

Dokumentation Trustcenter

Certificate Practice Statement

Änderungshistorie:

Version	Stand	Änderungen	Autor	Status
1.0	10.09.2003	Initialversion für Pilotphase 2.1	Georgios Raptis	Intern freigegeben
1.1	11.03.2004	Ergänzungen für TC Phase 2	KG/RK	Entwurf
1.2	06.04.2004	Einarbeitung interner Anmerkungen	KG/RK	Freigabe
1.3	16.09.2004	Ergänzung und Konkretisierung	KG/RK	Freigabe

1	Einleitung.....	4
1.1	Überblick	4
1.2	Identifikation des Dokumentes	4
1.3	Infrastruktur und Anwendungsbereich.....	4
1.4	Kontaktinformationen	5
2	Generelle Vorschriften.....	6
2.1	Verpflichtungen	6
2.2	Haftung.....	7
2.3	Finanzielle Verantwortung.....	7
2.4	Rechtliche Auslegung und Durchsetzung.....	7
2.5	Gebühren	8
2.6	Veröffentlichungen und Verzeichnisdienste	8
2.7	Einhaltung der CPS und Audit.....	9
2.8	Datenschutzrichtlinien	9
2.9	Regelung der Urheberrechte und der Eigentumsrechte	10
3	Identifizierung und Authentisierung	11
3.1	Erstregistrierung	11
3.2	Routinemäßige Erneuerung / Rezertifizierung	12
3.3	Erneuerung / Rezertifizierung nach Revokation, ohne dass der Schlüssel kompromittiert wurde	12
3.4	Revokationsantrag	12
4	Betriebliche Abläufe	13
4.1	Antrag auf Ausstellung von Zertifikaten.....	13
4.2	Ausstellung von Zertifikaten	13
4.3	Entgegennahme von Zertifikaten	13
4.4	Suspendierung und Revokation von Zertifikaten.....	13
4.5	Verfahren zur Sicherheitsüberwachung	14
4.6	Archivierung	15
4.7	Schlüsselwechsel.....	16
4.8	Kompromittierung und Wiederaufnahme des regulären Betriebes.....	16
4.9	Einstellung des Betriebs.....	17
5	Physische, organisatorische und personelle Sicherheitsmaßnahmen.....	18
5.1	Physische Sicherheitsmaßnahmen	18

Certificate Practice Statement

5.2	Organisatorische Sicherheitsmaßnahmen	19
5.3	Personelle Sicherheitsmaßnahmen.....	19
6	Technische Sicherheitsmaßnahmen	21
6.1	Schlüsselpaarerzeugung und Installation.....	21
6.2	Schutz des privaten Schlüssels.....	21
6.3	Weitere Aspekte des Schlüsselmanagements	21
6.4	Aktivierungsdaten.....	21
6.5	Sicherheitsmaßnahmen für Computersysteme	21
6.6	Life-Cycle der Sicherheitsmaßnahmen	22
6.7	Sicherheitsmaßnahmen für Netzwerke	22
6.8	Sicherheitsmaßnahmen für kryptographische Module	22
7	Profile für Zertifikate und Revokationslisten	23
7.1	Profile für Zertifikate	23
7.2	Profil der Revokationslisten.....	23
8	Verwaltung dieses Certification Practice Statement	23
8.1	Ablauf einer Änderung.....	23
8.2	Richtlinien für die Veröffentlichung dieses CPS	23
8.3	Genehmigungsverfahren des CPS.....	23

1 Einleitung

1.1 Überblick

Dieses Certification Practice Statement (CPS) enthält die Richtlinien für den Betrieb des Trustcenters der DGN Service GmbH sowie für die Vergabe von Zertifikaten. Ferner werden in diesem Dokument Informationen über die Anwendung der angebotenen Zertifikate bereitgestellt. Zertifikate werden nach dem Grad der Vertrauenswürdigkeit in Zertifikatsklassen unterteilt. Dabei werden u.a. das Niveau der Identifikationsprüfung sowie die Sicherheit des Schlüsselmediums berücksichtigt. Nähere spezifische Informationen zu den einzelnen Zertifikatsklassen werden in den jeweiligen Certificate Policies (CPs) aufgeführt.

Die hier beschriebenen Richtlinien gelten zusammen mit den Certificate Policies als Maßstab für das Niveau der Sicherheit des Trustcenters und der Zertifikate und bilden die Vertrauensgrundlage der Endteilnehmer und der Öffentlichkeit gegenüber dem Trustcenter.

Certificate Policy und Certificate Practice Statement sind Bestandteil der Allgemeinen Geschäftsbedingungen für Sicherheitsdienstleistungen, die der Teilnehmer mit der Beantragung einer Smartcard anerkennt.

Dieses Dokument bezieht sich auf technische und organisatorische Sachverhalte, die sich nicht auf eine spezielle Zertifikatsklasse beschränken. Es gilt übergreifend für alle Certificate Policies. Die Gliederung sowie die Empfehlungen des RFC 2527 (Version von März 1999) der IETF werden angewandt.

1.2 Identifikation des Dokumentes

Daten:

- Name: Certification Practice Statement des Trustcenters der DGN Service GmbH
- Version: 1.3
- Datum: 16.09.04
- Status: freigegeben
- OID: 1.3.6.1.4.1.15787.2.1.1.1

1.3 Infrastruktur und Anwendungsbereich

Das Trustcenter wird von der Firma DGN Service GmbH betrieben. Es werden Zertifikate für Mitglieder des Gesundheitswesens aber auch für die Öffentlichkeit ausgestellt.

1.3.1 CA

Die Root-CA des DGN Trustcenters ist eine Wurzelinstanz, d.h., der Root-CA Schlüssel ist selbstsigniert. Untergeordnete CA-Zertifikate (Sub-CAs) werden von der Root-CA zertifiziert. Die Sub-CAs zertifizieren die öffentlichen Schlüssel. Die ausgestellten Zertifikate werden u.a. auch in dem CA-System aufbewahrt. Mit den selben Schlüsseln stellen die Root- und Sub-CAs auch Revokationslisten (CRLs) aus.

1.3.2 RA

Das DGN Trustcenter verfügt über eine Registrierungsstelle, die Endteilnehmer sowie Mitarbeiter des Trustcenters identifiziert. Darüber hinaus arbeitet das DGN Trustcenter mit weiteren externen RAs zusammen. Die externen RAs sind an die Sicherheitsrichtlinien des DGN Trustcenters gebunden, so dass ein hohes Sicherheitsniveau garantiert wird.

1.3.3 Endteilnehmer

Die Vergabe von Zertifikaten richtet sich primär, aber nicht exklusiv, an Teilnehmer im Gesundheitswesen. Für die Endteilnehmer existieren verschiedene Zertifikatsklassen, die in den entsprechenden CPs beschrieben werden. Als Endteilnehmer gelten in diesem Zusammenhang natürliche Personen, die für sich selbst, aber auch für Systeme der Datenverarbeitung, wie z.B. Webserver oder Router, Zertifikate beantragen.

1.3.4 Anwendbarkeit

Die Anwendbarkeit der Zertifikate wird in den jeweiligen Certificate Policies definiert.

1.4 Kontaktinformationen

Ansprechpartner ist die Firma:

DGN Service GmbH

Richard-Oskar-Mattern-Straße 6

40547 Düsseldorf

Telefonisch ist die DGN Service GmbH zu erreichen unter 0211 77008-0

Weitere Informationen über das Trustcenter sind unter www.dgn-service.de/trustcenter verfügbar. Unter der selben Adresse kann auch der „Fingerabdruck“ des jeweiligen CA-Zertifikats abgerufen werden.

Dieses CPS sowie die CP für die einzelnen Zertifikatsklassen werden von der DGN-Service GmbH verwaltet. Als Kontaktpersonen stehen Herr Goldberg und Herr Kurz unter o.g. Adresse und Telefonnummer zur Verfügung.

2 Generelle Vorschriften

2.1 Verpflichtungen

In diesem Abschnitt werden die Verpflichtungen sowohl des Trustcenters, der externen RAs als auch der Endteilnehmer aufgeführt. Ziel ist die durchgehende Einhaltung eines hohen Sicherheitsniveaus.

2.1.1 Verpflichtungen des Trustcenters, CA

Die CA als Instanz des Trustcenters verpflichtet sich, nach den Richtlinien dieses CPS sowie der jeweiligen CP zu arbeiten. Insbesondere wird dem Schutz des privaten Schlüssels der CA absolute Priorität gegeben. Die CA stellt Zertifikate für Endteilnehmer nach der jeweiligen CP aus. Dafür vertraut sie der RA und lehnt unautorisierte Anträge ab. Die CA verpflichtet sich, Revokationsanträge schnellstmöglich zu bearbeiten und eine entsprechende CRL auszustellen. Die CA verpflichtet sich, qualifiziertes Personal zu beschäftigen, dessen Zuverlässigkeit geprüft wurde. Die Sicherheitsvorkehrungen werden eingehalten.

2.1.2 Verpflichtungen des Trustcenters, RA

Die RA verpflichtet sich, nach den Richtlinien dieses CPS sowie der jeweiligen CP zu arbeiten, die Identifizierung der Endteilnehmer zuverlässig zu prüfen und die externen RAs auf die Einhaltung der Richtlinien und der Sicherheitsvorkehrungen zu verpflichten und ggfs. zu überprüfen. Die Sicherheitsvorkehrungen werden eingehalten.

2.1.3 Verpflichtungen des Trustcenters, IS (Information Services) und Verzeichnisdienst.

Die IS und der Verzeichnisdienst verpflichten sich, nach den Richtlinien dieses CPS sowie der jeweiligen CP zu arbeiten, die Zertifikate der Endteilnehmer sowie die CRLs zuverlässig zu publizieren und die Datenschutzbestimmungen einzuhalten. Die Sicherheitsvorkehrungen werden eingehalten.

2.1.4 Verpflichtungen des Endteilnehmers (Zertifikatsinhabers)

Der Endteilnehmer, der ein Zertifikat des Trustcenters beantragt und erhält, verpflichtet sich, dieses CPS sowie die jeweilige CP zu lesen und zu akzeptieren. Er verpflichtet sich, sein Zertifikat gemäß der im Zertifikat bzw. CP(S) angegebenen Zwecke und mit angemessener Vorsicht einzusetzen. Er muss seinen privaten Schlüssel schützen und darf ihn keinesfalls zusammen mit den zugehörigen PINs aufbewahren. Er muss die PINs nach Erhalt seines privaten Schlüssels vor der erstmaligen Verwendung unverzüglich ändern. Eine Weitergabe des privaten Schlüssels oder der PINs ist nicht gestattet. Der Zertifikatsinhaber muss sein Zertifikat sperren, wenn er den Verdacht hat, dass der Schlüssel kompromittiert, abhanden gekommen oder verloren gegangen ist. Seine PINs muss er ändern, wenn der Verdacht besteht, dass sie anderen Personen bekannt wurden. Er ist verpflichtet, ggf. geänderte persönliche Daten (z.B. Name, Adresse usw.) an das Trustcenter zu melden.

2.1.5 Verpflichtungen des Endteilnehmers (Überprüfer eines Zertifikates)

Der Endteilnehmer, der ein Zertifikat überprüfen möchte oder zur Verschlüsselung nutzt, verpflichtet sich, dieses CPS sowie die jeweilige CP zu lesen und zu akzeptieren. Er verpflichtet sich, das Zertifikat zu prüfen und gemäß der zulässigen Zwecke einzusetzen. Vor der Überprüfung einer Signatur bzw. vor der Durchführung einer Verschlüsselung muss er die Gültigkeit des Zertifikats anhand der aktuellen CRL prüfen.

2.2 Haftung

Das Trustcenter der DGN Service GmbH haftet gemäß seiner Allgemeinen Geschäftsbedingungen. Für die Ausstellung eines Zertifikates, die auf falschen Daten einer externen RA beruht, haftet die externe RA gemäß ihren Allgemeinen Geschäftsbedingungen und nicht das Trustcenter der DGN Service GmbH.

2.3 Finanzielle Verantwortung

2.3.1 Schadenersatz

Entsprechende Regelungen sind in den Allgemeinen Geschäftsbedingungen enthalten.

2.3.2 Treuhänderische Beziehungen

Durch die Benutzung eines ausgestellten Zertifikates entsteht keine treuhänderische Beziehung zwischen dem Trustcenter der DGN Service GmbH und einem Endteilnehmer. Der Endteilnehmer ist für die Benutzung seines Zertifikates allein verantwortlich; die DGN Service GmbH übernimmt keinerlei Verantwortung für Rechtsgeschäfte, die mit Einsatz eines Zertifikates getätigt werden.

2.3.3 Administrative Prozesse

Keine Bestimmungen

2.4 Rechtliche Auslegung und Durchsetzung

2.4.1 Zugrunde liegende gesetzliche Bestimmungen

Der Betrieb des Trustcenters, dieses CPS und die CPs unterliegen dem Recht der Bundesrepublik Deutschland. Das Trustcenter der DGN Service GmbH stellt keine qualifizierten Zertifikate im Sinne des deutschen Signaturgesetzes aus. Die ausgestellten Zertifikate sind geeignet, um fortgeschrittene Signaturen zu erstellen, die als Beweismittel vor Gericht gelten können. Für Geschäftsbeziehungen mit ausländischen Personen wird die Anwendung des UN-Kaufrechts ausgeschlossen. Im übrigen gelten die Allgemeinen Geschäftsbedingungen der DGN Service GmbH.

2.4.2 Schlichtungsverfahren

Keine Bestimmungen

2.5 Gebühren

Die Gebühren für Leistungen des Trustcenters können der aktuellen Preisliste (unter www.dgn-service.de) entnommen werden.

2.6 Veröffentlichungen und Verzeichnisdienste

2.6.1 Veröffentlichungen des Trustcenters

Das Trustcenter publiziert unter <http://www.dgn-service.de/trustcenter/> folgende Informationen:

Dieses CPS, die CP für die jeweiligen Zertifikatsklassen, die aktuell gültigen CRLs, die CA-Zertifikate mit dem jeweiligen „Fingerabdruck“ sowie Bedienungsanleitungen für Endteilnehmer.

Die o.g. Informationen können auch über andere Mittel veröffentlicht werden. So kann beispielsweise der „Fingerabdruck“ der CA-Zertifikate auch über die Hotline der DGN Service GmbH erfragt werden. Die Rufnummer der Hotline ist auf der o.g. Website veröffentlicht.

Der Endteilnehmer wird persönlich informiert, wenn sein Zertifikat gesperrt wurde oder wenn eine Sperrung abgelehnt wurde.

2.6.2 Aktualisierungen

Sofern aktualisierte Informationen vorliegen, werden sie schnellstmöglich publiziert. Die Gültigkeitsdauer einer CRL ist abhängig von der Zertifikatsklasse und wird daher in der zugehörigen CP geregelt.

2.6.3 Zugriffskontrolle

Den Endteilnehmern und der Öffentlichkeit wird lesender Zugriff auf die o.g. Informationen gewährt. Schreibenden Zugriff haben nur autorisierte Mitarbeiter des Trustcenters sowie der DGN Service GmbH. Die Systeme sind gegen unautorisierte Schreibzugriffe besonders geschützt.

2.6.4 Verzeichnisdienst

Ein zentraler Verzeichnisdienst für die ausgestellten Zertifikate der DGN Service GmbH steht der Öffentlichkeit unter der Adresse <ldap://cert.dgn-service.de> zur Verfügung. Darüber hinaus können anwendungs-, dienste- oder klassenspezifische Verzeichnisdienste angeboten werden.

2.7 Einhaltung der CPS und Audit

Das Trustcenter der DGN Service GmbH erklärt, dass es nach den hier beschriebenen Richtlinien sowie nach den Dokumenten und Prozessen, die im Qualitätsmanagement-Handbuch beschrieben sind, arbeitet.

2.7.1 Frequenz des Audits

Ein Audit findet mindestens einmal im Quartal statt.

2.7.2 Identität/Qualifikation des Auditors

Die Audits werden im Rahmen einer internen Revision durch den Revisor des Trustcenters durchgeführt.

2.7.3 Beziehung des Auditors zum Trustcenter

Der Auditor ist mit der Rolle des Revisors des Trustcenters betraut. Er nimmt keine weiteren Aufgaben im regulären Betrieb des Trustcenters wahr.

2.7.4 Umfang des Audits

Es werden alle Instanzen, Rollen, Prozesse, Personen, Protokolle und Log-Dateien des Trustcenters stichprobenartig überprüft.

2.7.5 Maßnahmen nach Feststellung von Mängeln

Werden Mängel festgestellt, werden sofort geeignete Maßnahmen zu deren Beseitigung eingeleitet. Falls die Sicherheit des Trustcenters gefährdet ist, wird der Betrieb bis zur Beseitigung der Mängel eingestellt.

2.7.6 Veröffentlichung der Ergebnisse des Audits

Die Ergebnisse des Audits werden nicht veröffentlicht.

2.8 Datenschutzrichtlinien

Im Rahmen des Betriebs des Trustcenters werden persönliche Daten erhoben. Diese werden nach den Richtlinien des Bundesdatenschutzgesetzes sowie der Datenschutzgesetze der Länder behandelt. Informationen, die nicht unmittelbar dem Betrieb des Trustcenters dienen, werden nicht gespeichert.

2.8.1 Vertrauliche Informationen

Alle persönlichen Daten, die nicht im Zertifikat enthalten sind (Ausnahme: Zertifikatssperrung, Zeitpunkt der Sperrung), gelten als vertrauliche Informationen. Eine Ausnahme stellen die Informationen dar, deren Veröffentlichung der Eigentümer der Information zugestimmt hat.

2.8.2 Nicht vertrauliche Informationen

Alle Daten, die im Zertifikat enthalten sind, gelten als nicht vertraulich, es sei denn, der Eigentümer der Information hat der Veröffentlichung widersprochen. Informationen, die für die Überprüfung eines Zertifikats benötigt werden, sind generell nicht vertraulich und werden veröffentlicht.

Ferner gelten jene Informationen als nicht vertraulich, die zwar nicht im Zertifikat enthalten sind, deren Veröffentlichung der Eigentümer der Information explizit zugestimmt hat. Diese Informationen werden ebenfalls veröffentlicht.

2.8.3 Informationen zur Sperrung von Zertifikaten

In einer CRL wird die Seriennummer eines gesperrten Zertifikates sowie der Zeitpunkt der Sperrung veröffentlicht.

2.8.4 Veröffentlichung von Informationen nach gerichtlicher Anforderung

Nach gerichtlicher Anforderung sowie bei Anfragen von Strafverfolgungsbehörden gemäß §14 Abs. 2 SigG werden alle angeforderten Informationen ausschließlich der anfordernden Behörde übergeben. Die Auskünfte werden im Trustcenter dokumentiert. Die betroffenen Endteilnehmer werden, falls zulässig, informiert.

2.8.5 Veröffentlichung von Informationen nach Aufforderung durch den Eigentümer der Information

Informationen, die einen Endteilnehmer betreffen, werden ihm übergeben, wenn er sie schriftlich anfordert.

2.8.6 Weitere Umstände für die Veröffentlichung von vertraulichen Informationen.

Vertrauliche Informationen werden unter keinen anderen Umständen veröffentlicht.

2.9 Regelung der Urheberrechte und der Eigentumsrechte

Die CA-Zertifikate sowie die privaten und öffentlichen Schlüssel der CA des Trustcenters der DGN Service GmbH sind Eigentum der DGN Service GmbH sofern in der jeweiligen CP keine anderweitige Regelung getroffen wird. Die Zertifikate sowie die privaten und öffentlichen Schlüssel der Endteilnehmer sind Eigentum der jeweiligen Endteilnehmer.

3 Identifizierung und Authentisierung

In diesem Abschnitt werden die Prozeduren zur Feststellung der Identität eines Endteilnehmers, der ein Zertifikat beantragt, beschrieben.

3.1 Erstregistrierung

3.1.1 Namenstypen

Wird in der jeweiligen Certificate Policy geregelt.

3.1.2 Aussagekraft von Namen

Wird in der jeweiligen Certificate Policy geregelt.

3.1.3 Interpretationsregeln für Namensformen

Wird in der jeweiligen Certificate Policy geregelt.

3.1.4 Eindeutigkeit von Namen

Wird in der jeweiligen Certificate Policy geregelt.

3.1.5 Maßnahmen zur Auflösung von Streitigkeiten über einen Namen

Eine Überprüfung durch das Trustcenter findet nicht statt. Vielmehr ist der Antragsteller dafür verantwortlich, dass durch seinen Antrag keine Markenrechte, Warenzeichen usw. verletzt werden. Das Trustcenter übernimmt für solche Streitigkeiten keine Verantwortung oder Haftung. Pseudonyme oder Server-Namen, die geltendes Recht verletzen, sind nicht zulässig. Ein auf einen unzulässigen Namen ausgestelltes Zertifikat wird sofort nach bekannt werden gesperrt. Spezielles wird in der jeweiligen Certificate Policy geregelt.

3.1.6 Anerkennung von Warenzeichen

Siehe Abschnitt 3.1.5. Spezielles wird in der jeweiligen Certificate Policy geregelt.

3.1.7 Maßnahmen zur Überprüfung des Besitzes des privaten Schlüssels, der zum zertifizierten öffentlichen Schlüssel gehört.

Im Trustcenter werden private Schlüssel erzeugt. Die zugehörigen öffentlichen Schlüssel werden unmittelbar nach der Erzeugung an eine Identität gebunden. Die Zertifizierung fremderzeugter Schlüssel erfolgt nur in besonderen Fällen. Das Verfahren zur Sicherstellung des Besitzes der zugehörigen privaten Schlüssel wird im Einzelfall geregelt und in einem gesonderten Dokument wie unter 2.6.1 beschrieben veröffentlicht.

3.1.8 Authentisierung von Organisationen

Wird in der jeweiligen Certificate Policy geregelt.

3.1.9 Authentifizierung von Personen

Wird in der jeweiligen Certificate Policy geregelt.

3.2 Routinemäßige Erneuerung / Rezertifizierung

Wird in der jeweiligen Certificate Policy geregelt.

3.3 Erneuerung / Rezertifizierung nach Revokation, ohne dass der Schlüssel kompromittiert wurde

Wird in der jeweiligen Certificate Policy geregelt.

3.4 Revokationsantrag

Wird in der jeweiligen Certificate Policy geregelt.

4 Betriebliche Abläufe

4.1 Antrag auf Ausstellung von Zertifikaten

Wird in der jeweiligen Certificate Policy geregelt.

4.2 Ausstellung von Zertifikaten

Wird in der jeweiligen Certificate Policy geregelt.

4.3 Entgegennahme von Zertifikaten

Wird in der jeweiligen Certificate Policy geregelt.

4.4 Suspendierung und Revokation von Zertifikaten

4.4.1 Revokationsgründe

Ein Zertifikat kann aus folgenden Gründen revoziert (widerrufen) werden:

- Kompromittierung des privaten Schlüssels des Endteilnehmers oder der CA
- Verlust oder Diebstahl des privaten Schlüssels des Endteilnehmers
- Vertragsbruch seitens des Endteilnehmers oder des Trustcenters
- Ausstellung des Zertifikats auf Grundlage falscher Daten
- Änderung der Daten des Endteilnehmers, die auf dem Zertifikat gespeichert sind (z.B. Namensänderung)
- Auf Wunsch des Endteilnehmers

Spezielles wird in der jeweiligen Certificate Policy geregelt.

4.4.2 Berechtigte Personen, die eine Revokation veranlassen können

Wird in der jeweiligen Certificate Policy geregelt.

4.4.3 Prozedur für einen Antrag auf Revokation

Wird in der jeweiligen Certificate Policy geregelt.

4.4.4 Revokationsfristen

Wird in der jeweiligen Certificate Policy geregelt.

4.4.5 Suspendierung von Zertifikaten

Wird nicht vorgenommen.

4.4.6 Aktualisierungsfrequenz einer CRL (Liste revozierter Zertifikate)

Wird in der jeweiligen Certificate Policy geregelt.

4.4.7 CRL: Anforderungen an Endteilnehmer

Wird in der jeweiligen Certificate Policy geregelt.

4.4.8 Anforderungen an die Verfügbarkeit von CRLs

Das Trustcenter der DGN-Service GmbH stellt CRLs über einen LDAP-Server (s.o.) zur Verfügung. Dieser Dienst wird bezüglich Verfügbarkeit, Sicherheit und Ausfallsicherheit besonders geschützt.

4.4.9 Anforderungen an Endteilnehmer zur online-Überprüfung eines Zertifikates (Statusabfrage)

Die Überprüfung eines Zertifikates ist nur über eine Revokationsliste möglich. Es gilt 4.4.7

4.4.10 Andere Formen der Bekanntgabe von Revokationen

Wird in der jeweiligen Certificate Policy geregelt.

4.4.11 Spezielle Prozesse bei der Kompromittierung von privaten Schlüsseln

Falls der begründete Verdacht einer Kompromittierung des privaten Schlüssels eines Endteilnehmers besteht, ist der Endteilnehmer verpflichtet, seine Zertifikate sperren zu lassen. Falls der private Schlüssel der CA kompromittiert wird, werden alle Zertifikate, die mit diesem Schlüssel zertifiziert wurden, widerrufen.

Spezielles wird in der jeweiligen Certificate Policy geregelt.

4.5 Verfahren zur Sicherheitsüberwachung

4.5.1 Überwachte Ereignisse

Sicherheitsrelevante Ereignisse, wie z.B. der Betrieb der CA-Komponente, die Erstellung von Sperrlisten oder die Arbeiten des Sicherheitsadministrators werden in Log-Dateien oder in Papierprotokollen vermerkt.

4.5.2 Frequenz der Überprüfung von Protokollaufzeichnungen

Reguläre Überprüfungen der Protokolle (einschließlich Log-Dateien) werden regelmäßig durchgeführt. Bei Verdacht auf außergewöhnliche Ereignisse werden Sonderüberprüfungen durchgeführt.

4.5.3 Zeitraum der Aufbewahrung von Log-Dateien und Protokollen

Log-Dateien und Protokolle werden sofern gesetzlich vorgeschrieben und erlaubt mindestens 10 Jahre aufbewahrt.

4.5.4 Schutz von Log-Dateien und Protokollen

Elektronische Log-Dateien werden mit Mechanismen des Betriebssystems besonders gegen Löschung und Manipulation geschützt. Protokolle auf Papier werden in geschützten Räumen aufbewahrt.

4.5.5 Backup der Log-Dateien

Die Log-Dateien werden bei vorliegenden Änderungen tagesaktuell gesichert. Eine dauerhafte Offline-Sicherung auf Band erfolgt tagesaktuell nach einem Backup-Plan.

4.5.6 Interne oder externe Log-Systeme

Die Log-Dateien werden intern gespeichert und aufbewahrt.

4.5.7 Benachrichtigung bei sicherheitsrelevanten Ereignissen

Die Mitarbeiter des Trustcenters sind verpflichtet, sicherheitsrelevante Ereignisse sofort an den Sicherheitsbeauftragten zu melden.

4.5.8 Bewertung der Sicherheit

Eine Bewertung der Sicherheit wird vom Sicherheitsbeauftragten und vom Revisor durchgeführt.

4.6 Archivierung

4.6.1 Archivierte Daten und Ereignisse

Es werden alle Protokolle der unter 4.5.1. angeführten Ereignisse archiviert. Darüber hinaus werden alle Anträge auf Zertifizierung der Endteilnehmer archiviert.

4.6.2 Zeitraum der Aufbewahrung von archivierten Daten

Es gelten die Regelungen, die unter 4.5.3. beschrieben werden.

4.6.3 Schutz von archivierten Daten

Es gelten die Regelungen, die unter 4.5.4. beschrieben werden.

4.6.4 Backup von archivierten Daten

Es gelten die Regelungen, die unter 4.5.5. beschrieben werden.

4.6.5 Anforderungen für die Zeitstempelung von archivierten Daten

Für die Zeitstempelung elektronisch generierter Daten werden DCF77-Empfänger benutzt.

4.6.6 Interne oder externe Archivierungssysteme

Es gelten die Regelungen, die unter 4.5.6. beschrieben werden.

4.6.7 Abrufprozeduren für archivierte Daten

Die archivierten Daten werden entweder auf Papier oder als Text gespeichert, so dass ein Abruf auch über längere Zeit gewährleistet wird. Der Sicherheitsbeauftragte, der Revisor oder der Leiter des Trustcenters können einen Abruf von Daten autorisieren.

4.7 Schlüsselwechsel

Die Prozeduren zum Schlüsselwechsel beim Endteilnehmer werden in der jeweiligen Certificate Policy beschrieben. Falls ein Schlüsselwechsel der CA notwendig wird und eine Kompromittierung nicht stattgefunden hat, wird der neue Schlüssel zusammen mit seinem Fingerprint mit geeigneten Mitteln publiziert. Falls ein Schlüssel kompromittiert wurde, gelten die unter 4.8.3. aufgeführten Regelungen.

4.8 Kompromittierung und Wiederaufnahme des regulären Betriebes

4.8.1 Prozeduren für den Fall, dass Rechner, Software und/oder Daten beschädigt wurden

Falls Rechner, Software und/oder Daten beschädigt wurden, wird der Betrieb des Systems unterbrochen. Es erfolgt eine Wiederherstellung der Software und der Daten aus dem Backup. Falls der Verdacht einer mutwilligen Beschädigung oder Manipulation besteht, wird der Vorfall analysiert und die Systeme in einem sicheren Zustand wiederhergestellt. Abwehrmaßnahmen zur Vermeidung ähnlicher Vorfälle werden ergriffen und gegebenenfalls rechtliche Schritte eingeleitet. Es erfolgt eine erneute Bewertung der Sicherheit und eine Revision zur Aufdeckung von Schwachstellen.

Falls durch Beschädigung von Systemen und/oder Daten eine CRL nicht sicher veröffentlicht werden kann, wird der Verzeichnisdienst abgeschaltet.

4.8.2 Prozeduren für den Fall, dass das CA-Zertifikat revoziert wird

Eine Revokation des CA-Zertifikates hat zur Folge, dass alle Zertifikate, die mit dem revozierten CA-Zertifikat zertifiziert wurden, unmittelbar revoziert werden. Die Endteilnehmer werden informiert. Ein neuer CA-Schlüssel wird erzeugt und eingesetzt. Die CA wird wie in der initialen Phase in Betrieb genommen.

4.8.3 Prozeduren für den Fall, dass der private Schlüssel der CA kompromittiert wurde

Bei begründetem Verdacht auf Kompromittierung des CA-Schlüssels wird dieser umgehend revoziert.

4.8.4 Prozeduren für den Fall einer Katastrophe

Eine schnellstmögliche Wiederaufnahme des Betriebes unter Einhaltung aller Sicherheitsvorkehrungen wird angestrebt. Die Endteilnehmer werden über den beabsichtigten Zeitraum der Abschaltung des Trustcenters mit geeigneten Mitteln informiert.

4.9 Einstellung des Betriebs

Falls der Betrieb des Trustcenters eingestellt werden soll, werden die Endteilnehmer mindestens 3 Monate zuvor informiert. Alle Zertifikate werden rechtzeitig widerrufen. Anschließend wird der private CA-Schlüssel revoziert und sicher zerstört. Die DGN Service GmbH stellt den Fortbestand der Archive und die Abrufmöglichkeiten der archivierten Daten sowie einer komplett-CRL sicher.

Darüber hinaus wird die Einstellung des Betriebes dem Bundesministerium für Finanzen und den obersten Finanzbehörden der Länder unverzüglich angezeigt.

5 **Physische, organisatorische und personelle Sicherheitsmaßnahmen**

5.1 Physische Sicherheitsmaßnahmen

5.1.1 Lage und Konstruktion der Betriebsstätten des Trustcenters

Das Trustcenter wird im Rechenzentrum der Deutschen Apotheker- und Ärztebank (CA), bzw. in den Räumen der DGN Service GmbH (RA, weitere Dienste) betrieben. Die Räume bieten bedingt durch ihre Konstruktion einen Schutz, der dem erforderlichen Sicherheitsniveau angemessen ist.

5.1.2 Zutrittskontrollen

CA:

Die Betriebsräume sind durch elektronische und mechanische Schlösser und durch eine Alarmanlage geschützt. Eine Videoüberwachung der Zugangswege findet permanent statt. Nur vom Sicherheitsbeauftragten autorisierten Personen wird Zutritt zu den Räumen des Trustcenters gewährt. Der Zutritt erfolgt ausschließlich im 4-Augen-Prinzip.

RA/IS:

Die Betriebsräume befinden sich innerhalb des Bürogebäudes der DGN Service GmbH. Sie sind in einem speziellen Raum untergebracht, zu dem nur vom Sicherheitsbeauftragten autorisierten Personen Zutritt gewährt wird.

Der Zutritt durch nicht mit entsprechenden Rollen des Trustcenters betrauten Personen regelt eine gesonderte Besucherregelung.

5.1.3 Stromversorgung und Klimatisierung

Das Trustcenter verfügt über 2 unabhängige redundante Stromkreise (CA-Systeme, öffentliches Verzeichnisdienste) mit USV-Systemen (alle TC-Systeme). Alle Computer haben redundante Netzteile.

5.1.4 Abwehr von Wasserschäden

Ein angemessener Schutz vor Wasserschäden ist gewährleistet. Die Räumlichkeiten haben entweder einen doppelten Boden (CA/RA/IS) oder sind im 5. Stock untergebracht (weitere Dienste).

5.1.5 Abwehr von Feuerschäden

Eine Feuermeldeanlage ist vorhanden. Feuerlöscher sind nach den gültigen Brandschutzbestimmungen überall vorhanden.

5.1.6 Aufbewahrung von Medien

Alle Backup-Bänder sowie Papier-Archive werden in verschlossenen Schränken gesichert aufbewahrt.

5.1.7 Abfallentsorgung

Alle sicherheitskritischen Unterlagen und Datenträger werden sicher physisch vernichtet, bevor sie entsorgt werden.

5.1.8 Externes Backup

Die Anträge der Endteilnehmer, die von einer auswärtigen Stelle verarbeitet werden, werden in dieser auswärtigen Stelle sicher archiviert. Andere externe Backups werden nicht vorgenommen.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollen

Als Bestandteil des Organisationskonzeptes des Trustcenters existiert ein umfangreiches Rollenkonzept, welches die Rollen und deren Aufgaben beschreibt.

5.2.2 Involvierte Personen pro Arbeitsschritt

Die Festlegung der in die jeweiligen Arbeitsschritte involvierten Personen erfolgt über die Zuweisung zu den Rollen. Dabei wird die Unverträglichkeit von Rollen entsprechend des Organisationskonzeptes berücksichtigt.

5.2.3 Identifikation und Authentifizierung der Rollen

Die Identifikation und Authentifizierung von Rollen erfolgt auf Grundlage des als Bestandteil des Organisationskonzeptes des Trustcenters umgesetzten Rollen- und Rechtemodells.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Sicherheitsüberprüfung der Personen, die sicherheitskritische Rollen im Trustcenter einnehmen

Ein polizeiliches Führungszeugnis wird von allen Personen, die dem Trustcenter-Betrieb angegliedert sind, vorgelegt.

5.3.2 Sicherheitsüberprüfung für weiteres Hilfspersonal

Personen, die nicht am Trustcenter-Betrieb teilnehmen, müssen immer durch autorisiertes Trustcenter-Personal begleitet werden. Eine Sicherheitsüberprüfung findet nach den Richtlinien des Unternehmens, bei dem sie angestellt sind, statt.

5.3.3 Anforderungen an Kenntnisse und Weiterbildung

Für den Betrieb des Trustcenters wird nur qualifiziertes Personal eingesetzt. Jeder Mitarbeiter des Trustcenters wird speziell geschult.

5.3.4 Frequenz und Anforderungen an eine regelmäßige Weiterbildung

Es werden regelmäßig Weiterbildungsveranstaltungen besucht sowie relevante Publikationen und Literatur speziell in Sachen Sicherheit angeboten.

5.3.5 Sanktionen für die unautorisierte Benutzung von Systemen

Bei unautorisierten Aktionen, die die Sicherheit des Systems gefährden können, können arbeitsrechtliche Maßnahmen ergriffen werden. Bei strafrechtlicher Relevanz werden die zuständigen Behörden informiert.

5.3.6 Anforderungen an die Arbeitsverträge

Für die Arbeitsverträge des Personals gilt das Recht der Bundesrepublik Deutschland.

5.3.7 Dokumentation, die dem Personal zur Verfügung steht

Folgende Dokumentation wird dem Personal zur Verfügung gestellt:

Qualitätsmanagement-Handbuch bestehend aus: Modell des Trustcenters, CPS, CP, Rollendefinition, Unverträglichkeiten von Rollen (Rollenmatrix), Prozessbeschreibungen für den regulären Betrieb, Backup-Prozesse, Abkürzungsverzeichnis und Glossar, Formulare für den regulären Betrieb, Notfallprozeduren, Dokumentation der Installation.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselpaarerstellung und Installation

Wird in der jeweiligen Certificate Policy geregelt.

6.2 Schutz des privaten Schlüssels

Wird in der jeweiligen Certificate Policy geregelt.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche Schlüssel werden sowohl im Verzeichnisdienst als auch auf Backup-Bändern archiviert.

6.3.2 Gültigkeitsdauer der Schlüsselpaare

Wird in der jeweiligen Certificate Policy geregelt.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs)

Die PINs der CA-Schlüssel werden bei der Erzeugung festgelegt.
Spezielles wird in der jeweiligen Certificate Policy geregelt.

6.4.2 Schutz der Aktivierungsdaten

Die PINs der CA werden nur autorisierten Personen mitgeteilt. Für die PINs der Endteilnehmer-Schlüssel siehe die entsprechende CP.

6.4.3 Weitere Aspekte

Die PINs der CA-Schlüssel werden unter Wahrung des 4-Augen-Prinzips verwendet. Dazu werden geeignete technische und organisatorische Verfahren eingesetzt.

6.5 Sicherheitsmaßnahmen für Computersysteme

6.5.1 Spezifische Sicherheitsmaßnahmen für die Computersysteme

Der Betrieb des Trustcenters basiert auf einem Sicherheitskonzept nach IT-Grundschutz. Dieses berücksichtigt für die Komponenten mit hohem bzw. sehr hohem Schutzbedarf weiterführende Maßnahmen, die auf Basis einer ergänzenden Sicherheitsanalyse festgelegt werden.

6.5.2 Sicherheitseinstufung

Eine Sicherheitseinstufung der Computersysteme wurde nicht durchgeführt.

6.6 Life-Cycle der Sicherheitsmaßnahmen

6.6.1 Sicherheitsmaßnahmen für die Entwicklung

Die Entwicklung der Software wird vom Institut für Kryptographie der TU-Darmstadt bzw. von der Firma FlexSecure durchgeführt, die geeignete Sicherheitsmaßnahmen ergreifen. Jede neue Version wird in einer baugleichen Testumgebung getestet und abgenommen, bevor sie im Produktivbetrieb eingesetzt wird.

6.6.2 Sicherheitsmanagement

Die kryptographischen Module (Provider) der Software sind digital signiert. Fremde Software, die nicht dem Betrieb des Trustcenters dient, wird nicht installiert. Der Sicherheitsbeauftragte überwacht die Einhaltung der Sicherheitsziele und Sicherheitsmaßnahmen des Trustcenters.

6.6.3 Sicherheitseinstufung

Eine Sicherheitseinstufung wird nicht durchgeführt.

6.7 Sicherheitsmaßnahmen für Netzwerke

Die CA ist nicht mit einem Netzwerk verbunden. Die übrigen 2 Computersysteme des Trustcenters sind in einem dedizierten LAN untereinander verbunden, so dass keine Sicherheitsmaßnahmen erforderlich sind. Nichts desto trotz sind auf allen Maschinen Firewalls installiert, die Netzwerkverkehr nur für bestimmte Adressen, Ports und Dienste erlauben bzw. die Anbindung weiterer Systeme unterbinden.

6.8 Sicherheitsmaßnahmen für kryptographische Module

Das kryptographische Modul ist ein FIPS140-1 level 3 zertifiziertes Modul. Dessen Sicherheitseigenschaften können dem o.g. Standard entnommen werden.

7 Profile für Zertifikate und Revokationslisten

7.1 Profile für Zertifikate

Wird in der jeweiligen Certificate Policy geregelt.

7.2 Profil der Revokationslisten

Wird in der jeweiligen Certificate Policy geregelt.

8 Verwaltung dieses Certification Practice Statement

8.1 Ablauf einer Änderung

Dieses Certification Practice Statement wird durch die DGN Service GmbH verwaltet und kann jederzeit geändert werden. Eine Änderung wird unter www.dgn-service.de bekannt gegeben.

8.2 Richtlinien für die Veröffentlichung dieses CPS

Das jeweils gültige CPS wird ebenso wie Änderungen unter www.dgn-service.de veröffentlicht.

8.3 Genehmigungsverfahren des CPS

Das Inkrafttreten und die Veröffentlichung des CPS setzt eine Freigabe voraus. Die Freigabe kann durch mindestens zwei Personen mit folgenden Rollen erfolgen:

Leiter Trustcenter

Sicherheitsbeauftragter

Qualitätsbeauftragter.