

Teilnehmervereinbarung Zertifikatsdienstleistungen

(Subscriber Agreement Certificate Services)

Version: 2.0

OID: 2.16.756.1.89.1.0.2.0.2

WICHTIG: Sofern der Teilnehmer die Zertifikatsdienstleistung über seine Organisation direkt oder über einen Wiederverkäufer (nachfolgend: Reseller) bezieht, ist seine Organisation verpflichtet, den Teilnehmer und gegebenenfalls Zertifikatsinhaber, die nicht Teilnehmer sind, über diese Teilnehmervereinbarung aufzuklären und die Einhaltung der Bestimmungen einzufordern.

Dieses Dokument unterliegt dem Audit der SwissSign als akkreditierte Zertifizierungsstelle und darf weder abgeändert noch durch Nebenabreden entkräftet oder abgeändert werden.

Freigabe und Versionierung

Autor	Datum	Version	Kommentar
Ingolf Rauh	2017-07-14	1.0	Erstellung

Freigabe durch

Zeichnungsbefugte SwissSign	Digitale Signatur
Reinhard Dietrich (CISO) SwissSign AG	
Markus Naef (CEO) SwissSign AG	

Inhalt

1. Geltungsbereich	4
2. Einhaltung regulatorische Vorgaben	4
3. Vertragsbestandteile	4
4. Wiederausstellung und Attributänderung	4
5. Revozierung der Zertifikate	5
6. Zertifikatsablauf.....	6
7. Verzeichnisdienst.....	6
8. Kundendienst, Helpdesk, Support	6
9. Pflichten des TEILNEHMERS und ZERTIFIKATINHABERS im Umgang mit den Zertifikaten	6
9.1 Richtigkeit der Information	6
9.2 Schlüsselgenerierung	6
9.3 Schutz des privaten Schlüssels	6
9.4 Annahme des Zertifikats	7
9.5 Nutzung des Zertifikats	7
9.6 Meldepflicht und Ungültigerklärung (Revozierung)	7
9.7 Beendigung der Zertifikatsnutzung.....	7
9.8 Reaktion bei Missbrauch	7
9.9 Revokation bei Pflichtverletzungen	7
9.10 Managed PKI Zugangszertifikate	7
9.11 OCSP Stapling	8
9.12 Besondere Beachtung der Sorgfaltspflicht	8
10. Besondere Pflichten für Platinum Zertifikate	8
11. Relevante Informationen seitens SWISSIGN	9
12. Inkrafttreten, Dauer, Kündigung, Wirkung der Kündigung im Allgemeinen	9
13. Forderungen und Einstellung der ZERTIFIKATSDIENSTLEISTUNGEN bei Zahlungsverzug	9
14. Kundendaten und Datenschutz.....	9
15. Beizug Dritter	10
16. Gewährleistung	10
17. Haftung.....	10
18. Aus- und Einfuhr; internationaler Einsatz von Zertifikaten	10
19. Rechte an geistigem Eigentum	11
20. Teilungültigkeit dieser Vereinbarung.....	11
21. Änderung der TEILNEHMERVEREINBARUNG ZERTIFIKATSDIENSTLEISTUNGEN	11
22. Abtretung und Übertragung von Rechten und Pflichten.....	11
23. Aussergerichtliche Streitbeilegung	11
24. Anwendbares Recht und Gerichtsstand	11

1. Geltungsbereich

Mit der Antragstellung für Zertifikate und Dienstleistungen, die auf einem der öffentlich vertrauenswürdigen Wurzelzertifikate der schweizerischen oder liechtensteinischen SwissSign Platinum CA, SwissSign Gold CA oder SwissSign Silver CA basieren, stimmt der Teilnehmer einer Zertifikatsdienstleistung (nachfolgend: TEILNEHMER) der Teilnehmervereinbarung (nachfolgend: TEILNEHMERVEREINBARUNG) zu. Ein TEILNEHMER ist der Antragsteller eines SwissSign Zertifikates, der dieses von SwissSign bezieht und für sich selbst oder ein Subject (Server oder andere Person, nachfolgend: ZERTIFIKATSINHABER) ausstellt.

Die TEILNEHMERVEREINBARUNG regelt das Vertragsverhältnis zwischen TEILNEHMER sowie der SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Schweiz, (nachfolgend: SWISSSIGN) betreffend die Nutzung von Zertifikaten von SWISSSIGN (nachfolgend als Sammelbegriff: ZERTIFIKATSDIENSTLEISTUNGEN).

Ein TEILNEHMER kann Zertifikatsdienstleistung direkt oder über einen Reseller beziehen.

Die Ausstellung der Zertifikate erfolgt in Übereinstimmung mit den Vorschriften der CP/CPS des jeweiligen Wurzelzertifikates. Die CP/CPS sind in ihrer jeweils aktuellsten Form unter <https://repository.swissign.com> erhältlich.

Diese TEILNEHMERVEREINBARUNG sind auf alle TEILNEHMER und ZERTIFIKATSINHABER anwendbar, unabhängig von einer allfälligen Konzernverbindung derselben zur CA. Sie gelten als 'Subscriber Agreement' wie auch als 'Terms of Use Agreement' im Sinne der CA/Browser Forum Baseline Requirements, der ETSI Normen und entsprechenden Programmen der Betreiber von öffentlich vertrauenswürdigen Wurzelzertifikatsverzeichnissen („Trusted Root Certificate Stores“).

Voraussetzung für die Nutzung der ZERTIFIKATSDIENSTLEISTUNGEN ist die Einhaltung der kommerziellen Vertragsbedingungen, die Basis für die Nutzung durch den TEILNEHMER sind. Die kommerziellen Vertragsbedingungen sind nicht Gegenstand dieser TEILNEHMERVEREINBARUNG. Sie können auch zwischen Dritten (z.B.

Reseller, Arbeitgeber des Teilnehmers usw.) bestehen.

Der TEILNEHMER anerkennt, dass weder aus dieser TEILNEHMERVEREINBARUNG noch aus der Nutzung der ZERTIFIKATSDIENSTLEISTUNG Rechtsansprüche gegen SWISSSIGN entstehen können, es sei denn, SWISSSIGN verletzt Haftungsbedingungen gemäss Absatz 17 «Haftung».

2. Einhaltung regulatorische Vorgaben

Soweit die Ausstellung und Verwaltung von Zertifikaten gesetzlichen Anforderungen untersteht (z.B. Schweiz: ZertES, EIDI-V; Liechtenstein: Signaturgesetz, eIDAS), gewährleistet SWISSSIGN die Einhaltung der betreffenden Vorgaben und Ausführungsbestimmungen. Die SWISSSIGN untersteht insoweit der Aufsicht der zuständigen Stellen (Schweiz: Anerkennungsstelle; Liechtenstein: Amtes für Kommunikation) und es erfolgen Audits und Prüfungen unter Beachtung der für die betreffenden Zertifikate relevanten Standards (z.B. ETSI, CA Browser Forum) und gesetzlichen Regelungen.

3. Vertragsbestandteile

Die anwendbare CP/CPS des signierenden, vertrauenswürdigen Wurzelzertifikates ist integrierender Bestandteil dieser Teilnehmervereinbarung Zertifikatsdienstleistungen und hat bei Widersprüchen Vorrang.

Die anwendbare CP/CPS ist in ihrer jeweils aktuellsten Form unter <https://repository.swissign.com> erhältlich.

4. Wiederausstellung und Attributänderung

Reissuing/Rekeying: Wiederholtes Ausstellen eines Zertifikates ist möglich. Dieses kann wahlweise mit neuen selbst erzeugten Schlüsseln erfolgen, oder durch Verwendung des bereits vorhandene Schlüsselpaars oder durch Verwendung eines durch SWISSSIGN erzeugtes Schlüsselpaar geschehen. Alle Subjekt und SAN Attribute bleiben hierbei gleich. Das Reissuing kann im Self-Service (Weboberfläche) angeboten werden, automatisiert im Rahmen einer Managed PKI oder durch den Helpdesk von SWISSSIGN erfolgen.

Änderung von SAN Attribut oder Subjekt bedürfen eine Neuausstellung des Zertifikates .

5. Revozierung der Zertifikate

Revozierte Zertifikate können nicht mehr aktiv genutzt werden und werden ausnahmslos als ungültig in sogenannten Revozierungslisten („CRL“) und dem Onlineservice zur Revozierung („OCSP“) publiziert.

SWISSSIGN kann jederzeit und wo angemessen ohne vorherige Benachrichtigung das Zertifikat eines TEILNEHMERS oder ZERTIFIKATINHABERS mit sofortiger Wirkung aus beispielsweise folgenden Gründen maximal 24 Stunden nach entdeckten Eintreten des Falles für ungültig erklären:

- a) Der ZERTIFIKATINHABER oder TEILNEHMER fordert die SWISSSIGN schriftlich dazu auf, sein Zertifikat für ungültig zu erklären,
- b) Der TEILNEHMER oder ZERTIFIKATINHABER verstösst gegen die vereinbarten Bedingungen und/oder anwendbare Gesetze, Vorschriften und Verordnungen.
- c) Der TEILNEHMER oder ZERTIFIKATINHABER meldet SWISSSIGN, dass die ursprüngliche Zertifikatsanforderung unberechtigt war, und nicht genehmigt war oder die Genehmigung zurückgezogen wurde.
- d) SWISSSIGN erhält Hinweise, dass der private Schlüssel des TEILNEHMERS oder ZERTIFIKATINHABERS, der mit dem öffentlichen Schlüssel des Zertifikats korrespondiert, potentiell kompromittiert ist oder dass das Zertifikat auf andere Weise potentiell missbraucht worden ist.
- e) SWISSSIGN gelangt zur Kenntnis, dass der TEILNEHMER oder ZERTIFIKATINHABER eine oder mehrere materielle Verpflichtungen aus diesen TEILNEHMERVEREINBARUNG verletzt hat.
- f) SWISSSIGN gelangen Umstände zur Kenntnis, die darauf hinweisen, dass die Benutzung eines vollqualifizierten Domänennamens oder einer IP-Adresse des Zertifikates nicht länger rechtlich erlaubt ist (z.B. ein Gericht oder Schiedsgericht hat das Recht eines Registranden eines Domänennamens zur Verwendung des Domänennamens widerrufen, ein relevanter Lizenz- oder Dienstleistungsvertrag zwischen dem Registranden eines Domänennamens und dem Zertifikatsantragsteller wurde gekündigt, oder die Registrierungsstelle eines Domänennamens hat die Erneuerung des Domänennamens versäumt).
- g) SWISSSIGN gelangt zur Kenntnis, dass ein Wildcard Zertifikat benutzt wurde, um einen in betrügerischer Weise irreführenden, untergeordneten vollqualifizierten Domänennamen zu authentisieren.
- h) SWISSSIGN gelangt ein Wechsel der im Zertifikat enthaltenen Information zur Kenntnis.
- i) SWISSSIGN gelangt zur Kenntnis, dass das Zertifikat nicht in Übereinstimmung mit den CA/Browser Forum Baseline Requirements oder der anwendbaren CP/CPS der SWISSSIGN ausgestellt worden ist oder aufgrund neuer Vorschriften nicht mehr länger gültig sein darf.
- j) SWISSSIGN gelangt zur Auffassung, dass im Zertifikat enthaltene Informationen ungenau oder irreführend sind.
- k) SWISSSIGN stellt aus irgendeinem Grund den Betrieb ein und hat keine Vorkehrungen getroffen, dass eine andere Zertifizierungsstelle Unterstützung für die Ungültigkeitserklärung des Zertifikats anbietet.
- l) Das Recht der SWISSSIGN, mit den CA/Browser Forum Baseline Requirements konforme Zertifikate auszustellen, läuft aus oder wird widerrufen oder gekündigt, sofern SWISSSIGN keine Vorkehrungen getroffen hat, die für die Revozierung relevanten Verzeichnisse CRL/OCSP weiterhin zu unterhalten.
- m) SWISSSIGN gelangt eine möglichen Kompromittieren eines privaten Schlüssels einer SubCA oder Managed PKI, die zur Ausstellung des Zertifikats verwendet worden ist, zur Kenntnis.
- n) Der technische Inhalt oder das Format des Zertifikats stellt ein inakzeptables Risiko für die Anbieter von Anwendungssoftware oder Dritte dar (z. B. kann das CA/Browser Forum festlegen, dass ein überholter Kryptografie-/Schlüssel-Algorithmus oder eine überholte Schlüsselgrösse ein inakzeptables Risiko darstellt, und dass solche Zertifikate innerhalb einer bestimmten Frist von den Zertifizierungsstellen für ungültig erklärt und ersetzt werden sollen).

- o) Ein privater Schlüssel der SWISSSIGN Zertifizierungsstelle in der Vertrauenskette des Zertifikates wurde kompromittiert,

Für weitere Gründe einer Ungültigkeitserklärung wird auf die CP/CPS verwiesen.

Darüber hinaus ist die SWISSSIGN berechtigt, alle Vorfälle zu untersuchen und bei Bedarf gerichtlich vorzugehen.

Nach der Ungültigkeitserklärung wird das entsprechende Zertifikat ungültig. Der Zertifikatsinhaber haftet für alle Schäden, die aus der Nutzung eines für ungültig erklärten Zertifikats entstehen. Die SWISSSIGN übernimmt keine Haftung für Schäden gleich welcher Art, die aus einer solchen Nutzung entstehen. Der TEILNEHMER hat keinen Anspruch auf kostenlosen Ersatz des für ungültig erklärten Zertifikates.

Die Ungültigkeitserklärung eines Zertifikates ist beschrieben unter <https://www.swissign.com/de/revoizierung>.

6. Zertifikatsablauf

Der Geltungszeitraum eines SWISSSIGN Zertifikats ist auf die maximal verbleibende Laufzeit des Zertifikats der ausstellenden CA minus 10 Tage beschränkt. Es liegt in der alleinigen Verantwortung des Zertifikatsinhabers, die ununterbrochene Nutzung von SWISSSIGN Zertifikaten sicherzustellen. Aus diesem Grund empfiehlt SWISSSIGN dem TEILNEHMER, mindestens 30 Tage vor Ablauf des Zertifikats ein neues Zertifikat anzufordern bzw. mindestens 1 Tag vor Ablauf des Zertifikats eine Zertifikatserneuerung einzuleiten.

7. Verzeichnisdienst

SWISSSIGN führt einen öffentlichen Verzeichnisdienst über die von ihr herausgegebenen Zertifikate. Mit Zustimmung des TEILNEHMERS werden seine Zertifikate im Verzeichnisdienst publiziert. Die Zertifikate sind mit dem Herausgeber «SWISSSIGN» gekennzeichnet. Daraus kann auf ein Vertragsverhältnis zwischen SWISSSIGN und TEILNEHMER oder SWISSSIGN und ZERTIFIKATSINHABER geschlossen werden.

8. Kundendienst, Helpdesk, Support

SWISSSIGN stellt einen Kundendienst («Helpdesk» oder «Support») zur Verfügung. Dieser ist mittels Kontaktformular unter <https://www.swissign.com/de/kontakt> oder via E-Mail unter helpdesk@swissign.com erreichbar. Kommentare und Rückmeldungen zu dieser TEILNEHMERVEREINBARUNG können ebenfalls hierüber eingereicht werden.

9. Pflichten des TEILNEHMERS und ZERTIFIKATSINHABERS im Umgang mit den Zertifikaten

9.1 Richtigkeit der Information

Der TEILNEHMER und ZERTIFIKATSINHABER stellt sicher und gewährleistet, jederzeit SWISSSIGN und/oder dem Reseller korrekte und vollständige Informationen zu geben, sowohl im Zertifikatsantrag als auch anderweitig, sofern diese im Zusammenhang mit der Ausstellung von Zertifikaten gefordert werden. Das gilt insbesondere aber nicht ausschliesslich für Domännennamen, Bezeichnungen des Namens und Sitzes der Organisation, seiner Zeichnungsberechtigten und Zugangsverantwortlichen. Sofern sich Änderungen ergeben, wird der ZERTIFIKATSINHABER den TEILNEHMER kontaktieren und der TEILNEHMER diese in einem direkten kommerziellen Vertragsverhältnis mit SWISSSIGN direkt SWISSSIGN melden, ansonsten erfolgt die Meldung über den Reseller an SWISSSIGN im Rahmen einer Änderungsbestellung durch den Reseller.

9.2 Schlüsselgenerierung

Sofern der TEILNEHMER das Schlüsselpaar selber generiert, wählt er einen Algorithmus und Schlüssellänge gemäss ETSI Norm TS 119 312, die als anerkannt gilt für den Einsatz dieses Zertifikates während der Gültigkeitsdauer.

9.3 Schutz des privaten Schlüssels

Der TEILNEHMER stellt sicher und gewährleistet, alle sinnvollen Massnahmen ergriffen zu haben, und dass der ZERTIFIKATSINHABER die alleinige Kontrolle über die privaten Schlüssel hat. Das betrifft auch alle Massnahmen diesen vertraulich zu halten und jederzeit angemessen zu schützen.

9.4 Annahme des Zertifikats

Der TEILNEHMER verpflichtet sich und gewährleistet, dass er mit dem ZERTIFIKATSINHABER den Zertifikatsinhalt bei Erhalt auf Richtigkeit hin überprüft.

9.5 Nutzung des Zertifikats

Der TEILNEHMER stellt sicher, dass er SSL Serverzertifikate nur auf denjenigen Servern installiert, die unter der Bezeichnung im subjectAlt-Name des Zertifikates zugänglich sind. Alle Zertifikate werden nur gemäss dem geltenden Recht und nur im Einklang mit der TEILNEHMER-VEREINBARUNG genutzt.

Der TEILNEHMER verpflichtet sich den Schlüssel des Zertifikates nur für den Zweck zu verwenden, für den das Zertifikat ausgestellt ist.

9.6 Meldepflicht und Ungültigerklärung (Revozierung)

Der TEILNEHMER und der ZERTIFIKATSINHABER stellen sicher, sofort das Zertifikat zu revozieren oder SWISSIGN um die Ungültigerklärung des Zertifikates zu bitten, falls:

- a) irgendeine Information im Zertifikat ungültig oder falsch ist oder wird; oder
- b) das Kompromittieren, der Missbrauch oder der Diebstahl des Privaten Schlüssels entdeckt oder vermutet wird, bezogen auf den öffentlichen Schlüssel, der mit dem Zertifikat verknüpft ist.
- c) Auf den privaten Schlüssel nicht mehr zugegriffen werden kann.

9.7 Beendigung der Zertifikatsnutzung

Der TEILNEHMER und ZERTIFIKATSINHABER hat die Nutzung des privaten Schlüssels sofort einzustellen, falls ein Missbrauch oder Diebstahl des privaten Schlüssels stattgefunden hat und das Zertifikat revoziert wurde. Das gilt auch für den Fall, dass der TEILNEHMER oder ZERTIFIKATSINHABER darüber Kenntnis erlangt, dass ein von der CA herausgegebenes Zertifikat in der Zertifikatskette kompromittiert wurde und nicht mehr gültig ist. Sofern die Gültigkeit des Zertifikates oder eines Zertifikates in der Zertifikatskette abgelaufen ist, darf dieses nur noch für die Entschlüsselung eingesetzt werden. Ein revozier-

tes Zertifikat kann nicht mehr in den gültigen Zustand versetzt werden.

9.8 Reaktion bei Missbrauch

Der TEILNEHMER setzt binnen vorgegebener Zeit alle Anweisungen der SWISSIGN durch, die im Zusammenhang mit dem Diebstahl des privaten Schlüssels stehen. SWISSIGN wird bei ihren Anweisungen die üblichen Bürozeiten berücksichtigen, sofern die Dringlichkeit dies erlaubt, und sich bemühen, die Anweisungen angemessen zu erläutern.

9.9 Revokation bei Pflichtverletzungen

Der TEILNEHMER und der ZERTIFIKATSINHABER anerkennt und akzeptiert, dass SWISSIGN das Recht hat, ein Zertifikat sofort zu revozieren, wenn der TEILNEHMER oder ZERTIFIKATSINHABER die entsprechende CP/CPS oder dieses Managed PKI Setup Agreement verletzt, oder wenn SWISSIGN entdeckt, dass das Zertifikat für gesetzeswidrige Aktivitäten eingesetzt wurde, wie z.B. Phishing Attacken, Betrug oder Verbreitung von Schadsoftware.

Bestehen Anhaltspunkte dafür, dass der TEILNEHMER oder ZERTIFIKATSINHABER sich nicht an weitergehende gesetzliche oder vertragliche Verpflichtungen hält, hat SWISSIGN das Recht, nach Mahnung und Ansetzung einer angemessenen Nachfrist zur Behebung der Verletzung, sämtliche gemäss vorliegendem Vertrag ausgestellten Zertifikate zu revozieren.

9.10 Managed PKI Zugangszertifikate

Eine Managed PKI ist eine Zertifikatsdienstleistung, die es dem TEILNEHMER ermöglicht selbstständig für seine Organisation und Domänen Zertifikate ohne Einzelgenehmigung auszustellen. Hierfür erhält der TEILNEHMER Zugangszertifikate.

Der TEILNEHMER garantiert die Verwendung aller Zugangszertifikate, die von SWISSIGN im Rahmen dieser Managed PKI Verträge ausgestellt werden, gemäss den Vorschriften der geltenden SWISSIGN CP/CPS.

Er stellt sicher, dass die Zugangszertifikate entsprechend den Schutzvorschriften für Zertifikate gemäss den oben genannten Vorschriften dieses

Paragraphen 9 sorgfältig zu behandeln. Er hat insbesondere die Zugangszertifikate und die zugehörigen Passwörter getrennt voneinander aufzubewahren. Er ist haftbar für alle Schäden, die insbesondere aus der nicht genehmigten, nicht vorgesehenen oder unsorgfältigen Benutzung dieser Zertifikate resultieren.

Hat der TEILNEHMER Grund zur Annahme, dass ein unberechtigter Dritter die Zugangsmittel zur Managed PKI kennt oder unbefugter Weise Zugriff nehmen kann, muss er dies unverzüglich direkt SWISSSIGN melden.

PINs und Passwörter müssen geheim gehalten werden und alle Daten hierüber müssen verschlossen an einem sicheren Ort aufbewahrt werden, der Dritten nicht zugänglich ist. Haben Dritte Zugang zu seinem Konto bei SWISSSIGN, hat der TEILNEHMER deren Handlungen als eigene anrechnen zu lassen.

Der TEILNEHMER muss sicherstellen, dass sein hierfür im Einsatz befindliches IT System, welches für die Signatur und Verschlüsselung von Daten gebraucht wird, mit der gebotenen Sorgfalt auf Viren geprüft und auf dem neuesten Stand gehalten wird, um den Einsatz von Software zu verhindern, welche das Ziel hat, die Signaturen oder Zertifikate zu kompromittieren.

9.11 OCSP Stapling

Der TEILNEHMER muss bei reger Nutzung einer mit öffentlich vertrauenswürdigen SSL Zertifikaten geschützten Webseite und bei Einsatz von SSL EV Zertifikaten sicherstellen, dass OCSP Stapling Webserverseitig implementiert wird.

9.12 Besondere Beachtung der Sorgfaltspflicht

Der TEILNEHMER anerkennt, die Verletzung seiner Sorgfaltspflichten insbesondere bei öffentlich vertrauenswürdigen Zertifikaten bei SWISSSIGN zu einem finanziellen Schaden und/oder anderen Nachteil führen kann, wie z.B. Ausschluss aus Root Programmen oder Sanktionierung bei Anerkennungen / Zertifizierungen oder aufsichtsrechtliche Nachteile.

10. Besondere Pflichten für Platinum Zertifikate

ZERTIFIKATSDIENSTLEISTUNGEN, die unter der SWISSSIGN Platinum CA und zugehörigen CP/CPS (siehe 3) ausgestellt wurden unterliegen besonderen Pflichten des ZERTIFIKATINHABERS:

Die ZERTIFIKATSINHABER eines eIDAS oder ZertES konformen, qualifizierten Zertifikates oder Siegelzertifikates nutzen dieses ausschliesslich auf einer sicheren, gesetzlich vorgeschriebenen Signaturerstellungseinheit oder im Rahmen des Signaturservices unter Beachtung der gesetzlichen Anforderungen. Der TEILNEHMER stellt sicher, dass kryptographische Funktionen und der Einsatz des privaten Schlüssels nur auf diesen Geräten erfolgt.

Auf erste Anfrage von SWISSSIGN ist die Nutzung der geeigneten Signaturerstellungseinheit SWISSSIGN nachzuweisen. Der ZERTIFIKATSINHABER eines unter der SWISSSIGN Platinum CA und zugehörigen CP/CPS (siehe 3) auf SmartCard oder HSM ausgestellten Zertifikates verpflichtet sich zum sorgfältigen Umgang mit dieser Signaturerstellungseinheit (SmartCard, HSM) gemäss Ziffer 8 auch nach Ablauf der Gültigkeit des darauf befindlichen Zertifikates.

Eine Wiederverwertung dieser Einheit ist untersagt.

Platinum Zertifikate, welche als EIDI-V kompatibel gekennzeichnet sind, dürfen nur genutzt werden unter Beachtung der EIDI-V Verordnung SR 641.201.1.

Die Platinumzertifikate sehen keine Obergrenze von Transaktionswerten vor.

Die SWISSSIGN empfiehlt für alle anderen Zertifikate die Verwendung einer sicheren Signaturerstellungseinheit.

Der TEILNEHMER anerkennt, dass SWISSSIGN Platinum CA und zugehörigen CP/CPS (siehe 3) auch die Ausgabe von Zertifikaten ermöglicht, die nicht als qualifiziert oder geregelt anerkannt werden.

11. Relevante Informationen seitens SWISSIGN

Alle relevanten Informationen über Missbrauch, Kompromittierung, Algorithmenänderungen, Systemausfälle etc. werden seitens SWISSIGN kommuniziert über die Systemstatusseite <https://www.swissign.com/de/systemstatus>.

12. Inkrafttreten, Dauer, Kündigung, Wirkung der Kündigung im Allgemeinen

Der Vertrag kommt mit der Ausstellung des Zertifikates zustande und gilt während dessen Dauer. Er endet mit Ablauf des betroffenen Zertifikates oder mit der Revozierung (Zurückziehen).

Mit Beendigung des Vertrags erlischt die Gültigkeit des Zertifikates. Gegebene Zeitstempel und Signaturen bleiben gültig, sofern die Signaturzertifikate nicht revoziert wurden. Noch gültige Zertifikate werden revoziert.

Die Kündigung hat immer schriftlich zu erfolgen.

13. Forderungen und Einstellung der ZERTIFIKATSDIENSTLEISTUNGEN bei Zahlungsverzug

Der TEILNEHMER kann Forderungen der SWISSIGN nicht mit allfälligen Gegenforderungen verrechnen.

Sofern ein Zahlungsausfall des RESELLERS oder TEILNEHMERS bezüglich der ZERTIFIKATSDIENSTLEISTUNG eintritt, gelten die nachfolgenden Vorschriften:

- a) Schuldet der TEILNEHMER oder RESELLER das Leistungsentgelt an SWISSIGN, so gerät der Schuldner durch Mahnung in Verzug.
- b) Wird auch innerhalb der Nachfrist die Zahlung nicht geleistet, informiert SWISSIGN im Falle einer über den RESELLER verkauften ZERTIFIKATSDIENSTLEISTUNG den TEILNEHMER des Resellers über den Verzug des Resellers.
- c) SWISSIGN hält den TEILNEHMER direkt zur Zahlung der ihn betreffenden, offenen Leistungen innert einer letzten Zahlungsfrist an und informiert ihn über die bei Nichtzahlung drohende Leistungseinstellung.

Wird innerhalb der letzten Zahlungsfrist die Zahlung weder von einem Reseller noch vom TEILNEHMER geleistet, ist SWISSIGN berechtigt, den Zugang zu den ZERTIFIKATSDIENSTLEISTUNGEN zu sperren und die betreffenden, nicht bereits vollständig bezahlten Zertifikate zu revozieren oder die Leistung eingeschränkt zur Verfügung zu stellen.

14. Kundendaten und Datenschutz

Die SWISSIGN verpflichtet sich, die anwendbaren Datenschutzgesetzgebungen für ihre jeweilige CA einzuhalten.

Die Daten im Zertifikat sind als öffentlich verfügbare Daten anzusehen.

Die für die Leistungserbringung notwendigen Daten werden durch SWISSIGN gespeichert und vertraulich behandelt. Die im Rahmen der Prüftätigkeit erhobenen Daten, insbesondere Personendaten dürfen nur für den Zweck und im Umfang, soweit dieser für die Erfüllung und Durchführung des ZERTIFIKATSDIENSTLEISTUNG erforderlich ist, verwendet werden. Die Nutzung für andere Zwecke oder gar die Weitergabe an Dritte ist strikt untersagt. Vorbehalten bleibt die Weitergabe an (z. B. im Falle einer Kontrolle, externe Registrierungstätigkeit) beauftragte, berechnigte Dritte oder durch behördliche Anordnungen. Beauftragte, berechnigte Dritte unterliegen den Datenschutzbestimmungen in gleicher Weise wie SWISSIGN.

Zum Schutz der Daten wird Sicherheitstechnologie nach Stand der Technik eingesetzt.

Der TEILNEHMER und ZERTIFIKATSINHABER seinerseits verpflichtet sich, die auf ihn lokal anwendbaren Datenschutzvorschriften einzuhalten sowie die Datenschutzbestimmungen der CP/CPS (siehe 3).

Zur Einhaltung der gesetzlichen Vorschriften muss die SWISSIGN Zertifizierungs- und Registrierungsstelle alle Zertifikatsinhaberdaten, Dokumentationen und Auditinformationen für einen Mindestzeitraum von 11 Jahren nach Beendigung eines Zertifikats aufbewahren.

Das Datenschutzniveau in der Schweiz ist von der Europäischen Kommission als angemessen

bestätigt. Für eine rechtmässige Datenübermittlung aus Mitgliedstaaten der Europäischen Union in die Schweiz ist damit die Voraussetzung erfüllt, dass bei der empfangenden Stelle im Drittland ein angemessenes Datenschutzniveau gewährleistet sein muss.

15. Beizug Dritter

SWISSSIGN kann zur Erfüllung ihrer Leistungen jederzeit Dritte beiziehen.

16. Gewährleistung

Der TEILNEHMER hat geliefertes Material, insbesondere die gelieferten Zertifikate, nach Ausstellung zu prüfen oder prüfen zu lassen und umgehend (spätestens innerhalb von 7 Arbeitstagen), jedoch auf jeden Fall vor dem ersten Einsatz, allfällige Mängel, unrichtige und/oder unvollständige Angaben zu rügen. Werden offensichtliche Mängel nicht umgehend nach Erhalt, versteckte Mängel nicht umgehend nach Entdeckung gerügt, gelten die Mängelrechte als verwirkt. Den TEILNEHMER trifft die Beweislast für den geltend gemachten Mangel, den Zeitpunkt der Feststellung und für die Rechtzeitigkeit der Mängelrüge.

Erfolgt eine Mängelrüge, steht SWISSSIGN das Wahlrecht zwischen einer Nachbesserung und einer Ersatzlieferung zu. Mangelhafte Zertifikate werden für ungültig erklärt und durch neue ersetzt. Weitergehende Mängelrechte werden ausdrücklich wegbedungen.

SWISSSIGN übernimmt keine Gewährleistung für die Kompatibilität der gelieferten Zertifikate mit nicht schweizerischem Recht und behält sich vor, Zertifikatsanträge von den TEILNEHMER abzulehnen, falls gesetzliche Exportbeschränkungen oder Exporteinschränkungen oder Compliance-Vorschriften von SWISSSIGN einer Lieferung entgegenstehen.

17. Haftung

SWISSSIGN haftet gegenüber dem TEILNEHMER für alle Schäden, die sie dem TEILNEHMER verursacht, sofern sie nicht beweist, dass sie kein Verschulden betrifft. Die Haftung für leichte Fahrlässigkeit ist ausgeschlossen.

Gegenüber Dritten gelten die Haftungsvorschriften der CP/CPS (siehe 3.).

Keine Partei haftet für das ordentliche Funktionieren von Systemen Dritter, so insbesondere des Internets. SWISSSIGN haftet nicht für die vom TEILNEHMER verwendeten Systeme und Software.

Der TEILNEHMER verpflichtet sich, SWISSSIGN von sämtlichen Ansprüchen Dritter freizustellen, die aus der vertrags- bzw. rechtswidrigen oder missbräuchlichen Nutzung der ZERTIFIKATSDIENSTLEISTUNG resultieren. Die Freistellung umfasst auch die Verpflichtung, SWISSSIGN von Rechtsverteidigungskosten (z. B. Gerichts- und Anwaltskosten) vollständig freizustellen.

Beide Parteien haften für das Verhalten ihrer Hilfspersonen sowie beigezogener Dritter (z.B. Subunternehmer, Zulieferanten) wie für ihr eigenes.

Bei Personenschäden haften die Parteien für jedes Verschulden. In keinem Fall haften die Parteien insbesondere für indirekte Schäden, für mittelbare Schäden, für Folgeschäden, für Datenverlust, für Mehraufwand oder Ansprüche Dritter, für entgangenen Gewinn oder nicht realisierte Einsparungen sowie für Schäden aus verspäteter Lieferung oder Leistung.

In jedem Falle gelten vorrangig die Haftungsvorschriften des Bundesgesetzes über die elektronische Signatur sowie von Art. 59a des Schweizerischen Obligationenrechts.

18. Aus- und Einfuhr; internationaler Einsatz von Zertifikaten

Der TEILNEHMER und ZERTIFIKATSINHABER nimmt zur Kenntnis, dass die Aus- bzw. Einfuhr und die Verwendung von ZERTIFIKATSDIENSTLEISTUNGEN in von Sanktionen und Embargos betroffene Länder untersagt ist (vgl. <https://www.swissign.com/export>).

Der TEILNEHMER und ZERTIFIKATSINHABER nimmt zur Kenntnis, dass der Einsatz und der Gebrauch von digitalen Zertifikaten sowie der Austausch von signierten und/oder verschlüsselten Daten ausserhalb der Schweiz, Liechtenstein und der EU/EWR ausländischen Rechtsordnungen

gen unterstehen und daher abweichende, allenfalls weitergehende oder weniger weitgehende Wirkungen entfalten können, als dies nach schweizerischem, liechtensteinischen oder EU Recht der Fall ist.

Der Austausch verschlüsselter Daten wie auch der Export/Import kryptografischer Software oder kryptografischer Datenträger unterliegt zudem in gewissen ausländischen Staaten gesetzlichen Restriktionen. Die Abklärung der diesbezüglichen rechtlichen Gegebenheiten obliegt immer dem TEILNEHMER.

19. Rechte an geistigem Eigentum

Durch die ZERTIFIKATSDIENSTLEISTUNG werden keine Immaterialgüterrechte (z.B. Urheber-, Marken-, Design- oder Patentrechte usw.) auf den TEILNEHMER übertragen. Sämtliche Immaterialgüterrechte an dem von SWISSIGN ausgehändigten Material (Dokumentationen, Geräte, Software usw.) verbleiben bei SWISSIGN oder den daran berechtigten Dritten. Der TEILNEHMER erhält im Falle einer Lieferung von Material oder ausführbarer Software eine im Rahmen des Vertragszweckes stehende nicht ausschliessliche, nicht übertragbare und auf die Dauer des Vertrages zeitlich begrenzte Lizenz zu dessen Gebrauch. Der TEILNEHMER hat keine Änderungs- oder Weiterentwicklungsrechte.

20. Teilungültigkeit dieser Vereinbarung

Erweisen sich einzelne Bestimmungen dieser TEILNEHMERVEREINBARUNG als ungültig oder rechtswidrig, so wird die Gültigkeit des Vertrages davon nicht berührt. Die betreffende Bestimmung soll in diesem Fall durch eine wirksame, wirtschaftlich möglichst gleichwertige Bestimmung ersetzt werden.

21. Änderung der TEILNEHMERVEREINBARUNG ZERTIFIKATSDIENSTLEISTUNGEN

SWISSIGN behält sich vor, diese Teilnehmervereinbarung Zertifikatsdienstleistungen jederzeit zu ändern. Die jeweilige Neuversion wird rechtzeitig vor Inkrafttreten auf der Webseite <https://repository.swissign.com> veröffentlicht und über die Systemstatusseite kommuniziert: <https://www.swissign.com/de/systemstatus>.

Die geänderten TEILNEHMERVEREINBARUNG gelten als genehmigt, sofern der TEILNEHMER nicht innert Monatsfrist nach erfolgter Kenntnisnahme schriftlich widerspricht. Ein Widerspruch gilt als Kündigung des Vertrags und führt automatisch zu dessen Auflösung.

22. Abtretung und Übertragung von Rechten und Pflichten

Der TEILNEHMER darf Forderungen gegenüber SWISSIGN ohne schriftliche Zustimmung von SWISSIGN weder abtreten noch verpfänden.

Der TEILNEHMER hat nicht das Recht, die aus diesem Vertrag fließenden Rechte und Pflichten abzutreten oder zu übertragen.

23. Aussergerichtliche Streitbeilegung

Die Parteien bemühen sich bei Streitigkeiten vor Anrufung der ordentlichen Gerichte, eine einvernehmliche Lösung zu suchen, und verpflichten sich im Rahmen ihrer gesetzlichen Pflichten, an gesetzlich vorgesehenen aussergerichtlichen Streitbeilegungsverfahren teilzunehmen.

24. Anwendbares Recht und Gerichtsstand

Auf das Rechtsverhältnis aus dieser TEILNEHMERVEREINBARUNG ist ausschliesslich schweizerisches Recht anwendbar. Vorbehalten ist das liechtensteinische Signaturrecht für Zertifikate, die von der liechtensteinischen CA ausgestellt und signiert wurden. Die Bestimmungen des Übereinkommens der Vereinten Nationen vom 11. April 1980 über Verträge über den internationalen Warenkauf (Wiener Kaufrecht, CISG) sind in jedem Falle wegbedungen.

Ausschliesslicher Gerichtsstand ist Zürich, Schweiz. Für Teilnehmer und Zertifikatsinhaber mit ausländischem Wohn- bzw. Geschäftssitz gilt Zürich, Schweiz, als Betreibungsort und als ausschliesslicher Gerichtsstand für alle zivilrechtlichen Verfahren.