Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheit im De-Mail-Verbund

Voraussetzungen der Akkreditierung als De-Mail-Provider

Jens Mehrfeld / Dr. Astrid Schumacher
-Projektleitung De-Mail im BSI-

De-Mail und die Justiz – Chancen für den Elektronischen Rechtsverkehr

Berlin 03. Februar 2011

De-Mail-Konzept

Zuverlässige und geschützte Infrastruktur

- E-Mail PLUS Sicherheit PLUS Datenschutz

Definierte **De-Mail-Dienste angeboten von dafür zugelassenen Anbietern**

- nachgewiesene Sicherheit & Vertrauenswürdigkeit durch umfangreiche Vorab-Prüfungen

→ Einführung eines **Akkreditierungsverfahrens** für Diensteanbieter von De-Mail-Diensten, um die **Vertraulichkeit der Kommunikation & die Identität der Kommunikationspartner** zu gewährleisten.

Gesetzlicher Rahmen: De-Mail-Gesetzentwurf

§ 17 I 1:

Diensteanbieter, die De-Mail-Dienste anbieten wollen, müssen sich auf schriftlichen Antrag von der zuständigen Behörde akkreditieren lassen.

§ 2:

Zuständige Behörde (…) ist das BSI

§ 17 I 2:

Die Akkreditierung ist zu erteilen, wenn der De-Mail-Diensteanbieter nachweist, dass er die Voraussetzungen nach § 18 erfüllt (...).

Voraussetzungen der Akkreditierung, § 18

Nr. 1: Zuverlässigkeit und Fachkunde

Nr. 2: Geeignete Deckungsvorsorge

Nr. 3: Technische und organisatorische Anforderungen an die Pflichten nach den §§ 3 bis 13 und 16 (...)

Nr. 4: Erfüllung der datenschutzrechtlichen Anforderungen bei Gestaltung und Betrieb der Dienste

→ Formale Grundlage für die Umsetzung von § 18 wird ein von der zuständigen Behörde veröffentlichtes Akkreditierungsschema mit Verfahrensbeschreibung sein, in dem die erforderlichen Nachweise und das konkrete Vorgehen festgelegt sind

Technische & Organisatorische Anforderungen

§ 18 II 2: Die Einhaltung des Stands der Technik wird vermutet, wenn die **Technische Richtlinie 01201 De-Mail des BSI** (…) eingehalten wird.

→ Bestandteil des Gesetzes

→ BSI hat Hoheit über die TR; nach § 18 II 3 ist vor wesentlichen Änderungen der Ausschuss Standardisierung iSv § 22 anzuhören

→ umfasst alle technisch-organisatorischen Anforderungen an Funktionalität, Interoperabilität und Sicherheit für alle (obligatorischen & optionalen) Dienste

→ stellt Rahmenbedingungen auf und erleichtert die praktische Umsetzung in Prüfvorschriften

TR - Aufbau

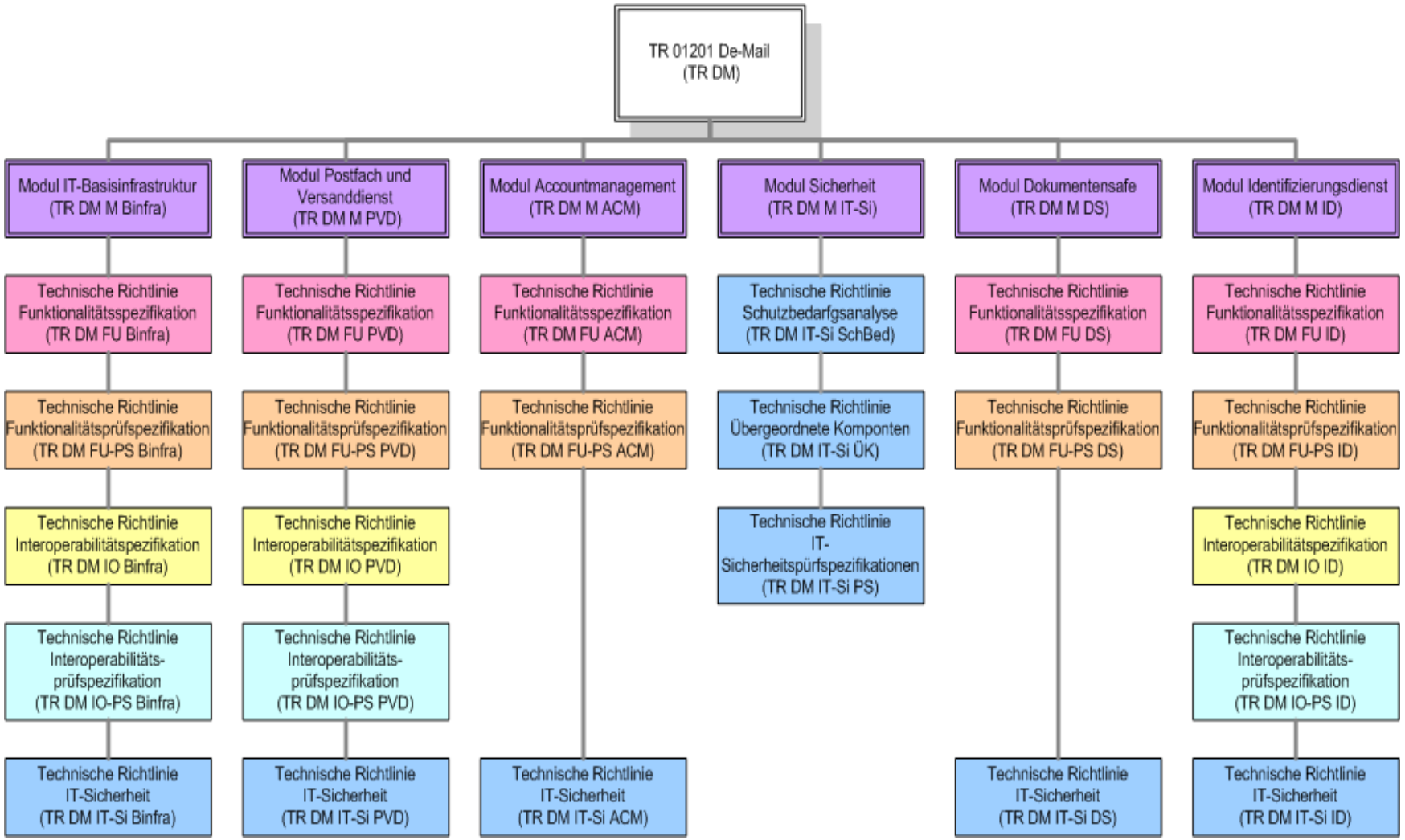
Wurzeldokument

- Allgemeine Beschreibung des Verfahrens und der einzelnen Module

6 Module

- IT-Basisinfrastruktur
- Postfach- und Versanddienst
- Accountmanagement
- Dokumentensafe
- Identifzierungsdienst
- IT-Sicherheit

TR-Landschaft



IT-Sicherheit

Grundlage: **ISO 27001 auf Basis von IT-Grundschutz**

Prüfungen erweitert um **De-Mail spezifische Anforderungen** u.a.:

- Definition von Dienste übergreifenden Sicherheitsanforderungen
- Sicherheitsmanagement & Sicherer Betrieb der Infrastruktur
- Maßnahmen gegen Verlust der Vertraulichkeit, Integrität und Verfügbarkeit, unberechtigte Nutzung
- Rollenkonzepte
- Penetrationstests und IS-Revision
- Verschlüsselte Übertragung zum Nutzer und zwischen den Diensteanbietern

Ergänzt um **datensicherheitsbezogene Aspekte** im Datenschutz-Nachweis

Accountmanagement

Im Accountmanagement werden **alle Aspekte im Zusammenhang mit den Benutzerdaten** geregelt.

Dazu zählen:

- Identifizierung
- Registrierung
- Verwaltung der Daten

Dies gilt sowohl für natürliche Personen als auch Institutionen (Unternehmen, öffentliche Stellen, usw.)

Postfach- und Versanddienst

Beschreibung / Spezifikation von:

- Anforderungen bei den Versandoptionen „Persönlich“ und „Absenderbestätigt“
- Funktionsweise und Formate der Bestätigungsnachrichten
  - Versand-, Eingangs- und Abholbestätigung
- Anforderungen an die Nachrichtenverwaltung
- Anforderungen an die Vertraulichkeit und Integrität bei Übertragung der Nachrichten

IT-Basisinfrastruktur

Anforderungen an die **allgemeine Infrastruktur** und Dienste- übergreifenden Funktionen

- Aufbau, Funktionen des Verzeichnisdienstes
- Ablauf der Abfrage des Verzeichnisdienstes zwischen den Diensteanbietern
- Persönliches Adressbuch der Nutzer
- Schadsoftwareprüfung
- Domainverwaltung

Dokumentenablage - optional

Beschreibung der **Funktionen** die die Dokumentenablage anbieten muss:

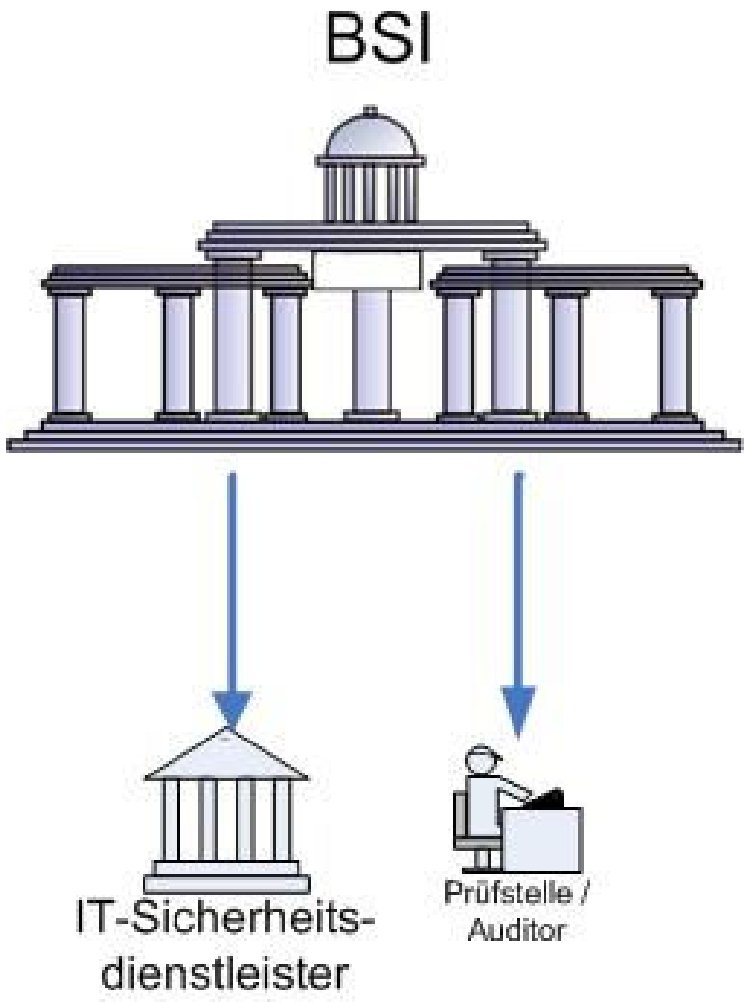
- Einstellen von Dokumenten
- Verwaltung der Dokumenten in Ordnern / Kategorien
- Löschen von Dokumenten
- Verschlüsselte Ablage der Dokumente auf den Systemen des Dienste

Identifizierungsdienst - optional

Beschreibung der Funktionen zum Versand und zu den Formaten der **Ident-Karten**

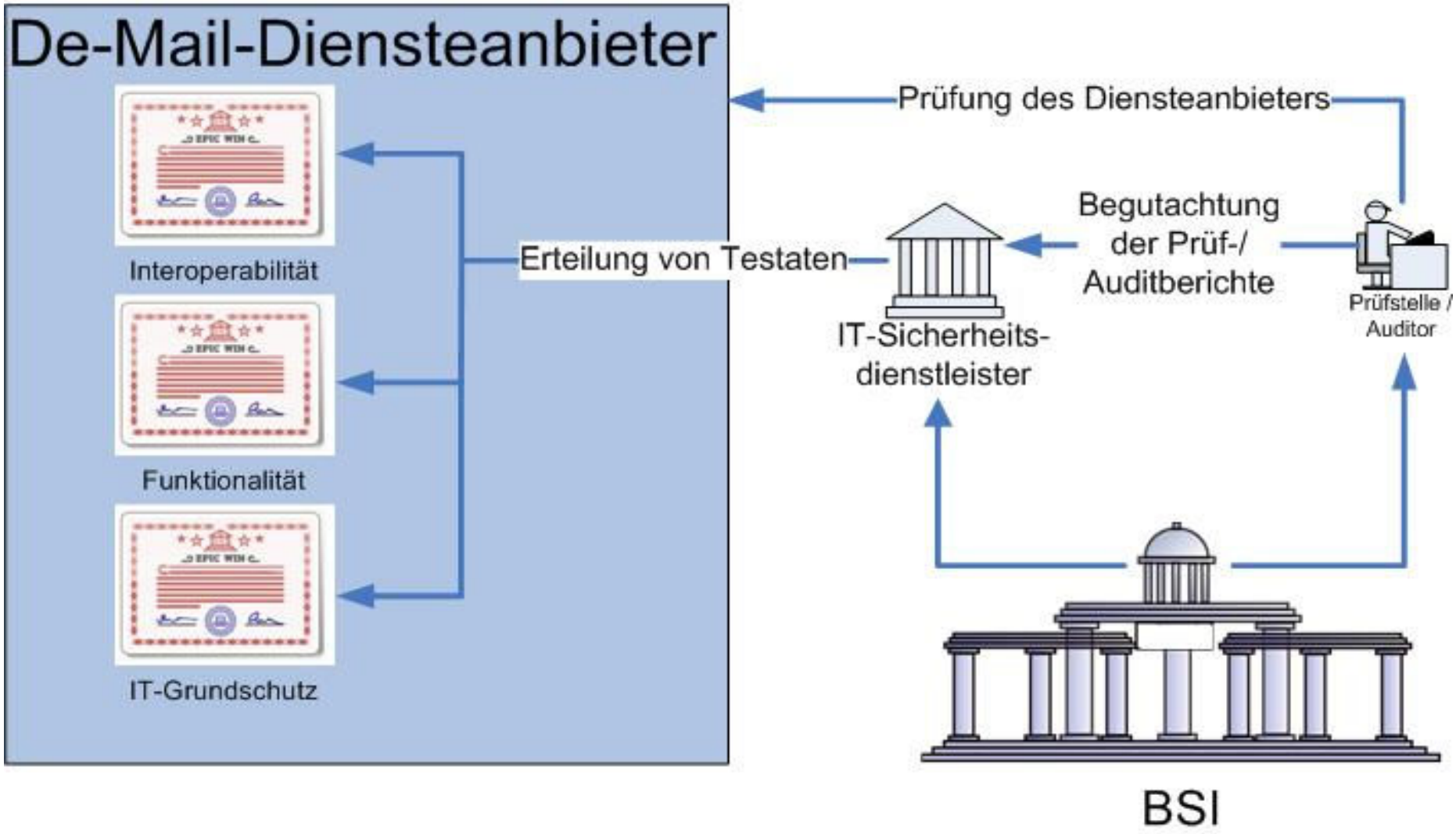
- Für natürliche Personen und Institutionen mit Name und Adresse
- Altersnachweise (ü16, ü18 oder konkretes Alter)
- Bestätigung der De-Mail-Adresse

Vertrauensanker: Prüfungen



- BSI z**ertifiziert IT-Sicherheitsdienstleister**, die Testate ausstellen
- BSI **zertifiziert Auditoren und anerkennt Prüfstellen**, die die erforderlichen Prüfungen durchführen und Berichte erstellen
- Ziel: **Prüfung des DMDA** auf Erfüllung der Anforderungen aus § 18 De-Mail-GE

Erbringung von Nachweisen



Akkreditierung

Ein Diensteanbieter legt der zuständigen Behörde folgende Unterlagen vor:

- alle Einzel-Nachweise
- Nachweis Deckungsvorsorge
- Nachweis Zuverlässigkeit & Fachkunde

Die zuständige Behörde

- prüft Unterlagen auf Vollständigkeit & Plausibilität
- erteilt Akkreditierung und vergibt
- das De-Mail Gütezeichen

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Jens Mehrfeld/Dr. Astrid Schumacher
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5371
Fax: +49 (0)22899-10-9582-5371

jens.mehrfeld@bsi.bund.de
astrid.schumacher@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de