Bundesamt
für Sicherheit in der
Informationstechnik

Migration auf TLS 1.2

Handlungsleitfaden

Version 1.2

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

Aktuelle Hinweise zur Version 1.2

Bonn, 20.06.2016

Dieser Migrationsleitfaden wurde parallel zum Mindeststandard TLS veröffentlicht, der im Wesentlichen auf der TR-02102-2 basiert. Die TR-02102-2 ist im ersten Quartal 2016 aktualisiert worden. Teile dieser Aktualisierung betreffen auch direkt die Umsetzung des Mindeststandards und entsprechend die Ausführungen im Migrationsleitfaden. Die wesentliche Änderung betrifft die Abkündigung von SHA-1 und damit der TLS-Versionen 1.0 und 1.1.

Für die Sektoren Behörde-Wirtschaft-, Inter- und Intra-Behörden-Kommunikation muss TLS 1.2 gemäß TR "eingesetzt" werden. Im Sektor Bürger-Behörde-Kommunikation spricht der Standard lediglich vom "primären Anbieten" statt von "Einsetzen" und die TR erlaubte in der damaligen Fassung den Rückfall auf TLS 1.0/1.1. Damit sollte eine gewisse Abwärtskompatibilität zum Browser des Bürgers gewährleistet werden. Durch die Aktualisierung der TR im Februar 2016 ist dieser Rückfall nicht mehr vorgesehen.

Der Migrationsleitfaden beinhaltet im Anhang auch Anleitungen zur Migration, etwa der Webserver Apache und Internet Information Server bzw. der jeweils genutzten Cryptobibliotheken OpenSSL und Shannel.dll, die nach der TR-Aktualisierung in Teilen nicht mehr zutreffen, was entsprechend auch für das Fallbeispiel gilt. Im Wesentlichen betrifft dies die Konfiguration von Apache/OpenSSL.

Apache

Anleitungen für die Nutzung nur angegebener Protokollversionen und Cyphersuiten unter Apache 2.4.x finden Sie unter

https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslprotocol

bzw.

https://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslciphersuite

OpenSSL

Die in der Regel von Apache, aber auch von anderen Anwendungen genutzte Kryptobibliothek OpenSSL lässt sich ebenso entsprechend konfigurieren. Hinweise finden Sie in der offiziellen OpenSSL-Dokumentation, aber auch in der BSI-Veröffentlichung zur Schwachstellenanalyse in OpenSSL:

https://www.bsi.bund.de/DE/Publikationen/Studien/OpenSSL-Bibliothek/opensslbibliothek.html

Informationen zur Konfiguration finden Sie im Kapitel 7, inklusive einer konkreten

Umsetzung der Empfehlungen zu Cyphersuiten gemäß TR-02102-2 im Kapitel 7.8.2.

Weitere Änderungen

Tabelle 7, "Die auszuwählenden Cypher-Suites gemäß TR-02102-2", Seite 19: Die Verwendungsfristen sind in der aktuellen TR-Auflage von 2021+ auf 2022+ verlängert worden.

Änderungen der TR-03116-4

Auch die TR-03116-4 "Kryptographische Vorgaben für Projekte der Bundesregierung. Teil4: Kommunikationsverfahren in Anwendungen" wird von dem Mindeststandard und dem Migrationsleitfaden referenziert und wurde im Februar 2016 aktualisiert. Der Leitfaden ist hier auf Seite 20, Tabelle 9 "Mindestschlüssellängen für X.509-Zertifikate" betroffen. Die hier angegebenen Schlüssellängen werden in der aktuellen TR-Fassung nicht mehr für eine Verwendung bis "2021+" freigegeben, sondern lediglich bis 2021. Hinzugekommen sind größere Schlüssellängen mit Verwendung bis 2022+. Zudem finden sich diese Angaben in der TR nicht mehr unter Kapitel 4.1.4, sondern unter Kapitel 5.1.4.

Allgemeiner Hinweis: Im Themenkomplex Transportverschlüsselung/TLS gibt es kontinuierlich Veränderungen, neue Sicherheitslücken und -empfehlungen - bitte halten Sie sich diesbezüglich auf dem Laufenden. Hinweise finden Sie auf den Seiten des BSI sowie tagesaktuell über die zahlreichen Presse-Kanäle zur IT-Security. Dieser Migrationsleitfaden stellt hingegen nicht immer den aktuellsten Stand dar und ist als allgemeine Umsetzungshilfe zu verstehen - technische Details sollten Sie vor der Übernahme grundsätzlich selbst prüfen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Zielstellung und Nutzen des Leitfadens

Der vorliegende Handlungsleitfaden unterstützt IT-Sicherheitsbeauftragte, IT-Fachpersonal und IT-Verfahrensverantwortliche, TLS-Transportverschlüsselung in der Protokollversion TLS 1.2 mit Perfect Forward Secrecy (PFS) gemäß der TR-02102-2 zu planen und einzuführen bzw. ältere Versionen zu migrieren.

Das Bundesamt für Sicherheit in der Informationstechnik hat zur Gewährleistung eines einheitlichen Mindestsicherheitsniveaus bei der sicheren Datenübertragung einen Mindeststandard nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des TLS-Protokolls in der Bundesverwaltung entwickelt, verbindlich gemäß Erlass vom 13. März 2015 als Allgemeine Verwaltungsvorschrift durch das Bundesministerium des Innern nach Zustimmung des Rates der IT-Beauftragten der Ressorts.
Die Migration auf TLS 1.2 mit PFS gemäß des Mindeststandards soll folgende Ziele erreichen:

1. eine angriffsresistentere Übertragung sensitiver und vertraulicher Daten durch effektivere Transportverschlüsselung;
2. den Austausch schwacher durch starke Transportverschlüsselungsverfahren bzw. deren Einführung;
3. die Erreichung eines einheitlichen Mindestsicherheitsniveaus in der Bundesverwaltung durch Umsetzung des Mindeststandards TLS 1.2.

Diese Migration betrifft zahlreiche IT-Systeme, Infrastrukturkomponenten und Interessengruppen, welche mitunter selbst eine Migration ihrer Anwendungen durchführen müssen.
Das BSI unterstützt die TLS-Migration in folgenden Phasen:

1. Für die Planungsphase formuliert das BSI die Ziele und Herausforderungen der Migration auf TLS 1.2.
2. Für die Konzeptionsphase legt das BSI die adäquaten Verschlüsselungsverfahren fest und benennt so den Soll-Zustand. Ferner stellt das BSI der Bundesverwaltung für die Konzeption Produkte, z. B. OpenVAS in Bundeslizenz, und Beratungsleistungen bereit.
3. Für die Umsetzungsphase gibt das BSI technische und organisatorische Hinweise zur Migration der betroffenen Anwendungen bzw. Technologien und ergänzt diese um Hinweise für eine Restrisikoanalyse, um die Migrationspfade und -alternativen bestimmen zu können.

In diesem Dokument wird ausschließlich die Transportverschlüsselung auf Basis des SSL/TLS-Protokolls berücksichtigt. Andere eingesetzte Mechanismen werden durch den Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung [Mindeststandard SSL/TLS] nicht berührt.

1.1 Zielgruppen des Migrationsleitfadens

Der vorliegende Migrationsleitfaden gliedert sich in zwei Bereiche für zwei Zielgruppen:

- Die Kapitel 1-5 richten sich primär an IT-Sicherheitsbeauftragte und IT-Verantwortliche aus der Verwaltung. Zunächst erläutern die Kapitel 1-3 Hintergründe des Mindeststandards/ Migrationsleitfadens und das Sektormodell zur Einteilung betroffener Verfahren. Anschließend wird ein Vorgehensmodell für die Organisation der Migration an die Hand gegeben und als Fallbeispiel illustriert.
- Der umfangreiche Anhang richtet sich primär an IT-Administratoren und bietet Arbeitshilfen wie konkrete Anleitungen zur Aktivierung/Konfiguration von TLS 1.2 in diversen Anwendungen (Browser, Webserver) sowie Kompatibilitätstabellen.

1.2 Klartext: Wer muss was migrieren – und was nicht?

Sinn und Zweck des Mindeststandards TLS 1.2 ist die Sicherstellung verschlüsselter Übertragung von schutzbedürftigen Daten über unsichere Netze.

Schutzbedürftige Daten weisen mindestens einen Schutzbedarf (bzgl. eines der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit) von „normal“ auf. Darunter fallen auch alle Daten, die Webseiten veröffentlicht werden, da hier auf jeden Fall die Integrität zu schützen ist.

Sichere Netze sind auf jeden Fall IVBB, NdB, IBVB sowie Behördennetze, die Teil eines Informationsverbunds sind, bei dem alle nötigen IT-Grundschutzmaßnahmen umgesetzt sind. Grundsätzlich dürfen auch Netze, die für VS-NfD freigegeben sind als sicher im Sinne des Mindeststandards angesehen werden.

Unsichere Netze sind unscharf definiert. Prototypisch für ein unsicheres Netz ist das Internet; insbesondere auch, wenn darüber zwei Standorte einer Behörde verbunden werden.

Ausnahmen: Generell ist zu prüfen, ob die Transportverschlüsselung die Sicherheit erhöht – wenn nicht, kann von einem sicheren Netz im Sinne des Mindeststandards ausgegangen werden.

Ein Sonderfall ist die vor allem für den Sektor „Bürger-Behörden-Kommunikation“ relevante **Abwärtskompatibilität:** In Anbetracht der vernachlässigbaren Vertraulichkeitserfordernisse für öffentliche Webseiten, kann hier auf TLS-1.2-Zwang verzichtet werden – daher spricht der Mindeststandard hier explizit von „anbieten“ und nicht von „anwenden“.

Zusammengefasst: Ausnahmen zur Pflicht, Transportverschlüsselung TLS 1.2 mit PFS einzusetzen, können bei als sicher anzusehenden Netzen bestehen. Ausnahmen müssen gegenüber dem BSI hinreichend begründet und notifiziert werden, ebenso nicht fristgerechte Migrationen.

2 Der Mindeststandard TLS 1.2

Der Mindeststandard TLS 1.2 gilt für die Datenübertragung über unsichere Netze.

Da schutzbedürftige Daten in unsicheren Netzen auch dann Bedrohungen ausgesetzt sind, wenn die Verschlüsselung nur ein schwaches Sicherheitsniveau aufweist oder inkonsistent implementiert oder betrieben wird, fordert der Mindeststandard den Einsatz von TLS in der aktuellen Version 1.2 und mit Perfect Forward Secrecy.

2.1 Rahmenbedingung

Die Forderung nach TLS 1.2 mit PFS betrifft verschiedene Cipher-Suites mit jeweils unterschiedlichen Schlüssellängen gemäß der Tabelle 1 in der TR-02102-2.

Der Mindeststandard nimmt zudem Bezug auf die anwendungsspezifischen Vorgaben zu Zertifikatsausgabe, -verarbeitung und -rückruf der TR-03116-4.

Er gilt ab sofort für alle neuen Systeme mit Transportverschlüsselung. Bestandssysteme sind anhand der nachfolgend genannten Fristen zu migrieren, wenn keine alternative Transportverschlüsselung mit vergleichbarem minimalem Sicherheitsniveau eingesetzt wird:

- Bürger-Behörden-Kommunikation (Webserver und Browser): 1.7.2015
- Wirtschaft-Behörden-Kommunikation (Fachverfahren zwischen Wirtschaft und Behörden): 31.12.2016
- Inter-Behörden-Kommunikation (Fachverfahren zwischen Behörden): 31.12.2016
- Intra-Behörden-Kommunikation (Dienste und Fachverfahren innerhalb einer Behörde): 1.7.2017

Anwendungen, die Daten mit mindestens hohem Schutzbedarf verarbeiten, sind vorrangig zu migrieren.

Sollte eine Behörde die Migration acht Wochen vor Ablauf der Frist nicht vollständig durchführen können, so hat sie den Sachverhalt gemäß Mindeststandard direkt oder über den IT-Sicherheitsbeauftragten ihres Ressorts an das BSI zu notifizieren. Die direkte Notifikation der Bundesbehörde an das BSI ist vom Behördenleiter zu unterschreiben. Bei Notifikation der Bundesbehörde an den IT-Sicherheitsbeauftragten des Ressorts oder seine stellvertretend beauftragte Stelle, erfolgt dessen oder deren Notifikation an das BSI unverzüglich. Die Notifikation des IT-Sicherheitsbeauftragten des Ressorts an das BSI ist dann von diesem oder der von ihm stellvertretend beauftragten Stelle zu unterschreiben. Das Formular zur Notifikation findet sich im internen Bereich der Sicherheitsberatung des BSI.

3 Das Sektormodell des Mindeststandards

Das Sektormodell dient einer Unterteilung in vier Bereiche, für die jeweils eine eigene Frist für den Abschluss der Migration gilt – die *Meilensteine* des Gesamtprojekts.

Anhand des Sektormodells lassen sich die IT-Systeme der Behörde nach Anzahl (Externe Bindung) und Vielfältigkeit (Systemheterogenität) der mit ihnen verbundenen Endsysteme und Fachverfahren einordnen. Anhand dieser Einordnung wiederum lassen sich anschließend Prioritäten für die zeitliche Abfolge der Migration der einzelnen Dienste setzen.

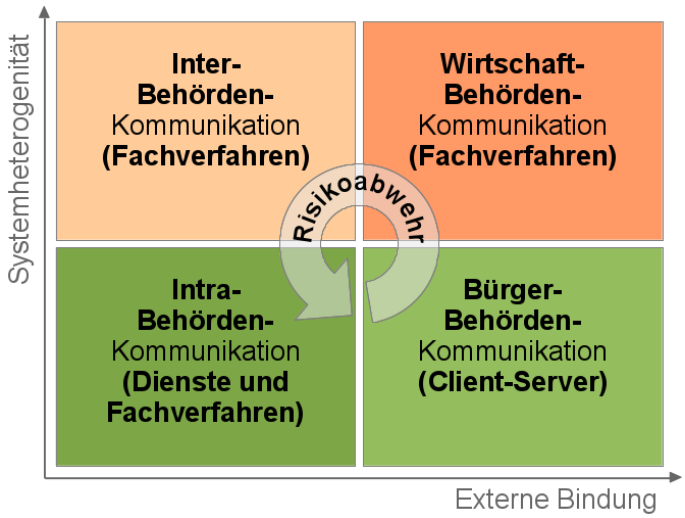

Abbildung 1: Priorisierung der Sektoren; der Pfeil zeigt den zeitlichen Ablauf.

Hintergrund: Die Migration der IT-Systeme und Fachverfahren ist nach der in Abbildung 1 illustrierten Reihenfolge durchzuführen. Sie basiert auf einer zügigen Herstellung der Risikoabwehr und der Komplexität der Systeme. Während der Ressortabstimmungen zur Verbindlichmachung des Mindeststandards wurde davon ausgegangen, dass Dienste und Fachverfahren in den Bereichen „Bürger-BehördenKommunikation“ (Sektor 1) und „Intra-Behörden-Kommunikation“ (Sektor 4) zügig migriert werden können – die Notwendigkeit einer schnellen Umsetzung aber vor allem bei der Bürger-Behörden-Kommunikation besteht. Der Aufwand für Fachverfahren in Sektor 2 „Wirtschaft-Behörden-Kommunikation“ und Sektor 3 „Inter-Behörden-Kommunikation“ wurde im Abstimmungsprozess aufgrund des größeren Individualanteils und der größeren Vielfalt der verbundenen Systeme höher eingeschätzt – bedingt durch organisatorischen Aufwand bzgl. der Zusammenarbeit mit externen Partnern und der Notwendigkeit, Infrastruktur-Komponenten wie Router, Firewalls oder Load-Balancer in die Migrationsstrategie einbeziehen zu müssen.

Die Verfahren und Dienste einer Behörde werden im Rahmen der nachfolgend im Verfahrensmodell beschriebenen Ist-Analyse in die Sektoren eingeordnet. Zur Priorisierung bzgl. zeitlicher, finanzieller und personeller Ressourcen können die Dimensionen „Externe Bindung“ und „Systemheterogenität“ herangezogen werden:

- Die Dimension „Externe Bindung“ berücksichtigt *quantitative Kriterien:* Der zeitlichen

Priorisierung dienen Nutzer- und System-Anzahl, der fachlichen etwaige Zuständigkeiten. Überlappungen mit dem ISMS externer Anwendungen können sowohl zeitlicher als auch fachlicher Priorisierung dienen.

- Die Dimension „Systemheterogenität“ berücksichtigt *qualitative Kriterien:* Der zeitlichen Priorisierung dienen die Aspekte Kompatibilität zu angebunden Nutzern und Art der IT-Systeme. Zuständigkeiten und Vorgaben für bestimmte Fachverfahren stützen die fachliche Priorisierung. Letztlich können Verfahrensvorschriften und Gesetze eine Migration beschleunigen oder verlangsamen.

In allen Sektoren obliegt es der migrierenden Organisation, geeignete **Alternativlösungen** für jene Systeme zu finden, die nicht migriert werden können. Dabei müssen nicht migrierbare Systeme in absehbarer Zeit und mit angemessenem Aufwand gegen Systeme ausgetauscht werden, die die Vorgaben des Mindeststandards TLS 1.2 erfüllen. Das BSI ist über solche nicht migrierbaren Systeme der jeweiligen Sektoren innerhalb der jeweils festgelegten Frist zu unterrichten.

4 Vorgehensmodell zur Migration

Dieses Kapitel beschreibt ein Vorgehensmodell zur Migration, die einzubeziehenden Organisationsebenen und die von diesen durchzuführenden Migrationsaufgaben.

Die Migration umfasst folgende Phasen:

1) **Ist-Analyse,** also die Erhebung des aktuellen Stands der eingesetzten Informationstechnik samt ihrer Dokumentation.
2) **Soll-Konzept,** also die Planung des zu erreichenden Zustands der eingesetzten Informationstechnik konform zum Mindeststandard TLS 1.2.
3) **Risikobetrachtung,** also die Erhebung und Dokumentation der Restrisiken, falls die Informationstechnik nicht gemäß des Mindeststandards TLS 1.2 vollständig migriert werden kann.
4) **Migrationsdurchführung,** also die Anpassung der Informationstechnik gemäß des Soll-Konzepts.

Eine TLS-Migration adressiert drei Organisationsebenen einer Behörde, wie in Schaubild 2 dargestellt.

- Die technischen Verantwortlichen (*technische Ebene*) führen die Ist-Analyse und die Migration in Kooperation mit den Verfahrensverantwortlichen durch.
- Die Verantwortlichen für die Verfahren (*Verfahrensebene*) übernehmen das Soll-Konzept und die Risikobetrachtung.
- Die Behördenleitung (*Leitungsebene*), im Besonderen das Management für die Informationssicherheit, ist in allen Phasen zu involvieren.

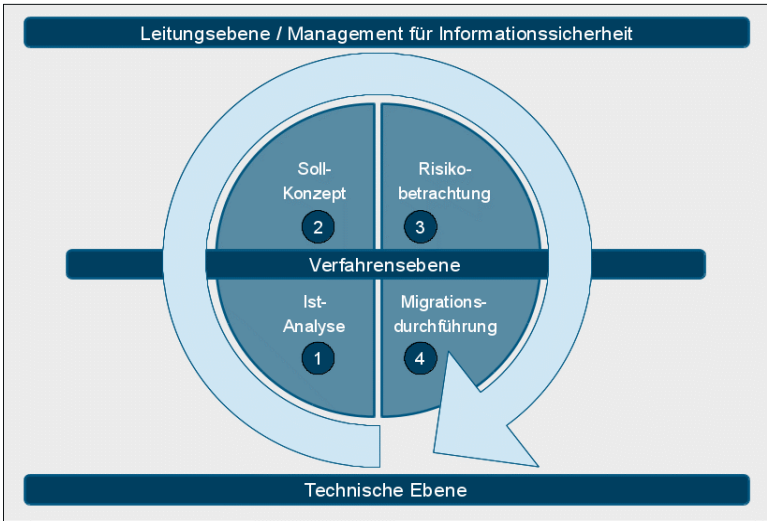

Abbildung 2: Überblick der vom Migrationsprozess betroffenen Organisationsebenen

Schon im Vorfeld der Migration sollten zusätzlich alle Interessengruppen (Stakeholder) mit

einer gezielten Informationspolitik frühzeitig in die Migration einbezogen werden.

Die wichtigsten Interessengruppen im öffentlichen Bereich sind:

- die Behördenleitung, verantwortlich für die Informationssicherheit,
- Entscheidungsträger(innen) aus den Fachbereichen und der IT,
- Anwender(innen),
- IT-Mitarbeiter(innen),
- die Interessenvertretungen,
- der/die Beauftragte für den Datenschutz,
- Bürger(innen) und Unternehmen.

Die Akzeptanz der Migration auf TLS 1.2 bei den jeweiligen Stakeholdern ist ein kritischer Erfolgsfaktor. Je nach Stakeholder ist aufgrund rechtlicher Rahmenbedingung die Zustimmung zum Migrationsvorhaben unabdingbar (BDSG, BPersVG, UP Bund etc.).

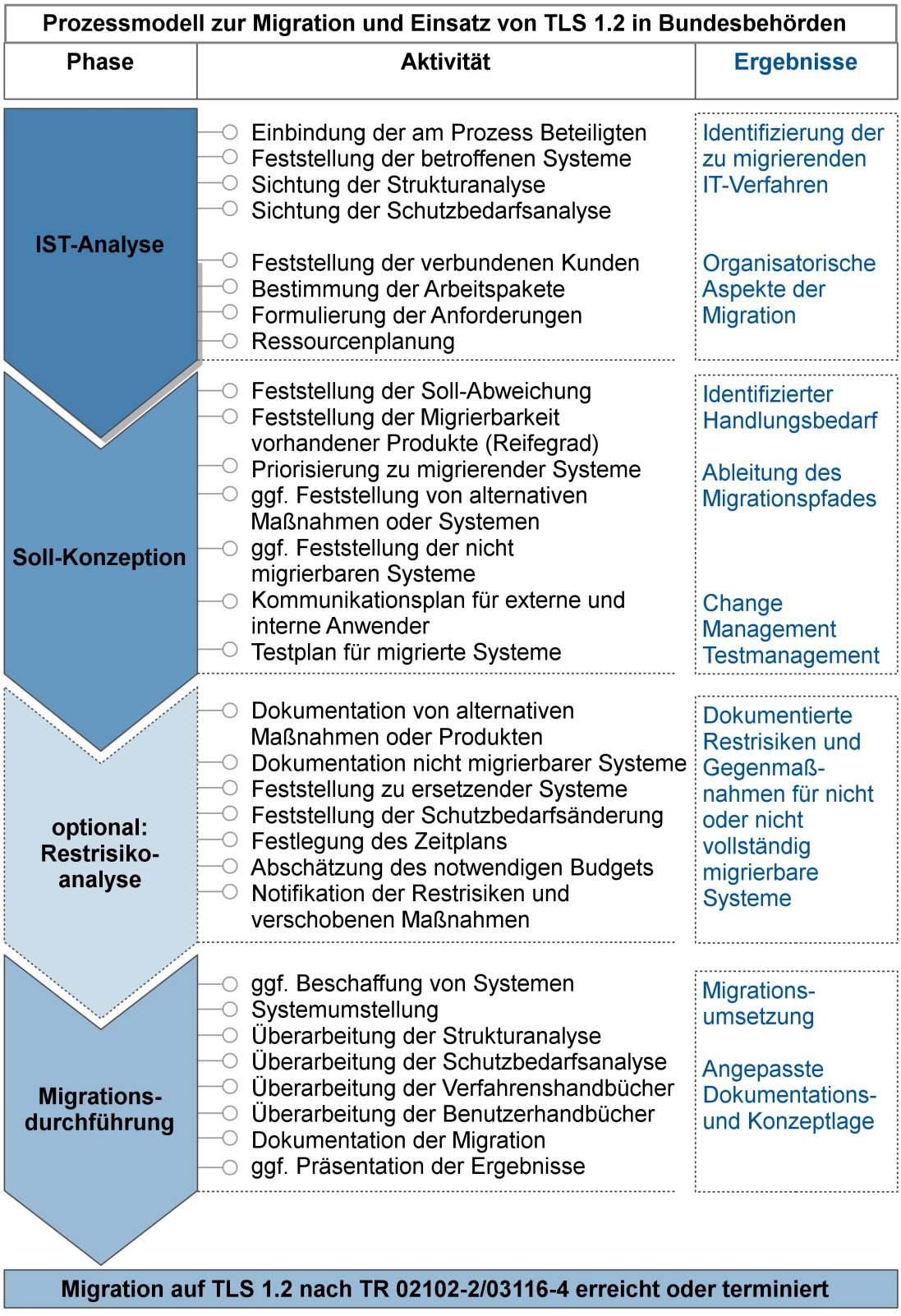

Abbildung 3: Der Migrationsprozess zu TLS 1.2 im Überblick

Die oben dargestellten Migrationsphasen umfassen die im Prozessmodell der Abbildung 3 dargestellten Migrationsaufgaben.

Die folgenden Unterkapitel beschreiben die in Abbildung 3 gezeigten Migrationsphasen und ihre Teilaufgaben. Der Beschreibung dieser Teilaufgaben wird der Zusammenhang zu den beteiligten Organisationsebenen vorangestellt.

4.1 Ist-Analyse

Ziel der Ist-Analyse ist die Erkenntnis darüber, welche Versionen des TLS/SSL-Protokolls in welchen Komponenten der IT-Verfahren zur Transportverschlüsselung eingesetzt werden und ob diese den Anforderungen des BSI-Mindeststandards [Mindeststandard SSL/TLS] sowie der technischen Richtlinie [TR-02102-2] entsprechen.

Folglich können damit die zu migrierenden Verfahren und Systeme identifiziert und die entsprechenden organisatorischen Ressourcen zugewiesen werden.

4.1.1 Organisation der Ist-Analyse

Die Migrationsaufgaben der drei Organisationsebenen bei der Ist-Analyse werden in nachfolgender Tabelle beschrieben.

Migrationsaufgaben	Leitungsebene	Verfahrens-ebene	Technische Ebene
Feststellung der betroffenen IT-Verfahren und IT-Systeme	G	M	V
Sichtung der IT-Sicherheitskonzepte (insbesondere der Struktur- und Schutzbedarfsanalyse) der IT-Verfahren	G	M	V
Feststellung der Migrationsfähigkeit der verbundenen Anwender	G	M	V
Bestimmung der Arbeitspakete und Ressourcenplanung	G	V	M

Tabelle 1: Organisation der Migrationsaufgaben der Ist-Analyse
Legende: G= Genehmigung, V= Verantwortung, M= Mitarbeit

Im Ergebnis der Ist-Analyse sind die zu migrierenden Verfahren und Systeme identifiziert, in der Regel tabellarisch dokumentiert, sowie die organisatorischen Aspekte der Migration bestimmt.

4.1.2 Aktivitäten der Ist-Analyse

Feststellung und Priorisierung der betroffenen IT-Verfahren und IT-Systeme

Anhand der in einer Behörde eingesetzten IT-Verfahren erfolgt eine Bewertung, ob diese für eine TLS-Migration in Betracht kommen (siehe „Migrationsstrategien in Kap. 3). Zu

untersuchen sind alle IT-Verfahren, deren Protokolle der Anwendungsschicht als Transportverschlüsselung TLS/SSL verwenden.

Für die Sektoren „Bürger-Behörden-Kommunikation“ (Sektor 1) und „Intra-Behörden-Kommunikation“ (Sektor 4) werden vor allem folgende Anwendungen zur Standardkommunikation zu untersuchen sein.

Auf der Seite des Kommunikationsanbieters sind dies z. B.:

- Webdienste/-server und Webanwendungen (z. B. Apache Webserver oder Microsoft IIS),
- Maildienste/-server (z. B. Microsoft Exchange Server),
- Authentisierungs- und Verzeichnisdienste (z. B. Active Directory oder OpenLDAP),
- Groupware (z. B. Microsoft Sharepoint Server),
- Web-Content-Management-Systeme (z. B. Government Site Builder),
- Serverbetriebssysteme (z. B. Windows Server 2008 R2 oder Linux SLES 11) oder
- Videokonferenz- und Telekommunikationssysteme.

Auf der Seite des Kommunikationskonsumenten:

- Internetbrowser (z. B.Internet Explorer, Firefox, Opera, Chrome),
- Client-Anwendungssoftware (z. B. Microsoft Outlook, Mozilla Thunderbird),
- Client-Betriebssysteme (z. B. Microsoft Windows XP, Windows 7, Windows 8) oder
- Videokonferenz- und Telekommunikationsanwendungen.

Untersuchung der Kommunikations-Ports

Zu untersuchen sind alle Standarddienste, wie die oben aufgeführten Anwendungen, die über bestimmte Standardports kommunizieren, da diese Standardports Aufschluss über die Anwendungsprotokolle unter Nutzung von TLS geben können. Folgend eine Auswahl an gängigen TLS/SSL-gesicherten Diensten:

Port	Gesicherter Dienst	Protokoll	Verwendung
443	HTTP (Hypertext Transfer Protokoll)	https	Webdienst
465, 587	SMTP (Simple Mail Transfer Protokoll)	Ssmtp, smtps	Maildienst (Postausgang)
995	POP3 (Post Office Protokoll)	Pop3s	Maildienst (Posteingang)
636	LDAP (Lightweight Directory Access Prot.)	Ldaps	Verzeichnisdienst
585, 993	IMAP (Internet Message Access Protokoll)	Imap4-ssl	Mailverwaltungsdienst
989, 990	FTP (File Transfer Protokoll)	ftps	Datentransferdienst
992	TELNET (Telecommunication Network)	telnets	Fernsteuerungsdienst

Tabelle 2: Auswahl Anwendungsdienste/-protokolle mit TLS/SSL-Bezug[1]

Untersuchung der eingesetzten Technologie

Im nächsten Schritt soll die Untersuchung der Technologien der Komponenten sowie die entsprechende Versionsnummer der Technologieprodukte folgen.

Dazu gehört die Identifizierung

- der Komponenten der IT-Verfahren,
- der Produktbezeichnungen und Versionsnummern der Komponenten,
- des Betriebssystems,
- die von den Komponenten verwendeten Kryptobibliotheken samt ihrer TLS-1.2-Fähigkeit und der verwendeten Cipher-Suites und
- ihres Schutzbedarfs[2].

Die Ergebnisse der Ist-Analyse der IT-Struktur der IT-Verfahren können in tabellarischer Form dargestellt werden.

	Komponente	Produkt	Produktversion	Basis-Betriebssystem	Kryptobibliothek	TLS-1.2-fähig	Verwendete Cipher	Schutzbedarf
1	Webserver / Webdienst	Apache	2.4.7	Debian Linux	OpenSSL 0.98	Nein	...	Normal
2	Webserver / Webdienst	Internet Information Server	8.5	Windows Server 2012 R2	Schannel.dll	Ja	...	Hoch
3	...							

Tabelle 3: Beispiel einer Ist-Analyse der IT-Struktur und IT-Verfahren (serverseitig)

1 Je nach technischer Konfiguration des betroffenen IT-Verfahrens können abweichende Ports Verwendung finden. Die betroffenen Ports sind daher je System konkret festzustellen, z. B. mit dem Hilfsmittel OpenVAS.

2 In den Beispieltabellen wird aus redaktionellen Gründen statt des Schutzziels Vertraulichkeit, Integrität und Verfügbarkeit nur ein allgemeiner Schutzbedarf genannt. TLS 1.2 adressiert vorrangig die Vertraulichkeit, wobei die Integrität der Daten zusätzlich geschützt wird. Zudem bestimmt das Schutzniveau eines einzelnen Schutzziels den Gesamtwert des allgemeinen Schutzbedarfs.

	Komponente	Produkt	Produkt-version	TLS-1.2-Fähig	Schutzbedarf	Verbreitung
1	Webclient	Internet Explorer	8/Win 7	Ja	Hoch	30%
2	Webclient	Internet Explorer	6/Win XP	Nein	Hoch	15%
3	Webclient	Mozilla Firefox	27	Ja	Hoch	60%
4	...					

Tabelle 4: Beispiel einer Ist-Analyse der IT-Struktur und IT-Verfahren (clientseitig)

Untersuchung der Zertifikate

TLS 1.2 mit PFS kann mit vorhandenen PKI-Zertifikaten betrieben werden, weil Zertifikate der Authentisierung, nicht aber der Transportsicherung der Kommunikation dienen.

Im Zuge der Migration sollte die Kompatibilität der Zertifikate zu den Vorgaben aus Kapitel 4.1 der [TR-03116-4] geprüft werden:

	Zertifikat	Herausgeber	Typ	Verschlüsselungsfunktion und -länge	Hash-Funktion und -Länge	Gültigkeitsdauer	Rückrufprüfung möglich	KeyUsage eingeschränkt
1	Webserver	Unternehmen A	Wild Card Zertifikat	RSA 2048	SHA-256	3 Jahre	Ja	Ja
2	E-Mail-Server	Unternehmen A	Einzelzertifikat	RSA 2048	SHA-1	5 Jahre	Ja	Ja
3	LDAP-Server	-	Selbst Signiertes Einzelzertifikat	RSA 1024	SHA-1	10 Jahre	Nein	Nein
4	...							

Tabelle 5: Beispiel einer Ist-Analyse der PKI-Zertifikate

Sichtung der IT-Sicherheitskonzepte (insbesondere der Struktur- und Schutzbedarfsanalyse) der IT-Verfahren

Auf Grundlage der IT-Sicherheitskonzepte der IT-Verfahren können diejenigen Komponenten eines IT-Verfahrens identifiziert werden, deren Anwendungsprotokoll zur Transportverschlüsselung das SSL- bzw. TLS-Protokoll verwendet. Hierzu ist die Dokumentation der Technologien der Komponenten sowie die entsprechende Versionsnummer der Technologieprodukte zu recherchieren. Diese Informationen geben Aufschluss über die aktuelle TLS-Kompatibilität und demnach über den Handlungsbedarf sowie die anzuwendende Migrationsstrategie.

Feststellung der Migrationsfähigkeit der verbundenen Anwender

Zur Umstellung auf TLS 1.2 muss neben der Migrationsfähigkeit der betroffenen IT-Verfahren und -Systeme insbesondere die Kompatibilität auf der Gegenseite der Kommunikation (Clientseite) analysiert werden. Die Kompatibilität zur Kommunikation auf Basis von TLS 1.2

muss bei den Clients ebenso gegeben sein. Hier ist die Migrationsregel für Sektor 1 (siehe Kapitel 3) zu beachten.

Bestimmung der Arbeitspakete und Ressourcenplanung

Die Ergebnisse der Ist-Analyse können in einen vorläufigen Projektplan einfließen, in welchem zuerst die erforderlichen Arbeitspakete der Migration und die dafür erforderlichen Zeitaufwände, möglichen Beschaffungskosten und Personalaufwände abgeschätzt werden.

4.1.3 Technische Hilfsmittel für die Ist-Analyse

Die Analyse der Server und Clients hinsichtlich der eingesetzten TLS-Versionen und Cipher-Suiten kann mittels Analysetools (ssllabs.com [SSL TEST]) oder detailliert mit dem Tool [OpenVAS] durchgeführt werden.

Zur Evaluierung der Kompatibilität der ermittelten Komponenten eines IT-Verfahrens bzw. der in den Komponenten verwendete Technologien, ist im Anhang eine Übersicht in Form einer Kompatibilitätsmatrix dargestellt. Die Matrix macht Aussagen über die TLS-1.2-Kompatibilität von Technologien, die in der Bundesverwaltung überwiegend eingesetzt werden und dient zur Vorauswahl für die zu migrierenden Komponenten.

4.2 Soll-Konzept

Im Soll-Konzept wird die Migration der einzelnen IT-Verfahren und IT-Systeme, also die Herstellung des Zielzustands gemäß des Mindeststandards TLS 1.2 bei Abweichungen vom festgestellten Ist-Zustand, zeitlich und fachlich priorisiert.

Im Ergebnis liegen dann eine Prioritätenliste der zu migrierenden Verfahren samt eines abgestimmten Projektplans sowie ein Testplan vor. Dafür erlässt die Behörde eine Richtlinie über die zu verwendenden Cipher-Suites gemäß des Mindeststandards TLS 1.2.

Der Projektplan sollte enthalten:

- Prioritäten aller betroffenen IT-Verfahren und IT-Systeme;
- Auflistung der erforderlichen Beschaffungsmaßnahmen (ggf. mit Anträgen, Lieferzeiten und alternativen Produkten);
- Definition der Testfälle in einer Testmatrix;
- Beschreibung der erforderlichen Maßnahmen zur Systemumstellung.

Die genannten Informationen sollten mindestens mit den nachfolgend aufgeführten Projektrahmenbedingungen in einem Projektplan abgebildet werden:

- Ressourcenzuweisung
- Budget
- Zeitplan

Das Migrationsvorhaben kann anhand eines Kommunikationsplans an die internen und externen Nutzer der IT-Systeme und IT-Fachverfahren vermittelt werden.

4.2.1 Organisation des Soll-Konzepts

Die Migrationsaufgaben der drei Organisationsebenen bei der Soll-Konzeption werden in nachfolgender Tabelle beschrieben.

Migrationsaufgaben	Leitungsebene	Verfahrensebene	Technische Ebene
Feststellung der Soll-Abweichung betroffener IT-Verfahren und IT-Systeme	G	M	V
Feststellung der Migrierbarkeit vorhandener Systeme sowie Priorisierung der migrierbaren Systeme	G	M	V
Feststellung der nicht migrierbaren Systeme	G	M	V
Kommunikationsplanung zum Vorhaben der Migration an den relevanten Adressatenkreis	G	V	M
Testplan für migrierte Systeme	G	M	V

Tabelle 6: Migrationsaufgaben der Ist-Analyse
Legende: G= Genehmigung, V= Verantwortung, M= Mitarbeit

4.2.2 Aktivitäten des Soll-Konzepts

Feststellung der Soll-Abweichung betroffener IT-Verfahren und IT-Systeme

Zur Migration zum TLS-1.2-Protokoll mit Perfect Forward Secrecy (PFS) gemäß Mindeststandard TLS 1.2 sind beide Seiten der Kommunikation zu betrachten.

Dazu wird nochmals auf die Migrationsregel für Sektor 1 (siehe Kapitel 3) hingewiesen, die besagt, dass Behörden im Sektor 1 „Bürger-Behörden-Kommunikation“ das TLS-1.2-Protokoll mit PFS für ihre Systeme primär, aber nicht ausschließlich anzubieten haben, da die Seite des Bürgers nicht im Verfügungsbereich der betreffenden Behörde liegt. Das bedeutet, dass die Behörde immer und zuerst das TLS-1.2-Protokoll mit PFS beim Aufbau der schutzbedürftigen Kommunikation anzubieten hat, aber bei der Schlüsselaushandlung die vom Bürger maximal unterstützte TLS-Protokollversion und Schlüssel akzeptieren kann. Schwache Schlüssel oder Protokollversionen sind dabei dennoch zu vermeiden.

Diese Ausnahme gilt nicht für die verbleibenden Sektoren 2-4 (siehe Abbildung 2). In diesen Sektoren ist das Protokoll TLS 1.2 mit PFS zu verwenden.

Die einzusetzenden Cipher-Suites sind in Tabelle 7 [TR-02102-2, Seite 6, Tab. 1] gegeben:

	Schlüsseleinigung und -authentisierung		Verschlüsselung	Betriebs-modus	Hash	Verwendung bis
TLS_	ECDHE_ECDSA_	WITH_	AES_128_	CBC_GCM_	SHA256	2021+
			AES_256_	CBC_GCM_	SHA384	2021+
	ECDHE_RSA_	WITH_	AES_128_	CBC_GCM_	SHA256	2021+
			AES_256_	CBC_GCM_	SHA384	2021+
	DHE_DSS_	WITH_	AES_128_	CBC_GCM_	SHA256	2021+
			AES_256_	CBC_	SHA256	2021+
				GCM_	SHA384	2021+
	DHE_RSA_	WITH_	AES_128_	CBC_	SHA256	2021+
				GCM_	SHA384	2021+
			AES_256_	CBC_	SHA256	2021+
				GCM_	SHA384	2021+

Tabelle 7: Die auszuwählenden Cipher-Suites gemäß TR-02102-2

Die Dokumentation der Analyseergebnisse kann wie folgt tabellarisch erfasst werden:

Nr	Pro-dukt	Produkt-version	Basis-Be-triebs-system	Krypto-Bibliothek	TLS-1.2-fä-hig	Verwen-dete Cipher	Schutz-bedarf	Migra-tion	Einzuset-zende Ci-pher	Prio-rität
Server										
1	Apache Webser ver	2.4.7	Debian Linux	OpenSSL 0.89	Nein	RSA_...	Nor-mal	Ja	DHE_...	2
2	Internet Infor-mation Server	8.5	Windows Server 2012 R2	SChan-nel.dll	Ja	DHE_...	Hoch	Nein	DHE_...	-
3	...									
Client										
4	Internet Explo-rer	8	Verbrei-tung: 30%	SChan-nel.dll	Ja	...	Hoch	Nein	Ephemeral (Config)	3
5	Mozilla Firefox	27	Verbrei-tung: 60%	NSS, PKCS #11	Ja	...	Hoch	Nein	Ephemeral (Config)	3
6	...									

Tabelle 8: Beispiel zur Erfassung der TLS-1.2-Kompatibilität

Feststellung des Migrationsbedarfs für Zertifikate

Die TR-03116-4 gibt vor, dass

1. der Aussteller eines Zertifikats vertrauenswürdig sein muss, wobei die Vertrauenswürdigkeit an seiner Zertifizierung bzw. Auditierung und dem Rechtsstand des Ausstellers gemessen wird [TR-03116-4, Kap. 4.1.1];

2. Zertifikationsattribute prüfbar sein müssen, vor allem der Zertifikatsrückruf (CRLDistributionPoint, AuthorityInfoAccess) und die Einschränkung der Zertifikatsverwendung (BasicConstraints, KeyUsage, keine Wildcards im Common Name) [TR-03116-4, Kap. 4.1.2, Kap. 4.1.3] und
3. die Domänenparameter und Schlüssellängen aus Tabelle 9 [TR-03116-4, Kap 4.1.4, Tabelle 11] einzuhalten sind.

Algorithmus	Minimale Schlüssellänge	Min. Outputlänge der Hashfunktion	Verwendung bis
ECDSA	224 Bit	SHA224	2021+
DSA	2048 Bit	SHA224	2021+
RSASSA-PSS	2048 Bit	SHA224	2021+

Tabelle 9: Mindestschlüssellängen für X.509-Zertifikate

Sollte eine dieser Vorgaben nicht erfüllt sein, ist das Zertifikat zu erneuern. In diesem Fall können die Ergebnisse der Zertifikatsprüfung wie in Tabelle 10 notiert werden.

	Zertifikat	Herausgeber	Typ	Verschlüsselungsfunktion und -Länge	Hash-Funktion und -Länge	Gültigkeitsdauer	Rückrufprüfung möglich	KeyUsage eingeschränkt	Migration?	Begründung
1	Webserver (extern erreichbar)	Unternehmen A	Wild Card Zertifikat	RSA 2048	SHA256	3 Jahre	Ja	Ja	Ja	Wildcard-Zertifikat
2	E-Mail-Server	Unternehmen A	Einzelzertifikat	RSA 2048	SHA1	5 Jahre	Ja	Ja	Ja	Hash-Funktion
3	LDAP-Server	-	Selbst Signiertes Einzelzertifikat	RSA 1024	SHA1	10 Jahre	Nein	Nein	Ja	Hash-Funktion, Gültigkeitsdauer, Rückrufprüfung, KeyUsage
4	...									

Tabelle 10: Beispiel zur Erfassung der X.509-Zertifikatskompatibilität

Feststellung der Migrierbarkeit vorhandener, sowie Priorisierung der migrierbaren Systeme

Aus der dokumentierten Soll-Abweichung kann zunächst gefolgert werden, ob Systeme nur neu konfiguriert oder auf aktuellere Versionen migriert werden müssen. Eine Priorisierung und damit auch zeitliche Anordnung des Migrationsvorhabens ergibt sich dann aus der Gesamtschau der zu migrierenden Anwendungen, ihrem Schutzbedarf und der Zahl der

angeschlossenen Nutzer.

Feststellung der nicht migrierbaren Systeme

Aus der dokumentierten Soll-Abweichung kann weiterhin gefolgert werden, welche Systeme nicht migrierbar sind, etwa weil die Produktwartung und -unterstützung vom Hersteller aufgekündigt wurde. Eine Dokumentation ist erforderlich.

Testplan für migrierte Systeme

Bei Bedarf kann aus dem Migrationsplan ein Testplan abgeleitet werden.

Kommunikationsplanung zum Vorhaben der Migration an den relevanten Adressatenkreis

Die Ergebnisse oder ausgewählte Aspekte der Ist-Analyse, der dokumentierten Soll-Abweichung sowie des Testplans, sollten mindestens an die betroffenen Nutzer und ggf. an alle Anspruchsgruppen (siehe Kap. 4) kommuniziert werden. Dazu gehört auch die Vorbereitung des Supports auf die zu erwartenden Fragen.

4.3 Risikobetrachtung

In der Risikoanalyse werden die Risiken der nicht vollständig erfolgten migrierten Fachverfahren und Anwendungen untersucht. Im Ergebnis sind die Restrisiken zu dokumentieren und geeignete Gegenmaßnahmen einzurichten und zu dokumentieren.

Sollte das Schutzniveau der Alternativen nicht an den Mindeststandard TLS 1.2 heranreichen, so sind diese Maßnahmen zu notifizieren. Dabei ist zu beachten, dass eine Risikoanalyse lediglich einen Zeitpunkt abbildet und auch Legacy-Systeme immer wieder von neuen Attacken betroffen sein können, wie jüngst beispielsweise durch Poodle, Breach oder Logjam.

4.3.1 Organisation der Risikobetrachtung

Die Migrationsaufgaben der drei Organisationsebenen bei der Risikoanalyse werden in nachfolgender Tabelle beschrieben.

Migrationsaufgaben	Leitungsebene	Verfahrens-ebene	Technische Ebene
Dokumentation nicht oder nicht vollständig migrierbarer und zu ersetzender Systeme	G	M	V
Planung und Umsetzung von alternativen Maßnahmen zur Risikominimierung für nicht migrierbare Systeme	G	M	V
Prüfung/Aktualisierung/Erstellung von IT-Risikoanalysen für betroffene Verfahren	G	M	V
Notifikation der Restrisiken und verschobenen Maßnahmen	G/V	M	M

Tabelle 11: Migrationsaufgaben der Risikobetrachtung
Legende: G= Genehmigung, V= Verantwortung, M= Mitarbeit

4.3.2 Aktivitäten der Risikobetrachtung

Dokumentation nicht migrierbarer Systeme

Alle IT-Systeme, die nicht auf die TLS-Version 1.2 migriert werden können, sind zu dokumentieren.

Feststellung zu ersetzender Systeme

Werden potenzielle Schäden bei Eintritt einer Gefährdung als nicht tragbar eingestuft, sind die betroffenen Systeme als „zu ersetzen“ zu dokumentieren.

Die Neubeschaffung dieser Standarddienste oder Neuausschreibung von Fachverfahren liegt daher nahe. Bis zum Zeitpunkt der Inbetriebnahme der erneuerten Standarddienste oder Fachverfahren sind Alternativmaßnahmen einzusetzen, z. B. TLS-Proxies. Sollte das Schutzniveau der Alternativen nicht an den Mindeststandard TLS 1.2 heranreichen, so sind diese Maßnahmen zu notifizieren.

Prüfung/Aktualisierung/Erstellung von IT-Risikoanalysen für betroffene Verfahren

Ergibt sich der Bedarf der Nutzung weiterer TLS/SSL-Implementierungen neben der Version TLS 1.2, muss in einer Risikoanalyse abgewogen werden, welche Restrisiken durch diese Anforderung bestehen, und wie diesen entgegengewirkt werden kann. Dabei ist zu analysieren, welche Gefährdungen wirken können und zu schätzen, wie wahrscheinlich das Eintreten einer Gefährdung ist bzw. mit welchem potenziellen Schaden bei Eintritt einer Gefährdung zu rechnen ist.

Notifikation der Restrisiken und verschobenen Maßnahmen

Sollte eine Anwendung oder ein System, die/das schützenswerte Daten überträgt, im Ergebnis des in diesem Leitfaden vorgestellten Vorgehens nicht oder nur eingeschränkt innerhalb der vom Mindeststandard TLS 1.2 vorgegebenen Fristen migriert werden können, ist die Notifizierung beim BSI durchzuführen.

Diese beginnt mit einer Aufbereitung des Sachverhalts über das Notifikationsformular im internen Bereich der Sicherheitsberatung des BSI, welches mit einem internen Entscheidungsvermerk an die IT-Leitung weitergeleitet wird. Nach Unterzeichnung der Notifizierung ist diese direkt an die Sicherheitsberatung des BSI, an den IT-Sicherheitsbeauftragten des Ressorts oder dessen beauftragte Stelle zu senden.

4.4 Migrationsdurchführung

In der Migrationsdurchführung wird die in der Soll-Konzeption erstellte Planung ausgeführt.

4.4.1 Organisation der Migrationsdurchführung

Die Migrationsaufgaben der drei Organisationsebenen bei der Migrationsdurchführung werden in nachfolgender Tabelle beschrieben.

Migrationsaufgaben	Leitungsebene	Verfahrens-e-bene	Technische Ebene
Durchführung und Dokumentation der Migration, ggf. Beschaffung von Systemen	G	M	V
Test der Migration	G	M	V
Revision der Strukturanalyse, Schutzbedarfsanalyse und des IT-Sicherheitskonzeptes sowie des Betriebshandbuches	G	M	V
Ggf. Präsentation der Ergebnisse	G	V/M	V/M

Tabelle 12: Migrationsaufgaben der Ist-Analyse
Legende: G= Genehmigung, V= Verantwortung, M= Mitarbeit

4.4.2 Aktivitäten der Migrationsdurchführung

Durchführung und Dokumentation der Migration, ggf. Beschaffung von Systemen

Die für die Migration erforderlichen Systemumstellungen sind gemäß des Migrationsplans (Kap. 4.2) durchzuführen und zu dokumentieren.

Ausgewählte Migrationsbeispiele sind in Kapitel 5 illustriert.

Die geplanten Beschaffungsmaßnahmen sind durchzuführen.

Aufgeschobene Migrationsaufgaben, z. B. für nicht vollständig migrierte Systeme, sind zu dokumentieren, zu notifizieren und für einen späteren Zeitpunkt zu terminieren (Kap. 4.3.2).

Test der Migration

Die für die Migration erforderlichen Systemumstellungen sind gemäß der Testpläne (Kap.4.2.1) durchzuführen.

Revision der Systemdokumentation

Die erfolgten Systemumstellungen sind entsprechend zu dokumentieren. Davon betroffen sind IT-Sicherheitskonzepte (insbesondere der Struktur- und Schutzbedarfsanalyse) sowie das Betriebshandbuch, also System- und Prozessdokumentation sowie Benutzerhandbücher (Kap. 4.4.1. Veraltete Dokumente sind zu widerrufen.

Präsentation der Ergebnisse

Die Ergebnisse der Migration sind gegenüber der Behördenleitung und weiteren möglichen Interessengruppen aufzubereiten.

5 Fallbeispiel

Das folgende Fallbeispiel aus dem Bereich Bürger-Behörden-Kommunikation illustriert den gesamten Migrationsprozess in aller Kürze am typischen Beispiel einer öffentlichen Website mit Kommunikationsformular für den Bürger.

Nachdem die Amtsleitung der Behörde die Migration auf TLS 1.2 mit PFS beschlossen und die entsprechenden Verantwortlichen für das IT-Management und für die IT-Sicherheit mit dieser beauftragt hat, stellen die Verantwortlichen den Ist-Zustand fest [Kap. 4.1.1, S. 13].

Die Behörde kann zur Aufdeckung aller relevanten Systeme das Werkzeug OpenVAS aus dem Rahmenvertrag des BSI abrufen und einsetzen.

Die Verantwortlichen stellen anhand der Schutzbedarfsanalyse auf Basis des Sicherheitskonzepts oder im Zuge der Migration außerdem fest, ob in der Kommunikation mit dem Bürger über ein Formular auf der Website der Bundesbehörde schutzbedürftige Daten übertragen werden, nämlich Name, E-Mail-Adresse und eine Nachricht, welche weitere schutzbedürftige Daten enthalten kann. Daher wird analog zum IT-Grundschutz, Maßnahme M 5.66 Verwendung von TLS/SSL, das TLS-Protokoll für die Datenübertragung eingesetzt.

Das System wird dem Sektor „Bürger-Behörden-Kommunikation“ zugeordnet, in dem laut Mindeststandard TLS 1.2 das Protokoll TLS 1.2 mit PFS anzubieten ist. Veränderungen auf niedrigere Protokollversionen bei laufenden Sitzungen, so genannte Protocol Downgrades, sind zu unterbinden. Für die Authentisierung soll die TR-03116-4 herangezogen werden.

Aus der Ist-Analyse könnte sich etwa folgende Kompatibilitätstabelle ergeben [Kap. 4.2.1, S. 18]:

Nr	Produkt	Produktversion	Basis-Betriebssystem	Krypto-Bibliothek	TLS-1.2-FÄHIG	Verwendete Cipher	Schutzbedarf	Migration	Einzusetzende Cipher	Priorität
Server										
1	Apache Webserver	2.4.7	Debian Linux	OpenSSL 0.89	Nein	RSA_...	Hoch	Ja	DHE_...	2
Client										
3	Internet Explorer	8	Verbreitung: 30%	SChannel.dll	Ja	...	Hoch	Nein	Ephemeral (Config)	-
4	Mozilla Firefox	27	Verbreitung: 60%	NSS, PKCS #11	Ja	...	Hoch	Nein	Ephemeral (Config)	-
5	Internet Explorer	6	Verbreitung: 10%	SChannel.dll	Nein	SSL3, RC4	Hoch	Nein	Ephemeral (Config)	-

Tabelle 13: Beispielhafte Kompatibilitätstabelle für die Transportsicherung

Da die Bundesbehörde keinen Einfluss auf die von Bürgern verwendeten Browser hat, kann sie dort keine Migration auslösen. Die Bundesbehörde reagiert wie folgt:

> Die 10% der sich mit dem Internet Explorer 6 verbindenden Nutzer werden aufgrund des Schutzbedarfs der Daten auf alternative Browser hingewiesen und von der Website ausgeschlossen (etwa über eine angepasste 404-Seite). Transportverschlüsselung wird ab der Version TLS 1.1 angeboten. Da der eingesetzte Apache Webserver in der vorhandenen Konfiguration nicht TLS-1.2-kompatibel ist, muss er migriert werden. Damit ist die Analyse der Restrisiken [Kap. 4.3, S. 21] entbehrlich.
>
> Da TLS 1.2 mit PFS in der Bürger-Behörden-Kommunikation lediglich prioritär angeboten, nicht wie in den übrigen Sektoren zwangsläufig eingesetzt werden muss, ist die Nutzung von TLS 1.1 gemäß TR-02102-2 gestattet, sofern TLS 1.2 nicht möglich ist. Der Webserver handelt dann mit dem Browser des Bürgers die passende und von der Behörde maximal zulässige Cipher-Suite aus.
>
> Sollten die Migration aus technischen oder organisatorischen Gründen nicht (termingerecht) durchführbar sein, sind Gründe, betroffene Systeme sowie geplante Maßnahmen zu notifizieren.

Die Kompatibilitätsanalyse der Zertifikate zeigte einen Migrationsbedarf an:

Zertifikat	**Herausgeber**	**Typ**	**Verschlüsselungsfunktion und -Länge**	**Hash**	**Gültigkeit**	**Rückrufprüfung möglich**	**KeyUsage eingeschränkt**	**Migration?**	**Begründung**
Webserver (extern erreichbar)	Unternehmen A	Wild Card Zertifikat	RSA 2048	SHA 256	3 Jahre	Ja	Ja	Ja	Wildcard-Zertifikat
E-Mail-Server	Unternehmen A	Einzelzertifikat	RSA 2048	SHA 1	5 Jahre	Ja	Ja	Ja	Hash-Funktion
LDAP-Server	-	Selbst Signiertes Einzelzertifikat	RSA 1024	SHA 1	10 Jahre	Nein	Nein	Ja	Hash Gültigkeit, Rückrufprüfung, KeyUsage

Tabelle 14: Beispielhafte Kompatibilitätstabelle für die Authentisierung

Mit der Entscheidung der Amtsleitung gibt diese die notwendigen Ressourcen für die

Migration der Transportsicherung und der Authentisierung frei und weist die Verantwortlichen zur Durchführung an. Sollte das von den Verantwortlichen geschätzte Datum des Migrationsabschlusses nach der im Mindeststandard genannten Frist liegen, so notifiziert die Behörde diesen Umstand gemäß der Vorgaben des Mindeststandards.

6 Anhang

6.1 Die technische Migration der Transportsicherung

Die Migration eines Webservers verläuft zweiteilig, also die Aktualisierung des Webservers selbst und der eingebundenen Kryptographiebibliothek. Da auch Webservices auf der Transportebene von Webservern ausgeliefert werden, sind die folgenden Hinweise für Webservices analog umsetzbar.

6.1.1 Migration der Webserver

6.1.1.1 Apache & Co.

Apache greift für die Verschlüsselung auf Module von OpenSSL oder GnuTLS zurück.

Bei der Migration des Webservers ist daher darauf zu achten, dass dieser die entsprechenden Module unterstützt. TLS 1.2 mit PFS wird laut der Arbeitshilfe [Kap. 6.3.3, S. 34] von OpenSSL ab der Version 1.0.1c unterstützt. Diese Bibliothek wird mit Apache der Version 2.2.2 und ab 2.4.1 unterstützt.

Nginx unterstützt ab der Version 1.0.6 OpenSSL der Version 1.0.1c.

6.1.1.2 Internet Information Server

Die TLS-Funktionalität der Windows Server und Clients wird von Microsofts Kryptographiebibliothek `SChannel.dll` bereitgestellt. TLS 1.2 mit PFS wird ab dem Windows Server 2008 SR2 und Windows 7 unterstützt [Kap. 6.3.1 und 6.3.3]. Für frühere Windows-Versionen ist eine Aktualisierung oder Rekonfiguration der Kryptographiebibliothek `SChannel.dll` nur durch Austausch der gesamten Betriebsplattform zu erreichen. Eine Migration auf eine Windows-Betriebssystemplattform ab Version 2008 R2 oder Windows 7 wird daher dringend empfohlen.

Sollte auf einem Windows Server ein Webserver von Apache oder Nginx betrieben werden, so gelten die Anmerkungen aus dem vorherigen Kapitel. Die Apache oder Nginx Webserver greifen auf Windows-Systemen nicht auf Microsofts Kryptobibliothek zu.

Allerdings ist folgender Seiteneffekt zu bedenken: Sollte nur der Webserver ausgetauscht werden, findet jede andere SSL-verschlüsselte Übertragung von möglicherweise sensitiven Daten z. B. mit Datenbank-Servern oder Microsofts Update Servern nicht mit TLS 1.2 mit PFS statt.

6.1.2 Migration der Kryptographiebibliotheken

6.1.2.1 OpenSSL

Die Transportverschlüsselung wird für Option 1 in der apache.conf für Apache ab Version 2.4 wie folgt konfiguriert:

```
SSLEngine On
# erlaube nur TLS 1.0 bis TLS 1.2
SSLProtocol All -SSLv2 -SSLv3
# vermeide CRIME/BREACH Angriffe
SSLCompression Off
# Die Priorisierung des Servers hat Vorrang vor der des Clients
SSLHonorCipherOrder On
# Cipher-Suites mit PFS bevorzugen, 3DES für IE8(XP) erlauben
SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384
EECDH+aRSA+SHA256 EECDH+AESGCM EECDH EDH+AESGCM EDH+aRSA HIGH !
MEDIUM !LOW !aNULL !eNULL !LOW !RC4 !MD5 !EXP !PSK !SRP !DSS"
# Header add Strict-Transport-Security "max-age=1555200" # HTTPSonly
für 180 Tage erzwingen
```

Sollte sich die Behörde für die Option 2 entscheiden, dann ist nach der Aktualisierung der OpenSSL-Bibliothek nur folgende Zeile der vorherigen Konfiguration der apache.conf zu ändern:

```
…
# erlaube SSL 3.0 bis TLS 1.2
SSLProtocol all -SSLv2
# vermeide Man-In-The-Middle nach CVE-2009-3555
SSLInsecurRenegotiation Off
...
```

6.1.2.2 SChannel.dll

Die Transportverschlüsselung wird für Microsoft-Server unter Microsoft-Betriebssystemen über die SChannell.dll konfiguriert. Aufgrund der regelmäßigen Patches seitens des Herstellers, ist eine statische Anleitung zur Konfiguration an dieser Stelle ungeeignet. Stets aktuelle Hinweise zur standardkonformen Einrichtung von TLS 1.2 sowie eine konfigurierbare Batch-Datei für die Konfiguration der Cipher-Suites finden sich auf der BSI-Homepage unter www.bsi.bund.de.

Es sei darauf hingewiesen, dass Microsoft mit dem Update von Windows 7 im August/September 2014 auf TLS 1.2 umgestellt hat. Darüber hinaus bietet Microsoft seit dem 13.05.2015 ein Update zur manuellen Installation an, das die Reihenfolge der verwendeten

Verschlüsselungsalgorithmen in Windows abändert und zusätzliche Cipher-Suites mit Unterstützung von PFS integriert. Über WSUS/Windows Update wird das Update ab dem vierten Quartal 2015 ausgeliefert.

6.1.3 Migration der Browser

Die Eignung eines Browsers zu TLS 1.2 mit PFS kann, sofern nicht schon während der Ist-Analyse [Kap. 4.1.1, S. 13] und Soll-Feststellung [Kap. 4.2.1, S. 18] geschehen, auf verschiedenen Wegen festgestellt werden:

- anhand der Arbeitshilfe [Kap. 6.3.2, S. 34],
- anhand von Verbindungsversuchen zu einem Webserver, der nur TLS 1.2 mit PFS anbietet oder
- anhand von Testprogrammen.

Die Liste der vom Browser unterstützen Cipher-Suites sollte folgende Einträge enthalten, wie sie am Beispiel des Testprogramms der Universität Hannover[3] nachfolgend dargestellt werden:

```
(c0,2b) ECDHE-ECDSA-AES128-GCM-SHA256

(c0,2f) ECDHE-RSA-AES128-GCM-SHA256

...

Preferred SSL/TLS version: TLSv1

..

This connection uses TLSv1.2 with ECDHE-RSA-AES128-GCM-SHA256 and a 128
Bit key for encryption.
```

Sollte der Browser keine der im Mindeststandard genannten Cipher-Suites [Kap. 4.1, S. 13] unterstützen, ist eine Migration vorzunehmen.

6.1.3.1 Internet Explorer

Für Windows-Clients bis zur Produktversion Vista kommen die in den nachfolgenden Kapiteln beschriebenen alternativen Browser in Frage, die eigene Kryptobibliotheken einsetzen und damit nicht auf die Microsoft-eigene `SChannel.dll` zugreifen.

Für Windows-Clients ab der Produktversion 7 kommt Internet Explorer ab der Version 8 in Frage.

TLS 1.2 kann dort über „Internetoptionen/Erweitert/Sicherheit“ und dort die Option „TLS 1.2“ aktiviert werden.

3 https://cc.dcsec.uni-hannover.de

In Windows 8 ist TLS 1.2 mit PFS standardmäßig aktiviert.

6.1.3.2 Firefox

Firefox unterstützt ab der Version 24 das Protokoll TLS 1.2, das aber nicht voreingestellt ist. Es wird wie folgt aktiviert[4]:

Eingeben von `about:config` in die Adressleiste des Browsers, dann suchen nach `secure.tls.version:`

`secure.tls.version.max` sollte auf Wert `3` (=TLS 1.2) eingestellt sein

`secure.tls.version.min` sollte auf Wert `2` (=TLS 1.1) eingestellt sein, kann aber in Ausnahmefällen für die Abwärtskompatibilität auf Wert `1` (=TLS 1.0) eingestellt sein

In großen Betriebsumgebungen kann die Konfigurationsdatei `prefs.js` für Firefox auch mittels Automatisierungswerkzeugen zentral verteilt und für den Benutzerzugriff gesperrt werden.

Während das hier beschriebene reine (aber nicht ausschließliche) Anbieten von TLS 1.2 für den Sektor Bürger-Behörden-Kommunikation genügt, müssen für die drei verbleibenden Sektoren die Anforderungen der TR-02102-2 fristgerecht eingehalten werden. In Firefox sind die Cipher-Suiten über die about:config-Seite und dort die Einstellungen zu „security.ssl3“ konfigurierbar.

6.1.3.3 Chrome und Opera

Der Chrome-Browser unterstützt seit Version 30 standardmäßig das Protokoll TLS 1.2 mit PFS.

Menü „Einstellungen“

- „Erweiterte Einstellungen anzeigen“
- „Proxy-Einstellungen ändern“
- Tab „Erweitert“
- „Sicherheit“
- Option „TLS 1.2 verwenden“

Achtung: Es existieren im Internet Anleitungen, wie diese Einstellungen verändert werden

4 Die aktuelle Version der TR 2102-2 „Verwendung von TLS“ erlaubt keine Verwendung von TLS 1.0 mehr; die Verwendung zur Wahrung von Abwärtskompatibilität unterliegt der Verantwortung der betreffenden Behörde.

können sollen:Bitte beachten Sie, dass diese Einstellung gegen alle Erwartungen keinen Einfluss auf das Protokollverhalten von Chrome hat und Google auch keine Konfigurationsmöglichkeiten für SSL/TLS vorsieht. Diese grafische Oberfläche konfiguriert tatsächlich nur den Internet Explorer (Chrome nutzt die an dieser Stelle zu findenden Proxy-Einstellungen des IE, „aufgrund einiger unglücklicher historischer Entscheidungen“).[5]

Der Browser kann über die Kommandozeile mit folgenden Parametern gestartet werden:

`chrome --ssl-version-max` *X* `--ssl-version-min` *Y*

Dabei entsprechen X und Y jeweils einem der folgenden Werte: `ssl3`, `tls1`, `tls1.1` oder `tls1.2`.

Auch hier genügt das Anbieten von TLS 1.2 lediglich für die Bürger-Behörden-Kommunikation, konkrete Cipher-Suites gemäß TR-02102-2 lassen sich via Blacklist über die Kommandozeilenoption

`--cipher-suite-blacklist=`

gefolgt von entsprechenden Hex-Codes ausschließen; die Codes der einzelnen Cipher-Suites finden sich in der Chrome-Dokumentation unter https://code.google.com/p/chromium/codesearch#chromium/usr/include/nss/sslproto.h

Der Opera-Browser ist ab der Version 10 für TLS 1.2 konfigurierbar:

Menü „Einstellungen“

- „Erweiterte Einstellungen“

- „Sicherheit“

- „Sicherheitsprotokolle“

- Option „TLS 1.2 verwenden“

Das Vorgehen funktioniert analog für den Browser Safari ab Version 7. Eine weitere Konfiguration der Cipher-Suiten ist nicht vorgesehen.

6.1.4 Migration der Zertifikate

Bei der erneuten Beschaffung der Zertifikate ist vorher auf die Vertrauenswürdigkeit der ausstellenden Stelle zu achten. Nach Erhalt der Zertifikate sollten die in Kapitel 4.2.2 bzw. TR-03116-4, Kapitel 4.1, genannten Attribute geprüft werden.

Die Prüfung eines Zertifikats kann zum Beispiel anhand von OpenSSL vorgenommen werden:

5 https://code.google.com/p/chromium/issues/detail?id=391955

```
# Herausgeber prüfen
openssl verify -CApath <Pfad zum Zertifikat> -verbose
<zertifikatsname.crt>
# Gültigkeitsdauer des Zertifikats abfragen
openssl x509 -noout -dates -in <zertifikatsname.crt>
```

Abschließend sei auf den Sonderfall der einseitigen Authentisierung hingewiesen.

Dabei können Anwender über ein Zertifikat die Identität des Servers feststellen, obschon bei der Kommunikation keine schutzbedürftigen Daten übertragen werden.

In diesem Fall hat die Behörde die Authentisierung nach dem Mindeststandard TLS 1.2 auszulegen, d.h. der Schlüsselaustausch erfolgt auf Basis der in der TR-02102-2 vorgegebenen Verfahren. Nach erfolgter Authentisierung kann die Behörde die Transportverschlüsselung für die Sitzung aufrecht erhalten oder auf eine nicht verschlüsselte Seite umleiten.

6.1.5 Migration von Web-Anwendungen und Fachverfahren

Frameworks zur Entwicklung und Abwicklung von Web-Anwendungen bringen häufig eigene TLS-Bibliotheken [Kap. 6.3.3] mit. Die Unterstützung für TLS 1.2 mit PFS bringen Microsoft .NET ab Version 4.5 (schannel.dll) und Java JSSE ab Version 7 mit.

Andere Web-Anwendungen verschlüsseln nur den Datentransport zum Client mit SSL, so dass die Migration dann analog zur Migration der Betriebssysteme, Server, Kryptographiebibliotheken und Browser aus den vorherigen Kapiteln [Kap. 6.1.1-6.1.3] durchgeführt werden kann.

Aufgrund der großen Freiheitsgrade bei der Entwicklung und dem Betrieb von Web-Anwendungen, können an dieser Stelle keine standardisierten und einheitlichen Verfahren vorgeschlagen werden.

Allerdings wird an dieser Stelle dringend empfohlen, den Schwerpunkt der Migration von Web-Anwendungen auf die Ist-Analyse, Soll-Konzeption und Restrisikoanalyse in Zusammenarbeit mit den Systemarchitekten und Entwicklern zu legen. Unter Umständen müssen neue Prozessmodelle und Werkzeuge für die Entwicklung genutzt werden.

Bei der Restrisikoanalyse sollten vor allem die weiteren Sicherheitsmaßnahmen der betreibenden Behörde betrachtet werden, um die Notwendigkeit der TLS-Transportverschlüsselung für die Kommunikation z. B. zwischen Applikations- und Datenbankservern entscheiden zu können.

6.2 Referenzverzeichnis

Kürzel	Quelle
[TR – 02102-1]	TR BSI 02102: "Kryptographische Verfahren:Empfehlungen und Schlüssellängen“ https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
[TR – 02102 - 2]	Technische Richtlinie BSI 02102-2: "Kryptographische Verfahren:Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)" https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.html
[TR-02102-3]	Technische Richtlinie BSI 02102-3: „Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)“ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3_pdf.pdf
[TR – 03116 - 4]	Technische Richtlinie BSI 03116 Teil 4: „Vorgaben für Kommunikationsverfahren im eGovernment“, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html
[Mindeststandard SSL/TLS]	Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung, https://www.bsi.bund.de/DE/Publikationen/Mindeststandards/SSL-TLS-Protokoll/SSL-TLS-Protokoll_node.html
[TLS/SSL Best Practices]	SSL/TLS Deployment Best Practices https://www.ssllabs.com/projects/best-practices/
[SSL TEST SSLLABS]	SSLLABS SSL Test https://www.ssllabs.com/ssltest/
[OpenVAS]	Tool OpenVAS (Open Vulnerability Assessment System) http://www.openvas.org/
[RFC 5246]	Request for Common 5246 - The Transport Layer Security v 1.2, http://tools.ietf.org/html/rfc5246
[RFC 4346]	Request for Common 4346 - The Transport Layer Security v 1.1, http://tools.ietf.org/html/rfc4346
[RFC 2246]	Request for Common 22476 - The Transport Layer Security v 1.0, http://www.ietf.org/rfc/rfc2246
[IANA CSR]	IANA Transport Layer Security (TLS) Parameters - TLS Cipher-Suite Registry http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml
	TLS/SSL unterstützende Cipher-Suites http://www.hep.by/gnu/gnutls/Supported-ciphersuites.html#ciphersuites
[BARD]	A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL, Gregory V. Bard http://eprint.iacr.org/2006/136
[GSK BSI]	IT-Grundschutzkataloge BSI, 2013, 13. Ergänzungslieferung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html
[Kaplan]	„Applied Crypto Hardening“ (Draft), Aaron Kaplan et al., 2014 https://bettercrypto.org/static/applied-crypto-hardening.pdf

6.3 Kompatibilitätsmatrizen

6.3.1 Windows-Kompatibilität zu SSL und TLS 1.x

Adaptiert von: http://blogs.msdn.com/b/kaushal/archive/2011/10/02/support-for-ssl-tls-protocols-on-windows.aspx

WindowsVersion	TLS 1.2	TLS 1.1	TLS 1.0
XP & Server 2003	Nein	Nein	Ja
Vista & Server 2008	Nein	Nein	Ja
7 & Server 2008 R2	Ja	Ja	Ja
8 & Server 2012	Ja	Ja	Ja

Tabelle 15: Windows-Kompatibilität zu SSL und TLS 1.x

6.3.2 Browser-Kompatibilität zu TLS 1.2

Browser	Version mit TLS 1.2
Google Chrome	>29
Firefox	>24
Internet-Explorer	>11 (8 und 10 nur für Win 7)

Tabelle 16: Browser-Kompatibilität zu TLS 1.2

6.3.3 TLS-Unterstützung durch Bibliotheken

Adaptiert von: http://en.wikipedia.org/w/index.php?title=Comparison_of_TLS_implementations

Bibliothek	TLS 1.2	TLS 1.1	TLS 1.0
cryptlib	Ja	Ja	Ja
CyaSSL	Ja	Ja	Ja
GnuTLS	Ja	Ja	Ja
MatrixSSL	Ja	Ja	Ja
NSS	Ja	Ja	Ja
OpenSSL 1.0.1c	Ja	Ja	Ja
LibreSSL	Ja	Ja	Ja
PolarSSL	Ja	Ja	Ja
XP/2003 (SChannel.dll)	Nein	Nein	MSIE 7
Vista/2008 (SChannel.dll)	Nein	Nein	Ja
Win7/2008R2 (SChannel.dll)	Ja	Ja	Ja
Win8/2012 (SChannel.dll)	Ja	Ja	Ja
Secure Transport	Ja	Ja	Ja
JSSE/JDK 1.6	Nein	Nein	Ja
JSSE/JDK 1.7	Ja	Ja	Ja
Bouncy Castle 1.5	Ja	Ja	Ja

Tabelle 17: TLS-Unterstützung durch Bibliotheken

6.3.4 Unterstützung der Cipher-Suites der TR-02102-2 durch Bibliotheken

Adaptiert von: http://en.wikipedia.org/w/index.php?title=Comparison_of_TLS_implementations

Bibliothek	ECDHE-ECDSA	ECDHE-RSA	DHE-RSA	DHE-DSS
cryptlib	Ja	Nein	Ja	Ja
CyaSSL	Ja	Ja	Ja	Nein
GnuTLS	Ja	Ja	Ja	Ja
MatrixSSL	Ja	Ja	Ja	Nein
NSS	Ja	Ja	teilweise	teilweise
OpenSSL	Ja	Ja	Ja	Ja
LibreSSL	Ja	Ja	Ja	Ja
PolarSSL	Ja	Ja	Ja	Nein
SChannel XP, 2003	Nein	Nein	Nein	max. 1024
SChannel Vista, 7, 8, 2008, 2008R2, 2012	Ja	Ja	Nein	max. 1024
Secure Transport	Ja	Ja	Ja	Ja
JSSE	Ja	Ja	max. 2048	max. 2048

Tabelle 18: Unterstützung der Cipher-Suites der TR-02102-2 durch Bibliotheken