



HIN Health Info Net AG

Sicherheits- und Zertifizierungskonzept

Ergänzungsdokument zur QuoVadis CP/CPS

Version 1.0
Januar 2011

Referenzierte Dokumente

Referenz	Bezeichnung
[1]	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES) vom 19. Dezember 2003
[2]	Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES) vom 3. Dezember 2004
[3]	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates (ETSI TS 101 456 V1.4.3 2007-05)
[4]	Electronic Signatures and infrastructures (ESI); Electronic Signature Formats (ETSI TS 101 733 V1.5.1 2003-12)
[5]	Qualified Certificate Profile (ETSI TS 101 862 V1.3.3 2006-01)
[6]	Electronic Signatures and infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms (ETSI 102 176-1 V2.0.0 2007-11)
[7]	Electronic Signatures and infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices (ETSI 102 176-1 V2.0.0 2007-11)
[8]	Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile (IETF RFC 3280 2002-04)
[9]	Internet X.509 Public Key Infrastructure; Qualified Certificates Profile (IETF RFC 3739 2004-03)
[10]	X.509 Internet Public Key Infrastructure; Online Certificate Status Protocol – OCSP (IETF RFC 2560)
[11]	Internet X.509 Public Key Infrastructure; Certificate Policy and Certification Practices Framework (IETF RFC 3647 2003-11)

Inhaltsverzeichnis

1	Einleitung	7
1.1	Überblick	7
1.2	Titel und Identifikation des Dokuments.....	7
1.3	PKI Teilnehmer	8
1.3.1	Zertifizierungsstellen (CA).....	8
1.3.2	Registrierungsstellen (RA).....	8
1.3.3	Zertifikatsinhaber (Subscriber).....	9
1.3.4	Zertifikatsprüfer (Relying parties)	9
1.3.5	Weitere Teilnehmer	9
1.4	Zertifikatsnutzung	9
1.5	Verwaltung der Richtlinien	10
1.5.1	Zuständige Stelle – Aufsichtsstelle.....	10
1.5.2	Kontaktpersonen / Ansprechpartner	10
1.5.3	Stelle für die Bestimmung der Eignung der CPS	10
1.5.4	Genehmigungsverfahren für die CPS.....	10
1.6	Definitionen und Abkürzungen	10
2	Verantwortlichkeiten für Publikation und Verwaltung	13
2.1	Dokumentablage	13
2.2	Veröffentlichung der Zertifizierungsdaten	13
2.3	Zeitpunkt oder Häufigkeit der Veröffentlichung.....	13
2.4	Zugangskontrolle zur Dokumentablage	13
3	Identifikation und Authentisierung.....	14
3.1	Namensgebung.....	14
3.1.1	Namensarten	14
3.1.2	Notwendigkeit für aussagekräftige Namen.....	14
3.1.3	Anonymität oder Pseudonyme der Zertifikatsinhaber	14
3.1.4	Regeln für die Auslegung unterschiedlicher Namensformen	14
3.1.5	Eindeutigkeit von Namen.....	14
3.1.6	Erkennung, Authentisierung und Rolle von Marken.....	14
3.2	Anfängliche Identitätsüberprüfung	14
3.3	Identifikation und Authentisierung für Anträge auf Zertifikatserneuerung	15
3.4	Identifikation und Authentisierung für Anträge auf Ungültigkeitserklärung	15
4	Betriebsanforderungen für den Zertifikatslebenszyklus.....	16
4.1	Zertifikatsantrag.....	16
4.1.1	Wer kann einen Zertifikatsantrag einreichen.....	16
4.1.2	Registrierungsverfahren und Verantwortlichkeiten	16
4.2	Bearbeitung des Zertifikatsantrags	17
4.2.1	Durchführung von Identifikation und Authentifizierung	17
4.2.2	Genehmigung oder Ablehnung von Zertifikatsanträgen.....	17
4.2.3	Dauer der Bearbeitung von Zertifikatsanträgen	17
4.2.4	Regeln für die Erfassung.....	18
4.3	Ausstellung von Zertifikaten	19
4.3.1	Von der CA bei der Zertifikatsausstellung durchgeführte Schritte	19
4.3.2	Benachrichtigung des Antragstellers über die Zertifikatsausstellung durch die CA	19
4.4	Annahme von Zertifikaten	19
4.5	Nutzung von Schlüsselpaaren und Zertifikaten	19

4.6	Verlängerung von Zertifikaten (Certificate Renewal).....	19
4.7	Zertifikatserneuerung (Certificate Re-Key).....	19
4.8	Änderung von Zertifikaten.....	19
4.9	Ungültigkeitserklärung und Suspendierung von Zertifikaten.....	19
4.10	Dienste zum Zertifikatsstatus.....	20
4.11	Ende der Zertifikatsnutzung.....	20
4.12	Hinterlegung und Wiederherstellung von Schlüsseln.....	20
5	Einrichtung, Verwaltung und Betriebskontrollen.....	21
5.1	Physische Kontrollen.....	21
5.2	Verfahrenskontrollen.....	21
5.2.1	Vertrauenswürdige Rollen.....	21
5.2.2	Anzahl der pro Aufgabe erforderlichen Personen.....	21
5.2.3	Identifikation und Authentisierung für die einzelnen Rollen.....	21
5.2.4	Rollen mit getrennten Pflichten.....	21
5.3	Personalkontrollen.....	21
5.3.1	Qualifikation, Erfahrung, Überprüfungsanforderungen.....	21
5.3.2	Verfahren zur Überprüfung des Hintergrunds und der Kenntnisse.....	22
5.3.3	Schulungsanforderungen.....	22
5.3.4	Häufigkeit der Fortbildung und Anforderungen.....	22
5.3.5	Häufigkeit und Abfolge von Stellenwechseln.....	22
5.3.6	Strafen für nicht autorisiertes Vorgehen.....	22
5.3.7	Anforderungen für unabhängige Vertragsnehmer.....	22
5.3.8	Dem Personal bereitgestellte Dokumentation.....	22
5.4	Verfahren zur Audit-Protokollierung.....	22
5.4.1	Art der aufgezeichneten Vorgänge.....	22
5.4.2	Häufigkeit der Protokollverarbeitung.....	23
5.4.3	Archivierungsdauer für das Auditprotokoll.....	23
5.4.4	Schutz des Auditprotokolls.....	23
5.4.5	Verfahren zur Sicherung des Auditprotokolls.....	23
5.4.6	Auditerfassungssystem (intern bzw. extern).....	23
5.4.7	Benachrichtigung des den Vorgang verursachenden Inhabers.....	23
5.4.8	Bewertung von Sicherheitslücken.....	23
5.5	Archivierung von Aufzeichnungen.....	23
5.5.1	Art der archivierten Aufzeichnungen.....	23
5.5.2	Archivierungsdauer.....	23
5.5.3	Schutz des Archivs.....	23
5.5.4	Verfahren zum Backup des Archivs.....	24
5.5.5	Anforderungen für das Zeitstempeln (Datieren) der Aufzeichnungen.....	24
5.5.6	Archiverfassungssystem (intern bzw. extern).....	24
5.5.7	Verfahren zur Erlangung und Überprüfung archivierter Daten.....	24
5.6	Auswechseln der Schlüssel.....	24
5.7	Verletzungen und Wiederherstellung im Notfall.....	24
5.8	Beendigung der CA oder RA.....	24
5.8.1	Ereignisse für eine Beendigung.....	24
5.8.2	Ablauf der Gültigkeit.....	24
5.8.3	Kompromittierung einer CA.....	25
5.8.4	Einstellung der Geschäftstätigkeit.....	25
6	Technische Sicherheitskontrollen.....	26

6.1	Erzeugung und Installation von Schlüsselpaaren	26
6.1.1	Erzeugung von Schlüsselpaaren	26
6.1.2	Bereitstellung des privaten Schlüssels an den Zertifikatsinhaber	26
6.1.3	Bereitstellung des öffentlichen Schlüssels an den Zertifikatsaussteller	26
6.1.4	Bereitstellung des öffentlichen Schlüssels der CA an die Zertifikatsprüfer	26
6.1.5	Schlüssellängen	26
6.1.6	Erzeugung und Qualitätsprüfung von Parametern des öffentlichen Schlüssels	26
6.1.7	Verwendungszweck der Schlüssel (gemäss Feld „KeyUsage X.509 v3“)	26
6.2	Schutz der privaten Schlüssel und Kontrolle beim Bereitstellen von Signaturerstellungseinheiten	26
6.3	Weitere Aspekte der Verwaltung von Schlüsselpaaren	26
6.3.1	Archivierung des öffentlichen Schlüssels	26
6.3.2	Nutzungszeiträume von Zertifikaten und Schlüsselpaaren	27
6.4	Aktivierungsdaten	27
6.5	Sicherheitskontrollen der Computer	27
6.5.1	Spezifische technische Anforderungen für die Sicherheit der Computer	27
6.6	Technische Kontrollen zum Lebenszyklus	27
6.7	Sicherheitskontrollen des Netzwerks	27
6.8	Zeitstempel	27
7	Zertifikats-, CRL- und OCSP-Profile	28
7.1	Zertifikatsprofile	28
7.1.1	CA Zertifikat der „HIN Health Info Net CA“	28
7.1.2	HIN ID Zertifikat für natürliche Personen	30
7.1.3	HIN ID Zertifikat für natürliche Personen mit Organisationseintrag	32
7.1.4	HIN ID Zertifikat für Arztpraxis oder Institution	34
7.1.5	HIN ID Zertifikat für Devices (z.B. Mail-Appliances)	36
7.2	Sperrlisten (CRL) Profile	38
7.2.1	Sperrliste der „HIN Health Info Net CA“	38
7.3	OCSP Profile	38
8	Audit zur Einhaltung gesetzlicher Vorgaben und andere Beurteilungen	39
8.1	Häufigkeit oder Voraussetzungen der Beurteilung	39
8.2	Von der Beurteilung abgedeckte Themen	39
8.3	Massnahmen bei Bekanntwerden von Mängeln	39
8.4	Mitteilung der Resultate	39
9	Sonstige geschäftliche und rechtliche Bestimmungen	40
9.1	Gebühren	40
9.1.1	Gebühren für die Zertifikatsausstellung oder Erneuerung	40
9.1.2	Gebühren für den Zertifikatszugriff	40
9.1.3	Gebühren für Revozierungs- oder Statusanfragen	40
9.1.4	Gebühren für andere Dienstleistungen	40
9.2	Finanzielle Verantwortung	40
9.2.1	Haftung	40
9.2.2	Haftung für Zertifikatsinhaber und RA's	40
9.3	Vertraulichkeit von Geschäftsinformationen	40
9.4	Vertraulichkeit von Personendaten	40
9.4.1	Offenlegung im Rahmen gerichtlicher oder administrativer Prozesse	40
9.5	Rechte des geistigen Eigentums	40
9.6	Zusicherungen und Gewährleistungen	41
9.7	Gewährleistungsausschluss	41

9.8	Haftung.....	41
9.8.1	Haftung der Health Info Net AG	41
9.8.2	Haftung der Zertifikatsinhaber.....	41
9.9	Schadenersatz	41
9.10	Inkrafttreten und Aufhebung	41
9.10.1	Inkrafttreten	41
9.10.2	Aufhebung	41
9.10.3	Konsequenzen der Aufhebung	41
9.11	Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern.....	41
9.12	Änderung der Richtlinien.....	41
9.13	Konfliktbeilegung	42
9.14	Geltendes Recht und Gerichtsstand	42
9.15	Konformität mit dem geltenden Recht.....	42
9.16	Weitere Bestimmungen	42
9.16.1	Geltungsbereich.....	42
9.16.2	Übertragung der Rechte und Pflichten	42
9.16.3	Salvatorische Klausel	42
9.16.4	Sprache.....	42
9.16.5	Methoden zur Verhinderung dynamischer Veränderungen	42
9.17	Signaturprüfung.....	43

1 Einleitung

Dieses Dokument stellt eine Ergänzung zu den Zertifizierungspraktiken (Certification Practice Statement, nachfolgend CPS) der QuoVadis Limited, Bermuda, dar. Es beschreibt die Spezifikationen der „HIN Health Info Net CA“ eine Dienstleistung der Health Info Net AG (nachfolgend HIN genannt), welche durch die QuoVadis Limited, Bermuda, betrieben wird.

Die „Health Info Net CA“ ist eine unter der „QuoVadis Root CA 3“ operierende Zertifizierungsstelle (nachfolgend „CA“). Für die Zertifizierungspraktiken der CA ist einzig dieses Dokument massgebend.

Die CA stellt Zertifikate aus, welche unter dem Namen „HIN Zertifikat“ ausschliesslich durch HIN vertrieben werden. Die anwendbaren allgemeinen Vertragsgrundlagen von HIN (Allgemeine Geschäftsbedingungen (AGB), Leistungsbeschreibung HIN Abo / HIN Praxispaket, Rahmenbestimmungen für die elektronische Datenkommunikation, Software-Lizenzvertrag) regeln Abschluss, Inhalt und Abwicklung von Verträgen zwischen HIN und ihren Kundinnen und Kunden über den Erwerb und den Einsatz von „HIN Zertifikat“ Zertifikaten. Bei Widersprüchen mit dem vorliegenden Dokument gehen die allgemeinen Vertragsgrundlagen von HIN vor. Für alle von der „HIN Health Info Net CA“ ausgestellten Zertifikate wird eine Gebühr erhoben, die durch HIN festgelegt wird.

Der Aufbau der CAs orientiert sich an der generellen strategischen Ausrichtung bestehender internationaler Standards in Bezug auf die Festlegung und den Betrieb einer CA für eine Public-Key-Infrastruktur (PKI).

Die QuoVadis CPS unterliegt regelmässigen, internationalen Prüfungen und kann nach den Vorgaben der zuständigen Stelle geändert werden.

Die aufgeführten Überschriften dieses Ergänzungsdokuments referenzieren auf die Nummerierung der QuoVadis CP/CPS. Alle nicht aufgeführten Kapitel werden durch die QuoVadis CP/CPS abgedeckt.

1.1 Überblick

In Ergänzung zur QuoVadis CP/CPS ist HIN berechtigt fortgeschrittene Zertifikate auszustellen und zu verwalten. Hierfür werden innerhalb der QuoVadis PKI die „HIN Health Info Net CA“ für diesen Zweck betrieben.

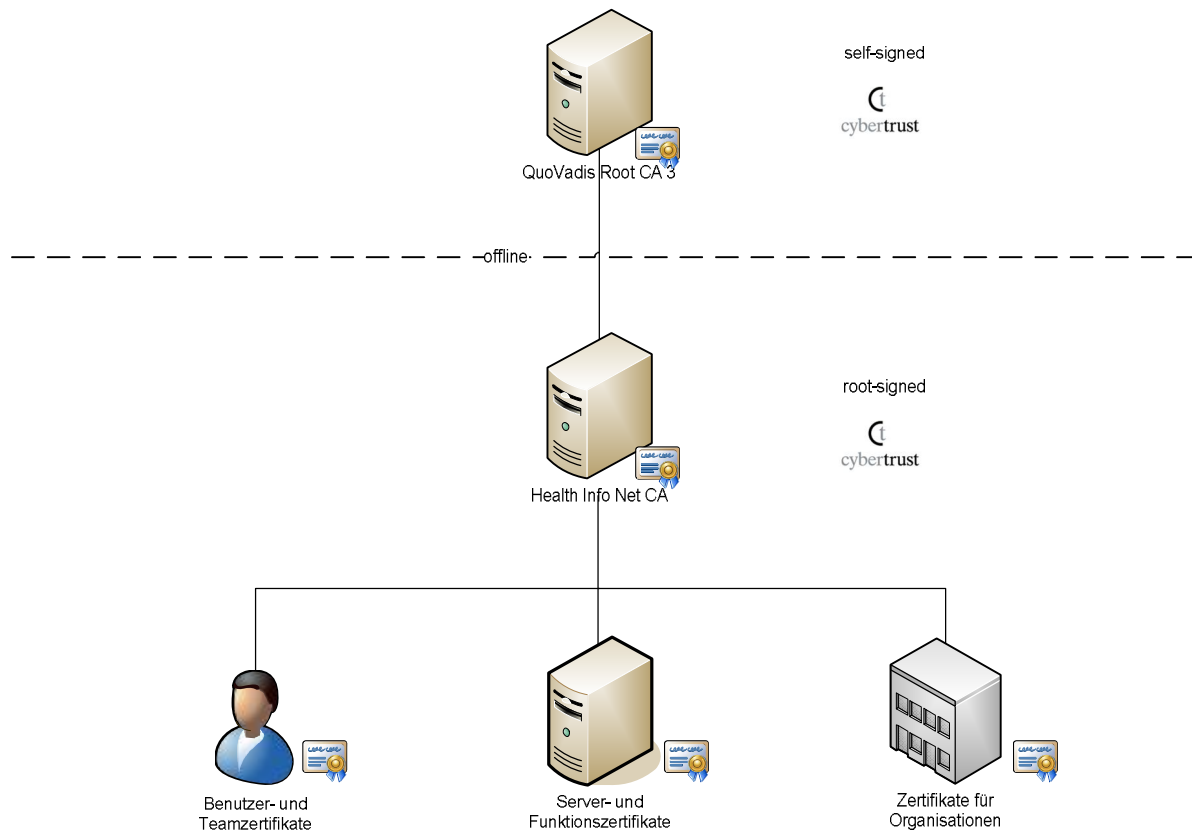
1.2 Titel und Identifikation des Dokuments

Dieses Dokument trägt den Titel

„HIN Health Info Net AG – Sicherheits- und Zertifizierungskonzept“

wie auf dem Deckblatt angegeben.

1.3 PKI Teilnehmer



1.3.1 Zertifizierungsstellen (CA)

Die aufgeführte PKI enthält ein Stammzertifikat, das den Namen „QuoVadis Root CA 3“ trägt. Die „HIN Health Info Net CA“ ist durch die zuständigen Root CA signiert.

1.3.2 Registrierungsstellen (RA)

Die unter der QuoVadis CP/CPS und diesem Ergänzungsdokument tätigen Registrierungsstellen (nachfolgend „RA“) werden ausschliesslich von HIN und allfällige durch HIN beauftragte Dritte betrieben.

In der Registrierungsstelle führen die Registrierungsverantwortlichen die anwenderrelevanten Arbeiten durch. Diese Aufgaben umfassen neben der sicheren Identifizierung auch die Bearbeitung der Anwenderdaten und die Weiterleitung von Informationen an die übergeordnete Zertifizierungsstelle. Die Ausstellung des Zertifikats erfolgt auf Veranlassung der Registrierungsstelle.

Die Registrierungsstelle der HIN ist:

RA	Ort	Kontaktperson	Kontakt	Öffnungszeiten
HEALTH INFO NET AG	Pflanzschulstrasse 3 CH-8411 Winterthur	Roger Schäfer, Leiter HIN Einzelkunden	Tel.: +41 52 235 02 70 Fax: +41 52 235 02 72 Mail: info@hin.ch	Mo.-Fr.: 08:00 bis 18:00
HIN Suisse Romande	Grand-Rue 38 2034 Peseux	Didier Boillat, Directeur pour la Suisse romande	Tel.: 0848 830 741 Fax: 032 / 732 15 69 Mail: infosr@hin.ch	Mo.-Fr.: 08:00 bis 12:00 13:00 bis 17:00 ohne Do Nachmittag

1.3.3 Zertifikatsinhaber (Subscriber)

Es gelten die Bestimmungen der QuoVadis CP/CPS.

1.3.4 Zertifikatsprüfer (Relying parties)

Es gelten die Bestimmungen der QuoVadis CP/CPS.

1.3.5 Weitere Teilnehmer

Es gelten die Bestimmungen der QuoVadis CP/CPS.

1.4 Zertifikatsnutzung

Es gelten die Bestimmungen der QuoVadis CP/CPS.

1.5 Verwaltung der Richtlinien

1.5.1 Zuständige Stelle – Aufsichtsstelle

Die Ausführungen in diesem Dokument wurden von HIN erstellt und werden von ihr auch aktualisiert.

Health Info Net AG
Pflanzschulstrasse 3
8400 Winterthur
Schweiz

Telefon: 0848 830 740
Erreichbar während den Bürozeiten:
Mo. – Fr. 08:00 – 18:00 Uhr

1.5.2 Kontaktpersonen / Ansprechpartner

Die zuständige Kontaktperson für das vorliegende Sicherheits- und Zertifizierungskonzept innerhalb HIN ist der Zertifikatsmanager.

Zertifikatsmanager Health Info Net AG

Mail: info@hin.ch

Tel.: 0848 830 740

1.5.3 Stelle für die Bestimmung der Eignung der CPS

Der Zertifikatsmanager der HIN bereitet zusammen mit der QuoVadis die Entscheidungen über die Eignung und Anwendbarkeit dieser CP/CPS vor. Die Geschäftsleitung der HIN entscheidet über die Freigabe des Sicherheits- und Zertifizierungskonzepts.

1.5.4 Genehmigungsverfahren für die CPS

Die Genehmigung des vorliegenden Sicherheits- und Zertifizierungskonzepts erfolgt durch die Bevollmächtigten der HIN. Die Genehmigung der QuoVadis CP/CPS, welche integrierter Bestandteil des vorliegenden Sicherheits- und Zertifizierungskonzepts ist, erfolgt durch die Bevollmächtigten der QuoVadis und ist in der QuoVadis CP/CPS geregelt.

Die Veröffentlichung des vorliegenden Sicherheits- und Zertifizierungskonzepts erfolgt elektronisch im Format PDF auf der Seite www.hin.ch/de/pki.

1.6 Definitionen und Abkürzungen

Begriffe

Begriff/Abkürzungen	Erklärung/Definition
Anbieterin von Zertifizierungsdiensten oder Zertifizierungsstelle Certification Service Provider (CSP) oder Certificate Authority (CA)	Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt (HIN)
Aussage über die Zertifizierungspraktiken Certificate Practice Statement (CPS)	Aussage über die Regeln und Richtlinien, die von QuoVadis für die Ausstellung von Zertifikaten effektiv umgesetzt werden. Die CPS definiert die Ausrüstungen, die Politik und die Verfahren, die von der Anbieterin von Zertifizierungsdiensten in Übereinstimmung mit der von ihr gewählten Zertifizierungspolitik verwendet werden.
Benutzer/-in des Zertifikats User or Relying Party	Person oder Prozess, die oder der sich bei der Verwendung dieses Zertifikats auf die überprüften elektronischen Signaturen verlässt.
Digitales Zertifikat Certificate	elektronische Bescheinigung, die einen Signaturprüfchlüssel mit dem Namen einer Person verknüpft.
Elektronische Signatur oder Signatur Digital Signature	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dieser Daten dienen. Eindeutige Kennzeichnung digitaler Daten durch die Anwendung asymmetrischer kryptographischer Verfahren.

Begriff/Abkürzungen	Erklärung/Definition
ETSI	European Telecommunications Standards Institute
Fortgeschrittene elektronische Signatur Advanced Signature	Elektronische Signatur, die folgende Anforderungen erfüllt: <ol style="list-style-type: none"> 1. Sie ist ausschliesslich der Inhaberin oder dem Inhaber zugeordnet 2. Sie ermöglicht die Identifizierung der Inhaberin oder des Inhabers 3. Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann. 4. Sie ist mit den Daten, auf die sie sich bezieht, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann
Generierung der Zertifikate Issuing Certificates	Dienst von QuoVadis für die Erzeugung eines digitalen Zertifikats auf der Grundlage des Namens der Antragsteller/in eines Zertifikats und ihrer/seiner allfälliger Attribute, die bei der Registrierung überprüft werden.
Hash	Kryptographische Prüfsumme über einen Datensatz (oder Text) beliebiger Länge, um dessen Integrität sicher zu stellen. Der Prüfwert wird Hash-Wert genannt.
Inhaber/-in des Zertifikats Distinguished Name (DN)	Natürliche Person, die Inhaberin des Signaturschlüssels ist, der dem im Zertifikat aufgeführten Signaturprüfschlüssel zugeordnet ist.
Kryptographische Module Hardware Security Module (HSM):	Hardware Einheit, in der geheime Schlüssel vor unbefugtem Zugriff geschützt, erzeugt, gespeichert und verwendet werden können.
Liste der für ungültig erklärten Zertifikate (Widerrufsliste) Certificate Revocation List (CRL)	von der Anbieterin von Zertifizierungsdiensten signierte Liste, die alle Seriennummern der Zertifikate enthält, welche vor Ablauf ihrer Gültigkeit für ungültig erklärt wurden
Passphrase	Wird im Zusammenhang mit dem HIN Client (Applikation zum Verwalten der persönlichen Zertifikate) und dient der Aktivierung respektive Öffnung einer Sitzung in der der private Schlüssel verwendet wird
PIN Personal Identification Number	Wird im Zusammenhang mit einer Signaturerstellungseinheit benötigt und dient der Aktivierung respektive der Öffnung einer Sitzung in der der private Schlüssel verwendet wird.
PKI Public Key Infrastructure (PKI):	Erforderliche Organisation für die Anwendung asymmetrischer kryptographischer Verfahren, insbesondere für die digitale Signatur.
Öffentlicher Schlüssel Public Key	Hälfte eines asymmetrischen Schlüsselpaares, welche öffentlich zugänglich ist. Mit diesem Schlüssel verschlüsselte Daten können nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden.
Privater Schlüssel Private Key	Hälfte eines asymmetrischen Schlüsselpaares, welches nur dem Zertifikatsinhaber bekannt bzw. zugänglich sein darf.
Registrierungsstelle Registration Authority (RA)	Dienst der HIN, der darin besteht, die Identität und wenn nötig die Attribute jeder Antragstellerin und jedes Antragstellers eines Zertifikats zu überprüfen, bevor ihr/sein Zertifikat erzeugt oder die Aktivierungsdaten (oder das Passwort) zur Aktivierung der Nutzung des Signaturschlüssels zugewiesen werden
Schlüsselpaar Key Pair	Signaturschlüssel und dazugehöriger Signaturprüfschlüssel, die mathematisch durch einen asymmetrischen Signaturalgorithmus miteinander verknüpft sind.

Begriff/Abkürzungen	Erklärung/Definition
Sicherheitspolitik Security Policies (SP):	Gesamtheit von Regeln und Richtlinien, die auf Grund einer Risikoanalyse zur Reduzierung der Wahrscheinlichkeit von möglichen Zwischenfällen (vorbeugende Massnahmen) und zur Behebung der Auswirkungen solcher Zwischenfälle (Korrekturmassnahmen) ausgearbeitet wurden, um die für die Anbieterin von Diensten der elektronischen Zertifizierung als schützenswert identifizierten Ressourcen zu schützen. Mit der Sicherheitsstrategie und -politik kann die gesamthafte zu erreichende Sicherheitsstufe für ein Informationssystem und besonders für jedes Element der Sicherheitsarchitektur eindeutig definiert werden.
Signaturprüf Schlüssel Verification Key	Daten wie Codes oder öffentliche kryptografische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.
Signaturschlüssel Key	einmalige Daten wie Codes oder private kryptografische Schlüssel, die von der Inhaberin oder vom Inhaber zur Erstellung einer elektronischen Signatur verwendet werden.
Signaturkarte Smart Card	Trägermedium für geheime Schlüssel und Zertifikate, die durch verschiedene Eigenschaften und Mechanismen (z.B. PIN Code) vor unbefugtem Zugriff geschützt sind.
Token Token/USB Token	Kryptographisches Hardwaremodul (Alternative zur Signaturkarte), welches durch verschiedene Eigenschaften und Mechanismen (z.B. PIN Code respektive Passwort) vor unbefugtem Zugriff geschützt ist.
Trust Center Trust Center (TC)	Dienste und Instanzen einer PKI, die für die Erzeugung, Ausgabe und Information über die Gültigkeit von Zertifikaten verantwortlich sind.
Ungültigerklärung/Revozierung des Zertifikats Certificate Revocation	Dienst der HIN, welcher die Gültigkeit eines Zertifikats vor dessen Ablauf aufhebt.
Verteilung der Zertifikate Certificate Enrollment	Dienst von HIN, der darin besteht, das Zertifikat nach seiner Generierung der Inhaberin oder dem Inhaber und – bei Einwilligung der Inhaberin oder des Inhabers – den Benutzerinnen und Benutzern des Zertifikats zur Verfügung zu stellen.
Verwaltung des Zertifikatstatus Identification	Dienst von QuoVadis, anhand dessen die Benutzerinnen und Benutzer eines Zertifikats überprüfen können, ob dieses für ungültig erklärt worden ist
Zeitstempel Timestamping Service	Dienst von QuoVadis, der eine mit dem Datum, der Uhrzeit und der qualifizierten Signatur von QuoVadis versehene Bescheinigung abgibt, wonach bestimmte digitale Daten zu einem bestimmten Zeitpunkt existiert haben.
Zertifizierungsstelle Certification Authority (CA)	siehe „Anbieterin von Zertifizierungsdiensten“
Zertifizierungspolitik: Certificate Policy	Gesamtheit von Regeln, welche die Anwendbarkeit eines Zertifikats für einen bestimmten Personenkreis und/oder eine Klasse spezieller Anwendungen mit gemeinsamen Sicherheitsanforderungen vorschreiben.

2 Verantwortlichkeiten für Publikation und Verwaltung

2.1 Dokumentablage

Die Aufbewahrungszeit der Dokumentation richtet sich nach Schweizer Recht und beträgt ab der letzten Eintragung zumindest 11 Jahre.

HIN veröffentlicht alle aktuellen Dokumente welche in Zusammenhang mit der „HIN Health Info Net CA“ stehen auf der Internetseite www.hin.ch/de/pki. Die Veröffentlichung von aktualisierten Versionen erfolgt ohne vorherige Ankündigung an die Zertifikatsinhaber.

Die auf der Veröffentlichungsseite publizierten Dokumente sind aktuelle, geprüfte und digital signierte Versionen.

Die gescannten Dokumente sowie das Begleitprotokoll im Rahmen eines Zertifikatsantrages werden in das Format PDF überführt und mittels fortgeschrittener Signatur, unter Einbezug des qualifizierten Zeitstempels von QuoVadis, abgesichert bevor das Dokument ins interne elektronische Archiv abgelegt werden.

2.2 Veröffentlichung der Zertifizierungsdaten

Ein Zertifikat wird nach der Ausstellung unverzüglich über den Verzeichnisdienst veröffentlicht, sofern der Zertifikatbesitzer nichts anderes gefordert hat.

Im Übrigen gelten die Bestimmungen der QuoVadis CP/CPS.

2.3 Zeitpunkt oder Häufigkeit der Veröffentlichung

Es gelten die Bestimmungen der QuoVadis CP/CPS.

2.4 Zugangskontrolle zur Dokumentablage

Es gelten die Bestimmungen der QuoVadis CP/CPS.

3 Identifikation und Authentisierung

3.1 Namensgebung

3.1.1 Namensarten

Bei allen HIN Zertifikaten werden alle Informationsfelder von der zuständigen Registration Authority anhand der entsprechenden Dokumentation und einer Kopie eines amtlichen Lichtbildausweises, bei persönlichen Identitäten, verifiziert und bestätigt.

Es sind folgende Daten durch die RA aufzunehmen:

	Validierung (prüfen mit)
Name	ZSR- und EAN-Register Passkopie
Vorname	ZSR- und EAN-Register Passkopie
Instituisname	ZSR- und EAN-Register / TwixTel
Adresse	ZSR- und EAN-Register / TwixTel
PLZ / Ort	ZSR- und EAN-Register / TwixTel
Land	
Mailadresse	Siehe 4.2.4 Regeln für die Erfassung

3.1.2 Notwendigkeit für aussagekräftige Namen

Der Name muss den Zertifikatsinhaber eindeutig identifizieren und in einer für Menschen verständliche Formen im „commonName“ (CN) des Zertifikates vorliegen.

Die restlichen Regelungen sind der QuoVadis CP/CPS zu entnehmen.

3.1.3 Anonymität oder Pseudonyme der Zertifikatsinhaber

Es gelten die Bestimmungen der QuoVadis CP/CPS.

3.1.4 Regeln für die Auslegung unterschiedlicher Namensformen

Neben dem ASCII-Zeichensatz wird zusätzlich der Zeichensatz UTF-8 oder der Zeichensatz ISO-8859-1 zugelassen.

Ergänzend gelten die Bestimmungen der QuoVadis CP/CPS.

3.1.5 Eindeutigkeit von Namen

Es gelten die Bestimmungen der QuoVadis CP/CPS.

3.1.6 Erkennung, Authentisierung und Rolle von Marken

Es gelten die Bestimmungen der QuoVadis CP/CPS.

3.2 Anfängliche Identitätsüberprüfung

Der Registrierungsvorgang (gemäß Kapitel 4.1) jeder unter dem geltenden Sicherheits- und Zertifizierungskonzept operierenden Registrierungsstelle muss Massnahmen zur Feststellung der Identität von natürlichen Personen umfassen. Die in den Registrierungsformularen festgelegten Regeln können wie folgt zusammengefasst werden:

- § Bevor ein Zertifikatsantrag gestellt werden kann, wird mit HIN ein Geschäftsvertrag abgeschlossen
- § Eine Person, ein Arzt oder eine Institution deklariert sich selbst und unterzeichnet den Antrag
- § Kopien von Lichtbildausweisen (Pass oder Identitätskarte) werden beigelegt sowie weiterer Legitimationen und an die Registrierungsstelle gesandt
- § Die RA überprüft die Dokumente und Legitimationen anhand der ihr verfügbaren Systeme. Die Überprüfung wird dokumentiert und von der RA Person visiert

3.3 Identifikation und Authentisierung für Anträge auf Zertifikatserneuerung

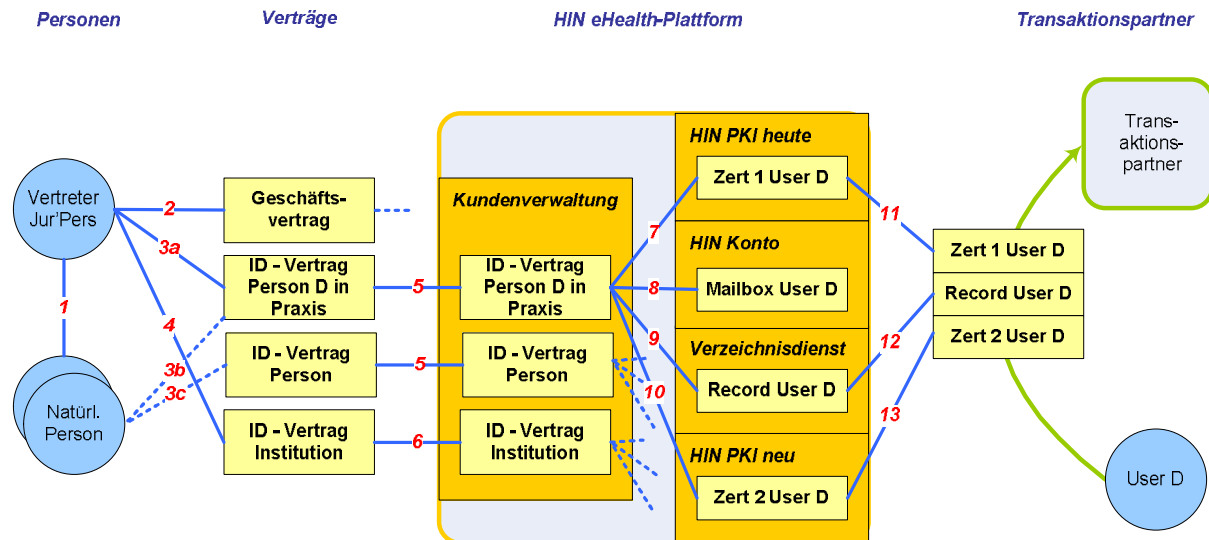
Es gelten die Bestimmungen der QuoVadis CP/CPS.

3.4 Identifikation und Authentisierung für Anträge auf Ungültigkeitserklärung

Es gelten die Bestimmungen der QuoVadis CP/CPS.

4 Betriebsanforderungen für den Zertifikatslebenszyklus

4.1 Zertifikatsantrag



4.1.1 Wer kann einen Zertifikatsantrag einreichen

Anträge können von natürlichen als auch juristischen Personen eingereicht werden, die den im Antragsformular, der Sicherheits- und Zertifizierungskonzept und den jeweils geltenden Vertragsgrundlagen entsprechen.

4.1.2 Registrierungsverfahren und Verantwortlichkeiten

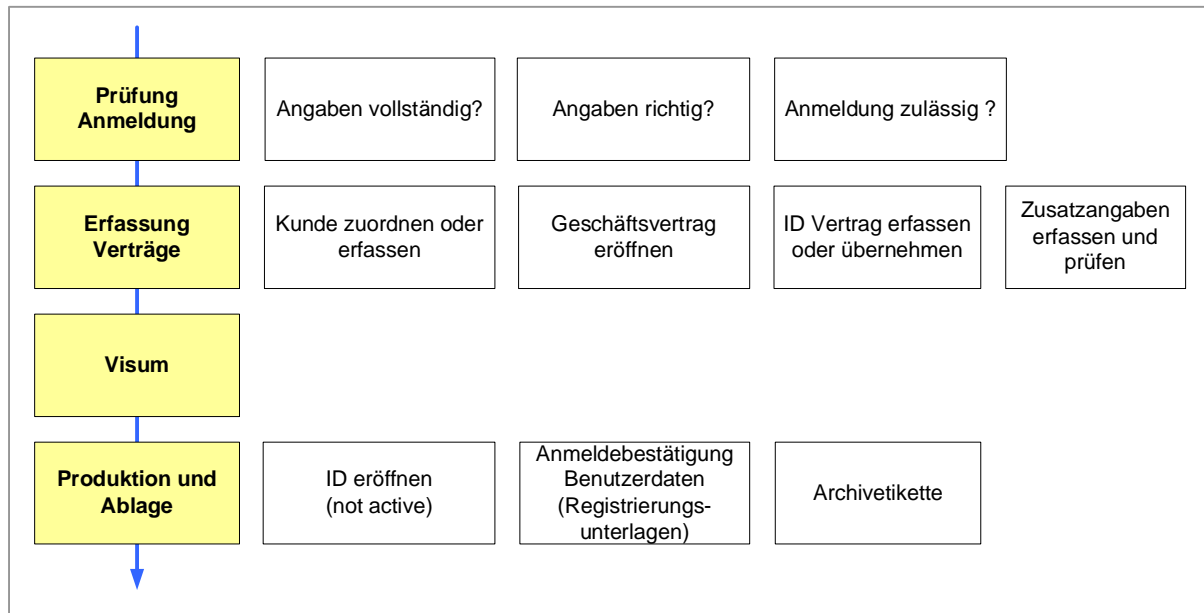
Der Antragssteller muss die Antragsformalitäten von HIN befolgen. Das Zertifikat wird nur nach erfolgreichem Abschluss des Registrierungsverfahrens ausgestellt. Die grundlegenden Schritte zur Registrierung eines Zertifikats lauten:

Tätigkeit / Verfahren	Verantwortlichkeit
§ Bestätigung der Organisationszugehörigkeit (wo notwendig)	HIN AG
§ Vertreter der juristischen Person, der Institution oder die natürliche Person selbst schliesst einen oder mehrere ID-Vertrag / ID-Verträge (Praxispaket) mit HIN ab	Vertreter der juristischen Person, der Institution oder die natürliche Person selbst
§ Erfassungsprozess inklusive Validierung/Härtung auf die Person respektive Institution	HIN AG
§ Zertifikatsgenerierungsprozess	HIN AG
§ Eingeschriebener Versand der Benutzerdaten / Registrierungsunterlagen Online-Registrierung /	HIN AG
§ Aktivierung der HIN ID im Zusammenhang mit HIN Plattform	Vertreter der juristischen Person, der Institution oder die natürliche Person selbst
§ Eintrag in Verzeichnis falls nicht anders gewünscht.	HIN AG

4.2 Bearbeitung des Zertifikatsantrags

4.2.1 Durchführung von Identifikation und Authentifizierung

Die RA der HIN identifiziert den Antragsteller anhand der vom Antragsteller zur Identifikation vorgelegten Dokumente, wie in Kapitel 3.2 festgelegt.



4.2.2 Genehmigung oder Ablehnung von Zertifikatsanträgen

Die RA der HIN genehmigt einen Zertifikatsantrag wenn alle folgenden Kriterien erfüllt sind:

- § Korrekt und original unterzeichneter Antrag und Kopie eines amtlichen Lichtbildausweises vorhanden, wo notwendig
- § Legitimationen vorhanden
- § ZSR-, GLN (EAN)- oder FMH Registereintrag vorhanden (wo vorhanden)
- § Adresse in ZSR, GLN- oder FMH Register vorhanden
- § Visum einer RA Person ist vorhanden
- § Antrag für persönliches Zertifikat mit persönlichen Daten

Wenn der Antragsteller eines der oben genannten Kriterien nicht erfüllt oder in anderer Weise die Bestimmungen dieses oder anderer relevanter Dokumente verletzt, muss die zentrale RA der HIN den Antrag ablehnen. HIN behält sich das Recht vor, Zertifikatsanträge ohne Angabe von Gründen abzulehnen.

4.2.3 Dauer der Bearbeitung von Zertifikatsanträgen

Die Bearbeitung von Anträgen erfolgt in nützlicher Frist.

4.2.4 Regeln für die Erfassung

	Person in Institution	Institution	Person
Mussfelder	Praxisname / Name der Institution	Praxisname / Name der Institution	
	Titel		Titel
	Personenname		Personenname
	Vorname		Vorname
	Adresse	Adresse	Adresse
	Common Name	Common Name	Common Name
	E-Mail-Adresse	E-Mail-Adresse	E-Mail-Adresse
Common Name	Nach dem Format [Vorname Nachname]	Name der Praxis / Name der Institution	Nach dem Format [Vorname Nachname]
E-Mail-Adresse	Siehe unten	Siehe unten	Siehe unten

Regeln für E-Mail-Adressen

Wenn Kunden eine HIN Identität bestellen, nennen sie ihre gewünschte E-Mail-Adresse. Dabei handelt es sich um einen Wunsch, den HIN in der Regel gerne erfüllt. Dabei gilt es zu beachten, dass irreführende oder unpassende E-Mail-Adressen nicht akzeptiert werden

- a) irreführende E-Mail-Adressen
Eine E-Mail-Adresse ist irreführend, wenn sie etwas vorgibt, was den Tatsachen widerspricht. Dies ist der Fall, wenn eine Person oder Firma einen Namen verwendet, der ihr nicht gehört.
Beispiel: Herr Dr. Hans Müller nennt sich Dr. Beat Meier (beat.meier@hin.ch).
Praxis Dr. Müller nennt sich Praxis Dr. Meier (praxismeier@hin.ch).
- b) Ausnahmen irreführender E-Mail-Adressen
Erlaubt sind folgende Ausnahmen (=Ausnahme der Ausnahme):
 1. Praxisinhaber Dr. Hans Müller nennt sich (=persönliches Abo) praxismueller@hin.ch. Begründung: Es ist seine Praxis, also darf er ihren Namen verwenden. Für Ärzte, die in der Praxis arbeiten, aber nicht deren Inhaber sind, gilt diese Ausnahme nicht.
 2. Umgekehrt: Die Praxis von Dr. Hans Müller nennt sich drmueller@hin.ch (Begründung siehe Punkt 1.)
 3. Herr Dr. Hans Müller nennt sich (wieso auch immer) HAM (ham@hin.ch). Diese Ausnahme gilt insbesondere für bestehende E-Mail-Adressen.
- c) Unpassende E-Mail-Adressen
Unpassend ist eine E-Mail-Adresse dann, wenn sie provokativ ist, gegen ethische Nomen verstösst oder unsinnig ist.
Beispiel: kill_knut@hin.ch
batman@hin.ch
adsasdfkoiuiop@hin.ch

Wir empfehlen E-Mail-Adressen, die möglichst aussagekräftig sind.

- d) Person in Institution
„Bevorzugt werden Adressen wie dr.carl.muster@hin.ch, dr.c.muster@hin.ch, carl.muster@hin.ch, c.muster@hin.ch“
- e) Institutionen (Praxen)
Auch bei Institutionen empfehlen wir möglichst aussagekräftige Namen. Die Adresse soll den Namen der Institutionen enthalten. Wenn es eine Praxis ist, soll dies aus dem Namen ersichtlich sein. Die Adresse kann auch ein Team bezeichnen.
praxis.carl.muster@hin.ch, praxis.muster@hin.ch, praxis.c.muster@hin.ch, praxis.talhof@hin.ch, mpa.muster@hin.ch
- f) Person
Mindestens der Nachname soll vollständig enthalten sein. Bei häufigen Namen empfehlen wir die Verwendung von Vornamen und Initialen. Wir ermuntern Ärzte, den Zusatz Dr. zu verwenden.

4.3 Ausstellung von Zertifikaten

4.3.1 Von der CA bei der Zertifikatsausstellung durchgeführte Schritte

Es gelten die Bestimmungen der QuoVadis CP/CPS.

4.3.2 Benachrichtigung des Antragstellers über die Zertifikatsausstellung durch die CA

Der Antragssteller wird durch die RA der HIN über die Zertifikatsausstellung per E-Mail informiert.

4.4 Annahme von Zertifikaten

Ein Zertifikat wird durch den Zertifikatsinhaber akzeptiert, wenn

§ das Zertifikat verwendet wird oder

§ innerhalb von 10 Tagen nach Erhalt kein Widerspruch erfolgt.

Fehlerhaft ausgestellte Zertifikate sind der ausstellenden RA unverzüglich zu melden.

Im Übrigen gelten die Bestimmungen der QuoVadis CP/CPS.

4.5 Nutzung von Schlüsselpaaren und Zertifikaten

Es gelten die Bestimmungen der QuoVadis CP/CPS.

4.6 Verlängerung von Zertifikaten (Certificate Renewal)

Es gelten die Bestimmungen der QuoVadis CP/CPS.

Eine Zertifikaterneuerung bedeutet die Ausstellung eines neuen Zertifikats ohne Änderung des öffentlichen Schlüssels oder irgendeiner anderen Information im Zertifikat.

Die HIN PKI unterstützt die Verlängerung von Zertifikaten nicht.

4.7 Zertifikatserneuerung (Certificate Re-Key)

Es gelten die Bestimmungen der QuoVadis CP/CPS.

4.8 Änderung von Zertifikaten

Es gelten die Bestimmungen der QuoVadis CP/CPS.

Die von HIN benutzte PKI unterstützt die Änderung von Zertifikaten nicht.

4.9 Ungültigkeitserklärung und Suspendierung von Zertifikaten

Bei einer Ungültigkeitserklärung von Zertifikaten wird in jedem Fall der Zertifikatshalter und der Vertretungsmachtgeber (nur bei Zertifikaten mit Firmeneintrag) durch HIN informiert. Eine allfällige Neuausstellung von Zertifikaten nach einer Ungültigkeitserklärung ist jeweils mit einer erneuten Prüfung der Identität verbunden.

Um den zeitgerechten Widerruf bzw. Sperrung eines Zertifikats zu gewährleisten und intern auf Zertifikatsprobleme mit hoher Priorität mit entsprechendem Nachdruck zu reagieren (vgl. QuoVadis CP/CPS Kapitel 4.9.5), unterhält HIN eine durchgehende 7/24-Erreichbarkeit auf E-Mail-Basis. Die allgemeine Erreichbarkeit ist unter Kapitel 1.3.2, Registrierungsstellen (RA) ersichtlich. Dies kann zur Revozierung des Zertifikats führen (verpflichtet jedoch nicht dazu), was normalerweise die Konsequenz einer solchen Aktion ist.

Suspendierungen (temporäres Aussetzen der Gültigkeit) von Zertifikaten wird nicht unterstützt. Dies betrifft jedoch nicht die Suspendierung von HIN Identitäten.

Des Weiteren gelten die Bestimmungen der QuoVadis CP/CPS.

4.10 Dienste zum Zertifikatsstatus

Der Status von digitalen Zertifikaten, die innerhalb der von HIN benutzten PKI ausgestellt werden, wird in einer Sperrliste (Certificate Revocation List – kurz CRL) veröffentlicht oder über den OCSP (Online Certificate Status Protocol) Abfragedienst zugänglich gemacht.

CRL für fortgeschrittene Zertifikate: <http://crl.quovadisglobal.com/hinicag1.crl>

OCSP Abfragedienst: <http://ocsp.quovadisglobal.com>

Adresse des Verzeichnisdienstes: <http://ldap.quovadisglobal.com>

Im Übrigen gelten die Bestimmungen der QuoVadis CP/CPS.

4.11 Ende der Zertifikatsnutzung

Das Ende der Zertifikatsnutzung tritt ein, wenn:

- § ein Zertifikat für ungültig erklärt wird;
- § die Gültigkeitsdauer eines Zertifikates abgelaufen ist.

4.12 Hinterlegung und Wiederherstellung von Schlüsseln

Nur die Schlüssel der Verschlüsselungszertifikate können hinterlegt und wiederhergestellt werden, falls dies durch den Antragssteller bei der Registrierung gewünscht wurde. Für andere Schlüssel wird keine Hinterlegung oder Wiederherstellung angeboten.

5 Einrichtung, Verwaltung und Betriebskontrollen

5.1 Physische Kontrollen

Es gelten die Bestimmungen der QuoVadis CP/CPS.

5.2 Verfahrenskontrollen

5.2.1 Vertrauenswürdige Rollen

Um eine Aufteilung der Pflichten zu gewährleisten, wird der Registrierungsprozess von getrennten Rollen-Gruppen betrieben. Es handelt sich dabei um:

- § Registrationsmitarbeitende (RM): Entgegennahme von Zertifikatsanträgen, Identifikation von Zertifikatswerbern im Rahmen der Registrierung, Beratung der Zertifikatsinhaber
- § Zertifikatsaussteller (ZA): Entgegennahme und Zweitprüfung von Zertifikatsanträgen, Ausstellung von Zertifikaten, Verwaltung und Archivierung der Zertifikats-, Token- und Aktivierungsdaten
- § Systemadministratoren (SA): sie sind verantwortlich für die Administration, Installation, Konfiguration und Wartung der lokalen Systeme, laufende Systembetreuung, Datensicherung und -wiederherstellung für die täglichen Abläufe.

Jeder Mitarbeiter kann zur selben Zeit nur einer dieser Rollen-Gruppen angehören, wobei das 4-Augenprinzip bei Zertifikatsanträgen immer zu berücksichtigen ist.

5.2.2 Anzahl der pro Aufgabe erforderlichen Personen

Jede Rolle wird zumindest von einer Person und einer weiteren Person als Stellvertretung ausgeübt. In der Rollen-Gruppe der RM sind auf jeder RA mindestens 2 Personen (1 Verantwortlicher + 1 Stellvertreter) mit den Registrationsaufgaben betraut.

5.2.3 Identifikation und Authentisierung für die einzelnen Rollen

Die Identifikation und Autorisierung für die Rolle ZA erfolgt durch Anmeldung im Netzwerksystem mit Benutzernamen und Passwort sowie durch Verwendung eines Zertifikats. Die Identifikation und Autorisierung für die Rolle SA erfolgt durch Anmeldung im Netzwerksystem mit Benutzernamen und Passwort.

5.2.4 Rollen mit getrennten Pflichten

Um eine strikte Trennung der Pflichten, wie in Abschnitt 5.2.1 beschrieben, zu gewährleisten, müssen die Rollen in Bezug auf Zugang und Betrieb an verschiedene Personen vergeben werden.

5.3 Personalkontrollen

5.3.1 Qualifikation, Erfahrung, Überprüfungsanforderungen

Um die Rolle RM zugewiesen zu bekommen, muss ein Mitarbeiter über gute Fähigkeiten im Umgang mit anderen Menschen und ein umfassendes Verständnis des Registrierungsprozesses bei HIN verfügen.

Um die Rolle ZA zugewiesen zu bekommen, muss ein Mitarbeiter über Fachkenntnisse in Bezug auf Technologie und Anwendungen, welche die PKI nutzen, verfügen. Vor Aufnahme ihrer Tätigkeit müssen sämtliche Mitarbeiter, welche die Rolle ZA ausüben, eine Vereinbarung zur Vertraulichkeit und Geheimhaltung unterzeichnen. Zudem müssen diese Mitarbeiter im Bereich Sicherheit, Sicherheitstechnologie und Sicherheitsmethodik adäquat ausgebildet sein.

Um die Rolle SA zugewiesen zu bekommen, muss ein Mitarbeiter über Fachkenntnisse in Bezug auf allgemeiner EDV, Hardware und Betriebssysteme verfügen.

Bestätigung der Fachkenntnisse:

- a) Die Bestätigung der Fachkenntnisse der Personen im und um das QuoVadis Trustcenter wurde durch den Zertifizierungsbericht der KPMG bestätigt. Diese Fachkenntnisse umfassen: ausgebildete Informatiker/in oder adäquate Ausbildung; breites Technologie-Know-how (Windows Plattformen, Linux, Mac usw.); vertiefte Kenntnisse in den Gebieten Security, Infrastruktur, Internet; praktische Erfahrungen in den Technologien PKI (Public Key Infrastructure), Smartcard, elektronische Zertifikate, digitale Signaturen etc.; sehr gute Englisch-Kenntnisse in Wort und Schrift

- b) Die Registrationsmitarbeitenden (RM) und die Zertifikatsaussteller (ZA) der HIN werden durch Fachpersonal von QuoVadis geschult und geprüft. Der Nachweis der Fachkenntnisse wird mittels schriftlicher Bestätigung festgehalten.
- c) Der Nachweis der Fähigkeiten der Systemadministratoren wird mittels schriftlicher Bestätigung durch den Bereichsleiter IT HIN festgehalten.

5.3.2 Verfahren zur Überprüfung des Hintergrunds und der Kenntnisse

Die HIN stellt keine Personen im Bereich der Zertifikatsausstellung ein, von denen HIN bekannt ist, dass sie wegen eines schwerwiegenden Verbrechens oder Vergehens verurteilt wurden, welche ihre Eignung für die jeweilige Position beeinträchtigen könnte. Bei Neu- oder Wiederanstellungen werden Strafregisterauszüge verlangt. Die strafrechtliche Unbescholtenheit des Personals wird in regelmässigen Abständen von maximal 2 Jahren mittels Strafregisterauszug überprüft.

Bei Neu- oder Wiederanstellungen werden die geforderten Kenntnisse anhand von Zeugnissen und/oder adäquaten Dokumenten zu belegen.

5.3.3 Schulungsanforderungen

Werden Mängel bei erforderlichen Fachkenntnissen festgestellt, werden diese durch geeignete Schulungsmassnahmen behoben. Diese Schulungsmassnahmen werden durch die Personalabteilung von HIN bestimmt. Wenn nötig, können die Bevollmächtigten der QuoVadis beigezogen werden.

5.3.4 Häufigkeit der Fortbildung und Anforderungen

Die Fortbildung der Mitarbeiter erfolgt je nach Bedarf, abhängig von den Anforderungen des Unternehmens oder der Einzelperson.

5.3.5 Häufigkeit und Abfolge von Stellenwechseln

Ein Stellenwechsel der Mitarbeiter erfolgt je nach Bedarf, abhängig von den Anforderungen des Unternehmens oder auf Antrag der Einzelperson.

5.3.6 Strafen für nicht autorisiertes Vorgehen

Die HIN behält sich das Recht vor, ein nicht autorisiertes Vorgehen im vollen Umfang geltender Schweizerischer Gesetze zu verfolgen.

5.3.7 Anforderungen für unabhängige Vertragsnehmer

Die HIN garantiert, dass allfällige Dritte, welche sie bezieht, sorgfältig ausgewählt werden. Die Dritten werden auf Geheimhaltung verpflichtet.

5.3.8 Dem Personal bereitgestellte Dokumentation

Die HIN stellt ihren Mitarbeitern die für die Ausübung ihrer Tätigkeit notwendigen Dokumentationen und Arbeitsanweisungen zur Verfügung.

5.4 Verfahren zur Audit-Protokollierung

Aufgrund von Aufgabenteilungen zwischen HIN und QuoVadis kommen unterschiedliche Aufzeichnungsformate zusammen. Grundsätzlich können textorientierte Dateiformate (z.B. Logdateien, auswertbare XML Dateien, etc.), Excel-Tabellen (.XLS oder .XLSX) oder datenbankbasierte Applikationen, bei denen die Daten in Felder von Datenbanktabellen strukturiert und auswertbar gespeichert werden, geführt.

5.4.1 Art der aufgezeichneten Vorgänge

Die folgenden Vorgänge werden aufgezeichnet:

- § neue Zertifikatsanträge
- § Bewilligung von Anträgen durch den ZA
- § abgelehnte Zertifikatsanträge
- § Ungültigkeitserklärung von Zertifikaten

§ Sperrung von Zertifikaten

§ Ablauf von Zertifikaten

Die oben stehende Liste ist nicht abschliessend und ausserdem auf Vorgänge beschränkt, die in direktem Zusammenhang mit der Zertifikatsverwaltung stehen. Insbesondere umfasst sie keine technischen Vorgänge, die an einer anderen Stelle protokolliert werden.

5.4.2 Häufigkeit der Protokollverarbeitung

Die Protokolle werden in regelmässigen Abständen und bei Verdachtsmomenten auditiert.

5.4.3 Archivierungsdauer für das Auditprotokoll

Die Protokoll Daten in der HIN Zertifikatsdatenbank werden nicht gelöscht.

5.4.4 Schutz des Auditprotokolls

Ein Lesezugriff wird für Mitarbeiter gewährt, die diesen Zugang im Zuge ihrer Pflichten benötigen. Die folgenden Rollen können diesen Zugang erhalten:

§ Zertifikatsaussteller (ZA)

§ Auditor

Das Protokollbuch wird in der Datenbank gespeichert.

5.4.5 Verfahren zur Sicherung des Auditprotokolls

Das Protokollbuch ist ein fester Bestandteil der HIN Zertifikatsdatenbank und unterliegt daher dem täglichen Backup. Nur Mitarbeiter mit der Rolle ZA, sowie autorisierte Personen haben Zugang zu den Backupmedien.

5.4.6 Auditerfassungssystem (intern bzw. extern)

Das Auditprotokoll oder Protokollbuch ist ein fester Bestandteil der in HIN verwendeter Software.

5.4.7 Benachrichtigung des den Vorgang verursachenden Inhabers

Es ist nicht vorgesehen, dass der Zertifikatsinhaber über Protokolleinträge informiert wird.

5.4.8 Bewertung von Sicherheitslücken

Die HIN RA behält sich das Recht vor, QuoVadis über Versuche zu informieren einen nicht autorisierten Zugang zu erlangen.

5.5 Archivierung von Aufzeichnungen

5.5.1 Art der archivierten Aufzeichnungen

Sämtliche Antragsdokumente, unterzeichnete Checklisten und Journale werden physisch archiviert.

5.5.2 Archivierungsdauer

Die Aufbewahrungszeit der Dokumentation richtet sich nach Schweizer Recht und beträgt ab der letzten Eintragung zumindest 11 Jahre.

5.5.3 Schutz des Archivs

Das physische Archiv bietet ausreichend Schutz gegen unbefugten Zugriff auf Daten und Dokumente.

5.5.4 Verfahren zum Backup des Archivs

Die Datensicherung wird regelmässig durchgeführt und an einem sicheren Ort aufbewahrt.

5.5.5 Anforderungen für das Zeitstempeln (Datieren) der Aufzeichnungen

Alle in der Datenbank sowie in den Protokolldateien enthaltenen Daten werden mit der Systemzeit des Systems zum Zeitpunkt der Aufzeichnung des Vorgangs datiert.

Die Systemzeit aller Server wird mittels einer Zeitquelle im Internet synchronisiert.

Die eingescannten Registrierungsdaten erhalten mit der elektronischen Archivierung einen Zeitstempel zugewiesen.

5.5.6 Archiverfassungssystem (intern bzw. extern)

HIN benutzt kein internes elektronisches Archivierungssystem, sondern legt die Dokumente in physischer Form ab.

5.5.7 Verfahren zur Erlangung und Überprüfung archivierter Daten

Nur autorisierte Personen sind berechtigt, die Archive vollständig zu sichten. Die Archivinhalte werden nicht vollständig freigegeben, ausser wenn dies vom Gesetz verlangt wird. HIN kann sich entscheiden, auf Verlangen einer der in der Transaktion involvierten Instanzen oder deren berechtigten Vertretern die Archivaufzeichnungen einzelner Transaktionen freizugeben. Für die Kostendeckung der Abfrage bzw. der Wiedergewinnung der Aufzeichnungen kann eine Bearbeitungsgebühr erhoben werden.

5.6 Auswechseln der Schlüssel

Es gelten die Bestimmungen der QuoVadis CP/CPS.

5.7 Verletzungen und Wiederherstellung im Notfall

Es gelten die Bestimmungen der QuoVadis CP/CPS.

5.8 Beendigung der CA oder RA

5.8.1 Ereignisse für eine Beendigung

Die folgenden Ereignisse werden in den nachfolgenden Kapiteln beschrieben:

- § Ablauf der Gültigkeit des Root CA Zertifikats
- § Ablauf der Gültigkeit des Zertifikats der ausstellenden CA
- § Kompromittierung des Root CA Zertifikats
- § Kompromittierung des Zertifikats der ausstellenden CA
- § Einstellung des Betriebs

5.8.2 Ablauf der Gültigkeit

Die relevanten Root und CA Zertifikate haben die folgenden Gültigkeiten:

CA Name	Ablaufdatum	Letzte(s) CA/Zertifikat ausgestellt
QuoVadis Root CA 3	24.11.2031	23.11.2021 (CA)
HIN Health Info Net CA	08.06.2020	07.06.2017 (End-Zertifikat)

Keine ausstellende CA darf kein Ablaufdatum besitzen welches nach dem Ablaufdatum der darüber liegenden Root CA liegt.

Um dies sicherzustellen wird die folgende Praxis angewandt:

- § Anfangs November 2021 wird eine neue QuoVadis Root Certification Authority erzeugt. Neue ausstellende CAs werden danach nur noch von der neuen Root CA signiert.
 - § 3 Jahre vor Ablauf einer ausstellenden CA wird eine neue ausstellende CA erzeugt. Nachfolgend dürfen keine Zertifikate mehr von der ablaufenden CA ausgestellt werden. Neue Zertifikate oder Zertifikatserneuerungen dürfen nur noch über die neue CA ausgestellt werden.
- Dieser Prozess wird benötigt um sicherzustellen, dass Zertifikatsinhaber oder Signaturüberprüfer nur eine Sperrliste benutzen müssen.

5.8.3 Kompromittierung einer CA

Eine Kompromittierung einer CA ist ein schwerwiegendes Ereignis welche katastrophale Auswirkungen auf HIN respektive QuoVadis Limited haben könnte.

Hinsichtlich dieser Tragweite ist eine strikte Vorgehensweise notwendig, um eine allfällige Kompromittierung zu analysieren.

Im Falle einer Kompromittierung werden die folgenden Schritte von den Geschäftsleitungen und den Verwaltungsräten der HIN als auch QuoVadis Limited autorisiert:

- § Alle existierenden Zertifikate, die von dieser CA ausgestellt wurden werden revoziert.
- § Alle Zertifikatsinhaber werden per E-Mail über die Kompromittierung und die Revozierung ihrer Zertifikate informiert. Darüber hinaus wird unmittelbar nach der Revozierung eine aktualisierte Sperrliste (CRL) ausgegeben.
- § Eine entsprechende Mitteilung wird auf den Websites von HIN und QuoVadis Limited publiziert. Darin wird festgehalten, dass die CA kompromittiert wurde, alle Zertifikate revoziert wurden und nicht mehr darauf vertraut werden darf.
- § Die Versicherungsgesellschaften werden über mögliche eintretende Schadensfälle informiert.
- § Die Behörden von Bermuda, KPMG sowie Ernst & Young müssen detailliert über die Kompromittierung der CA in Kenntnis gesetzt werden.

5.8.4 Einstellung der Geschäftstätigkeit

Gründe für eine Einstellung der Geschäftstätigkeit können z.B. sein, dass die Geschäftsleitungen, Verwaltungsräte und Aktionäre der HIN oder QuoVadis Limited dies beschliessen, dass eine der Gesellschaften von einem Mitbewerber übernommen wird oder dies aufgrund finanzieller Schwierigkeiten zu erfolgen hat.

Beim Eintritt eines obenstehenden Szenarios oder eines anderen, hier nicht aufgeführten Falls, der zur Einstellung der Geschäftstätigkeit führt, hat die HIN oder QuoVadis Limited bestimmte Verantwortlichkeiten zu erfüllen, die in den jeweiligen Signaturgesetzen aufgeführt sind.

Im Falle einer Einstellung der Geschäftstätigkeit werden die entsprechenden Stellen mindestens 30 Tage im Voraus darüber informiert und über die geplante Vorgehensweise in Kenntnis gesetzt. Darüber hinaus werden die folgenden Aktionen von den Geschäftsleitungen und den Verwaltungsräten der HIN als auch QuoVadis Limited autorisiert:

- § Alle existierenden Zertifikate, die von dieser CA ausgestellt wurden, werden revoziert.
- § Alle Zertifikatsinhaber werden per E-Mail über die Einstellung der Geschäftstätigkeit und die Revozierung ihrer Zertifikate informiert.
- § Eine aktualisierte Sperrliste (CRL) mit einer Gültigkeit von 11 Jahren und signiert von der QuoVadis Root CA 3 ausgegeben.
- § Die Signaturschlüssel der ausstellenden CAs oder die bei Geschäftseinstellung der QuoVadis Limited betroffenen Root CAs werden zerstört nachdem die korrespondierenden und aktualisierten Sperrlisten ausgegeben und publiziert wurden.
- § Die Websites
 - www.hin.ch
 - www.quovadisglobal.com
 - www.quovadisglobal.chwerden mit der neusten Sperrliste und einer Information, dass die Geschäftstätigkeit eingestellt wird, den Zertifikaten nicht mehr vertraut werden sollte und man sich an die entsprechende Stelle wenden soll.
- § Alle CA Informationen, sämtliche Unterlagen laufender Versicherungen und Kundendaten inkl. Zertifikatsanträge und Verträge werden an eine Schweizerische Treuhandunternehmung übergeben.

6 Technische Sicherheitskontrollen

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

Die Signaturerstellungsdaten der Zertifikatsinhaber werden jeweils direkt auf der CA erzeugt. Der Schlüssel der Zertifikatsinhaber entspricht einer Länge von 2048 Bit (RSA-Schlüssel). Der verwendete Hash-Algorithmus zur Erstellung der Signatur von Zertifikaten ist SHA-1.

Detailangaben sind aus Vertraulichkeitsgründen in einem separaten Dokument aufgeführt und werden nicht veröffentlicht.

6.1.2 Bereitstellung des privaten Schlüssels an den Zertifikatsinhaber

Die Erzeugung des Schlüsselmaterials erfolgt unter Obhut des Antragsstellers und auf Basis einer kommerziellen Crypto-Bibliothek.

Die Applikation regelt die Stärke der Passphrase (Passwort). Es werden 6 Zeichen mit mindestens je einem Gross- und einem Kleinbuchstaben, einem Sonderzeichen und einer Zahl verlangt.

Im Übrigen gelten die Bestimmungen der QuoVadis CP/CPS.

6.1.3 Bereitstellung des öffentlichen Schlüssels an den Zertifikatsaussteller

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.1.4 Bereitstellung des öffentlichen Schlüssels der CA an die Zertifikatsprüfer

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.1.5 Schlüssellängen

Die Wahl der Schlüssellängen und Signaturalgorithmen orientiert sich nach den Vorgaben des ETSI Algorithmenpapiers (ETSI TS 102 176-1 v 2.0.0, November 2007).

6.1.6 Erzeugung und Qualitätsprüfung von Parametern des öffentlichen Schlüssels

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.1.7 Verwendungszweck der Schlüssel (gemäss Feld „KeyUsage X.509 v3“)

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.2 Schutz der privaten Schlüssel und Kontrolle beim Bereitstellen von Signaturerstellungseinheiten

Die Applikation sorgt für den Schutz des privaten Schlüssels.

Im Übrigen gelten die Bestimmungen der QuoVadis CP/CPS.

6.3 Weitere Aspekte der Verwaltung von Schlüsselpaaren

6.3.1 Archivierung des öffentlichen Schlüssels

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.3.2 Nutzungszeiträume von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsdauer von Zertifikaten beträgt höchstens 3 Jahre.

Im Übrigen gelten die Bestimmungen der QuoVadis CP/CPS.

6.4 Aktivierungsdaten

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.5 Sicherheitskontrollen der Computer

Die Server der HIN werden durch beauftragte Dritte betrieben und sind durch Firewalls geschützt. Der Zugang zum System erfolgt ausschliesslich über sichere Protokolle.

6.5.1 Spezifische technische Anforderungen für die Sicherheit der Computer

Die HIN setzt ein in Schichten aufgeteiltes Sicherheitskonzept ein, um die Sicherheit und Integrität der zur Ausführung der HIN Software verwendeten Computer zu gewährleisten. Die folgenden Kontrollen stellen die Sicherheit der von HIN betriebenen Computersystemen sicher:

- § es werden nur Software-Pakete von vertrauenswürdigen Softwarearchiven installiert;
- § Authentifizierung und Autorisation für alle Funktionen
- § proaktives Patchmanagement.

6.6 Technische Kontrollen zum Lebenszyklus

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.7 Sicherheitskontrollen des Netzwerks

Es gelten die Bestimmungen der QuoVadis CP/CPS.

6.8 Zeitstempel

Der Zeitstempelservice von QuoVadis nutzt zur Synchronisierung zwei unabhängige, geographisch getrennte Zeitquellen. Damit kann sichergestellt werden, dass die Zeitangaben nicht manipuliert werden können. Ist die Zeitdifferenz zu gross wird eine erneute Abstimmung durchgeführt.

Der Zeitstempeldienst von QuoVadis nutzt zur bescheinigten Zeitangabe die weltweit standardisierte UTC/GMT Zeit. Davon kann jederzeit die genaue mitteleuropäische Zeit (MEZ) unter Berücksichtigung der Sommerzeit abgeleitet werden.

Des Weiteren gelten die Bestimmungen der QuoVadis CP/CPS.

7 Zertifikats-, CRL- und OCSP-Profile

7.1 Zertifikatsprofile

Die Profile, Sperrlisten und Online-Statusabfragen für die „HIN Health Info Net CA“ sind entsprechend den Vorgaben ETSI TS 101 456, IETF RFC 3280 (PKIX) sowie ITU-T X.509 v3.

Es finden keine Cross-Zertifizierungen statt und somit weisen die Zertifikate auch keine Modifikationen auf.

Im Übrigen gelten die Bestimmungen der QuoVadis CP/CPS.

7.1.1 CA Zertifikat der „HIN Health Info Net CA“

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Version	version	2 (bedeutet Version 3)
Seriennummer	serialNumber	0a 29
Signaturalgorithmus	signatureAlgorithm sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Aussteller	issuer directoryName	CN = QuoVadis Root CA 3 O = QuoVadis Limited C = BM
Gültigkeit	validity notBefore notAfter	8. Juni 2010 19:35:41 8. Juni 2020 19:35:41
Antragsteller	subject directoryName	CN = HIN Health Info Net CA O = Health Info Net AG C = CH
Schlüssel und Algorithmus zur Prüfung der Signatur des Zertifikatsinhabers	subjectPublicKeyInfo rsaEncryption	{1.2.840.113549.1.1.1} Algorithmus
öffentlicher Schlüssel des Zertifikatsinhabers	subjectPublicKey	30 82 02 0a 02 82 02 01 00 ec e6 8d ... 5c fe da 6b 03 02 03 01 00 01
Objektbezeichner des Schlüssels des Zertifikatsausstellers	authorityKeyIdentifier	{2.5.29.35} wird von der CA vergeben
Objektbezeichner des Schlüssels des Zertifikatsinhabers	subjectKeyIdentifier	{2.5.29.14} wird von der CA vergeben
Schlüsselerverwendung	keyUsage	{2.5.29.15} <u>kritisch</u> gesetzt sind keyCertSign (5), cRLSign (6)
Basiseinschränkungen	basicConstraints cA pathLenConstraint	{2.5.29.19} <u>kritisch</u> TRUE null keine Beschränkung
Zertifikatsrichtlinien	certificatePolicies extnValue id-qt-cps	{2.5.29.32} {1.3.6.1.4.1.8024.0.3.800.0} {1.3.6.1.5.5.7.2.1} Richtlinienkennzeichner-ID: CPS http://www.hin.ch/de/pki
Zugriff auf Stelleninformationen	authorityInformationAccess id-ad-ocsp accessLocation id-ad-caIssuers accessLocation	{1.3.6.1.5.5.7.1.1} {1.3.6.1.5.5.7.48.1} http://ocsp.quovadisglobal.com {1.3.6.1.5.5.7.48.2} http://trust.quovadisglobal.com/qvrca3.crt
Sperrlistenverteilungspunkte	cRLDistributionPoints extnValue	{2.5.29.31} http://crl.quovadisglobal.com/qvrca3.crl

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Fingerabdruckalgorithmus	sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Fingerabdruck		30 5b ea e9 b0 57 ac 8c 0d cc 48 e5 3d da f2 42 32 ad eb c4

7.1.2 HIN ID Zertifikat für natürliche Personen

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Version	version	2 (bedeutet Version 3)
Seriennummer	serialNumber	wird von der CA vergeben
Signaturalgorithmus	signatureAlgorithm sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Aussteller	issuer directoryName	- CN = HIN Health Info Net CA O = Health Info Net AG C = CH
Gültigkeit	validity notBefore notAfter	maximal 3 Jahre yymmddhhnssZ (UTC, ETSI TS 102 820) yymmddhhnssZ (UTC, ETSI TS 102 820)
Antragsteller	subject directoryName	<i>obligatorisch</i> E = E-Mail Adresse CN = Vorname(n), Nachname SN = HIN Login L = Wohnort C = Land (ISO 3166) Codierung der Namen in UTF8 Subset ISO 8859-1
Schlüssel und Algorithmus zur Prüfung der Signatur des Zertifikatsinhabers	subjectPublicKeyInfo rsaEncryption	{1.2.840.113549.1.1.1} Algorithmus
öffentlicher Schlüssel des Zertifikatsinhabers	subjectPublicKey	2048 Bit tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers
Objektbezeichner des Schlüssels des Zertifikatsausstellers	authorityKeyIdentifier	{2.5.29.35} 41 b9 bc 13 15 24 d9 64 ac a0 ae 77 20 46 3b fa 56 40 d6 2a
Objektbezeichner des Schlüssels des Zertifikatsinhabers	subjectKeyIdentifier	{2.5.29.14} wird von der CA vergeben
Schlüsselverwendung	keyUsage	{2.5.29.15} <u>kritisch</u> Folgende Verwendungen sind aktiv: digitalSignature (0) keyAgreement (4)
Erweiterte Schlüsselverwendung	extKeyUsage	{2.5.29.37} Folgende Verwendungen sind gesetzt: {1.3.6.1.5.5.7.3.2} Client auth.
Alternativer Name des Inhabers	subjectAltName rfc822Name	{2.5.29.17} emailAddress
Basiseinschränkungen	basicConstraints cA	{2.5.29.19} <u>kritisch</u> FALSE
Zertifikatsrichtlinien	certificatePolicies extnValue id-qt-cps	{2.5.29.32} {1.3.6.1.4.1.8024.0.3.800.0} {1.3.6.1.5.5.7.2.1} Richtlinienkennzeichner-ID: CPS http://www.hin.ch/de/pki

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Zugriff auf Stelleninformationen	authorityInformationAccess id-ad-ocsp accessLocation id-ad-caIssuers accessLocation	{1.3.6.1.5.5.7.1.1} {1.3.6.1.5.5.7.48.1} http://ocsp.quovadisglobal.com {1.3.6.1.5.5.7.48.2} http://trust.quovadisglobal.com/hinicag1.crt
Sperrlistenverteilungspunkte	cRLDistributionPoints extnValue	{2.5.29.31} http://crl.quovadisglobal.com/hinicag1.crl
Fingerabdruckalgorithmus	sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Fingerabdruck		20 Bytes wird von der CA vergeben

7.1.3 HIN ID Zertifikat für natürliche Personen mit Organisationseintrag

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Version	version	2 (bedeutet Version 3)
Seriennummer	serialNumber	wird von der CA vergeben
Signaturalgorithmus	signatureAlgorithm sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Aussteller	issuer directoryName	CN = HIN Health Info Net CA O = Health Info Net AG C = CH
Gültigkeit	validity notBefore notAfter	maximal 3 Jahre yymmddhhnssZ (UTC, ETSI TS 102 820) yymmddhhnssZ (UTC, ETSI TS 102 820)
Antragsteller	subject directoryName	<i>obligatorisch</i> E = E-Mail Adresse CN = Vorname(n), Nachname SN = HIN Login O = Praxis Institutionsname C = Land (ISO 3166) <i>optional</i> OU = Organisationseinheit L = Wohnort Codierung der Namen in UTF8 Subset ISO 8859-1
Schlüssel und Algorithmus zur Prüfung der Signatur des Zertifikatsinhabers	subjectPublicKeyInfo rsaEncryption	{1.2.840.113549.1.1.1} Algorithmus
öffentlicher Schlüssel des Zertifikatsinhabers	subjectPublicKey	2048 Bit tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers
Objektbezeichner des Schlüssels des Zertifikatsausstellers	authorityKeyIdentifier	{2.5.29.35} wird von der CA vergeben
Objektbezeichner des Schlüssels des Zertifikatsinhabers	subjectKeyIdentifier	{2.5.29.14} 41 b9 bc 13 15 24 d9 64 ac a0 ae 77 20 46 3b fa 56 40 d6 2a
Schlüsselverwendung	keyUsage	{2.5.29.15} <u>kritisch</u> Folgende Verwendungen sind aktiv: digitalSignature (0) keyAgreement (4)
Erweiterte Schlüsselverwendung	extKeyUsage	{2.5.29.37} Folgende Verwendungen sind gesetzt: {1.3.6.1.5.5.7.3.2} Client auth.
Alternativer Name des Inhabers	subjectAltName rfc822Name	{2.5.29.17} emailAddress
Basiseinschränkungen	basicConstraints cA	{2.5.29.19} <u>kritisch</u> FALSE
Zertifikatsrichtlinien	certificatePolicies extnValue id-qt-cps	{2.5.29.32} {1.3.6.1.4.1.8024.0.3.800.0} {1.3.6.1.5.5.7.2.1} Richtlinienkennzeichner-ID: CPS http://www.hin.ch/de/pki

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Zugriff auf Stelleninformationen	authorityInformationAccess id-ad-ocsp accessLocation id-ad-caIssuers accessLocation	{1.3.6.1.5.5.7.1.1} {1.3.6.1.5.5.7.48.1} http://ocsp.quovadisglobal.com {1.3.6.1.5.5.7.48.2} http://trust.quovadisglobal.com/hinicag1.crt
Sperrlistenverteilungspunkte	cRLDistributionPoints extnValue	{2.5.29.31} http://crl.quovadisglobal.com/hinicag1.crl
Fingerabdruckalgorithmus	sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Fingerabdruck		20 Bytes wird von der CA vergeben

7.1.4 HIN ID Zertifikat für Arztpraxis oder Institution

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Version	version	2 (bedeutet Version 3)
Seriennummer	serialNumber	wird von der CA vergeben
Signaturalgorithmus	signatureAlgorithm sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Aussteller	issuer directoryName	CN = HIN Health Info Net CA O = Health Info Net AG C = CH
Gültigkeit	validity notBefore notAfter	maximal 3 Jahre yymmddhhnssZ (UTC, ETSI TS 102 820) yymmddhhnssZ (UTC, ETSI TS 102 820)
Antragsteller	subject directoryName	<i>obligatorisch</i> E = E-Mail Adresse CN = Name der Praxis Institution SN = HIN Login O = Praxis Institutionsname C = Land (ISO 3166) <i>optional</i> OU = Organisationseinheit L = Wohnort Codierung der Namen in UTF8 Subset ISO 8859-1
Schlüssel und Algorithmus zur Prüfung der Signatur des Zertifikatsinhabers	subjectPublicKeyInfo rsaEncryption	{1.2.840.113549.1.1.1} Algorithmus
öffentlicher Schlüssel des Zertifikatsinhabers	subjectPublicKey	2048 Bit tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers
Objektbezeichner des Schlüssels des Zertifikatsausstellers	authorityKeyIdentifier	{2.5.29.35} 41 b9 bc 13 15 24 d9 64 ac a0 ae 77 20 46 3b fa 56 40 d6 2a
Objektbezeichner des Schlüssels des Zertifikatsinhabers	subjectKeyIdentifier	{2.5.29.14} wird von der CA vergeben
Schlüsselverwendung	keyUsage	{2.5.29.15} <u>kritisch</u> Folgende Verwendungen sind aktiv: digitalSignature (0) keyAgreement (4)
Erweiterte Schlüsselverwendung	extKeyUsage	{2.5.29.37} {1.3.6.1.5.5.7.3.2} Client auth.
Alternativer Name des Inhabers	subjectAltName rfc822Name	{2.5.29.17} emailAddress
Basiseinschränkungen	basicConstraints cA	{2.5.29.19} <u>kritisch</u> FALSE
Zertifikatsrichtlinien	certificatePolicies extnValue id-qt-cps	{2.5.29.32} {1.3.6.1.4.1.8024.0.3.800.0} {1.3.6.1.5.5.7.2.1} Richtlinienkennzeichner-ID: CPS http://www.hin.ch/de/pki

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Zugriff auf Stelleninformationen	authorityInformationAccess id-ad-ocsp accessLocation id-ad-caIssuers accessLocation	{1.3.6.1.5.5.7.1.1} {1.3.6.1.5.5.7.48.1} http://ocsp.quovadisglobal.com {1.3.6.1.5.5.7.48.2} http://trust.quovadisglobal.com/hinicag1.crt
Sperrlistenverteilungspunkte	cRLDistributionPoints extnValue	{2.5.29.31} http://crl.quovadisglobal.com/hinicag1.crl
Fingerabdruckalgorithmus	sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Fingerabdruck		20 Bytes wird von der CA vergeben

7.1.5 HIN ID Zertifikat für Devices (z.B. Mail-Appliances)

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Version	version	2 (bedeutet Version 3)
Seriennummer	serialNumber	wird von der CA vergeben
Signaturalgorithmus	signatureAlgorithm sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Aussteller	issuer directoryName	CN = HIN Health Info Net CA O = Health Info Net AG C = CH
Gültigkeit	validity notBefore notAfter	maximal 3 Jahre yymmddhhnssZ (UTC, ETSI TS 102 820) yymmddhhnssZ (UTC, ETSI TS 102 820)
Antragsteller	subject directoryName	<i>obligatorisch</i> E = E-Mail Adresse CN = Name der Praxis Institution SN = HIN Login O = Praxis Institutionsname C = Land (ISO 3166) <i>optional</i> OU = Organisationseinheit Codierung der Namen in UTF8 Subset ISO 8859-1
Schlüssel und Algorithmus zur Prüfung der Signatur des Zertifikatsinhabers	subjectPublicKeyInfo rsaEncryption	{1.2.840.113549.1.1.1} Algorithmus
öffentlicher Schlüssel des Zertifikatsinhabers	subjectPublicKey	2048 Bit tatsächlicher Wert des öffentlichen Schlüssels des Zertifikatsbesitzers
Objektbezeichner des Schlüssels des Zertifikatsausstellers	authorityKeyIdentifier	{2.5.29.35} 41 b9 bc 13 15 24 d9 64 ac a0 ae 77 20 46 3b fa 56 40 d6 2a
Objektbezeichner des Schlüssels des Zertifikatsinhabers	subjectKeyIdentifier	{2.5.29.14} wird von der CA vergeben
Schlüsselverwendung	keyUsage	{2.5.29.15} <u>kritisch</u> Folgende Verwendungen sind aktiv: digitalSignature (0) keyAgreement (4)
Erweiterte Schlüsselverwendung	extKeyUsage	{2.5.29.37} Folgende Verwendungen sind gesetzt: {1.3.6.1.5.5.7.3.1} Server auth. {1.3.6.1.5.5.7.3.2} Client auth.
Alternativer Name des Inhabers	subjectAltName DNS-Name	{2.5.29.17} alternative Domain-Namen
Basiseinschränkungen	basicConstraints cA	{2.5.29.19} <u>kritisch</u> FALSE
Zertifikatsrichtlinien	certificatePolicies extnValue id-qt-cps	{2.5.29.32} {1.3.6.1.4.1.8024.0.3.800.0} {1.3.6.1.5.5.7.2.1} Richtlinienkennzeichner-ID: CPS http://www.quovadisglobal.com/cps

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Zugriff auf Stelleninformationen	authorityInformationAccess id-ad-ocsp accessLocation id-ad-caIssuers accessLocation	{1.3.6.1.5.5.7.1.1} {1.3.6.1.5.5.7.48.1} http://ocsp.quovadisglobal.com {1.3.6.1.5.5.7.48.2} http://trust.quovadisglobal.com/hinicag1.crt
Sperrlistenverteilungspunkte	cRLDistributionPoints extnValue	{2.5.29.31} http://crl.quovadisglobal.com/hinicag1.crl
Fingerabdruckalgorithmus	sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Fingerabdruck		20 Bytes wird von der CA vergeben

7.2 Sperrlisten (CRL) Profile

Es werden nur direkte CRLs erzeugt. Die Erweiterungen „Issuer Alternative Name“, „Delta CRL Indicator“ oder „Freshest CRL“ werden nicht geführt.

Der Aufbau der Sperrlisten orientiert sich nach RFC 3280/5280.

Die Sperrlisten werden an mehreren Orten gleichzeitig hinterlegt und mittels URL Rerouting verfügbar gemacht.

7.2.1 Sperrliste der „HIN Health Info Net CA“

Beschreibung	Feld	Inhalt / OID / Bemerkungen
Version	version	1 (bedeutet Version 2)
Signaturalgorithmus	signatureAlgorithm sha1WithRSAEncryption	{1.2.840.113549.1.1.5}
Aussteller	issuerName	CN = HIN Health Info Net CA O = Health Info Net AG C = CH
Gültigkeit	thisUpdate nextUpdate	yymmddhhnssZ (UTC, ETSI TS 102 820) yymmddhhnssZ (UTC, ETSI TS 102 820)
<i>Liste der revozierten Zertifikate</i>		
Seriennummer	serialNumber	Seriennummer des revozierten Zertifikats
Grund der Revozierung	reasonCode	Auswahl aus folgenden Werten: unspecified (0), keyCompromise (1), cAC- ompromise (2), affiliationChanged (3), super- seded (4), cessationOfOperation (5), certifi- cateHold (6), removeFromCRL (8), privi- legeWithdrawn (9), aACompromise (10)
Ungültigkeitsdatum	invalidityDate	yymmddhhnssZ (UTC, ETSI TS 102 820)
Objektbezeichner des Schlüssels des Zertifikatsausstellers	authorityKeyIdentifier	{2.5.29.35} wird von der CA vergeben
Nummer der Sperrliste	cRLNumber	{2.5.29.20} wird von der CA vergeben
Ausgabeverteilungspunkt	issuingDistributionPoint extnValue	{2.5.29.28} http://crl.quovadisglobal.com/hinicag1.crl
Fingerabdruckalgorithmus	sha1WithRSAEncryption	{1.2.840.113549.1.1.5}

7.3 OCSP Profile

Es gelten die Bestimmungen der QuoVadis CP/CPS.

8 Audit zur Einhaltung gesetzlicher Vorgaben und andere Beurteilungen

HIN unterliegt den Audits, die im Rahmen des Managed PKI Vertrags mit QuoVadis ausgeführt werden.

8.1 Häufigkeit oder Voraussetzungen der Beurteilung

Überprüfungen erfolgen in regelmässigen Abständen von 1-2 Jahren sowie bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts.

Zusätzliche Überprüfungen erfolgen stichprobenartig bzw. bei begründetem Verdacht des Vorliegens sicherheitsrelevanter Mängel. QuoVadis nimmt die Überprüfung entweder selbst vor oder bestellt einen Sachverständigen, der für QuoVadis ein Gutachten erstellt.

8.2 Von der Beurteilung abgedeckte Themen

Gegenstand der Überprüfung sind alle Anforderungen, die sich aus den Rechten und Pflichten des Managed PKI Vertrags ergeben.

Die von einer Überprüfung betroffenen Bereiche werden jeweils durch QuoVadis in Zusammenarbeit mit HIN festgelegt. Für Risiken, die zwingend eine Überprüfung notwendig machen, können bestimmte Bereiche im Voraus festgelegt werden. Der Zertifikatsmanager erstellt und koordiniert mit QuoVadis einen Prüfplan für die geplanten Prüfaktivitäten.

8.3 Massnahmen bei Bekanntwerden von Mängeln

Aufgedeckte Mängel werden in Abstimmung mit QuoVadis von sich aus zeitnah behoben. Schwerwiegende Mängel mit hohem Risiko innert 2 Wochen, Mängel im mittleren Schweregrad in 1 Monat, alle anderen spätestens innerhalb 3 Monaten.

8.4 Mitteilung der Resultate

Die Ergebnisse der Überprüfung werden durch die Aufsichtsstelle innerhalb nützlicher Frist dem Zertifikatsmanager von HIN mitgeteilt.

Anleitungen zur Behebung oder allfällige Umgehungsmaßnahmen werden HIN umgehend bekannt gemacht.

9 Sonstige geschäftliche und rechtliche Bestimmungen

9.1 Gebühren

siehe Preisliste

9.1.1 Gebühren für die Zertifikatsausstellung oder Erneuerung

siehe Preisliste

9.1.2 Gebühren für den Zertifikatszugriff

Der Abruf von Zertifikaten über den Verzeichnisdienst der QuoVadis ist kostenfrei.

9.1.3 Gebühren für Revozierungs- oder Statusanfragen

Die Sperre oder der Widerruf von Zertifikaten als auch der Zugang zu den Sperrlisten und Statusinformationen ist kostenfrei.

9.1.4 Gebühren für andere Dienstleistungen

Siehe Preisliste

9.2 Finanzielle Verantwortung

9.2.1 Haftung

Für die in 9.8.1 „Haftung der Health Info Net AG“ erwähnten Ereignisse haftet HIN bis zur einer gemeinsamen Sublimite von maximal CHF 50'000 pro Ereignis und maximal 200'000 pro Kalenderjahr.

9.2.2 Haftung für Zertifikatsinhaber und RA's

Die Zertifikatsinhaber sind für einen ausreichenden Versicherungsschutz ihrer aus diesem „Sicherheits- und Zertifizierungskonzept“ fließenden Haftung selbst besorgt.

Für die Tätigkeiten der RA's haftet HIN gemäss 9.2.1.

9.3 Vertraulichkeit von Geschäftsinformationen

Es gelten die Bestimmungen der QuoVadis CP/CPS.

9.4 Vertraulichkeit von Personendaten

Es gelten die Bestimmungen der QuoVadis CP/CPS.

9.4.1 Offenlegung im Rahmen gerichtlicher oder administrativer Prozesse

Generell werden keine Dokumente oder Unterlagen von HIN gegenüber Strafverfolgungsbehörden oder Beamten solcher Stellen offen gelegt, es sei denn, es werden von einem zuständigen Gericht ordnungsgemäss ausgefertigte Urkunden, Verfügungen, Anordnungen, Urteile oder Anforderungen vorgelegt, welche die Vorlage von Informationen verlangen. Dies gilt insbesondere auch für die Offenlegung von Zertifikatsinformationen bei der Verwendung von Pseudonymen.

9.5 Rechte des geistigen Eigentums

Alles geistige Eigentum, einschliesslich aller Urheberrechte an sämtlichen digitalen Zertifikaten sowie elektronischen und anderen Dokumenten sind und bleiben Eigentum der HIN respektive der QuoVadis Limited.

9.6 Zusicherungen und Gewährleistungen

Es gelten die Bestimmungen der QuoVadis CP/CPS.

9.7 Gewährleistungsausschluss

Es gelten die Bestimmungen der QuoVadis CP/CPS.

9.8 Haftung

9.8.1 Haftung der Health Info Net AG

HIN haftet einzig für Schäden, die aufgrund ihres absichtlichen oder grobfahrlässigen Verhaltens entstehen.

Soweit gesetzlich zulässig, übernimmt HIN keinerlei Haftung für entgangenen Gewinn, Datenverlust, mittelbare Schäden oder Folgeschäden. HIN haftet nicht für Schäden, welche dadurch verursacht werden, dass Zertifikatsinhaber oder Zertifikatsprüfer die anwendbaren Bestimmungen nicht einhalten.

HIN übernimmt keinerlei Haftung für Schäden, die durch höhere Gewalt (insbesondere Naturkatastrophen, Ausfall der Strom- oder Telekommunikationsnetze, unabwendbare Einwirkungen Dritter wie z.B. Viren- oder Hackerangriffe, staatliche Massnahmen) entstehen. HIN wird wirtschaftlich angemessene Massnahmen ergreifen, um die Auswirkungen höherer Gewalt rechtzeitig auf das Minimum zu beschränken. Schäden, die aufgrund einer Verzögerung entstehen, die durch Ereignisse höherer Gewalt verursacht wurden, werden nicht durch HIN abgedeckt.

9.8.2 Haftung der Zertifikatsinhaber

Der Zertifikatsinhaber haftet für sämtlichen Schaden, der aus der Verletzung seiner aus Gesetz, Vertrag oder des vorliegenden Sicherheits- und Zertifizierungskonzepts resultierenden Verpflichtungen entsteht.

9.9 Schadenersatz

Die diesbezüglichen Bestimmungen finden sich unter Ziffer 9.8 des Sicherheits- und Zertifizierungskonzepts.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Dieses Dokument sowie die jeweiligen Änderungen treten zum Zeitpunkt ihrer Veröffentlichung auf der Website von HIN unter <http://www.hin.ch/de/pki> in Kraft.

9.10.2 Aufhebung

Dieses Sicherheits- und Zertifizierungskonzept tritt mit der Veröffentlichung einer neuen Fassung auf der Website von HIN unter <http://www.hin.ch/de/pki> ausser Kraft.

9.10.3 Konsequenzen der Aufhebung

Sämtliche Bestimmungen betreffend die Vertraulichkeit persönlicher und sonstiger Daten bleiben auch nach Beendigung weiterhin gültig.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

Sofern nichts Gegenteiliges in diesem Dokument bestimmt ist, kann HIN Benachrichtigungen per E-Mail, auf dem postalischen Weg, per Fax oder auf Webseiten bereitstellen.

9.12 Änderung der Richtlinien

HIN nimmt Änderungen an diesem Sicherheits- und Zertifizierungskonzept nach Rücksprache mit QuoVadis vor.

Neufassungen des Sicherheits- und Zertifizierungskonzepts treten mit ihrer Veröffentlichung auf der Website von HIN in Kraft und ersetzen alle früheren Fassungen dieses Dokuments (vgl. Ziffer 9.10).

9.13 Konfliktbeilegung

Im Fall einer Streitigkeit oder Auseinandersetzung in Verbindung mit der Erfüllung, Durchführung oder Auslegung dieses Dokuments werden sich die Parteien bemühen, zu einer gütlichen Einigung zu kommen.

9.14 Geltendes Recht und Gerichtsstand

Anwendbar ist ausschliesslich Schweizer Recht. Ausschliesslicher Gerichtsstand ist Winterthur.

9.15 Konformität mit dem geltenden Recht

Dieses Sicherheits- und Zertifizierungskonzept und alle damit verbundenen Rechte oder Pflichten stimmen mit Schweizer Recht überein.

9.16 Weitere Bestimmungen

9.16.1 Geltungsbereich

Alle enthaltenen Regelungen gelten zwischen HIN als CSP und den RA's. Die RA's verpflichten sich diese Regelungen ihrerseits entsprechend in die Verträge zwischen ihnen und den Zertifikatinhabern zu integrieren. Falls HIN mit den Zertifikatsinhabern direkt Verträge abschliesst, werden sie in diese integriert.

9.16.2 Übertragung der Rechte und Pflichten

Der Zertifikatsinhaber ist nicht berechtigt, seine Rechte oder Pflichten ganz oder teilweise abzutreten.

HIN ist berechtigt, ihre Rechte oder Pflichten ganz oder teilweise auf Dritte, insbesondere andere Konzerngesellschaften, zu übertragen.

9.16.3 Salvatorische Klausel

Werden einzelne Bestimmungen des Sicherheits- und Zertifizierungskonzepts von einem zuständigen Gericht als ungültig oder als nicht rechtskräftig angesehen, so wird die Gültigkeit der QuoVadis CP/CPS und des Sicherheits- und Zertifizierungskonzepts im Übrigen davon nicht berührt.

9.16.4 Sprache

Für rechtlich verbindliche Dokumente wie die CP/CPS, die Allgemeinen Geschäftsbedingungen oder die Registrierungsformulare ist die deutsche Fassung dieser Dokumente massgebend.

9.16.5 Methoden zur Verhinderung dynamischer Veränderungen

Zur Verhinderung dynamischer Veränderungen wird empfohlen geeignete Dateiformate zu verwenden, die die Einbettung von Signaturen erlauben (z.B. PDF oder XML). Eine Veränderung des Inhalts würde zur sofortigen Ungültigkeit der Signatur führen, die die Software direkt erkennt.

Weiter kann mit S/MIME Signaturen gearbeitet werden, die das zu signierende Objekt in sich einbetten. Der Vorteil liegt darin, dass die Signaturdatei die Originaldaten beinhaltet und somit die Prüfung eine dynamische Veränderung sofort aufzeigen kann. Nachteilig ist jedoch das jeweilige „Auspacken“ der Information respektive des Objekts aus der Signatur bei der separaten Verwendung.

Eine dritte Möglichkeit wäre die Verwendung einer abgesetzten Signatur mit anschliessender Verschlüsselung des Datenobjekts. Dies kann durch die Verwendung eines Verschlüsselungszertifikats erfolgen oder durch die Verwendung dafür vorgesehener Software oder Hardware.

Der Signaturerbringer ist dafür verantwortlich, dass die zu signierende Datei keine dynamischen Inhalte enthält, die das angezeigte Ergebnis möglicherweise verändern könnte (z. B. Beträge oder Sätze, die nach einem bestimmten Datum geändert werden).

Der Signaturerbringer darf keine dynamischen Inhalte in Dateien, die der Signaturerbringer bereitstellt, anbringen, die anschliessend in einem elektronischen Prozess genutzt werden könnten. Im Falle, dass der Signaturerbringer ein Dokument unterschreiben möchte, das er nicht selbst erzeugt hat, muss er sicherstellen, dass keine dynamischen Inhalte vorhanden sind. Deshalb wird empfohlen keine Dokumente zu unterzeichnen, die Makros oder ausführbaren Code besitzen. Und es wird nahegelegt entsprechenden Inhalt zuerst in ein Format zu überführen, das keine dynamischen Elemente mehr aufweist (z.B. TIFF, PDF, JPEG...).

9.17 Signaturprüfung

Die Signaturerstellung umfasst folgende Schritte:

- § Auswahl des Zertifikats auf der sicheren Signaturerstellungseinheit
- § Bildung der Zertifikatskette zum Ausstellerzertifikat und zum vertrauenswürdigen Stammzertifikat
- § Bildung des Hashwertes mittels eines sicheren Hash-Verfahrens (z.B. SHA-256)
- § Erzeugung der Signaturinformationen unter Zuhilfenahme des privaten Schlüssels, des Zertifikats des Signators sowie dem errechneten Hash-Wert. Der Zugriff auf den privaten Schlüssel ist nur möglich bei vorgängiger Eingabe des geheimen PINs.

Die Signaturprüfung umfasst folgende Schritte:

- § Erneutes Rechnen des Hash-Wertes aufgrund des in der Signatur angegebenen Hash-Algorithmus und Vergleich mit dem Hash-Wert, der in der Signatur eingebettet ist. Hierbei kann festgestellt werden, ob die Originaldatei kompromittiert wurde.
- § Prüfung der Zertifikatskette bis zum vertrauenswürdigen Stammzertifikat.
- § Prüfung der Zertifikate gegen eine Sperrliste oder OCSP Dienst mit dem Zeitpunkt der Signatur, um sicherzustellen, dass das für die Signatur benutzte Zertifikat nicht gesperrt war

Die Prüfung einer digitalen Signatur bedarf nicht nur die Prüfung der mathematischen Korrektheit, sondern setzt auch die Prüfung der Gültigkeit des für die Signatur verwendeten Zertifikats zum Zeitpunkt der Signatur voraus.

Die Prüfung des Zertifikats umfasst unter anderem auch die Prüfung des gesamten Zertifizierungspfad, das heisst, es muss geprüft werden, ob das Zertifikat von einer vertrauenswürdigen Zertifikatsausgabestelle stammt und ob alle Zertifikate in der Zertifikatskette nicht in einer Sperrliste aufgeführt sind.

Die meisten Signaturerstellungs- oder Prüfprogramme beinhalten bereits zahlreiche vertrauenswürdige Stammzertifikate oder nutzen diejenigen, die vom eingesetzten Betriebssystem als vertrauenswürdig angesehen werden. Wichtig ist jedoch, dass alle Zertifikate zum Zeitpunkt der Signatur gültig sind/waren.