D-TRUST
Ein Unternehmen der Bundesdruckerei

PKI DISCLOSURE STATEMENT

ENGLISH

PKI-NUTZERINFORMATION

DEUTSCH

PKI DISCLOSURE STATEMENT

This document provides PKI service users with useful information about the general conditions for trust services offered by D-Trust GmbH, the trust service provider oft he Bundesdruckerei Group.

Version:	1.7
Date of release:	2020-11-12
Effective date:	2020-11-12
Classification:	– Public –

PUBLISHING DETAILS

Trademarks

Trademarks are used without any guarantee that they are not subject to copyright.

Notes

D-Trust GmbH accepts no liability for direct or indirect damage resulting from or related to the use of this document.

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin, Germany
Tel.: +49 (0) 30 25 98 - 0

Contents

1. Contact details

1.1 General contact details

Important addresses	
Your trust service provider (TSP): D-Trust GmbH Kommandantenstraße 15 10969 Berlin, Germany Tel.: + 49 (0)30 / 25 93 91 – 0 Fax: + 49 (0) 30 / 25 93 91 –22 info@D-TRUST.net www.D-TRUST.net	**Your sales contact:** D-Trust GmbH | A Bundesdruckerei company Kommandantenstraße 15 10969 Berlin, Germany Tel.: + 49 (0) 30 / 25 98 – 0 Vertrieb@d-trust.net https://www.bundesdruckerei.de/en/

1.2 Reporting security problems with TLS certificates[1]

The TSP provides the following Internet page for reporting security problems with TLS certificates (for instance, in the case of suspected misuse):

https://www.bundesdruckerei.de/en/Service-Support/Support/Reporting-a-certificate-problem

E-mail: ssl-issue@bdr.de

1.3 Revocation of certificates (both TLS certificates and non-TLS certificates)

Have your certificates revoked if:

- you suspect or are certain that the private key has been compromised
- you lose the signature or seal card or if you lose sole control over the private key even if it is not stored on a signature or seal card
- the certificate data changes (e. g. name, addresses or affiliation with the organization).

You should also have your certificates revoked if you do not need your signature or seal card any longer (this includes the decryption of documents). In order to cancel your signature or seal card, enter an incorrect PIN (see section 5) several times in order to cancel the certificates, or destroy the chip on the card mechanically.

You have three options for having your certificate revoked:

1. Online:

Depending on your product, you can use the revocation method permitted for you 24/7 to revoke certificates.

To revoke certificates online, please have the following information ready:

- Request/card ID
- Revocation password

Also possible

- SMS TAN

[1] Only for TLS certificates according to EVCP, OVCP and QCP-w.

Products	Persons authorized to revoke	Revocation methods
HPC (HBA) **(Health Professional Card)**	"Sperrantragsteller_AS" Subscriber authorized to revoke certificates and who has a health professional card or a secure module card (SMC-B).	▪ Request portal https://ehealth.d-trust.net/antragsportal/
	"Sperrantragsteller_KHG" Parties authorized to revoke certificates, such as the card issuer's representatives	▪ Activation portal https://ehealth.d-trust.net/freigabeportal/ ▪ SOAP interface (technical interface)
Qualified signature and seal cards	If you know your card ID or request ID and your revocation password, please use the revocation website of D-TRUST to revoke your certificates.	▪ https://my.d-trust.net/sperren
Qualified seal (without a card)	If you have purchased your certificates via the CSM (Certificate Service Manager) and you are an operator, please revoke your certificates using the online revocation function of the Certificate Service Manager (CSM) or contact your CSM operator.	▪ https://mycsm.d-trust.net/csm/
	If you know your request ID and your revocation password, please use the revocation website of D-TRUST to revoke your certificates.	▪ https://my.d-trust.net/sperren
Qualified website authentication certificate	If you have purchased your certificates via the CSM (Certificate Service Manager) and you are an operator, please revoke your certificates using the online revocation function of the Certificate Service Manager (CSM) or contact your CSM operator.	▪ https://mycsm.d-trust.net/csm/
	If you know your request ID and your revocation password, please use the revocation website of D-TRUST to revoke your certificates.	▪ https://my.d-trust.net/sperren

2. By phone:

If you require telephone support when revoking your certificates, please contact our call and support center on workdays from 7am to 6pm by calling +49 (0)30-2598-0.

To revoke certificates by phone, you will need to provide the following information to our call and support center:

- Name of the caller
- Name of the certificate owner if the caller is not the holder
- Request/card ID
- Revocation password

3. In writing:

Sign your revocation request by hand and send it to our revocation service at the following address:

D-Trust GmbH
Sperrdienst
Kommandantenstraße 15
10969 Berlin, Germany

Our revocation service needs the following information for a written revocation of your certificates:

- Name of the sender
- Name of the certificate owner if the sender is not the holder
- Request/card ID, if possible
- If possible, revocation password
- The signature of the sender

If your revocation request can be unambiguously identified on the basis of your hand-written signature, the certificate will be revoked the day D-Trust GmbH's revocation service receives the letter.

Retroactive or temporary revocation or suspension of certificates is generally not possible. A certificate, once revoked, cannot be restored, i.e. the revocation process is final and irreversible.
If your certificate contains further information (such as a company name) involving third parties, these are then also authorized to have your certificate revoked.

2. Qualified trust services

2.1 Types of qualified trust services offered

Trust service	Applicable policies	Relevant OIDs[2]
Creation of qualified certificates for individuals on a secure signature creation device (signature card)	▪ ETSI 319 411-2 QCP-n-qscd ▪ Certificate Policy of D-Trust GmbH ▪ Certification Practice Statement of the D-TRUST Root PKI	▪ 0.4.0.194112.1.2 ▪ 1.3.6.1.4.1.4788.2.150.1
Creation of qualified certificates for legal entities on a secure signature creation device (seal card)	▪ ETSI 319 411-2 QCP-l-qscd ▪ Certificate Policy of D-Trust GmbH ▪ Certification Practice Statement of the D-TRUST Root PKI	▪ 0.4.0.194112.1.3 ▪ 1.3.6.1.4.1.4788.2.150.2
Creation of qualified certificates for legal entities without QSCD	▪ ETSI 319 411-2 QCP-l ▪ Certificate Policy of D-Trust GmbH ▪ Certification Practice Statement of the D-TRUST Root PKI ▪ Certification Practice Statement of the D-TRUST CSM PKI	▪ 0.4.0.194112.1.1 ▪ 1.3.6.1.4.1.4788.2.150.5
Creation of qualified certificates for website authentication (qualified TLS certificate)	▪ ETSI 319 411-2 QCP-w ▪ Certificate Policy of D-Trust GmbH ▪ Certification Practice Statement of the D-TRUST CSM PKI ▪ Certification Practice Statement of the D-TRUST Root PKI	▪ 0.4.0.194112.1.4 ▪ 1.3.6.1.4.1.4788.2.150.4

D-Trust GmbH as a qualified trust service provider holds a certificate of conformity with the above-stated policies for the above-mentioned services. The certificates can be used for applications which are compatible with the types of use shown in the certificate (key use and extended key use). Relying parties are solely responsible for their acts.

The rules of the Certificate Policy of D-Trust GmbH also apply.

[2] An Object Identifier (OID) provides an unambiguous identification of the certificate type and references the applicable policies for issuance.

2.2 Possible restrictions in qualified certificates and archiving period

Trust service	Archiving period	Possible restrictions
Creation of qualified certificates for individuals on a secure signature creation device (signature card)	In the case of qualified signature and seal certificates, the provisions of section 16 (4) VDG on permanent storage[3] apply to certificates, identification data, including contact data.	Any certificate restrictions can be seen in the certificate itself (e. g. test certificates, monetary restriction).
Creation of qualified certificates for legal entities on a secure signature creation device (seal card)		
Creation of qualified certificates for legal entities without QSCD		
Creation of qualified certificates for website authentication (qualified TLS certificate)	The archiving period totals at least 7 years after the certificate has expired.	

2.3 Information on the legal effect

The legal effect of the electronic signature, seal and time stamp is defined in Regulation (EU) No 910/2014 of the European Parliament and of the Council, in short: eIDAS Regulation.

Sec. 13 (1) No. 3 of the German Trust Services Act (VDG, Vertrauensdienstegesetz), i.e. of the law implementing the eIDAS Regulation, stipulates that the trust service provider must inform the public pursuant to Sec. 13 (1) VDG of the legal effect of the qualified trusted services offered. We would like to inform you in the following section of the legal effect of our qualified trust services.

Trust service	Feature	Legal effect
Creation of qualified certificates for individuals on a secure signature creation device (signature card)	Qualified signature certificate for generating qualified signatures	• The electronic signature has the same legal effect as the handwritten signature (Art. 25 eIDAS Regulation); • Sec. 126 a of the German Civil Code (BGB, Bürgerliches Gesetzbuch) (electronic form) and sec. 371a of the German Code of Civil Procedure (ZPO, Zivilprozessordnung) (on the probative value of electronic documents)
Creation of qualified certificates for legal entities on a secure signature creation device (seal card)	Qualified seal certificate for generating qualified seals	eIDAS also contains rules on the probative value of electronic instruments: presumption of the integrity of data and of the accuracy of the stated source of the data with which the qualified electronic seal is

[3] For more details, see section 2c of the privacy policy in section 5 of this document.

		associated (see Art. 35 (2) eIDAS Regulation)
Creation of qualified certificates for legal entities without QSCD	Qualified seal certificate for generating advanced seals	eIDAS also contains rules on the probative value of electronic instruments: It is linked to the data to which it relates in such a way that any subsequent change in the data is detectable (see Art. 36 (d) eIDAS Regulation).

Anybody who can use your signature or seal card – i.e. anybody who has your card and knows your PIN – can perform acts which are legally binding upon you because he or she has your "digital signature" or "digital seal". Any electronic signature or seal generated with your card is generally attributed to you.

It is therefore extremely important that you carefully protect your card and your PIN against unauthorized access.

3. Terms and conditions for using the signature/seal multicard

Signature/seal multicard
The signature/seal multicard allows an unlimited number of signatures or seals to be made with just once-off successful PIN verification. In this case, the PIN only needs to be entered again when the system is restarted or a new card is used. This signature/seal card may only be used within a secure environment, especially in the case of non-supervised use.

To ensure the security of the service, the subscriber must adhere to the following rules:

- It is the responsibility of the subscriber to ensure that the technical components used in conjunction with the signature/seal multicard are secure and intended for such use:
  - protection against malware is established on connected IT systems,
  - the network must be considered to be trustworthy and
  - the signature/seal multicard is operated only under supervision or in a closed environment where the signature/seal multicard is protected against unauthorized access.

If the signature key holder has doubts regarding the level of security in the application environment, they should contact a recognised conformity assessment body.

4. Obligations of subscribers[4]

The subscriber must comply with the rules that require consent and are laid down in the Subscriber Agreement. In the event that the subscriber violates the above obligations, D-TRUST is entitled to have the qualified certificate revoked without replacement.
You can find the Subscriber Agreement in the appendix and on our website at the following link:
D-TRUST Subscriber Agreement

[4] The documents as CP, CPS, TSPS, Disclosure Statements and Subscriber Agreements as well as all published certificates are linked in the D-TRUST repository: https://www.bundesdruckerei.de/en/Repository

5. Important links

- Certificate validation with OCSP:
  https://www.bundesdruckerei.de/en/OCSP-Request
- Certificate validation with LDAP:
  https://www.bundesdruckerei.de/en/LDAP-Request
- D-TRUST repository:
  https://www.bundesdruckerei.de/en/Repository
- Privacy policy:
  https://www.d-trust.net/internet/files/Info_DSGVO_P.pdf
- General Terms and Conditions of Business of D-Trust GmbH:
  https://www.d-trust.net/internet/files/agb_d-trust.pdf
- Trusted list of the Federal Network Agency:
  https://www.nrca-ds.de/en/tsl_e.htm

Other relevant documents in the repository of D-Trust GmbH:

- Subscriber Agreement:
  http://www.d-trust.net/internet/files/D-TRUST_Subscriber_Agreement.pdf
- 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 Cloud PKI:
  http://www.d-trust.net/internet/files/D-TRUST_Cloud_PKI_CPS.pdf
- CPS of D-TRUST in the telematics infrastructure:
  http://www.d-trust.net/internet/files/D-TRUST_TSP-TI_CPS.pdf

6. General information

6.1 Complaint and arbitration procedure

Should you have any problems or questions which you cannot settle with our support on an amicable basis, you can refer the case to the Federal Network Agency as your contact partner for complaints and arbitration; furthermore, you can also obtain details of such proceedings from the Federal Network Agency.

6.2 Provision of certification and trust services by D-Trust GmbH

D-Trust GmbH distributes trust services pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Council ("eIDAS Regulation") as well as further certification services.

6.3 Revocation

You cannot revoke your certificate product order because the production and provision of the certificate constitute goods which are produced according to customer specifications and are clearly tailored to your personal needs.

6.4 Applicable law

Any legal relations between Bundesdruckerei, D-Trust GmbH and the customer shall be subject to the laws of the Federal Republic of Germany. The UN Convention on Contracts for the International Sale of Goods shall be excluded.

6.5 Place of jurisdiction

The place of jurisdiction for all disputes shall be Berlin in as far as the customer is a merchant, a legal entity under public law and/or a special-assets institution under public law or in as far as no general place of jurisdiction exists in Germany with regard to the customer. Bundesdruckerei shall be at liberty to enforce its rights at the place being the general place of jurisdiction for the customer. An exclusive place of jurisdiction, if any, shall not be affected by the foregoing provision.

6.6 Place of performance

The place of performance for the generation of the certificate is Berlin for both D-TRUST/ Bundesdruckerei and the customer.

7. Rules for the use of the electronic signature

Below we have compiled some rules for the secure use of qualified certificates.

7.1 PIN

Trust service	Possible PINs	Type of PIN
Creation of qualified certificates for individuals on a secure signature creation device (signature card)	PIN 1 PIN 2	You receive a PIN letter.
Creation of qualified certificates for legal entities on a secure signature creation device (seal card)	PIN 2	You receive a PIN letter.
Creation of qualified certificates for legal entities without QSCD	PIN 1	The PIN is generated by the certificate holder as part of the key generation procedure.
Creation of qualified certificates for website authentication (qualified TLS certificate)	PIN 1	The PIN is generated by the certificate holder as part of the key generation procedure.

The PINs are:

- PIN1 (card PIN) for authentication and encryption
- as well as PIN2 (signature PIN) for the signature. PIN2 is protected in its as-supplied condition by a transport PIN. The transport PIN is a security feature of the card which enables you to see that your personal signature key was never used before. Before you use the signature key for the first time, you are prompted to change PIN2 (see PIN letter, signature PIN, 5 digits, numerals only) to a series of **at least 6 numbers (we recommend using at least 8 numbers)**.
- It is not until you have made this change that you can use the signature key and hence sign. If you are not prompted to change PIN2 when you are using your signature card for the first time, or if the PIN2 communicated to you is not accepted or if your transport PIN has more than 5 digits, this may

mean that your signature card has been manipulated. There is a chance that somebody used your signature card before you received it. **PIN1 (card PIN) is not affected by this.**

Our support center staff will be pleased to assist you if you have any questions concerning the use of your PINs (for contact details, please see the last page).

7.2 PUK

D-TRUST signature cards are supplied with two so-called PUKs. These are special PINs which you can use to reset the retry counters of PIN1 (card PIN) and PIN2 (signature PIN). This means: If one of the two PINs of the signature card was blocked because an incorrect value was entered three times for the corresponding PIN (card error message: "Card blocked"), you can then enter the corresponding PUK in order to unblock the card again. **It is not possible to change the existing PINs by entering the PUK.** The number of unblocking operations using the PUK is limited to 10 attempts.

If the attempt to unblock the card failed, the only option is to apply for a replacement card – against payment of a fee.
Our support center staff will be pleased to assist you if you have any questions concerning the use of your PINs and PUKs (for contact details, please see the last page).

7.3 Signature check

You need a signature verification software in order to verify an electronic signature.
The signature software automatically checks the validity and origin of the certificate as well as the integrity of the signed data and supplies the result of the check in a message. The legally relevant contents of the document are once again displayed in a view which is part of your signature application software and protected against unnoticed manipulation.
In order to ensure the security of your signature application software, you must protect your computer and the operating system against threats. In particular, use anti-virus programs in their latest version for this purpose.

7.4 Need to renew signatures

Technical developments can lead to a lowering of the security value of qualified, signed, sealed or time-stamped data. It is therefore necessary to electronically re-sign, re-seal or time-stamp again such data in due time using the latest signature technology available at that time.

7.5 Annex – Subscriber Agreement

You can find the Subscriber Agreement in the appendix to this document.

APPENDIX

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 4pm 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) as well as further details regarding qualified products such as TLS certificates (QWACs) or seal and signature certificates.

PKI-NUTZERINFORMATION (PKI DISCLOSURE STATEMENT)

Dieses Dokument informiert den Nutzer von PKI-Dienstleitungen der D-Trust GmbH, dem Vertrauensdiensteanbieter der Bundesdruckerei Gruppe, über die wesentlichen Rahmenbedingungen der angebotenen Vertrauensdienste.

Version:	1.7
Datum der Freigabe:	12.11.2020
Datum des Inkrafttretens:	12.11.2020
Klassifizierung:	- öffentlich-

IMPRESSUM

Marke

Markennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Hinweise

Die D-Trust GmbH haftet nicht für direkte oder indirekte Schäden, die sich aus der Verwendung dieses Dokuments ergeben oder damit in Beziehung stehen.

D-Trust GmbH

Kommandantenstraße 15
10969 Berlin
Tel.: +49 (0) 30 25 98 - 0

Inhaltsverzeichnis

1. Kontaktinformationen

1.1 Allgemeine Kontaktinformationen

Wichtige Adressen	
Ihr Vertrauensdiensteanbieter (TSP): D-Trust GmbH Kommandantenstraße 15 10969 Berlin Tel.: + 49 (0) 30 / 25 93 91 – 0 Fax: + 49 (0) 30 / 25 93 91 –22 info@D-TRUST.net www.D-TRUST.net	**Ihr Vertriebskontakt:** D-Trust GmbH | Ein Unternehmen der Bundesdruckerei Kommandantenstr. 15 10969 Berlin Tel.: + 49 (0) 30 / 25 98 – 0 Vertrieb@d-trust.net www.bundesdruckerei.de

1.2 Meldung von Sicherheitsvorfällen mit TLS-Zertifikaten[5]

Zur Meldung von Sicherheitsvorfällen mit TLS-Zertifikaten (z.B. im Fall eines Missbrauchsverdachts), hält der TSP folgende Internetseite bereit:

https://www.bundesdruckerei.de/de/Service-Support/Support/Meldung-eines-Zertifikatsproblems

E-Mail: ssl-issue@bdr.de

1.3 Widerruf von Zertifikaten (sowohl TLS-Zertifikate als auch non-TLS-Zertifikate)

Lassen Sie Ihre Zertifikate widerrufen, bei

- Verdacht oder Gewissheit der Kompromittierung des privaten Schlüssels.
- Verlust der Signatur- oder der Siegelkarte bzw. Verlust der alleinigen Kontrolle über den privaten Schlüssel auch ohne, dass dieser auf einer Signatur- oder Siegelkarte gespeichert ist.
- Änderungen an Zertifikatsdaten jeglicher Art (z.B. Namen, Adressen oder Organisationszugehörigkeiten).

Lassen Sie Ihre Zertifikate auch sperren, wenn Sie Ihre Signatur- oder Siegelkarte nicht mehr benötigen (auch nicht zum Entschlüsseln von Dokumenten). Sie können die Signatur- oder Siegelkarte unbrauchbar machen, indem Sie die Zertifikate durch mehrfach falsche PIN-Eingabe (siehe Kapitel 5) unbrauchbar machen oder den Chip auf der Karte mechanisch zerstören.

Sie haben drei Möglichkeiten Ihr Zertifikat zu widerrufen:

1. Online:

Sie können entsprechend Ihrem Produkt, den für Sie zulässigen Sperrweg 24x7 zum Widerrufen von Zertifikaten nutzen.

Für die online Sperrung halten Sie bitte folgende Informationen bereit:

- Antrags-/Karten-ID
- Sperrpasswort

Weiterhin möglich

[5] Nur für TLS-Zertifikate gemäß EVCP, OVCP und QCP-w.

- SMS-TAN

Produkte	Sperrberechtigte	Sperrwege
HBA (HPC) **(Heilberufs-ausweis)**	Sperrantragsteller_AS Zur Sperrung von Zertifikaten berechtigter Zertifikatsnehmer, welcher über einen HBA oder einen SMC-B verfügt.	▪ Antragsportal https://ehealth.d-trust.net/antragsportal/
	Sperrantragsteller_KHG Zur Sperrung von Zertifikaten berechtigte Stellen, z.B. Vertreter des Kartenherausgebers	▪ Freigabeportal https://ehealth.d-trust.net/freigabeportal/ ▪ SOAP-Schnittstelle (technische Schnittstelle)
Qualifizierte Signatur-und Siegelkarten	Wenn Sie Ihre Karten-ID bzw. Antrags-ID und Ihr Sperrpasswort kennen, nutzen Sie bitte zum Sperren die Sperr-Webseite der D-Trust GmbH.	▪ https://my.d-trust.net/sperren
Qualifiziertes Siegel (ohne Karte)	Wenn Sie Ihre Zertifikate über den CSM (Certificate Service Manager) erworben haben und Operator sind, sperren Sie bitte direkt über die Online-Sperrfunktion des Certificate Service Managers (CSM) oder kontaktieren Sie Ihren CSM Operator.	▪ https://mycsm.d-trust.net/csm/
	Wenn Sie Ihre Antrags-ID und Ihr Sperrpasswort kennen, nutzen Sie bitte zum Sperren die Sperr-Webseite der D-Trust GmbH	▪ https://my.d-trust.net/sperren
Qualifiziertes Webseitenzertifikat	Wenn Sie Ihre Zertifikate über den CSM (Certificate Service Manager) erworben haben und Operator sind, sperren Sie bitte direkt über die Online-Sperrfunktion des Certificate Service Managers (CSM) oder kontaktieren Sie Ihren CSM Operator.	▪ https://mycsm.d-trust.net/csm/
	Wenn Sie Ihre Antrags-ID und Ihr Sperrpasswort kennen, nutzen Sie bitte zum Sperren die Sperr-Webseite der D-Trust GmbH	▪ https://my.d-trust.net/sperren

2. Telefonisch:

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.

Für die telefonische Sperrung benötigt unser Call- und Supportcenter folgende Informationen:

- Name des Anrufers
- Name des Zertifikatinhabers, falls nicht Anrufer selbst
- Antrags-/Karten-ID
- Sperrpasswort

3. Schriftlich:

Sie richten einen handschriftlich unterschriebenen Sperrauftrag an unseren Sperrdienst. Senden Sie diesen an die folgende Adresse:

D-Trust GmbH
Sperrdienst
Kommandantenstraße 15
10969 Berlin

Für den schriftlichen Widerruf Ihrer Zertifikate benötigt unser Sperrdienst folgende Informationen:

- Name des Absenders
- Name des Zertifikatinhabers, falls nicht Absender selbst
- wenn möglich Antrags-/Karten-ID
- wenn möglich Sperrpasswort
- Unterschrift des Absenders

Falls Ihr Sperrauftrag anhand Ihrer Unterschrift eindeutig identifiziert werden kann, wird der Widerruf an dem Tag durchgeführt, an dem das Schreiben beim Sperrdienst der D-Trust GmbH eingetroffen ist.

Eine rückwirkende oder vorübergehende Sperrung bzw. Suspendierung von Zertifikaten ist generell nicht möglich. Eine einmal vorgenommene Sperrung entspricht einem Widerruf und kann nicht rückgängig gemacht werden und ist somit endgültig.
Wenn in Ihrem Zertifikat weitere Angaben (z.B. ein Firmenname) aufgenommen werden, durch die Dritte involviert sind, so sind auch diese berechtigt, Ihr Zertifikat zu widerrufen.

2. Qualifizierte Vertrauensdienste

2.1 Angebotene Arten von qualifizierten Vertrauensdiensten

Vertrauensdienst	Anwendbare Richtlinien	Relevante OIDs[6]
Erstellung von qualifizierten Zertifikaten für natürliche Personen auf einer sicheren Signaturerstellungseinheit (Signaturkarte).	▪ ETSI 319 411-2 QCP-n-qscd ▪ Zertifikatsrichtlinie der D-Trust GmbH ▪ Certification Practice Statement der D-TRUST Root PKI	▪ 0.4.0.194112.1.2 ▪ 1.3.6.1.4.1.4788.2.150.1
Erstellung von qualifizierten Zertifikaten für juristische Personen auf einer sicheren Signaturerstellungseinheit (Siegelkarte).	▪ ETSI 319 411-2 QCP-l-qscd ▪ Zertifikatsrichtlinie der D-Trust GmbH ▪ Certification Practice Statement der D-TRUST Root PKI	▪ 0.4.0.194112.1.3 ▪ 1.3.6.1.4.1.4788.2.150.2
Erstellung von qualifizierten Zertifikaten für juristische Personen ohne QSCD.	▪ ETSI 319 411-2 QCP-l ▪ Zertifikatsrichtlinie der D-Trust GmbH ▪ Certification Practice Statement der D-TRUST Root PKI ▪ Certification Practice Statement der D-TRUST CSM PKI	▪ 0.4.0.194112.1.1 ▪ 1.3.6.1.4.1.4788.2.150.5
Erstellung von qualifizierten Zertifikaten für Webseitenauthentifizierung (qualifiziertes TLS-Zertifikat)	▪ ETSI 319 411-2 QCP-w ▪ Zertifikatsrichtlinie der D-Trust GmbH ▪ Certification Practice Statement der D-TRUST CSM PKI ▪ Certification Practice Statement der D-TRUST Root PKI	▪ 0.4.0.194112.1.4 ▪ 1.3.6.1.4.1.4788.2.150.4

Die D-Trust GmbH als qualifizierter Vertrauensdiensteanbieter hat für die genannten Dienste eine entsprechende Konformitätsbestätigung zu den genannten Richtlinien. Die Zertifikate dürfen für die Anwendungen benutzt werden, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen (Schlüsselverwendung und erweiterte Schlüsselverwendung). Zertifikatsnutzer handeln auf eigene Verantwortung.

Weiterhin gelten die Regelungen der Zertifikatsrichtlinie der D-Trust GmbH.

[6] Ein Object Identifier (OID) identifiziert den Zertifikatstyp eindeutig und referenziert die anwendbaren Richtlinien zur Ausstellung.

2.2 Mögliche Beschränkungen in qualifizierten Zertifikaten und Archivierungszeitraum

Vertrauensdienst	Archivierungsdauer	mögliche Einschränkungen
Erstellung von qualifizierten Zertifikaten für natürliche Personen auf einer sicheren Signaturerstellungseinheit (Signaturkarte).	Für qualifizierte Signatur- und Siegelzertifikate gelten für Zertifikate, Zertifikatsnachweisdaten, einschließlich der Kontaktdaten die Vorgaben des § 16 Abs. 4 Vertrauensdienstegesetz zur dauerhaften Aufbewahrung[7].	Mögliche Zertifikats-beschränkungen sind im Zertifikat selbst ersichtlich (z.B. Testzertifikate, monetäre Beschränkung)
Erstellung von qualifizierten Zertifikaten für juristische Personen auf einer sicheren Signaturerstellungseinheit (Siegelkarte).		
Erstellung von qualifizierten Zertifikaten für juristische Personen ohne QSCD.		
Erstellung von qualifizierten Zertifikaten für Webseiten-authentifizierung (qualifiziertes TLS-Zertifikat).	Die Archivierungsdauer beträgt mindestens 7 Jahre nach Ablauf der Gültigkeit des Zertifikats.	

[7] Für weitere Informationen siehe Abschnitt 2c der Datenschutzerklärung im Abschnitt 5.

2.3 Unterrichtung zur Rechtwirkung

Die Rechtswirkung der elektronischen Signatur, Siegel und Zeitstempel ist in Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates, kurz eIDAS Verordnung, definiert.

Das VDG als Durchführungsgesetz der eIDAS-Verordnung verlangt in § 13 (1) Nr. 3. VDG, dass der Vertrauensdiensteanbieter gemäß § 13 (1) VDG über die Rechtswirkung der angebotenen qualifizierten Vertrauensdienste unterrichtet. In dem folgenden Absatz möchten wir Sie deshalb über die Rechtswirkung unserer qualifizierten Vertrauensdienste informieren.

Vertrauensdienst	Ausprägung	Rechtswirkung
Erstellung von qualifizierten Zertifikaten für natürliche Personen auf einer sicheren Signaturerstellungseinheit (Signaturkarte).	Qualifiziertes Signaturzertifikat für die Erzeugung qualifizierter Signaturen.	• Elektronische Unterschrift hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift (Art. 25 eIDAS-Verordnung); • § 126 a BGB (elektronische Form) und §371a ZPO (zur Beweiskraft elektronischer Dokumente)
Erstellung von qualifizierten Zertifikaten für juristische Personen auf einer sicheren Signaturerstellungseinheit (Siegelkarte).	Qualifiziertes Siegelzertifikat für die Erzeugung qualifizierter Siegel.	Die eIDAS enthält zudem Regelungen zur Beweiskraft elektronischer Instrumente: Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist (vgl. Art 35 (2) eIDAS-Verordnung)
Erstellung von qualifizierten Zertifikaten für juristische Personen ohne QSCD.	Qualifiziertes Siegelzertifikat für die Erzeugung fortgeschrittener Siegel.	Die eIDAS enthält zudem Regelungen zur Beweiskraft elektronischer Instrumente: Es ist so mit den Daten, auf die es sich bezieht, verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann (vgl. Art 36 (d) eIDAS-Verordnung).

Wer die Möglichkeit hat, Ihre Signatur- oder Siegelkarte zu benutzen, d.h. Ihre Karte hat und Ihre PIN kennt, kann rechtskräftig für Sie agieren, da er im Besitz Ihrer „digitalen Unterschrift" bzw. „digitalen Siegels" ist. Jede mit Ihrer Karte erzeugte elektronische Signatur bzw. jedes Siegel wird grundsätzlich Ihnen zugeordnet.

Es ist daher außerordentlich wichtig, dass Sie Ihre Karte und Ihre PIN mit größter Sorgfalt vor unbefugtem Zugriff schützen.

3. Einsatzbedingungen von Massensignatur- / Massensiegelkarte

Massensignaturkarte/Massensiegelkarte
Bei der Massensignatur- / Massensiegelkarte ist gegebenenfalls eine unbegrenzte Anzahl von Signaturen bzw. Siegeln durch eine einzelne erfolgreiche PIN-Verifikation möglich. Eine erneute Eingabe der PIN ist in diesem Fall erst bei einem Neustart des Systems oder bei Einsatz einer neuen Karte erforderlich. Diese Signatur- / Siegelkarte darf – insbesondere bei einem unbeaufsichtigten Betrieb - nur innerhalb einer gesicherten Umgebung betrieben werden.

Um die Sicherheit des Dienstes zu gewährleisten, muss sich der Zertifikatsnehmer an folgende Regeln halten:

- Es liegt im Verantwortungsbereich des Zertifikatsnehmers Sorge dafür zu tragen, dass diejenigen technischen Komponenten, die er in Verbindung mit der Massensignatur- / Massensiegelkarte nutzt, sicher und zu einer solchen Nutzung bestimmt sind:
  - ein Schutz vor Schadsoftware auf verbundenen IT-Systemen etabliert ist,
  - das Netzwerk als vertrauenswürdig einzuschätzen ist und
  - die Massensignatur- / Massensiegelkarte nur unter Aufsicht oder in einer abschließbaren Umgebung, in der Massensignatur- / Massensiegelkarte vor unbefugten Zugriff geschützt ist, betrieben wird.

Hat der Signaturschlüssel-Inhaber Zweifel an der ausreichenden Sicherheit seiner Einsatzumgebung, sollte er eine anerkannte Konformitätsbestätigungsstelle kontaktieren.

4. Pflichten der Zertifikatsnehmer

Der Zertifikatsnehmer muss sich an die, in der Verpflichtungserklärung (subscriber agreement) genannten, zustimmungspflichtigen Regeln halten. Verletzt der Zertifikatsnehmer die genannten Pflichten, kann die D-TRUST das qualifizierte Zertifikat ersatzlos sperren lassen.
Die Verpflichtungserklärung (subscriber agreement) finden Sie im Anhang und auf unserer Webseite unter folgendem Link: D-TRUST_Subscriber_Agreement

5. Wichtige Links

- Zertifikatsüberprüfung mittels OCSP:
  https://www.bundesdruckerei.de/de/2720-ocsp-abfrage
- Zertifikatsüberprüfung mittel LDAP:
  https://www.bundesdruckerei.de/de/2936-ldap-abfrage
- D-TRUST Repository[8]:
  https://www.d-trust.net/repository
- Datenschutzerklärung:
  https://www.d-trust.net/internet/files/Info_DSGVO_P.pdf
- D-TRUST AGB:
  https://www.d-trust.net/internet/files/agb_d-trust.pdf
- Vertrauensliste der Bundesnetzagentur:
  https://www.nrca-ds.de/en/tsl_e.htm

[8] Im Repository sind alle Dokumente wie CP, CPS, TSPS, Nutzerinformationen und Verpflichtungserklärungen sowie alle veröffentlichten Zertifikate abgelegt.

Weitere relevante Dokumente im Repository der D-Trust GmbH:

- Subscriber Agreement / Verpflichtungserklärung:
  http://www.d-trust.net/internet/files/D-TRUST_Subscriber_Agreement.pdf
- 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 Cloud PKI:
  http://www.d-trust.net/internet/files/D-TRUST_Cloud_PKI_CPS.pdf
- CPS der D-TRUST in der Telematikinfrastruktur:
  http://www.d-trust.net/internet/files/D-TRUST_TSP-TI_CPS.pdf

6. Allgemeine Informationen

6.1 Beschwerde- und Schlichtungsverfahren

Sollten Sie Probleme oder Fragen haben, die Sie nicht einvernehmlich mit unserem Support klären konnten, haben Sie die Möglichkeit, die Bundesnetzagentur als Ansprechpartner für Beschwerde- und Schlichtungsverfahren sowie zu Einzelheiten der Inanspruchnahme solcher Verfahren zu befragen.

6.2 Bereitstellen von Zertifizierungs- und Vertrauensdiensten der D-Trust GmbH

Die D-Trust GmbH vertreibt Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments („eIDAS-Richtlinie") sowie weitere Zertifizierungsdienste.

6.3 Widerruf

Sie können Ihre Vertragserklärung im Hinblick auf die Bestellung eines Zertifikatsprodukts nicht widerrufen, da es sich bei der Erstellung und Überlassung von Zertifikatsprodukten um Ware handelt, die nach Kundenspezifikationen angefertigt und eindeutig auf Ihre persönlichen Bedürfnisse zugeschnitten ist.

6.4 Anwendbares Recht

Für sämtliche Rechtsbeziehungen zwischen der Bundesdruckerei, der D-Trust GmbH und dem Kunden findet deutsches Recht Anwendung. UN-Kaufrecht ist ausgeschlossen.

6.5 Gerichtsstand

Der Gerichtstand für alle Rechtsstreitigkeiten ist Berlin, soweit der Kunde Kaufmann, eine juristische Person des öffentlichen Rechts bzw. ein öffentlich rechtliches Sondervermögen ist oder in der Bundesrepublik Deutschland keinen allgemeinen Gerichtstand hat. Die Bundesdruckerei kann ihre Rechte auch am allgemeinen Gerichtstand des Kunden geltend machen. Ein etwaiger ausschließlicher Gerichtstand bleibt von der vorliegenden Vereinbarung unberührt.

6.6 Erfüllungsort

Erfüllungsort der Zertifikatserstellung für die D-TRUST/ Bundesdruckerei und den Kunden ist Berlin.

7. Regeln für den Umgang mit der elektronischen Signatur

Wir haben einige Regeln für den sicheren Umgang mit qualifizierten Zertifikaten zusammengestellt.

7.1 Die PIN

Vertrauensdienst	Mögliche PINs	Art der PIN
Erstellung von qualifizierten Zertifikaten für natürliche Personen auf einer sicheren Signaturerstellungseinheit (Signaturkarte).	PIN 1 PIN 2	Sie erhalten einen PIN-Brief.
Erstellung von qualifizierten Zertifikaten für juristische Personen auf einer sicheren Signaturerstellungseinheit (Siegelkarte).	PIN 2	Sie erhalten einen PIN-Brief.
Erstellung von qualifizierten Zertifikaten für juristische Personen ohne QSCD.	PIN 1	PIN wird durch den Zertifikatsnehmer im Rahmen der Schlüsselerzeugen selbst generiert.
Erstellung von qualifizierten Zertifikaten für Webseitenauthentifizierung (qualifiziertes TLS-Zertifikat)	PIN 1	PIN wird durch den Zertifikatsnehmer im Rahmen der Schlüsselerzeugen selbst generiert.

Bei den PINs handelt es sich um:

- die PIN1 (auch Card-PIN) für Authentifizierung und Verschlüsselung
- sowie die PIN2 (Signatur-PIN) für die Signatur. Die PIN2 ist im Auslieferungszustand durch einen Transport-PIN geschützt. Die Transport-PIN ist ein Sicherheitsmerkmal der Karte, welches Ihnen ermöglicht festzustellen, dass Ihr persönlicher Signaturschlüssel noch nie benutzt wurde. Vor der ersten Benutzung des Signaturschlüssels werden Sie dazu aufgefordert die PIN2 (siehe PIN-Brief, Signatur-PIN, 5 Stellen, nur Ziffern) zu in **mindestens 6 Ziffern zu ändern (wir empfehlen mindestens 8 Ziffern).**
- Erst nach dieser Änderung ist es möglich, den Signaturschlüssel zu nutzen und damit eine Signatur auszuführen. Werden Sie bei der ersten Benutzung Ihrer Signaturkarte nicht zur Änderung der PIN2 aufgefordert oder wird die Ihnen mitgeteilte PIN2 nicht akzeptiert oder Ihre Transport-PIN mehr als 5-stellig ist, ist Ihre Signaturkarte möglicherweise vorher manipuliert worden. Es besteht die Möglichkeit, dass jemand Ihre Signaturkarte benutzt hat, bevor sie Ihre Karte erhalten haben. **PIN1 (Card-PIN) ist von dieser Regelung nicht betroffen.**

Unser Supportcenter unterstützt Sie gern bei der Handhabung der PINs (Kontakt siehe letzte Seite).

7.2 Die PUK

Die Signaturkarten von D-TRUST, werden mit zwei so genannten PUKs ausgeliefert. Dabei handelt es sich um spezielle PINs, mit deren Hilfe Sie den Fehlbedienungszähler von PIN1 (Card-PIN) und PIN2 (Signatur-PIN) zurücksetzen können. Das bedeutet: Wurde eine der beiden PINs der Signaturkarte aufgrund einer dreimaligen Fehleingabe der entsprechenden PIN gesperrt (Fehlermeldung Karte: „Karte geblockt"), haben Sie durch die Eingabe der entsprechenden PUK die Möglichkeit, die Karte wieder zu entsperren. **Eine Änderung der bestehenden PINs durch die Eingabe der PUK ist nicht möglich.** Die Anzahl der Entsperrvorgänge durch die PUK ist auf 10 Versuche limitiert.

Kann die Karte nicht erfolgreich entsperrt werden, kann nur – kostenpflichtig – eine Austauschkarte beantragt werden.
Unser Supportcenter unterstützt Sie gern bei der Handhabung der PINs und PUKs (Kontakt siehe letzte Seite).

7.3 Signaturprüfung

Zur Überprüfung einer elektronischen Signatur benötigen Sie eine Signaturprüfsoftware.
Selbsttätig überprüft die Signatursoftware die Gültigkeit und die Herkunft des Zertifikates sowie die Unversehrtheit der signierten Daten und gibt das Ergebnis der Prüfung in einer Meldung aus. Der rechtlich maßgebliche Inhalt des Dokumentes wird dabei wieder in einer Darstellungsweise angezeigt, die Bestandteil Ihrer Signaturanwendungssoftware ist und gegen unbemerkte Manipulation gesichert ist.
Die Sicherheit Ihrer Signaturanwendungssoftware ist nur gewährleistet, wenn Sie Ihren Computer und das Betriebssystem gegen Bedrohungen absichern. Dazu verwenden Sie insbesondere Virenschutzprogramme in der jeweils aktuellsten Version.

7.4 Notwendigkeit zur Signaturerneuerung

Der Sicherheitswert von qualifiziert signierten, gesiegelten oder zeitgestempelten Daten kann durch technische Entwicklungen geringer werden. Deshalb müssen solche Daten rechtzeitig unter Verwendung der jeweilig aktuellen Signaturtechnologie erneut elektronisch signiert, gesiegelt oder zeitgestempelt werden.

7.5 Anhang – Verpflichtungserklärung / Subscriber Agreement

Im Anhang an dieses Dokument finden Sie die Verpflichtungserklärungen (Subscriber Agreement).

ANHANG

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
  - iv. ich Kenntnis über die Kompromittierung der ausstellenden CA erlange,
  - v. das betreffende Zertifikat gesperrt wurde oder
  - vi. 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 sperren:**

d) Verdacht oder Gewissheit der Kompromittierung des privaten Schlüssels

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

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

Wenn Sie Ihr Zertifikat sperren 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 Sperren 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 bei der Sperrung 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: Die Sperrung 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:
  c. Wenn Sie Operator sind, sperren Sie bitte direkt über die Online-Sperrfunktion des Certificate Service Managers (CSM)
  d. 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) sperren möchten, nutzen Sie bitte folgende Sperrwege:
  c. Wenn Sie berechtigter Zertifikatsnehmer sind, können Sie Ihren Heilberufsausweis (Sperrantragsteller_AS) über das Antragsportal https://ehealth.d-trust.net/antragsportal sperren.
  d. Zur Sperrung 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) sperren.

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