Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	IT-Basisinfrastruktur Funktionalitätsspezifikation
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 1.1
Version:	1.3

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: de-mail@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Dieses Modul beinhaltet die funktionalen Spezifikationen der IT-Basisinfrastruktur und ist Bestandteil von [TR DM IT-BInfra M].

In diesem Modul werden die zwingenden Anforderungen an die IT-Basisinfrastruktur von De-Mail technikneutral beschrieben. eine Spezifikation von Protokollen und zugehörigen Parametern erfolgt nur dort, wo dies aus funktionaler Sicht explizit erforderlich ist.

2 Öffentlicher Verzeichnisdienst (ÖVD)

Im ÖVD können Daten eines Nutzers vom DMDA veröffentlicht werden, soweit der Nutzer dies ausdrücklich verlangt. Andere De-Mail-Nutzer können auf diese zugreifen und in dem Datenbestand suchen.

2.1 Allgemeine Anforderungen

Jeder DMDA muss einen eigenen ÖVD betreiben. Für die Nutzer muss eine Suche über die ÖVD aller DMDA möglich sein. Die Suche darf nur für authentisierte Nutzer möglich sein. Suchanfragen stellt der Nutzer dazu immer an den ÖVD seines eigenen DMDA. Dieser muss die Suchanfragen für den Nutzer an den zuständigen ÖVD des fremden DMDA weiterleiten.

Die Suche muss erfolgen können für

- natürliche Personen anhand [Vorname, Name, DMDA] oder [Name, DMDA],
- Institutionen anhand [Name, DMDA],
- und jeweils anhand der [De-Mail-Adresse].

Weitere Suchmöglichkeiten können durch den DMDA angeboten werden.

Es werden maximal 200 Einträge zurückgesendet. Der ÖVD des Nutzers präsentiert diesem schließlich das Ergebnis. Die Ergebnisse müssen diskriminierungsfrei sortiert werden, d.h. die Suchergebnisse müssen anhand objektiver Kriterien aufgelistet werden. Der Nutzer hat somit selbst keinen unmittelbaren Zugriff auf die ÖVD anderer DMDAs.

Das Ergebnis einer Abfrage muss spätestens nach einer Gesamtzeit von 20 Sekunden geliefert werden. Jeder DMDA muss innerhalb von 10 Sekunden (von der Anfrage bis einschließlich der Übermittlung des Ergebnisses) geantwortet haben.

Dem Nutzer ist nur die Suche und der lesende Zugriff auf die Informationen des ÖVD gestattet. Schreibenden bzw. löschenden Zugriff haben ausschließlich DMDA-interne Dienste, z. B. das Accountmanagement.

Änderungen an Daten im Accountmanagement sind im ÖVD zu übernehmen. Dazu gehören:

- Neuer Eintrag (De-Mail-Konto freigeschaltet und Nutzer hat Attribute zur Veröffentlichung freigegeben),
- Eintrag löschen (Nutzer möchte Eintrag entfernen oder Konto wurde aufgelöst),
- Attribute ändern (Nutzer hat Attribute geändert),
- Attribute löschen (Nutzer hat die Freigabe für ÖVD zurückgezogen).

3 Persönliches Adressbuch

Das persönliche Adressbuch dient der dezentralen Speicherung von Kontakten bzw. Adressierungsinformationen, die innerhalb der einzelnen De-Mail-Dienste verwendet werden können. Das persönliche Adressbuch ist unabhängig von dem ÖVD. Mittels eines persönlichen Adressbuchs kann der Nutzer seine Kontakte verwalten und über die De-Mail-Dienste nutzen. Zur Verwaltung zählen

- neue Kontakte anlegen,
- bestehende Kontakte löschen und
- Attribute innerhalb eines bestehenden Kontaktes ändern.

Für jeden Nutzer kann ein persönliches Adressbuch mittels Web-Applikation zur Verfügung gestellt werden.

Es müssen mindestens alle Informationen, die auch für den ÖVD definiert sind, gespeichert werden können (vgl. [TR DM IT-BInfra IO]). Zusätzliche Attribute können gespeichert werden. Es kann die Erstellung von Verteilerlisten angeboten werden und innerhalb der De-Mail-Dienste genutzt werden.

Im persönlichen Adressbuch kann wie im ÖVD gesucht werden.

4 Nutzung von IT-Basisdiensten

Eine Manipulation von Diensten und deren Informationen und Daten, einschließlich der Meta-Informationen, muss von dem DMDA durch geeignete Maßnahmen verhindert werden.

4.1 Protokollierungsinformationen

Alle Informationen, die für die Dienste und die Nachweise benötigt werden, sind innerhalb der DMDA-Infrastruktur in Protokollierungsdatenbanken integer und authentisch zu speichern. Protokollierungsdaten müssen so gespeichert werden, dass sie für notwendige und berechtigte Auswertungen verfügbar sind. Lesenden Zugriff auf die Protokollierungsdaten erhalten die jeweiligen berechtigten Personen. Ein unberechtigtes teilweises oder komplettes Löschen ist durch geeignete Maßnahmen zu verhindern.

5 Zusammenwirken der DMDA

Die DMDA sind verpflichtet, untereinander zusammenzuarbeiten. Die technische Zusammenarbeit hinsichtlich der Funktionalität bezieht sich dabei auf folgende Aspekte:

- die Übermittlung von De-Mails an den jeweiligen DMDA, der innerhalb der Empfängeradresse referenziert ist;
- die Entgegennahme von De-Mails durch den DMDA, der innerhalb der Empfängeradresse referenziert ist;
- die Übermittlung von Eingangs- und Abholbestätigungen an den Absender einer De-Mail;
- die Übermittlung von Anfragen an den ÖVD des DMDAs, der innerhalb der Suchanfrage referenziert ist;
- die Entgegennahme von Anfragen von anderen DMDAs hinsichtlich des ÖVD und die Übermittlung der Antwort;
- die Übernahme von Antworten zu Anfragen an den ÖVD des DMDAs, wenn sich die Antwort auf die Anfrage bezieht;
- die Übermittlungen von Meldungen, die bei bestimmten Konstellationen des Prozessablaufes (z.B. ungültige De-Mail-Adresse) erzeugt werden können.