SUBSCRIBER AGREEMENT

ENGLISH

VERPFLICHTUNGSERKLÄRUNG

DEUTSCH

SUBSCRIBER AGREEMENT

Please note the following when using these certificates:

▪ **Signature cards** ▪ **Seal cards** ▪ **Seal certificates without a card** ▪ **E-mail certificates (S/MIME)**	▪ **TLS certificates (website certificates)**
I hereby confirm that - I have ordered a certificate for myself or on behalf of my organization. - I use my personal account in the D-TRUST Portal (https://portal.d-trust.net/) for me alone or, as an authorized representative, for a legal entity (organization). - I will initiate the complaint process if I do not receive my signature or seal card within two weeks after receiving notice of dispatch. The card must be revoked in this case. - 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. - I will not use the certificate received until the correctness of the data contained in such certificate has been successfully verified. - I will create and use the certificate or private key, respectively, exclusively for the approved purposes and in line with the Certification Practice Statement (CPS). - I will respond promptly to the TSP's instructions regarding the rights and obligations listed here. **Applies additionally to seal certificates without a card and e-mail certificates (S/MIME):** - I hereby confirm that I generated the key pair (if I myself generated it) 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.	**I hereby confirm that** - all declarations by and information concerning the subscriber (represented by me) provided to D-Trust 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. - I will install the TLS certificate exclusively on servers of precisely the organization that has been confirmed in the certificate with its name (CN and O). - I generated the key pair using one of the following algorithms (rsa, dsa, ecdsa-Fp or ecgdsa-Fp). - I will not use the certificate received until the correctness of the data contained in such certificate has been successfully verified. - I will only create and use the certificate or private key exclusively for the approved purposes and in line with the Certification Practice Statement (CPS). - I will respond promptly to the TSP's instructions regarding the rights and obligations listed here.

Publication of certificates in the LDAP directory

I hereby acknowledge and agree to the following certificate products being published in the LDAP directory:

- E-mail certificates (S/MIME) with the exception of certificates from the D-Trust V-PKI
- TLS certificates (website certificates)
- Seal certificates

Certificate revocation

I hereby warrant that I will no longer use the certificate and the pertinent private key and will have them revoked using one of the methods referred to below as soon as one of the following events occurs:

- Suspicion or certainty that the private key has been compromised
- Loss of exclusive control over the private key (e.g. a non-authorized party has stolen your PIN)
- 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 the revocation website of D-Trust GmbH to revoke your certificate:
  - Revocation website of D-Trust GmbH: https://my.d-trust.net/sperren
  - If you require telephone support to revoke your certificates, please contact our call and support center:

    Monday to Friday 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 ordered your card using a personal account on the D-TRUST Portal (https://portal.d-trust.net/), please revoke the card in your account.

  When the card is revoked, all of the pertinent certificates will also be revoked.
- If you purchased your certificates via the CSM (Certificate Service Manager), please use the following revocation methods:
  - If you are an operator, revoke your certificate directly using the online revocation function of the Certificate Service Manager (CSM)
  - 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:
  - 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.
  - 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).

I hereby acknowledge and agree that

- I will immediately stop using my private keys as soon as
  - I become aware that the issuing CA has been compromised,
  - the certificate in question has been revoked or
  - the validity end date of the certificate has been reached.
- D-Trust is entitled to revoke the certificate immediately if the applicant violates the terms of the Subscriber Agreement or the applicable CP, TSPS or CPS,
- D-Trust is entitled to revoke the certificate immediately in the event of a violation against the TLS Baseline Requirements, S/MIME Baseline Requirements or the Guidelines for the Issuance and Management of Extended Validation Certificates of the CA/Browser Forum,
- within the scope of checking application data, the HR department, my superiors, 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 D-Trust root certificates 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.

You can find the applicable documents here:

- Certificate Policy (CP) of D-Trust GmbH:
  http://www.d-trust.net/internet/files/D-TRUST_CP.pdf
- D-TRUST Trust Service Practice Statement (TSPS):
  https://www.d-trust.net/internet/files/D-TRUST_TSPS.pdf
- CPS of D-TRUST Root PKI:
  http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CPS.pdf
- CPS of D-TRUST CSM PKI:
  http://www.d-trust.net/internet/files/D-TRUST_CSM_PKI_CPS.pdf
- CPS of D-TRUST in the telematics infrastructure:
  http://www.d-trust.net/internet/files/D-TRUST_TSP-TI_CPS.pdf
- PKI disclosure statement for qualified certificates (PKI DS):
  https://www.d-trust.net/internet/files/D-TRUST_PKI_Disclosure_Statement.pdf
- CA/Browser Forum Guidelines:
  https://www.cabforum.org

as well as further details regarding qualified products such as TLS certificates (QWACs) or seal and signature certificates.

For a clear assignment of the CPS applicable to your product, you can find the corresponding URL within the certificate at the following location:
Certificate policies **->** D-Trust policy identifier (1.3.6.1.4.1.4788.2.x.x) **->** URL of the CPS.

Alternatively, you can also use this Overview.
(https://www.d-trust.net/files/dokumente/pdf/terms-and-conditions_product-service.pdf)

VERPFLICHTUNGSERKLÄRUNG

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

<table>
<tr>
<td>

- **Signaturkarten**
- **Siegelkarten**
- **Siegelzertifikate ohne Karte**
- **E-Mail Zertifikate (S/MIME)**

</td>
<td>

- **TLS-Zertifikate (Webseitenzertifikate)**

</td>
</tr>
<tr>
<td>

Ich versichere hiermit, dass

- ich für meine eigene Person oder im Auftrag meiner Organisation ein Zertifikat bestellt habe.
- ich mein persönliches Konto im D-Trust Portal (https://portal.d-trust.net/) nur für meine eigene Person oder als Vertretungsberechtigte für eine juristische Person (Organisation) nutze.
- ich den Reklamationsprozess einleite, wenn ich meine Signatur- bzw. Siegelkarte nicht innerhalb von zwei Wochen nach Versandmeldung erhalte.

  Die Karte muss in diesem Fall gesperrt werden.
- 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, Organisations-zugehörigkeit) ich diese unaufgefordert meinem technischen Ansprechpartner meiner Organisation oder der D-Trust zur Verfügung stelle.
- ich das erhaltene Zertifikat erst nach erfolgreich abgeschlossener Überprüfung der enthaltenen Daten auf deren Richtigkeit hin einsetzen werde.
- ich das Zertifikat bzw. den privaten Schlüssel ausschließlich für zugelassene Zwecke im Einklang mit dem Certification Practice Statement (CPS)verwenden werde.
- ich auf die Anweisungen des TSP bzgl. der hier aufgeführten Rechte und Pflichten zeitnah reagiere.

Gilt zusätzlich für Siegelzertifikate ohne Karte und E-Mail-Zertifikate (S/MIME):

- Ich versichere hiermit, dass ich 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 habe.

</td>
<td>

Ich versichere hiermit, dass

- 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 ich diese unaufgefordert der D-Trust zur Verfügung stellen werde.
- ich ausschließlich (auch als der vom Zertifikatsnehmer mit Zertifikats-beantragung, -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.
- ich das TLS-Zertifikat ausschließlich auf Servern exakt der Organisation installieren werde, die im Zertifikat mit ihrem Namen (CN und O) bestätigt worden sind.
- ich das Schlüsselpaar mit einem der folgenden Algorithmen generiert habe (rsa, dsa, ecdsa-Fp oder ecgdsa-Fp).
- ich das erhaltene Zertifikat erst nach erfolgreich abgeschlossener Überprüfung der enthaltenen Daten auf deren Richtigkeit hin, einsetzen werde.
- ich das Zertifikat bzw. den privaten Schlüssel ausschließlich für zugelassene Zwecke im Einklang mit dem Certification Practice Statement (CPS), erstellen und verwenden werde.
- ich auf die Anweisungen des TSP bzgl. der hier aufgeführten Rechte und Pflichten zeitnah reagiere werde.

</td>
</tr>
</table>

Veröffentlichung von Zertifikaten im LDAP-Verzeichnis

Ich nehme zur Kenntnis und erkläre mich damit einverstanden, dass die folgenden Zertifikatsprodukte im LDAP-Verzeichnis veröffentlicht werden:

- E-Mail-Zertifikate (S/MIME) mit Ausnahme von Zertifikaten aus der D-Trust V-PKI
- TLS-Zertifikate (Webseitenzertifikate)
- Siegelzertifikate

Widerruf bzw. Sperrung von Zertifikaten

Ich versichere, 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:

- Verdacht oder Gewissheit der Kompromittierung des privaten Schlüssels
- Verlust der alleinigen Kontrolle über den privaten Schlüssel (z.B. ein Unbefugter hat Ihre PIN ausgespäht)
- 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:
  - die Sperr-Webseite der D-Trust GmbH: https://my.d-trust.net/sperren
  - Wenn Sie telefonische Unterstützung beim Widerruf Ihrer Zertifikate benötigen, kontaktieren Sie bitte unser Call- und Supportcenter:

    Montag bis Freitag 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 Karte über ein persönliches Konto im D-Trust Portal (https://portal.d-trust.net/) bestellt haben, sperren Sie bitte die Karte in Ihrem Konto.

  Mit der Sperrung der Karte werden alle dazugehörigen Zertifikate widerrufen.
- Wenn Sie Ihre Zertifikate über den CSM (Certificate Service Manager) erworben haben, nutzen Sie bitte folgende Sperrwege:
  - Wenn Sie Operator sind, widerrufen Sie bitte direkt über die Online-Sperrfunktion des Certificate Service Managers (CSM)

  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:
  - Wenn Sie berechtigter Zertifikatnehmer sind, können Sie Ihren Heilberufsausweis (Sperrantragsteller_AS) über das Antragsportal https://ehealth.d-trust.net/antragsportal widerrufen.
  - 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.

Ich nehme zur Kenntnis und erkläre mich damit einverstanden, dass

- ich die Nutzung meiner privaten Schlüssel umgehend einstellen werde, sobald
  - ich Kenntnis über die Kompromittierung der ausstellenden CA erlange,
  - das betreffende Zertifikat widerrufen wurde oder
  - das Gültigkeits-Enddatum des Zertifikats erreicht ist.
- D-Trust berechtigt ist, das Zertifikat sofort zu widerrufen, wenn der Antragsteller gegen die Bedingungen der Verpflichtungserklärung (Subscriber Agreement) bzw. gegen die anwendbaren CP, TSPS oder CPS verstößt,
- D-Trust berechtigt ist, das Zertifikat sofort zu widerrufen, wenn ein Verstoß gegen die TLS Baseline Requirements, S/MIME Baseline Requirements oder der Guidelines for the Issuance and Management of Extended Validation Certificates des CA/Browser Forums vorliegt,
- 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 die anwendbaren Dokumente:

- Zertifikatsrichtlinie (CP) der D-Trust GmbH:
  http://www.d-trust.net/internet/files/D-TRUST_CP.pdf
- D-TRUST Trust Service Practice Statement (TSPS):
  https://www.d-trust.net/internet/files/D-TRUST_TSPS.pdf
- CPS der D-TRUST Root PKI:
  http://www.d-trust.net/internet/files/D-TRUST_Root_PKI_CPS.pdf
- CPS der D-TRUST CSM PKI:
  http://www.d-trust.net/internet/files/D-TRUST_CSM_PKI_CPS.pdf
- CPS der D-TRUST in der Telematikinfrastruktur:
  http://www.d-trust.net/internet/files/D-TRUST_TSP-TI_CPS.pdf
- PKI-Nutzerinformationen für qualifizierte Zertifikate (PKI DS):
  https://www.d-trust.net/internet/files/D-TRUST_PKI_Disclosure_Statement.pdf
- CA/Browser Forum Guidelines:
  https://www.cabforum.org

sowie weiterführende Informationen zu qualifizierten Produkten wie TLS-Zertifikate (QWAC), Siegel- und Signaturzertifikate.

Für eine eindeutige Zuordnung, der für Ihr Produkt anwendbares CPS, können Sie die entsprechende URL innerhalb des Zertifikats an der folgenden Stelle finden:
Zertifikatsrichtlinien -> Richtlinienbezeichner der D-Trust (1.3.6.1.4.1.4788.2.x.x) **->** URL der CPS.

Alternativ können Sie hierzu auch diese Übersicht verwenden.
(https://www.d-trust.net/files/dokumente/pdf/terms-and-conditions_produkt-dienstleistung.pdf)