



Als führender Vertrauensdiensteanbieter in Europa
ermöglichen wir die innovativsten, digitalen
Geschäftsmodelle.

Leistungsbeschreibung Online Identifikation Smart Registration Service

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Switzerland

<https://trustservices.swisscom.com>
E-Mail: sts.salessupport@swisscom.com



1 Inhalt

1	Inhalt	2
2	Übersicht zum Service	3
3	Definitionen	4
3.1	Service Access Interface Point (SAIP)	4
3.2	Servicespezifische Definitionen	4
4	Ausprägungen und Optionen	5
4.1	Definition der Leistungsausprägungen und Optionen	6
4.2	Ablauf der Identifikation und Registrierung	7
4.2.1	Auswahl des Verfahrens	7
4.2.2	Bezahlung	8
4.2.3	Optional: Installation des Authentisierungsmittels	8
4.2.4	Identifikationsprozess	8
4.2.5	Nutzungsbestimmungen	9
4.2.6	Signatur	9
4.2.7	Rückerstattung	9
4.3	Einschränkungen der Identifikationsverfahren	9
4.4	Self-Service Portale für Mobilnummer basierende Authentisierungsverfahren.	10
4.4.1	Überprüfung des Registrierungsstatus	10
4.4.2	Test der Signaturfähigkeit	11
4.5	Service Desk	11
5	Leistungsdarstellung und Verantwortlichkeiten	12
6	Service Level	13
6.1	Service Level	13
6.1.1	Gültigkeitszeitraum der zugesandten URL und Wiederholungsversuche	13
6.1.2	Smart Registration Service	13
6.1.3	Service Level Partneridentifikationen	14
7	Rechnungsstellung und Mengenreport	15
8	Besondere Regelungen	15
8.1	Austausch der Identifikationspartner	15
8.2	Datenbearbeitung durch Dritte aus dem In- oder Ausland, Notfallzugriffe	16
8.3	Identifikation von Personen mit Wohnsitz ausserhalb EU/EWR/Schweiz	16



2 Übersicht zum Service

Der Signing Service und der Smart Registration Service gemäss dieser Leistungsbeschreibung ist eine serverbasierte Fernsignatur- und Identifikationsleistung der Swisscom IT Services Finance S.E., Wien (AT), nachfolgend "Swisscom ITSF" genannt und der Swisscom (Schweiz) AG. Der Signing Service und der Smart Registration Server werden in den Rechenzentren von Swisscom (Schweiz) AG in der Schweiz und Partnern in der EU bereitgestellt und Swisscom Trust Services AG (nachfolgend „Swisscom“) vertreibt die Services in eigenem Namen oder räumt Dritten wiederum das Recht ein, die Services in eigenem Namen zu vertreiben.

Der Service zur Bereitstellung von Identifikationsleistungen von Swisscom (nachfolgend "**Smart Registration Service**" oder der Einfachheit halber «Service» oder "SRS" genannt) ermöglicht einem Signierenden sich mittels mehrerer angebotener Identifikationsverfahren für den Signing Service von Swisscom Trust Services zu registrieren. Die ordnungsgemässe Registrierung berechtigt zukünftig unseren Verkaufspartnern und deren Kunden, dem Signierenden Signaturen auszustellen. Hierfür ist ein Vertragsverhältnis mit einem Anbieter des Signaturangebotes der Swisscom Trust Services notwendig. Die Swisscom Trust Services bieten keine Signaturen im Direktverkauf an Privatpersonen an.

Die Registrierung setzt dabei voraus, dass der Signierende auch eine Authentisierung einsetzt, die dann später für die Freigabe der Signatur genutzt wird. Das kann beispielsweise die Mobile ID App sein oder eine Kombination von Passwort und Einmalcode via SMS oder ein andere angebotene Authentisierungslösung. Sofern die Authentisierung auf einer App oder einem Hardwaretoken basiert, muss diese in der Regel vorab initialisiert worden sein.

Swisscom Trust Services greift bei den Identifikationsverfahren des Smart Registration Service auf Partner (nachfolgend "**Identifizierer**" genannt) zurück und beauftragt diese in Einklang mit der EU- und schweizerischen Gesetzgebung über die elektronische Signatur mit der Durchführung des jeweiligen Identifikationsverfahrens.

Nach erfolgreicher Durchführung des jeweiligen Identifikationsverfahrens archiviert Swisscom die Identifikationsdaten für die gesetzlich vorgeschriebene Dauer und verwaltet die Annahme der Swisscom Nutzungsbestimmungen.

Die identifizierte Person kann fortan auf Basis des während des Identifikationsverfahrens geprüften Authentisierungsmittels (z.B. Mobilnummer) und bis zum Ablauf der Gültigkeit der Identifikation über den Vertrauensdienst von Swisscom – je nach Identifikationsmethode – fortgeschrittene oder qualifizierte elektronische Signaturen erstellen ("Repetitive Signing").

Smart Registration Service

- Anwahl der Identifikationsmethode
- Registrierung mit Authentisierungsmittel zur Willensbekundung
- Archivierung der Registrierungsevidenzen
- Einholen Zustimmung zu Nutzungsbestimmungen



Identifizierer

- Bereitstellung der Registrierungsmethode
- Identifikation und Registrierung



Signing Service

- Signatur basierend auf Smart Registration Service Identifikation





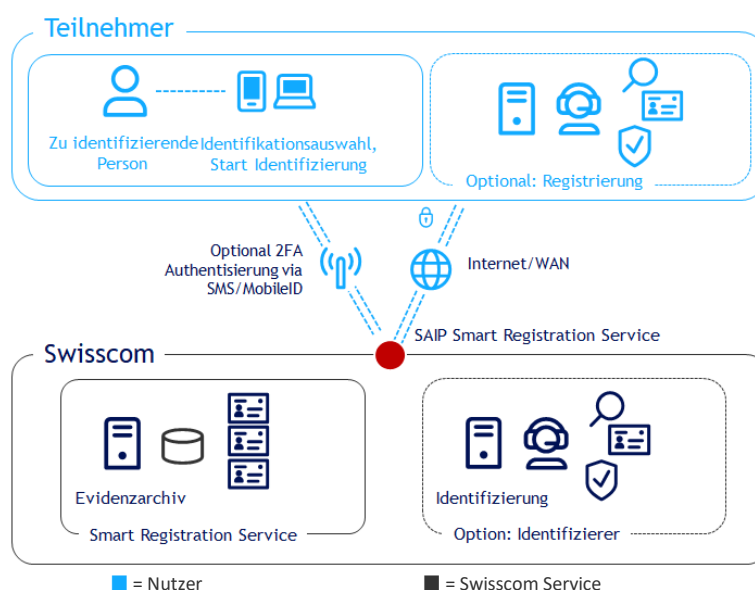
3 Definitionen

3.1 Service Access Interface Point (SAIP)

Der Service Access Interface Point (SAIP) ist der vertraglich vereinbarte, geografische und/oder logische Punkt, an dem ein Service dem Leistungsbezüger, also dem Nutzer, bereitgestellt, überwacht und die erbrachten Service Level ausgewiesen werden.

Der SAIP ist hierbei die Webseite <https://srsident.trustservices.swisscom.com>. Hier kann der Nutzer verschiedene Verfahren auswählen, direkt oder mit Gutscheincode bezahlen und durchführen. Je nach Verfahren wird er dann weitergeleitet zum Identifizierer, der ihn identifiziert.

Folgende rein schematische Darstellung dient der Veranschaulichung der Leistungen und Leistungs-Komponenten des Smart Registration Service:



Der Nutzer kommuniziert dabei zunächst über Internet mit dem Swisscom Smart Registration Service (SRS). Nach Weiterleitung kommuniziert er direkt mit dem Identifizierungsdienstleister. Dieser stellt die Identifizierungsdaten, die sogenannten "Evidenzen" der Swisscom bereit. Sofern nicht bereits während der Registrierung geschehen, muss der Signierende noch die Nutzungsbestimmungen zum Signing Service unterzeichnen. Hierbei sendet Swisscom eine SMS mit den Links zu den Nutzungsbestimmungen aus, die dann mit der Authentisierungsmethode akzeptiert werden müssen. Mobilfunkdienste, die für die Identifikation, Authentifikation oder Willensbekundung genutzt werden sind nicht Bestandteil des Service Level Versprechens. Die Verfügbarkeit des Services ist dann gegeben, wenn Anfragen durch den Service entgegengenommen werden und entsprechend der Schnittstellenbeschreibung zum SAIP korrekt beantwortet werden. Die Antwort kann auch eine dokumentierte Fehlermeldung sein.

3.2 Servicespezifische Definitionen

Begriff	Beschreibung
eIDAS-Vo	EU-Verordnung über elektronische Identifikation und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.
Evidenz	Beweis in Form eines signierten PDF-Dokuments. Dieses PDF enthält typischerweise die Fotos und Scans, die während dem Identifikationsprozess erstellt wurden, sowie die erhobenen Daten oder andere regulatorisch geforderte Daten zum Identifikationsnachweis. Die Evidenz ist mit der elektronischen Signatur der Organisation versehen, die die Identifikation durchgeführt hat.
Fortgeschrittene elektronische Signatur (FES)	Fortgeschrittene elektronische Signatur, die der Signing Service gemäss Zertifikatsrichtlinien von Swisscom (Schweiz) AG bzw. von Swisscom IT Service Finance S.E. zur Verfügung stellt.
Identifizierer	Sofern der Nutzer kein eigenes Identifizierungs- und Registrierungsverfahren einbringt, bietet Swisscom die Identifikation und Registrierung durch einen Identifikationspartner, «Identifizierer», an.



Begriff	Beschreibung
MobileID	Managed Service für die sichere Benutzer-Authentisierung via Mobiltelefon. MobileID kann von verschiedenen Schweizer Providern, unter anderem Swisscom, bezogen werden.
Nutzungsbestimmungen (für den Swisscom Signaturdienst)	Die Nutzungsbestimmungen regeln im Verhältnis zwischen Swisscom (Schweiz) AG bzw. Swisscom IT Services Finance S.E. und dem Signierenden auf einer Nutzerapplikation die Bedingungen für die Nutzung der Signaturzertifikate und Signaturdienstleistung. Diese sind unter https://trustservices.swisscom.com/repository/ abrufbar.
OTP	One Time Password – Einmalpasswort, welches für eine einmalige Nutzung erzeugt und über SMS übertragen wird.
Passwort mit One Time Passwort	Verfahren zur 2-Faktor Authentisierung, bei der für die Willensbekundung zur Signatur für den Signaturservice sowohl ein Passwort gewählt wird und zusätzlich noch ein per SMS gesendetes Einmalpasswort eingegeben wird.
Qualifizierte elektronische Signatur (QES)	Qualifizierte elektronische Signatur, die der Signing Service gemäss Zertifikatsrichtlinien von Swisscom (Schweiz) AG bzw. von Swisscom ITSF zur Verfügung stellt.
RA Delegationsvertrag	Vertrag zwischen Swisscom und dem Identifizierer, auf den Swisscom für die Durchführung der Identifikationsverfahren Rückgriff nimmt.
Registrierung	Regulierter Prozess zur Ermittlung und Speicherung von Identifikationsdaten sowie mit diesen Identifikationsdaten verbundenen Authentisierungsmittel, die für die Auslösung einer elektronischen Signatur via Signing Service erforderlich sind.
Registrierungsstelle (RA)	Registrierungsstelle (Registration Authority) Zuständige Stelle für die Identifikation der Signierenden. Teile des Prozesses der Registrierungsstelle können im Rahmen eines RA Delegationsvertrages durch Swisscom (Schweiz) AG oder Swisscom ITSF an Dritte ausgelagert werden.
Nutzer	Swisscom erbringt die Leistungen gemäss vorliegender Leistungsbeschreibung zu Gunsten des Nutzers. Der Nutzer ist entweder direkt Kunde von Swisscom mit einem Smart Registration Vertrag (inklusive Annahmeerklärung gegenüber Swisscom (Schweiz) AG) oder er hat einen kommerziellen Vertrag mit einem Reseller von Swisscom Leistungen.
Nutzerapplikation	Der Nutzer gibt einem oder mehreren zu identifizierenden Personen Zugang zu einer Applikation, mit der er oder sie sich im Einklang mit den Nutzungsbestimmungen von Swisscom für den Signaturservice registrieren können und der Nutzer stellt dabei die Auswahl der Registrierungsmethode sicher, sendet ggfs. Vorabidentifikationsdaten und leitet die empfangene URL zum Identifizierungspartner an die Person weiter. Die Nutzerapplikation in diesem Zusammenhang ist nicht Bestandteil dieser Leistungsbeschreibung, sie wird ausserhalb des Swisscom Service z.B. durch Partner von Swisscom oder dem Nutzer selber bereitgestellt.
VZertES	Schweizerische Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate.
ZertES	Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate.
Zu identifizierende Person	Natürliche Person, die vorgängig identifiziert werden muss, um danach mit Authentifikation und Willensbekundung ein Dokument elektronisch zu signieren.

4 Ausprägungen und Optionen

Standardausprägung	Smart Registration Service
Identifikation durch Identifizierer:	
SRS Video EU: Videoidentifikation für EU Signaturen	<input type="radio"/>
SRS Bank DE: Identifikation mittels eBanking Account	<input type="radio"/>
SRS eID DE: eID Identifikation (Deutschland)	<input type="radio"/>
SRS Selfie Ident EU: Selbstidentifikation für EU Signaturen	<input type="radio"/>
SRS Video CH: Videoidentifikation für CH Signaturen	<input type="radio"/>
SRS Autoident CH: Selbstidentifikation für CH Signaturen	<input type="radio"/>



Standardausprägung	Smart Registration Service
Nutzung des Self-Service Portals	●

● = Standard (im Preis inbegriffen) ○ = Gegen Aufpreis

4.1 Definition der Leistungsausprägungen und Optionen

Leistungsausprägung/Option	Definition
SRS Video EU: Videoidentifikation für EU-Signaturen	Mit SRS Video EU erhält der Nutzer eine URL auf eine Webseite oder einen Verweis auf eine App, wo er den Videoidentifikationsdienst aufrufen kann. Hierfür ist es notwendig, einen PC mit Webcam oder ein mit Kamera und einer auf der Webseite angezeigten App ausgestattetes Smartphone zu haben. Im Rahmen einer Websession muss die zu identifizierende Person benutzergeführt durch einen Operator des Videoidentifizierers seinen Ausweis zeigen und Fragen zur Bestätigung der Ausweisdaten und der Lebendigkeit im Video beantworten. Anschliessend werden die so ermittelten Daten an Swisscom übertragen.
SRS Bank DE: Identifikation mittels eBanking Account	Mit SRS Bank DE erhält der Nutzer eine URL auf eine Webseite, wo er den Bankidentifikationsdienst aufrufen kann, der zunächst die Identifikationsdaten der zu identifizierenden Person inklusive Mobilnummer für zukünftige Willensbekunden erfragt. Anschliessend gibt die zu identifizierende Person das Konto ihrer e-Banking fähigen Hausbank ein. Sie loggt sich auf ihr Bankkonto ein und bestätigt die von der Bank gestellten Anfragen zur Authentisierung und führt eine Referenzüberweisung durch. Die Mobilnummer wird nun noch durch ein SMS Einmalpasswort bestätigt. Nach diesem Login verlässt die zu identifizierende Person wieder ihr Bankkonto und ist damit identifiziert. Die Identifikationsdaten, die Mobilnummer und Referenz auf den Bankloginvorgang werden an Swisscom übertragen. Der Identifizierer verwahrt in diesem Fall die genauen Vorgangsdaten als delegierte Registrierungsstelle.
SRS eID DE: Identifikation mit eID (Deutschland)	Der Nutzer erhält eine URL, wo er gebeten wird, eine App auf seinem Android oder Apple Smartphone zu installieren und zu nutzen, mit welcher folgende Schritte durchgeführt wurden: <ul style="list-style-type: none"> - Foto der Vorder- und Rückseite des deutschen Personalausweises oder eines elektronischen deutschen Aufenthaltstitels/eID Card mit eID Funktion - Freigabe zum Auslesen und Auslesen über NFC der Chipinformationen des Ausweisdokumentes in Bezug auf die Identität - Die Mobilnummer wird bestätigt mittels eines Einmalpasswortes, welches per SMS übergeben wird. Der Ergebnisdatensatz der Identitätsprüfung wird dann Swisscom zur Verfügung gestellt.
SRS Selfie Ident EU: Selbstidentifikation für EU Signaturen	Die zu identifizierende Person muss zunächst die Selfie Ident App herunterladen und installieren und die Anweisungen der App befolgen: <ul style="list-style-type: none"> • Die Vorder- und ggfs. Rückseite des zugelassenen Ausweisdokumentes muss zunächst mit der rückwärtigen Kamera des Smartphones erfasst werden. • Das Ausweisdokument muss so gekippt und bewegt werden, dass im Lichtschein alle optischen Sicherheitsmerkmale (z.B. Hologramme) erkannt werden können. • Das Ausweisfoto wird abgeglichen mit einer Eigenaufnahme der zu signierenden Person mittels der Frontkamera. • Es findet ein Liveness Check statt, indem z.B. in einer Videoaufnahme zwei vorgegebene zufällige Worte gesprochen werden oder eine bestimmte Bewegung gefordert wird. • Es findet die Prüfung der Identifikationsdaten im Hintergrund statt mit Hilfe von AI Algorithmen (Dauer bis zu 2 Minuten). • Anschliessend wird die Mobilnummer geprüft und die Nutzungsbestimmungen der Swisscom akzeptiert.



Leistungsausprägung/Option	Definition
	<ul style="list-style-type: none">Hierbei wird die Authentisierungsmethode (Mobile ID App oder Passwort / Einmalcodeverfahren) initialisiert: d.h. im Nachgang zu dieser Identifikationsmethode wird keine SMS mit den Nutzungsbestimmungen ausgesendet. <p>Der Ergebnisdatensatz wird dann an Swisscom übermittelt. Da keine persönliche Benutzerführung erfolgt, ist der Nutzer selber dafür verantwortlich die korrekten Ausweise (z.B. keinen Führerausweis/Führerschein) zu zeigen, sondern stets ein Pass- oder ID Dokument gemäss der Länderliste, die beim Kauf angezeigt wurde.</p>
SRS Video CH: Videoidentifikation für CH Signaturen	<p>Mit SRS Video CH erhält der Nutzer eine URL auf eine Webseite, auf der er den Videoidentifikationsdienst direkt oder mittels App aufrufen kann. Hierfür ist es notwendig, einen PC mit Webcam oder ein mit Kamera und einer auf der Webseite angezeigten App ausgestattetes Smartphone zu haben. Die Identifikation kann wahlweise via Browser auf dem PC (nicht mobil) oder via einer besonderen App durchgeführt werden. Im Rahmen einer Websession muss die zu identifizierende Person benutzergeführt durch einen Operator des Videoidentifizierers seinen Ausweis zeigen und Fragen zur Bestätigung der Ausweisdaten und der Lebendigkeit im Video beantworten. Anschliessend werden die so ermittelten Daten an Swisscom übertragen.</p>
SRS Autoident CH: Selbstidentifikation für CH Signaturen	<p>Die zu identifizierende Person muss zunächst die Autoident App herunterladen und installieren und die Anweisungen der App befolgen:</p> <ul style="list-style-type: none">Die Vorder- und ggfs. Rückseite des zugelassenen Ausweisdokumentes muss zunächst mit der rückwärtigen Kamera des Smartphones erfasst werden.Das Ausweisdokument muss so gekippt und bewegt werden, dass im Lichtschein alle optischen Sicherheitsmerkmale (z.B. Hologramme) erkannt werden können.Das Ausweisfoto wird abgeglichen mit einer Eigenaufnahme der zu signierenden Person mittels der Frontkamera.Es findet ein Liveness Check statt, indem z.B. in einer Videoaufnahme zwei vorgegebene zufällige Worte gesprochen werden oder eine bestimmte Bewegung gefordert wird.Es findet die Prüfung der Identifikationsdaten im Hintergrund statt mit Hilfe von AI Algorithmen (Dauer bis zu 2 Minuten).Auch wird die Mobilnummer geprüftDer Ergebnisdatensatz wird dann an Swisscom übermittelt.Die Nutzungsbestimmungen der Swisscom werden im Anschluss per SMS Aussendung und Aufruf des Links in der SMS mit Mobile ID (App) oder Passwort/Einmalcode akzeptiert. <p>Da keine persönliche Benutzerführung erfolgt, ist der Nutzer selber dafür verantwortlich die korrekten Ausweise (z.B. keinen Führerausweis/Führerschein) zu zeigen, sondern stets ein Pass- oder ID Dokument gemäss der Länderliste, die beim Kauf angezeigt wurde.</p>
Nutzung des Self-Service Portals	<p>Das Self-Service Portal ermöglicht die Überprüfung der Registrierung. Es kann überprüft werden, ob die Registrierung korrekt für den jeweiligen Rechtsraum, das Signaturniveau und unter Akzeptanz der Nutzungsbestimmungen erfolgt ist. Ggfs. kann die Akzeptanz der Nutzungsbestimmungen auch ausgelöst werden.</p>

4.2 Ablauf der Identifikation und Registrierung

4.2.1 Auswahl des Verfahrens

Die zu identifizierende Person besucht die Webseite

<https://srsident.trustservices.swisscom.com>

Sie wählt ein passendes Verfahren nach folgenden Kriterien aus:

- Das Verfahren lässt eine Registrierung nach dem passenden Rechtsraum zu. Für Signaturen nach EU-Recht muss ein Registrierungsverfahren gewählt werden, welches in der EU nach der eIDAS Regulierung zugelassen ist. Für



Signaturen nach Schweizer Recht muss ein Verfahren ausgewählt werden, welches nach dem Schweizer Signaturgesetz ZertES zugelassen ist.

- Die rechtliche Signaturqualität muss stimmen: In der Regel verlangen qualifizierte elektronische Signaturen, die in der Regel eine Handschrift ersetzen können, eine aufwändigere Registrierung als fortgeschrittene elektronische Signaturen. Fortgeschrittene elektronische Signaturen könnten aber für bestimmte Rechtsprozesse (z.B. Kreditvergabe) nicht erlaubt sein. Der Nutzer hat diese Bedingungen bei der Auswahl des Identifikationsverfahrens in eigener Verantwortung zu beachten. Der Nutzer nimmt zur Kenntnis, dass die Auswahl eines für die gewünschte elektronische Signatur unzulässigen Identifikationsverfahrens dazu führt, dass im Prozess zur Erstellung der elektronischen Signatur eine Fehlermeldung kommt und die Erstellung der elektronischen Signatur verhindert wird.
- Das Identifikationsmittel muss passen. Bei jeder Identifikationsmethode steht dabei, welche Voraussetzungen gegeben sein müssen. Für eine eID Identifikation muss die Person im Besitz einer staatlich anerkannten eID Lösung sein und z.B. auch über ein Smartphone mit NFC verfügen und/oder über eine App, die staatlich anerkannt ist. Für Video- und Autoidentifikationsverfahren muss ein maschinenlesbarer Ausweis (Pass oder ID-Karte der EU/CH) vorliegen.
- Preis/Gutscheincode: Die Verfahren haben – je nach Aufwand – unterschiedliche Preise. Sofern nicht mit Kreditkarte sondern Gutscheincode bezahlt wird, kann der Gutscheincode auf ein bestimmtes Verfahren eingeschränkt sein. Hierbei ist ggfs. eine Rückfrage erforderlich mit der Partei, die den Gutscheincode übergeben hat.

4.2.2 Bezahlung

Nachdem das passende Verfahren gewählt wurde, kann der Nutzer die Identifikation mittels angegebener Kreditkarte oder Gutscheincode bezahlen. Durch Kreditkartenverkäufe kommen Verträge mit Privatkunden zustande, die im Anschluss einen Zahlungsbeleg erhalten. Juristische Personen sollten vertraglich über die Partner von Swisscom Trust Services einzelne Gutscheine oder im Direktverkauf ein Gutscheinpaket (mindestens 200 Registrierungen) erwerben. Nur Gutscheinkunden erhalten eine Rechnung.

4.2.3 Optional: Installation des Authentisierungsmittels

Bevor der Installationsprozess gestartet wird, muss das Authentisierungsmittel, welches später für die Signaturfreigabe genutzt werden soll, installiert werden. Wird kein Authentisierungsmittel installiert, wird der Nutzer gezwungen eine Kombination von selbstgewähltem Passwort und Einmalcode via SMS zu nutzen. Ansonsten kann er eines der angebotenen Authentisierungsmittel, z.B. die Mobile ID App vorab installieren. Z.B. kann dann ein Fingerabdruck anstelle eines Passwortes verwendet werden. Wichtig ist, dass die Installation immer VOR der Identifikation erfolgt.

4.2.4 Identifikationsprozess

Zum Start des Identifikationsprozesses wird der Benutzer nun zum Anbieter weitergeleitet. Parallel dazu erhält der Benutzer auch per angegebener E-Mail Adresse den Link zugesendet, unter dem er die Identifikation beim entsprechenden Anbieter starten kann. Die Links / Weiterleitungen haben Verfallsdaten (siehe unten).

Der Identifikationsprozess wird nun nach den Anweisungen am Bildschirm mit dem externen Identifikationsanbieter durchgeführt. Gegebenenfalls müssen bereits vorab Daten mitgegeben werden, die nun im Prozess abgefragt werden. Teilweise ist hier auch eine App des Anbieters zu installieren oder der Prozess kann komplett im Browser abgewickelt werden.

Während des Identifikationsprozesses ist darauf zu achten:

- Je nach Verfahren die notwendigen Mittel zur Verfügung zu haben, z.B. eine ausreichende Kamera oder einen NFC Leser etc.
- Bei Vorzeigen eines Ausweisdokumentes, stets das korrekte Dokument (Pass oder EU/CH ID) vorzuweisen und z.B. keinen Ausländerausweis, Führerausweis, etc.
- Ggfs. abzuwarten, dass die App oder der Prozess die Daten auch zur Swisscom überträgt und den Prozess nicht vorzeitig abzubrechen.

In vielen Situationen können Sie bei der Identifikation eine E-Mail Adresse vorab mitteilen. Sie erhalten dann eine E-Mail mit einem Link, wo ein ggfs. abgebrochener Prozess wieder aufgenommen werden kann.

Grundsätzlich erfolgt eine Identifikationsleistung anhand des angebotenen Materials und anhand der Qualität der vom Nutzer eingesetzten Geräte. Sollten z.B. die Ausweisbilder verwaschen sein oder nicht lesbar sein oder ein falscher Ausweis vorgelegt worden sein, oder Ausweise als nicht ausreichend sicher eingestuft werden, so kann die Registrierung zurückgewiesen werden. Mit Bezahlung besteht kein Anspruch auf eine positive Registrierung sondern die Bezahlung deckt die Kosten für einen durchgeführten Versuch eines Identifikationsprozesses.



4.2.5 Nutzungsbestimmungen

Im Prozess müssen die Nutzungsbestimmungen der Swisscom Trust Services akzeptiert werden. Für die Akzeptanz wird erstmalig das Authentifizierungsmittel eingesetzt. Sofern dieses ein Passwort beinhaltet, wird das Passwort zum ersten Mal gesetzt. Häufig werden die Nutzungsbestimmungen bereits im Prozess des externen Identifikationsanbieters angezeigt und akzeptiert. Sollte das nicht so erfolgt sein, wird eine SMS mit den Nutzungsbestimmungen an die im Registrierungsprozess angegebene Mobilnummer gesendet. Der Link in der SMS muss dann geöffnet werden und die Nutzungsbestimmungen müssen mit dem vorgesehenen Authentifizierungsmittel bestätigt werden. Sofern der Anweisung in der SMS nicht Folge geleistet wird, wird die SMS binnen 15 Tage häufiger zugestellt. Sollte danach keine Zustimmung erfolgen, so wird der Registrierungsprozess gelöscht und es muss für eine Signatur eine neue Registrierung durchgeführt werden.

4.2.6 Signatur

Erst nach Akzeptanz der Nutzungsbestimmungen und der Einlieferung der Evidenz durch den Identifikationsanbieter kann der Nutzer bei den Partnersignaturapplikationen und -anwendungen signieren.

Die Registrierungen haben je nach eingesetztem Verfahren Ablaufdaten, z.B. können sie am Ablaufdatum des Ausweises gebunden sein oder sind generell nur für ein Jahr gültig. Vor Ablauf wird der Nutzer nochmals mit einer SMS gewarnt, dass er sich neu registrieren lassen muss, sofern die Mobilnummer bekannt ist.

4.2.7 Rückerstattung

Sollte ein Fehler aufgrund von Fehlern im Registrierungsprozess entstanden sein, besteht entweder bei einer Kartenzahlung das Anrecht auf eine Rückerstattung oder bei Einsatz eines Vouchers auf die Möglichkeit eines Ersatzvouchers.

Gründe sind insbesondere:

- Nicht erhaltene SMS auf Mobilnummern innerhalb der EU, Schweiz und EWR
- Abbrüche der App oder des Prozesses aufgrund von Fehlverhalten
- "Hängenbleiben" des Prozesses länger als 15 Minuten

Des Weiteren können Vouchers rückerstattet werden für Verfahren, die nach Kauf des Vouchers aus dem Angebot herausgenommen wurden.

Kein Anrecht auf Rückerstattung besteht bei:

- Einsatz von SIM Karten mit Mobilnummern, die ausserhalb der EU/Schweiz/EWR zugelassen sind
- Nicht-Erhalt von SMS aufgrund von Einstellungen oder Filter am Mobilgerät
- Abbruch des Prozesses binnen 15 Minuten nach einem angeblichen Hängenbleiben.
- Einsatz von nicht zugelassenen ID oder Passdokumenten
- Nicht-Befolgen von Anweisungen im Prozess
- Eingabe von falschen Daten, z.B. auch Kontonummern
- Einsatz von Nicht-NFC fähigen Endgeräten bei Identifikation mit einer eID Karte, die ein NFC Verfahren voraussetzt.
- Keine Akzeptanz der Nutzungsbestimmungen

4.3 Einschränkungen der Identifikationsverfahren

Regulatorisch begründet können die verschiedenen Identifikationsverfahren nur in ihrem jeweilig zugelassenen Rechtsraum und unter bestimmten Bedingungen gemäss nachfolgender Übersicht eingesetzt werden.

Für die Identifikation werden nur Pässe und IDs aus den Schengen Staaten akzeptiert, unabhängig davon, was die Anbieter noch auf den Länderlisten angeben.

Die Angaben in der Spalte "Rechtsraum" haben folgende Bedeutung:

- EU: QES: Identifikationsverfahren in der EU (eIDAS-Vo) zugelassen für qualifizierte elektronische Signaturen.
- EU: FES: Identifikationsverfahren in der EU (eIDAS-Vo) zugelassen für fortgeschrittene elektronische Signaturen.
- CH: QES: Identifikationsverfahren in der Schweiz (ZertES) zugelassen für qualifizierte elektronische Signaturen.
- CH: FES: Identifikationsverfahren in der Schweiz zugelassen für fortgeschrittene elektronische Signaturen.

Alle Identifikationsverfahren können nur so lange im Rahmen des Smart Registration Service angeboten werden, solange diese auch vom Anbieter regulatorisch zugelassen angeboten werden. Sind die Voraussetzungen für eine regulatorisch und/oder gesetzliche korrekte Leistungserbringung nicht mehr gegeben, werden diese Optionen unabhängig von Kündigungsfrist des Smart Registration Service von Swisscom Trust Services aufgekündigt und aus dem Angebot herausgenommen.



Leistungsausprägung/ Option	Rechtsraum	Einschränkung
SRS own		Projektspezifisch – wird im Umsetzungskonzept festgelegt
SRS video EU	EU: QES EU: FES CH: FES	Die Videoidentifikation ist eingeschränkt auf bestimmte Länder und bestimmte Ausweistypen, siehe unter https://trustservices.swisscom.com/downloads "Länderliste für die Videoidentifikation-Kurier-POS". Elektronische Signaturen basierend auf dem Authentisierungsmittel "Mobilnummer" können ab Identifikation maximal während 5 Jahren bzw. maximal bis zum Ablaufdatum des vorgezeigten Ausweisdokumentes erstellt werden. Danach muss erneut identifiziert werden. Sprachführung mindestens Englisch und Deutsch.
SRS bank DE	EU: QES EU: FES CH: FES	Voraussetzung ist ein Online-Bankkonto bei einem deutschen Bankinstitut, hierbei werden einige wenige Banken nicht unterstützt (Hinweise unter https://trustservices.swisscom.com/downloads , «SRS Bank DE/QES Ident»). Elektronische Signaturen basierend auf dem Authentisierungsmittel "Mobilnummer" können ab Identifikation maximal während 2 Jahre erstellt werden. Danach muss erneut identifiziert werden. Sprachführung Deutsch.
SRS eID DE	EU: QES EU: FES CH: FES	Voraussetzung ist die Verwendung des deutschen Personalausweises oder einen in Deutschland zugelassenen elektronischen Aufenthaltstitel mit eID Funktion. Elektronische Signaturen basierend auf dem Authentisierungsmittel "Mobilnummer" können ab Identifikation maximal während 5 Jahren bzw. maximal bis zum Ablaufdatum des vorgezeigten Ausweisdokumentes erstellt werden. Danach muss erneut identifiziert werden. Sprachführung mindestens Englisch und Deutsch.
SRS Selfie Ident EU	EU: QES EU: FES CH: FES	Die Identifikation ist eingeschränkt auf die Nutzung von maschinenlesbaren Ausweisen und bestimmte Ausweistypen, siehe unter https://trustservices.swisscom.com/downloads "Länderliste für die SRS Selfie Ident EU Identifikation". Elektronische Signaturen basierend auf dem Authentisierungsmittel "Mobilnummer" können ab Identifikation maximal während 5 Jahren bzw. maximal bis zum Ablaufdatum des vorgezeigten Ausweisdokumentes erstellt werden. Danach muss erneut identifiziert werden. Sprachführung mindestens Englisch und Deutsch.
SRS Video CH	EU: FES CH: QES CH: FES	Die Videoidentifikation ist eingeschränkt auf bestimmte Länder und bestimmte Ausweistypen, siehe unter https://trustservices.swisscom.com/downloads "Länderliste für die Videoidentifikation ". Elektronische Signaturen basierend auf dem Authentisierungsmittel "Mobilnummer" können ab Identifikation maximal während 5 Jahren bzw. maximal bis zum Ablaufdatum des vorgezeigten Ausweisdokumentes erstellt werden. Danach muss erneut identifiziert werden. Sprachführung mindestens Englisch und Deutsch.
SRS Autoident CH	EU: FES CH: QES CH: FES	Die Autoidentifikation ist eingeschränkt auf bestimmte Länder und bestimmte maschinenlesbare Ausweistypen, siehe unter https://trustservices.swisscom.com/downloads "Länderliste für die Videoidentifikation ". Elektronische Signaturen basierend auf dem Authentisierungsmittel "Mobilnummer" können ab Identifikation maximal während 2 Jahren bzw. maximal bis zum Ablaufdatum des vorgezeigten Ausweisdokumentes erstellt werden. Danach muss erneut identifiziert werden. Sprachführung mindestens Englisch und Deutsch.

4.4 Self-Service Portale für Mobilnummer basierende Authentisierungsverfahren.

Zwei Self-Service Portale ermöglichen die korrekte Überprüfung des Registrierungsstatus oder ermöglichen auch ohne Empfang der SMS mit den Links zu den Nutzungsbestimmungen diese zu akzeptieren. Darüber hinaus ermöglicht ein zweites Portal eine Testunterschrift durchzuführen, um damit auch den reibungslosen Ablauf einer Signatur vorab zu testen oder auf Probleme aufmerksam gemacht zu werden. Z.B. könnte ein Wechsel des Mobilgerätes oder der SIM Karte dazu führen, dass die Mobile ID als Authentisierungsmethode nicht mehr akzeptiert wird, da sich der Besitzfaktor geändert hat.

4.4.1 Überprüfung des Registrierungsstatus

Die Überprüfung des Registrierungsstatus erfolgt unter:



<https://smart-flow.scapp.swisscom.com/>

Nach Login mit Mobilnummer, die durch eine SMS mit einem einzugebenden Einmalcode überprüft wird, wird angezeigt, ob die Registrierung für eine qualifizierte elektronische Signatur (Level of Assurance Faktor 4) oder eine fortgeschrittene elektronische Signatur (Level of Assurance Faktor 3) in welchem Rechtsraum (Schweiz = CH, oder eIDAS Staaten EU/EWR) zulässig ist. Es wird darüber hinaus die Authentifizierungsmethode angezeigt und die Ablaufzeit der Gültigkeit der Registrierung. Sofern die Nutzungsbestimmungen noch nicht akzeptiert wurden oder diese aktualisiert wurden, können diese hier durch Druck auf den Button "Nutzungsbestimmungen" akzeptiert werden. Die Online-Identifikationsseite kann über den Button "Zur Identifikation" erreicht werden.

4.4.2 Test der Signaturfähigkeit

Auf der Seite

<https://check-signature.scapp.swisscom.com/>

kann überprüft werden, ob tatsächlich eine Signatur mit einem auf Mobilnummer basierenden Authentisierungsverfahren ausgelöst werden kann. Hierzu ist ein Text "Hello World" testhalber mit dem Authentisierungsverfahren zu signieren.

Nach der Signatur wird das Ergebnis angezeigt:

4.5 Service Desk

Swisscom stellt ein Servicedesk (1st Level Support) für die Identifikationen zur Verfügung, die mit Kreditkarten erworben wurden. Nutzer, die die Identifikationen per Voucher durchführen, wenden sich an die Stelle, die Ihnen die Voucher übergeben hat. Entsprechend den Anfragen löst Swisscom bei Bedarf die Incidents direkt mit den Servicestellen der Identifizierer, sofern kein eigenes Identifikationsverfahren eingesetzt wird.



5 Leistungsdarstellung und Verantwortlichkeiten

Einmalige Leistungen

Tätigkeiten (S = STS/N = Nutzer)	S	N
Bereitstellung des Service		
1. Der Nutzer kann auf https://srsident.trustservices.swisscom.com die geeignete Registrierung aufrufen und mit Vouchercode oder Kreditkarte bezahlen	✓	
2. Beendigung von Identifikationsverfahren, die den regulatorischen oder gesetzlichen Ansprüchen nicht mehr genügen, oder vom Anbieter nicht mehr unterstützt werden.	✓	

Wiederkehrende Leistungen

Tätigkeiten (S = STS/N = Nutzer)	S	N
Standardleistungen		
1. Bereitstellung und Pflege der Service Infrastruktur und Betrieb des Zugangs.	✓	
2. Sicherstellung der Konformität der Identifikationsverfahren zu den jeweiligen Arten der elektronischen Signatur gemäss Kategorisierung in Ziffer 4.3.	✓	
3. Auswahl des geeigneten, mit der gewünschten elektronischen Signatur kompatiblen Identifikationsverfahrens gemäss Ziffer 4.		✓
4. Bereitstellung und Pflege der Schnittstelle zu den von Swisscom ausgewählten Partnern für die Durchführung der Identifikation	✓	
5. Information an die zu identifizierende Person über die anstehende Identifikation, den Zweck der Identifikation und das zu befolgende Vorgehen im Rahmen der Identifikation	✓	
6. Bereitstellung eines Zugangs zum Identifikationsdienstleister für die zu identifizierende Person	✓	
7. Verantwortung für die Durchführung der Identifikation der zu identifizierenden Person nach Bereitstellung der URL durch Aufforderung oder Benutzerführung im geeigneten Portal und Einhalten aller Vorschriften für das gewählte Identifikationsverfahren, d.h. insbesondere Bereitstellung der erforderlichen Mittel (z.B. Kamera, NFC Zugang am Mobilgerät) und der notwendigen Identifizierungsmittel (Kontonummer mit Kontozugang, korrekte geforderte ID/Pass Dokumente), Akzeptanz der Nutzungsbestimmungen, genügende Ausleuchtung bei Videoverfahren, Installation der notwendigen Identifikationsapps/-programme, notwendige Eingaben oder Aussagen zu gestellten Fragen.		✓
8. Einsammeln der Evidenzdaten von den externen Identifikationsdienstleistern.	✓	
9. Melden von Sicherheitsvorfällen, die die Identifikation betreffen		✓
10. Sicherung der Konformität zur gewählten Signaturart und Rechtsraum	✓	
11. Gesetzeskonforme Archivierung der Identifikationsevidenzen und Zustimmungen zu den Nutzungsbestimmungen	✓	
12. Support und Koordinierung und Beauftragung der Supportfälle beim jeweiligen Identifizierungsdienstleister unter Nennung der Vertragsnummer, Auftragsreferenz, Zeitpunkt der Identifikation und genutzter Identifikationsmethode sowie Mobilnummer	✓	
13. Nennung der Auftragsreferenz, Zeitpunkt der Identifikation, genutzte Identifikationsmethode und Mobilnummer im Falle eines Support Cases.		✓
14. Verfügung stellen des Gutscheinsystems und Einlösemöglichkeiten von Gutscheinen sowie Abwicklung von Kreditkartenzahlungen über Zahlungsdienstleister.	✓	
15. Rechnungstellung (per E-Mail) an den Nutzer	✓	
16. Kostenübernahme für abgebrochene Identifikationen (z.B. Videoidentifikation) sofern diese aufgrund eines fehlerhaften Prozesses bei Swisscom Trust Services erfolgte unter Einhaltung der Mitwirkungsleistungen des Nutzers.	✓	
17. Der Nutzer stellt sicher, dass er seinen ständigen Wohnsitz in der Schweiz, dem EWR oder einem Land der EU hat		✓
18. Eigene Kommunikationskosten des Nutzers zur Inanspruchnahme von Supportdienstleistungen (z.B. Telefon, Porto, etc.)		✓



Tätigkeiten (S = STS/N = Nutzer)	S	N
19. Der Nutzer akzeptiert, dass er keine Anspruch auf eine Registrierung hat. Diese kann aus Risikogründen abgelehnt werden. Die einzige Entschädigung ist hierbei eine Rückzahlung der Kosten, die er für diese Registrierung bezahlt hat. Alternativ kann Swisscom auch einen Gutschein für eine weitere Registrierungsmethode zustellen.		✓
20 Support ausschliesslich per Webform bzw. E-Mail und Versuch der Problembehebung durch Gutschein für alternatives Verfahren, bzw. Rückzahlung. Telefonsupport, persönlicher Support und persönliche Analyse des jeweiligen Problemfalls sind nicht vorgesehen.	✓	

6 Service Level

6.1 Service Level

6.1.1 Gültigkeitszeitraum der zugesandten URL und Wiederholungsversuche

Die Links mit den Weiterleitungen zu den Identifikations Providern, die nach Bezahlung per E-Mail dem Empfänger zugesendet werden, unterliegen Verfallsdaten. Sofern die Identifikation binnen der unten angegebenen Zeit nicht eingelöst wurde oder nach Fehler erneut gestartet wurde, müssen die Identifikationen erneut erworben werden. Die Verfallszeit berechnet sich immer ab Kaufdatum und verlängert sich nach einem Fehlversuch. Es gibt auch ein Maximallimit an Wiederholungen, sollte die Identifikation fehlerhaft sein.

Service Level & Zielwerte	SRS Video EU SRS eID DE	SRS Bank DE	SRS Selfie Ident EU	SRS Video CH	SRS Autoide nt CH
Verfallszeiten in Tagen	90	30	30	90	90
Anzahl Wiederholungen	Kein Limit	5	5	Kein Limit	Kein Limit

6.1.2 Gültigkeit von Gutscheincodes

Es wird eine Gültigkeit von Gutscheincodes für maximal 18 Monate garantiert. Sollten Verfahren während dieser Zeit aus regulatorischen oder betrieblichen Gründen nicht mehr zur Verfügung stehen, so können diese Codes zum anteiligen Preis zurückerstattet werden oder aufgrund besonderer Vereinbarung gegen Gutscheincodes ähnlicher Identifikationsverfahren eingetauscht werden.

6.1.3 Smart Registration Service

Die nachfolgenden Service Levels beziehen sich grundsätzlich auf die vereinbarte Monitored Operation Time. Definitionen der Begriffe (Operation Time, Monitored Operation Time, Support Time, Availability, Security und Continuity) sowie die Beschreibung des Messverfahrens und des Reportings ergeben sich aus dem [Vertragsbestandteil „Basisdokument“](#). Folgende Service Levels werden erbracht. Bei mehreren möglichen Service Levels pro Ausprägung erfolgt die Auswahl des Service Levels im Servicevertrag.

Service Level & Zielwerte			Smart Registration Service
Operation Time			
Monitored Operation Time	Mo-So	00:00-24:00	●
Provider Maintenance Window	PMW-DC	PMW Data Center Swisscom	●
	PMW-S: mit Vorankündigung für sicherheits- und systemkritische Updates	Täglich 19:00-07:00, nur für angekündigte Wartungen	●
Support Time			



Service Level & Zielwerte			Smart Registration Service
Support Time ¹	Mo-Fr	08:00-17:00 ²	●
Störungsannahme	Mo-So	00:00-24:00	●
Availability			
Service Availability			
<ul style="list-style-type: none">Zugang zum Smart Registration Service 99.5%			●
Security			
Siehe Basisdokument			●
Continuity			
Service Continuity (STSSC)	Best Effort		●
	RTO 4 h RPO 1 h		○

● = Standard (im Preis inbegriffen) ○ = Gegen Aufpreis — = Nicht erhältlich

6.1.4 Service Level Partneridentifikationen

Der Service Level der Partneridentifikationen richten sich nach den verschiedenen SLAs der involvierten Partner.

Service Level & Zielwerte		SRS Video EU SRS eID DE	SRS Bank DE	SRS Selfie Ident EU	SRS Video CH	SRS Autoide nt CH
SLA Zeiten						
Operation Time	Mo-So 00:00-24:00		●	●		
	Mo-Sa 07:00-22:00				●	●
	Mo-So 07:00-24:00	●				
Support Time	Mo-Fr 08:00-17:00	●	●	●		
Störungsannahme	Mo-So 00:00-24:00	●	●	●		
Performance						
Call Pickup Rate	80% der Calls werden während der ersten 90 Sekunden angenommen, auf Monatsbasis gemessen	●	—	—		
	90% der Calls werden während der ersten 120 Sekunden angenommen, auf Monatsbasis gemessen	●	—	—		

¹ Wurde der Service über einen Swisscom Partner bezogen so ist dieser grundsätzlich bei Störungen zu kontaktieren. Der Partner wird die Störung an Swisscom weiterleiten, sofern er diese nicht beheben kann.

² Feiertagsregelung siehe "Basisdokument (Kapitel SLA-Definitionen)"



Service Level & Zielwerte		SRS Video EU SRS eID DE	SRS Bank DE	SRS Selfie Ident EU	SRS Video CH	SRS Autoide nt CH
	95% der Calls werden während der ersten 180 Sekunden angenommen, auf Monatsbasis gemessen	●	—	—		
Bearbeitungszeit	Maximale Bearbeitungsdauer Ende Identifikationsdialog bis Einlieferung Evidence: 1 Minute	—	●	—		
	Maximale Bearbeitungsdauer Ende Identifikationsdialog bis Einlieferung Evidence: 20 Minuten	●	—	—		
	Durchschnittliche Bearbeitungsdauer für die Prüfung der Identität: 1-2 Minuten			●		
	Maximale Bearbeitungsdauer Ende Identifikationsdialog bis Einlieferung Evidence: 15 Minute				●	●
Unterstützte Sprachen	D=Deutsch, E=Englisch, F=Französisch, I=Italienisch, K=Kroatisch, S=Spanisch	D,E,F	D,E	D,E	D,E,I,F	Viele Sprachen, mindestens D,E,I,F

● = Standard (im Preis inbegriffen) ○ = Gegen Aufpreis — = Nicht erhältlich

7 Rechnungsstellung und Mengenreport

Der Nutzer erhält per E-Mail im Falle der Kreditkartenzahlung einen Zahlungsbeleg inklusive Höhe der Mehrwertsteuer. Gutscheinkunden erhalten eine Rechnung. Die Preise ergeben sich aus den Preisankündigungen auf der Webseite oder dem Bestellformular für die Gutscheine.

8 Besondere Regelungen

8.1 Austausch der Identifikationspartner

Swisscom behält sich vor die Identifikationspartner für die jeweiligen Services durch gleichwertige Partner mit einem Angebot derselben Prozessabläufe, wie sie in dieser Leistungsbeschreibung zu finden sind, zu ersetzen. Die jeweils eingesetzten Partnerunternehmen sind in der Bestellung benannt.

Swisscom behält sich weiterhin vor den gleichen Identifikationsservice von mehreren Partnern parallel anzubieten.



8.2 Datenbearbeitung durch Dritte aus dem In- oder Ausland, Notfallzugriffe

Die Archivierung der von den Identifizierern übermittelten Identifikationsdaten findet ausschliesslich auf Swisscom Servern in der Schweiz statt. Je nach vom Nutzer gewählter Identifikationsmethode werden im Servicevertrag benannte Identifizierer aus der EU und der Schweiz beigezogen, die die jeweilige Identifikation durchführen. Diese Identifizierer sind im Rahmen der Übertragung der Datenverarbeitung vertraglich zum Datenschutz gemäss DSGVO verpflichtet.

Swisscom schliesst mit den externen Identifizierern eine Vereinbarung zur Auftragsdatenverarbeitung unter der EU Datenschutz-Grundverordnung und Schweizerischem Datenschutzgesetz ab, sofern diese nicht eigenständig als Datenverantwortliche gegenüber der zu identifizierenden Person auftreten.

8.3 Identifikation von Personen mit Wohnsitz ausserhalb EU/EWR/Schweiz

Der Smart Registration Service und die Swisscom Trust Services richten sich an Personen mit Wohnsitz in der EU, dem EWR und der Schweiz, da für Personen mit Wohnsitz ausserhalb dieser Regionen häufig andere rechtliche Bestimmungen (z.B. Konsumentenschutz und Datenschutzrecht) gelten. Es ist optional möglich, Registrierungen auch für Personen ausserhalb der EU, dem EWR und der Schweiz zuzulassen. Hierfür muss diese Möglichkeit explizit optional bestellt werden. Es werden dann die rechtlichen Möglichkeiten geprüft und ggfs. die Nutzungsbestimmungen oder andere Bestimmungen angepasst.