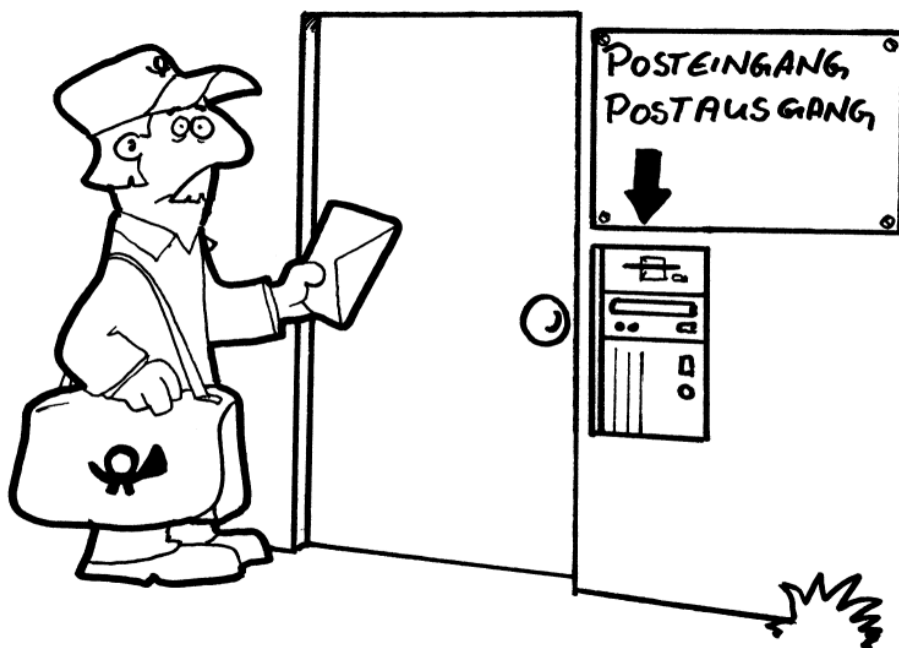


Eröffnung des Zugangs für die elektronische Kommunikation

Teil 2

Empfehlungen für Sofortmaßnahmen / Rahmenbedingungen auf dem
Weg zur elektronischen Kommunikation



In der folgenden Ausarbeitung wird i.d.R. der Plural verwendet. Im Hinblick auf die leichtere Lesbarkeit wurde auf die jeweils weibliche und männliche Form verzichtet. Der Plural soll selbstverständlich beide umfassen.

Verfasser

Arbeitskreis „Digitales Rathaus“ des Deutschen Städtetages,

Arbeitsgruppe „Sofortmaßnahmen“

Dr. Martin Hagen, Freie Hansestadt Bremen

Hans-Peter Kinny, Stadt Aachen

Ulrich Mahner, Niedersächsischer Städtetag, Hannover

Volker Rombach, KDZ Hellweg-Sauerland, Iserlohn

Stefan Schoenfelder, Stadt Münster, citeq

Jürgen Thiel, Landeshauptstadt Düsseldorf

Hans-Volker Winkler, Landeshauptstadt München (Anhang 2)

Stand: September 2003

Deutscher Städtetag, Köln

Lindenallee 13 – 17

50968 Köln

Alle Rechte vorbehalten

Literaturverzeichnis

- Begründung zum Dritten Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften, Stand 05.04.2002
(<http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=38&tsid=220&tdid=1791&page=0>)
- Schritte auf dem Weg zum digitalen Rathaus, Deutscher Städtetag, 2000
(<http://edoc.difu.de/staedtetag/>)
- Welche elektronische Signatur braucht die Kommunalverwaltung? Deutscher Städtetag, Mai 2002
(<http://edoc.difu.de/staedtetag/>)
- Wo ist der Schlüssel zum digitalen Rathaus? Keymanagement und Infrastruktur im kommunalen E-Government, Deutscher Städtetag, Oktober 2002
(<http://edoc.difu.de/staedtetag/>)
- Eröffnung des Zugangs für die elektronische Kommunikation, Teil 1 – Grundsätzliche Ausführungen, Deutscher Städtetag Mai 2003
(<http://edoc.difu.de/staedtetag/>)
- Rechtskonformes E-Government, Antworten auf Kernfragen beim Bau eines virtuellen Rathauses, Bundesministerium für Wirtschaft und Arbeit, Begleitforschung zum Leitprojekt MEDIA@Komm, Januar 2003
(<http://www.bmwi.de/homepage/download/infogesellschaft/rechtsratgeber.pdf>)
- SAGA, Standards und Architekturen für E-Government-Anwendungen, Version 1.1
(<http://www.bund.de/saga>)

Inhaltsverzeichnis

Managementsummary	5
1 Warum „Sofortmaßnahmen“?	7
1.1 Änderung des Verwaltungsverfahrenrechtes des Bundes	7
1.2 Änderung des Landesverwaltungsverfahrensgesetzes	7
1.3 Zwang zum Handeln	8
1.4 Neue Anforderungen an die zentrale Maileingangsstelle	9
2 Sofortmaßnahmen sind nur ein erster Schritt.....	12
2.1 Formularbasierte Webanwendungen	12
2.2 Versand signierter und / oder verschlüsselter E-Mails durch Kommunen.....	12
2.3 Ein umfassendes Konzept für die elektronische Kommunikation.....	13
3 Drei Stufen der E-Mail-Kommunikation	14
3.1 Stufe 1 – Die Verwaltung kann noch keine signierten und/oder verschlüsselten E-Mails verarbeiten	14
3.2 Stufe 2 – Die Verwaltung kann keine Signaturen, aber verschlüsselte E-Mails verarbeiten	15
3.3 Stufe 3 – Die Verwaltung kann signierte und verschlüsselte E-Mails verarbeiten..	16
4 Was ist zu tun	18
4.1 Informationen für den Bürger	18
4.2 Informationen für den Mitarbeiter	18
4.3 Technische und organisatorische Maßnahmen	19
4.4 Konzept für die langfristige Nutzung des neuen Kommunikationsmediums für die Verwaltung	19
Anhang.....	21
Anhang 1: Informationen für den Bürger – Mustertexte	21
Anhang 2: Textbausteine für Rückantworten an den Bürger	26
Anhang 3: Mustertexte für generelle Dienstanweisungen.....	34

Management Summary

Der Bundesgesetzgeber und inzwischen auch nach und nach die Landesgesetzgeber haben die gesetzlichen Voraussetzungen für eine rechtsverbindliche Kommunikation im Verwaltungsverfahren geschaffen. Sie wecken damit Erwartungen bei Bürgerinnen und Bürgern sowie Unternehmen auch mit Kommunalverwaltungen rechtsverbindlich elektronisch kommunizieren zu können. Durch die Veröffentlichung von E-Mail-Adressen auf Internetseiten und Briefköpfen unterstützen auch die Kommunen diese Erwartungen. Dabei dürfte meist nicht bekannt sein, dass die Kommunen durch diese Veröffentlichung bereits einen Zugang für eine rechtsverbindliche elektronische Kommunikation eröffnet haben.

Die Möglichkeit, dass bisher in Papierform einzureichende Schriftstücke nun auch elektronisch übermittelt werden können, erfordert organisatorische und technische Vorbereitungen in den Verwaltungen. Diese Handreichung soll Hinweise geben, wie sich die gesetzlichen Änderungen in der kommunalen Praxis auswirken. Insbesondere sollen die Möglichkeiten der Kommunen zur aktiven Gestaltung der elektronischen Kommunikation aufgezeigt werden. Durch die Nutzung dieser Möglichkeiten kann einem bloßen Reagieren vorgebeugt werden.

Dabei ist davon auszugehen, dass – auch abhängig von der Größe der Kommune – unterschiedliche Rahmenbedingungen bestehen, die zu jeweils individuellen Lösungen führen werden. In erster Linie kommen die Kommunikation per E-Mail oder über von den Verwaltungen angebotene elektronische Formulare in Frage. Rechtsverbindlich kann auf diesen Wegen allerdings nur dann kommuniziert werden, wenn Mitteilungen mit einer elektronische Signatur versehen werden. Hierbei handelt es sich um ein komplexes mathematisch technisches Verfahren, mit der die Urheberschaft und die Unverändertheit einer Nachricht bestätigt wird.

Ein Blick auf die Internetseiten der Kommunen - vor allem der kleineren und mittleren - zeigt, dass nur in wenigen Fällen Formulare angeboten werden. Auch für den Empfang signierter E-Mails sind entsprechende technische Vorkehrungen zu treffen.

Die Kommunalverwaltungen sind nicht verpflichtet entsprechende Möglichkeiten anzubieten. Allerdings ist zu erwarten, dass der öffentliche und der politische Druck die Verwaltungen sehr schnell veranlassen wird, entsprechende Möglichkeiten anzubieten.

Hierzu ist zu aller erst das eigene Personal mit dem Thema vertraut zu machen. Der Umgang mit einer rechtsverbindlichen E-Mail stellt weitergehende Anforderungen an organisatorische Regelungen. Mitarbeiterinnen und Mitarbeiter müssen wissen, wie sie E-

Mails behandeln müssen, welche Probleme bei der Kommunikation auftauchen können, und wie auf diese zu reagieren ist.

Daneben müssen die technischen Voraussetzungen geschaffen werden, um überhaupt signierte Nachrichten empfangen zu können. Aber mit dem Empfang alleine ist es nicht getan. Die Signatur ist ein Formerfordernis, dessen Einhaltung auch technisch überprüft werden muss. Die Ergebnisse entsprechender Prüfungen müssen dokumentiert und archiviert werden.

Die Schaffung einer zentralen Maileingangsstelle kann helfen, den technischen, personellen und finanziellen Aufwand zu reduzieren. Die Einrichtung einer solchen Stelle wird deshalb empfohlen.

Ein weiterer wesentlicher Aspekt zur Vermeidung insbesondere technischer Probleme ist die Vorgabe technischer Rahmenbedingungen für die elektronische Kommunikation durch die Kommune. Technische Standards und für die Verarbeitung in der Kommune geeignete Dateiformate sollten im Rahmen der Eröffnung des Zugangs für die elektronische Kommunikation vorgegeben werden. Hinsichtlich elektronischer Signaturen und Verschlüsselung sollten angesichts der fehlenden Interoperabilität der derzeitigen Verfahren der Einsatz konkreter Produkte vorgegeben werden. So kann dafür gesorgt werden, dass die Kommune nur elektronische Eingänge erreichen, die sie auch bearbeiten kann.

Aber auch für den Fall, dass Eingänge nicht verarbeitet werden können, sind Vorkehrungen zu treffen. Die Mitarbeiterinnen und Mitarbeiter müssen auch mit solchen Eingänge verantwortlich umgehen und entsprechende Maßnahmen treffen.

Für eine Reihe der beschriebenen Fragestellungen enthält diese Handreichung Formulierungsvorschläge. Diese können aber eine intensive Diskussion jeder einzelnen Verwaltung über ein eigenes Konzept für eine umfassende Nutzung der elektronischen Kommunikation nicht ersetzen. Ein solches Konzept muss darüber hinaus in eine allgemeine E-Government-Strategie der Kommune eingebunden sein.

1 Warum „Sofortmaßnahmen“?

1.1 Änderung des Verwaltungsverfahrenrechtes des Bundes

Am 1. Februar 2003 ist das „Dritte Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften“ in Kraft getreten¹. Mit den darin enthaltenen Änderungen verschiedener verfahrensrechtlicher Vorschriften wurden die rechtlichen Voraussetzungen für die rechtsverbindliche elektronische Kommunikation in Verwaltungsverfahren geschaffen. Insbesondere wurde im Verwaltungsverfahrensgesetz des Bundes der § 3 a „Elektronische Kommunikation“ als zentrale Vorschrift hierzu eingefügt. Er enthält folgende Regelungen:

§ 3a Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

(3) Ist ein der Verwaltung übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Verwaltung übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

1.2 Änderung der Verwaltungsverfahrensgesetze der Länder

Das Verwaltungsverfahrensgesetz des Bundes hat zunächst keine Auswirkungen auf Kommunen. Dies gilt auch für den Fall, dass diese Bundesrecht ausführen.

Maßgeblich sind vielmehr die Verwaltungsverfahrensgesetze der Länder. Diese werden nach aller Voraussicht die Bundesregelungen in gleichem oder ähnlichem Wortlaut übernehmen. So haben zum Beispiel die Länder Bayern, Sachsen, Berlin, u.a. bereits novellierte Gesetze erlassen, in denen ebenfalls qualifizierte Signaturen als Voraussetzung für den Ersatz der Schriftform festgeschrieben werden. In Hamburg ist in das "Gesetz zur

¹ BGBl. I, Nr. 60 S. 3322 ff.. Die Neufassung des Verwaltungsverfahrensgesetzes findet sich unter <http://bundesrecht.juris.de/bundesrecht/vwvfg/gesamt.pdf>

Anpassung verwaltungsrechtlicher Vorschriften an den elektronischen Rechtsverkehr" eine Öffnungsklausel aufgenommen worden, welche die Frage der zulässigen Signaturen auf eine Rechtsverordnung auslagert. Eine Übersicht über den Stand der Anpassung der Verwaltungsverfahrensgesetze der Länder enthält Anhang 4.

Weder das Verwaltungsverfahrensgesetz des Bundes noch voraussichtlich die entsprechenden Landesgesetze enthalten eine Verpflichtung für die Kommunen, die elektronische Kommunikation zu ermöglichen. Trotzdem ist davon auszugehen, dass „politischer Druck“ die Kommunen zwingen wird, diese Möglichkeit anzubieten.

1.3 Zwang zum Handeln

Bereits mit Inkrafttreten der jeweiligen Landesgesetze gibt es einen faktischen Zwang zu handeln, da nach geltender Rechtsauffassung nahezu alle Kommunen durch konkludentes Handeln die im § 3a Absatz 1 des Verwaltungsverfahrensgesetzes des Bundes beschriebene Voraussetzung für die elektronische Kommunikation geschaffen haben.

Für die Möglichkeit der elektronischen Kommunikation kommt es wesentlich darauf an, ob der jeweilige Empfänger einen so genannten „Zugang“ für diese Kommunikationsform eröffnet hat.

Zurzeit wird die Auffassung vertreten, dass Kommunen durch die Angabe ihrer E-Mail-Adresse auf Briefbögen oder Internetseiten diesen Zugang eröffnet haben. Ausführliche Erläuterungen hierzu enthält die Handreichung „Eröffnung des Zugangs für die elektronische Kommunikation - Teil 1: Grundsätzliche Ausführungen“ des Deutschen Städtetages. Darin werden auch die hier zugrunde gelegten Prämissen begründet.

Demnach ist anzunehmen, dass Bürgerinnen und Bürger nach Inkrafttreten des Verwaltungsverfahrensgesetzes des jeweiligen Landes davon ausgehen, dass Sie zukünftig alle bisher in Papierform und handschriftlich unterschrieben einzureichende Schriftstücke in elektronischer Form an die Kommunen senden können². Aufgrund der weiten Verbreitung des Mediums E-Mail, wird dieses Medium voraussichtlich in erheblichem Maße genutzt werden und auch elektronische Signaturen werden zum Einsatz kommen.

² Zur Frage, inwieweit eine gesetzlich erforderliche Schriftform ersetzt werden kann, sh. Handreichung „Eröffnung des Zugangs für die elektronische Kommunikation – Teil 1: Grundsätzliche Ausführungen“ des Deutschen Städtetages

Einen anderen Weg zur Kommunikation zwischen Kommune und Bürger stellen E-Government-Anwendungen dar, bei denen der Bürger durch das Ausfüllen elektronischer Formulare und interaktiver Eingabemasken im Webbrowser sein Anliegen darstellt. Hier gibt die Kommune die technischen Rahmenbedingungen nahezu vollständig vor. Die neuesten Ergebnisse der Begleitforschung zum MEDIA@Komm Wettbewerb zeigen bei der Verbreitung von E-Government-Anwendungen trotz ermutigender Ansätze in vielen Kommunen allerdings noch erheblichen Nachholbedarf und eine ausschließlicher Nutzung dieser Kommunikationsform ist kurz- bis mittelfristig nicht möglich.³

Die nachfolgenden Ausführungen beziehen sich daher vorrangig auf den E-Mail Empfang durch Kommunen.

1.4 Neue Anforderungen an die zentrale Maileingangsstelle

Mit der Einführung der elektronischen Kommunikation sind umfangreiche organisatorische und technische Maßnahmen in den Kommunalverwaltungen verbunden, die nicht zuletzt auch Maßnahmen zur Personalqualifikation erforderlich machen. Dabei geht es vor allem um den Empfang, das Weiterleiten und die Verarbeitung elektronisch signierter und / oder verschlüsselter E-Mails.

Um den technischen, personellen und finanziellen Aufwand zu reduzieren, bietet es sich an, die dazu nötigen technischen und organisatorischen Maßnahmen an einer zentralen Maileingangsstelle zu konzentrieren. Eine evtl. bereits vorhandene zentrale Maileingangsstelle ist um Funktionen zur Signaturprüfung, Ver- und Entschlüsselung, Protokollierung und ggf. Archivierung, Weiterleitung und eine Zeitstempelfunktion zu erweitern. Andernfalls sind diese Funktionen durch eine Vielzahl wenn nicht alle Mitarbeiter einer Kommune zu beherrschen, durchzuführen und zu dokumentieren. Der Archivierung von Mails inklusive der Dokumentation des Zeitpunkts des Maileingangs und der Ergebnisse der Viren- und Signaturprüfung kommt hierbei eine wesentliche Bedeutung zu.

Zurzeit schlagen Kommunen und Hersteller zur Lösung dieser Problematik verschiedene Lösungen hierfür vor. Unter anderem erarbeitet das Bundesamt für Sicherheit in der

³ Siehe hierzu „Arbeitspapiere aus der Begleitforschung zum Städtewettbewerb MEDIA@Komm – 8/2003“ unter http://www.mediakomm.net/document.php?document_id=207.

Informationstechnik (BSI) ein Konzept für eine „Virtuelle Poststelle“, die auch für Kommunen eine Lösungsmöglichkeit darstellen könnte⁴.

Aufgrund der Vielzahl der am Markt verfügbaren Techniken und Produkte kann eine Verwaltung nicht alle möglichen Signatur- und Verschlüsselungstechniken unterstützen. Gegenüber dem Kommunikationspartner ist demnach eine verbindliche Vorgabe erforderlich, welche Signatur- und Verschlüsselungstechniken von der Verwaltung verarbeitet werden können und welche durch die Verwaltung selbst eingesetzt werden, um vertrauliche Informationen zu versenden. Gleichzeitig ist der Kommunikationspartner darauf hin zu weisen, wie die Kommune bei Verwendung abweichender Techniken mit der eingehenden E-Mail verfährt und welche Konsequenzen sich daraus ergeben. Neben diesen Festlegungen sind die von der Kommune verarbeitbaren Dateiformate festzuschreiben, da E-Mails mit oder ohne Signatur und Verschlüsselung zwar empfangen werden können, Kommunen aber nicht jede auf dem Markt befindliche Anwendung zur Anzeige und Weiterverarbeitung von Dateianhängen vorhalten können.

Die „Rahmenbedingungen für die elektronische Kommunikation“ sind an exponierter Stelle im Internetangebot z.B. durch einen entsprechenden Link auf der Homepage der Kommune dem Bürger zur Einsicht anzubieten. Zusätzlich sollte an den Stellen des Internetauftritts, an denen E-Mail-Adressen angeboten werden (z.B. in einem Bürgerinformationssystem, in dem Zuständigkeiten und Erreichbarkeiten von Dienststellen dargestellt sind) ein Link auf diese Informationen geschaltet werden und auf Briefköpfen und in E-Mails der Kommune auf diese Informationen hingewiesen werden.

Für die Verwendung von elektronischen Signaturen und Verschlüsselung ist zusätzliche Hard- und Software für die Signaturprüfung, etc. erforderlich. An dieser Stelle kann keine Auflistung mit dem Anspruch auf Vollständigkeit erfolgen; zu unterschiedlich sind die vorhandenen IT-Systeme und Ausstattungen in den Kommunen und das Angebot der Hersteller.

Die erforderliche technische Ausstattung unterscheidet sich dabei je nach verfolgtem Szenario. Es wird davon ausgegangen, dass die Kommune über einen Internet-Auftritt und

⁴ Informationen hierzu im Internet unter http://www.bescha.bund.de/bescha_akt/projekte/index.html

im Prinzip Verwaltungsweite E-Mail-Kommunikation verfügt. Ein Virenschanner ist an zentraler Stelle (Mail-Gateway, Mailserver) zwingend erforderlich.

Zum schrittweisen Umstieg auf die elektronische Kommunikation werden im Folgenden drei Stufen vorgeschlagen, die es den Kommunen ermöglichen sollen, ihren Bürgerinnen und Bürgern die elektronische Kommunikation anzubieten. Bereits im Rahmen des stufenweisen Vorgehens bietet es sich an, bestimmte Aufgaben zentral (zum Beispiel in einer zentralen Maileingangsstelle ggf. auch in Verbindung mit einem Dienstleister) zu erledigen.

2 Sofortmaßnahmen sind nur ein erster Schritt

Diese Sofortmaßnahmen können erforderliche grundlegende Überlegungen zur Nutzung der elektronischen Kommunikationsmöglichkeiten nicht ersetzen. Sie dienen lediglich dazu, auf die gesetzlichen Änderungen kurzfristig zu reagieren.

Insbesondere beschäftigen sich die Sofortmaßnahmen nicht mit folgenden Fragestellungen:

2.1 Formularbasierte Webanwendungen

Die größten Gestaltungsmöglichkeiten für die Verwaltung mit Aussicht auf einen entsprechenden Mehrwert bestehen in der Verwendung von formularbasierten Web-Anwendungen, die auch eine medienbruchfreie Weiterverarbeitung der übermittelten Daten ermöglichen. Dabei werden die erforderlichen Informationen direkt in elektronische Formulare eingegeben und an die Verwaltung übertragen. Diese Übertragung erfolgt nicht per E-Mail sondern mit anderen Übertragungsprotokollen.

Die technische Umsetzung kann durchgängig von den Kommunen bestimmt werden und erfordert auch in diesem Fall die Berücksichtigung spezifischer Maßnahmen für Signatur und Verschlüsselung. Für den Transport und rechtsverbindlichen Austausch von Nachrichten unter Einbeziehung von Verschlüsselung und Signatur empfiehlt der Kooperationsausschuß Automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich (KoopA ADV) den OSCI-Standard⁵. Dabei erfolgt der Datenaustausch auf Basis der Beschreibungssprache XML⁶. Weitere Empfehlungen zu Standards enthalten die „Standards und Architekturen für E-Government-Anwendungen (SAGA)⁷, welche im Projekt Bund-Online 2005 entwickelt wurden.

2.2 Versand signierter und / oder verschlüsselter E-Mails durch Kommunen

Die Nutzung der elektronischen Kommunikation durch die Kommunen bedarf eines durchgängigen Konzeptes. Hierzu muss beispielsweise geklärt werden, wie die Kommune Rückantworten an den Bürger unter Datenschutzgesichtspunkten verschlüsselt und

⁵ OSCI = Online Services Computer Interface (www.osci.de)

⁶ XML = Extensible Markup Language (<http://www.w3.org/XML/>)

⁷ Nähere Informationen zu SAGA siehe (www.bund.de/saga)

signiert, wie die Kommune an den erforderlichen Schlüssel des Bürgers kommt, u.a.m. Dieses kann nicht als Sofortmaßnahme beschrieben werden.

2.3 Ein umfassendes Konzept für die elektronische Kommunikation

- Die Sofortmaßnahmen sind ein Baustein in einem umfassenden Konzept. Ein solches Konzept bedarf eindeutiger organisatorischer, technischer und personeller Regelungen. Es ist nicht kurzfristig in voller Breite und Tiefe realisierbar, hat erhebliche Finanzinvestitionen zur Folge und steht im Zusammenhang mit weiteren Maßnahmen im Handlungspaket „E-Government“.

3 Drei Stufen der E-Mail-Kommunikation

Die rechtsverbindliche Kommunikation zwischen Bürger und Verwaltung wird nur in seltenen Fällen bereits heute ohne zusätzliche Maßnahmen durchgeführt werden können. Die Voraussetzungen in den einzelnen Kommunen unterscheiden sich dafür noch zu stark. Im nachfolgenden werden drei verschiedene Stufen für die Ausgangssituation unterschieden.

Alle Stufen der hier vorgestellten E-Mail Kommunikation basieren auf folgenden Grundannahmen:

Es gibt drei handelnde Akteure:

- Absender
- Zentrale Maileingangsstelle
- Sachbearbeiter/in.

Sofern im weiteren Dokument die Bezeichnung „E-Mail“ verwendet wird, ist die Gesamtsendung inklusive etwaiger Dateianhänge gemeint.

3.1 Stufe 1 – Die Verwaltung kann noch keine signierten und/oder verschlüsselten E-Mails verarbeiten

Betrachtet wird der Umgang mit einer signierten und/oder verschlüsselten E-Mail. Dabei ist es unerheblich, welche Signatur- bzw. welche Verschlüsselungsmechanismen verwendet werden.

Das Virenschannen ist die erste Aufgabe, nachdem die Mail auf dem Mail-Gateway⁸ der Verwaltung angekommen ist.

Bei **verschlüsselten** Mails ist eine Virusprüfung nicht möglich. Da verschlüsselte E-Mails in dieser Stufe auch nicht entschlüsselt werden können, ist eine solche Mail mit entsprechendem Hinweis an den Absender zurückzusenden. Bei einer **signierten**, aber

⁸ Hierbei handelt es sich um das aus dem Internet direkt ansprechbare Rechnersystem, welches nicht identisch mit dem eigentlichen Mailserver sein muss. I.d.R. ist dieses System in einer durch eine Firewall geschützten demilitarisierten Zone angesiedelt, während der Mailserver im „sicheren“ LAN steht.

nicht verschlüsselten Mail kann die Virusprüfung in der Regel durchgeführt werden. Sofern kein Virus gefunden wird oder ein identifizierter Virus entfernt werden kann, wird die Mail an den Sachbearbeiter weitergeleitet.⁹

Der Sachbearbeiter prüft, ob für die Bearbeitung des Vorgangs ein Schriftformerfordernis existiert. Ist das nicht der Fall, wird die Mail weiter bearbeitet.¹⁰

Wenn ein Schriftformerfordernis existiert, informiert der Sachbearbeiter den Absender darüber, dass die Signatur nicht geprüft werden kann und damit die elektronische Kommunikation für diesen Fall nicht genutzt werden kann. Er bittet um Nachreichung des Antrages auf nicht-elektronischem Weg. Hierbei ist ein Hinweis auf die von der Kommune vorgegebenen Rahmenbedingungen für die elektronische Kommunikation zu geben.

3.2 Stufe 2 – Die Verwaltung kann keine Signaturen, aber verschlüsselte E-Mails verarbeiten

In dieser Stufe öffnet sich die Verwaltung dem Empfang von verschlüsselten E-Mails. Dieses Modell gilt für Verwaltungen, die verschlüsselte E-Mails verarbeiten, aber noch keine Signaturen prüfen. Werden Entschlüsselungsfunktionen vom Sachbearbeiter direkt vorgenommen, so bedeutet dies, dass vom Sachbearbeiter auch die Virenprüfung durchgeführt werden muss, da erst entschlüsselte E-Mails auf Viren geprüft werden können. Diese Vorgehensweise bedeutet einen erheblich höheren Aufwand für den Virenschutz in der jeweiligen Verwaltung, da nun absichtlich oder unabsichtlich Virenverseuchte E-Mails bis an den Arbeitsplatz des Sachbearbeiters gelangen können. Darüber hinaus muss der einzelne Sachbearbeiter erhöhte Sachkenntnis für den Umgang mit verschlüsselten Mails und den Umgang mit Computerviren haben. Aus diesem Grund ist der Einsatz einer zentralen Maileingangsstelle mit Virenschutz- und Entschlüsselungsfunktionen sinnvoll.

Es wird deshalb davon ausgegangen, dass eine verschlüsselte E-Mail in der Maileingangsstelle empfangen wird. In diesem Szenario wird durch Einsatz geeigneter Softwareprodukte in der Maileingangsstelle erkannt, dass eine verschlüsselte Mail vorliegt.

⁹ Auf die Problematik der Virenbehandlung und ggf. Benachrichtigung der Sender wird hier nicht eingegangen.

¹⁰ Anmerkung: Es wird davon ausgegangen, dass die Mail lesbar ist.

Dort erfolgt die Entschlüsselung mit einer Entschlüsselungskomponente. Wenn die Entschlüsselung erfolgreich war, wird das Virenschannen wie bei Stufe 1 durchgeführt.

Wenn die E-Mail nicht entschlüsselt werden kann, wird eine Nachricht an den Absender geschickt, mit der Bitte um Überprüfung des Verschlüsselungsverfahrens gemäß den veröffentlichten Rahmenbedingungen für die elektronische Kommunikation bzw. die Wahl eines nicht-elektronischen Weges.

Nach dem Virenschannen wird wie in Stufe 1 weiter verfahren, sowohl für signierte wie auch nicht signierte E-Mails.

3.3 Stufe 3 – Die Verwaltung kann signierte und verschlüsselte E-Mails verarbeiten

Dieses Modell geht davon aus, dass die Verwaltung wenigstens jeweils eine Form der Verschlüsselung und qualifizierten Signatur verarbeiten kann. Da Signaturkarten für die qualifizierte Signatur nach SigG noch wenig verbreitet und z.T. nicht interoperabel sind, ist diese Stufe zurzeit kaum anzutreffen. Hier sind Marktentwicklungen abzuwarten, die auch technische Veränderungen mit sich bringen können. Dennoch ist nachfolgende generelle Vorgehensweise auf der Basis der derzeitig verfügbaren Technik vorzusehen.

Der Absender schickt eine Mail, die zuerst signiert und dann verschlüsselt wird. Dieser Prozess ist bis zum Abschluss der Virenprüfung der gleiche wie bei Stufe 2.

Es schließt sich die Prüfung der elektronischen Signatur durch die zentrale Mailingangsstelle an. Zunächst wird geprüft, ob die Signatur von der Verwaltung verarbeitet werden kann. Die Verwendung von Signaturen, die nicht den jeweiligen Landesgesetzen entsprechen, hat hinsichtlich der Rechtswirksamkeit der abgegebenen Erklärung eine erhebliche Bedeutung. Eine in dieser Form signierte E-Mail erfüllt nicht ein etwaiges Schriftformerfordernis und ist damit generell einer einfachen nicht signierten E-Mail gleichzusetzen. Der Absender ist hierüber zu informieren.¹¹

Wenn die Signatur verarbeitet werden kann, folgt die Zertifikatsprüfung. Diese kann auf verschiedenen Wegen vergleichbar zu den gängigen electronic cash-Verfahren erfolgen.

¹¹ Eine alternative Organisation, in der die signierte und verschlüsselte E-Mail zuerst dem Sachbearbeiter zugeleitet wird, wird hier nicht betrachtet, da aufwendige und mit zahlreichen Konsequenzen verbundene technische und organisatorische Rahmenbedingungen geschaffen werden müssen. Dies kann allenfalls in Ausnahmefällen sinnvoll sein.

So kann die Signatur gegen lokal vorhandene und ggf. regelmäßig replizierte Sperrlisten geprüft werden¹². Alternativ erfolgt die Überprüfung online in Verbindung mit einem Trustcenter. An die Zertifikatsprüfung schließt sich die mathematische Prüfung an (Integritätsprüfung).

Ist die Mail erst verschlüsselt und dann signiert worden, müssen die Funktionen der Integritäts- und Signaturprüfung vor der Entschlüsselung und dem Virenschannen erfolgen.

Die E-Mail mit dem Prüfprotokoll wird an den Sachbearbeiter weitergeleitet. Sind Zertifikat und Signatur gültig oder keine Signatur erforderlich, erfolgt die Bearbeitung.

Anderenfalls wird eine Mail mit der Bitte um Nachreichung des Antrages auf nicht-elektronischem Weg an den Absender gesendet. Hier sind datenschutzrechtliche Belange zu berücksichtigen.

¹² Bei diesem Verfahren werden in regelmäßigen Abständen Listen mit gesperrten Signaturen vom Trustcenter herunter geladen. Die Prüfung erfolgt dann gegen diese lokalen Sperrlisten.

4 Was ist zu tun

Ausgehend von den in Kapitel 3 dargestellten spezifischen Voraussetzungen in der jeweiligen Verwaltung sind grundlegend folgende Maßnahmenblöcke anzugehen:

- Informationen für den Bürger
- Informationen für die Mitarbeiter der Verwaltung
- Technische und organisatorische Maßnahmen zur Schaffung der Voraussetzungen für die weiteren Stufen der Kommunikation
- Konzept für die langfristige Nutzung des neuen Kommunikationsmediums für die Verwaltung

4.1 Informationen für den Bürger

In allen Stufen sind dem Bürger die zum jeweiligen Zeitpunkt geltenden „Rahmenbedingungen für die elektronische Kommunikation“ mit der Verwaltung darzustellen. Diese sind auf der Homepage gesondert hervorzuheben (z.B. durch einen eigenen Link). Hier ist zunächst eine formelle Zugangseröffnung seitens der Verwaltung zu erklären. Darüber hinaus müssen diese Ausführungen sowohl die nutzbaren Techniken und ggf. erforderliche Einschränkungen darstellen, als auch die Konsequenzen aus dem Verwenden nicht unterstützter Techniken für den Bürger aufzeigen. Dazu gehört auch die Festlegung der seitens der Verwaltung unterstützten Dateiformate und Funktionalitäten einzelner Anwendungen. Mustertexte hierzu finden sich im Anhang 1.

4.2 Informationen für die Mitarbeiter

Entsprechend § 3a des Verwaltungsverfahrensgesetzes des Bundes bzw. der jeweiligen Paragraphen der Landesgesetze ändert sich für viele Mitarbeiter die Bearbeitung von Eingängen durch das Hinzukommen der elektronischen Kommunikation in Ergänzung zu den bisherigen Kommunikationsformen. Mit diesem neuen Kommunikationskanal sind gesetzliche Pflichten für die Verwaltung und den einzelnen Mitarbeiter verbunden, die dem Mitarbeiter in der Anfangsphase nicht klar sind und zur Verunsicherung führen. Für die Beantwortung eingehender Mails sind Musterformulierungen in Form eines Bausteinsystems als Anhang 2 beigefügt.

Darüber hinaus müssen die sich innerhalb einer Verwaltung zwangsweise ergebenden technischen und organisatorischen Änderungen den Mitarbeitern erläutert werden und in

die entsprechenden Dienstanweisungen eingearbeitet werden. Hierzu finden sich Musterformulierungen im Anhang 3.

4.3 Technische und organisatorische Maßnahmen

Für die einzelnen Stufen der Kommunikation sind abhängig von den gegebenen spezifischen Voraussetzungen technische und organisatorische Maßnahmen erforderlich. Nachfolgende Tabelle listet die erforderlichen technischen Voraussetzungen auf.

	Stufe 1	Stufe 2	Stufe 3
Virusprüfung	●	●	●
Entschlüsselungsfunktionalität	-	●	●
Signaturprüfung	-	-	●
Zeitstempelfunktion	-	-	●
Archivierungsfunktionalität	-	-	○

Die Hard- und Software für Entschlüsselung (Stufe 2 und 3) und Signatur (Stufe 3) ist zurzeit höchst proprietär. Genau aus diesem Grund sollte die Kommune nur bestimmte Signatur- und Entschlüsselungsprogramme einsetzen, die konform zu Standards sind. Für den Betrieb und Aufbau von Public Key Infrastrukturen, mit denen die Schlüssel für die Signatur verwaltet werden ist in Deutschland der Standard ISIS-MTT¹³ entwickelt worden. Das entsprechende Produktangebot und die Marktdurchdringung lassen aber noch auf sich warten.

Die Schaffung entsprechender technischer Voraussetzungen muss mit organischen Regelungen für die zuständigen Organisationseinheiten verknüpft werden.

4.4 Konzept für die langfristige Nutzung des neuen Kommunikationsmediums für die Verwaltung

Wie bereits in Kapitel 2.3 dargestellt, ist die Einführung der elektronischen Kommunikation in einer Verwaltung ein Prozess, der vielfältige Auswirkungen hat und Änderungen mit sich bringt, die nicht kurzfristig und losgelöst von den heutigen Verwaltungsprozessen

¹³ <http://www.isis-mtt.org>

vollzogen werden können. Nur durch eine ganzheitliche Betrachtung können wirtschaftliche und langfristig sinnvolle Änderungen in den Prozessen geplant und umgesetzt werden.

Innerhalb einer Verwaltung wird daher die Bildung eines Projektteams empfohlen, das die elektronische Kommunikation aus den Blickwinkeln

- Technik
- Organisation
- Personal
- Finanzen

beleuchtet und eine Ziel- und Maßnahmenplanung erstellt. Diese ist an den langfristigen E-Government-Leitlinien einer Verwaltung auszurichten und beinhaltet nicht nur die Betrachtung der Kommunikationsbeziehungen und Arbeitsprozesse mit Bürgern sondern auch der Wirtschaft, Verbänden, Vereinen und anderen Behörden. Eine frühzeitige Einbeziehung der Personalvertretungen und behördlichen Datenschutzbeauftragten ist in diesem grundlegenden Veränderungsprozess sinnvoll.

Grundlagen und Hinweise zur Erarbeitung eines solchen Konzeptes finden sich in den folgenden Publikationen des Deutschen Städtetages:

- Digitale Signatur auf der Basis multifunktionaler Chipkarten – Ein Leitfaden
- Schritte auf dem Weg zum digitalen Rathaus
- Wo ist der Schlüssel zum Digitalen Rathaus?
- Welche elektronische Signatur braucht die Kommunalverwaltung
- Eröffnung des Zugangs für die elektronische Kommunikation – Teil 1: Grundsätzliche Ausführungen¹⁴

¹⁴ Die Fundstellen der Dokumente sind im Literaturverzeichnis auf Seite 3 zu finden.

Anhang 1: Informationen für den Bürger – Mustertexte

Nachfolgend sind für die einzelnen Stufen Mustertexte für die Rahmenbedingungen für die elektronische Kommunikation wiedergegeben. Diese müssen auf die jeweiligen Bedingungen in der Verwaltung angepasst werden.

Aufgrund der erheblichen Bedeutung sollten die Informationen über den Zugang für die elektronische Kommunikation an möglichst auffälliger Stelle des Internetangebotes einer Kommune (z.B. in Form eines Buttons „Elektronische Kommunikation“) aufgenommen werden. Neben den Mustertexten können hier noch weitere Informationen wie z.B. Anwendungsbeispiele, Hilfefunktionen oder weiterführende Links erscheinen.

Ergänzend bietet es sich an, auch auf den Briefköpfen der Kommune – auf denen in der Regel auch die E-Mail-Adressen angegeben sind – auf diese Informationen hinzuweisen.

Mustertext für die Eröffnung des Zugangs für die elektronische Kommunikation

Die Stadt XYZ bietet Möglichkeiten zur elektronischen Kommunikation an. Für den Bereich der Verwaltungsverfahren richtet sich die elektronische Kommunikation nach § 3 a des Verwaltungsverfahrensgesetzes¹⁵. Danach ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet hat.

Die Stadt XYZ hat diesen Zugang nach Maßgabe der folgenden technischen Rahmenbedingungen für die elektronische Kommunikation eröffnet¹⁶.

Technische Rahmenbedingungen für die elektronische Kommunikation

Mustertext für die Stufe 1 - Die Verwaltung kann noch keine signierten und/oder verschlüsselten E-Mails verarbeiten:

Die Stadt XYZ kann aus technischen und organisatorischen Gründen zurzeit noch keine verschlüsselten und/oder signierten E-Mails entschlüsseln und auf Echtheit und Unverfälschtheit prüfen. Wir werden Sie an dieser Stelle darüber informieren, sobald

¹⁵ Hier ist die jeweils länderspezifische Rechtsgrundlage anzugeben !

¹⁶ An dieser Stelle sollte gegebenenfalls auf einen entsprechenden Ratsbeschluss verwiesen werden. Siehe hierzu auch Ziffer 2.3.5 der Handreichung „Eröffnung des Zugangs für die elektronische Kommunikation – Teil 1: Grundsätzliche Ausführungen“ des Deutschen Städtetages

verschlüsselte und/oder signierte E-Mails bearbeitet werden können. In der Konsequenz gelten folgende Regelungen:

Senden Sie eine verschlüsselte E-Mail an die Kommune, werden Sie darüber informiert, dass Ihre E-Mail nicht bearbeitet wird. In jedem Fall gilt, dass Sie auf diesem Weg nicht mit der Kommune kommunizieren können.

Senden Sie eine signierte E-Mail an die Kommune, die nicht verschlüsselt ist, wird sie wie eine nicht signierte E-Mail behandelt. Sie werden seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Bei elektronischem Schriftverkehr, der nach geltendem Recht der Schriftform bedarf, verwenden Sie bitte bis auf weiteres keine elektronischen Übertragungsformen.

Ist eine E-Mail nicht verarbeitbar, z.B. wegen technischer Probleme oder bei Befall der Mail mit Computerviren, so gilt sie als nicht lesbar. Soweit möglich werden Sie seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Bitte senden Sie bis auf weiteres vertrauliche bzw. datenschutzrechtlich relevante Informationen auf postalischem Weg an die Verwaltung.

Möchten Sie E-Mails mit Dateianhängen an die Verwaltung versenden, so beachten Sie bitte, dass die Verwaltung nicht alle auf dem Markt gängigen Dateiformate und Anwendungen unterstützen kann. Folgende Dateiformate können verarbeitet werden:

Adobe Acrobat ab Version X (.pdf), Rich Text Format (.rtf), Microsoft Word ab Version 7, Microsoft EXCEL ab Version 7, ...

Verwenden Sie abweichende Dateiformate, so kann die Mail nicht bearbeitet werden. Sie werden seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Diese Hinweise gelten nur für die Kommunikation mit der Stadt XYZ und gelten nicht für Verweise auf Angebote von Dritten.

Sollten Sie Fragen zur Verschlüsselung und/oder elektronischen Signatur haben, wenden Sie sich bitte an

Name:

E-Mail-Adresse:

Telefon:

Technische Rahmenbedingungen für die elektronische Kommunikation
Mustertext für die Stufe 2 - Die Verwaltung kann keine Signaturen, aber
verschlüsselte E-Mails verarbeiten:

Leider kann die Stadt XYZ aus technischen und organisatorischen Gründen zurzeit noch keine elektronischen Signaturen auf Echtheit und Gültigkeit prüfen. Wir werden Sie an dieser Stelle darüber informieren, sobald Signaturen geprüft werden können. In der Konsequenz gelten folgende Regelungen:

Folgende Verschlüsselungsverfahren werden seitens der Stadt XYZ unterstützt:

S/Mime

PGP ab Version xxx

GnuPP ab Version xxx

Zur Verschlüsselung vertraulicher bzw. datenschutzrechtlich relevanter Inhalte benötigen Sie als Absender den öffentlichen Schlüssel der Kommune. Der öffentliche Schlüssel der Kommune steht unter folgendem Link zum Download bereit.

<http://www.Stadt-XYZ.de/schluessel.htm>

Sollten bei der Entschlüsselung Schwierigkeiten auftreten, so werden Sie seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Senden Sie eine signierte E-Mail an die Kommune, wird sie wie eine nicht signierte E-Mail behandelt. Soweit möglich werden Sie seitens des Empfängers über die damit verbundenen Konsequenzen informiert. Bei elektronischem Schriftverkehr, der nach geltendem Recht der Schriftform bedarf, verwenden Sie bitte bis auf weiteres keine elektronischen Übertragungsformen.

Ist eine E-Mail nicht verarbeitbar, z.B. wegen technischer Probleme oder bei Befall der Mail mit Computerviren, so gilt sie als nicht lesbar. Sie werden seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Möchten Sie E-Mails mit Dateianhängen an die Verwaltung versenden, so beachten Sie bitte, dass die Verwaltung nicht alle auf dem Markt gängigen Dateiformate und Anwendungen unterstützen kann. Folgende Dateiformate können verarbeitet werden:

Adobe Acrobat ab Version X (.pdf), Rich Text Format (.rtf), Microsoft Word ab Version 7 (.doc), Microsoft EXCEL ab Version 7 (.xls), ...

Verwenden Sie abweichende Dateiformate, so kann die Mail nicht bearbeitet werden. Sie werden seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Diese Hinweise gelten nur für die Kommunikation mit der Stadt XYZ und gelten nicht für Verweise auf Angebote von Dritten.

Sollten Sie Fragen zur Verschlüsselung und/oder elektronischen Signatur haben, wenden Sie sich bitte an

Name:

E-Mail-Adresse:

Telefon:

Technische Rahmenbedingungen für die elektronische Kommunikation

Mustertext für die Stufe 3 - Die Verwaltung kann signierte und verschlüsselte E-Mails verarbeiten:

Leider kann die Stadt XYZ aus technischen und organisatorischen Gründen nicht alle am Markt befindlichen Verschlüsselungs- und Signaturverfahren unterstützen.

Folgende Verschlüsselungsverfahren werden seitens der Stadt XYZ unterstützt:

S/Mime

PGP ab Version xxx

GnuPP ab Version xxx

Zur Verschlüsselung vertraulicher bzw. datenschutzrechtlich relevanter Inhalte benötigen Sie als Absender das öffentliche Schlüsselteil der Kommune. Das öffentliche Schlüsselteil der Kommune steht unter folgendem Link zum Download bereit:

<http://www.Stadt-XYZ.de/schluessel.htm>

Sollten bei der Entschlüsselung Schwierigkeiten auftreten, so werden Sie soweit möglich seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Die in einigen Fällen gegebene Erfordernis der Schriftform kann bei elektronischen Dokumenten durch eine qualifizierte elektronische Signatur eines Dokumentes entsprechend SigG erfüllt werden. Signaturschlüssel folgender Trustcenter können auf Echtheit und Gültigkeit geprüft werden:

TeleSec

SignTrust

...

Wird Ihrerseits für die Signatur einer E-Mail ein Signaturschlüssel verwendet, der nicht obigen Anforderungen entspricht oder dessen Prüfung nicht zu einem positiven Ergebnis führt, gilt die E-Mail als nicht signiert. Sie werden seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Ist eine E-Mail nicht verarbeitbar, z.B. wegen technischer Probleme oder bei Befall der Mail mit Computerviren, so gilt sie als nicht lesbar. Sie werden seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Möchten Sie E-Mails mit Dateianhängen an die Verwaltung versenden, so beachten Sie bitte, dass die Verwaltung nicht alle auf dem Markt gängigen Dateiformate und Anwendungen unterstützen kann. Folgende Dateiformate können verarbeitet werden:

Adobe Acrobat ab Version X, Rich Text Format (.rtf), Microsoft Word ab Version 7, Microsoft EXCEL ab Version 7, ...

Verwenden Sie abweichende Dateiformate, so kann die Mail nicht bearbeitet werden. Sie werden seitens des Empfängers über die damit verbundenen Konsequenzen informiert.

Diese Hinweise gelten nur für die Kommunikation mit der Stadt XYZ und gelten nicht für Verweise auf Angebote von Dritten.

Sollten Sie Fragen zur Verschlüsselung und elektronischen Signatur haben, wenden Sie sich bitte an

Name:

E-Mail-Adresse:

Telefon:

Anhang 2: Textbausteine für Rückantworten an den Bürger

Zur Handhabung:

In der linken Spalte „Sachverhalt“ sind die Gegebenheiten beschrieben, die dem Sachbearbeiter einen schnellen Überblick über die gegebene Situation verschaffen.

In der Spalte „Text“ findet sich ein Textvorschlag zum Sachverhalt.

Um im „Bausteinverfahren“ zu kompletten Re-Mail-Texten zu gelangen, sind die Bausteine je nach Charakter mit „Kurzbezeichnungen“ versehen:

- die mit „E“ beginnenden dienen bei der Antwort zur Einleitung des Textes;
- der mit „B“ beginnende bestätigt den Mail-Erhalt, wenn das Anliegen nicht sofort bearbeitet werden kann;
- die mit „P“ beginnenden beschreiben einen Sachverhalt / ein konkretes Problem, also den Anlass für die Re-Mail;
- die mit „M“ beginnenden formulieren einen Handlungsvorschlag, um in der Sache weiter zu kommen;
- die mit „S“ beginnenden schließen den Text ab.

Es wird sich in der Praxis ergeben, dass bestimmte Kombinationen häufiger auftreten, sie können dann als Gesamtdokument (z.B.: E01 / P01 / M03 / S01) erfasst werden.

Die „Bemerkungen“ und Verweise „Weiter mit ...“ dienen der weiteren Orientierung des Sachbearbeiters zur E-Mail-Erstellung.

Sofern in der Antwort auf das Anliegen des Absenders Bezug genommen wird, sind die Belange des Datenschutzes zu beachten.

Damit inhaltlich auf die „Rahmenbedingungen für die elektronische Kommunikation“ Bezug genommen werden kann, setzt dies voraus, dass sich diese - möglichst grafisch markant - auf der städt. Homepage befinden. Dabei sollte unter Bezug auf das Landesverwaltungsverfahrensgesetz und die sogenannte „Zugangseröffnung“ erläutert werden, auf welche Weise und wofür die Kommune den elektronischen Zugang eröffnet hat. Ein Mustertext findet sich in dieser Broschüre im Anhang 1.

Sachverhalt	Text	Baustein Nr.	Bemerkung	Siehe ----- weiter mit
Einleitung				
Einleitungssatz	Sehr geehrter <Herr / Frau>, mit E-Mail vom <Datum> haben Sie <Sachverhalt kurz ausführen> (z.B. gegen die mit Bescheid vom <Datum> erteilte Baugenehmigung Widerspruch eingelegt.)	E 01	Durch Benutzen der Funktion „Antwort“ im E-Mail-Programm kann die ursprüngliche E-Mail automatisch angehängt werden	----- B 01 bzw. P 01 bis P 011
Bestätigung des Eingangs				
Bestätigung des Eingangs, wenn keine unmittelbare Bearbeitung erfolgen kann	Wir bestätigen Ihnen den Eingang Ihrer E-Mail. Wir werden Ihr Anliegen so bald wie möglich bearbeiten. Bis dahin bitten wir Sie um ein wenig Geduld.	B 01	wie bei E 01	S 04
Grund für die Re-Mail / Problembeschreibung				
E-Mail kann nicht gelesen werden; ggf. nicht zugelassener Standard	Leider können wir die uns übersandte E-Mail nicht lesen: Sie verwenden einen Standard, der für die elektronische Kommunikation mit uns nicht zugelassen ist.	P 01	wie bei E 01	M 03
Dateianhang (Dateianhang) nicht lesbar; nicht zugelassenes Dateiformat	Leider können wir den Dateianhang, den Sie Ihrer E-Mail beigefügt haben, nicht lesen/öffnen: Sie verwenden ein Dateiformat, das für die elektronische Kommunikation mit uns nicht zugelassen ist.	P 02	wie bei E 01	M 03
Ausführbare	Leider haben Sie uns ein Mail	P 03	wie bei E 01	M 02

Sachverhalt	Text	Baustein Nr.	Bemerkung	Siehe ----- weiter mit
Datei (z.B. .exe) übersandt	mit einer ausführbaren Datei übersandt, die wir wegen der damit verbundenen Virengefahr und den mit Viren verbundenen Folgen nicht öffnen können.			
Makros im Dateianhang, deren Ausführung für das Lesen des Textes notwendig sind	Leider enthält das uns als Dateianhang übersandte Dokument Makros, ohne die der Text offensichtlich nicht vollständig gelesen werden kann. Wegen der mit Makros verbundenen Virengefahr können wir diese nicht ausführen.	P 04	wie bei E 01	M 01
Dateianhang enthielt Viren ; Dateianhang gelöscht	Wie wir beim Maileingang festgestellt haben, enthielt der uns übermittelte Dateianhang Viren. Wir mussten den Dateianhang wegen der mit Viren verbundenen Folgen löschen.	P 05		M 01
Handschriftliche Unterschrift bzw. eine qualifizierte elektronische Signatur erforderlich	Für Ihr Anliegen ist nach den gesetzlichen Vorschriften eine handschriftliche Unterschrift bzw. eine qualifizierte elektronische Signatur erforderlich.	P 06		M 04 M 05 M 06
Es wurde eine „fortgeschrittene Signatur“ verwendet; Schriftform nicht erfüllt	Leider handelt es sich bei der von Ihnen verwendeten elektronischen Signatur nur um eine sog. „fortgeschrittene Signatur“. Diese erfüllt nicht die erforderliche Schriftform.	P 07		M 05 M 06

Sachverhalt	Text	Baustein Nr.	Bemerkung	Siehe ----- weiter mit
Dateianhang mit Passwort geschützt	Der Ihrem E-Mail beigefügte Dateianhang konnte nicht bearbeitet werden, da diese Datei mit einem Passwort versehen ist.	P 08		M 07
Verschlüsselungsverfahren wird nicht unterstützt	Sie haben ein Verschlüsselungsverfahren angewandt, das wir nicht einsetzen. Wir können Ihr Anliegen deshalb leider nicht bearbeiten.	P 09		M 08
Web-Anwendung vorhanden	Sie haben uns Ihr Anliegen mit einem formlosen E-Mail zugeleitet. Für diesen Prozess bieten wir jedoch eine <interaktive> Web-Anwendung an, die eine rasche Bearbeitung ohne Medienbruch ermöglicht.	P 10		M 09
nicht zuständig	Für das uns zugeleitete Anliegen sind wir sachlich/örtlich nicht zuständig.	P 11		M 10
Problemlösung / konkrete Maßnahme				
Übersendung eines Dateianhangs ohne Viren bzw. Makros	Wir bitten Sie, uns einen Dateianhang ohne Computerviren/Makros zu übersenden, damit wir Ihr Anliegen bearbeiten können.	M 01		P 04 P 05 ----- S 01

Sachverhalt	Text	Baustein Nr.	Bemerkung	Siehe ----- weiter mit
Lösung ohne ausführbare Datei wählen	Wir bitten Sie, eine Lösung zu wählen, die keine ausführbare Datei erfordert.	M 02		P 03 ----- S 01
Hinweis auf Kommunikationsregeln; Antrag wiederholen	Bitte informieren Sie sich auf unserer Homepage (www.Stadt-XYZ.de) über die „Rahmenbedingungen für die elektronische Kommunikation“, die bei der Kommunikation mit uns beachtet werden müssen. Bitte senden Sie uns den Vorgang erneut in regelkonformer Ausführung, oder – falls Ihnen das nicht möglich ist - ggf. per Post, damit wir ihn bearbeiten können.	M 03		P 01 P 02 ----- S 01
Elektronische Signatur technisch nicht möglich; erneute Übersendung des Antrags in Papierform	Wir verwenden derzeit elektronische Signaturen nur in dem auf unserer Homepage (www.Stadt-XYZ.de) ausgewiesenen Umfang. Deshalb bitten wir Sie, uns Ihren Antrag erneut in Papierform zu übersenden.	M 04		P 06 ----- S 01
Zugelassene qualifizierte Signatur verwenden; neuer Antrag	Wir bitten Sie, den Vorgang erneut an uns zu senden und dabei eine von uns zugelassene qualifizierte Signatur zu verwenden.	M 05		P 06 ----- M 06
Hinweis auf zugelassene qualifizierte Signaturen	Die für die elektronische Kommunikation mit uns zugelassenen qualifizierten Signaturen finden Sie in	M 06		P 06 P 07 -----

Sachverhalt	Text	Baustein Nr.	Bemerkung	Siehe ----- weiter mit
	<p>unseren Rahmenbedingungen für die elektronische Kommunikation auf unserer Homepage (www.Stadt-XYZ.de).</p> <p>Falls Sie keine dieser Signaturen besitzen, bitten wir Sie auf die Papierform auszuweichen.</p>			S 01
Passwort mitteilen	Bitte teilen Sie das Passwort mit, damit wir Ihr Anliegen bearbeiten können.	M 07		P 08 ----- S 01
zugelassenes Verschlüsselungsverfahren verwenden; ggf. papiergebundene Kommunikation	<p>Bitte teilen Sie uns Ihr Anliegen unter Verwendung des in der Kommunikation mit uns zugelassenen Verschlüsselungsstandards erneut mit oder weichen Sie auf die papiergebundene Kommunikation aus.</p> <p>Die für eine elektronische Kommunikation mit uns geltenden Regeln finden Sie auf unserer Homepage (http://www.Stadt-XYZ.de).</p>	M 08	Eine Verschlüsselung durch den Absender setzt üblicherweise voraus, dass die Kommune einen öffentlichen Schlüssel besitzt und diesen z.B. auf ihrer Homepage bekannt gibt.	P 09 ----- S 01
Web-Anwendung benutzen	Wir bitten Sie, uns Ihr Anliegen erneut mitzuteilen und dabei die von uns hierfür eingerichtete Webanwendung zu benutzen. Die Anwendung finden Sie unter http://www.Stadt-XYZ.de .	M 09	Soweit möglich, sollten die Daten im beiderseitigen Interesse mittels der Web-Anwendung eingegeben werden	P 10 ----- S 01
Weiterleitung	Wir haben Ihre E-Mail	M 10	Mit der	P 11

Sachverhalt	Text	Baustein Nr.	Bemerkung	Siehe ----- weiter mit
an zuständige Organisationseinheit	deshalb an <Organisationseinheit> mit der Bitte um zuständige Erledigung weitergeleitet		Weiterleitungsfunktion im E-Mail-Programm kann die „Abgabennachricht“ erstellt und der Vorgang gleichzeitig weitergeleitet werden.	----- S 01
Schluss				
Bedauern , dass Anliegen nicht erledigt werden kann	Wir bedauern, dass Ihr Anliegen auf dem von Ihnen gewählten Weg nicht erledigt werden konnte.	S 01		----- S 02 oder S 03 S 04
Hoffen , dass weiter geholfen werden konnte	.. und hoffen, Ihnen mit unserer Auskunft weiter geholfen zu haben.	S 02		S 01 ----- S 04
Hoffen auf baldige Erledigung	.. und hoffen, dass dies bald geschehen kann.	S 03		S 01 -----

Sachverhalt	Text	Baustein Nr.	Bemerkung	Siehe ----- weiter mit
				S 04
Gruß	Mit freundlichen Grüßen <Absenderangaben, z.B. sogenannte "V-Card" ¹⁷ >	S 04		

¹⁷ V-Card = elektronische Visitenkarte, die in E-Mail-Programmen an erstellte Nachrichten angehängt werden kann und Angaben zum Absender (Name, Anschrift, Telefonische Erreichbarkeit, etc.) enthält

Anhang 3: Mustertexte für generelle Dienstanweisungen

Nachfolgende Mustertexte können als Vorlagen für die Überarbeitung von Dienstvorschriften herangezogen werden. Die für die Beantwortung eingehender E-Mails geeigneten Formulierungen finden sich als Textbausteine in Anhang 2 dieser Ausarbeitung.

Für die **Stufe 1** (die Verwaltung kann noch keine signierten und/oder verschlüsselten E-Mails verarbeiten) ist die Dienstanweisung E-Mail um folgende Punkte zu ergänzen:

Elektronischer Posteingang:

- Im Falle, dass eine unverschlüsselte und/oder unsignierte E-Mail zugesandt wird, deren Inhalt laut Rechtsvorschrift der Schriftform bedarf, informiert der Sachbearbeiter den Absender der E-Mail mit Verweis auf die veröffentlichten Rahmenbedingungen für die elektronische Kommunikation darüber, dass ein Schreiben dieses Inhaltes bis auf weiteres nicht per E-Mail angenommen werden kann.
- In den Fällen, in denen eine E-Mail aufgrund einer Verschlüsselung nicht lesbar ist, informiert der Sachbearbeiter den Absender mit Verweis auf die veröffentlichten Rahmenbedingungen für die elektronische Kommunikation darüber, dass verschlüsselte E-Mails bis auf weiteres nicht bearbeitet werden können.
- Bei Empfang einer mit elektronischer Signatur versehenen E-Mail, deren Inhalt rechtserheblich sein könnte, weist der Sachbearbeiter den Absender per E-Mail mit Verweis auf die veröffentlichten Rahmenbedingungen für die elektronische Kommunikation darauf hin, dass die Signatur aus technischen Gründen bis auf weiteres nicht nachprüfbar ist.
- Wenn eine E-Mail nicht verarbeitbar ist (z.B. aufgrund von Dateianhängen mit nicht unterstützten Dateiformaten, Befall mit Computerviren, etc.), weist der Sachbearbeiter den Absender unter Angabe des Grundes mit Verweis auf die veröffentlichten Rahmenbedingungen für die elektronische Kommunikation darauf hin.

Für die **Stufe 2** (die Verwaltung kann keine Signaturen, aber verschlüsselte E-Mails verarbeiten) ist die Dienstanweisung E-Mail um folgende Punkte zu ergänzen:

Elektronischer Posteingang:

- Im Falle der Zusendung einer E-Mail, bei der eine nicht unterstützte Verschlüsselungstechnik verwendet wurde, weist der Sachbearbeiter den Absender unter Angabe des Grundes mit Verweis auf die veröffentlichten Rahmenbedingungen für die elektronische Kommunikation darauf hin.

Für die **Stufe 3** (die Verwaltung kann signierte und verschlüsselte E-Mails verarbeiten) ist die Dienstanweisung E-Mail um folgende Punkte zu ergänzen:

Elektronischer Posteingang:

- Wird bei einer E-Mail eine elektronische Signatur verwendet, um die durch eine Rechtsvorschrift geforderte Schriftform zu erfüllen und wird die eingesetzte Signaturtechnik nicht unterstützt, weist der Sachbearbeiter den Absender unter Angabe des Grundes mit Verweis auf die veröffentlichten Rahmenbedingungen für die elektronische Kommunikation darauf hin, dass seine E-Mail nicht bearbeitet werden kann.
- Wird bei einer E-Mail eine Signatur verwendet, um die durch eine Rechtsvorschrift geforderte Schriftform zu erfüllen und ist das Prüfergebnis der Signaturprüfung negativ, weist der Sachbearbeiter den Absender unter Angabe des Grundes mit Verweis auf die veröffentlichten Rahmenbedingungen für die elektronische Kommunikation darauf hin, dass seine E-Mail nicht bearbeitet werden kann.

Anhang 4: Übersicht über den Stand der Anpassung der Verwaltungsverfahrensgesetze der Länder