

Bündnis-E-Vergabe

Certification Practice Statement

– Zertifikatsrichtlinien für fortgeschrittene Software-Zertifikate
des Bündnis-E-Vergabe –

Version 1.3

Datum des Inkrafttretens: 22.05.2009



Deutscher Sparkassen Verlag GmbH
S-TRUST¹
Am Wallgraben 115
70565 Stuttgart
Deutschland

+49 800-4787878
<http://www.s-trust.de>

Dieses CPS findet keine Anwendung auf Dienstleistungen, die S-TRUST als Zertifizierungsdiensteanbieter nach § 2 Nr. 8 Signaturgesetz (SigG) leistet, und/oder auf Dienstleistungen von S-TRUST im Zusammenhang mit qualifizierten Zertifikaten nach § 2 Nr. 7 SigG. Ferner findet dieses CPS keine Anwendung auf Dienstleistungen, die S-TRUST als Zertifizierungsdiensteanbieter im Rahmen des VeriSign Trust Network (VTN) leistet. Für solche Leistungen gelten gesonderte Regelungen.

¹ S-TRUST ist ein Unternehmenskennzeichen der Deutscher Sparkassen Verlag GmbH.

Dokumentenhistorie

Version	Datum	Beschreibung/ Änderungsgrund
1.3	22.05.2009	<ul style="list-style-type: none"> ▪ CPS Abschnitt 1.1 – Internetlink zu angeschlossenen Plattformbetreibern/ Softwareanbietern hinzugefügt. ▪ CPS Abschnitt 1.3.2 – Registrierungsstelle kann auch ein Dritter sein. ▪ CPS Abschnitt 3.2 – Anpassungen und Ergänzungen hinsichtlich vorzulegender amtlicher Ausweise. ▪ CPS Abschnitt 4.2 – Anpassungen bei der Bearbeitung des Zertifikatantrages ▪ CPS Abschnitt 4.4 u. 6.1.2 – Das zur Aktivierung erforderliche Passwort wird dem Zertifikatsinhaber auf einem nicht elektronischen Weg per Post, mitgeteilt. (I.d.R. gestrichen) ▪ CPS Abschnitt 4.7.2 – Klarstellung ▪ CPS Abschnitt 4.7.3.1 - Internetschnittstelle zur Sperrung aktualisiert. Die Sperrung ohne Sperrpasswort ist nicht nur schriftlich sondern auch per Fax möglich. ▪ CPS Abschnitt 5.3.2 – Anpassung hinsichtlich des bei der Registrierungsstelle des DSV eingesetzten Personal (Einsatz von Leiharbeitnehmern). ▪ CPS Abschnitt 5.3.7 – Anpassungen für den Einsatz von Leiharbeitnehmern.
1.2	20.09.2007	<ul style="list-style-type: none"> ▪ CPS Abschnitt 4.2 – Prozesspunkt 2 aktualisiert. ▪ CPS Abschnitt 4.2 – „Geschäftsführer/Bevollmächtigter“ aktualisiert in „Geschäftsführer/-inhaber bzw. Bevollmächtigter mit Prokura“ ▪ CPS Abschnitt 2.1 - gelöscht: „Ein Abruf der E-Vergabe-Zertifikate über einen LDAP-Verzeichnisdienst ist nicht möglich.“
1.1	03.08.2007	<ul style="list-style-type: none"> ▪ Allgemeine typografische und orthografische Korrekturen ▪ CPS Abschnitt 4.4 und 6.1.2 „... passwortgesicherte PKCS#12-Datei, in einem ZIP-Container, per E-Mail zugestellt.“ Gelöscht: “in einem ZIP-Container“
1.0	23.07.2007	<ul style="list-style-type: none"> ▪ Erstversion

Impressum

Deutscher Sparkassen Verlag GmbH
Postanschrift: 70547 Stuttgart
Hausanschrift: Am Wallgraben 115, 70565 Stuttgart
Telefon: +49 711 782-0
Telefax: +49 711 782-1635
E-Mail: info@s-trust.de

Aufsichtsratsvorsitzender: Dr. Siegfried Naser, Sitz der Gesellschaft: Stuttgart, Registergericht: Stuttgart, Handelsregister: Nr. B/748, Bankverbindung: Baden-Württembergische Bank (BW-Bank), BLZ: 600 501 01, Konto: 1366860, USt. ID-Nr.: DE 147830796, Geschäftsführung: Dr. Bernd Kobarg (Vorsitzender), Wilhelm Gans, Jürgen Schneider

© 2009 Deutscher Sparkassen Verlag GmbH, Stuttgart

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Inhaltsverzeichnis

1	Einleitung	7
1.1	Überblick	7
1.2	Dokumentenidentifikation	7
1.3	Instanzen der PKI	7
1.3.1	Zertifizierungshierarchie	7
1.3.2	Registrierungsstelle	8
1.3.3	Zertifikatsantragsteller/-inhaber	8
1.3.4	Vertrauende Dritte	8
1.4	Verwendung von Zertifikaten	9
1.4.1	Zulässige Verwendung von Zertifikaten	9
1.4.2	Unzulässige Anwendung von Zertifikaten	9
1.5	Policy-Verwaltung	10
1.5.1	Ansprechpartner	10
1.5.2	Änderungsprozedur	10
2	Bekanntmachung und Verzeichnisdienst	10
2.1	Verzeichnisse	10
2.2	Veröffentlichung von Zertifikatsinformationen	10
2.3	Veröffentlichung von Geschäftsbedingungen	10
2.4	Häufigkeit und Zyklen für Veröffentlichungen	10
3	Identifizierung und Authentifizierung	11
3.1	Namensgebung	11
3.1.1	Namensart	11
3.1.2	Anonymität und Pseudonyme für Zertifikatsinhaber	11
3.1.3	Eindeutigkeit von Namen	11
3.2	Erstmalige Identifizierung/Registrierung	12
4	Anforderungen an den Lebenszyklus von Zertifikaten	12
4.1	Zertifikatsantrag	12
4.2	Bearbeitung des Zertifikatsantrags	12
4.3	Annahme bzw. Ablehnung des Antrags	13
4.4	Zertifikatsausstellung	14
4.5	Zertifikatsübergabe und -annahme	14
4.5.1	Verfahren der Zertifikatsanerkennung	14
4.5.2	Veröffentlichung der Zertifikate	14
4.6	Nutzung der Schlüsselpaare und der Zertifikate	14
4.6.1	Nutzung der privaten Schlüssel durch den Zertifikatsinhaber	14
4.6.2	Nutzung der Zertifikate durch vertrauende Dritte	14
4.7	Sperrung von Zertifikaten	15
4.7.1	Gründe für eine Sperrung	15
4.7.2	Sperrberechtigte	15
4.7.3	Verfahren für eine Sperrung	16
4.7.4	Fristen für die Beantragung einer Sperrung	16
4.7.5	Bearbeitungszeit für Anträge auf Sperrung	16
4.7.6	Sperrbestätigung für Zertifikatsinhaber	17
4.7.7	Prüfung des Zertifikatsstatus' durch Dritte	17
4.7.8	Periode für die Erstellung der Sperrlisten	17

4.7.9	Erscheinungsintervall der Sperrlisten	17
4.7.10	Online-Verfügbarkeit von Sperr-/Statusinformationen	17
4.7.11	Spezielle Maßnahmen bei Schlüsselkompromittierung	17
5	Physikalische, organisatorische und personelle Sicherheitsmaßnahmen	17
5.1	Physikalische Sicherheitsmaßnahmen	17
5.1.1	Lage und Konstruktion des Standortes	17
5.1.2	Räumlicher Zugang	18
5.1.3	Stromversorgung und Klimakontrolle	18
5.1.4	Schutz vor Wasserschäden	18
5.1.5	Brandschutz	18
5.1.6	Schutz von Datenträgern	18
5.1.7	Entsorgung	19
5.1.8	Datensicherung	19
5.2	Organisatorische Sicherheitsmaßnahmen	19
5.2.1	Sicherheitskritische Rollen	19
5.2.2	Anzahl benötigter Personen bei sicherheitskritischen Aufgaben	19
5.2.3	Identifikation und Authentifizierung von Rollen	19
5.2.4	Trennung von Rollen und Aufgaben	19
5.3	Personelle Sicherheitsmaßnahmen	20
5.3.1	Anforderungen an Qualifikation, Erfahrung	20
5.3.2	Überprüfung der Vertrauenswürdigkeit	20
5.3.3	Anforderungen an Schulung und Fortbildung	21
5.3.4	Nachschulungsintervalle und -anforderungen	21
5.3.5	Häufigkeit und Abfolge der Arbeitsplatzrotation	21
5.3.6	Verfahren bei unbefugten Handlungen	21
5.3.7	Vertragsbedingungen mit dem Personal	21
5.4	Protokollierung sicherheitskritischer Ereignisse	22
5.5	Schlüsselwechsel der Wurzel-CA	23
5.6	Archivierung	23
5.6.1	Arten von zu archivierenden Daten	23
5.6.2	Archivierungsfristen	23
5.6.3	Verfahren zur Beschaffung von Archivdaten	23
5.7	Wiederanlauf nach Katastrophen	24
5.7.1	Notfallprozeduren	24
5.7.2	Wiederherstellung nach Kompromittierung von Systemen	24
5.7.3	Kompromittierung von CA-Schlüsseln	24
5.7.4	Notbetrieb im Katastrophenfall	24
5.8	Betriebsbeendigung	24
6	Technische Sicherheitsmaßnahmen	24
6.1	Erzeugung und Installation von Schlüsseln	24
6.1.1	Erzeugung von Schlüsselpaaren	24
6.1.2	Auslieferung privater Schlüssel	25
6.1.3	Übergabe öffentlicher Schlüssel an den Schlüsseleigentümer	25
6.1.4	Schlüssellängen	25
6.1.5	Verwendungszweck der Schlüssel	25
6.2	Schutz der privaten Schlüssel und kryptographischen Module	25
6.2.1	Standards und Schutzmechanismen der kryptographischen Module	25

6.2.2	Mehrpersonenkontrolle über private Schlüssel	26
6.2.3	Hinterlegung privater Schlüssel	26
6.2.4	Sicherung und Wiederherstellung privater Schlüssel	26
6.2.5	Archivierung privater Schlüssel	26
6.2.6	Speicherung privater Schlüssel	26
6.2.7	Methoden zur Aktivierung privater Schlüssel	26
6.2.8	Methoden zur Vernichtung privater Schlüssel	26
6.3	Weitere Aspekte der Verwaltung von Schlüsselpaaren	27
6.3.1	Archivierung öffentlicher Schlüssel	27
6.3.2	Verwendungsdauer von Zertifikaten und Schlüsselpaaren	27
6.4	Sicherheitsbestimmungen für Computer	27
6.5	Maßnahmen zur Netzwerksicherheit	27
7	Profile	28
7.1	Zertifikatsprofile	28
7.2	Profil der Sperrlisten	28
8	Audits, Revisionen und weitere Prüfungen	28
8.1	Identität und Qualifikation des Prüfers	28
8.2	Veröffentlichung der Ergebnisse der Audits und Revisionen	28
9	Sonstige geschäftliche und rechtliche Bestimmungen	28
9.1	Vergütung	28
9.2	Vertraulichkeit betrieblicher Informationen	28
9.2.1	Art der geheim zu haltenden Informationen	28
9.2.2	Öffentliche Informationen	28
9.3	Vertraulichkeit personenbezogener Informationen	29
9.4	Geistiges Eigentum	29
9.5	Sorgfalts-, Mitwirkungspflichten u. Obliegenheiten des Zertifikatsinhabers	29
9.5.1	Aufbewahrung und Nutzung der privaten Schlüssel und Zertifikate	29
9.5.2	Geheimhaltung	29
9.5.3	Anzeige- und Mitteilungspflichten	29
9.6	Nutzung durch Dritte	30
9.7	Haftung des Zertifikatsinhabers	30
9.8	Störungen	30
9.9	Haftung von S-TRUST	31
9.10	Verjährung	31
9.10.1	Verkürzung der regelmäßigen Verjährungsfrist	31
9.10.2	Verkürzung der 10-jährigen Verjährungsfrist	31
9.10.3	Verjährung von Mängelrechten	31
9.10.4	Geltung gesetzlicher Regelungen	31
9.11	Gültigkeit des CPS	32
9.11.1	Gültigkeitszeitraum	32
9.11.2	Ende der Gültigkeit	32
9.12	Anwendbares Recht	32
9.13	Gerichtsstand	32
9.14	Vorrang zwingender gesetzlicher Regelungen	32
10	Anhang: Definitionen und Abkürzungen	33

1 Einleitung

1.1 Überblick

Die Deutscher Sparkassen Verlag GmbH betreibt unter dem Unternehmenskennzeichen **S-TRUST** Zertifizierungsdienste für die Erzeugung, Ausgabe, Verwaltung und Sperrung von fortgeschrittenen Software-Zertifikaten als Dienstleister des Bündnis-E-Vergabe.

Das **Bündnis-E-Vergabe** ist eine u.a. Kooperation des Beschaffungsamts des Bundesministeriums des Innern, der ausschreibungs-abc-GmbH, der subreport Verlag Schawe GmbH, der cosinex GmbH und der Administration Intelligence AG. Eine Übersicht über alle am Bündnis-E-Vergabe angeschlossenen Ausschreibungsplattformen und entsprechenden Softwareanbietern finden Sie im Internet unter <https://www.s-trust.de/evergabe-fortgeschritten/index.htm>.

Bei diesem Dokument handelt es sich um die E-Vergabe-Zertifizierungsrichtlinien (Certification Practice Statement, CPS). Darin werden die Verfahren erläutert, die S-TRUST als Zertifizierungsstelle (Certification Authorities, CAs) bei der Bereitstellung von Zertifizierungsdiensten für das Bündnis-E-Vergabe anwendet. Diese umfassen insbesondere die Ausgabe, Verwaltung und Sperrung von fortgeschrittenen Software-Zertifikaten gemäß den Vorgaben des Bündnis-E-Vergabe.

Dieses CPS findet keine Anwendung auf Dienstleistungen, die S-TRUST als Zertifizierungsdiensteanbieter nach § 2 Nr. 8 Signaturgesetz (SigG) leistet, und/oder auf Dienstleistungen von S-TRUST im Zusammenhang mit qualifizierten Zertifikaten nach § 2 Nr. 7 SigG. Ferner findet dieses CPS keine Anwendung auf Dienstleistungen, die S-TRUST als Zertifizierungsdiensteanbieter im Rahmen des VeriSign Trust Network (VTN) leistet. Für solche Leistungen gelten gesonderte Regelungen.

1.2 Dokumentenidentifikation

Die Dokumentenbezeichnung für das vorliegende CPS lautet:

„Bündnis-E-Vergabe Certification Practice Statement (E-Vergabe CPS)“

Für die Referenzierung des CPS wird folgender CPS-URL-Qualifier im Zertifikat verwendet:

<http://www.s-trust.de/evergabe-fortgeschritten/nutzung>

1.3 Instanzen der PKI

1.3.1 Zertifizierungshierarchie

S-TRUST verwendet für die Ausstellung der verschiedenen Zertifikatstypen für das Bündnis- E-Vergabe jeweils eine Zertifizierungsinstanz (CA). Durch die Zertifizierungsinstanzen und die von ihnen ausgestellten Zertifikate wird die in der folgenden Abbildung dargestellte Zertifizierungshierarchie definiert.

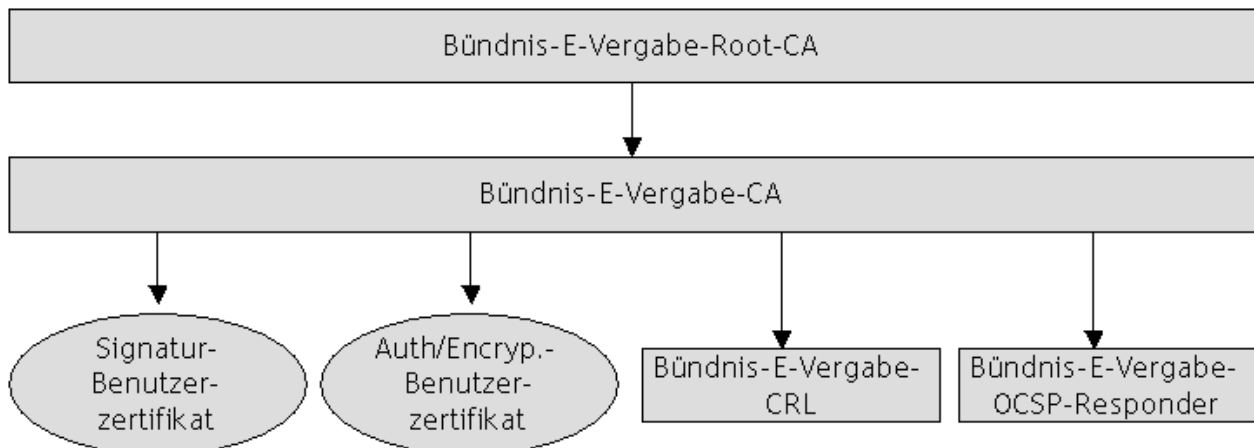


Abbildung 1: Zertifizierungshierarchie

Auf der obersten Stufe dieser Zertifizierungshierarchie befindet sich

- die Bündnis-E-Vergabe-Root-CA, die
 - die Bündnis-E-Vergabe-CA signiert

Auf der zweiten Hierarchiestufe befinden sich:

- die Bündnis-E-Vergabe-CA, die
 - die Signatur- und
 - die Authentifizierungs-/Verschlüsselungs-Zertifikate,
 - die Sperrliste (CRL) mit den Sperrstatusinformationen für alle Personenzertifikate und
 - den OCSP-Responder für Signatur-, Authentifizierungs- und Verschlüsselungszertifikate
 signiert.

1.3.2 Registrierungsstelle

Registrierungsstelle ist die Deutscher Sparkassen Verlag GmbH (DSV) oder ein durch den DSV beauftragter Dritter. Die Registrierungsstelle für das Bündnis-E-Vergabe hat die Aufgabe, Zertifikatsantragsteller zu identifizieren und die Antragsdaten zu erfassen.

1.3.3 Zertifikatsantragsteller/-inhaber

Die Zertifikate werden nur auf natürliche Personen ausgestellt. Es gelten die Nutzungsbedingungen, die unter <http://www.s-trust.de/evergabe-fortgeschritten/nutzung> veröffentlicht sind. „Zertifikatsantragsteller/-inhaber“ sind Personen, die Zertifikate des Bündnis-E-Vergabe von S-TRUST beantragen oder nutzen.

1.3.4 Vertrauende Dritte

Ein vertrauender Dritter ist eine natürliche Person oder Stelle, die sich auf die Vertrauenswürdigkeit eines im Rahmen des Bündnis-E-Vergabe ausgestellten Zertifikats und/oder einer digitalen Signatur verlässt.

1.4 Verwendung von Zertifikaten

Nutzern von E-Vergabe-Anwendungen im Rahmen des Bündnis-E-Vergabe werden jeweils 2 Zertifikate auf Softwarebasis zur Verfügung gestellt:

- a) ein Signaturzertifikat,
- b) ein Authentifizierungs-/Verschlüsselungszertifikat.

Mit den Zertifikaten können sich Nutzer von E-Vergabe-Anwendungen u. a. an diesen authentisieren sowie vertrauliche Daten, wie z. B. Ausschreibungs-/Angebotsdokumente oder E-Mails signieren und/oder verschlüsseln.

Es besteht die Möglichkeit, dass ein Zertifikat den Firmennamen oder ein ähnliches Unternehmenskennzeichen enthält. Solche Angaben können in das Zertifikat nur aufgenommen werden, wenn der Zertifikatsantragsteller eine entsprechende Berechtigung durch Vorlage einer schriftlichen Bestätigung des Rechteinhabers an dem Firmennamen oder dem Unternehmenskennzeichen nachweist. Der Rechteinhaber ist zur Sperrung des Zertifikats berechtigt (siehe CPS 4.7.3.2).

1.4.1 Zulässige Verwendung von Zertifikaten

Die von S-TRUST ausgegebenen E-Vergabe-Zertifikate zur Signatur und die zugeordneten Schlüssel sind zur Signatur von Dokumenten sowie E-Mails im Rahmen des Bundes-E-Vergabe vorgesehen.

Die von S-TRUST ausgegebenen E-Vergabe-Zertifikate zur Authentifizierung/Verschlüsselung und die zugeordneten Schlüssel dürfen nur zu Authentifizierungszwecken und zur Transportverschlüsselung eingesetzt werden.

1.4.2 Unzulässige Anwendung von Zertifikaten

Zertifikate dürfen nur im Rahmen des gesetzlich Zulässigen verwendet werden. Dies gilt insbesondere hinsichtlich der Beachtung der geltenden Ausfuhr- und Einfuhrbestimmungen.

S-TRUST-Zertifikate sind nicht zur Verwendung oder zum Weitervertrieb als Kontroll- oder Steuerungseinrichtungen in gefährlichen Umgebungen oder für Verwendungszwecke vorgesehen, ausgelegt oder zugelassen, bei denen ein ausfallsicherer Betrieb erforderlich ist, wie z. B. der Betrieb von nuklearen Einrichtungen, Flugzeugnavigations- oder -kommunikations-systemen, Luftverkehrskontrollsystemen oder Waffenkontrollsystemen, wobei ein Ausfall direkt zum Tode, zu Personenschäden oder schweren Umweltschäden führen kann. Personenzertifikate dürfen nicht als Server- oder Organisationszertifikate verwendet werden.

CA-Zertifikate dürfen ausschließlich für CA-Funktionen verwendet werden. Des Weiteren dürfen Personenzertifikate nicht als CA-Zertifikate verwendet werden.

Nach Ablauf der Gültigkeitsdauer oder Sperrung von Zertifikaten dürfen die persönlichen Schlüssel nicht mehr zur Signierung verwendet werden.

1.5 Policy-Verwaltung

1.5.1 Ansprechpartner

Der Ansprechpartner für dieses CPS ist:

Deutscher Sparkassen Verlag GmbH

Produktmanagement Zertifizierungsdienstleistungen

Am Wallgraben 115

70565 Stuttgart

Deutschland

<http://www.s-trust.de>

1.5.2 Änderungsprozedur

S-TRUST behält sich vor, den Inhalt dieses CPS zu ändern oder zu ergänzen. Dies insbesondere, um die Leistung zu verbessern oder an technische Entwicklungen anzupassen, und wenn dies aufgrund von Vorgaben des Bündnis-E-Vergabe notwendig erscheint. Die Revision und Freigabe unterliegt der ausschließlichen Verantwortung der Deutscher Sparkassen Verlag GmbH.

2 Bekanntmachung und Verzeichnisdienst

2.1 Verzeichnisse

Über einen OCSP-Verzeichnisdienst kann der Status der E-Vergabe-Zertifikate abgerufen werden. Der OCSP-Verzeichnisdienst ist unter den folgenden Adressen zu erreichen:

- <http://ocsp.s-trust.de/>

Zertifikate können auf Basis der E-Mail-Adresse oder des vollständigen Namens des Zertifikatsinhabers unter <http://www.s-trust.de/eVergabe-fortgeschritten> gesucht und heruntergeladen werden.

2.2 Veröffentlichung von Zertifikatsinformationen

Neben der Online-Abfrage der Gültigkeit der E-Vergabe-Zertifikate per OCSP-Dienst erstellt S-TRUST Sperrlisten, in denen Sperrinformationen enthalten sind. Die Sperrlistenpfade sind in jedem E-Vergabe-Zertifikat als http-Angabe kodiert.

2.3 Veröffentlichung von Geschäftsbedingungen

Es gelten die Nutzungsbedingungen für fortgeschrittene Software-Zertifikate des Bündnis-E-Vergabe sowie die Bündnis-E-Vergabe-Bedingungen für vertrauende Dritte, die unter <http://www.s-trust.de/evergabe-fortgeschritten/nutzung> heruntergeladen werden können.

2.4 Häufigkeit und Zyklen für Veröffentlichungen

Die ausgegebenen E-Vergabe-Zertifikate werden nicht über einen LDAP-Verzeichnisdienst veröffentlicht.

Die Veröffentlichung der sonstigen von S-TRUST ausgestellten CA-Zertifikate erfolgt nach ihrer Erstellung.

Die Zyklen für die Veröffentlichung von Sperrlisten sind in Abschnitt 4.7.8 angegeben.

Die Veröffentlichung des Certification Practice Statement erfolgt nach dessen Erstellung bzw. Aktualisierung. Informationen zur Gültigkeit der CPS siehe Abschnitt 9.11.

3 Identifizierung und Authentifizierung

3.1 Namensgebung

3.1.1 Namensart

Die für das Bündnis-E-Vergabe ausgestellten Zertifikate enthalten eindeutige Namen (*DistinguishedName*) in den Feldern *issuer* und *subject* nach X.501.

Alle Zertifikate enthalten im Feld *issuer* die Attribute:

- CommonName
- Organization
- Organizational Unit
- State or Province
- Country

der ausgebenden CA.

Alle Zertifikate enthalten im Feld *subject* einen *DistinguishedName* nach X.501. Dabei werden die folgenden Attribute verwendet:

- CommonName
- Country
- Organization (optional)
- Zertifikatsspezifische Attribute:
 - SerialNumber
- E-Mail-Adresse

3.1.2 Anonymität und Pseudonyme für Zertifikatsinhaber

Die Verwendung eines Pseudonyms anstelle des wahren Namens ist ausgeschlossen.

3.1.3 Eindeutigkeit von Namen

Es ist sichergestellt, dass die Kombination der Zertifikatsinhalte „Vor-, Nachname“ und „E-Mail-Adresse“ immer nur einmal in einem gültigen Zertifikatspaar vorhanden ist. Ferner sind die für das Bündnis-E-Vergabe ausgestellten Zertifikate durch eine eindeutige Nummer im Attribut SerialNumber stets eindeutig identifizierbar.

3.2 Erstmalige Identifizierung/Registrierung

Bei E-Vergabe-Zertifikaten wird die Identität authentisiert, indem die vom Zertifikatsantragsteller eingereichten und unterschriebenen Identitätsangaben mit den Angaben einer Kopie eines gültigen amtlichen Personalausweises verglichen werden und übereinstimmen müssen (alternativ zur Personalausweiskopie kann eine Kopie eines gültigen – nicht nur vorläufigen – amtlichen Reisepasses plus aktueller Meldebescheinigung eingereicht werden).² Ist der amtliche Ausweis einschließlich der darin enthaltenen personenbezogenen Daten nicht in deutscher und/oder englischer Sprache, ist der Zertifikatsantragsteller verpflichtet, zusätzlich eine amtlich beglaubigte Übersetzung des Ausweises in deutscher Sprache oder eine Übersetzung in deutscher Sprache, die von einem amtlich bestellten und vereidigten Übersetzer hergestellt wurde, der die Richtigkeit seiner Übersetzung unter Bezug auf seine amtliche Bestellung und Vereidigung ausdrücklich bestätigt, vorzulegen. Die Prüfung der Daten des Zertifikatsantragstellers erfolgt in diesem Fall anhand der vorgelegten Übersetzung des amtlichen Ausweises.

Enthält der Personalausweis keine Unterschrift, ist die Personalausweiskopie mit einer eigenhändigen Unterschrift des Zertifikatsantragstellers zu versehen und diese durch eine siegelführende Behörde oder einen Notar zu beglaubigen.

E-Vergabe-Zertifikate leisten einen Nachweis der Identität auf Basis des in Kapitel 4.2 beschriebenen Authentifizierungsprozesses.

4 Anforderungen an den Lebenszyklus von Zertifikaten

4.1 Zertifikatsantrag

S-TRUST stellt auf Antrag Zertifikate zur Nutzung bei angeschlossenen Anbietern von E-Vergabe-Systemen aus.

E-Vergabe-Zertifikate können von natürlichen Personen beantragt werden. Die Beantragung erfolgt unter Angabe der persönlichen Daten auf <http://www.sparkassen-shop.de/eVergabe>.

4.2 Bearbeitung des Zertifikatsantrags

Eingehende Zertifikatsanträge werden von S-TRUST auf Richtigkeit und Vollständigkeit geprüft, indem die online erfassten Antragsdaten mit den Daten in dem papiergebunden, unterschriebenen Zertifikatsantrag sowie mit den Angaben auf der beigefügten Ausweiskopie verglichen werden.

Der Prozess sieht wie folgt aus:

1. Der Antragsteller beantragt sein E-Vergabe-Zertifikat unter der Angabe seiner persönlichen Daten auf <http://www.sparkassen-shop.de/eVergabe>.
2. Der Antragsteller erhält eine Bestätigungs-E-Mail mit beigefügtem Zertifikatsantrag, diesen druckt er aus, unterschreibt diesen eigenhändig und sendet diesen per Post mit der Kopie seines gültigen – nicht nur vorläufigen – amtlichen Personalausweises

² S-TRUST stellt im Rahmen dieses Vertrages keine qualifizierten Zertifikate nach § 2 Nr. 7 Signaturgesetz (SigG) aus. Daher unterscheidet sich das Verfahren zur Identifizierung des Zertifikatsantragstellers von den in § 5 SigG, § 4 SigV vorgeschriebenen Verfahren zur Identitätsprüfung.

(Vorder- und Rückseite) an S-TRUST. Alternativ zur Personalausweiskopie kann der Antragsteller eine Kopie seines gültigen amtlichen Reisepasses inkl. einer aktuellen Meldebescheinigung einreichen. Ist der amtliche Ausweis einschließlich der darin enthaltenen personenbezogenen Daten nicht in deutscher und/oder englischer Sprache, ist der Zertifikatsantragsteller verpflichtet, zusätzlich eine amtlich beglaubigte Übersetzung des Ausweises in deutscher Sprache oder eine Übersetzung in deutscher Sprache, die von einem amtlich bestellten und vereidigten Übersetzer hergestellt wurde, der die Richtigkeit seiner Übersetzung unter Bezug auf seine amtliche Bestellung und Vereidigung ausdrücklich bestätigt, vorzulegen.

3. S-TRUST überprüft die Zertifikatsantragsdaten anhand der Ausweiskopie sowie die Übereinstimmung der Unterschrift auf der Ausweiskopie und dem eingereichten Antragsformular. Bei Ausweisen, die nicht in deutscher und/oder englischer Sprache sind, erfolgt die Prüfung der Daten anhand der vorgelegten Übersetzung des amtlichen Ausweises.

Soll ein Firmen- oder Organisationsname in das Zertifikat aufgenommen werden, so muss diese Firmen- oder Organisationszugehörigkeit zusätzlich gegenüber S-TRUST nachgewiesen werden. Hierzu ist die Einreichung folgender Unterlagen erforderlich:

1. Eine durch einen Zeichnungsberechtigten der Firma/Organisation (Geschäftsführer/-inhaber bzw. Bevollmächtigter mit Prokura) unterzeichnete „Einwilligungserklärung zur Aufnahme des Firmen- oder Organisationsnamens in das E-Vergabe-Zertifikat“.
Wird die Einwilligungserklärung durch eine Person erteilt, die nicht im Handelsregister als vertretungsberechtigt eingetragen ist, ist deren Bevollmächtigung zur Erteilung der Einwilligungserklärung (zusätzlich zu der weiteren Voraussetzung nach Ziff. 2 unten) nachzuweisen.
2. Ein aktueller mit Firmenstempel versehener Handelsregisterauszug als Nachweis der Zeichnungsberechtigung.
Ist das Unternehmen nicht im Handelsregister eingetragen, muss der Nachweis anhand eines anderen geeigneten Dokuments (z. B. Gewerberegisterauszug, Auszug aus der Handwerksrolle, Nachweis der Kammermitgliedschaft etc.) oder alternativ anhand der Angabe der D-U-N-S-Nummer erbracht werden.
Erfolgt der Nachweis der Zeichnungsberechtigung anhand der D-U-N-S-Nummer, muss sichergestellt sein, dass der Zeichnungsberechtigte als Verantwortlicher in der Wirtschaftsauskunftsdatei von Dun & Bradstreet (D&B) geführt ist. Unter <http://www.upik.de> hat der Zertifikatsantragsteller die Möglichkeit, kostenfrei seine D&B-Daten zu prüfen.

4.3 Annahme bzw. Ablehnung des Antrags

Mindestvoraussetzung für die Annahme des E-Vergabe-Zertifikatsantrags durch S-TRUST ist, dass die Identifizierung und Authentifizierung aller erforderlichen Antragsdaten erfolgreich war. S-TRUST lehnt – unbeachtet etwaiger weiterer Ablehnungsgründe – in folgenden Fällen den Zertifikatsantrag ab:

- Der Antragsteller kann nicht zweifelsfrei identifiziert werden.
- Der Personalausweis oder Reisepass ist nicht mehr gültig.

- Es bestehen Zweifel an der Echtheit der Unterschrift.

4.4 Zertifikatsausstellung

Nach erfolgreicher Prüfung und Genehmigung des Antrags werden die Signatur-, Verschlüsselungs-/Authentifizierungszertifikate erstellt und dem Zertifikatsantragsteller als passwortgesicherte PKCS#12-Datei per E-Mail zugestellt.

Das zur Aktivierung erforderliche Passwort wird dem Zertifikatsinhaber auf einem nicht elektronischen Weg per Post mitgeteilt.

4.5 Zertifikatsübergabe und -annahme

4.5.1 Verfahren der Zertifikatsanerkennung

Der Zertifikatsinhaber hat vor einer erstmaligen Nutzung des Zertifikats dessen Inhalt auf Richtigkeit und Vollständigkeit zu überprüfen. Er darf das Zertifikat nicht nutzen, wenn dieses Fehler enthält.

4.5.2 Veröffentlichung der Zertifikate

Zertifikate können auf Basis der E-Mail-Adresse oder des vollständigen Namens eines Benutzers unter <http://www.s-trust.de/evergabe-fortgeschritten> gesucht und heruntergeladen werden. Ein Abruf der E-Vergabe-Zertifikate über einen LDAP-Verzeichnisdienst ist nicht möglich.

4.6 Nutzung der Schlüsselpaare und der Zertifikate

4.6.1 Nutzung der privaten Schlüssel durch den Zertifikatsinhaber

Die Verwendung des privaten Schlüssels, der dem öffentlichen Schlüssel im Zertifikat entspricht, ist erst gestattet, nachdem der Zertifikatsinhaber das Zertifikat angenommen hat. Das Zertifikat darf nur rechtmäßig gemäß den Nutzungsbedingungen für fortgeschrittene Software-Zertifikate des Bündnis-E-Vergabe verwendet werden. Die Verwendung des Zertifikats muss den im Zertifikat enthaltenen KeyUsage-Felderweiterungen entsprechen.

Zertifikatsinhaber müssen ihre privaten Schlüssel vor unbefugtem Gebrauch schützen und dürfen den privaten Schlüssel nach dem Ablauf der Gültigkeitsdauer oder der Sperrung des Zertifikats nicht mehr benutzen.

4.6.2 Nutzung der Zertifikate durch vertrauende Dritte

Die Nutzung der Zertifikate durch vertrauende Dritte muss diesem CPS folgen. Vor einem Vertrauen auf ein Zertifikat hat der vertrauende Dritte zumindest Folgendes unabhängig zu prüfen:

- die Eignung der Nutzung eines Zertifikats für einen bestimmten Zweck, der durch das vorliegende CPS nicht verboten oder anderweitig beschränkt ist,
- dass die Nutzung des Zertifikats den im Zertifikat enthaltenen KeyUsage-Felderweiterungen entspricht,
- den Status des Zertifikats und aller darüberliegenden CA-Zertifikate der Zertifizierungskette. Falls eines der Zertifikate in der Zertifikatskette gesperrt oder

dessen Gültigkeit abgelaufen ist, darf der vertrauende Dritte auf das Zertifikat oder ein anderes gesperrtes Zertifikat in der Zertifikatskette nicht vertrauen.

4.7 Sperrung von Zertifikaten

4.7.1 Gründe für eine Sperrung

Ein E-Vergabe-Zertifikat wird in den folgenden Fällen durch S-TRUST (oder durch den Zertifikatsinhaber) gesperrt und die Sperrung in einer Sperrliste veröffentlicht, wenn

- der Zertifikatsinhaber seiner Zahlungsverpflichtung innerhalb eines Monats nach Fälligkeit nicht nachkommt.
- S-TRUST, ein am Bündnis-E-Vergabe angeschlossener Anbieter/Betreiber eines E-Vergabe-Systems oder ein Nutzer eines E-Vergabe-Systems Grund zu der Annahme oder den dringenden Verdacht hat, dass der private Schlüssel eines E-Vergabe-Zertifikatsinhabers kompromittiert wurde.
- S-TRUST oder ein am Bündnis-E-Vergabe angeschlossener Anbieter/Betreiber eines E-Vergabe-Systems Grund zu der Annahme hat, dass der Zertifikatsinhaber erheblich gegen eine wesentliche Pflicht, Zusicherung oder Gewährleistung verstoßen hat.
- das Vertragsverhältnis mit dem Zertifikatsinhaber beendet ist oder wegen Vorliegen eines wichtigen Grundes gekündigt wurde.
- die Firma/Organisation, deren Namen in dem Zertifikat enthalten ist, dies verlangt.
- S-TRUST oder ein am Bündnis-E-Vergabe angeschlossener Anbieter/Betreiber eines E-Vergabe-Systems Grund zu der Annahme hat, dass die Ausgabe des Zertifikats auf eine Art und Weise erfolgte, die wesentlich von den im geltenden CPS vorgeschriebenen Verfahren abweicht.
- S-TRUST oder ein am Bündnis-E-Vergabe angeschlossener Anbieter/Betreiber eines E-Vergabe-Systems Grund zu der Annahme hat, dass eine wesentliche Angabe im Zertifikatsantrag nicht der Wahrheit entspricht.
- die Informationen im Zertifikat falsch sind, z. B. weil sich Angaben nach der Zertifikatserstellung geändert haben.

4.7.2 Sperrberechtigte

Die folgenden Parteien sind berechtigt, die Sperrung von Zertifikaten zu beantragen:

- Zertifikatsinhaber: Kann die Sperrung eigener Zertifikate beantragen (und durchführen).
- Bestätigende und/oder für die berufsbezogenen oder sonstigen Angaben zuständigen Stellen: Kann ein Zertifikat sperren lassen, falls im Zertifikat Angaben über diese Stelle aufgenommen wurden (z.B. Firmennamen).
- S-TRUST: Kann die Sperrung von Personenzertifikaten und CA-Zertifikaten entsprechend CPS 4.7.1 beantragen (und durchführen) .

4.7.3 Verfahren für eine Sperrung

4.7.3.1 Sperrung auf Wunsch des Zertifikatsinhabers

S-TRUST sperrt ein E-Vergabe-Zertifikat auf Wunsch des Zertifikatsinhabers nach erfolgter Identifizierung. Die Sperrung kann verlangt werden

- über die Internet-Schnittstelle <https://www.s-trust.de/evergabe-fortgeschritten/sperr/index.htm> (Sperrpasswort erforderlich),
- per Fax, unter der Angabe folgender Daten:
 - Vor- und Nachname entsprechend Zertifikat
 - E-Mail-Adresse entsprechend Zertifikat
 - Sperrpasswort
 - Ort und Datum
 - Unterschrift
- Schriftlich oder per Fax, unter der Angabe folgender Daten:
 - Vor- und Nachname entsprechend Zertifikat
 - E-Mail-Adresse entsprechend Zertifikat
 - Ort und Datum
 - Unterschrift
 - eine persönlich unterschriebene Kopie des Personalausweises oder Reisepasses

4.7.3.2 Sperrung durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle

Sperrungen durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle können schriftlich durch Nachweis der Sperrberechtigung beantragt werden.

Hierfür sind zwingend folgende Angaben notwendig:

- Vor- und Nachname des Zertifikatsinhabers entsprechend Zertifikat
- E-Mail-Adresse des Zertifikatsinhabers entsprechend Zertifikat
- Ort und Datum
- Vor- und Nachname sowie die Unterschrift des Sperrberechtigten bzw. des gesetzlichen Vertreters und Firmenstempel
- Kopie des Personalausweises oder Reisepasses des Sperrberechtigten

Die Angaben sind S-TRUST auf einem Firmenbriefpapier einzureichen.

4.7.4 Fristen für die Beantragung einer Sperrung

Bei einer bekannten, vermuteten oder drohenden Kompromittierung der privaten Schlüssel sind die entsprechenden Zertifikate unverzüglich zu sperren.

4.7.5 Bearbeitungszeit für Anträge auf Sperrung

Sperranträge über die Internet-Schnittstelle werden sofort verarbeitet. Sperranträge, die schriftlich oder per Fax bei S-TRUST eingehen, werden während den Geschäftszeiten umgehend bearbeitet.

4.7.6 Sperrbestätigung für Zertifikatsinhaber

Der Zertifikatsinhaber wird nach erfolgreicher Sperrung seines Zertifikats per E-Mail benachrichtigt. Dabei wird die im Zertifikat angegebene E-Mail-Adresse verwendet.

4.7.7 Prüfung des Zertifikatsstatus' durch Dritte

Vertrauende Dritte dürfen sich nur auf den Inhalt eines E-Vergabe-Zertifikats verlassen, wenn sie zuvor zumindest bei der Prüfung von Signatur- und Verschlüsselungs-/Authentifizierungszertifikaten den Sperrstatus über die entsprechenden Sperrlisten bzw. über den OCSP-Verzeichnisdienst geprüft haben.

4.7.8 Periode für die Erstellung der Sperrlisten

Sperrlisten für E-Vergabe-Zertifikate werden mindestens einmal pro Tag veröffentlicht.

4.7.9 Erscheinungsintervall der Sperrlisten

Die Sperrlisten werden mindestens alle 24 Stunden aktualisiert und unmittelbar nach der Erstellung in die Datenbank gestellt. Die Sperrlisten sind über den im Zertifikat hinterlegten CRL-Verteilungspunkt abrufbar. Über OCSP ist der aktuelle Zertifikatsstatus jederzeit abrufbar.

4.7.10 Online-Verfügbarkeit von Sperr-/Statusinformationen

Informationen zu Sperrung und andere Statusinformationen über Zertifikate sind über eine web-basierte Datenbank unter <http://www.s-trust.de/evergabe-fortgeschritten> sowie über OCSP online abrufbar.

Der Zertifikatsstatus-Service via OCSP hat eine Verfügbarkeit von 99,9 % ohne geplante Unterbrechungen. Geplante Wartungsarbeiten erfolgen i. d. R. außerhalb der typischen Geschäftszeiten.

4.7.11 Spezielle Maßnahmen bei Schlüsselkompromittierung

Sofern bei der Kompromittierung eines privaten Schlüssels der Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter und Geräte unsicher sind, wird eine entsprechende Untersuchung durchgeführt.

5 Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Physikalische Sicherheitsmaßnahmen

5.1.1 Lage und Konstruktion des Standortes

Die Zertifizierungsinfrastruktur von S-TRUST wird in einem baulich geschützten Bereich betrieben, der den Vorgaben der Norm ETSI TS 102 042 entspricht. Für die Betriebssicherheit und den Katastrophenfall werden die IT-Systeme doppelt ausgelegt und betrieben. Die Unterbringung der redundanten Systeme erfolgt in örtlich getrennten Räumen.

5.1.2 Räumlicher Zugang

Folgende Maßnahmen zur Zugangskontrolle gewährleisten einen hohen Schutz gegen unbefugtes Eindringen in die einzelnen Räume und unbefugten Zugriff auf die sicherheitskritischen Systeme und Daten:

- Die IT-Systeme für Zertifizierungsdienste von S-TRUST sind durch 6 Sicherheitsstufen räumlich geschützt.
- Der Zugang zu den ersten 5 Stufen erfordert den Einsatz von kontaktlosen Dienstausweiskarten.
- Ab der Stufe 3 bis Stufe 5 wird zusätzlich Zugangsschutz mittels biometrischer Merkmale eingesetzt.
- In Bereichen, in denen kryptographisches Material erstellt und gespeichert wird, wird Zutritt im Vier-Augen-Prinzip gefordert.
- Der räumliche Zugang wird automatisch protokolliert und per Video aufgezeichnet.
- Unbegleitetes Personal, einschließlich nicht vertrauenswürdiger Mitarbeiter oder Besucher, dürfen diese gesicherten Bereiche nicht betreten.

5.1.3 Stromversorgung und Klimakontrolle

Die gesicherten Einrichtungen von S-TRUST sind mit Stromversorgungssystemen zur Gewährleistung durchgehender, ununterbrochener Zufuhr von elektrischem Strom ausgestattet.

Zur Kontrolle der Temperatur und relativen Luftfeuchtigkeit sorgen Heizungs-/Ventilierungs-/Klimatisierungssysteme. Die Funktion der Klimaanlage wird zentral überwacht.

5.1.4 Schutz vor Wasserschäden

S-TRUST hat angemessene Vorsichtsmaßnahmen getroffen, um die Auswirkungen durch Wassereinträge auf die PKI-Systeme zu minimieren.

5.1.5 Brandschutz

S-TRUST hat angemessene Vorsichtsmaßnahmen getroffen, um Brände oder andere schädigende Einwirkungen durch Flammen oder Rauch zu verhüten. Die Brandschutzmaßnahmen von S-TRUST wurden unter Einhaltung der örtlichen Brandschutzbestimmungen gestaltet.

5.1.6 Schutz von Datenträgern

Datenträger mit sicherheitskritischen Informationen (z. B. Daten-Back-ups) werden innerhalb der Einrichtungen von S-TRUST oder in einer gesicherten Lagereinrichtung an anderer Stelle mit den entsprechenden physischen und logischen Zugangskontrollen zur Beschränkung des Zugangs auf autorisiertes Personal und zum Schutz dieser Datenträger vor Unfallschäden (z. B. Wasser-, Brand- und elektromagnetische Schäden) aufbewahrt. Datenträger mit besonders kritischen Informationen werden ausschließlich in den Schließfächern eines Tresors aufbewahrt.

5.1.7 Entsorgung

Datenträger, die zur Erfassung oder Übertragung von vertraulichen Informationen verwendet werden, werden gemäß den regulären Entsorgungsrichtlinien entsorgt. Sie werden z. B. durch Schreddern des Datenträgers physikalisch unbrauchbar gemacht.

Papierdokumente, die vertrauliche Informationen enthalten, werden vor ihrer Entsorgung geschreddert.

5.1.8 Datensicherung

Bei S-TRUST wird regelmäßig eine Datensicherung der Systemdaten, der Audit-Protokolldaten und anderer vertraulicher Informationen durchgeführt.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Sicherheitskritische Rollen

Sämtliche sicherheitskritische Tätigkeiten der Zertifizierungsdienste sind zu Rollen zusammengefasst, die in einem internen Rollenkonzept beschrieben werden. Diese Tätigkeiten dürfen ausschließlich von Personen durchgeführt werden, die den entsprechenden Rollen zugewiesen sind. Alle diese Rollen sind durch vertrauenswürdige (Sicherheitsüberprüfung) und qualifizierte Mitarbeiter besetzt. Sicherheitskritische Rollen sind insbesondere:

- Registrierungsmitarbeiter,
- Mitarbeiter der Schlüsselgenerierung,
- Mitarbeiter der Systemadministration,
- Sicherheitspersonal,
- zuständiges technisches Personal und
- für die Leitung der vertrauenswürdigen Infrastruktur zuständige leitende Angestellte.

5.2.2 Anzahl benötigter Personen bei sicherheitskritischen Aufgaben

Der Zugriff auf zentrale, sicherheitskritische Systeme der Zertifizierungsdienste wird im Vier-Augen-Prinzip durchgeführt.

5.2.3 Identifikation und Authentifizierung von Rollen

Die Identifikation und Authentifizierung der Rollen erfolgt beim Zutritt zu sicherheitsrelevanten Räumen und beim Zugriff auf sicherheitsrelevante Systeme mithilfe von kontaktlosen Dienstausweiskarten und/oder Benutzername und Passwort.

5.2.4 Trennung von Rollen und Aufgaben

Das Rollenkonzept regelt auch, welche Rollen eine Funktionstrennung erfordern. Dabei liegen die folgenden Regeln zugrunde:

- Die Leitung darf keine operativen oder administrativen Aufgaben übernehmen.
- Auditoren dürfen keine operativen oder administrativen Aufgaben übernehmen.
- Administratoren dürfen keine operativen Aufgaben übernehmen.

- Personen, die die Zutrittsrechte zu den Räumlichkeiten der Zertifizierungsdienste verwalten, dürfen keine sonstigen operativen oder administrativen Aufgaben übernehmen.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Qualifikation, Erfahrung

S-TRUST stellt sicher, dass das für die Zertifizierungsdienste eingesetzte Personal die für seine Aufgabe notwendige Fachkunde, Erfahrung und Qualifikation besitzt. S-TRUST verlangt von Mitarbeitern, die für Zertifizierungsdienste tätig werden möchten, Nachweise vorzulegen über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen. Der Nachweis erfolgt anhand geeigneter Dokumente (z. B. Schulungs-Zertifikate, Arbeitszeugnisse, Ausbildungszeugnisse). S-TRUST führt Schulungen für Mitarbeiter auch selbst durch.

5.3.2 Überprüfung der Vertrauenswürdigkeit

S-TRUST stellt sicher, dass das für die Zertifizierungsdienste eingesetzte Personal die für einen sicheren Betrieb notwendige Zuverlässigkeit besitzt.

Es gelten folgende Voraussetzungen:

- polizeiliches Führungszeugnis, das keine Einträge enthält,
- lückenloser beruflicher Werdegang,
- Zeugnisse ehemaliger Arbeitgeber oder sonstige Referenzen,
- Auskünfte einer Auskunftsdatei (z. B. der SCHUFA),
- Sozialversicherungsnachweise anderer Arbeitgeber,
- Bestätigung, dass die Person nicht Mitglied einer verbotenen Partei oder Vereinigung ist,
- Nachweis der Fachkunde für Zertifizierungsdienste.

Vom Sicherheitsmanager wird in einer Richtlinie festgelegt, welche Vorkommnisse akzeptabel sind und wann ggf. ein Gremium über die Vertrauenswürdigkeit entscheiden muss.

Abweichend hiervon ist S-TRUST berechtigt, für seine Registrierungsstelle neben eigenen Arbeitnehmern auch Dritte, z.B. Leiharbeitnehmer, einzusetzen. Bei Einsatz von Leiharbeitnehmern ist es ausreichend, wenn nachfolgende persönliche Zuverlässigkeitsvoraussetzungen im Arbeitsverhältnis zwischen Leiharbeitnehmer und verleihendem Arbeitgeber erfüllt sind und der verleihende Arbeitgeber sich zur Einhaltung der Voraussetzungen vertraglich verpflichtet hat und S-TRUST zu einer Überprüfung der Einhaltung der Anforderungen berechtigt ist:

- unbefristetes, ungekündigtes Arbeitsverhältnis,
- mindestens 6 Monate beim verleihenden Arbeitgeber beschäftigt,
- polizeiliches Führungszeugnis, das keine Einträge enthält.

5.3.3 Anforderungen an Schulung und Fortbildung

Das für die Zertifizierungsdienste eingesetzte Personal wird vor Aufnahme der Tätigkeit ausreichend geschult. S-TRUST stellt außerdem die zur kompetenten Erfüllung der beruflichen Pflichten erforderliche betriebliche Weiterbildung zur Verfügung. S-TRUST überprüft und erweitert seine Schulungsprogramme regelmäßig nach Bedarf. Die Schulungsprogramme sind auf die individuellen Tätigkeitsbereiche abgestimmt und beinhalten u. a.:

- grundlegende PKI-Konzepte,
- Sensibilisierung für IT-Sicherheit,
- von den Mitarbeitern umzusetzende Sicherheitsmaßnahmen,
- von den Produkten umgesetzte Sicherheitsmaßnahmen,
- Verhalten bei Verletzung der Sicherheitsbestimmungen,
- Einweisung in Notfallmaßnahmen,
- Einsatz von Passwörtern, PINs und Chipkarten,
- Bedeutung der Datensicherung und deren Durchführung,
- Vertraulichkeit der Tätigkeit,
- Umgang mit personenbezogenen Daten.

5.3.4 Nachschulungsintervalle und -anforderungen

S-TRUST bietet seinem Personal im erforderlichen Umfang und den erforderlichen Abständen Auffrischungsschulungen und Fortbildungslehrgänge an, um die Aufrechterhaltung des Leistungsstands sicherzustellen, der zur kompetenten und zufriedenstellenden Erfüllung der beruflichen Pflichten erforderlich ist.

5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Die Trennung von Rollen und Aufgaben gemäß Abschnitt 5.2.4 und die Durchführung sicherheitskritischer Aufgaben im Vier-Augen-Prinzip machen eine regelmäßige Rollenumverteilung nicht erforderlich.

5.3.6 Verfahren bei unbefugten Handlungen

Im Falle unbefugter Handlungen oder anderer Verstöße gegen die Anweisungen, Richtlinien und Verfahren von S-TRUST werden entsprechende Disziplinarmaßnahmen verhängt. Diese Disziplinarmaßnahmen können von Entzug oder Änderung der Aufgaben und Zugriffsrechte bis zur Kündigung gehen und richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen.

5.3.7 Vertragsbedingungen mit dem Personal

S-TRUST verpflichtet die im Zertifizierungsdienst eingesetzten Mitarbeiter auf die Einhaltung von Anweisungen und gesetzlichen Vorschriften. Diese beinhalten insbesondere eine Verpflichtung, personenbezogene Daten vertraulich zu behandeln.

Werden Leiharbeitnehmer eingesetzt, ist durch vertragliche Vereinbarungen mit dem verleihenden Arbeitgeber sicherzustellen, dass die Leiharbeitnehmer entsprechenden Verpflichtungen unterliegen.

Unter eingeschränkten Umständen können externe Personen (unabhängige Auftragnehmer oder Berater) zur Besetzung vertrauenswürdiger Positionen eingesetzt werden. Unabhängigen Auftragnehmern und Beratern, die eine Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen haben, wird der Zugang zu den gesicherten Einrichtungen von S-TRUST nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

5.4 Protokollierung sicherheitskritischer Ereignisse

S-TRUST protokolliert manuell oder automatisch die folgenden wichtigen Ereignisse:

- Ereignisse im Lebenszyklus der Zertifikate und Schlüsselpaare, einschließlich:
 - Registrierung für Zertifikate,
 - Ausstellung von Zertifikaten,
 - Veröffentlichung von Zertifikaten,
 - Auskünfte des OCSP-Verzeichnisdienstes,
 - Sperranfragen an die CA,
 - durchgeführte Sperrungen,
 - Erstellung und Veröffentlichung von Sperrlisten.
- Ereignisse im Lebenszyklus der CA-Zertifikate und Schlüsselpaare, einschließlich
 - Prüfung der Herkunft des Schlüsselpaares,
 - Ausstellung von Zertifikaten,
 - Veröffentlichung von Zertifikaten,
 - Auskünfte des OCSP-Verzeichnisdienstes,
 - Durchgeführte Sperrungen von CA-Zertifikaten,
 - Erstellung und Veröffentlichung von Sperrlisten.
- Sicherheitsrelevante Ereignisse, einschließlich:
 - erfolgreiche und fehlgeschlagene Versuche, auf das PKI-System zuzugreifen,
 - von Mitarbeitern durchgeführte PKI- und Sicherheitssystemoperationen,
 - Lesen, Schreiben oder Löschen sicherheitsempfindlicher Dateien oder Datensätze,
 - Änderungen an Sicherheitsprofilen,
 - Systemabstürze, Hardwarefehler oder andere Anomalien,
 - Firewall- und Router-Vorgänge.
- Ereignisse der Zutrittskontrollanlagen, einschließlich:

- Betreten und Verlassen von gesicherten Räumen,
- fehlgeschlagene Zutrittsversuche und Alarmer,
- Vergabe und Entzug von Zutrittsberechtigungen,
- Beantragung, Ausgabe und Sperrung von Zutrittskarten.

Die Protokolleinträge enthalten die folgenden Daten:

- Uhrzeit und Datum des Eintrags,
- Serien- oder laufende Nummer des Eintrags bei automatischen Journaleinträgen,
- Identität der Stelle, die den Eintrag macht,
- Art des Eintrags.

5.5 Schlüsselwechsel der Wurzel-CA

Ein Schlüsselwechsel der Wurzel-CA ist in folgenden Fällen erforderlich:

- Die Gültigkeit des Zertifikats der Zertifizierungsinstanz läuft ab.
- Es besteht der Verdacht, dass der private Schlüssel der Zertifizierungsinstanz oder der private Schlüssel, mit dem die Wurzel-CA das Zertifikat der Zertifizierungsinstanz signiert hat, kompromittiert wurde.
- Die dem Schlüsselpaar zugeordneten Algorithmen oder die verwendete Schlüssellänge bieten nach aktuellem Wissensstand für die vorgesehene Nutzungsdauer keine ausreichende Sicherheit.

5.6 Archivierung

5.6.1 Arten von zu archivierenden Daten

S-TRUST archiviert:

- alle Daten, die gemäß Abschnitt 5.4 erfasst werden,
- Informationen in Zertifikatsanträgen, zzgl. entsprechender Ausweiskopien,
- Zusatzdokumente zu Zertifikatsanträgen, z. B. Registerauszüge, wenn der Firmen-/ Organisationsname in das Zertifikat aufgenommen wird.

5.6.2 Archivierungsfristen

S-TRUST bewahrt Unterlagen gemäß den gesetzlichen Bestimmungen auf.

5.6.3 Verfahren zur Beschaffung von Archivdaten

Im internen Sicherheitskonzept sind die Vorgaben und Prozeduren für die Beschaffung von Archivdaten festgelegt. Insbesondere ist dort definiert:

- welche Rollen Einsicht in Archivdaten erhalten dürfen,
- welche Art von Dokumenten von den einzelnen Rollen eingesehen werden darf,
- für welche Zwecke Archivdaten von den einzelnen Rollen eingesehen werden dürfen.

5.7 Wiederanlauf nach Katastrophen

5.7.1 Notfallprozeduren

Für das Trustcenter existieren interne Notfallpläne, in denen die Prozeduren und Verantwortlichkeiten bei Notfällen und Katastrophen geregelt sind. Zielsetzung dieser Notfallprozeduren ist die Minimierung von Ausfällen der Zertifizierungsdienstleistungen bei gleichzeitiger Aufrechterhaltung der Sicherheit.

5.7.2 Wiederherstellung nach Kompromittierung von Systemen

Nach einer vermuteten oder tatsächlichen Kompromittierung von Systemen, Software oder Daten finden die Notfallprozeduren Anwendung. Zur Wiederherstellung der kompromittierten Systeme, Software oder Daten werden insbesondere die letzten, von der Kompromittierung nicht betroffenen Sicherungskopien der Systemkonfigurationen und Daten verwendet.

5.7.3 Kompromittierung von CA-Schlüsseln

Im Falle der Kompromittierung oder vermuteten Kompromittierung von privaten Schlüsseln für Zertifizierungsdienste wird das jeweilige Zertifikat sofort gesperrt. Gleichzeitig werden alle mithilfe dieses Zertifikats direkt oder mittelbar ausgestellten Zertifikate gesperrt. Sofern der Verdacht besteht, dass die für die Erzeugung und Anwendung des privaten Schlüssels eingesetzten Algorithmen, Parameter oder Geräte unsicher sind, wird von der Zertifizierungsstelle eine entsprechende Untersuchung durchgeführt. Alle betroffenen Zertifikatsinhaber werden von S-TRUST benachrichtigt.

5.7.4 Notbetrieb im Katastrophenfall

Für den Katastrophenfall wird der Betrieb durch die redundante Infrastruktur aufrechterhalten.

5.8 Betriebsbeendigung

Falls S-TRUST den Betrieb einstellen muss, unternimmt S-TRUST wirtschaftlich angemessene Anstrengungen, E-Vergabe-Zertifikatsinhabern, vertrauende Dritte und andere betroffene Stellen vorab über diese Betriebsbeendigung zu informieren.

Zum Zeitpunkt der Einstellung des Betriebs werden die Zertifikate der E-Vergabe-CA gesperrt und die zugehörigen Schlüssel außer Betrieb genommen.

6 Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsseln

6.1.1 Erzeugung von Schlüsselpaaren

Die Erzeugung der Schlüsselpaare für die Zertifikatsinhaber wird in den Räumlichkeiten von S-TRUST vorgenommen.

Die Schlüsselpaare für die CA-Zertifikate werden ebenfalls in den Räumlichkeiten von S-TRUST generiert. Die zur Schlüsselgenerierung von CA-Zertifikaten verwendeten kryptographischen Module erfüllen die Anforderungen von FIPS 140-1 Level 3.

6.1.2 Auslieferung privater Schlüssel

Die privaten Schlüssel der E-Vergabe-Zertifikate werden in einer sicheren Umgebung bei S-TRUST generiert und dem Zertifikatsantragsteller als passwortgesicherte PKCS#12-Datei per E-Mail zugestellt.

Das zur Aktivierung erforderliche Passwort wird dem Zertifikatsinhaber auf einem nicht elektronischen Weg per Post mitgeteilt.

6.1.3 Übergabe öffentlicher Schlüssel an den Schlüsseleigentümer

Siehe 6.1.2

6.1.4 Schlüssellängen

Die Schlüssel der Root- und CA-Zertifikate entsprechen einer Länge von zurzeit 2048 Bit (RSA-Schlüssel).

Die Schlüssel der Personenzertifikate entsprechen einer Länge von zurzeit 2048 Bit (RSA-Schlüssel).

Die Root-, CA- und Personenzertifikate sind ISIS-MTT-konform und verwenden den Hash-Algorithmus SHA 256.

Diese Mindestlängen können sich ändern, wenn die eingesetzten Algorithmen nicht mehr den Sicherheitsanforderungen entsprechen oder sich die gesetzlichen Vorgaben ändern.

6.1.5 Verwendungszweck der Schlüssel

Die Schlüsselpaare der Zertifikatsinhaber dürfen ausschließlich zu den in Abschnitt 1.4 genannten Zwecken verwendet werden. Der Verwendungszweck ist in der Extension „keyUsage“ der Zertifikate angegeben.

Die privaten Schlüssel der CAs werden ausschließlich zur Signierung von Zertifikaten und Sperrlisten verwendet.

Die privaten Schlüssel des OCSP-Verzeichnisdienstes werden ausschließlich zur Signierung von OCSP-Antworten verwendet.

6.2 Schutz der privaten Schlüssel und kryptographischen Module

S-TRUST hat eine Kombination aus physischen, logischen und verfahrensrechtlichen Kontrollen implementiert, um die Sicherheit von privaten CA-Schlüsseln zu gewährleisten. Zertifikatsinhaber sind dazu verpflichtet, die erforderlichen Vorkehrungen zu treffen, um den Verlust, die Offenlegung, die Änderung oder die unbefugte Nutzung von privaten Schlüsseln zu verhindern.

6.2.1 Standards und Schutzmechanismen der kryptographischen Module

Für die Generierung von Schlüsselpaaren für ausstellende Root-CAs und die Speicherung von privaten CA-Schlüsseln verwendet S-TRUST kryptographische Hardware-Module, die bei FIPS 140-1 Level 3 zertifiziert wurden oder die entsprechenden Anforderungen erfüllen.

6.2.2 Mehrpersonenkontrolle über private Schlüssel

Jeglicher administrativer oder operativer Zugriff auf die privaten Schlüssel der CAs wird im Vier-Augen-Prinzip durchgeführt.

6.2.3 Hinterlegung privater Schlüssel

Die Hinterlegung privater Schlüssel ist nicht vorgesehen.

6.2.4 Sicherung und Wiederherstellung privater Schlüssel

Private Schlüssel der E-Vergabe-CA werden in einem HSM erzeugt und gesichert. Die Sicherung privater Schlüssel von Personenzertifikaten ist nicht vorgesehen.

6.2.5 Archivierung privater Schlüssel

Private Schlüssel der E-Vergabe-CA werden archiviert. Private Schlüssel von Personenzertifikaten werden nicht archiviert.

6.2.6 Speicherung privater Schlüssel

Die privaten Schlüssel zu den Signaturzertifikaten und Verschlüsselungs-/Authentisierungszertifikaten werden durch S-TRUST generiert und den Zertifikatsinhabern als PKCS#12-Datei zur Verfügung gestellt. Die Speicherung der entsprechenden privaten Schlüssel obliegt den Zertifikatsinhabern. Seitens S-TRUST erfolgt keine Speicherung der privaten Schlüssel der Zertifikatsinhaber.

Die privaten Schlüssel der CA-Zertifikate werden ausschließlich in den jeweiligen HSM gespeichert und können nicht ausgelesen werden.

6.2.7 Methoden zur Aktivierung privater Schlüssel

Die privaten Schlüssel zu den Signaturzertifikaten und Verschlüsselungs-/Authentisierungszertifikaten werden durch die Eingabe eines alphanumerischen 16-stelligen Passwortes aktiviert.

Der Zertifikatsinhaber ist angehalten, wirtschaftlich angemessene Maßnahmen zum physischen Schutz seines Arbeitsplatzes zu ergreifen, um die Nutzung des Arbeitsplatzes und seines zugehörigen privaten Schlüssels durch Dritte zu verhindern.

Alle Zertifikatsinhaber müssen die Aktivierungsdaten (Schlüsselpasswort) für ihre privaten Schlüssel gegen Verlust, Diebstahl, Änderung, unbefugte Offenlegung oder unbefugte Nutzung schützen.

6.2.8 Methoden zur Vernichtung privater Schlüssel

Die Vernichtung der privaten Schlüssel zu den Signaturzertifikaten und Verschlüsselungs-/Authentisierungszertifikaten obliegt dem Zertifikatsinhaber.

Falls private CA-Schlüssel nicht mehr verwendet werden, werden diese über Systemeinstellungen außer Betrieb genommen.

6.3 Weitere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Im Rahmen der routinemäßigen Sicherungsverfahren von S-TRUST werden Personenzertifikate und dazugehörige öffentliche Schlüssel gesichert und archiviert.

6.3.2 Verwendungsdauer von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsdauer eines Zertifikats endet mit seinem Ablauf oder durch Sperrung. Die Gültigkeitsdauer von Schlüsselpaaren entspricht der Gültigkeitsdauer der zugehörigen Zertifikate. Sie können jedoch weiterhin zur Entschlüsselung und Signaturüberprüfung verwendet werden.

Die Gültigkeitsdauer der Signatur- und der Authentifizierungs-/Verschlüsselungs-Personenzertifikate beträgt 2 Jahre ab Ausstellungsdatum.

6.4 Sicherheitsbestimmungen für Computer

S-TRUST stellt sicher, dass es sich bei den Systemen zur Verwaltung von CA-Software und Dateien um vertrauenswürdige Systeme handelt, die vor unbefugtem Zugriff sicher sind. Außerdem beschränkt S-TRUST den Zugang zu Produktions-Servern auf Personen mit einem legitimen geschäftlichen Grund für diesen Zugang. Gewöhnliche Anwendungsbenutzer haben kein Benutzerkonto (Account) auf Produktions-Servern.

Das Produktionsnetzwerk von S-TRUST ist von anderen Komponenten logisch getrennt. Diese Trennung verhindert den Netzwerkzugang mit Ausnahme von definierten Anwendungsprozessen. S-TRUST verwendet Firewalls, um das Produktionsnetzwerk vor internen und externen Eindringlingen zu schützen und um die Art und die Quelle von Netzwerkaktivitäten zu beschränken, die auf Produktionssysteme zugreifen können.

S-TRUST verlangt die Verwendung von Kennwörtern, die eine Mindestlänge haben und aus einer Kombination von alphanumerischen Zeichen und Sonderzeichen bestehen. S-TRUST verlangt, dass die Kennwörter regelmäßig geändert werden.

Der direkte Zugriff auf S-TRUST-Datenbanken, die die CA-Operationen von S-TRUST unterstützen, ist auf vertrauenswürdige Personen in der Produktionsbetriebsgruppe von S-TRUST beschränkt, die einen legitimen geschäftlichen Grund für diesen Zugang haben.

6.5 Maßnahmen zur Netzwerksicherheit

S-TRUST hat mehrere Maßnahmen zur Netzwerksicherheit implementiert, darunter die folgenden:

- Die IT-Systeme sind prinzipiell durch Firewalls vom Internet getrennt. Es werden nur Kommunikationswege (Ports) freigeschaltet, die zwingend erforderlich sind.
- Einige Kommunikationsverbindungen zwischen Systemen unterschiedlicher Netzwerksegmente (z. B. Anwender und Zertifikatsverwaltungssystem) sind durch Verschlüsselung und kryptographische Authentifizierung gesichert.
- Mögliche Angriffe oder Missbräuche der öffentlich verfügbaren Systeme werden durch ein Intrusion Detection System überwacht und ggf. abgewehrt.

- Die Sicherheit der Netzwerke wird regelmäßig geprüft. Bei gefundenen Sicherheitslücken werden sofort entsprechende Gegenmaßnahmen eingeleitet.

7 Profile

7.1 Zertifikatsprofile

S-TRUST-Zertifikate basieren auf dem Standard X.509v3 und erfüllen die Anforderungen

- der ITU-T-Empfehlung X.509 (1997): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework vom Juni 1997 und
- von RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile vom April 2002 (“RFC 3280”).

Ferner basieren die ausgestellten Zertifikate im Rahmen auf der E-Vergabe der ISIS-MTT-Spezifikation.

7.2 Profil der Sperrlisten

Die ausgestellten Sperrlisten sind gemäß X.509 v1 aufgebaut.

8 Audits, Revisionen und weitere Prüfungen

S-TRUST führt regelmäßig interne Audits durch, um die Einhaltung der Sicherheitsmaßnahmen sicherzustellen. Neben internen, selbst durchgeführten Audits werden auch externe Prüfungen durchgeführt.

8.1 Identität und Qualifikation des Prüfers

Interne Audits beim DSV werden durch den Sicherheitsmanager durchgeführt. Dieser besitzt umfangreiche Kompetenz und Erfahrung im Bereich IT-Security.

8.2 Veröffentlichung der Ergebnisse der Audits und Revisionen

Die Ergebnisse werden nicht veröffentlicht.

9 Sonstige geschäftliche und rechtliche Bestimmungen

9.1 Vergütung

Es gilt die jeweils aktuelle Preisliste von S-TRUST.

9.2 Vertraulichkeit betrieblicher Informationen

9.2.1 Art der geheim zu haltenden Informationen

Als geheim zu haltende Informationen gelten alle Informationen, die nicht Bestandteil des Zertifikats sind, insbesondere Geschäfts- und Betriebsgeheimnisse .

9.2.2 Öffentliche Informationen

Als öffentlich gelten alle Informationen in ausgestellten und veröffentlichten Zertifikaten, die Sperrlisten sowie alle veröffentlichten Versionen des CPS.

9.3 Vertraulichkeit personenbezogener Informationen

Für personenbezogene Daten gelten die Datenschutzgesetze.

Personenbezogene Daten werden nur unmittelbar beim Betroffenen selbst und nur insoweit erhoben, als dies für Zwecke der Zertifizierungsdienste im Rahmen der E-Vergabe erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere Zwecke dürfen die Daten nur verwendet werden, wenn der Betroffene eingewilligt hat.

Der Betroffene ist berechtigt, eine etwaige Einwilligung zur Speicherung, Verarbeitung, Nutzung und Weitergabe seiner Daten zu darüber hinausgehenden anderen Zwecken jederzeit mit Wirkung für die Zukunft zu widerrufen.

9.4 Geistiges Eigentum

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

9.5 Sorgfalts-, Mitwirkungspflichten u. Obliegenheiten des Zertifikatsinhabers

9.5.1 Aufbewahrung und Nutzung der privaten Schlüssel und Zertifikate

Die privaten Schlüssel und Zertifikate sind mit besonderer Sorgfalt aufzubewahren, um zu verhindern, dass sie missbräuchlich genutzt werden.

Der Zertifikatsinhaber wird die privaten Schlüssel und Zertifikate nur unter Beachtung der Anforderungen an die Einsatzumgebung (z. B. sichere Hard- und Software) nutzen.

9.5.2 Geheimhaltung

Der Zertifikatsinhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von den zum Schutz der privaten Schlüssel verwendeten Identifikationsdaten erlangt. Denn jede Person, die im Besitz der privaten Schlüssel, Zertifikate und/oder der Identifikationsdaten ist, kann diese nutzen und sich im Geschäfts-/Rechtsverkehr als Zertifikatsinhaber ausgeben. Zur Geheimhaltung ist insbesondere Folgendes zu beachten:

- Die Identifikationsdaten (z. B. Passwort, Sperrpasswort) dürfen weder notiert noch elektronisch abgespeichert werden;
- bei Eingabe der Identifikationsdaten (z. B. Passwort) ist sicherzustellen, dass Dritte diese nicht ausspähen können.

9.5.3 Anzeige- und Mitteilungspflichten

Der Zertifikatsinhaber ist verpflichtet,

- bei Verlust eines privaten Schlüssels, Zertifikats und/oder von Identifikationsdaten sowie bei jedem Verdacht einer missbräuchlichen Verwendung unverzüglich sein Zertifikat zu sperren;
- ihm übermittelte Schriftstücke mit Identifikationsdaten (z. B. Brief mit Passwort) unverzüglich auf offensichtliche Mängel (z. B. Beschädigungen) zu untersuchen und solche unverzüglich S-TRUST mitzuteilen. Stellt der Zertifikatsinhaber Beschädigungen fest, darf er ihm übermittelte Identifikationsdaten zur Vermeidung etwaigen

Missbrauchs nicht nutzen, es sei denn, S-TRUST erteilt hierzu eine ausdrückliche Freigabe;

- Mängel, Schäden oder sonstige Störungen unverzüglich S-TRUST anzuzeigen;
- Zertifikate unverzüglich zu sperren oder sperren zu lassen, wenn die darin enthaltenen Angaben nicht oder nicht mehr den Tatsachen entsprechen (z. B. infolge Namensänderung) insbesondere, wenn durch eine Weiterverwendung gegen gesetzliche Bestimmungen verstoßen würde.

9.6 Nutzung durch Dritte

Dem Zertifikatsinhaber werden Entgelte und Schäden zugerechnet, die durch eine befugte oder unbefugte Nutzung der Zertifizierungsdienste durch Dritte dadurch entstanden sind, dass diese Kenntnis von Identifikationsdaten oder Sperrpasswort erhalten haben, wenn und soweit der Zertifikatsinhaber dies zu vertreten hat. Für die Haftung von S-TRUST gilt im Übrigen Kapitel 9.9.

9.7 Haftung des Zertifikatsinhabers

Der Zertifikatsinhaber haftet für Schäden, die S-TRUST durch von ihm verursachte fehlerhafte Angaben in einem Zertifikat sowie durch von ihm zu vertretenden fehlerhaften Einsatz der Zertifizierungsdienste entstehen. Eine weitergehende Haftung des Zertifikatsinhabers nach den gesetzlichen Bestimmungen bleibt unberührt.

9.8 Störungen

S-TRUST wird Störungen seiner technischen Einrichtungen im Rahmen der bestehenden betrieblichen und technischen Möglichkeiten, spätestens jedoch innerhalb von höchstens 24 Stunden, beseitigen.

Vorübergehende Störungen der technischen Einrichtungen von S-TRUST bis zu 3 Stunden gelten nicht als Pflichtverletzung und begründen keine Ansprüche des Zertifikatsinhabers gegen S-TRUST, insbesondere sind in diesem Fall ausgeschlossen Minderung oder – auch anteilige – Rückzahlung der Vergütung, Schadenersatzansprüche.

Aufgrund der Struktur des Internets hat S-TRUST keinen Einfluss auf die Datenübertragung im Internet und übernimmt deshalb keine Verantwortung für die Verfügbarkeit, Zuverlässigkeit und Qualität von Telekommunikationsnetzen, Datennetzen und technischen Einrichtungen Dritter. Leistungsstörungen aufgrund höherer Gewalt hat S-TRUST nicht zu verantworten.

Ist der Zertifikatsinhaber privater Verbraucher, stehen ihm bei offensichtlicher Schlechtleistung durch S-TRUST Ansprüche nur zu, wenn der Zertifikatsinhaber S-TRUST diese innerhalb von 2 Wochen nach Bereitstellung der Leistungen schriftlich anzeigt. Zur Fristwahrung genügt die rechtzeitige Absendung der Anzeige über die Schlechtleistung.

Ist der Zertifikatsinhaber Unternehmer, so gelten die gesetzlichen Regelungen (§ 377 HGB) über die Untersuchungs- und Rügepflichten auch für die nach diesem Vertrag erbrachten Leistungen.

9.9 Haftung von S-TRUST

Schadenersatzansprüche des Zertifikatsinhabers, gleich aus welchem Rechtsgrund, sowie seine Ansprüche auf Ersatz vergeblicher Aufwendungen sind ausgeschlossen, es sei denn, die Schadensursache beruht auf einer zumindest fahrlässigen Verletzung wesentlicher Vertragspflichten (Kardinalpflichten); in diesem Falle ist die Haftung der Höhe nach auf den typischerweise vorhersehbaren Schaden begrenzt. Dies gilt auch bei Verzug oder Unmöglichkeit von S-TRUST.

Gegenüber Unternehmen, juristischen Personen des öffentlichen Rechts und öffentlich-rechtlichem Sondervermögen haftet S-TRUST auch nicht für sogenannte (Mangel-) Folgeschäden, entgangenen Gewinn und sonstige Vermögensschäden.

Die vorstehende Haftungsbegrenzung gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, aufgrund grober Fahrlässigkeit oder Vorsatz sowie bei arglistigem Verschweigen eines Mangels oder arglistiger Täuschung, bei einer verschuldensunabhängigen Haftung, z. B. nach dem Produkthaftungsgesetz, allgemeinen Gleichbehandlungsgesetz oder soweit S-TRUST ausnahmsweise eine Garantie übernommen hat.

Im Umfang der vorstehenden Haftungsbeschränkung verzichtet der Zertifikatsinhaber auf Ansprüche aus Verschulden bei Vertragsverhandlungen (Culpa in contrahendo).

Die Haftungsbeschränkung gilt auch gegenüber Dritten, die in den Schutzbereich der Vertragsbeziehung einbezogen werden, sowie zugunsten der gesetzlichen Vertreter, Arbeitnehmer, Mitarbeiter oder sonstigen Verrichtungs- und Erfüllungsgehilfen von S-TRUST. Die vorstehende Haftungsbeschränkung gilt für vertrauende Dritte in gleicher Weise.

9.10 Verjährung

9.10.1 Verkürzung der regelmäßigen Verjährungsfrist

Für vertragliche Ansprüche, bei denen der Beginn der Verjährungsfrist von der Kenntnis der den Anspruch begründenden Umstände und der Person des Schuldners abhängt oder davon, dass diese Kenntnis ohne grobe Fahrlässigkeit hätte erlangt werden müssen, gilt anstelle der regelmäßigen Verjährungsfrist von 3 Jahren (§ 195 BGB) eine Verjährungsfrist von 2 Jahren.

9.10.2 Verkürzung der 10-jährigen Verjährungsfrist

Für vertragliche Schadenersatzansprüche, die gemäß § 199 Abs. 3 Nr. 1 BGB ohne Rücksicht auf die Kenntnis oder grob fahrlässige Unkenntnis in 10 Jahren von ihrer Entstehung an verjähren, gilt anstelle der 10-jährigen Verjährungsfrist eine Verjährungsfrist von 8 Jahren.

9.10.3 Verjährung von Mängelrechten

Für auf Kaufrecht beruhende Mängelansprüche gilt anstelle der 2-jährigen Verjährungsfrist (§ 438 Abs. 1 Nr. 3 BGB) eine Verjährungsfrist von 1 Jahr; ausgenommen ist der Verbrauchsgüterkauf über neue Sachen, für den die gesetzliche 2-jährige Verjährungsfrist gilt.

9.10.4 Geltung gesetzlicher Regelungen

Bei einer von S-TRUST zu vertretenden Verletzung von Leben, Körper oder Gesundheit sowie bei einem sonstigen Schaden, der auf einer vorsätzlichen oder grob fahrlässigen

Pflichtverletzung beruht, gelten die gesetzlichen Verjährungsfristen. Die gesetzlichen Verjährungsfristen gelten ferner bei arglistigem Verschweigen eines Mangels und bei Rückgriffsansprüchen nach §§ 478 f. BGB.

Im Übrigen gelten die gesetzlichen Regelungen.

9.11 Gültigkeit des CPS

9.11.1 Gültigkeitszeitraum

Dieses CPS ist vom Tag seiner Veröffentlichung an auf unbestimmte Zeit gültig.

9.11.2 Ende der Gültigkeit

Die Gültigkeit dieses CPS endet mit der Veröffentlichung einer neuen Version, einer Mitteilung von S-TRUST, dass dieses CPS außer Kraft tritt, oder bei Einstellung der Zertifizierungsdienste.

9.12 Anwendbares Recht

Auf die Geschäftsbeziehungen findet – vorbehaltlich der in Artikel 29 des Einführungsgesetzes zum Bürgerlichen Gesetzbuch (EGBGB) zwingend geregelten Ausnahmen – deutsches Recht Anwendung.

9.13 Gerichtsstand

Gerichtsstand ist Stuttgart, sofern der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist. Ein etwaiger ausschließlicher Gerichtsstand bleibt unberührt.

9.14 Vorrang zwingender gesetzlicher Regelungen

Zwingende gesetzliche Regelungen gehen den entsprechenden Bestimmungen im vorliegenden CPS vor; bei einem etwaigen Widerspruch zwischen diesem CPS und zwingenden gesetzlichen Regelungen gelten allein die zwingenden gesetzlichen Regelungen, entgegenstehende Bestimmungen des vorliegenden CPS finden insoweit keine Anwendung.

10 Anhang: Definitionen und Abkürzungen

Aktivierungsdaten	Vertrauliche Daten, mit denen sich ein legitimer Nutzer eines privaten Schlüssels gegenüber dem System, das den Schlüssel speichert, authentisiert und somit den Schlüssel aktiviert. Üblicherweise werden Kennwörter und PINs als Aktivierungsdaten verwendet.
Asymmetrische Kryptoverfahren	Kryptographische Verfahren, die auf 2 verschiedenen Schlüsseln basieren, wobei einer öffentlich und einer privat (geheim) ist. Dadurch ist es möglich, dass jemand mit dem öffentlichen Schlüssel eine Nachricht verschlüsselt, die nur der Besitzer des geheimen Schlüssels wieder entschlüsseln kann.
Attribut	Datenfeld in Zertifikaten und Sperrlisten.
Authentisierung, Authentifizierung	Vorgang des Nachweises der Authentizität durch kryptographische Verfahren. Durch ein festgelegtes Verfahren wird festgestellt, ob jemand wirklich derjenige ist, der er vorgibt zu sein, bzw. dass die Daten wirklich von einer bestimmten Person stammen. Authentisierung bezeichnet dabei den Nachweis, Authentifizierung die Prüfung dieses Nachweises.
Authentisierungszertifikat	Zertifikat zu einem Schlüsselpaar, mit dem eine sichere Authentisierung durchgeführt werden kann.
Authentizität	Echtheit von Daten bzw. ihrer Urheberschaft.
CA	Certification Authority – englischer Begriff für eine Zertifizierungsinstanz.
Certification Practice Statement (CPS)	Darlegung der Praktiken, die ein Zertifizierungsdiensteanbieter bei der Ausgabe der Zertifikate anwendet.
CRL	Certificate Revocation List – Sperrliste.
Dienstekarte	Chipkarte, mit der die CA und der OCSP-Verzeichnisdienst Signaturen erstellen. Die Dienstekarten sind sichere Signaturerstellungseinheiten.
DistinguishedName (DN)	Namensform nach X.501. Ein DN besteht aus verschiedenen Attributen und entsprechenden Werten und soll eine Entität eindeutig kennzeichnen. Die wichtigsten Attribute in dieser CPS sind

CommonName (cn), Organization (o) und Country (c).

(D-U-N-S)-Nummer

Mit der D&B D-U-N-S Nummer können Unternehmen eindeutig ihren Muttergesellschaften, Niederlassungen, Hauptsitzen und Filialen zugeordnet werden. D-U-N-S Nummern werden zentral von D&B vergeben und gepflegt. Jede Nummer wird nur einem Unternehmen zugeteilt. Somit kann das Unternehmen auch dann identifiziert werden, wenn sich z. B. die Firmierung ändert.

Elektronische Signatur

Daten, die mit anderen elektronischen Daten logisch verknüpft sind und mit denen sich deren Authentizität und Integrität prüfen lassen. D. h., mittels einer elektronischen Signatur kann sowohl die Unverfälschtheit einer Nachricht als auch der Unterzeichner eines elektronischen Dokumentes verifiziert werden.

FIPS 140-1

US-amerikanischer Standards zur Prüfung und Bewertung der Sicherheit kryptographischer Soft- und Hardware. FIPS 140-1 unterscheidet 4 Levels, wobei Level 1 die geringsten und Level 4 die höchsten Anforderungen an die Sicherheit stellt.

Hashfunktion

Funktion zur Berechnung von Prüfsummen-Länge. Für digitale Signaturen werden Hashfunktionen verwendet, die kollisionsresistent sind, d.h. zu denen sich nach heutigem Kenntnisstand keine zwei Eingaben finden lassen, deren Funktionswert gleich ist.

Hardware-Sicherheitsmodul (HSM)

Gerät zur sicheren Speicherung und Anwendung kryptographischer Schlüssel. Im Unterschied zu Chipkarten besitzen HSMs meist eine eigene Stromversorgung und implementieren oft aufwendige Sicherheitsmechanismen wie ein sicheres Key-Back-up von Schlüsseln, die Protokollierung sicherheitsrelevanter Ereignisse oder ein rollenbasiertes Zugriffskonzept.

HTTP

Hypertext Transfer Protocol – besonders im Internet verbreitetes Kommunikationsprotokoll.

ISIS-MTT

Spezifikation für Datenformate, Kommunikationsprotokolle und Prozeduren in einer PKI.

LDAP	Lightweight Directory Access Protocol – von der IETF standardisiertes Protokoll zum Zugriff auf Verzeichnisse.
OCSP	Online Certificate Status Protocol – von der IETF standardisiertes Protokoll zur Online-Abfrage von Statusinformation von Zertifikaten.
OCSP-Responder	Server, der einen OCSP-Verzeichnisdienst implementiert.
OCSP-Verzeichnisdienst	Verzeichnisdienst, der Zertifikate und ihren aktuellen Sperrstatus über das OCSP-Protokoll bereitstellt.
Öffentlicher Schlüssel	Nicht-geheimer Teil eines Schlüsselpaars bei asymmetrischen Schlüsselpaaren.
PIN	Personal Identification Number – Geheimzahl zur Authentifizierung eines Individuums z. B. gegenüber einer Chipkarte.
PKCS	Public Key Cryptography Standard – Standard für kryptographische Verfahren, Datenformate und Schnittstellen in einer PKI.
PKI	Public Key Infrastruktur – technisches Umfeld für den Einsatz asymmetrischer Kryptoverfahren. Eine PKI basiert üblicherweise auf Zertifikaten und einer Zertifizierungshierarchie. Wichtige Komponenten einer PKI sind daher die Zertifizierungsinstanzen, Registrierungsinstanzen und Verzeichnisdienste. Darüber hinaus umfasst die PKI aber auch die Teilnehmer (Anwender), dezentrale Komponenten wie z. B. Client-Komponenten zur Speicherung und Anwendung der Schlüssel und Zertifikate sowie umfassende technische und organisatorische Prozesse.
Privater Schlüssel	Geheimer Teil eines Schlüsselpaars bei asymmetrischen Schlüsselpaaren.
Registrierungsmitarbeiter	Rolle im Zertifizierungsdienst von S-TRUST, der die Registrierung der Antragsteller durchführt.
Registrierungsinstanz	Stelle eines Zertifizierungsdienstes, die die Anträge zur Ausstellung oder Sperrung von Zertifikaten erfasst und die Antragsteller identifiziert.
RFC	Request for Comment – Dokumententyp der Internet Engineering Task Force (IETF), in der diese Standards vorschlägt und veröffentlicht.
Wurzel-CA	Oberste Zertifizierungsinstanz einer Zertifizierungshierarchie. Das Zertifikat der Wurzel-

	CA wird von ihr selbst signiert und muss den Teilnehmern der PKI auf eine vertrauenswürdige Weise (z. B. offline) zugänglich gemacht werden.
RSA	Asymmetrisches Kryptoverfahren für Verschlüsselung und digitale Signatur, benannt nach Rivest, Shamir, Adleman.
SHA-256	Vom US-amerikanischen Standardisierungsinstitut normierte Hashfunktion.
Sperrliste	Liste, in der ein Anbieter eines Zertifizierungsdienstes die Sperrinformation der von ihm ausgestellten und noch nicht abgelaufenen Zertifikate veröffentlicht.
Sperrstatus	Status eines Zertifikats bzgl. Sperrung.
URL	Uniform Resource Locator – Adresse von Systemen oder Daten im Internet.
Verschlüsselungszertifikat	Zertifikat zu einem Schlüsselpaar, das eine verschlüsselte Kommunikation ermöglicht.
Verzeichnisdienst	In einer PKI: Dienst, über den Zertifikate oder Informationen zu Zertifikaten (z. B. Sperrinformationen) oder zur PKI abgerufen werden können.
X.501	Von der ITU definierter Standard, der die Struktur von Verzeichnissen und entsprechende Namensformen zur Identifizierung der Objekte in Verzeichnissen festlegt.
X.509	Von der ITU definierter Standard, der unter anderem die heute überwiegend verwendeten Datenformate für Zertifikate und Sperrlisten definiert
Zertifikat	Eine elektronische Bescheinigung, mit der ein öffentlicher Signaturschlüssel dem Zertifikatsinhaber zugeordnet wird und dessen Identität bestätigt wird. Ein Zertifikat enthält Angaben zum Eigentümer, zum Aussteller und zur Nutzung des Zertifikats sowie den öffentlichen Schlüssel des Eigentümers. Außerdem enthält das Zertifikat eine digitale Signatur, welche die Authentizität und Integrität der im Zertifikat enthaltenen Daten sicherstellt.
Zertifikatsinhaber	Entität, für die das Zertifikat ausgestellt wird. Der Zertifikatsinhaber ist im Zertifikat als „Subject“ eingetragen.
Zertifizierungsdienst	Dienst, der Zertifikate ausstellt oder andere Dienstleistungen im Zusammenhang mit Zertifikaten

	erbringt, beispielsweise Verzeichnisdienste, Zeitstempeldienste, Schlüsselhinterlegungsdienste.
Zertifizierungshierarchie	Hierarchisch geordnete Struktur, bestehend aus den Zertifizierungsinstanzen und den von ihnen ausgestellten Zertifikaten. Auf der untersten Hierarchiestufe stehen die Zertifikate der Endanwender. Unter jeder Zertifizierungsinstanz hängen an entsprechenden Ästen die Entitäten, für die sie Zertifikate ausstellt. Die oberste(n) Zertifizierungsinstanz(en) nennt man Wurzel-CA(s) (Englisch: Root-CA).
Zertifizierungsinstanz	Logische Einheit einer Zertifizierungsstelle zur Ausstellung (Signierung) von Zertifikaten. Jeder Zertifizierungsinstanz sind jeweils ein oder mehrere Schlüsselpaare zur Signierung der Zertifikate zugeordnet.