützt werden, dann sollte zur Vereinbarung des Session Key das Diffie-Hellman Verfahren oder die Elliptischen Kurven hinzugezogen werden.

Nachhaltig geschützt (bezüglich der Vertraulichkeit) muss eine Verbindung (Session) dann sein, wenn über die Verbindung z.B. Schlüssel transportiert werden. Nachhaltig ist die Verbindung dann geschützt, wenn selbst aus Kenntnis der privaten Schlüssel der Kommunikationsteilnehmer der ausgehandelte Session Key nicht bestimmt werden kann.

Bei gewissen Konfigurationsmodi bei SSL/TLS (Technologie u.a. zur Sicherung des Internetbanking) können nach Bekanntgabe des privaten Schlüssels des Server rückwirkend sämtliche Verbindungen zum Server entschlüsselt werden, sofern die ausgetauschten Daten gesammelt worden sind. IPSEC besitzt im Gegensatz zu SSL/TLS diese Schwäche nicht, weil wahlweise das Diffie-Hellman Verfahren oder die Elliptischen Kurven zur Vereinbarung des Session Key hinzugezogen werden können.

Diffie-Hellman oder Elliptische Kurven, falls die Vertraulichkeit nachhaltig geschützt werden muss.	Empfohlen

Vom Ephemeral-Static und Static-Static Mode (zu beiden Begriffen siehe RFC 2631) wird jedoch abgeraten. (Z.B. TLS bietet die Möglichkeit, die Schlüssel mit der erwähnten Methode online zu vereinbaren.)

Standards: IEEE P1363, PKCS#3, RFC 2631. Die Schlüsseleinigung auf Basis von Diffie-Hellman und von Elliptischen Kurven ist u.a. in den IPSEC Standards (RFC 2409, 2412) definiert.

RSA	Unter Beobachtung

Bei RSA basiert jedoch die Schlüsselvereinbarung auf Basis des Schlüsseltransports, siehe Kapitel 8.6.1.4 „Schlüsseltransport“. RSA erhält in diesem Kontext den Status „Unter Beobachtung“, weil es bisher noch kein in den bekannten Sicherheitstechnologien implementiertes Verfahren für die online Vereinbarung eines Session Key mit RSA gibt.

8.7 Authentische, vertrauliche Daten und Verbindungen

Betreffend authentischen Daten und Verbindungen sind unter anderem nachfolgende Aspekte zu beachten:

- Die Authentisierung bei Verbindungen erfolgt online. Wenn das Benutzerzertifikat nicht mehr gültig oder revoziert ist, dann sollte im PKI Umfeld jede auf diesem Zertifikat basierende Authentifizierung für ungültig erklärt werden.
- Die Authentizität der Verbindung muss so lange, wie die Verbindung steht, geschützt werden.
- Der Schutz der Authentizität der Daten bedarf der Nachhaltigkeit. Die Daten müssen unter Umständen (z.B. bei Aufbewahrungspflichten) über die Gültigkeitsdauer des Zertifikats hinweg ihre Authentizität bewahren (s. Standard im Kapitel 0 „Standards: siehe ISO/IEC JTC1/Sc37
- Langfristig gültige Signatur“).
- Die Authentizität im PKI Umfeld kann bei authentischen Verbindungen auch über den Schlüsseltransport mit anschliessendem MAC oder HMAC realisiert werden, während die Authentizität der Daten im PKI Umfeld mittels digitaler Signatur realisiert wird.
- Bei vertraulichen Verbindungen werden die Informationen nur auf der Verbindung geschützt und lagern dann unter Umständen im Klartext auf den Clients oder Server.

- Die Daten lagern abhängig von den Anforderungen möglicherweise verschlüsselt auf dem Datenträger. Der Wechsel der entsprechenden Schlüssel muss so gestaltet werden, dass die mit dem alten Schlüssel verschlüsselten Daten wieder gelesen werden können. Dies stellt eine erhöhte Anforderung an das Key Management.

8.8 Sicherheitstechnologie

Eine Sicherheitstechnologie ist ein Standard, welcher in ein Produkt umgesetzt kann oder eine abgeschlossene Komponente eines Produkts bilden könnte (Halbfertigware)[11]. Eine Sicherheitstechnologie/ -applikation, wie z.B. bei SSL/TLS, besteht aus einer Vielzahl von Sicherheitsverfahren, so dass gewisse Protokolle, Netzwerkabschnitte geschützt werden. SSL z. B. unterstützt für die Authentisierung, Schlüsselvereinbarung, Chiffrierung und Integritätsprüfung der Pakete unterschiedliche Verfahren und Algorithmen.

Zwei Beispiele aus den Möglichkeiten eines Protokollablaufs bei SSL:

- Schlüsseleinigung mit Diffie-Hellman, Authentisierung mit Signatur nach Diffie-Hellman, Verschlüsselung 3 DES, MAC mit Hashfunktion SHA-1
- Schlüsseltransport mit RSA, Authentisierung mit Signatur RSA, Verschlüsselung IDEA im CBC Mode, MAC mit Hashfunktion SHA-1

Folgende Sicherheitstechnologien werden hier für die Standardisierung vorgeschlagen:

- SSL/TLS
- WTLS
- Kerberos
- SSH
- IPSEC
- S/MIME
- XML Security
- PGP
- Web Services Security
- Protokoll für Zeitstempeldienste
- Transaktionssicherheit

Die verschiedenen Sicherheitstechnologien können wahlweise unterschiedliche kryptographische Algorithmen verwenden. Die jeweiligen Sicherheitstechnologien müssen aber auch so konfiguriert werden können, dass nur die im Kapitel 8.3 erwähnten Verfahren verwendet werden dürfen.

Bemerkung: Zusätzlich zur Angabe, ob die jeweilige Sicherheitstechnologie dringend empfohlen, empfohlen, nicht empfohlen ist oder unter Beobachtung steht, wird angefügt, an welcher Schnittstelle S1, S2, S3 sie eingesetzt werden sollte. (Zur Definition von S1, S2, S3 s. Kapitel 5.2 „Schnittstellen“, Seite 22.) Beispiel:

[11] Mehr zur Abgrenzung zu den Sicherheitsverfahren im Kapitel 8.8.

Bei der Sicherheitstechnologie YZ wird folgende Angabe gemacht.

S1 S2

Die Sicherheitstechnologie YZ soll gemäss den dort gemachten Empfehlungen bei der Schnittstelle S1 (Endgerät-System) und S2 (System-System) eingesetzt werden, aber nicht an der Schnittstelle S3 (System-Clearingstelle).

8.8.1 SSL/TLS

Secure Socket Layer (SSL) und Transport Layer Security (TLS) sind Sicherheitstechnologien, welche unter der Anwendungsschicht gemäss Internetmodell und über dem Transportprotokoll TCP eingebaut sind und theoretisch alle Anwendungsprotokolle über TCP absichern können. In der Praxis ist aber meistens nur die Absicherung von HTTP durch die verschiedenen Produkthersteller realisiert worden. SSL und TLS sind etwa zu 95% gleich aufgebaut, doch zueinander inkompatibel.

S1 S2 S3

Secure Socket Layer (SSL) v.3.0	Dringend empfohlen

Standards: Zu SSL v.3.0 gibt es nur einen RFC Draft, doch gilt SSL v.3.0 als de facto Standard.

Secure Socket Layer (SSL) v.2.0	Nicht empfohlen

Transport Layer Security (TLS) 1.0	Dringend empfohlen

Standards: TLS v.1.0 ist von IETF (www.ietf.org) im RFC 2246 definiert.

Transport Layer Security (TLS) Extensions	Empfohlen

Standards: RFC 3546, Tcpcrypt

Transport Layer Security (TLS) 1.1	Empfohlen

Standards: TLS v.1.1 ist von IETF (www.ietf.org) im RFC 4346 definiert.

Transport Layer Security (TLS) 1.2	Unter Beobachtung

Standards: TLS v.1.2 ist von IETF (www.ietf.org) im RFC 5246 definiert.

8.8.2 WTLS

Wireless Transport Layer Security (WTLS) dient der Absicherung der Mobilkommunikation (Handy). WTLS, SSL und TLS sind bezüglich des Meldungsaustausches und des Meldungsinhaltes sehr ähnlich, doch zueinander inkompatibel.

S1

Wireless Transport Layer Security (WTLS)	Empfohlen[12]

Standard: WTLS ist vom WAP Forum (www.wapforum.org) spezifiziert worden, damit WAP Anwendungen gesichert werden können. Hierzu gibt es einen entsprechenden Standard.

8.8.3 Kerberos

Kerberos ist ein Sicherheitsprotokoll, welches vor allem innerhalb eines Verwaltungs- oder Firmennetz zur Sicherung der Client Server Kommunikation und zur Autorisation verwendet wird.

Kerberos	für organisationsinternen Einsatz Empfohlen

Für organisationsübergreifenden Einsatz ist SAML vorzuziehen.

8.8.4 Secure Shell (SSH)

Secure Shell (SSH) wird hauptsächlich zur Sicherung der Kommunikation bei IT-Management Aufgaben, wie die Konfiguration eines Server, verwendet.

S1 S2 S3

Secure Shell (SSH)	Unter Beobachtung

Standards: Secure Shell ist von der IETF (www.ietf.org) seit Januar 06 als Standard verabschiedet worden und in den RFC 4250 bis 4256, 4332, 4344, 4419, 4462 und weiteren definiert worden.

8.8.5 IPSEC

IPSEC dient der Sicherung der IP Pakete (z.B. UDP/TCP Anwendungen u.a. für Virtuelle Private Networks VPN's). Die entsprechenden Standards sind von der IETF (www.ietf.org) in den jeweiligen RFC spezifiziert worden. IPSEC muss unterstützt werden und kann gleichzeitig mit anderen Sicherheitstechnologien eingesetzt werden.

S1 S2 S3

IP Security (IPSEC) V.1.X	Dringend empfohlen

Standards: IPSEC ist von der IETF (www.ietf.org) in den entsprechenden RFC 2402, 2406, 2409, 2412 und in den zugehörigen standardisiert worden.

IP Security (IPSEC) Version 2.0	Nicht empfohlen

IP Security Version 2.0 weist bei der Ableitung der Session Key für die Vertraulichkeit und Authentisierung/Integrität erhebliche Schwächen auf. Insbesondere kann die im ursprüngli-

[12] Ob WTLS eingesetzt wird oder nicht, hängt unter anderem davon ab, ob Dienste im eGovernment via Mobilphon (mit WAP) angeboten werden oder nicht. Falls WAP zum Einsatz kommt und sensitive Daten darüber transportiert werden, dann wird empfohlen, den Datenaustausch mit WTLS abzusichern.

chen RFC Standard 4306 IKE v.2 beschriebene Art der Schlüsselableitung die Brute Force Attacke und die Plausibilitätsprüfung eines Schlüsselkandidaten sehr beschleunigen.

Standards: IKEv2 IETF RFC 5996 und 5998, MIKEY RFC 4738, NAT and IKE RFC3947. Weiteres zur IKE Roadmap http://www.spinics.net/lists/ietf-ann/msg55308.html .

8.8.6 S/MIME

S/MIME steht für Secure MIME und dient der Sicherung der E-Mail und des Datentransports im Store and Forward Modus. Die Sicherungsmechanismen greifen direkt in der Applikation ein (in der Schicht 4 beim Internetmodell).

	S1	S2	S3
Secure MIME (S/MIME) v.2.0	Dringend empfohlen		

Standard: RFC 2311 S/MIME Version 2 Message Specification und zugehörige

	S1	S2	S3
Secure MIME (S/MIME) v.3.1	Empfohlen		

Standards: Die entsprechenden Standards sind von der IETF (www.ietf.org) in dem RFC 3851 und zugehörige spezifiziert worden.

8.8.7 Secure HTTP (S-HTTP)

Protokoll zur Sicherung von http Inhalten. (Nicht verwechseln mit HTTPs, welches als geschütztes HTTP Protokoll über SSL oder TLS bezeichnet wird.)

	S1	S2	S3
Secure HTTP (RFC 2660)	Nicht empfohlen		

Standard: The Secure Hypertext Transfer Protocol (RFC 2660)

8.8.8 XML Security

Als XML Security wird die Sicherung der Dokumente im XML-Format bezeichnet. Darunter fallen:

- XML Signature
- XML Encryption

Ähnlich wie bei S/MIME handelt es sich hier um einen Schutz für eine Store and Forward Kommunikation.

8.8.8.1 XML Signature

XML Signature ist ein gemeinsamer, allgemein anerkannter Standard von den Standardisierungsgremien W3C (www.w3C.org), OASIS (www.oasis-open.org) und IETF (www.ietf.org) (s. RFC 3275).

Dieser Standard beschreibt digitale Signaturen und Authentisierverfahren mit HMAC Verfahren für beliebige Daten (in der Regel jedoch XML), indem ein XML-Schema und ein Regelwerk (für die Generierung und Überprüfung des Signaturwerts) bereitgestellt werden. Die

Signatur kann dabei ein oder mehrere Dokumente bzw. Daten unterschiedlicher Art (Bild, Text, usw.) umfassen.

Für die Platzierung der XML-Signatur gibt es folgende drei Möglichkeiten:

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

Ein zentrales Merkmal von XML Signature ist die Möglichkeit, anstelle des gesamten XML-Dokuments, nur bestimmte Teile davon zu signieren. Zur Authentizität können sowohl HMAC Verfahren, als auch digitale Signaturen eingesetzt werden.

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

	S1	**S2**	**S3**
XML Signature			Dringend empfohlen

Standards: RFC 3275, XML Signature and Syntax Processing Recommendation, February 2002, von W3C (www.w3C.org).

8.8.8.2 XML Encryption

XML Encryption definiert die Verschlüsselung von XML-Dokumenten und ist ein W3C (www.w3C.org) Standard und von OASIS (www.oasis-open.org) anerkannt, jedoch im Gegensatz zu XML Signature noch kein IETF Standard (www.ietf.org).

	S1	**S2**	**S3**
XML Encryption			Dringend empfohlen

Standard: XML Encryption and Syntax Processing Recommendation, December 2002, von W3C (www.w3C.org).

8.8.9 OpenPGP

Pretty Good Privacy (PGP) ist ein Produkt zur Sicherung der E-Mail und wurde von Phil Zimmermann entwickelt. Wegen der weiten Verbreitung und Nutzung hat sich PGP zum de facto Standard „gemausert“. PGP ist in RFC 2440 standardisiert worden. Dieser Standard nennt sich OpenPGP.

Im Unterschied zu S/MIME werden hier andere Datenformate verwendet.

S1	**S2**	**S3**

Open Pretty Good Privacy (OpenPGP), wenn X.509v.3 Zertifikate unterstützt werden.	Empfohlen,

Standards: RFC 2440 für PGP. RFC 3156 spezifiziert die Interoperabilität mit S/MIME.

8.8.10 Web Services Security

Die zunehmende Wichtigkeit von XML als Datenaustausch- und Spezifikationsformat wie auch die Einführung von Web Services als Middleware bewirkt eine aktive Standardisierung von XML-Sicherheitsstandards in den beiden Gremien W3C (www.w3C.org) und OASIS (www.oasis-open.org).

Unter den Begriff "Web Services Security" fallen unterschiedliche Aspekte der Informationssicherheit, wie

- XML Security (s. Kapitel 8.8.8)
- WS-Security (SOAP Message Security)
- WS-SecureConversation
- WS-ReliableMessaging (s. Kapitel 6.8.9.1)
- Security Assertion Markup Language (SAML)
- Web Services Policy Framework, Web Services Policy Attachment und WS-SecurityPolicy
- eXtensible Access Control Markup Language (XACML)
- eXtensible rights Markup Language (XRML)
- WS-Trust
- XML Key Management Standard (XKMS)
- Transaktionssicherheit (engl. Transaction Security)
- WS Security Profiles

8.8.10.1 WS-Security (SOAP Message Security)

SOAP Message Security ist ein Standard zum sicheren Austausch von SOAP Nachrichten über ungeschützte Verbindungen. Dabei werden die Vertraulichkeit, die Integrität und Authentizität der SOAP Meldungen auf Basis von XML Security geschützt. Zudem werden auch noch die Integration von Security Tokens, wie Kerberos Tickets, wie X.509v.3 Zertifikate spezifiziert.

S1 **S2** **S3**

SOAP Message Security V1.1	Empfohlen

Standard: SOAP Message Security (http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf)

8.8.10.2 WS-SecureConversation

WS-SecureConversation ist ein Standard; er erweitert den WS-Security Standard für den sicheren Austausch von SOAP Nachrichten im Falle von Wiederholungen durch die Definition und Austausch von Sicherheitskontexten und Herleitung von Session Keys.

S1	S2	S3

WS-SecureConversation V1.3	Empfohlen

Standard: WS-SecureConversation (http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html)

8.8.10.3 Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) ist ein XML Format, um Informationen über die Authentisierung und Autorisierung representieren und auszutauschen.

S1	S2	S3

Security Assertion Markup Language (SAML) v.1.1	Empfohlen

Security Assertion Markup Language (SAML V1.1) (http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf)

Security Assertion Markup Language (SAML) v.2	Dringend empfohlen

Standard: Security Assertion Markup Language (SAML V2.0) (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

8.8.10.4 Web Services Policy Framework

Web Services Policy Framework ist ein Standard für die Definition von Sicherheitsregeln (policies). Es definiert ein allgemeines Modell für die Syntax und Sematik fürs Formulieren von Sicherheitsregeln. Der allgemeine Rahmen definiert das Generelle zur Syntax und Semantik von Sicherheitsregeln.

S1	S2	S3

Web Services Policy 1.5 - Framework	Empfohlen

Standard: Web Service Policy 1.5 – Framework (http://www.w3.org/TR/ws-policy/)

8.8.10.5 Web Services Policy Attachment

Web Services Policy Attachment ist ein Standard für die Zuordnung von Richtlinien (policies) an Endpunkte, Meldungen, Ressourcen und Operationen.

S1	S2	S3

Web Services Policy 1.5 - Attachment	Empfohlen

Standard: Web Service Policy 1.5 – Attachment (http://www.w3.org/TR/ws-policy-attach/)

8.8.10.6 WS-SecurityPolicy

WS-SecurityPolicy ist ein Standard für die Festlegung von Sicherheits-Beteuerungen für SOAP Message Security, WS-Trust und WS-SecureConversation.

S1 **S2** **S3**

WS-SecurityPolicy 1.2	Empfohlen

Standard: WS-SecurityPolicy (http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.2/ws-securitypolicy.html).

8.8.10.7 eXtensible Access Control Markup Language (XACML)

eXtensible Access Control Markup Language (XACML) ist ein XML Format zum Repräsentieren und Austauschen von Regeln über die Zugangskontrolle (engl. Access Control).

S1 **S2** **S3**

eXtensible Access Control Markup Language (XACML) V2.0	Empfohlen

Standard: eXtensible Access Control Markup Language (XACML) v.2.0, Februar 2005 (http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf)

8.8.10.8 XRML (eXtensible Rights Markup Language)

XRML ist eine XML Sprache zur Spezifikation von Rechten und Bedingungen, welche mit verschiedenen Arten von Quellen und digitalen Inhalten verknüpft werden können. Zudem kann eine Vertrauensumgebung aus mehreren Domänen definiert werden, um über die einzelnen Domänen hinweg die Integrität der Rechte und Bedingungen zu schützen.

Verwendung

Zur Definitionen von Rechten und Bedingungen.

S1 **S2** **S3**

XRML (eXtensible Rights Markup Language) v.2.0	Empfohlen

Standard: XRML (eXtensible Rights Markup Language) v.2.0, November 2001, OASIS (www.oasis-open.org http://www.xrml.org/)

8.8.10.9 WS-Trust

Definiert einen Mechanismus für das Erstellen , Erneuern , Validieren und Annullieren von Sicherheitsmarken auf dem Prinzip des “brokered trust”.

S2 **S3**

WS-Trust 1.3	Empfohlen

Standard: OASIS, WS Trust 1.3, 19.März 2007, http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html

8.8.10.10 XKMS

XML Key Management Specification (XKMS) ist vom W3C Consortium (www.w3C.org) entwickelt worden und definiert die Anbindung von XML Security an eine Public Key Infrastruktur.

XKMS	Empfohlen

Standard: W3C XML Key Management Specification (XKMS), Recommendation 2.0, 28 June 2005

Einschränkung: XKMS eignet sich für Key Management Aufgaben innerhalb einer Verwaltungseinheit oder eines Unternehmens. Im Bereich der verbindlichen Kommunikation (Unterschrift) im eGovernment sind Vorschriften vorhanden, welche die Möglichkeiten von XKMS beträchtlich einschränken und folglich den Einsatz XKMS ohne ein entsprechendes Profil in Frage stellen.

8.8.10.11 Web Services Coordination (WS-Coordination)

Definiert ein erweiterbares Rahmenwerk für die Koordination von verteilten Aktivitäten.

S1 **S2** **S3**

WS-Coordination V1.1 + Errata	Empfohlen

Standard: WS-Coordination (http://docs.oasis-open.org/ws-tx/wstx-wscoor-1.1-spec-errata-os.pdf)

8.8.10.12 Web Services Atomic Transaction (WS-AtomicTransaction)

Definiert die Koordination von verteilten Aktivitäten auf der Basis atomischer Transaktionen.

S1 **S2** **S3**

WS-Transaction V1.1 + Errata	Empfohlen

Standard: WS-Transaction (http://docs.oasis-open.org/ws-tx/wstx-wsat-1.1-spec-errata-os.pdf)

8.8.11 Protokoll für Zeitstempeldienste

Zeitstempel sollen belegen, dass gewisse Dokumente zu einer bestimmten Zeit vorliegen, und enthalten unter anderem eine Zeitangabe und eine Signatur. Zeitstempeldienste werden von einem vertrauenswürdigen Dritten (engl. Trusted Third Party) erbracht. Das Protokoll zur Anforderung von Zeitstempeldiensten und der Auslieferung von Zeitstempel wird im Englischen als Time Stamp Protocol (TSP) bezeichnet und ist im RFC 3161 standardisiert. Zeitstempeldienste werden unter anderem zum Schutz der langfristigen Gültigkeit von digitalen Signaturen eingesetzt (s. Kapitel 0 „Standards: siehe ISO/IEC JTC1/Sc37

Langfristig gültige Signatur“).

Time Stamp Protocol (TSP)	Empfohlen

Standard: RFC 3161

8.9 Übergreifende Datensicherheitsstandards

Übergreifende Sicherheitsstandards umfassen die Standards, welche nicht nur bestimmten Anwendungsfällen, bzw. Kommunikationsszenarien, zugeordnet werden können, sondern bei verschiedenen Sicherheitstechnologien eingesetzt werden können, wie etwa

- Smart Card Anbindung
- Schnittstelle zum Directory
- Zertifikatsinhalte und –formate und Zertifikatsmanagement
- Abfrage des Status eines Zertifikats
- Schnittstelle zur Applikation

8.9.1 Smart Card Anbindung

Unter einer Smart Card wird hier eine Smart Crypto Card verstanden, eine Chipkarte mit Mikroprozessor, welcher die kryptographischen Operationen mit den privaten Schlüsseln vornimmt. Zudem dürfen die privaten Schlüssel den Chip (Mikroprozessor auf der Karte) nicht verlassen.

Es gibt eine Fülle von Standards zu Smart Cards. Hier wird aber nur empfohlen, welche Schnittstellen die Sicherheitstechnologie unterstützen muss, damit sie die Daten an die Smart Card übergeben und von dort das Resultat der Verarbeitung dieser Daten in Empfang nehmen kann.

Andere Medien für die Schlüsselaufbewahrung, wie USB Tokens oder HSM, mit äquivalenten Sicherheitsmerkmalen haben den gleichen Empfehlungsstatus wie eine Smart Crypto Card Anbindung.

ISO/IEC 7816 alle Teile	Dringend empfohlen

ISO/IEC 14443 1-4	Unter Beobachtung

ISO/IEC 15693 1-3	Unter Beobachtung

ISO/IEC 18092 (NFCIP 1)	Unter Beobachtung

Standard: ISO/IEC 21481 (NFCIP-2), ISO/IEC 13157 (NF-SEC).

Für RFID gilt ISO/IEC 18000.

EU Referenzen zur Privacy Data Protection Impact und Opinion WP180 Dokumente:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

Bei kritischem Datentransport müssen ergänzende End zu End Sicherheitsmechanismen vorgesehen werden.

Für die Herstellung der qualifizierten Signatur wird verlangt, dass die Smart Card nach gewissen Sicherheitskriterien zertifiziert worden ist, siehe dazu [TAV].

In [a006d] sind die Anforderungen des Bundes an die Smart Cards selber und deren Ein- und Anbindung definiert. (Informationen zu Chipkarten, siehe [RwEw]).

PC/SC	Dringend empfohlen

URL: www.pcscworkgroup.com

PKCS#11 (soweit Smart Card und HSM relevant)	Dringend empfohlen

URL:http://www.rsa.com/rsalabs/node.asp?id=2124

8.9.2 Schnittstelle zum Directory

Hier wird definiert, welches Protokoll zur Anfrage von Personendaten, Zertifikaten oder CRL Listen von der Sicherheitstechnologie unterstützt werden sollte.

LDAPv.3	Dringend empfohlen

Standards: s. Kapitel 6.6 „Verzeichnisdienste“.

8.9.3 Zertifikatsinhalte und Inhalt der CRL

8.9.3.1 Allgemeines

Die Zertifikatsformate sind in den Standards X.509v.3 und im RFC 5280 standardisiert, wobei in Zweifelsfällen der RFC Standard zu bevorzugen ist. Die Profile qualifizierter Zertifikate werden im Dokument [TAV] des BAKOM und zum Teil im RFC 3739 standardisiert, wobei in Zweifelsfällen die Vorschrift [TAV] des BAKOM verbindlich ist.

Zertifikate werden nicht nur für die Herstellung von Signaturen herausgegeben, sondern z.B. auch zur Verschlüsselung von E-Mail. *Die Zertifikatsinhalte, die Inhalte der CRL und das Zertifikatsmanagement werden jedoch in einem separaten Dokument beschrieben.*

8.9.3.2 Zertifikatsmanagement

Man muss konfigurieren können, welche CA Zertifikate als vertrauenswürdig gelten und welche nicht. Insbesondere müssen auch CA Zertifikate entfernt werden können, welche per default als vertrauenswürdig gelten.

8.9.3.3 Identitätskennung und Zertifikatsinhalte

Nicht nur die Identität, welche im Distinguished Name enthalten ist, sondern sämtliche ins Zertifikat aufgenommenen Identitätskennungen, wie E-Mail Adresse, URL, sind zuerst auf Zugehörigkeit zu prüfen, ansonsten kann die Authentisierung auf Basis von Zertifikaten umgangen werden, s. [Mud].

Mit der Überarbeitung von ElDI-V ist weiter ein technisches Reglement [TAV-MWST] eingeführt worden, welches die zu verwenden digitalen Identitäten in den Zertifikaten im Kontext zur Mehrwertsteuer konformen elektronischen Rechnungsstellung definiert.

8.9.3.4 Ergänzung zum Zertifikat

Zertifikate für Server	Dringend empfohlen

Es sollte zwischen digitaler Authentisierung und digitaler Unterschrift unterschieden werden. Eine digitale Authentisierung beinhaltet lediglich die Identifikation des Absenders. Es wird empfohlen, dass die Authentifikation der Systeme im eGovernment Umfeld gut geschützt ist, damit man sich auf die von dort gelieferte Information verlassen kann. Ein guter Schutz wird mit Public Key Verfahren erreicht. Dazu werden aber Zertifikate benötigt.

Eine digitale Unterschrift beinhaltet immer eine Authentisierung und einen Integritätsschutz. Nach Inkrafttreten des entsprechenden Artikels im OR (14 Abs. 2^{bis}) und des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) kann man (im privaten Geschäftsverkehr) - der Handunterschrift gleichgestellt - elektronisch unterschreiben. Dies gilt aber nur für elektronische Unterschriften von natürlichen Personen.

Will man z.B. die Web Service Dienste (im eGovernment) mit den entsprechenden Sicherheitstechnologien rechtlich verbindlich und gesichert benutzen, dann ist u.a. das Folgende absolut erforderlich (im Sinne einer Forderung nach einem Sollzustand):

- Zertifikate für Server können von nach ZertES anerkannten Zertifizierungsstellen (CA) erstellt, herausgegeben und eingesetzt werden.
- Digitale Unterschriften von einem Server, welche mit den zu diesen Zertifikaten korrespondierenden privaten Schlüsseln hergestellt worden sind, haben eine ähnliche Beweiskraft wie die digitalen Unterschriften von natürlichen Personen, welche zu Art. 14 Abs. 2^{bis} OR konform sind. Sofern entsprechende, noch zu definierende Sicherheitsanforderungen im Umgang mit Serverzertifikaten und mit den dazu passenden privaten Schlüssel eingehalten werden.

Unter anderem sehen wir folgende mögliche Einsatzgebiete:

- Digitale Belege oder Quittungen für die elektronische Geschäftsführung, für die Eingabe von (Rechts)Schriften an das Bundesgericht
- Digitale Belege für den elektronischen Geschäftsverkehr zwischen Privaten und den Bundesämter
- Zeitstempeldienste (Art. 12 ZertES) u.a. für die Archivierung

Mit der Überarbeitung von ElDI-V sind neben den Zeitstempeldiensten und der Signatur von Zertifikaten weitere Anwendung von Server Zertifikaten (Funktionszertifikate) auf Bundesebene eingeführt und definiert worden. Mit der Überarbeitung von ElDI-V ist weiter ein technisches Reglement [TAV-MWST] eingeführt worden, welches die zu verwenden digitalen Identitäten in den Zertifikaten im Kontext zur Mehrwertsteuer konformen elektronischen Rechnungsstellung definiert.

8.9.4 Unterschrift - Digitalisierung der eGov Prozesse

Das ZertES und dessen zugehörige Verordnung [VZertES] und Ausführungsvorschriften [TAV] sind in Kraft.

Durch die entsprechende Revision des Obligationenrechts (OR) sind die elektronischen Signaturen im privaten Geschäftsverkehr zwischen Privaten, nicht aber zwischen Privaten und den Behörden oder behördenintern geregelt, siehe u.a. [DigSig]. Das VwVG (Verwaltungsverfahren auf Bundesebene) ist infolge der neuen Gesetze zum Bundesgericht revidiert worden. Die Dokumente können im Verwaltungsverfahren mit den Behörden bei Zustimmung der Parteien elektronisch eingereicht werden. Dort ist aber die Sendung mit einer anerkannten elektronischen Signatur zu versehen. Dies entspricht einer qualifizierten Signatur, welche mit einem Zertifikat eines nach ZertES anerkannten Anbieters ausgestellt worden wird.

Sinngemäss wird also empfohlen: Dort wo reelle Government Prozesse digitalisiert werden und dabei eine Handunterschrift verlangt wird, soll die Handunterschrift durch eine qualifizierte elektronische Unterschrift ersetzt werden, welche mit einem Zertifikat eines anerkannten Anbieters verifiziert werden kann.

Ab 1.1.2007 gelten das Bundesgerichtsgesetz (BGG) und das Verwaltungsgerichtsgesetz für die elektronische Eingabe von Rechtsschriften an die beiden Gerichte. Dazu werden auch anerkannte qualifizierte Signaturen gefordert.

8.9.5 Herunterladen von Dokumenten mit aktiven Komponenten (Java, JavaScript, ActiveX)

Falls eine Operation mit dem privaten Schlüssel (des Benutzers) vorgenommen werden muss/soll, sei dies nur für die Authentisierung, für das Leisten einer verbindlichen elektronischen Signatur oder für die Entschlüsselung einer E-Mail, dann muss Folgendes beachtet werden:

- Der ganze Vorgang vom Start bis zur Beendigung muss so gestaltet sein, dass keine versteckten Programme wie Java, JavaScript, ActiveX heruntergeladen werden müssen/dürfen.
- Die Applikation beim Endgerät, welche für die eGovernment Dienstleistung benötigt wird, muss so konfiguriert werden können, dass das Herunterladen der genannten Programme nicht erlaubt ist oder das Herunterladen anzeigt.
- Der eGovernment Vorgang muss trotz der genannten Einstellung abgewickelt werden können.

8.9.6 Abfrage des Status eines Zertifikats

Der Status eines Zertifikats kann über die CRL Liste oder mit dem OCSP-Protokoll abgefragt werden. Folgende Protokolle zur Anfrage der CRL Listen sollten von der Sicherheitstechnologie unterstützt werden.

HTTP, LDAP	Dringend empfohlen

Standards: s. Kapitel 6.4 „Anwendungsprotokolle“ und 6.6 „Verzeichnisdienste“.

OCSP	Empfohlen

Standards: s. Kapitel 6.6 „Verzeichnisdienste“.

8.9.7 Schnittstelle zur Applikation

Nachdem eine Entität (z.B. User, Server, Client) auf Basis von Zertifikaten authentisiert worden ist, sollte die Sicherheitstechnologie eine Schnittstelle der Applikation zur Verfügung stellen. Über diese Schnittstelle sollte der Inhalt des Zertifikats der soeben authentisierten Entität übergeben werden können. Zweck dieser Schnittstelle ist es, die Autorisierung auf Basis einer Public Key basierten Authentisierung vorzunehmen. Warum dies so wichtig ist, ist unter anderem in [Mud] und [Nem] beschrieben.

Schnittstelle an die Applikation	Unter Beobachtung

Leider keine Standards diesbezüglich vorhanden.

8.10 Prüfung digitaler Unterschriften

In diesem Kapitel werden Mindestanforderungen an die Prüfung von digitalen Unterschriften gestellt. Die Auflistung der Kriterien basiert auf IETF RFC 3850. Wenn nur einer der folgenden Kriterien erfüllt ist, dann muss die Sicherheitsapplikation eine Fehlermeldung herausgeben und je nach Policy die Verbindung abbrechen.

- Die Signatur kann mit dem Public Key im entsprechenden Zertifikat nicht erfolgreich geprüft werden.
- Die in der Applikation angezeigte oder zugängliche Absenderadresse stimmt nicht mit der Adresse im Zertifikat überein oder ist nicht im Zertifikat enthalten. (Deshalb die Wichtigkeit der Empfehlungen in Kapitel 8.9.3.2 und 8.9.7). Warum hier eine Fehlermeldung wichtig ist, siehe [Mud].
- Die Zertifikatskette führt nicht zu einer CA, welcher man vertraut.
- Die CRL und Revokationsinformationen (z.B. nach OCSP) können nicht überprüft werden.
- Eine ungültige CRL wurde empfangen, oder deren Gültigkeit ist abgelaufen.
- Das Zertifikat ist bereits abgelaufen oder revoziert worden.

Weitere Empfehlungen an die Herstellung und Prüfung von digitalen Unterschriften sind in den technischen Empfehlungen CWA 14170 und CWA 14171 von CEN enthalten.

8.11 Key Management

8.11.1 Generierung der Schlüssel

In *ETSI TS 102 176* ist definiert, wie die Schlüssel für die jeweiligen Public Key Verfahren generiert werden. Dort wird weiter definiert, welche Tests die Zufallzahlengeneratoren erfüllen müssen.

Die Zufallszahlengeneratoren werden auch für die Erzeugung der symmetrischen Schlüssel verwendet.

8.11.2 Aufbewahrung der Schlüssel

s. Kapitel 8.9.1 „Smart Card Anbindung“ und Standard PKCS#11.

8.11.3 Schnittstelle Operation mit (privaten) Schlüssel

s. Kapitel 8.9.1 „Smart Card Anbindung“ und Standard PKCS#11.

Bei der PKCS#12 Anbindung handelt es sich um ein File, welches in die Sicherheitsapplikation eingebunden wird. Die privaten Schlüssel sind dann, im Gegensatz zur Smart (Crypto) Card Anbindung, von der Sicherheitsapplikation lesbar.

PKCS#12 sollte nur im Server Umfeld eingesetzt werden, doch auch hier empfiehlt sich der Einsatz eines HSM.

8.11.4 Schlüsselwechsel infolge Schlüsselerneuerung

Der Schlüsselwechsel bildet für die vertrauliche und authentische Verbindungen nur geringe Probleme (s. auch Kapitel 8.7 „Authentische, vertrauliche Daten und Verbindungen“). Jedoch beim Schutz der Authentizität und Vertraulichkeit der Daten sind besondere Sicherheitsmassnahmen zu treffen.

- Vertraulichkeit: (Public Key) Umverschlüsselungsassistent, Schlüsselwiedergewinnung (engl. Key Recovery), verschlüsselten Folder, wobei mehrere Entitäten auf unterschiedliche Art und Weise auf die Daten zugreifen können.
- Authentizität: s. Kapitel 0 „Standards: siehe ISO/IEC JTC1/Sc37
- Langfristig gültige Signatur“

8.11.5 Vereinbaren eines Session Key

In den verschiedenen Sicherheitsapplikationen/-technologien, wie SSL oder IPSEC sind die Verfahren zur Vereinbarung eines Session Key definiert. Sie basieren meistens auf Schlüsseltransport und online Session Key Vereinbarung (s. Kapitel 8.6.1.4, 8.6.4).

8.11.6 Schlüsseltransport

ISO/IEC 11770 1-4 Schlüsseltransport	Unter Beobachtung

Standard: ISO/IEC 11770 1/4 . In den Teilen 2/3 sind keine Meldungsheader (Nr.), Fehlermeldungen (etc.) im Sinne Transportprotokolle erwähnt, ergo wäre dies noch unvollständig.

8.12 Koordination

Es bedarf einer Koordination der Namensgebung (z.B. WS Addressing), der Zertifikatsinhalte, der Autorisierung und Authentisierung und der Interaktionen der einzelnen Sicherheitstechnologien (z.B. SSL/TLS mit SAML), damit die Sicherheit durchgängig ist und keine Unterbrüche erfährt. Unterbrüche sind z.B. dann vorhanden, wenn während des Geschäftsprozesses ein WS Consumer sich mehrmals (und unterschiedlich) authentisieren muss. *Diese Koordination sollte beobachtet und weiter standardisiert werden.*

9 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt, oder welche **eCH** referenziert, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

10 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliography

Fachliteratur

[a006d] a006d Smart Card Version 1.3, Informatikrat des Bundes, Pascal Horner, Stefan Zbinden

[AcLs] Adams Carlisle, Lloyd Steve, Understanding Public-Key Infrastructure, MTP Publishing 1999, ISBN 1 57870 166 x

[Bek] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung vom 2. Januar 2004, RegTP

[FiR] Roy T. Fielding, Architectural Styles and the Design of Network-based Software Architectures, Dissertation an University of California Irvine, www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

[GSHB] Grundschutzhandbuch, Hrsg. Deutsches Bundesamt für Sicherheit, ISBN 3 88784 915 9, http://www.bsi.de/gshb/deutsch/menue.htm

[GuA] Gustavo Alonso, et al., Web Services, Springer Verlag, 2003, ISBN 3 540 44008 9

[Hem] Hein Mathias, TCP/IP, Thomson Publishing, 1998, 4. Auflage, ISBN 3 8266 4035 7

[Hermes] Hermes, Führen und Abwickeln von Projekten der Informations- und Kommunikationstechnik, Herausgeber Informatik Strategieorgan Bund, Art.-Nr. 609.201 (Verkauf bei Bundespublikationen)

[Mau] Maurer Ueli, Provable Security in Cryptography, Diss. ETH (Nr. 9260) 1990, referee J. Massey, co-referee W. Diffie

[MOV] Alfred Menezes, Paul van Orschot, Vanstone Scott, Handbook of Applied Cryptography, CRC Press 1996, ISBN 0 8493 8523 7 http://cacr.math.uwaterloo.ca/hac/

[Mud] Muster Daniel, Digitale Unterschriften und PKI, 3. Auflage 2006, ISBN 3 9522387 3 3

[Nem] Mark O'Neal, et al, Web Services Security, Mc Graw Hill/ Osborne, 2003, ISBN 0 07 222471 1

[NaMa] Nussbacher Alfred, Mistlbacher August, XML Entpackt, MITP Press, 2002, ISBN 3 8266 0884 4

[RwEw] Rankl Wolfgang, Effing Wolfgang, Handbuch der Chipkarten, 3. Auflage, Carl Hanser Verlag 1999, ISBN 3 446 21115 2

[Sad] Salomon David, Data Privacy and Security, Springer Verlag 2003, ISBN 0 387 00311 8

[Sch] Schneier Bruce, Angewandte Kryptographie, Addison Wesley, 1. Auflage 1996, ISBN 3 89319 854 7

[Stw] Stallings William, Network and Internetwork Security, Prentice Hall 1995, ISBN 0 13 180050 7

[Vau]	Vaudenay Serge, Security Flaws induced by CBC Padding Applications to SSL, IPSEC, WTLS, Advances in Cryptology EUROCRYPT 02, Amsterdam, Netherland, Lecture Notes in Computer Science No. 2332, pp. 534-545, Springer-Verlag, 2002 oder bei: http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Vau02a
[WSA]	Web Services Architecture, W3C Working Group Note 11 February 2004 www.w3.org/TR/2004/NOTE-ws-arch-20040211/
[ZeCs]	Zwicky Elisabeth, Copper Simon, Einrichten von Internet Firewalls, O'Reilly 2001, ISBN 3 89721 346 X
[ZoT]	Zimmermann Olaf, Mark Tomlinson, Stefan Peuser, Perspectives on Web Services, Springer Verlag 2003, ISBN 3 540 00914 0
eGIF	eGovernment Interoperability Framework, EIF European Interoperability Framework
eGov Standard Frankreich	Le cadre commun d´interoperabilité des systemes d'information publics
SAGA.de	Standards und Architekturen für E-Government-Anwendungen in Deutschland, V.4.0, Bundesministerium des Innern
eGIF Neuseeland	http://archive.ict.govt.nz/plone/archive/standards/e-gif/e-gif-v-3-3/standards.1.html Interoperability eGIF Version 3.3 Part.1 Standards

Erlasse (www.admin.ch Systematische Rechtssammlung)

[TAV]	Technische und administrative Vorschriften des BAKOM vom 6. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)
[TAV-MWST]	Verordnung der ESTV vom 12.Oktober 2007 über Zertifizierungsdienste im Bereiche EIDI-V: Technische und administrative Vorschriften des EFD über Zertifizierungsdienste im Bereich ElDI-V im Zusammenhang mit der Ausstellung von Zertifikaten basierend auf fortgeschrittenen Zertifikaten (SR 641.201.11)
BGG	Bundesgesetz vom 17. Juni 2005 über das Bundesgericht (SR 173.110)
BinfV	Verordnung vom 26. September 2003 über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung ; SR 172.010.58)
ElDI-V	Verordnung des EFD vom 30. Januar 2002 über die elektronisch übermittelten Daten und Informationen (SR 641.201.1)
OR	Bundesgesetz vom 30.März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht ; SR 220)
VGG	Bundesgesetz vom 17. Juni 2005 über das Verwaltungsgericht (SR 173.32)
VwVG	Bundesgesetz vom 20. Dezember 1968 über das Verwaltungsverfahren (SR 172.021)
VZertES	Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)
WIsB	Weisung Informatiksicherheit Bund CH (IRB)
ZertES	Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)

CEN Standards (www.cen.eu)

CWA 14170: CEN (European Committee for Standardization), Security Requirements for Signature Creation Applications, May 2004

CWA 14171 CEN (European Committee for Standardization), General Guidelines for electronic signature verification, May 2004

eCH (www.ech.ch)

eCH-0018	XML Best Practices
eCH-0036	Dokumentation für den XML-orientierten Datenaustausch

ECMA (www.ecma-international.org)

Open Office XML Format

ESTI (www.etsi.org)

ETSI TS 102 176 v.1.2.1	Electronic Signatures and Infrastructures (ESI) - Algorithms and Parameters for Secure Electronic Signatures

IEEE Standards (www.ieee.org)

IEEE P1363	Standard for RSA, Diffie-Hellman and related Public-Key Cryptography

IETF Standards (www.ietf.org)

RFC 768	User Datagram Protocol
RFC 791	Internet Protocol
RFC 793	Transmission Control Protocol
RFC 959	File Transfer Protocol
RFC 1050	Remote Procedure Call Protocol Specification
RFC 1123	Requirements for Internet Hosts - Application and Support
RFC 1180	TCP/IP Tutorial
RFC 1321	The MD5 Message Digest Algorithm
RFC 1349	Type of Service in the Internet Protocol Suite
RFC 1730	Internet Message Access Protocol Version 4
RFC 1750	Randomness Recommendations for Security
RFC 1831	Remote Procedure Call Protocol Specification. Version 2
RFC 1866	Hypertext Markup Language - 2.0.
RFC 1939	Post Office Protocol - Version 3
RFC 1945	Hypertext Transfer Protocol 1.0
RFC 1952	GZIP file format specification version 4.3
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types

RFC 2047	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
RFC 2048	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2104	HMAC Keyed-Hashing for Message Authentication
RFC 2228	FTP Security Extensions
RFC 2242	Security Architecture for the Internet Protocol
RFC 2246	Transport Layer Security (TLS)
RFC 2251	LDAPv.3 Lightweight Directory Access Protocol
RFC 2311	S/MIME Version 2 Message Specification und zugehörige
RFC 2315	PKCS #7: Cryptographic Message Syntax Version
RFC 2402	IP Authentication Header
RFC 2407	DOI The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408	ISAKMP Internet Security Association and Key Management Protocol
RFC 2409	The Internet Key Exchange
RFC 2412	The Oakley Key Determination Protocol
RFC 2439	POP3 Extension Mechanism
RFC 2440	PGP Message Exchange Formats
RFC 2460	Internet Protocol, Version 6 (IPv6)
RFC 2518	HTTP Extensions for Distributed Authoring – WEBDAV
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
RFC 2616	Hypertext Transfer Protocol 1.1
RFC 2631	Diffie-Hellman Key Agreement Method
RFC 2634	Enhanced Security Services for S/MIME
RFC 2640	Internationalization of the File Transfer Protocol
RFC 2817	Upgrading to TLS Within HTTP/1.1
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format
RFC 2854	The 'text/html' Media Type.
RFC 2965	HTTP State Management Mechanism
RFC 3126	*Electronic* Signature Formats for long term electronic Signatures
RFC 3156	MIME Security with Pretty Good Privacy (PGP)
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
RFC 3174	US Secure Hash Algorithm 1 (SHA-1)

RFC 3232	Assigned Numbers
RFC 3275	XML Signature Syntax and Processing
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3384	LDAP (version 3) Replication Requirements
RFC 3447	Public-Key Cryptography Standards (PKCS) #1
RFC 3534	The application/OGG Media Type
RFC 3546	Transport Layer Security (TLS) Extensions
RFC 3739	Qualified Certificates Profile
RFC 3850	S/MIME v.3.1 Certificate Handling
RFC 3851	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1
RFC 3852	Cryptographic Message Syntax
RFC 4180	Common Format and MIME Type for Comma-Separated Values (CSV) Files
RFC 4252	The Secure Shell (SSH) Authentication Protocol
RFC 4253	The Secure Shell (SSH) Transport Layer Protocol
RFC 4288	Media Type Specifications and Registration Procedures BCP
RFC 4289	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures BCP
RFC 4294	IPv6 Node Requirements
RFC 4306	The Internet Key Exchange (IKE v.2) Protocol
RFC 4346	The Transport Layer Security (TLS) Protocol Version 1.1
RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol
RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models
RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms?
RFC 4634	US Secure Hash Algorithms (SHA and HMAC-SHA)
RFC 4918	HTTP Extensions Web Distributed Authoring and Versioning (WebDAV)
RFC 4918	HTTP Extensions Web Distributed Authoring and Versioning (WebDAV)
RFC5095	Deprecation of Type 0 Routing Headers in IPv6
RFC 5096	Mobile IPv6 Experimental Messages
RFC 5126	CMS Advanced Electronic Signatures (CAdES)
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2

RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5785	Defining Well-Known Uniform Resource Identifiers (URI's)
RFC 5797	FTP Command and Extension Registry

ISO Standards (www.iso.org)

ISO 15929: 2002	Graphic technology -- Prepress digital data exchange -- Guidelines and principles for the development of PDF/X standards
ISO 15930 1-8	Graphic technology - Prepress digital data exchange - Use of PDF
ISO 19005-1: 2005	Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)
ISO 7498-2	Information processing systems, Open Systems Interconnection, Basic Reference Model Part 2 Security Architecture
ISO/IEC 7816 1-4	Identification Cards-Integrated Circuits
ISO/IEC 29500-1-4	Information technology - Document description and processing languages - Office Open XML File Formats
ISO/IEC 14496-14	Information technology - Coding of audio-visual objects - Part 14: MP4 file format
ISO/IEC 16262	Information technology - ECMAScript language specification

ITU Standards (www.itu.org)

ITU-T X.509v.3	Information Technology - Open Systems Inter-connections - Public Key and Attribute Certificate Framework
ITU-T X.519	Information Technology - Open Systems Inter-connections – The Directory: Protocol Specification
ITU-T X.525	Information Technology - Open Systems Inter-connections – The Directory: Replication

NIST Standards (www.nist.gov)

FIPS 46-3	DES Digital Encryption Standard
FIPS 81	DES Modes of Operation
FIPS 180-1	SHA Secure Hash Algorithm
FIPS 180-3/4	SHA 224/256/384/512 Secure Hash Algorithm
FIPS 186-2	DSS Digital Signature Standard
FIPS 197	AES Advanced Encryption Standard

OASIS Standards (www.oasis-open.org)

Business Process Execution Language for Web Service v.1.1, December 2003

Directory Services Markup Language (DSML) v.2.0, January 2002

ebXML Collaborative Partner Profile Agreement (CPPA) v.2, June 2002

ebXML Messaging Service Specification v.2.0, April 2002

ebXML Registry Information Model (RIM) v.2.0, March 2002

ebXML Registry Services Specification (RS) v.2.0, February 2002

Extensible Access Control Markup Language (XACML) v.1.0, January 2003

OASIS Open Document Format for Office Applications v.1.0 May 2005

Security Assertion Markup Language (SAML) v.1.1, March 2003

Universal Description, Discovery and Integration (UDDI) v.2.0, February 2003

Username Token Profile, Working Draft, August 2003

Web Services Atomic Transaction Version 1.1. 12. July 2007

Web Services Business Activity Version 1.1 + Errata, 12. July 2007

Web Services Coordination (WS-Coordination) Version 1.1 + Errata, 12. July 2007

Web Services Policy 1.5 Framework, 4.September 2007

Web Services Reliable Messaging, Version 1.1, 7. January 2008

Web Services Security Rights Expression Language (REL) Token Profile 1.1, 1st February 2006

Web Services Security SAML Token Profile 1.1, 1st February 2006

Web Services Security UsernameToken Profile 1.1, February 2006

Web Services Security X.509 Certificate Token Profile 1.1 + Errata, November 2006

Web Services Security, SOAP Messages Security 1.0, March 2004

Web Services Security, SOAP Messages with Attachments (SwA) Profile 1.1, 1. February 2006

Web Services Trust 1.3, 19. March 2007

Object Management Group (www.omg.org)

Unified Modeling Language (UML)

BPMN 2.0, OMG Final Adopted Specification , Januar 2011

OMA (www.openmobilealliance.org), WAP Forum (www.wapforum.org)

WTLS, Wireless Transport Layer Security

WAP, Wireless Application Protocol Architecture

WDP, Wireless Datagram Protocol

WSP, Wireless Session Protocol Specification

WTP, Wireless Transaction Protocol

Online Service Computer Interface (www.osci.de)

OSCI-Transport v.1.2/2 Online Service Computer Interface

PC/SC (www.pcscworkgroup.com)

PC/SC	Interoperability Specification for ICCs and Personal Computer Systems

RSA Standards (www.rsa.com)

PKCS#1	RSA Encryption Standard v.2.1
PKCS#3	Diffie-Hellman Key Agreement Standard
PKCS#7	Cryptographic Message Syntax Standard v.1.5
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Syntax Standard

Schweizerische Normenvereinigung SNV (www.snv.ch)

SN 612030 Interlis Version 1

SN 612031 Interlis Version 2

SNR CWA 14842-3: 2003 Electronic Commerce – Shop presentation and transactions-Part 3: ICT security requirements

SNR CWA 14842-1: 2003 Electronic Commerce – Shop presentation and transactions-Part 1: Regulatory and self-regulatory requirements

WFMC Standards (www.wfmc.org)

XML Process Definition Language (XPDL) Version 2.X

W3C Standards (www.w3C.org)

CSS Cascading Style Sheet Recommendation 2.0, 12 May 1998

HTML 4.01 Specification W3C Recommendation, 24 December 1999

PNG Portable Network Graphics, W3C Recommendation, 10 November 2003

RDF Resource Description Framework Model und Syntax Specification Recommendation, 22 February 1999

SOAP v.1.2, June 2003

SVG Scalable Vector Graphic, W3C Recommendation 1.1, 14 January 2003

WSDL Web Services Description Language v.1.1, 15 March 2001

WSDL Web Services Description Language Version 2.0 Part 1: Core Language, 26 June 2007

XHTML Extensible Hypertext Markup Language Recommendation 2.0, August 2002

XKML XML Key Management Specification v.2.0, Draft April 2003

XKMS, XML Key Management Specification (XKMS) Recommendation 2.0, 28 June 2005

XML Encryption and Syntax Processing Recommendation, December 2002

XML Extensible Markup Language (XML) Recommendation v.1.1, November 2003

XML Schema Part 0: Primer Second Edition, W3C Recommendation, 28 October 2004

XML Schema Part 0: Primer, W3C Recommendation, 2nd May 2001

XML Schema Part 1: Structures Second Edition, W3C Recommendation, 28 October 2004

XML Schema Part 1: Structures W3C Recommendation 2nd May 2001

XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2001

XML Schema Part 2: Datatypes W3C Recommendation 2nd May 2001

XML Signature and Syntax Processing Recommendation, February 2002

XML Path Language (XPath) Version 1.0, W3C Recommendation, 16 November 1999

XML Path Language (XPath) 2.0, W3C Recommendation, 23 January 2007

Anhang B – Abkürzungen

2D	Zweidimensional
3DES	Triple DES
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Cooperation
API	Application Programmers Interface
Appl.	Application
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BAKOM	Bundesamt für Kommunikation
B2B	Business to Business
B2C	Business to Customer
BGP	Border Gateway Protocol
BMI	(Deutsches) Bundesministerium des Innern
BPEL	Business Process Execution Language
BPEL4WS	Business Process Execution Language for Web Services
BPMN	Business Process Modeling Notation
BSI	(Deutsches) Bundesamt für Sicherheit in der Informationstechnik

BVA	(Deutsches) Bundesverwaltungsamt
bzw.	beziehungsweise
CA	Certification Authority, zu Deutsch Zertifizierungsstelle
CAPI	1) Common Application Programming Interface 2) Microsoft Crypto API
CBC	Cipher Block Chaining Mode
CEN	Comité Européen de Normalisation
Cert	Certificate
CODEC	Compression Decompression Algorithm
CORBA	Common Object Request Broker Architecture
CPPA	Collaborative Partner Profile Agreement
CRL	Certificate Revocation List
CS	Clearingstelle
CSP	1) Cryptographic Service Provider 2) Certificate Service Provider
CSS	Cascading Style Sheets Language
CSV	Comma Separated Value List
d.h.	das heisst
DAP	Directory Access Protocol
DB	Data Base, Datenbank
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIR	Directory Service
DMZ	Demilitarised Zone
DNS	Domain Name Service, Domain Name Server
DSA	1) Digital Signature Algorithm 2) Directory System Agent
DSML	Directory Services Markup Language
DSS	Digital Signature Standard
DTD	Document Type Definition
DVD	Digital Versatile Disk
DXF	Drawing Exchange Format
ebXML	Electronic Business for XML
EC	Elliptic Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMA International	Association for Standartizing ICT Information and Communication Systems (vor 1994: European Computer Manufacturer Association)
ECW	Enhanced Compressed Wavelet

EDI	Electronic Data Interchange
ED/FACT	Electronic Data Interchange for Administration, Commerce and Transport
EIF	Europäisches Interoperability Framework
EIS	Enterprise Information System
engl.	Englisch
EPS	Encapsulated Post Script
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
FIPS	Federal (USA) Information Processing Standards
FTP	File Transfer Protocol
FTPD	FTP-Daemon
G2B	Government to Business
G2C	Government to Citizen
G2Con	Government to Consumer
G2G	Government to Government
G2O	Government to Organisation
G-I	Government internal
GIF	Graphic Interchanged Format
GML	Geography Markup Language
GOSIP	Government Open Systems Interconnection Profile
GUI	Graphical User Interface
GZIP	Gnu Zip (Zigzag Inline Package)
HD	High Definition
HMAC	Keyed-Hash Message Authentication Code
Hrsg.	Herausgeber
HSM	High Speed Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICT	Information and Communication Technology
IDA	Interchange of Data between Administrations
IDEA	International Data Encryption Algorithm
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol

IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IMKA	Interministerielle Koordinierungsausschuss für die Informationstechnik in der Bundesverwaltung
IP	Internet Protocol
IPSEC	IP Security Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISB	Informatikstrategieorgan Bund
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Informationstechnologie, Information Technology
ITU	International Telecommunication Union
J2EE	Java 2 Enterprise Edition
JAAS	Java Authentication and Authorization Service
JAXP	Java API for XML
JDBC	Java Database Connectivity
JMS	Java Message Service
JPEG	Joint Photographic Expert Group
JPG	Joint Photographic Expert Group
JTA	Java Transaction API
KBSt	(Deutsche) Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern
KoopA	(Deutscher) Kooperationsausschuss ADV Bund/Länder/Kommunaler Bereich
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Information Format
MAC	1) Message Authentication Code 2) Media Access Control
Mbps	Million Bits per second
MD5	Message Digest Algorithm 5
MIME	Multipurpose Internet Mail Extensions
MP3	MPEG Layer 3
MPEG	Moving Pictures Experts Group
MTT	MailTrusT
NFS	Network File System
NGO	Non Government Organisation
NIST	(American) National Institute for Standards and Technology
NSP	Network Security Policy

NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
ODF	OASIS Open Document Format for Office Applications
OGG	Xiph.org's container format
OMA	Open Mobile Alliance
OMG	Open Management Group
OR	Schweizerisches Obligationenrecht
ORB	Object Request Broker
OS	Operating System
OSCI	Online Services Computer Interface
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First
PC	Personal Computer
PC/SC	Personal Computer/ Smart Card
PCA	Policy Certification Authority
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDF	Portable Document Format
PDF/X	PDF Exchange (Subset of PDF)
PGP	Pretty Good Privacy
PIN	Persönliche Identifikationsnummer, Personal Identification Number
PK	Public Key
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure, Public Key Infrastruktur
PKIX	IETF Working Group „Public-Key Infrastructure (X.509)“
PNG	Portable Network Graphics
POP3	Post Office Protocol Version 3
PS	Post Script
QT	QuickTime
RDF	Resource Description Framework
RegTP	(Deutsche) Regulierungsbehörde für Telekommunikation und Post
resp.	Respektive
REST	Representational State Transfer
RFC	Request for Comment
RFP	Request for Proposals

RIFF	Resource Interchange File Format
RIP	Routing Information Protocol
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RSA	Rivest Shamir Adleman Public Key Verfahren
RTF	Rich Text Format
s.	Siehe
S1-S3	Schnittstellen S1, S2 und S3, vgl. Kap.5.2 des Dokuments
S/MIME	Secure Multipropose Internet Mail Extension
SAGA	Standards und Architekturen für eGovernment Anwendungen
SAGA.ch	Standards und Architekturen für eGovernment Anwendungen Schweiz
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SEGA	Schweizerische Effekten und Giro AG
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNV	Schweizerische Normenvereinigung
SOA	1) Service-Oriented Architecture 2) Sarbanes Oxley Act
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
SVG	Scalable Vector Graphic
SW	Software
sym.	Symmetrisch
TAV	Technische und Administrative Vorschriften
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
TSP	Time Stamp Protocol
u.a.	unter anderem
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol

UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
usw.	und so weiter
UTF	Unicode Transformation Format
v.	Version
VPN	Virtual Private Networks
VxD	Virtual Device Driver
W3C	World Wide Web Consortium
WAN	Wide Area Network
WAP	Wireless Application Protocol
WAV	WAVEform audio format
WDP	Wireless Datagram Protocol
WFMC	Workflow Management Coalition
WML	Wireless Markup Language
WMV/A	Windows Media Video/Audio
WS	Web Services
WSDL	Web Services Description Language
WS-I	Web Services Interoperability Organization
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWW	World Wide Web
XACML	XML Access Control Markup Language
XHMTL	Extensible Hypertext Markup Language
XKMS	XML Key Management Specification
XLI	X Libary Interface
XML	Extensible Markup Language
XPath	XML Path Language
XPDL	XML Process Definition Language
XSDL	XML Schema Definition Language
XSD	XML Schema Definition
XSL	Extensible Stylesheet Language
XSL-FO	XSL Formatting Objects
XSLT	Extensible Stylesheet Language Transformation

z.B.	zum Beispiel
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur
ZIP	Zigzag Inline Package

Anhang C – Glossar

Das hier vorgestellte Glossar setzt sich aus Begriffen und den dazugehörigen Erklärungen zusammen, welche einerseits von der Web Page des Instituts für Wirtschaft und Verwaltung (www.iwv.ch) in Bern stammen und für den hier vorliegenden Zweck angepasst worden sind, anderseits aus [Mud] entnommen sind oder welche auch im Rahmen der Herstellung dieses Dokuments definiert worden sind.

Administration	Im Zusammenhang mit eGovernment entspricht „Administration“ der Verwaltung im Sinne einer Abgrenzung zu Exekutive, Legislative, Judikative und dem Staat im umfassenden Sinne. Ausschliessend formuliert gilt als öffentliche Verwaltung alles, was nicht Gesetzgebung, Rechtsprechung ist. Grundsätzlich gilt die Administration als eine öffentliche Verwaltung oder als ein Vollzugsorgan, das durch die Regierung gesteuert und durch die Justiz kontrolliert wird.
AES	Ein von John Daemen und Vincent Rijmen entwickeltes symmetrisches Verschlüsselungsverfahren, welches von der NIST zum Standard deklariert worden ist.
Amtsgang, virtueller	Der virtuelle Amtsgang beschreibt, wie Amtsgeschäfte mit Hilfe der Informations- und Kommunikationstechnologie (IKT) erledigt werden können.
API	Application Programming Interface ist eine spezifizierte SW Schnittstelle, welche z.B. die Wahl, die Form und den Inhalt der Parameter für die Eingabe in eine SW Applikation festlegt.
Asymmetrisches Verschlüsselungsverfahren	Verschlüsselungsmethode oder -verfahren, wobei die Schlüssel für die Verschlüsselung und die Entschlüsselung unterschiedlich sind.
Authentisierung	Vorgang zur Bestimmung der Authentizität.
Authentizität	Ein Sicherheitsdienst zur Bestimmung der Identität, für die Definition s. Kapitel 8.2 „Schutzziele“.
Benchmark	Der Begriff „Benchmark“ stammt aus dem Vermessungswesen. In Anlehnung dazu wird „Benchmark“ zum Vergleich spezifizierter Standards mit ausgewählten Unternehmens-, Bereichs- oder Produktzielen verwendet. In der öffentlichen Verwaltung kann ein (Leistungs-)Vergleich zwischen unterschiedlichen oder auch zwischen gleichartigen Bereichen vorgenommen werden.
Best Practice	„Best Practice“ ist eine allgemein anerkannte, in der Praxis umgesetzte und sehr bewährte Lösung. Dabei werden Produkte, Dienstleistungen, (IT) Realisierungen auf Grund von einheitlichen Qualitätskriterien miteinander verglichen.

Certificate Revocation List	Certificate Revocation List, kurz CRL, englischer Fachausdruck für die von der CA (s. Certification Authority) beglaubigte Liste der für ungültig erklärten Zertifikate. Die Beglaubigung erfolgt mittels digitaler Signatur.
Certification Authority	Certification Authority, kurz CA, zu Deutsch auch Zertifizierungsstelle oder Zertifikatsaussteller, ist eine Instanz, welche die Beglaubigung von Schlüsseln für PK Verfahren mittels Zertifikaten (s. Zertifikat) vornimmt.
Challenge Response	Challenge Response ist ein Verfahren zur Authentisierung eines Teilnehmers oder einer Instanz. Dabei muss die zu authentisierende Person oder Instanz die Gegenpartei davon überzeugen (Challenge), dass sie ein Geheimnis kennt, ohne dabei das Geheimnis der Gegenpartei mitzuteilen.
CORBA	CORBA ist ein Akronym für Common Object Request Broker Architecture und standardisiert eine Middleware Architektur und deren Protokolle.
Datenschutz	Datenschutz hat zwei Bedeutungen, einerseits den Schutz der Daten, anderseits den Schutz der Daten, wie ihn das Bundesgesetz zum Datenschutz (DSG) be- oder vorschreibt. Das Bundesgesetz über den Datenschutz regelt unter anderem das Sammeln von Personendaten, deren Schutz, deren Verarbeitung, deren Veröffentlichung und Weiterreichung. Damit sollen die Persönlichkeit und die Grundrechte von Personen geschützt werden, über welche Daten gesammelt und bearbeitet werden.
DES	Symmetrisches, von IBM entwickeltes Verschlüsselungsverfahren mit einer Schlüssellänge von 56 Bit.
Dienst	Ein Dienst, engl. Service, ist eine konkrete und genau definierte eGovernment Anwendung, welcher einen ganzen „Geschäftsfall“ abhandelt, wie z.B. die elektronische Eingabe von Dokumenten an ein Gericht.
Diffie Hellman	Ein von W. Diffie und W. Hellman entwickeltes Public Key Verfahren.
DMZ	Der Begriff „DMZ“ steht für Demilitarisierte Zone (engl. Demilitarised Zone) und wird in der IKT Security im Bereich Firewall verwendet. DMZ sind vom internen Netz und vom Internet abgetrennte Netzbereiche. Sie sind nicht so sicher, wie das interne, aber auch nicht so unsicher wie das externe Netz. Im Netzbereich DMZ werden z.B. Server installiert, welche E-Mails vom internen Netz ans Internet weiterreichen und umgekehrt oder welche die HTTP Pakete vom internen ans externe Netz weitereichen und umgekehrt. In die DMZ werden z.B. auch der Web-Server oder der Inhaltsprüfungsserver verlegt, welcher die Inhalte von HTTP oder E-Mail Paketen auf Viren prüft.
eAdministration	eAdministration bezeichnet den Einsatz der Informations- und Kommunikationstechnologien (IKT) zur Unterstützung des amtlichen Geschäftsverkehrs.
eBusiness	Unter eBusiness wird die Abwicklung von Geschäftsprozessen mit Hilfe von Informations- und Kommunikationstechnologie (IKT) verstanden.

eCommerce	eCommerce umfasst den Teil des eBusiness, welcher sich mit der Vereinbarung und Abwicklung rechtsverbindlicher Geschäftstransaktionen befasst. Es wird zwischen drei Beziehungstypen unterschieden: - Business-to-Business (Unternehmen – Unternehmen) - Business-to-Consumer (Unternehmen – Endverbraucher) - Consumer-to-Consumer (Spezialfall, wo das Unternehmen nur als Vermittler auftritt, z.B. Online-Auktionen).
eGovernment	eGovernment umfasst die Unterstützung der Beziehungen, Prozesse und der politischen Partizipation innerhalb aller staatlichen Ebenen sowie gegenüber allen Anspruchsgruppen durch Bereitstellung von Interaktionsmöglichkeiten mittels elektronischer Medien.
EIF	Europäisches Interoperability Framework
Einmal-Passwort	Einmal-Passwort ist ein Verfahren zur Authentisierung, wobei bei jeder Authentisierung ein neues (zeitabhängiges) Passwort verwendet wird. Ein Passwort wird somit im Allgemeinen nur einmal verwendet.
electronic Public Services (ePS)	Abgabe von öffentlichen Leistungen an die Leistungsempfänger, Privatpersonen oder Unternehmungen über lokale, regionale oder nationale Portale.
elektronische Signatur	Die elektronische, auch digitale, Signatur schützt die Authentizität und Integrität einer Datei. Die elektronische Signatur basiert auf dem Hashwert (s. Hashwert) der zu schützenden Datei und einem PK Verfahren (s. PK Verfahren). Der Hashwert der Datei wird mit dem privaten Schlüssel verschlüsselt. Das Resultat davon wird als elektronische Signatur bezeichnet.
Elliptische Kurven	Ein von N. Koblitz und V.S. Miller unabhängig voneinander entwickeltes Public Key Verfahren.
Entität	Eine Entität ist eine Instanz im IT Umfeld, welche eine Identität aufweist. Eine Entität kann ein User, Client, Server, Web Service Dienst, Mobilephone, PDA oder ein Verzeichnisdienst sein (Aufzählung nicht abschliessend).
Erweiterbarkeit	Erweiterbarkeit bezeichnet die Fähigkeit, den Bestandteilen der Anwendung wirtschaftlich neue Funktionalität hinzufügen oder die bestehende zu erweitern, ohne dass diese dadurch beeinträchtigt wird.
FIPS	FIPS steht für Federal (USA) Information Processing Standards der Standardisierungsorganisation NIST.
Flexibilität	Die Flexibilität bezeichnet die allgemeine Fähigkeit, eine bestehende Architektur zu modifizieren, um neue Anforderung Kosten optimiert zu realisieren.
GIF	Abkürzung für "Graphics Interchange Format" - Grafik-Austauschformat. Neben JPEG ist GIF das wichtigste Format für Browser-konforme Bilder.
Government internal (G-I)	Beziehung innerhalb der staatlichen Organe jeweils auf der Bundes-, Kantons- und Gemeindeebene (ISB-spezifischer Begriff im Sinne von externem eGovernment).

Government to Business (G2B)	Beziehung zwischen Staat und Privatwirtschaft auf Basis von Informations- und Kommunikationstechnologien (IKT). Der Begriff lehnt sich an die Bezeichnung Business to Business (B2B) und beschreibt die Beziehung zwischen Staat und Privatwirtschaft auf Basis der Informations- und Kommunikationstechnologien (IKT). Der Staat unterhält nicht nur mit natürlichen Personen, sondern auch mit juristischen Personen viele Beziehungen. Deren Gestaltung und die Abwicklung der einhergehenden Geschäftsfälle kann auf elektronischem Wege erleichtert werden.
Government to Citizen (G2C)	Beziehung zwischen Staat und Bürger in politischen Angelegenheiten (häufig analoge Verwendung zu G2C). Der Citizen ist der Bürger im politischen Sinne, also die mit politischen Rechten ausgestattete Person. Government to Citizen bezeichnet demnach die über das Internet geführte Kommunikation zwischen Staat und Bürger in politischen Angelegenheiten. Die Bürger sind dabei nicht dem Staat untergeordnete Subjekte, sondern diesem übergeordnet, weil sie Entscheidungen treffen und das staatliche Handeln in einer Demokratie damit legitimieren.
Government to Consumer (G2Con)	Beziehung zwischen Staat und Einzelpersonen im Sinne von Kunden oder Konsumenten. Der Begriff „Consumer“ ist der Privatwirtschaft entlehnt und bezeichnet im eGovernment-Bereich Einzelpersonen als Kunde oder Konsument in einem weit gefassten Sinne. Die Kundenrolle umfasst viele Formen, angefangen beim Fall, wo die Einwohner als Subjekt des Staates aufgefasst werden, z.B. als Sozialhilfeempfänger, Patient oder Student, bis hin zum Fall, wo der Staat und seine Subjekte in eine – vielleicht zwar nicht freiwillige, aber dennoch klassische – Kunden-Lieferanten-Beziehung treten, also wo Menschen Käufer oder Bezüger von öffentlichen Gütern und Dienstleistungen sind.
Government to Government (G2G)	Behördenverkehr zwischen Verwaltungsstellen.
Government to Organisation (G2O)	Government to Organisation (G2O) steht für die „Beziehung zwischen Bund, Kantonen und Gemeinden einerseits und den privatwirtschaftlichen Partnern (Unternehmen) und öffentlichrechtlichen Organisationen (Verbänden, etc.) andererseits.“ Government to Organisation (G2O) ist ein ISB-spezifischer Begriff (ISB: Informatikstrategieorgan Bund), welcher an Stelle von „Government to Business“ verwendet wird. G2O enthält G2B und schliesst darüber hinaus öffentlich-rechtliche Organisationen wie Verbände, Vereine, Parteien etc. ein.
guichet virtuel (www.ch.ch)	Internet-Portal, welches nach dem täglichen Leben der Gesellschaft bzw. den Lebenslagen aufgebaut ist. Die Idee des guichet virtuel ist ein Internet-Portal, das in seinem Aufbau nicht der Verwaltungsstruktur und auch nicht den staatlichen Prozessen folgt (z.B. www.admin.ch), sondern dem täglichen Leben der Gesellschaft bzw. den Lebenslagen.
Hashfunktion	Eine Hashfunktion stellt aus einer Datei eine kryptographische Prüfsumme mit bestimmter Länge her. Im Unterschied zu einer gewöhnlichen Prüfsumme, lässt sich der Prüfsummenwert aus Kenntnis einer Datei nicht voraussagen. Zugleich ist es schwierig, zwei Dateien so herzustellen, dass sie denselben Prüfsummenwert ergeben. Der Prüfsummenwert wird auch als Hashwert bezeichnet. Bekannte Hashfunktionen sind SHA-1 und MD5. Die Hashfunktionen bilden eine wichtige Komponente zur Bildung der digitalen Signatur.

Hashverfahren	Ein Hashverfahren ist eine genau definierte Hashfunktion, z.B. SHA-1
Hashwert	Ein Prüfsummenwert einer Datei, wobei dieser Wert mittels einer Hashfunktion hergestellt worden ist.
Hochsicherheit	Von Hochsicherheit wird in diesem Zusammenhang gesprochen, wenn das Schutzbedürfnis eines der Sicherheitsdienste als „sehr hoch“ klassifiziert worden ist.
HTML	Standardisierte Seitenbeschreibungssprache für WWW-Seiten im Internet bzw. Intranet, welche von Dr. Charles F. Goldfarb entwickelt wurde.
HTTP	Das Hypertexttransferprotokoll (HTTP) baut auf dem Internetprotokoll auf und ermöglicht einen für den Anwender einfachen Datenaustausch. HTTP und HTML verhalfen dem Internet bei einer breiten Masse von Computer-Anwendern zum Durchbruch.
IDEA	International Data Encryption Algorithm, kurz IDEA, ist ein symmetrisches Chiffrierverfahren mit einer Schlüssellänge von 128 Bit. IDEA wurde zu Beginn der 90er Jahre von X. Lai und J. Massey entwickelt.
IEEE	Institute of Electrical and Electronics Engineers. Standardisierungsgremium u.a. für elektrotechnische Anwendungen. Seit einigen Jahren an der Standardisierung von Algorithmen und Verfahren für die Public Key Kryptographie beteiligt.
IETF	Internet Engineering Task Force (www.ietf.org), kurz IETF, ist ein Standardisierungsgremium für die Internetprotokolle und dazu anverwandte Dienste.
IKT	IKT steht für Informations- und Kommunikationstechnologien. Beispiele: Internet, Intranet, Extranet, WAP (Wireless Application Protocol), E-Mail, UMTS (Universal Mobile Telecommunication System).
Information	Information ist zur Verfügung gestelltes „Wissen“ oder eine zur Verfügung gestellte Beschreibung. Die Information kann in verschiedenen Formen und Ausprägungen zur Verfügung gestellt werden, z.B. in Form einer Datei, eines Buches, einer Nachricht oder eines Zeitungsartikels.
Integrität	Ein Sicherheitsdienst zur Erkennung von ungewollten Manipulationen, für die Definition s. Kapitel 8.2 „Schutzziele“.
Internet	Das Internet ist ein öffentliches Computernetz, über welches vor allem Daten mittels Internetprotokollen ausgetauscht werden. Die einzelnen Seiten können benutzerfreundlich mittels der URI (Uniform Ressource Identifier) angewählt werden.
Internetprotokoll (IP)	Das Internetprotokoll ist aus dem Arpanet (U.S. Militär- und Forschungsnetzwerk) Ende der 60er Jahre entstanden. Es ermöglicht die Kommunikation der Computer untereinander über kleine Netzabschnitte, wie auch über grosse Netzwerke
Interoperabilität	Technische Interoperabilität bezeichnet die medienbruchfreie Realisierung Transaktionsdiensten zwischen Behörden übergreifenden Fachanwendungen.
IPSEC	IPSEC steht für IP Security und ist eine von der IETF standardisierte Sicherheitstechnologie zur Absicherung der IP Pakte.

ITU	Die International Telecommunication Union (ITU), früher CCITT genannt, ist eine internationale Organisation für Koordinierung, Normierung und Entwicklung von Telekommunikationsdiensten. (www.itu.org)
JPEG	1) Joint Photographic Expert Group (JPEG) ist eine Kommission, welche das Verfahren zum Komprimieren und Speichern von Bild- und Videodaten festlegt. 2) Dateiformat, welches nach der hier erwähnten Gruppe benannt wurde.
Komprimieren	Komprimieren (zusammenpressen, verdichten) bedeutet in der Informatik, möglichst viel Unwesentliches, d.h. möglichst viel Redundanz, herauszunehmen. Redundanz liegt in einer Information dann vor, wenn Änderungen vorgenommen werden können, dabei aber die Bedeutung oder Aussagekraft der Information nicht verändert wird. Eine Information ist frei von Redundanz, wenn jede an der Information vorgenommene Änderung zu einer anderen Bedeutung oder Aussage führt. Informationen frei von jeder Redundanz gibt es in der Praxis nicht.
NIST	National Institute of Standards and Technology ist ein nationales Standardisierungsgremium der USA. (www.nist.gov)
OASIS	Organization for the Advancement of Structured Information Standards. Standardisierungsgremium für Web Services. (www.oasis-open.org)
OMA	Open Mobile Alliance Ltd, kurz OMA, ist die Nachfolgeorganisation des WAP Forums.
OMG	OMG steht für Open Management Group und ist ein Standardisierungsgremium für CORBA.
PC/SC	PC/SC ist ein Standard für die Anbindung von Smart Cards. Die Standards werden von der PC/SC Workgroup herausgegeben. (www.pcscworkgroup.com)
PDF	Das Portable Document Format (PDF) des Unternehmens Adobe Systems ist ein vielseitiges Dateiformat zur Darstellung von Dokumenten, welches die Schriften, die Formatierungen, die Farben und Grafiken eines beliebigen Quelldokuments (weitgehend) beibehält, unabhängig vom Betriebssystem und vom Programm, mit welchen es erstellt wurde.
PGP	Pretty Good Privacy. SW, entwickelt von P. Zimmermann, zum Verschlüsseln und Signieren von E-Mails.
PK Verfahren	Public Key Verfahren, kurz PK Verfahren, ist ein asymmetrisches Verschlüsselungsverfahren (s. asymmetrisches Verschlüsselungsverfahren), wobei aus dem einen Schlüssel kein Rückschluss auf den anderen gemacht werden kann. Der eine Schlüssel wird veröffentlicht und wird folglich public Key genannt, während der andere Schlüssel (private Key) geheim gehalten wird. Public Key Verfahren dienen der Authentisierung, dem Schutz der Integrität und der vertraulichen Kommunikation. PK Verfahren bilden die Basis für die Herstellung digitaler Signaturen und digitaler Zertifikate.
PKCS	Public Key Cryptography Standard. Standards herausgegeben von RSA Laboratories.

Post Script	Von Adobe System Inc. 1984 auf den Markt gebrachte Seitenbeschreibungssprache für das seitenweise Ausdrucken und Speichern von Grafiken und Texten.
Public Key Infrastructure	Public Key Infrastructure, kurz PKI ist die benötigte Infrastruktur, damit die Benutzer mit Public Key Verfahren Daten authentisch, integer oder vertraulich austauschen können. Eine PKI besteht unter anderem aus - einer Certification Authority - einem Verzeichnisdienst, wo die Zertifikate publiziert werden.
Public Key Umverschlüsselungsassistent	Ein (Public Key) Umverschlüsselungsassistent ist ein Programm, welches die Daten mit dem alten (privaten) Schlüssel entschlüsselt und mit dem neuen (öffentlichen) verschlüsselt.
Revozieren	Etwas, z.B. ein digitales Zertifikat, öffentlich und beglaubigt für ungültig erklären lassen.
Router	Ein Router ist ein Steuerungselement in einem Netz primär für die Datenkommunikation. Zu seinen Aufgaben gehört u.a., die Datenpakete anhand ihrer Zieladresse auf den richtigen Übertragungsabschnitt weiterzuleiten.
Routing-Protokoll	Ein Protokoll, welches den Router hilft, die Netztopologie kennen zu lernen, so dass die Pakete zielgerichtet weitergeleitet werden können.
RSA	Public Key Verfahren nach den Erfinder URLn Rivest, Shamir und Adleman benannt.
S/MIME	Sicherheitstechnologie und -standard von der IETF für die Absicherung der E-Mail Kommunikation.
SAGA.ch	SAGA.ch steht für Standards und Architekturen für eGovernment Anwendungen Schweiz und ist ein vom Verein ***eCH*** hergestelltes Dokument, welches in verdichteter Form die technischen Richtlinien für die Umsetzung von eGovernment Anwendungen in der Schweiz darstellt.
Service Public	Unter Service Public wird meist die Sicherstellung einer flächendeckenden und Kosten günstigen Grundversorgung mit Infrastrukturleistungen verstanden. Diese Leistungen können sowohl materieller (Verkehr, Telekommunikation, Post, Energie usw.) als auch immaterieller Art sein (Gesundheit, Bildung, Kultur etc.). Unerheblich ist dabei, ob die Leistungserbringung durch die öffentliche Hand selbst oder durch private Dritte erfolgt (auf Basis Leistungsvereinbarung/-auftrag).
Session Key	Temporärer, vereinbarter, symmetrischer Schlüssel zweier oder mehrerer Teilnehmer für die Dauer einer Kommunikationsverbindung.
Signatur, digitale	Die digitale Signatur schützt die Authentizität und Integrität einer Datei. Die digitale Signatur basiert auf dem Hashwert (s. Hashwert) der zu schützenden Datei und einem PK Verfahren (s. PK Verfahren). Der Hashwert der Datei wird mit dem privaten Schlüssel verschlüsselt. Das Resultat davon wird als digitale Signatur bezeichnet.
Smart Card	Eine Smart Card ist ein genormtes Stück Plastik mit einem darauf integrierten Mikroprozessor, welcher unter anderem kryptographische Operationen durchführt.
SOAP	Ist ein Middleware Protokoll zum Austausch von Meldungen im Bereich Web Services.

SSL/TLS	SSL steht für den englischen Ausdruck Secure Socket Layer und ist eine von Netscape entwickelte Sicherheitstechnologie, ursprünglich zur Sicherung des HTTP-Protokolls. SSL hat sich zum de facto Standard erhoben. TLS, Transport Layer Security, ist eine von der IETF standardisierte Sicherheitstechnologie und basiert etwa zu 95% auf SSL, doch die beiden Verfahren sind untereinander nicht kompatibel.
Symmetrisches Verfahren	Verschlüsselungsmethode, wobei die Schlüssel für die Ver- und Entschlüsselung identisch sind.
Telnet	Telnet ist ein TCP/IP Anwendungsprotokoll, welches zur entfernten Administration von Servern über das Netz verwendet wird.
Transaktion	1) Transaktionen umfassen die Auslösung von Prozessen der Güterbewegung oder der Erbringung von Dienstleistungen bzw. den gesamten Nachrichtenaustausch, welcher während der Durchführung eines solchen Prozesses notwendig ist. 2) Von Transaktionen wird in der Technik gesprochen, wenn - mehrere Instanzen eingebunden sind. - Datenänderungen bei unterschiedlichen Instanzen vorgenommen werden. - Datenkonsistenz nach der Aktion vorhanden sein muss, ansonsten die Aktion rückgängig gemacht werden muss.
UDDI	Das Directory oder Verzeichnis, wo die Web Services Dienste in der WSDL Sprache publiziert werden, wird als Universal Description Discovery Integration, kurz UDDI, bezeichnet. Die Struktur und die Anfragen auf dieses Verzeichnis sind von der OASIS (www.oasis-open.org) standardisiert worden.
UML	Unified Modeling Language (UML) ist eine Sprache oder eine Darstellungsweise, wie der Prozess gemäss dem „orchestration model“ beschrieben werden kann. Dabei werden die möglichen Zustände im Ablauf mittels Blockdiagrammen (engl. state charts) beschrieben und angegeben, ob und wie die einzelnen Zustände in andere übergehen können.
Unterschrift, digitale	s. Signatur, digitale.
Use Case	Ein Use Case ist eine konkrete IT Anwendung oder ein konkreter Ablauf, welcher durch die IT abgewickelt wird.
Verfügbarkeit	Ein Sicherheitsdienst für das termingerechte Zurverfügungstellen von Informationen, für die Definition s. Kapitel 8.2 „Schutzziele“.
Vertraulichkeit	Ein Sicherheitsdienst zur Wahrung von Geheimnissen oder privaten Informationen, für die Definition s. Kapitel 8.2 „Schutzziele“.
W3C	Standardisierungsgremium für XML und darauf basierende Anwendungen. (www.w3C.org)
WAP Forum	Ehemaliges Standardisierungsgremium für das Wireless Application Protocol (WAP). Nachfolgeorganisation ist die OMA.
Web Services	Zur Definition von Web Services, s. Kapitel 6.8.
WSDL	Web Service Description Language (WSDL) ist eine von W3C standardisierte Beschreibung der Dienste im Bereich Web Services. (www.w3C.org)

WS-I	Web Services Interoperability Organization, kurz WS-I, ist ein Standardisierungsgremium, welches die Interoperabilität bei den Web Services erreichen will. (www.ws-i.org)
WTLS	WTLS steht für Wireless Transaction Layer Security ist eine vom WAP Forum standardisierte Sicherheitstechnologie zur Absicherung des WAP-Protokolls. WTLS basiert etwa zu 95% auf SSL, doch die beiden Verfahren sind untereinander nicht kompatibel.
WWW	World Wide Web. Ein Internetdienst zur plattformunabhängigen Bereitstellung von untereinander verbundenen Dokumenten.
XML	XML steht für eXtensible Markup Language und ist eine "vereinfachte" Version der Standard Generalized Markup Language (SGML). Die Entwicklung von XML begann 1996, und seit Februar 1998 ist XML ein W3C-Standard. XML soll es den Web-Site-Programmierern erleichtern, SGML-Anwendungen zu schreiben und dabei eigene Dokumententypen festzulegen. XML bietet viele Mechanismen, welche u.a. die Datenverwaltung im Netz erleichtern sollen.
Zertifikat, digitales	Ein digitales Zertifikat ist eine mittels digitaler Signatur hergestellte Beglaubigung, dass ein öffentlicher Schlüssel (s. PK Verfahren) zu einer Entität gehört (s. Entität). Im Volksmund wird ein digitales Zertifikat als digitales Äquivalent zu einem Pass bezeichnet. Dies ist aber irreführend. Ein digitales Zertifikat alleine identifiziert eine Person nicht, dies im Gegensatz zum Pass.