A
Bundesdruckerei
company

GUIDE FOR USING TLS CERTIFICATES TODAY

Version 1.0

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin, Germany
Tel.: +49 (0) 30 2593 91 – 0
Fax: +49 (0) 30 2593 91 – 22
www.d-trust.net
HRB 74346
VAT ID: DE202620438
WEEE Reg. No. DE 99554320

BUNDESDRUCKEREI

CONTENTS

1 Preamble

When it comes to creating trust among your communication partners, i.e. customers and website visitors, TLS[1] certificates are an important component of any Internet website today or of server-client communication security. What's more, the encrypted connection established by these certificates and used to transmit personal data meets the requirements of the EU's General Data Protection Regulation (GDPR).

Even though the underlying technology has been around for more than 15 years and is widely used, there are still questions and the need to improve secure use of this technology.

The aim of this guide is to present to you, as a user of TLS certificates, a compact and concise overview of the different TLS certificate variants and to provide you with important information on how to use and manage TLS certificates. The guide should help you to select the right TLS certificates for your applications, to use them securely and to take suitable precautions for their management.

The information is based on the current state of the art and will be revised as required.

2 TLS certificates - General information

TLS certificates have two main functions. These are:

- secure encryption of communications between two systems, such as the web server and the client (browser),
- and proof of identity. Proof of identity can be anywhere between very rudimentary and very detailed.

A key pair is used at the web server end for encryption. This key pair is made up of a private and a public key. The private key is the elementary component that establishes the encrypted connection for communication. This is why the private key must be kept secret at all time and should not be sent to any third parties.

The public key of the key pair is part of the TLS certificate and clearly shows who this public key is assigned to. This key is public and is used to initiate the actual encryption process.

The contents of the TLS certificate must be protected so that changes do not go unnoticed. This is why the certificate is signed by an independent authority, also referred to as a trusted third party or trust service provider. Before the TLS certificate is created and signed, this trust service provider checks the requested entries in the certificate to ensure they are correct. Depending on the scope of the data listed, this process may take a couple of seconds or even weeks.

Since the quality of the trust service provider is significant for trust in the certificates, comprehensive and repeated verification and monitoring processes must be in place to

[1] People frequently talk about SSL certificates when in fact TLS certificates are meant. This guide uses the term TLS certificate only because SSL certificates reference an obsolete technology.

ensure compliance with specific standards, such as the Baseline Requirements[2], the Extended Validation Guidelines[3] or the specific ETSI standards. Only then will the trust service provider of browsers, applications and operating systems be classified as trusted and its root certificates will be included in the root stores of these systems. These certificates are referred to as publicly trusted.

Trust service providers that comply with the requirements of the EU's eIDAS regulation[4] and have had their service confirmed as a qualified trust service can also be included in the European Union's Trusted List[5]. With eIDAS, the European Union has defined its own trust territory which serves the development and promotion of Europe's digital single market.

This step is essential if automated trusted and encrypted communications are to become established at all.

The following TLS certificate variants are currently available on the market:

- TLS certificates without domain validation and without publicly trusted status (in short: non-PTC)
- TLS certificates based on domain validation (domain validated – in short: DV certificates)
- TLS certificates based on domain and organization validation (organization validated – in short: OV certificates)
- TLS certificates based on domain and extended organization validation (organization validated – in short: EV certificates)
- Qualified certificates for website authentication based on a domain and extended organization validation (certificate for Europe's digital single market based on the EU's eIDAS regulation – in short: QWAC)

2.1 Distinctions between TLS certificates

There is no difference between non-PTC, DV, OV, EV or QWAC certificates in terms of their encryption properties. If the same encryption algorithms and key lengths are used, all of these certificates are equally good in terms of encryption.

The difference when it comes to TLS certificates is in the number of certificate attributes that are checked and confirmed, i.e. in the legal recognition of the certificate. The QWAC certificate is currently the only certificate with full legal recognition. This certificate can be used within Europe's digital single market in order to verify whether the institution behind a website or a server is a genuine and legitimate institution.

[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/#/

	Non-PTC certificate	**DV certificate**	**OV certificate**	**EV certificate**	**QWAC certificate**
Ethics check	X	X	X	X	X
Domain check		X	X	X	X
Organization check			X	X	X
Extended check				X	X
If applicable, other attributes acc. to EU rules					X

Table: Quantity and type of TLS certificate attributes checked

The time needed to issue TLS certificates varies significantly and depends on the number of attributes to be checked by the trust service provider. The information provided below is based on experience and depends on whether the request documents were complete and if the requester’s contact person was available:

DV certificate: from a few seconds to one day

OV certificate: One to three working days

EV certificate: One to ten working days

QWAC certificate: One to 20 working days

2.2 Recommended area of application for TLS certificates

The different TLS certificate variants are used in different areas of application. The information provided here is based on our experience and market observations. Generally speaking, it can be said to depend on which information is or must be made available to the communication partner regarding the actual server owner.

DV certificates: Individuals, partnerships, all areas which, apart from the domain name, do not wish to provide any other identity information; entities whose current status, e.g. existence, is difficult or impossible to ascertain.

OV certificates: Industry, service area, public administration

EV certificates: Industry, service area, news portals (e.g. of newspapers), public administration, especially for capturing and processing personal information (online purchases, user portals, ...)

QWAC certificates: Financial sector in Europe, public administration in Europe

3 Important information when using TLS certificates

In addition to the information provided in our Certificate Policy and Certificate Practice Statements[6], we would also like to make the following suggestions:

3.1 Request process

Leave enough time when requesting your certificate. It can always happen that the trust service provider will request further information, which may delay issuance.

Provide the necessary documents in good time. Before submitting your request, please find out which documents are required, the quality in which they are required and how up to date they must be. If you submit documents early, this will speed up processing considerably.

3.2 Contact person and technical team

Have a team available that can accompany a certificate exchange process. For regulatory or technical reasons, it may be necessary to replace a certificate during its term. It is very helpful in this case if you have personnel at hand who can guarantee this within the shortest time. We, as a trust service provider, will accompany you in this process as best we can.

Make sure that competent contacts within the company can be reached within a period of less than 24 hours, e.g. to respond to inquiries or exchange actions within this period. Experience up to now shows that the availability of a contact person at the TLS certificate holder end can have a critical impact on secure operations. Especially when third parties approach the service provider with information that a customer's TLS certificate is not being used correctly or that there are errors in content, it is important for the contact person to be available so that these issues can be quickly clarified.

Against this background we would like to ask you to keep your contact data up to date and, if necessary, to set up collective e-mail addresses in order to be able to provide information to a larger circle of recipients in a timely manner.

3.3 Test websites

These websites provide important information on how your customer will ultimately see your website in different cases (valid, blocked, expired) in the various browsers.

You can currently find the D-TRUST test websites under the following link:

OV certificates:

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

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

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

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

EV certificates

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

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

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

QWAC certificates

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

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

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

3.4 Storing the private key

When it comes to critical infrastructures, we recommend storing the key material on Hardware Security Modules (HSMs). These security modules effectively protect the private key against unauthorized access and duplication.

3.5 Public restriction of trust services authorized to issue

You as a website operator can publicly limit the number of trust services that are allowed to issue certificates for your domains.

This is implemented via the DNS CAA entries. CAA is part of the DNS. Every trust service provider is obliged to check the CAA record before issuing certificates. If the trust service provider is not allowed to issue it, it will not issue a TLS certificate.

When it receives the application and immediately before activating the certificate, D-TRUST checks the domains named with a view to a corresponding CAA entry. Validated domains can be used for certificate generation if the CAA entry is empty or if D-TRUST has been entered as the CA by the domain holder.

Valid values are dtrust.de, d-trust.de, dtrust.net, d-trust.net, D-Trust GmbH as well as D-Trust.

D-TRUST cannot issue TLS certificates if a different CA is stated in the CAA Resource Record.

3.6 Domain validation made easier

As part of revising permissible domain validation variants, two new variants have been created, among other things, which allow you to store e-mail addresses in the DNS which the CA can use to contact you. This makes things much easier and we recommend that this be used.

Use the ‘DNS TXT Record Email Contact’ or ‘CAA contactemail Property’ methods to store authorized e-mails.

You should make the following entries if you want to enable trust service providers to contact you via e-mail addresses specified by you for the purpose of domain validation:

DNS TXT Record Email Contact Method:

The DNS TXT entry must be placed on the ‘_validation-contactemail’ subdomain of the domain to be validated. The entire RDATA value of this TXT record must be a valid e-mail address as defined in RFC 6532, section 3.2, without additional padding or structure, otherwise it cannot be used.

CAA contactemail Property Method:

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

We also recommend that you work with DNS providers that support DNSSEC.

3.7 Certificate pinning

In the past, we noted on several occasions that certificate pinning led to delays in the commissioning of new issuances and also in the case of exchange certificates. This went so far that we, as a trust service provider, were asked to revoke a certificate only after the new certificate had been successfully rolled out in the infrastructure.

If you are pinning an end certificate, it is essential to consider the transition period required to integrate a new certificate into your infrastructure. A legitimate exchange may result in us having to revoke your originally pinned certificate within 24 to 120 hours. For you, this can mean that your services can no longer be accessed in a trusted, verifiable manner.

In the event that you want or need to resort to certificate pinning due to security measures, the following measures can mitigate the effects of revocation:

1. Pin on more than one certificate. Ideally, at least one certificate is from a third-party provider[8] or
2. Do not pin on an end-entity certificate, but on the SubCA certificate (intermediate certificate).

3.8 Force HSTS use

We recommend that you configure your web server to force the use of http Strict Transport Security (HSTS). This can protect against the connection encryption being overridden by downgrade attacks as well as session hijacking.

[7] The e-mail address listed is an example.
[8] This is generally referred to as second source.

3.9 Infrastructures with requirements for highest possible availability

It has proven to be beneficial, especially in critical infrastructures, for certificate customers to hold TLS certificates from more than one provider for particularly important areas. This enables a quick change to the second-source certificate and thus uninterrupted continuation of IT operations.

Please note, however, that this must also be taken into account for certificate pinning, and CAA entries (e.g. permission to issue certificates) must also be extended for this purpose.

4 About us

Berlin-based D-TRUST GmbH is a company of the Bundesdruckerei Group. D-TRUST is a pioneer in the field of secure digital identities. The company has been listed with the German Federal Network Agency as a qualified trust service provider in accordance with the European eIDAS Regulation since 2016. D-TRUST issues, among other things, qualified digital certificates for electronic signatures, seals and the qualified remote signature. D-TRUST also offers other PKI products and services.

Business partners, customers and employees expect payment data, personal information, passwords or other sensitive data to be transmitted in a secure manner. As a trust service provider, D-TRUST GmbH issues certificates to meet different requirements and purposes.

In addition to meeting with the highest security requirements of the Federal Office for Information Security (BSI) and the Federal Network Agency (BnetzA) based on the eIDAS Regulation, D-TRUST's services especially consider the requirements of interoperability and usability.

In response to global networking, the requirements of international committees, such as ETSI, CEN, ISO, IETF and the CA/B-Forum, must also be continuously taken into account and implemented. These requirements also have a considerable role to play in shaping the guidelines for the IT infrastructures and processes of trust service providers while forming the basis for a high level of trust as the digitalization of business processes moves forward.

4.1 TLS certificate offer by D-TRUST

As a trust service provider, D-TRUST issues TLS certificates in compliance with the requirements of eIDAS (ETSI EN 319 411-1/DVCP, ETSI EN 319 411-1/OVCP, 319 411-1/EVCP and 319 411-2/QCP-w) and distributes the root certificate used among the respective manufacturers (e.g. browsers, OSs, etc.). All of the certificates listed below contain organization validation according to one of the above policies along with the required details in the certificate. Internet domains that are contained in server names are additionally validated using domain validation methods (Domain Validation – DV).

Depending on regulatory changes, the listed product properties may change at very short notice or be omitted without substitution.

4.1.1 Advanced DV SSL ID

D-TRUST offers encryption based on current hash algorithms to protect data in Server2Server or Server2Client communication against fraudulent acquisition (phishing) of sensitive business and customer data. Domain ownership is ensured by the 'domain validation' (DV) that is generally used with TLS certificates. A wildcard (*.domain.com) can be optionally added to Advanced DV SSL ID certificates. This product is expected to be available beginning Q3/2020.

4.1.2 Advanced SSL ID

In addition to domain validation (DV), D-TRUST also carries out 'Organization Validation' (OV) for these TLS certificates in order to confirm the identity for customers. A wildcard (*.domain.com) can be optionally added to Advanced SSL ID certificates.

4.1.3 Advanced EV SSL ID

With ‘Extended Validation’ (EV), D-TRUST offers the highest level of TLS security, which shows every customer that he or she is on a secure website where the identity of the operator has been clearly proven. The name of the certificate holder and of the issuing certification authority are also displayed directly in the browser's address bar. Unlike Organization Validation (OV), a special validation method of the CA/B Forum with Extended Validation is used for authentication.

4.1.4 Advanced EV SSL ID

D-TRUST offers security for server-based web applications that can be used to secure encrypted communication (based on https/TLS protocols). Depending on the provider, the address line is also highlighted in green and the name of the certificate holder and of the issuing certification authority are also displayed directly. Furthermore, a so-called QC Statement also identifies this certificate as a Qualified Website Authentication Certificate (QWAC).

4.1.5 Qualified Website PSD2 ID

D-TRUST provides an eIDAS-compliant qualified TLS certificate for authentication and encryption of communication as part of applications to implement the PSD2 directive.

4.2 TLS certificates without certification

These certificates are essentially the same as the products listed in 4.1, although identities and Internet domains are verified at a lower level. This verification is limited to ethical and export control checks. The CAs used are not subject to certification, so that the identification processes can be freely designed. With these certificates, the customer decides on the trustworthiness of the root and issuer certificates used within third-party software (e.g. e-mail clients, operating systems, browsers, etc.), so that these applications are also secured with the help of the customer's certificates, thus reducing the cost of setting up and maintaining a PKI to a minimum.

Depending on changes based on the state of the art, the listed product properties may change or be omitted without substitution.

4.2.1 Basic Domain SSL ID

D-TRUST offers Basic Domain SSL ID to secure server-based web applications that can be used to secure encrypted communication based on https/TLS protocols. The certificate contains information about domains. This product is expected to be available beginning Q3/2020.

4.2.2 Basic SSL ID

D-TRUST offers Basic SSL ID to secure server-based web applications that can be used to secure encrypted communication based on https/TLS protocols. In addition to the information on domains, the certificate also contains organizational entries.

5 Glossary

CA: Certificate Authority/ Certification Authority

A CA is a trusted certificate authority that issues digital certificates. For this reason, CAs in Europe are officially referred to as Trust Service Providers (TSPs).

CAA: Certificate Authority Authorization

Before issuing a certificate, the certification authority must check whether a CAA record exists. Adding a CAA record prevents unauthorized issuance of certificates for a domain or subdomain and any possible misuse.

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

The CA/B Forum publishes standards and rules for issuing and managing TLS certificates.

CEN: Comité Européen de Normalisation

The European Committee for Standardization promotes the European economy in global trade, ensures the well-being of citizens and promotes environmental protection.

DNS: Domain Name System

The DNS answers queries regarding name resolution.

DNSSEC: Domain Name System Security Extensions

DNSSEC is an extension of the DNS security mechanisms to guarantee the authenticity and integrity of data.

GDPR: General Data Protection Regulation

The General Data Protection Regulation is an EU regulation that standardizes the processing of personal data, both private and public, throughout the EU.

eIDAS: electronic IDentification, Authentication and trust Services

The eIDAS regulation is an EU regulation and is designed to create uniform regulations for signatures and the provision of trust services in the EU’s digital single market.

End-entity certificate

End-entity certificates are issued by the CA to a specific entity, which in turn does not issue any further certificates using these end-entity certificates.

ETSI: European Telecommunications Standards Institute

ETSI is a European standardization institution that develops globally applicable standards for information and communication technologies.

HSM: Hardware Security Module

As an independent hardware component, an HSM can generate or manage keys for cryptographic procedures, protect signatures and identities or secure the transmission of data.

HSTS: HTTP Strict Transport Security

HSTS serves as a security measure for web servers or web hosting services that informs users and web browsers how to handle the connection between response headers sent at the very beginning and later sent back to the browser.

IETF: Internet Engineering Task Force

The IETF is an international standardization organization which focuses on the technical development of the Internet architecture in order to improve its functionality.

ISO International Standards Organization

ISO is an international standardization organization that develops valid standard norms to facilitate the exchange of international goods and services and to promote mutual cooperation in scientific, technological and economic activities.

PKI: Public Key Infrastructure

A PKI is a system that can issue, distribute and validate digital certificates. The certificates issued are used to secure computer-supported communication.

RFC: Request for Comments

The RFC is a series of technical and organizational documents about the Internet that describe, treat and define the network.

SSL: Secure Sockets Layer

See TLS.

SubCA certificate

Sub-Certificate Authority or Sub-Certification Authority.

The SubCA certificate ensures the trustworthiness of the TLS certificate by connecting to the root certificate of the certification authority.

TLS: Transport Layer Security

People frequently talk about SSL certificates when in fact TLS certificates are meant. This guide uses the term TLS certificate only because SSL certificates reference an obsolete technology.

TXT Record

With a TXT entry, or a TXT Resource Record, a freely definable text can be stored in a DNS zone.

Certificate pinning

Certificate pinning is the process of binding a certificate to a specific host and certification authority.