Ein
Unternehmen
der Bundesdruckerei

LEITFADEN ZUR ZEITGEMÄßEN ANWENDUNG VON TLS-ZERTIFIKATEN

Version 1.0

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin
Tel.: +49 (0) 30 2593 91 – 0
Fax: +49 (0) 30 2593 91 – 22
www.d-trust.net
HRB 74346
USt-ID: DE202620438
WEEE-Reg.-Nr. DE 99554320

BUNDESDRUCKEREI

INHALTSVERZEICHNIS

1 Präambel

TLS[1]-Zertifikate sind ein wichtiger Bestandteil eines zeitgemäßen Internetauftritts bzw. einer Server-Client-Kommunikationsabsicherung, um Vertrauen bei Ihren Kommunikationspartnern, wie z.B. bei Kunden und Websitebesuchern, zu schaffen. Darüber hinaus dient die durch diese Zertifikate etablierte verschlüsselte Verbindung bei der Übermittlung von personenbezogenen Daten der Erfüllung von Anforderungen gemäß der EU-Verordnung DSGVO.

Obwohl die zugrundeliegende Technologie bereits weit über 15 Jahre bekannt ist und verbreitet angewendet wird, gibt es bis zum heutigen Tag Fragen und Verbesserungsbedarf in der sicheren Anwendung.

Ziel dieses Leitfadens ist es, Ihnen als Nutzer von TLS-Zertifikaten kompakt sowie übersichtlich die unterschiedlichen Varianten von TLS-Zertifikaten vorzustellen und wichtige Hinweise zur Nutzung bzw. Verwaltung von TLS-Zertifikaten zu geben. Diese sollen Sie dabei unterstützen, für Ihre Anwendungsfälle die richtigen TLS-Zertifikate auszuwählen, diese sicher anzuwenden und angemessene Vorkehrungen in der Verwaltung dieser zu treffen.

Die Hinweise entsprechen dem derzeitigen Stand der Technik und werden anlassbezogen angepasst.

2 TLS-Zertifikate im Allgemeinen

TLS-Zertifikate erfüllen grundsätzlich zwei Funktionen. Hierbei handelt es sich

- um die sichere Verschlüsselung der Kommunikation zwischen zwei Systemen, wie z.B. dem Webserver und dem Client (Browser),
- und um einen Identitätsnachweis. Der Identitätsnachweis kann zwischen sehr rudimentär und sehr detailliert schwanken.

Zur Realisierung der Verschlüsselungsfunktion kommt auf Seiten des Webservers ein Schlüsselpaar zum Einsatz, welches aus einem privaten und einem öffentlichen Schlüssel besteht. Der private Schlüssel ist elementarer Bestandteil des Aufbaus der verschlüsselten Kommunikationsverbindung. Aus diesem Grund ist dieser immer und unter allen Umständen geheim zu halten und darf auf keinen Fall gegenüber Dritten distribuiert werden.

Der zum Schlüsselpaar zugehörige öffentliche Schlüssel ist Bestandteil des TLS-Zertifikats. Damit ist für jedermann ersichtlich, wem dieser öffentliche Schlüssel zugeordnet ist. Er ist öffentlich, damit über ihn der eigentliche Verschlüsselungsprozess initial eingeleitet werden kann.

Inhalte des TLS-Zertifikats müssen vor unbemerkten Änderungen geschützt werden. Aus diesem Grund ist das Zertifikat signiert. Dies nimmt eine unabhängige Stelle vor, auch der vertrauenswürdige Dritte oder Vertrauensdiensteanbieter genannt. Vor der Erstellung und

[1] Umgangssprachlich wird häufig von SSL-Zertifikaten gesprochen, wenn TLS-Zertifikate gemeint sind. In diesem Leitfaden wird ausschließlich der Begriff TLS-Zertifikat verwendet, da SSL-Zertifikate auf eine veraltete Technologie referenzieren.

Signatur des TLS-Zertifikats prüft dieser Vertrauensdiensteanbieter die gewünschten Einträge im Zertifikat auf inhaltliche Richtigkeit. Je nach Umfang der aufgeführten Daten kann dieser Prozess innerhalb von Sekunden oder aber bis zu Wochen abgeschlossen werden.

Da für die Vertrauenswürdigkeit der Zertifikate die Qualität der Tätigkeit des Vertrauensdiensteanbieters entscheidend ist, muss dieser einen umfangreichen und wiederkehrenden Überprüfungs- und Überwachungsprozesss zur Einhaltung spezifischer Standards, wie z.B. den Vorgaben der Baseline Requirements[2], der Extended Validation Guidelines[3] bzw. spezifischer ETSI-Standards, bestehen. Nur dann wird der Vertrauensdiensteanbieter von Browsern, Anwendungen und Betriebssystemen als vertrauenswürdig eingestuft und seine Rootzertifikate werden in die Rootstores dieser Systeme aufgenommen. Diese Zertifikate werden als publicly trusted (öffentlich vertrauenswürdig) bezeichnet.

Vertrauensdiensteanbieter, die den Vorgaben der EU-Verordnung eIDAS[4] folgen und ihren Dienst als einen qualifizierten Vertrauensdienst bestätigt bekommen haben, können darüber hinaus auch in die Vertrauensliste der Europäischen Union[5] aufgenommen werden. Die Europäische Union hat mit der eIDAS einen eigenen Vertrauensraum definiert, welcher der Entwicklung und Förderung des digitalen europäischen Binnenmarktes dient.

Erst nach diesem Schritt ist es überhaupt möglich, automatisiert vertrauenswürdige verschlüsselte Kommunikationsprozesse zu etablieren.

Aktuell sind die folgenden TLS-Zertifikatsvarianten im Markt verfügbar:

- TLS-Zertifikate ohne Domain Validierung und ohne den Status publicly trusted (kurz: Non-PTC)
- TLS-Zertifikate auf Basis einer Domain Validierung (Domain Validated – kurz: DV-Zertifikate)
- TLS-Zertifikate auf Basis einer Domain und Organisationsvalidierung (Organization Validated – kurz: OV-Zertifikate)
- TLS-Zertifikate auf Basis einer Domain und erweiterten Organisationsvalidierung (Extended Validated – kurz: EV-Zertifikate)
- Qualifizierte Zertifikate für die Website-Authentifizierung auf Basis einer Domain und erweiterten Organisationsvalidierung (Zertifikat für den digitalen europäischen Binnenmarkt auf Grundlage der EU-Verordnung eIDAS – kurz: QWAC)

2.1 Unterscheidung der TLS-Zertifikate

Es gibt keinen Unterschied bei non-PTC-, DV-, OV-, EV- oder QWAC-Zertifikaten hinsichtlich ihrer Verschlüsselungseigenschaften. Technisch ist diese bei der Verwendung gleicher Verschlüsselungsalgorithmen und Schlüssellängen bei allen Zertifikaten gleich gut.

Der Unterschied zwischen diesen TLS-Zertifikaten liegt in der Anzahl der überprüften und bestätigten Zertifikatsattribute bzw. der rechtlichen Würdigung des Zertifikats. Eine rechtliche Würdigung kommt derzeit ausschließlich dem QWAC-Zertifikat zu. Dieses dient dem

[2] https://cabforum.org/baseline-requirements-documents/
[3] https://cabforum.org/extended-validation/
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[5] https://webgate.ec.europa.eu/tl-browser/#/

Nutzer innerhalb des digitalen europäischen Binnenmarkts, um sicher prüfen zu können, ob hinter einer Website oder einem Server eine echte und rechtmäßige Institution steht.

	Non-PTC-Zertifikat	**DV-Zertifikat**	**OV-Zertifikat**	**EV-Zertifikat**	**QWAC -Zertifikat**
Ethikprüfung	X	X	X	X	X
Domainprüfung		X	X	X	X
Organisations-prüfung			X	X	X
Erweiterte Prüfung				X	X
Ggf. weitere Attribute gemäß EU-Vorschriften					X

Tabelle: Menge und Art der überprüften Attribute der TLS-Zertifikate

Abhängig von der Anzahl der durch den Vertrauensdiensteanbieter zu überprüfenden Attribute kann die Ausstellungsdauer von TLS-Zertifikaten stark variieren. Die nachfolgenden Angaben sind Erfahrungswerte und abhängig von der Vollständigkeit der Antragsunterlagen bzw. der Erreichbarkeit von Ansprechpartnern auf Seiten des Antragsstellers:

DV-Zertifikat: innerhalb von Sekunden bis zu einem Tag

OV-Zertifikat: 1-3 Arbeitstage

EV-Zertifikat: 1-10 Arbeitstage

QWAC-Zertifikat: 1-10 Arbeitstage

2.2 Empfohlener Einsatzbereich der TLS-Zertifikate

Die verschiedenen Varianten der TLS-Zertifikate kommen in unterschiedlichen Anwendungsbereichen zum Einsatz. Die hier aufgeführten Informationen entsprechen unseren Erfahrungswerten und Beobachtungen im Markt. Generell kann man sagen, dass dies davon abhängig ist, welche Informationen dem Kommunikationspartner über den eigentlichen Serverinhaber zur Verfügung gestellt werden sollen oder müssen.

DV-Zertifikate: Einzelpersonen, Personengesellschaften, alle Bereiche, die vom Domainnamen abgesehen, keine weiteren Identitätsinformationen bereitstellen wollen; Entitäten, deren aktueller Stand, z.B. deren Existenz, schwer oder gar nicht nachvollziehbar ist.

OV-Zertifikate: Industrie, Dienstleistungsbereich, öffentliche Verwaltung

EV-Zertifikate: Industrie, Dienstleistungsbereich, Nachrichtenportale (z.B. von Zeitungen), öffentliche Verwaltung, insbesondere bei der Erfassung und Verarbeitung von personenbezogenen Informationen (Online-Käufe, Nutzerportale, …)

QWAC-Zertifikate: Finanzwirtschaft in Europa, öffentliche Verwaltung in Europa

3 Wichtige Hinweise die Nutzung von TLS-Zertifikaten

Über die in unseren Certificate Policy und unseren Certificate Practice Statements[6] aufgeführten Ausführungen hinaus, möchten wir Ihnen folgende Anregungen geben:

3.1 Antragsprozess

Planen Sie mit einem angemessenen zeitlichen Vorlauf die Beantragung Ihres Zertifikats. Es ist immer möglich, dass der Vertrauensdiensteanbieter Sie um weitere Informationen bittet, was wiederum die Ausstellung verzögern kann.

Stellen Sie rechtzeitig die notwendigen Dokumente bereit. Bitte erkundigen Sie sich im Vorfeld des Antragsprozesses, welche Dokumente und in welcher Qualität bzw. Aktualität benötigt werden. Die frühzeitige Bereitstellung der notwendigen Unterlagen verkürzt die Bearbeitungszeit erheblich.

3.2 Ansprechpartner und technisches Team

Halten Sie ein Team verfügbar, welches einen Zertifikats-Austauschprozess begleiten kann. Es kann aus regulatorischen oder technischen Gründen vorkommen, dass ein Zertifikat während seiner Laufzeit ausgetauscht werden muss. Hier ist es extrem hilfreich, wenn Sie für diesen Zweck Personal haben, welches dies innerhalb kürzester Zeit gewährleisten kann. Wir als Vertrauensdiensteanbieter werden Sie in diesem Prozess bestmöglich begleiten.

Stellen Sie sicher, dass kompetente Ansprechpartner unternehmensintern innerhalb einer Frist von weniger als 24 Stunden erreicht werden können, um z.B. innerhalb dieser Frist auf Anfragen bzw. Austauschaktionen reagieren zu können. In der Vergangenheit hat sich gezeigt, dass das Thema Erreichbarkeit eines Ansprechpartners beim TLS-Zertifikatsinhaber kritische Auswirkungen auf den sicheren Betrieb haben konnte. Gerade wenn Dritte auf den Vertrauensdiensteanbieter mit Hinweisen zugehen, dass möglicherweise das TLS-Zertifikat eines Kunden nicht richtig genutzt wird oder inhaltliche Fehler existieren, ist eine schnelle Erreichbarkeit zur Klärung dieser Fragen notwendig.

[6] deutsch: https://www.bundesdruckerei.de/de/2833-repository/, englisch: https://www.bundesdruckerei.de/en/Repository/

Vor diesem Hintergrund möchten wir Sie bitten, die Daten von Ansprechpartnern aktuell zu halten und ggf. Sammel-E-Mail-Adressen einzurichten, um einem größeren Empfängerkreis Informationen zeitnah zur Verfügung stellen zu können.

3.3 Testwebseiten

Diese geben Ihnen wichtige Hinweise, wie letztendlich Ihr Kunde Ihre Webseite in den unterschiedlichen Fällen (gültig, gesperrt, abgelaufen) in den unterschiedlichen Browsern wahrnehmen wird.

Die Testwebseiten der D-TRUST finden Sie aktuell unter dem folgenden Link:

OV-Zertifikate:

Gültig: https://certdemo-ov-valid.ssl.d-trust.net/

Abgelaufen: https://certdemo-ov-expired.ssl.d-trust.net/

Gesperrt: https://certdemo-ov-revoked.ssl.d-trust.net/

EV-Zertifikate

Gültig: https://certdemo-ev-valid.ssl.d-trust.net/

Abgelaufen: https://certdemo-ev-expired.ssl.d-trust.net/

Gesperrt: https://certdemo-ev-revoked.ssl.d-trust.net/

QWAC-Zertifikate

Gültig: https://certdemo-qualified-ev-valid.ssl.d-trust.net/

Abgelaufen: https://certdemo-qualified-ev-expired.ssl.d-trust.net/

Gesperrt: https://certdemo-qualified-ev-revoked.ssl.d-trust.net/

3.4 Speicherung des privaten Schlüssels

Bei kritischen Infrastrukturen empfehlen wir die Lagerung des Schlüsselmaterials auf Hardware Security Modulen (HSMs). In diesen Sicherheitsmodulen ist der private Schlüssel wirksam gegen unbefugte Zugriffe und Duplizieren geschützt.

3.5 Öffentlich nachvollziehbare Beschränkung der ausstellungsberechtigten Vertrauensdienste

Sie als Webseitenbetreiber können öffentlich nachvollziehbar die Anzahl der Vertrauensdienste einschränken, die für Ihre Domains Zertifikate ausstellen dürfen.

Dies wird über die DNS-CAA-Einträge realisiert. CAA ist Bestandteil des DNS. Jeder Vertrauensdiensteanbieter ist verpflichtet, den CAA Record vor Zertifikatsausstellung zu prüfen. Ist ihm eine Ausstellung nicht erlaubt, wird er auch kein TLS-Zertifikat ausstellen.

D-TRUST prüft sowohl bei Antragsannahme als auch unmittelbar vor Freischaltung des Zertifikats enthaltene Domains auf einen entsprechenden CAA-Eintrag. Geprüfte Domains

können zur Zertifikatserstellung verwendet werden, wenn entweder der CAA-Eintrag leer ist oder D-TRUST als CA vom Domaininhaber eingetragen wurde.

Zulässige Werte sind dtrust.de, d-trust.de, dtrust.net, d-trust.net, D-Trust GmbH, D-TRUST sowie D-Trust.

D-TRUST kann keine TLS-Zertifikate ausstellen, wenn in dem CAA Ressource Record eine andere CA aufgeführt ist.

3.6 Erleichterung der Domainvalidierung

Im Rahmen der Überarbeitung der zulässigen Domainvalidierungsvarianten wurden u.a. zwei neue Varianten geschaffen, die es Ihnen erlauben, E-Mail-Adressen im DNS zu hinterlegen, über die Sie die CA kontaktieren darf. Dies stellt eine wichtige Erleichterung dar, die wir Ihnen zu Nutzung empfehlen.

Nutzen Sie die Methoden „DNS TXT Record Email Contact" oder „CAA contactemail Property", um autorisierte E-Mails zu hinterlegen.

Die folgenden Einträge sollten Sie vornehmen, wenn Sie Vertrauensdiensteanbietern ermöglichen wollen, Sie über von Ihnen bestimmte E-Mail-Adressen zum Zweck der Domainvalidierung zu kontaktieren:

DNS TXT Record Email Contact Methode:

Der DNS TXT-Eintrag muss auf der Unterdomäne "_validation-contactemail" der zu validierenden Domäne platziert werden. Der gesamte RDATA-Wert dieses TXT-Records muss eine gültige E-Mail-Adresse gemäß der Definition in RFC 6532 Abschnitt 3.2 sein, ohne zusätzliche Auffüllung oder Struktur, oder er kann nicht verwendet werden.

CAA contactemail Property Methode:

Beispiel: CAA 0 contactemail domainowner@example.com[7]

Darüber hinaus empfehlen wir Ihnen, mit DNS-Providern zusammenzuarbeiten, die DNSSec unterstützen.

3.7 Zertifikats-Pinning

In der Vergangenheit haben wir mehrfach beobachtet, dass Zertifikats-Pinning zu Verzögerungen in der Inbetriebnahme von Neuausstellungen als auch bei Austauschzertifikaten geführt hat. Das ging so weit, dass wir als Vertrauensdiensteanbieter gebeten wurden, die Sperrung eines Zertifikats erst vorzunehmen, nachdem das neue Zertifikat in der Infrastruktur erfolgreich ausgerollt wurde.

Sollten Sie auf ein Endzertifikat pinnen, müssen Sie unbedingt die Übergangsphase beachten, die Sie zur Integration eines neuen Zertifikats in Ihrer Infrastruktur benötigen. Eine berechtigte Austauschaktion kann dazu führen, dass wir innerhalb einer Frist von 24 bis

[7] Bei der aufgeführten E-Mail-Adresse handelt es sich um ein Beispiel.

120 Stunden Ihr ursprünglich gepinntes Zertifikat sperren müssen. Das kann für Sie bedeuten, dass dann Ihre Services nicht mehr vertrauenswürdig überprüfbar erreichbar sind.

Für den Fall, dass Sie auf ein Zertifikats-Pinning aufgrund von Sicherheitsmaßnahmen zurückgreifen wollen oder müssen, können die folgenden Maßnahmen, die Auswirkungen einer Sperrung reduzieren:

1. Pinnen Sie auf mehr als auf ein Zertifikat. Idealerweise ist mindestens ein Zertifikat von einem Drittanbieter[8]. oder
2. Pinnen Sie nicht auf ein Endentity-Zertifikat, sondern auf das SubCA-Zertifikat (Intermediate-Zertifikat).

3.8 HSTS-Einsatz erzwingen

Wir empfehlen Ihnen, Ihren Webserver so zu konfigurieren, dass die Nutzung von http Strict Transport Security (HSTS) erzwungen wird. Dies kann vor der Aushebelung der Verbindungsverschlüsselung durch Downgrade-Attacken als auch vor Session Hijacking schützen.

3.9 Infrastrukturen mit Anforderungen an höchstmöglicher Verfügbarkeit

Es hat sich, insbesondere im Bereich von kritischen Infrastrukturen, als förderlich erwiesen, dass Zertifikatskunden für besonders wichtige Bereiche TLS-Zertifikate von mehr als einem Anbieter vorhalten. Dies ermöglicht einen schnellen Wechsel auf das second-source-Zertifikat und so eine unterbrechungsfreie Fortsetzung des IT-Betriebs.

Bitte beachten Sie aber, dass in diesem Fall dies beim Zertifikats-Pinning berücksichtigt werden muss und hierzu auch CAA-Einträge (z.B. Erlaubnis zur Zertifikatsausstellung) zu erweitern sind.

[8] Allgemein wird hier von second source gesprochen.

4 Über uns

Die D-Trust GmbH mit Sitz in Berlin ist ein Unternehmen der Bundesdruckerei-Gruppe. D-TRUST gilt als einer der Vorreiter im Umfeld sicherer digitaler Identitäten. Das Unternehmen ist bereits seit 2016 als qualifizierter Vertrauensdiensteanbieter gemäß der europäischen eIDAS-Verordnung bei der Bundesnetzagentur gelistet. D-TRUST stellt u.a. qualifizierte digitale Zertifikate für elektronische Signaturen, Siegel und die qualifizierte Fernsignatur aus, zudem bietet D-TRUST weitere PKI-Produkte und Dienstleistungen an.

Geschäftspartner, Kunden und Mitarbeiter erwarten, dass Zahlungsdaten, persönliche Informationen, Passwörter oder andere sensible Daten sicher übertragen werden. Die D-Trust GmbH erstellt als Vertrauensdienste-Anbieter für verschiedene Anforderungen und Verwendungszwecke das passende Zertifikat.

Bei der Bereitstellung der D-TRUST Vertrauensdienste werden nicht nur die höchsten Sicherheitsanforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Bundesnetzagentur (BNetzA) auf Basis der eIDAS Verordnung nachweislich umgesetzt, sondern auch die Anforderungen hinsichtlich Interoperabilität und Nutzbarkeit konsequent berücksichtigt.

Aufgrund der globalen Vernetzung müssen zudem die Anforderungen der internationalen Gremien wie ETSI, CEN, ISO, IETF und CA/B-Forum kontinuierlich nachverfolgt und umgesetzt werden. Diese haben ebenfalls maßgeblichen Einfluss auf die Gestaltung der Richtlinien für IT-Infrastrukturen und -Prozesse von Vertrauensdienste-Anbietern und bilden die Basis für ein Höchstmaß an Vertrauen bei gleichzeitig fortschreitender Digitalisierung von Geschäftsprozessen.

4.1 TLS-Zertifikatsangebot der D-TRUST

D-TRUST stellt als Vertrauensdiensteanbieter TLS-Zertifikate nach den Anforderungen der eIDAS (ETSI EN 319 411-1 / DVCP, ETSI EN 319 411-1 / OVCP, 319 411-1 / EVCP bzw. 319 411-2 / QCP-w) und mittels Verteilung des verwendeten Stammzertifikats bei den entsprechenden Herstellern (z.B. Browser, Betriebssysteme u. A.) sicher. Sämtliche folgend aufgeführten Zertifikate beinhalten eine Organisationsprüfung nach einer der o.g. Policies mit den jeweils vorgeschriebenen Angaben im Zertifikat. Internet-Domains, die in Servernamen enthalten sind, werden zusätzlich mit Domain-Validierungsverfahren überprüft (Domain Validation - DV).

Die aufgeführten Produkteigenschaften können sich in Abhängigkeit von regulativen Änderungen sehr kurzfristig ändern oder ersatzlos entfallen.

4.1.1 Advanced DV SSL ID

D-TRUST bietet eine Verschlüsselung auf Basis aktueller Hash-Algorithmen an, um Daten in der Server2Server- oder Server2Client-Komunikation gegen das Ausspähen (Phishing) sensibler Geschäfts- und Kundendaten zu schützen. Durch die bei TLS-Zertifikaten grundsätzlich zum Einsatz kommende „Domain-Validierung" (DV) wird der Domain-Besitz sichergestellt. Bei den Advanced DV SSL ID Zertifikaten ist als Option eine Wildcard (*.domain.com) zubuchbar. Dieses Produkt ist voraussichtlich ab Q3/2020 verfügbar.

4.1.2 Advanced SSL ID

Zusätzlich zur Domain-Validierung (DV) führt D-TRUST bei diesen TLS-Zertifikaten eine „Organisations-Validierung" (OV) durch um die Identität gegenüber Kunden sicherzustellen. Bei den Advanced SSL ID Zertifikaten ist als Option eine Wildcard (*.domain.com) zubuchbar.

4.1.3 Advanced EV SSL ID

Mit der Ausprägung „Extended Validation" (EV) bietet D-TRUST die höchste Stufe an TLS-Sicherheit an, die jedem Kunden aufzeigt, dass er sich auf einer gesicherten Webseite befindet, bei der die Identität des Betreibers einwandfrei bewiesen ist. Ebenso wird der Name des Zertifikatsinhabers sowie der ausstellenden Zertifizierungsstelle direkt in der Adressleiste des Browsers angezeigt. Zur Authentifizierung dient im Unterschied zur Organisations-Validierung (OV) ein speziell um den „Extended Validation" -Standard (EV) erweitertes Prüfverfahren des CA/B Forums.

4.1.4 Qualified EV SSL ID

D-TRUST bietet die Absicherung von serverbasierten Webanwendungen an, mit denen eine verschlüsselte Kommunikation (auf Basis der Protokolle https/TLS) sichergestellt werden kann. Auch hier wird je nach Anbieter die Adresszeile grün hervorgehoben und zusätzlich der Name des Zertifikatinhabers sowie der ausstellenden Zertifizierungsstelle direkt angezeigt. Zusätzlich weist u. a. ein sogenanntes „QC-Statement" dieses Zertifikat als „Qualified Website Authentication Certificate (QWAC)" aus.

4.1.5 Qualified Website PSD2 ID

D-TRUST stellt ein eIDAS konformes qualifiziertes TLS-Zertifikat zur Authentisierung und Verschlüsselung der Kommunikation im Rahmen von Anwendungen zur Umsetzung der PSD2-Richtlinie zur Verfügung.

4.2 TLS-Zertifikate ohne Zertifizierung

Diese Zertifikate entsprechen im Wesentlichen den in 4.1 aufgeführten Produkten, wobei die Prüfung von Identitäten und Internet-Domains auf einem geringeren Level stattfindet. Diese beschränkt sich auf ethische und exportkontrollrechtliche Prüfungen. Die eingesetzten CAs unterliegen keiner Zertifizierung, so dass die Identifikationsprozesse frei gestaltet werden können. Über die Vertrauenswürdigkeit der verwendeten Root- und Ausstellerzertifikate innerhalb von Drittanbieter-Software (z.B. E-Mail Clients, Betriebssysteme, Browser u. A.) entscheidet bei diesen Zertifikaten der Kunde, so dass mit Hilfe der Zertifikate des Auftragnehmers auch diese Anwendungen abgesichert sind und die Kosten für das Aufsetzen und der Pflege einer eigenen PKI auf ein Minimum reduziert wird.

Die aufgeführten Produkteigenschaften können sich in Abhängigkeit von Änderungen nach dem Stand der Technik ändern oder ersatzlos entfallen.

4.2.1 Basic Domain SSL ID

D-TRUST bietet die Basic Domain SSL ID an zur Absicherung von serverbasierten Webanwendungen, mit denen eine verschlüsselte Kommunikation auf Basis der Protokolle

https/TLS sichergestellt werden kann. Das Zertifikat beinhaltet Angaben zu Domains. Dieses Produkt ist voraussichtlich ab Q3/2020 verfügbar.

4.2.2 Basic SSL ID

D-TRUST bietet die Basic SSL ID an zur Absicherung von serverbasierten Webanwendungen, mit denen eine verschlüsselte Kommunikation auf Basis der Protokolle https/TLS sichergestellt werden kann. Das Zertifikat beinhaltet neben den Angaben zu Domains auch Organisationseinträge.

5 Glossar

CA: Certificate Authority/ Certification Authority.

Eine CA ist eine vertrauenswürdige Zertifizierungsstelle, die digitale Zertifikate herausgibt. Daher werden CAs in Europa offiziell als Vertrauensdiensteanbieter (VDA) / Trust Service Provider (TSP) und im deutschsprachigen Raum umgangssprachlich oft auch als Trust Center bezeichnet.

CAA: Certificate Authority Authorization.

Vor der Ausstellung eines Zertifikats muss die Zertifizierungsstelle prüfen, ob ein CAA-Record vorliegt. Durch das Hinzufügen eines CAA-Records wird verhindert, dass unbefugt Zertifikate für eine Domain oder Subdomain ausgestellt und ggf. missbraucht werden.

CA/B-Forum: Certification Authority Browser Forum/ CA/Browser Forum.

Das CA/B-Forum veröffentlicht Standards und Regeln für Ausstellung und Verwaltung von TLS-Zertifikaten.

CEN: Comité Européen de Normalisation.

Das Europäische Komitee für Normung fördert die europäische Wirtschaft im globalen Handel, gewährleistet das Wohlbefinden der Bürger und treibt den Umweltschutz voran.

DNS: Domain Name System.

Das DNS beantwortet Anfragen zur Namensauflösung.

DNS-Sec: Domain Name System Security Extensions.

Die DNS-Sec ist eine Erweiterung von Sicherheitsmechanismen des DNS zur Gewährleistung der Authentizität und Integrität von Daten.

DSGVO: Datenschutz-Grundverordnung.

Die Datenschutz-Grundverordnung ist eine EU-Verordnung und vereinheitlicht die Verarbeitung personenbezogener Date, sowohl private wie öffentliche, EU-weit.

eIDAS: electronic IDentification, Authentication and trust Services.

Die eIDAS-Verordnung ist eine EU-Verordnung und soll einheitliche Regelungen für Signaturen und die Bereitstellung von Vertrauensdiensten im digitalen EU-Binnenmarkt schaffen.

Endentity Zertifikat

Endentity Zertifikate werden von der CA an eine bestimmte Entität ausgestellt, die ihrerseits keine weiteren Zertifikate damit ausstellt.

ETSI: European Telecommunications Standards Institute.

ETSI ist eine europäische Standardisierungsinstitution und schafft weltweit anwendbare Standards für die Informations- und Kommunikationstechnologien.

HSM: Hardware Security Modul.

Als eigenständige Hardware-Komponente kann ein HSM Schlüssel für kryptografische Verfahren erzeugen oder verwalten, Signaturen und Identitäten schützen oder die Übertragung von Daten absichern.

HSTS: HTTP Strict Transport Security.

HSTS dient als Sicherheitsmaßnahme für Webserver oder Webhosting-Dienst, das Benutzer und Webbrowser darüber informiert, wie die Verbindung zwischen Response Header, der ganz am Anfang gesendet und später zurück zum Browser gesendet wird, zu handhaben ist.

IETF: Internet Engineering Task Force.

Die IETF ist eine internationale Standardisierungsorganisation und befasst sich mit der technischen Weiterentwicklung der Internetarchitektur, um dessen Funktionsweise zu verbessern.

ISO International Standards Organization.

Die ISO ist eine internationale Standardisierungsorganisation und entwickelt gültige Standardnormen, um den Austausch internationaler Waren und Dienstleistungen zu erleichtern und die gegenseitige Zusammenarbeit im Bereich der wissenschaftlichen, technologischen und wirtschaftlichen Aktivitäten zu fördern.

PKI: Public Key Infrastructure.

Eine PKI ist ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.

RFC: Request for Comments.

Die RFC ist eine Reihe technischer und organisatorischer Dokumente zum Internet, die das Netz beschreiben, behandeln und definieren.

SSL: Secure Sockets Layer.

Siehe TLS.

SubCA-Zertifikat

Sub-Certificate Authority oder Sub-Certification Authority.

Das SubCA-Zertifikat stellt mit Hilfe der Verbindung zu dem Root-Zertifikat der Zertifizierungsstelle die Vertrauenswürdigkeit des TLS-Zertifikats sicher.

TLS: Transport Layer Security.

Umgangssprachlich wird häufig von SSL-Zertifikaten gesprochen, wenn TLS-Zertifikate gemeint sind. In diesem Leitfaden wird ausschließlich der Begriff TLS-Zertifikat verwendet, da SSL-Zertifikate auf eine veraltete Technologie referenzieren.

TXT-Record

Mit einem TXT-Eintrag, bzw. einem TXT Resource Record, kann ein frei definierbarer Text in einer DNS-Zone abgelegt werden.

Zertifikats-Pinning

Beim Zertifikats-Pinning wird ein Zertifikat an einen bestimmten Host und eine bestimmte Zertifizierungsstelle gebunden.