BUNDESDRUCKEREI

Zertifikatsrichtlinie der D-TRUST GmbH

Version 3.4

D-TRUST EINE MARKE DER BUNDESDRUCKEREI

COPYRIGHT UND NUTZUNGSLIZENZ

Zertifikatsrichtlinie der D-TRUST GmbH
©2018 D-TRUST GmbH

Anfragen zu einer sonstigen, in der vorgenannten Lizenz nicht enthaltenen Nutzungsart dieser CP der D-TRUST GmbH sind zu richten an:

D-TRUST GmbH
Kommandantenstr. 15
10969 Berlin, Germany
Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

Dokumentenhistorie

Version	Datum	Beschreibung
2.0	23.02.2015	Im Rahmen der Umstrukturierung der Zertifikatsrichtlinie der D-TRUST GmbH, wurde die Version des Dokumentes auf 2.0 hochgezählt. Die Dokumentenhistorie der Zertifikatsrichtlinie bis zu diesem Zeitpunkt kann in der Version 1.12 vom 17.11.2014 nachgelesen werden. ▪ Es wurden Inhalte, die die konkrete Umsetzung betreffen in die jeweilige CPS verschoben. Es ist aus dem jeweiligen Zertifikat zu erkennen unter welcher CPS dieses Zertifikat entstanden ist.
2.1	05.10.2015	▪ Editorische Änderungen und Hinweis auf Zertifikate ohne CPS-Eintrag
2.2	03.10.2016	▪ Umstellung auf EN 319 411-1
3.0	01.01.2017	▪ Einführung von qualifizierten Produkten gemäß EN 319 411-2 und eIDAS
3.1	01.04.2017	▪ Einführung eines qualifizierten Zeitstempeldienstes gemäß EN 319 421
3.2	01.10.2017	▪ Editorische Änderungen und Hinweise auf das Vertrauensdienstegesetz (VDG)
3.3	28.03.2018	▪ Editorische Änderungen und Angleichung an Mozilla Root Store Policy 2.5 ▪ Anpassung Nutzungslizenz an „Creative Commons Attribution" ▪ Ergänzung der OID für die PKI der E.ON SE und der Uniper
3.4	08.05.2018	▪ Anpassung vom Abschnitt 9.4 an die Datenschutzgesetzänderung zum 25.05.2018

Inhaltsverzeichnis

1. Einleitung

1.1 Überblick

Dieses Dokument beschreibt die Zertifikatsrichtlinie (engl. *Certificate Policy*, im Folgenden CP genannt) der von D-TRUST GmbH betriebenen Vertrauensdienste.

1.1.1 Vertrauensdiensteanbieter

Der Vertrauensdiensteanbieter (Trust Service Provider, im Folgenden TSP genannt) ist – auch im juristischen Sinne – die

D-TRUST GmbH
Kommandantenstr. 15
10969 Berlin.

Der TSP kann Teilaufgaben an Partner oder externe Anbieter auslagern.

Für die Einhaltung der Verfahren im Sinne dieses Dokuments bzw. etwaiger gesetzlicher oder zertifizierungstechnischer Anforderungen an den TSP, bleibt der TSP, vertreten durch die Geschäftsführung oder deren Beauftragte, verantwortlich.

Die D-TRUST GmbH stellt auch Zertifikate für eigene Zwecke aus. Hierbei werden ebenfalls die entsprechenden gesetzlichen bzw. zertifizierungstechnischen Anforderungen eingehalten.

1.1.2 Über dieses Dokument

Diese CP stellt Vorgaben und Anforderungen an die PKI und regelt somit den Zertifizierungsprozess während der gesamten Lebensdauer der End-Entity-Zertifikate (EE-Zertifikate) sowie das Zusammenwirken, Rechte und Pflichten der PKI-Teilnehmer[1].

Die gesamte CP ist rechtsverbindlich, soweit dies im Rahmen der deutschen bzw. europäischen Gesetzgebung zulässig ist. Sie enthält Aussagen über Pflichten, Gewährleistung und Haftung für die PKI-Teilnehmer. Soweit nicht ausdrücklich genannt, erfolgen auf Basis dieser CP keine Zusicherungen oder Garantien im Rechtssinne.

Die Kenntnis der in dieser CP beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Zertifikatnutzern, Vertrauen in die Komponenten und PKI-Teilnehmer aufzubauen und Entscheidungen zu treffen, inwieweit das durch die PKI gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

Die Struktur dieses Dokumentes ist eng an den Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" angelehnt, um eine einfache Lesbarkeit und Vergleichbarkeit mit anderen CPs zu erreichen.

[1] Im Interesse einer leichteren Lesbarkeit wird in diesem Dokument auf die weibliche Form der PKI-Teilnehmer und sonstigen genannten Personengruppen verzichtet. Es wird gebeten, die weibliche Form jeweils als eingeschlossen anzusehen.

1.1.3 Eigenschaften der PKI und Notation

Diese Regelungen sind in dem zum Zertifikat gehörenden Certification Practice Statement (im Folgenden CPS genannt) beschrieben.

Die D-TRUST GmbH bietet unter dieser Policy diverse Produkte an, die die Anforderungen aus dieser Zertifikatsrichtlinie in ihren speziellen Produkteigenschaften erfüllen. Die Dienste werden nach Möglichkeit barrierefrei angeboten.

Die Erfüllung dieser Anforderungen wird in einem CPS beschrieben, welches zu einem Produkt oder einer Produktgruppe zugeordnet werden kann.

Die D-TRUST GmbH verwendet mehrere CPS-Dokumente. Welches CPS zu dem jeweiligen Zertifikat gehört, ist in jedem Zertifikat im Zertifikatsfeld „cpsURI" ersichtlich.

Vertrauensdienste die mit dem Zusatz „qualifiziert" genannt werden, sind qualifizierte Vertrauensdienste im Sinne der eIDAS. Vertrauensdienste die nicht mit dem Zusatz „qualifiziert" genannt werden, sind nichtqualifizierte Vertrauensdienste im Sinne der eIDAS.

Sollte in dem vorliegenden Zertifikat kein CPS hinterlegt sein, so liegt die Umsetzung der in dieser CP geforderten Regelungen im Ermessen des TSP. Zertifikate, in denen keine CPS eingetragen wurde, unterliegen keiner Zertifizierung im Sinne EN 319 411-1, EN 319 411-2, bzw. der eIDAS.

Dienste, die mit Zertifikaten ohne CP (PolicyOID) oder/und CPS-Eintrag (cpsURI) betrieben werden, sind im eigentlichen Sinne keine Vertrauensdienste im Sinne der eIDAS sondern Dienste für technische Verfahren.

Die Zugehörigkeit der Zertifikate zu dieser Policy ist durch die eingetragen OID zu erkennen:

Qualifizierte Personenzertifikate auf qualifizierter Signaturerstellungseinheit
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-n-qscd wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.1

Qualifizierte Siegelzertifikate auf qualifizierter Signaturerstellungseinheit
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-l-qscd wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.2

Qualifizierte Webseitenzertifikate (SSL/TLS)
Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-w wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.150.4

Nichtqualifizierte Webseitenzertifikate (SSL/-TLS)
Für die EV-Policy-OID wird die Verwendung bei EV-Zertifikaten gemäß EN 319 411-1 und [GL-BRO] vergeben: 1.3.6.1.4.1.4788.2.202.1

Für OV-Zertifikate gemäß EN 319 411-1 wird die allgemeine Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.1

Nichtqualifizierte Zertifikate
Für Zertifikate der Zertifizierungsklasse EN 319 411-1 LCP wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.2

Für Zertifikate der E.ON SE PKI der Zertifizierungsklasse EN 319 411-1 LCP wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.210.1

Für Zertifikate der Uniper PKI der Zertifizierungsklasse EN 319 411-1 LCP wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.212.1

Für Zertifikate der Zertifizierungsklasse EN 319 411-1 NCP wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.200.3

Für Zertifikate ohne Zertifizierungsklasse wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.500[2]

Für Zertifikate, die ausschließlich zu Testzwecken ausgestellt wurden, wird die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.2.2[2]

Alle anderen Zertifikate unter dieser Policy enthalten die Policy-OID: 1.3.6.1.4.1.4788.2.200.1

Nichtqualifizierte Zertifikate der Cloud PKI
Die geheimen Schlüssel für Zertifikate aus der Cloud PKI verbleiben in der gesicherten Umgebung des Trust Service Provider. Für solche Zertifikate werden zusätzlich die folgenden OIDs vergeben.

Für Zertifikate der Zertifizierungsklasse EN 319 411-1 LCP wird zusätzlich die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.250.1

[2] Hierbei handelt es sich um Zertifikate, die alleine für technische Anwendungen oder Testzwecke vorgesehen sind. Es handelt sich somit NICHT um einen Vertrauensdienst im Sinne der eIDAS.

Qualifizierte Zertifikate der Cloud PKI
Die geheimen Schlüssel für Zertifikate aus der Cloud PKI verbleiben in der gesicherten Umgebung des Trust Service Provider. Für solche Zertifikate werden zusätzlich die folgenden OIDs vergeben.

Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-n-qscd wird zusätzlich die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.100.1

Für Zertifikate der Zertifizierungsklasse EN 319 411-2 QCP-l-qscd wird zusätzlich die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.100.2

Für den qualifizierten Zeitstempeldienst gemäß EN 319 421 BTSP wird zusätzlich die folgende Policy-OID vergeben: 1.3.6.1.4.1.4788.2.100.3

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Zertifikatsrichtlinie der D-TRUST GmbH
Kennzeichnung (OID):	Dieses Dokument erhält die Policy-OID: 1.3.6.1.4.1.4788.2.200.1
Version	3.4

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Die Zertifizierungsstellen (Certification Authority – CA) stellen Zertifikate sowie Sperrlisten aus. Möglich sind folgende Arten von Zertifikaten:

- Personenzertifikate für natürliche Personen (EE-Zertifikat),
- Siegelzertifikate für juristische Personen (EE-Zertifikat), Gruppenzertifikate für Personengruppen, Funktionen und IT-Prozesse (EE-Zertifikat),
- Maschinenzertifikate für IT-Prozesse und Kommunikationsverbindungen (SSL-Zertifikate / EE-Zertifikat), die einen technischen Einsatzzweck haben aber auch das End-Entity-System (subject) entsprechend authentisieren können,
- Maschinenzertifikate für IT-Prozesse und Kommunikationsverbindungen, die einen rein technischen Einsatzzweck haben. Zertifikatsinhalte werden hierbei nicht verifiziert,
- Zertifizierungsinstanzen (nachgeordnete CA-Zertifikate des TSP) und
- Dienstezertifikate für juristische Personen (EE-Zertifikat sowie Dienstezertifikate für Zeitstempel) unter denen unter anderem auch der qualifizierte Zeitstempel ausgestellt wird.

Die Wurzelinstanzen stellen Zertifikate ausschließlich mit der Erweiterung basicConstraints: cA=TRUE (CA-Zertifikat) aus. Untergeordnete CAs stellen EE-Zertifikate und/oder weitere CA-Zertifikate aus. Die Zertifizierungsstelle ist in den ausgestellten Zertifikaten und CRLs namentlich im Feld issuer benannt.

Die Zertifizierungsstelle betreibt als TSP Dienste im Sinne Kapitel III Verordnung (EU) Nr. 910/2014 i.V.m. (52) der Erwägungsgründe (Service für fernausgelöste Signaturen)

1.3.2 Registrierungsstellen (RA)

Diese Regelungen sind in der zum Zertifikat gehörenden CPS beschrieben.

1.3.3 Zertifikatnehmer (ZNE) und Endanwender (EE)

Diese Regelungen sind in der zum Zertifikat gehörenden CPS beschrieben.

1.3.4 Zertifikatnutzer (ZNU)

Zertifikatnutzer (englisch *relying parties*) sind natürliche oder juristische Personen, die die Zertifikate der D-TRUST GmbH nutzen und Zugang zu den Diensten des TSP haben.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Zertifikate, die dieser Certificate Policy unterliegen, können im Allgemeinen für alle Zwecke verwendet werden. Der Zertifikatsnehmer ist dafür verantwortlich, Zertifikate so zu verwenden, dass die Verwendung den anwendbaren gesetzlichen Bestimmungen entspricht. Dies gilt insbesondere für die Einhaltung der jeweils anwendbaren Ausfuhr- oder Einfuhrbestimmungen.

Weitere Regelungen sind in dem zum Zertifikat gehörenden CPS beschrieben.

1.4.2 Verbotene Verwendungen von Zertifikaten

Die Verwendung von Zertifikaten für Dienste und Systeme, die bei Störungen oder Ausfällen zu großen materiellen oder immateriellen Schäden führen sowie Schäden an Leib und Leben verursachen können, ist nicht gestattet.

Hierzu zählen u.a. Atomkraftwerke, Chemieproduktionsanlagen oder Luftfahrtsysteme sowie insbesondere Dienste und Systeme, die in Zusammenhang mit kritischen Infrastrukturen stehen.

Hiervon abweichende Regelungen können im Einzelnen mit dem Vertrauensdiensteanbieter schriftlich vereinbart werden.

Weitere Regelungen sind in dem zum Zertifikat gehörenden CPS beschrieben.

1.4.3 Verwendung von Dienstezertifikaten

Der TSP verwendet Dienstezertifikate zur Erbringung von Vertrauensdienste gemäß [eIDAS]. Dienstezertifikate werden durch den TSP selbst und zur eigenen Verwendung ausgestellt. Sie unterliegen den Anforderungen der jeweilig anwendbaren Zertifizierung.

Zu den Verwendungsarten zählen:

- CA-Zertifikate zur CA- und Zertifikatserstellung,

- Signatur von Sperrauskünften[3]
- Signatur von Zeitstempeln[4]

1.5 Aktualisierung der CP/des CPS

1.5.1 Zuständigkeit für das Dokument

Diese CP wird durch die D-TRUST GmbH gepflegt und aktualisiert. Der Beauftragte der Geschäftsführung übernimmt die Abnahme des Dokuments.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

D-TRUST GmbH
Redaktion CP und CPS
Kommandantenstr. 15

10969 Berlin, Germany

Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

1.5.3 Verträglichkeit von CPs fremder CAs mit dieser CP

In dieser CP werden Mindestanforderungen beschrieben, die von allen PKI-Teilnehmern erfüllt werden müssen.

Sowohl in CA- als auch in EE-Zertifikaten können weitere CPs über Policy-OIDs referenziert werden, die dieser CP nicht widersprechen. Die Referenz einer Policy-OID in den Zertifikatserweiterungen bestätigt seitens der CA die Kompatibilität der Zertfizierungspraktiken mit der referenzierten CP (z. B. NCP 0.4.0.2042.1.1 gemäß EN 319 411-1).

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Betroffene Dritte *(Third parties concerned)*	Enthält ein Zertifikat Angaben über die Vertretungsmacht des Zertifikatnehmers für dritte Personen, so werden diese Stellen als „Betroffene Dritte" bezeichnet.
CA-Zertifikat *(CA certificate)*	das für eine Zertifizierungsinstanz ausgestellte Zertifikat zum Signaturschlüssel der CA
Certification Authority (CA)	Instanz der Root PKI, siehe Abschnitt 1.3.1.
Certificate Policy (CP)	Zertifikatsrichtlinie.

[3] OCSP-Auskünfte werden durch gesonderte OCSP-Dienstezertifikate signiert.

[4] Zeitstempel werden durch gesonderte Dienstezertifikate signiert.

Certification Practice Statement (CPS)	Umsetzungserklärung der CA
Certificate Service Manager (CSM)	Webanwendung zur Ausstellung fortgeschrittener Zertifikate
Cross-Zertifikat	Zertifikat, das verwendet wird, um andere CAs für vertrauenswürdig zu bestätigen.
D-TRUST Root CA	Wurzelzertifizierungsstelle, siehe Abschnitt 1.3.1.
D-TRUST-Root-PKI	Von der D-TRUST GmbH betriebene PKI.
Distinguished Name	Ein aus mehreren Namensbestandteilen bestehender technischer Name, der in Zertifikaten die ausstellende CA und/oder den Zertifikatnehmer innerhalb der Root PKI eindeutig beschreibt. Der Distinguished Name ist im Standard [X.501] definiert.
EE-Zertifikat	Siehe End-Entity-Zertifikat.
Elektronisches Siegel	Ein elektronisches Siegel dient als Nachweis, dass ein elektronisches Dokument von einer juristischen Person ausgestellt wurde und belegt den Ursprung und die Unversehrtheit des Dokuments.
Endanwender *(End-Entity /Subject)*	*Subject*, die Identität des Endanwenders ist mit dem Zertifikat und dem zugehörigen Schlüsselpaar verknüpft, siehe auch Abschnitt 1.3.3.
End-Entity-Zertifikat	Zertifikat, das nicht zum Zertifizieren anderer Zertifikate oder CRLs verwendet werden darf.
EV-Zertifikate	Zertifikat mit erweiterter Validierung des Zertifikatsnehmers (extended validation)
Postident Basic	Verfahren zur Identifizierung, angeboten von der Deutschen Post AG.
Qualifizierter Vertrauensdienst	Elektronischer Dienst entsprechend Art. 3 Abs. 17 eIDAS
Qualifiziertes Zertifikat	ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat, das die Anforderungen des Anhangs I der eIDAS erfüllt
Registrierungsstelle *(Registration Authority - RA)*	Registration Authority – (RA), Einrichtung der PKI, die die Teilnehmeridentifizierung vornimmt, siehe Abschnitt 1.3.2.
sign-me	Ist ein Service der Bundesdruckerei GmbH für fernausgelöste Signaturprozesse
Signaturkarte	Prozessorchipkarte, die für die Erzeugung elektronischer Signaturen und für andere PKI-Anwendungen benutzt werden kann.

Soft-PSE	Software Personal Security Environment, auch Software-Token genannt, enthalten das EE-Schlüsselpaar, das EE-Zertifikat sowie das Zertifikat der ausstellenden CA-Instanz.
Sperrberechtigter (Dritter) *(Third party authorized to revoke)*	Natürliche oder juristische Person, die zur Sperrung eines Zertifikats berechtigt ist.
Statusabfragedienst	PKI-Dienstleistung zur Online-Abfrage über den Status eines Zertifikats (OCSP)
Token	Trägermedium für Zertifikate und Schlüsselmaterial.
Trustcenter	Der Sicherheitsbereich in den Räumen der D-TRUST GmbH.
Trust Service Provider	Vertrauensdiensteanbieter (ehem. Zertifizierungs-diensteanbieter)
Verzeichnisdienst *(Repository service)*	PKI-Dienstleistung zum Online-Abrufen von Informationen, wie Zertifikaten und Sperrlisten, erfolgt i. d. R. über das LDAP-Protokoll.
Vertrauensdienst	Elektronischer Dienst entsprechend Art. 3 Abs. 16 eIDAS
Vertrauensdiensteanbieter *(Trust Service Provider - TSP)*	Anbieter von Vertrauensdiensten entsprechend Art. 3 Abs. 19 eIDAS
VideoIdent	Verfahren zur Identifizierung, angeboten von Identity TM AG
Zertifikatnehmer *(Subscriber)*	*Subscriber*, natürliche oder juristische Personen, die EE-Zertifikat beantragen und inne haben, siehe Abschnitt 1.3.3.
Zertifikatnutzer *(Relying Party)*	Relying Party, natürliche oder juristische Personen, die Zertifikate nutzen, siehe Abschnitt 1.3.4.
Zertifikatsrichtlinie	Certificate Policy – (CP), siehe Abschnitt 1.1.
Zertifizierungsdiensteanbieter	Anbieter von Zertifizierungsdiensten. Wird gleichbedeutend mit dem Begriff Vertrauensdiensteanbieter verwendet.
Zertifizierungsstelle	Certification Authority – (CA), Instanz der Root PKI, siehe Abschnitt 1.3.1.

1.6.2 Abkürzungen

BDSG	Bundesdatenschutzgesetz
BRG	Baseline Requirements Guidelines
CA	Certification Authority
CN	Common Name

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSGVO	Datenschutz-Grundverordnung
EVCP	Extended Validation Certificate Policy
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
HSM	Hardware Security Module
ISO	International Organization for Standardization
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
NetSec-CAB	Network Security Requirements- CA/Browser Forum
NCP	Normalized Certificate Policy
NCP+	Normalized Certificate Policy requiring a secure user device
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSE	Personal Security Environment
PUK	Personal Unblocking Key
QCP	Qualified Certificate Policy
QCP-l	Qualified Certificate Policy for Legal Persons
QCP-n	Qualified Certificate Policy for Natural Persons
QCP-w	Qualified Certificate Policy for Qualified Website-Authentication
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RFC	Request for Comment
SSCD	Secure Signature Creation Device
SUD	Secure User Device
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8

1.6.3 Referenzen

[AGB]	Allgemeine Geschäftsbedingungen der Bundesdruckerei GmbH für den Verkauf von Vertrauensdiensten der D-TRUST, aktuelle Version
[BRG]	Baseline Requirements des CA/Browser Form, CA/Browser Forum, Version 1.5.4, 04.10.2017
[CPS]	Certification Practice Statement der D-TRUST PKI, D-TRUST GmbH, aktuelle Version. Die geltende CPS wird im jeweiligen Zertifikat referenziert.
[eIDAS]	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
[ETSI-ALG]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites; ETSI TS 119 312 V1.2.1 (2017-05)
[EN 319 411-1]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; ETSI EN 319 411-1 V1.1.1 (2016-02)
[EN 319 411-2]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements; ETSI EN 319 411-2 V2.1.1 (2016-02)
[EN 319 412]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures; ETSI EN 319 412-1 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; ETSI EN 319 412-2 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons; ETSI EN 319 412-3 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates; ETSI EN 319 412-4 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements; ETSI EN 319 412-5 V2.2.1 (2016-02)
[GL-BRO]	Guidelines for Extended Validation Certificates, CA/Browser Forum, Version 1.6.7, 23. November 2017
[ISO 3166]	ISO 3166-1:1997: Codes for the representation of names of countries and their subdivisions - Part 1: Country codes
[NetSec-CAB]	CA / Browser Forum Network and Certificate System Security Requirements, Version 1.1, 01. Oktober 2017
[RFC 2247]	Using Domains in LDAP/X.500 Distinguished Names, January 1998

[RFC 3647] Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, November 2003

[RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mai 2008

[RFC 6818] Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013

[RFC 6960] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013

[RFC 6962] Certificate Transparency

[VDG] Vertrauensdienstegesetz (Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist)

[X.501] ITU-T RECOMMENDATION X.501, Information technology – Open Systems Interconnection – The Directory: Models, Version August 2005

[X.509] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der TSP veröffentlicht CRLs und Zertifikate im LDAP-Verzeichnis unter: ldap://directory.d-trust.net

Der vollständige zertifikatsspezifische Link ist dem Zertifikat selbst zu entnehmen.

Zusätzlich werden CA-Zertifikate auf den Webseiten der D TRUST GmbH veröffentlicht und können über den folgenden Link abgefragt werden:
https://www.bundesdruckerei.de/de/2825-repository

Der TSP stellt einen Online-Dienst (OCSP) zur Abfrage des Sperrstatus von Zertifikaten der D-TRUST zur Verfügung. Der Link ist dem Zertifikat zu entnehmen. Zusätzlich können Endanwender den Status ihrer Zertifikate über die folgende Webseite abfragen:

https://www.bundesdruckerei.de/de/2720-ocsp-abfrage.

Der Status der Zertifikate kann dort bis mindestens ein Jahr nach Ablauf der Gültigkeit der Zertifikate abgerufen werden. Diese CP und die Verpflichtungserklärung (Subscribers Agreement) können im PDF-Format von den Antragsseiten des TSP herunter geladen werden:

https://www.bundesdruckerei.de/de/2833-repository.

Kundenspezifisch können abweichende Verfahren für die Übermittlung der Verpflichtungserklärung vereinbart werden.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

2.3 Häufigkeit von Veröffentlichungen

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

2.4 Zugriffskontrollen auf Verzeichnisse

Zertifikate, Sperrlisten, CPS und CPs können öffentlich und unentgeltlich abgerufen werden. Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom TSP vorgenommen.

Weitere, nicht öffentliche Dokumente, können bei begründetem Interesse auf Nachfrage in den relevanten Teilen ausgegeben werden.

3. Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung für Zertifikate der D-TRUST GmbH erfolgt gemäß produkt- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Zertifizierungen (z.B. eIDAS, EN 319 411-1 oder EN 319 411-2)

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

4. Betriebsanforderungen

Die Betriebsanforderung für Zertifikate der D-TRUST GmbH erfolgt gemäß produkt- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Zertifizierungen (z.B. eIDAS, EN 319 411-1 oder EN 319 411-2)

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

5. Nicht-technische Sicherheitsmaßnahmen

Der TSP etabliert nicht-technische Sicherheitsmaßnahmen, die die Anforderungen aus [EN 319 411-1], [EN 319 411-2], [GL-BRO] und [eIDAS] erfüllen.

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

6. Technische Sicherheitsmaßnahmen

Der TSP etabliert technische Sicherheitsmaßnahmen, die die Anforderungen aus[EN 319 411-1], [EN 319 411-2], [GL-BRO] und [eIDAS] erfüllen. Aktuelle Angaben zu verwendeten Signatur- und Verschlüsselungsalgorithmen sind dem CPS Abschnitt 7.1.3 zu entnehmen.

Zertifikatnehmer und Zertifikatnutzer müssen vertrauenswürdige Computer und Software verwenden.

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

Die von CAs der D-TRUST-PKI ausgestellten Zertifikate erfüllen die Anforderungen der Standards ITU [X.509], IETF[RFC 5280] und IETF [RFC 6818], sowie der ETSI [ETSI EN 319 412]. Abweichungen werden ggf. in einem referenzierten Dokument beschrieben.

QCP
Die ausgestellten qualifizierten Zertifikate erfüllen die Anforderungen aus [eIDAS] Anhang I, III und IV.

EVCP
Die ausgestellten EV-Zertifikate erfüllen die Anforderungen aus[GL-BRO].

Die Profile sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

7.2 Sperrlistenprofile

Die ausgestellten Sperrlisten erfüllen die Anforderungen der Standards ITU [X.509], IETF [RFC 5280] und IETF [RFC 6818].

Die Profile sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

7.3 Profile des Statusabfragedienstes (OCSP)

Der Statusabfragedienst ist konform zum Standard [RFC 6960].

Die Profile sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

8. Auditierung und andere Prüfungen

Diese Regelungen sind im jeweiligen zum Zertifikat gehörenden CPS beschrieben.

9. Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

9.1.1 Preise für Zertifikate

Die Vergütung für die in diesem Dokument beschriebenen Leistungen sind in der Preisliste bzw. in der jeweiligen Vereinbarung festgelegt.

9.1.2 Preise für den Zugriff auf Zertifikate

Die Abfrage von Zertifikaten im Verzeichnisdienst ist kostenlos.

9.1.3 Preise für Sperrungen oder Statusinformationen

Sperrungen und das Abrufen von Statusinformationen sind kostenlos.

9.1.4 Preise für andere Dienstleistungen

Soweit angeboten siehe Preisliste bzw. in der jeweiligen Vereinbarung.

9.1.5 Regeln für Kostenrückerstattungen

Es gelten die jeweiligen Vereinbarungen mit dem Kunden bzw. [AGB].

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

Die D-TRUST GmbH verfügt über die nötigen Mittel sowie die finanzielle Stabilität, den Betrieb von Vertrauensdiensten ordnungsgemäß durchzuführen.

Der TSP erfüllt die Anforderung gemäß Artikel 24 Absatz 2 Buchstabe c [eIDAS] in Verbindung mit § 10 VDG und verfügt in Bezug auf das Haftungsrisiko für Schäden gemäß Artikel 13 über eine Haftpflichtversicherung gemäß § 10 VDG (jeweils 250 000 Euro für einen Schaden, der durch ein haftungsauslösendes Ereignis verursacht worden ist). Nicht-qualifizierte Vertrauensdienste sind durch eine Betriebshaftpflichtversicherung abgedeckt.

Der TSP erfüllt die Anforderungen von [GL-BRO] 8.4. Die Mindestversicherungshöhe für Vermögenschäden („professional liabilities“) in Höhe von fünf Millionen US Dollars wird gewährleistet.

9.2.2 Andere Ressourcen für Betriebserhaltung und Schadensdeckung

Keine Angaben.

9.2.3 Versicherung oder Gewährleistung für Endnutzer

Keine Angaben.

9.3 Vertraulichkeit von Geschäftsdaten

9.3.1 Definition von vertraulichen Geschäftsdaten

Die Vertraulichkeit von Informationen kann vereinbart werden, sofern sie nicht bereits durch geltendes Recht definiert ist.

9.3.2 Geschäftsdaten, die nicht vertraulich behandelt werden

Als öffentlich gelten alle Informationen in ausgestellten und veröffentlichten Zertifikaten sowie die unter Abschnitt 2.2 genannten Daten.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten

Der TSP kann im Einzelfall verpflichtet werden, die ihm als vertrauliche Geschäftsdaten benannten Daten durch entsprechende technische und organisatorische Maßnahmen gegen Preisgabe und Ausspähung zu schützen, und zu unterlassen, diese Daten zweckentfremdet zu nutzen oder sie Drittpersonen offen zu legen, soweit eine solche Verpflichtung nicht gegen das Gesetz verstößt. Im Rahmen der organisatorischen Maßnahmen werden die vom TSP eingesetzten Mitarbeiter in dem gesetzlich zulässigen Rahmen zur Geheimhaltung der vertraulichen Daten verpflichtet.

9.4 Datenschutz von Personendaten

9.4.1 Datenschutzkonzept

Der TSP arbeitet auf Basis eines Datenschutzkonzeptes, das den Schutz der personenbezogenen Daten regelt. Der TSP erfüllt die Anforderungen nach dem Bundesdatenschutzgesetze (BDSG) sowie ab dem 25.5.2018 der Datenschutz-Grundverordnung (DSGVO).

9.4.2 Definition von Personendaten

Es gilt Art. 4 Abs. 1 DSGVO.

9.4.3 Daten, die nicht vertraulich behandelt werden

Daten, die für ihre Zweckerfüllung veröffentlicht werden müssen (Sperrlisten, Statusinformationen, veröffentlichte Zertifikate), gehören nicht zu den vertraulich behandelten Daten.

9.4.4 Zuständigkeiten für den Datenschutz

Der TSP gewährleistet die Einhaltung des Datenschutzes. Alle Mitarbeiter des TSP sind auf die Einhaltung des Datenschutzes verpflichtet worden. Die interne Kontrolle erfolgt durch den betrieblichen Datenschutzbeauftragten, die externe Kontrolle erfolgt durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

9.4.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Dem Zertifikatnehmer wird spätestens bei Antragstellung kenntlich gemacht, welche persönlichen Daten im Zertifikat enthalten sein werden. Zertifikate werden nur veröffentlicht, wenn der Zertifikatnehmer dem bei der Antragstellung zustimmt.

Soweit keine andere Rechtsgrundlage herangezogen wird, willigt der Zertifikatnehmer spätestens mit der Antragstellung in die Verwendung seiner personenbezogenen Daten ein bzw. hat die Einwilligung von ggf. betroffenen Dritten zu diesem Zeitpunkt eingeholt.

Alle für die Bereitstellung des Services nicht mehr benötigten personenbezogenen Daten werden umgehend gelöscht. Für personenbezogene Daten, die zum Zertifikatsnachweis benötigt werden, gelten die Fristen nach Abschnitt 5.5.2 des CPS.

9.4.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Der TSP, als privatrechtliches Unternehmen, unterliegt der DSGVO, dem BDSG, dem Vertrauensdienstgesetz sowie den Gesetzen der Bundesrepublik Deutschland. Auskünfte werden entsprechend erteilt.

Endanwender wenden sich bei Auskunftsanfragen gemäß BDSG an die jeweils verantwortliche Stelle im Sinne des BDSG.

9.4.7 Andere Bedingungen für Auskünfte

Auskünfte anderer Art als unter Abschnitt 9.4.6 beschrieben werden nicht erteilt.

9.5 Gewerbliche Schutz- und Urheberrechte

9.5.1 TSP

Bestand und Inhalt von Urheber- und sonstigen Immaterialgüterrechten richten sich nach den allgemeinen gesetzlichen Vorschriften.

9.5.2 Zertifikatnehmer

Der Zertifikatnehmer verpflichtet sich zur Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten.

9.6 Zusicherungen und Garantien

9.6.1 Leistungsumfang des TSP

Es gelten die jeweiligen Vereinbarungen und [AGB] und diese CP. Soweit nicht ausdrücklich erwähnt, räumt der TSP keine Garantien oder Zusicherungen im Rechtssinne ein.

Der TSP stellt sicher, dass die in dem jeweils zugehörigen CPS beschriebenen Verfahren eingehalten werden.

QCP, EVCP, OVCP, LCP

Der TSP sorgt für die eindeutige Identifizierung der Zertifikatnehmer und/oder (nach Vereinbarung) des Endanwenders und die Zuordenbarkeit des öffentlichen Schlüssels zum Endanwender gemäß den anwendbaren Vorgaben. Der TSP stellt sicher, dass ein in Zertifikaten verwendeter Name (DistinguishedName im Feld subject) innerhalb der D-TRUST PKI und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist und stets dem gleichen Zertifikatnehmer zugeordnet ist. Dadurch ist die eindeutige Identifizierung des Zertifikatnehmers anhand des im Zertifikat verwendeten Namens (subject) gewährleistet.

Der TSP betreibt die CAs und stellt den Verzeichnisdienst und die Sperrinformationen bereit.

EVCP

Der TSP übernimmt keine Garantien im gesetzlichen Sinne nach dem BGB, unterwirft sich aber den Bestimmungen gemäß Abschnitt 7.1 [GL-BRO] hinsichtlich "Legal Existence", "Identity", "Right to Use Domain Name", "Authorization for EV Certificate", "Accuracy of Information", "Subscriber Agreement", "Status", "Revocation" und gewährleistet deren Einhaltung.

Zusätzlich hält der TSP den Betrieb von Reportingmechanismen gemäß Abschnitt 4.9.3 [BRG] vor. Die Reportingmechanismen bieten Zertifikatnehmern, Zertifikatnutzern, Lieferanten von Anwendungssoftware und anderen betroffenen Dritten die Möglichkeit ihnen suspekte Zertifikate des TSP anzuzeigen. Der TSP geht dann dem Verdacht (z. B. Betrug, Phishing etc.) nach.

Der TSP kann Teilaufgaben an Partner oder an externe Anbieter auslagern. Der TSP stellt sicher, dass in diesem Fall die Bestimmungen von CP und CPS eingehalten werden.

9.6.2 Leistungsumfang der RA

Der TSP betreibt Registrierungsstellen (RA). Die RA erbringt Identifizierung und Registrierung. Es gelten die [AGB] sowie die Bestimmungen dieser CP.

9.6.3 Zusicherungen und Garantien des Zertifikatnehmers

Es gelten die jeweiligen Vereinbarungen und [AGB] und diese CP.

QCP, EVCP, OVCP, LCP

Der Zertifikatnehmer willigt in die Verpflichtungserklärung (Subscriber Agreement) ein, die Zusicherungen und Garantien des Zertifikatnehmers beinhaltet.

EVCP, OVCP, LCP

Der Zertifikatnehmer verpflichtet sich, den Endanwender über seine Rechte und Pflichten zu informieren. Das Subscriber Agreement entspricht den Anforderungen von [GL-BRO].

EVCP

Das Subscriber Agreement entspricht den Anforderungen von Abschnitt 10.3 [GL-BRO].

9.6.4 Zusicherungen und Garantien des Zertifikatnutzers

Zusicherungen und Garantien des Zertifikatnutzers werden nach dieser CP nicht geregelt. Es entsteht zwischen dem TSP und dem Zertifikatnutzer kein Vertragsverhältnis. Im Übrigen gelten die [AGB] sowie gesetzliche Bestimmungen.

9.7 Haftungsausschlüsse

9.7.1 Haftungsausschlüsse des TSP

Es gelten die jeweiligen Vereinbarungen und [AGB].

EVCP

Soweit EV-Zertifikate ausgegeben werden, gelten ergänzend die nachfolgenden Bestimmungen gemäß Abschnitt 18 [GL-BRO]:

Soweit der TSP ohne Abweichungen nach den Bestimmungen dieser Zertifikatsrichtlinie das EV-Zertifikat ausgegeben hat, ist seine Haftung für Schäden ausgeschlossen, die mit dem Zertifikat verursacht wurden.

Der TSP haftet insbesondere und ausdrücklich nicht für Schäden, die durch die Nutzung oder Nicht-Nutzung von Zertifikaten ohne Zertifizierung entstehen.

9.8 Haftungsbeschränkungen

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

Soweit bei der Ausstellung des EV-Zertifikats von den Bestimmungen dieser Zertifikatsrichtlinie abgewichen wurde, gelten die nachfolgenden Haftungsbestimmungen ebenfalls in Übereinstimmung mit den Vorgaben nach Abschnitt 18 [GL-BRO]:

Für die korrekte Antragsprüfung und den daraus resultierenden Inhalt der EV-Zertifikate haftet der TSP der Bundesdruckerei GmbH nur im Rahmen seiner Prüfungsmöglichkeiten. Die Erteilung von EV-Zertifikaten bestätigt nur, dass D-TRUST zum Zeitpunkt der Antragstellung der erforderliche Identitäts- bzw. Legitimationsnachweis nach den Vorgaben dieser Zertifikatsrichtlinie erbracht wurde. Soweit eine ausgelagerte Registrierungsstelle erforderliche Identitätsprüfungen bezogen auf den Zertifikatsnehmer vornimmt, hat diese Registrierungsstelle die Vorgaben der D-TRUST im Einklang mit den Bestimmungen dieser Zertifikatsrichtlinie bei der Identitätsprüfung einzuhalten, wozu sie sich verpflichtet. Verstößt die Registrierungsstelle gegen diese Vorgaben, so hat sie D-TRUST und die Bundesdruckerei GmbH hinsichtlich der daraus resultierenden Ansprüche des Zertifikatsnehmers oder sonstiger Dritter freizustellen. Selbiges gilt für die Fälle, dass der Zertifikatnehmer als Registrierungsstelle selbst Identifizierung von Zertifikatsnehmern vornimmt, die zu seiner eigenen Organisation gehören.

Der Zertifikatnehmer haftet für Schäden, die D–TRUST und/ oder der Bundesdruckerei GmbH durch von ihm verursachte fehlerhafte Angaben im EV-Zertifikat, sowie durch von ihm verschuldeten, fehlerhaften Einsatz der EV-Zertifikate entstehen.

Im Übrigen ist in den vorgenannten Fällen die Haftung des TSP auf einen Betrag von maximal 2.000,00 US Dollars bzw. auf den entsprechenden EURO Betrag am Tag des Schadenseintritts pro EV-Zertifikat begrenzt.

9.9 Schadensersatz

9.9.1 Ansprüche des TSP gegenüber Zertifikatnehmern

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.9.2 Ansprüche der Zertifikatnehmer gegenüber dem TSP

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.10 Gültigkeitsdauer der CP und Beendigung der Gültigkeit

9.10.1 Gültigkeitsdauer der CP

Diese CP gilt ab dem Zeitpunkt der Veröffentlichung und bleibt wirksam bis zum Ablauf des letzten, unter dieser CP ausgestellten Zertifikates. Es gilt jeweils die Version der CP, die zum Zeitpunkt der Antragsstellung veröffentlicht ist.

9.10.2 Beendigung der Gültigkeit

Siehe Abschnitt 9.10.1.

9.10.3 Auswirkung der Beendigung

Siehe Abschnitt 9.10.1.

9.11 Individuelle Mitteilungen und Absprachen mit PKI-Teilnehmern

Mitteilungen des TSP an Zertifikatnehmer werden an die letzte in den Unterlagen von D-TRUST GmbH verzeichnete Anschrift oder der entsprechenden E-Mail-Adresse aus dem Antrag (elektronisch signiert) versendet.

9.12 Nachträge

9.12.1 Verfahren für Nachträge

Nachträge zu dieser CP werden in dieses Dokument eingearbeitet und unter demselben OID veröffentlicht. Editorische Änderungen werden markiert.

9.12.2 Benachrichtigungsmechanismen und –fristen

Keine Angaben.

9.12.3 Bedingungen für OID-Änderungen

Keine Angaben.

9.13 Bestimmungen zur Schlichtung von Streitfällen

Beschwerden bezüglich der Einhaltung oder Umsetzung dieser CP sind beim TSP (D-TRUST GmbH, Kommandantenstr. 15, 10969 Berlin, Germany) schriftlich einzureichen. Soweit nicht innerhalb einer Frist von 4 Wochen nach Einreichung der Beschwerde abgeholfen wurde, gilt: Für sämtliche Rechtsbeziehungen zwischen der Bundesdruckerei, der D-TRUST GmbH und Dritten, die Rechtsbeziehungen aus dieser CP herleiten, findet deutsches Recht unter Ausschluss des UN-Kaufrechts Anwendung.

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

https://www.bundesdruckerei.de/de/Service-Support/Support/Zertifikatssicherheitsvorfall-melden

Dort kann über ein Formular der Sicherheitsvorfall beschrieben und an den genannten E-Mail-Kontakt versendet werden.

9.14 Gerichtsstand

Es gelten die [AGB].

9.14.1 Einhaltung geltenden Rechts

Diese CP unterliegt dem Recht der Bundesrepublik Deutschland sowie dem Recht der Europäischen Union.

9.15 Sonstige Bestimmungen

9.15.1 Vollständigkeitserklärung

Folgende Dokumente sind Gegenstand der geltenden Vereinbarungen an denen PKI-Teilnehmer beteiligt sind:

- Vertrags- und Antragsunterlagen,
- die zum Zeitpunkt der Antragsstellung gültigen [AGB] bzw. die ggf. wirksam einbezogene Fassung derselben,
- die zum Zeitpunkt der Antragsstellung gültige CP
- bei qualifizierten Zertifikaten und qualifizierten Zeitstempeldiensten die zum Zeitpunkt der Antragsstellung gültige PKI Nutzerinformation.

Für SSL CAs, deren Sub- sowie Root-CAs gelten die folgenden Dokumente:

- Vertrags- und Antragsunterlagen,
- die zum Zeitpunkt der Antragsstellung gültigen [AGB], bzw. die ggf. wirksam einbezogene Fassung derselben,
- die zum Zeitpunkt der Antragsstellung gültige Version der [GL-BRO], die zum Zeitpunkt der Antragsstellung gültige CP.

9.15.2 Abgrenzungen

entfällt

9.15.3 Salvatorische Klausel

Durch etwaige Unwirksamkeit einer oder mehrerer Bestimmung dieser CP wird die Wirksamkeit der übrigen Bestimmungen nicht berührt.

9.15.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.15.5 Höhere Gewalt

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].

9.16 Andere Bestimmungen

9.16.1 Konflikt von Bestimmungen

Die unter 9.16.1 genannten Regelungen sind abschließend. Sie gelten untereinander in der in 9.16.1 aufgeführten Reihenfolge jeweils nachrangig.

9.16.2 Einhaltung von Ausfuhrgesetzen und -vorschriften

Es gelten die etwaigen jeweiligen Vereinbarungen und [AGB].