

Dokumentation Trustcenter

Certificate Policy für Zertifikatsklasse "medisign Card"

Änderungshistorie:

Version	Stand	Änderungen	Autor	Status
1.0	10.09.2003	Initialversion	Georgios Raptis	Intern freigegeben
1.1	11.03.2004	Ergänzungen für TC Phase 2	Kurz / Goldberg	Entwurf
1.2	22.04.2004	Einarbeitung interner Anmerkungen	Kurz / Goldberg	zur Auslieferung an medisign
1.3	21.06.2004	Einarbeiten von Anmerkungen medisign	Otten / Kurz / Goldberg	Freigegeben
1.3.1	16.09.2004	Ergänzung und Konkretisierung	Knut Goldberg	Freigegeben

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

6.1	Schlüsselpaarerzeugung und Installation.....	18
6.2	Schutz des privaten Schlüssels.....	19
6.3	Weitere Aspekte des Schlüsselmanagements	20
6.4	Aktivierungsdaten.....	20
6.5	Sicherheitsmaßnahmen für Computersysteme	21
6.6	Life-Cycle der Sicherheitsmaßnahmen	21
6.7	Sicherheitsmaßnahmen für Netzwerke	21
6.8	Sicherheitsmaßnahmen für kryptographische Module	21
7	Profile für Zertifikate und Revokationslisten	22
7.1	Profile für Zertifikate	22
7.2	Profil der Revokationslisten.....	23
8	Verwaltung dieser Certificate Policy	23
8.1	Ablauf einer Änderung.....	23
8.2	Richtlinien für die Veröffentlichung dieser Certificate Policy.....	23
8.3	Genehmigungsverfahren der Certificate Policy	23

1 Einleitung

1.1 Überblick

Diese Certificate Policy (CP) enthält zusammen mit dem Certification Practice Statement (CPS) die Richtlinien für den Betrieb des Trustcenters der DGN Service GmbH sowie für die Vergabe von smartcard-basierten Zertifikaten durch dieses Trustcenter für die medisign GmbH. In dieser Policy werden spezifische Informationen über die Anwendung der angebotenen Zertifikate, die der hier beschriebenen Zertifikatsklasse angehören, bereitgestellt. Nähere spezifische Informationen zu den generellen Richtlinien für den Betrieb des Trustcenters der DGN Service GmbH werden im Certification Practice Statement aufgeführt.

Die hier beschriebenen Richtlinien gelten zusammen mit dem Certification Practice Statement 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 der medisign GmbH, die der Teilnehmer mit der Beantragung einer Smartcard anerkennt.

Dieses Dokument bezieht sich auf technische und organisatorische Sachverhalte, die sich auf die spezielle, hier aufgeführte Zertifikatsklasse beschränken. Informationen, die übergreifend für alle Certificate Policies gelten, werden im CPS angeboten. Für evtl. vorhandene andere Zertifikatsklassen gelten eigene Certificate Policies. Die Gliederung sowie die Empfehlungen des RFC 2527 (Version von März 1999) der IETF werden angewandt.

1.2 Identifikation des Dokumentes

Name: Certificate Policy der Zertifikatsklasse medisign Card für personengebundene Zertifikate (Signaturzertifikat, Verschlüsselungszertifikat, Authentisierungszertifikat) auf einer Signaturkarte mit der Kennzeichnung als medisign Smartcard.

Version: 1.3.1

Datum: 16.09.2004

Status: freigegeben

OID: 1.3.6.1.4.1.15787.2.1.3.2.3

1.3 Infrastruktur und Anwendungsbereich

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

1.3.1 CA

Die Root-CA des DGN Service 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-CA der medisign GmbH zertifiziert die öffentlichen Schlüssel der Endteilnehmer. 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.

Die CA der medisign GmbH stellt nur Zertifikate der Klasse „medisign Card“ aus. Hierbei handelt es sich um Smartcard-basierte Zertifikate, deren Produktion die Regeln dieser CP, der CPS des DGN Service Trustcenters zugrunde liegt. Das CA-Zertifikat wird mit „Type C“ im CN gekennzeichnet.

1.3.2 RA

Die Identifizierung der Antragsteller wird durch zuvor bestellte Personen der medisign Vertriebspartner durchgeführt. Diese erfolgt entweder persönlich oder durch Prüfung der Antragsdaten gegen bereits registrierte Daten des Antragstellers, die auf Basis einer persönlichen Vorstellung erhoben wurden.

Das Trustcenter führt eine Antragsprüfung und gegebenenfalls eine Identifizierung auf Basis von Ausweisdaten durch. Näheres regelt Abschnitt 3.1.9 „Authentifizierung von Personen“.

1.3.3 Endteilnehmer

Die Vergabe von Zertifikaten richtet sich primär, aber nicht exklusiv, an Vertreter des deutschen Gesundheitswesens.

1.3.4 Anwendbarkeit

Die Zertifikate der hier beschriebenen Zertifikatsklasse können für Verschlüsselung (Verschlüsselungszertifikat), Authentisierung (Authentisierungszertifikat) und Signatur (Signaturzertifikat) verwendet werden. Die mit dem Signaturzertifikat erzeugten Signaturen sind fortgeschrittene Signaturen (keine qualifizierte Signaturen) im Sinne des deutschen Signaturgesetzes. Die Zertifizierung weiterer untergeordneter Zertifikate ist nicht gestattet.

1.4 Kontaktinformationen

Ansprechpartner ist die Firma:

medisign GmbH

Richard-Oskar-Mattern-Strasse 6

40547 Düsseldorf

Telefonisch ist die medisign GmbH zu erreichen unter 0211/5382230.

Weitere Informationen über das Trustcenter sind unter <http://www.dgn-service.de/trustcenter> verfügbar. Medisign-spezifische Informationen werden unter <http://www.medisign.de> bereitgestellt. Unter der selben Adresse kann auch der „Fingerabdruck“ des CA-Zertifikats abgerufen werden.

2 Generelle Vorschriften

2.1 Verpflichtungen

In diesem Abschnitt werden die Verpflichtungen sowohl des Trustcenters 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 dieser CP sowie des CPS zu arbeiten. Insbesondere wird dem Schutz des privaten Schlüssels der CA absolute Priorität gegeben. Die CA stellt Zertifikate für Endteilnehmer u.a. nach dieser 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 des Trustcenters verpflichtet sich, nach den Richtlinien dieser CP sowie des CPS zu arbeiten und die Identifizierung der Endteilnehmer zuverlässig zu prüfen. medisign wird eine Verpflichtung auf Identifizierung der Endteilnehmer von jedem Vertriebspartner von medisign einholen. 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 dieser CP sowie des CPS 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 der hier beschriebenen Zertifikatsklasse beantragt und erhält, verpflichtet sich, diese CP sowie das CPS zu lesen und zu akzeptieren. Er verpflichtet sich, sein Zertifikat gemäß der im Zertifikat und in dieser CP 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 lassen, 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, diese Certification Policy sowie das CPS 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

Die medisign GmbH haftet gemäß ihrer Allgemeinen Geschäftsbedingungen.

2.3 Finanzielle Verantwortung

2.3.1 Schadenersatz

Entsprechende Regelungen sind in den Allgemeinen Geschäftsbedingungen der medisign GmbH enthalten.

2.3.2 Treuhänderische Beziehungen

Durch die Benutzung eines ausgestellten Zertifikates entsteht keine treuhänderische Beziehung zwischen der medisign GmbH und einem Endteilnehmer. Der Endteilnehmer ist für die Benutzung seines Zertifikates allein verantwortlich; die medisign

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, diese Certification Policy und das CPS des DGN Service Trustcenters unterliegen dem Recht der Bundesrepublik Deutschland. Es werden keine qualifizierten Zertifikate im Sinne des deutschen Signaturgesetzes ausgestellt. 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 medisign GmbH.

2.4.2 Schlichtungsverfahren

Keine Bestimmungen

2.5 Gebühren

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

2.6 Veröffentlichungen und Verzeichnisdienste

2.6.1 Veröffentlichungen des Trustcenters

Das Trustcenter publiziert unter www.medisign.de folgende Informationen:

Diese Certificate Policy, das CPS, die aktuelle gültige CRL, das Root- und CA-Zertifikat mit seinem „Fingerabdruck“.

Die o.g. Informationen können auch über andere Mittel veröffentlicht werden. So kann beispielsweise der „Fingerabdruck“ der CA-Zertifikate auch über die Hotline der medisign GmbH erfragt werden. Die Rufnummer der Hotline wird dem Teilnehmer mit dem Ausstattungspaket mitgeteilt und ist auf der o.g. Website veröffentlicht.

2.6.2 Aktualisierungen

Sofern aktualisierte Informationen, z.B. im Falle einer Zertifikatssperrung, vorliegen, werden sie schnellstmöglich publiziert. Eine neue CRL wird mindestens alle 35 Tage ausgegeben.

2.6.3 Zugriffskontrolle

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

2.6.4 Verzeichnisdienst

Ein Verzeichnisdienst für die ausgestellten Zertifikate steht der Öffentlichkeit zur Verfügung. Der Verzeichnisdienst des Trustcenters ist unter der Adresse `ldap://cert.dgn-service.de:389` zu erreichen.

2.7 Einhaltung der Certificate Policy 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 als Revisor des Trustcenters beauftragt. 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 bzw. der Mängelbeseitigung 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.

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. 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 aber explizit zugestimmt hat.

2.8.3 Informationen zur Sperrung von Zertifikaten

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

Der Endteilnehmer wird persönlich informiert, wenn sein Zertifikat aus einem anderen als von ihm angegebenem Grund gesperrt wurde oder wenn seine beauftragte Sperrung abgelehnt wurde.

2.8.4 Veröffentlichung von Informationen nach gerichtlicher Anforderung

Nach gerichtlicher Anforderung werden alle angeforderten Informationen ausschließlich der anfordernden Behörde übergeben. 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

Das Root-Zertifikat der DGN Service GmbH sowie die zugehörigen privaten und öffentlichen Schlüssel sind Eigentum der DGN Service GmbH. Das Sub-CA-Zertifikat

der medisign GmbH sowie die zugehörigen privaten und öffentlichen Schlüssel sind Eigentum der medisign GmbH. 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

Es werden Namenshierarchien genutzt, die X.501-Distinguished-Names benutzen. Für Personen wird entweder der reale Name oder ein Pseudonym verwendet, das als solches gekennzeichnet sein muss (Zusatz „:PN“ am Common Name). Für juristische Personen und für Maschinen werden keine Zertifikate dieser Zertifikatsklasse ausgestellt.

3.1.2 Aussagekraft von Namen

Die Eindeutigkeit der Identifikation des Endteilnehmers durch seinen Namen (DN) im Zertifikat wird garantiert. Dieser Name (DN) muss sich nicht auf den realen Namen des Teilnehmers beschränken.

3.1.3 Interpretationsregeln für Namensformen

Der Zusatz „:PN“ bedeutet, dass es sich beim vorliegenden Namen um ein Pseudonym handelt.

3.1.4 Eindeutigkeit von Namen

Die Distinguished Names der Endteilnehmer sind eindeutig. Eine Seriennummer wird im DN aufgenommen. Sie wird bei Namensgleichheit hochgezählt und garantiert die Eindeutigkeit der DNs.

3.1.5 Maßnahmen zur Auflösung von Streitigkeiten über einen Namen

Durch die Verwendung einer Seriennummer im Distinguished Name wird eine Eindeutigkeit von DNs erreicht. Diese Seriennummer wird auch für eine neue Chipkarte, die für die gleiche Person ausgestellt wird, hochgezählt. Ein Endteilnehmer darf seine ihm zugewiesene Seriennummer nicht ablehnen. Ein Pseudonym kann anstelle des Namens einer Person verwendet werden. Das selbe Pseudonym darf nicht von mehreren Personen benutzt werden. Der Antragsteller, der seinen Antrag zuerst gestellt hat, bekommt das Pseudonym, sofern keine Markenrechte, Warenzeichen usw. verletzt werden. Das Trustcenter überprüft solche Rechte nicht. Allein der Antragsteller ist für solche Überprüfungen verantwortlich. Pseudonyme, die geltendes Recht

verletzen, sind nicht zulässig. Ein auf einen unzulässigen Namen ausgestelltes Zertifikat wird sofort nach Bekannt werden gesperrt.

3.1.6 Anerkennung von Warenzeichen

Nur natürliche Personen dürfen ein Zertifikat dieser Zertifikatsklasse beantragen und erhalten. Da der Name auf dem Zertifikat sich explizit auf eine natürliche Person bezieht, ist eine Anerkennung von Warenzeichen nicht relevant. Falls ein Pseudonym (erkennbar am Zusatz „:PN“ hinter dem Namen im Distinguished Name) an Stelle des Namens verwendet wird, darf dieses keine Warenzeichen, Markenrechte usw. verletzen. Das Trustcenter überprüft solche Rechte nicht. Allein der Antragsteller ist für solche Überprüfungen verantwortlich. Falls das Trustcenter über eine Verletzung solcher Rechte informiert wird, wird nach den gesetzlichen Bestimmungen das Zertifikat widerrufen.

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

Der private Schlüssel wird im Trustcenter erzeugt. Der zugehörige öffentliche Schlüssel wird unmittelbar nach der Erzeugung an eine Identität gebunden. Fremd-erzeugte Schlüssel werden nicht zertifiziert, daher wird keine Überprüfung des Besitzes durchgeführt.

3.1.8 Authentisierung von Organisationen

Nur natürliche Personen dürfen ein Zertifikat dieser Zertifikatsklasse beantragen und erhalten.

3.1.9 Authentifizierung von Personen

Personen, die ein Zertifikat dieser Zertifikatsklasse beantragen, werden wie folgt authentisiert:

a) bei der Antragstellung durch eine der folgenden Möglichkeiten:

- Durch persönliche Identifikation bei einem autorisierten Mitarbeiter. Der autorisierte Mitarbeiter (Registrar), der auch einer externen Registration Authority angehören darf, identifiziert den Antragsteller.
- Durch Prüfung der Antragsdaten gegen bereits registrierte Daten des Antragstellers, die auf Basis einer persönlichen Vorstellung erhoben wurden und durch Beifügung einer Kopie des amtlichen Personalausweises oder Reisepasses zum Antrag auf Ausstellung einer Smartcard und Prüfung der Daten durch die RA des Trustcenters.
- Durch einen elektronisch signierten Antrag, falls der Antragsteller ein Zertifikat dieser Zertifikatsklasse besitzt, welches noch gültig ist („Rezertifizierung“).

b) bei der Zustellung der Smartcard durch eine der folgenden Möglichkeiten:

- Durch das PostIdent-Verfahren der Deutschen Post AG. Ein Mitarbeiter der Deutschen Post AG überprüft und bestätigt die Identität eines Antragstellers

anhand eines gültigen Ausweisdokuments. Die Daten des Ausweisdokuments (welches auch die aktuelle Anschrift enthalten muss) werden mitprotokolliert.

- Durch persönliche Übergabe durch einen autorisierten Mitarbeiter. Der autorisierte Mitarbeiter (Registrar), der auch einer externen Registration Authority angehören darf, überprüft und bestätigt die Identität eines Antragstellers anhand eines gültigen Ausweisdokuments. Die Daten des Ausweisdokuments (welches auch die aktuelle Anschrift enthalten muss) werden mitprotokolliert.

3.1.10 Aufnahme von berufsgruppenspezifischen Attributen in das Zertifikat

Der Antragsteller kann die Aufnahme eines berufsgruppenspezifischen Attributes (Arzt, Zahnarzt, Apotheker) in die Zertifikate durch Beifügung seiner Approbationsurkunde zum Kartenantrag beantragen. Das Trustcenter ist nicht verpflichtet, beantragte berufsgruppenspezifische Attribute in die Zertifikate aufzunehmen und kann die Aufnahme ohne Angabe von Gründen verweigern.

3.2 Routinemäßige Erneuerung / Rezertifizierung

Eine routinemäßige Rezertifizierung findet nicht statt. Nach Ablauf des Gültigkeitszeitraums der Zertifikate muss ein neuer Antrag gestellt werden.

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

Für eine Erneuerung nach Revokation muss ein neuer Antrag gestellt werden. Die entsprechenden Regelungen werden angewandt.

3.4 Revokationsantrag

Die Revokation eines Zertifikates dieser Zertifikatsklasse kann jede Person telefonisch oder schriftlich per E-Mail, Fax oder Brief veranlassen, die mindestens folgende Daten des Zertifikatseigentümers angeben kann: Vorname, Name und Revokationspasswort. Kann bei telefonischem Sperrantrag das Revokationspasswort nicht mitgeteilt werden, werden zusätzliche Daten abgefragt.

Falls eine Person mehrere Signaturkarten besitzt und nur eine davon revoziert werden soll, müssen spezifische Merkmale der zu revozierenden Signaturkarte angegeben werden. Wenn die zu sperrende Signaturkarte nicht sicher identifiziert werden kann, werden alle Signaturkarten des Antragstellers revoziert.

4 Betriebliche Abläufe

4.1 Antrag auf Ausstellung von Zertifikaten

Ein Antrag auf Ausstellung von Zertifikaten dieser Zertifikatsklasse darf nur persönlich von einer natürlichen Person gestellt werden. Die Identifikation des Antragstellers erfolgt nach den Regelungen unter 3.1.9. dieser Certificate Policy. Die Antragsprüfung erfolgt durch die RA. Der Antrag wird im Trustcenter von 2 Registraren bearbeitet, die die elektronisch vorliegenden Antragsdaten im RA-System überprüfen.

4.2 Ausstellung von Zertifikaten

Die CA erstellt für jeden Antrag der RA drei Schlüsselpaare und drei zugehörige Zertifikate (Signatur-, Verschlüsselungs-, Authentisierungszertifikat), die auf einer Signaturkarte angebracht werden. Die privaten Schlüssel sind durch eine von der CA zufällig gewählte 6-stellige Transport-PIN geschützt. Transport-PINs werden bis zum Zeitpunkt des Versendens verschlüsselt aufbewahrt.

4.3 Entgegennahme von Zertifikaten

Die vom Trustcenter personalisierte Signaturkarte wird per Post im PostIdent-Verfahren der Deutschen Post AG zugestellt oder persönlich übergeben. Erst nach Eintreffen der Empfangs- bzw. Übergabebestätigung im Trustcenter, wird die zugehörige PIN auf Sicherheitspapier gedruckt und versandt.

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, der medisign GmbH oder des Trustcenters
- Ausstellung des Zertifikats auf Grundlage falscher Daten
- Änderung der Daten des Endteilnehmers, die auf dem Zertifikat gespeichert sind (z.B. Namensänderung)
- Wegfall der Berechtigung zum Führen eines berufsgruppenspezifischen Attributes (Arzt, Zahnarzt, Apotheker)
- Auf Wunsch des Endteilnehmers

4.4.2 Berechtigte Personen, die eine Revokation veranlassen können

Telefonische Revokation: Jede Person, die folgende Daten des Zertifikatseigentümers angeben kann: Vorname, Name und Revokationspasswort, ist berechtigt, eine telefonische Revokation zu veranlassen.

Schriftliche oder elektronische Revokation: berechtigt ist der Zertifikatseigentümer und berechtigte Mitarbeiter der medisign GmbH, ihrer Vertriebspartner und des Trustcenters.

4.4.3 Prozedur für einen Antrag auf Revokation

Telefonisch: o.g. Daten werden erfragt, ggf. noch Einzelheiten über die zu revozierende Signaturkarte.

Schriftlich oder elektronisch: Die Signatur und das angegebene Revokationspasswort werden geprüft.

Nach erfolgreicher Prüfung des Antrages wird ein interner Antrag auf Revokation in das RA-System eingegeben und an die CA weitergeleitet. Der Zeitpunkt der Eingabe des Antrages in das RA-System gilt als Sperrzeitpunkt. Anschließend stellt die CA eine neue CRL (Revokationsliste) aus. Es werden stets alle drei Zertifikate einer Signaturkarte revoziert. Die neue CRL wird vom Verzeichnisdienst der Öffentlichkeit zur Verfügung gestellt.

4.4.4 Revokationsfristen

Eine Revokation wird so schnell wie möglich durchgeführt, mindestens aber mit Ablauf des nächsten Werktages nach Eingang des Sperrantrages.

4.4.5 Suspendierung von Zertifikaten

Wird nicht vorgenommen.

4.4.6 Aktualisierungsfrequenz einer CRL (Liste revozierter Zertifikate)

Die CRL wird aktualisiert, wenn ein Zertifikat widerrufen wird, spätestens jedoch alle 35 Tage.

4.4.7 CRL: Anforderungen an Endteilnehmer

Ein Endteilnehmer, der ein Zertifikat benutzen möchte (insbesondere, wenn eine Signatur überprüft wird), ist verpflichtet, die aktuelle CRL herunterzuladen und zu überprüfen, ob das entsprechende Zertifikat widerrufen wurde. Die Benutzung eines Zertifikates ohne vorherige Überprüfung ist nicht gestattet.

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 Abschnitt 4.4.7.

4.4.10 Andere Formen der Bekanntgabe von Revokationen

Die Überprüfung der Revokation eines Zertifikates ist nur über eine Revokationsliste möglich. Andere Formen sind nicht vorgesehen.

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.

4.5 Verfahren zur Sicherheitsüberwachung

Es gelten die Regelungen, die im Certification Practice Statement beschrieben werden.

4.6 Archivierung

Es gelten die Regelungen, die im Certification Practice Statement beschrieben werden.

4.7 Schlüsselwechsel

Die Prozeduren zum Schlüsselwechsel der CA werden im Certification Practice Statement beschrieben. Ein Wechsel von Schlüsseln auf der Signaturkarte eines Endteilnehmers wird nicht durchgeführt.

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 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-Zertifikats hat zur Folge, dass alle Zertifikate, die mit dem revozierten CA-Zertifikat zertifiziert wurden, unmittelbar revoziert sind. 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

Wenn der Verdacht der Kompromittierung des CA-Schlüssels besteht, 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

Es gelten die Regelungen, die im Certification Practice Statement beschrieben werden.

5 **Physische, organisatorische und personelle Sicherheitsmaßnahmen**

Es gelten die Regelungen, die im Certification Practice Statement beschrieben werden.

6 **Technische Sicherheitsmaßnahmen**

6.1 Schlüsselpaarerzeugung und Installation

6.1.1 Schlüsselpaarerzeugung

Die CA des Trustcenters erzeugt die Schlüsselpaare der Endteilnehmer. Private Schlüssel werden nicht auslesbar auf Smartcards gespeichert. Damit wird gewährleistet, dass die Qualität der Schlüssel hohen Anforderungen entspricht.

6.1.2 Auslieferung des privaten Schlüssels

Der private Schlüssel des Endteilnehmers wird per Post im PostIdent-Verfahren der Deutschen Post AG oder persönlich ausgeliefert. Private Schlüssel sind nicht auslesbar auf Smartcards gespeichert.

6.1.3 Auslieferung des öffentlichen Schlüssels an den Zertifikatsinhaber

Der öffentliche Schlüssel des Endteilnehmers wird zusammen mit dem privaten Schlüssel und dem Zertifikat auf der Smartcard ausgeliefert. Zusätzlich wird der öffentliche Schlüssel als Bestandteil des Teilnehmerzertifikats im Zertifikatsverzeichnis veröffentlicht.

6.1.4 Auslieferung der öffentlichen Root- und CA-Schlüssel

Die öffentlichen Schlüssel der Root des Trustcenters der DGN Service GmbH und der Sub-CA der medisign GmbH werden über die o.g. Publikationsadresse im Internet zum Abruf bereitgestellt. Der Endteilnehmer muss dabei den publizierten Fingerprint mit dem Fingerprint des öffentlichen Schlüssels vergleichen.

6.1.5 Verwendete Schlüssellängen

Es werden die jeweils von der RegTP bzw. BSI empfohlenen Schlüssellängen verwendet. Diese sind z.Z. 2048 bit für den CA-Schlüssel und 1024 bit für die Schlüssel der Endteilnehmer. Eine Vergrößerung der Schlüssellänge kann in der Zukunft erfolgen, ohne dass dieser im CPS vermerkt wird.

6.1.6 Parameter der öffentlichen Schlüssel

Die Parameter der öffentlichen Schlüssel werden von der CA des Trustcenters erzeugt.

6.1.7 Qualität der Parameter

Die Parameter werden bei deren Festlegung sorgfältig ausgewählt und überprüft.

6.1.8 Schlüsselerzeugung in Software oder in Hardware

Die Schlüssel der CA werden in einem Hardware-Kryptomodul innerhalb der CA erzeugt. Die Schlüssel der Endteilnehmer werden innerhalb der CA mit Unterstützung des Hardware-Kryptomoduls erzeugt.

6.1.9 Verwendungszweck der Schlüssel und Beschränkungen (wie im entsprechenden Feld des X.509v3 Zertifikates aufgeführt).

Beschränkungen aller Zertifikate: CA:False (critical)

Die Schlüssel der Endteilnehmer haben folgenden Verwendungszweck, wie im entsprechenden Feld des X.509v3 Zertifikates aufgeführt:

Signatur Schlüssel:

Non Repudiation, Digital Signature (critical)

Verschlüsselungsschlüssel:

Data Encipherment, Key Encipherment (critical)

Authentisierungsschlüssel:

Digital Signature (critical)

6.2 Schutz des privaten Schlüssels

6.2.1 Standards des Schlüssel erzeugenden kryptographischen Moduls

Das die Teilnehmerschlüssel erzeugende Modul erfüllt derzeit keine bestimmten Standards. Das die Schlüsselerzeugung unterstützende Hardware-Kryptomodul ist nach FIPS-140 zertifiziert. Das kryptographische Modul, das die Teilnehmerschlüssel beinhaltet (Signaturkarte) ist E4hoch evaluiert.

Das Hardware-Kryptomodul der CA-Zertifikate ist FIPS-140 zertifiziert.

6.2.2 Schlüsselteilung (key-sharing Algorithmus)

Die Schlüssel der Endteilnehmer werden nicht geteilt.

6.2.3 Schlüssel hinterlegung

Eine Hinterlegung der Teilnehmerschlüssel findet nicht statt.

6.2.4 Backup von privaten Schlüsseln

Ein Backup von privaten Schlüsseln existiert nicht.

6.2.5 Archivierung privater Schlüssel

Es existiert kein Backup von Schlüsseln von Endteilnehmern.

6.2.6 Speicherung privater Schlüssel in ein Kryptomodul

Die privaten Schlüssel eines Endteilnehmers werden während der Personalisierung der Signaturkarte unmittelbar nach der Erzeugung durch die CA auf die Signaturkarte geschrieben. Dieser Prozess läuft ohne Möglichkeiten der Unterbrechung und des manuellen Eingriffs automatisch ab.

6.2.7 Aktivierung privater Schlüssel

Ein privater Schlüssel einer Signaturkarte kann nach Eingabe einer 6-stellige PIN aktiviert werden. Durch die zehnmahlige Eingabe einer falschen PIN wird die Signaturkarte unwiderruflich blockiert.

6.2.8 Vernichtung privater Schlüssel

Die Schlüssel einer Signaturkarte können vernichtet werden, indem der Chip auf der Karte physisch vernichtet (durchgeschnitten) wird.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

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

6.3.2 Gültigkeit der Schlüsselpaare

Die Schlüssel der Root-CA sind 16 Jahre, die der Sub-CA sind 8 Jahre gültig, es sei denn, die verwendeten Algorithmen und Schlüssellängen werden nicht mehr empfohlen. Eine Erneuerung des Zertifikats findet mindestens alle 4 Jahre statt, wobei der private Schlüssel nicht erneuert werden muss, wenn die empfohlenen Algorithmen und Schlüssellängen dies erlauben. Ein CA-Schlüssel bzw. CA-Zertifikat wird so lange verwendet, wie die Gültigkeitsdauer der damit ausgestellten Endteilnehmer-Zertifikate seine restliche Gültigkeitsdauer nicht übersteigt.

Die Teilnehmerschlüssel sind 4 Jahre gültig.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation der Aktivierungsdaten (PINs)

Die PINs der Endteilnehmer-Schlüssel werden als zufällige 6-stellige Zahlen von der CA erzeugt. Der Endteilnehmer verpflichtet sich, die PINs unverzüglich bei der ersten Inbetriebnahme seiner Signaturkarte zu ändern.

6.4.2 Schutz der Aktivierungsdaten

Die PINs werden vor deren Auslieferung von der CA verschlüsselt übermittelt und unmittelbar vor dem Drucken durch die Druckapplikation entschlüsselt und auf Sicherheitspapier gedruckt. Sie können nur nach erkennbarer Beschädigung des Sicherheitspapiers gelesen werden.

Auf der Signaturkarte werden die PINs elektronisch durch die Signaturkarte selbst geschützt. Sie können nicht ausgelesen werden. Der Endteilnehmer verpflichtet sich, die PINs unverzüglich (bei der ersten Inbetriebnahme seiner Signaturkarte) zu ändern. Eine Weitergabe der PINs an weitere Personen ist nicht gestattet. Wenn der Verdacht besteht, dass eine andere Person die PINs kennt, ist der Zertifikatsinhaber verpflichtet, sie unverzüglich zu ändern. Eine regelmäßige Änderung der PINs (z.B. monatlich) wird aus Sicherheitsgründen generell empfohlen.

6.4.3 Weitere Aspekte

Keine.

6.5 Sicherheitsmaßnahmen für Computersysteme

Es gelten die Regelungen, die im Certification Practice Statement beschrieben werden.

6.6 Life-Cycle der Sicherheitsmaßnahmen

Es gelten die Regelungen, die im Certification Practice Statement beschrieben werden.

6.7 Sicherheitsmaßnahmen für Netzwerke

Es gelten die Regelungen, die im Certification Practice Statement beschrieben werden.

6.8 Sicherheitsmaßnahmen für kryptographische Module

Solange die Aktivierungsdaten (PINs) geheim bleiben, ist das Modul (d.h. der Chip auf der Signaturkarte) sicher.

7 Profile für Zertifikate und Revokationslisten

7.1 Profile für Zertifikate

7.1.1 Version

Die vom Trustcenter der DGN Service GmbH ausgestellten Zertifikate sind X.509v3 Zertifikate.

7.1.2 Zertifikatserweiterungen

Die Teilnehmerzertifikate haben folgende Erweiterungen:

- Basic Constraint
- Key Usage
- Certificate Policy
- CRL Distribution Point
- Subject Alternative Name
- Authority Key Identifier
- Subject Key Identifier
- Admission

7.1.3 Object-Identifiers der kryptographischen Algorithmen

RSA: 1.2.840.113549.1.1.1

SHA-1: 1.2.840.113549.1.1.5

7.1.4 Namensformen

Die Distinguished Names der Zertifikate haben folgende Form:

C= *Landeskennung*

CN= *Vorname Nachname*

SN= *Seriennummer*

7.1.5 Beschränkungen für Namen

Keine Bestimmungen.

7.1.6 Object Identifiers für die Certificate Policies

Für jede Certificate Policy gibt es einen object identifier, der in der jeweiligen CP aufgeführt wird. Der OID für diese Certificate Policy ist unter 1.2. aufgeführt.

7.1.7 Verwendung von Erweiterungen für Policy Constraints

Keine Bestimmungen.

7.1.8 Syntax und Semantik des Policy Qualifiers

Keine Bestimmungen.

7.1.9 Verarbeitungssemantik für kritische Certificate Policy Extension

Keine Bestimmungen.

7.2 Profil der Revokationslisten

7.2.1 Version

Die vom Trustcenter der DGN Service GmbH ausgestellten Revokationslisten sind X.509v2 CRLs.

7.2.2 CRL und CRL entry extensions

Für die CRLs werden keine Erweiterungen verwendet

8 Verwaltung dieser Certificate Policy

8.1 Ablauf einer Änderung

Diese Certificate Policy wird durch die medisign GmbH und das Trustcenter der DGN Service GmbH verwaltet und kann jederzeit geändert werden. Eine Änderung wird unter www.medisign.de bekannt gegeben.

8.2 Richtlinien für die Veröffentlichung dieser Certificate Policy

Die jeweils gültige CP wird ebenso wie Änderungen unter www.medisign.de veröffentlicht.

8.3 Genehmigungsverfahren der Certificate Policy

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

Leiter Trustcenter

Sicherheitsbeauftragter

Qualitätsbeauftragter.