BSI – Technische Richtlinie

Bezeichnung: De-Mail
Anwendungsbereich: De-Mail
Kürzel: BSI TR 01201
Version: 1.7
Inhaltsverzeichnis

1 Einleitung .................................................................................................................................... 5
2 Aufbau der Technischen Richtlinie De-Mail .............................................................................. 6
3 De-Mail-Dienste .......................................................................................................................... 7
    3.1 Postfach- und Versanddienst (PVD) ..................................................................................... 7
    3.2 Dokumentenablage (DA) ....................................................................................................... 7
    3.3 Identitätsbestätigungsdienst (ID) .......................................................................................... 7
    3.4 Accountmanagement ............................................................................................................. 7
    3.5 IT-Basisinfrastruktur ............................................................................................................ 7
4 Interoperabilität der De-Mail-Dienste ......................................................................................... 8
5 Informationssicherheit ................................................................................................................ 9
6 Prüfung der De-Mail-Dienste ..................................................................................................... 10
    6.1 Funktionsprüfung der De-Mail-Dienste ............................................................................... 10
    6.2 Interoperabilitätsprüfung der De-Mail-Dienste .................................................................... 10
7 Rahmenbedingungen .................................................................................................................. 11
    7.1 Clientseitige Sicherheit ......................................................................................................... 11
    7.2 Unterstützung von Standard-Software ................................................................................ 11
    7.3 Graphische Benutzeroberflächen ....................................................................................... 12
    7.4 Speicheraufgaben ................................................................................................................ 12
    7.5 Allgemeine Verfügbarkeit der Anwendung und Daten ......................................................... 12
8 Abkürzungsverzeichnis .............................................................................................................. 13
9 Übersicht TR-Dokumente ......................................................................................................... 15
10 Literaturverzeichnis ................................................................................................................ 17

Abbildungsverzeichnis

Abbildung 1: Dokumentenstruktur Technische Richtlinie De-Mail (TR DM) (vgl. Zuordnung der
Bezeichnungen und der Modulnummern in Abschnitt 9) ............................................................. 6

Tabellenverzeichnis

Tabelle 1: Übersicht der Speicheraufgaben .................................................................................. 12
Tabelle 2: Abkürzungen ............................................................................................................... 14
Tabelle 3: Übersicht TR-Dokumente ........................................................................................... 16
Tabelle 4: Literaturverzeichnis .................................................................................................... 20

Bundesamt für Sicherheit in der Informationstechnik
1 Einleitung

Die Technische Richtlinie (TR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit dem Titel „Technische Richtlinie De-Mail“ stellt das Rahmenwerk der Testierung dar und beschreibt die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die De-Mail-Dienste erfüllen müssen, sowie zur Prüfung dieser Eigenschaften.

Die TR ist modular aufgebaut entsprechend der in De-Mail enthaltenen Dienste und das vorliegende Dokument referenziert auf dienstspezifische Module.
Die TR De-Mail des BSI umfasst die Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die die De-Mail-Dienstanbieter (DMDA) erfüllen müssen, sowie die Anforderungen zur Prüfung dieser Eigenschaften.


Weiterhin enthält jedes Modul Prüffälle (bis auf das Modul Informationssicherheit) zur Funktionalität, sowie teilweise zur Interoperabilität. Für die De-Mail-Dienste, die eine Kommunikation zwischen verschiedenen De-Mail-Diensten umfassen, sind zu verwendende Datenstrukturen und Übertragungsprotokolle definiert.
3 De-Mail-Dienste

3.1 Postfach- und Versanddienst (PVD)


3.2 Dokumentenablage (DA)


Der Dienst ist optional und muss nicht angeboten werden.

3.3 Identitätsbestätigungsdiendst (ID)


Der Dienst ist optional und muss nicht angeboten werden.

3.4 Accountmanagement


3.5 IT-Basisinfrastruktur

ÖVD, persönliches Adressbuch sowie IT-Basis-Dienste (Log-Informationen, Nutzung authentischer Zeitquellen und DNS) werden durch die sogenannte IT-Basisinfrastruktur den De-Mail-Diensten zur Verfügung gestellt. Der Dienst wird im Modul [TR DM IT-BInfra M] beschrieben.
4 Interoperabilität der De-Mail-Dienste

Die Spezifikation der notwendigen Datenstrukturen, Datenformate und Transportprotokolle erfolgt für die Dienste PVD [TR DM PVD M], ID [TR DM ID M] und IT-Basisinfrastruktur [TR DM IT-BInfra M].
5 Informationssicherheit

6 Prüfung der De-Mail-Dienste

6.1 Funktionsprüfung der De-Mail-Dienste

Nachfolgend sind Prüffälle spezifiziert, mit denen die Funktionalität von De-Mail geprüft werden kann.

Die Spezifikation der notwendigen Prüffälle erfolgt in den Modulen:
- Post- und Versanddienst [TR DM PVD FU-PS],
- Identifizierungsdienst [TR DM ID FU-PS],
- IT-Basisinfrastruktur [TR DM IT-BInfra FU-PS],
- Accountmanagement [TR DM ACM FU-PS],
- Dokumentenablage [TR DM DA FU-PS].

6.2 Interoperabilitätsprüfung der De-Mail-Dienste

Die Spezifikation der notwendigen Prüffälle erfolgt in den Modulen:
- Post- und Versanddienst [TR DM PVD IO-PS],
- Identifizierungsdienst [TR DM ID IO-PS],
- IT-Basisinfrastruktur [TR DM IT-BInfra IO-PS].
7 Rahmenbedingungen

In diesem Kapitel sind die Rahmenbedingungen beschrieben, die für alle Funktionen aller De-Mail-Dienste gelten.

7.1 Clientseitige Sicherheit

Im Allgemeinen kann De-Mail nur wenig Einfluss auf die Nutzerumgebung nehmen, da diese nicht im unmittelbaren Einflussbereich von De-Mail liegt. Der DMDA hat jedoch die Aufgabe, den Nutzer durch die folgenden beiden Bereichen zu unterstützen:

- Sensibilisierung und Beratung: Der Nutzer ist über bestehende Cybersicherheitsrisiken zur informieren und wie diese vermieden werden können. Es sind sowohl technische als auch organisatorische Maßnahmen zu nennen und Hilfestellungen zur Umsetzung anzubieten.

- Technische Produktlösungen: Der DMDA hat für seine Nutzer entsprechende technische Komponenten zu empfehlen. Hierzu wären mindestens folgende Komponenten für eine sichere Client-Lösungen zu betrachten:
  - Virenscanner-Produkte,
  - Personal-Firewall-Produkte,
  - Signaturerstellungs- bzw. -verifikationslösungen,
  - Ver-/Entschlüsselungslösungen,
  - Hardware-Token,
  - Chipkartenlesegeräte.

Die Nutzung der De-Mail-Dienste sollten derart gestaltet sein, dass

- eine Manipulation,
- eine Nutzung durch unberechtigte Personen oder Anwendungen,
- ein Einsehen, Löschen oder Manipulation der Daten durch unberechtigte Personen oder
- das Ausführen von Schadcode über die Anwendung,

auch vom Client des Nutzers aus, möglichst nicht erfolgen oder durch den Nutzer selbst verhindert und bemerkt werden kann.

7.2 Unterstützung von Standard-Software

7 Rahmenbedingungen

7.3 Graphische Benutzeroberflächen

Die graphische Oberfläche von De-Mail-Webanwendungen ist so zu gestalten, dass sie sich durch eine einfache Bedienung auszeichnen und die Darstellung der Daten und Funktionen übersichtlich ist. Die Basisfunktionalität muss innerhalb der Darstellung der Anwendung deutlich erkennbar sein.

Die Gestaltung der Web-Oberflächen von De-Mail sollte entsprechend den Gesetzgebungen zur Barrierefreiheit (Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV)) vorgenommen werden.

7.4 Speicheranforderungen


<table>
<thead>
<tr>
<th>Konto</th>
<th>Minimaler Speicherplatz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natürliche Personen</td>
<td>100 MB</td>
</tr>
<tr>
<td>Institutionen</td>
<td>100 MB</td>
</tr>
</tbody>
</table>

Tabelle 1: Übersicht der Speicheranforderungen

7.5 Allgemeine Verfügbarkeit der Anwendung und Daten

Es ist ein Regelbetrieb von 7x24 Stunden mit hoher Verfügbarkeit vorzusehen. Die Verfügbarkeit aller Dienste darf den im Rahmen-Sicherheitskonzept (vgl. [TR DM IS M]) festgelegten Wert nicht unterschreiten.
## 8 Abkürzungsverzeichnis

Es wird an dieser Stelle ein zentrales Abkürzungsverzeichnis geführt.

<table>
<thead>
<tr>
<th>Abkürzung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM</td>
<td>Accountmanagement</td>
</tr>
<tr>
<td>ALG</td>
<td>Application Level Gateway</td>
</tr>
<tr>
<td>BSI</td>
<td>Bundesamt für Sicherheit in der Informationstechnik</td>
</tr>
<tr>
<td>CSP</td>
<td>Crypto Service Provider</td>
</tr>
<tr>
<td>DA</td>
<td>Dokumentenablage</td>
</tr>
<tr>
<td>DBMS</td>
<td>Datenbankmanagementsystem</td>
</tr>
<tr>
<td>DM</td>
<td>De-Mail</td>
</tr>
<tr>
<td>DMDA</td>
<td>De-Mail-Diensteanbieter</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarisierte Zone</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>Ende-zu-Ende</td>
<td>Ende-zu-Ende</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>ID</td>
<td>Identitätsbestätigungsdienst</td>
</tr>
<tr>
<td>IT</td>
<td>Informationstechnik</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MESZ</td>
<td>Mitteleuropäische Sommerzeit</td>
</tr>
<tr>
<td>MEZ</td>
<td>Mitteleuropäische Zeit</td>
</tr>
<tr>
<td>nPA</td>
<td>neuer Personalausweis</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>ÖVD</td>
<td>Öffentlicher Verzeichnisdienst des DMDA</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>PVD</td>
<td>Postfach- und Versanddienst</td>
</tr>
</tbody>
</table>
### Abkürzungsverzeichnis

<table>
<thead>
<tr>
<th>Abkürzung</th>
<th>Beschreibung</th>
</tr>
</thead>
<tbody>
<tr>
<td>RZ</td>
<td>Rechenzentrum</td>
</tr>
<tr>
<td>SAK</td>
<td>(qualifizierte) Signaturanwendungskomponente</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SSEE</td>
<td>Sichere Signaturerstellungseinheit</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TR</td>
<td>Technische Richtlinie</td>
</tr>
<tr>
<td>URI</td>
<td>Universal Resource Identifier</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
<tr>
<td>W3C</td>
<td>World Wide Web Consortium</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
</tbody>
</table>

*Tabelle 2: Abkürzungen*
### Übersicht TR-Dokumente

<table>
<thead>
<tr>
<th>Nummer</th>
<th>Bezeichnung</th>
<th>Titel</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI-TR 01201 Teil 1</td>
<td>TR DM IT-BInfra M</td>
<td>Technische Richtlinie IT-Basisinfrastruktur Modul</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 1.1</td>
<td>TR DM IT-BInfra FU</td>
<td>Technische Richtlinie IT-Basisinfrastruktur Funktionalitätsspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 1.2</td>
<td>TR DM IT-BInfra FU-PS</td>
<td>Technische Richtlinie IT-Basisinfrastruktur Funktionalitätsprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 1.3</td>
<td>TR DM IT-BInfra Si</td>
<td>Technische Richtlinie IT-Basisinfrastruktur IT-Sicherheit</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 1.4</td>
<td>TR DM IT-BInfra IO</td>
<td>Technische Richtlinie IT-Basisinfrastruktur Interoperabilitätsspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 1.5</td>
<td>TR DM IT-BInfra IO-PS</td>
<td>Technische Richtlinie IT-Basisinfrastruktur Interoperabilitätsprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 2</td>
<td>TR DM ACM M</td>
<td>Technische Richtlinie Accountmanagement Modul</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 2.1</td>
<td>TR DM ACM FU</td>
<td>Technische Richtlinie Accountmanagement Funktionalitätsspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 2.2</td>
<td>TR DM ACM FU-PS</td>
<td>Technische Richtlinie Accountmanagement Funktionalitätsprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 2.3</td>
<td>TR DM ACM Si</td>
<td>Technische Richtlinie Accountmanagement IT-Sicherheit</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 3</td>
<td>TR DM PVD M</td>
<td>Technische Richtlinie Postfach- und Versanddienst Modul</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 3.1</td>
<td>TR DM PVD FU</td>
<td>Technische Richtlinie Postfach- und Versanddienst Funktionalitätsspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 3.2</td>
<td>TR DM PVD FU-PS</td>
<td>Technische Richtlinie Postfach- und Versanddienst Funktionalitätsprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 3.3</td>
<td>TR DM PVD Si</td>
<td>Technische Richtlinie Postfach- und Versanddienst IT-Sicherheit</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 3.4</td>
<td>TR DM PVD IO</td>
<td>Technische Richtlinie Postfach- und Versanddienst Interoperabilitätsspezifikation</td>
</tr>
<tr>
<td>Nummer</td>
<td>Bezeichnung</td>
<td>Titel</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 3.5</td>
<td>TR DM PVD IO-PS</td>
<td>Technische Richtlinie Postfach- und Versanddienst Interoperabilitätsprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 4</td>
<td>TR DM ID M</td>
<td>Technische Richtlinie Identitätsbestätigungsdienst Modul</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 4.1</td>
<td>TR DM ID FU</td>
<td>Technische Richtlinie Identitätsbestätigungsdienst Funktionalitätsspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 4.2</td>
<td>TR DM ID FU-PS</td>
<td>Technische Richtlinie Identitätsbestätigungsdienst Funktionalitätssprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 4.3</td>
<td>TR DM ID Si</td>
<td>Technische Richtlinie Identitätsbestätigungsdienst IT-Sicherheit</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 4.4</td>
<td>TR DM ID IO</td>
<td>Technische Richtlinie Identitätsbestätigungsdienst Interoperabilitätsspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 4.5</td>
<td>TR DM ID IO-PS</td>
<td>Technische Richtlinie Identitätsbestätigungsdienst Interoperabilitätssprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 5</td>
<td>TR DM DA M</td>
<td>Technische Richtlinie Dokumentenablage Modul</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 5.1</td>
<td>TR DM DA FU</td>
<td>Technische Richtlinie Dokumentenablage Funktionalitätsspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 5.2</td>
<td>TR DM DA FU-PS</td>
<td>Technische Richtlinie Dokumentenablage Funktionalitätssprüfspezifikation</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 5.3</td>
<td>TR DM DA Si</td>
<td>Technische Richtlinie Dokumentenablage IT-Sicherheit</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 6</td>
<td>TR DM IS M</td>
<td>Technische Richtlinie Informationssicherheit</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 6.1</td>
<td>TR DM IS GS</td>
<td>Technische Richtlinie Informationssicherheit nach ISO27001 auf der Basis von IT-Grundschatz</td>
</tr>
<tr>
<td>BSI-TR 01201 Teil 6.2</td>
<td>TR DM IS 27001</td>
<td>Technische Richtlinie Informationssicherheit auf Basis von ISO/IEC 27001</td>
</tr>
</tbody>
</table>

*Tabelle 3: Übersicht TR-Dokumente*
## Literaturverzeichnis

Es wird an dieser Stelle ein zentrales Literaturverzeichnis geführt.

<table>
<thead>
<tr>
<th>Bezeichnung</th>
<th>Titel</th>
</tr>
</thead>
<tbody>
<tr>
<td>[BSI 100-1]</td>
<td>BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)</td>
</tr>
<tr>
<td>[BSI 100-2]</td>
<td>BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise</td>
</tr>
<tr>
<td>[BSI 100-3]</td>
<td>BSI-Standard 100-3: Risikoanalyse auf der Basis von IT Grundschutz</td>
</tr>
<tr>
<td>[ETSI TS 102 231]</td>
<td>Electronic Signatures and Infrastructures (ESI) – Provision of harmonized Trust-service status information (Ref: RTS/ESI-000083)</td>
</tr>
<tr>
<td>[ICAO-MRTD]</td>
<td>ICAO – Doc 9303 Machine readable Travel Documents- Appendix 2 to Section IV 1 to Section III, Appendix 3 to Section III</td>
</tr>
<tr>
<td>Bezeichnung</td>
<td>Titel</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>[RFC 2119]</td>
<td>S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, 1997</td>
</tr>
<tr>
<td>[RFC 2487]</td>
<td>SMTP Service Extension for Secure SMTP over TLS</td>
</tr>
<tr>
<td>[RFC 2782]</td>
<td>A. Gulbrandsen, P. Vixie, L. Esibov RFC 2782: A DNS RR for specifying the location of services (DNS SRV)</td>
</tr>
<tr>
<td>[RFC 2822]</td>
<td>RFC 2822 Internet Message Format</td>
</tr>
<tr>
<td>[RFC 3851]</td>
<td>Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1, RFC 3851</td>
</tr>
<tr>
<td>[RFC 3958]</td>
<td>L. Daigle, A. Newton RFC 3958: Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)</td>
</tr>
<tr>
<td>[RFC 4056]</td>
<td>RFC 4056 „Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)“</td>
</tr>
<tr>
<td>[RFC 4398]</td>
<td>RFC 4398 „Storing Certificates in the Domain Name System (DNS)“</td>
</tr>
<tr>
<td>Bezeichnung</td>
<td>Titel</td>
</tr>
<tr>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>[RFC 5280]</td>
<td>Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 5280</td>
</tr>
<tr>
<td>[RFC 6376]</td>
<td>RFC 6376 „DomainKeys Identified Mail (DKIM) Signatures“</td>
</tr>
<tr>
<td>[RFC 8551]</td>
<td>Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0, RFC 8551</td>
</tr>
<tr>
<td>Bezeichnung</td>
<td>Titel</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>[XAdES]</td>
<td>ETSI TS 101 903 XAdES</td>
</tr>
</tbody>
</table>

*Tabelle 4: Literaturverzeichnis*