Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

SICHERHEITSEMPFEHLUNGEN FÜR BEHÖRDEN, TEIL 2: SSL/TLS

VERSION 1.1 – 15.02.2016

Thomas Zefferer – thomas.zefferer@a-sit.at
Johannes Feichtner – johannes.feichtner@a-sit.at
Bernd Prünster – bernd.pruenster@a-sit.at

Zusammenfassung: SSL/TLS spielt im Behördenumfeld als zentrale Technologie zur sicheren Datenübertragung im Internet eine wichtige Rolle. Über Verbindungen, die mit SSL/TLS gesichert sind, können Daten authentifiziert, integritätsgesichert und vertraulich ausgetauscht werden. Aufgrund der Verwendung kryptographischer Methoden birgt die Implementierung, Konfiguration und Verwendung von SSL/TLS jedoch auch eine gewisse Komplexität. Gleichzeitig können durch eine falsche Verwendung Schwachstellen entstehen, die zu einer Kompromittierung der Sicherheit übertragener Daten führen können. Um hier Abhilfe zu schaffen, gibt dieses Dokument Empfehlungen zur korrekten Konfiguration und Verwendung von SSL/TLS. Hauptaugenmerk wird dabei auf die Wahl geeigneter Protokollversionen und Cipher-Suites, die die verwendeten kryptographischen Algorithmen und Schlüssellängen definieren, gelegt. Das A-SIT Tool auf http://demoapps.a-sit.at/ssl-tool/ ermöglicht die Online-Prüfung bezüglich dieser Empfehlungen.

Konkret werden in diesem Dokument folgende Empfehlungen zur Verwendung von SSL/TLS gegeben:

- Es wird empfohlen, für SSL/TLS nur kryptographische Algorithmen und Schlüssellängen zu verwenden, die über ein adäquates Sicherheitsniveau verfügen. Für symmetrische Verfahren wird eine Mindestschlüssellänge von 100 Bit (128 Bit bei AES, 112 Bit bei 3DES), für asymmetrische Verfahren von 1500 Bit für bestehende bzw. 2000 Bit für neue Systeme (1536 Bit bzw. 2048 Bit bei RSA und 192 Bit bzw. 224 Bit bei EC-Protokollen) empfohlen.

- Es wird empfohlen, stets die höchst mögliche Protokollversion von SSL/TLS zu verwenden. Es wird empfohlen, SSL 2.0 und SSL 3.0 vollständig zu vermeiden und TLS 1.0 nur einzusetzen, wenn dies zwingend notwendig ist.

- Es wird empfohlen, jene Cipher-Suites zu verwenden, die einerseits eine breite Unterstützung auf gängigen Browsern aufweisen und die andererseits ein ausreichendes Maß an Sicherheit durch Verwendung geeigneter kryptographischer Algorithmen gewährleisten. Eine Liste empfohlener Cipher-Suites ist in diesem Dokument enthalten.

- Es wird empfohlen, als Transferformate für private Schlüssel bzw. Server-Zertifikate die Formate PKCS#12 bzw. PKCS#7 zu verwenden.

- Es wird empfohlen, Web-Server, die SSL/TLS verwenden, stets aktuell zu halten und deren Konfigurationen aktuellen Entwicklungen laufend anzupassen.

Revision History

Version	Datum	Autor	Anmerkungen
0.1	02.10.2014	Thomas Zefferer	Initialversion
0.2	03.10.2014	Johannes Feichtner	Internes Feedback
0.3	05.10.2014	Thomas Zefferer	Finaler Draft
0.4	14.10.2014	Herbert Leitold	Kommentare und Ergänzungen
1.0	17.10.2014	Thomas Zefferer	Finalisierung Version 1.0
1.1*	15.02.2016	Bernd Prünster	Aktualisierung 02.2016

*Die Änderungen von Version 1.0 zu Version 1.1 beinhalten eine Aktualisierung der Vorgaben unter Berücksichtigung aktueller externer Sicherheitsempfehlungen wie beispielsweise RFC 7525 [28] und neu entdeckter Schwachstellen wie Logjam [30].

Inhaltsverzeichnis

Revision History 2
Inhaltsverzeichnis 2
1. Einleitung 3
2. Grundlagen 3
3. Analyse der Verfügbarkeit und Unterstützung 5
3.1. Identifikation potentieller Cipher-Suites 5
3.2. Analyse der Verbreitung identifizierter Cipher-Suites 6
4. Analyse der Sicherheit 7
4.1. Kriterien 7
4.1.1. MUSS-Kriterien 8
4.1.2. SOLL-Kriterien 8
4.2. Anwendung der Kriterien auf potentielle Cipher-Suites 8
5. Empfehlungen 9
5.1. Empfohlene Mindestschlüssellängen 9
5.2. Empfohlene Versionen von SSL und TLS 9
5.3. Empfohlene Cipher-Suites 9
5.3.1. Cipher-Suites mit hoher Sicherheit und adäquater Unterstützung 10
5.3.2. Cipher-Suites mit hoher Sicherheit und adäquater Unterstützung 10
5.3.3. Cipher-Suites mit ausreichender Sicherheit und breiter Unterstützung 10
5.4. Empfohlene Transferformate 11
5.5. Empfehlungen zur Konfiguration und zum Betrieb von Web-Servern 12
6. SSL/TLS-Prüftool 12
7. Fazit 12
Referenzen 14
Anhang A: Cipher-Suites 16
Anhang B: Unterstützung von Cipher-Suites durch Web-Browser und Web-Server 26
Anhang C: Empfohlene Cipher-Suites 33

1. Einleitung

Das Protokoll Transport Layer Security (TLS), welches umgangssprachlich nach wie vor auch oft als Secure Sockets Layer (SSL) bezeichnet wird, stellt eine Grundlage der sicheren Client-Server-Kommunikation im Internet dar. Das Protokoll wurde 1999 unter dem Namen SSL veröffentlicht. Ab Version 3.1 des Protokolls wurde dieses unter dem Namen TLS weiterentwickelt. SSL Version 3.1 entspricht daher TLS 1.0.

TLS spielt vor allem in Zusammenhang mit dem Protokoll HTTP eine zentrale Rolle. Durch die Anwendung von HTTP über TLS können sichere HTTPS-Verbindungen zwischen Web-Servern und Web-Browsern etabliert werden. Über diese sicheren Verbindungen können Daten verschlüsselt, authentifiziert und integritätsgesichert ausgetauscht werden. Dementsprechend kommt TLS in Verbindung mit HTTPS vor allem bei sicherheitskritischen webbasierten Anwendungen häufig zum Einsatz. Beispiele dafür sind die Bereiche E-Government oder E-Banking. Damit ist TLS auch für Behörden von zentraler Bedeutung.

In einer Kurzstudie [1] wurden von A-SIT österreichische gv.at-Domänen in Bezug auf deren Verwendung der Protokolle TLS und HTTPS analysiert. Dabei konnten einige Domänen identifiziert werden, die Cipher-Suites und Schlüssellängen verwenden, die nicht diesen Empfehlungen entsprechen.

Die durchgeführte Kurzstudie untermauert damit die Annahme, dass eine generelle Notwendigkeit für Empfehlungen zur Verwendung und Konfiguration der TLS-Technologie im Behördenumfeld besteht. Dieser Notwendigkeit wird durch das vorliegende Dokument nachgekommen, indem dieses Empfehlungen zur serverseitigen Verwendung und Konfiguration des TLS-Protokolls zusammenfasst. Besonderes Augenmerk wird dabei auf die Auswahl geeigneter Cipher-Suites gelegt, welche kryptographische Algorithmen und Schlüssellängen definieren, die zur Absicherung von TLS-Verbindungen zur Anwendung kommen. Damit baut dieses Dokument auf der von A-SIT erstellten Studie auf, in der allgemeine Empfehlungen zur Verwendung kryptographischer Algorithmen und Schlüssellängen gegeben wurden [2].

Die Struktur des vorliegenden Dokuments entspricht im Wesentlichen der Methodik, die zur Erarbeitung den eben erwähnten Empfehlungen verfolgt wurde. In Abschnitt 2 werden zunächst grundlegende Begriffe und Konzepte, die im Rahmen von TLS relevant sind, eingeführt und erläutert. Im Speziellen wird auf die Rolle und Verwendung von Cipher-Suites eingegangen. Im Anschluss wird in Abschnitt 3 die Verfügbarkeit verschiedener Cipher-Suites auf aktuellen Web-Browsern und durch verbreitete Web-Server-Software untersucht. Auf diese Weise werden jene Cipher-Suites identifiziert, die über eine entsprechend breite Unterstützung verfügen. In Abschnitt 4 werden potentielle Cipher-Suites anhand definierter Kriterien in Bezug auf deren Sicherheitsniveau untersucht. Aus den Ergebnissen dieser Untersuchungen werden in Abschnitt 5 Empfehlungen zur Verwendung von SSL/TLS gegeben. In Abschnitt 6 wird schließlich noch das von A-SIT entwickelte Tool zur Überprüfung von SSL/TLS-Konfigurationen vorgestellt.

2. Grundlagen

Über TLS können sichere Verbindungen zwischen einem Server und einem Client hergestellt werden. Bei Verwendung im Zusammenhang mit HTTP kann so etwa ein sicherer Datenaustausch zwischen Web-Servern und Web-Browsern gewährleistet werden. Die Absicherung des Kommunikationspfades zwischen Server und Client basiert auf kryptographischen Methoden. Diese bieten im Rahmen von TLS folgende Features:

- Authentifizierung des Servers
- Authentifizierung des Clients (optional und im Web-Kontext eher unüblich)
- Verschlüsselung der Nutzdaten
- Integritätssicherung der Nutzdaten

Da für die Umsetzung dieser Features unterschiedliche kryptographische Methoden benötigt werden, müssen sich Server und Client vor der eigentlichen Datenübertragung auf eine Menge zu verwendender Methoden einigen. Diese Menge wird als Cipher-Suite bezeichnet und im Rahmen des Verbindungsaufbaus ausgehandelt. Dies ist in Abbildung 1, welche einen vereinfachten TLS-Verbindungsaufbau zeigt, dargestellt.

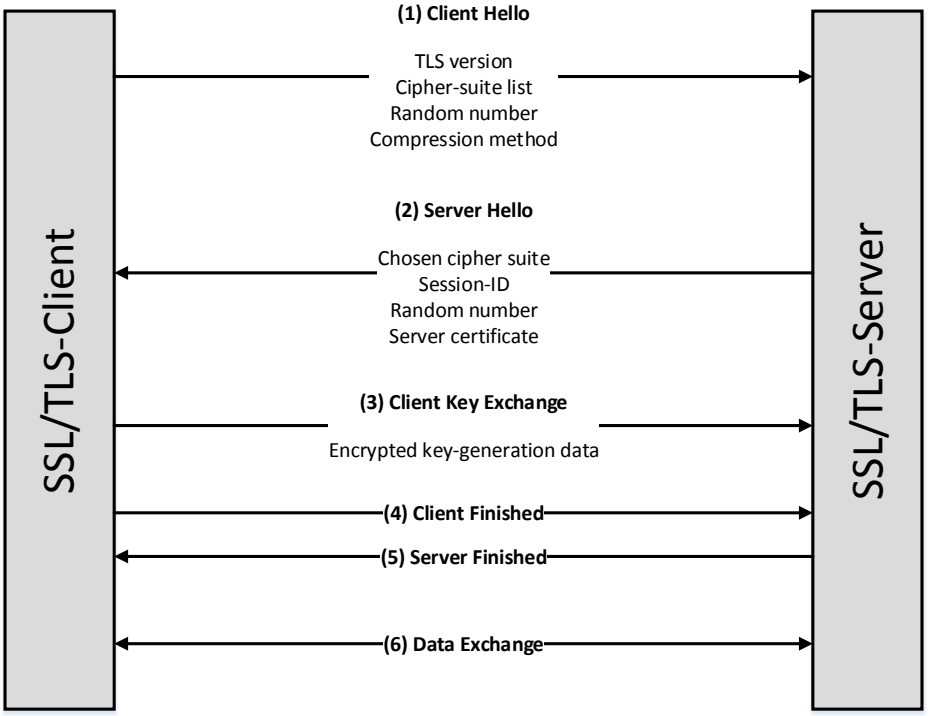

Abbildung 1. TLS-Verbindungsaufbau (adaptiert von [3]).

Im ersten Schritt (Client Hello) übermittelt der Client an den Server eine nach Priorität geordnete Liste unterstützter Cipher-Suites. Aus dieser Liste wählt der Server anhand definierter Prioritäten eine geeignete Cipher-Suite aus. Diese wird dem Client im zweiten Kommunikationsschritt (Server Hello) mitgeteilt.

Cipher-Suites können über eine ID bestehend aus zwei Bytes identifiziert werden. Üblich ist auch die Repräsentation in Form einer Zeichenkette, aus der die in der Cipher-Suite enthaltenen Algorithmen und Schlüssellängen ersichtlich sind. Dabei haben sich mit der IANA-Notation und der OpenSSL-Notation zwei unterschiedliche Formate etabliert. Beispielsweise wird die Cipher-Suite mit der ID 0xC013 durch folgende Bezeichnungen beschrieben:

- IANA-Notation: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- OpenSSL-Notation: ECDHE-RSA-AES128-SHA

Aus Gründen der Einheitlichkeit und im Sinne der Unabhängigkeit von einer bestimmten TLS-Implementierung werden in diesem Dokument Cipher-Suites im Folgenden immer in IANA-Notation angeführt.

Über den Namen einer Cipher-Suite werden, wie aus obigem Beispiel ersichtlich, vier Algorithmen identifiziert. Der erste Algorithmus (im obigen Beispiel ECDHE) bezeichnet das für den Schlüsselaustausch zu verwendende Verfahren. Der zweite Algorithmus (im obigen Beispiel RSA) gibt an, welches Verfahren für die Authentifizierung des Servers verwendet werden muss. Der dritte angegebene Algorithmus beschreibt das Verfahren zur Verschlüsselung von Nutzdaten. Im obigen Beispiel ist dies AES mit 128 Bit Schlüssellänge im CBC-Verfahren. Der vierte Algorithmus (im obigen Beispiel SHA) bezeichnet schließlich das zu verwendende Verfahren zur Gewährleistung der Integrität der übertragenen Nutzdaten.

Da über die zwischen Client und Server ausgehandelte Cipher-Suite die zur Kommunikationsabsicherung über TLS verwendeten kryptographischen Algorithmen festgelegt werden, ist die Wahl einer geeigneten Cipher-Suite von entscheidender Bedeutung. Die Wahl der Cipher-Suite kann bei der Verwendung von TLS im Rahmen von HTTPS prinzipiell auf zweierlei Art und Weise beeinflusst werden:

- Der Web-Browser (bzw. die Benutzerin oder der Benutzer) kann die Verwendung sicherer Cipher-Suites erzwingen, indem dieser im Rahmen des Kommunikationsaufbaus (Client Hello) nur jene Cipher-Suites vorschlägt, die den Sicherheitsanforderungen entsprechen.

- Der Web-Server kann über eine interne Prioritätenliste im Zuge des Verbindungsaufbaus (Server Hello) jene Cipher-Suites auswählen, die den gegebenen Sicherheitsanforderungen entsprechen.

In der Praxis ist der erste Ansatz nur schwer umsetzbar, da Benutzerinnen und Benutzer in der Regel nicht über das nötige Know-How verfügen, um unterstützte Cipher-Suites im Web-Browser entsprechend zu konfigurieren. In den meisten Fällen werden Web-Browser daher mit jenen Cipher-Suites betrieben, die vom Browser-Hersteller konfiguriert wurden.

Ziel dieses Dokuments ist es daher, Betreibern von Servern in Form von Empfehlungen eine Grundlage zu liefern, welche Cipher-Suites serverseitig für eine priorisierte Verwendung konfiguriert werden sollen. Für die Erarbeitung dieser Empfehlungen werden dabei folgende Aspekte berücksichtigt:

- **Sicherheit:** Es werden nur jene Cipher-Suites empfohlen, die ein geeignetes Sicherheitsniveau gewährleisten können.

- **Verbreitung und Unterstützung:** Es werden primär jene Cipher-Suites empfohlen, die in aktuellen Web-Browsern eine breite Unterstützung finden und auch von gängigen TLS-Implementierungen unterstützt werden.

Neben der Empfehlung konkreter Cipher-Suites werden in diesem Dokument außerdem weitere relevante Empfehlungen zur Konfiguration und zur Verwendung von SSL/TLS gegeben.

3. Analyse der Verfügbarkeit und Unterstützung

In diesem Abschnitt wird die Verfügbarkeit und Unterstützung verschiedener Cipher-Suites durch aktuelle Web-Browser und Web-Server analysiert. Dazu werden zunächst potentielle Cipher-Suites gesammelt und aus diesen jene identifiziert, die sowohl durch Browser als auch durch Web-Server breit unterstützt werden.

3.1. Identifikation potentieller Cipher-Suites

Um eine Grundlage für eine systematische Analyse und Identifikation geeigneter und zu empfehlender Cipher-Suites zu schaffen, wird in einem ersten Schritt eine weitgehend erschöpfende Liste verfügbarer Cipher-Suites erstellt. Dazu werden unterschiedliche Quellen herangezogen:

- Relevante Standards wie zum Beispiel:
    - RFC 5289 [4]
    - RFC 4492 [5]
    - RFC 6460 [6]
    - RFC 5246 [7]
- Dokumentationen zu existierenden TLS-Implementierungen wie:

    - OpenSSL [8]
    - Microsofts SChannel [9]
- Einschlägige Web-Ressourcen wie beispielsweise:
    - Qualys SSL Labs [10]
    - The Sprawl [11]
- Einschlägige Analyse-Tools wie zum Beispiel:
    - A-SIT SSL/TLS-Prüftool [12]
    - Qualys SSL Server Test [13]
    - Qualys SSL Browser Test [14]

Aus diesen Quellen kann eine weitgehend vollständige Liste von derzeit definierten Cipher-Suites erstellt werden. Für jede dieser Cipher-Suites werden in weiterer Folge folgende Daten erhoben:

- ID
- Name
- SSL/TLS-Protokoll
- Verfahren für den Schlüsselaustauch
- Verfahren für die Authentifizierung
- Verschlüsselungsalgorithmus
- Schlüssellänge des Verschlüsselungsalgorithmus
- MAC-Verfahren

Die resultierende Liste an Cipher-Suites inklusive deren Eigenschaften kann Anhang A dieses Dokuments entnommen werden.

3.2. Analyse der Verbreitung identifizierter Cipher-Suites

Die Identifizierung potentieller Cipher-Suites ergibt eine Liste von über 250 Cipher-Suites. In der Praxis ist jedoch nur eine Untermenge dieser Cipher-Suites von tatsächlicher Bedeutung. Viele der in Anhang A angeführten Cipher-Suites werden von aktuellen Web-Browsern nicht unterstützt.

Um jene Cipher-Suites, die auch in der Praxis von Bedeutung sind, zu identifizieren, wird für jede in Anhang A angeführte Cipher-Suite deren Unterstützung durch aktuelle Web-Browser und Web-Server untersucht. Dabei wird der Fokus auf die laut W3Counter [15] am weitesten verbreiteten Web-Browser Google Chrome, Mozilla Firefox, Microsoft Internet Explorer und Apple Safari gelegt. Von jeder Browser-Software wird jeweils die aktuellste Version für eine spezielle Plattform untersucht. Hier ist zu beachten, dass sich auf unterschiedlichen Plattformen und Betriebssystemen mitunter Unterschiede in den unterstützten Cipher-Suites ergeben können.

Ähnlich wird auch in Bezug auf Web-Server vorgegangen. Laut Netcraft [16] sind aktuell die Web-Server Apache, Microsoft IIS, nginx und Google Web Server (GWS) am weitesten verbreitet. Dementsprechend wird der Fokus zunächst auf diese Web-Server gelegt. Daneben wird auch Server-Software der Firmen IBM und Oracle analysiert. Von IBM wurde anhand verfügbarer

Dokumentation [23] untersucht, welche Cipher-Suites von der Web-Server Software Websphere, bzw. von der von dieser Software genutzten Komponente IBM Global Security Kit (GSKit), unterstützt werden. Oracle bietet ein breites Portfolio an Server-Komponenten, für die Cipher-Suites konfiguriert werden können [25]. Für einige Oracle-Produkte enthält die zugehörige Dokumentation eine explizite Auflistung unterstützter Cipher-Suites [27], für andere Server-Lösungen wird in Bezug auf unterstützte Cipher-Suites auf die aktuelle Java Secure Socket Extension (JSSE) verwiesen [26]. In diesem Dokument wird die aktuelle JSSE-Version als relevante SSL/TLS-Implementierung angenommen. Unterstützte Cipher-Suites können der zugehörigen Dokumentation entnommen werden [24]. Obwohl sowohl Apache als auch nginx theoretisch unterschiedliche TLS-Implementierungen unterstützen, wird für die vorgenommene Analyse eine Verwendung von OpenSSL angenommen, da dies die derzeit meistverwendete TLS-Implementierung ist. Auch hier wird stets die aktuellste Version der Web-Server-Software bzw. der verwendeten TLS-Implementierung analysiert.

Die Unterstützung von Cipher-Suites auf unterschiedlichen Web-Browsern und Web-Servern wird auf zweierlei Art und Weise evaluiert. Zunächst werden – wo verfügbar – vorhandene Produktdokumentationen analysiert. Die auf diese Weise erhaltenen Angaben werden zusätzlich über einschlägige Tools [12][13][14] überprüft. Das Resultat dieser Analyse ist in Anhang B dargestellt, wo für jede identifizierte Cipher-Suite unterstützende Web-Browser und Web-Server angeführt sind. Anhang B enthält nur jene Cipher-Suites, die zumindest von einem der analysierten Browser oder Web-Server unterstützt werden. Da unterstützte Cipher-Suites sowohl auf Web-Servern als auch auf Web-Browsern konfiguriert und verändert werden können, können die in Anhang B gezeigten Daten punktuell von tatsächlich im Einsatz befindlichen Systemen abweichen. Speziell sind aus Gründen der Vollständigkeit in Anhang B auch jene Cipher-Suites gelistet, die vom Hersteller standardmäßig deaktiviert sind, jedoch prinzipiell unterstützt und damit auch aktiviert werden können.

Anhang B zeigt die Unterstützung von Cipher-Suites exemplarisch für die vier oben genannten Web-Browser auf bestimmten Plattformen. Detailliertere Informationen zur Unterstützung von Cipher-Suites auf verschiedenen (auch mobilen) Web-Browsern können [14] entnommen werden. Insgesamt zeigt sich, dass wie erwartet die aktuell verfügbaren Web-Browser der limitierende Faktor sind. Cipher-Suites, die von Web-Browsern unterstützt werden, sind auch auf den meisten Web-Servern verfügbar. Umgekehrt wird jedoch nur ein Bruchteil aller von Web-Servern, bzw. deren TLS-Implementierungen, unterstützten Cipher-Suites auch auf Web-Browsern unterstützt.

4. Analyse der Sicherheit

Um potentielle Cipher-Suites in Bezug auf deren Sicherheit zu evaluieren, werden im Folgenden Sicherheitskriterien definiert und motiviert. Diese werden im Anschluss auf potentielle Cipher-Suites angewendet. Dadurch können schlussendlich jene Cipher-Suites extrahiert werden, die ein geeignetes Maß an Sicherheit aufweisen.

4.1. Kriterien

In der Praxis muss bei der Konfiguration unterstützter Cipher-Suites ein Balanceakt zwischen Sicherheit und breiter Unterstützung gefunden werden. Als sehr sicher eingestufte Cipher-Suites werden von vielen Web-Browsern oft (noch) nicht unterstützt. Gleichzeitig bieten breit unterstützte Cipher-Suites oft nicht (mehr) das geforderte Sicherheitsniveau. Durch automatische Updates wird von Seiten der Browser-Hersteller versucht, dieses Problem zu minimieren. Jedoch kann in der Praxis nicht immer davon ausgegangen werden, dass der Nutzer immer die aktuellste Version eines Browsers benutzt. Erschwerend kommt hinzu, dass eine Vielzahl mobiler Endgeräte weit über den vom Hersteller gewollten Produktlebenszyklus hinaus verwendet werden. Dadurch ergibt sich eine nicht zu vernachlässigende Anzahl an Endgeräten, welche nicht dem aktuellen Stand der Entwicklung entsprechen. Exemplarisch wird hier auf die aktuelle Verteilung unterschiedlicher Android-Versionen [29] verwiesen. Folglich kann auch keine breite Unterstützung für Cipher-Suites mit höchstmöglichem Sicherheitsniveau angenommen werden.

Die Anforderungen an die Sicherheit von Cipher-Suites können sich je nach Anwendungsszenario unterscheiden. Sicherheitskritische Anwendungen werden in der Wahl zulässiger Cipher-Suites in

der Regel restriktiver sein als weniger kritische Anwendungen. Um verschiedene Anwendungsfälle mit unterschiedlichen Sicherheitsanforderungen abdecken zu können, werden in diesem Abschnitt zwei Kategorien von Kriterien definiert.

- **MUSS-Kriterien:** Diese müssen in jedem Fall und unabhängig vom konkreten Anwendungsszenario eingehalten werden.

- **SOLL-Kriterien:** Diese müssen für weniger kritische Anwendungsfälle nicht eingehalten werden, sehr wohl jedoch in Szenarien mit erhöhten Sicherheitsanforderungen.

MUSS- und SOLL-Kriterien für Cipher-Suites werden in den folgenden Unterabschnitten näher definiert. Diese greifen auch die in RFC 7525 [28] definierten Empfehlungen auf.

4.1.1. MUSS-Kriterien

- Die Cipher-Suite MUSS Verschlüsselung unterstützen. Der NULL-Cipher ist nicht erlaubt. Nur so ist sichergestellt, dass die Vertraulichkeit der über die TLS-Verbindung übertragenen Daten gewährleistet bleibt.

- Die Cipher-Suite MUSS einen sicheren Verschlüsselungsalgorithmus verwenden. Schwache Algorithmen wie RC2, RC4, DES, IDEA, GHOST28147 oder SEED sind nicht zulässig. Nur so ist sichergestellt, dass die Vertraulichkeit der über die TLS-Verbindung übertragenen Daten gewährleistet bleibt.

- Die Cipher-Suite MUSS Authentifizierung unterstützen. Anonyme Cipher-Suites sind nicht zulässig. Nur so kann der Client den Server eindeutig authentifizieren.

- Die unterstützte Authentifizierung MUSS zertifikatsbasiert sein. PSK-Varianten sind nicht zulässig. Nur so kann der Client den Server sicher authentifizieren.

- Die Cipher-Suite MUSS Perfect Forward Secrecy (PFS) unterstützen. Nur so ist sichergestellt, dass über TLS übertragene Daten auch im Falle einer späteren Kompromittierung des Schlüssels weiter geschützt bleiben[1].

4.1.2. SOLL-Kriterien

- Die Cipher-Suite SOLL TLS 1.2 zugeordnet sein.

- Die Cipher-Suite SOLL AES als Verschlüsselungsalgorithmus verwenden. Damit wird für die Verschlüsselung von Daten ein bewährter und standardisierter Algorithmus verwendet.

- Die Cipher-Suite SOLL einen SHA2-basierten Ansatz oder GCM zur Integritätssicherung verwenden. SHA1 SOLL vermieden werden. Damit wird der Einsatz eines potentiell schwachen Hash-Algorithmus verhindert.

4.2. Anwendung der Kriterien auf potentielle Cipher-Suites

Durch die Anwendung der definierten Sicherheitskriterien kann schließlich eine finale Menge relevanter Cipher-Suites erarbeitet werden. Die erhaltenen Cipher-Suites können in zwei Kategorien unterteilt werden.

- Cipher-Suites für sicherheitskritische Anwendungsszenarien erfüllen alle MUSS- und alle SOLL-Kriterien.

[1] Prinzipiell sind Anwendungsfälle denkbar, in denen PFS keine notwendige Anforderung ist. Für Anwendungen im Behördenumfeld, an das sich dieses Dokument richtet, ist die durchgehende Verwendung von PFS jedoch sinnvoll, zumal eine breite Unterstützung entsprechender Cipher-Suites auf aktuellen Web-Browsern bereits gegeben ist. Die Unterstützung von PFS wird in diesem Dokument daher als MUSS-Kriterium definiert.

- Cipher-Suites für weniger kritische Anwendungsszenarien erfüllen alle MUSS-Kriterien.

Die auf diese Weise identifizierten Cipher-Suites sind in Anhang C tabellarisch angeführt.

5. Empfehlungen

Basierend auf den Resultaten der durchgeführten Analysen kann für die Verwendung und serverseitige Konfiguration von SSL/TLS eine Reihe von Empfehlungen formuliert werden. Diese Empfehlungen werden in den folgenden Unterabschnitten gegeben.

5.1. Empfohlene Mindestschlüssellängen

Detaillierte Empfehlungen zu kryptographischen Algorithmen und Schlüssellängen wurden in einem getrennten Dokument formuliert [2]. Aus diesem können folgende Richtwerte übernommen werden:

- Für symmetrische Verfahren kann derzeit bei Verwendung eines entsprechenden Algorithmus eine Mindestschlüssellänge von 100 Bit empfohlen werden. Damit ergeben sich bei Verwendung von üblichen Algorithmen wie 3DES oder AES tatsächliche empfohlene Schlüssellängen von 112 (3DES) bzw. 128 (AES) Bit.

- Für asymmetrische Verfahren kann eine Mindestschlüssellänge von 1500 Bit für bestehende bzw. von 2000 Bit für neue Systeme empfohlen werden. Für RSA kann damit eine Schlüssellänge von 1536 Bit bzw. von 2048 Bit als geeignet angesehen werden. Entsprechend kann für kryptographische Verfahren basierend auf elliptischen Kurven wie ECDSA eine Schlüssellänge von 192 Bit bzw. 224 Bit empfohlen werden.

- Für Hash-Verfahren wird aktuell eine Länge von 155 bis 224 Bit empfohlen. Damit ist etwa SHA-1 mit einer Länge von 160 Bit bereits am unteren Ende des empfohlenen Spektrums. Stattdessen kann die Verwendung anderer Hash-Algorithmen wie Vertreter der SHA2-Familie empfohlen werden.

- Seit Bekanntwerden der Logjam-Attacke [30] wird bei der Verwendung von Diffie-Hellman Cipher-Suites (Präfix DHE) in jedem Fall eine Parameterlänge entsprechend der Mindestschlüssellänge asymmetrischer Verfahren empfohlen. Unabhängig davon wird die Verwendung von selbstgenerierten Diffie-Hellman Gruppen empfohlen. Weitere Details und eine schrittweise Anleitung zu entsprechender Konfiguration verbreiteter Webserver sind unter [31] verfügbar.

5.2. Empfohlene Versionen von SSL und TLS

Es wird empfohlen, SSL 2.0 unter keinen Umständen zu verwenden, da diese Version seit längerer Zeit Schwachstellen aufweist. Es wird außerdem empfohlen, SSL 3.0 nicht mehr zu verwenden[2]. Die niedrigste SSL/TLS-Version, die verwendet und serverseitig unterstützt werden sollte ist TLS 1.0. Niedrigere Versionen sollten serverseitig deaktiviert werden, um mögliche Risiken, die sich durch einen Fallback auf SSL 2.0 oder SSL 3.0 ergeben können, auszuschließen. Generell wird empfohlen, stets die höchst mögliche TLS-Version (derzeit TLS 1.2) zu verwenden. Niedrigere TLS-Versionen wie TLS 1.0 oder TLS 1.1 sollten wenn nötig nur aus Kompatibilitätsgründen verwendet werden. Speziell bei der Verwendung von TLS 1.0 muss auf eine korrekte Konfiguration des Servers geachtet werden, um potentielle Sicherheitsprobleme ausschließen zu können.

5.3. Empfohlene Cipher-Suites

Es werden drei Kategorien von Cipher-Suites empfohlen. Die erste Kategorie enthält Cipher-Suites, die ein hohes Maß an Sicherheit bringen und eine adäquate Unterstützung auf aktuellen Web-Browsern aufweisen. Die zweite Kategorie enthält ebenfalls Cipher-Suites mit hoher Sicherheit, die derzeit auf aktuellen Web-Browsern jedoch noch nicht breit unterstützt werden. Die

[2] Durch Vermeidung von SSL 3.0 kann etwa der kürzlich entdeckten POODLE-Schwachstelle [33] entgegengewirkt werden.

dritte Kategorie enthält schließlich Cipher-Suites mit nach wie vor ausreichender Sicherheit, die aber eine breitere Unterstützung auf aktuellen Web-Browsern bieten. Die geeignete Kategorie kann je nach Anwendungsfall gewählt werden. In jedem Fall sollte stets die höchstmögliche Anzahl an Cipher-Suites serverseitig unterstützt werden, um ein ausreichendes Maß an Kompatibilität mit verschiedenen Clients zu gewährleisten.

5.3.1. Cipher-Suites mit hoher Sicherheit und adäquater Unterstützung

Die folgende Tabelle enthält empfohlene Cipher-Suites mit hoher Sicherheit und adäquater Unterstützung durch aktuelle Clients. Diese Cipher-Suites können jederzeit bedenkenlos unterstützt werden.

Tabelle 1. Empfohlene Cipher-Suites mit hoher Sicherheit und guter Browser-Unterstützung.

Name	Protokoll
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2

5.3.2. Cipher-Suites mit hoher Sicherheit und beschränkter Unterstützung

Die folgende Tabelle enthält empfohlene Cipher-Suites mit hoher Sicherheit, jedoch beschränkter Unterstützung durch aktuelle Clients. Auch diese Cipher-Suites können jederzeit bedenkenlos unterstützt werden. Neben diesen sollten jedoch noch weitere Cipher-Suites unterstützt werden, um ein entsprechendes Maß an Client-Kompatibilität zu gewährleisten.

Tabelle 2. Empfohlene Cipher-Suites mit hoher Sicherheit und geringer Browser-Unterstützung.

Name	Protokoll
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS 1.2

5.3.3. Cipher-Suites mit ausreichender Sicherheit und breiter Unterstützung

Die folgende Tabelle enthält empfohlene Cipher-Suites mit ausreichender Sicherheit und breiter Unterstützung. Diese Cipher-Suites sollten zusätzlich zu den oben empfohlenen Cipher-Suites mit

hoher Sicherheit verwendet werden, wenn eine breite Unterstützung auf möglichst vielen (vor allem älteren) Web-Browsern Priorität hat.

Tabelle 3. Empfohlene Cipher-Suites mit ausreichender Sicherheit und breiter Unterstützung.

Name	Protokoll
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0

Bei der Konfiguration unterstützter Cipher-Suites ist auch auf deren Priorisierung zu achten. Es wird empfohlen, sichere Cipher-Suites (Tabelle 1 und Tabelle 2) priorisiert zu konfigurieren, sodass diese bevorzugt verwendet werden, falls diese vom Web-Browser unterstützt werden. Nur wenn keine gemeinsame Cipher-Suite aus Tabelle 1 oder Tabelle 2 zwischen Web-Server und Web-Browser ausgehandelt werden kann, soll auf Cipher-Suites aus Tabelle 3 zurückgegriffen werden. Andere als die in den obigen Tabellen gelisteten Cipher-Suites sollen nicht verwendet werden.

5.4. Empfohlene Transferformate

In Folge werden Formate für den Transfer von Zertifikaten oder privaten Schlüsseln empfohlen. Bei der Speicherung, Übermittlung und Verwahrung privater Schlüssel ist zu beachten, dass dies ein kritisches Element hinsichtlich der Sicherheit darstellt. Es sind besondere Sicherheitsmaßnahmen vorzusehen, um eine Kompromittierung effektiv zu verhindern. Die hier definierten Empfehlungen haben keine Relevanz in Bezug auf die Sicherheit dieser Elemente, sondern definieren lediglich Formate, die einen Austausch zwischen verschiedenen gängigen Plattformen und Produkten unterstützen.

Für die Speicherung privater Schlüssel wird das Format PKCS#12 [17] empfohlen. Zusätzlich wird für die Speicherung der Server-Zertifikate das Format PKCS#7 [18] empfohlen. In diesem Format sind Zertifikate in einer festgelegten ASN.1-Struktur und nach den Distinguished Encoding Rules (DER) kodiert abgespeichert. Eine zusätzliche BASE64-Kodierung ist optional möglich, jedoch nicht notwendig. Es wird empfohlen, den gesamten Zertifizierungspfad inklusive des Root-Zertifikats zu speichern.

5.5. Empfehlungen zur Konfiguration und zum Betrieb von Web-Servern

Als Ergänzung zu den bisher gemachten Empfehlungen sind noch einige weitere Aspekte für die sichere Verwendung von SSL/TLS zu beachten. Diese werden im Folgenden angeführt.

- Es wird empfohlen, beim Betrieb von TLS-Implementierungen wie OpenSSL stets deren aktuellste verfügbare Version zu verwenden. Die Heartbleed- [19] und die FREAK-Sicherheitslücke [20] zeigten, dass auch TLS-Implementierungen von Schwachstellen betroffen sein können. Eine im September 2015 veröffentlichte Seitenkanalattacke [22] dokumentiert, dass Implementierungsfehler, die nicht unmittelbar TLS-Implementierungen selbst betreffen, auch zu in der Praxis ausnutzbaren Sicherheitslücken führen können. Jedoch stellt auch in diesem Zusammenhang eine Aktualisierung der eingesetzten TLS-Implementierung eine ausreichende Gegenmaßnahme dar. Zusammenfassend lässt sich festhalten, dass nur durch die ständige Aktualisierung der verwendeten Bibliotheken und Implementierungen ein Schutz gegen bekannte Schwachstellen erreicht werden kann.

- Es wird empfohlen, bei der Konfiguration von Web-Servern, die TLS unterstützen, auf gängige Best Practices zurückzugreifen. Hier ist zu beachten, dass sich diese mitunter im Laufe der Zeit ändern können. So gilt beispielsweise erst seit Bekanntwerden der CRIME- oder BREACH-Attacke [21] die serverseitige Deaktivierung der Datenkompression bei Verwendung von TLS-Verbindungen als Best Practice.

Neben den hier definierten Empfehlungen gibt das Dokument Applied Crypto Hardening der Organisation bettercrypto.org [32] weitere Empfehlungen und Anleitungen zur richtigen und sicheren Konfiguration und zum Betrieb von Web-Servern.

6. SSL/TLS-Prüftool

Als Ergänzung zu den in diesem Dokument definierten Empfehlungen und als Unterstützung bei der Konfiguration von Web-Servern wurde ein Tool entwickelt, über das TLS-Konfigurationen von Web-Servern und Web-Browsern überprüft werden können. Das Tool erlaubt die Prüfung bezüglich dieser Empfehlungen auf http://demoapps.a-sit.at/ssl-tool/ bzw. steht unter [12] auch zum Download bereit und ergänzt bestehende einschlägige Tools wie jene, die unter www.ssllabs.com bereitgestellt werden.

7. Fazit

SSL/TLS ist eine zentrale und breit verwendete Technologie für den sicheren Datenaustausch im Internet. Verbindungen, die über SSL/TLS abgesichert sind, sind prinzipiell in der Lage, die Authentizität, Integrität und Vertraulichkeit kommunizierter Daten zu gewährleisten. Voraussetzung dafür ist jedoch eine korrekte Verwendung des Protokolls bzw. die korrekte Konfiguration der Protokoll-Implementierung.

Um Behörden diesbezüglich zu unterstützen, wurden im vorliegenden Dokument diverse Empfehlungen zur Verwendung von SSL/TLS gegeben. Hauptaugenmerk wurde dabei auf die Wahl geeigneter kryptographischer Algorithmen, Schlüssellängen, Protokollversionen und Cipher-Suites gelegt. Daneben wurden einige allgemeine Empfehlungen definiert, die Behörden bei der sicheren Verwendung von SSL/TLS unterstützen können.

Neben der Erarbeitung und Definition einschlägiger Empfehlungen wurde zudem ein Tool entwickelt und bereitgestellt, das bei der Analyse von SSL/TLS-Servern und entsprechender Clients wie Web-Browsern hilfreich sein kann. Über dieses Tool können bestehende SSL/TLS-

Konfigurationen wie etwa konfigurierte und unterstützte Cipher-Suites einfach überprüft werden. Zusammen mit den definierten Empfehlungen bietet dieses Tool somit Behörden eine Unterstützung bei der Verwendung und Konfiguration von SSL/TLS.

Referenzen

[1] Peter Teufl, Andreas Reiter, Alexander Marsalek, Sandra Kreuzhuber: Kurzstudie HTTPS (SSL, TLS) Analyse österreichischer GV.AT Domänen. A-SIT. 2014.

[2] Thomas Zefferer: Sicherheitsempfehlungen für Behörden – Teil 1: Kryptographische Methoden. A-SIT. 2014.

[3] IBM Knowledge Center: An Overview of the SSL or TLS handshake. http://129.33.205.81/support/knowledgecenter/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009930_.htm?lang=en. Aufgerufen am 11.01.2016.

[4] Network Working Group: RFC 5289 - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM). http://tools.ietf.org/html/rfc5289. 2008.

[5] Network Working Group: RFC 4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). http://tools.ietf.org/html/rfc4492. 2006.

[6] Internet Engineering Task Force (IETF): RFC 6460 - Suite B Profile for Transport Layer Security (TLS). http://tools.ietf.org/html/rfc6460. 2012.

[7] Network Working Group: RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2. http://www.ietf.org/rfc/rfc5246.txt. 2008.

[8] OpenSSL Software Foundation: OpenSSL documents, ciphers. https://www.openssl.org/docs/apps/ciphers.html#CIPHER_SUITE_NAMES. Aufgerufen am 30.09.2014.

[9] Microsoft: Cipher Suites in Schannel. http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757%28v=vs.85%29.aspx. Aufgerufen am 11.01.2016.

[10] Qualys SSL Labs. https://www.ssllabs.com/index.html. Aufgerufen am 11.01.2016.

[11] The Sprawl: TLS and SSL Cipher Suites. http://www.thesprawl.org/research/tls-and-ssl-cipher-suites/. Aufgerufen am 11.01.2016.

[12] A-SIT: SSL/TLS Test. http://demoapps.a-sit.at/ssl-tool/. Aufgerufen am 11.01.2016.

[13] Qualys SSL Server Test. https://www.ssllabs.com/ssltest/. Aufgerufen am 11.01.2016.

[14] Qualys SSL/TLS Capabilities of Your Browser. https://www.ssllabs.com/ssltest/clients.html. Aufgerufen am 11.01.2016.

[15] W3Counter: December 2015 Market Share. http://www.w3counter.com/globalstats.php?year=2015&month=12. Aufgerufen am 11.01.2016.

[16] Netcraft: December 2015 Web Server Survey. http://news.netcraft.com/archives/2015/12/31/december-2015-web-server-survey.html. Aufgerufen am 12.01.2016.

[17] RSA Laboratories: PKCS #12: Personal Information Exchange Syntax Standard. http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm. Aufgerufen am 14.01.2016.

[18] RSA Laboratories: PKCS #7: Cryptographic Message Syntax Standard. http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-7-cryptographic-message-syntax-standar.htm. Aufgerufen am 14.01.2016.

[19] The Heartbleed Bug. http://heartbleed.com/. Aufgerufen am 14.01.2016.

[20] Tracking the FREAK Attack. https://freakattack.com/. Aufgerufen am 11.01.2016

[21] Breachattack. http://breachattack.com/. Aufgerufen am 06.01.2014.

[22] Florian Weimer: Factoring RSA Keys With TLS Perfect Forward Secrecy. https://people.redhat.com/~fweimer/rsa-crt-leaks.pdf. Aufgerufen am 13.01. 2016

[23] IBM: IBM Global Security Kit (GSKit) 8.0.14 Security Target. Version 3.5. 2012.

[24] Oracle: Java Cryptography Architecture Oracle Providers Documentation for JDK 8. http://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html. Aufgerufen am 11.01.2016.

[25] Oracle: Oracle Products and Services. http://www.oracle.com/us/products/index.html. Aufgerufen am 11.01.2016.

[26] Oracle: Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server 12.2.1.http://docs.oracle.com/middleware/1221/wls/SECMG/ssl_overview.htm#SECMG718. Aufgerufen am 11.01.2016.

[27] Oracle: Oracle® Fusion Middleware Administering Oracle Traffic Director. http://docs.oracle.com/middleware/1221/otd/admin/security.htm#OTADG235. Aufgerufen am 11.01.2016.

[28] Internet Enginnering Task Force (IETF): RFC 7525 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). https://tools.ietf.org/html/rfc7525. Mai 2015. Aufgerufen am 11.01.2016

[29] Android. Distribution of Android operating systems used by Android phone owners in October 2015, by platform version. http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/. Aufgerufen am 11.01.2016.

[30] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann *22nd ACM Conference on Computer and Communications Security* (CCS '15), Denver, CO, October 2015 https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

[31] Guide to Deploying Diffie-Hellman for TLS https://weakdh.org/sysadmin.html Aufgerufen am 11.01.2016

[32] Bettercrypto.org: Applied Crypto Hardening. https://bettercrypto.org/static/applied-crypto-hardening.pdf. Aufgerufen am 11.01.2016.

[33] Google: This POODLE bites: exploiting the SSL 3.0 fallback. http://googleonlinesecurity.blogspot.com.au/2014/10/this-poodle-bites-exploiting-ssl-30.html. Aufgerufen am 17.10.2014.

Anhang A: Cipher-Suites

Die folgende Tabelle enthält eine möglichst vollständige Auflistung verfügbarer Cipher-Suites. Zu jeder Cipher-Suite sind deren Eigenschaften wie zugrundeliegende SSL/TLS-Protokollversion und verwendete Algorithmen und Schlüssellängen angeführt. Jene Cipher-Suites, die in diesem Dokument als empfehlenswert klassifiziert werden, sind entsprechend dem in diesem Dokument verwendeten Farbschema farblich markiert.

Cipher-ID	Name	Protokoll	Schlüsselaustausch	Authentifizierung	Verschlüsselung	Schlüssellänge	MAC
0x000000	TLS_NULL_WITH_NULL_NULL	(Session Establishment)	NULL	NULL	NULL	0	NULL
0x000001	TLS_RSA_WITH_NULL_MD5	TLS 1.0	RSA	RSA	NULL	0	MD5
0x000002	TLS_RSA_WITH_NULL_SHA	TLS 1.0	RSA	RSA	NULL	0	SHA
0x000003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS 1.0	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5
0x000004	TLS_RSA_WITH_RC4_128_MD5	TLS 1.0	RSA	RSA	RC4_128	128	MD5
0x000005	TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	RSA	RSA	RC4_128	128	SHA
0x000006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS 1.0	RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5
0x000007	TLS_RSA_WITH_IDEA_CBC_SHA	TLS 1.0	RSA	RSA	IDEA_CBC	128	SHA
0x000008	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
0x000009	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	RSA	RSA	DES_CBC	56	SHA
0x00000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	RSA	RSA	3DES_EDE_CBC	168	SHA
0x00000B	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0	DH	DSS	DES40_CBC	40	SHA
0x00000C	TLS_DH_DSS_WITH_DES_CBC_SHA	TLS 1.0	DH	DSS	DES_CBC	56	SHA
0x00000D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DH	DSS	3DES_EDE_CBC	168	SHA
0x00000E	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0	DH	RSA	DES40_CBC	40	SHA
0x00000F	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS 1.0	DH	RSA	DES_CBC	56	SHA
0x000010	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DH	RSA	3DES_EDE_CBC	168	SHA
0x000011	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0	DHE	DSS	DES40_CBC	40	SHA
0x000012	TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS 1.0	DHE	DSS	DES_CBC	56	SHA
0x000013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DHE	DSS	3DES_EDE_CBC	168	SHA
0x000014	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0	DHE	RSA	DES40_CBC	40	SHA
0x000015	TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS 1.0	DHE	RSA	DES_CBC	56	SHA
0x000016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DHE	RSA	3DES_EDE_CBC	168	SHA

0x000017	TLS_DH_Anon_EXPORT_WITH_RC4_40_MD5	TLS 1.0	DH	Anon	RC4_40	40	MD5
0x000018	TLS_DH_Anon_WITH_RC4_128_MD5	TLS 1.0	DH	Anon	RC4_128	128	MD5
0x000019	TLS_DH_Anon_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0	DH	Anon	DES40_CBC	40	SHA
0x00001A	TLS_DH_Anon_WITH_DES_CBC_SHA	TLS 1.0	DH	Anon	DES_CBC	56	SHA
0x00001B	TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA	TLS 1.0	DH	Anon	3DES_EDE_CBC	168	SHA
0x00001C	SSL_FORTEZZA_KEA_WITH_NULL_SHA	SSL 3.0	FORTEZZA	KEA	NULL	0	SHA
0x00001D	SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA	SSL 3.0	FORTEZZA	KEA	FORTEZZA_CBC	80	SHA
0x00001E	TLS_KRB5_WITH_DES_CBC_SHA	Erweiterung zu TLS 1.0	KRB5	KRB5	DES_CBC	56	SHA
0x00001F	TLS_KRB5_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0	KRB5	KRB5	3DES_EDE_CBC	168	SHA
0x000020	TLS_KRB5_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0	KRB5	KRB5	RC4_128	128	SHA
0x000021	TLS_KRB5_WITH_IDEA_CBC_SHA	Erweiterung zu TLS 1.0	KRB5	KRB5	IDEA_CBC	128	SHA
0x000022	TLS_KRB5_WITH_DES_CBC_MD5	Erweiterung zu TLS 1.0	KRB5	KRB5	DES_CBC	56	MD5
0x000023	TLS_KRB5_WITH_3DES_EDE_CBC_MD5	Erweiterung zu TLS 1.0	KRB5	KRB5	3DES_EDE_CBC	168	MD5
0x000024	TLS_KRB5_WITH_RC4_128_MD5	Erweiterung zu TLS 1.0	KRB5	KRB5	RC4_128	128	MD5
0x000025	TLS_KRB5_WITH_IDEA_CBC_MD5	Erweiterung zu TLS 1.0	KRB5	KRB5	IDEA_CBC	128	MD5
0x000026	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	Erweiterung zu TLS 1.0	KRB5_EXPORT	KRB5_EXPORT	DES_CBC_40	40	SHA
0x000027	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA	Erweiterung zu TLS 1.0	KRB5_EXPORT	KRB5_EXPORT	RC2_CBC_40	40	SHA
0x000028	TLS_KRB5_EXPORT_WITH_RC4_40_SHA	Erweiterung zu TLS 1.0	KRB5_EXPORT	KRB5_EXPORT	RC4_40	40	SHA
0x000029	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	Erweiterung zu TLS 1.0	KRB5_EXPORT	KRB5_EXPORT	DES_CBC_40	40	MD5
0x00002A	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5	Erweiterung zu TLS 1.0	KRB5_EXPORT	KRB5_EXPORT	RC2_CBC_40	40	MD5
0x00002B	TLS_KRB5_EXPORT_WITH_RC4_40_MD5	Erweiterung zu TLS 1.0	KRB5_EXPORT	KRB5_EXPORT	RC4_40	40	MD5
0x00002C	TLS_PSK_WITH_NULL_SHA	Erweiterung zu TLS 1.0	PSK	PSK	NULL	0	SHA
0x00002D	TLS_DHE_PSK_WITH_NULL_SHA	Erweiterung zu TLS 1.0	DHE	PSK	NULL	0	SHA
0x00002E	TLS_RSA_PSK_WITH_NULL_SHA	Erweiterung zu TLS 1.0	RSA	PSK	NULL	0	SHA
0x00002F	TLS_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	RSA	RSA	AES_128_CBC	128	SHA
0x000030	TLS_DH_DSS_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	DH	DSS	AES_128_CBC	128	SHA
0x000031	TLS_DH_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	DH	RSA	AES_128_CBC	128	SHA
0x000032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	DHE	DSS	AES_128_CBC	128	SHA
0x000033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	DHE	RSA	AES_128_CBC	128	SHA
0x000034	TLS_DH_Anon_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	DH	Anon	AES_128_CBC	128	SHA
0x000035	TLS_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	RSA	RSA	AES_256_CBC	256	SHA

0x000036	TLS_DH_DSS_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	DH	DSS	AES_256_CBC	256	SHA
0x000037	TLS_DH_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	DH	RSA	AES_256_CBC	256	SHA
0x000038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	DHE	DSS	AES_256_CBC	256	SHA
0x000039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	DHE	RSA	AES_256_CBC	256	SHA
0x00003A	TLS_DH_Anon_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	DH	Anon	AES_256_CBC	256	SHA
0x00003B	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	RSA	RSA	NULL	0	SHA256
0x00003C	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	RSA	RSA	AES_128_CBC	128	SHA256
0x00003D	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	RSA	RSA	AES_256_CBC	256	SHA256
0x00003E	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	TLS 1.2	DH	DSS	AES_128_CBC	128	SHA256
0x00003F	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	DH	RSA	AES_128_CBC	128	SHA256
0x000040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS 1.2	DHE	DSS	AES_128_CBC	128	SHA256
0x000041	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0	RSA	RSA	CAMELLIA_128_CBC	128	SHA
0x000042	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0	DH	DSS	CAMELLIA_128_CBC	128	SHA
0x000043	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0	DH	RSA	CAMELLIA_128_CBC	128	SHA
0x000044	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0	DHE	DSS	CAMELLIA_128_CBC	128	SHA
0x000045	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0	DHE	RSA	CAMELLIA_128_CBC	128	SHA
0x000046	TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0	DH	Anon	CAMELLIA_128_CBC	128	SHA
0x000047	TLS_ECDH_ECDSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	NULL	0	SHA
0x000048	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	RC4_128	128	SHA
0x00004A	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	3DES_EDE_CBC	168	SHA
0x00004B	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	AES_128_CBC	128	SHA
0x00004C	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	AES_256_CBC	256	SHA
0x000062	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel	RSA_EXPORT 1024	RSA_EXPORT 1024	DES_CBC	56	SHA
0x000063	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel	DHE	DSS	DES_CBC	56	SHA
0x000064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel	RSA_EXPORT 1024	RSA_EXPORT 1024	RC4_56	56	SHA
0x000065	TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel	DHE	DSS	RC4_56	56	SHA
0x000066	TLS_DHE_DSS_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel	DHE	DSS	RC4_128	128	SHA
0x000067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	DHE	RSA	AES_128_CBC	128	SHA256

0x000068	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	TLS 1.2	DH	DSS	AES_256_CBC	256	SHA256
0x000069	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	DH	RSA	AES_256_CBC	256	SHA256
0x00006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS 1.2	DHE	DSS	AES_256_CBC	256	SHA256
0x00006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	DHE	RSA	AES_256_CBC	256	SHA256
0x00006C	TLS_DH_Anon_WITH_AES_128_CBC_SHA256	TLS 1.2	DH	Anon	AES_128_CBC	128	SHA256
0x00006D	TLS_DH_Anon_WITH_AES_256_CBC_SHA256	TLS 1.2	DH	Anon	AES_256_CBC	256	SHA256
0x000080	TLS_GOSTR341094_WITH_28147_CNT_IMIT	Erweiterung zu TLS 1.0	VKO GOST R 34.10-94	VKO GOST R 34.10-94	GOST28147	256	GOST28147
0x000081	TLS_GOSTR341001_WITH_28147_CNT_IMIT	Erweiterung zu TLS 1.0	VKO GOST R 34.10-2001	VKO GOST R 34.10-2001	GOST28147	256	GOST28147
0x000082	TLS_GOSTR341094_WITH_NULL_GOSTR3411	Erweiterung zu TLS 1.0	VKO GOST R 34.10-94	VKO GOST R 34.10-94	NULL	0	GOSTR3411
0x000083	TLS_GOSTR341001_WITH_NULL_GOSTR3411	Erweiterung zu TLS 1.0	VKO GOST R 34.10-2001	VKO GOST R 34.10-2001	NULL	0	GOSTR3411
0x000084	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0	RSA	RSA	CAMELLIA_256_CBC	256	SHA
0x000085	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0	DH	DSS	CAMELLIA_256_CBC	256	SHA
0x000086	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0	DH	RSA	CAMELLIA_256_CBC	256	SHA
0x000087	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0	DHE	DSS	CAMELLIA_256_CBC	256	SHA
0x000088	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0	DHE	RSA	CAMELLIA_256_CBC	256	SHA
0x000089	TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0	DH	Anon	CAMELLIA_256_CBC	256	SHA
0x00008A	TLS_PSK_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0	PSK	PSK	RC4_128	128	SHA
0x00008B	TLS_PSK_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0	PSK	PSK	3DES_EDE_CBC	168	SHA
0x00008C	TLS_PSK_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	PSK	PSK	AES_128_CBC	128	SHA
0x00008D	TLS_PSK_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	PSK	PSK	AES_256_CBC	256	SHA
0x00008E	TLS_DHE_PSK_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0	DHE	PSK	RC4_128	128	SHA
0x00008F	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0	DHE	PSK	3DES_EDE_CBC	168	SHA
0x000090	TLS_DHE_PSK_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	DHE	PSK	AES_128_CBC	128	SHA
0x000091	TLS_DHE_PSK_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	DHE	PSK	AES_256_CBC	256	SHA
0x000092	TLS_RSA_PSK_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0	RSA	PSK	RC4_128	128	SHA
0x000093	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0	RSA	PSK	3DES_EDE_CBC	168	SHA
0x000094	TLS_RSA_PSK_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	RSA	PSK	AES_128_CBC	128	SHA
0x000095	TLS_RSA_PSK_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	RSA	PSK	AES_256_CBC	256	SHA
0x000096	TLS_RSA_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0	RSA	RSA	SEED_CBC	128	SHA
0x000097	TLS_DH_DSS_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0	DH	DSS	SEED_CBC	128	SHA

0x000098	TLS_DH_RSA_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0	DH	RSA	SEED_CBC	128	SHA
0x000099	TLS_DHE_DSS_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0	DHE	DSS	SEED_CBC	128	SHA
0x00009A	TLS_DHE_RSA_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0	DHE	RSA	SEED_CBC	128	SHA
0x00009B	TLS_DH_Anon_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0	DH	Anon	SEED_CBC	128	SHA
0x00009C	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	RSA	RSA	AES_128_GCM	128	SHA256
0x00009D	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	RSA	RSA	AES_256_GCM	256	SHA384
0x00009E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	DHE	RSA	AES_128_GCM	128	SHA256
0x00009F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	DHE	RSA	AES_256_GCM	256	SHA384
0x0000A0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	DH	RSA	AES_128_GCM	128	SHA256
0x0000A1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	DH	RSA	AES_256_GCM	256	SHA384
0x0000A2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS 1.2	DHE	DSS	AES_128_GCM	128	SHA256
0x0000A3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS 1.2	DHE	DSS	AES_256_GCM	256	SHA384
0x0000A4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	TLS 1.2	DH	DSS	AES_128_GCM	128	SHA256
0x0000A5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	TLS 1.2	DH	DSS	AES_256_GCM	256	SHA384
0x0000A6	TLS_DH_Anon_WITH_AES_128_GCM_SHA256	TLS 1.2	DH	Anon	AES_128_GCM	128	SHA256
0x0000A7	TLS_DH_Anon_WITH_AES_256_GCM_SHA384	TLS 1.2	DH	Anon	AES_256_GCM	256	SHA384
0x0000A8	TLS_PSK_WITH_AES_128_GCM_SHA256	Erweiterung zu TLS 1.2	PSK	PSK	AES_128_GCM	128	SHA256
0x0000A9	TLS_PSK_WITH_AES_256_GCM_SHA384	Erweiterung zu TLS 1.2	PSK	PSK	AES_256_GCM	256	SHA384
0x0000AA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	Erweiterung zu TLS 1.2	DHE	PSK	AES_128_GCM	128	SHA256
0x0000AB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	Erweiterung zu TLS 1.2	DHE	PSK	AES_256_GCM	256	SHA384
0x0000AC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256	Erweiterung zu TLS 1.2	RSA	PSK	AES_128_GCM	128	SHA256
0x0000AD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384	Erweiterung zu TLS 1.2	RSA	PSK	AES_256_GCM	256	SHA384
0x0000AE	TLS_PSK_WITH_AES_128_CBC_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	PSK	PSK	AES_128_CBC	128	SHA256
0x0000AF	TLS_PSK_WITH_AES_256_CBC_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	PSK	PSK	AES_256_CBC	256	SHA384
0x0000B0	TLS_PSK_WITH_NULL_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	PSK	PSK	NULL	0	SHA256
0x0000B1	TLS_PSK_WITH_NULL_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	PSK	PSK	NULL	0	SHA384
0x0000B2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	DHE	PSK	AES_128_CBC	128	SHA256
0x0000B3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	DHE	PSK	AES_256_CBC	256	SHA384
0x0000B4	TLS_DHE_PSK_WITH_NULL_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	DHE	PSK	NULL	0	SHA256

0x0000B5	TLS_DHE_PSK_WITH_NULL_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	DHE	PSK	NULL	0	SHA384
0x0000B6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	RSA	PSK	AES_128_CBC	128	SHA256
0x0000B7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	RSA	PSK	AES_256_CBC	256	SHA384
0x0000B8	TLS_RSA_PSK_WITH_NULL_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	RSA	PSK	NULL	0	SHA256
0x0000B9	TLS_RSA_PSK_WITH_NULL_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	RSA	PSK	NULL	0	SHA384
0x00C001	TLS_ECDH_ECDSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	NULL	0	SHA
0x00C002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	RC4_128	128	SHA
0x00C003	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	3DES_EDE_CBC	168	SHA
0x00C004	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	AES_128_CBC	128	SHA
0x00C005	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	ECDSA	AES_256_CBC	256	SHA
0x00C006	TLS_ECDHE_ECDSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	ECDSA	NULL	0	SHA
0x00C007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	ECDSA	RC4_128	128	SHA
0x00C008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	ECDSA	3DES_EDE_CBC	168	SHA
0x00C009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	ECDSA	AES_128_CBC	128	SHA
0x00C00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	ECDSA	AES_256_CBC	256	SHA
0x00C00B	TLS_ECDH_RSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	RSA	NULL	0	SHA
0x00C00C	TLS_ECDH_RSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	RSA	RC4_128	128	SHA
0x00C00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	RSA	3DES_EDE_CBC	168	SHA
0x00C00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	RSA	AES_128_CBC	128	SHA
0x00C00F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	RSA	AES_256_CBC	256	SHA
0x00C010	TLS_ECDHE_RSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	RSA	NULL	0	SHA
0x00C011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	RSA	RC4_128	128	SHA
0x00C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	RSA	3DES_EDE_CBC	168	SHA
0x00C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	RSA	AES_128_CBC	128	SHA

0x00C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDHE	RSA	AES_256_CBC	256	SHA
0x00C015	TLS_ECDH_Anon_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	Anon	NULL	0	SHA
0x00C016	TLS_ECDH_Anon_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	Anon	RC4_128	128	SHA
0x00C017	TLS_ECDH_Anon_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	Anon	3DES_EDE_CBC	168	SHA
0x00C018	TLS_ECDH_Anon_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	Anon	AES_128_CBC	128	SHA
0x00C019	TLS_ECDH_Anon_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	ECDH	Anon	AES_256_CBC	256	SHA
0x00C01A	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	3DES_EDE_CBC	168	SHA
0x00C01B	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	3DES_EDE_CBC	168	SHA
0x00C01C	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	3DES_EDE_CBC	168	SHA
0x00C01D	TLS_SRP_SHA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	AES_128_CBC	128	SHA
0x00C01E	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	AES_128_CBC	128	SHA
0x00C01F	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	AES_128_CBC	128	SHA
0x00C020	TLS_SRP_SHA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	AES_256_CBC	256	SHA
0x00C021	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	AES_256_CBC	256	SHA
0x00C022	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.1	SRP	SHA	AES_256_CBC	256	SHA
0x00C023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2	ECDHE	ECDSA	AES_128_CBC	128	SHA256
0x00C024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2	ECDHE	ECDSA	AES_256_CBC	256	SHA384
0x00C025	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2	ECDH	ECDSA	AES_128_CBC	128	SHA256
0x00C026	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2	ECDH	ECDSA	AES_256_CBC	256	SHA384
0x00C027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	ECDHE	RSA	AES_128_CBC	128	SHA256
0x00C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2	ECDHE	RSA	AES_256_CBC	256	SHA384
0x00C029	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	ECDH	RSA	AES_128_CBC	128	SHA256
0x00C02A	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2	ECDH	RSA	AES_256_CBC	256	SHA384
0x00C02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2	ECDHE	ECDSA	AES_128_GCM	128	SHA256
0x00C02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2	ECDHE	ECDSA	AES_256_GCM	256	SHA384
0x00C02D	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2	ECDH	ECDSA	AES_128_GCM	128	SHA256
0x00C02E	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2	ECDH	ECDSA	AES_256_GCM	256	SHA384
0x00C02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	ECDHE	RSA	AES_128_GCM	128	SHA256
0x00C030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	ECDHE	RSA	AES_256_GCM	256	SHA384

0x00C031	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	ECDH	RSA	AES_128_GCM	128	SHA256
0x00C032	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	ECDH	RSA	AES_256_GCM	256	SHA384
0x00C033	TLS_ECDHE_PSK_WITH_RC4_128_SHA	Erweiterung zu TLS 1.1	ECDHE	PSK	RC4_128	128	SHA
0x00C034	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.1	ECDHE	PSK	3DES_EDE_CBC	168	SHA
0x00C035	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.1	ECDHE	PSK	AES_128_CBC	128	SHA
0x00C036	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.1	ECDHE	PSK	AES_256_CBC	256	SHA
0x00C037	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	ECDHE	PSK	AES_128_CBC	128	SHA256
0x00C038	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	ECDHE	PSK	AES_256_CBC	256	SHA384
0x00C039	TLS_ECDHE_PSK_WITH_NULL_SHA	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	ECDHE	PSK	NULL	0	SHA
0x00C03A	TLS_ECDHE_PSK_WITH_NULL_SHA256	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	ECDHE	PSK	NULL	0	SHA256
0x00C03B	TLS_ECDHE_PSK_WITH_NULL_SHA384	Erweiterung zu TLS 1.0, TLS, 1.1 und TLS 1.2	ECDHE	PSK	NULL	0	SHA384
0x00CC13	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2	ECDHE	RSA	ChaCha20_Poly1305	256	SHA256
0x00CC14	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2	ECDHE	ECDSA	ChaCha20_Poly1305	256	SHA256
0x00CC15	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2	DHE	RSA	ChaCha20_Poly1305	256	SHA256
0x00FEFE	SSL_RSA_FIPS_WITH_DES_CBC_SHA	SSL 3.0	RSA_FIPS	RSA_FIPS	DES_CBC	56	SHA
0x00FEFF	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	RSA_FIPS	RSA_FIPS	3DES_EDE_CBC	168	SHA
0x00FFE0	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	RSA_FIPS	RSA_FIPS	3DES_EDE_CBC	168	SHA
0x00FFE1	SSL_RSA_FIPS_WITH_DES_CBC_SHA	SSL 3.0	RSA_FIPS	RSA_FIPS	DES_CBC	56	SHA
0x010080	SSL2_RC4_128_WITH_MD5	SSL 2.0	RSA	RSA	RC4_128	128	MD5
0x020080	SSL2_RC4_128_EXPORT40_WITH_MD5	SSL 2.0	RSA	RSA	RC4_128_EXPORT40	40	MD5
0x030080	SSL2_RC2_CBC_128_CBC_WITH_MD5	SSL 2.0	RSA	RSA	RC2_CBC_128_CBC	128	MD5
0x040080	SSL2_RC2_CBC_128_CBC_WITH_MD5	SSL 2.0	RSA	RSA	RC2_CBC_128_CBC	128	MD5
0x050080	SSL2_IDEA_128_CBC_WITH_MD5	SSL 2.0	RSA	RSA	IDEA_128_CBC	128	MD5
0x060040	SSL2_DES_64_CBC_WITH_MD5	SSL 2.0	RSA	RSA	DES_64_CBC	64	MD5
0x0700C0	SSL2_DES_192_EDE3_CBC_WITH_MD5	SSL 2.0	RSA	RSA	DES_192_EDE3_CBC	192	MD5
0x080080	SSL2_RC4_64_WITH_MD5	SSL 2.0	RSA	RSA	RC4_64	64	MD5
N/A	SSL_CK_RC4_128_WITH_MD5	SSL 2.0	N/A	N/A	RC4	128	MD5
N/A	SSL_CK_DES_192_EDE3_CBC_WITH_MD5	SSL 2.0	N/A	N/A	DES_192_EDE3_CBC	192	MD5
N/A	SSL_CK_RC4_128_EXPORT40_MD5	SSL 2.0	N/A	N/A	RC4_128_EXPORT40	128	MD5

N/A	SSL_CK_DES_64_CBC_WITH_MD5	SSL 2.0	N/A	N/A	DES_64_CBC	64	MD5
N/A	SSL_RSA_WITH_NULL_MD5	SSL 3.0	RSA	RSA	NULL	0	MD5
N/A	SSL_RSA_WITH_NULL_SHA	SSL 3.0	RSA	RSA	NULL	0	SHA
N/A	SSL_RSA_EXPORT_WITH_RC4_40_MD5	SSL 3.0	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5
N/A	SSL_RSA_WITH_RC4_128_MD5	SSL 3.0	RSA	RSA	RC4_128	128	MD5
N/A	SSL_RSA_WITH_RC4_128_SHA	SSL 3.0	RSA	RSA	RC4_128	128	SHA
N/A	SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	SSL 3.0	RSA_EXPORT	RSA_EXPORT	RC_CBC_40	40	MD5
N/A	SSL_RSA_WITH_IDEA_CBC_SHA	SSL 3.0	RSA	RSA	IDEA_CBC	128	SHA
N/A	SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
N/A	SSL_RSA_WITH_DES_CBC_SHA	SSL 3.0	RSA	RSA	DES_CBC	56	SHA
N/A	SSL_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0	RSA	RSA	3DES_EDE_CBC	168	SHA
N/A	SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0	DH	DSS_EXPORT	DES40_CBC	40	SHA
N/A	SSL_DH_DSS_WITH_DES_CBC_SHA	SSL 3.0	DH	DSS	DES_CBC	56	SHA
N/A	SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	DH	DSS	3DES_EDE_CBC	168	SHA
N/A	SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0	DH	RSA_EXPORT	DES40_CBC	40	SHA
N/A	SSL_DH_RSA_WITH_DES_CBC_SHA	SSL 3.0	DH	RSA	DES_CBC	56	SHA
N/A	SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0	DH	RSA	3DES_EDE_CBC	168	SHA
N/A	SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0	DHE	DSS_EXPORT	DES40_CBC	40	SHA
N/A	SSL_DHE_DSS_WITH_DES_CBC_SHA	SSL 3.0	DHE	DSS	DES_CBC	56	SHA
N/A	SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	DHE	DSS	3DES_EDE_CBC	168	SHA
N/A	SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0	DHE	RSA_EXPORT	DES40_CBC	40	SHA
N/A	SSL_DHE_RSA_WITH_DES_CBC_SHA	SSL 3.0	DHE	RSA	DES_CBC	56	SHA
N/A	SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0	DHE	RSA	3DES_EDE_CBC	168	SHA
N/A	SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	SSL 3.0	DH	Anon	RC4_40	40	MD5
N/A	SSL_DH_anon_WITH_RC4_128_MD5	SSL 3.0	DH	Anon	RC4_128	128	MD5
N/A	SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0	DH	Anon	DES40_CBC	40	SHA
N/A	SSL_DH_anon_WITH_DES_CBC_SHA	SSL 3.0	DH	Anon	DES_CBC	56	SHA
N/A	SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	SSL 3.0	DH	Anon	3DES_EDE_CBC	168	SHA
0x00C072	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2	ECDHE	ECDSA	CAMELLIA_128_CBC	128	SHA256
0x00C073	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2	ECDHE	ECDSA	CAMELLIA_256_CBC	256	SHA384
0x00C074	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2	ECDH	ECDSA	CAMELLIA_128_CBC	128	SHA256

0x00C075	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2	ECDH	ECDSA	CAMELLIA_256_CBC	256	SHA384
0x00C076	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2	ECDHE	RSA	CAMELLIA_128_CBC	128	SHA256
0x00C077	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2	ECDHE	RSA	CAMELLIA_256_CBC	256	SHA384
0x00C078	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2	ECDH	RSA	CAMELLIA_128_CBC	128	SHA256
0x00C079	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2	ECDH	RSA	CAMELLIA_256_CBC	256	SHA384
N/A	SSL_CK_RC4_128_EXPORT40_WITH_MD5	SSL 2.0	N/A	N/A	RC4_128_EXPORT40	128	MD5
N/A	SSL_CK_RC2_128_CBC_WITH_MD5	SSL 2.0	N/A	N/A	RC2_128_CBC	128	MD5
N/A	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	SSL 2.0	N/A	N/A	RC2_128_CBC_EXPORT40	128	MD5
N/A	SSL_CK_IDEA_128_CBC_WITH_MD5	SSL 2.0	N/A	N/A	IDEA_128_CBC	128	MD5

Anhang B: Unterstützung von Cipher-Suites durch Web-Browser und Web-Server

Die folgende Tabelle enthält eine Auflistung jener Cipher-Suites, die von gängigen Web-Browsern und Web-Server-Software unterstützt werden. Die nachstehende Tabelle entspricht damit jener aus Anhang A, ist jedoch um jene Cipher-Suites reduziert, die von keiner der betrachteten Software-Komponenten unterstützt werden. In diesem Dokument empfohlene Cipher-Suites sind wieder entsprechend dem verwendeten Farbschema markiert.

Name	Protokoll	Chrome 37	Firefox 32	IE 11	Safari 7	Apache (OpenSSL)	Microsoft IIS (SChannel)	Nginx (OpenSSL)	GWS	IHS (IBM) (GSKit)	Oracle (JSSE)
SSL_CK_RC4_128_WITH_MD5	SSL 2.0					x	x	x			
SSL_CK_DES_192_EDE3_CBC_WITH_MD5	SSL 2.0					x	x	x			
SSL_CK_RC4_128_EXPORT40_MD5	SSL 2.0						x				
SSL_CK_DES_64_CBC_WITH_MD5	SSL 2.0					x	x	x			
SSL_CK_RC4_128_EXPORT40_WITH_MD5	SSL 2.0					x		x			
SSL_CK_RC2_128_CBC_WITH_MD5	SSL 2.0					x		x			
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	SSL 2.0					x		x			
SSL_CK_IDEA_128_CBC_WITH_MD5	SSL 2.0					x		x			
SSL_RSA_WITH_NULL_MD5	SSL 3.0					x		x			x
SSL_RSA_WITH_NULL_SHA	SSL 3.0					x		x			x
SSL_RSA_EXPORT_WITH_RC4_40_MD5	SSL 3.0					x		x			x
SSL_RSA_WITH_RC4_128_MD5	SSL 3.0					x		x			x
SSL_RSA_WITH_RC4_128_SHA	SSL 3.0					x		x			x
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5	SSL 3.0					x		x			
SSL_RSA_WITH_IDEA_CBC_SHA	SSL 3.0					x		x			
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0					x		x			x
SSL_RSA_WITH_DES_CBC_SHA	SSL 3.0					x		x			x
SSL_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0					x		x			x
SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0					x		x			
SSL_DH_DSS_WITH_DES_CBC_SHA	SSL 3.0					x		x			
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA	SSL 3.0					x		x			
SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0					x		x			

SSL_DH_RSA_WITH_DES_CBC_SHA	SSL 3.0					x		x			
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0					x		x			
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0					x		x			x
SSL_DHE_DSS_WITH_DES_CBC_SHA	SSL 3.0					x		x			x
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	SSL 3.0					x		x			x
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0					x		x			x
SSL_DHE_RSA_WITH_DES_CBC_SHA	SSL 3.0					x		x			x
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0					x		x			x
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	SSL 3.0					x		x			x
SSL_DH_anon_WITH_RC4_128_MD5	SSL 3.0					x		x			x
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	SSL 3.0					x		x			x
SSL_DH_anon_WITH_DES_CBC_SHA	SSL 3.0					x		x			x
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	SSL 3.0					x		x			x
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0										
SSL_RSA_FIPS_WITH_DES_CBC_SHA	SSL 3.0										
TLS_RSA_WITH_NULL_MD5	TLS 1.0					x	x	x			
TLS_RSA_WITH_NULL_SHA	TLS 1.0						x				
TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS 1.0					x	x	x			
TLS_RSA_WITH_RC4_128_MD5	TLS 1.0	x	x		x	x	x	x	x		
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	x	x		x	x	x	x	x		
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS 1.0					x		x			
TLS_RSA_WITH_IDEA_CBC_SHA	TLS 1.0					x		x			
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0					x		x			
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0					x	x	x			
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	x	x	x	x	x	x	x	x	x	
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0					x		x			
TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS 1.0					x	x	x			
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0			x		x	x	x			
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0					x		x			
TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS 1.0					x		x			
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0		x		x	x		x			

TLS_DH_Anon_EXPORT_WITH_RC4_40_MD5	TLS 1.0					x		x			
TLS_DH_Anon_WITH_RC4_128_MD5	TLS 1.0					x		x			
TLS_DH_Anon_EXPORT_WITH_DES40_CBC_SHA	TLS 1.0					x		x			
TLS_DH_Anon_WITH_DES_CBC_SHA	TLS 1.0					x		x			
TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA	TLS 1.0					x		x			
TLS_KRB5_WITH_DES_CBC_SHA	Erweiterung zu TLS 1.0										x
TLS_KRB5_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0										x
TLS_KRB5_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0										x
TLS_KRB5_WITH_DES_CBC_MD5	Erweiterung zu TLS 1.0										x
TLS_KRB5_WITH_3DES_EDE_CBC_MD5	Erweiterung zu TLS 1.0										x
TLS_KRB5_WITH_RC4_128_MD5	Erweiterung zu TLS 1.0										x
TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	Erweiterung zu TLS 1.0										x
TLS_KRB5_EXPORT_WITH_RC4_40_SHA	Erweiterung zu TLS 1.0										x
TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	Erweiterung zu TLS 1.0										x
TLS_KRB5_EXPORT_WITH_RC4_40_MD5	Erweiterung zu TLS 1.0										x
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel					x	x	x			
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel					x	x	x			
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel					x	x	x			
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel					x		x			
TLS_DHE_DSS_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0, SSL 3.0 kompatibel					x		x			
TLS_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	x	x	x	x	x	x	x	x	x	x
TLS_DH_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	x	x	x			x				x
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	x	x		x	x		x			x
TLS_DH_anon_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0										x
TLS_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	x	x	x	x	x	x	x	x	x	x
TLS_DH_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0		x	x			x				x
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	x	x		x	x		x			x

TLS_DH_anon_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0										x
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0		x			x		x			
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0		x			x		x			
TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_GOSTR341094_WITH_28147_CNT_IMIT	Erweiterung zu TLS 1.0					x		x			
TLS_GOSTR341001_WITH_28147_CNT_IMIT	Erweiterung zu TLS 1.0					x		x			
TLS_GOSTR341094_WITH_NULL_GOSTR3411	Erweiterung zu TLS 1.0					x		x			
TLS_GOSTR341001_WITH_NULL_GOSTR3411	Erweiterung zu TLS 1.0					x		x			
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0		x			x		x			
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0		x			x		x			
TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_PSK_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_PSK_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_PSK_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_PSK_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_RSA_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DH_DSS_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DH_RSA_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_DSS_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DHE_RSA_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_DH_Anon_WITH_SEED_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_ECDH_ECDSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x

TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x
TLS_ECDHE_ECDSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x		x	x		x	x		x
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x	x	x	x
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x	x	x
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x	x	x
TLS_ECDH_RSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDH_RSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x			x
TLS_ECDHE_RSA_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDHE_RSA_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x		x	x		x	x		x
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1		x		x	x		x	x	x	x
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x		x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x		x
TLS_ECDH_Anon_WITH_NULL_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDH_Anon_WITH_RC4_128_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDH_Anon_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDH_Anon_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_ECDH_Anon_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1					x		x			x
TLS_RSA_WITH_NULL_SHA256	TLS 1.2					x	x	x			x
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2			x	x	x	x	x	x	x	x

TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2			x	x	x	x	x	x	x	x
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	TLS 1.2					x		x			
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2					x		x			
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS 1.2			x		x	x	x			x
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2				x	x		x			x
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	TLS 1.2					x		x			
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2					x		x			
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS 1.2			x		x	x	x			x
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2				x	x		x			x
TLS_DH_Anon_WITH_AES_128_CBC_SHA256	TLS 1.2					x		x			x
TLS_DH_Anon_WITH_AES_256_CBC_SHA256	TLS 1.2					x		x			x
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	x		x		x		x	x	x	x
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2			x		x		x	x	x	x
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	x		x		x		x			x
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2			x		x		x			x
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2					x		x			
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x			
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS 1.2					x		x			x
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x			x
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	TLS 1.2					x		x			
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x			
TLS_DH_Anon_WITH_AES_128_GCM_SHA256	TLS 1.2					x		x			x
TLS_DH_Anon_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x			x
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2				x	x		x			x
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2				x	x		x			x
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2				x	x		x			x
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2				x	x		x			x

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2	x	x	x		x	x	x	x	x	x
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2			x		x	x	x	x	x	x
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2					x		x			x
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x			x
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	x	x			x		x	x	x	x
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x	x	x	x
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2					x		x			x
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x			x
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2	x							x		
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2	x							x		
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2					x		x			
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2					x		x			
TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2					x		x			
TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2					x		x			
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2					x		x			
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2					x		x			
TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2					x		x			
TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2					x		x			

Anhang C: Empfohlene Cipher-Suites

Die folgende Tabelle enthält alle empfohlenen Cipher-Suites. Alle angeführten Cipher-Suites erfüllen die in diesem Dokument definierten MUSS-Kriterien. Dunkelgrün hinterlegte Cipher-Suites erfüllen zusätzlich alle SOLL-Kriterien, bieten damit eine hohe Sicherheit und darüber hinaus eine adäquate Unterstützung auf gängigen Web-Browsern. Hellgrün hinterlegte Cipher-Suites bieten ebenfalls hohe Sicherheit durch Unterstützung aller MUSS- und SOLL-Kriterien, allerdings nur beschränkte Unterstützung auf Web-Browsern. Serverseitig können diese Cipher-Suites bedenkenlos unterstützt werden. Um die Client-Kompatibilität weiter zu erhöhen, können zusätzlich die orange hinterlegten Cipher-Suites serverseitig unterstützt werden. Diese bieten ein ausreichendes Maß an Sicherheit, erfüllen jedoch nicht alle in diesem Dokument definierten SOLL-Kriterien.

Name	Protokoll	Chrome 37	Firefox 32	IE 11	Safari 7	Apache (OpenSSL)	Microsoft IIS (SChannel)	Nginx (OpenSSL)	GWS	IHS (IBM) (GSKit)	Oracle (JSSE)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS 1.2	x	x	x		x	x	x	x	x	x
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	x	x			x		x	x	x	x
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2			x	x	x	x	x	x	x	x
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS 1.2			x		x	x	x	x	x	x
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x	x	x	x
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2			x		x		x			x
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS 1.2					x		x			x
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2				x	x		x			x
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS 1.2			x		x	x	x			x
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	x		x		x		x			x
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS 1.2					x		x			x
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2				x	x		x			x
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS 1.2			x		x	x	x			x
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2					x		x			
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	Erweiterung zu TLS 1.2					x		x			
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2					x		x			

TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	Erweiterung zu TLS 1.2					x		x			
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2	x							x		
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Erweiterung zu TLS 1.2	x							x		
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x	x	x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x		x
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0	x	x		x	x		x			x
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	Erweiterung zu TLS 1.0		x	x			x				x
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0		x			x		x			
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x	x	x
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1	x	x	x	x	x	x	x	x		x
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	x	x		x	x		x			x
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Erweiterung zu TLS 1.0	x	x	x			x				x
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0		x			x		x			
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	Erweiterung zu TLS 1.0					x		x			
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1				x	x		x	x	x	x
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Erweiterung zu TLS 1.0 und TLS 1.1		x		x	x		x	x	x	x
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0		x		x	x		x			
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS 1.0			x		x	x	x			