Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	Postfach- und Versanddienst IT-Sicherheit
Anwendungsbereich:	De-Mail
Kürzel:	BSI TR 01201 Teil 3.3
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
© Bundesamt für Sicherheit in der Informationstechnik 2017

Inhaltsverzeichnis

1 Einleitung 4
2 IT-Strukturanalyse 5
2.1 Erfassung des IT-Verbundes 5
3 Bedrohungen 6
3.1 Bedrohung durch Schadsoftware 6
3.2 Abstreiten der Kommunikation 6
4 Sicherheitsziele 7
4.1 Schutz des Nutzers vor Schadsoftware 7
4.2 Vertrauliche Speicherung und Verarbeitung der Nachrichten 7
4.3 Nachvollziehbarkeit der Kommunikation 7
5 Anforderungen 8
5.1 Prüfung auf Schadsoftware 8
5.2 Kryptokonzept 8
5.2.1 Integritätssicherung 8
5.2.2 Prüfung der Integrität 8
5.2.3 Verschlüsselung von Nachrichten 8
5.2.4 Entschlüsselung von Nachrichten 8
5.2.5 Datenspeicherung 8
5.3 Erstellung von Bestätigungen 9
5.4 Prüfen und Setzen von Metadaten 9

1 Einleitung

Dieses Modul beinhaltet die IT-Sicherheitsanforderungen, die über die generellen Anforderungen aus dem Modul [TR DM Si M] hinausgehen und speziell für den PVD anzuwenden sind, und ist Bestandteil von [TR DM PVD M].

2 IT-Strukturanalyse

Die Grundlage für die Erarbeitung dieses Moduls bildet die in [TR DM Si ÜK] angenommene Netzinfrastruktur eines DMDA.

Bei der Erstellung des realen IT-Sicherheitskonzepts sind die hier enthaltenen Bedrohungen, Sicherheitsziele, zwingenden Anforderungen und Empfehlungen zu berücksichtigen. Näheres regelt [TR DM Si M].

2.1 Erfassung des IT-Verbundes

In diesem Modul wird auf den IT-Verbund verwiesen, der bereits in [TR DM Si ÜK] skizziert ist.

3 Bedrohungen

Es werden in diesem Abschnitt nur die Bedrohungen für den PVD betrachtet, die sich zusätzlich zu den Bedrohungen aus [TR DM Si ÜK] durch die Funktionalität des PVD ergeben.

3.1 Bedrohung durch Schadsoftware

Über elektronische Nachrichten kann Schadsoftware verbreitet werden. Dies kann beim Empfänger erhebliche Schäden, beispielsweise durch den Verlust von Daten oder durch die Kompromittierung von Daten, verursachen. Die Gefahr droht dem Rechnersystem des Nutzers.

3.2 Abstreiten der Kommunikation

Ein Nutzer kann die Kommunikation mit einem anderen Nutzer abstreiten. Er kann behaupten, dass er eine Nachricht nicht erhalten hat.

4 Sicherheitsziele

Im Folgenden werden weitergehende Sicherheitsziele des PVD beschrieben, die über die in [TR DM Si ÜK] Aufgeführten gelten.

4.1 Schutz des Nutzers vor Schadsoftware

Der Nutzer muss durch geeignete Maßnahmen vor Schäden durch Schadsoftware geschützt werden.

4.2 Vertrauliche Speicherung und Verarbeitung der Nachrichten

Es ist durch geeignete Maßnahmen sicherzustellen, dass die Möglichkeit der Einsichtnahme des Nachrichteninhalts durch Unbefugte (u.a. auch Innentäter) verhindert wird.

4.3 Nachvollziehbarkeit der Kommunikation

Der Versand und die Zustellung einer Nachricht müssen für den Absender nachvollziehbar sein, so dass dieser seine gesamte De-Mail-Kommunikation auch gegenüber Dritten nachweisen kann (vgl. [TR DM PVD FU]).

5 Anforderungen

5.1 Prüfung auf Schadsoftware

Durch geeignete Maßnahmen ist sicherzustellen, dass Nachrichtenentwürfe, die vom Absender dem Postfach- und Versanddienst übergeben werden, unmittelbar nach Übermittlung auf Schadsoftware geprüft werden.

5.2 Kryptokonzept

5.2.1 Integritätssicherung

Alle Nachrichten werden gegen unbefugte Veränderungen insoweit geschützt, als dass unbefugte Veränderungen zuverlässig erkannt werden können (vgl. [TR DM PVD FU]).

5.2.2 Prüfung der Integrität

Der PVD des Empfängers prüft bei Abruf der Nachrichten durch den Empfänger die Integrität der Nachrichten. Ist das Prüfergebnis negativ, so ist mit vorab festgelegten Maßnahmen darauf zu reagieren.

5.2.3 Verschlüsselung von Nachrichten

Nachrichten werden durch den PVD des Absenders unmittelbar nach Anbringen der Transportsicherung verschlüsselt gespeichert und übertragen. Die Metadaten werden dabei nicht verschlüsselt.

Die Verschlüsselung der Daten hat unmittelbar nach Eingang auf den Systemen des DMDA zu erfolgen.

Die Gültigkeit der öffentlichen Schlüssel muss regelmäßig geprüft werden.

5.2.4 Entschlüsselung von Nachrichten

Die Entschlüsselung darf ausschließlich zur Prüfung auf Schadsoftware und zur Auslieferung an den Nutzer zu durchgeführt werden. Dieser Vorgang erfolgt automatisiert.

5.2.5 Datenspeicherung

Die Speicherung der Daten beim DMDA muss verschlüsselt erfolgen.

Es gelten folgende Regelungen für die Daten:

- langfristige Speicherung (z.B. Nachrichten im Postfach)
  - Die Daten müssen einzeln oder gesammelt verschlüsselt und vor unberechtigtem Zugriff gespeichert werden
- kurzfristige Speicherung (z.B. in Warteschlange bei Virenscanner)
  - Das Dateisystem, auf dem die Daten abgelegt werden, muss verschlüsselt sein.

5.3 Erstellung von Bestätigungen

Der DMDA erstellt sowohl Versand-, Eingangs- und Abholbestätigungen.

5.4 Prüfen und Setzen von Metadaten

Der DMDA prüft die korrekte Verwendung von Metadaten, setzt weitere Metadaten und ersetzt nicht-korrekte Metadaten vor der Erstellung von Nachrichten.