SUBSCRIBER AGREEMENT
ENGLISH

VERPFLICHTUNGSERKLÄRUNG
DEUTSCH

SUBSCRIBER AGREEMENT

Please note the following when using these certificates:

1. I hereby confirm that

In the event that you have requested an TLS certificate, the following is applicable:

- all declarations by and information concerning the subscriber (represented by me) provided to D-Trust GmbH regarding the respective TLS certificate are always true and that any changes made known to me will be automatically made available to D-TRUST,
- I alone (as well as the service provider commissioned by the subscriber with certificate application, installation and management, currently represented by me) am responsible for protecting the private key and, if applicable, the revocation password against misuse, loss, disclosure, manipulation or unauthorized use,
- the TLS certificate will be installed exclusively on servers of precisely the organization that has been confirmed in the certificate with its name (CN and O)
- the key pair was generated using one of the following algorithms (rsa, dsa, ecdsa-Fp or ecgdsa-Fp).

In the event that you have ordered a certificate (except TLS certificates) for yourself or on behalf of your organization, the following is applicable:

- all information in the certificate is true in as far as I have knowledge of such information and, in the event that any changes come to my knowledge (e. g. name, organizational affiliation), that I will automatically make such changes known to the technical contact person of my organization or to D-TRUST
- the key pair (if I myself generated it) was generated using an algorithm in accordance with ETSI TS 119 312 (best practice) or, in the case of government projects, in accordance with the cryptographic specifications of BSI TR-03116-4 or TR-02102-1.

In both cases, the following is also applicable:

- the certificate received will not be used until the correctness of the data contained in such certificate has been successfully verified,
- the certificate or private key, respectively, will be created and used exclusively for the approved purposes and in line with the Certification Practice Statement (CPS),
- the use of private keys will be immediately discontinued as soon as
  i. I become aware that the issuing CA has been compromised,
  ii. the certificate in question is revoked or
  iii. the certificate has reached the end of its validity period.

2. Furthermore, I hereby warrant that I will no longer use the certificate and the pertinent private key and will cause their revocation using one of the methods referred to below as soon as one of the following events occurs:

a) Suspicion or certainty that the private key has been compromised

b) Loss of exclusive control over the private key (e.g. a non-authorized party has stolen your PIN)

c) Any changes in certificate data (e.g. name, addresses or affiliation with the organization).

If you wish to revoke your certificate, you can use the following revocation methods depending on how you requested your certificate:

- If you know your card ID or request ID and your revocation password, please use D-TRUST's revocation website to revoke your certificate:
  a. Revocation website of D-Trust GmbH: https://my.d-trust.net/sperren
  b. If you require telephone support to revoke your certificates, please contact our call and support center:

     workdays from 7am to 6pm by calling +49 (0)30-2598-0.

     Note: Your certificate can only be revoked if you can provide our service staff with the request ID and the corresponding revocation password.

- If you purchased your certificates via the CSM (Certificate Service Manager), please use the following revocation methods:
  a. If you are an operator, revoke your certificate using the online revocation function of the Certificate Service Manager (CSM)
  b. or contact your CSM operator.

- If you have a health professional card and you wish to revoke your qualified certificates in the health sector telematics infrastructure (TSP-X.509QES), please use the following revocation methods:
  a. If you are an authorized subscriber, you can revoke your health professional card (Sperrantragsteller_AS) via the request portal: https://ehealth.d-trust.net/antragsportal.
  b. Parties authorized to revoke certificates, such as the card issuer's representatives (Sperrantragsteller_KHG), can revoke certificates via the activation portal https://ehealth.d-trust.net/freigabeportal or the SOAP interface (technical interface).

3. I hereby acknowledge and agree that

- as part of checking application data, the HR department or my superiors, respectively, or customers may be contacted in order to check the application and the application data with a view to my affiliation with the organization and/or authorization as the person responsible for the key,
- D-TRUST will store all the information from the certificate application and the subsequent authentication, verification and, if applicable, revocation operations and that D-TRUST will forward such information to the successor organization should the original organization discontinue its operations,
- D-TRUST generally publishes non-qualified certificates for certificate status requests, and
- the browser and operating system manufacturers, as a result of integrating root certificates of D-TRUST and the resultant error-message-free use of certificates by subjects, are beneficiary third parties.

More information regarding the certificates applied for can be found at: http://www.d-trust.net/repository. There you will also find, among other things, the Certificate Policy (CP), the D-TRUST Trust Service Practice Statement (TSPS), the Certification Practice Statement (CPS), the PKI disclosure statement for qualified certificates (PDS) as well as further details regarding qualified products such as TLS certificates (QWACs) or seal and signature certificates.

VERPFLICHTUNGSERKLÄRUNG

Bei Verwendung der Zertifikate haben Sie die folgenden Punkte zu beachten:

1. Ich versichere hiermit, dass

Im Falle, dass Sie ein TLS-Zertifikat beantragt haben gilt:

- alle Erklärungen und Informationen des Zertifikatsnehmers, vertreten durch meine Person, gegenüber D-TRUST in Bezug auf das betreffende TLS-Zertifikat stets der Wahrheit entsprechen und im Fall von mir bekannten Änderungen unaufgefordert D-TRUST zur Verfügung gestellt werden.
- ausschließlich ich (auch als der vom Zertifikatsnehmer mit Zertifikatsbeantragung, -installation und/oder -verwaltung beauftragte, derzeit durch mich vertretene Dienstleister) für den Schutz des privaten Schlüssels sowie ggf. des Sperrpassworts vor Missbrauch, Verlust, Preisgabe, Änderung oder unbefugter Benutzung verantwortlich bin.
- das TLS-Zertifikat ausschließlich auf Servern exakt der Organisation installiert wird, die im Zertifikat mit ihrem Namen (CN und O) bestätigt worden sind.
- das Schlüsselpaar mit einem der folgenden Algorithmen generiert wurde (rsa, dsa, ecdsa-Fp oder ecgdsa-Fp).

Im Falle, dass Sie für Ihre eigene Person oder im Auftrag Ihrer Organisation ein Zertifikat bestellt haben (ausgenommen TLS-Zertifikaten) gilt:

- alle Informationen im Zertifikat stets der Wahrheit entsprechen, soweit ich von diesen Informationen Kenntnis oder Wissen habe und im Fall von mir bekannten Änderungen (wie z.B. Name, Organisationszugehörigkeit) ich diese unaufgefordert meinem technischen Ansprechpartner meiner Organisation oder der D-TRUST zur Verfügung stelle.
- das Schlüsselpaar, falls ich es selbst erstellt habe, mit einem Algorithmus nach der ETSI TS 119 312 (Best Practice) bzw. bei Projekten der Bundesregierung nach den kryptographischen Vorgaben aus BSI TR-03116-4 oder TR-02102-1 generiert wurde.

Weiterhin gilt in beiden Fällen:

- das erhaltene Zertifikat erst nach erfolgreich abgeschlossener Überprüfung der enthaltenen Daten auf deren Richtigkeit hin, eingesetzt wird,
- das Zertifikat bzw. der private Schlüssel ausschließlich für zugelassene Zwecke im Einklang mit dem Certification Practice Statement (CPS), erstellt und verwendet wird,
- die Nutzung privater Schlüssel umgehend eingestellt wird, sobald
  - i. ich Kenntnis über die Kompromittierung der ausstellenden CA erlange,
  - ii. das betreffende Zertifikat widerrufen wurde oder
  - iii. das Gültigkeits-Enddatum des Zertifikats erreicht ist.

2. Des Weiteren versichere ich, das Zertifikat und den dazugehörigen privaten Schlüssel bei Eintritt eines der folgenden Ereignisse nicht mehr einzusetzen und mittels eines der unten genannten Verfahren zu widerrufen:

a) Verdacht oder Gewissheit der Kompromittierung des privaten Schlüssels

b) Verlust der alleinigen Kontrolle über den privaten Schlüssel (z.B. ein Unbefugter hat Ihre PIN ausgespäht)

c) Änderungen an Zertifikatsdaten jeglicher Art (z.B. Namen, Adressen oder Organisationszugehörigkeiten)

Wenn Sie Ihr Zertifikat widerrufen möchten, stehen Ihnen abhängig von Ihrem Antragsweg folgende Sperrwege zur Verfügung:

- Wenn Sie Ihre Karten-ID bzw. Antrags-ID und Ihr Sperrpasswort kennen, nutzen Sie bitte zum Widerrufen Ihrer Zertifikate die Sperr-Webseite der D-Trust GmbH:
  a. die Sperr-Webseite der D-Trust GmbH: https://my.d-trust.net/sperren
  b. Wenn Sie telefonische Unterstützung beim Widerruf Ihrer Zertifikate benötigen, kontaktieren Sie bitte unser Call- und Supportcenter:

     werktags von 07:00 Uhr bis 18:00 Uhr unter der +49 (0)30-2598-0

     Hinweis: Der Widerruf Ihres Zertifikats kann nur erfolgen, wenn Sie die Antrags-ID und das zugehörige Sperrpasswort an unseren Servicemitarbeiter übergeben.

- Wenn Sie Ihre Zertifikate über den CSM (Certificate Service Manager) erworben haben, nutzen Sie bitte folgende Sperrwege:
  a. Wenn Sie Operator sind, widerrufen Sie bitte direkt über die Online-Sperrfunktion des Certificate Service Managers (CSM)
  b. oder kontaktieren Sie Ihren CSM Operator.

- Wenn Sie einen Heilberufsausweis haben und Ihre qualifizierten Zertifikate aus der Telematikinfrastruktur des Gesundheitswesens des HBA (TSP-X.509QES) widerrufen möchten, nutzen Sie bitte folgende Sperrwege:
  a. Wenn Sie berechtigter Zertifikatnehmer sind, können Sie Ihren Heilberufsausweis (Sperrantragsteller_AS) über das Antragsportal https://ehealth.d-trust.net/antragsportal widerrufen.
  b. Zum Widerruf von Zertifikaten berechtigte Stellen, z.B. Vertreter des Kartenherausgebers (Sperrantragsteller_KHG) können über das Freigabeportal https://ehealth.d-trust.net/freigabeportal oder die SOAP-Schnittstelle (technische Schnittstelle) widerrufen.

3. Ich nehme zur Kenntnis und erkläre mich damit einverstanden, dass

- im Zuge der Prüfung der Antragsdaten ggf. die Personalabteilung bzw. Vorgesetzte oder Auftraggeber kontaktiert werden, um sowohl den Auftrag als auch die Antragsdaten bezüglich meiner Organisationszugehörigkeit und / oder Autorisierung als Schlüsselverantwortlichen zu überprüfen,
- D-TRUST sämtliche Informationen aus der Zertifikatsbeantragung sowie der darauffolgenden Authentifizierung, Verifikation und ggf. Widerruf speichert und im Falle einer Betriebseinstellung an die Nachfolgeorganisation übergibt,
- D-TRUST nicht-qualifizierte Zertifikate standardmäßig zur Zertifikatsstatusabfrage veröffentlicht und
- die Browser- und Betriebssystemhersteller durch die Integration von Root-Zertifikaten der D-TRUST und der daraus resultierenden fehlermeldungsfreien Nutzung von Zertifikaten durch die Endanwender profitierende Dritte sind.

Weitere Informationen zu den beantragten Zertifikaten erhalten Sie unter http://www.d-trust.net/repository. Hier finden Sie u.a. auch die Certificate Policy (CP), das D-TRUST Trust Service Practice Statement (TSPS), das Certification Practice Statement (CPS), die PKI-Nutzerinformationen für qualifizierte Zertifikate (PDS) sowie weiterführende Informationen zu qualifizierten Produkten wie TLS-Zertifikate (QWAC), Siegel- und Signaturzertifikate.