# Kurzgutachten zur Zertifizierung des Verfahrens „Verschlüsselungsautomat S/MIME“

# nach DSGSVO Schleswig-Holstein

# (Datenschutz-Prüfsiegel)

**Version: 1.7**

Stand: 31.05.2016

Status: Freigegeben

Verantwortlich: Mission 100 e.V.

# Inhaltsverzeichnis

**Verzeichnis der Abbildungen**

# 1 Einleitung

## 1.1 Zweck der Begutachtung

Die Begutachtung von Produkten im Datenschutzumfeld ist in einigen Datenschutzgesetzen (u.a. Bundesdatenschutzgesetz / BDSG, Landesdatenschutzgesetz Bremen) zwar aufgenommen worden, eine komplette Konkretisierung in Gestalt von Verordnungen oder Durchführungsgesetzen ist neben Schleswig-Holstein bislang aber erst in wenigen Bundesländern erfolgt.

Rechtsgrundlage der Gütesiegelvergabe in Schleswig-Holstein ist § 4 Absatz 2 des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG-SH), der von öffentlichen Stellen des Landes Schleswig-Holstein fordert, dass vorrangig solche Produkte zum Einsatz kommen sollen, die mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar sind.

Mit Satz 2 des § 4 Abs. 2 ist die Voraussetzung zum Erlass einer Landesverordnung geschaffen worden. Mit der Landesverordnung über ein Datenschutzgütesiegel (DSGSVO) wurde hiervon Gebrauch gemacht. Die DSGSVO regelt die Einzelheiten und Anforderungen an die Vergabe von Datenschutz-Gütesiegeln. Diese Regelungen sind die Grundlage dieses Gutachtens.

Aufgrund der Vergleichbarkeit der landes- und bundesgesetzlichen Regelungen lassen sich die zur Erlangung des Datenschutz-Gütesiegels erforderlichen Eckwerte auch auf andere Bereiche übertragen, so auch auf den im BDSG geregelten nicht-öffentlichen Bereich.

Gleichwohl muss das zu zertifizierende Produkt auch und gerade wegen der landesgesetzlichen Regelung insbesondere im öffentlichen Bereich, potentiell zur Nutzung durch öffentliche Stelle geeignet sein. In diesem Sinne reicht für eine Produkteignung aus, dass eine öffentliche Stelle das auditierte Verfahren selbst nutzen könnte.

Entsprechend § 1 Abs. 2 der DSGSVO sind IT-Produkte im Sinne der Verordnung Hardware, Software und automatisierte Verfahren, die zur Nutzung durch öffentliche Stellen geeignet sind.

Mit dem zur Begutachtung vorliegenden Produkt „Verschlüsselungsautomat S/MIME“ können Kunden der Port Sol 19 (überwiegend Sozialversicherer), durch eine Ende-zu-Ende Verschlüsselung das Verfahren De-Mail auch für im Umfeld vom Berufsgeheimnisträgerschaften anfallende Sozialdaten nutzen.

Im vorliegenden Gutachten wird geprüft, inwieweit das Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit gerecht wird.

## 1.2 Gegenstand der Begutachtung

### 1.2.1 Kurzbeschreibung

Vorbemerkung: Eine detaillierte Beschreibung des Produkts ist im Anhang 2 zu finden.

Gegenstand der Begutachtung ist das Produkt „Verschlüsselungsautomat S/MIME“ (nachfolgend kurz „Verschlüsselungsautomat“) der Port Sol 19 GmbH in der Version 1.0. Hierbei handelt es sich um ein AddOn für ein E-Mail-System auf der Basis von De-Mail. De-Mail ist die Umsetzung des De-Mail-Gesetzes durch einen zertifizierten Provider. De-Mail schafft die Voraussetzung für einen sicheren Versand mit Informationen in öffentlichen Netzen, insbesondere durch eine eindeutige Authentisierung von Sender und Empfänger einer Nachricht und eine Protokollierung, die Kommunikationsvorgänge beweissicher nachvollziehbar macht. De-Mail ist jedoch von Hause aus nicht geeignet für den Versand besonderer personenbezogenen Daten wie Sozialdaten. Der BfDI schreibt für den Versand von Sozialdaten ausdrücklich eine Ende-zu-Ende-Verschlüsselung vor. Das De-Mail Gesetz tut das nicht. Eine Ende-zu-Ende-Verschlüsselung ist folglich in der Implementierung durch die Provider im Regelfall auch nicht vorhanden.

Der Verschlüsselungsautomat schließt diese Lücke. Für den Fall, dass im öffentlichen Zertifikatsspeicher des De-Mail-Providers ein S/MIME-Schlüssel des Adressaten der E-Mail verfügbar ist, wird dieser Schlüssel beschafft, mit seiner Hilfe die E-Mail inklusive aller Anlagen verschlüsselt und anschließend zum Versand an das De-Mail-System übergeben. Gibt es einen solchen Schlüssel nicht, unterbleibt der Versand. Dies alles erfolgt automatisch, d.h. der Absender hat keine Möglichkeit, eine unverschlüsselte Nachricht zu versenden. Auf Empfängerseite erscheint die Nachricht als gewöhnliche S/MIME-verschlüsselte Mail. Weil der Verschlüsselungsautomat das öffentliche Schlüsselverzeichnis eines zertifizierten De-Mail-Providers nutzt, ist eine sichere Authentisierung des verwendeten Schlüsselmaterials gewährleistet.

Der Verschlüsselungsautomat ist als Web Service implementiert und in erster Linie für den Einsatz in einer Programm-zu-Programm-Kommunikation entwickelt worden, in der E-Mails automatisiert von anderen Applikationen erzeugt werden, kann aber auch so eingesetzt werden, dass er E-Mails schützt, die mittels eines Mail-Clients manuell generiert werden.

Nicht Teil des Produkts und damit nicht Gegenstand der Begutachtung ist die Entschlüsselung von Nachrichten, da diese mit Standardmitteln des Systems des Empfängers der Mail erfolgt, bei menschlichen Empfängern z.B. mittels des Mail-Clients und gegebenenfalls spezieller Plugins.

### 1.2.2 Abgrenzung

Port Sol 19 hat als Hersteller der Software keinen Einfluss darauf, in welcher Umgebung sie eingesetzt wird. Technisch gesehen ist ein Einsatz des Produkts in verschiedenen Konstellationen möglich. Die Begutachtung gilt nur für den Einsatz in folgender Konfiguration:

- Der Verschlüsselungsautomat wird zusammen mit einem De-Mail-Verfahren eines zertifizierten De-Mail-Providers genutzt.
- Es kommt das Verschlüsselungsverfahren S/MIME zum Einsatz.

  Anmerkung: In anderen Produktvarianten ist auch die Nutzung weiterer Verschlüsselungsverfahren möglich. Diese Funktionen sind in der evaluierten Fassung nicht vorhanden.

- Der Verschlüsselungsautomat wird auf einer datenschutzkonformen Plattform und in einem sicheren internen Netzwerk betrieben.

  Erläuterung: Wie jede Software wird auch der Verschlüsselungsautomat in einer vom Anwender gewählten Umgebung eingesetzt. Der Anwender wählt die Produkte aus, z.B. das Betriebssystem, und konfiguriert diese nach eigener Maßgabe unter Einhaltung der Vorgaben des Verschlüsselungsautomaten (siehe Betriebshandbuch). Ebenso definiert der Anwender die physische Umgebung des Einsatzes. Inwieweit datenschutzrechtliche Belange dadurch verletzt werden könnten, dass diese Plattformen unsicher implementiert oder betrieben werden, kann durch eine darauf eingesetzte Software nicht beeinflusst werden. Jedenfalls erzeugt der Verschlüsselungsautomat keine neuen Sicherheitsrisiken. Für den Fall, dass ein Verfahren, welches den Verschlüsselungsautomaten nutzen wird, datenschutzrechtlich zu beanstanden wäre, gilt das das bereits heute ohne den Einsatz des AddOn.

Nicht Teil des Produkts und damit nicht Gegenstand der Begutachtung ist die Entschlüsselung von Nachrichten, da diese mit Standardmitteln des Systems des Empfängers der Mail erfolgt, bei menschlichen Empfängern z.B. mittels des Mail-Clients und gegebenenfalls S/MIME-Plugins.

## 1.3 Art der Begutachtung

Es handelt sich um eine Prüfung im Rahmen einer Erstzertifizierung.

# 168 2 Teil I - Allgemeiner Teil

169 entsprechend Vorgabe „Prüfschema des Gutachtens für die Produktzertifizierung“ / V 1.1 vom
170 17.06.2015; siehe **Error! Reference source not found.**.

## 171 2.1 Zeitpunkt der Prüfung

| | |
|---|---|
| Juni 2015 | Vollständigkeitsprüfung der Dokumentation |
| 29. Juni 2015 | Vor-Ort-Begutachtung des Entwicklungslabors und des Verschlüsselungsautomaten |
| August 2015 | Erstmalige Begutachtung des Verschlüsselungsautomaten nach den Vorschriften des Datenschutz Gütesiegels |

172 weitere Details siehe Kapitel 2.10.

## 173 2.2 Adresse des Antragstellers

| | |
|---|---|
| Firma: | Port Sol 19 GmbH |
| Ansprechpartner: | Ludwig Schreyer |
| Adresse: | Lortzingstraße 2<br>55127 Mainz |
| Telefon: | +49 (0) 6131 785600 |
| E-Mail: | ludwig.schreyer@bgn.de |

## 174 2.3 Adressen der Sachverständigen

**Prüfstelle:**

| | |
|---|---|
| Firma: | Mission 100 e.V. |
| Ansprechpartner: | Michael J. Erner |
| Adresse: | Gartenäckerstr. 13<br>86825 Bad Wörishofen |
| Telefon: | +49 8247 99 88 780 |
| E-Mail: | info@mission100.org |

175

| **Gutachter:** | **Rechtlicher Gutachter** | **Technischer Gutachter** |
|---|---|---|
| Firma: | Mission 100 e.V. | Mission 100 e.V. |
| Name: | Michael J. Erner | Friedrich Abraham |
| Adresse: | Gartenäckerstr. 13<br>86825 Bad Wörishofen | Auf den Dreien 52<br>50354 Hürth |
| Telefon: | +49 (0) 172 451 05 04 | +49 (0) 172 98 24 009 |
| E-Mail: | me@mission100.org | fa@mission100.org |

## 176 2.4 Kurzbezeichnung des IT-Produktes

177 Verschlüsselungsautomat S/MIME

## 178 2.5 Detaillierte Bezeichnung des IT-Produktes

### 179 2.5.1 Produktbezeichnung

180 Bezeichnung: „Verschlüsselungsautomat S/MIME“

181 Geprüfte Version: 1.0

182 Stand: 31. Mai 2016

### 2.5.2 Produktbeschreibung

Funktion des Produkts ist die Erweiterung von De-Mail um eine Ende-zu-Ende-Verschlüsselung. „Ende-zu-Ende“ bedeutet: Vom Verschlüsselungsautomaten bis zum Empfänger einer Mail.

Der Verschlüsselungsautomat umfasst

- Entgegennahme von zu versendenden Nachrichten
- Bestimmung des anzuwendenden Verschlüsselungsverfahrens
  - Abfrage eines öffentlichen Verzeichnisdiensts (ÖVD) auf Existenz eines öffentlichen Schlüssels für eine asymmetrische Verschlüsselung
  - Gegebenenfalls, d.h. falls ein solcher Schlüssel nicht existiert: Abbruch des Versandvorgangs
- Verschlüsselung der Nachricht
  - Asymmetrisch (Default): S/MIME
- Versand
  - Verschlüsselte E-Mail
- Bounce Management

Nicht Teil des Produkts und damit nicht Gegenstand der Begutachtung ist die Entschlüsselung von Nachrichten, da diese mit Standardmittel des Systems des Empfängers der Mail erfolgt, bei menschlichen Empfängern z.B. mittels des Mail-Clients und gegebenenfalls spezieller Plugins. Die Entschlüsselung wird als Interpretation einer E-Mail verstanden.

### 2.5.3 Abgrenzung

Folgende technische Komponenten sind Teil des geprüften Produkts

- Webservice „Verschlüsselungsautomat“

Folgende technische Komponenten und Verfahren sind ausdrücklich **nicht** Teil des geprüften Produkts:

- JAVA Application Server
- Apache Tomcat
- JDK (Java SE Development Kit)
- Camel, CFX Framework
- Diverse Beans
- Server Plattform inkl. Virtualisierungsumgebung
- Verteilerlogik
- Mailserver
- De-Mail Gateways
- Client Systeme/Applikationen

Diese Objekte sind systemtechnische Voraussetzungen für den Produkteinsatz.

Siehe Liste der technische Komponenten und Verfahren im vorigen Kapitel; es handelt sich bei dem Produkt um einen Webservice.

Das Release Management erfolgt mittels SVN.

## 2.6 Zweck und Einsatzbereich

Das Produkt ermöglicht die Nutzung von De-Mail zum Versand von Daten, die durch den gesetzlichen Datenschutz geschützt werden, insbesondere auch von Sozialdaten im Sinn der Sozialgesetzbücher (SGB).

"De-Mail" ist Bestandteil des Programms "E-Government 2.0". So betreibt etwa das Land Schleswig-Holstein den Einsatz von De-Mail in Fällen, in den aus Gründen des Landesrechts die Schriftform vorgeschrieben ist. Siehe hierzu zum Beispiel die Ausführung der Staatskanzlei Schleswig-Holstein zu De-Mail und dem Personalausweis.

Zu den aktuellen Schwächen von De-Mail gehört das Fehlen einer Ende-zu-Ende-Verschlüsselung und die daraus entstehenden Begrenzungen des Einsatzes im Bereich der Verarbeitung von personenbezogenen Daten. Das De-Mail-Gesetz bleibt bei der Definition des Begriffs „Vertraulichkeit“ vage und schreibt Verschlüsselung in §§ 4 und 5 nur für Teilbereiche vor. Ende-zu-Ende-Verschlüsselung ist optional (siehe § 5 Abs.3) und wird von De-Mail-Anbietern auch nicht zwangsläufig angeboten, siehe hierzu auch die Ausführungen des ULD.

Aus diesem Grund scheidet De-Mail alleine als Übermittlungsverfahren für Sozialdaten aus. Der BfDI schreibt für den Versand von Sozialdaten zwischen Institutionen eine Ende-zu-Ende Verschlüsselung explizit vor. Siehe dazu „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“ des BfDI.

Die Port Sol 19 GmbH hat aufgrund dessen eine Erweiterung für De-Mail entwickelt. Zur Sicherstellung einer Ende-zu-Ende Verschlüsselung wird ein „Verschlüsselungsautomat“ angeboten.

Das Verfahren ist sowohl im öffentlichen als auch im nichtöffentlichen Bereich einsetzbar.

Anmerkung: Der Verschlüsselungsautomat ist, technisch gesehen, auch ohne De-Mail, nämlich in einer reinen SMTP-Umgebung nutzbar. Diese Konfiguration reicht aber für den Einsatz zur Übermittlung von personenbezogenen bzw. Sozialdaten im Regelfall nicht aus.

## 2.7 Modellierung des Datenflusses

Nachfolgende Bild zeigt den Datenfluss des Verschlüsselungsautomaten.

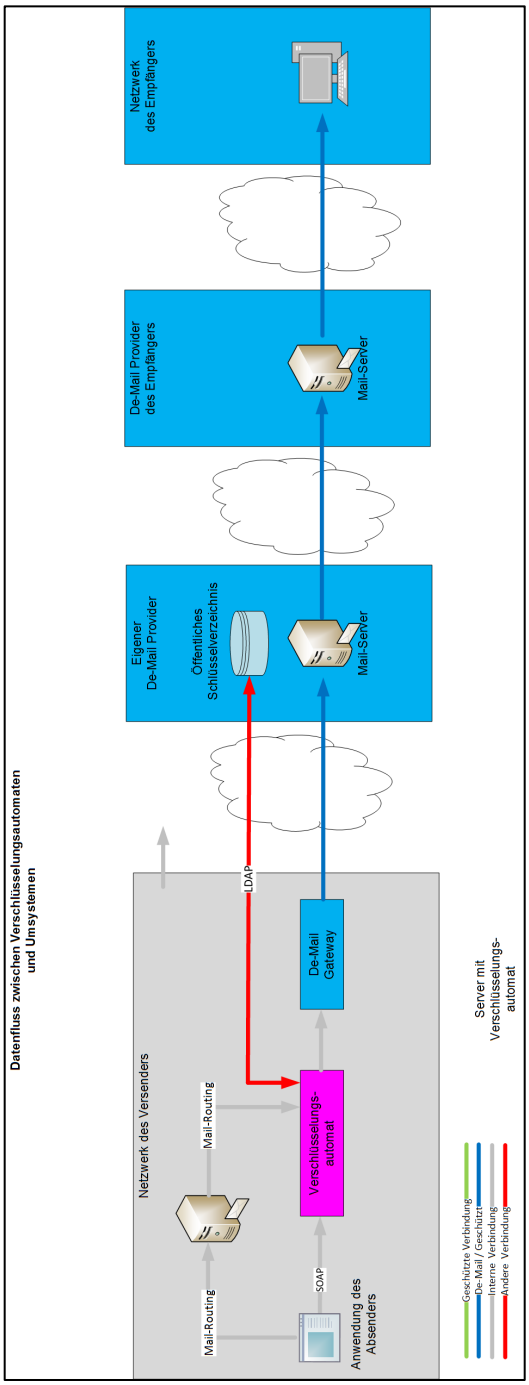


Abbildung 1 Datenfluss zu den Umsystemen

## 2.8 Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog v 2.0 vom 28.11.2014.

## 2.9 Angewandte Evaluationsmethoden

### 2.9.1 Modus der Prüfung

Das begutachtete Produkt (siehe Kapitel 2.4) ist bisher noch nicht nach den Vorschriften des Gütesiegels Datenschutz geprüft worden. Die Begutachtung dient der Erstzertifizierung.

### 2.9.2 Vorgehensweise

Das Entwicklungslabor im Haus der Port Sol19 GmbH in Mainz wurde am 29.6.2015 begutachtet.

Das Produkt selbst wurde am 29.6.2015 betrachtet. Dies schloss eine stichprobenartige Diskussion des Codes ein. Der Quell-Code lag den Prüfern seither zur Begutachtung vor.

Alle in diesem Gutachten getroffenen Aussagen basieren auf der Grundlage dieser Prüfungen.

### 2.9.3 Veränderungen im Produkt

Da es sich hierbei um eine Erstzertifizierung handelt, ist dieser Punkt nicht anwendbar.

## 2.10 Zusammenfassung der Prüfergebnisse

Nach Ansicht der Auditoren werden folgende Prüfergebnisse erzielt: Die Erfüllung der Einzelforderung des Anforderungskatalogs wird bestätigt.

Anmerkung: Das Produkt erscheint aus Nutzersicht wie eine Erweiterung („Plugin“) des Mail-Systems. Zahlreiche Einzelforderungen des Anforderungskatalogs sind gegebenenfalls von dieser aufrufenden Anwendung zu erfüllen, weil die Ausgestaltung vom Einsatzkontext abhängt.

## 2.11 Ausgleichende Maßnahmen

Nicht relevant

## 2.12 Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das Produkt erweitert De-Mail um Ende-zu-Ende-Verschlüsselung und ermöglicht so die Nutzung von De-Mail zum Versand insbesondere auch von besonderen personenbezogenen Daten im Anwendungsbereich der §§ 3 Abs. 9 BDSG, 203 StGB und Sozialdaten im Sinn der Sozialgesetzbücher (SGB).

Der Verschlüsselungsautomat erfüllt die Grundsätze der Datensparsamkeit und der zweckgebundenen Verarbeitung. Der Automat hat alleine den Zweck, Nachrichten zu verschlüsseln und anschließend einem Mail-Server zum Versand zu übergeben. Dazu werden nur die Daten benutzt, die dafür notwendig sind, nämlich die Mailadressen des Senders und des Empfängers sowie die Nachricht selbst. Die zu verarbeiteten Daten werden während der Verschlüsselung im Hauptspeicher gehalten und anschließend unmittelbar gelöscht, somit nicht gespeichert. Dies ist auch im Fehlerfall so. Kann eine Mail nicht zugestellt werden, so findet kein Queuing statt, sondern das Objekt wird mit einer Fehlernummer an die aufrufende Applikation zurückgegeben.

Alle benutzten Daten sind bereits beim Nutzer des Automaten vorhanden (in der Anwendung, die den Automaten benutzt). Einziges neues Datum ist das ggf. vorhandene öffentliche Zertifikat bzw. der öffentliche Schlüssel des Empfängers, der aus Datenschutzsicht nicht relevant ist.

Eine Weitergabe der Daten erfolgt an den vom Nutzer des Automaten definierten Mail-Empfänger.

Das Produkt erzeugt dabei selbst keine eigenen personenbezogenen Daten und führt keine Auswertungen durch. Es ist möglich, aber nicht obligatorisch, die Vorgänge des Verschlüsselungsautomaten zu protokollieren (Logging). Dabei handelt es sich jedoch um eine Funktion der genutzten Plattformen (Betriebssystem, Tomcat). Entsprechend wird in diesem Gutachten vorausgesetzt, dass der Verschlüsselungsautomat In einer sicheren Umgebung läuft.

Bestätigung

Hiermit bestätigen wir, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und der Datensicherheit entspricht.

Wir versichern, an der Entwicklung und Betreuung des Verfahrens nicht beteiligt gewesen zu sein und mit Ausnahme des Prüfauftrages für das Datenschutz-Gütesiegels über keine geschäftliche oder private Beziehung zu der Auftraggeberin zu verfügen.

gez. M. Erner

(Michael J. Erner)

Bad Wörishofen, den 10. Okt. 2015

gez, F. Abraham

(Friedrich Abraham)

Hürth, den 15. Oktober 2015

# 3 Teil II: Erfüllung der Rechtsvorschriften

## 3.1 § 11 BDSG / § 17 LDSG SH

Das Produkt Verschlüsselungsautomat setzt auf die technische Infrastruktur des DE-Mail-Systems auf, für die bereits eine Auftragsdatenverarbeitung existiert. Es ist insoweit zu fragen, ob die Regelungen des § 11 BDSG hier im Sinne eines erweiterten Anwendungsbereiches relevant sind. Dies kann hier sowohl für Primär- als auch für Sekundärdaten verneint werden, da durch den Einsatz des Verschlüsselungsautomaten eine Lücke im De-Mail-System geschlossen wird, auf die schon bei den unterschiedlichen De-Mail-Anbietern in den AGB unter dem Stichwort „Ende-zu-Ende-Verschlüsselung hingewiesen wird. Durch den Einsatz des Verschlüsselungsautomaten wird somit schon durch den Auftraggeber die Möglichkeit der Verarbeitung von personenbezogenen Daten durch Dritte wie den Auftragnehmer nach dem Stand der Technik reduziert.

## 3.2 Berufsgeheimnisträger gem. § 203 StGB, § 80 Abs. 5 SGB X

Zum Anwendungsbereich des Verschlüsselungsautomaten im Umfeld von Berufsgeheimnisträgern ist zunächst auf den Aspekt der Offenbarung des § 203 abzustellen. Offenbart wird ein Geheimnis, wenn es einer anderen Person zugänglich gemacht wird, d.h., mündlich, schriftlich oder durch Einsichtnahme. Hierzu gehört auch eine Weitergabe von Geheimnissen unter Kollegen.

Weiterhin muss ein Geheimnis anvertraut sein. Letzteres ist immer dann anzunehmen, wenn es zu einer Kommunikation zwischen dem Betroffenen und dem Träger eines Berufsgeheimnisses kommt, hier im Fall einer Email die Situation, dass ein Berufsgeheimnisträger einem Betroffenen eine Nachricht im Umfeld des Geheimnisses zukommen lassen möchte und hierbei sicherzustellen hat, dass dabei eine Offenbarung vermieden wird. Dies wird einerseits durch den Prozess der Verschlüsselung selbst gewährleistet, da die eingesetzten Verschlüsselungsverfahren dem Stand der Technik entsprechen. Ebenso wird eine Offenbarung an einen Unberechtigten dahingehend vermieden, dass aus einem öffentlichen Zertifikatsspeicher des De-Mail-Providers ein S/MIME-Schlüssel des Adressaten der E-Mail beschafft wird, mit dem die E-Mail inklusive aller Anlagen verschlüsselt und zum Versand an das De-Mail-System übergeben wird. Weiters wird hierbei ausgeschlossen, dass ein Versand erfolgt, wenn es keinen Schlüssel im Verzeichnis gibt. Durch hinterlegte Automatismen hat ein Berufsgeheimnisträger damit keine Möglichkeit, eine unverschlüsselte Nachricht zu versenden.

Der Verschlüsselungsautomat ist ferner in einer Umgebung einsetzbar, in der es ohne Verschlüsselung nicht erlaubt ist, besondere personenbezogene Daten elektronisch zu versenden, d.h., es ist ohne Verschlüsselung nur auf dem Wege der gelben Post erlaubt, Nachrichten zu verschicken. In diesem Umfeld eröffnet der Verschlüsselungsautomat die Möglichkeit elektronischer Kommunikation.

Damit sind zum Einsatz des Systems weiterhin die Vorschriften des Telekommunikationsgeheimnisses zu wahren. Hierbei ist einerseits darauf zu achten, dass der Verschlüsselungsautomat in einer datenschutzkonformen Umgebung eingesetzt wird. Die hierzu erforderlichen Anforderungen sind im Datenschutzhinweisblatt zum Verfahrens beschrieben.

Daneben ist auf eine erforderliche Einwilligung des/der Berechtigten abzustellen, d.h. Sender und Empfänger müssen in das Verfahren eingewilligt haben und diese Einwilligung muss auch widerrufbar sein. Dies wird dadurch realisiert, dass nur Berechtigte - im Umfeld von Sonderrechtsverpflichteten diese selbst - einen Schlüssel erstellen und ebenso diesen wieder löschen oder deaktivieren können. Eine weitere Verwendung des Verschlüsselungsverfahrens ist durch die Unmöglichkeit eines Versandes ohne Schlüssel ausgeschlossen, d.h. ein Widerruf einer Einwilligung zur Nutzung des Systems wird ad hoc ebenfalls durch die Löschung des Schlüssels des Berechtigten wirksam. Eine Protokollierung der Einwilligung/Schüsselerstellung ist obsolet, da alleinig das Erstellen und das

darauf folgende Vorhandensein eines Schlüssels eine Einwilligung des Berechtigten durch aktives Tun voraussetzt.

Somit kann der durch den Verschlüsselungsautomaten der Anwendungsbereich auch auf den Kreis von Berufsgeheimnisträgern (gem. § 203 StGB; § 80 Abs. 5 SGB X) ausgedehnt werden, da die jeweiligen Anbieter keine Möglichkeit der Kenntnisnahme von besonderen personenbezogenen Daten der Auftraggeber erlangen können.

## 3.3 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten gem. § 42a BDSG

Der Verschlüsselungsautomat selbst schließt eine unrechtmäßige Kenntnisnahme von Daten gem. 42a BDSG aus. Einerseits ist dies durch die Bounce-Funktion gewährleistet, andererseits werden durch die Implementierung, bei der die zu verschlüsselnden Daten unmittelbar nach Vorgang gelöscht werden, keine verwertbaren Sekundärdaten gespeichert, die ein Risiko für Betroffene darstellen könnten.

## 3.4 Erläuterungen zur technischen Bewertung

### 3.4.1 Sicherheit von Verschlüsselung

Verschlüsselung als Maßnahmen der Kontrolle des Zugangs zu Information erzeugt, wie jede andere Sicherheitsmaßnahme auch, keinen absoluten Schutz vor Missbrauch und kann deswegen die Offenlegung von entsprechend gesicherten Personendaten auch nur erschweren, aber nicht zu 100% verhindern. Zu hinterfragen ist also, welchen Aufwand jemand betreiben müsste, um die Sicherheitsmaßnahme zu umgehen, in diesem Fall also einen Verschluss brechen.

Auch das BDSG fordert nur angemessenen, nicht aber absoluten Schutz von Personendaten. Einer positiven Bewertung liegt folglich die These zugrunde, dass State-of-the-Art-Technologie ausreichend sein sollte, um auch im Sinn des Datenschutzes als ausreichend sicher zu gelten. Andernfalls wäre es in letzter Konsequenz unmöglich, Personendaten überhaupt elektronisch zu übertragen, ohne Datenschutzrecht zu brechen, nicht nur bei Datenübertragung wie bei E-Mailing, sondern auch in der Sprachkommunikation.

Im Verschlüsselungsautomaten kommt der RC2-Algorithmus zum Einsatz, was als State-of-the-Art gelten darf. Erfolgreiche einfache kryptoanalytische Angriffe, etwa Brute Force, also das Ermitteln des Schlüssels zum Beispiel durch einfaches Durchprobieren, sind mit der gegenwärtig verfügbaren Hardware auszuschließen, sofern die verwandten Schlüssel ausreichend lang sind. Der Verschlüsselungsautomaten benutzt RSA-Schlüssel mit einer Länge von 2048 Bits. Erfolgreiche Angriffe sind bei dieser Schlüssellänge nicht bekannt. Erfolgreich könnten theoretisch Known-Message.Attacken sein. Allerdings wird dafür ein sehr langer, bekannter Text benötigt. Das Restrisiko eines Bruchs der Verschlüsselung ist somit gegeben, setzt allerdings Mittel voraus, die nur in seltenen Ausnahmefällen vorhanden sein dürften.

### 3.4.2 Sicherheit des eingesetzten Verschlüsselungsverfahren

Als Verfahren für die E-Mail-Verschlüsselung wird S/Mime eingesetzt, das als Industriestandard für Verschlüsselung in der Kommunikation gilt.

### 3.4.3 Sicherheit des Schlüsselmaterials

Eine Verschlüsselung kann nur dann als hinreichend sicher betrachtet werden, wenn angenommen werden darf, dass ein Angreifer keinen Zugang zu den verwendeten privaten Schlüsseln erlangt. Auch hier gilt jedoch, dass „kein Zugang“ interpretiert werden muss im Sinn von „nicht unter normalen Umständen“ bzw. „nur unter einem Einsatz von zeitlichen Aufwand und sonstigen Mittel, die das üblicherweise anzunehmende Maß erhebliche überschreiten, denn natürlich lässt sich immer ein

Szenario konstruieren, in dem ein Angreifer Zugriff auf Schlüssel erlangen könnte, zum Beispiel durch Anwendung physischer Gewalt gegen den Schlüsselinhaber.

Der Verschlüsselungsautomat benutzt S/Mime-Zertifikate, die im öffentlichen Schlüsselverzeichnis (ÖVZ) eines akkreditierten De-Mail-Providers hinterlegt werden. Die Generierung bzw. Beschaffung und die Hinterlegung eines Zertifikats sind allein Aufgabe des Inhabers, also hier eines Teilnehmers im De-Mail-Verfahren. Nutzer der Zertifikate haben darauf keinen Einfluss hat.

Die Akkreditierung des ÖVZ-Betreibers als De-Mail-Provider setzt voraus, dass der Provider ein sicheres Verfahren der Identifizierung von Teilnehmern betreibt. Deshalb darf angenommen werden, dass die im ÖVZ hinterlegten Zertifikate tatsächlich zu den Personen oder Institutionen gehören, deren Identität dort angegeben ist. Insbesondere kann unterstellt werden, dass Zertifikat und E-Mail-Adresse zueinander gehören.

Problematisch ist die Beantwortung der Frage, ob das Zertifikat, technisch gesehen, ausreichend gut ist. Denkbar wäre zum Beispiel, dass die Generierung durch eine nicht vertrauenswürdige Instanz erfolgte, die bei der. Generierung eine Kopie erzeugt hat, möglicherweise erzwungen durch die Rechtslage in dem Land, in dem das Unternehmen tätig ist.

Bei der positiven Beurteilung des Verschlüsselungsautomaten ging der Gutachter diesbezüglich von der Überlegung aus, dass Sicherheitsmängel bei der Erzeugung von Zertifikaten gleichzusetzen sind mit solchen bei der Verwendung, zum Beispiel der bewussten Veröffentlichung eines privaten Schlüssels, also letztlich als Verfehlung des Zertifikatsinhabers gesehen werden müssen. Der Nutzer eines im ÖVZ hinterlegten Zertifikats darf bei dessen Verwendung nämlich grundsätzlich davon ausgehen, dass dies eine bilaterale vertrauliche Kommunikation erlaubt. Im Rahmen seiner Sorgfaltspflicht muss aber der Nutzer des Zertifikats den Inhaber auf die Art der beabsichtigten Verwendung und die daraus resultierenden Risiken hinweisen. Deswegen wurde in das Datenschutzblatt ein entsprechender Hinweis aufgenommen.

### 3.4.4 Bewertung der Zukunftsfähigkeit des Produkts

Die technischen und gesetzlichen Anforderungen an die Kommunikation im Kundenkreis des Verschlüsselungsautomaten sind im Laufe der Zeit Änderungen unterworfen, die kontrolliert werden müssen. Das betrifft im Umfeld des Verschlüsselungsautomaten insbesondere

- Gesetze und Compliance-Anforderungen: BDSG, SGB X, Technische Richtlinien des BSI zur Verschlüsselung und für den Healthcare-Bereich, u.a. TR-02102.
- Technische Anforderungen: Laufende Überprüfung der Architektur und der eingesetzten Komponenten, ob diese noch den Sicherheitsanforderungen genügen

Gesetzliche Anforderungen werden durch Juristen im Hause und durch die Revision des Dachverbandes der gesetzlichen Unfallversicherungen geprüft. Technische und Compliance-Anforderungen prüft der Sicherheitsbeauftragte der Portsol 19 GmbH im Rahmen regelmäßiger Audits. Hierzu liegen Prüfberichte vor.

Die Sicherheit von bestimmten, aufgrund der implementierten Algorithmen prinzipiell geeigneten Verschlüsselungsverfahren wie S/MIME bzw. RSA wird aus der Länge der aktuell verwendeten Schlüssel berechnet. Welche Schlüssellängen jeweils als ausreichend betrachtet werden, hängt wiederum mit der Leistungsfähigkeit der Technik, die für mögliche Angriffe verfügbar ist, zusammen. Die derzeit verwandten Schlüssellängen sind laut TR-02102 ausreichend.

- Bei der S/MIME Verschlüsselung selbst wird aktuell RC2-CBC eingesetzt (128 Bit Schlüssellänge). Im Rahmen des Change Management Konkret sollen Schlüssellängen regelmäßig geprüft werden.
- Bei Signaturen in Zertifikaten: Der Verschlüsselungsautomat stellt selber keine Zertifikate aus. Er holt nur Zertifikate aus dem Öffentlichen Verzeichnisdienst der De-Mail Anbieter. Die hier eingesetzten Algorithmen kann Portsol 19 nicht beeinflussen. Im Datenschutzhinweisblatt wird darauf verwiesen, dass die De-Teilnehmer selbst auf die Einhaltung von Mindestnormen achten müssen. Der Öffentliche Verzeichnisdienst von T-Systems zum Beispiel (dieser wird

im Rahmen der BGN genutzt) setzt als Mindestanforderung RSA 2048 Bit an. Es ist abzusehen, dass das ab 2017 nicht mehr als ausreichend betrachtet wird. Es gibt seitens der BGN regelmäßigen Kontakt zu T-Systems, in dem auf diese Problematik verwiesen wird. Konkret wird dabei darauf hinweisen, dass Schlüssellängen unter 3000 Bit ab 2017 nicht mehr als hinreichend akzeptiert werden.

# 4 Anhang 2: Verfahrensbeschreibung

Diese Kapitel enthält eine kurze Beschreibung des Verfahrens, wie es anlässlich der Begutachtung durch Port Sol 19 präsentiert und durch die Auditoren geprüft wurde.

Die Zeichnungen in diesem Abschnitt sind nur schematisch und in technischen Details nicht notwendigerweise exakt.

Wenn nachfolgend von „E-Mail“ die Rede ist, so umfasst dieser Begriff:

- Den Inhalt der Nachricht, also den so genannten Mail Body
- Alle Anhänge
- Die Verbindungsdaten, also z.B. Angaben zum Absender und Empfänger sowie den Betreff

## 4.1 E-Mail-Sicherheit

Die Übertragung von E-Mails im Internet ist im Hinblick auf alle denkbaren Sicherheitsziele unsicher.

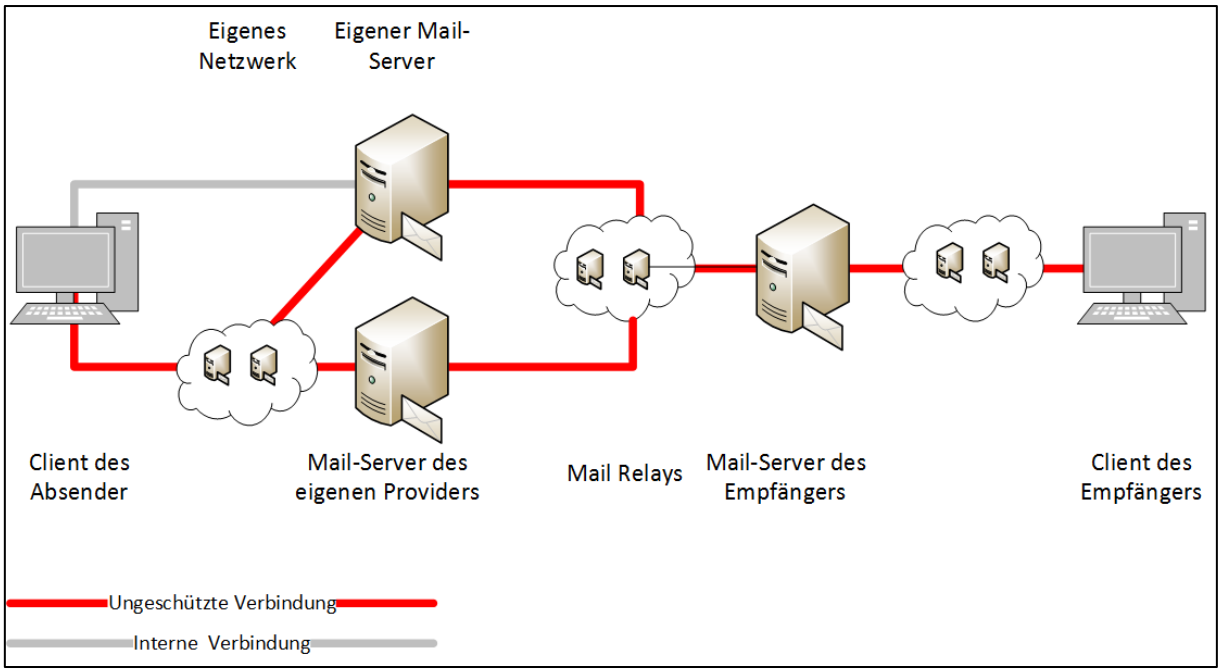


Abbildung 2: E-Mail

E-Mails werden über offene Netze transportiert und dabei von einer unbekannten Anzahl unbekannter Systeme, z.B. Netzwerkkomponenten und Mail Relays, verarbeitet. Nicht nur die Administratoren dieser Systeme, auch alle anderen Teilnehmer im Netz, im Prinzip also jeder, hat potenziell Zugriff auf die E-Mails.

- Vertraulichkeit: Ist nicht gegeben, weil die Nachrichten transparent übertragen werden
- Integrität: Ist nicht gegeben; Nachrichten können bei der Übertragung durch Dritte beliebig geändert werden, auch durch Verfälschung infolge technischer Probleme
- Authentizität: Ist nicht gegeben; abgesehen davon, dass bereits die Verifikation des Inhabers einer Mail-Adresse dem Nutzer überlassen bleibt, können Identitäten problemlos gefälscht werden, also z.B. Nachrichten unter fremden Absenderangaben versandt werden
- Nicht-Abstreitbarkeit: Ist nicht gegeben; weder ist sicher, dass eine Mail den Empfänger erreichen wird, noch kann bewiesen werden, dass sie es tatsächlich hat.

## 4.2 De-Mail

Mit dem De-Mail-Gesetz vom 28.4.2011 hat der Gesetzgeber in Deutschland die Grundlage für eine erhebliche Verbesserung der Mail-Sicherheit geschaffen.

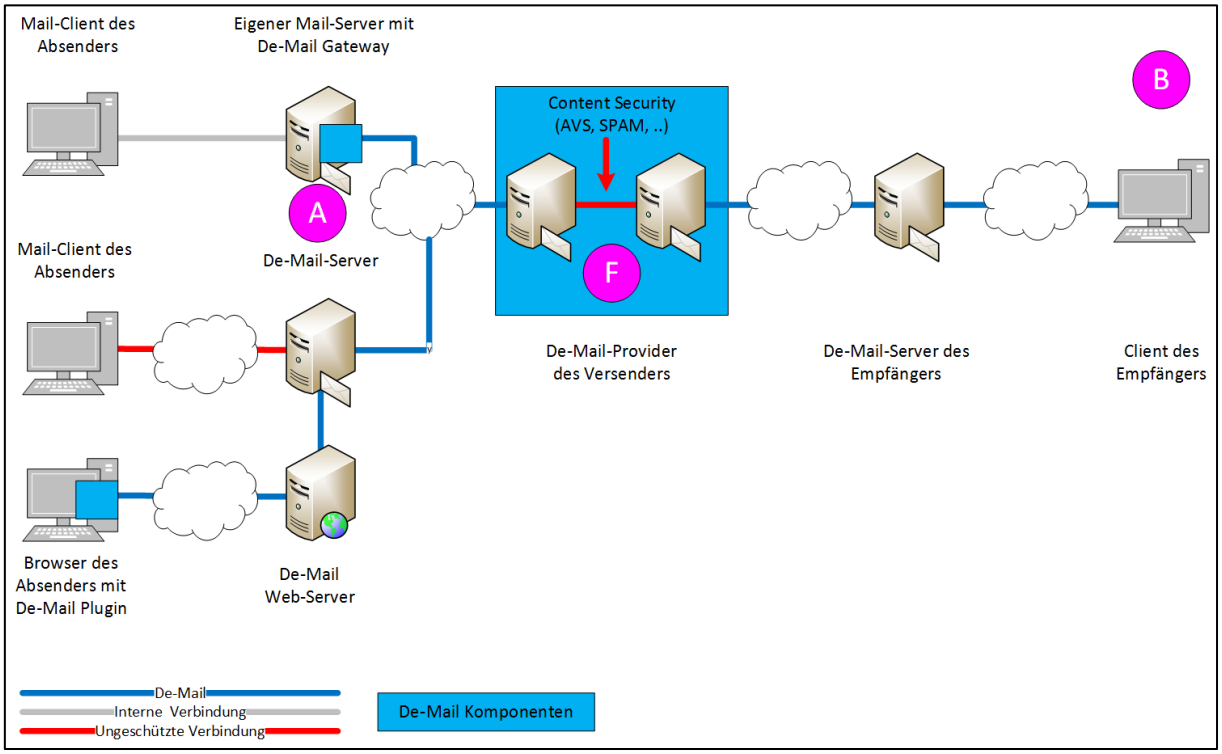


Abbildung 3: De-Mail

Bei De-Mail übernehmen ausgewählte und speziell dafür zertifizierte Betreiber die Aufgabe des Mail-Providers und erweitern den Funktionsumfang von Mail und Sicherheitskomponenten. Die wesentlichen Elemente sind:

- Sichere Authentisierung der Teilnehmer und in der Folge eindeutige Zuordnung von Adressen zu Teilnehmern
- Verschlüsselung des Transportwegs (in Abbildung 3: De-Mail die Teile der Strecke von A nach B in öffentlichen Netzwerken)
- Protokollierung des Versands und der Zustellung

Die genaue Ausgestaltung des Service bleibt dem De-Mail-Anbieter vorbehalten. Jedoch muss er die gesetzlichen Vorgaben einhalten, was im Rahmen der Zulassung über einen speziellen Kriterienkatalog geprüft wird. Letzterer wurde vom Bundesbeauftragten für Datenschutz und die Informationsfreiheit (BfDI) veröffentlicht.

Das De-Mail-Gesetz schreibt nur eine Transportverschlüsselung vor, nicht aber eine Ende-zu-Ende-Verschlüsselung, weshalb eine solche auch nicht angenommen werden kann und auch tatsächlich nicht vorhanden ist. Die Deutsche Telekom etwa entschlüsselt Mails vorübergehend zum Zwecke des Content-Filtering (SPAM-Schutz) und zur Abwehr von Malware (AVS) (siehe Zeichnung oben/Markierung F).

Die Situation stellt sich somit wie folgt dar:

- Vertraulichkeit: Ist weitgehend gegeben, weil die Nachrichten verschlüsselt übertragen werden; Zugriff ist grundsätzlich weiter beim De-Mail-Betreiber möglich
- Integrität: dto.
- Authentizität: Ist vollständig gegeben
- Nicht-Abstreitbarkeit: Ist vollständig gegeben.

## 4.3 Verschlüsselungsautomat

Aufgrund der fehlenden Ende-zu-Ende-Verschlüsselung eignet sich De-Mail ohne Erweiterung nicht zum Versand besonderer personenbezogener Daten. Insbesondere deshalb hat der BfDI die Anwendung im Rahmen des Versands von Sozialdaten ausgeschlossen.

Eine solche Erweiterung ist grundsätzlich bereits mit ausreichend starker Inhaltsverschlüsselung, etwa mittels S/MIME oder PGP, denkbar. Praktisch stößt das Vorgehen aber an die Grenzen, die seit jeher den Umgang mit Verschlüsselung so kompliziert machen und dazu führen, dass E-Mail-Verschlüsselung nach wie vor die Ausnahme ist. Als Beispiele seien zu nennen:

- Absender und Empfänger müssen sich bilateral auf ein technisches Verfahren einigen.
- Die Verwaltung der Schlüssel ist dem einzelnen Nutzer überlassen; öffentliche Schlüsselverzeichnisse leisten nur Unterstützung.
- Die Anwendbarkeit bei automatisch generierten Mails ist schwierig.

Der Verschlüsselungsautomat von Port Sol 19 löst diese Probleme.

- Es können verschiedene Verfahren der Verschlüsselung parallel genutzt werden, je nachdem, welche Möglichkeiten der Entschlüsselung ein Empfänger hat.
- Verschlüsselung erfolgt für einen wohl definierten Empfängerkreis grundsätzlich.
- Die Schlüsselverwaltung ist automatisiert und nutzt u.a. den ÖVD des De-Mail-Systems.
- Das Verfahren kann sowohl bei manuell in einem Client generierten Mails wie auch über eine Programmschnittstelle genutzt werden.

Die Situation für De-Mail plus Verschlüsselungsautomat stellt sich somit wie folgt dar:

- Vertraulichkeit: Ist durch Ende-zu-Ende-Verschlüsselung gegeben.
- Integrität: Dto.
- Authentizität: Ist vollständig durch De-Mail sichergestellt
- Nicht-Abstreitbarkeit: Dto.

## 4.4 Arbeitsweise des Verschlüsselungsautomaten

### 4.4.1 Übersicht

Das folgende Bild zeigt die Arbeitsweise des Verschlüsselungsautomaten.

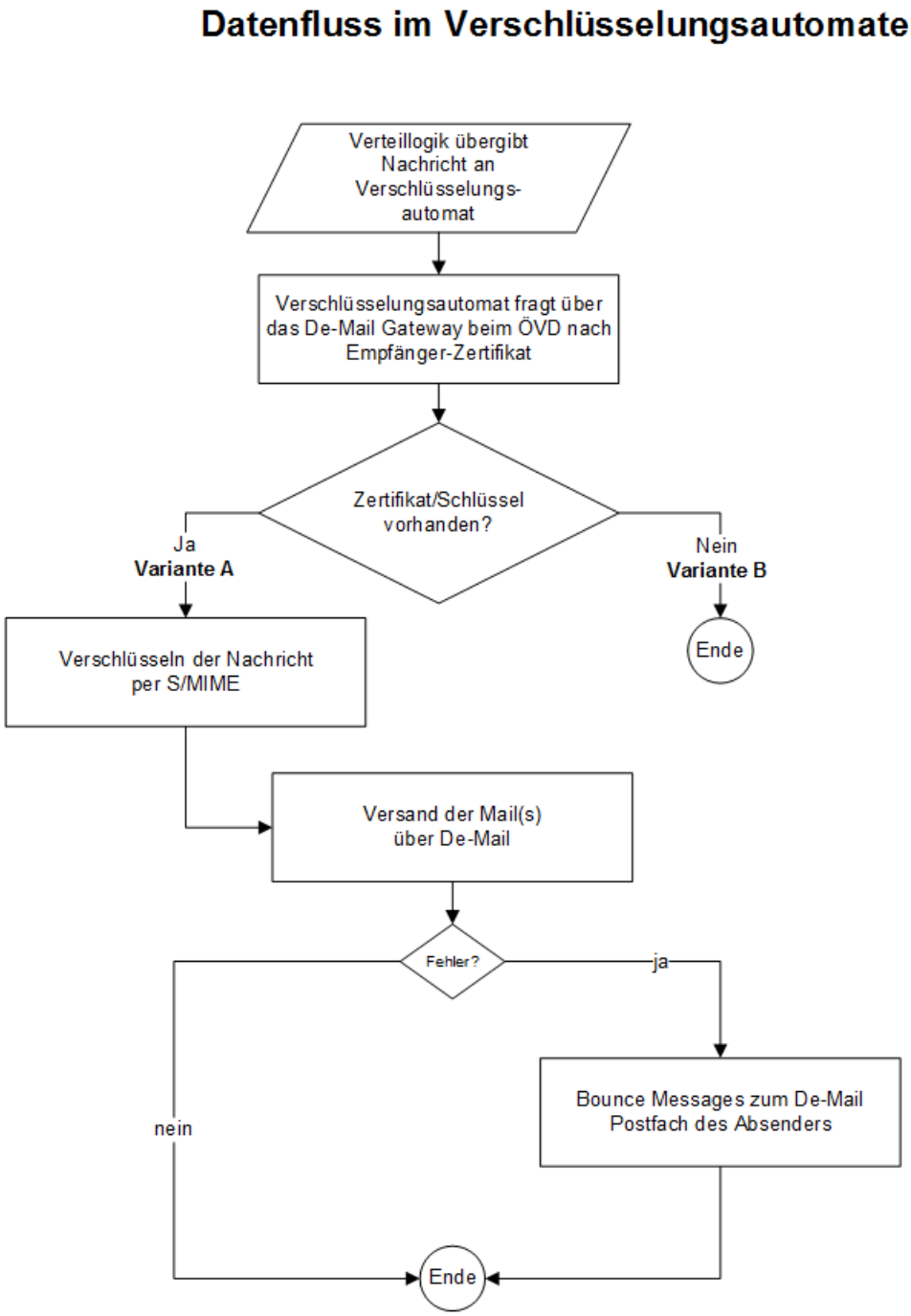


Abbildung 4: Datenfluss im Verschlüsselungsautomaten

Erläuterungen hierzu:

- Verwandte Verschlüsselungsverfahren:
  - Übergeordnetes Verfahren: S/MIME
  - Algorithmus: RC2 CBC
  - Schlüsseltyp RSA / Schlüssellänge 2048 Bit
  - Signaturalgorithmus SHA 224 und höher
  - Kryptobibliotheken: OpenSource (BouncyCastle V1.52)
- Schlüsselmanagement
  - Das Schlüsselmanagement erfolgt entsprechend den Vorgaben des De-Mail-Gesetzes durch einen zertifizierten De-Mail-Provider.
  - Die Schlüssel werden dort in einem öffentlichen Verzeichnis bereitgestellt.
  - Die Schlüsselverwaltung im Verschlüsselungsautomaten beschränkt sich auf die Beschaffung der Keys aus dieser Quelle. Der Zugriff erfolgt via LDAP bzw. LDAPS, und zwar bei jedem Verschlüsselungsvorgang neu.

### 4.4.2 Verschlüsseln der Nachricht

Zum Punkt „Verschlüsseln der Nachricht“ aus „Abbildung 4: Datenfluss im Verschlüsselungsautomaten“:

Der Verschlüsselungsautomat erhält über die in [2] Kapitel 7.4 beschriebene Schnittstelle eine versandbereite, transparente E-Mail. Diese wurde von einem beliebigen Programm, z.B. einem Mail-Client wie Outlook, erstellt.

Diese Nachricht wird nun nach dem S/MIME-Verfahren, das in RFC 5751 beschrieben ist, verschlüsselt, ehe es an das De-Mail-Gateway übergeben wird, das den eigentlichen Versand erledigt. Zum Einsatz kommt dabei der öffentliche Schlüssel des Empfängers der Nachricht, der aus dem ÖVZ des De-Mail-Providers stammt. Der Schlüssel wird bei jedem Versand neu beschafft. Die Verschlüsselung nutzt den Algorithmus RC2 CBC.

## 4.5 Anmerkungen

### 4.5.1 Anmerkungen zum Verfahren

Das Produkt bzw. Verfahren erzeugt im Kontext seines Einsatzes keine neuen datenschutzrechtlichen Risiken. Es speichert keine Daten und arbeitet als „Black Box“ mit einem festen Funktionsumfang, der auf Verschlüsselung begrenzt ist und weder von normalen noch privilegierten Nutzern der Plattformen oder Umsysteme verändert werden kann.

Es gibt Konfigurationsparameter, welche für die reklamierte Datenschutzgüte relevant sind, d.h. eine Fehlkonfiguration kann hier dazu führen, dass das Sicherheitslevel nicht mehr zwingend datenschutzkonform ist. Das betrifft:

- Die Nutzung des Verschlüsselungsautomaten ohne De-Mail
- Eine symmetrische Verschlüsselung der Mail (Anhangverschlüsselung unter Verwendung eines Einmalschlüssels) anstelle von S/MIME.

Diese sicherheitskritischen Parameter sind dokumentiert.

Demgegenüber eliminiert das Verfahren Risiken im E-Mailing allgemein und in De-Mail im Speziellen und leistet so einen Beitrag für mehr Datenschutz.