Sicherheitsrichtlinien des Zertifizierungsdiensteanbieters DATEV

Certification Practice Statement

- Signatur- und Verschlüsselungszertifikate auf SmartCard/mIDentity
- Version 2.5.1
- Datum des Inkrafttretens 07.05.2012

Stand 05 | 12

Dokumentinformationen

Dokumenthistorie

Version	Stand	Kap./Seite	Grund der Änderung, besondere Hinweise
2.5.1	07.05.2012	Kapitel 6.1. Seite 21	Erweiterung um die Zertifikate CA DATEV STD 02, CA DATEV INT 02, CA DATEV BT 02, CA DATEV STD 98, CA DATEV INT 98, CA DATEV BT 98
2.5	31.01.2012	alle	Schaffung einer neuen Dokumenten-struktur nach RFC 3647

Inhaltsverzeichnis

Inhaltsverzeichnis

1 Einführung

1.1 Überblick

Zertifikate: Als Basis für elektronische Signaturen und für elektronische Verschlüsselung dienen Zertifikate. Das sind elektronische Ausweise, die einer Person zugeordnet werden. Neben den persönlichen Daten wie Geschlecht, Name und E-Mail-Adresse des Inhabers enthalten die Zertifikate noch elektronische Schlüssel, die zur Verschlüsselung und Signatur herangezogen werden.

SmartCards: Der Endkunde erhält Benutzerzertifikate von DATEV auf seiner SmartCard. SmartCards sind Chipkarten, auf denen die Daten unveränderbar hinterlegt werden und damit vor Manipulation geschützt sind.

Signaturen: Elektronische Signaturen im Sinne des Signaturgesetzes sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen. Eine einfache elektronische Signatur kann schon aus einem eingescannten Schriftzug bestehen. Im Gegensatz zur fortgeschrittenen oder qualifizierten Signatur werden hierbei keinerlei Identifizierungsmechanismen zu Grunde gelegt. Eine einfache elektronische Signatur hat daher einen eher unverbindlichen Charakter.

Das Signaturgesetz beschreibt drei unterschiedliche Signaturarten:

- die einfache elektronische Signatur,
- die fortgeschrittene elektronische Signatur,
- die qualifizierte elektronische Signatur.

Diese Sicherheitsrichtlinie (als Certification Practice Statement) widmet sich ausschließlich den fortgeschrittenen Signatur- und Verschlüsselungszertifikaten. Sie beschreiben detailliert die Regeln für die Produktion und Ausgabe der SmartCards, für die darauf hinterlegten Zertifikate sowie den für die Freischaltung der Zertifikate erforderlichen Identifizierungsprozess. Fortgeschrittene elektronische Signaturen unterliegen höheren Anforderungen als einfache elektronische Signaturen (ausschließliche Zuordnung zum Signaturschlüsselinhaber, Ermöglichung der Identifizierung des Signaturschlüsselinhabers etc.), erfüllen jedoch nicht die Anforderungen, die nach der EG-Richtlinie für die Anerkennung im Rechtsverkehr vorgegeben werden.

Die fortgeschrittenen elektronischen Signaturen bilden also eine Zwischenstufe zwischen einfachen elektronischen Signaturen und qualifizierten elektronischen Signaturen.

Nach RFC 3647 legt das „Certification Practice Statement (CPS)“ die Praktiken dar, die ein Zertifizierungsdienst bei der Ausgabe der Zertifikate anwendet.

Das vorliegende Dokument ist nach RFC 3647 aufgebaut und enthält die entsprechenden Gliederungspunkte, hierdurch wird eine Überprüfung vereinfacht sowie die Transparenz und die Vergleichbarkeit mit anderen CPS verbessert.

Dementsprechend beschreibt dieses Dokument das Vorgehen des Zertifizierungsdiensteanbieters DATEV eG bei der Beantragung, Generierung, Auslieferung und Verwaltung der von ihm erzeugten fortgeschrittenen Zertifikate.

Diese Sicherheitsrichtlinien sollen Anwendern (Zertifikatsinhabern und -nutzern) als Entscheidungshilfe dienen, um die Vertrauenswürdigkeit der von DATEV eG ausgegebenen Zertifikate einschätzen zu können. Grundkenntnisse bezüglich elektronischer Verschlüsselungsmechanismen und Anwendungen von elektronischen Signaturen werden vorausgesetzt.

1.2 Name und Kennzeichnung des Dokuments

Diese Sicherheitsrichtlinie trägt den Titel:

Sicherheitsrichtlinien des Zertifizierungsdiensteanbieters DATEV eG „Certification Practice Statement“ für Signatur- und Verschlüsselungszertifikate auf SmartCard/mIDentity

Die Versionsnummer 2.5 und tritt am 01.03.2012 in Kraft.

Die OID der maßgeblichen Certification Policy lautet:

(ASN.1 notation) {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)}

(OID) 0.4.0.2042.1.2

Beschreibung: NCP+ certificate policy (Normalized Certificate Policy requiring a secure user device), definiert in ETSI TS 102 042: „Electronic Signatures

and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates“

Die Sicherheitsrichtlinien werden jedes Jahr inhaltlich auf Gültigkeit geprüft und gegebenenfalls aktualisiert. Darüber hinaus werden gravierende Änderungen sofort in die Sicherheitsrichtlinien aufgenommen.

Die Sicherheitsrichtlinien werden im Internet unter:
- www.datev.de/zertifikat-policy-std
- www.datev.de/zertifikat-policy-int
- www.datev.de/zertifikat-policy-bt

für die Öffentlichkeit bereitgestellt. Die Kunden der DATEV eG werden speziell über Internet informiert (z. B. über die DATEV-Homepage www.datev.de).

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen
Die Zertifizierungsstellen (Certification Authority – CA) im Sinne dieses CPS sind die technischen Einrichtungen und organisatorischen Einheiten, mit denen der Zertifizierungsdiensteanbieter DATEV eG die fortgeschrittenen Zertifikate ausstellt und verwaltet. Der Zertifizierungsdiensteanbieter verwendet für die Erstellung der verschiedenen Zertifikatstypen jeweils eine Zertifizierungsstelle, die je einem oder mehreren Schlüsselpaaren zur Signierung der Zertifikate zugeordnet ist.

Die Zertifizierungsstellen „DATEV STD“, „DATEV INT“ und „DATEV BT“ stellen Teilnehmerzertifikate (Endnutzerzertifikate) und Sperrlisten aus.

1.3.2 Registrierungsstellen
Registrierungsstellen (RAs), sind Stellen, die Registrierungen innerhalb oder im Auftrag der DATEV eG durchführen. Dabei stehen für die Bestellung der Zertifikate den DATEV-Mitgliedern und deren Mandanten alle DATEV-Bestellsysteme zur Verfügung. Des Weiteren können Zertifikate per Papierformular angefordert werden. Hierbei erfolgt die Prüfung und Erfassung der Aufträge in einer zentralen Registrierungsstelle innerhalb der DATEV.

1.3.3 Zertifikatsinhaber
Zertifikatsinhaber sind natürliche Personen, für die von einer DATEV-CA Teilnehmerzertifikate ausgestellt werden.

1.3.4 Zertifikatsnutzer
Zertifikatsnutzer sind alle Personen und Organisationen, die Zertifikate einer DATEV-CA nutzen können und Zugang zu den Diensten der DATEV eG haben.

Teilnehmer, die keine Verpflichtungen gegenüber der DATEV eG eingegangen sind, sind nicht Bestandteil dieser Richtlinie.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten
Teilnehmerzertifikate können von Zertifikatsinhabern für sichere Anwendungen zur Authentisierung, elektronischen Signatur sowie zur Nachrichtenentschlüsselung genutzt werden. Zertifikatsnutzer können Teilnehmerzertifikate zur Validierung von Authentisierungen und elektronischen Signaturen sowie zur Nachrichtenentschlüsselung nutzen.

CA-Zertifikate dürfen ausschließlich für CA-Funktionen (Signatur von Teilnehmerzertifikaten und Sperrlisten) verwendet werden.

1.4.2 Verbotene Verwendungen von Zertifikaten
Andere Verwendungsarten als im Teilnehmerzertifikat festgelegt sind nicht zulässig wie z. B. die Erstellung von CA- oder Root-Zertifikaten. CA-Zertifikate dürfen zu keiner anderen Verwendungsart genutzt werden als die in 1.4.1 beschriebenen CA-Funktionen.

1.5 Verwaltung des CPS

Die DATEV eG ist als Zertifizierungsdiensteanbieter verantwortlich für die Aktualisierung und Weiterführung dieser Sicherheitsrichtlinie. Bei gravierenden Inhaltsänderungen oder Inhaltserweiterungen wird eine neue Versionsnummer vergeben. Bei unwesentlichen Inhaltsveränderungen ist die Vergabe einer neuen Versionsnummer nicht notwendig.

Unter meldepflichtige Änderungen fallen Änderungen, die ihrem Wesen nach so gravierend sind, dass der Anwender über ihre Existenz informiert werden muss. Hierzu zählen z. B. Prozessänderungen, Änderungen der Einfuhrbestimmungen, Betriebseinstellungen.

Die DATEV eG verpflichtet sich, gemäß dieser Sicherheitsrichtlinie zu handeln. Ebenso sind Zertifikatsinhaber zur Anerkennung dieser Sicherheitsrichtlinien verpflichtet.

1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird kontinuierlich durch die DATEV eG gepflegt. Die Richtlinie ist durch ein Mitglied der Geschäftsleitung freigegeben. Alle sicherheitsrelevanten Änderungen bedürfen einer erneuten Freigabe. Die Organisation der Dokumentenverwaltung erfolgt durch die:
DATEV eG
Paumgartnerstraße 6-14
DE-90329 Nürnberg

1.5.2 Kontakte/Ansprechpartner

DATEV eG
Abteilung Security-Systeme
Paumgartnerstraße 6-14
DE-90329 Nürnberg
E-Mail info@datev.de
Internet www.datev.de
Telefon +49 911 319-0
Telefax +49 911 319-3196

1.5.3 Verantwortlichkeit über die Vereinbarkeit der Richtlinien mit den Vorgaben nach RFC 3647 und ETSI TS 102 042

Die im Abschnitt 1.5.2 genannte Organisation ist für die Entscheidung verantwortlich, ob diese Sicherheitsrichtlinien und alle entsprechenden Dokumente, die diese Sicherheitsrichtlinien ergänzen oder dieser untergeordnet sind, mit den Vorgaben des RFC 3647 vereinbar sind.

Die Sicherheitsrichtlinie der DATEV erfüllt alle Anforderungen als Certification Practice Statement (CPS) gemäß der technischen Spezifikation ETSI TS 102 042 des European Telecommunications Standards Institute.

Die Erfüllung aller Anforderungen der Spezifikation wird jährlich durch ein Assessment einer „competent independent party“ gemäß ETSI TS 102 042 geprüft und mit einem Zertifikat bestätigt. Die Zertifizierung der DATEV für dieses CPS wurde auf der Basis des „Zertifizierungsschema für Zertifikate des akkreditierten Bereichs der Zertifizierungsstelle der TÜV-Informationstechnik GmbH“, Version 1.2 vom 28.01.2011, TÜViT GmbH durchgeführt. Die TÜViT ist durch die Deutsche Akkreditierungsstelle GmbH (DAkkS GmbH) für IT-Sicherheitsprüfungen anerkannt.

Die Prüfanforderungen wurden gemäß der technischen Spezifikation ETSI TS 102 042 „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates”, Version 2.1.2, 2010-04, European Telecommunications Standards Institute gestaltet. Die anwendbare ETSI Certification Policy ist NCP+; erweiterte standardisierte Certification Policy, die eine sichere Nutzereinheit fordert.

1.6 Definitionen und Abkürzungen

Siehe Anhang A

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der Zertifizierungsdiensteanbieter DATEV eG stellt einen öffentlichen Verzeichnisdienst bereit, in dem die von DATEV erzeugten Zertifikate eingesehen und überprüft werden können.

Hat der Teilnehmer zugestimmt, ist der Download seiner Zertifikate unter www.datev.de/zertifikatsabfrage möglich.

Mögliche Sperren nach Verlust oder Diebstahl der Zertifikate werden in Sperrlisten vermerkt. Die Sperrlisten und der Verzeichnisdienst werden noch bis zu zwei Jahre nach Einstellung der Tätigkeit der CA weitergeführt.

2.1.1 OCSP-Online-Statusprüfung

Mithilfe der DATEV-Software „Sicherheitspaket" ist es möglich, den Status eines Signatur- oder Verschlüsselungszertifikates online abzufragen. Hier erkennt der Anwender, ob ein Zertifikat gültig ist, ob es eventuell gesperrt wurde oder abgelaufen ist. Die Prüfung geschieht über ein Online Certificate Status Protocol (OCSP). Das Zertifikat enthält die für den Zugriff auf den OCSP-Responder notwendige Adresse. Im OCSP-Responder werden die Zertifikate ab dem Datum der Ausstellung bis mindestens 2 Jahre nach Ablauf der Zertifikatsgültigkeit nachprüfbar gehalten. Für den Fall der Einstellung des Betriebs gelten gesonderte Bedingungen (siehe 5.8).

2.1.2 Verfügbarkeit des Statusabfragedienstes

Der Statusabfragedienst ist je 24 Stunden an 7 Tagen der Woche verfügbar. Die maximale Ausfallzeit pro Jahr beträgt 7 Tage.

2.1.3 Online-Statusabfrage

Die Website www.datev.de/zertifikatsabfrage ermöglicht die Abfrage des Status von Signatur- und Verschlüsselungszertifikaten.

2.1.4 Sperrlisten

Sperrlisten werden im Trustcenter zum Schutz vor Zertifikatsmissbrauch geführt. Hier werden alle gesperrten Zertifikate gekennzeichnet. Es empfiehlt sich, bevorzugt die Online-Prüfung mittels OCSP-Protokoll durchzuführen.

2.1.5 Directoryservice (Verzeichnis der öffentlichen Schlüssel für Verschlüsselung)

Das Verzeichnis der Verschlüsselungszertifikate befindet sich unter www.datev.de/zertifikatsabfrage.

Hier finden Sie alle von DATEV ausgegebenen und vom Zertifikatsinhaber zum Download freigegebenen aktuellen Verschlüsselungszertifikate. Lässt ein Zertifikatsinhaber sein zugehöriges Signaturzertifikat sperren, so wird automatisch auch gleichzeitig sein Verschlüsselungszertifikat aus dem Schlüsselverzeichnis entfernt.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der Zertifizierungsdiensteanbieter DATEV eG veröffentlicht folgende Informationen zu DATEV-CA:

- Teilnehmer-Zertifikate, so dies vom Antragsteller gewünscht wurde,
- CA-Zertifikate (Trust-Anchor),
- Sperrung eines CA-Zertifikats,
- Sperrlisten (CRLs) und Statusinformationen,
- dieses CPS,
- Einstellung der Tätigkeit einer CA.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Teilnehmer-Zertifikate werden veröffentlicht, falls dies vom Antragsteller so beantragt wurde. Veröffentlichte Teilnehmer-Zertifikate bleiben bis zum Ende ihrer Gültigkeit sowie mindestens für ein weiteres Jahr bis zum Jahresende abrufbar.

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und mindestens fünf Jahre nach Ablauf der Gültigkeit der CA vorgehalten.

Sperrlisten werden regelmäßig und bis zum Ende der Gültigkeit des ausstellenden CA-Zertifikats ausgestellt. Der Eintrag der Sperrvermerke im Verzeichnisdienst für das Signaturzertifikat und das Verschlüsselungszertifikat sowie die Löschung des Verschlüsselungszertifikats im Directory-Service erfolgt zweimal täglich um ca. 12:00 Uhr und um ca. 21:00 Uhr. Die Aktualisierung der Sperrlisten erfolgt alle 24 Stunden.

Die Sperrlisten werden mindestens ein Jahr nach Ablauf der Gültigkeit der CA vorgehalten.

Wird ein Austausch eines Teilnehmerzertifikats wegen Ablauf der Zertifikatsgültigkeit notwendig, so wird der Zertifikatsinhaber acht Wochen vor Ablauf schriftlich informiert.

Ist die Sperrung eines CA-Zertifikats erforderlich, werden alle Zertifikatsinhaber separat schriftlich oder wahlweise per E-Mail über die Sperrung der Zertifikate sowie den Sperrgrund informiert.

Das CPS wird spätestens zum Gültigkeitsbeginn veröffentlicht und ist mindestens bis zum Gültigkeitsende abrufbar.

Für den Fall, dass die CA ihren Betrieb einstellt, kündigt der Zertifizierungsdiensteanbieter DATEV eG die Einstellung seiner Tätigkeit mindestens drei Monate im Voraus an.

Die Ankündigung erfolgt im Internet auf den Seiten des Zertifizierungsdiensteanbieters.

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 Zertifizierungsdiensteanbieter vorgenommen.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen
Für die Namensvergabe für Zertifikate ist der Standard [X.501] maßgebend. Das Attribut *DistinguishedName* ist für die Namensvergabe obligatorisch.

Sind E-Mail-Adressen in den Zertifikaten enthalten, so werden diese unter der [X.509] Extension *SubjectAltName* im Format nach RFC 822 hinterlegt.

3.1.2 Notwendigkeit für aussagefähige Namen
Personenbezogene Zertifikate werden eindeutig als solche kenntlich gemacht.

Maschinen, Rollen oder pseudonymisierte (nicht personenbezogene) Zertifikate sind, um Verwechslungsfreiheit zu garantieren, ebenfalls als solche kenntlich.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsinhabern
Ein als Pseudonym oder anonym ausgestelltes Zertifikat ist durch die Kennung „:PN" als solches kenntlich. Wenn Zertifikate mit Pseudonymen erstellt werden, so wird die reale Identität des Zertifikatsinhabers in den Unterlagen der RA bzw. CA hinterlegt.

3.1.4 Regeln für die Interpretation verschiedener Namensformen
Maschinen, Rollen oder pseudonymisierte (nicht personenbezogene) Zertifikate müssen, um Verwechslungsfreiheit zu garantieren, als solche kenntlich sein.

Für Verschlüsselungs- bzw. Authentifizierungszertifikate ist die E-Mail-Adresse des Zertifikatshalters im SubjectAltName als RFC822 bzw. innerhalb des DistinguishedName eingetragen. Im Signaturzertifikat ist die E-Mail-Adresse des Zertifikatshalters im SubjectAltName bzw. DN eingetragen.

3.1.5 Eindeutigkeit von Namen
Bei der Vergabe von Namen (Nutzer- oder PKI-Zertifikate) ist sichergestellt, dass der gewählte „Distinguished Name" des Zertifikatsinhabers innerhalb der ausstellenden CA eindeutig ist. Der Name des Ausstellerzertifikates ist innerhalb der teilnehmenden PKI eindeutig.

3.2 Erstmalige Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels
Nach Übernahme der Bestelldaten in das Produktionssystem werden für jeden Zertifikatsinhaber mehrere Zertifikate und die jeweils zugehörigen Schlüsselpaare generiert und auf eine sichere Signaturerstellungseinheit aufgebracht. Der private Schlüssel des Signaturzertifikats wird nach Abschluss der Produktion vernichtet. Damit ist sichergestellt, dass ausschließlich der Zertifikatsinhaber im Besitz des zugehörigen privaten Schlüssels ist. Vor Veröffentlichung des Zertifikats muss der Empfang durch den Zertifikatsinhaber bestätigt werden, siehe 4.4.2.

3.2.2 Authentifizierung von Organisationszugehörigkeiten
Keine Vorgaben

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers
Alle fortgeschrittenen elektronischen Unterschriften müssen an natürliche Personen gekoppelt sein. SmartCard-Inhaber, die die elektronische Signatur nutzen wollen, müssen sich daher bei DATEV identifizieren. Der Zertifikatsinhaber erhält (im Download-Verfahren) ein Identifizierungsformular. Dieses ergänzt er mit seinen persönlichen Daten (Name, Vorname und E-Mail-Adresse) und den Daten seines Personalausweises (Ausweisnummer, Geburtsdatum und Ausstellungsbehörde), unterschreibt das Formular und sendet es anschließend zusammen mit einer Kopie seines Ausweises an das Trustcenter der DATEV eG.
Die Identitätsprüfung erfolgt anhand der eingereichten und gegebenenfalls weiterer Unterlagen. Dabei ist ein Legitimationsniveau sichergestellt wie bei einer persönlichen Identifizierung.

3.2.4 Ungeprüfte Angaben zum Zertifikatsinhaber
Die Registrierungsstelle gewährleistet, dass ungeprüfte Angaben nicht die Verbindung der Person zum Schlüsselpaar, Schlüsselaktivierungsdaten, Name und E-Mail-Adresse betreffen.

3.2.5 Prüfung der Berechtigung zur Antragstellung
Keine Vorgaben

3.2.6 Kriterien für den Einsatz interoperierender Systeme

Die PKI der DATEV eG realisiert die Interoperabilitätsspezifikation „Common-PKI", gemäß den Festlegungen unter http://www.t7ev.org/common-pki.html.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Rekeying)

3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung

Sofern der Zertifikatsinhaber bei Ablauf der Zertifikatsgültigkeit den dazu gehörenden Vertrag bei der DATEV eG nicht kündigt, stellt DATEV eG neue Zertifikate bereit.

3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Einmal durchgeführte Sperrungen können nicht mehr rückgängig gemacht werden. DATEV kann allerdings eine Ersatzkarte mit neuen Zertifikaten erstellen.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Informationen zur Durchführung der Sperrung und Sperrzeit von Zertifikaten stellt das Trustcenter online auf https://karte-sperren.datev.de zur Verfügung. (Zu den Sperrgründen siehe 4.9.1)

Der Sperrantrag kann schriftlich, telefonisch oder online übermittelt werden.

3.4.1 Sperrung durch den Zertifikatsinhaber

Der Zertifikatsinhaber kann sein Zertifikat sperren (Sperrgründe siehe 4.9.1).

3.4.2 Sperrung durch den Vertragspartner

Neben dem Zertifikatsinhaber ist auch der Vertragspartner (in der Regel das DATEV-Mitglied), über den die SmartCard bestellt wurde, berechtigt, die Sperrung der Zertifikate zu veranlassen.

3.4.3 Schriftliche Sperrung

Der schriftliche Sperrantrag ist zu richten an:
DATEV eG
Logistik-Center
90329 Nürnberg
oder per Fax an die Nummer:
+49 911 319-3741

Zur Sperrung der Karte sind folgende Angaben erforderlich:

- Name und Vorname des Zertifikatsinhabers,
- wenn möglich, SmartCard-User-ID (wenn mehrere Zertifikate auf ein und dieselbe Person ausgestellt sind, ist diese Angabe unbedingt erforderlich),
- Beraternummer, unter der die Karte bestellt wurde,
- Unterschrift des Zertifikatsinhabers oder ggf. Unterschrift des Mitglieds, auf dessen Rechnung die Karte bestellt wurde.

3.4.4 Telefonische Sperrung

Unter der Telefonnummer +49 911 319-0 erreichen Sie während der normalen Geschäftszeiten die Zentrale der DATEV eG, die Sie an den zuständigen Ansprechpartner im Logistik-Center weiterleitet.

Zur Sperrung der Karte sind folgende Angaben erforderlich:

- Name und Vorname des Zertifikatsinhabers,
- wenn möglich, SmartCard-User-ID (wenn mehrere Zertifikate auf ein und dieselbe Person ausgestellt sind, ist diese Angabe unbedingt erforderlich),
- Beraternummer, unter der die Karte bestellt wurde.

3.4.5 Online-Sperrung

Um dem Karteninhaber auch an Wochenenden oder Feiertagen eine zeitnahe Sperrung seiner Zertifikate zu ermöglichen, bietet DATEV eine Online-Sperrung mittels einer Internet-Eingabemaske an.

Hierzu ruft der Karteninhaber die URL https://karte-sperren.datev.de auf und kann seine Zertifikate unmittelbar mit User-ID und Sperrpasswort sperren, welches ihm mit dem PIN-Brief übermittelt wurde.

Gibt der Karteninhaber das Sperrpasswort fünfmal hintereinander falsch ein, ist eine Online-Sperrung nicht mehr möglich. Er muss dann auf die anderen beschriebenen Verfahren ausweichen.

3.4.6 Aufhebung der Sperre

Einmal durchgeführte Sperrungen können nicht mehr rückgängig gemacht werden. DATEV kann allerdings eine Ersatzkarte mit neuen Zertifikaten erstellen. Die Preise sind der aktuellen Preisliste zu entnehmen.

4 Betriebliche Maßnahmen

4.1 Zertifikatsantrag
Der Zertifikatsantrag unterstützt die zweifelsfreie Identifizierung des Antragstellers und dokumentiert das Ergebnis des Antragsprozesses.

4.1.1 Wer kann einen Zertifikatsantrag stellen
Die Nutzung der DATEV-Zertifizierungsdienstleistungen ist in der Regel den DATEV-Kunden (Mitglieder und deren Mandanten) vorbehalten.

4.1.2 Registrierungsprozess und Zuständigkeiten
Die Registrierung ist ein wohl dokumentierter Prozess, der die Anforderungen der Identifizierung nach Kapitel 3.2 erfüllt.

Der Zertifikatsantrag enthält Angaben, die den Anspruch auf zweifelsfreie Identifizierung des Zertifikatsinhabers sicherstellen.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung
Vor einer Veröffentlichung der Zertifikate werden die Zertifikatsinhaber zuverlässig nach einem dokumentierten Prozess identifiziert.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen
Die Vorgaben zur Annahme eines Zertifikatsantrages sind dokumentiert.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen
Keine Vorgaben.

4.3 Zertifikatsausgabe

4.3.1 Aktionen des Zertifizierungsdiensteanbieters bei der Ausgabe von Zertifikaten
Eine Ausgabe von Zertifikaten erfolgt für angenommene Zertifikatsanträge.

Die Aktionen bei der Zertifikatsausgabe erfolgen anhand dokumentierter Prozesse. Dabei ist sichergestellt, dass die eindeutige Verbindung von Zertifikatsinhaber und privatem Schlüssel besteht.

Nach Übernahme der Antragsdaten in das Produktionssystem werden für jeden Zertifikatsinhaber mehrere Zertifikate und die jeweils zugehörigen Schlüsselpaare generiert und auf eine sichere Signaturerstellungseinheit aufgebracht. Der private Schlüssel des Signaturzertifikats wird nach Abschluss der Produktion vernichtet. Alle Zertifikate werden mit dem Signaturschlüssel des Zertifizierungsdienstes signiert.

Werden vertrauenswürdige Dritte zur Produktion herangezogen, erfüllen diese die gleichen Sicherheitsvorschriften wie DATEV selbst. Die produzierten Signaturerstellungseinheiten werden per Post ausgeliefert. Aus Sicherheitsgründen wird die zur Signatur benötigte PIN mit separater Post verschickt.

4.3.2 Benachrichtigung des Zertifikatsinhabers über die Ausgabe des Zertifikats durch die CA
Es erfolgt keine gesonderte Benachrichtigung des Zertifikatnehmers nach der Fertigstellung des Zertifikats.

4.4 Zertifikatsannahme

4.4.1 Verhalten für eine Zertifikatsannahme
Der Karteninhaber hat bei Erhalt und vor der Nutzung die Inhalte der Zertifikate zu kontrollieren. Die Vorgehensweise finden Sie in der Info-Datenbank im Dokument „Überprüfung der SmartCard-/mIDentity-Zertifikate mit dem Microsoft Internet Explorer" (Dok.-Nr. 1015490).

4.4.2 Veröffentlichung des Zertifikats durch die CA
Ist ein Zertifikatsinhaber als Person identifiziert, werden seine Zertifikate nach Bestätigung des Erhalts in einem automatischen Prozess innerhalb eines vorgegebenen Zeitrasters in die Auskunftssysteme übernommen. Nach Übernahme der Zertifikate stehen diese den Nachfragenden über die beschriebenen Verfahren und Wege zur Verfügung (siehe 2.1.3).

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Zertifikatausgabe
Siehe 2.1.3

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber
Der private Schlüssel eines Nutzers darf nur für Anwendungen benutzt werden, die in Übereinstimmung mit den im Teilnehmerzertifikat angegebenen Nutzungsarten stehen. Die folgenden Nutzungsarten sind vorgesehen:

- Authentifizierung von Benutzer- oder Anwendungsdaten (Nutzungsart digital signature),
- Entschlüsselung von Benutzer- oder Anwendungsdaten oder von symmetrischen Schlüsseln, welche in dem sogenannten Hybridverfahren für die Verschlüsselung solcher Daten dienen (Nutzungsarten data-Encryption bzw. KeyEncryption),
- Kennzeichnung der Verbindlichkeit (Nutzungsart non-repudiation) einer elektronischen Signatur durch den Zertifikatsinhaber.

Der Karteninhaber stellt die Nutzung der Zertifikate nach Ablauf der Gültigkeit bzw. nach Sperrung der Zertifikate ein. Ausnahme: Archivfunktion zur Entschlüsselung von Daten.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber
Der Zertifikatsinhaber darf die Zertifikate nur im Rahmen der definierten Schlüsselverwendung nutzen. Somit ist eine Nutzung von Signaturzertifikaten zur Verschlüsselung (und umgekehrt) nicht zulässig.

4.6 Zertifikatserneuerung

4.6.1 Bedingungen für eine Zertifikatserneuerung
Endanwenderzertifikate werden mit einer Geltungsdauer von fünf Jahren erteilt. Die Zertifikate werden nicht über die ursprüngliche Geltungsdauer verlängert. Bei Ablauf der Gültigkeit von Zertifikaten wird ein Folgezertifikat ausgestellt. Sofern der Zertifikatsinhaber bei Ablauf der Zertifikatsgültigkeit den dazu gehörenden Vertrag bei der DATEV eG nicht kündigt, stellt DATEV eG neue Zertifikate bereit.

Wird ein Austausch eines Teilnehmerzertifikats wegen Ablauf der Zertifikatsgültigkeit notwendig, so wird der Zertifikatsinhaber acht Wochen vor Ablauf schriftlich informiert.

4.6.2 Wer darf eine Zertifikatserneuerung beantragen
Die Erneuerung kann bei Bedarf durch Zertifikatsinhaber oder das DATEV-Mitglied beauftragt werden.

4.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung
Siehe 4.6.1

4.6.4 Benachrichtigung des Zertifikatsinhabers über die Ausgabe eines neuen Zertifikats
Die Benachrichtigung des Zertifikatsinhabers folgt entsprechend dokumentierter Prozesse (siehe 4.6.1 und 4.3.2).

4.6.5 Verhalten für die Annahme einer Zertifikatserneuerung
Anhand dokumentierter Prozesse wird die sichere Übergabe und Bedingungen, die zu einer Annahme des Zertifikates führen, beschrieben.

4.6.6 Veröffentlichung der Zertifikatserneuerung durch die CA
Siehe 2.1

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Erneuerung des Zertifikats
Erneuerte Zertifikate werden nach Erfüllung der Vorgaben an den Zertifikatsinhaber unverzüglich in den Verzeichnisdienst eingestellt.

4.7 Zertifizierung nach Schlüsselerneuerung

Nicht zutreffend.

4.8 Zertifikatsänderung

Eine Änderung im Zertifikat führt zur Neuausstellung. Mögliche Gründe sind:
- der Name im Zertifikat erlaubt keine eindeutige Zuordnung zum Zertifikatsinhaber,
- die Zuordnung der im Zertifikat enthaltenen E-Mail-Adresse zum Zertifikatshalter ist nicht mehr gegeben.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Bedingungen für eine Sperrung
Eine Sperrung muss erfolgen, wenn
- ein Zertifikat Angaben enthält, die nicht oder nicht mehr der Realität entsprechen (z. B. Namenswechsel nach Heirat),
- Schwächen im verwendeten Kryptoalgorithmus bekannt werden,
- die geheimen Schlüssel kompromittiert werden,
- der Kartenvertrag gekündigt wird,
- der Zertifizierungsdienst seinen Betrieb einstellt,
- bei Zahlungsverzug.

Der Zertifikatsinhaber hat die Möglichkeit, sein Zertifikat aus folgenden

Gründen zu sperren:
- Die SmartCard wird verloren oder gestohlen,
- Zertifikate enthalten falsche Angaben,
- die SmartCard ist defekt,
- die SmartCard wird nicht mehr benötigt (Kündigung des Vertrages).

4.9.2 Wer kann eine Sperrung beantragen
Der Zertifikatsinhaber kann sein Zertifikat sperren (Sperrgründe siehe 4.9.1). Neben dem Zertifikatsinhaber ist auch der Vertragspartner (in der Regel das DATEV-Mitglied), über den die SmartCard bestellt wurde, berechtigt, die Sperrung der Zertifikate zu veranlassen.

In bestimmten Fällen ist der Zertifizierungsdienst berechtigt, ohne vorherige Zustimmung des Zertifikatsinhabers Zertifikate zu sperren. Diese sind im Einzelnen in 4.9.1 aufgeführt.

4.9.3 Verfahren für einen Sperrantrag
Der Sperrantrag kann schriftlich, telefonisch oder online übermittelt werden.
Zur Sperrung der Karte sind die nachfolgend beschriebenen Angaben erforderlich.

4.9.4 Schriftliche Sperrung
Siehe 3.4.3

4.9.5 Telefonische Sperrung
Siehe 3.4.4

4.9.6 Online-Sperrung
Siehe 3.4.5

4.9.7 Fristen für einen Sperrantrag
Siehe 4.9.10

4.9.8 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch die DATEV
Erreicht der Kündigungs-/Sperrantrag das Logistik-Center von DATEV, wird er während der normalen Geschäftszeiten entgegengenommen. Die Weitergabe an das DATEV-Trustcenter erfolgt unverzüglich am gleichen Werktag des Antragseingangs (bis spätestens 15:30 Uhr möglich) bzw. am folgenden Werktag nach Ablauf der Kündigungsfrist. Zwischen dem Zeitpunkt der Entgegennahme des Sperrauftrages im Logistik-Center und dem Eintrag des Sperrvermerks im Verzeichnisdienst liegt maximal ein Werktag.

Der Eintrag der Sperrvermerke im Verzeichnisdienst für das Signaturzertifikat und das Verschlüsselungszertifikat sowie die Löschung des Verschlüsselungszertifikats im Directory Service erfolgt zweimal täglich um ca. 12:00 Uhr und um ca. 21:00 Uhr.

4.9.9 Verfügbare Methoden zum Prüfen von Sperrinformationen
Die Prüfung von Sperrinformationen kann über den Abruf von Sperrlisten und über einen OCSP-Dienst erfolgen.

4.9.10 Frequenz der Veröffentlichung von Sperrlisten
Die Aktualisierung der Sperrlisten erfolgt alle 24 Stunden.

4.9.11 Maximale Latenzzeit für Sperrlisten
Die Aktualisierung der Sperrlisten erfolgt alle 24 Stunden. Sperrlisten werden unmittelbar nach ihrer Erzeugung veröffentlicht.

4.9.12 Online-Verfügbarkeit von Sperrinformationen
Zur Onlineprüfung steht ein OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieses Dienstes wird in Form eines URL in den Zertifikaten angegeben und auf der Webseite der DATEV veröffentlicht.

4.9.13 Anforderungen zur Online-Prüfung von Sperrinformationen
Die DATEV empfiehlt den Zertifikatsnutzern dringend die Online-Prüfung von Zertifikaten und weist in Handbüchern und Verfahrensanweisungen darauf hin.

4.9.14 Andere Formen zur Anzeige von Sperrinformationen
Es gibt keine anderen Formen zur Anzeige von Sperrinformationen.

4.9.15 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels
Wird dem Zertifizierungsdiensteanbieter (DATEV) die Kompromittierung eines privaten Schlüssels bekannt, wird das entsprechende Zertifikat gesperrt. Handelt es sich um die Kompromittierung des privaten Schlüssels eines CA-Zertifikats, werden das CA-Zertifikat und sämtliche zugeordneten Teilnehmerzertifikate gesperrt.

4.9.16 Bedingungen für eine Suspendierung
Eine Suspendierung (zeitliche Aussetzung) von Zertifikaten ist nicht vorgesehen. Einmal gesperrte Zertifikate können nicht erneuert oder verlängert werden.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes
Der Statusabfragedienst ist über das Protokoll OCSP verfügbar. Auch mit Hilfe der DATEV-Software „Sicherheitspaket" ist es möglich, den Status eines Signatur- oder Verschlüsselungszertifikates online abzufragen. Hier erkennt der Anwender, ob ein Zertifikat gültig ist, ob es eventuell gesperrt wurde oder abgelaufen ist. Die Prüfung geschieht über ein Online Certificate Status Protocol (OCSP). Das Zertifikat enthält die für den Zugriff auf den OCSP-Responder notwendige Adresse. Im OCSP-Responder werden die Zertifikate ab dem Datum der Ausstellung bis mindestens 2 Jahre nach Ablauf der Zertifikatsgültigkeit gehalten. Für den Fall der Einstellung des Betriebes gelten gesonderte Bedingungen.

4.10.2 Verfügbarkeit des Statusabfragedienstes
Der Statusabfragedienst ist je 24 Stunden an 7 Tagen der Woche verfügbar. Die maximale Ausfallzeit pro Jahr beträgt 7 Tage.

4.10.3 Optionale Leistungen
Die Website www.datev.de/zertifikatsabfrage ermöglicht die Abfrage des Status von Signatur- und Verschlüsselungszertifikaten.

Hier sind alle von DATEV ausgegebenen und vom Zertifikatsinhaber zum Download freigegebenen aktuellen Verschlüsselungszertifikate zu finden. Lässt ein Zertifikatsinhaber sein zugehöriges Signaturzertifikat sperren, so wird automatisch auch gleichzeitig sein Verschlüsselungszertifikat aus dem Schlüsselverzeichnis entfernt.

4.11 Kündigung durch den Zertifikatsinhaber
Im Fall einer Kündigung durch den Zertifikatsinhaber wird das Zertifikat unverzüglich gesperrt.

4.12 Schlüsselhinterlegung und Wiederherstellung

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel
Für die privaten Signaturschlüssel der Zertifikatsinhaber (der Kunden) gibt es kein Backup-Konzept. Sie sind ausschließlich auf der sicheren Signaturerstellungseinheit (SmartCard) der Teilnehmer gespeichert und können nicht wiederhergestellt werden.

Die privaten Verschlüsselungsschlüssel der Zertifikatsinhaber können auf Anforderung der Zertifikatsinhaber wiederhergestellt werden. Hierzu ist im Trustcenter ein Verfahren implementiert, das bei einem Defekt der Erstkarte die Herstellung einer Ersatz-SmartCard mit dem gleichen privaten Verschlüsselungsschlüssel ermöglicht. Dabei werden die privaten Verschlüsselungsschlüssel der Zertifikatsinhaber innerhalb der sicheren Umgebung des Trustcenters verschlüsselt in einer Datenbank hinterlegt. Eine weitere Sicherung der Schlüssel besteht nicht.

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln
Nicht zutreffend.

5 Allgemeine Sicherheitsmaßnahmen

5.1 Bauliche Sicherheitsmaßnahmen

5.1.1 Lage und Gebäude

Die Räumlichkeiten des Trustcenters befinden sich auf dem Betriebsgelände der Fa. DATEV eG in Nürnberg. Die Räume, in denen das Trustcenter untergebracht ist, befinden sich in einem eigenen Sicherheitsbereich, innerhalb eines in Betonbauweise ausgeführten Betriebsgebäudes.

5.1.2 Zugang

Der Gebäudekomplex, in dem sich das Trustcenter befindet, ist mit einer Zutrittskontrollanlage ausgestattet. Die Zugänge werden durch einen Mitarbeiter des Betriebsschutzes oder von der Sicherheitszentrale aus, per Videokamera, überwacht. Es haben nur berechtigte Personen (Mitarbeiter, registriertes Fremdpersonal und angemeldete Besucher) Zutritt. Der Zeitraum des Aufenthalts aller Personen im Betriebsgelände wird dokumentiert. Die Räume des Trustcenters sind durch gesonderte Zutrittskontrollsysteme gesichert. Der Zutritt zu diesem Bereich ist nur für die im jeweiligen Bereich beschäftigten Mitarbeiter sowie Führungspersonal und die zuständigen Administratoren möglich.

5.1.3 Strom, Heizung und Klimaanlage

Die Räume des Trustcenters sind mit einer Klimaanlage ausgestattet, die die Einhaltung der für den Betrieb notwendigen Umgebungstemperatur gewährleistet.

Die sichere Stromversorgung des Trustcenters wird durch eine unterbrechungsfreie Stromversorgung garantiert. Bei längeren Ausfällen der Energiezufuhr übernimmt eine hausinterne Netzersatzanlage die Stromversorgung der Produktionsanlagen.

5.1.4 Wassergefährdung

Alle Räume, in denen technische Komponenten untergebracht sind, verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Brandschutz

Im Trustcenter ist eine Brandmeldeanlage installiert. Die Errichtung erfolgte nach den Richtlinien des VdS (Verband der Sachversicherer). Die Prüfung übernimmt im regelmäßigen Turnus ebenfalls der VdS. Die Anlagen werden aus einer ständig besetzten Sicherheitszentrale überwacht. Im Alarmfall werden von hier aus alle notwendigen Maßnahmen eingeleitet.

5.1.6 Lager und Archiv

Daten mit sensiblen oder sicherheitskritischen Inhalten werden zugriffsgeschützt in abgeschlossenen Räumen oder Tresoren gelagert bzw. archiviert.

5.1.7 Müllbeseitigung

Sämtliche für sicherheitskritische Systeme oder Informationen genutzte Unterlagen, Datenträger und Chipkarten werden vor der Entsorgung gemäß dem Stand der Technik gelöscht bzw. durch physikalische Einwirkung unlesbar bzw. unbrauchbar gemacht.

5.1.8 Desaster Backup

Folgende Daten innerhalb der Zertifizierungsstelle (CA) werden nach vorgegebenen Verfahren gesichert und stehen zur Wiederherstellung nach Notfällen bzw. für Auskünfte bereit:

- Elektronische Schlüssel der CA,
- Antragsdaten der Zertifikatsinhaber,
- Statusdaten zu den Zertifikaten,
- Daten der Auskunftssysteme,
- Protokolldaten.

5.2 Verfahrensvorschriften

Der Betrieb des Zertifizierungsdienstes bzw. der Registrierungsstelle erfolgt anhand von dokumentierten Verfahrensvorschriften im Rahmen der Sicherheits-Policy der entsprechenden Organisation.

5.2.1 Rollenkonzept

Jeder an den Prozessen des Zertifizierungsdienstes beteiligte Mitarbeiter ist einer definierten Rolle zugeordnet, das heißt, er hat eine bestimmte Aufgabe zu erfüllen. Jede Rolle wird in einem Betriebskonzept genau beschrieben. Dort sind alle Tätigkeiten der beschriebenen Rollen genau geregelt.

Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen.

Alle an den Prozessen des Zertifizierungsdienstes beteiligten Mitarbeiter müssen die unter 5.3 beschriebenen Anforderungen erfüllen. Nur unter dieser Voraussetzung können sie eine Rolle innerhalb des Zertifizierungsdienstes übernehmen.

5.2.2 Mehraugenprinzip
Sicherheitskritische Vorgänge müssen mindestens im Vier-Augen-Prinzip durchgeführt werden.

5.2.3 Identifikation und Authentifizierung für einzelne Rollen
Das Rollenkonzept wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutrittsberechtigungen, Abfrage von Wissen und Verfahrensanweisungen durchgesetzt.

Die durchführende Person muss sich, bevor sie Zugriff auf sicherheitskritische Anwendungen erhält, erfolgreich authentifizieren; sie ist rechenschaftspflichtig.

5.2.4 Rollenausschlüsse
Das Rollenkonzept sieht diverse Rollenausschlüsse vor, die verhindern, dass eine Person allein ein Zertifikat ausstellen und in den Verzeichnisdienst einstellen kann.

5.3 Personalkontrolle

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit
Jeder Mitarbeiter des Zertifizierungsdienstes muss bei Neueinstellung ein Führungszeugnis nach § 30 Abs. 1 des Bundeszentralregistergesetzes vorlegen. Voraussetzung für die Einstellung bei DATEV und damit beim Zertifizierungsdienst ist, dass das Führungszeugnis keine Auffälligkeiten, insbesondere keine Einträge bzgl. einer gerichtlichen Verurteilung, aufweist.

Jeder Mitarbeiter, der innerhalb des Zertifizierungsdienstes eine Rolle übernimmt, wird im Rahmen einer Schulung auf seine zukünftige Tätigkeit vorbereitet.

5.3.2 Methoden zur Überprüfung der Rahmenbedingungen
Die Einhaltung der Rahmenbedingungen wird kontinuierlich durch den Trustcenter-Leiter überprüft. Regelmäßige externe Audits sichern die Güte dieses Prozesses.

5.3.3 Anforderungen an Schulungen
Die DATEV schult regelmäßig die Personen, die im Zertifizierungsdienst tätig sind. Ergeben sich Änderungen im Tätigkeitsbereich der Mitarbeiter, werden Ergänzungsschulungen durchgeführt.

5.3.4 Häufigkeit von Schulungen und Belehrungen
Schulungen und Belehrungen finden jährlich statt.

5.3.5 Häufigkeit und Folge von Job-Rotation
Nicht zutreffend.

5.3.6 Maßnahmen bei unerlaubten Handlungen
Schwerwiegende Verstöße gegen Sicherheitsvorkehrungen werden disziplinarisch geahndet.

5.3.7 Anforderungen an freie Mitarbeiter
Nicht zutreffend.

5.3.8 Dokumente, die dem Personal zur Verfügung gestellt werden müssen
Verfahrensanweisungen für Trustcenterleitung, Administratoren und Trustcenter-Mitarbeiter.

5.4 Überwachungsmaßnahmen
Der Zertifizierungsdiensteanbieter betreibt umfangreiche Überwachungsmaßnahmen zur Absicherung der Zertifizierungsdienstleistungen und deren zu Grunde liegenden IT-Systemen und Dokumenten. Diese Maßnahmen sind im Sicherheitskonzept beschrieben.

Die Überwachungsmaßnahmen werden durch organisatorische Regelungen ergänzt. Beispielsweise sieht die Besucherregelung unter anderem vor, dass Besucher mindestens 24 Stunden vor dem Besuch namentlich angemeldet sein müssen und vor ihrem Besuch die Personaldokumente vorlegen. Im Bereich des Trustcenters müssen Besucher stets in Begleitung eines Mitarbeiters des Zertifizierungsdiensteanbieters sein.

Ein weiterer Bestandteil des Sicherheitskonzepts ist eine Risikoanalyse, die Bedrohungen für den Betrieb des Zertifizierungsdiensteanbieters umfassend analysiert sowie Anforderungen und Gegenmaßnahmen definiert. Ferner ist eine Restrisikoanalyse enthalten, in der die Vertretbarkeit des Restrisikos aufgezeigt wird.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Die Archivierung der Identifizierungsunterlagen und Antragsunterlagen der Zertifikatsinhaber erfolgt im Zentralarchiv der DATEV.

Folgende Dokumente werden für jeden Zertifikatsinhaber, der einen Identifizierungsprozess durchlaufen hat, in Papierform (Original) und als elektronisches Dokument archiviert:

- Identifizierungs-Checkliste,
- Ausweiskopie,
- ggf. Bestätigung des Kartenerhalts.

Log-Daten werden im Trustcenter archiviert, ebenso die öffentlichen Schlüssel der Zertifizierungsstelle mit dem Namen CA „DATEV STD", „DATEV INT", „DATEV BT".

5.5.2 Aufbewahrungsfristen für archivierte Daten

Die Dokumente werden mindestens für einen Zeitraum von zehn Jahren, gerechnet ab dem Ausstellungszeitpunkt des jeweiligen Zertifikates, im Archiv aufbewahrt. Technische Log-Daten werden ebenfalls für mindestens zehn Jahre im Trustcenter archiviert. Die Archivierung der öffentlichen Schlüssel der Zertifizierungsstelle erfolgt mindestens sechs Jahre über den Gültigkeitszeitraum hinaus.

5.5.3 Sicherung des Archivs

Das Archiv befindet sich in gesicherten Räumen und unterliegt dem Rollen- und Zutritts-Kontrollkonzept des Trustcenters.

5.5.4 Datensicherung des Archivs

Die Dokumentation erfolgt unverzüglich, so dass sie nachträglich nicht unbemerkt verändert werden kann. Die Vertraulichkeit und Integrität der Daten werden gewahrt. Die Anforderungen des Datenschutzgesetzes werden erfüllt.

5.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Alle Systemzeiten werden täglich kontrolliert.

5.5.6 Archivierung (intern/extern)

Die Archivierung erfolgt im Trustcenter, sowie im gleichwertig gesicherten Zentralarchiv der DATEV eG.

5.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Das Verfahren zur Beschaffung und Prüfung von Archivinformationen unterliegt dem Rollenkonzept des Trustcenters.

5.6 Schlüsselwechsel beim Zertifizierungsdiensteanbieter

Ist der Austausch eines CA-Zertifikats erforderlich, z. B. wegen Ablauf der Gültigkeitsdauer, wird es durch ein neues vom Zertifizierungsdiensteanbieter erstelltes CA-Zertifikat ersetzt. Es ist möglich, dass zu einem bestimmten Zeitpunkt mehrere gültige CA-Zertifikate existieren. Die aktuell gültigen CA-Zertifikate werden unter www.datev.de/zertifikate abruf- und prüfbar gehalten.
Die Angabe der Gültigkeitszeiträume wird über das Internet unter www.datev.de/zertifikate publiziert.

Wird ein Austausch eines Teilnehmerzertifikats wegen Ablauf der Zertifikatsgültigkeit notwendig, so wird der Zertifikatsinhaber acht Wochen vor Ablauf schriftlich informiert.

5.7 Kompromittierung und Geschäftsweiterführung beim Zertifizierungsdiensteanbieter

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Vorfälle werden durch den Zertifizierungsdiensteanbieter bewertet und entsprechend den Vorgaben des Sicherheitskonzeptes behandelt.

5.7.2 Rechnerressourcen-, Software- und/oder Datenkompromittierung

Vorfälle werden durch den Zertifizierungsdiensteanbieter bewertet und entsprechend den Vorgaben des Sicherheitskonzepts behandelt.

5.7.3 Kompromittierung des privaten Schlüssels des Zertifizierungsdiensteanbieter

Wird dem Zertifizierungsdiensteanbieter die Kompromittierung des privaten Schlüssels eines CA-Zertifikats angezeigt, wird das CA-Zertifikat gesperrt.

Ist die Sperrung eines CA-Zertifikats erforderlich, werden folgende Schritte durchgeführt:

1. Alle untergeordneten Endbenutzerzertifikate werden gesperrt.
2. Alle Zertifikatsinhaber werden separat schriftlich oder wahlweise per E-Mail über die Sperrung der Zertifikate sowie den Sperrgrund informiert.

3. Die Sperrung eines CA-Zertifikats wird auf den Internetseiten des Zertifizierungsdiensteanbieters veröffentlicht. Für die CA wird ein Zertifikat mit neuem Schlüsselpaar generiert.
4. Der Vorfall wird durch den Zertifizierungsdiensteanbieter bewertet und entsprechend dem Sicherheitskonzepts des Trustcenters behandelt.

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

Für den Wiederanlauf des Zertifizierungsdienstes nach einem Notfall existiert beim Zertifizierungsdiensteanbieter ein Konzept zur Wiederherstellung des ordnungsgemäßen Betriebes. Das Konzept wird ständig fortgeschrieben. Es garantiert die Wiederherstellung der Systeme und die Weiterführung der Zertifizierungstätigkeit innerhalb einer angemessenen Zeit.

Berücksichtigt sind in dem Wiederanlaufkonzept u. a. Szenarien wie die Kompromittierung eines privaten Schlüssels einer CA, das Bekanntwerden von Schwächen verwendeter Algorithmen, Zerstörung der technischen Infrastruktur durch Brand oder höhere Gewalt etc.

5.8 Schließung eines Zertifizierungsdiensteanbieters oder einer Registrierungsstelle

Sollte die DATEV eG beabsichtigen, den Betrieb des Zertifizierungsdiensteanbieters einzustellen, wird die Einstellung der Tätigkeit mindestens 3 Monate im Voraus angekündigt. Die Ankündigung erfolgt im Internet auf den Seiten des Zertifizierungsdiensteanbieters. Zertifikate, die nach der Ankündigung der Einstellung des Betriebes erstellt worden sind, richten sich in ihrer Gültigkeitsdauer nach dem verbleibenden Zeitraum des Betriebes. Nach der Einstellung der Tätigkeit werden alle noch gültigen Zertifikate gesperrt. Die Sperrlisten und der Verzeichnisdienst werden noch bis zu 2 Jahre nach Einstellung der Tätigkeit weitergeführt. Falls DATEV die Sperrlisten und den Verzeichnisdienst nicht selbst weiterführt, erfolgt dies durch die Firma Deutsche Post Com GmbH (DPCom).

6 Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren
Die Generierung der elektronischen Schlüssel für die Teilnehmerzertifikate erfolgt innerhalb der sicheren Umgebung des Trustcenters ausschließlich auf dafür geeigneten Systemen (siehe 6.2.1).

Die Generierung der CA-Schlüssel wird ausschließlich auf dafür geeignete Systeme (siehe 6.2.1) unter Aufsicht der Zertifizierungsstelle der TÜV Informationstechnik GmbH durchgeführt. Die TÜViT ist durch die Deutschen Akkreditierungsstelle GmbH (DAkkS GmbH) für IT-Sicherheitsprüfungen anerkannt.

6.1.2 Lieferung privater Schlüssel an Zertifikatsinhaber
Die Daten verlassen die sichere Umgebung ausschließlich auf der SmartCard (Sichere Signaturerstellungseinheit (SSEE)).
Bei Nutzung der DATEV E-Mail-Verschlüsselung im Rahmen von DATEVnet sind die unter 6.2.6 genannten Einschränkungen zu beachten.

6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber
Ist ein Zertifikatsinhaber als Person identifiziert, werden seine Zertifikate in einem automatischen Prozess innerhalb eines vorgegebenen Zeitrasters in die Auskunftssysteme übernommen. Nach Übernahme der Zertifikate stehen diese den Nachfragenden über die beschriebenen Verfahren und Wege zur Verfügung.

6.1.4 Lieferung öffentlicher Schlüssel des Zertifizierungsdiensteanbieters an Zertifikatsnutzer
Die öffentlichen Schlüssel der Zertifizierungsdienste sind über die Webseite der DATEV abrufbar.
http://www.datev.de/zertifikate
Zusätzlich werden die Root-Zertifikate auf der SmartCard abgelegt.

6.1.5 Schlüssellängen
Die Schlüssellängen entsprechen dem aktuellen Stand der Technik und Kryptographie.

Für alle CA-Zertifikate und Teilnehmerzertifikate, die den ETSI-TS 102 042 NCP+ Anforderungen genügen, kommen folgende Schlüssellängen und kryptografische Verfahren zum Einsatz:

CA-Zertifikate (CA DATEV STD 01, CA DATEV STD 02, CA DATEV INT 01, CA DATEV INT 02, CA DATEV BT 01, CA DATEV BT 02)
Algorithmen: RSA-Schlüssellänge: 2048 Bit, Hash: SHA-1, Padding: PKCS#1 V. 1.5
Laufzeit: 8 Jahre

Teilnehmerzertifikate
Algorithmen: RSA-Schlüssellänge: 2048 Bit, Hash: SHA-1, Padding: PKCS#1 V. 1.5
Laufzeit: 5 Jahre

CA-Zertifikate (CA DATEV STD 99, CA DATEV STD 98, CA DATEV INT 99, CA DATEV INT 98, CA DATEV BT 99, CA DATEV BT 98)
Algorithmen: RSA-Schlüssellänge: 2048 Bit, Hash: SHA-512, Padding: PKCS#1 V. 1.5
Laufzeit: 8 Jahre

Teilnehmerzertifikate
Algorithmen: RSA-Schlüssellänge: 2048 Bit, Hash: SHA-512, Padding: PKCS#1 V. 1.5
Laufzeit: 5 Jahre

6.1.6 Festlegung der Schlüssel-Parameter und Qualitätskontrolle
Siehe 6.1.5

6.1.7 Schlüsselverwendungen
Die Zertifikatsnutzung (KeyUsage) für Endnutzerzertifikate umfasst:
- Elektronische Signatur (ContentCommitment, früher NonRepudiation),
- Authentifizierung (DigitalSignature) und
- Verschlüsselung (DataEncipherment, KeyEncipherment).

Andere KeyUsages für Endnutzerzertifikate werden in diesem CPS nicht betrachtet.

Die Zertifikatsnutzung (KeyUsage) für CA-Zertifikate umfasst:
- Zertifikatssignatur,
- Offline-Signieren der Zertifikatssperrliste,
- Signieren der Zertifikatssperrliste.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

Die DATEV gewährleistet die ordnungsgemäße Sicherung der privaten Schlüssel.

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module
Die verwendeten kryptographischen Module verwenden anerkannte

Sicherheitsstandards. Als sichere Signaturerstellungseinheiten der Zertifikatsinhaber werden nach Common Criteria EAL5+ evaluierte Prozessorchipkarten eingesetzt.

Für die Schlüssel der CA werden Hochsicherheitsmodule des Typs „ProtectServer Gold“ eingesetzt, diese sind FIPS 140-2 Level 3-konform.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)
Durch das Rollenkonzept wird der Mehrpersonen-Zugriff auf die privaten Schlüssel geregelt und die Umsetzung sichergestellt.

6.2.3 Hinterlegung privater Schlüssel
Die Hinterlegung des privaten Signaturschlüssels eines Teilnehmers der Zertifizierungsstelle ist nicht zulässig. Die Hinterlegung privater Verschlüsselungsschlüssel ist in Kapitel 4.12 beschrieben.

6.2.4 Sicherung privater Schlüssel
Für die privaten Signaturschlüssel der Zertifikatsinhaber (der Kunden) gibt es kein Backup-Konzept. Sie sind ausschließlich auf der sicheren Signaturerstellungseinheit (SmartCard) der Teilnehmer gespeichert und können nicht wiederhergestellt werden.

Der Karten-PIN ist vor unberechtigten Zugriff zu schützen, damit die Nutzung der Karte unter der alleinigen Kontrolle des Karteninhabers ist.

Die privaten Verschlüsselungsschlüssel der Zertifikatsinhaber können auf Anforderung der Zertifikatsinhaber wiederhergestellt werden. Hierzu ist im Trustcenter ein Verfahren implementiert, das bei einem Defekt der Erstkarte die Herstellung einer Ersatz-SmartCard mit dem gleichen privaten Verschlüsselungsschlüssel ermöglicht.

Ein Backup des privaten Schlüssels für den Signaturschlüssel der CA des Zertifizierungsdiensteanbieters ist vorgesehen. Das Verfahren ist im Betriebskonzept des Trustcenters beschrieben. Hierbei werden ausschließlich geeignete kryptografische Module eingesetzt.

6.2.5 Archivierung privater Schlüssel
Der private Schlüssel der Zertifizierungsstelle wird bis zum Ablauf seiner Gültigkeit gesichert, um nach einem Notfall den Wiederanlauf des Betriebs zu gewährleisten. Das Konzept zum Wiederanlauf ist Teil des Betriebskonzeptes des Trustcenters.

Die privaten Verschlüsselungsschlüssel der Zertifikatsinhaber sind innerhalb der sicheren Umgebung des Trustcenters verschlüsselt in einer Datenbank hinterlegt. Eine weitere Sicherung der Schlüssel besteht nicht.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen (DATEV E-Mail-Verschlüsselung)
Die Übertragung der Teilnehmerschlüssel auf die SmartCard (SSEE) erfolgt von dem unter 6.1.1 beschriebenen dedizierten System. Ein Transfer aus der SmartCard heraus ist nicht möglich.

Auf Anforderung des Zertifikatsinhabers kann der archivierte private Verschlüsselungsschlüssel aus dem Trustcenter auf ein System übertragen werden, das zur zentralen Entschlüsselung von E-Mails dient (Entschlüsselungs-Gateway).

Der Transport zum und die Speicherung der privaten Entschlüsselungsschlüssel auf dem Entschlüsselungs-Gateway erfolgt verschlüsselt. Die Anwendung der privaten Schlüssel auf dem Entschlüsselungs-Gateway findet ausschließlich in einem HSM (Hardware-Security-Modul) statt.

Die aus dem Trustcenter im Rahmen der DATEV E-Mail-Verschlüsslung exportierten privaten Entschlüsselungsschlüssel existieren somit außerhalb eines HSMs niemals im Klartext. Zum Versand vertraulicher Mitteilungen über DATEV an den Zertifikatsinhaber verwendet DATEV dessen archivierte öffentliche Verschlüsselungsschlüssel. Eine Veröffentlichung des Verschlüsselungszertifikats an Dritte erfolgt nicht.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen
Die privaten Schlüssel der CA werden in Hardware-Security-Modulen gespeichert, diese sind FIPS 140-2 Level 3-konform.

6.2.8 Aktivierung privater Schlüssel

Private Endanwender-Schlüssel werden durch Eingabe der PIN aktiviert. Die privaten CA-Schlüssel können nur im Vieraugen-Prinzip und von den zuständigen Rollen für die zulässigen Nutzungsarten (keyCertSign, cRLSign) aktiviert werden.

6.2.9 Deaktivierung privater Schlüssel

Die privaten CA-Schlüssel werden durch Beendigung der Verbindung zwischen HSM und Anwendung deaktiviert.

Die jeweilige Anwendung deaktiviert den privaten Endanwender-Schlüssel, spätestens aber das Ziehen der Karte aus dem Kartenleser.

Eine dauerhafte Deaktivierung der privaten Endanwender-Schlüssel auf Chipkarten erfolgt, wenn die PIN-Eingabe aufeinander folgend mehrfach fehlerhaft ist. Die Anzahl der Reaktivierungsvorgänge der Karte durch Eingabe der PUK ist begrenzt.

6.2.10 Zerstörung privater Schlüssel

Für die Zerstörung werden geeignete Verfahren verwendet.

6.2.11 Beurteilung kryptographischer Module

Der Zertifizierungsdiensteanbieter betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren, um die Qualität der erzeugten Endanwender-Schlüssel zu sichern. Die eingesetzten HSMs sind FIPS 140-2 Level 3-konform.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Die öffentlichen Schlüssel der Zertifizierungsstelle mit dem Namen CA „DATEV STD", „DATEV INT", „DATEV BT" werden archiviert. Die Archivierung erfolgt mindestens sechs Jahre über den Gültigkeitszeitraum hinaus. Die öffentlichen Schlüssel der Teilnehmer sind online über die Prüfroutinen der DATEV-Software „Sicherheitspaket" zugänglich.

Hat der Teilnehmer zugestimmt, ist der Download seiner Zertifikate unter www.datev.de/zertifikatsabfrage möglich.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Siehe 6.1.5

6.4 Aktivierungsdaten

Der PIN-Brief mit den Aktivierungsdaten wird über einen separaten Postweg an den Zertifikatinhaber versandt. Durch den Einsatz einer so genannten Transport-PIN, mittels der die Karte aktiviert werden muss, ist der Zertifikatinhaber vor Manipulationen geschützt.

Die Aktivierungsdaten der CA-Schlüssel werden gemäß internen Verfahrensanweisungen im 4AP gesichert.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

6.5.1 Spezifische technische Sicherheitsanforderungen

Alle IT-Komponenten der PKI unterliegen den Sicherheitsanforderungen der existierenden IT-Sicherheitsrichtlinien.

6.5.2 Beurteilung von Computersicherheit

Die Beurteilung erfolgt im Rahmen von regelmäßigen internen und externen Audits.

6.6 Technische Maßnahmen während der Lebenszyklen

Die Beurteilung erfolgt im Rahmen von regelmäßigen internen und externen Audits.

6.7 Vorkehrungen zur Netzwerksicherheit

Die Übertragung sicherheitskritischer Daten erfolgt durch eine angemessene Absicherung der Kommunikationskanäle. Alle sicherheitsrelevanten Komponenten, auf die aus dem Internet zugegriffen werden kann, sind durch Firewalls geschützt, die kontinuierlich aktualisiert werden.

6.8 Zeitstempel

Nicht zutreffend.

7 Format der Zertifikate und Sperrlisten

Die von DATEV herausgegebenen Zertifikate und Sperrlisten (CRLs) entsprechen dem [X.509]-Standard (Version 3) sowie dem Common-PKI (Version 2.0) spezifizierten Zertifikats- und Sperrlisten-Profil. Die detaillierte Beschreibung dieser Profile finden Sie unter www.datev.de/zertifikats-profile.

8 Überprüfungen und andere Bewertungen

Siehe 1.5.3

9 Andere finanzielle und rechtliche Angelegenheiten

9.1 Kosten

Die Zertifizierungsdienstleistungen der DATEV eG sind kostenlos (Ausnahme Ersatzkarte). Die Kosten der Lesegeräte finden Sie im Internet unter www.datev.de/smartcard.

9.2 Finanzielle Zuständigkeiten

Hierzu finden die AGB der DATEV Anwendung: www.datev.de/agb

9.3 Vertraulichkeitsgrad von Geschäftsdaten

Die DATEV eG gewährleistet durch geeignete Verschlüsselungsverfahren, dass im Rahmen der DATEV-CA zugängliche Daten (z. B. CPS-Dokumente anderer Teilnehmer) auf Wunsch vertraulich behandelt werden.

9.3.1 Definition von vertraulichen Informationen
Vertrauliche Informationen sind Informationen, die lediglich im Rahmen der Zertifizierungsdienstleistungen zugänglich gemacht werden und nicht für eine breite Öffentlichkeit bestimmt sind.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören
Sperrlisten und öffentliche Zertifikatsverzeichnisse gehören nicht zu den vertraulichen Informationen.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen
Die in 1.5.2 genannte Organisation stellt sicher, dass für vertrauliche Informationen Zuständigkeiten definiert werden und die Einhaltung der Vorschriften von Daten- und Geheimschutz überwacht wird.

9.4 Datenschutz von Personendaten

Die Haftung sowie die rechtlichen Rahmenbedingungen der DATEV eG sind in den für SmartCards geltenden besonderen Bedingungen für SmartCards geregelt (online unter www.datev.de/bedingungen-sc).

9.5 Geistiges Eigentumsrecht

Die Eigentumsrechte an der Certificate Policy und den Schlüsseln des Zertifizierungsdiensteanbieters liegen bei DATEV eG.

9.6 Zusicherungen und Garantien

Die Haftung sowie die rechtlichen Rahmenbedingungen der DATEV eG sind in den für SmartCards geltenden besonderen Bedingungen geregelt: www.datev.de/bedingungen-sc

9.7 Haftungsausschlüsse

Die Haftung sowie die rechtlichen Rahmenbedingungen der DATEV eG sind in den für SmartCards geltenden besonderen Bedingungen geregelt: www.datev.de/bedingungen-sc

9.8 Haftungsbeschränkungen

Die Haftung sowie die rechtlichen Rahmenbedingungen der DATEV eG sind in den für SmartCards geltenden besonderen Bedingungen geregelt: www.datev.de/bedingungen-sc

9.9 Schadensersatz

Die Haftung sowie die rechtlichen Rahmenbedingungen der DATEV eG sind in den für SmartCards geltenden besonderen Bedingungen geregelt: www.datev.de/bedingungen-sc

9.10 Gültigkeitsdauer und Beendigung

Dieses CPS wird kontinuierlich überprüft und aktualisiert und gilt bis auf Widerruf.

9.11 Individuelle Mitteilungen und Absprachen mit Teilnehmern

Die Inhalte der Sicherheitsrichtlinien gelten ausschließlich für den Kundenkreis der DATEV eG. Diese werden sowohl über deren Existenz, über die URL der Sicherheitsrichtlinien, als auch über etwaige Änderungen informiert. Der Kundenkreis wird regelmäßig durch die DATEV eG in geeigneter Form informiert.

Diese Sicherheitsregeln gelten für die von DATEV an ihren Kundenkreis ausgegebenen SmartCards. Darüber hinaus gelten sie auch für die damit im Zusammenhang stehenden Leistungen des DATEV-Trustcenters. Diese müssen prinzipiell dann offen gelegt werden, wenn sie Auswirkungen auf das allgemeine Sicherheitsniveau oder die Preisgestaltung haben.

Im Übrigen – insbesondere für die sonstigen Hard- und Software-Komponenten – gelten gesonderte Bedingungen bzw. die Allgemeinen Geschäftsbedingungen der DATEV

eG (siehe www.datev.de/agb und www.datev.de/bedingungen-sc).

9.12 Ergänzungen

Nachträge zum CPS werden schriftlich ergänzt oder bei elektronischer Abrufbarkeit so ergänzend hinterlegt, dass sie dem Abrufenden unmittelbar als Ergänzung offensichtlich werden.

9.13 Verfahren zur Schlichtung von Streitfällen

Grundsätzlich ist die Abteilung „Security-HW/Rechteverwaltung online" (E-Mail: sc-sicherheitspaket@datev.de) für die Organisation einer einvernehmlichen Konfliktbeilegung zuständig. Ist eine gütliche Einigung unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze nicht zu erreichen, so kann von den DATEV-Mitgliedern der Vertreterrat der DATEV eingeschaltet werden. Die Mitglieder des Vertreterrats sind auf den Internetseiten der DATEV unter www.datev.de/Vertreterrat veröffentlicht.

9.14 Anwendbares Recht

Siehe Bedingungen für SmartCards: www.datev.de/bedingungen-sc

9.15 Einhaltung geltenden Rechts

Siehe Bedingungen für SmartCards: www.datev.de/bedingungen-sc

9.16 Sonstige Bestimmungen

9.16.1 Nutzung im Ausland

Die DATEV-Verschlüsselungs-Software und -Hardware unterliegt sowohl deutschen Exportbestimmungen als auch ausländischen Importbestimmungen. Sowohl die Ausfuhr dieser Produkte als auch die Einfuhr und die Verwendung im Zielland können aus diesem Grund einer Genehmigungspflicht unterliegen. Zuständige Behörde für die Ausfuhr aus Deutschland ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle. Für Einfuhr und Verwendung sind die entsprechenden Behörden im Zielland zuständig.

Um Gesetzesverstöße zu vermeiden, muss daher vor jedem Versenden bzw. jeder Mitnahme der genannten DATEV-Software und DATEV-Hardware die Genehmigungspflicht geklärt sein. Gegebenenfalls notwendige Genehmigungen müssen vorliegen. Erst dann dürfen die betreffenden DATEV-Programme in das jeweilige Zielland ausgeführt bzw. mitgenommen werden. Eine Verletzung der Ausfuhrbestimmungen ist, nach dem deutschen Außenwirtschaftsrecht, eine Verletzung der Einfuhrbestimmungen nach den Gesetzen des Ziellandes strafbar.

Der Versand bzw. die Mitnahme in die EU-Staaten Belgien, Bulgarien, Dänemark, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich (Nordirland und GB) und Zypern kann nach einer entsprechenden Rechtsänderung inzwischen genehmigungsfrei erfolgen. Auf Grund bereits vorliegender Genehmigungen können die genannten DATEV-Produkte derzeit nach Australien, Kanada, Neuseeland, Norwegen, Schweiz, USA, Israel, Indien, Vereinigte Arabische Emirate, Japan und Südafrika versendet werden. Allerdings müssen dabei die entsprechenden Zollformalitäten beachtet werden, da die Ausfuhr ansonsten nicht von der Genehmigung abgedeckt ist.

Für oben nicht genannte Länder ist das Antragsverfahren beim Bundesamt für Wirtschaft und Ausfuhrkontrolle kostenlos. Sollten jedoch Gutachter für das Erwirken einer Einfuhrgenehmigung benötigt werden, so kann dies dem Antragsteller in Rechnung gestellt werden. Genauere Informationen zur Antragstellung und Antragsabwicklung erteilt das Bundesamt für Wirtschaft und Ausfuhrkontrolle. Die für die Ausstellung einer Signaturkarte erforderliche Identifizierung kann problemlos vom Ausland aus durchgeführt werden. Voraussetzung ist ein gültiges Ausweisdokument.

Anhang A

A1 - Abkürzungen

Kürzel	Erläuterung
AGB	Allgemeine Geschäftsbedingungen
ASN	Abstract Syntax Notation
CA	Certificate Authority (Zertifizierungsstelle)
CPS	Certification Practice Statement
CA	Certificate Authority (Zertifizierungsstelle)
CRL	Certificate Revocation List (Sperrliste)
EAL	Evaluation Assurance Level
ETSI-TS	European Telecommunications Standards Institute - Technical Specification
FIPS	Federal Information Processing Standard
HSM	Hardware security module
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PN	Pseudonym
NCP	Normalized Certification Policy gemäß TS 102 042
CRL	Certificate Revocation List (Sperrliste)
OCSP	Online Certificate Status Protocol
OID	object identifier
PIN	Personal identification number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
PUK	Personal Unblocking Key
RA	registration authority
RFC	Request for Comments
SSEE	Sichere Signaturerstellungseinheit (engl. SSCD)
URL	Uniform Resource Locator (einheitliche (Internet-) Ressourcenadresse)
VdS	Verband der Sachversicherer
WWW	World Wide Web

A2 - Referenzierte Dokumente

Kürzel	Quelle
RFC 3647	www.ietf.org/rfc/rfc3647.txt Stand: November 2003
TS 102 042	www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.01.02_60/ts_102042v020102p.pdf Stand: April 2010
[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

Anhang B Cross-Reference

Table 1: Cross-reference RFC 3647 clauses and ETSI policy references

RFC 3647 section	TS 102 042
1 INTRODUCTION	
1.1 Overview	5.1
1.2 Document name and identification	5.2
1.3 PKI participants	5.3 7 Introductory text
1.4 Certificate usage	5.3
1.5 Policy administration	ETSI see covering pages
1.5.1 Organization administering the document	ETSI
1.5.2 Contact person	See cover pages
1.5.3 Person determining CPS suitability for the policy	-
1.5.4 CPS approval procedures	7.1
1.6 Definitions and acronyms	3
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	
2.1 Repositories	7.3.5
2.2 Publication of certification information	7.3.5, 7.3.6, 7.3.4
2.3 Time or frequency of publication	7.3.5, 7.3.6
2.4 Access controls on repositories	7.4.6
3 IDENTIFICATION AND AUTHENTICATION	
3.1 Naming	7.3.3
3.2 Initial identity validation	7.3.1
3.3 Identification and authentication for re-key requests	7.3.2
3.4 Identification and authentication for revocation request	7.3.6
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	
4.1 Certificate Application	7.3.1
4.2 Certificate application processing	7.3.3
4.3 Certificate issuance	7.3.3
4.4 Certificate acceptance	7.3.1
4.5 Key pair and certificate usage	6.2, 6.3
4.6 Certificate renewal	7.3.2

RFC 3647 section	TS 102 042
4.7 Certificate re-key	7.3.2
4.8 Certificate modification	7.3.2
4.9 Certificate revocation and suspension	7.3.6
4.10 Certificate status services	7.3.6
4.11 End of subscription	-
4.12 Key escrow and recovery	7.2.4
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	
5.1 Physical controls	7.4.1, 7.4.4, 7.4.5
5.2 Procedural controls	7.4.5, 7.4.3, 7.4.6
5.3 Personnel controls	7.4.3
5.4 Audit logging procedures	7.4.11
5.5 Records archival	7.4.11
5.6 Key changeover	7.2
5.7 Compromise and Disaster Recovery	7.4.8
5.8 CA or RA termination	7.4.9
6 TECHNICAL SECURITY CONTROLS	
6.1 Key pair generation and installation	7.2.1, 7.2.3, 7.2.8, 7.2.9
6.2 Private Key Protection and Cryptographic Module Engineering Controls	7.2.1, 7.2.2, 7.2.6, 7.2.7
6.3 Other aspects of key pair management	7.2.1, 7.2.2, 7.2.5
6.4 Activation data	7.2.7, 7.2.9
6.5 Computer security controls	7.4.5, 7.4.6, 7.4.7
6.6 Life cycle technical controls	7.4.5, 7.4.6, 7.4.7
6.7 Network security controls	7.4.6
6.8 Time-stamping	N/A
7 CERTIFICATE, CRL, AND OCSP PROFILES	
7.1 Certificate profile	7.3.3 a)
7.2 CRL profile	7.3.6
7.3 OCSP profile	-

RFC 3647 section	TS 102 042
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS	
8.1 Frequency or circumstances of assessment	5.4.1
8.2 Identity/qualifications of assessor	CWA 14172-2 (tbd)
8.3 Assessor's relationship to assessed entity	CWA 14172-2 (tbd)
8.4 Topics covered by assessment	5.4.2, 5.4.3, 8.4
8.5 Actions taken as a result of deficiency	5.4.1, 8.4
8.6 Communication of results	5.4.1
9 OTHER BUSINESS AND LEGAL MATTERS	
9.1 Fees	7 intro
9.2 Financial responsibility	7.5
9.3 Confidentiality of business information	
9.4 Privacy of personal information	7.3.1 o), 7.3.3 e), 7.4.10, 7.4.11 j)
9.5 Intellectual property rights	Cover pages
9.6 Representations and warranties	-
9.7 Disclaimers of warranties	-
9.8 Limitations of liability	6.4
9.9 Indemnities	-
9.10 Term and termination	-
9.11 Individual notices and communications with participants	7.3.4
9.12 Amendments	ETSI Procedures
9.13 Dispute resolution provisions	7.5
9.14 Governing law	-
9.15 Compliance with applicable law	7.4.10
9.16 Miscellaneous provisions	-
9.17 Other provisions	7.5

Partnerschaftliche Zusammenarbeit

Weitere Unterstützung für die Arbeit mit den DATEV-Anwendungen sowie das Neueste über Programme und Dienstleistungen finden Sie unter **www.datev.de/service**.

DATEV eG
90329 Nürnberg
Telefon +49 911 319-0
Telefax +49 911 319-3196
E-Mail info@datev.de
Internet www.datev.de
Paumgartnerstraße 6–14

Art.-Nr. 19586 2012-05-01