Nutzungsbestimmungen für die Nutzung des Vertrauensdienstes von Swisscom ITSF mit digitalen Zertifikaten für fortgeschrittene oder qualifizierte elektronische Siegel für juristische Personen (Swisscom ITSF Zertifikatsklasse "Saphir" bzw. "Diamant")

1 Geltungsbereich dieser Nutzungsbestimmungen

Diese Nutzungsbestimmungen gelten im Verhältnis zwischen dem Kunden (Juristische Personen, nachfolgend "Siegelersteller" genannt) und Swisscom IT Services Finance S.E., PKI Dienstleistungen, Mariahilfer Strasse 123/3, 1060 Wien, Österreich, Firmennummer 378965b (nachfolgend "Swisscom ITSF" genannt), für die Nutzung des Vertrauensdienstes von Swisscom ITSF mit digitalen Zertifikaten für fortgeschrittene oder qualifizierte elektronische Siegel.

Ob für den Siegelersteller die nachfolgenden Bestimmungen zu dem fortgeschrittenen elektronischen Siegel oder zu den qualifizierten elektronischen Siegeln massgeblich sind, richtet sich nach seiner Bestellung im Antragsformular, in dem er bestimmt, für welche Siegelart er ein digitales Zertifikat bei Swisscom ITSF beantragt.

2 Leistungen von Swisscom ITSF

2.1 Vertrauensdienst allgemein

Für die Ausstellung digitaler Zertifikate für fortgeschrittene und qualifizierte elektronische Siegel ist Swisscom ITSF in Österreich anerkannte Anbieterin von fortgeschrittenen und qualifizierten Vertrauensdiensten gemäss der EU-Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO) und dem österreichischen Signatur- und Vertrauensdienstegesetz (SVG) und wird von einer Bestätigungsstelle geprüft und von der SVG-Aufsichtsstelle beaufsichtigt.

Der Vertrauensdienst wird nach den jeweils aktuellen Zertfikatsrichtlinien von Swisscom ITSF erbracht. Diese Zertifikatsrichtlinien ("Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten)") bilden Bestandteil der vorliegenden Nutzungsbestimmungen. Das Dokument kann der Siegelersteller im Internet unter https://trustservices.swisscom.com/repository (im Bereich "EU") einsehen und herunterladen.

Im Rahmen des Vertrauensdienstes erstellt Swisscom ITSF ein digitales Zertifikat, das unter anderem Angaben zum Siegelersteller enthält. Swisscom ITSF verknüpft dieses Zertifikat mit derjenigen Datei, die der Siegelersteller, handelnd durch seine Mitarbeiter oder sonstige Vertreter, mit einem elektronischen Siegel versehen will (z.B. Rechnung im Format PDF). Damit wird das elektronische Siegel auf dem Dokument dem Siegelersteller zugeordnet. Dadurch können auch Dritte auf das elektronische Siegel und die im Zertifikat enthaltenen Angaben vertrauen.

Je nach Bestellung im Antragsformular, wird jeweils ein fortgeschrittenes elektronisches Siegel nach Artikel 3 Ziffer 26 eIDAS-VO oder ein qualifiziertes elektronisches Siegel nach Artikel 3 Ziffer 27 eIDAS-VO erstellt. Eine andere Nutzungsart des digitalen Zertifikats ist im Rahmen der Nutzung des Vertrauensdienstes gemäss den vorliegenden Nutzungsbestimmungen unzulässig ("Nutzungsbeschränkung").

2.2 Identifikationsprozess und Aufbewahrung der Angaben

Swisscom ITSF oder die von Swisscom ITSF beauftragte Registrierungsstelle prüft im Identifikationsprozess Angaben zum Siegelersteller und die Identität seiner Vertreter (z.B. Mitarbeiter) anhand von Dokumenten und Angaben, die Swisscom ITSF oder die von Swisscom ITSF beauftragte Registrierungsstelle vom Siegelersteller verlangt (Kundendaten). Die Prüfung der Kundendaten kann auf verschiedene Arten und unter Vorlage unterschiedlicher Dokumente (z.B. Identitätskarte, Auszug aus dem Firmenbuch) erfolgen und richtet sich nach der konkreten Ausgestaltung des Identifikationsprozesses durch Swisscom ITSF oder der von ihr beauftragten Registrierungsstelle.

Swisscom ITSF registriert und hinterlegt die im Identifikationsprozess erhobenen Kundendaten gemäss den geltenden Vorschriften. Der Umgang mit den Kundendaten ist in Ziffer 7 dieser Nutzungsbestimmungen beschrieben.

2.3 Ausstellen von Zertifikat und Schlüssel, Siegelerstellung

Swisscom ITSF erstellt das digitale Zertifikat und das kryptographische Schlüsselpaar für den Siegelerstellungsvorgang auf einem speziellen Server in einer sicheren Signaturerstellungseinheit (Hardware Security Module). Das digitale Zertifikat ist eine Bescheinigung, die den öffentlichen Schlüssel des asymmetrischen kryptografischen Schlüsselpaars dem Siegelersteller zuordnet. Nur der Siegelersteller verfügt via seinem SSL/TLS geschützten Zugang über die Möglichkeit, elektronische Siegel über diesen Weg erstellen zu lassen (vgl. hierzu auch Ziffern 3 und 4 dieser Nutzungsbestimmungen).

Das digitale Zertifikat hat eine Gültigkeitsdauer von maximal 3 Jahren.

2.4 Prüfung des elektronischen Siegels

Der Vertrauensdienst von Swisscom ITSF ermöglicht die Validierung der Gültigkeit des elektronischen Siegels. Auch Dritte (oft "relying party" genannt) können die Gültigkeit des elektronischen Siegels validieren, z.B. für qualifizierte elektronische Siegel auf der Internetseite www.signatur.rtr.at/de/vd/Pruefung.html. Zu den Rechtswirkungen des elektronischen Siegels sind die Ausführungen in Ziffer 5 dieser Nutzungsbestimmungen zu beachten.

2.5 Verfügbarkeit

Swisscom ITSF ist bemüht, den Vertrauensdienst ohne Unterbrechungen zur Verfügung zu stellen. Allerdings übernimmt Swisscom ITSF keine Haftung für die ständige Verfügbarkeit des Signing Services. Swisscom ITSF kann die Verfügbarkeit vorübergehend beschränken, wenn dies zum Beispiel im Hinblick auf Kapazitätsgrenzen, die Sicherheit oder Integrität der Server oder zur Durchführung technischer Wartungs- oder Instandsetzungsmassnahmen erforderlich ist und dies der ordnungsgemässen oder verbesserten Erbringung der Leistungen dient (Wartungsarbeiten). Swisscom ITSF bemüht sich hierbei um Berücksichtigung der Interessen der Nutzer des Vertrauensdienstes.

3 Nutzungsvoraussetzungen

Der Siegelersteller hat ein angemessenes Verständnis von digitalen Zertifikaten und elektronischen Siegeln.

Mit Zugangszertifikaten authentisiert der Siegelersteller eine Applikation (nachfolgend "Teilnehmerapplikation" genannt) gegenüber Swisscom ITSF, die er selbst betreibt oder durch einen Dritten betreiben lässt, und die die Nutzung des Vertrauensdienstes von Swisscom ITSF ermöglicht. Die Teilnehmerapplikation kann zum Beispiel die Buchhaltungssoftware des Siegelerstellers oder das Internetportal eines Dritten sein. Wer die Teilnehmerapplikation betreibt und deren Anbindung zum Vertrauensdienst von Swisscom ITSF sicherstellt, ist der sogenannte Teilnehmer. Die Anbindung der Teilnehmerapplikation an den Vertrauensdienst von Swisscom ITSF ist Gegenstand eines eigenen Vertrags mit dem Teilnehmer (nachfolgend "All-in Signing Service Vertrag" genannt): Falls der Siegelersteller selbst auch der Teilnehmer ist, schliesst er selbst einen All-in Signing Service Vertrag ab. Falls der Siegelersteller nicht selbst Teilnehmer ist, setzt die Nutzung des Vertrauensdienstes gemäss den vorliegenden Nutzungsbestimmungen einerseits den Bestand eines All-in Signing Service Vertrags des Teilnehmers und andererseits eine Berechtigung des Teilnehmers durch den Siegelersteller zur Anbindung der Teilnehmerapplikation voraus.

Aus den Bestimmungen der vom Siegelerstellers verwendeten Teilnehmerapplikation können sich Einschränkungen in der Nutzung des Vertrauensdienstes ergeben.

4 Mitwirkungspflichten des Siegelerstellers

Der Siegelersteller übermittelt das von ihm ausgefüllte Antragsformular elektronisch und qualifiziert elektronisch unterschrieben an Swisscom ITSF. Darin bestätigt der Siegelersteller auch die Annahme der vorliegenden Nutzungsbestimmungen. Falls der Siegelersteller und der Teilnehmer identisch sind, übermittelt er ebenfalls die unterzeichnete Konfigurations- und Annahmeerklärung an Swisscom ITSF.

Ist der Siegelersteller nicht selbst Teilnehmer, wird die Konfigurations- und Annahmeerklärung durch den Teilnehmer ausgefüllt, unterschrieben und an Swisscom ITSF übergeben.

Der Siegelersteller hat die Teilnehmerapplikation gegenüber Swisscom ITSF zu authentisieren:

- Falls Siegelersteller und Teilnehmer identisch sind, stellt der Siegelersteller das Zugangszertifikat für fortgeschrittene Siegel Swisscom ITSF elektronisch zu (z.B. per E-Mail).

- Falls Siegelersteller und Teilnehmer nicht identisch sind, autorisiert der Siegelersteller den Teilnehmer gegenüber Swisscom ITSF durch eine entsprechende Erklärung. Damit erklärt sich der Siegelersteller auch einverstanden, dass das Zugangszertifikat mit der Teilnehmerapplikation des Teilnehmers von Swisscom ITSF verwendet werden darf.

- Falls qualifizierte elektronische Siegel erstellt werden sollen, erstellt der Siegelersteller den privaten Schlüssel zum Zugangszertifikat auf einem HSM (Minimumstandard FIPS 140 Level 2) oder einer durch Swisscom zugelassenen technischen Lösung zur Aufbewahrung und übergibt das Zugangszertifikat an-schliessend. Sofern kein von Swisscom zugelassener technischer Prozess zur Erstellung vorgesehen ist, findet die Erstellung in einer gemeinsamen Zeremonie mit der Swisscom Registrierungs-stelle statt. Der Siegelersteller muss dann fortwährend sicherstellen, dass die Aufbewahrungslösung oder das HSM mit dem privaten Schlüssel durch die Teilnehmerapplikation erreichbar ist.

Sobald die Teilnehmerapplikation mittels Zugangszertifikaten mit dem Vertrauensdienst von Swisscom ITSF verbunden ist, gibt es pro Siegelerstellungsvorgang keine zusätzliche Einzelauthentisierung, d.h. alle über diese Schnittstelle übertragenen Dokumentenkomprimate (Hash) werden, je nach Bestellung im Antragsformular, mit einem fortgeschrittenen oder qualifizierten elektronischen Siegel versehen. Der Siegelersteller stellt daher sicher, dass die Personen, denen er über die Teilnehmerapplikation Zugriff zum Vertrauensdienst gemäss den vorliegenden Nutzungsbestimmungen gewährt, vorgängig auf die folgenden Punkte aufmerksam gemacht werden:

- Funktionsweise des Vertrauensdienstes,
- Nutzungsvoraussetzungen gemäss Ziffer 3,
- Mitwirkungspflichten gemäss dieser Ziffer 4,
- Rechtswirkungen gemäss Ziffer 5.

In jedem Fall hat der Siegelersteller für das Verhalten dieser Personen im Zusammenhang mit der Nutzung des Vertrauensdienstes gemäss diesen Nutzungsbestimmungen einzustehen, als ob es sein eigenes wäre.

Der Siegelersteller verpflichtet sich und seine Vertreter, im Rahmen des Identifikationsprozesses gegenüber Swisscom ITSF bzw. der Registrierungsstelle vollständige und wahre Angaben zu machen.

Allfällige Aufzeichnungen des Passwortes zur Aufbewahrung des privaten Schlüssels oder des privaten Schlüssels des Zugangszertifikates für die Authentisierung gegenüber den Servern des Vertrauensdienstes von Swisscom ITSF dürfen keiner unbefugten Person

bekannt gemacht werden, sind sicher aufzubewahren und vor Zugriffen unberechtigter Dritter zu schützen.

Der Siegelersteller verpflichtet sich, das auf ihn ausgestellte digitale Zertifikat unverzüglich für ungültig erklären zu lassen, wenn sein Passwort Unbefugten offengelegt wurde, der private Schlüssel des Zugangszertifikates kompromittiert wurde oder wenn der Siegelersteller weiss oder vermutet, dass eine unbefugte Person von Passwort zur Aufbewahrung des privaten Schlüssels oder vom privaten Schlüssel Kenntnis erlangt hat (Kompromittierung). Die Ungültigkeitserklärung kann bei der Registrierungsstelle oder bei Swisscom ITSF gemäss den Verfahren in den Zertifikatsrichtlinien in Auftrag gegeben werden.

Der Siegelersteller verpflichtet sich, alle Änderungen in seinem Namen bzw. in seiner Firma sofort Swisscom ITSF anzuzeigen und niemals Zertifikate mit nicht korrekten Kundendaten im Sinne von Ziffer 2.2 dieser Nutzungsbestimmungen zu verwenden.

Der Siegelersteller verpflichtet sich, alle zumutbaren und zeitgemässen Möglichkeiten zu nutzen, seine an den Vertrauensdienst von Swisscom ITSF angebundene Infrastruktur gegen Angriffe und Schadsoftware ("Viren", "Würmer", "Trojaner" und dergleichen) zu schützen, insbesondere durch Verwendung stets aktueller Software.

Der Siegelersteller verpflichtet sich, die elektronischen Siegel nach Erstellung gemäss Ziffer 2.4 dieser Nutzungsbestimmungen zu prüfen und allfällige Unstimmigkeiten im digitalen Zertifikat Swisscom ITSF rasch zu melden.

5 Rechtswirkungen des elektronischen Siegels

Die Verwendung des fortgeschrittenen oder qualifizierten elektronischen Siegels dient in der Regel dazu, den Herkunftsnachweis sowie die Integrität des Inhalts einer Datei zu gewährleisten. Das elektronische Siegel ist nicht mit dem rechtlichen Konzept der elektronischen Signatur zu verwechseln. Zudem sind die Rechtswirkungen des höherwertigen qualifizierten elektronischen Siegels nicht dieselben wie diejenigen des fortgeschrittenen elektronischen Siegels. Es obliegt dem Siegelersteller, die Rechtswirkungen der gewählten Art der elektronischen Siegel (mit und ohne Zeitstempel) im Voraus und nötigenfalls in Abstimmung mit dem Teilnehmer abzuklären. Swisscom übernimmt hierfür keine Verantwortung.

Qualifizierte elektronische Siegel (Zertifikat der Swisscom-Klasse Diamant): Das über den AIS erstellte qualifizierte elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 27 eIDAS-VO mit den Rechtswirkungen gemäss Art. 35 eIDAS-VO.

Fortgeschrittenes elektronisches Siegel (Zertifikat der Swisscom-Klasse Saphir): Das über den AIS erstellte fortgeschrittene elektronische Siegel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 26 eIDAS-VO mit der Rechtswirkung gemäss Art. 35 eIDAS-VO.

Einfacher elektronischer Zeitstempel: Der über den AIS erstellte einfache elektronische Zeitstempel erfüllt die in der CP/CPS definierten Eigenschaften und die Definition gemäss Art. 3 Ziff. 33 eIDAS-VO mit den Rechtswirkungen gemäss Art. 41 eIDAS-VO. Es handelt sich nicht um einen qualifizierten elektronischen Zeitstempel gemäss Art. 3 Ziff. 34 eIDAS-VO.

Die Rechtswirkungen des höherwertigen qualifizierten elektronischen Siegels sind nicht dieselben wie diejenigen des fortgeschrittenen elektronischen Siegels. Weiter haben weder das fortgeschrittene elektronische Siegel noch das qualifizierte elektronische Siegel die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift oder eine qualifizierte elektronische Signatur. Je nach Situation benötigen gewisse Dokumente also die handschriftliche Unterschrift, eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel ggfs. mit einem elektronischen Zeitstempel, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.

Über AIS gemäss den Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten ausgestellte elektronische Siegel von den Issuing CAs "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten) können bei Anwendbarkeit anderen Rechts als dem EU-Recht abweichende, allenfalls weitergehende oder weniger weitgehende Wirkungen entfalten als dies nach EU-Recht der Fall ist.

Der Austausch verschlüsselter Daten und die Ausstellung von Zertifikaten unterliegt zudem in/mit gewissen Staaten gesetzlichen Restriktionen.

Der Siegelersteller nimmt zur Kenntnis, dass er Dritten gegenüber für Schäden haften kann, die diese erleiden, weil sie sich auf ein gültiges digitales Zertifikat von Swisscom ITSF verlassen haben.

Die Verwendung gewisser technischer Algorithmen unterliegt zudem in gewissen Staaten gesetzlichen Restriktionen. Es obliegt dem Siegelersteller, die diesbezüglichen Gegebenheiten vorgängig abzuklären.

6 Nutzungsdauer

Der Siegelersteller kann den Vertrauensdienst gemäss den vorliegenden Nutzungsbestimmungen während der Dauer des All-in Signing Service Vertrags mit Swisscom ITSF nutzen, vorausgesetzt, dass ein gültiges Zertifikat vorliegt, die darin enthaltenen Angaben unverändert sind und der Siegelersteller die vorliegenden Nutzungsbedingungen einhält.

7 Umgang mit Daten des Siegelerstellers

7.1 Allgemein

Swisscom ITSF erhebt, speichert und bearbeitet nur Daten, die für die Erbringung des Vertrauensdienstes benötigt werden. Der Umgang mit den Daten richtet sich neben der den anwendbaren Gesetzen auch nach den in Ziffer 2.1 erwähnten Zertifikatsrichtlinien.

Swisscom ITSF zieht für die Erbringung der Vertrauensdienste Swisscom (Schweiz) AG mit Sitz in der Schweiz bei. Swisscom (Schweiz) AG betreibt die IT-Systeme zur Erbringung der Vertrauensdienste und diese Systeme stehen in der Schweiz. Die fortgeschrittenen oder qualifizierten Zertifikate werden somit auf Servern in der Schweiz ausgestellt. Es handelt sich deshalb um Auftragsdatenbearbeitung in der Schweiz durch Swisscom (Schweiz) AG, die im Auftrag von

Swisscom ITSF erfolgt. Swisscom ITSF hat die hierfür erforderlichen datenschutzrechtlichen Vereinbarungen mit Swisscom (Schweiz) AG abgeschlossen.

Mit der Annahme der Nutzungsbestimmungen akzeptiert der Siegelersteller ausdrücklich die Aufnahme und Verarbeitung der von ihm erhobenen Kundendaten wie in dieser Ziffer beschrieben.

7.2 Identifikationsdokumentation

Zum Zweck der Erstellung des digitalen Zertifikats, zur Aufrechterhaltung der Nachvollziehbarkeit des Vertrauensdienstes und für die allfällige Revokation von Zertifikaten erfasst und speichert Swisscom ITSF folgende Daten:

Vom Antragsteller im Identifikationsprozess gemäss Ziffer 2.2 dieser Nutzungsbestimmungen gelieferte Angaben und Dokumente, z. B. Handelsregisterauszug, Auszug aus dem Unternehmensregister, Vollmachten oder sonstige Belege betreffend spezifische Attribute.

Mobiltelefonnummer des Antragstellers für die Authentisierung bei einer allfälligen Revokation.

Vom Vertreter des Siegelerstellers, der bei Swisscom ITSF den Antrag auf Ausstellen des digitalen Zertifikats stellt: Kopie der relevanten Seiten des Lichtbildausweises mit den darin enthaltenen Informationen (insbesondere Geschlecht, Vornamen, Familienname, Geburtsdatum, Gültigkeitsdatum des Ausweisdokuments, Nationalität).

7.3 Digitales Zertifikat

Gestützt auf die Daten, die im Identifikationsprozess vom Siegelersteller angegeben und erhoben wurden, stellt Swisscom ITSF ein digitales Zertifikat aus, welches über den Siegelersteller folgende Angaben enthält:

- Formaler Name bzw. Firma (gemäss Organisationsnachweis)
- Firmenbuchnummer bzw. Handelsregisternummer oder sonstige Registernummer
- Zweistelliger ISO 3166 Ländercode
- Ausstellungszeitpunkt des Zertifikats, Siegelerstellungszeitpunkt

Das digitale Zertifikat ist nach Abschluss des Siegelerstellungsvorgangs in der Datei, die mit einem fortgeschrittenen oder qualifizierten elektronischen Siegel versehen wurde, enthalten. Wer im Besitz dieser Datei ist, kann die oben aufgeführten Angaben aus dem Zertifikat jederzeit einsehen. Damit können Dritte die Angaben zum Siegelersteller überprüfen und auch sehen, dass Swisscom ITSF als Vertrauensdiensteanbieterin hinter der Zertifizierung dieser Daten und des Siegelerstellungsvorgangs steht.

7.4 Daten nach Abschluss des Siegelerstellungsvorgangs

Swisscom ITSF behält die in Ziffer 7.2 beschriebenen Daten während der Nutzungsdauer gemäss Ziffer 6 dieser Nutzungsbestimmungen auf, damit der Siegelersteller den Vertrauensdienst nutzen kann. Weiter behält Swisscom ITSF verschiedene Daten zum Identifikationsprozess, zum digitalen Zertifikat und zum Siegelerstellungsvorgang während 7 Jahren (fortgeschritten) resp. 30 Jahren (qualifiziert) ab dem letzten Siegelerstellungsvorgang auf. Damit wird sichergestellt, dass die Nachvollziehbarkeit der Korrektheit des mit einem elektronischen Siegel versehenen Dokuments in den Jahren nach deren Erstellung aufrechterhalten werden kann. Swisscom ITSF zeichnet hierbei alle einschlägigen Informationen über die von Swisscom ITSF ausgegebenen und empfangenen Daten auf und bewahrt diese so auf, dass sie verfügbar sind, um insbesondere bei Gerichtsverfahren entsprechende Beweise liefern zu können und um die Kontinuität des Vertrauensdienstes sicherzustellen.

Einerseits behält Swisscom ITSF hierfür folgende Daten auf:

- Logdateien zum Siegelerstellungsvorgang (enthält insbesondere die Zugangsidentifikation, Vorgangsnummer, ablaufbezogene Daten)
- Hashwert des Dokuments, auf welchem ein elektronisches Siegel angebracht wurde

Andererseits behält Swisscom ITSF die Angaben gemäss Ziffer 7.2 dieser Nutzungsbestimmungen auf und führt eine Zertifikatsdatenbank.

Swisscom ITSF löscht die in dieser Ziffer 7.4 beschriebenen Daten nach Ablauf von höchstens 7 Jahren (fortgeschritten) resp. 30 Jahren (qualifiziert) nach Ablauf des digitalen Zertifikats.

Bei Aufgabe der Geschäftstätigkeit einer externen Registrierungsstelle werden die dort aufbewahrten Daten an Swisscom ITSF transferiert.

8 Beizug Dritter durch Swisscom

Swisscom ITSF darf zur Erfüllung ihrer Pflichten Dritte beiziehen. Insbesondere wird Swisscom (Schweiz) AG in der Schweiz für den Betrieb der IT-Systeme zur Erbringung der Vertrauensdienste beigezogen. Dritte können von Swisscom ITSF auch zur Durchführung des Identifikationsprozesses (inklusive Aufbewahrung der Identifikationsdokumentation) beauftragt werden (Registrierungsstellen).

9 Haftung und höhere Gewalt

Swisscom ITSF hat stets die Anforderungen, die das Gesetz und die technischen Standards an die Anbieterinnen von Vertrauensdiensten stellt, zu erfüllen. Hierfür setzt Swisscom ITSF angemessene und dem aktuellen Stand der Technik entsprechende Sicherheitsmassnahmen ein. Der Siegelersteller nimmt zur Kenntnis, dass trotz aller Anstrengungen von Swisscom ITSF, des Einsatzes moderner Technik und Sicherheitsstandards sowie der Kontrolle durch die Anerkennungsstelle betreffend die Einhaltung der gesetzlichen Vorschriften eine absolute Sicherheit und Fehlerlosigkeit des Vertrauensdienstes nicht gewährleistet werden kann.

Sofern Swisscom ITSF nicht beweist, dass sie kein Verschulden trifft, haftet sie dem Siegelersteller gegenüber unbeschränkt für Schäden, die dieser erleidet, weil Swisscom ITSF den Pflichten aus der eIDAS-VO nicht nachgekommen ist.

Sofern Swisscom ITSF nicht beweist, dass sie kein Verschulden trifft, haftet Swisscom ITSF bei anderen Vertragsverletzungen dem Siegelersteller gegenüber für den nachgewiesenen Schaden wie folgt:

Falls der Siegelersteller mit dem Teilnehmer identisch ist und der Teilnehmer einen All-in Signing Vertrag direkt mit Swisscom hat, richtet sich die Haftung nach den Bestimmungen dieses All-in Signing Vertrags.

Für alle anderen Konstellationen (z.B. Siegelersteller ist mit Teilnehmer nicht identisch oder der All-in Signing Vertrag des Teilnehmers wurde nicht mit Swisscom, sondern mit einem Partner von Swisscom abgeschlossen) gilt:

Die Haftung für Sach- und Vermögenschäden infolge leichter Fahrlässigkeit ist für die gesamte Vertragsdauer auf höchstens EUR 5'000 beschränkt. Die Haftung von Swisscom ITSF für leichte fahrlässig verursachte indirekte Schäden, Folgeschäden, entgangenen Gewinn, Datenverluste, Schäden infolge Downloads, Ansprüche Dritter und Reputationsverluste ist ausgeschlossen. Swisscom ITSF haftet dem Siegelersteller gegenüber für Personenschäden immer unbeschränkt. Swisscom ITSF haftet dem Siegelersteller gegenüber nicht für das ordentliche Funktionieren von Systemen Dritter, insbesondere nicht für die vom Siegelersteller verwendete Hard- und Software oder für die vom Siegelersteller für das Ansteuern des Vertrauensdienstes verwendete Teilnehmerapplikation.

In keinem Fall haftet Swisscom ITSF dem Siegelersteller gegenüber für Schäden, die sich aus der Nichtbeachtung oder Überschreitung einer Nutzungsbeschränkung durch den Siegelersteller ergeben. Swisscom ITSF haftet dem Siegelersteller gegenüber ebenfalls nicht, wenn die Erbringung der Leistung auf Grund höherer Gewalt zeitweise unterbrochen, ganz oder teilweise beschränkt oder unmöglich ist. Als höhere Gewalt gelten insbesondere Naturereignisse von besonderer Intensität (Lawinen, Überschwemmungen, Erdrutsche usw.), kriegerische Ereignisse, Aufruhr, unvorhersehbare behördliche Restriktionen. Kann Swisscom ITSF ihren vertraglichen Verpflichtungen nicht nachkommen, wird die Vertragserfüllung oder der Termin für die Vertragserfüllung dem eingetretenen Ereignis entsprechend hinausgeschoben. Swisscom ITSF haftet nicht für allfällige Schäden, die dem Siegelersteller durch das Hinausschieben der Vertragserfüllung entstehen.

10 Änderungen der Nutzungsbestimmungen

Swisscom ITSF behält sich das Recht vor, diese Bedingungen zu ändern und zu ergänzen. Insbesondere bei Änderungen der eIDAS-VO oder des österreichischen Signatur- und Vertrauensdienstegesetzes oder der auf seiner Grundlage erlassenen Verordnungen sowie bei Anordnungen der Bestätigungsstelle oder der Aufsichtsstelle kann Swisscom ITSF gezwungen sein, die in Ziffer 2.1 dieser Nutzungsbestimmungen erwähnten Zertifikatsrichtlinien und die vorliegenden Nutzungsbestimmungen anzupassen. Der Siegelersteller wird bei Änderungen zumindest ein Monat vor Geltungsbeginn von Swisscom ITSF oder von einer von ihr beauftragten Registrierungsstelle über die Änderungen und die ihm zustehende Widerspruchsfrist informiert. Diese Information kann über SMS an die vom Siegelersteller hinterlegte Mobilfunknummer oder per E-Mail erfolgen. Der Siegelersteller kann die Annahme der neuen Bedingungen ablehnen, indem er auf die Nutzung des Vertrauensdienstes gemäss diesen Nutzungsbestimmungen ab dem Geltungsbeginn verzichtet. Nutzt der Siegelersteller den Vertrauensdienst ab ihrem Geltungsbeginn weiter, gilt dies als Annahme der geänderten Bedingungen.

11 Anwendbares Recht und Gerichtsstand

Alle Rechtsbeziehungen im Zusammenhang mit diesen Nutzungsbestimmungen unterstehen dem österreichischen Recht.

Im Konfliktfall bemühen sich die Parteien um eine einvernehmliche Streitbeilegung. Unter Vorbehalt zwingender Gerichtsstände ist der Gerichtsstand in Wien, Österreich.

12 Wie Sie uns erreichen können

Bei Fragen bezüglich der Leistungserbringung gemäss den vorliegenden Nutzungsbestimmungen kann der Siegelersteller Swisscom ITSF über die folgende Internetseite kontaktieren:
https://trustservices.swisscom.com.