bitkom

Stellungnahme

Februar 2024

BSI TR-03176: Sichere Datenübermittlung in der Registermodernisierung

Zusammenfassung

Die Technische Richtlinie BSI TR-03176 beschäftigt sich mit der sicheren Datenübermittlung im Kontext der Registermodernisierung. Ziel dieser Technischen Richtlinie (TR) ist es, Anforderungen für einen sicheren sowie nachvollziehbaren Datenaustausch für konkrete Protokolle zu definieren. Die technische Richtlinie ist in mehrere Teile gegliedert:

- Rahmendokument
- Teil-TR 1: XBasisdaten
- Teil-TR 2: XUnternehmen.Basisdaten (in Planung)
- Teil-TR 3: XDatenschutzcockpit (in Planung)

Das Rahmendokument sowie Teil-TR 1 „XBasisdaten“ wurden vom Bundesamt für Sicherheit in der Informationstechnik (BS) in der Version 0.9 vorab veröffentlicht. Das Bitkom-Feedback adressiert u.a. die folgenden Punkte:

- Nutzbarkeit zentraler Security-Mechanismen
- Einräumung von Anpassungszeiträumen
- ergänzende Mechanismen zum Logging
- einheitliche Verwendung von Fachbergriffen

Die detaillierten Anmerkungen zur Version 0.9 der technischen Richtlinie sind den nachfolgenden Kommentierungstabellen zu entnehmen.

87%

Der Bürgerinnen und Bürger fordern von ihrer Stadt oder Gemeinde mehr Nachdruck bei der Digitalisierung.

bitkom

Kommentierung des Rahmendokuments (TR-03176)

Kapitel-nummer	Kapitelname	Passage / Abbildung / Tabelle	Kurzbeschreibung	Kommentar / Vorschlag / Frage / Kritik
2	Begriffs-definitionen	*Wird von „Ende-zu-Ende“ gesprochen, ist damit von Empfangssystem zu Sendesystem (beispielsweise von Fachverfahren zu Register) gemeint.*	Wortreihenfolge ändern	Die Reihenfolge sollte typischerweise in Datenflussrichtung angegeben werden: „Sendesystem zu Empfangssystem“
2	Begriffs-definitionen	*System, welches eine Schnittstelle zwischen der Registermodernisierungsbehörde und dem Empfangssystem zum Abruf von Basisdaten und/oder IDNr zur Verfügung stellt*	Abkürzung undefiniert	Die Abkürzung „IDNr“ wird hier ohne vorherige Einführung oder Vorkommen im Abkürzungsverzeichnis verwendet.
2	Begriffs-definitionen	*Daten, die mit den Inhaltsdaten verbunden werden, um den korrekten Transport der Fachdaten zu gewährleisten; sie enthalten selber keine Fachdaten*	Fachbegriff verwenden	Der Begriff „Inhaltsdaten“ wird als Begriff nicht erklärt. Zur besseren Klarheit könnte hier stattdessen der definierte Begriff „Fachnachricht“ verwendet werden.
3.1	Allgemeine Anforderungen, RaD.3.1.1	*"OPS.1.1.3.A15 und CON.8.A20 des IT-Grundschutz-Kompendiums MÜSSEN eingehalten werden"*	Fachlicher Hinweis	CON.8.A20 (Überprüfung von externen Komponenten (B)) --> Die Anforderung erschwert den Einsatz von Open-Source-Bibliotheken.
3.1	Allgemeine Anforde-rungen, RaD.3.1.2	*Ein System, welches nicht Empfangssystem ist, MUSS eine Nachricht an das für den weiteren Transport zum Empfangssystem zuständige System oder das Empfangssystem weiterleiten.*	Fachbegriff verwenden	„Ein System, welches nicht Empfangssystem ist“ kann unserer Einschätzung nach durch den definierten Begriff Intermediärsystem für verbesserte Klarheit ausgetauscht werden.
3.1	Allgemeine Anforde-rungen, RaD.3.1.2	*Für die Feststellung, welches System dies ist, MÜSSEN vertrauenswürdige Datenbanken verwendet werden.*	Fachbegriff verwenden & fehlende Definition von Vertrauenswür-digkeit	Möglicher Austausch durch verständlichere Formulierung „Zur Bestimmung des zuständigen Intermediärsytems…“. Zudem ist unklar, was konkret mit „Vertrauenswürdige Datenbanken“ gemeint ist. Ist damit beabsichtigt den Einsatz von DNS oder Routing zu adressieren? Bei Routing wäre ein Einsatz von DB eher unüblich. Aus Anbietersicht stellt sich die Frage, welche Kriterien an die Vertrauenswürdigkeit gelegt werden. Hierzu sollten Hinweise in der Vorgabe existieren.

3.2	Fehler-behandlung, RaD.3.2.3	*Ein an der Datenübermittlung beteiligtes System MUSS eine Nachricht so lange aufbewahren, bis sie entweder das auf dem Datenübertragungsweg nächste zuständige System erreicht hat,*	Fachbegriff verwenden	Statt „zuständige System“ könnte hier Intermediärsystem verwendet werden
3.2	Fehler-behandlung, RaD.3.2.4	*Findet ein Kommunikationsmodell Anwendung, bei dem ein System selbsttätig eine Nachricht an ein anderes System weiterreicht (symmetrische Kommunikation), […]*	Unklare Verwendung	Hier ist unklar wie der Begriff der „symmetrischen Kommunikation“ zur vorhergehenden Erklärung passt
3.3	Nachrichten-validierung	*In der öffentlichen Verwaltung werden verschiedene Standards zur Darstellung von Daten in maschinenlesbaren Formaten verwendet, […]*	Begriffsschärfung	Nachfolgend wird zwischen Schemas der Nachrichten und der verwendeten Dateiformate unterschieden. Da Schema und Format in der Regel ähnlich verwendet werden, sollte bereits hier statt Format „Dateiformat“ verwendet werden, um mit der Verwendung in [RaD.3.3.2] übereinzustimmen. Ggf. sind Formate an dieser Stelle aber auch als Abstraktion der beiden Begriffe zu verstehen?
3.3	Nachrichten-validierung, RaD.3.3.3	*Falls eine Inhaltsdatenverschlüsselung verwendet wird und die verschlüsselten Inhaltsdaten in einer Containernachricht transportiert werden, […]*	Fachbegriff undefiniert	„Containernachricht“ sollte als Begriff vorher definiert oder entsprechend umschrieben werden.

3.4	Krypto-grafische Anforde-rungen, RaD.3.4.1	*Es DÜRFEN NUR Protokolle eingesetzt werden, die kryptografische Algorithmen verwenden, welche in der TR-03116-4 2 [3] für den jeweils vorgesehenen Zweck zulässig sind. Diese Zwecke sind: a) die Sicherstellung der Vertraulichkeit auf Inhaltsdatenebene (Ende-zu-Ende-Verschlüsselung), b) die Sicherstellung der Vertraulichkeit auf Transportebene (Transportverschlüsselung), c) die Sicherstellung der Integrität und Authentizität auf Inhaltsdatenebene (Ende-zu-Ende Verifikation) sowie d) die Sicherstellung der Integrität und Authentizität auf Transportebene (Transportverifikation).*	Anpassungs-zeiträume bei Versionswechsel der technischen Richtlinie	Anpassungszeitraum an neue Versionen der technischen Richtlinie sollte vorhanden sein. Hierbei ist zu berücksichtigen, dass technische Restriktionen von älteren Systemen, die nicht im Verantwortungsbereich des Betreibers liegen, zu Übergangsfristen führen sollten. Es sollten alternative Vorgehensweisen berücksichtigt werden.
3.4	Krypto-grafische Anforde-rungen, RaD.3.4.2	*Es MUSS eine Ende-zu-Ende-Verschlüsselung für die Verschlüsselung der Inhaltsdaten zwischen den beteiligten Akteuren eingesetzt werden. Kommen bei der Übermittlung der Inhaltsdaten mehr als zwei technische Systeme zum Einsatz, so MÜSSEN die zwischengeschalteten Systeme ihren Dienst ohne Kenntnis der Inhaltsdaten erfüllen können und DÜRFEN NICHT in die Lage versetzt werden, Inhaltsdaten im Klartext einzusehen*	Begriffs-angleichung, Definition Inhaltsdaten & Nutzbarkeit zentraler Security-Mechanismen	„Akteur“ wird im Dokument nur an dieser Stelle verwendet und sollte zu Vereinheitlichung der Begriffe z.B. durch „Partei“ ausgetauscht werden, sofern dies hier gemeint ist. Statt der Umschreibung „zwischengeschaltete Systeme kann hier ein Fachbegriff verwendet werden: „Alle Intermediärsysteme müssen…“. Unklar ist die Anforderung, dass die Intermediärsysteme ihren Dienst ohne Kenntnis der Inhaltsdaten erfüllen können. Was genau darf nicht bekannt sein? Statt Inhaltsdaten sollte man hier einen der vorgestellten Begriffe verwenden. Schlüsseltext z.B. muss den Systemen bekannt sein. Die Formulierung sollte zudem klarstellen, dass zentrale Security-Mechanismen wie Proxy und Malewarescanning trotzdem nutzbar sind (diese müssen zum sinnvollen Einsatz die Inhaltsdaten analysieren).

3.5.2	Protokoll zu betriebs- und sicherheits-relevanten Ereignissen, RaD.3.5.2.1	*Es MUSS ein Protokoll über alle betriebs- und sicherheitsrelevanten Ereignisse geführt werden. Dabei MUSS der Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen [4] umgesetzt werden.*	Alternativen zulassen	Allgemeine Anmerkung zu Logging: Führt zu sehr hohen Betriebskosten, hier sollte die Möglichkeit eröffnet werden, Alternativen - ähnlich gleichwirksame Mechanismen - einzusetzen z.B. EDR System, MS Defender for Identity.
3.5.3	Protokoll zur transpa-renten Nachvollzieh-barkeit organisa-torischer Aspekte der Daten-übermittlung, RaD.3.5.3.1	*Jede Stelle, die an einer Datenübermittlung beteiligt ist, MUSS ein Protokoll zur transparenten Nachvollziehbarkeit der organisatorischen Aspekte der Datenübermittlung führen.*	Unklare Verwendung	Hier wird ein neuer Begriff „Stelle“ verwendet, statt bisherige Begrifflichkeiten zu nutzen. Was ist hier mit beteiligten Stellen, die außerhalb des Zugriffsbereichs des Anbieters liegen (z.B. Netzwerkrouter)?
3.6	Monitoring, [RaD.3.6.2	*Wird diese Menge überschritten, so DARF NUR dann das Empfangssystem dem Sendesystem antworten, nachdem die Verantwortlichen beider Systeme die Rechtmäßigkeit der Nachrichtenübermittlung festgestellt haben.*	Unklare Verwendung	Es ist unklar, auf welche Weise die Rechtmäßigkeit definiert wird.
3.7	Löschung von Daten, RaD.3.7.2	*Daten MÜSSEN mindestens durch einfaches Löschen im Dateisystem entfernt werden. Kopien MÜSSEN in die Löschung mit einbezogen werden (z.B. Backups oder andere Rücksicherungen).*	Unklare Verwendung & redaktionelle Anmerkung	Was versteht man unter „einfaches Löschen“? Anmerkung: Daten sollten bei Backups nicht explizit gelöscht werden, sondern herausaltern (Löschkonzept pbD -Norm Referenz DIN 66398 / ISO 27555) Redaktionelle Anmerkung: Anforderung 3.7.3 sollte vor 3.7.2 stehen.

Einige unserer Anmerkungen zielen darauf ab, zentrale Begrifflichkeiten zu definieren bzw. einheitlich zu verwenden. Vor diesem Hintergrund empfehlen wir der technischen Richtlinie ein übergreifendes Schaubild voranzustellen, mit dem die wesentlichen Komponenten, Akteure und Begriffe vorgestellt / eingeordnet werden. Man könnte ein solches Schaubild im Rahmendokument verankern und dann noch einmal etwas detaillierter im TR-Teil zu XBasisdaten aufgreifen.

bitkom

Kommentierung des Teils-TR XBasisdaten (TR-03176-1)

Kapitel-nummer	Kapitelname	Passage / Abbildung / Tabelle	Kurzbeschreibung	Kommentar / Vorschlag / Frage / Kritik
1.1	Abgrenzung	*Auch die Kommunikationsbeziehung 4 wird von dieser Teil-TR nicht betrachtet.*	Unklare Formulierung	Unklar, wieso das der Fall ist. Werden hier keine XBasisdaten übermittelt? Gerne Begründung einfügen.
1.1	Abgrenzung	*Auf Basis dieser Abgrenzung sind die Kommunikationsbeziehungen 2 und 3 als äquivalent zu betrachten, da das DSC einen Onlinedienst darstellt.*	Unklare Formulierung	Wieso sind diese dann in Abbildung 1 nicht äquivalent eingetragen mit Netzübergang? Ist der DSC nur eine interne Webapp? Farben werden in der Grafik nicht erklärt.
1.1	Abgrenzung	*Im Zuge des Abrufs einer berechtigten Stelle ist der Abruf von Basisdaten durch eine öffentlich erreichbare Stelle gesondert zu betrachten (Kommunikationsbeziehung 2).*	Widerspruch	Ein Widerspricht ergibt sich hier auf ersten Blick mit dem Satz davor, dass 2 und 3 äquivalent betrachtet werden.
2.1	Einführung in das Kommuni-kations-modell	*alleine für die Inhaltsnachricht zuständig ist. Das bedeutet, dass er für die Errichtung der Ende-zu-Ende-Sicherheit die Verantwortung übernehmen muss*	Unklare Formulierung	Unklar, wieso diese Verantwortung aus dem Satz davor folgt.
2.1	Einführung in das Kommuni-kations-modell	*Er stellt die Authentizität, Integrität und Vertraulichkeit eventuell notwendiger Transportnachrichten sicher.*	Wortwahl	Wieso sind diese nur „eventuell“ notwendig?
2.1	Einführung in das Kommuni-kations-modell	*Neben einem direkten Kanal zwischen den Fachsystemen von Autor und Leser oder der Kommunikation über Intermediäre sind auch weitere Implementierungsmöglichkeiten denkbar. Diese Intermediäre übernehmen [...]*	Satzstruktur	Durch die Satzstruktur, welche mit „sind auch weitere Implementierungsmöglichkeiten denkbar“ endet, erwartet man nicht, dass sich der nächste Satz dann wieder auf den ersten Teil des letzten Satzes bezieht.

2.1	Einführung in das Kommuni-kations-modell	*Darüber hinaus stellt er sicher, dass die notwendigen Informationen zur Errichtung einer Ende-zu-Ende-Sicherheit vorliegen.*	Unklare Formulierung	Lässt die Frage offen, ob er die Anwendung der Ende-zu-Ende Sicherheit auch sicherstellen muss.
3.1	Authentisie-rung und Autorisierung	*MÜSSEN die Vorgaben der TR-03116-4 [5] werden*	Fehlendes Wort	.. eingehalten werden
3.4	Protokoll-ierung	*den Akteur, an welchen die Nachricht an das nächste System im Übertragungsweg übermittelt wurde.*	Unklare Formulierung	Unklar, ob hier einfach die Identität des nächsten Systems übermittelt werden soll. Wer ist hier der Akteur?
3.4	Protokoll-ierung	*die beteiligten Akteure, also Herkunft und Ziel einer Nachricht, sowie Autor und Leser einer Nachricht.*	Unklare Formulierung	Inwiefern unterscheiden sich die beiden Begriffspaare hier?
3.4	Protokoll-ierung	*Intermediärsysteme auf dem Transportkanal (sofern vorhanden) protokollieren:*	Unklare Formulierung	Was ist hier mit Intermediärsystemen, die außerhalb des Zugriffsbereichs (Netzwerkrouter im Internet) liegen?
3.4	Protokoll-ierung	*die beteiligten Akteure, also der Autor sowie Intermediärsysteme, von denen die Nachricht empfangen wurde,*	Unklare Formulierung	Woher erhält der Leser Informationen über die Intermediärsysteme auf dem gewählten Kommunikationsweg?

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Marc Danneberg | Bereichsleiter Public Sector
T 030 27576-526 | m.danneberg@bitkom.org

Esther Steverding | Referentin Public Sector
T 030 27576-216 | e.steverding@bitkom.org

Verantwortliches Bitkom-Gremium

AK Digitale Verwaltung