

Nutzungsbestimmungen Zertifizierungsdienst Swisscom (Qualifizierte und fortgeschrittene elektronische Signaturen)

Nutzungsbestimmungen für die Nutzung des Zertifizierungsdienstes von Swisscom mit qualifizierten und fortgeschrittenen Zertifikaten für qualifizierte und fortgeschrittene elektronische Signaturen (Swisscom Zertifikatsklasse "Saphir und Diamant")

1 Geltungsbereich dieser Nutzungsbestimmungen

Diese Nutzungsbestimmungen gelten im Verhältnis zwischen Ihnen und Swisscom (Schweiz) AG, Alte Tiefenaustrasse 6, Worblaufen, Schweiz, Firmennummer CHE-101.654.423 (nachfolgend "Swisscom" genannt), für Ihre Nutzung des Zertifizierungsdienstes von Swisscom mit qualifizierten und fortgeschrittenen Zertifikaten für qualifizierte und fortgeschrittene elektronische Signaturen.

2 Leistungen von Swisscom

2.1 Zertifizierungsdienst allgemein

Für ihre Zertifizierungsdienste mit qualifizierten Zertifikaten ist Swisscom in der Schweiz anerkannte Anbieterin von Zertifizierungsdiensten gemäss schweizerischem Bundesgesetz über die elektronische Signatur (ZertES; SR 943.03) und wird von der ZertES-Anerkennungsstelle geprüft und beaufsichtigt. Für ihre Zertifizierungsdienste mit fortgeschrittenen Zertifikaten ist Swisscom Anbieterin von Zertifizierungsdiensten, die gemäss international anerkannten technischen Standards erbracht werden.

Allgemein wird der Zertifizierungsdienst nach den jeweils aktuellen Zertifikatsrichtlinien von Swisscom erbracht. Diese Zertifikatsrichtlinien - Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten der Klasse "Diamant" (qualifiziert) und „Saphir“ (fortgeschritten) - bilden Bestandteil der vorliegenden Nutzungsbestimmungen. Das Dokument können Sie im Internet unter

https://www.swisscom.ch/de/business/enterprise/angebot/security/digital_certificate_service.html

(im Bereich "CH") einsehen und herunterladen.

Im Rahmen des Zertifizierungsdienstes erstellt Swisscom ein digitales Zertifikat, das unter anderem Angaben zu Ihrer Person enthält. Je nach Teilnehmerapplikation wird unterschieden zwischen Zertifikaten mit Klarnamen oder Zertifikaten mit Pseudonym (siehe dazu Ziffer 7.3). Swisscom verknüpft dieses digitale Zertifikat mit derjenigen Datei, die Sie elektronisch signieren (z.B. PDF-Dokument Ihrer Bank). Damit wird die elektronische Signatur auf dem Dokument Ihrer Person zugeordnet, ähnlich wie bei der eigenhändigen Unterschrift, wo der Namensschriftzug auf dem Dokument der unterzeichnenden Person zugeordnet wird. Dadurch können auch Dritte auf die elektronische Signatur und die im digitalen Zertifikat enthaltenen Angaben vertrauen.

Je nach der von der Teilnehmerapplikation (siehe dazu Ziffer 3) angebotenen Signaturart wird jeweils entweder eine qualifizierte elektronische Signatur gemäss Artikel 2 Buchstabe e des schweizerischen Bundesgesetzes über die elektronische Signatur (ZertES; SR 943.03) oder eine fortgeschrittene Signatur erstellt. Eine andere Nutzungsart des qualifizierten Zertifikats ist im Rahmen der Nutzung des Zertifizierungsdienstes gemäss den vorliegenden Nutzungsbestimmungen unzulässig ("Nutzungsbeschränkung").

2.2 Identifikationsprozess und Aufbewahrung der Angaben

Swisscom oder die von Swisscom beauftragte Registrierungsstelle prüft im Identifikationsprozess Ihre Identität. Für qualifizierte elektronische Signaturen erfolgt dies anhand Ihres Passes oder einer für die Einreise in die Schweiz anerkannten Identitätskarte oder anhand eines zertifizierten, gleichwertigen Prozesses, in welchem auf die persönliche Anwesenheit verzichtet werden kann.

Jeweils abhängig von der konkreten Ausgestaltung des Identifikationsprozesses, können Sie im Identifikationsprozess für fortgeschrittene elektronische Signaturen aufgefordert werden, auch andere Dokumente vorzulegen als bei der qualifizierten elektronischen Signatur.

Auf der Basis Ihres Identifikationsprozesses für qualifizierte elektronische Signaturen können Sie auch fortgeschrittene elektronische Signaturen gemäss diesen Nutzungsbestimmungen erstellen, sofern die von Ihnen verwendete Teilnehmerapplikation verschiedene Signaturarten anbietet. Hingegen kann nicht jeder Identifikationsprozess für fortgeschrittene elektronische Signaturen auch für das höherwertige Signaturniveau der qualifizierten elektronischen Signatur verwendet werden.

Swisscom registriert und hinterlegt die im Identifikationsprozess zu Ihrer Person erhobenen Angaben gemäss den geltenden Vorschriften. Der Umgang mit Ihren Daten ist in Ziffer 6 dieser Nutzungsbestimmungen beschrieben.

Weiter betreibt Swisscom einen Verzeichnisdienst, der öffentlich zugänglich ist. Der Verzeichnisdienst ermöglicht es, den Identifikationsstatus einer Person zu prüfen, damit eine bereits identifizierte und registrierte Person den Identifikationsprozess nicht noch einmal durchlaufen muss. Dabei werden nach Angabe der entsprechenden Mobiltelefonnummer folgende Daten überprüft und angezeigt: identifiziert für FES oder QES, Berechtigung Signaturen nach Schweizer und/ oder EU-Recht zu erstellen, bestätigte Mobiltelefonnummer, Swisscom interne Seriennummer der Identifikation und Hinweis, falls die Signaturerlaubnis in Kürze abläuft (Datum).

2.3 Ausstellen Zertifikat und Schlüssel, Signaturerstellung

Swisscom erstellt das fortgeschrittene oder qualifizierte Zertifikat und das kryptographische Schlüssel-paar für den Signaturvorgang auf einem speziellen Server (Hardware Security Module, HSM). Das fortgeschrittene oder qualifizierte Zertifikat ist eine Bescheinigung, die den öffentlichen Schlüssel des asymmetrischen kryptografischen Schlüsselpaars Ihnen zuordnet. Nur Sie verfügen über die Aktivierungsdaten, mit welchen Sie den privaten Schlüssel unter Einsatz einer mit Ihrer Identität verbundenen Authentisierungsmethode verwenden können (z.B. Mobile ID, oder eine zugelassene App wie z.B. die Mobile ID App oder SMS-Authentisierungsverfahren, vgl. hierzu auch Ziffern 3 und 4 dieser Nutzungsbestimmungen). Sobald Sie nach entsprechender Aufforderung die Aktivierungsdaten eingeben, erstellt Swisscom für Sie die fortgeschrittene oder qualifizierte elektronische Signatur.

Swisscom erstellt für jeden Signaturvorgang ein neues digitales Zertifikat (mit einer kurzen Gültigkeitsdauer von 10 Minuten) mit einem neuen Schlüsselpaar.

2.4 Prüfung der elektronischen Signatur

Der Zertifizierungsdienst von Swisscom ermöglicht die Validierung der Gültigkeit der elektronischen Signatur. Auch Dritte (oft "relying party" genannt) können die Gültigkeit Ihrer elektronischen Signatur validieren (z.B. für qualifizierte elektronische Signaturen auf der Internetseite www.validator.ch). Zu den Rechtswirkungen der verschiedenen elektronischen Signaturen sind die Ausführungen in Ziffer 5 dieser Nutzungsbestimmungen zu beachten.

2.5 Verfügbarkeit

Swisscom ist bemüht, den Zertifizierungsdienst ohne Unterbrechungen zur Verfügung zu stellen. Allerdings übernimmt Swisscom keine Haftung für die ständige Verfügbarkeit des Signing Services, auch nicht für Verzögerungen oder Blockaden des Netzwerksystems, Verfügbarkeit von Mobildiensten und Internetverbindungen. Swisscom 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 bemüht sich hierbei um Berücksichtigung der Interessen der Nutzer des Zertifizierungsdienstes. Den aktuellen Status zur Verfügbarkeit des Dienstes finden Sie unter:

<https://trustservices.swisscom.com/service-status/>

3 Nutzungsvoraussetzungen

Sie haben ein angemessenes Verständnis von digitalen Zertifikaten sowie von qualifizierten und fortgeschrittenen elektronischen Signaturen.

Sie nutzen ein Endgerät und melden sich bei einem Internetportal oder einer Applikation an, welche die Nutzung des Zertifizierungsdienstes von Swisscom ermöglichen (sogenannte "Teilnehmerapplikation"). Es kann sich zum Beispiel um die Buchhaltungssoftware Ihres Arbeitgebers oder um das Internetportal Ihrer

Bank oder Versicherung handeln. Aus den Bestimmungen der von Ihnen verwendeten Teilnehmerapplikation können sich Einschränkungen in der Nutzung des Zertifizierungsdienstes ergeben. Insbesondere bestimmt die von Ihnen verwendete Teilnehmerapplikation, ob Sie fortgeschrittene oder qualifizierte elektronische Signaturen erstellen können. Sie legt ebenfalls fest, ob Sie einen einmaligen Identifikationsprozess für jede elektronische Signatur durchlaufen (Einmalsignatur), oder ob Sie nach dem Identifikationsprozess während einer bestimmten Dauer mehrere elektronische Signaturen erstellen können. Die Anbindung der Teilnehmerapplikation an den Zertifizierungsdienst von Swisscom ist Gegenstand eines eigenen Vertrags.

Sie verfügen über ein für die Willensbekundung für die elektronische Signatur zugelassenes Authentisierungsmittel (z.B. ein Mobiltelefon). Dafür kommen eine Passwort-SMS-Authentifizierung, eine zugelassene App, wie z.B. die Mobile ID App oder andere anerkannte Signaturfreigabemethoden in Frage. Die konkrete Signaturfreigabe ergibt sich aus der Anbindung der von Ihnen verwendeten Teilnehmerapplikation.

Falls die Signaturfreigabe per Mobile ID erfolgt, müssen Sie für die Nutzung des Zertifizierungsdienstes über eine Mobile ID bei einem Schweizer Mobile ID Provider (z.B. Swisscom) oder die Mobile ID App verwenden, die zuvor mit Ihrer Mobiltelefonnummer initialisiert wurde, verfügen.

4 Ihre Mitwirkungspflichten

Sie verpflichten sich, im Rahmen des Identifikationsprozesses gegenüber Swisscom bzw. der Registrierungsstelle vollständige und wahre Angaben zu machen.

Sie verpflichten sich, bei der Verwendung von Passwörtern, sofern im Rahmen der Erstellung der elektronischen Signatur vorgesehen, keine Daten zu verwenden, die sich auf Daten zu Ihrer Person beziehen (Geburts-tag und dergleichen). Allfällige Aufzeichnungen von PIN bzw. des persönlichen Passwortes im Rahmen der Authentifizierung dürfen keiner anderen Person bekannt gemacht werden und sind sicher und getrennt von Ihrem Authentifizierungsmittel (z.B. Mobiltelefon) aufzubewahren oder zu verschlüsseln und vor Zugriffen Dritter zu schützen.

Sofern Sie das Authentisierungsverfahren Passwort in Kombination mit einem von Swisscom per SMS übermittelten Einmalpasswort nutzen, vergewissern Sie sich, dass diese Eingabe der geforderten Daten immer auf Eingabefenstern des Swisscom Systems erfolgt. Näherer Hinweise hierzu können Sie [diesem Dokument](#) entnehmen.

Wenn z. B. Ihr Mobilgerät, die SIM-Karte bzw. das persönliche Passwort, das Sie im Authentisierungsverfahren angeben müssen, gestohlen wurde oder wenn Sie wissen oder vermuten, dass eine andere Person davon Kenntnis erlangt hat (Kompromittierung) sind Sie zu folgendem verpflichtet:

- Sie verzichten unverzüglich auf das Erstellen von Signaturen,
- Sie ändern gegebenenfalls die Zugangsdaten (z.B. in der Mobile ID Registrierungsseite,

der Mobile ID App oder Passwort) und sperren gegebenenfalls Ihre SIM-Karte.

Sobald es Änderungen an einem für die Authentisierung verwendeten Gerät (z.B. Ihrer Mobilfunknummer oder SIM-Karte) oder den Identitätsdaten gibt, informieren Sie Ihre Registrierungsstelle oder auch Swisscom direkt über diese Änderungen.

Sie verpflichten sich, alle zumutbaren und zeitgemässen Möglichkeiten zu nutzen, Ihr für die Authentisierung oder Signatur benötigtes Endgerät und Ihr Mobiltelefon gegen Angriffe und Schadsoftware ("Viren", "Würmer", "Trojaner" und dergleichen) zu schützen, insbesondere durch Verwendung stets aktueller Software aus offizieller Quelle.

Sie verpflichten sich, die elektronischen Signaturen nach Erstellung gemäss Ziffer 2.4 dieser Nutzungsbestimmungen zu prüfen und allfällige Unstimmigkeiten im digitalen Zertifikat Swisscom rasch zu melden.

5 Rechtswirkungen der elektronischen Signatur

Der Zertifizierungsdienst gemäss den vorliegenden Nutzungsbestimmungen erstellt jeweils entweder eine qualifizierte elektronische Signatur gemäss Artikel 2 Buchstabe e des schweizerischen Bundesgesetzes über die elektronische Signatur (ZertES; SR 943.03) oder eine fortgeschrittene elektronische Signatur gemäss den Zertifikatsrichtlinien von Swisscom.

Die von Ihnen für das Erreichen des Zertifizierungsdienstes genutzte Teilnehmerapplikation (vgl. hierzu Ziffer 3 dieser Nutzungsbestimmungen) bestimmt für jeden Signaturvorgang die Signaturart (qualifizierte oder fortgeschrittene elektronische Signatur). Swisscom hat auf diese Wahl keinen Einfluss.

Die von Ihnen genutzte Teilnehmerapplikation wird bei Swisscom einen qualifizierten Zeitstempel mit der qualifizierten oder fortgeschrittenen elektronischen Signatur verbinden lassen. Je nach Einstellung des Zugangs zum Zertifizierungsdienst von Swisscom wird also eine elektronische Signatur mit oder ohne qualifiziertem Zeitstempel erstellt. Bei der Prüfung der Signatur (vgl. hierzu Ziffer 2.4 dieser Nutzungsbestimmungen) können Sie prüfen, ob die elektronische Signatur mit einem qualifizierten Zeitstempel verbunden ist oder nicht.

Nur die mit einem qualifizierten Zeitstempel verbundene qualifizierte elektronische Signatur ist bei Anwendung von Schweizer Recht der eigenhändigen Unterschrift gleichgestellt, sofern keine abweichenden gesetzlichen oder vertraglichen Regelungen vorgehen (Artikel 14 Schweizer Obligationenrecht). Je nach Situation benötigen gewisse Dokumente die eigenhändige Unterschrift, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.

Eine fortgeschrittene elektronische Signatur ist (im Unterschied zur qualifizierten elektronischen Signatur) in der Schweiz nicht gesetzlich geregelt und genügt nicht dem rechtlichen Erfordernis der Schriftlichkeit im Sinne des Artikel 14 des Schweizer Obligationenrechts, sie hat also nicht die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift. Das rechtliche Erfordernis der handschriftlichen Unterschrift kann elektronisch grundsätzlich nur durch die qualifizierte

elektronische Signatur (in Verbindung mit einem qualifizierten Zeitstempel) gleichwertig ersetzt werden, die nicht mit der fortgeschrittenen elektronischen Signatur auf der Basis eines fortgeschrittenen Zertifikats gemäss den vorliegenden Nutzungsbestimmungen zu wechseln ist.

Es obliegt Ihnen, vor der Verwendung des Zertifizierungsdienstes Ihre Anforderungen und die Rechtswirkungen der qualifizierten elektronischen Signatur oder der fortgeschrittenen elektronischen Signatur in diesem Kontext abzuklären.

Sie nehmen zur Kenntnis, dass die mit dem schweizerischen Zertifizierungsdienst von Swisscom erstellten qualifizierten oder fortgeschrittenen elektronischen Signaturen bei Anwendbarkeit des Rechts eines anderen Landes als der Schweiz abweichende, allenfalls weniger weitgehende Wirkungen entfalten können und möglicherweise Formvorschriften (wie die Formvorschrift der Schriftlichkeit) nicht erfüllt werden können.

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

Die Aufnahme von Zusatzangaben in einem digitalen Zertifikat (spezifische Attribute wie z.B. Vertretungsberechtigung für Ihre Arbeitgeberin) erfolgt rein deklaratorisch, der Bestand eines Attributs und dessen Rechtswirkungen richten sich nach dem anwendbaren Recht (Stellvertretungsrecht, Gesellschaftsrecht usw.) und entzieht sich dem Einfluss- und Verantwortungsbereich von Swisscom. Swisscom übernimmt in diesem Zusammenhang nur Verantwortung für die Überprüfung des Nachweises eines Attributs im Zeitpunkt der Identitätsprüfung anhand der von Swisscom verlangten Nachweisen. Spezifische Attribute in den digitalen Zertifikaten geben nicht alle möglichen Situationen des Zivilrechts wieder (Kollektivzeichnungs-berechtigung, Zeichnungsberechtigung nur in Spezialfällen usw.).

6 Nutzungsdauer

Unter Berücksichtigung der Nutzungsvoraussetzungen gemäss Ziffer 3 dieser Nutzungsbestimmungen können Sie den Zertifizierungsdienst gemäss den vorliegenden Nutzungsbestimmungen mit einer während der Registrierung hinterlegten Authentisierungsmethode während einer Dauer von maximal fünf Jahren nutzen, wobei sich diese Dauer für qualifizierte elektronische Signaturen entsprechend verkürzt, wenn die Gültigkeitsdauer des von Ihnen vorgelegten Identifikationsdokuments früher abläuft oder das anerkannte Identifikationsverfahren generell eine kürzere Nutzungszeit vorsieht.

7 Umgang mit Ihren Daten

7.1 Allgemein, Datenschutzerklärung

Swisscom erhebt, speichert und bearbeitet nur Daten, die für die Erbringung des Zertifizierungsdienstes benötigt werden. Der Umgang mit den Daten richtet sich neben den anwendbaren schweizerischen Gesetzen (Schweizerisches Datenschutzgesetz, Schweizerisches Gesetz über die elektronische Signatur für qualifizierte elektronische Signaturen) auch nach den oben in Ziffer

2.1 dieser Nutzungsbestimmungen erwähnten Zertifikatsrichtlinien.

Der Umgang mit Ihren Daten ist weiter in der [Datenschutzutzerklärung für die Nutzung Zertifizierungsdienstes](https://trustservices.swisscom.com) von Swisscom geregelt, die Sie unter <https://trustservices.swisscom.com> abrufen können.

7.2 Identifikationsdokumentation

Zum Zweck der Erstellung des digitalen Zertifikats und zur Aufrechterhaltung der Nachvollziehbarkeit des Zertifizierungsdienstes erfasst und speichert Swisscom oder die Registrierungsstelle von Swisscom von Ihnen folgende Daten (soweit diese überhaupt von Ihnen im Identifikationsprozess gemäss Ziffer 2.2 dieser Nutzungsbestimmungen bekannt gegeben wurden):

Persönliche Vor-Ort-Identifikation:

- Kopie der relevanten Seiten des von Ihnen vorgelegten Ausweisdokuments (Pass, Identitätskarte, eventuell andere Dokumente gemäss Ziffer 2.2, wenn nur fortgeschrittene elektronische Signaturen erstellt werden sollen) mit den darin enthaltenen Informationen (insbesondere Namen, Vorname, Geschlecht, Geburtsdatum, Gültigkeitsdatum des Ausweisdokuments, Nationalität)
- Persönlich verwendetes Authentisierungsmittel (z.B. Mobiltelefonnummer)
- Fotografie von Ihnen aus dem Identifikationsgespräch.

Videoidentifikation bzw. Autovideoidentifikation:

- Fotografie von Ihnen aus der Videoidentifikation
- Fotografien der relevanten Seiten des von Ihnen vorgelegten Ausweisdokuments
- Audioaufzeichnung des Videogesprächs
- Technische Angaben (z.B. IP-Adresse) des von Ihnen verwendeten Endgerätes
- Im Lichtbildausweis enthaltene Informationen (insbesondere Namen, Vorname, Geschlecht, Geburtsdatum, Gültigkeitsdatum und Seriennummer des Ausweisdokuments, Nationalität)
- Persönlich verwendetes Authentisierungsmittel (z.B. Mobiltelefonnummer)
- Sofern unterstützt: Aus dem Chip Ihres Ausweisdokuments ausgelesene Daten (z.B. Name, Vorname, Geburtsdatum, Adresse, Gültigkeitsdatum und Seriennummer des Ausweisdokuments, Nationalität)

eID Identifikation:

- Persönlich verwendetes Authentisierungsmittel (z.B. Mobiltelefonnummer)
- Daten eines zugelassenen eID Dienstes auf den aus der Ferne mittels Authentisierungsmittel zugegriffen wird (z.B. Name, Vorname, Geschlecht, Geburtsdatum, Adresse, Gültigkeitsdatum und Seriennummer des Ausweisdokuments, Nationalität)

e-Banking Account basierte Identifikation:

- Ihre von Ihnen bzw. dem Betreiber der Signaturapplikation übermittelten Personendaten (insbesondere Namen, Vorname, Geschlecht, Geburtsdatum, Geburtsort, Wohnadresse, Nationalität)
- Persönlich verwendetes Authentisierungsmittel (z.B. Mobiltelefonnummer)

- Ihr für das eBanking verwendete Bankkonto (IBAN/BIC/Namen der Bank)
- ggfs. Schufa-ID oder ID eines anderen Bonitätsauskunftsunternehmens
- ggfs. Daten zur Referenztransaktion
 - Kontoinhaber
 - Kontonummer
 - Zeitpunkt der Referenzüberweisung
 - Transaktionsfreigabeverfahren

Sonstige von Ihnen im Identifikationsprozess gelieferten Angaben und Dokumente z.B. auch zu Ihrer Organisation, wie z.B. Handelsregisterauszüge, Vollmachten, Gesellschafterverträge oder sonstige Belege betreffend besonderer Attribute im Zertifikat.

7.3 Digitales Zertifikat

Gestützt auf die Daten, die im Identifikationsprozess von Ihnen angegeben und erhoben wurden, stellt Swisscom auf Anfrage der Teilnehmerapplikation und mit Ihrer Willensbekundung ein qualifiziertes oder fortgeschrittenes Zertifikat aus, welches folgende Angaben über Sie enthalten kann.

Sofern die Teilnehmerapplikation die Verwendung von Klarnamen vorsieht:

- Vornamen, Familienname
- Informeller Name zur vereinfachten Darstellung (z.B. Rufname)
- Zweistelliger ISO 3166 Ländercode

Sofern die Teilnehmerapplikation die Verwendung von Pseudonym vorsieht:

- Pseudonym
- Informelle Bezeichnung zur vereinfachten Darstellung (z.B. Kennzeichnung PSEUDONYM)
- Zweistelliger ISO 3166 Ländercode

Darüber hinaus können folgende Angaben im Zertifikat enthalten sein:

- Weitere Angaben z.B. zur Sicherstellung der Eindeutigkeit des digitalen Zertifikats:
 - Unternehmungsbezeichnung
 - E-Mail Adresse
 - Nummer/ID des vorgelegten Ausweisdokuments
- Mobiltelefonnummer
- Angezeigter Text zur Freigabe der Signatur der von Ihnen verwendeten Signaturapplikation (z.B. „Bitte bestätigen Sie die Signatur der Datei test.pdf in der Applikation XYZ“)
- Für Identifikation verantwortliche Registrierungsstelle
- Ausstellungszeitpunkt

Das digitale Zertifikat ist nach Abschluss des Signaturvorgangs in der elektronisch signierten Datei enthalten. Wer im Besitz der elektronisch signierten Datei ist, kann die oben aufgeführten Angaben aus dem digitalen Zertifikat jederzeit einsehen. Damit können Dritte die Angaben zu Ihrer Person überprüfen und

auch sehen, dass Swisscom als schweizerische Zertifizierungsdiensteanbieterin hinter der Zertifizierung dieser Daten und des Signaturvorgangs steht.

7.4 Daten nach Abschluss des Signaturvorgangs

Die Registrierungsstelle von Swisscom bzw. Swisscom selbst behält die in Ziffer 7.2 beschriebenen Daten während der Nutzungsdauer gemäss Ziffer 6 dieser Nutzungsbestimmungen auf, damit Sie den Zertifizierungsdienst nutzen können. Weiter ist Swisscom (ggfs. unter Zuhilfenahme einer Registrierungsstelle) bei qualifizierten elektronischen Signaturen gesetzlich verpflichtet, verschiedene Daten zum Identifikationsprozess, zum digitalen Zertifikat und zum Signaturvorgang während 11 Jahren ab dem letzten Signaturvorgang aufzubewahren. Im Falle von fortgeschrittenen elektronischen Signaturen behält Swisscom gemäss ihren Zertifikatsrichtlinien verschiedene Daten zum Identifikationsprozess, zum digitalen Zertifikat und zum Signaturvorgang während 7 Jahren ab dem letzten Signaturvorgang auf. Damit wird sichergestellt, dass die Nachvollziehbarkeit der Korrektheit des elektronisch signierten Dokuments in den Jahren nach deren Erstellung aufrechterhalten werden kann. Swisscom zeichnet hierbei alle einschlägigen Informationen über die von Swisscom 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 Zertifizierungsdienstes sicherzustellen.

Einerseits behält Swisscom hierfür folgende Daten auf:

- Logdateien zum Signaturvorgang (enthält insbesondere Geschäftspartnernummer, Vorgangsnummer, ablaufbezogene Daten)
- Hashwert des signierten Dokuments

Sofern Swisscom die Angaben gemäss Ziffer 7.2 dieser Nutzungsbestimmungen nicht selbst aufbewahrt, liefert die Registrierungsstelle Swisscom diese Angaben, soweit dies für die Erbringung des Zertifizierungsdienstes gemäss den gesetzlichen Vorschriften nötig ist. Swisscom führt zudem eine Zertifikatsdatenbank. Swisscom löscht die in dieser Ziffer 7.4 beschriebenen Daten nach Ablauf von höchstens 17 Jahren ab Durchführung des Identifikationsprozesses gemäss Ziffer 2.2 dieser Nutzungsbestimmungen. Im Falle einer Identifikation nur nach Anforderung von fortgeschrittenen elektronischen Signaturen gemäss Ziffer 2.2 löscht Swisscom diese Daten nach Ablauf von höchstens 13 Jahren ab Durchführung des Identifikationsprozesses.

8 Beizug Dritter

Swisscom darf zur Erfüllung ihrer Pflichten Dritte beziehen. Insbesondere wird Swisscom Trust Services AG, Zürich, Schweiz als Lieferant für Technologie und Dienstleistungen beigezogen. Weitere Dritte werden insbesondere zur Durchführung des Identifikationsprozesses (inklusive Aufbewahrung der Identifikationsdokumentation) von Swisscom beauftragt (Registrierungsstellen).

9 Haftung und höhere Gewalt

Swisscom hat stets die Anforderungen, die das Gesetz und die technischen Standards an die Anbieterinnen von Zertifizierungsdiensten stellt, zu erfüllen. Hierfür setzt Swisscom angemessene und dem aktuellen Stand

der Technik entsprechende Sicherheitsmassnahmen ein. Sie nehmen zur Kenntnis, dass trotz aller Anstrengungen von Swisscom, des Einsatzes moderner Technik und Sicherheitsstandards sowie der Kontrolle durch eine unabhängige Stelle betreffend die Einhaltung der technischen Standards und bei qualifizierten elektronischen Signaturen der Kontrolle durch die ZertES-Anerkennungsstelle betreffend die Einhaltung der gesetzlichen Vorschriften eine absolute Sicherheit und Fehlerlosigkeit des Zertifizierungsdienstes nicht gewährleistet werden kann.

Sofern Swisscom nicht beweist, dass sie kein Verschulden trifft, haftet sie Ihnen gegenüber unbeschränkt für Schäden, die Sie erleiden, weil Swisscom ihren Pflichten aus dem schweizerischen Bundesgesetz über die elektronische Signatur nicht nachgekommen ist. Unterichtet Swisscom Sie direkt oder durch den Betreiber der Teilnehmerapplikation vor einer Signaturerstellung über ein Transaktionslimit bei Rechtsgeschäften mit Geldzahlungen (inklusive im Zusammenhang mit der Erstellung einer elektronischen Signatur mit dem Zertifizierungsdienst von Swisscom) und ist dieses Transaktionslimit für Dritte z.B. durch Angabe des Transaktionslimits im Zertifikat ersichtlich, so haftet Swisscom nicht für Schäden, die bei einer über diese Beschränkungen hinausgehenden Verwendung der Dienste entstanden sind.

Sofern Swisscom nicht beweist, dass sie kein Verschulden trifft, haftet Swisscom bei anderen Vertragsverletzungen (insbesondere im Zusammenhang mit fortgeschrittenen Zertifikaten und fortgeschrittenen elektronischen Signaturen) Ihnen gegenüber für den nachgewiesenen Schaden wie folgt: Die Haftung für Sach- und Vermögensschäden infolge leichter Fahrlässigkeit ist für die gesamte Vertragsdauer auf höchstens CHF 5'000 beschränkt. Die Haftung von Swisscom für leichte fahrlässig verursachte indirekte Schäden, Folgeschäden, entgangenen Gewinn, Datenverluste, Schäden infolge Downloads, Ansprüche Dritter und Reputationsverluste ist ausgeschlossen. Swisscom haftet Ihnen gegenüber für Personenschäden immer unbeschränkt. Swisscom haftet Ihnen gegenüber nicht für das ordentliche Funktionieren von Systemen Dritter, insbesondere nicht für die von Ihnen verwendete Hard- und Software oder für die von Ihnen für das Ansteuern des Zertifizierungsdienstes verwendete Teilnehmerapplikation.

Swisscom haftet Ihnen gegenüber 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, Erdbeben usw.), kriegerische Ereignisse, Aufruhr, unvorhersehbare behördliche Restriktionen sowie Pandemien oder Epidemien. Kann Swisscom ihren vertraglichen Verpflichtungen nicht nachkommen, wird die Vertragserfüllung oder der Termin für die Vertragserfüllung dem eingetretenen Ereignis entsprechend hinausgeschoben. Swisscom haftet nicht für allfällige Schäden, die dem Kunden durch das Hinausschieben der Vertragserfüllung entstehen.

10 Änderungen der Nutzungsbestimmungen

Swisscom behält sich das Recht vor, diese Bedingungen zu ändern und zu ergänzen. Insbesondere bei Änderungen des Bundesgesetzes über die elektronische Signa-

tur (ZertES; SR 943.03) und seiner Ausführungsgesetzgebung sowie bei Anordnungen der ZertES-Anerkennungsstelle oder einer unabhängigen Stelle zur Prüfung der fortgeschrittenen elektronischen Signaturen kann Swisscom gezwungen sein, die in Ziffer 2.1 dieser Nutzungsbestimmungen erwähnten Zertifikatsrichtlinien und die vorliegenden Nutzungsbestimmungen anzupassen. Sie werden bei Änderungen zumindest ein Monat vor Geltungsbeginn von Swisscom oder von einer von ihr beauftragten Registrierungsstelle über die Änderungen und die Ihnen zustehende Widerspruchsfrist informiert, sofern Sie nicht nur für eine Einmalsignatur registriert wurden. Diese Information kann über SMS an die von Ihnen hinterlegte Mobilfunknummer erfolgen. Sie können die Annahme der neuen Bedingungen ablehnen, indem Sie auf die Nutzung des Zertifizierungsdienstes gemäss diesen Nutzungsbestimmungen ab dem Geltungsbeginn verzichten. Nutzen Sie den Zertifizierungsdienst 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 schweizerischen Recht.

Im Konfliktfall bemühen wir uns um eine einvernehmliche Streitbeilegung. Unter Vorbehalt zwingender Gerichtsstände (insbesondere für Konsumenten gemäss Artikel 32 und 35 der schweizerischen Zivilprozessordnung) ist der Gerichtsstand Bern in der Schweiz.

12 Wie Sie uns erreichen können

Wenn Sie Fragen bezüglich der Leistungserbringung gemäss den vorliegenden Nutzungsbestimmungen haben, können Sie Swisscom über die folgende Internetseite kontaktieren www.swisscom.com/signing-service.