



Bundesministerium
für Wirtschaft
und Technologie

MEDIA@Komm
Transfer

Spezifikationsbericht

„Elektronische kommunale Poststelle (eKomP)“

Von

Landeshauptstadt Saarbrücken

Stadt Hagen

Städtetag Rheinland Pfalz

Stadt Oldenburg

Ostalbkreis

Stadt Rosenheim

Stadt Würzburg

Im Rahmen der Initiative

MEDIA@Komm-Transfer

Gefördert vom

Bundesministerium für Wirtschaft und Technologie

Koordiniert und unterstützt von

Transferagentur ***MEDIA@Komm-Transfer***

Cappgemini Deutschland GmbH

Oktober 2006

Impressum

Dieser Bericht ist Teil der Veröffentlichungsreihe „Spezifikationsberichte“ im Rahmen des Projekts *MEDIA@Komm-Transfer*, das durch das Bundesministerium für Wirtschaft und Technologie im Zeitraum Frühling 2004 bis Herbst 2006 gefördert wurde.

Herausgeber:

Bundesministerium für Wirtschaft und Technologie

Referat P3 – Öffentlichkeitsarbeit –

www.bmwi.de

Download:

www.mediakomm-transfer.de

Redaktion:

Transferkommune Saarbrücken, Petra Carl, Mitarbeiterin im Hauptamt, Nunzia Lombardo-Schnur, Mitarbeiterin im Personal- und Organisationamt, Klaus Schirra, Mitarbeiter im Informations- und Kommunikationsinstitut

Transferkommune Hagen, Gerd Thurau, Mitarbeiter im Hagener Betrieb für Informationstechnologie, Ina Tepper, Mitarbeiterin im Hagener Betrieb für Informationstechnologie

Transferkommune Oldenburg, horsten Roskamp, Datenschutzbeauftragter im Zweckverband Kommunale Datenverarbeitung

Transferkommune Ostalbkreis, Tanja Breitmeier, E-Government-Beauftragte

Transferkommune Rosenheim, Manfred Grundei, Leiter des Amtes für Informationsverarbeitung

Transferkommune Würzburg, Dr. Bernd Schmitt, Leiter des Projektes <Würzburg integriert!> der Stadt Würzburg

Herbert Benz, KommWis GmbH im Auftrag des Städtetages Rheinland-Pfalz

Unterstützt durch Transferagentur *MEDIA@Komm-Transfer*, Dr. Helmut Drücke, Robert Wilke, Dr. Norbert Niemeier, Koordinator bei der Erstellung der Berichte, Capgemini Deutschland GmbH, Public Services

Qualitätsgesichert durch Dr. Norbert Niemeier (Projektleiter) und Ricarda König, Capgemini Deutschland GmbH, Public Services

Design und Umsetzung Inhalt:

Graphic Services, Capgemini Deutschland GmbH

Stand: Oktober 2006

Vorwort

An der Nahstelle von Staat, Wirtschaft und Bürger sind leistungsfähige Kommunen ein wesentlicher Erfolgsfaktor für die Wettbewerbsfähigkeit unseres Landes. In Verbindung mit einer Optimierung der Prozesse bietet der Einsatz von E-Government-Lösungen ein hohes Potenzial für Verbesserungen. So können kommunale Aufgaben effizienter erbracht werden. Die Qualität und Transparenz der Dienste kann gesteigert werden. Der Kontakt zu Bürgern und Wirtschaft wird verstärkt. Erweiterte Dienstleistungen werden möglich.

Anders als auf den Ebenen von Bund und Ländern mit ausgeprägten E-Government-Initiativen stehen die ca. 12.000 Kommunen und Kreise vor der großen Aufgabe, geeignete Lösungen mit beschränktem Know-how und Ressourcen bereitzustellen. Mit dem Förderprogramm *MEDIA@Komm* hat das Bundesministerium für Wirtschaft und Technologie (BMWi) in den Jahren 1999 bis 2003 die Entwicklung von rechtssicherem kommunalem E-Government maßgeblich vorangetrieben. Wichtige Standards für Dienste der öffentlichen Verwaltung (OSCI) mit großer Bedeutung auch für Bund und Länder (SAGA, KoopA ADV) sind entstanden.

Mit *MEDIA@Komm-Transfer* hat das BMWi seine Aktivität zum E-Government in den Jahren 2004 bis 2006 fortgeführt. Zentrale Handlungsfelder waren Harmonisierung, Verbreitung und Internationalisierung. Getragen wird *MEDIA@Komm-Transfer* von 20 Transferkommunen, die in einem Wettbewerb aus mehr als 100 Interessenten ausgewählt wurden, und der Transferagentur, die vom BMWi mit der zentralen Koordination beauftragt wurde.

Die Transferkommunen haben 24 mit Blick auf E-Government besonders relevante kommunale Themen ausgewählt und in enger Abstimmung untereinander sowie in eigener Regie erarbeitet. Die Ergebnisse liegen nun in Form von Spezifikationsberichten vor. In diesen Berichten wurden strategische, technische, funktionale und organisatorische Anforderungen an E-Government untersucht. Den Transferkommunen, die diese Themen mit hohem Einsatz bearbeitet haben, und den Experten der Qualitätssicherung gilt ein besonderer Dank.

Die in den Spezifikationsberichten zusammengetragenen Anforderungen, Verfahren, Vorgehensweisen und Erfahrungen stehen allen Akteuren für eigene weitere Schritte in das E-Government zur Verfügung. Aufgezeigter Nutzen und Wirtschaftlichkeit der harmonisierten Verfahren machen deutlich, dass E-Government sich lohnt für Verwaltung, Wirtschaft und Bürger. Als Leitfäden sollen diese Spezifikationsberichte Impulse für den Transfer und die Verbreitung des E-Governments in Deutschland geben und helfen, bisherige Zurückhaltung in der Umsetzung zu überwinden.

Ein Erfolgsfaktor von *MEDIA@Komm-Transfer* waren Netzwerke und Kooperationen, die zwischen Kommunen und zwischen Staat und Wirtschaft geknüpft wurden. Jetzt kommt es darauf an, dass die Akteure und Netzwerke (Kommunen, Datenzentralen und Softwareunternehmen, Deutschland-Online, kommunale Spitzenverbände, Ver-

bände der Wirtschaft, Initiative D21) die angestoßenen Entwicklungen weiterführen und für möglichst flächendeckende Breitenwirksamkeit sorgen. Denn E-Government entwickelt sich mehr und mehr zu einem wesentlichen Standortfaktor im globalen Wettbewerb.

Berlin, im Oktober 2006

Bundesministerium für Wirtschaft und Technologie

Inhaltsverzeichnis

Impressum	2
Vorwort	3
Inhaltsverzeichnis	5
Abbildungsverzeichnis	7
Tabellenverzeichnis	8
Abkürzungsverzeichnis	9
1 Einleitung	12
1.1 Ziele und Inhalte der Spezifikationsberichte.....	12
1.2 Gegenstand und Bearbeiter des Spezifikationsberichts „Elektronische kommunale Poststelle“	14
2 Harmonisierung im Rahmen der Initiative <i>MEDIA@KommTransfer</i>	16
3 Beschreibung des Verfahrens „Elektronische kommunale Poststelle“	19
3.1 Definition und Funktionalität	19
3.2 Einsatzfelder.....	19
3.3 Nutzen	19
3.4 Wirtschaftlichkeit	20
3.5 Berücksichtigung sonstiger Harmonisierungs- und Standardisierungsaktivitäten	22
3.6 Gesetzliche Vorgaben	24
3.6.1 Gesetzliche Schriftform nach dem Verwaltungsverfahrensgesetz	24
3.6.2 Übergreifende Gesetze und Verordnungen.....	25
4 Die Spezifikation des Verfahrens „Elektronische Kommunale Poststelle“	26
4.1 Technische Anforderungen	26
4.1.1 Interoperabilität.....	26
4.1.2 Anbindung an die materielle Infrastruktur	27
4.1.3 Standardbausteine und Verfahren.....	28
4.1.4 Normbedingte Anforderungen	29
4.1.5 Sicherheitstechnische Anforderungen	31
4.1.6 Zuverlässigkeit.....	31
4.1.7 Leistungsfähigkeit und Ausfallsicherheit.....	32
4.1.8 Dokumentation	33
4.1.9 Allgemeine Systemanforderungen	36

4.2	Funktionale Anforderungen	37
4.2.1	Verfügbarkeit	37
4.2.2	Vertraulichkeit.....	38
4.2.3	Authentizität.....	39
4.2.4	Integrität.....	40
4.2.5	Nichtabstreitbarkeit.....	41
4.3	Organisatorische Anforderungen	44
4.3.1	Allgemeine Anforderungen	44
4.3.2	Unterschiedliche Kommunikationsbeziehungen.....	45
4.3.3	Mögliche Betreibermodelle	48
	Literaturverzeichnis.....	53
	Anhang 1: Schutzbedarfsfeststellung	55
	Anhang 2: Regelungsbedarf für Dienstvereinbarungen/Dienstanweisungen....	60

Abbildungsverzeichnis

Abbildung 1: Charakterisierung der Spezifikationsberichte	13
Abbildung 2: Der Beitrag der Harmonisierungsvorhaben zur Fortentwicklung des E-Governments	17
Abbildung 3: Netzverknüpfung in Rheinland-Pfalz.....	23
Abbildung 4: Poststellen-Konzept.....	24
Abbildung 5: Übersicht DIN ISO 9241	30
Abbildung 6: Übersicht DIN ISO 9126	30

Tabellenverzeichnis

Tabelle 1: Absender- und Empfängerauthentizität.....	39
Tabelle 2: Schutzbedarfsklassen	55
Tabelle 3: Schutzbedarfsfeststellung für das Sicherheitsziel Vertraulichkeit	56
Tabelle 4: Schutzbedarfsfeststellung für das Sicherheitsziel Integrität	57
Tabelle 5: Schutzbedarfsfeststellung für das Sicherheitsziel Authentizität und Nicht- Abstreitbarkeit der übertragenen Daten.....	58
Tabelle 6: Schutzbedarfsfeststellung für das Sicherheitsziel Authentizität der Kommunikationspartner	58
Tabelle 7: Schutzbedarfsfeststellung für das Sicherheitsziel Vertraulichkeit	59
Tabelle 8: Schutzbedarfsfeststellung für das Sicherheitsziel Vertraulichkeit	59

Abkürzungsverzeichnis

Art.	Artikel
BGG	Bundesgesetz zur Gleichstellung behinderter Menschen
BITV	Barrierefrei Informationstechnik-Verordnung
BMWi	Bundesministerium für Wirtschaft und Technologie (vormals Bundesministerium für Wirtschaft und Arbeit, BMWA)
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bsp.	Beispiel
bzw.	beziehungsweise
d. h.	das heißt
DIN	Deutsches Institut für Normung
DMS	Dokumentenmanagement-System
ebd.	ebenda
EDV	Elektronische Datenverarbeitung
eKomP	Elektronische Kommunale Poststelle
etc.	et cetera (lat.: und weiteres)
f.	folgende
ff.	fortfolgende
ggf.	gegebenenfalls
GVBL	Gesetz- und Verordnungsblatt
http	Hypertext Transfer Protocol
https	Hypertext Transfer Protocol Secure
i.A.	im Allgemeinen
i. d. R.	in der Regel
ISIS-MTT	Industrial Signature Interoperability Standard-Mailtrust-Standard
IT	Informationstechnik/-technologie
IuK	Informations- und Kommunikationstechnik/-technologie
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung

KNRP	Kommunalnetz Rheinland-Pfalz
MACs	Message Authentication Codes
MB	Megabyte
o. ä.	oder ähnliches
OSCI	Online Services Computer Interface
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
PDF	Portable Document Format (Format der Firma Adobe)
RAID	Redundant Array of Independent Discs
rlp-Netz	radio link protocol (automatische Antwortanforderung)
RMI	Remote Method Invocation („Entfernter Methodenaufruf“)
RTF	Rich Text Format
s.	siehe
S.	Seite
SAGA	Standards und Architekturen für E-Government-Anwendungen
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol (Einfaches Objekt-Zugriffs-Protokoll)
SSL	Secure Socket Layer
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetz
u. a.	unter anderem
u. U.	unter Umständen
VwVfG	Verwaltungsverfahrensgesetz
vgl.	vergleiche
VPN	Virtual Private Network
XML	Extensible Markup Language
XÖV	XML-Standards in der öffentlichen Verwaltung (Zusammenfassung der verschiedenen, fachlich orientierten Standards für den interoperablen Datenaustausch im E-Government)
z. B.	zum Beispiel

z. T. zum Teil

1 Einleitung

Die Initiative *MEDIA@Komm-Transfer* des Bundesministeriums für Wirtschaft und Technologie verfolgt das Ziel, E-Government auf kommunaler Ebene zu fördern. Ein Netzwerk von zwanzig Transferkommunen erarbeitete Ansätze im nationalen und internationalen Bereich, wie kommunales E-Government weiterentwickelt werden kann. Hierbei wurden sie von der Transferagentur unterstützt, die durch Capgemini Deutschland gestellt wird.

Die Initiative *MEDIA@Komm-Transfer* ist in drei Aufgabenbereiche untergliedert (nähere Informationen siehe Kapitel 2):

- **Harmonisierung:** Ziel der Harmonisierung war es, Anforderungen an kommunales E-Government über regionale Grenzen hinweg zu bestimmen und zu dokumentieren. Die Transferkommunen haben sich hierfür in Arbeitsgruppen zusammengefunden und mit Unterstützung der Transferagentur zu einzelnen Themenstellungen Spezifikationsberichte erarbeitet, die ein wesentliches Ergebnis der Initiative *MEDIA@Komm-Transfer* darstellen.
- **Verbreitung:** Die in den Transferkommunen vorliegenden Erfahrungen und die Ergebnisse der Harmonisierung wurden auf zentralen und regionalen Veranstaltungen einem breiten Publikum vorgestellt und in individuellen Workshops mit interessierten Kommunen diskutiert. So wurde eine breite Öffentlichkeit für das Thema kommunales E-Government erreicht.
- **Internationale Kooperation:** Weiteres Ziel war es, auch auf internationaler Ebene kommunales E-Government aus Deutschland bekannt zu machen und mit internationalen Initiativen zu vernetzen. Kooperationen wurden insbesondere im Bereich der EU und Osteuropa etabliert.

Bei dem hier vorliegenden Dokument handelt es sich um einen Spezifikationsbericht aus dem Aufgabenbereich der Harmonisierung. Im Folgenden werden die Ziele und Inhalte der Spezifikationsberichte zunächst allgemein und anschließend bezogen auf das in diesem Bericht behandelte Verfahren erläutert.

1.1 Ziele und Inhalte der Spezifikationsberichte

Ein wesentliches Resultat der Arbeiten der einzelnen Vorhaben im Rahmen der Harmonisierung sind die Spezifikationsberichte. Die Spezifikationsberichte beschreiben Verfahren und Konzepte mit dem Ziel, eine Harmonisierung innerhalb des kommunalen E-Governments voranzutreiben (s. Abbildung 1).

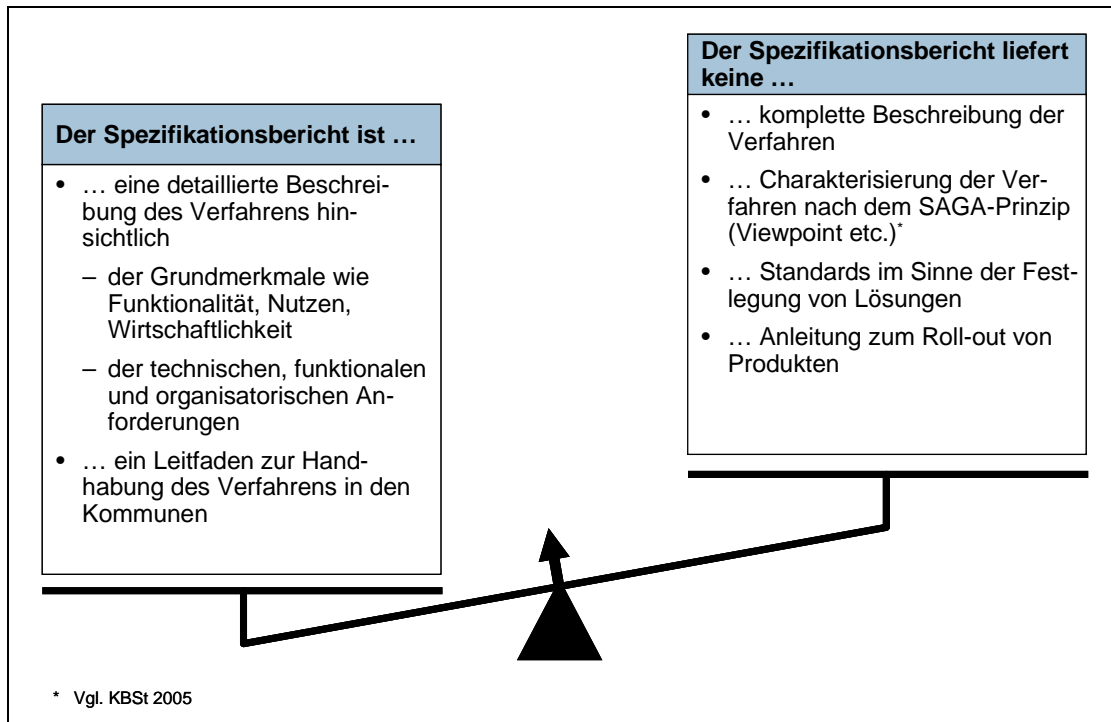


Abbildung 1: Charakterisierung der Spezifikationsberichte

Hauptadressaten¹ der Spezifikationsberichte sind folglich zuerst Kommunen,² die sich damit befassen, die in den Spezifikationsberichten beschriebenen Anwendungen oder Komponenten des E-Governments einzuführen. Zweite Zielgruppe sind Unternehmen, die Softwarelösungen für die in den Berichten beschriebenen E-Government-Anwendungen und -Komponenten entwickeln.

Die Spezifikationsberichte dienen vor allem als Leitfaden. Darüber hinaus sind es Berichte aus der Praxis mit Fallbeispielen zur Verdeutlichung von abstrakten Anforderungen. Weiterhin stellen die Transferkommunen ihre Vorgehensweisen zum jeweiligen Harmonisierungsverfahren vor. Damit wird der pragmatische Charakter der Spezifikationsberichte deutlich hervorgehoben.

Die Spezifikationsberichte sind das Ergebnis von interkommunalen Arbeitsgruppen, in denen die beteiligten Transferkommunen kooperativ zusammengearbeitet haben. Die Grundlage der Berichte sind die konkreten Entwicklungs- und Implementierungsaktivitäten der Kommunen, die an der jeweiligen Arbeitsgruppe beteiligt waren. Die Definition und Konkretisierung der jeweiligen Inhalte der Spezifikationsberichte erfolgte gemeinsam mit der Transferagentur. Um die Berichte auf ein solides Fundament

¹ In dem vorliegenden Dokument wird aus Gründen der besseren Lesbarkeit auf die gesonderte Nennung beider Genera verzichtet. Bei Nennung nur einer grammatikalischen Form sind grundsätzlich sowohl weibliche als auch männliche Personen gemeint.

² Der Begriff „Kommunen“ wird hier als Oberbegriff für alle kommunalen (Gebiets-)Körperschaften, wie Gemeinden, Kreise, kreisfreie Städte oder Kommunalverbände mit eigenen Selbstverwaltungsaufgaben, verwendet (vgl. Andersen 1997, S. 174).

zu stellen, wurden diese von Anfang an mit Experten aus Kommunen, Verbänden, Wissenschaft und Wirtschaft abgestimmt. Hiermit geht die Zielstellung einher, einen möglichst breiten Konsens herzustellen und somit eine Doppel- oder Parallelarbeit an Spezifikationen in verschiedenen kommunalen Gremien zu vermeiden. Dies schont wertvolle Ressourcen und reduziert aufwändige und – aufgrund oftmals verfestigter Interessenlagen – mühselige Ex-Post-Abstimmungen mit ungewissem Ausgang. Überdies ist im Falle verwaltungsebenenübergreifender Anwendungen und Verfahren die frühzeitige Kooperation bei der Erstellung von Spezifikationen zwingend.

Vor diesem Hintergrund wurden die Spezifikationen in allen relevanten Harmonisierungsvorhaben mit den Vertretern der nationalen Gremien (z. B. TeleTrust, DIN, OSCI-Leitstelle) diskutiert und mit den Arbeitsgruppen der Initiative Deutschland-Online abgestimmt. Außerdem wurde bei der Erarbeitung der Spezifikationen der Sachverstand der Vertreter der MEDIA@Komm-Regionen Bremen, Esslingen und des Städteverbundes Nürnberg hinzugezogen, sofern dies inhaltlich geboten schien und alle Beteiligten dies als sinnvoll ansahen.

1.2 Gegenstand und Bearbeiter des Spezifikationsberichts „Elektronische kommunale Poststelle“

Der vorliegende Bericht beschreibt die technischen, funktionalen und organisatorischen Anforderungen beim Aufbau und Betrieb einer elektronischen kommunalen Poststelle. Die eKomP stellt eine wesentliche Voraussetzung und einen zentralen Bestandteil bei der Gewährleistung einer sicheren, vertraulichen und rechtsverbindlichen Kommunikation zwischen der Kommune und ihren Partnern dar. Als virtueller und zentraler Postein- und -ausgang der Kommune ist die eKomP eine Ergänzung der bestehenden Zugangsmöglichkeiten zu kommunalen Dienstleistungen für alle Akteure. Die eingehenden Daten werden gemäß den rechtlichen Vorgaben behandelt und zur elektronischen Weiterverarbeitung innerhalb der Kommunen bereitgestellt.

Eine Arbeitsgruppe mit einer vergleichsweise großen personellen Zusammensetzung hat im Verlaufe der Projektzeit zusammengetragen, was nachfolgende Kommunen beachten sollten, wenn sie sich an die Aufgabe machen, eine eKomP einzurichten. Die Besetzung der AG erfolgte durch eine freiwillige Beteiligung der mitwirkenden Kommunen.

An der Erstellung des Spezifikationsberichtes wirkten mit:

- für die federführende Transferkommune Saarbrücken:
 - Frau Petra Carl, Mitarbeiterin im Hauptamt;
 - Frau Nunzia Lombardo-Schnur, Mitarbeiterin im Personal- und Organisationsamt;
 - Herr Klaus Schirra, Mitarbeiter im Informations- und Kommunikationsinstitut;
- für die beteiligte Transferkommune Hagen:

- Herr Gerd Thureau, Mitarbeiter im Hagener Betrieb für Informationstechnologie;
- Frau Ina Tepper, Mitarbeiterin im Hagener Betrieb für Informationstechnologie;
- für die beteiligte Transferkommune Oldenburg:
 - Herr Thorsten Roskamp, Datenschutzbeauftragter im Zweckverband Kommunale Datenverarbeitung;
- für die beteiligte Transferkommune Ostalbkreis:
 - Frau Tanja Breitmeier, E-Government-Beauftragte;
- für die beteiligte Transferkommune Rosenheim:
 - Herr Manfred Grundei, Leiter des Amtes für Informationsverarbeitung;
- für die beteiligte Transferkommune Würzburg: Dr. Bernd Schmitt, Leiter des Projektes <Würzburg integriert!> der Stadt Würzburg;
- Herr Herbert Benz, KommWis GmbH im Auftrag des Städtetages Rheinland-Pfalz;
- unterstützend von der Transferagentur:
 - Herr Dr. Helmut Drücke, Mitarbeiter im Bereich Public Services der Capgemini Deutschland GmbH;
 - Herr Robert Wilke, Mitarbeiter im Bereich Public Services der Capgemini Deutschland GmbH;
 - Herr Dr. Norbert Niemeier, Koordinator bei der Erstellung der Berichte, Mitarbeiter im Bereich Public Services der Capgemini Deutschland GmbH.

Die Autoren danken Herrn Dr. Martin Hagen, E-Government-Referat beim Senator für Finanzen der Freien Hansestadt Bremen und Herrn Jan Hegewald, sd&m AG, für wertvolle Anregungen zu diesem Spezifikationsbericht.

Nach der Einleitung, in der der Projektrahmen und das Projektziel der Harmonisierung von Vorhaben von *MEDIA@Komm-Transfer* erläutert werden, wird das Verfahren eKomP ausführlich und unter verschiedenen Aspekten vorgestellt. Kapitel 3 beschreibt die Funktionalität und die Einsatzfelder, benennt den Nutzen für verschiedene Nutzergruppen und diskutiert die Frage der Wirtschaftlichkeit. Inwiefern sonstige Harmonisierungs- und Standardisierungsaktivitäten auf diesem Feld berücksichtigt werden müssen, wird ebenfalls erörtert.

Das Kapitel 4 stellt die technischen, funktionalen und organisatorischen Anforderungen der eKomP dar. Damit bildet dieses Kapitel das Kernstück des Spezifikationsberichts. Wo immer sinnvoll, werden Praxisbeispiele aus den Transferkommunen eingestreut.

2 Harmonisierung im Rahmen der Initiative *MEDIA@KommTransfer*

Harmonisierung ist – wie eingangs dargestellt – neben der Verbreitung und der Internationalisierung eine der drei Hauptaktivitäten der Initiative *MEDIA@Komm-Transfer* des Bundesministeriums für Wirtschaft und Technologie (BMWi, vormals Bundesministerium für Wirtschaft und Arbeit, BMWA).

Diese Initiative ist ein wesentlicher Pfeiler der Bemühungen der Bundesregierung, eine leistungsfähigere und dabei kostengünstigere öffentliche Verwaltung zu schaffen. *MEDIA@Komm-Transfer* unterstützt im Rahmen von Deutschland-Online die Modernisierung der Kommunalverwaltungen in Deutschland. Ein selbstorganisierter Prozess der Entwicklung und Verbreitung von E-Government-Verfahren wird in Gang gebracht, der geeignet ist, Verwaltungsvorgänge zu vereinfachen, die Beteiligungsmöglichkeiten für die Bürgerinnen und Bürger zu fördern und die Nachfrage bei Hard- und Softwareherstellern sowie bei Dienstleistern zu erhöhen.

MEDIA@Komm-Transfer soll dazu beitragen, die Entwicklung von E-Government bundesweit zu beschleunigen und zu harmonisieren sowie die Position des E-Government-Standorts Deutschland im internationalen Wettbewerb zu verbessern.

Durch die Verknüpfung besonders viel versprechender kommunaler und regionaler Initiativen zu einem länderübergreifenden E-Government-Netzwerk sollen der Transfer von Best Practice-Verfahren und von Know-how erleichtert, Standards weiterentwickelt und Selbstorganisationsprozesse für die weiterführende Verbreitung angestoßen werden. Gleichzeitig soll die Zusammenarbeit mit der Wirtschaft intensiviert werden, damit das Wachstums- und Beschäftigungspotenzial von E-Government genutzt werden kann. Dies schließt auch die Vertiefung internationaler Kontakte und Kooperationen zur Förderung der digitalen Integration Europas und die Erschließung neuer Exportchancen mit ein.

Die zwanzig *MEDIA@Komm-Transfer*-Kommunen, welche im Jahre 2003 im Rahmen einer Interessenbekundung von einer unabhängigen Jury, gebildet von Vertretern der kommunalen Spitzenverbände,³ des BMWi und der Wissenschaft, ausgewählt wurden, entwickeln Verfahren und Komponenten. Sie beschreiben diese unter technischen, funktionalen und organisatorischen Gesichtspunkten.

Zur Unterstützung und Koordination der dezentralen Aktivitäten in den Transferkommunen wählte das BMWi die Unternehmensberatung Capgemini als Transferagentur für die mehr als zweijährige Laufzeit des Projekts *MEDIA@Komm-Transfer* aus.

Die Harmonisierungsvorhaben im *MEDIA@Komm-Transfer*-Projekt haben eine wesentliche Bedeutung in der Herausbildung von zukunftsfähigem E-Government, das

³ Die kommunalen Spitzenverbände haben sich beim letzten Wahlgang ihrer Stimme enthalten.

als integriertes, nutzenorientiertes und wirtschaftliches E-Government – fokussiert auf medienbruchfreie Transaktionen – zu verstehen ist.

Harmonisierung bedeutet, jenseits der historisch gewachsenen, zum Teil gravierend unterschiedlichen Lösungsansätze, einzelne Verwaltungsverfahren bzw. Komponenten in ihren wesentlichen Anforderungen zu spezifizieren. Es werden funktionale und technische Anforderungen sowie die organisatorischen Voraussetzungen zur Gewährleistung einer rechtsverbindlichen, authentifizierten und sicheren Transaktion zwischen kommunaler Verwaltung und ihren Kunden ausreichend und detailliert dargestellt.

Nach Maßgabe des in Art. 28a Grundgesetz verbrieften kommunalen Selbstverwaltungsrechts und des sich daraus ableitenden, spezifisch kommunalen Vergaberechts können weiterreichende Ziele, wie etwa eine für die Kommunen und Marktteilnehmer verbindliche Standardisierung von Verfahren und Komponenten, nicht verfolgt werden. Standardisierungen kann es unter den verfassungsrechtlichen Rahmenbedingungen in Deutschland nur für die Bundesverwaltung und die Landesbehörden in ihrem rechtlichen Wirkungsbereich geben. So können sich Bundes- und Landesverwaltungen dazu verpflichten, zur Unterstützung der internen wie externen Aufgabenverrichtung und Kommunikation standardisierte Verfahren und Produkte beispielsweise aus der XÖV-Welt zu verwenden. Gegenüber den Kommunen wird es dagegen immer nur ein Angebot geben, ein einheitliches Verfahren zu nutzen.

Von zentraler Bedeutung ist die Präzisierung unterschiedlicher Themenstellungen in den Spezifikationsberichten, sei es in technischer, funktionaler oder organisatorischer Hinsicht. Dies bedeutet, dass durch die Spezifikationsberichte eine Klärung der Semantik erfolgt. Bestehende Ansätze und Lösungen werden konkret für die Kommunen beschrieben und ausgearbeitet. Diese können als Richtschnur für das Handeln der Kommunen dienen. Über spezifische Anpassungen können einzelne Kommunen die Inhalte der Spezifikationsberichte auf ihren konkreten Bedarf hin ausrichten (siehe Abbildung 2).

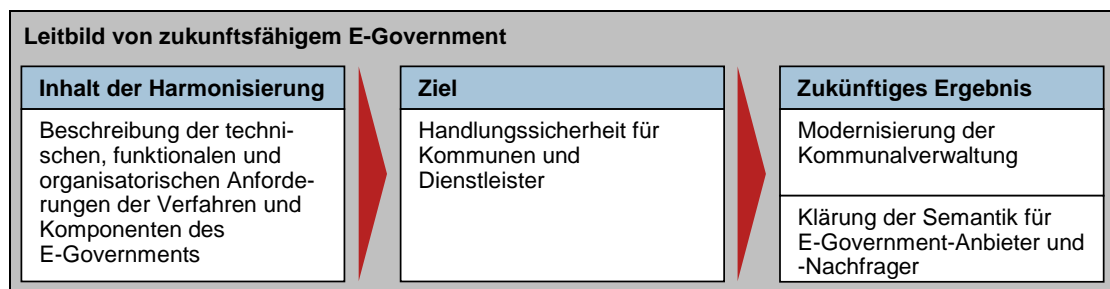


Abbildung 2: Der Beitrag der Harmonisierungsvorhaben zur Fortentwicklung des E-Governments

Weiterhin besteht die Hoffnung, dass die mit den Spezifikationsberichten gegebene Harmonisierung der Verfahren dazu führen wird, dass Kommunen ihre Ausschreibungen weitgehend nach diesen harmonisierten Verfahren ausrichten und Softwarehersteller zunehmend ihre Produkte entsprechend der Verfahrensbeschreibungen

entwerfen bzw. anpassen. Dies ist ein Beitrag, um dem Flickenteppich aus Einzellösungen durch eine relative Vereinheitlichung der Vorgehensweisen und der Softwareprodukte – oder zumindest deren Schnittstellen – entgegen zu wirken.

Harmonisierungsaktivitäten bewegen sich strikt im vorwettbewerblichen Raum, dienen aber dazu, den Wettbewerb transparenter zu gestalten. Harmonisierung trägt somit dazu bei, das Handlungsfeld für Kommunen wie für Produkt- und Dienstleistungsanbieter transparent zu gestalten und einen gemeinsamen Bezugsrahmen für Angebot und Nachfrage zu schaffen.

Was ist nun der Gegenstand der Harmonisierung? Betrachtet werden die technischen, funktionalen und organisatorischen Anforderungen an das jeweilige Verfahren. Nur wenn der Datenaustausch aufgrund einheitlicher Protokolle und eindeutiger semantischer Festlegungen erfolgt, können Transaktionen medienbruchfrei und mit gegenüber heutigen Verhältnissen erheblich verringertem Aufwand durchgeführt werden. Zukunftsfähiges E-Government ist ferner nur möglich, wenn die Geschäftsprozesse innerhalb der Verwaltung und in den Kooperationen mit externen (privaten oder öffentlichen) Akteuren angepasst sind. Eine wesentliche Aufgabe der Spezifikationsberichte besteht folglich darin, für die jeweiligen Harmonisierungsvorhaben die technischen und funktionalen Merkmale der Verfahren bzw. Komponenten zu definieren und die organisatorischen Voraussetzungen zu identifizieren, die einen Datenaustausch und einen optimierten Geschäftsprozess möglich machen sowie die Funktionalität des Verfahrens sicherstellen.

3 Beschreibung des Verfahrens „Elektronische kommunale Poststelle“

3.1 Definition und Funktionalität

Die Elektronische Kommunale Poststelle (eKomP) stellt als zentrales E-Mail- und OSCI-Transport-Gateway⁴ sowie als Dienstleister für Web-Applikationen eine zentrale Basiskomponente zur Abwicklung einer sicheren, nachvollziehbaren und vertraulichen Kommunikation zwischen kommunalen Behörden und externen Kommunikationspartnern dar.

Die eKomP unterstützt damit die Kommunen bei den wichtigen Fragen der elektronischen Zugangseröffnung und Zustellung⁵.

3.2 Einsatzfelder

Die eKomP ist für interkommunale elektronische und möglichst medienbruchfreie Bearbeitung von Prozessen eine Basisanforderung zur Gewährleistung der Rechtssicherheit im elektronischen Geschäftsverkehr. Ihre Aufgabe liegt in der Unterstützung der E-Government-Anwendungen bei der Abwicklung einer sicheren, nachvollziehbaren und vertraulichen Kommunikation zwischen zwei Partnern im Rahmen des E-Government-Angebotes behördlicher Dienstleistungen. Dabei wird den verschiedenen Akteuren (Behörden und deren externe Kommunikationspartner, wie Bürgern, Wirtschaft und anderen Behörden) eine komfortable Möglichkeit gegeben, ihren Geschäftsverkehr auf dem elektronischen Weg rechtssicher abzuwickeln.

Als virtueller und zentraler Postein- und -ausgang der Kommune ist die eKomP eine Ergänzung der bestehenden Zugangsmöglichkeiten zu kommunalen Dienstleistungen für alle Akteure. Die eingehenden Daten werden gemäß den rechtlichen Vorgaben behandelt und zur elektronischen Weiterverarbeitung innerhalb der Kommunen bereitgestellt. Weiter ist vorstellbar, dass die eKomP „Sicherheitsdienste“ für die dezentrale Verwendung, z.B. an einzelnen Arbeitsplätzen, zur Verfügung stellt.

3.3 Nutzen

In den letzten Jahrzehnten sind nahezu alle verwaltungsinternen Arbeiten informationstechnisch unterstützt worden. Verfahren für die wichtigen Querschnittsaufgaben einer Verwaltung stehen in großer Zahl zur Verfügung. Sie arbeiten allerdings über-

⁴ OSCI-Transport ist ein Kommunikationsprotokoll, das die Anforderungen der Sicherheit, Nachvollziehbarkeit und Vertraulichkeit erfüllt.

⁵ Siehe dazu auch die Berichte des Deutschen Städtetages.

wiegend noch auf der Basis einer Fallsachbearbeitung durch die Mitarbeiter in den Verwaltungen. Nun gilt es, den Bürger in einen elektronischen, rechtssicheren Kommunikationsprozess zu führen sowie die Sachbearbeitung durch transaktionsbezogene Dialoge mit dem Bürger zu vereinfachen und zu beschleunigen.

In diese Zielrichtung weisen immer mehr gesetzliche Regelungen (s. dazu ausführlicher unten im Text). Insbesondere für professionelle Nutzer wird die elektronische Kommunikation vorgeschrieben. Beispiele können schon jetzt aus dem Steuer- und Umweltbereich genannt werden. Auch Ausschreibungen und Vergaben sollen zukünftig elektronisch durchgeführt werden. Das heißt, dass auf die Kommunen in den nächsten Jahren ein verstärkter Handlungsdruck zukommen wird, elektronisch, rechtssicher und nachvollziehbar zu kommunizieren.

Zur Sicherstellung der Vertraulichkeit und Urheberschaft von Dokumenten spielen elektronische Zertifikate/ Signaturen und Verschlüsselungstechniken eine zentrale Rolle. Die eKomP unterscheidet sich von einem reinen Mailserver dadurch, dass sie mit signierten und verschlüsselten Dokumenten „umgehen“ kann und die notwendigen Quittungen über Ein- und Auslieferungen erstellt.

Eine besondere Herausforderung für die Kommunen, aber auch für die Landes- und Bundesverwaltung, besteht darin, die Entstehung mehrerer paralleler Lösungen zu vermeiden, die dieselben Funktionen abdecken. Aus strukturellen Gründen des Verwaltungsaufbaus in Deutschland besteht aber genau diese Gefahr. Einzelne Verwaltungsbereiche versuchen, für ihren Bereich Lösungen zu entwickeln. Beispiele sind das Steuer- und Kfz-Wesen, wo Bundes- und Länderbehörden Vorgaben machen. Auf die Kommunen als „Kunden“ dieser Lösungen kommt dann das Problem zu, verschiedene Systeme parallel zu betreiben. Das erhöht die Kosten unnötig. Eine eKomP kann, als standardisiertes Zugangstool eingesetzt, helfen, diese Kosten zu vermeiden und eine effiziente Lösung für den rechtssicheren Datenverkehr bereitzustellen.

3.4 Wirtschaftlichkeit

Bei der Wahl über die Einrichtung einer eKomP stehen Entscheider vor einem Dilemma. Sie müssen gleichzeitig zwei Aspekten genügen, die sich gegenseitig beeinflussen:

- **Handlungsdruck:** Dieser entsteht durch gesetzliche Vorgaben. Der Zugang zu einer Poststelle muss faktisch eröffnet werden, wenn sich die Kommune bei der Nutzung der elektronischen Kommunikation nicht inkonsequent verhalten will (s. unter anderem die entsprechenden Formulierungen in den Verwaltungsverfahrensgesetzen des Bundes und der Länder, § 3a). Für den Bürger bzw. die Wirtschaft ist informeller und rechtsverbindlicher E-Mail-Verkehr ohne nähere Ausführungen nur schwer nachvollziehbar.
- **Rechtfertigungsdruck:** Die aufzuwendenden Kosten müssen begründet werden.

Beide Ausgangssituationen müssen argumentativ unterstützt werden.

Im Folgenden soll der Fokus auf den Rechtfertigungsdruck gelegt werden, da die Fragen nach den Aufwänden und dem Nutzen einer eKomP kontrovers diskutiert werden. Zwangsläufig stehen bei der schwierigen Finanzlage der Kommunen Fragen nach den Synergieeffekten im Vordergrund. Oft wird dieser Aspekt als der einzig relevante für die Bewertung zur Einführung einer eKomP herangezogen.

Diese Betrachtungsweise, d.h. die Fokussierung allein auf den Wirtschaftlichkeitsaspekt, ist jedoch in diesem speziellen Falle nicht sinnvoll. Die Gründe hierfür sollen nachstehend ausgeführt werden:

Die Prozesse und Verwaltungsvorgänge, die über eine eKomP abgewickelt werden können, sind zur Zeit im kommunalen Umfeld zunächst nur rudimentär vorhanden – gezielte Prozess- und Organisationsbewertungen haben nur im Ansatz stattgefunden. Hinzu kommt, dass eine Verwaltung im Gegensatz zu privaten Firmen gezwungen sein wird, parallel für jeden in der eKomP platzierten Prozess auch den herkömmlichen, papiergebundenen Zugang aufrecht zu erhalten, um hier eine Diskriminierung (ältere Mitmenschen, Nicht-PC-BesitzerInnen, etc.) zu vermeiden. Zwei Prozesse für den gleichen Verwaltungsvorgang führen aber in der Regel nicht zu einer Kostenminimierung.

Für Prozesse, die ein Schriftformerfordernis aufweisen, muss der Nutzer der eKomP die qualifizierte elektronische Signatur zum Einsatz bringen. Alle angedachten Einsatzmöglichkeiten in diesem Bereich leiden aber unter der mangelhaften Verbreitung der Signatur in der Bevölkerung, was wiederum das Aufkommen hoher Nutzungszahlen – woraus sich eine Wirtschaftlichkeit ableiten lassen würde – verhindert. Zwar sind hier die mittelfristigen Aussichten durch verschiedene Aktionen privater und öffentlicher Protagonisten besser, kurzfristig ist jedoch mit einer signifikanten Ausweitung der Nutzerzahlen nicht zu rechnen.

Die Wirtschaftlichkeit könnte weiterhin durch zusätzliche Einnahmen erhöht werden, wenn sich für den Nutzer ein wirtschaftlicher Vorteil ergäbe, für den dieser bereit wäre zu bezahlen.

Der wirtschaftliche Betrieb einer eKomP wird aber zusätzlich dadurch in Frage gestellt, dass in einem zweiten Schritt notwendige Hintergrundsysteme für eine eKomP bereits in der Start- und Einrichtungsphase als unabdingbar angenommen werden. So werden regelmäßig im Zusammenhang mit der Einrichtung einer eKomP Kosten einer Archivierung und eines Workflow-Systems diskutiert, obwohl der Einsatz dieser mächtigen Systeme in der Startphase eher hinderlich als nützlich ist und auch alternative Möglichkeiten zur Verfügung stehen.

Zusammenfassend lässt sich an dieser Stelle feststellen, dass ein unmittelbarer wirtschaftlicher Synergieeffekt durch die Einrichtung einer eKomP eher nicht zu erwarten ist. Vielmehr sollten in der jetzigen Phase die Kommunen die sehr neue und innovative Technik erlernen und den Zeitgewinn dafür nutzen, die eigenen Prozesse zu analysieren und mit Blick auf einen elektronischen Datenaustausch neu zu strukturieren,

da eine identische elektronische Abbildung der papiergebundenen Prozesse alle Chancen auf Synergien verhindern würde. Daneben sollten sich die kommunalen Gebietskörperschaften mit dem Gedanken vertraut machen, gemeinsam mit anderen Kommunen eine eKomP zu betreiben, was den Nutzen und die Wirtschaftlichkeit erhöhen würde.

Im rechtlichen und internen organisatorischen Bereich (Dienstsanweisungen, Dienstvereinbarungen, Fragen der Zugangseröffnung, usw.) sind bisher nur Teilaspekte behandelt worden. Ein Weiterkommen ist hier nur zu erwarten, wenn gleichsam durch das Experimentieren mit der Technik und den ersten fortschrittlichen Bürgern die Probleme aufgezeigt werden. Es sollte also die Gunst der frühen Stunde genutzt werden, um sich rechtzeitig auf die Probleme von „morgen“ einzustellen, bevor die heutigen Mail-Massen in den rechtlich verbindlichen Bereich überführt werden.

3.5 Berücksichtigung sonstiger Harmonisierungs- und Standardisierungsaktivitäten

Standardisierungen finden auch auf regionaler und überregionaler Ebene statt. Unausgeglichene Haushalte und steigende Infrastrukturkosten zwingen Entscheidungsträger (Oberbürgermeister, Bürgermeister und Landräte) zur interkommunalen Zusammenarbeit. Projekte zwischen Städten, Städten und Landkreisen, usw. gewinnen zunehmend an Bedeutung. In einigen Bundesländern werden überregionale Ansätze forciert, die wegen der vorhandenen zentralen Infrastrukturen viel versprechende Möglichkeiten bieten. Anschließend werden einige Beispiele dazu vorgestellt.

Fokus 1: Zusammenarbeit im Saarland

Im Saarland haben sich Städte, Gemeinden, Kreise, der Stadtverband Saarbrücken und kommunale Spitzenverbände sowie landesweit tätige kommunale Institutionen zu einem Zweckverband „Elektronische Verwaltung für saarländische Kommunen ‚eGo-Saar‘“ zusammengeschlossen, um auf dem Gebiet von E-Government die Eigenkräfte der Mitglieder zu bündeln und zur Lösung der gemeinsam festgesetzten Prioritäten einzusetzen.

Unter dem Dach von eGo-Saar ist wegen der im Saarland nicht vorhandenen kommunalen Datenzentrale auch ein Fachkompetenzteam „Virtuelle Poststelle, elektronische Signaturen, elektronischer Rechtsverkehr“ institutionalisiert. Die Aufgabe dieses Kompetenzteams liegt darin, die notwendige konzeptionelle Arbeit für eine im Saarland gemeinsam zu nutzende eKomP vorzubereiten.

Die Transferkommune Saarbrücken ist in diesem Kompetenzteam ebenfalls vertreten und hat den Wissenstransfer zwischen dem Harmonisierungsvorhaben eKomP und den saarländischen Standardisierungsaktivitäten hergestellt.

Fokus 2: Zusammenarbeit in Rheinland-Pfalz

In Rheinland-Pfalz haben die kommunalen Spitzenverbände und das Land eine Zusammenarbeit im Bereich der Basistechnologie für E-Government-Anwendungen vereinbart. Konkret werden Lizenzen für den staatlichen und kommunalen Bereich für Middleware-Komponenten beschafft und auch gemeinsam betrieben. Zur Sicherstellung der Vertraulichkeit betreibt das Land das staatliche rlp-Netz. Die Kommunen wiederum sind im Kommunalnetz (KNRP) zusammengeschlossen. Zwischen beiden virtuellen privaten Netzen gibt es Gateway-Übergänge.

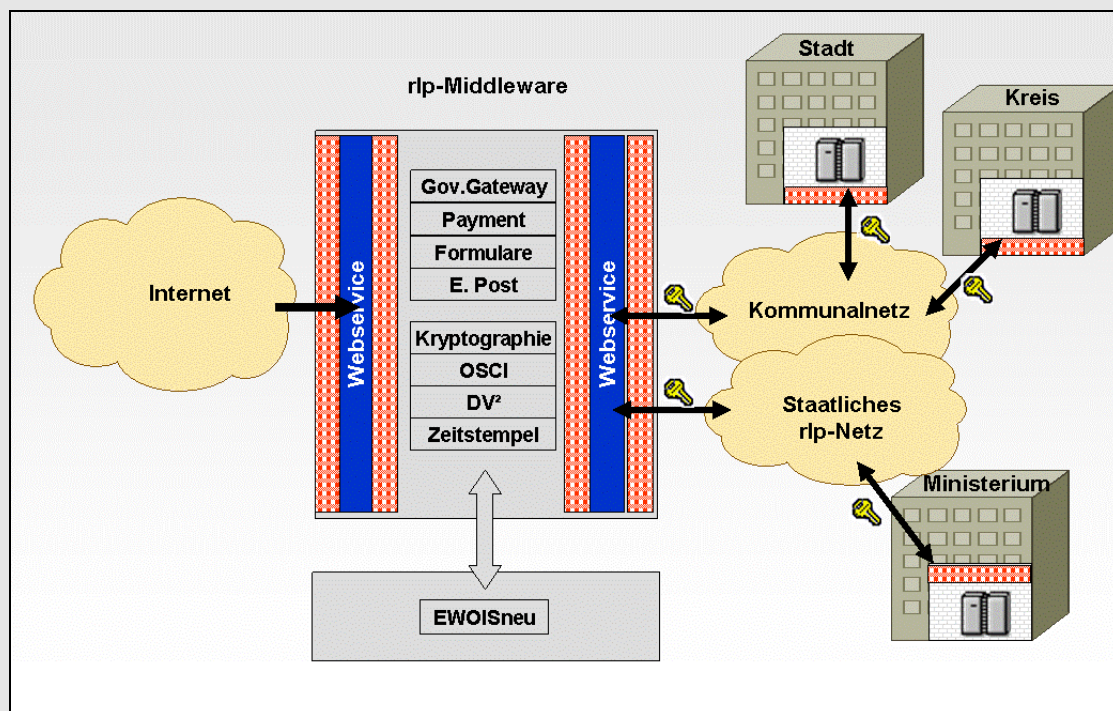
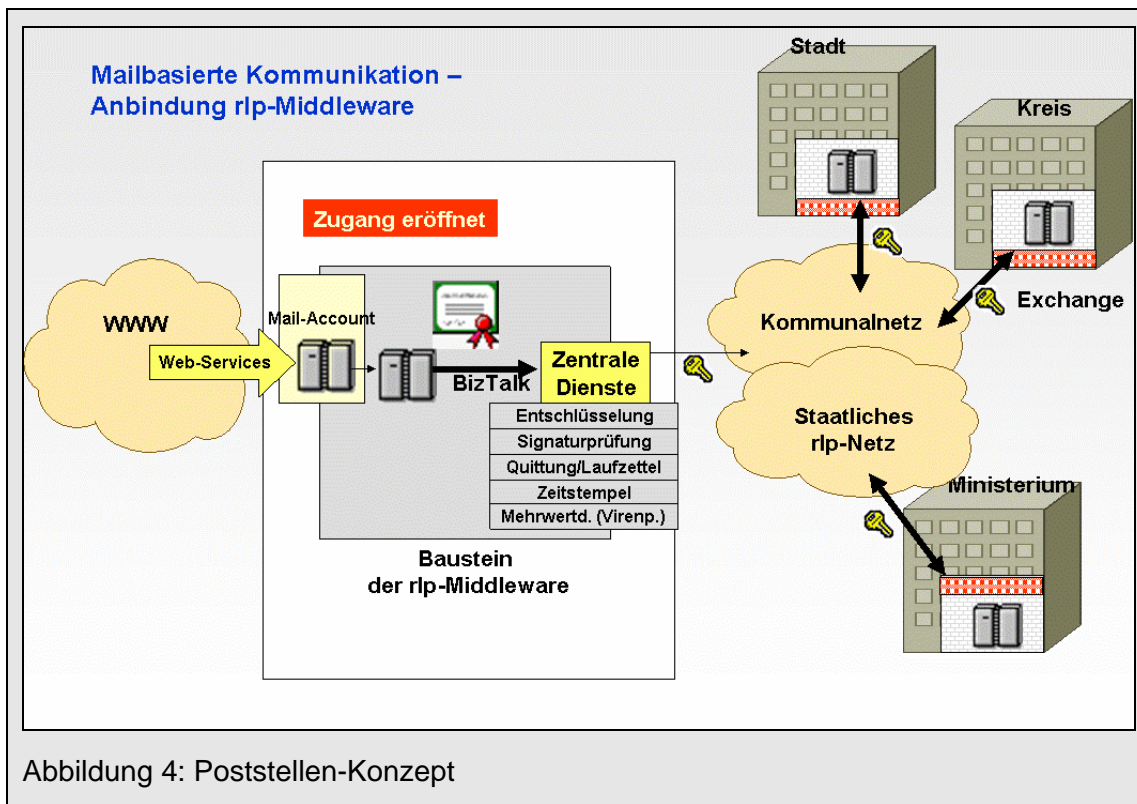


Abbildung 3: Netzverknüpfung in Rheinland-Pfalz

Beide Netze sind so gestaltet, dass eine verschlüsselte Datenkommunikation für den personenbezogenen Datenverkehr sichergestellt ist. Der flächendeckende Ansatz bietet die ideale Basis für die Umsetzung zentraler Modelle. Die eKomP wird in eine gesicherte Zone vor die Übergänge in das sichere staatliche und kommunale Netz gestellt. Damit können der Bürger und die Wirtschaft Post rechtssicher in der zentralen Poststelle, konkret in die Postfächer der Ministerien und Kommunen, einliefern. Die Post wird danach nach innen an die kommunalen und staatlichen Behörden weitergeben. Alle notwendigen Dienste (Signaturprüfung, Entschlüsselung, Quittungserstellung, Virenprüfung, SPAM-Filterung, usw.) werden über die zentrale Poststelle bereitgestellt. Der Übergang nach innen erfolgt über verschiedene Adapter. Von der reinen Mailweiterleitung bis hin zur XML-Übergabe an ein Dokumentenmanagementsystem muss dabei auf die jeweilige Anforderung reagiert werden können.



3.6 Gesetzliche Vorgaben

Bei Erstellung bzw. Aufbau einer eKomP sind neben den rein technischen/organisatorischen Voraussetzungen auch gesetzliche Festlegungen einzuhalten. Die wesentlichen gesetzlichen Vorschriften betreffen zum einen die gesetzliche Schriftform und zum anderen Regelungen zum Einsatz von Systemen der Informationstechnik.

Darüber hinaus ist zu beachten, dass immer mehr Fachgesetze die ausschließliche oder optionale Einführung elektronischer Kommunikation fordern. Dazu gehören z. B. die neue EU-Richtlinie zur Vergabe, das Justizkommunikationsgesetz, die Umsetzung des Kyoto-Protokolls und das Steuerwesen.

3.6.1 Gesetzliche Schriftform nach dem Verwaltungsverfahrensgesetz

Das Verwaltungsverfahren ist grundsätzlich formfrei (vgl. § 10 VwVfG). Es ist einfach, zweckmäßig und zügig durchzuführen und grundsätzlich nicht an bestimmte Formen gebunden. Ausnahmen ergeben sich aus besonderen Rechtsvorschriften, in denen eine bestimmte Form des Verfahrens vorgeschrieben wird. Eine solche Ausnahme regelt das Verfahrensrecht bereits selbst. Sofern eine Rechtsvorschrift die Schriftform anordnet, muss nach dem Signaturgesetz bei elektronischen Dokumenten eine qualifizierte elektronische Signatur angebracht werden (vgl. § 3a Abs. 2 Satz 2 VwVfG).

In fast allen Bundesländern wurden die Regelungen des Bundesrechtes in den jeweiligen Landesverwaltungsverfahrensgesetzen analog umgesetzt.

Da die Bundes- und Landesgesetze in hohem Maße das Schriftformgebot verankert haben und die notwendigen Signaturkomponenten noch nicht ausreichend in der Bürgerschaft und der Wirtschaft verbreitet sind, ergeben sich bei E-Government-Prozessen derzeit noch gewisse Anlaufprobleme. In Rheinland-Pfalz betreibt der Gemeinde- und Städtebund eine Rechtsdatenbank für seine Mitglieder. Um zu verdeutlichen, wie stark die formgebundenen Vorschriften das Verwaltungshandeln reglementieren, wurde eine Abfrage in diesem System auf das Online-Landesrecht Rheinland-Pfalz durchgeführt. In den landesrechtlichen Vorschriften war über 1.500-mal das Wort „schriftlich“ enthalten. Vor diesem Hintergrund wird die eKomP in Zukunft eine zentrale Rolle spielen. Die Mehrzahl der Anträge und Bescheide wird mit elektronischen Signaturen ausgestattet sein. Mit dem zentralen Dienst „Signaturprüfung“ übernimmt die eKomP eine zentrale Querschnittsaufgabe.

3.6.2 Übergreifende Gesetze und Verordnungen

Zu dieser Gruppe von Regelungen gehören die Gesetze und Verordnungen, welche die Barrierefreiheit, i. S. einer Gleichbehandlung behinderter Menschen, behandeln.

Zum 01.05.2002 ist das „Bundesgesetz zur Gleichstellung behinderter Menschen“ (BGG) in Kraft getreten. In § 11 BGG und der dazu erlassenen Bundesverordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung – BITV) werden gezielte Anforderungen an eine barrierefreie Informationstechnik (Intranet, Internet und Anwendungen) gestellt. Dass dieses Gesetz dringend Berücksichtigung bei vorhandenen, wie auch zukünftigen IT-Maßnahmen bedarf, ist u. a. aus dem in diesem Gesetz zugestandenen Verbandsklagerecht ersichtlich.

Eine Reihe von Bundesländern hat bereits in Anlehnung an die Bundesregelungen für ihren Aufgabenbereich eigene Landesgesetze und Rechtsverordnungen erlassen.

Im Detail auf die Spezifikationen, ihre Auswirkungen und Lösungsmöglichkeiten einzugehen, ist aufgrund der Ländervariationen und der Vielzahl möglicher Konstellationen einer eKomP nicht sinnvoll. In jedem Fall sind die jeweils gültigen Spezifikationen bei Beschaffung bzw. Modifikation einer „eKomP“ zu beachten.

4 Die Spezifikation des Verfahrens „Elektronische Kommunale Poststelle“

Im Rahmen der Spezifikation des Verfahrens werden die technischen, funktionalen und organisatorischen Anforderungen dargestellt. Damit wird die eKomP in ihren grundsätzlichen Merkmalen für den Know-how-Aufbau in den Kommunen beschrieben. Diese Spezifikation stellt aber keinen Ersatz einer detaillierten technischen Spezifikation für die Konzeption einer eKomP dar.

4.1 Technische Anforderungen

4.1.1 Interoperabilität

Allgemein ist Interoperabilität die Fähigkeit eines Systems oder einzelner Systemkomponenten, Informationen gemeinsam zu nutzen und kooperierend (Verarbeitungs-)Prozesse zu steuern. Im Zusammenhang mit E-Government ist ein Teil der Interoperabilität als die Fähigkeit einer Software zu verstehen, die elektronische Signatur für alle verschiedenen Systeme, die es am Markt gibt, einzusetzen. Interoperabilität bedeutet dabei auch, verschiedene Niveaus elektronischer Signaturen, elektronische Signaturen verschiedener Herausgeber (Trustcenter), Kartenleser sowie die entsprechenden Transportprotokolle zu verstehen.

Die eKomP stellt neben dem Internetauftritt einer Kommune das virtuelle Eingangstor zur Abwicklung des Schriftverkehrs eines Bürgers oder eines Wirtschaftsbetriebes zur Verwaltung dar. Um die digitalen Willenskundgebungen, Dokumente und Grafiken medienbruchfrei in den Verwaltungsablauf integrieren zu können, ist Interoperabilität ein wichtiges Grundziel.

Zur Wahrung der Interoperabilität muss die Poststelle das Zusammenspiel mit den inneren Verwaltungssystemen beherrschen. Dazu werden Schnittstellen benötigt, die Übergänge in den normalen Mailverkehr, die verwaltungsinternen Fachverfahren und ggf. Archivierungssysteme- und Dokumentenmanagementsysteme erlauben.

Die massiven Angriffe aus dem Internet zwingen eine Verwaltung, die Kommunikationskanäle von außen nach innen nahezu vollständig abzuriegeln. Standardprotokolle wie XML, SOAP, RMI können z.B. über die Standardports wie https transportiert werden. Diese Protokolle eignen sich für den Austausch mit den inneren Systemen. Für die auszutauschenden Daten muss zunächst eine Normstruktur gefunden werden, an Hand derer das XML-Schema erstellt wird.

Hier liegt derzeit noch ein Hemmschuh für die komplette verwaltungsseitige Implementierung von XML-Strukturen. In den letzten Jahren haben sich erst wenige normierte XML-Standards etabliert. Das Meldewesen bildet den Vorreiter. Über die OSCI-Leitstelle sind einige Aufgabenbereiche aus dem Melderecht (z.B. die elektro-

nische Rückmeldung über X-Meld 1.2, usw.) normiert worden. Im Bereich der Archivierung setzt sich zunehmend das Schema X-Domea durch. Auch im Bereich der Justiz gibt es das Format XJustiz.

4.1.2 Anbindung an die materielle Infrastruktur

Wie bereits in der Einleitung dargestellt, werden zwei Formen der elektronischen Poststelle unterschieden: die mail-basierte und die webbasierte. Anzumerken ist, dass in vielen Fällen ein Gemischtbetrieb die Regel sein wird. Es sollten beide Wege erschlossen werden, um so dem Bürger mehrere Kanäle der Einlieferung von elektronischer Post zu ermöglichen. Die mail-basierte Form dürfte allerdings nur zum Empfang von Nachrichten von einer Kommune Verwendung finden.

Die Nachweisführung einer E-Mail-Zustellung an den Bürger über dessen Provider stellt in der Praxis ein Problem dar. Aus diesem Grund wird für den Versand von elektronischer, „rechtssicherer“ Post an den Bürger oder Unternehmer letztlich nur die webbasierte Form greifen.

Ausgehend von dieser Erkenntnis wird nachfolgend auf beide Varianten und ihre technischen Anforderungen eingegangen.

E-Government-Komponenten können sicherheitstechnisch nur in einem abgeschotteten Zonenmodell betrieben werden. Gerade der Aufbau einer solchen sicherheitstechnischen Infrastruktur wird für viele kleinere Kommunen ein großes Problem darstellen. In einigen Bundesländern werden derzeit alternative Modelle geprüft, die zentrale E-Government-Komponenten zum Inhalt haben. Zentrale, mandantenfähige Systeme sollen unter Verwendung eines Portals so implementiert sein, dass sie gegenüber dem Bürger und der Wirtschaft als große Poststelle mit unterteilten Mandaten sichtbar werden. Die dort eingelieferte Eingangs- und Ausgangspost wird im Innenverhältnis über ein sicheres Netz (i. d. R. verschlüsselter VPN-Tunnel) unmittelbar an die Kommunen weiter geleitet.

In zentralen Zonenmodellen können die Verfügbarkeit und die erforderlichen Sicherheitslevels deutlich ökonomischer angeboten werden. Vorteile in der Beschaffung und in der Administration wirken sich finanziell positiv für kleinere Kommunen aus. Hinzu kommt, dass in vielen Kommunen nicht das notwendige Wissen vorhanden ist, um Systeme in dieser Komplexität zu betreiben.

Durch die Einrichtung von Sicherheitszonen erfolgt eine Transformation zwischen den Daten der äußeren Internetzone und den Fachverfahren.

Ein weiterer Punkt sei an dieser Stelle noch angesprochen. Der Systembetrieb kann ausgelagert und auf Dritte über ein Auftragsverhältnis übertragen werden.

Für die infrastrukturelle Anbindung⁶ ergeben sich folgende Alternativen:

⁶ Im Konzept „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ (Landesbeauftragter für den Datenschutz Niedersachsen 2004) werden im Kapitel 10 die Rahmenbedingungen konkretisiert.

- der Eigenbetrieb in einer Systemumgebung der jeweiligen Kommune,
- der Fremdbetrieb durch einen öffentlich-rechtlichen Dritten (kommunales oder staatliches Rechenzentrum),
- der Fremdbetrieb durch einen privat-rechtlichen Dritten,
- der Zentralbetrieb eines mandantenfähigen Poststellensystems durch einen zentralen öffentlich-rechtlichen Betreiber. Ob es Überlegungen gibt, diese Form auch privatrechtlich aufzusetzen, ist derzeit nicht bekannt.

4.1.3 Standardbausteine und Verfahren

Analysen der ersten E-Government-Projekte zeigen, dass gewisse Funktionen immer wieder bei der Umsetzung von E-Government-Prozessen benötigt werden. Es liegt daher nahe, Komponenten zu entwickeln, die quasi als Middleware Querschnittsaufgaben übernehmen.

Zu unterscheiden ist dabei zwischen Modulen, die innerhalb der elektronischen Poststelle notwendige Teilaufgaben übernehmen, Zustände feststellen sowie über Ergebnisse Rückmeldung geben (aufrufbare Module), und solchen, die gleichsam die Endverarbeitung – besser gesagt, die Übergabe von Daten an andere und von anderen Subsystemen (über Schnittstellen) – ermöglichen.

Bei den aufrufbaren Modulen sollten folgende Elemente nutzbar sein:

- Entschlüsselung:
eine Funktion zur Entschlüsselung der verschlüsselten Nachrichten unter Benutzung der von Zertifizierungsdiensteanbietern ausgestellten Zertifikate;
- Verschlüsselung:
Ermittlung des Verschlüsselungszertifikates des Kommunikationspartners und die Verschlüsselung;
- Signaturprüfung:
 - mathematische Signaturprüfung;
 - Zertifikatsprüfung;
 - einheitliche Prüfung von Mehrfachsignaturen;
- Signaturbildung;
- Prüfung auf schädliche Inhalte (Virenprüfung);
- Contentfilterung;
- Bereitstellung von Zeitstempeln;
- Nutzung interner Verzeichnisdienste;
- Einbindung in den normalen Mailfluss der Kommune (Übergabe an die Standard-Mailsysteme/ Übernahme von den Standard-Mailsystemen);

- Funktionen zur Authentifizierung von Benutzern/Administratoren.

Diese aufrufbaren Komponenten, insbesondere aber die kryptographischen Systemkomponenten, werden auch in anderen Subsystemen wie z.B. dem Formularservice oder auch in fachspezifischen Entwicklungen benötigt. Insoweit ist es besonders wichtig, dass bei der Auswahl dieser Komponenten Interoperabilität gegeben ist.

Der Bürger wiederum wirkt nur dann effektiv mit, wenn einheitliche Grundsysteme mit Wiedererkennungswert ohne hohen Administrationsaufwand E-Government-Aufgaben abwickeln. Der Bürger wird kein Verständnis dafür zeigen, falls er mehrere unterschiedliche Clientkomponenten installieren muss, nur weil es keine einheitliche Basis bei der Auswahl der E-Government-Basismodule gegeben hat.

Über bereitgestellte Schnittstellen sollen die unterschiedlichen Subsysteme der Kommunen erreichbar sein. Dies sind insbesondere:

- Formularservice:
 - Übernahme von Formularen bzw. Formulardaten in die eKomp;
- Archivierungssystem:
 - Überführung der Posteingänge in ein Archivierungssystem;
 - Überführung der Quittungen und Laufzettel in ein Archivierungssystem;
 - Überführung der Kopien der versendeten Postausgänge (Post aus den Fachämtern) ins Archivsystem;
- Dokumentenmanagement:
 - Überführung der Eingangspost aus der elektronischen Poststelle in ein Dokumentenmanagementsystem (DMS);
 - Übernahme von Postausgängen aus den DMS zum rechtssicheren Versand;
- Fachverfahren:
 - Über eine spezielle Schnittstelle sollte elektronische Post unmittelbar einem Fachverfahren zugeleitet werden können. Hier sind insbesondere die nicht formgebundenen Anträge zu nennen und zwar insbesondere solche, die in großen Mengen unmittelbar an eine Fachapplikation adressiert werden sollen (formlose Anträge, politische Meinungsumfragen, Bestellungen ohne Formblätter, usw.).

Die Schnittstellenanbindung sollte jeweils über ein normiertes XML-Schema oder einen SOAP-Zugriff realisierbar sein.

4.1.4 Normbedingte Anforderungen

Heute besteht bereits eine Vielzahl schriftlich fixierter Anforderungsprofile – zusammengefasst in DIN ISO-Normen, auf die zurückgegriffen werden kann.

SAGA (Standards und Architekturen für E-Government-Anwendungen) greift in seiner aktuellen Version im Wesentlichen auch auf diese Normen zurück, interpretiert diese und stellt diesen zum Teil bereits technische Realisierungsmöglichkeiten gegenüber. Erwähnung finden sollte auch der Kostenfaktor, d.h. SAGA ist kostenlos, während jede der DIN ISO-Normen in der Beschaffung nicht unerhebliche Kosten verursacht.

Welche Anforderungen und Norm(en) relevant sind, ist abhängig vom jeweiligen IT-Produkt zur Realisierung der eKomP.

An dieser Stelle folgt ein kurzer Exkurs zu zwei der wichtigsten DIN-Normen, die das Projekt „eKomP“ beeinflussen werden:

DIN Norm ISO 9241: Thematik „Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten“

Hierbei geht es im Wesentlichen um die Nutzungsfreundlichkeit einer Software.

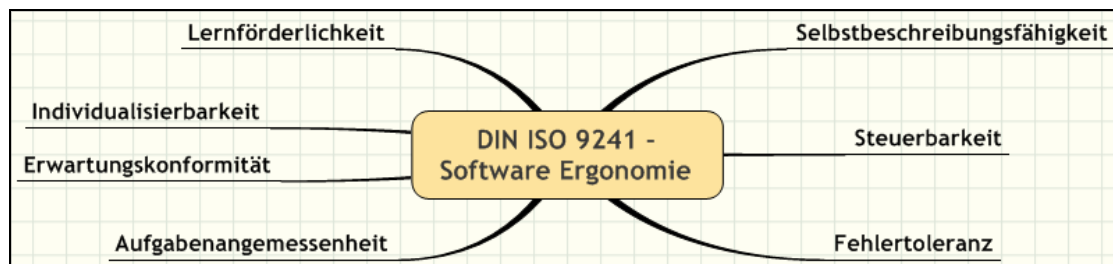


Abbildung 5: Übersicht DIN ISO 9241⁷

DIN Norm ISO 9126: Thematik „Softwarequalität“

Unter der ISO 9126 versteht man die Gesamtheit aller Merkmale, welche die Qualität einer Software definieren.

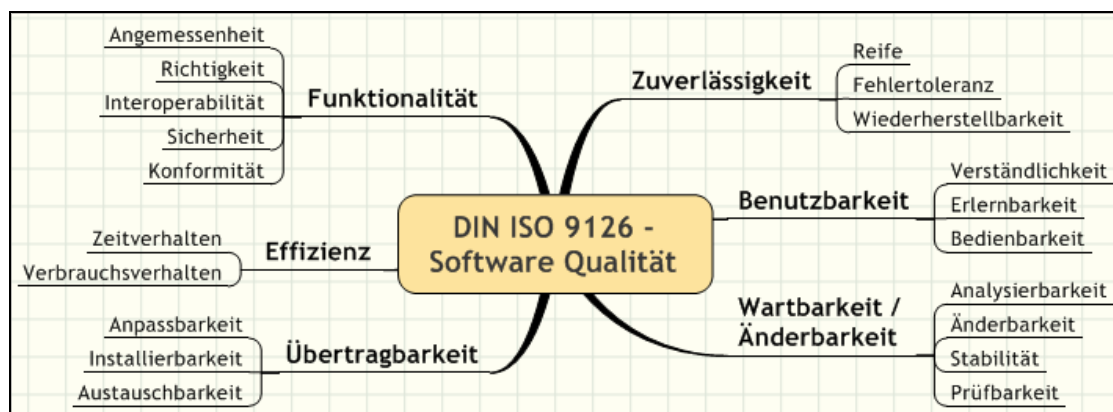


Abbildung 6: Übersicht DIN ISO 9126⁸

⁷ Vgl. DIN 2006.

⁸ Vgl. DIN 2001.

Welchen Stellenwert die einzelnen DIN-Normen bzw. -Segmente einnehmen bzw. welche weiteren Gesichtspunkte Beachtung finden, ist im IT-Kompetenzbereich und Strategiekonzept der jeweiligen Kommune verankert.

4.1.5 Sicherheitstechnische Anforderungen

Basisschutz

Der Basisschutz jeder IT ist unabdingbar. Durch zunehmenden IT-Einsatz, steigenden Vernetzungsgrad und immer höhere Leistungsfähigkeit der Technik werden die versehentlichen und vorsätzlichen Angriffe nicht nur häufiger, sondern nehmen auch in ihrer Gefährlichkeit zu. Die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) liefern hierzu auf fast 3000 Seiten alle erdenklichen Hinweise bzw. Prüfmöglichkeiten und beschreiben die erforderlichen Vorgehensweisen.⁹ Dank der vorbildlichen Gliederung können trotz des inhaltlichen Umfangs schnell die Problemfelder der eingesetzten IT-Systeme und deren Schutzverbesserungen mit Hilfe von Maßnahmenkatalogen auch für die eKomP ermittelt werden (siehe auch Anhang 1).

Transaktionsschutz

Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass der Datenschutz gewährleistet wird. Die unberechtigte Einsichtnahme, Speicherung, Veränderungen und der Verlust der Daten müssen ausgeschlossen werden. Hierzu gehören die schon oben genannten Schutzmaßnahmen gegen bösartige Programme, die Überwachung von Zugriffsregelungen und Berechtigungen und die automatische Datensicherung. Es muss jedoch angemerkt werden, dass jeder Benutzer von IT-Einrichtungen innerhalb seines Aufgabenbereiches grundsätzlich selbst für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist.

4.1.6 Zuverlässigkeit

Im Rahmen der technischen Anforderungen bestehen an die eKomP Forderungen, die unter dem Oberbegriff Zuverlässigkeit zusammengefasst werden können. Dabei lässt sich dieser Begriff in die Bereiche Transaktionsschutz, Informationsredundanz und Zuverlässigkeitserwartungen grob unterteilen.

Transaktionsschutz bedeutet dabei im engeren Sinne, dass jeder am Gesamtkomplex beteiligte Datenspeicher seinen eigenen Zustand sichern und zurücksetzen kann. Diese Sicherungsmaßnahmen können auch verteilt über Schnittstellen gewährleistet werden, um so die Rücksetz- und Wiederaufnahmemaßnahmen zu gewährleisten. Die hierfür erforderlichen Schnittstellen müssen gesondert beschrieben sein. Für den Bereich eKomP stellt dies einen hohen Anspruch dar, da ein Teil der pro-

⁹ Vgl. BSI 2006.

zessbeteiligten Komponenten nicht zwangsläufig im eigenen Einflussbereich liegen muss.

Zuverlässigkeitserwartungen haben etwas mit den Erwartungen der Nutzer und deren Anforderungen zu tun. Insofern müssten diese zunächst aus Nutzersicht spezifiziert werden. Zu den Grunderwartungen können im vorgenannten Zusammenhang die Funktionstüchtigkeit des Systems einer eKomP, der Support und das reibungslose, intuitive technische Handling des Systems gezählt werden. Diese Erwartungen müssen entsprechend der organisatorischen und strategischen Vorgaben im eigenen Umfeld funktions- und aufgabenbezogen ergänzt werden.

4.1.7 Leistungsfähigkeit und Ausfallsicherheit

Die Leistungsfähigkeit einer eKomP, auch als Performanz bezeichnet, beschreibt im Allgemeinen deren Leistung bezüglich des Bedarfs an Betriebsmitteln (Hardware) und der Qualität der Ausgabe. Die Anzahl der Nutzer einer eKomP dürfte anfangs wohl recht gering sein. Mittelfristig können aber hohe Steigerungsraten erwartet werden, so dass die eKomP bei einer hohen Last ihre Aufgaben ebenso effizient und damit ohne Verschwendung von Ressourcen erfüllen muss. Die eKomP muss derart skalierbar sein, dass sich bei einer Erhöhung der Benutzeranzahl keine nennenswerten Performanzeinbußen ergeben. Für die Skalierung der Hardware sind Parameter, wie z. B.

- die Anzahl der zu erwartenden E-Mails pro Tag,
- die durchschnittliche Größe der E-Mails und Dokumente in Megabyte (MB),
- die Anzahl der Transaktionen mit Krypto-Funktionen (Ver-/ Entschlüsselung)

von hoher Bedeutung. Als Faustregel gilt laut Aussage des BSI, dass die Bearbeitungszeit für verschlüsselte E-Mails bei Einsatz eines zentralen Verschlüsselungs- und Signatursystems für die kryptographische Behandlung ein-/ausgehender Nachrichten um etwa zehn bis dreißig Prozent gegenüber der Bearbeitung nicht verschlüsselter/ signierter Mails steigt.

Solange keine Erfahrungswerte vorliegen, sind hinsichtlich der o.g. Parameter grobe Schätzungen bzw. Annahmen vorzunehmen, um Richtwerte für die Last, die eine eKomP zu bewältigen hat, zu ermitteln. Um die Antwortzeiten des Systems bei mittlerer bis hoher Last grundsätzlich kurz zu halten, empfiehlt es sich bei einem modularen Aufbau einer eKomP, die einzelnen Dienste auf separaten Rechnern zu installieren (z. B. Trennung der Datenbank vom Kernsystem). Weitere Hinweise hierzu liefern u.U. auch die Produkthandbücher der Anbieter von eKomP-Lösungen.

Die Erhöhung der Sicherheit einer eKomP gegen einen Ausfall kann durch den Einsatz von technischen Redundanzen und organisatorischen Maßnahmen erreicht werden. Das BSI hält eine hohe Ausfallsicherheit und eine sehr hohe Verfügbarkeit

von Daten/System einer eKomP für erforderlich.¹⁰ Die maximal tolerierbare Ausfallzeit sollte dabei eine Stunde nicht überschreiten.¹¹ Eine entsprechend hohe Verfügbarkeit wird bei einer Disponibilität „rund um die Uhr“ (24 Stunden an sieben Tagen) mit einer maximalen Ausfallrate von zwei Ausfällen pro Jahr erreicht.¹² Technisch lässt sich die Ausfallwahrscheinlichkeit z.B. durch folgende Möglichkeiten minimieren:

- Bereitstellung einer zusätzlichen Komponente, die bei einem Ausfall zum Einsatz kommt. Beispielsweise ein unterbrechungsfreie Stromversorgung (USV) oder ein Notstromgenerator im Falle eines Stromausfalles.
- Redundante Auslegung der Hardware, z.B. durch Einsatz eines RAID5-Arrays (Redundant Array of Independent Disks), bei dem die Datensicherheit beim Ausfall einer Festplatte durch Verteilung der Daten und Paritätsinformationen auf mehreren Festplatten gewährleistet wird.
- Verwendung paralleler Komponenten, z.B. durch Konzipierung eines Failover-Clusters, bei dem bei einem Ausfall des ersten Systems das zweite System automatisch die Aufgaben des ersten übernehmen kann.

Für weitere technische Maßnahmen zur Erhöhung der Ausfallsicherheit wird auf das IT-Grundschutzhandbuch des BSI verwiesen.

4.1.8 Dokumentation

Der Betrieb einer eKomP stellt hohe Anforderungen an Sicherheit und Nachweisbarkeit hinsichtlich der ablaufenden Prozesse und der verarbeiteten Daten.

Diese Anforderungen können nur erfüllt werden, wenn eine Dokumentation vorhanden ist, die zum einen das Verfahren in Form von Konzepten, Regeln, Handbüchern, Anleitungen usw. in organisatorischer und technischer Hinsicht beschreibt („beschreibende“ Dokumentation) und zum anderen die tatsächlich ablaufenden Prozesse und dabei verarbeiteten Daten in Form von Protokolldateien, Prüfberichten, Versionslisten, usw. nachweisbar macht („protokollierende“ Dokumentation).

Dokumente der ersten Kategorie („beschreibend“) sollten mehr oder weniger bei allen IT-gestützten Verfahren vorhanden sein. Sie sind für den Betrieb der eKomP erforderlich und liefern vor allem Informationen für die Betreiber, Nutzer und Revisoren des Verfahrens.

Dazu gehören im Wesentlichen:

- ein Verfahrenshandbuch zur Beschreibung
 - der ablaufenden Prozesse,
 - der Datenstrukturen,

¹⁰ Vgl. BSI 2003, S. 54 f.

¹¹ Ebd.

¹² Ebd.

- der Fehlersituationen und -maßnahmen, usw.;
- ein Systemhandbuch mit Anweisungen/Hinweisen
 - zu Installation und Konfiguration der eingesetzten Komponenten,
 - zu Betrieb und Wartung des Verfahrens,
 - zur Datensicherung (Verfügbarkeit, Ausfallsicherheit, Wiederanlaufverfahren),
 - zu Komponenten der Anwendung (Hardware, Software, Infrastruktur),
 - zu Systemvoraussetzungen,
 - zu Herstellern und Ansprechpartnern, usw.;
- eine Bedienungsanleitung für
 - Administratoren der eKomP (Systemverwaltung mit Sonderrechten),
 - Benutzer der eKomP (Poststelle und sonstige interne Nutzer);
- ein Sicherheitskonzept mit
 - Sicherheitsrichtlinien, eingeordnet in das allgemeine Sicherheitskonzept,
 - Auflistung der Benutzer, Rechte, Gruppen, Profile usw.,
 - Hinweisen zur Revisionssicherheit (Nachvollziehbarkeit der Prozesse),
 - Richtlinien zum Datenschutz (Nachweisbarkeit);
- Regelwerke/Dienstvereinbarungen/Dienstanweisungen für u. a.
 - Festlegung der Postfächer,
 - Regelungen zu deren Organisation,
 - Regeln zum Einsatz von Signaturen,
 - Regelungen zur Zugangseröffnung, Zugangsbeschränkung (z.B. Dateiformate), usw.

Dokumente der zweiten Kategorie („protokollierend“) sind speziell für die Anwendung eKomP zwingend erforderlich. Sie dienen dazu, die Nachweisbarkeit, Vollständigkeit, Unversehrtheit und Widerspruchsfreiheit der vollzogenen Prozesse, verarbeiteten Daten und beteiligten Personen zu gewährleisten, d.h. letztendlich die Rechtssicherheit zu gewährleisten.

Dazu gehören:

- der Laufzettel¹³, welcher

¹³ Vgl. Landesbeauftragter für den Datenschutz Niedersachsen 2004, Kap. 8.8.

- generiert und mit Informationen versehen wird, während eine Nachricht die eKomP durchläuft,
- alle relevanten Operationen und Ergebnisse bei der Bearbeitung durch die einzelnen Module der Poststelle enthält,
- Zeitpunkte von Ereignissen (z.B. Signierung, Weiterleitung, Signaturprüfung, evtl. über Zeitstempeldienst) enthält,
- Ergebnisse der Signaturprüfung enthält,
- der jeweiligen Nachricht bzw. dem Dokument eindeutig zugeordnet werden muss,
- vor nachträglicher Manipulation geschützt sein muss,
- in Kopie auch dem Absender der Nachricht zusammen mit einer Empfangsquittung zugestellt wird;
- die Posteingangs- und -ausgangskontrolle:
 - dient wie ein normales Posteingangs-/ausgangsbuch dem Nachweis der empfangenen und versandten elektronischen Post,
 - enthält u. a. folgende Daten:
 - Datum/Uhrzeit Posteingang/-ausgang,
 - Absender/Empfänger,
 - Herleitungs-/Weiterleitungsinformationen,
 - Prüfergebnis laut Laufzettel,
 - Hashwert (wegen Integritätskontrolle) usw.
 - eine Empfangsquittung (optional): es ist empfehlenswert, dem Absender eine Quittung über den Empfang zukommen zu lassen bzw. ihn über fehlerhafte Nachrichten zu informieren;
- das Logging/Protokollieren der Ereignisse der eKomP, der Infrastruktur und evtl. beteiligter E-Government-Anwendung:
 - zur technischen Revision und Fehlersuche/-behandlung,
 - zur Protokollierung von Administratoraktivitäten (Revision),
 - zur Auflistung der Aktivitäten mit Zeitpunkt und aufgerufenem Prozess,
 - soll keine Inhaltsdaten,
 - darf nur personenbezogene Daten enthalten, soweit diese erforderlich sind;
- die lückenlose Aufzeichnung von Programmständen, Wartungsaktivitäten, Datensicherungsterminen, usw., welche:
 - im Wesentlichen zur technischen Revision und Fehlersuche/-behandlung dient,

- hilft, Datenverluste (Laufzettel, Posteingangs/-ausgangsdaten) zu vermeiden.

Mit einer derart breit und detailliert angelegten Dokumentation wird den Anforderungen an eine klare Berichterstattung und Handreichung zum Verfahren genüge getan.

4.1.9 Allgemeine Systemanforderungen

Die in einer eKomP verwendeten Komponenten sollten sich in die vorhandene materielle, funktionelle und organisatorische Intranet- und Internetstruktur der Kommune einfügen. Je nach Nutzergruppe differieren die damit verbundenen Anforderungen naturgemäß. Den „goldenen Mittelweg“ zu finden, ist die elementare Aufgabe des Projektteams bzw. der EDV-Abteilung, denn eine effiziente, kundenfreundliche und letztlich wirtschaftliche Bereitstellung von Verwaltungsleistungen ist das Ziel jeder Kommunalverwaltung.

Hinsichtlich Hardware und Software steht grundsätzlich die ganze Palette des Marktes zur Verfügung. Es sollten bei der Anschaffung eines solchen Systems aber in jedem Fall vermieden werden:

- unnötige Systemvielfalt in Hardware und Software,
- exotische, bzw. nicht den allgemeinen Standards (SAGA, etc.) entsprechende Hard- und Softwareprodukte (auch bezüglich Softwareentwicklungs- und Entwicklungsvorgaben),
- fehlende Anpassungsfähigkeit/Skalierbarkeit von Hard- und Software an geänderte Anforderungen,
- Softwareprodukte mit hohem laufenden Betreuungs- und Administrationsaufwand,
- diffizile, für den Nutzer nicht intuitiv bedienbare Softwareprodukte,
- nicht ausreichend definierte Rollenkonzepte,
- nicht bzw. nicht ausreichend berücksichtigte Normen,
- fehlende bzw. unzureichende Softwaredokumentation,
- fehlender bzw. unzureichender Softwaresupport,
- mangelnde Intranet-Integrationsfähigkeit,
- mangelnde Internet-Eignung (z.B. nicht browserbasierte Anwendung),
- mangelnde Hardware-Ausfallsicherheit, indem entsprechende Redundanzen geschaffen werden (Definition der Verfügbarkeitsrichtlinie, RAID, Spiegelung, etc.),
- fehlende Datenbankvernetzungen, damit Synergien durch Einmalerfassung geschaffen werden,
- nicht ausreichende Schutz- und Sicherheitsmaßnahmen (Firewall, Virens Scanner, Logfile, Verschlüsselung, Signatur, etc.),

- nicht realistisch konzipierte Datensicherungskonzeptionen und Recovery-Szenarien (Wiederherstellungszeitraum, -art, -umfang, -variabilität).

Einzelne der hier angesprochenen Punkte werden bereits in diesem Spezifikationsbericht mehrfach, jeweils unter anderen Gesichtspunkten angesprochen, daher wird von einer zusätzlichen Beschreibung abgesehen.

4.2 Funktionale Anforderungen

Die Sicherheitsziele der IT sind primär Vertraulichkeit, Verfügbarkeit sowie Verbindlichkeit mit den Teilaspekten Integrität, Authentizität und Nichtabstreitbarkeit bzw. Rechtssicherheit.¹⁴ Die Lösung zur technischen Absicherung der elektronischen Kommunikation besteht im Wesentlichen aus Verschlüsselung und Signaturen.

4.2.1 Verfügbarkeit

Unter Verfügbarkeit subsumiert man i.A. die Nutzbarkeit der für die elektronische Kommunikation benötigten technischen Einrichtungen. So muss sichergestellt sein, dass die technischen Komponenten der eKomP möglichst jederzeit durch Umsetzung technischer und organisatorischer Maßnahmen (z. B. redundante Auslegung der Hardware, regelmäßiges Backup) verfügbar sind. Konkrete Maßnahmenempfehlungen hinsichtlich der Verfügbarkeit sind dem IT-Grundschutzhandbuch des BSI zu entnehmen.

Im Rahmen eines sicheren Umgangs mit kryptographischen Schlüsseln ist ein entsprechendes Schlüsselmanagement erforderlich.¹⁵ So sind geheime und private Schlüssel vor Preisgabe und Modifikation zu schützen, indem bei der Schlüsselerzeugung keine schwachen Schlüssel generiert werden und bei einem Transport geheimer Schlüssel ein sicherer Kanal zwischen den Kommunikationspartnern gewählt wird. Um bei Verlust eines geheimen Schlüssels verschlüsselte Daten anschließend wieder verfügbar zu machen, kommen folgende Alternativen in Betracht:

- Eine sichere Aufbewahrung von Kopien der geheimen Schlüssel bei autorisierten Hinterlegungsinstanzen, durch die geheime Schlüssel bei Bedarf rekonstruiert werden können (key recovery).
- Festlegung von Vertreterregelungen, welche die Zugriffserlaubnis auf verschlüsselte Daten durch andere Mitarbeiter der Organisationseinheit bestimmen.
- Die zusätzliche Verschlüsselung eines vertraulichen Dokuments mit einem oder mehreren weiteren öffentlichen Schlüsseln, deren zugehörige private Schlüssel

¹⁴ Vgl. BSI 2004a, S. 11.

¹⁵ Vgl. BSI 2004b, S. 20.

sicher hinterlegt sind. Bei Bedarf ist dann eine Entschlüsselung des Dokuments mit einem der hinterlegten Schlüssel möglich (message recovery).

Zum Schutz vor einem schadhafte Code (Computerviren, Trojanische Pferde, usw.) ist die Installation eines aktuellen Virenschutzproduktes auf den eKomp-Endsystemen (Clients) zwingend erforderlich. Um unerwünschte und schadhafte Inhalte wirkungsvoll zu blockieren und zu eliminieren, ist die Virenschutzsoftware regelmäßig möglichst täglich zu aktualisieren.

Da die für die digitalen Signaturen verwendeten Hash- und Public-Key-Algorithmen mit der Zeit unsicher werden (können) und die Datenformate bzw. die Hard-/Software einem stetigen technischen Wandel unterliegen und ggf. nach einigen Jahren durch „modernere“ Formate bzw. Systeme abgelöst werden, ist bei der Realisierung einer eKomp das Problem der Langzeitaufbewahrung der Informationen zu berücksichtigen. Um die Daten so zu speichern, dass ihr Beweiswert erhaltend bleibt, sind die Signaturen entsprechend dem Signaturgesetz bzw. der Signaturverordnung zu erneuern. Die langfristige sichere Erhaltung von digitalen Informationen/Dokumenten bedingt ein detailliertes Gesamtkonzept, welches jedoch nicht Gegenstand dieses Spezifikationsberichts ist. Weitere Informationen bezüglich der Langzeitarchivierung elektronischer Dokumente sind unter www.archisig.de oder bei der Niedersächsischen Staatskanzlei, Planckstraße 2, 30169 Hannover erhältlich.

4.2.2 Vertraulichkeit

Das Sicherheitsziel „Vertraulichkeit“ steht für die Gewährleistung der Geheimhaltung von Daten und Informationen vor Unbefugten.¹⁶ Bei der alltäglichen, nicht elektronischen Kommunikation wird dies z.B. durch verschlossene Briefe erreicht. Im Fall der elektronischen Kommunikation besteht die Gefahr, dass E-Mails auf dem Weg vom Sender zum Empfänger von Unbefugten gelesen werden. Kritisch ist dies insbesondere, wenn sensible (personenbezogene) Daten (Gesundheitsdaten, Sozialdaten, usw.) ausgetauscht werden. In diesen Fällen kann eine vertrauliche Kommunikation nur durch Einsatz von Verschlüsselungstechniken, bei der der Klartext mit Hilfe eines Algorithmus in einen Geheimtext übersetzt wird, erreicht werden. Web-Seiten, über die eine individuelle Kommunikation stattfinden soll, sollten daher grundsätzlich per SSL-Verschlüsselung (Secure Socket Layer) auf der Basis des hierfür verwendeten Protokolls HTTPS abgesichert werden.¹⁷ Explizit für die sichere Datenübertragung im kommunalen Bereich existiert das im Rahmen des Projektes *MEDIA@Komm* entwickelte Protokoll OSCI (Open Services Computer Interface), welches für eine Web-Verbindung eine entsprechende Java-Anwendung auf dem Client voraussetzt. OSCI kann ebenso für die E-Mail-Kommunikation eingesetzt werden. Mit Hilfe eines OSCI-fähigen E-Mail-Programms werden die Nachrichten, einschließlich der Anhänge, verschlüsselt und per OSCI anstelle von SMTP (Simple Mail Transfer Protocol) an den

¹⁶ Vgl. BSI 2004b, S. 12.

¹⁷ Vgl. BSI 2004b, S. 14 ff.

oder die Empfänger übertragen. Für die verschlüsselte E-Mail-Kommunikation auf der Basis von SMTP bestehen grundsätzlich zwei Möglichkeiten:

- 1) Verschlüsselung der gesamten Nachricht, wobei hierfür das eingesetzte E-Mail-Programm mit verschlüsselten Nachrichten umgehen muss.
- 2) Chiffrierung einer Datei, die der E-Mail als Anhang beigefügt wird. Die Verschlüsselungsfunktionen können dann von einem speziellen Programm ausgeführt werden.

Um mit möglichst vielen Partnern vertraulich und unkompliziert kommunizieren zu können, ist der Einsatz eines Public-Key-Verfahrens, bei dem jeder Teilnehmer mit einem öffentlichen (jedermann zugänglichen) und privaten Schlüssel ausgestattet wird, unerlässlich. Voraussetzung für den sicheren Einsatz ist

- die Geheimhaltung des privaten Schlüssels, z. B. auf einer nicht auslesbaren Chipkarte,
- der Schutz des öffentlichen Schlüssels vor Veränderung sowie
- die verlässliche Zuordnung des öffentlichen Schlüssels zum Inhaber des privaten Schlüssels durch elektronische Zertifikate.

4.2.3 Authentizität

Man unterscheidet bei der Authentizität i.allg. zwischen der Authentizität der Daten und der des Kommunikationspartners. Erstere besagt, dass die Daten tatsächlich von dem entsprechendem Kommunikationspartner stammen. Herkömmlich wird dies z.B. durch die persönliche Unterschrift des Absenders des Briefs erreicht. Bei der elektronischen Kommunikation wird die Authentisierung der Daten durch digitale Signaturen und so genannte Message Authentication Codes (MACs), kryptographische Checksummen zur Nachrichtensicherung, gewährleistet.

	Absender	Empfänger	Herkömmliche Form (Bsp.)	Elektronische Form (Bsp.)
Absenderauthentizität:	Kunde	Behörde	Vorlage des Personalausweises	Signaturen
Empfängerauthentizität:	Behörde	Kunde	Einschreiben mit Rückschein	Signaturen

Tabelle 1: Absender- und Empfängerauthentizität¹⁸

¹⁸ Eigene Darstellung, Daten entnommen aus BSI 2004c, S. 10 ff.

Die Authentizität des Kommunikationspartners wiederum drückt aus, dass der Partner derjenige ist, der er vorgibt zu sein. Bei der Kommunikation zwischen Kunde und Behörde ist zwischen zwei Datenübermittlungsarten zu unterscheiden: vom Kunden (z.B. Bürger) zur Behörde und von der Behörde zum Kunden. Die Sicherheit hängt sowohl im herkömmlichen als auch im elektronischen Fall von der zuverlässigen Authentisierung des Partners ab.

Als grundlegende Authentisierungsmethoden kommen für die elektronische Kommunikation folgende in Betracht:¹⁹

- 1) Passwort bzw. PIN (aus Ziffern bestehendes Passwort): Hierbei handelt es sich um ein geheimes Kennwort, welches zur Authentisierung übertragen oder zur Freigabe des eigentlichen Authentisierungsmechanismus verwendet wird.
- 2) PIN/TAN: Beim PIN/TAN-Verfahren dient die persönliche Identifikationsnummer (PIN) zur Authentisierung des Benutzers beim Systemzugang, während die Transaktionsnummer (TAN) als Geheimzahl zur expliziten Freigabe eines konkreten Vorgangs benutzt wird. Die TAN verliert nach einmaliger Nutzung ihre Gültigkeit.
- 3) Signaturen: Für die sichere Authentisierung können elektronische Signaturen im Rahmen eines Challenge-Response-Verfahrens verwendet werden. Hierbei sendet das Computersystem der Behörde dem Computer des Kunden eine Challenge, die nur der Computer des Kunden mit der richtigen Signatur korrekt beantworten kann (Response). Dieses Verfahren wird z.B. auch bei der Authentisierung über SSL verwendet.

Eine Beschränkung auf die elektronische Signatur als ausschließliche Authentisierungsmethode für die eKomP ist nicht empfehlenswert. Weitere Möglichkeiten, z.B. PIN/TAN, sind mit Hinblick auf die möglichen Änderungen rechtlicher Rahmenbedingungen offen zu halten.

Wegen des schnellen technologischen Wandels empfiehlt sich die kontinuierliche Untersuchung der Authentisierungsmethoden auf ihre Aktualität.

4.2.4 Integrität

Integrität der Daten bedeutet, dass die Daten bei der Übertragung nicht verändert werden. Bei der elektronischen Kommunikation besteht die Gefahr, dass die übertragenen Daten vorsätzlich oder unbewusst verändert werden. Dies kann durch aktives Eingreifen von Außenstehenden oder durch einen technischen Übertragungsfehler erfolgen. Das Ziel des Integritätsschutzes ist, derartige Änderungen zu verhindern bzw. sie erkennbar zu machen. Technisch lässt sich die Integrität durch den Einsatz elektronischer Signaturen und MACs sicherstellen. Beide Mechanismen bilden einen fälschungssicheren, kurzen Wert, welcher an die ursprünglichen Daten angehängt

¹⁹ Vgl. BSI 2004c, S. 33 ff.

wird. Dieser ermöglicht es dem Empfänger zu erkennen, ob die Daten während des Transports verändert wurden.

4.2.5 Nichtabstreitbarkeit

Die Nichtabstreitbarkeit besagt, dass sowohl der Absender nicht bestreiten kann, Urheber der Daten zu sein, als auch der Empfänger nicht widerlegen kann, die Daten erhalten zu haben. Auf konventionellem Weg kann dieses z.B. durch die persönliche Unterschrift oder die Quittierung des Erhalts eines Briefes erreicht werden. Elektronisch wird dieses durch Signaturen erreicht, wobei qualifizierte Signaturen eine höhere Anforderung an die Sicherheit bei der Erzeugung und Möglichkeit der Zuordnung zum Unterzeichner ermöglichen. Während die qualifizierten Signaturen den handschriftlichen Unterschriften bezüglich der Beweiskraft gleichgestellt sind und damit die „Nichtabstreitbarkeit der Herkunft“ charakterisieren, stellt die Quittierung des Erhalts einer Nachricht durch Signaturen ein Beispiel für die „Nichtabstreitbarkeit des Erhalts“ dar. Da in manchen Fällen der Zeitpunkt des Erhalts wichtig ist (z.B. bei Widersprüchen), ist der Einsatz von Zeitstempeln, die als nachprüfbare Bestätigung gelten, dass bestimmte Daten zu einem bestimmten Zeitpunkt existiert haben, erforderlich. Sofern diese von einer vertrauenswürdigen Instanz ausgestellt werden (akkreditierte bzw. qualifizierte Zeitstempel), wird ein hohes Maß an Vertrauenswürdigkeit erreicht. Mit dem Signaturgesetz (SigG) wurde neben der qualifizierten Signatur auch der qualifizierte Zeitstempel beschrieben. Dieser garantiert rechtssicher, dass ein elektronisches Dokument nach dem Aufbringen der Signatur nicht mehr verändert wurde. Die Praxis zeigt zur Zeit, dass insbesondere aus wirtschaftlichen Gründen auf akkreditierte Zeitstempel verzichtet und stattdessen eine qualifiziert signierte Systemzeit als interner Zeitstempel verwendet wird.

Bisher sind den mitwirkenden Transferkommunen keine Vorschriften bekannt, die einen qualifizierten akkreditierten Zeitstempel durch ein Trustcenter vorschreiben. In den Bundesländern sollte daher der Dialog mit den zuständigen Justizministerien gesucht werden, um den technischen Standard der vor Ort anerkannten Zeitstempel in jedem Bundesland festzulegen.

Zugangseröffnung gemäß § 3a Verwaltungsverfahrensgesetz

Mit der Änderung des Verwaltungsverfahrensgesetzes (VwVfG) vom 21. August 2002 hat der Bund erstmals die Möglichkeit einer rechtsverbindlichen Kommunikation mit Bundesbehörden auf elektronischem Wege eröffnet.

Voraussetzung für diese Art der Übermittlung ist die Zugangseröffnung durch den Empfänger. Empfänger elektronischer Dokumente ist sowohl die Behörde auf der einen Seite als auch der Bürger auf der anderen Seite. Die Möglichkeit der elektronischen Übermittlung von Dokumenten setzt daher voraus, dass sowohl die Behörde als auch der Bürger den Zugang eröffnen.

Die Zugangseröffnung ist an objektive und subjektive Voraussetzungen gebunden. Die objektive Voraussetzung für die Zugangseröffnung ist das Vorhandensein einer

geeigneten technischen Einrichtung. Subjektive Voraussetzung für die Zugangseröffnung ist die Erklärung des Absenders, dass er elektronisch kommunizieren will. Beim Bürger erfordert diese Voraussetzung ein Tätigwerden in Form einer Freigabeerklärung gegenüber der Behörde. Nach der herrschenden Rechtsauffassung wird bei Behörden und Firmen diese Erklärung durch das Veröffentlichen von E-Mail-Adressen auf Briefköpfen und Internetseiten konkludent unterstellt. Aus diesem Grund sollten potenzielle Mailingpartner in geeigneter Weise darauf hingewiesen werden, auf welche Weise und mit welchen Formaten mit der Behörde kommuniziert werden kann. Dies kann durch Hinweis auf Briefbögen und Internetseiten als auch bei der Bereitstellung von herunterladbaren und ausfüllbaren Formularen auf File-Servern erfolgen.

Das durch Rechtsvorschrift angeordnete Schriftformerfordernis kann durch die elektronische Form ersetzt werden, soweit die Rechtsvorschrift keine anderen Regelungen enthält. Im Falle der elektronischen Übermittlung muss das Schriftstück mit einer qualifizierten Signatur nach dem Signaturgesetz (SigG) versehen werden.

Falls einer Behörde ein elektronisch übermitteltes Dokument nicht zur Bearbeitung geeignet erscheint, muss dies dem Absender mit der Angabe der geeigneten Form übermittelt werden. Gleichmaßen muss die Behörde ein Dokument in einer geeigneten Weise übersenden, wenn der Empfänger geltend macht, ein übermitteltes Dokument nicht bearbeiten zu können. Die erneute Übermittlung kann als geeignetes elektronisches Dokument oder als Schriftstück erfolgen.

Mehrere Bundesländer haben bereits auf die Änderung des VwVfG des Bundes reagiert und analog diesem ihre Verwaltungsverfahrensgesetze auf Landesebene geändert. In den übrigen Ländern befindet sich das Gesetz noch im Entwurfsstadium.

Sofern von der Verwaltung der elektronische Zugang eröffnet wurde (ausdrücklich oder konkludent), sind diverse organisatorische Maßnahmen unabdingbar. Als Beispiele können die Einrichtung von Postfächern, die regelmäßige E-Mail-Eingangskontrolle, Vertretungsregelungen bei Abwesenheit von Mitarbeitern und die Behandlung nicht geeigneter Eingänge genannt werden. Es ist zweckmäßig, diese Regelungen im Rahmen einer Kommunikationsordnung bzw. E-Mail-Dienstanweisung zu treffen (siehe auch Anhang 2).

Zur Eröffnung des Zugangs sei an dieser Stelle auf das Dokument „Eröffnung des Zugangs für die elektronische Kommunikation“ des Deutschen Städtetages²⁰ verwiesen, das eine ausführliche Beschreibung und Handlungsempfehlungen für die Zugangseröffnung beinhaltet.

Authentizität von ausgedruckten elektronischen Dokumenten

Das Bundesministerium des Innern hat ein Rundschreiben zu amtlichen Beglaubigungen von Dokumenten und Unterschriften gemäß den § 33 und 34 des VwVfG er-

²⁰ Vgl. Deutscher Städtetag 2003.

lassen. Dieses Rundschreiben vom 1. Oktober 2004 enthält u.a. Ausführungen für die amtliche Beglaubigung von Ausdrucken elektronischer Dokumente und für die amtliche Beglaubigung elektronischer Dokumente. Es richtet sich an alle Behörden des Bundes sowie die bundesunmittelbaren Körperschaften, Stiftungen und Anstalten des öffentlichen Rechts. Sein Inhalt ist auf die amtlichen Beglaubigungen durch die in § 1 des Landesgesetzes über die Beglaubigungsbefugnis vom 21. Juli 1978 (GVBl. S.597), zuletzt geändert durch Artikel 9 des Gesetzes vom 21. Juli 2003 (GVBl. S. 155), BS 2010-4, genannten Stellen grundsätzlich übertragbar.

Demnach sind für die amtliche Beglaubigung von Ausdrucken elektronischer Dokumente und für die amtliche Beglaubigung elektronischer Dokumente folgende Beglaubigungsvermerke notwendig:

- für die amtliche Beglaubigung von Ausdrucken elektronischer Dokumente ohne qualifizierte elektronische Signatur:
 - Beglaubigungsvermerk, der die Gleichheit bestätigt,
 - genaue Bezeichnung des elektronischen Dokumentes,
 - eine Einschränkung, für wen der Ausdruck bestätigt wird,
 - Ort und Tag der Beglaubigung,
 - Bezeichnung der Stelle, welche die Beglaubigung vornimmt,
 - Unterschrift und Dienstsiegel;
- für die amtliche Beglaubigung von Ausdrucken elektronischer Dokumente mit qualifizierter elektronischer Signatur:
 - Beglaubigungsvermerk, der die Gleichheit bestätigt,
 - genaue Bezeichnung des elektronischen Dokumentes,
 - eine Einschränkung, für wen der Ausdruck bestätigt wird,
 - Signaturschlüsselinhaberin bzw. Signaturschlüsselinhaber,
 - Zeitpunkt der Verbindung des elektronischen Dokumentes mit der qualifizierten elektronischen Signatur,
 - Art des der qualifizierten elektronischen Signatur zugrunde liegenden Zertifikates,
 - laufende Nummer des der qualifizierten elektronischen Signatur zugrunde liegenden Zertifikates,
 - Beginn und Ende der Gültigkeit des der qualifizierten elektronischen Signatur zugrunde liegenden Zertifikates,
 - Beschränkungen der Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang,
 - Attribute der Signaturschlüsselinhaberin bzw. des Signaturschlüsselinhabers,

- eine Einschränkung, für wen der Ausdruck bestätigt wird,
- Ort und Tag der Beglaubigung,
- Bezeichnung der Stelle, welche die Beglaubigung vornimmt,
- Unterschrift und Dienstsiegel.

4.3 Organisatorische Anforderungen

4.3.1 Allgemeine Anforderungen

Der Einsatz einer eKomP verändert die Arbeitsorganisation. Unter anderem werden betriebliche Kommunikationsnetze mit den Funktionen einer eKomP ausgeweitet.

Es ist daher geboten, die Einführung einer eKomP durch ein Projektteam vorbereiten zu lassen. Bei der Besetzung ist darauf zu achten, dass mindestens folgende Funktionsbereiche beteiligt sind: Organisation, Technik, Recht, Poststelle, Personalvertretung, Datenschutz und ggf. weitere Mitarbeiter aus den jeweils betroffenen Behördenbereichen.

Eine Zusammenarbeit mit ausgelagerten Einrichtungen und kommunalen Partnern sollte initiiert werden, um frühzeitig Vorbereitungen für eine gemeinsam kommunal zu nutzende eKomP treffen zu können. Im Saarland wird beispielsweise eine landeseinheitliche Lösung angestrebt.

Zu Projektanfang sollte die Klärung einer zentralen Frage stehen – und zwar, ob eine bisher durch Papierschriftlichkeit geprägte Ende-zu-Ende-Kommunikation nun auch unter Einsatz einer eKomP aufrecht erhalten werden soll und ggf. auch muss. Danach ergeben sich erst die Varianten, wie eine behörden- bzw. organisations- oder funktionsbezogene Kommunikation umgestaltet werden kann (Wahl des Standortes der eKomP).

Kann ganz auf eine Ende-zu-Ende-Kommunikation verzichtet werden, so wird eine einzurichtende zentrale eKomP kostengünstiger, weil die in diesem Spezifikationsbericht angesprochenen Rahmenbedingungen, insbesondere die technischen, nur einmalig eingesetzt werden müssen. Auch ist der Schulungsaufwand für das Bedienpersonal geringer.

Weiterhin ist zu entscheiden, ob eine durch die eKomP veranlasste Weiterleitung empfangener signierter und/oder verschlüsselter Nachrichten im Hausnetz offen oder neu verschlüsselt mit internem Verfahren an den Zielempfänger zugestellt werden soll.

Mit Klärung des Realisierungsbedarfs und damit einhergehend mit der Festlegung auf die Verwaltungsvorgänge, die über eine eKomP abgewickelt werden sollen, werden die Prozesse mit Blick auf den elektronischen Prozessaustausch neu strukturiert. Die hier getroffenen Festlegungen sind Anhaltspunkte für die Beurteilung des Schutzbedarfs (Datenschutzanforderungen).

Sollen über die eKomP auch Postausgänge abgewickelt werden, so ist zu klären, wie Mitarbeiter einer Kommune ihre Verwaltung durch eine elektronische Signatur vertreten, insbesondere im Außenverhältnis. In diesem Zusammenhang gilt zu beachten, dass entsprechend den gesetzlichen Vorgaben qualifizierte Zertifikate stets auf eine natürliche Person zurückzuführen sein müssen. Inwiefern Abstufungen bei der Kommunikation Verwaltung – Verwaltung möglich sind, bedarf einer Einzelfallbetrachtung. Für den Einsatz einer eKomP und zur Steuerung des Verwaltungshandelns sind Regelungen in Dienstvereinbarungen und Dienstanweisungen notwendig.

In der Dokumentation „Die Virtuelle Poststelle im datenschutzgerechten Einsatz“²¹ sind weitere zu berücksichtigende Regelungen zu finden.

Im Rahmen der durchzuführenden Projektdefinition und -konzeption sind Regelungen bezüglich des zu leistenden Supports unerlässlich. Hierzu gehören in der frühen Planungsphase– abhängig vom jeweiligen Grund- und Ausbaukonzept – Überlegungen zu dessen Art und Umfang, Leistungserbringer und -empfänger sowie den damit verbundenen laufenden Kosten. Insbesondere Art und Umfang des Supports für externe Kunden (Bürger, Wirtschaft, andere Kommunen) sind aufgrund des hohen Kundenpotenzials als kostenintensiv einzustufen und mit dem grundsätzlich in der jeweiligen Kommune zu leistenden „Bürgerservice“ in Einklang zu bringen.

4.3.2 Unterschiedliche Kommunikationsbeziehungen

In der nachfolgenden Betrachtung wird auf die verschiedenen Beteiligten in einem Kommunikationsprozess eingegangen.

Kommunikationsbeziehung Bürger – Verwaltung

Bei den organisatorischen Vorgaben an die eKomP lohnt sich zunächst ein Blick auf die reale (über viele Jahrzehnte gewachsene) herkömmliche Poststelle einer Kommune.

Es wird unterschieden zwischen der normalen Behördenpost, die von der Poststelle geöffnet, eingesehen und weitergeleitet wird, und den vertraulichen Informationen, die an besondere Personengruppen oder Dienststellen weiterzuleiten sind, ggf. auch verschlossen.

Bei der Adressierung von Schriftgut hat sich ein Adressierungsstandard entwickelt, der für den geübten Poststellenmitarbeiter sofort umsetzbar ist (Beispiel: persönlich und vertraulich, zu Händen, privat usw.).

Aus der realen Post lassen sich folgende Szenarien ableiten:

- 1) allgemeine Post, d.h. Post, welche die Standardadresse der Kommune erhält,
- 2) Post mit einer gewissen Zweckbindung des Absenders, z.B. Adresse mit dem Zusatz „zu Händen“,

²¹ Vgl. Landesbeauftragter für den Datenschutz Niedersachsen 2004.

- 3) Post mit einer deutlichen Zweckbindung an eine Person oder eine Aufgabe, Beispiele: „Herrn Mustermann, Stadt Musterstadt“ oder „An den behördlichen Datenschutzbeauftragten der Stadt Musterstadt“,
- 4) globale Informationen, welche die Qualität der Einlieferung konkretisieren (vertraulich, persönlich usw.).

In der virtuellen Welt gibt es diesen Adressierungsstandard nicht. Es fehlt der „Umschlag“ mit weitergehenden Informationen.

Nach Öffnung der Post werden in den meisten Kommunen Sichtvermerke unterschiedlichster Art (Bürgermeister, Büroleiter, Abteilungsleiter usw.) angebracht.

Ausgehend von den bisher bekannten technischen Standards lassen sich aus der realen Poststelle folgende Varianten auf die eKomp übertragen:

- 1) Allgemeine Post (Kommunikation: Bürger – Behörde): Post, die keiner speziellen Ansprechstelle zugeordnet wird, kann offen oder verschlossen an die Kommune adressiert werden. Sofern eine Vertraulichkeit der Inhaltsdaten erforderlich ist, muss die Einlieferung verschlüsselt erfolgen. Dazu bieten die beiden Poststellenmodelle (mail- oder webbasiert) verschiedene Varianten. In der mailbasierten Form benötigt der Absender das öffentliche Verschlüsselungszertifikat des Empfängers. Dazu sollte eine Kommune in ihrem Internetangebot das Zertifikat an zentraler Stelle bereitstellen. Um zu gewährleisten, dass auch im Vertretungsfall eine Öffnung einer verschlüsselten E-Mail erfolgt, kann ein nicht personenbezogenes, fortgeschrittenes Verschlüsselungszertifikat gewählt werden.

Bei der webbasierten Poststelle ist der Absender über das Internetangebot der Kommune auf das gewünschte Zielsystem zu führen. Die webbasierte Poststelle stellt über einen Transporttunnel die Vertraulichkeit sicher. Für diese Einlieferung benötigt der Absender keine Zertifikate.

Die korrekte Einlieferung der elektronischen Post muss in beiden Systemen durch Quittungsmechanismen bestätigt werden.

- 2) Aufgabenbezogene Post: Bei dieser Post wird eine Untermenge der behörden-spezifischen Zuordnung vorgenommen. Es werden quasi kleine Unterpoststellen eingerichtet, die eine effektivere Aufgabenzuordnung sicherstellen. Aus organisatorischer Sicht gibt es keine Unterschiede zur Variante 1.
- 3) Personenbezogene Post (Kommunikation: Bürger – Amtsperson): Bei dieser Form kann die Kommunikation bis zu einer natürlichen Amtsperson erfolgen. Für vertrauliche Post ist eine Verschlüsselung notwendig. Zur Verschlüsselung muss der Absender/Bürger bestimmte Daten des Empfängers/der Amtsperson kennen, konkret die E-Mail-Adresse und das personenbezogene Verschlüsselungszertifikat. Bestimmte Personenkreise besitzen einen besonderen Schutz für Ihre Post. Dazu zählen Personalratsmitglieder, Gleichstellungsbeauftragte und weitere Positionen mit Sonderaufgaben.

Für diese Personengruppen ist sicherzustellen, dass die elektronische Post immer durchgeleitet wird. Dieser Kommunikationsfluss wird auch als Ende-zu-Ende-Verschlüsselung bezeichnet.

Für den personalisierten Arbeitsplatz mit Verschlüsselung müssen alle Anforderungen erfüllt werden, welche die Sicherheit des Wirkbetriebes, insbesondere den Schutz vor Viren und Würmern, betreffen.

Bezogen auf die unterschiedlichen Poststellenmodelle ergeben sich keine echten Unterschiede. In beiden Varianten ist die ungeöffnete Post an den Empfänger durchzuleiten.

- 4) Sichtvermerke/Mitzeichnungen usw.: Ein besonderer Punkt ist die interne Organisation. Sichtvermerke, Kopieempfang oder andere Varianten der Unterrichtung müssen über die vorhandenen Mailsysteme abgebildet werden. Es gilt der Grundsatz, dass elektronische Post nach dem Durchlaufen der zentralen Dienste (Entschlüsselung, Signaturprüfung, Virencheck usw.) in den normalen Kommunikationsfluss einzubinden ist. Dazu müssen zwingend Schnittstellen bereitgestellt werden. Nach der Überleitung in den normalen Mailfluss greifen die Instrumente dieses Dienstes. Fehlen in dem Mailsystem diese Funktionalitäten, können diese ggf. auch von der eKomP erbracht werden.

Kommunikationsbeziehung Verwaltung – Bürger

Bei der Kommunikationsbeziehung Verwaltung – Bürger handelt es sich vom Grundsatz her um eine normale, klassische Mailkommunikation oder um eine Ende-zu-Ende-Kommunikation. Es gibt Fälle, in denen allerdings auch mehrere natürliche Personen gleichsam zu adressieren sind (beispielsweise: Ehepartner, Gesamtschuldner usw.). In diesen Fällen gilt der Grundsatz, dass letztlich jede Person einzeln zu betrachten ist.

Ein Hemmnis für die Kommunikation zum Bürger ist dessen Zugangseröffnung. Konkret kann eine Kommune nur dann mit dem Bürger in Kontakt treten, wenn er dazu sein Einverständnis erklärt hat.

Die Behörde muss sicherstellen, dass sie in der Lage ist, den Willen des Bürgers festzustellen. Es wird derzeit an verschiedenen Stellen darüber nachgedacht, die Information „Es ist ein Zugang eröffnet“ elektronisch zu speichern. Zentrale Landessysteme bieten dabei den Vorteil, dass ein Bürger auch global oder in einem größeren Rahmen den Zugang eröffnen kann, ohne dass er dies nochmals einzeln gegenüber jeder einzelnen Organisationseinheit erklären muss.

Kommunikationsbeziehung Verwaltung – Wirtschaft

Der Kommunikationsfluss entspricht letztlich der Kommunikation Bürger – Verwaltung. Jeder Adressat aus dem behördlichen Bereich muss sich darüber im Klaren sein, ob er ein Unternehmen global oder eine natürliche Person, beispielsweise den Geschäftsführer, adressieren will. Auch hier gilt: Wenn vertrauliche oder personenbe-

zogene Daten übertragen werden, muss ein verschlüsselter Transport sicher gestellt sein.

Kommunikationsbeziehung Verwaltung – Verwaltung

Bei der letzten Form der Kommunikation wird beidseitig die Fragestellung der organisationsbezogenen oder personenbezogenen Adressierung im Einzelfall zu klären sein.

Zudem wird zwischenzeitlich in einigen Rechtsvorschriften vom Gesetzgeber gefordert, dass bestimmte Sicherheitsmerkmale transportseitig gewahrt werden müssen. So muss ab dem 01. Januar 2007 beispielsweise die länderübergreifende Rückmeldung im Meldewesen mit dem Transportprotokoll OSCI sichergestellt werden.

4.3.3 Mögliche Betreibermodelle

Um für die eKomP Betreibermodelle²² zu definieren sowie deren inhaltliche Ausgestaltung vornehmen und insbesondere datenschutzrechtlich einordnen zu können, werden den Funktionalitäten der eKomP entsprechend dreier Rollen klassifiziert:

- 1) OSCI-Intermediär,
- 2) Operator,
- 3) Geschäftsstelle.

Die Ausprägungen und mögliche Betreibermodelle werden im Folgenden diskutiert.

Rolle als OSCI-Intermediär

Die OSCI-Kommunikation ist eine Funktionalität der eKomP, in der ein OSCI-Intermediär Nachrichten empfängt und weiterleitet bzw. sie in Postfächern zur Abholung bereitstellt. Entsprechend dem OSCI Transport 1.2-Protokoll können dabei OSCI-konforme Nachrichten ver- und entschlüsselt sowie Signaturen erstellt und geprüft werden. Darüber hinaus generiert der OSCI-Intermediär einen Laufzettel zur Protokollierung von Verbindungs- und Prüfinformationen. Der OSCI-Intermediär öffnet nur den „äußeren Briefumschlag“ einer OSCI-Kommunikation. Die Rolle als Intermediär ist datenschutzrechtlich als Teledienst zu bewerten. Dieser „Provider“ kann von einer öffentlichen oder nicht-öffentlichen Stelle betrieben werden.

Rolle als Operator

Der Operator öffnet und schließt Briefumschläge mit Inhaltsdaten und prüft elektronische Signaturen, welche die Integrität und Authentizität von Dokumenten und insbesondere Zertifikaten gewährleisten sollen. Technisch gesehen, entschlüsselt er eingehende verschlüsselte Nachrichten und verschlüsselt ausgehende Nachrichten, die im Klartext vorliegen. Darüber hinaus ist es Teil der Aufgabe, die mathematische Kor-

²² Vgl. Landesbeauftragter für den Datenschutz Niedersachsen 2004.

rektheit der Signatur sowie die Gültigkeit der zugehörigen Zertifikate zu prüfen. Entscheidend ist, dass der Operator Inhaltsdaten nicht gezielt zur Kenntnis nimmt, sondern automatisiert abarbeitet. Die Rolle als Operator ist datenschutzrechtlich nicht länger als Teledienst zu bewerten.

Der Operator kann von einer Behörde selbst betrieben werden oder im Rahmen eines Outsourcings durch einen Betreiber, der auch eine nicht-öffentliche Stelle sein kann, im Sinne einer Auftragsdatenverarbeitung erfolgen. Letzteres ist möglich, sofern das einschlägige Datenschutzgesetz die Verarbeitung personenbezogener Daten einer öffentlichen Stelle durch eine andere öffentliche oder nicht-öffentliche Stelle zulässt und dem Outsourcing zu einer nicht-öffentlichen Stelle keine übergeordneten Rechtsnormen entgegenstehen.

Rolle als Geschäftsstelle

Die Geschäftsstelle nimmt Inhaltsdaten und Prüfergebnisse vom Operator entgegen und wertet sie aus – etwa, um sie der zuständigen Stelle zukommen zu lassen. Die Rolle der Geschäftsstelle ist datenschutzrechtlich weder als Teledienst noch als Auftragsdatenverarbeitung zu bewerten. Da die Geschäftsstelle Inhaltsdaten eigenverantwortlich zur Kenntnis nimmt und auswertet, liegt beim Outsourcing eine Funktionsübertragung vor. Diese ist nur zulässig, sofern eine Übermittlungsbefugnis existiert.

Allgemeine Anforderungen bei Betrieb der eKomP durch Dritte

Bei einem Betrieb der eKomP durch Dritte ist der Umfang der Dienstleistung exakt zu definieren. Das Auftragsverhältnis zu dem Dritten wird durch einen Betriebsvertrag begründet. Dieser Vertrag sollte folgende Themen regeln:

- 1) möglichst konkrete Bezeichnung des Gegenstands des Vertrags (Auftragsdatenverarbeitung), Umfang und Grenzen der übertragenen Tätigkeiten;
- 2) Vereinbarungen hinsichtlich erforderlicher Nachweise über erbrachte Vertragsleistungen;
- 3) Regelungen zur Vertragsänderung und -verlängerung, insbesondere hinsichtlich vertraglicher Nebenpflichten oder über ein Vertragsende hinaus sicherzustellen der Leistungen;
- 4) Regelungen hinsichtlich eventueller Unterauftragsverhältnisse;
- 5) Verpflichtung auf die maßgebenden datenschutzrechtlichen Bestimmungen und Regelungen über die Voraussetzungen der Weitergabe von im Rahmen des Auftragsverhältnisses bekannt gewordener Daten;
- 6) Weisungs-, Prüfungs- und Kontrollrechte des Auftraggebers;
- 7) Prüfungs- und Kontrollrechte des für den Auftraggeber zuständigen Datenschutzbeauftragten;
- 8) sicherzustellende technisch-organisatorische Maßnahmen des Auftragnehmers;

- 9) Regelungen über gegenseitige Hinweispflichten (Anzeige von Veränderungen);
- 10) Festlegung derjenigen (formalen) Pflichten, die sich aus den für den Auftraggeber geltenden datenschutzrechtlichen Vorschriften ergeben;
- 11) Regelungen über Konsequenzen bei Nichterfüllung vertraglicher Leistungen (Konventionalstrafen, Ersatzvornahme etc.) entsprechend der zu erwartenden Risiken;
- 12) Haftungsregelungen.

Betrieb einer Poststelle durch eine Kommune als Provider

Handelt eine Kommune beim Betrieb einer eKomP als Provider? Diese Frage wurde von der Projektgruppe als wesentlich für den Betrieb angesehen. Die Bundesnetzagentur (vormals Regulierungsbehörde) hat zu dieser Fragestellung eine Aussage getroffen, die aufgrund des grundlegenden Charakters hier ausführlich zitiert wird²³:

„ Vor diesem Hintergrund werfen Sie die Frage auf, ob die Einrichtung einer derartigen Poststelle als Telekommunikationsdienst gemäß § 3 Nr. 24 TKG bzw. die Körperschaft oder Person, die diese Poststelle betreibt, als Diensteanbieterin gemäß § 3 Nr. 6 TKG zu bewerten sei (sogleich zu I). Ihrem Schreiben entnehme ich auf Grund des Gespräches vom 3. Mai 2005 weiterhin, dass Sie eine Stellungnahme zur Anwendung der Vorschriften des Teils 7 des TKG zum Datenschutz, Fernmeldegeheimnis und der öffentlichen Sicherheit wünschen (sogleich zu II).

Einordnung in die Begriffsbestimmungen des TKG

Bezüglich der Einordnung des Betriebs einer elektronischen Poststelle im Sinne des § 3a VwVfG in die Begriffsbestimmungen des TKG kann ich Ihnen Folgendes mitteilen:

Für die Anwendung der Vorschriften des Telekommunikationsgesetzes bestehen in persönlicher Hinsicht drei Möglichkeiten:

- Betreiber eines Telekommunikationsnetzes
- Diensteanbieter und
- Betreiber einer Telekommunikationsanlage.

Die von Ihnen beschriebene virtuelle Poststelle erfüllt offenkundig nicht die Voraussetzungen eines Telekommunikationsnetzes gemäß § 3 Nr. 27 TKG.

²³ Das Zitat entstammt der Antwort der BNA auf eine Anfrage der Transferkommune Saarbrücken.

Des Weiteren ist der Betrieb einer Elektronischen Poststelle kein Telekommunikationsdienst gemäß § 3 Nr. 24 TKG, da allein mit der Bereitstellung einer elektronischen Poststelle nicht die Übertragung von Signalen über Telekommunikationsnetze angeboten wird. Die eKomP empfängt, speichert und versendet Signale. Die Übertragung der Signale wird von ihr hingegen nicht vorgenommen.

Die eKomP erfüllt demzufolge die Definition einer Telekommunikationsanlage gemäß § 3 Nr. 23 TKG, da sie eine technische Einrichtung darstellt, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, vermitteln, empfangen, steuern und kontrollieren kann. Die Stelle, die über die eKomP die Funktionsherrschaft, also die rechtliche Kontrolle, ausübt, ist demnach Betreiber einer Telekommunikationsanlage.

Eine abweichende Einordnung der Person, die die eKomP betreibt, kann sich dann ergeben, wenn die Person – über den Betrieb der Poststelle hinaus – im Zuge eines Gesamtangebots auch die Beförderung innerhalb der Behörden, die an die eKomP angeschlossen sind, erbringt. In diesem Fall ist das Angebot auf den Transport innerhalb der verbundenen Behörden ausgeweitet. Neben die Aufgabe, die Schnittstelle zu den Bürgern zu besorgen, tritt in diesem Fall die Transportfunktion. Dieser Teil des Gesamtangebots erfüllt die Voraussetzungen eines Telekommunikationsdienstes, so dass der Anbieter auch ein Diensteanbieter ist.

Anwendung der Vorschriften zum Fernmeldegeheimnis und Datenschutz

Viele Vorschriften in Teil 7 des TKG (Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit) knüpfen an die Eigenschaft des Diensteanbieters an, der gemäß § 3 Nr. 6 Buchstabe a, Nr. 10 TKG geschäftsmäßig Telekommunikationsdienste erbringt, also nachhaltig ein Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht bereithält. Des Weiteren richten sich vor allem die Regelungen im Bereich „Öffentliche Sicherheit“, d.h. die Überwachungsvorschriften und Auskunftsverpflichtungen, an Anbieter von Telekommunikationsdiensten für die Öffentlichkeit bzw. an Betreiber von für die Erbringung dieser Dienste geeigneten Telekommunikationsanlagen.

Der Betrieb einer elektronischen Poststelle ohne die Erbringung von Transportdienstleistungen führt, wie oben ausgeführt, nicht zu einer Einordnung des Betreibers als Diensteanbieter im Sinne des TKG, da schon kein Telekommunikationsdienst erbracht wird. Der Betrieb der Telekommunikationsanlage erfolgt darüber hinaus nicht für die Öffentlichkeit, sondern nur für die Behörde selbst. Folgerichtig liegen die Vor-

aussetzungen für eine Anwendbarkeit der Vorschriften aus Teil 7 des TKG im Fall des Betreibers einer reinen elektronischen Poststelle nicht vor.

Literaturverzeichnis

- Andersen 1997 Andersen, Uwe: Gemeinden/Kommunale Selbstverwaltung. In: Andersen, Uwe/ Woyke, Wichard (Hrsg.): Handwörterbuch des politischen Systems der Bundesrepublik Deutschland, 3. Aufl., Opladen: Leske & Budrich 1997, S. 172-180.
- BSI 2003 Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik: Informationen zur virtuellen Poststelle. Modul aus dem E-Government-Handbuch. Bonn 2005.
<http://www.bsi.bund.de/fachthem/egov/6.htm>
Abruf 19.08.2006.
- BSI 2004a Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik: Sichere Kommunikation im E-Government. Modul aus dem E-Government-Handbuch. Bonn 2005.
<http://www.bsi.bund.de/fachthem/egov/6.htm>
Abruf 19.08.2006.
- BSI 2004b Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik: Verschlüsselung und Signatur. Modul aus dem E-Government-Handbuch. Bonn 2005.
<http://www.bsi.bund.de/fachthem/egov/6.htm>
Abruf 19.08.2006.
- BSI 2004c Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik: Authentisierung im E-Government. Modul aus dem E-Government-Handbuch. Bonn 2005.
<http://www.bsi.bund.de/fachthem/egov/6.htm>
Abruf 19.08.2006.
- BSI 2006 Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz, Bonn 2006.
http://www.bsi.de/literat/bsi_standard/index.htm
Abruf 19.08.2006.
- Deutscher Städte-
tag 2003 Die Eröffnung des Zugangs für die elektronische Kommunikation.
<http://www.edoc.difu.de/orlis/DF7128-Teil1.pdf>
Abruf 09.04.2006 (nicht mehr verfügbar).
- DIN 2001 Deutsches Institut für Normung (DIN): DIN Norm ISO 9126. Software-Engineering - Qualität von Software-Produkten -

„Softwarequalität“.

- DIN 2006 Deutsches Institut für Normung (DIN): DIN Norm ISO 9241 (Norm-Entwurf). Ergonomie der Mensch-System-Interaktion - Teil 300: Einführung in Anforderungen und Messtechniken für elektronische optische Anzeigen (ISO/DIS 9241-300:2006).
- KBSt 2005 Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt): SAGA. Standards und Architekturen für E-Government-Anwendungen. Version 2.1. Schriftenreihe der KBSt. Band 82. September 2005.
http://www.kbst.bund.de/cln_011/nn_836960/Content/Standards/Saga/Standards/standards__node.html__nnn=true
Abruf 29.06.2006.
- Landesbeauftragter für den Datenschutz Niedersachsen 2004 Die virtuelle Poststelle im datenschutzgerechten Einsatz.
http://www.lfd.niedersachsen.de/master/C146101_L20_D0.html
Abruf 30.06.2006.

Anhang 1: Schutzbedarfsfeststellung

Das hier dargestellte Vorgehen des BSI²⁴, die so genannte E-Government-spezifische Schutzbedarfsfeststellung, betrachtet ausschließlich die Kommunikation zwischen Nutzern und Behörde und damit die Schnittstellen des Online-Dienstleistungsangebots.

Dabei wird hinsichtlich der Schadensauswirkungen auf der Seite der Nutzer sowie auf der Seite der Behörde der Schutzbedarf festgelegt.

Unter Schadensauswirkungen auf der Seite der Nutzer sind insbesondere die Beeinträchtigung des informationellen Selbstbestimmungsrechts (Auswirkungen auf die gesellschaftliche Stellung oder auf die wirtschaftlichen Verhältnisse des Nutzers) und Beeinträchtigungen der persönlichen Unversehrtheit zu verstehen.

Auf Behördenseite stehen das gesetzmäßige Verwaltungshandeln (z.B. Verstoß gegen Gesetze/ Vorschriften/ Verträge) und ein damit verbundener Imageverlust (z.B. negative Außenwirkungen) im Vordergrund. Andere Auswirkungen (z.B. Beeinträchtigung der Aufgabenerfüllung, finanzielle Auswirkungen) sind denkbar. Dabei sind insbesondere die finanziellen Auswirkungen nicht generell in absoluten Zahlen zu quantifizieren.

Als Orientierungshilfe werden im Folgenden fünf Schutzbedarfsklassen definiert. Da der Schutzbedarf meist nicht unmittelbar quantifizierbar ist, beschränkt sich die Definition auf eine qualitative Aussage:

Schutzbedarfsklasse	Ausprägung der Schutzbedarfsklasse
Kein	Ein besonderer Schutz ist nicht notwendig, da keine Schadensauswirkungen zu erwarten sind.
Niedrig	Die Schadensauswirkungen sind eng begrenzt.
Mittel	Die Schadensauswirkungen sind begrenzt und überschaubar.
Hoch	Die Schadensauswirkungen können beträchtlich sein.
Sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 2: Schutzbedarfsklassen

Die Schutzbedarfsklasse für das Verfahren wird anhand der Sicherheitsziele

²⁴ Vgl. BSI 2005.

- Vertraulichkeit,
- Verbindlichkeit (Verbindlichkeit der Kommunikation, Integrität, Authentizität und Nicht-Abstreitbarkeit der übertragenen Daten, Authentizität der Kommunikationspartner),
- Schriftformerfordernis sowie
- Verfügbarkeit der technischen Systeme auf Behördenseite

festgestellt.

Bei der Feststellung des Schutzbedarfs wird bei der eKomP davon ausgegangen, dass zahlreiche Möglichkeiten zur Kommunikation, z.B. Formulare oder E-Mail im Internet angeboten werden. Der Schutzbedarf für die Abwicklung von Dienstleistungen bzw. Transaktionen über das Internet ist hier nicht Gegenstand der Betrachtung.

1. Vertraulichkeit der Kommunikation

Werden Daten zwischen Kunden und Behörde ausgetauscht, so ist es in vielen Fällen notwendig, sicherzustellen, dass diese nicht von unberechtigten Dritten mitgelesen werden - die Vertraulichkeit der übertragenen Daten muss geschützt werden. Im herkömmlichen papiergestützten Verfahren wird dies in der Regel durch die Verwendung von Briefumschlägen sichergestellt.

Einordnung	Erläuterung	Schutzbedarf
Kein	Allgemeine Informationen; konventionelle Übermittlung durch Veröffentlichung in Broschüren/ Zeitungen/allgemein zugänglichen Medien oder Versand per Postkarte.	
Niedrig	Gering schützenswerte personenbezogene bzw. vertrauliche Daten; konventionelle Übermittlung durch Versand per Postkarte oder Brief.	
Mittel	Eingeschränkt schützenswerte personenbezogene bzw. vertrauliche Daten; konventionelle Übermittlung durch Versand per verschlossenen Brief.	
Hoch	Personenbezogene bzw. vertrauliche Daten; konventionelle Übermittlung durch Versand per verschlossenen Brief.	eKomP
Sehr hoch	Besonders schützenswerte personenbezogene bzw. vertrauliche Daten; konventionelle Übermittlung üblicherweise durch Versand per Postzustellungsurkunde oder persönliche Übergabe.	

Tabelle 3: Schutzbedarfsfeststellung für das Sicherheitsziel Vertraulichkeit

2. Verbindlichkeit der Kommunikation

Unter dem Sammelbegriff Verbindlichkeit von Daten sind im E-Government Schutzbedarfe hinsichtlich der Integrität, Authentizität und Nicht-Abstreitbarkeit der übertragenen Daten zu betrachten.

2.1 Integrität der übertragenen Daten

Werden Daten übertragen, so ist sicherzustellen, dass diese nicht auf dem Übertragungsweg verändert werden; ihre Integrität bedarf eines gewissen Schutzes.

Einordnung	Erläuterung	Schutzbedarf
Niedrig	Allgemeine Informationen	
Mittel	Informationen für einen eingeschränkten Benutzerkreis	
Hoch	Steuererklärung, Steuerbescheid	eKomp
Sehr hoch	Daten, die zu automatischen Handlungen oder zu Hilfeinsätzen führen	

Tabelle 4: Schutzbedarfsfeststellung für das Sicherheitsziel Integrität

2.2 Authentizität und Nicht-Abstreitbarkeit der übertragenen Daten

Es ist ferner zu prüfen, inwieweit es notwendig ist, die übersandten Daten ihrem Absender zuordnen zu können. Dies betrifft sowohl die Authentizität der kommunizierten Daten, d.h. die für den Empfänger verlässliche Zuordnung zum vermeintlichen Absender, als auch die Nicht-Abstreitbarkeit, also die gegenüber Dritten beweisbare Zuordnung.

Einordnung	Erläuterung	Schutzbedarf
Kein	Der Abruf allgemeiner Informationen	
Niedrig	Beispiel: Für die Vereinbarung eines persönlichen Beratungsgesprächs im Gesundheitsamt ist das Themengebiet und ggf. die Telefonnummer des Gesprächspartners relevant.	
Mittel	Beispiel: Die Mitteilung über die Änderung der Bankverbindung, auf die eine monatliche geringe Förderung überwiesen wird, sollte nur der Förderberechtigte vornehmen können.	
Hoch	Beispiel: Die Mitteilung über die Änderung der Bankverbindung, auf die eine einmalige hohe Summe überwiesen wird, darf nur der Förderberechtigte vornehmen können.	eKomP

Einordnung	Erläuterung	Schutzbedarf
Sehr hoch	Beispiel: Bei der Aushändigung des Personalausweises ist persönliches Erscheinen unter Vorlage eines Dokuments zur Authentisierung erforderlich. Der Erhalt des Ausweises wird gegengezeichnet (Nicht-Abstreitbarkeit).	

Tabelle 5: Schutzbedarfsfeststellung für das Sicherheitsziel Authentizität und Nicht-Abstreitbarkeit der übertragenen Daten

2.3 Authentizität der Kommunikationspartner

Die Nutzung der eKomP setzt voraus, dass Behörde und Nutzer sich „erkennen“ können.

Einordnung	Erläuterung	Schutzbedarf
Kein	Die Kommunikationspartner können ungenannt bleiben.	
Niedrig	Die Behauptung der Identität reicht aus.	
Mittel	Die Identität der Kommunikationspartner lässt sich plausibel nachprüfen.	
Hoch	Die Identität der Kommunikationspartner lässt sich verbindlich nachprüfen.	eKomP
Sehr hoch	Bei der Aushändigung des Dokuments xy ist persönliches Erscheinen unter Vorlage eines Dokuments zur Authentisierung erforderlich (Nicht-Abstreitbarkeit).	

Tabelle 6: Schutzbedarfsfeststellung für das Sicherheitsziel Authentizität der Kommunikationspartner

3. Schriftformerfordernis

Im Zuge der Schutzbedarfsfeststellung wird auch erhoben, ob ein Schriftformerfordernis besteht, da dieses direkten Einfluss auf die einzusetzenden Sicherheitsmechanismen hat.

Schutzbedarfsaspekt	Kommentar
Wird für diesen Kommunikationsschritt die Schriftform gefordert? Ist diese rechtliche Vorgabe notwendig oder kann das Gesetz/die Verordnung im Sinne des Bürokratieab-	Im Bereich der Behördenkommunikation (Behörde zu Behörde) kann geprüft werden, ob auch eine fortgeschrittene Signatur ausreichend ist. Änderungen im hoheitlichen oder fiskalischen

Schutzbedarfsaspekt	Kommentar
baus oder der Prozessoptimierung kurzfristig geändert werden?	Bereich, sofern andere Nutzergruppen betroffen, sind kaum realisierbar.
Gibt es in den zu Grunde liegenden Gesetzen und Verordnungen eine darüber hinausgehende Anforderung?	Viele Fachgesetze stellen eigene Anforderungen an das Verwaltungshandeln. Inwieweit die Nutzung der eKomP die gesetzlichen Anforderungen erfüllt, muss im Einzelfall geprüft werden. (Beispiel: Beamtenrecht – Urkunden)
Gibt es eine Abschwächung?	Nein.

Tabelle 7: Schutzbedarfsfeststellung für das Sicherheitsziel Vertraulichkeit

4. Verfügbarkeit der technischen Systeme auf Behördenseite

Online-Dienstleistungen können nur genutzt werden, wenn die technischen Systeme auf Behördenseite verfügbar sind. Es ist für jede Dienstleistung zu prüfen, in welcher Zeit-Größenordnung ein Ausfall der Systeme akzeptabel ist.

Einordnung	Erläuterung	Schutzbedarf
Niedrig bis mittel	Eine Ausfallzeit der Online-Dienstleistung von mehr als 24 Stunden kann toleriert werden.	
Hoch	Eine Ausfallzeit der Online-Dienstleistung zwischen einer und 24 Stunden wird als tolerabel eingeschätzt.	eKomP
Sehr hoch	Die maximal tolerierbare Ausfallzeit der Online-Dienstleistung liegt unter einer Stunde.	

Tabelle 8: Schutzbedarfsfeststellung für das Sicherheitsziel Vertraulichkeit

Anhang 2: Regelungsbedarf für Dienstvereinbarungen/Dienstanweisungen

Für den Einsatz der VPS und zur Steuerung des Verwaltungshandels sind Regelungen in Dienstvereinbarungen oder Dienstanweisungen notwendig.

Dienstvereinbarung

Inhalte einer Dienstvereinbarung können Eckpunkte über die Verarbeitung und Nutzung

- der personenbezogenen Daten der Beschäftigten, Daten- und Persönlichkeitsschutz,
- Rechte des Personalrates, Arbeitsplatzgestaltung und Arbeitsschutz, Benutzerbetreuung, Weiterbildungsangebote

sein.

Dienstanweisung

Im Rahmen einer Dienstanweisung zur Nutzung der VPS sollten u.a. folgende Regelungen Berücksichtigung finden:

- Festlegung der Postfächer (behörden-, organisations-, funktionsbezogen; zentral oder dezentral bzw. benutzerbezogen in Abhängigkeit von den Ergebnissen der örtlichen Kommunikationsanalyse),
- Regelungen zur Organisation und Verwaltung der Postfächer, Zuständigkeiten und Verantwortungsbereiche – insbesondere dort, wo es zu fach- oder amtsübergreifender Verantwortlichkeit kommt,
- Regelungen zum Einsatz der verschiedenen Signaturen (fortgeschritten, qualifiziert bzw. qualifiziert mit Anbieterakkreditierung, Verwendung eines Pseudonyms),
- Verpflichtung zur Eintragung der Behördenangabe nach § 37 Abs. 3 VwVfG im qualifizierten Zertifikat oder im qualifizierten Attributzertifikat nach dem SigG,
- Regelungen zur Zugangseröffnung, Zugangsbeschränkung (z.B.: Ausschreibungen, Charakter, Geschäftsverkehr, Attachements, Attribute),
- Verfahrensregelungen zur elektronischen Kommunikation mit dem Bürger (Notwendigkeit der Einverständniserklärung für die elektronische Nachrichtenübermittlung sowie deren Beschaffung, Hinterlegung, Änderung und Stornierung),
- Entscheidung zur Zulässigkeit oder zum Ausschluss der Privatnutzung (Nutzung der Signaturkarte als Amts- oder Funktionsträger),

- Sicherstellung von Datenschutz und Datensicherheit (getrennte Aufbewahrung von PIN und Signaturkarte, Ablage und Nutzung der Verschlüsselungszertifikate, Zugriff auf öffentliche Schlüssel der Kommunikationspartner),
- Regelungen zum Umgang und zur Verantwortung bei Gruppenzertifikaten und Verschlüsselungszertifikaten,
- Bestimmungen zur Aufbau- und zur Ablauforganisation (z.B. zur Sicherstellung des Anwendungs-, Sicherheits- und Schlüsselmanagements und zur Sicherstellung der Kontrollrechte),
- Festlegung von Bearbeitungsregeln für ein- und ausgehende elektronische Post:
 - Bestimmungen zur Vertretungsregelung und zur Verwaltung von internen Vertretungs- und Berechtigungsregelungen,
 - Festlegung eines Rollen- und Zugriffsrechtekonzeptes (z.B.: Administrator, Revisor, Sachbearbeiter),
 - Sicherstellung der regelmäßigen Abfrage der Postfächer,
 - Entscheidung zur Erstellungsform der Empfangsquittungen für externe und ggf. auch interne Nachrichten,
 - Bearbeitungsregelungen für Input und Output mit höherem Vertraulichkeitsbedarf (Umverschlüsselung, Weiterleitung von verschlüsselten E-Mails bei Ende-zu-Ende-Sicherheit ohne weitere Aktionen der eKomp),
 - Verfahrensregelungen zur Behandlung nicht geeigneter Eingänge (z.B. Speicherung von Nachrichten mit unvollständiger oder fehlerhafter Signatur oder von Dokumenten und Nachrichten, die nicht entschlüsselt werden konnten, Behandlung von Dokumenten und Nachrichten in einem nicht akzeptablen Datenformat),
 - Verfahrensregelungen zum Umgang mit bestimmten Prüfergebnissen (z.B. Zertifikatsprüfung: „Status undefiniert“),
 - Sicherstellung einer Information an den Absender und ggf. den Empfänger bei Nachrichten, die fehlerhaft sind oder einen schädlichen Inhalt haben, o.ä.,
 - Sicherstellung einer temporären Speicherung von Nachrichten mit schädlichem Inhalt in einer gesicherten Umgebung zu Beweis Zwecken,
 - Festlegung von Weiterleitungsregelungen,
 - Verpflichtung zum Einsatz von Signatur- und Verschlüsselungszertifikaten nach dem Schutzstufenkonzept,
 - Vorgaben zur Aufbewahrungsform von Verifikationsdaten (z.B. Übermittlungsprotokoll, Prüfprotokoll, Laufzettel der Transaktion),
 - Sicherstellung der Nachsignierung vor Ablauf der Gültigkeit der kryptographischen Algorithmen,

-
- Sicherstellung der Zeitstempelnutzung,
 - Festlegung der Zeichnungsbefugnisse,
 - Regelungen zur Trennung von Signatur und Verschlüsselung mit gesicherter Ablage der Schlüssel (Schlüsselmanagement, Sperrlistenabfrage, interner Verzeichnisdienst).
 - Verpflichtung zur Datensicherung und Datenarchivierung (Übernahme in ein elektronisches Archiv) und Festlegung von Formaten mit Eignung für eine Langzeitspeicherung.