PKI Disclosure Statement

PKI-Nutzerinformationen

ENGLISH

DEUTSCH

PKI DISCLOSURE STATEMENT

This document provides users of the PKI services with useful information about the general conditions for trust services offered by D-TRUST GmbH, Bundesdruckerei's trust service provider.

Version: 1.4
Date of issue: 01.12.2018
Effective date: 01.12.2018
Classification: – Public –

PUBLISHING DETAILS

Trademarks

Product names 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: 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:** Bundesdruckerei GmbH Kommandantenstraße 18 10969 Berlin, Germany Tel.: + 49 (0) 30 / 25 98 - 0 info@bdr.de support@bdr.de www.bundesdruckerei.de

1.2 Revocation of certificates

Have your certificates revoked:

- if you lost your signature or seal card or if you believe that your card could have been manipulated by third parties;
- if data in the certificate becomes invalid, for example, due to a change in name or if you have left the organization which is indicated in the certificate;
- 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 chapter 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:

- **Online:** You can request revocation electronically via the revocation website (https://my.d-trust.net/sperren). To do this, you will need your card ID/request ID and your revocation password.
- **In writing:** Sign your revocation request by hand and send it to our revocation service at the following address:

  Bundesdruckerei GmbH
  c/o D-TRUST GmbH
  Sperrdienst
  Kommandantenstraße 15
  10969 Berlin, Germany

  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.
- **By phone:** Until 31 March 2019, you can also revoke your certificate by calling us from 7am to 4pm and stating your revocation password.

  For qualified certificates for website authentication (QWAC), please use the online revocation function of the Certificate Service Manager (CSM).

Retroactive revocation is generally not possible. Temporary revocation or suspension of certificate is not offered. 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.

Revocation application by telephone	Revocation application by letter	Electronic revocation request
▪ Name of the caller ▪ Name of the certificate owner if the caller is not the holder ▪ Request/card ID, if possible ▪ Revocation password	▪ Name of the sender ▪ Name of the certificate owner if the sender is not the holder ▪ Request/card ID, if possible ▪ Revocation password, if possible ▪ The signature of the sender	▪ Request/card ID ▪ Revocation password Also possible ▪ SMS-TAN ▪ For QWACs: Access to the CSM

2. Qualified trust services

2.1 Types of qualified trust services offered

Trust service	Applicable policies	Relevant OIDs[1]
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
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
Qualified certificates for website authentication (qualified SSL/TLS certificate)	▪ ETSI 319 411-2 QCP-w ▪ Certificate Policy of D-TRUST GmbH ▪ Certification Practice Statement of the D-TRUST CSM PKI	▪ 0.4.0.194112.1.4 ▪ 1.3.6.1.4.1.4788.2.202.1

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.

2.2 Possible restrictions in qualified certificates and archiving period

Trust service	Possible restrictions	Archiving period
Qualified certificates for individuals on a secure signature creation device	Certificate restrictions (for instance, test certificates, monetary limit), if any, are	The German Trusted Services Act (Vertauensdienstegesetz) in conjunction with the German

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

(signature card)	shown in the certificate itself.	Trust Services Regulation (Vertrauensdiensteverordnung) requires permanent storage of certificate data.
Qualified certificates for legal entities on a secure signature creation device (seal card)	Certificate restrictions (for instance, test certificates, monetary limit), if any, are shown in the certificate itself.	The archiving period is product-specific and totals at least 10 years after the certificate has expired.
Qualified certificates for website authentication (qualified SSL/TLS certificate)	Certificate restrictions (for instance, test certificates), if any, are shown in the certificate itself.	The archiving period is product-specific and totals at least 7 years after the certificate has expired.

2.3 Legal information

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 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257 of 28 August 2014), in short: eIDAS Regulation.
The German Trusted Services Act (VDG, Vertauensdienstegesetz) implementing the eIDAS Regulation demands that the trust service provider informs you of the legal effect of the trust services offered. We would like to inform you in the following section of the legal effect of our qualified trust services.

2.3.1 Legal effect of the electronic signature

A qualified electronic signature has the same legal effect as a hand-written signature. A qualified electronic signature based on a qualified certificate issued in a Member State is recognized as a qualified electronic signature in all other Member States.
Pursuant to sections 126 and following of the German Civil Code [§§ 126 ff BGB], the legal "qualified electronic signature" has the same effect as a hand-written signature under civil law if the signed document additionally bears the signatory's name ("electronic form") and if such electronic form is not explicitly ruled out by law. Such an exclusion at present (September 2001) concerns the termination and modification of employment contracts (section 623 of the German Civil Code), the issuing of certificates and references for employees (section 630) as well as promises of life annuities (section 761), declarations of suretyship (section 766), promises (section 780) and declarations of acknowledgement (section 781).

2.3.2 Section 371a of the German Code of Civil Procedure [§ 371a ZPO] Evidentiary value of electronic documents

The provisions concerning the evidentiary value of private instruments are analogously applicable to private electronic documents which are provided with a qualified electronic signature. The prima-facie evidence of authenticity of a statement available in electronic form which is based on the verification of the qualified electronic signature according to Article 32 of the eIDAS Regulation (EU) No 910/2014 can only be questioned by facts which cast serious doubt on whether the statement was made by the person responsible for this.
This means that anybody who can use your signature card – i.e. anybody who has the card and the PIN – can perform acts which are legally binding upon you.
Any electronic signature generated using your digital signature key is generally deemed to be yours if your certificate was valid at the time it was generated and if there are no facts which disprove the presumption that you deliberately generated the electronic signature.

3. Obligations of subscribers[2]

Trust service	URL of the subscriber agreement	URL of the Certificate Practice Statement
Qualified certificates for natural persons on a secure signature creation device (signature card)	non-SSL	Root PKI CPS
Qualified certificates for legal entities on a secure signature creation device (seal card)	non-SSL	Root PKI CPS
Qualified certificates for website authentication (qualified SSL/TLS certificate)	SSL	CSM PKI CPS

4. 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:
  http://www.d-trust.net/repository
- D-TRUST Roots and CRLs:
  https://www.bundesdruckerei.de/en/Roots-and-CRLs
- Privacy policy:

  http://www.d-trust.net/internet/files/Info_DSGVO_P.pdf
- General Terms and Conditions of D-TRUST GmbH:
  http://www.d-trust.net/internet/files/agb_d_trust_d_0.pdf
- Trusted list of the Federal Network Agency:
  https://www.nrca-ds.de/en/tsl_e.htm

5. General Information

5.1 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.

5.2 Provision of certification and trust services by D-TRUST GmbH

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

[2] The documents are linked in the D-TRUST repository: http://www.d-trust.net/repository

5.3 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.

5.4 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.

5.5 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.

5.6 Place of performance

The place of performance for the generation of the certificate is Berlin for both Bundesdruckerei and the customer.

6. Rules for the use of the electronic signature[3]

Anybody who can use your signature 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". Any electronic signature generated with your digital signature key is generally attributed to you.
It is therefore extremely important that you carefully protect your signature card and your PIN against unauthorized access.
Below we have compiled some rules for the secure use of the signature card.

[3] An electronic seal is the electronic signature of a legal entity. This document therefore uses the term "signature" also with respect to seals.

6.1 PIN

Trust service	Possible PINs	Type of PIN
Qualified certificates for individuals on a secure signature creation device (signature card)	PIN 1 PIN 2	You receive a PIN letter.
Qualified certificates for legal entities on a secure signature creation device (seal card)	PIN 2	You receive a PIN letter.
Qualified certificates for website authentication (qualified SSL/TLS certificate)	PIN 1	The PIN is generated by the subscriber 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 centre staff will be pleased to assist you if you have any questions concerning the use of your PINs (for contact details, please see section 1.1).

6.2 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 centre 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 section 1.1).

6.3 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.

6.4 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.

6.5 Annex – Subscriber agreement

This annex contains the subscriber agreements for signature and seal cards (non-SSL) and/or qualified website certificates (SSL).

PKI-NUTZERINFORMATION (PKI DISCLOSURE STATEMENT)

Dieses Dokument informiert den Nutzer von PKI-Dienstleitungen der D-TRUST GmbH, dem Trustcenter der Bundesdruckerei GmbH, über die wesentlichen Rahmenbedingungen der angebotenen Vertrauensdienste

Version: 1.4
Erscheinungsdatum: 01.12.2018
Datum des Inkrafttretens: 01.12.2018
Klassifizierung: - öffentlich-

IMPRESSUM

Warenzeichen

Warennamen 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: 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:** Bundesdruckerei GmbH Kommandantenstraße 18 10969 Berlin Tel.: + 49 (0) 30 / 25 98 - 0 info@bdr.de support@bdr.de www.bundesdruckerei.de

1.2 Sperrung von Zertifikaten

Lassen Sie Ihre Zertifikate sperren,

- wenn Sie Ihre Signatur- oder Siegelkarte verloren haben oder wenn Sie den Verdacht haben, dass Ihre Karte von Dritten manipuliert worden sein könnte.
- wenn Angaben im Zertifikat ungültig werden, z. B. in Folge einer Namensänderung oder dem Ausscheiden aus der im Zertifikat angegebenen Organisation.
- 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 sperren zu lassen:

- **Online:** Sie beantragen die Sperrung elektronisch über die Sperr-Webseite (https://my.d-trust.net/sperren). Hierfür benötigen Sie Ihre Karten-ID/Antrags-ID und Ihr Sperrpasswort.
- **Schriftlich:** Sie richten einen handschriftlich unterschriebenen Sperrauftrag an unseren Sperrdienst.
  Senden Sie diesen an die folgenden Adresse:

  Bundesdruckerei GmbH c/o D-TRUST GmbH
  Sperrdienst
  Kommandantenstraße 15
  10969 Berlin

  Falls Ihr Sperrauftrag anhand Ihrer Unterschrift eindeutig identifiziert werden kann, wird die Sperrung an dem Tag durchgeführt, an dem das Schreiben beim Sperrdienst der D-Trust GmbH eingetroffen ist.
- **Telefonisch:** Sie haben noch bis zum 31.03.2019 von 7:00 Uhr – 16:00 Uhr die Möglichkeit, Ihr Zertifikat unter Angabe Ihres Sperrpasswortes telefonisch zu sperren.

  Für qualifizierte Webseitenzertifikate (QWAC) verwenden Sie bitte die Online-Sperrfunktion des Certificate Service Manager (CSM).

Eine rückwirkende Sperrung ist generell nicht möglich. Eine vorübergehende Sperrung bzw. Suspendierung von Zertifikaten wird nicht angeboten. Eine einmal vorgenommene Sperrung 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 sperren zu lassen.

Telefonischer Sperrauftrag	Schriftlicher Sperrauftrag	Elektronischer Sperrauftrag
▪ Name des Anrufers ▪ Name des Zertifikatinhabers, falls nicht Anrufer selbst ▪ wenn möglich Antrags-/Karten-ID ▪ Sperrpasswort	▪ Name des Absenders ▪ Name des Zertifikatinhabers, falls nicht Absender selbst ▪ wenn möglich Antrags-/Karten-ID ▪ wenn möglich Sperrpasswort ▪ Unterschrift des Absenders	▪ Antrags-/Karten-ID ▪ Sperrpasswort Weiterhin möglich ▪ SMS-TAN ▪ Für QWACs: Zugang zum CSM

2. Qualifizierte Vertrauensdienste

2.1 Angebotene Arten von qualifizierten Vertrauensdiensten

Vertrauensdienst	Anwendbare Richtlinien	Relevante OIDs[1]
Qualifizierte Zertifikate 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
Qualifizierte Zertifikate 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
Qualifizierte Zertifikate für Webseitenauthentifizierung (qualifiziertes SSL/TLS-Zertifikat)	▪ ETSI 319 411-2 QCP-w ▪ Zertifikatsrichtlinie der ▪ D-TRUST GmbH ▪ Certification Practice Statement der D-TRUST CSM PKI	▪ 0.4.0.194112.1.4 ▪ 1.3.6.1.4.1.4788.2.202.1

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.

2.2 Mögliche Beschränkungen in qualifizierten Zertifikaten und Archivierungszeitraum

Vertrauensdienst	mögliche Einschränkungen	Archivierungsdauer
Qualifizierte Zertifikate für natürliche Personen auf einer sicheren Signaturerstellungseinheit (Signaturkarte).	Mögliche Zertifikatsbeschränkungen sind im Zertifikat selbst ersichtlich (z.B. Testzertifikate, monetäre Beschränkung)	Das VDG in Verbindung mit dem VDV schreibt eine dauerhafte Speicherung der Zertifikatsdaten vor

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

Qualifizierte Zertifikate für juristische Personen auf einer sicheren Signaturerstellungseinheit (Siegelkarte).	Mögliche Zertifikatsbeschränkungen sind im Zertifikat selbst ersichtlich (z.B. Testzertifikate, monetäre Beschränkung)	Die Archivierungsdauer ist produktabhängig und beträgt mindestens 10 Jahre nach Ablauf der Gültigkeit des Zertifikats.
Qualifizierte Zertifikate für Webseitenauthentifizierung (qualifiziertes SSL/TLS-Zertifikat).	Mögliche Zertifikatsbeschränkungen sind im Zertifikat selbst ersichtlich (z.B. Testzertifikate)	Die Archivierungsdauer ist produktabhängig und beträgt mindestens 7 Jahre nach Ablauf der Gültigkeit des Zertifikats.

2.3 Rechtsbelehrung

Die Rechtswirkung der elektronischen Signatur, Siegel und Zeitstempel ist in Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73) kurz eIDAS Verordnung definiert.
Das Vertrauensdienstegesetz (VDG) zur Durchführung der eIDAS Verordnung verlangt, dass der Vertrauensdiensteanbieter Sie über die Rechtswirkung der angebotenen Vertrauensdienste informiert. In dem folgenden Absatz möchten wir Sie deshalb über die Rechtswirkung unsere qualifizierten Vertrauensdienste in Kenntnis setzen.

2.3.1 Rechtswirkung elektronische Signatur

Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Eine qualifizierte elektronische Signatur, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifizierte elektronische Signatur anerkannt.
Nach §§126ff BGB ist die gesetzliche „qualifizierte elektronische Signatur" der handschriftlichen Unterschrift der gesetzlichen Schriftform des Privatrechts gleichgestellt, wenn das signierte Dokument um den Namen des Unterzeichnenden ergänzt („elektronische Form") und diese elektronische Form vom Gesetz nicht explizit ausgeschlossen wird. Ein solcher Ausschluss betrifft derzeit (Sept. 2001) die Kündigung und Änderung von Arbeitsverhältnissen (§623 BGB), die Erteilung von Arbeitszeugnissen (§630 BGB) sowie Leibrentenversprechen (§761 BGB), Bürgschaftserklärungen (§766 BGB), Versprechen (§780) und Anerkennungserklärungen (§781 BGB).

2.3.2 §371a ZPO Beweiskraft elektronischer Dokumente

Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung der qualifizierten elektronischen Signatur nach Artikel 32 der eIDAS Verordnung (EU) Nr. 910/2014 ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung von der verantwortenden Person abgegeben worden ist.
Dies bedeutet, wer die Möglichkeit hat Ihre Signaturkarte zu benutzen, d.h. die Karte und die PIN besitzt, kann rechtskräftig für Sie agieren.
Jede mit Ihrem digitalen Signaturschlüssel erzeugte elektronische Signatur wird grundsätzlich Ihnen zugeordnet, falls Ihr Zertifikat zum Zeitpunkt der Erzeugung gültig war und nicht irgendwelche andere Fakten die Vermutung widerlegen, dass die elektronische Signatur von Ihnen willentlich erzeugt wurde.

3. Pflichten der Zertifikatnehmer[2]

Vertrauensdienst	URL der Verpflichtungserklärung	URL des Certificate Practice Statement
Qualifizierte Zertifikate für natürliche Personen auf einer sicheren Signaturerstellungseinheit (Signaturkarte).	non-SSL	Root PKI CPS
Qualifizierte Zertifikate für juristische Personen auf einer sicheren Signaturerstellungseinheit (Siegelkarte).	non-SSL	Root PKI CPS
Qualifizierte Zertifikate für Webseitenauthentifizierung (qualifiziertes SSL/TLS-Zertifikat)	SSL	CSM PKI CPS

4. 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:
  http://www.d-trust.net/repository
- D-TRUST Roots und CRLs:
  https://www.bundesdruckerei.de/de/2825-repository
- Datenschutzerklärung:

  http://www.d-trust.net/internet/files/Info_DSGVO_P.pdf
- D-TRUST AGB:
  http://www.d-trust.net/internet/files/agb_d_trust_d_0.pdf
- Vertrauensliste der Bundesnetzagentur:
  https://www.nrca-ds.de/en/tsl_e.htm

5. Allgemeine Informationen

5.1 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.

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

[2] Die Dokumente sind im D-TRUST Repository verlinkt: http://www.d-trust.net/repository

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

5.3 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.

5.4 Anwendbares Recht

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

5.5 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.

5.6 Erfüllungsort

Erfüllungsort der Zertifikatserstellung für die Bundesdruckerei und den Kunden ist Berlin.

6. Regeln für den Umgang mit der elektronischen Signatur[3]

Wer die Möglichkeit hat, Ihre Signaturkarte zu benutzen, d.h. Ihre Karte hat und Ihre PIN kennt, kann rechtskräftig für Sie agieren, da er im Besitz Ihrer „digitalen Unterschrift" ist. Jede mit Ihrem digitalen Signaturschlüssel erzeugte elektronische Signatur wird grundsätzlich Ihnen zugeordnet.
Es ist daher außerordentlich wichtig, dass Sie Ihre Signaturkarte und Ihre PIN mit größter Sorgfalt vor unbefugtem Zugriff schützen.
Wir haben einige Regeln für den sicheren Umgang mit der Signaturkarte zusammengestellt.

[3] Ein elektronisches Siegel ist die elektronische Signatur einer Juristischen Person. In diesem Dokument wird der Begriff Signatur deshalb auch für Siegel verwendet

6.1 Die PIN

Vertrauensdienst	Mögliche PINs	Art der PIN
Qualifizierte Zertifikate für natürliche Personen auf einer sicheren Signaturerstellungseinheit (Signaturkarte).	PIN 1 PIN 2	Sie erhalten einen PIN-Brief.
Qualifizierte Zertifikate für juristische Personen auf einer sicheren Signaturerstellungseinheit (Siegelkarte).	PIN 2	Sie erhalten einen PIN-Brief.
Qualifizierte Zertifikate für Webseitenauthentifizierung (qualifiziertes SSL/TLS-Zertifikat)	PIN 1	PIN wird durch den Zertifikatnehmer 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 eine 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).

6.2 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).

6.3 Signaturprüfung

Zur Überprüfung einer elektronischen Signatur benötigt 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.

6.4 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.

6.5 Anhang – Verpflichtungserklärung / Subscriber Agreement

Im Anhang an dieses Dokument finden Sie die Verpflichtungserklärungen (Subscriber Agreement) für Signatur- und Siegelkarten (non-SSL) bzw. qualifizierte Webseitenzertifikate (SSL)