Bundesamt
für Sicherheit in der
Informationstechnik

BSI TR-03108

Sicherer E-Mail-Transport

Anforderungen an E-Mail-Diensteanbieter für einen sicheren Transport von E-Mails

Version: 0.9 Entwurf
Datum: 20.08.15

Änderungshistorie

Version	Datum	Name	Beschreibung
0.9	20.08.15	BSI/Bierhoff	Erster Öffentlicher Entwurf

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

Inhaltsverzeichnis

Abbildungen

Tabellen

1 Einleitung

Ein Großteil unserer Kommunikation findet mittlerweile digital statt. Die E-Mail hat sich dabei als wichtiges Medium zum Austausch von Nachrichten etabliert. Häufig werden diese Nachrichten jedoch ohne die Anwendung von IT-Sicherheitsmaßnahmen, wie Verschlüsselung und Signatur, versandt. Dies liegt auch daran, dass Maßnahmen, wie Ende-zu-Ende-Verschlüsselung auf Grund des komplexen und aufwändigen Schlüsselmanagements, bisher keine breite Nutzerakzeptanz finden.

Die Technische Richtlinie richtet sich in diesem Zusammenhang an E-Mail-Diensteanbieter (EMDA). Sie gibt diesen die Möglichkeit, unabhängig von den IT-Fähigkeiten ihrer Nutzer, ein höheres Sicherheitsniveau anzubieten. Dieses Sicherheitsniveau soll, unter den konform zu dieser Technischen Richtlinie arbeitenden EMDAn, vollkommen transparent für deren Nutzer umgesetzt werden.

1.1 Konzept

Die Basis für die Anforderungen dieser Technischen Richtlinie ist ein Sicherheitskonzept, welches gemäß den Festlegungen in *Kapitel 3.1: Sicherheitskonzept* vom EMDA erstellt und umgesetzt wird. Darüber hinaus werden in der Technische Richtlinie spezifische fachliche und generelle Anforderungen an den EMDA formuliert, welche gemäß *Kapitel 3.2: Fachliche Anforderungen* und *Kapitel 3.3: Weitere Anforderungen* vom EMDA umgesetzt werden müssen. Ein Überblick über das zugrunde liegende Konzept, findet sich in der folgenden *Abbildung 1: Konzeptionelle Übersicht der Anforderungen*.

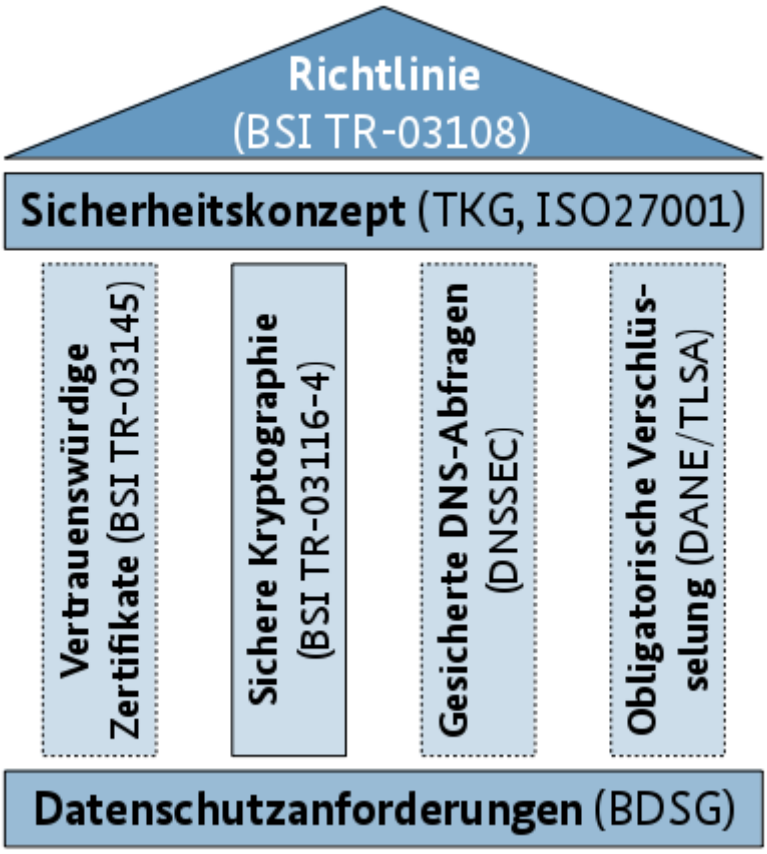

Abbildung 1: Konzeptionelle Übersicht der Anforderungen

Optional oder nach einer Übergangsfrist vom EMDA umzusetzende Anforderungen werden in der *Abbildung 1: Konzeptionelle Übersicht der Anforderungen* durch eine punktierte Umrandung dargestellt.

Die Anforderungen dieser Technische Richtlinie richten sich ausschließlich an einzelne EMDA. Ein Verbund oder ein Zusammenschluss von EMDAn wird nicht betrachtet. Durch die Formulierung von Anforderungen an einzelne EMDA und deren Schnittstellen soll eine Vergleichbarkeit erreicht werden. Des Weiteren soll hierüber eine höhere Verbreitung von sicheren Kommunikationsverbindungen und sicher betriebenen E-Mail-Diensten erzielt werden, um letztlich die Sicherheit der E-Mail-Infrastruktur insgesamt zu erhöhen.

Einen Überblick über das mit dieser Technischen Richtlinie angestrebte Szenario der Kommunikation zwischen EMDAn zeigt die *Abbildung 2: Übersicht der Inter-EMDA-Kommunikation*.

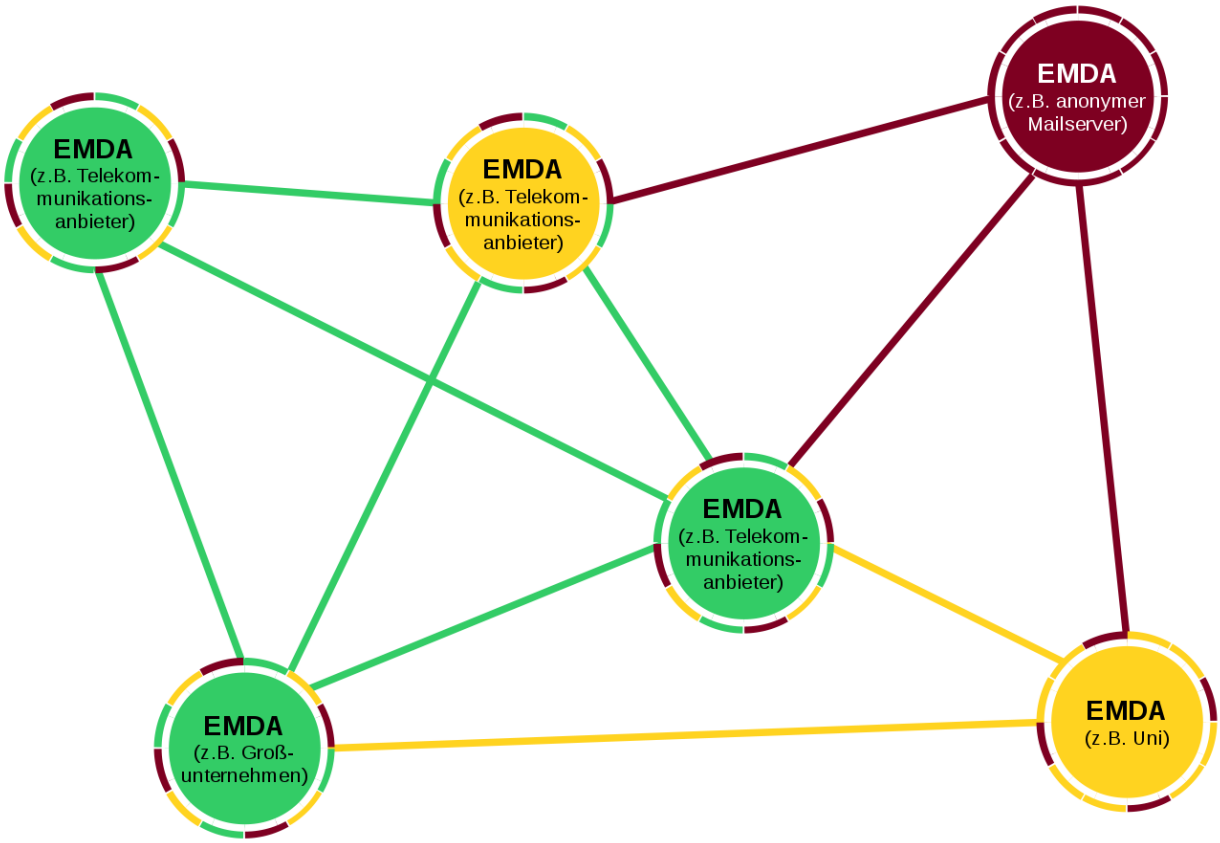

Abbildung 2: Übersicht der Inter-EMDA-Kommunikation

Neben anderen zertifizierten EMDAn kommuniziert ein zertifizierter EMDA zum Beispiel auch mit anderen:

- EMDAn, welche nicht zertifiziert sind, aber dennoch ein Sicherheitskonzept haben und Schnittstellen mit hochwertiger Kryptographie anbieten (gelber Kreis, grüne Schnittstelle),
- EMDAn, welche ein Sicherheitskonzept haben und schwache Kryptographie anbieten (gelber Kreis, gelbe Schnittstelle) und
- EMDAn, welche keinerlei Sicherheit implementiert haben (roter Kreis, rote Schnittstelle).

Die *Abbildung 2: Übersicht der Inter-EMDA-Kommunikation* sowie die oben genannte Liste decken nicht alle möglichen Konstellationen ab, lassen aber die Komplexität der Kommunikationsbeziehungen erahnen. Es wird auch deutlich, dass zertifizierte EMDAn neben Schnittstellen zu anderen zertifizierten EMDAn parallel Schnittstellen zu EMDAn haben, die weniger oder keinerlei Sicherheitsmaßnahmen ergreifen.

1.2 Zertifizierung

Ein EMDA hat die Möglichkeit im Rahmen einer Zertifizierung die Konformität zu den Anforderungen dieser Technischen Richtlinie nachzuweisen. Durch die Zertifizierung kann er eine besondere Vertrauenswürdigkeit nachweisen und damit die Rolle eines zertifizierten EMDA erfüllen. Für die Zertifizierung nach dieser Technischen Richtlinie existieren grundsätzlich zwei Szenarien.

1.2.1 Zertifizierung auf Basis ISO27001

Sofern der Antragsteller (EMDA) die Konformität zu dieser Technischen Richtlinie im Rahmen einer Zertifizierung nach [ISO/IEC 27001] nachweisen möchte, sind dafür zwei Schritte notwendig. Zunächst muss der Antragsteller ein Audit nach [ISO/IEC 27001] bei einem akkreditierten Auditor durchlaufen. Erst nach der erfolgreichen Erteilung eines entsprechenden Zertifikats werden die in *Kapitel 3: Anforderungen* definierten Anforderungen als sogenannte Controls geprüft. Kann auch für die Anforderungen eine Konformität festgestellt werden, wird auch ein Zertifikat gemäß den Anforderungen dieser Technischen Richtlinie erteilt. Der Antragsteller erhält damit zwei getrennt erteilte Zertifikate. Eines für die Konformität nach [ISO/IEC 27001] und eines für die Konformität zu dieser Technischen Richtlinie.

1.2.2 Zertifizierung nach Technischer Richtlinie

Die Konformität zu dieser Technischen Richtlinie kann auch außerhalb einer Zertifizierung nach [ISO/IEC 27001] erfolgen. Hierzu wendet sich der Antragsteller (EMDA) an eine durch das BSI akkreditierte Prüfstelle. Es gelten dabei die Anforderungen aus *Kapitel 3: Anforderungen* mit den dort definierten Übergangsregelungen und Verpflichtungen. Die Anforderung an ein Sicherheitskonzept gemäß [TKG 109] ist entsprechend verpflichtend umzusetzen und ersetzt das nach [ISO/IEC 27001] geforderte ISMS.

2 Infrastruktur

In diesem Kapitel werden die Teilnehmer der E-Mail-Infrastruktur, deren Schnittstellen zueinander und die Aufgaben des EMDA gemäß dieser Technischen Richtlinie definiert.

2.1 Teilnehmer und zugehörige Komponenten

Die folgende *Abbildung 3: Beteiligte Infrastrukturkomponenten* zeigt die an der Infrastruktur beteiligten Komponenten, sowie deren Kommunikationsbeziehungen zueinander.

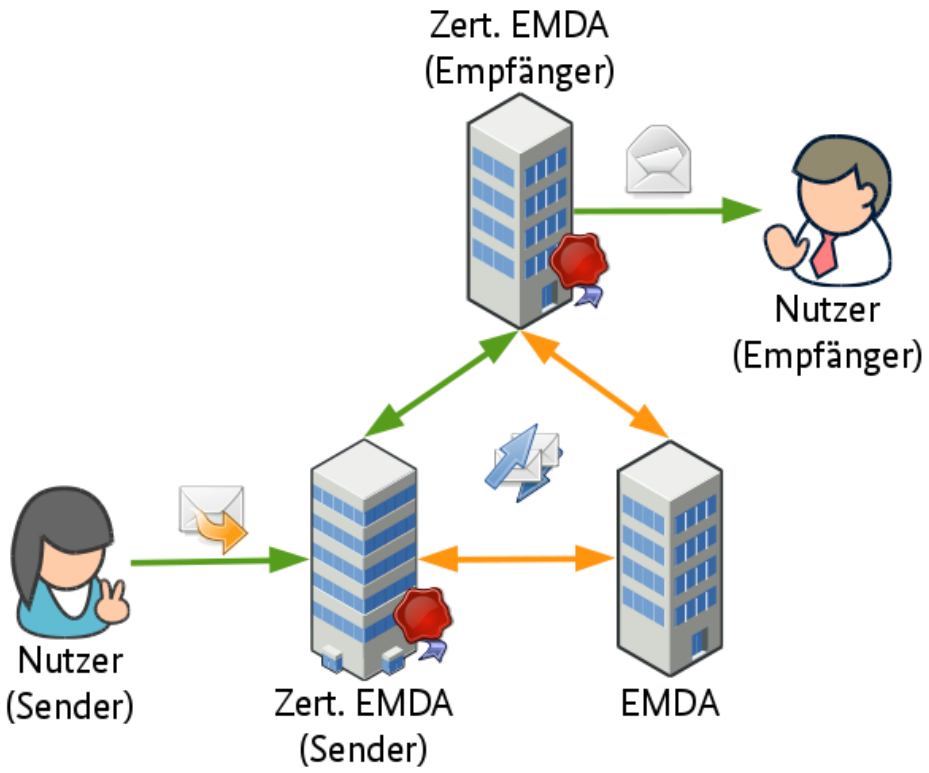

Abbildung 3: Beteiligte Infrastrukturkomponenten

Ziel der hier beschriebenen Anforderungen ist es, eine Infrastruktur zu schaffen, in der sichere Verbindungen zwischen zertifizierten EMDAn und dem Nutzer etabliert werden. Durch die sichere Kommunikation von Komponente zu Komponente wird eine Punkt-zu-Punkt-Sicherheit vom Sender bis zum Empfänger einer E-Mail erreicht. Es wird hierbei davon ausgegangen, dass die Systeme der einzelnen EMDA über ein grundsätzlich offenes Netzwerk (Internet) und auch mit nicht zertifizierten EMDAn kommunizieren. Auch in der Kommunikation mit nicht zertifizierten EMDAn sollen durch die hier formulierten Anforderungen die Voraussetzungen geschaffen werden, um möglichst sichere Verbindungen zu realisieren.

Die einzelnen Komponenten, die an der Kommunikation beteiligt sind, und deren Rollen innerhalb der Infrastruktur werden in den folgenden Kapiteln betrachtet. Im Kontext dieser Technischen Richtlinie können Sicherheitsaussagen naturgemäß nur für den Austausch von E-Mails zwischen zertifizierten EMDAn und deren Nutzern getroffen werden. In *Kapitel 2.2.2: Transparenz* werden die für eine solche Sicherheitsaussage notwendigen Regelungen getroffen.

2.1.1 Nutzer

Der Nutzer ist der Endanwender, der hier beschriebenen Infrastruktur. Er nutzt die Dienste eines oder mehrerer EMDA zum Versand und Empfang seiner E-Mails. Es wird an dieser Stelle bewusst nicht zwischen den Rollen Empfänger und Sender unterschieden, da für beide Rollen aus Sicht des EMDA die gleichen Sicherheitsmaßnahmen anzuwenden sind. Der EMDA muss sicherstellen, dass der Empfang und Versand von E-Mails durch den Nutzer ausschließlich unter Einhaltung von „EMLREQ_1: TLS (Nutzer zu TSP)“ erfolgt. Darüber hinaus informiert der EMDA seine Nutzer über IT-sicherheitsrelevante Vorfälle entsprechend dem [IT-Sicherheitsgesetz]. Weiterhin gibt er Hilfestellungen im Bezug auf IT-sicherheitsrelevante Themen gemäß „ADDREQ_2: Aufklärungspflicht“.

2.1.2 Zertifizierte E-Mail-Diensteanbieter

Dieser EMDA ist ein, gemäß dieser Technischen Richtlinie zertifizierter, Betreiber eines Mail Transfer Agents (MTA). Er nimmt als Sender die E-Mails seiner Nutzer zum Versand entgegen und leitet diese an einen empfangenden EMDA weiter. In seiner Rolle als Empfänger nimmt er die E-Mails von einem sendenden EMDA entgegen und stellt diese seinen Nutzern zum Abruf bereit. Die Anforderungen dieser Technischen Richtlinie richten sich ausschließlich an den EMDA und dessen Schnittstellen zu anderen EMDAn und Nutzern.

2.1.2.1 Sender

Bevor eine E-Mail von dem sendenden EMDA versendet wird, prüft dieser, ob von dem empfangenden EMDA Zertifikatsinformationen gemäß *Kapitel 2.2.1: Vertrauenswürdiger Zertifikatsaustausch* vorliegen bzw. automatisiert abgerufen werden können. Anschließend muss der EMDA versuchen eine Verbindung gemäß „EMLREQ_3: TLS (Ausgehend)“ aufzubauen.

Kann keine sichere Verbindung aufgebaut werden, wird die E-Mail ungeschützt zugestellt. Kann eine sichere Verbindung aufgebaut werden, wird die E-Mail an den empfangenden EMDA über eben diese zugestellt.

Sollte es beim Aufbau oder während der Verbindung zu sicherheitsrelevanten Fehlern kommen, müssen diese protokolliert werden. Ferner muss der zertifizierte EMDA mit dem empfangenden EMDA auf einem dritten Wege Kontakt aufnehmen, um den Fehler schnellstmöglich zu beseitigen. Gleichzeitig sind die nach [IT-Sicherheitsgesetz] bestehenden Meldepflichten einzuhalten. Ein Fehlerfall kann auch darin bestehen, dass Zertifikatsinformationen vom EMDA vorliegen, er aber nicht das Kommando zum Aufbau einer sicheren Verbindung unterstützt.

2.1.2.2 Empfänger

Der empfangende EMDA bietet für sendende EMDA eine Schnittstelle für den Empfang von E-Mails gemäß „EMLREQ_2: TLS (Eingehend)“ an. Über diese Schnittstelle nimmt der zertifizierte EMDA die E-Mail vom sendenden EMDA entgegen und legt diese anschließend im Postfach des Nutzers ab.

Sollte es beim Aufbau oder während der Verbindung zu sicherheitsrelevanten Fehlern kommen, müssen diese protokolliert werden. Ferner muss der EMDA mit dem sendenden EMDA auf einem dritten Wege Kontakt aufnehmen, um den Fehler schnellstmöglich zu beseitigen. Gleichzeitig sind die bestehenden Meldepflichten nach [IT-Sicherheitsgesetz] einzuhalten.

2.1.3 Nicht zertifizierte E-Mail-Diensteanbieter

E-Mail-Diensteanbieter (EMDA) ohne Zertifizierung können in dieser Technischen Richtlinie nur indirekt betrachtet werden. Diese agieren mutmaßlich außerhalb der Regelungen dieser Technischen Richtlinie. Daher können keine Anforderungen an diese gestellt werden . Da ein zertifizierter EMDA jedoch per se nicht

zwischen zertifizierten und nicht zertifizierten EMDAn unterscheiden kann, gelten für die Schnittstellen die gleichen Anforderungen und auch mit nicht zertifizierten EMDA sollten in der Regel sichere Verbindungen zu Stande kommen.

2.2 Aufgaben

In diesem Kapitel werden generelle Aufgaben, welche vom EMDA zu erfüllen sind beschrieben.

2.2.1 Vertrauenswürdiger Zertifikatsaustausch

Für eine vertrauenswürdige Kommunikation mit einem EMDA ist der Austausch von Zertifikaten, bzw. den in den Zertifikaten enthaltenen öffentlichen Schlüsseln, notwendig. Die Zertifikate sollen mittelfristig automatisiert durch die Nutzung von DANE/TLSA gemäß [IETF RFC 6698] über eine per DNSSEC gemäß [IETF RFC 6781] gesicherte Verbindung vom DNS-Server des EMDA abgerufen werden.

Übergangsweise (siehe *Kapitel 3.2: Fachliche Anforderungen*) dürfen die Zertifikate auch über alternative Verfahren (manueller Austausch, sog. Pinning) von dem EMDA bereitgestellt bzw. eingepflegt werden, wenn diese ein vergleichbares Sicherheitsniveau erfüllen.

2.2.2 Transparenz

Es muss für den Nutzer eines EMDA transparent zu erkennen sein, welche seiner E-Mails an einen zertifizierten EMDA gesendet bzw. von einem zertifizierten EMDA empfangen wurden.

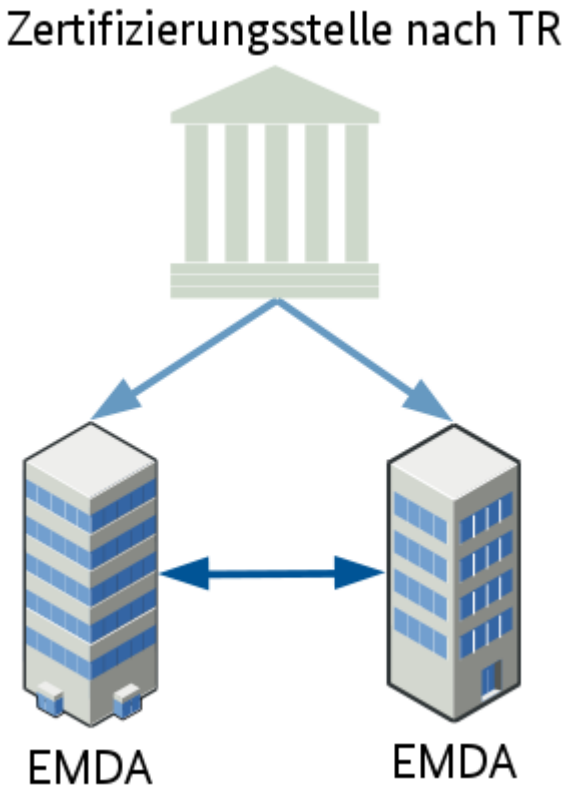

Abbildung 4: Transparenz durch Zertifizierung

Derzeit existiert für eine solche Funktionalität kein international abgestimmtes oder in der Praxis verbreitetes Verfahren. Die Anforderung muss gemäß „ADDREQ_3: Transparenz“ daher zunächst durch den Verweis auf die Liste der nach dieser Technischen Richtlinie zertifizierten EMDA auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik[1] erfolgen.

Informativ: Dem Sender sollte diese Information auch ohne sein Zutun schon vor dem Versand einer E-Mail bzw. beim Empfang einer E-Mail angezeigt werden. Die Gestaltung der Umsetzung eines entsprechenden Mechanismus obliegt dem jeweiligen EMDA.

Langfristig ist die Schaffung eines Mechanismus zur technisch verankerten Herbeiführung von Transparenz geplant. Insbesondere wird hierfür die Nutzung von Zertifikaten aus einer dedizierten CA geprüft. Diese könnten unter Verwendung von DANE/TLSA gemäß [IETF RFC 6698] oder CAA gemäß [IETF RFC 6844] im Resource Record des DNS-Servers (kurz: DNS-Record) hinterlegt werden.

1 Link: https://www.bsi.bund.de/ZertifizierungProduktenachTR

3 Anforderungen

In diesem Kapitel werden die prüfbaren Anforderungen an EMDA zusammengefasst. Diese sollen insbesondere den Prüfer beim Durchführen einer Prüfung gemäß dieser Technischen Richtlinie unterstützen. Neben der grundsätzlichen Anforderung, ein Informationssicherheitsmanagementsystem zu etablieren bzw. ein Sicherheitskonzept zu erstellen, finden sich hier fachliche und weitere grundsätzliche Anforderungen.

3.1 Sicherheitskonzept

Jeder EMDA soll ein Informationssicherheitsmanagementsystem (ISMS) nach [ISO/IEC 27001] betreiben. Das ISMS muss alle für Empfang, Verarbeitung, Speicherung, Versand und Auslieferung an den Nutzer relevanten Systeme und Komponenten umfassen. Das ISMS muss zusätzlich die im folgenden *Kapitel 3.2: Fachliche Anforderungen* aufgeführten Anforderungen beinhalten.

Übergangsweise wird anstelle eines, durch eine Zertifizierung nach [ISO/IEC 27001] nachgewiesenen ISMS, auch ein gemäß [TKG 109] erstelltes Sicherheitskonzept akzeptiert.

Anforderung	Aktuell	Zukünftig
Sicherheitskonzept gemäß [TKG 109]	Verpflichtend	Verpflichtend
Zertifizierung gemäß [ISO/IEC 27001]	Optional	Verpflichtend bei Rezertifizierung

Tabelle 1: Übergangsregelungen zum Sicherheitskonzept

3.2 Fachliche Anforderungen

Die folgenden fachlichen Anforderungen sind als ergänzend zu *Kapitel 3.1: Sicherheitskonzept* von den EMDA umzusetzende Maßnahmen, welche sich konkret auf den Betrieb eines E-Mail-Dienstes beziehen, zu verstehen. Wird die Zertifizierung des EMDA auf Basis einer vorhergehenden Zertifizierung gemäß [ISO/IEC 27001] durchgeführt, sind diese fachlichen Anforderungen als Controls zu bewerten.

Für die hier aufgeführten und im Rahmen einer Zertifizierung zu prüfenden fachlichen Anforderungen werden ebenfalls Übergangsfristen definiert, welche in der folgenden *Tabelle 2: Übergangsregelungen zu den fachlichen Anforderungen* dargestellt werden.

Anforderung	Aktuell	Zukünftig
EMLREQ_1: TLS (Nutzer zu TSP)	Verpflichtend	Verpflichtend
EMLREQ_2: TLS (Eingehend)	Verpflichtend	Verpflichtend
EMLREQ_3: TLS (Ausgehend)	Verpflichtend	Verpflichtend
EMLREQ_4: PKI-Zertifikate	Optional	Verpflichtend bei Rezertifizierung
EMLREQ_5: DANE (Eingehend)	Optional	Verpflichtend bei Rezertifizierung
EMLREQ_6: DANE (Ausgehend)	Optional	Verpflichtend bei Rezertifizierung

Tabelle 2: Übergangsregelungen zu den fachlichen Anforderungen

EMLREQ_1: TLS (Nutzer zu TSP): Die Kommunikation zwischen den Systemen des EMDA und dem Nutzer für den Versand und Empfang von E-Mails, für die Nutzeridentifikation und jede weitere mit dem Verfahren verbundene Kommunikation, muss über TLS nach [BSI TR-03116-4] erfolgen. Daher

muss der EMDA hochwertige Algorithmen gemäß der obengenannten Technischen Richtlinie bevorzugt anbieten. Sofern der EMDA seinen Nutzern den Zugang zu ihren E-Mails über ein Webmail-Interface erlaubt, muss der Zugriff auf dieses durch die Verwendung von HTTPS gemäß [IETF RFC 2818] geschützt sein. Weiterhin darf der EMDA die E-Mails nur unter Nutzung von STARTTLS gemäß [IETF RFC 3207] bereitstellen. Sofern eine abgesicherte Kommunikation nicht möglich ist, soll die Kommunikation zum Nutzer vom EMDA mit einer aussagekräftigen Fehlermeldung beendet werden, aus der auch ein technisch nicht versierte Nutzer den Grund des Abbruchs erkennen kann.

EMLREQ_2: TLS (Eingehend): Der EMDA muss Verbindungen von anderen EMDA über TLS nach [BSI TR-03116-4] zulassen. Bei allen eingehenden Verbindungen sind vorzugsweise Algorithmen einzusetzen, die sogenannte Forward Secrecy (auch Perfect Forward Secrecy, kurz: PFS) bieten und den Empfehlungen aus [BSI TR-03116-4] entsprechen. Der EMDA muss, um sichere TLS-Verbindungen zu erlauben STARTTLS gemäß [IETF RFC 3207] implementieren.

EMLREQ_3: TLS (Ausgehend): Bei Verbindungen zu anderen EMDA muss der EMDA immer dann STARTTLS gemäß [IETF RFC 3207] nutzen, wenn dieses vom empfangenden EMDA angeboten wird. Sofern STARTTLS vom empfangenden EMDA unterstützt wird, sollen vorzugsweise Algorithmen ausgehandelt werden, die sogenannte Forward Secrecy (auch Perfect Forward Secrecy, kurz: PFS) bieten und den Empfehlungen aus [BSI TR-03116-4] entsprechen.

EMLREQ_4: PKI-Zertifikate: Alle Zertifikate, die der EMDA zur Kommunikation mit anderen EMDAn nutzt, müssen von einer nach [BSI TR-03145] zertifizierten Certificate Authority (CA) ausgestellt werden.

EMLREQ_5: DANE (Eingehend): Die von dem EMDA verwendete(n) Domäne(n) müssen entsprechend der Regelungen der DENIC[2] für die DE-Zone durch DNSSEC gemäß [IETF RFC 6781] geschützt sein. Für Domänen, die außerhalb der DE-Zone liegen, sollen vom EMDA vergleichbare Anforderungen erfüllt werden. Darüber hinaus muss der EMDA die gemäß EMLREQ_4 verwendeten Zertifikate im DNS-Record durch die Nutzung von DANE/TLSA gemäß [IETF RFC 6698] hinterlegen.

EMLREQ_6: DANE (Ausgehend): Der EMDA prüft für alle Verbindungen zu anderen EMDA, unter Nutzung von DNSSEC gemäß [IETF RFC 6781], ob im DNS-Record des empfangenden MTA Informationen zur Nutzung von DANE/TLSA gemäß [IETF RFC 6698] hinterlegt sind. Sofern entsprechende Informationen vorhanden sind, wird die Authentizität der Verbindung auf Basis dieser Informationen überprüft.

3.3 Weitere Anforderungen

Die folgenden Anforderungen ergänzen die oben beschriebenen fachlichen Anforderungen. Sie enthalten vom EMDA zu schaffende Rahmenbedingungen für einen sicheren Betrieb.

ADDREQ_1: Datenschutz: Die Systeme des EMDA werden grundsätzlich in Deutschland betrieben, sodass der deutsche Datenschutz gemäß [BDSG] Anwendung findet. In Ausnahmefällen ist ein Betrieb im EU-Ausland und der Schweiz unter vergleichbaren oder höheren Datenschutzanforderungen legitim.

ADDREQ_2: Aufklärungspflicht: Der EMDA verpflichtet sich seine Nutzer über IT-Sicherheitsvorfälle gemäß [IT-Sicherheitsgesetz] zu informieren. Weiterhin verpflichtet er sich, seine Nutzer über IT-sicherheitsrelevante Themen aufzuklären. Diese Pflicht kann er durch den Verweis auf entsprechende Informationsangebote des Bundes[3] nachkommen.

ADDREQ_3: Transparenz: Der EMDA verpflichtet sich seine Nutzer bestmöglich darüber zu informieren, wenn E-Mails von Nutzern anderer EMDA empfangen wurden oder an die Nutzer anderer EMDA gesendet werden. Dies muss mindestens durch einen Verweis auf die Liste der zertifizierten Anbieter beim BSI[4] geschehen.

2 Link: http://www.denic.de/domains/dnssec.html
3 Link: https://www.bsi-fuer-buerger.de
4 Link: https://www.bsi.bund.de/ZertifizierungProduktenachTR

Literaturverzeichnis

BDSG	BfDI: Bundesdatenschutzgesetz
BSI TR-03116-4	Bundesamt für Sicherheit in der Informationstechnik: Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 4 - Kommunikationsverfahren im eGovernment
BSI TR-03145	Bundesamt für Sicherheit in der Informationstechnik: Secure Certification Authority operation
IETF RFC 2818	IETF: HTTP Over TLS
IETF RFC 3207	IETF: SMTP Service Extension for Secure SMTP over Transport Layer Security
IETF RFC 6698	IETF: The DNS-Based Authentication of Name Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
IETF RFC 6781	IETF: DNSSEC Operational Practices, Version 2
IETF RFC 6844	IETF: DNS Certification Authority Authorization (CAA) Resource Record
ISO/IEC 27001	ISO/IEC: 27001:2013 Information technology; Security techniques; Information security management systems; Requirements
IT-Sicherheitsgesetz	Bund: Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systemen (IT-Sicherheitsgesetz)
TKG 109	Bundesnetzagentur: Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 Telekommunikationsgesetz (TKG)