

<b>E-Mail-Policy</b>		<b>Konvention</b>
		<b>mailpol 2.0.3</b>
		<b>Entwurf öffentlich</b>
Kurzbeschreibung	<p>Diese Konvention legt technische und organisatorische Aspekte des Verhaltens der öffentlichen Verwaltung bei der elektronischen Datenübermittlung mittels E-Mail fest.</p> <p>Ziel dieses Dokumentes ist es, Mindestanforderungen für den Umgang der öffentlichen Verwaltung mit dem Kommunikationsmedium E-Mail zu definieren.</p> <p>Das gegenständliche Dokument gilt als Grundlage für Behörden, einerseits für die entsprechende technische Umsetzung und andererseits für die Erstellung der zu veröffentlichenden Policies, an der sich die Zielgruppen (Bürger, Wirtschaft, Behörden - siehe [INTPOL]) orientieren können.</p> <p>Dieses Dokument ersetzt die Dokumente</p> <ul style="list-style-type: none"> <li>• „Empfehlungen - Homogenisierung der symbolischen Adressen für X.400 und SMTP-Mail – T04“ [T.04] und</li> <li>• die „E-Mail-Policy 1.0.0“ [MAILPOL].</li> </ul>	
Autor(en)	<b>Bernd Martin</b> <b>Michael Liehmann</b>	<b>Projektteam / Arbeitsgruppe</b> <b>Internetpolicy</b>

Stelle	Vorgelegt am	Angenommen an	Abgelehnt am
<b>IKT-Board</b> <b>Länder</b> <b>Gemeinebund</b> <b>Städtebund</b>	29.06.2004 25.10.2005 25.10.2005 25.10.2005	29.06.2004  15.11.2005 15.11.2005	  15.11.2005

## E-Mail-Policy

### Inhaltsverzeichnis<sup>1</sup>

(1)	Einleitung .....	4
(2)	Inhalte der behördeneigenen E-Mail-Policy.....	4
(3)	Maßnahmenkatalog .....	6
(3.1)	Adressierungsrichtlinien <b>B</b> .....	6
(3.1.1)	Adressformat <b>B</b> .....	6
(3.1.2)	Namenskonventionen <b>B</b> .....	6
(3.1.3)	Einrichtung eines Postmasters <b>B</b> .....	7
(3.1.4)	Organisatorische Maßnahmen <b>B</b> .....	8
(3.2)	E-Mail-Transferprotokolle <b>B/O</b> .....	9
(3.2.1)	Client-Server-Kommunikation <b>B/O</b> .....	9
(3.2.2)	Nachrichten-Bodyparts <b>B</b> .....	9
(3.3)	E-Mailzertifikate <b>B</b> .....	9
(3.3.1)	Elektronisch signierte E-Mails <b>B</b> .....	10
(3.3.2)	Verschlüsselte E-Mails <b>B</b> .....	10
(3.4)	Standardkonformität <b>B</b> .....	11
(3.5)	Zugangsregelungen zu E-Mail-Systemen <b>B/O</b> .....	11
(3.5.1)	Standardzugang <b>B</b> .....	11
(3.5.2)	Remotezugang <b>O</b> .....	12
(3.6)	Formate <b>B</b> .....	12
(3.6.1)	Zugelassene Formate <b>B</b> .....	12
(3.6.2)	Unzulässige Formate <b>B</b> .....	12
(3.6.3)	Ausgehende Formate <b>B</b> .....	13
(3.7)	Größenbeschränkung bei E-Mails <b>B</b> .....	13
(3.8)	Automatisch generierte Notifikationen.....	13
(3.8.1)	Notifikation bei ungültiger Empfängeradresse <b>B</b> .....	13
(3.8.2)	Notifikation bei Formatverletzung <b>B</b> .....	13
(3.8.3)	Notifikation bei E-Mail-Übergröße <b>B</b> .....	13

<sup>1</sup> Im Maßnahmenkatalog werden Basisanforderungen mit einem **B** und optionale Anforderungen mit einem **O** markiert. Während Basisanforderungen verpflichtend in der behördeneigenen E-Mail-Policy zu behandeln sind, gelten optionale Anforderungen als Empfehlung.

---

(3.8.4)	Notifikation Out-of-Office <input type="checkbox"/>	14
(3.8.5)	Notifikation bei festgestellten Viren/Malware <input type="checkbox"/>	14
(3.8.6)	Notifikation bei Spam <input type="checkbox"/>	14
(4)	Malware und Viren	15
(4.1)	Möglichkeiten zum Eingriff	15
(4.1.1)	Behandlung am SMTP Gateway und/oder am E-Mail-Proxy <input type="checkbox"/>	15
(4.1.2)	Behandlung am Client <input type="checkbox"/>	15
(4.1.3)	Aufklärung <input type="checkbox"/>	15
(4.2)	Maßnahmen bei positiver Virenprüfung <input type="checkbox"/>	16
(4.2.1)	Quarantäne <input type="checkbox"/>	16
(4.2.2)	Weiterleitung von gesäuberter E-Mail <input type="checkbox"/>	16
(4.2.3)	Löschung <input type="checkbox"/>	16
(5)	Spam	16
(5.1)	Aktive Abwehrmaßnahmen	16
(5.2)	Passive Abwehrmaßnahmen	19
(5.2.1)	Schließung offener Relays <input type="checkbox"/>	19
(5.2.2)	Blockierung offener Relays <input type="checkbox"/>	19
(6)	Verfügbarkeit und Performance <input type="checkbox"/>	19
(7)	Maßnahmen zur Aufbewahrung von E-Mail	20
(7.1)	Mailarchivierung vs. Backup	20
(7.1.1)	Mailarchivierung <input type="checkbox"/>	20
(7.1.2)	Backup <input type="checkbox"/>	20
(7.2)	Protokollierung und Logging	20
(7.3)	Ausbildung der Endanwender	20
(8)	Offenlegung der Policy	21
(9)	Anhang	22
(9.1)	Beispielhafte E-Mail-Signatur	22
(9.2)	Beispielhafte Notifikation bei ungültiger Empfängeradresse	22
(9.3)	Beispielhafte Notifikation bei Formatverletzung	23
(9.4)	Beispielhafte Notifikation bei E-Mail-Übergröße	23
(9.5)	Beispielhafte Notifikation bei Out-of-Office	24
(10)	Referenzen	25

## (1) Einleitung

Diese Konvention legt technische und organisatorische Aspekte des Verhaltens der öffentlichen Verwaltung bei der elektronischen Datenübermittlung mittels E-Mail fest.

Das Dokument ist so aufgebaut, dass zu Beginn eine Übersicht angeführt wird über jene Themen, die in der von der Behörde zu erstellenden Policy behandelt werden müssen.

In weiterer Folge werden mit einem Maßnahmenkatalog sowohl Vorgaben vorgegeben, an die sich die Behörde unbedingt halten soll (Minimal- bzw. Basisanforderungen), aber auch optionale Vorgaben, für welche die Behörde nach eigenem Ermessen entscheiden kann, ob sie diese in ihre E-Mail-Policy mit aufnehmen will.

In speziellen Unterkapiteln werden die Themen Spam, Viren, Protokollierung und Archivierung genauer behandelt. Zum Schluss werden noch jene Punkte der E-Mail-Policy angeführt, die von der Behörde veröffentlicht werden müssen.

*Best Practice* Beispiele zu den diversen Punkten sollen der Zielgruppe dieses Dokuments eine praktische Hilfestellung bei der Erstellung der eigenen Policy geben.

### Ziel

Ziel dieses Dokumentes ist es, Mindestanforderungen für den Umgang der öffentlichen Verwaltung mit dem Kommunikationsmedium E-Mail zu definieren. Das gegenständliche Dokument gilt als Grundlage für Behörden, einerseits für die entsprechende technische Umsetzung und andererseits für die Erstellung der zu veröffentlichenden E-Mail-Policyinhalte, in welcher die Grundsätze und Verhaltensregeln für E-Mail-Kommunikationspartner einer Behörde (Bürger, Wirtschaft, Behörden – siehe [INTPOL]) klar festgelegt werden.

Dieses Dokument ersetzt die Dokumente

- „Empfehlungen - Homogenisierung der symbolischen Adressen für X.400 und SMTP-Mail – T04“ [T.04] und
- die „E-Mail-Policy 1.0.0“ [MAILPOL].

Ein Glossar kann im Dokument gefunden werden.

## (2) Inhalte der behördeneigenen E-Mail-Policy

Aufgrund der weiten Verbreitung von E-Mail ist dieser Kommunikationsweg zwischen Bürger, Wirtschaft und Behörde, aber auch zwischen Behörden zu ermöglichen und zu regeln. In diesem Abschnitt werden jene Bereiche angeführt, die in der von der Behörde erstellten E-Mail-Policy behandelt werden müssen. Der darauf folgende Abschnitt (3) beinhaltet eine Liste von Maßnahmen, zu denen die Behörde in ihrer eigenen E-Mail-Policy entweder verpflichtend Stellung nehmen muss bzw. auch optional Stellung nehmen kann. Die angegebenen verpflichtenden Maßnahmen stellen dabei Minimalanforderungen dar und sollen nicht unterschritten werden, der Behörde steht es allerdings frei, strengere Richtlinien zu erstellen. Eine Unterschreitung ist nur dann erlaubt, wenn es dafür eine nachvollziehbare Begründung gibt.

Welche Inhalte die Behörde jedenfalls veröffentlichen muss, wird im Abschnitt (8) geregelt.

An dieser Stelle sei noch anzumerken, dass aufgrund der verstärkten Internetpräsenz bei der Kommunikation Bürger zu Behörde die Verwendung von Web-Interfaces eine immer größer werdende Bedeutung gewinnt, die Kommunikation mittels E-Mail jedoch nicht gänzlich vernachlässigt werden kann.

**Best Practice:**

Der Kontakt zu Bürgerinnen und Bürgern sollte – wo immer möglich – über ein Web-Interface stattfinden. Dabei kann man sich z.B. Web-Formulare zunutze machen.

Die Behörden benötigen zusätzliche organisatorische Richtlinien, die darauf abzielen, den Umgang mit E-Mail-Systemen zu definieren und die zumindest folgende Vorgaben umfassen sollen. Mehrere dieser Vorgaben werden in dieser E-Mail-Policy bereits genauer ausgeführt und finden sich in den folgenden Kapiteln wieder.

- Richtlinien zum Einsatz von E-Mail
  - Es sollte festgehalten werden, für welchen Einsatz E-Mail vorgesehen ist. Dafür ist die Bekanntgabe notwendig, bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch E-Mails versandt werden dürfen. (vgl. dazu auch das jeweilig geltende Sicherheitshandbuch oder [SiHB]).
- Richtlinien für den eingehenden E-Mail-Verkehr
  - Organisatorische Zuständigkeit bestimmter Bediensteter für Organisationspostfächer
  - Abfragefrequenz von Organisationspostfächern
  - Verhalten (Meldewege) bei Malware- bzw. Virenverdacht (malicious software), im Speziellen bei Organisations-E-Mail-Boxen
- Richtlinien für ausgehenden E-Mail-Verkehr
  - Festlegung von Antwortverhalten (maximale Antwortzeit, inhaltliche Zuständigkeit, Approbation, Antwortzeit und -eigenschaften bei Organisationspostfächern, etc.)
  - Festlegung von Verbindlichkeitsformeln (Amtshaftung) und Verantwortung des Absenders
- Richtlinien für die Verwendung von digitalen Zertifikaten zu Signatur- und Verschlüsselungszwecken
  - Verwendung für dienstliche Tätigkeiten
  - Private Verwendung
- Richtlinien zur Corporate Identity
  - E-Mail-Formatierung (HTML oder Text)
  - Corporate-Identity (CI), Netiquette und E-Mail-Signaturen (Achtung: hier sind nicht elektronische Signaturen gemeint)
- Definition von Adressierungsrichtlinien und Protokollvorgaben für den behördlichen E-Mail-Verkehr
- Angaben über die Qualitätssicherung (Mechanismen und Maßnahmen, wie die Einhaltung der E-Mail-Policy sichergestellt wird)
- Richtlinien für private Nutzung von E-Mail-Ressourcen
  - Zulässigkeit der Verwendung von dienstlichen E-Mail-Adressen für privaten E-Mail-Verkehr
  - Zulässigkeit der Verwendung von privaten E-Mail-Konten auf dienstlich zur Verfügung gestellten Computern

**Best Practice:**

Ein Beispiel für eine E-Mail-Signatur (nicht zu verwechseln mit der elektronischen Signatur) findet sich im Anhang wieder (siehe (9.1)). Weitere Hinweise sind auch im jeweilig geltenden Sicherheitshandbuch bzw. im Österreichischen Sicherheitshandbuch [SiHB] zu finden.

**Hinweis:**

Die Erstellung, Publikation (Schulung) und Kontrolle der Einhaltung der vorgegebenen Richtlinien erfordert eine genaue Analyse des ressortinternen Sicherheitsbedarfes, stellt einen wesentlichen Faktor im Gesamtkontext der Sicherheit dar und liegt im Zuge der Organisationshoheit der Behörden in der Verantwortung derselben.

### (3) Maßnahmenkatalog

Zu den allgemeinen Vorgaben zählen zum einen Richtlinien zu Adressierungstechniken und zum anderen aber auch solche, die das Verfahren des E-Mail-Transfers definieren, Angaben zu E-Mail-Zertifikaten und Vorgaben mit der Zielsetzung eine grundsätzliche Standardkonformität garantieren zu können.

#### (3.1) Adressierungsrichtlinien



Im Bereich der Adressregeln sind folgende Definitionen zusammengefasst:

- Adressformat
- Namenskonventionen (Namingpolicy)
- Einrichten eines Postmasters

##### (3.1.1) Adressformat



Das Adressformat orientiert sich am SMTP-Standard, der verbindlich zum Einsatz kommt. Daher sind die E-Mail-Adressen seitens der Behörden grundsätzlich nach den Regeln des Internet-Standards [RFC 2822] zu gestalten.

**Best Practice:**

Beim Adressformat ist zu beachten, dass es wenige Möglichkeiten gibt, wo es trotz RFC konformen Namen bei E-Mailservern zu Problemen kommen kann.

##### (3.1.2) Namenskonventionen



Die Definition der für eine Behörde gültigen Adresskonzepte stellt einen wesentlichen Teil der internen Ablauforganisation dar. Grundsätzlich gibt es zwei Modelle, das personenbezogene und das organisationsbezogene Adressmodell.

Das Basisformat für die **persönliche Adresse** sieht folgendes vor:

[<Vorname>.<Nachname>@<Domainname>](#)

Im „local-name“ (<Vorname>.<Nachname>) ist von der Behörde selbst eine Regelung für die Unterscheidung von Personen mit Namensgleichheit festzulegen.

Vorschlag für Basisformate für **organisationsbezogene Adressen**:

Basisformat 1: [post.<Organisationsname>@<Domainname>](#) bzw.

[<Organisationsname>.post@<Domainname>](#)

Basisformat 2: [post@\[<Organisationsname>.<Domainname>](#)

**Best Practice:**

Die Länge des „local-name“, also dem Teil vor dem @, soll 50 Zeichen nicht überschreiten.

Der Domainname in der E-Mail-Adresse erfolgt nach den Regeln, die in den Policies für die Domain .gv.at [DOMAINPOL] bzw. [DOMAINREG] festgelegt sind. Nach Fertigstellung der überarbeiteten Domain-Policy sind die Vorgaben dieses Dokuments einzuhalten.

Für jede Organisationsdomain muss ein Organisationspostfach nach dem Schema [post@<Domainname>](#) existieren. Diese Adresse ist auch nach extern zu publizieren.

Für E-Mail-Adressen sind Namenskonventionen festzulegen, die im Speziellen klar regeln, wie Sonderzeichen (Umlaute, usw.) codiert werden sollen. Für die gängigsten Sonderzeichen wird folgendes empfohlen:

Zeichen	Konvention
ä	ae
ö	oe
ü	ue
ß	ss

**Best Practice:**

Für gültige E-Mail-Adressen von zwei namensgleichen Personen könnte eine mögliche Lösung so aussehen:

[Max-Gustav.Mustermann@bka.gv.at](#) und [Max-Fritz.Mustermann@bka.gv.at](#)

Bei den organisationsbezogenen Adressen ist das **Basisformat 1** zu bevorzugen. Demnach wäre eine gültige Adresse: [post.sektion2@bka.gv.at](#).

Ein Beispiel für ein gültiges Organisationspostfach ist [post@bmf.gv.at](#). Eine nachgeordnete Behörde des BMF würde folgende Organisationsadresse besitzen: [post.finanzeamt.tulln@bmf.gv.at](#).

Bei allen Organisationspostfächern muss sichergestellt sein, dass dieses Postfach zuverlässig betreut wird und geeignete Anti-SPAM- bzw. Anti-Viren-Lösungen geschaffen werden.

Organisationsbezogene Adressen dürfen in Ausnahmefällen genau dann von den hier angeführten Vorgaben abweichen (ohne dem Merkmal ‚post‘), wenn aus der behördeneigenen Policy klar hervorgeht, welche Adressen Organisationspostfächer sind. Die organisatorischen Maßnahmen müssen zumindest gleichwertig zu den in dieser E-Mail-Policy angeführten sein. In jedem Falle muss jedoch das Organisationspostfach für jede Organisationsdomain den in diesem Dokument angeführten Vorgaben entsprechen (Format und organisatorische Maßnahmen).

**(3.1.3) Einrichtung eines Postmasters**

Gemäß RFC 2821 hat jeder SMTP-Server, die Adresse [postmaster@<Domainbezeichnung>](#) zu unterstützen. Dies gilt auch für Behörden. Dieses Postfach ist in Bezug auf Abfragefrequenz und organisatorische Sicherstellung, dass eine Person dieses Postfach betreut, den Organisationspostfächern gleich gestellt.

### (3.1.4) Organisatorische Maßnahmen<sup>2</sup>



Anträge sollen sofern über E-Mail eingebracht über die vorgesehenen Organisationspostfächer entgegen genommen werden. Dies ist entweder in der Domain-Policy zu dokumentieren und in der E-Mail-Policy zu referenzieren oder umgekehrt. Nach einer ordnungsgemäßen Entgegennahme bei diesen Organisationspostfächern (d.h. nach Viren- und Spamprüfung) muss sichergestellt sein, dass eine Benachrichtigung über den positiven Eingang **bis spätestens zum Ende des nächsten Werktages** an den Absender erfolgt.

Sofern andere organisatorische Vorkehrungen getroffen werden, die dem Absender eine gleichwertige Qualität der Entgegennahme garantieren können, kann von diesen Vorgaben abgewichen werden. Diese ist in der behördeneigenen Policy anzuführen.

#### **Best Practice:**

Der Inhalt des Reply-To Felds in der Antwort-E-Mail soll wiederum die Organisationsadresse sein.

Nach technischen Möglichkeiten soll diese Benachrichtigung elektronisch signiert sein und als Inhalt das gesendete E-Mail inkl. Attachments beinhalten. Des Weiteren kann dabei vom behördlichen Zeitstempeldienst Gebrauch gemacht werden, dessen Zeitangabe für den Fristenlauf von Bedeutung ist. Auf jeden Fall muss aber eine korrekte Zeitangabe (Sicherstellung obliegt grundsätzlich der Behörde) in der Bestätigung angegeben werden, die verbindlich für den Beginn des Fristenlaufs ist. Für den Benutzer bedeutet der Erhalt der Bestätigung die ordnungsgemäße Entgegennahme von der Organisation/Behörde.

Alternativ dazu kann die Organisation auch andere Mechanismen umsetzen. So kann über Beilagen (Namen, Datum und Inhalt) mit Hilfe einer Einweg-Funktion (Hash) ein eindeutiger Wert berechnet werden und dieser in einer vom Zeitstempel signierten Antwort-E-Mail retourniert werden. Auch hier gilt, dass der Zeitstempel alternativ realisiert werden kann. Grundsätzlich gilt, dass Missbrauch ausgeschlossen sein muss.

#### **Best Practice:**

Eine Organisation kann bei Organisationspostfächern ein Service anbieten, das es erlaubt festzustellen, ob ein E-Mail zumindest vom E-Mail-Server entgegen genommen wurde.

Werden Anträge wider Erwarten an persönliche Postfächer adressiert, dann hat der jeweilige Empfänger dafür zu sorgen, dass diese der behördeneigenen Kanzleiordnung behandelt werden. Eine mögliche Verzögerung aufgrund von Abwesenheiten geht zu Lasten des Anbringers.

#### **Best Practice:**

An persönliche Postfächer adressierte E-Mails könnten z.B. durch Weiterleitung des Anbringens an das jeweilige Organisationspostfach bzw. die offizielle Einlaufadresse abgehandelt werden.

In der E-Mail-Policy soll auch festgehalten werden, welcher Alternativweg für ein Anbringen zur Verfügung steht. Diese Möglichkeit muss nicht auf das Medium E-Mail beschränkt sein, sondern kann z.B. in Form eines Allgemeinen Anbringens (Webformular) erfolgen.

---

<sup>2</sup> Dieser Punkt betrifft sowohl die E-Mail-Policy als auch die Domain-Policy.

### (3.2) E-Mail-Transferprotokolle

 B /  O

Das generelle Ziel der E-Government-Strategie ist die Einrichtung der Kommunikation nach offenen international verfügbaren und anerkannten Standards. Nur so können Interoperabilität, Kompatibilität und eine weite Verbreitung erreicht werden.

#### (3.2.1) Client-Server-Kommunikation

 B /  O

Daher werden für die Kommunikation zwischen Client und Server im E-Mail-Verkehr sowie für die Kommunikation zwischen E-Mail-Servern nachstehende Protokolle festgelegt:

Protokoll	Titel	RFC	
SMTP	Simple Mail Transfer Protocol	[RFC 2821]	<input checked="" type="checkbox"/>
POP3	Post Office Protocol – Version 3	[RFC 1939]	<input type="checkbox"/>
IMAP	Internet Message Access Protocol Version 4 rev.1	[RFC 2060]	<input type="checkbox"/>

Tabelle 1 - Übertragungsprotokolle

Unter Einhaltung der genannten Kompatibilitätsanforderungen, kann zur Erreichung einer höheren Funktionalität die Kommunikation zwischen Server und Client auch auf Basis von proprietären Protokollen stattfinden. Der Einsatz von proprietären Protokollen (z.B. MAPI mit MS-Exchange) setzt voraus, dass diese in die Sicherheitspolicy der Behörde eingebunden werden.

#### (3.2.2) Nachrichten-Bodyparts

 B

Die Nachrichten-Bodyparts haben sich generell nach den folgenden Standards zu orientieren:

Kurzbezeichnung	Titel	RFC
Internet Message Format	Internet Message Format	[RFC 2822]
MIME	Multipurpose Internet Mail Extension	[RFC 2045] (2046-2049, 2110)
Bodyparts für Signatur und Verschlüsselung		
S/MIME V3	S/MIME Version 3 Message Specification	[RFC 2633] (2631, 2632,2634)
CMS	Cryptographic Message Syntax	[RFC 2630]

Es ist darauf zu achten, dass die eingesetzten E-Mail-Server und Clients diese Standards unterstützen.

### (3.3) E-Mailzertifikate

 B

Die Verwendung von Zertifikaten im E-Mailverkehr führt zur Hebung von Sicherheit. Zertifikate können zum Signieren und zum Verschlüsseln von E-Mails verwendet werden.

---

Beim Einsatz von Zertifikaten ist darauf zu achten, dass das Port 389 für LDAP-Kommunikation in den Firewallkonfigurationen berücksichtigt wurde.

### **(3.3.1) Elektronisch signierte E-Mails**



Die Behörde muss elektronisch signierte E-Mails empfangen können.

Die E-Mails, die von der öffentlichen Verwaltung versendet werden, sollen nach Maßgabe der technischen Möglichkeiten durch eine Signatur eindeutig gekennzeichnet sein. Diese Maßnahme soll das Vertrauen der Empfänger zum Kommunikationsmedium E-Mail stärken und gleichzeitig ein Qualitätsmerkmal darstellen. Gültig signierte E-Mails mit gefälschten Absenderadressen können einfach und sicher erkannt werden.

Zu diesem Zweck wurde eine Richtlinie für den Einsatz von E-Mail-Zertifikaten in der öffentlichen Verwaltung festgelegt, die die Zertifikatsinhalte und die Prozessabläufe (organisatorisch und technisch) im Lebenszyklus eines Zertifikates festlegt [E-Mail-Zertifikate]. Darüber hinaus wird mit den einzelnen Zertifizierungsdiensteanbietern, die E-Mail-Zertifikate für die öffentliche Verwaltung bereitstellen, eine individuelle Prozessbeschreibung definiert [E-Mail-Zertifikate A-Trust].

Diese Spezifikationen bieten den Behörden als Anwender von E-Mail-Zertifikaten eine klare und standardisierte Anleitung zu den technischen Vorgaben, zum Erhalt und zur Verwendung dieser Zertifikate und schafft darüber hinaus die nötige Transparenz, zur Stärkung des angestrebten Vertrauens zu signierten E-Mails.

Die Benutzer müssen über das Versenden und den Umgang mit elektronisch signierten E-Mails auf deren E-Mail-Clients geschult werden.

### **(3.3.2) Verschlüsselte E-Mails**



Mit zunehmender Bedeutung nehmen auch verschlüsselte E-Mails zur Sicherstellung der Vertraulichkeit in das Kommunikationsverhalten der öffentlichen Verwaltung Einzug. Es steht der Behörde frei zu entscheiden, ob verschlüsselte E-Mails als Sicherheitsrisiko eingestuft werden oder nicht. Das Interesse der Aufrechterhaltung des Betriebs steht dabei im Vordergrund.

Die Benutzer und Benutzerinnen müssen über den Einsatz und die Verwendung von verschlüsselten E-Mails geschult werden. Im Speziellen müssen den Benutzern und Benutzerinnen die Richtlinien näher gebracht werden, bis zu welchem Vertraulichkeitsanspruch Dateien per E-Mail versandt werden dürfen. Die Problematiken zu den Themen Schlüsselmanagement und Backup bzw. Archivierung sollen von der Behörde geregelt werden.

**Best Practice:****Gruppen-Verschlüsselungszertifikate**

Es besteht die Möglichkeit, aus organisatorischen Gründen, eine überschaubare, kleine zusammenhängende Gruppe von Personen (einer Organisationseinheit) mit einem Schlüsselpaar auszustatten. Die Vorteile davon sind, dass sich Backup und eine Postfachbetreuung im Falle von Abwesenheiten etc. leichter regeln lassen und dabei die Anforderungen aus Vertraulichkeit trotzdem in einem geeigneten Ausmaß sichergestellt werden können. Aus diesem Grund wird auch empfohlen für das elektronische Signieren von E-Mails und für die E-Mail-Verschlüsselung jeweils eigene Zertifikate zu verwenden<sup>3</sup>. Es ist auch darauf zu achten, dass E-Mail-Clients eine ordnungsgemäße Nutzung von nur einer Funktionalität (elektronische Signatur oder Verschlüsselung) nicht erlauben und daher beide Zertifikate bekannt sein müssen (z.B. MS-Outlook).

**Problematiken mit verschlüsselten E-Mails:**

Verschlüsselte E-Mails können – sofern keine Gruppen-Verschlüsselungszertifikate zum Einsatz kommen – von Virenschaltern und Spamfiltern nicht behandelt werden. Es kann aber davon ausgegangen werden, dass verschlüsselte E-Mails keinen Spam darstellen. Die Charakteristik von verschlüsselten E-Mails lässt auch die potentielle Virengefahr auf ein sehr geringes Restrisiko sinken. Virenschalter am Client sollen dem entgegen wirken. Durch den Einsatz von Gruppen-Verschlüsselungszertifikaten kann organisatorisch und technisch sichergestellt werden, dass prinzipiell auch hier eine Viren- und Spamprüfung erfolgen kann.

**(3.4) Standardkonformität**

Von der IKT-Stabsstelle wird ein Testmailservice angeboten, das der Kompatibilitätsfeststellung der eingesetzten Systeme nach innen und nach außen dient. Die Behörde/der Betreiber des E-Mail-Dienstes kann damit den Nachweis der geforderten Konformität erbringen. (siehe [TESTMAILSERVICE])

**(3.5) Zugangsregelungen zu E-Mail-Systemen**

Die von den Behörden betriebenen Übertragungssysteme dürfen Daten erst nach erfolgreicher Identifizierung und Authentisierung des Senders senden (vgl. dazu das jeweilig geltende Sicherheitshandbuch oder auch das Österreichische Sicherheitshandbuch [SiHB], Teil 2, SYS 8.7). Dies bedeutet, dass der Benutzer/die Benutzerin sich vor Nutzung des Services E-Mail dem Dienst gegenüber authentifizieren muss.

**(3.5.1) Standardzugang**

Von einem Standardzugang wird gesprochen, wenn davon ausgegangen werden kann, dass sich die Benutzerin/der Benutzer in einem Netzwerksegment befindet, das unter der Kontrolle der jeweiligen Behörde bzw. deren Dienstleister ist.

Es ist darauf zu achten, dass das SMTP-Service nur dem gewünschten Benutzerkreis und nicht der Allgemeinheit zur Verfügung steht. Weiters darf der Zugriff auf das E-Mail-Postfach einer Benutzerin/eines Benutzers erst nach positiv abgeschlossener Authentifizierung erfolgen. Der geforderte Sicherheitsgrad muss nach der jeweilig zugrunde liegenden Sicherheitspolicy festgelegt und realisiert werden.

<sup>3</sup> Siehe dazu auch die OECD Crypto Guidelines, „Lawful Access“ (Abgerufen aus dem World Wide Web am 15. April 2004 unter [http://www.oecd.org/document/11/0,2340,en\\_2649\\_201185\\_1814731\\_1\\_1\\_1\\_1,00.htm](http://www.oecd.org/document/11/0,2340,en_2649_201185_1814731_1_1_1_1,00.htm))

**Best Practice:**

Der derzeitige SMTP Standard zur E-Mail-Übertragung erlaubt es jedermann, eine beliebige fremde Absenderadresse zu fälschen. Mit Hilfe von SASL (Simple Authentication and Security Layer, RFC 2222) kann z.B. eine einfache Authentifizierung gegenüber dem SMTP Server erreicht werden. Eine weitere Möglichkeit wäre SMTP-after-POP einzusetzen.

**(3.5.2) Remotezugang**

Der Zugang zum E-Mail-System vom Internet ist in internen Sicherheitspolicies bzw. Remote-Access Policies der jeweiligen Behörde zu regeln. Es ist darauf zu achten, dass schreibender Zugriff vom Internet auf Echtdaten des Postfaches (E-Mails versenden und löschen) nur nach positiv erfolgter starker End-to-End-Authentifizierung gewährt wird.

**Best Practice:**

Mögliche Lösungen wären z.B. mittels eines VPNs oder einer SSL getunnelten Verbindung, wobei eine beidseitige Authentifizierung stattfinden muss und die Schlüssellänge 100 bit nicht unterschreiten darf (symmetrische Verschlüsselung).

**(3.6) Formate**

Es wird festgelegt, welche Dateiformate von jedem E-Mail-Server der öffentlichen Verwaltung angenommen werden bzw. welche prinzipiell immer abgelehnt werden sollen.

Eine Einschränkung der Formate aus Sicherheitsgründen aber auch eine Erweiterung der zulässigen Formate sind unter Beachtung der Aufstellung in der Konvention „Dokumentenformate“ [DOKFORMATE] möglich.

**Best Practice:**

Verschlüsselte E-Mails stellen bei den Formaten ein Problem dar, zumal diese kaum bzw. überhaupt nicht auf Viren überprüft werden können. Ein Ausschluss derselben ist aber nicht anzuraten. Da serverbasierte Lösungen in diesen Fällen nicht zum Ziel führen, ist auf clientbasierte Lösungen (z.B. Virens Scanner, Personal Firewalls) zurückzugreifen. Näheres siehe unter Punkt (4.1.2).

**Hinweis:**

Ausnahmen von der Filterung von Dateiformaten bzw. Dateiendungen sollten nach Möglichkeit nicht durch Umgehung (z.B. durch Komprimieren mit Passwort), sondern durch organisatorische Maßnahmen und geeigneter Infrastruktur (z.B. Dateitransferserver mit Online-Virens Scanner) gelöst werden.

**(3.6.1) Zugelassene Formate**

Die Behörde veröffentlicht in der Policy jene Dateiformate, die mindestens angenommen werden.

Eine Liste von möglichen Dateiendungen und Dateitypen ist in der Konvention „Dokumentenformate“ [DOKFORMATE] angeführt.

**(3.6.2) Unzulässige Formate**

E-Mails deren Beilagen ausführbare Programme sind, sind im Allgemeinen abzuweisen. Dabei sollen die bestmöglichen Mechanismen nach den technischen Gegebenheiten ausgeschöpft werden.

Potentiell gefährlicher Inhalt sollte geblockt werden, um bereits präventiv vom Virens Scanner unerkannte Angriffe gar nicht zuzulassen. Zu den potentiell gefährlichen Inhalten zählen z.B.

- jeglicher ausführbarer Inhalt oder

- Inhalte mit Formatverletzungen (z.B. Archive mit falschen Inhaltsangaben)

Außerdem können jene Dateien abgewiesen werden, bei denen angenommen werden kann, dass sie nicht für dienstliche Zwecke bestimmt sind (z.B. mp3, wav, ...). In der Policy kann auch festgehalten werden, dass in Ausnahmefällen (bei Verdacht oder bei Problemen) kurzfristig bestimmte Attachmentformate ebenfalls abgewiesen werden.

Eine Liste der möglichen Dateiendungen und Dateitypen ist in der Konvention „Dokumentenformate“ [DOKFORMATE] angeführt.

### **(3.6.3) Ausgehende Formate**



Zur Erreichung von Interoperabilität sollen sich Behörden der angeführten Listen in der Konvention „Dokumentenformate“ [DOKFORMATE] für ausgehende Formate orientieren.

### **(3.7) Größenbeschränkung bei E-Mails**



Es wird festgelegt, welche Dateigröße von jedem E-Mail-Server der öffentlichen Verwaltung angenommen werden muss.

Der Empfang und das Senden von E-Mails mit einer Gesamtgröße von 6 MB je Einzelmail müssen grundsätzlich gewährleistet sein. Punktuelle Einschränkungen der Größe z.B. aufgrund der Leitungsanbindung wie dies z.B. bei Auslandslokationen von Dienststellen vorkommen kann, müssen in der E-Mail-Policy offengelegt werden.

### **(3.8) Automatisch generierte Notifikationen**

Dieser Abschnitt beschreibt, wann und unter welchen Umständen bzw. an wen automatisch generierte Notifikationen versendet werden sollen.

#### **(3.8.1) Notifikation bei ungültiger Empfängeradresse**



Kann eine E-Mail aufgrund einer ungültigen Empfängeradresse nicht angenommen werden, ist der Absender darüber zu informieren. Zu diesem Zweck ist vom Server eine automatische E-Mail zu generieren, die die nicht erreichten Empfänger, den Betreff und das Sendedatum beinhaltet.

#### **Best Practice:**

Ein Beispiel für eine mögliche Notifikation wird im Anhang angeführt (Anhang (9.2)).

#### **(3.8.2) Notifikation bei Formatverletzung**



Wird eine E-Mail wegen einer Formatverletzung abgewiesen (vgl. (3.6.1) und (3.6.2)), so ist zumindest einer der Kommunikationspartner (Absender oder Empfänger) darüber zu informieren. Zu diesem Zweck kann vom Server eine automatische E-Mail generiert werden, die den Grund der Ablehnung inkl. der Details zum fehlgeschlagenen Versuch, eine Referenz zur E-Mail-Policy und mögliche Alternativen beinhaltet. Dies gilt im Speziellen auch für Organisationspostfächer.

Die Abweisung ist im Zuge des Loggings zu protokollieren.

#### **Best Practice:**

Ein Beispiel für eine mögliche Notifikation wird im Anhang angeführt (Anhang (9.3)).

#### **(3.8.3) Notifikation bei E-Mail-Übergroße**



Wird eine E-Mail wegen einer Größenlimitierung abgewiesen, so ist zumindest der Absender darüber zu informieren. Zu diesem Zweck kann vom Server eine automatische E-Mail generiert werden, die den Grund der Ablehnung inkl. der Details zum

fehlgeschlagenen Versuch, eine Referenz zur E-Mail-Policy und mögliche Alternativen beinhaltet. Dies gilt im Speziellen auch für Organisationspostfächer.

Die Abweisung ist zu protokollieren.

**Best Practice:**

Ein Beispiel für eine mögliche Notifikation wird im Anhang angeführt (Anhang (9.4)).

**(3.8.4) Notifikation Out-of-Office**

**B/O**

Diese Art von automatischer Notifikation wird nur dann gemacht, wenn der Benutzer seine Abwesenheit dem System bekannt gegeben hat. Die Benachrichtigung über dessen Abwesenheit kann

- nur im behördeninternen Bereich oder
- an jeden Absender durchgeführt werden.

In der Abwesenheitsnotiz soll lediglich eine Minimalinformation angeführt werden. Werden solche Notifikationen nicht nur im organisationsinternen Bereich versendet, kann der Inhalt mehrsprachig verfasst werden. Deutsch und Englisch sind in solchen Fällen zu bevorzugen.

Auf jene als Spam klassifizierten E-Mails darf klarerweise keine Antwort bzw. Benachrichtigung gesendet werden (vgl. Abschnitt (3.8.6)).

**Best Practice:**

Der Inhalt der Benachrichtigung sollte in Form eines Templates in der Organisation zur Verfügung gestellt werden. Es ist darauf zu achten, dass keine Information bekannt gegeben wird, die die Sicherheit der Organisation gefährden kann. So könnte z.B. die Angabe, dass ein Mitarbeiter sich für längere Zeit im Urlaub befindet, potentielle Diebe/Übeltäter über den „leichten Zugang zu dessen Arbeitsplatz“ informieren. Ein mögliches Beispiel einer Abwesenheitsnotiz findet sich im Anhang wieder (Anhang (9.5)).

**(3.8.5) Notifikation bei festgestellten Viren/Malware**

**B/O**

Hierbei unterscheidet man zwischen einer Notifikation des Absenders und des Empfängers.

- Behördenintern kann eine Notifikation an den Absender verschickt werden. Es wird davon abgeraten, Notifikationen an jene Absender zu versenden, die außerhalb des eigenen Behördenbereichs angesiedelt sind.
- Es besteht auch die Möglichkeit den Empfänger über eine virenverseuchte E-Mail zu benachrichtigen.

Die Benachrichtigung sollte einen Verweis auf die E-Mail-Policy enthalten. Die Abweisung kann in den Logfiles protokolliert werden. Näheres zu Malware siehe unter (4).

Eine E-Mail, die als Malware kategorisiert wurde, kann im Sinne des verstärkten Interesses der Aufrechterhaltung des Betriebs von der Organisation auch ohne Notifikation zurückgewiesen werden. Ein solches Verhalten muss in der E-Mail-Policy dokumentiert sein.

**(3.8.6) Notifikation bei Spam**

**B/O**

Hierbei unterscheidet man zwischen einer Notifikation des Absenders und einer des Empfängers.

- Es muss sichergestellt werden, dass keine automatisch generierten Nachrichten an Absender von Spams gesendet werden (vgl. Punkt (5)).

- Der Empfänger kann zusammenfassend in einem vordefinierten Zeitintervall eine E-Mail erhalten, womit ihm die Möglichkeit geboten wird, seine in dieser Zeit erhaltenen Spam-E-Mails selbst noch einmal zu kontrollieren.

Näheres siehe unter (5).

## (4) Malware und Viren

Malware ist die Abkürzung für „malicious software“ und bedeutet in etwa „böartige Software“. Dabei handelt es sich um Software, die der User nicht auf seinem Rechner haben möchte.

Gegen Malware bei E-Mails können Gegenmaßnahmen wie Virens Scanner am Client, am Server und im Netzwerk eingesetzt werden. Am Client und am Server können Abwehrmaßnahmen über restriktivere Einstellungen erreicht werden.

### (4.1) Möglichkeiten zum Eingriff

Der Virens Scan kann an verschiedenen Punkten der Informationsübermittlung geschehen. Danach richten sich auch die Möglichkeiten und die Art und Weise der Reaktion.

#### (4.1.1) Behandlung am SMTP Gateway und/oder am E-Mail-Proxy B

Im Idealfall kann der MTA (Mail Transfer Agent) der Organisation eine mit Malware infizierte E-Mail bereits bei der Entgegennahme erkennen. Dann besteht für den MTA die Möglichkeit diese E-Mail schon während der Übermittlung über SMTP abzulehnen.

Um Timing und Systemlastproblemen vorzubeugen, können Scanner nicht direkt am MTA die eingehenden E-Mails überprüfen; ein zwischen MTA und Client eingefügter E-Mail-Proxy kann die alleinige Aufgabe übernehmen und zuverlässig alle E-Mails während der SMTP Bearbeitung behandeln.

#### (4.1.2) Behandlung am Client O

Eine weitere Untersuchung auf Viren kann am Client selbst erfolgen, nachdem die E-Mail bereits von einem MTA entgegengenommen wurde.

Bei einer Prüfung am Client wird der Empfänger vom Scanner meist automatisch informiert.

#### (4.1.3) Aufklärung B/O

Um die weitere Verbreitung von Malware einschränken zu können, ist eine fundierte und ausgiebige Aufklärung nötig.

#### Externe Aufklärung

Wenn eine E-Mail an ein organisationsbezogenes Postfach aus Malware-Gründen geblockt wird, soll – sofern technisch möglich – in der Fehlermeldung ein Verweis auf die E-Mail-Policy erfolgen (vgl. (3.8.5)).

#### Best Practice:

Aufgrund der Tatsache, dass Viren die Absenderadressen fälschen, ist eine Verständigung des Absenders wohl nur behördenintern vorzusehen. Dies gilt dann, wenn die E-Mail direkt vom behördeneigenen E-Mail-Server entgegen genommen wurde.

#### Interne Aufklärung

Es ist darauf zu achten, dass die Benutzer über die Gefahren aufgeklärt werden bzw. sich informieren können. Unter anderem gilt dies für Hoax E-Mails (Hoax: engl. Jux,

Schabernack), die an sich keine Gefahr darstellen. Auswirkungen entstehen jedoch dann, wenn die Benutzer den Anweisungen in bester Absicht Folge leisten.

## **(4.2) Maßnahmen bei positiver Virenprüfung**

Bei positiver Prüfung auf Virenbefall, ist einer der folgenden Maßnahmen einzuleiten bzw. in Erwägung zu ziehen.

### **(4.2.1) Quarantäne**

Geblockte E-Mails können in einem Quarantäneverzeichnis gespeichert werden. Die folgenden Punkte sollten dabei festgelegt werden:

- wie lange die E-Mail in diesem Container aufgehoben wird
- wie die Aufklärung der internen Anwender über die eingelangte E-Mail erfolgt

#### **Best Practice:**

In der Praxis werden E-Mails in Quarantäne sehr oft nach einer Woche Zwischenspeicherung gelöscht.

### **(4.2.2) Weiterleitung von gesäuberter E-Mail**

Kann der Inhalt der E-Mail von Viren und Malware befreit werden, soll diese mit einem entsprechenden Vermerk an den Empfänger weitergeleitet werden.

In diesem Text soll vermerkt sein, dass durch die Säuberung Dateninhalte verändert worden oder verloren gegangen sind bzw. sein könnten.

Der Empfänger entscheidet, ob der Absender kontaktiert werden muss, um die Korrektheit des Inhalts sicherzustellen.

### **(4.2.3) Löschung**

Die Behörde kann virenbehaftete E-Mails ohne Notifikation des Absenders bzw. Empfängers löschen. In Anbetracht des Punktes (3.1.4) sei an dieser Stelle aber nochmals auf eine ordnungsgemäße Benachrichtigung des Absenders hingewiesen, die bei einer negativen Virenprüfung erfolgen muss.

## **(5) Spam**

Unerwünscht, massenweise verschickte E-Mail-Nachrichten werden mit Spam bezeichnet. Um diesen entgegen zu wirken bedarf es so genannter Spam-Filter, die sich sowohl auf Server- als auch auf Clientseite befinden können.

#### **Best Practice:**

Im RFC 2505 findet sich eine Liste von Empfehlungen für SMTP MTAs wieder, die wirkungsvolle Schutzmaßnahmen gegen Spam aufzählt und beschreibt. Darin sind sowohl aktive als auch passive Abwehrmaßnahmen angeführt. Als Querreferenz wird hier im Zusammenhang mit DNS der RFC 1912 (u.a. Abschnitt 2.1) mit angegeben.

### **(5.1) Aktive Abwehrmaßnahmen**

Spam-Filter ermöglichen die Analyse einer E-Mail (Header und Body) nach unterschiedlichen Kriterien und geben eine Einschätzung über die Wahrscheinlichkeit ab, ob die untersuchte Nachricht Spam enthält oder nicht.

Da Spam-Versender in der Regel Ihre E-Mails nicht als UBE ("Unsolicited Broadcast Email") kennzeichnen, existieren zur Analyse eingehender Nachrichten keine objektiven Kriterien. Aktuelle Spam-Filter arbeiten daher mit verschiedenen Bewertungsverfahren,

um Spam hinreichend genau zu erkennen. Das Auftreten mehrerer Merkmale erhöht dabei die Wahrscheinlichkeit; das Überschreiten eines Schwellenwertes indiziert eine positive Erkennung.

Wird eine E-Mail als Spam klassifiziert, kann die Nachricht auch in Quarantäne gestellt werden. Die folgenden Punkte sollten dabei festgelegt werden:

- wie lange die E-Mail in diesem Container aufgehoben wird
- wie bzw. ob der Empfänger Zugriff zu den eingelangten E-Mails erhält

Alternativ sind Markierungen möglich (im Betreff z.B. durch Voranstellen von "[SPAM?]" oder in eigenen Header-Feldern, z.B. "X-Spam-Status: Yes"), um dem Empfänger eine Filterung zu ermöglichen.

Da Spam-Filter keine 100%-ige Genauigkeit bei der Erkennung bieten können, ist der Markierungsansatz vorzuziehen.

**Best Practice:****E-Mail-Formate (Plain-Text oder HTML)**

Bei HTML-Mails werden eingebettete Bilder von einem Web-Server heruntergeladen. Dabei kann die E-Mail-Adresse des Empfängers mitübermittelt werden. Aus diesem Grund ist das Versenden von Plain-Text Nachrichten vorzuziehen.

**Digitale Signaturen (S/MIME)**

Digitale Signaturen erlauben dem Absender das Unterschreiben einer E-Mail und damit dem Empfänger das Überprüfen dessen Identität. Bei der Verwendung von Digitalen Signaturen zur Bekämpfung von Spam werden nur E-Mails zugestellt, die signiert sind. Spam-Versender würden durch eine Signatur ihre Anonymität einbüßen.

**Formatierung von E-Mail-Adressen auf Internetseiten**

Spammer sammeln E-Mail-Adressen mit sogenannten Erntemaschinen, die sich frei im Internet bewegen, und auf Internetseiten, die dort befindlichen E-Mail-Adressen ablesen. Durch Formatieren bzw. durch Ersetzen einiger Zeichen der E-Mail-Adresse durch deren numerischen Werte kann dies erschwert werden. Eine beispielhafte E-Mail-Adresse könnte wie folgt aussehen: *max&#46;mustermann&#64;bka&#46;gv&#46;at*

**Betreffzeilen ausfüllen**

Eine aussagekräftige Betreffzeile ist nicht nur beim Einordnen der Relevanz der E-Mail hilfreich, sondern auch beim sofortigen bzw. automatischen Erkennen von Spam.

**Aufklärung**

Wie bei dem oberen Kapitel über Malware, müssen die Endanwender über den Sinn der hier beschriebenen Maßnahmen informiert sein.

**Mailing- bzw. Empfängerlisten**

Es wird empfohlen große Empfängerlisten über Mailinglisten abzuwickeln. Wird eine größere Anzahl von Empfängern trotzdem einzeln angeführt, so soll diese im BCC (Blind carbon copy) Feld eingetragen werden.

**Serverseitige Lösung – Reverse Lookup**

Es hat sich gezeigt, dass ein Reverse Lookup vom empfangenen E-Mail-Server durchaus zur Vermeidung von Spams beiträgt. Da davon ausgegangen werden kann, dass E-Mail-Server langfristige Installationen sind und daher auch in DNS-Servern eingetragen werden, ist eine Reverse Lookup Prüfung unter Einbeziehung einer geringen Lasterhöhung durchaus zu empfehlen (vgl. dazu RFC 1912 und RFC 2505).

**Nicht auflösbare Absender-Adressen**

Solche Adressen sollten standardmäßig abgewiesen werden, d. h. der Domainteil einer E-Mail-Adresse kann mit keinem E-Mailserver assoziiert werden bzw. ist kein Hostname (Überprüfung via DNS). Je nach Grund wird entweder ein temporärer Fehler (vorübergehenden Nameserverausfall) oder ein permanenter Fehler (bei einer negativen Antwort eines Nameservers) retourniert.

### Verhindern von gefälschten Absenderadressen

Über Einträge im DNS veröffentlicht eine Organisation zugleich die IP-Adressen der ausgehenden E-Mailserver. Jeder Empfänger kann beim Empfang einer E-Mail feststellen, ob die absendende IP-Adresse dazu legitimiert ist oder nicht und gegebenenfalls die Annahme der E-Mail verweigern. Unfälschbare Absenderadressen verhindern zwar keine Spammessages, jedoch können über einfache Blacklisten unerwünschte Domänen einfach blockiert werden. Mögliche Realisierungen können z.B. SPF<sup>4</sup> (Sender Policy Framework), CallerID bzw. Sender ID Framework<sup>5</sup>, RMX<sup>6</sup> (Reverse MX) oder DMP<sup>7</sup> (Designated Mailer Protocol) sein.

### Blackhole Listen

Aufgrund von sogenannten dynamischen Realtime Blackhole Lists (kurz als RBL bezeichnet), die aktuelle Listen von Spammer-Systemen führen, wird es möglich, E-Mails von bekannten „böswilligen“ Hosts bereits vor der Annahme abzulehnen.

## (5.2) Passive Abwehrmaßnahmen

Nicht oder ungenügend abgesicherte SMTP-Server werden als „Open Relay“ bezeichnet. Sie ermöglichen jedermann den Versand von (auch anonymen) E-Mails.

### (5.2.1) Schließung offener Relays



Kein SMTP-Server darf ein „Open Relay“ darstellen. Korrekt konfigurierte SMTP-Server akzeptieren E-Mails nur, wenn Ihnen entweder der Empfänger einer E-Mail (um sie in dessen Postfach auszuliefern) oder deren Absender bekannt sind. Da das SMTP-Protokoll per se keine Authentisierung kennt und die Absender-Angabe leicht gefälscht werden kann, erfordert die korrekte Konfiguration einen oder mehrere Mechanismen zur Sicherstellung einer legitimen Nutzung zum E-Mail-Versand. Während IP-basierte ACL-Lösungen (auch SMTP-after-POP) keinen Schutz gegen die Fälschung von IP-Adressen bieten, ist SMTP-auth ein brauchbares Verfahren zur Absicherung von SMTP-Servern gegen Missbrauch. Verständlicherweise schützt keines dieser Verfahren vor Spam, der direkt an den zuständigen SMTP-Server der Empfänger-Adresse versendet wird ("Direct-to-MX").

### (5.2.2) Blockierung offener Relays



Durch Einsatz von verbreiteten Listen mit IP-Adressen potentieller Spammer (DNSBL, "DNS-delivered Blocking/Blackhole List") wird Spam schon frühzeitig am SMTP-Port unterbunden.

Statt E-Mails generell entgegenzunehmen und durch Content-Filter zu analysieren, werden bereits die SMTP-Verbindungen von potentiellen Spammern blockiert.

## (6) Verfügbarkeit und Performance



Generell ist zu beachten, dass bei der Nutzung von Internetdiensten bezüglich deren Verfügbarkeit keine verbindliche Aussage getroffen werden kann. Der Transport von E-Mails ist von einer Summe von Netzwerkdiensten abhängig, deren Funktionalitäten üblicherweise nicht durch den Sender oder Empfänger beeinflussbar sind. Es existiert

<sup>4</sup> Siehe <http://spf.pobox.com/>

<sup>5</sup> [http://www.microsoft.com/mscorp/twc/privacy/spam\\_senderid.msp](http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.msp)

<sup>6</sup> <http://www.danisch.de/work/security/antispam.html>

<sup>7</sup> <http://www.pan-am.ca/dmp/draft-fecyk-dmp-01.txt>

deshalb keine Garantie, dass gesendete E-Mails tatsächlich den Posteingangsserver des Empfängers erreichen. Eine Aussage über die Transportdauer kann ebenso wenig getroffen werden. Es kann jedoch davon ausgegangen werden, dass die von der öffentlichen Verwaltung betriebenen Posteingangsserver-Systeme im Regelfall 24 Stunden am Tag zur Verfügung stehen und damit zum Empfangen und Versenden von E-Mails bereit sind.

## **(7) Maßnahmen zur Aufbewahrung von E-Mail**

### **(7.1) Mailarchivierung vs. Backup**

Um einen kontinuierlichen historischen Überblick über die E-Mail-Korrespondenz zu erhalten sind zweierlei Maßnahmen vorzusehen. Diese unterscheiden sich grundlegend in der, für eine qualitätsvolle Wiederherstellung der E-Mail, benötigten Zeit und in dem Ort der Sicherung.

#### **(7.1.1) Mailarchivierung**

**B/O**

Die Archivierung von E-Mails wird seitens eines E-Mail-Services nicht immer zentral zur Verfügung gestellt. Die Sicherung und Archivierung obliegt in diesen Fällen der Verantwortung des Benutzers/der Benutzerin selbst. Es ist dafür zu sorgen, dass der Benutzer entsprechend geschult wird.

Auf die Sicherung des privaten Schlüssels für verschlüsselte E-Mails ist Rücksicht zu nehmen.

#### **(7.1.2) Backup**

**B/O**

Die Sicherung der Daten des E-Mail-Systems ist als Bestandteil einer IT-Sicherheitspolicy zu sehen, die für das EDV-System von der Behörde selbst definiert wurde. In diesem Rahmen sind auch die Backup- und Restoreverfahren des E-Mail-Systems festzulegen. Auf die Sicherung des privaten Schlüssels für verschlüsselte E-Mails ist Rücksicht zu nehmen.

### **(7.2) Protokollierung und Logging**

Grundsätzlich dürfen unter Einhaltung der Datenschutzerfordernungen nur jene Daten protokolliert werden, die für die Sicherung der Funktionsweise des Systems und für die Einhaltung der organisatorischen und gesetzlichen Vorgaben benötigt werden. Liegt ein begründeter Verdacht auf rechtswidriges oder zum Normalverhalten abweichendes Verhalten vor, so können zu diesem Zweck in Abstimmung mit der Personalvertretung nach Klärung bzw. nach Rückfragen weitere entsprechende Maßnahmen gesetzt werden. Die Aufbewahrung von Protokolldateien ist so lange sicherzustellen, dass die organisatorischen und gesetzlichen Vorgaben für die Nachvollziehbarkeit von Problemfällen gewährleistet werden kann (vgl. §14 [DSG2000]).

### **(7.3) Ausbildung der Endanwender**

Basiselemente für die Ausbildung/Belehrung:

- Wissen über das E-Mail-System
  - Voraussetzungen über Zugriffsmöglichkeiten  
Die Endanwender müssen über die verschiedenen Formen des Zugangs informiert sein.
  - Abteilungspostfächer und die Vertretung derselben  
Die Bearbeitung der E-Mail, die an organisationsbezogene Postfächer übermittelt wird, muss geregelt sein. Es müssen Vertretungen (im Urlaubs- bzw. im Krankheitsfall) einsehbar vorgegeben sein. Die Prozesse, die zu

- einer Archivierung der organisationsbezogenen Postfächer führen, müssen bekannt sein.
  - Nutzung
    - Die Endanwender müssen über die Nutzungsvorschriften Bescheid wissen.
  - Archivierung
    - Die Endanwender müssen über die Prozesse, die zu einer effizienten E-Mail-Aufbewahrung führen, informiert sein.
- Wissen über die Sicherheitsmechanismen
  - Die Endanwender müssen sich ein Wissen über die Problematik der E-Mail-Sicherung aneignen können.
- Kenntnisnahme der Policy

#### **Best Practice:**

Ein E-Learning Konzept für die Basisdefinitionen der E-Mail-Policies, das um behördeninterne Ergänzungen für den internen Betrieb erweitert werden kann, soll als Bestandteil der Policy beigestellt werden. Dieses E-Learning Konzept soll im Rahmen der Einrichtung von E-Mail-Zugängen eingesetzt werden. Für die bereits aktiven Benutzer sind Vorkehrungen zu treffen, die den Erwerb dieses Wissens sicherstellen.

## **(8) Offenlegung der Policy**

Die E-Mail-Policy muss lt. Domain-Policy **Fehler! Verweisquelle konnte nicht gefunden werden.** veröffentlicht werden. Dabei müssen zumindest folgende Inhalte zu finden sein (vgl. E-Commerce-Gesetz [ECG]):

- Eigentümer – wer ist Betreiber des Servers (Impressum)
- Richtlinien für eingehenden E-Mail-Verkehr (Abfrageverhalten, Verhalten bei Anbringen, Reaktionsverhalten bei Malware bzw. Spamverdacht, Informationen zu Organisationsverantwortlichen, Formatsliste über annehmbare und ablehnbare Dokumentenformate, etwaige automatische Notifikationen, etc.)
- Richtlinien für ausgehenden E-Mail-Verkehr (welche Formate werden versendet, Informationen zu elektronischen Signaturen und ggf. Amtssignaturen, etwaige Notifikationen, etc.)
- Richtlinien für die Verwendung von digitalen Zertifikaten zu Signatur- und Verschlüsselungszwecken, ggf. Verweis auf weitere Policies (Adressen der CRL, Ausgabeprozedur, verwendete Zertifikatstypen, Bereitstellung der Zertifikate bzw. öffentlichen Schlüssel, etc.)
- Adress-Policy für Personen und Organisationen mit allfälligem Verweis auf ein Verzeichnis zur Zuordnung von Materien oder Personen zu Organisationspostfächern

## (9) Anhang

### (9.1) Beispielhafte E-Mail-Signatur

In diesem Beispiel gibt es sowohl eine eigene Besucher- als auch Postadresse (Besucher und Post). Fällt diese unter eine Adresse zusammen, dann wäre nur Adresse voranzustellen. Die E-Mail-Adresse wird mit angegeben, damit diese auch auf Ausdrucken und bei weitergeleiteten E-Mails immer vorhanden ist. Im Falle eines internationalen E-Mail-Verkehrs sollten englische Bezeichner (Textkonstanten, Organisationsbezeichner) verwendet werden.

```
--  
Max Mustermann [max.mustermann@organisation.gv.at]  
Sektionsleitung  
Sektion XY / Organisation  
Besucher: Musterstrasse 2, 1010 Wien  
Post: Musterstrasse 3, 1020 Wien  
Tel: +43 1 9999 11  
Fax: +43 1 9999 99  
Web: http://www.organisation.gv.at/
```

### (9.2) Beispielhafte Notifikation bei ungültiger Empfängeradresse

Wird eine E-Mail an eine ungültige Empfängeradresse adressiert, so ist eine Fehlermeldung an den Absender zu senden.

```
Das ist eine automatisch generierte E-Mail über den Status Ihrer  
versendeten Nachricht. Die E-Mail  
  
An: <Empfänger-E-Mail-Adressen gesamt>  
Betreff: <Betreff der versendeten E-Mail>  
Gesendet: <Datum der versendeten E-Mail>  
  
konnte folgenden Empfängern nicht zugestellt werden:  
<Empfänger-E-Mail-Adressen>  
  
-----  
  
This is an automatically generated Delivery Status  
Notification. Your message  
  
To: <Empfänger-E-Mail-Adressen gesamt>  
Subject: <Betreff der versendeten E-Mail>  
Sent: <Datum der versendeten E-Mail>  
  
did not reach the following recipient(s):  
<Empfänger-E-Mail-Adressen>
```

### (9.3) Beispielhafte Notifikation bei Formatverletzung

Ist einem E-Mail eine Datei beigefügt, die eine Formatverletzung zur Folge hat, kann diese gelöscht, durch eine Datei "deleted.txt" mit folgendem Inhalt ersetzt und an den E-Mail-Empfänger zugestellt werden. Die hier beispielhaft angegebenen Verweise sollen den Vorgaben der **Fehler! Verweisquelle konnte nicht gefunden werden.** entsprechen.

Attachment: \${FILE}

Eine dieser E-Mail beigefügte Datei wurde gelöscht, da sie eine Formatverletzung verursachte. Sollten Sie diese Datei benötigen, informieren Sie bitte die Absenderin/den Absender der E-Mail und ersuchen um eine neuerliche Übermittlung in einem gültigen Dateiformat. Nähere Informationen zu den gültigen und verbotenen Dateiformaten finden Sie unter

<http://www.organisation.gv.at/policies/formate.html?lang=de>

-----

The file attached to this email was removed because of a format violation. If you need the file, please contact the sender and ask for resending it in a valid format. For more information on allowed and forbidden documentformats see

<http://www.organisation.gv.at/policies/formate.html?lang=en>

### (9.4) Beispielhafte Notifikation bei E-Mail-Übergröße

Bei Übergröße der E-Mail durch zu große Beilagen kann diese geblockt werden. Der Absender kann eine Notifikation erhalten. Geht aus der Antwort eindeutig hervor, wer der ursprüngliche Empfänger der Nachricht hätte sein sollen, so kann die im Beispiel angeführte E-Mail-Adresse weggelassen und der Text dementsprechend angepasst werden. Die hier beispielhaft angegebenen Verweise sollen den Vorgaben der **Fehler! Verweisquelle konnte nicht gefunden werden.** entsprechen.

Die von Ihnen versendete E-Mail überschritt die erlaubte Größe und konnte nicht entgegen genommen werden:

<Empfänger-E-Mail-Adressen>

Nähere Informationen finden Sie unter

<http://www.organisation.gv.at/policies/email.html?lang=de>

-----

The mail you sent exceeded the mail size limit allowed and did not reach the following recipient(s):

<Empfänger-E-Mail-Adressen>

For further information see

<http://www.organisation.gv.at/policies/email.html?lang=de>

### (9.5) Beispielhafte Notifikation bei Out-of-Office

Ich bin in der Zeit vom DD. MMM YYYY bis einschließlich DD. MMM YYYY nicht erreichbar. In dringenden Fällen wenden Sie sich in dieser Zeit bitte an das Sekretariat (Hr./Fr. Max Mustermann, [max.mustermann@organisation.gv.at](mailto:max.mustermann@organisation.gv.at), Tel. +43 1 9999 22).

-----

I am not available during the time period starting on DD. MMM YYYY until DD. MMM YYY. In urgent matters please contact the secretary (Mr./Mrs. Max Mustermann, [max.mustermann@organisation.gv.at](mailto:max.mustermann@organisation.gv.at), tel. +43 1 9999 22).

## (10) Referenzen

### [DOKFORMATE]

Michael Liehmann, Bernd Martin, Robert Wollendorfer: Dokumentenformate. Konvention / Empfehlung, Version 1.0.2. Abgerufen aus dem World Wide Web am 31.05.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

### [DOMAINPOL]

Michael Liehmann, Bernd Martin: Domain-Policy. Konvention, Version 1.0.0. Abgerufen aus dem World Wide Web am 31.09.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

### [DOMAINREG]

Helmut Hummer, Bernd Martin, Gerhard Schwarz: Internetdomänenverwaltung gv.at Naming- und Domänenregistrierungs-Policy. Konvention / Empfehlung, Version 1.0.0. Abgerufen aus dem World Wide Web am 31.09.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

### [DSG2000]

Bundesgesetz über den Schutz personenbezogener Daten. (Datenschutzgesetz 2000 - DSG 2000). BGBl. I Nr. 165/1999. Ausgegeben am 17. August 1999. Abgerufen aus dem World Wide Web am 03.01.2005 unter <http://www.ris.bka.gv.at/taweb-cgi/taweb?x=d&o=r&v=bgbldf&d=BGBLPDF&i=593&p=1>

### [ECG]

152. Bundesgesetz - Jahrgang 2001: E-Commerce-Gesetz. Regelung bestimmter rechtlicher Aspekte des elektronischen Geschäfts- und Rechtsverkehrs (E-Commerce-Gesetz - ECG) und Änderung des Signaturgesetzes sowie der Zivilprozessordnung (NR: GP XXI RV 817 AB 853 S. 83. BR: AB 6499 S. 682.) [CELEX-Nr.: 300L0031]

### [E-Mail-Zertifikate]

Karlinger Gregor, Posch Reinhard: Richtlinien für E-Mail-Zertifikate in der Verwaltung. Konvention - Öffentlicher Entwurf. Version 1.0.1 vom 20. 01. 2003. Abgerufen aus dem World Wide Web am 2.1.2004 unter <http://www.cio.gv.at/it-infrastructure/emailservices/emailcertificates/Emailzertifikate.AllgemeineRichtlinien.1-0-1.pdf>

### [E-Mail-Zertifikate A-Trust]

Karlinger Gregor: Richtlinien für E-Mail-Zertifikate in der Verwaltung. Erläuterung - Öffentlicher Entwurf. Version 1.0.1 vom 20. 01. 2003. Abgerufen aus dem World Wide Web am 2.1.2004 unter <http://www.cio.gv.at/it-infrastructure/emailservices/emailcertificates/Emailzertifikate.ProzessablaeuferTrust.1-0-1.pdf>

### [INTPOL]

Bernd Martin, Robert Wollendorfer: Internet-Policy. Konvention / Empfehlung, Version 1.0.2. Abgerufen aus dem World Wide Web am 31.05.2005 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

**[MAILPOL]**

Mariel, Johannes: e-Mail-Policy. Empfehlung einer Policy, die der Sicherstellung der Interoperabilität der von den Bundesbehörden verwendeten E-Mailsysteme unter dem Aspekt der gesicherten Übertragung der Nachrichten dienen soll. Öffentlicher Entwurf, Version V1.0.0 29.08.03. Abgerufen aus dem World Wide Web am 10.12.03 unter <http://www.cio.gv.at/it-infrastructure/emailservices/mailpolicies/MailpolicyV100.pdf>

**[SecClass]**

Hörbe Rainer: Spezifikation Sicherheitsklassen im Portalverbund-System, SecClass 1.1.0/1.12.03, Empfehlung. Abgerufen aus dem World Wide Web am 18.02.2004 unter <http://reference.e-government.gv.at/Sicherheitsklassen.329.0.html>

**[SiHB]**

Chief Information Office, IKT-Stabsstelle, Österreichisches IT-Sicherheitshandbuch Teil 1: IT-Sicherheitsmanagement Version 2.2 November 2004 und Teil 2: IT-Sicherheitsmaßnahmen Version 2.2 November 2004. Abgerufen aus dem World Wide Web am 15. Dezember 2004 unter <http://www.cio.gv.at/securenetworks/sihb/>

**[T.04]**

Empfehlungen – Homogenisierung der symbolischen Adressen für X.400 und SMTP-Mail, Final Draft, 1994-11-10

**[T.06]**

Naming Policy „gv.at“ (Richtlinien zur Domänenverwaltung in den obersten Bundesbehörden) - Version 3.1 - 1998-07-24. Abgerufen aus dem World Wide Web am 20.04.2004 unter [http://www.cio.gv.at/ikt-board/beratungen/domain\\_gv/recommendation/1998\\_07\\_24\\_naming-policy.gv\\_V-3.1.pdf](http://www.cio.gv.at/ikt-board/beratungen/domain_gv/recommendation/1998_07_24_naming-policy.gv_V-3.1.pdf)

**[TESTMAILSERVICE]**

Abgerufen aus dem World Wide Web am 20.04.2004 unter <http://www.cio.gv.at/applications/mailtest/sit.at/mailkompat/servlet/MailServlet> bzw. <http://demo.a-sit.at/mailkompat/servlet/MailServlet>

**[TRANSPOL]**

Arbeitsgruppe Internetpolicy: Transport-Policy. Konvention zum E-Government Austria erarbeitet von Chief Information Office, Stabsstelle IKT-Strategie des Bundes. Öffentlicher Entwurf, Version 1.0.0, 29.06.2004. Abgerufen aus dem World Wide Web am 29.06.2004 unter <http://www.cio.gv.at/it-infrastructure/intpol/>

**Liste von RFCs**

RFC 1912	-	Common DNS Operational and Configuration Errors
RFC 1939	-	Post Office Protocol - Version 3
RFC 2045	-	Multipurpose Internet Mail Extensions (MIME)
RFC 2060	-	Internet Message Access Protocol - Version 4rev1
RFC 2222	-	Sender Policy Framework (SPF), A Convention to Describe Hosts Authorized to Send SMTP Traffic

- RFC 2251 - Lightweight Directory Access Protocol (v3)
- RFC 2315 - PKCS #7: Cryptographic Message Syntax Version 1.5
- RFC 2505 - Anti-Spam Recommendations for SMTP MTAs
- RFC 2630 - Cryptographic Message Syntax
- RFC 2633 - S/MIME Version 3 Message Specification
- RFC 2821 - Simple Mail Transfer Protocol
- RFC 2822 - Internet Message Format
- RFC 3275 - (Extensible Markup Language) XML-Signature Syntax and Processing

## Historie

Version 2.0.0	Datum 15.04.2004	Kommentar  Initialversion erstellt.
Ersteller Bernd Martin Michael Liehmann		
Version 2.0.1	Datum 30.09.2004	Kommentar <ul style="list-style-type: none"> <li>• Punkt (3.1.2): Erweiterung des Basisformats 1 um folgende Konvention &lt;Organisationsname&gt;.post@&lt;Domainname&gt;</li> <li>• Punkt (3.3): Ergänzung um den Hinweis, dass das Port 389 für die LDAP-Kommunikation offen sein muss.</li> <li>• Punkt (3.8.5): Klarstellung mit Hinweis, dass behördenfremde Absender keine Notifikation erhalten sollen.</li> <li>• Punkt (4.2.2) ist nur mehr optional und nicht mehr eine Basisanforderung.</li> <li>• Punkt (4.2.3) wurde neu aufgenommen.</li> <li>• Punkt (5): Aufnahme der Best Practice.</li> <li>• Punkt (5.1): Aufnahme/Aufgliederung der Best Practice Serverseitige Lösung – Reverse Lookup bzw. Nicht auflösbare Absender-Adressen, Verhindern von gefälschten Absenderadressen und Blackhole Listen.</li> <li>• Punkt (5.2.2): Editorieller Fehler - Löschung der Best Practice, weil schon in (5.1) enthalten.</li> <li>• Punkt (7.2): Aufnahme des Verweises auf DSGVO §14</li> </ul>
Ersteller Bernd Martin		
Version 2.0.2	Datum 18.02.2005	Kommentar <ul style="list-style-type: none"> <li>• Punkt (3.1.2): Es wird die Möglichkeit geboten, Organisationsadressen auch ohne dem Schlüsselwort „post“ zu definieren, wenn die entsprechenden organisatorischen Maßnahmen gesetzt sind.</li> <li>• Punkt (3.1.4): Es wird die Möglichkeit geboten, auch eine andere, jedoch qualitativ gleichwertige Entgegennahme zu realisieren.</li> <li>• Punkt (3.8.1): Die Notifikation bei einer ungültigen Empfängeradresse wird hinzugefügt.</li> <li>• Punkt (3.8.2): Die Verständigung bei einer Formatverletzung kann nunmehr an den Absender oder Empfänger gesendet werden.</li> <li>• Punkt (4.2.1): Best Practice wurde mit aufgenommen</li> <li>• Punkt (7.2): Ergänzung und Klarstellung mit „...und für die Einhaltung der organisatorischen und gesetzlichen Vorgaben</li> </ul>
Ersteller Bernd Martin		

		<p>benötig ...“</p> <ul style="list-style-type: none"> <li>• Punkt (9.1): Ein Beispiel für eine Notifikation bei einer ungültigen Empfängeradresse wird angefügt.</li> </ul>
Version	Datum	Kommentar
2.0.3	25.09.2005	
Ersteller Bernd Martin		<ul style="list-style-type: none"> <li>• Korrekturen von Tippfehlern</li> <li>• Punkt (2) und (3.5): Klarstellung, dass nur das jeweils geltende Sicherheitshandbuch anzuwenden sei.</li> <li>• Punkt (3.1.4): Vorgehensweise bei der Adressierung an persönliche Postfächer wurde auf die jeweils geltende Kanzleiordnung geändert und die die Weiterleitung an die offizielle Einlaufadresse als Best-Practice Möglichkeit aufgenommen.</li> </ul>