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

Leistungsbeschreibung Registrierungs- und Signaturfreigabemethoden

Swisscom Trust Services

Swisscom Trust Services AG

Konradstrasse 12
8005 Zürich

Switzerland

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

1 Inhalt

2 Übersicht zum Service

Der Smart Registration und Signing Service ist eine serverbasierte Fernsignaturlösung, die nach entsprechender Registrierung und Signaturfreigabe Signaturen mit Signaturzertifikaten der Swisscom IT Services Finance S.E., Wien (AT), nachfolgend "Swisscom ITSF" genannt und der Swisscom (Schweiz) AG und optional ggfs. weiterer Zertifizierungsdienste ermöglicht. Der Smart Registration und Signing Service wird in den Rechenzentren von Swisscom (Schweiz) AG in der Schweiz und Partnern in der EU bereitgestellt und Swisscom Trust Services AG (nachfolgend „Swisscom Trust Services“) vertreibt die Services in eigenem Namen oder räumt Dritten wiederum das Recht ein, die Services in eigenem Namen zu vertreiben.

Der Smart Registration und Signing Service ermöglicht die Integration verschiedener Registrierungs- und Signaturfreigabemethoden, einschliesslich Verfahren von Swisscom Gesellschaften oder Dritten, die im Rahmen dieser Leistungsbeschreibung beschrieben werden.

Die ordnungsgemässe Registrierung berechtigt den Signierenden über eine Teilnehmerapplikation Signaturen zu beziehen. Dafür ist es erforderlich, dass der Signierende einen Vertrag mit einem Anbieter einer Teilnehmerapplikation abschliesst, der die Swisscom Trust Services eingebunden hat. Die Teilnehmerapplikation und die Einbettung in die Fernsignaturlösung wird in einer eigenen Leistungsbeschreibung beschrieben. Swisscom Trust Services verkauft keine Signaturen direkt an Privatpersonen.

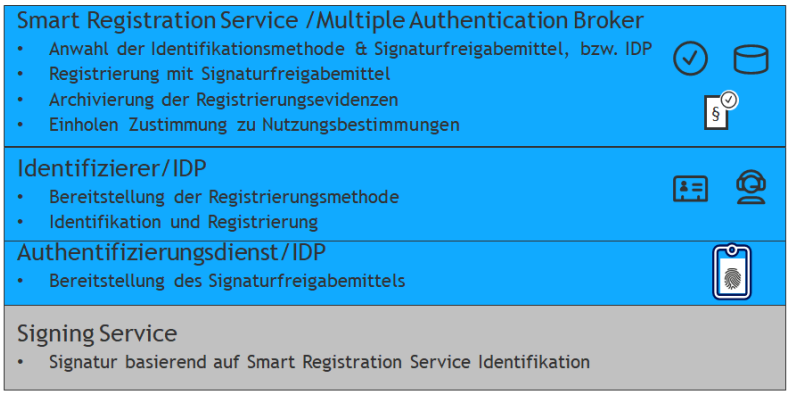
Die Registrierung erfordert eine zertifizierte Signaturfreigabemethode, die später für die Freigabe der Signatur verwendet wird. Dies kann die Mobile ID App sein oder eine Kombination von Passwort und Einmalcode per SMS oder eine andere Signaturfreigabemethode. Wenn eine App oder ein Hardwaretoken verwendet wird, muss dieses in der Regel vorher initialisiert worden sein.

Der Multiple Authentication Broker innerhalb des Smart Registration Service stellt den Signierenden die passenden und regulatorisch korrekten Identifikations- und/oder Signaturfreigabemethode bereit.

Swisscom Trust Services arbeitet mit Partnern zusammen, um die Identifikations- und Signaturfreigabemethoden des Smart Registration Service durchzuführen. Diese Partner werden "Identifikationspartner" genannt, wenn sie nur eine Identifikationsmethode zur Verfügung stellen, die mit einer oder mehreren Signaturfreigabemethoden kombiniert werden kann.

Wenn ein Nutzer sich bei einem Partner mit den von diesem Partner verwalteten Identitätsdaten authentisieren kann und diese Authentisierung später bei der Freigabe von Signaturen genutzt wird, dann wird dieser Partner als "IdP" (Identitätsprovider) bezeichnet. In diesem Fall besteht die Registrierung nur noch aus einer Authentisierung für den Service des IdP und der Akzeptanz der Nutzungsbestimmungen. Ein Beispiel für einen IdP könnte eine Bank sein.

Nach erfolgreicher Durchführung des Identifikationsverfahrens archiviert der Swisscom Zertifizierungs- bzw. Vertrauensdienst – sofern nicht anders vereinbart – die Identifikationsdaten für die gesetzlich vorgeschriebene Dauer und verwaltet die Annahme der Nutzungsbestimmungen des Swisscom Zertifizierungs- und Vertrauensdienstes. Die Signierenden können dann auf Basis des während des Identifikationsverfahrens geprüften Signaturfreigabemethode (z.B. App, IdP-App, Mobilnummer) und bis zum Ablauf der Gültigkeit der Identifikation fortgeschrittene oder qualifizierte elektronische Signaturen erstellen, so dass nicht jedes Mal eine Identifikation notwendig ist.

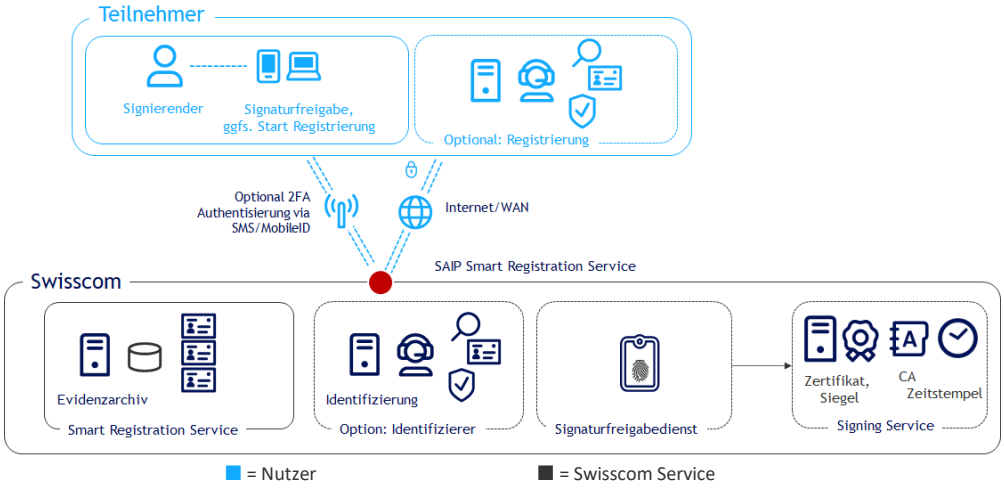


Nutzer der Identifikations- und Signaturfreigabemethode ist entweder der Teilnehmer, der diese im Rahmen des Signaturworkflows für seine Signierende anbietet oder der Signierende, der im Rahmen der Nutzung eines Registrierungsportals von Swisscom Trust Services diese Methoden nutzt.

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 entweder das Registrierungsportal https://srsident.trustservices.swisscom.com, über welches der Nutzer verschiedene Identifikationsverfahren auswählen kann oder der Multiple Authentication Broker des Smart Registration Service, über den die verschiedenen Signaturfreigabemethoden und optional auch Identifikationsverfahren inkl. Registrierung zur Verfügung gestellt werden. Die Verfahren auf dem Registrierungsportal kann man direkt oder mit Gutscheincode bezahlen und danach direkt durchführen.
Je nach Verfahren wird man dann zum. Identifikationspartner weitergleitet, der die Identifikation durchführt, bzw. zum Service für die Signaturfreigabe.
Folgende rein schematische Darstellung dient der Veranschaulichung der Leistungen und Leistungs-Komponenten des Smart Registration Service:



Im Falle des Multiple Authentication Brokers kommuniziert der Nutzer dabei zunächst über Internet mit dem Swisscom Smart Registration Service (SRS) und erhält verschiedene Verfahren zur Signaturfreigabe angeboten. Sollte er nicht registriert sein, wird er weitergeleitet zum Identifizierungsdienstleister. Dieser stellt die Identifizierungsdaten, für den Swisscom Zertifzierungs- und/oder Vertrauensdienst bereit. Sofern SMS oder Mobile ID bei der Signaturfreigabe oder Registrierung verwendet werden, werden diese über die Mobilfunkschnittstelle an das Smartphone des Nutzers übertragen. Mobilfunkdienste, die für die Identifikation und Signaturfreigabe genutzt werden, sowie persönlich installierte Apps oder Passkeys und deren Verfügbarkeit auf dem persönlichen Smartphone oder PC 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 des Reference Guides zum SAIP korrekt beantwortet werden. Die Antwort kann auch eine dokumentierte Fehlermeldung sein.
Die Schnittstellenbeschreibung zum Multiple Authentication Broker befindet sich unter https://trustservices.swisscom.com/downloads unter dem Link „Reference Guide“:
https://documents.swisscom.com/product/filestore/lib/e2007490-6fd4-4012-801d-b104801a9abc/reference_guide_smartregistration_signing-en.pdf?idxme=pex-search sowie Multiple Authentication Broker Integration Guide in der Partner Area:
trustservices.swisscom.com/hubfs/Website Files/Documents/Developer Documentation/MAB-IntegrationGuide-en.pdf
Für Signaturfreigabemethoden, die mobilfunkbasierend sind, werden die Identifikationen historisch bedingt auch offline im Identifikationsportal oder via RA-App (eigene Leistungsbeschreibung) angeboten.

3.2 Servicespezifische Definitionen

Begriff	Beschreibung
2-Faktor (Signaturfreigabe)	Qualifizierte elektronische Signaturen, die über Fernsignaturen angeboten werden oder qualifizierte/geregelte Siegel müssen mit einer Signaturfreigabemethode freigegeben werden, bei dem der Signierende 2 Faktoren anwendet. Diese 2 Faktoren müssen aus den drei Bereichen Besitz, Wissen und Sein (Biometrie) kommen. So z.B. der Besitz einer Mobilnummer oder einer App auf dem Smartphone kombiniert mit dem Wissen um ein Passwort oder einer PIN. Oder alternativ kann auch ein biometrisches Merkmal verwendet werden, wie z.B. ein Fingerabdruck.
Access Token	Das Access Token (oder Zugriffstoken) gibt einem Benutzer den Zugriff auf eine Ressource. Das Token identifiziert ihn gegenüber der Ressource. Im Signaturkontext wird zuvor die Identifikation und Signaturfreigabe sichergestellt. Das daraufhin ausgestellte Token ermöglicht den Nutzer eine Signaturanfrage auszustellen und genehmigt zu bekommen. Im OAuth 2.0 Standard sind sie definiert und können überdies auch noch verschiedene Eigenschaften haben, z.B. eine begrenzte Lebenszeit.
Audit	Konformitätsbewertungsstellen prüfen im Rahmen eines Audits die Konformität des Zertifizierungs- oder Vertrauensdienstes im Zusammenhang mit dem anwendbaren Recht und den anwendbaren Normen.
Anerkennungsstelle	Nach ZertES sind die Anerkennungsstellen für die Anerkennung von Zertifizierungsdiensten zuständig. In der Schweiz ist derzeit die KPMG die einzige Anerkennungsstelle. Das Pendant in der eIDAS Verordnung hierzu ist die Aufsichtsstelle.
Aufsichtsstelle	Nach eIDAS-VO ist eine Aufsichtsstelle damit beauftragt, die Qualifizierung der entsprechenden Vertrauensdienste sicherzustellen und damit die Sicherstellung eines vergleichbaren Sicherheitsniveaus. Sie bedient sich dabei dem Auditbericht der Konformitätsbewertungsstellen. Im Schweizer Signaturgesetz ZertES findet sich das Pendant der Anerkennungsstelle.
CEN/TS 419 241	CEN ist ein europäisches Komitee für Normung, welches mit dem Standard 419 241 einen Standard für Fernsignaturen herausbrachte. In diesem Standard wird unter anderem der Zugriff auf eine Signatur und damit auch die Signaturfreigabe normiert. Er ist im Schweizerischen Signaturrecht verankert und wird auch von verschiedenen Aufsichtsstellen in Europa für die Zulassung von Fernsignaturanbietern eingefordert.
Claimed ID	Die Claimed ID ist das Zugangskonto zum Signing Service des Swisscom Zertifizierungs- und Vertrauensdienstes. Sie besteht aus einem eindeutigen Kennzeichen für den Teilnehmer (z.B. die URL seiner Homepage) und dem Zusatz, welche Zertifikate bei der Signatur verwendet werden.
CH	Abkürzung für Schweiz bzw. Schweizer Rechtsraum.
DSG	Bundesgesetz über den Datenschutz der Schweiz. Die Fassung vom 1. September 2023 ist in grossen Teilen angeglichen an die Datenschutzgesetzgebung der EU (DSGVO).
DSGVO	Datenschutzgrundverordnung der EU. EU-Regulierung zum Datenschutz.
Dokument	Der Begriff Dokument wird, zur besseren Verständlichkeit, synonym für den Begriff Daten benutzt. Es können sowohl Dokumente als auch Daten signiert werden.
eIDAS-VO	Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG); regelt insbesondere auch die elektronische Signatur. Auf nationaler Ebene gibt es typischerweise sogenannte “Umsetzungsgesetze”, die gegebenenfalls noch Aspekte national regeln, die in der Verordnung nicht geregelt wurden. In Österreich ist das das SVG (Signatur- und Vertrauensdienstegesetz), welches z.B. den Aspekt der Archivierungsdauer für Daten regelt.

Begriff	Beschreibung
Elektronische Signatur	Die elektronische Signatur erlaubt die Anwendung eines technischen Verfahrens zur Überprüfung der Integrität eines Dokuments, einer elektronischen Nachricht oder anderer elektronischer Daten sowie der Identität des Signierenden. Sie bedient sich dabei den technischen Möglichkeiten eines Zertifikates.
Elektronisches Siegel	Das elektronische Siegel basiert in technischer Hinsicht auf den genau gleichen Verfahren wie die elektronische Signatur. Elektronisches Siegel sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen. Nach Schweizer Recht sind nur geregelte elektronische Siegel für UID-Einheiten gesetzlich geregelt, nicht hingegen fortgeschrittene elektronische Siegel. In der eIDAS Verordnung sind sowohl qualifizierte als auch fortgeschrittene Siegel gesetzlich geregelt.
ETSI EN 119 432	Protokoll aus 2021 der Standardisierungsorganisation des Europäischen Instituts für Telekommunikationsnormen (ETSI) für den Anschluss einer Signaturapplikation an ein Fernsignatursystem.
ETSI EN 119 461	Europäische Norm zur Konformitätsbewertung von Identifikationsmethoden für Vertrauensdienste.
EU	Abkürzung für Europäische Union und damit den Rechtsraum der Europäischen Union und des Europäischen Wirtschaftsraums (EWR, also Norwegen, Liechtenstein und Island).
Evidenz	Datensammlung, die den Nachweis einer Registrierung und insbesondere auch die Identität eines Signierenden bezeugen kann. Dieser Nachweis kann auch aus einem Verweis auf einen Datensatz (Evidenz) bestehen, die von einer delegierten Registrierungsstelle verwaltet wird.
Identifikationspartner (Standard-)	Anbieter von verschiedenen Standardidentifikationsmethoden, z.B. Videoidentifikation, Autoidentifikation, Identifikation anhand eines Bankkontos, anhand einer eID oder Chip Information auf dem Ausweisdokument.
IdP	Identity Provider: Eine externe Registrierungsstelle, die eine Identität einer Person bestätigt typischerweise durch eine Authentisierung und Abgleich mit einer Identitätsdatenbank. Das Authentisierungsverfahren kann später auch zur Signaturfreigabe genutzt werden. Im Smart Registration Service kommuniziert der IdP mit dem Multiple Authentication Broker. Der Authentication Broker erfährt nach der Registrierung aus der RA / Evidenz-Datenbank, für welche Signierende welcher IdP zuständig ist. Sofern der IdP sich bei der Authentisierung auf bereits vorhandene Identitätsprüfungen stützen kann, die auditiert für die elektronische Signatur verwendet werden dürfen, erfolgt auch die Registrierung mit einer erstmaligen Authentisierung und Akzeptanz der Nutzungsbestimmungen. Beispiel: eine Bank. Ein IdP kann aber auch nur das Authentisierungsmittel als Signaturfreigabemethode zur Verfügung stellen und dieses koppeln lassen mit den Ergebnissen eines Identitätsprüfers.
Lebenderkennung	Mit der Lebenderkennung oder dem Liveness Test wird festgestellt, dass eine Videosession tatsächlich von einer lebendigen Person vor Ort durchgeführt wird und nicht durch ein voraufgezeichnetes Video eine Person vorgetäuscht wird. Dies geschieht typischerweise durch zufällige Anweisungen an den Nutzer in der Videosession, die er befolgen muss.
Mobile ID	Managed Service für die sichere Benutzer-Authentisierung. Mobile ID kann von verschiedenen Providern, unter anderem Swisscom (Schweiz) AG, bezogen werden.
Mobile ID App	Managed Service App (Applikation), die vom Google Play Store oder Apple Store herunter geladen werden kann zur sicheren Benutzer-Authentisierung. Diese basiert auf Authentisierungsmöglichkeiten des Mobilgerätes wie z.B. Fingerprint oder Face Recognition. Die Mobile ID App wird über eine internationale Mobilnummer initialisiert und funktioniert mit einer laufenden Internetverbindung.

Begriff	Beschreibung
Multiple Authentication Broker	Interne Komponente im Smart Registration Service, welche sämtliche Kommunikation nach aussen in Bezug auf Registrierung und Signaturfreigabe sicherstellt und koordiniert welche Gestützt auf die Logik der Registrierungsstelle und ihrer RA Datenbank entscheidet der Multiple Authentication Broker, welche Signaturfreigabemethode, bzw. welcher externer IdP für die Signaturfreigabe angesprochen werden muss. Er stellt die Signaturfreigabedurchführung sicher – ggfs. durch Aufruf einer Registrierung für nicht registrierte Signierende. Nach erfolgter Signaturfreigabe ermöglicht der Broker dem Teilnehmer den Bezug eines Zugangstoken, um die Signatur beim Signing Service anzufragen.
NFC	Near Field Communication (NFC) ist eine drahtlose Kommunikation, die z.B. ein Smartphone mit einem Ausweisdokument herstellen kann, welches einen Chip beinhaltet. Damit können über ein gesichertes Protokoll die Ausweisdaten direkt ausgelesen werden, indem das Dokument an die Rückseite des Smartphones gehalten wird, wo sich typischerweise der NFC Leser befindet.
Nutzer	Swisscom Trust Services erbringt die Leistungen gemäss vorliegender Leistungsbeschreibung zu Gunsten des Nutzers. Der Nutzer ist entweder direkt Kunde von Swisscom Trust Services mit einem Smart Registration & Signing Vertrag (inklusive Annahmeerklärung gegenüber Swisscom (Schweiz) AG), einem Voucher Vertrag, einem kommerziellen Vertrag mit einem Reseller von Swisscom Trust Services oder er nutzt direkt das Registrierungsportal, das Swisscom Trust Services auf seinem Webauftritt anbietet.
Nutzungsbestimmungen (Subscriber Agreement)	Bestimmungen, die - gesetzlich vorgeschrieben - jeder Nutzer vor Zusammenarbeit mit einem Vertrauens- oder Zertifizierungsdienst akzeptieren muss. Sie müssen nicht unbedingt signiert werden, aber die Akzeptanz muss im Rahmen der Registrierung nachweisbar sichergestellt werden. Die Nutzungsbestimmungen regeln im direkten Verhältnis zwischen Swisscom (Schweiz) AG und dem Signierenden bzw. der Swisscom ITSF und dem Signierenden auf einer Teilnehmerapplikation die Bedingungen für die Nutzung der Signaturzertifikate und Signaturdienstleistung. Diese sind unter https://trustservices.swisscom.com/repository/ abrufbar..
OAuth	OAuth 2.0 steht für Open Authorization und ist ein Standard, mithilfe dessen eine Website oder Anwendung auf Ressourcen zugreifen kann, die von einem anderen Service angeboten werden. Es ist der massgebliche Branchenstandard für die Online-Autorisierung.
One-shot Signing	Sofern ein Signierender nicht häufig signiert, kann der Signaturprozess auch so aufgesetzt werden, dass in einer Sitzung die Identifikation und Signaturfreigabe erfolgt ohne den Einsatz eines Signaturmittels. Nachteil ist, dass der Signierende sich für die nächste Signatur wiederum identifizieren muss.
Open ID Connect	Ist eine Authentifizierungsschicht, die auf dem OAuth 2.0 Framework basiert und dazu dient, die Identität eines Nutzers mit Hilfe von Authentifizierungsserver zu überprüfen, beispielweise über einen IdP. Der Standard wird von der OpenID Foundation herausgegeben.
OTP	Einmalcode, der für eine einfache Nutzung via SMS an ein Mobilfunkgerät übertragen wird. Damit wird der Faktor „Besitz“ eines Mobilfunkgerätes mit der angegebenen Mobilnummer überprüft.
PAR	Die Pushed Authentication Request OAuth 2.0 Erweiterung beschreibt eine Technik, mit der ein OAuth-Flow aus dem Rückkanal heraus initiiert werden kann, anstatt eine URL zu erstellen. Diese bietet bessere Sicherheit und mehr Flexibilität bei der Erstellung komplexer Autorisierungsanfragen. Der Standard ist in RFC 9126 beschrieben.
Personensignatur	Signaturen durch natürliche Personen im Gegensatz zu Siegeln.
PWD	Password (-eingabe), für die Authentisierung am Service oder Signaturfreigabe zu verwendendes Password, welches den Faktor «Wissen» bietet.
QR Code	Der "Quick Response" Code ist ein zweidimensionaler Code, der von der japanischen Firma Denso Wave im Jahr 1994 entwickelt wurde und heute Standard ist für eine Prozessauslösung auf dem Smartphone.
RA	Registration Authority - Registrierungsstelle

Begriff	Beschreibung
RA-Agent	Autorisierter Bediener der RA-App
RA-Agentur	Organisation, die die RA-Agenten stellt
RA-App	App (Applikation), die im Store von Android oder iOS heruntergeladen wird. Diese ermöglicht einem ausgebildeten RA-Agenten die Identifikation für fortgeschrittene und qualifizierte Signaturen und überträgt die Daten an den RA-Service der Swisscom Trust Services. Die RA-Agenten arbeiten hier im Auftrag der Registrierungsstelle des Swisscom Zertifizierungs- und Vertrauensdienstes.
RA-Service	Service zur Entgegennahme und Archivierung der Evidenzen, Betrieb in Zusammenhang mit der RA App
Registrierungsstelle (RA), RA-Stelle	Interne oder (teilweise) externe delegierte Stelle, die die Registrierung übernimmt.
Registrierung	Eine Registrierung besteht immer aus einer Identifizierung, Akzeptanz der Nutzungsbestimmungen und Zuweisung und Überprüfung einer Signaturfreigabemethode.
Schlüssel	Eine elektronische Signatur stützt sich zunächst auf ein Schlüsselpaar, welches im HSM erzeugt wird. Des Weiteren wird vom Dokument ein Hash gebildet. Dieser Hash wird mit dem privaten Schlüssel verschlüsselt, so dass er später mit dem öffentlichen Schlüssel entschlüsselt werden kann. Die Signaturprüfung erfolgt dann umgekehrt: Es wird wiederum ein Hash vom Dokument gebildet. Mit dem öffentlichen Schlüssel wird der verschlüsselte Hash entschlüsselt und überprüft, ob er mit dem frisch gebildeten Hash des Dokumentes übereinstimmt. Ist das nicht der Fall, wurde das Dokument entweder verändert, oder der öffentliche Schlüssel passt nicht zum privaten Schlüssel, d.h. das Dokument wurde von jemandem anders signiert.
Signaturart	Bezeichnung für die in den Regularien definierten Arten der elektronischen Signatur: fortgeschritten oder qualifiziert/geregelt.
Signaturzertifikat bzw. Siegelzertifikat	Zertifikat, welches auf den Signierenden bzw. den Siegelersteller ausgestellt ist, von den Swisscom Zertifizierungs- und Vertrauensdiensten treuhänderisch verwaltet wird und zur Signatur bzw. Siegelerstellung verwendet wird.
Signaturfreigabemethode oder Signaturfreigabemethode	technisch gesehen ein Authentifizierungsmittel oder eine Methode, die während der Registrierung geprüft wurde. Es stellt mittels 1-Faktor (fortgeschritten) oder 2 unterschiedliche Faktoren aus zwei von drei Typen (Besitz, Wissen, Biometrie) (qualifiziert) die während der Registrierung geprüfte Identität sicher. Es wird dazu verwendet, dass der Signierende den alleinigen Zugriff auf den Schlüssel des Signaturzertifikates hat („sole control“ oder SCAL). Mit SCAL2 wird eine alleinige Zugriffskontrolle basierend auf 2 Faktoren beschrieben, mit SCAL1 eine Zugriffskontrolle mit einem Faktor. Mit der Signaturfreigabe bekundet der Signierende seinen Willen zur Signatur. SCAL 1 und SCAL 2 sind in CEN/TS 419 241 definiert
Signierender	Natürliche Person, die bei vorgängiger Identifikation und Signaturfreigabe ein Dokument elektronisch signiert.
Signing Service	Teil des Service, der basierend auf den Standard ETSI EN 119 432 die Signatur, das Siegel oder den Zeitstempel auf den Hash eines Dokumentes aufbringt, sofern die Anfrage hierzu auf einem Access Token basiert, welches der Smart Registration Service über den Multiple Authentication Broker bereitgestellt hat.
Smart Registration Service	Service von Swisscom Trust Services, der die Signaturfreigabe steuert und verwaltet, sowie die Evidenzen archiviert und Informationen über die Signaturfreigabe und Registrierung aus der RA-Datenbank bereitstellt. Nach aussenhin kommuniziert der Smart Registration Service über den Multiple Authentication Broker und über die Import Schnittstelle der RA Datenbank. Im Rahmen der Signatur bietet der Smart Registration Service die regulatorisch passenden Signaturfreigabemethode an und optional auch die passenden Registrierungsverfahren, sofern ein Signierender nicht registriert ist. Er greift dabei auch auf externe IdP und Services zurück. Über die Kommunikation mit dem Multiple Authentication Broker wird für Personensignaturen das Access Token für die Signaturanfrage am Signing Service zur Verfügung gestellt.

Begriff	Beschreibung
Store (Registrierungsmethoden oder Signaturfreigabemethoden)	Im Laufe des Signaturworkflow können – optional - im Rahmen eines Webview die verschiedenen regulatorisch passenden Möglichkeiten für eine Signaturfreigabe und/oder Registrierung angeboten werden, sofern diese nicht schon vorab bekannt sind. Die Auswahl erfolgt in einem von Swisscom Trust Services angebotenen Fenster («Store») im Rahmen eines Webviews. Alle Methoden des Stores können alternativ auch über eine OAuth 2.0 PAR-Schnittstelle angesprochen werden.
Teilnehmer	Swisscom Trust Services erbringt die Leistungen gemäss vorliegender Leistungsbeschreibung zu Gunsten des Teilnehmers. Der Teilnehmer ist entweder direkt Kunde von Swisscom Trust Services mit einem Signing Service Vertrag (inklusive Annahmeerklärung gegenüber Swisscom (Schweiz) AG) oder er hat einen kommerziellen Vertrag mit einem Wiederverkäufer der Swisscom Trust Services Leistung mit einer Annahmeerklärung gegenüber Swisscom (Schweiz) AG. Sofern im Falle von Siegelapplikationen aufgrund der fehlenden Einzelsignaturfreigaben der Teilnehmer nicht identisch mit dem Siegelersteller ist, benötigt der Teilnehmer eine Autorisierung dadurch, dass der Siegelersteller das Zugangszertifikat Swisscom Trust Services elektronisch zusendet oder übergibt, oder das vom Teilnehmer autorisierte Zugangszertifikat Swisscom Trust Services gegenüber akzeptiert.
Teilnehmerapplikation	Der Teilnehmer gibt den Signierenden und Signaturerstellern Zugang zu einer Applikation, mit der sie elektronische Signaturen, Siegel und Zeitstempel gemäss den Nutzungsbestimmungen von Swisscom (Schweiz) AG bzw. Swisscom ITSF erstellen können und der Teilnehmer stellt dabei neben der Authentisierung die Übertragung der Signaturdaten zum Fernsignaturservice der Swisscom Zertifizierungs- und Vertrauensdienste sicher ("Teilnehmerapplikation"). Die Teilnehmerapplikation nimmt die signierten Daten (Hash) entgegen und bereitet für den Signierenden das Dokument auf. Der Smart Registration & Signing Service bietet eine Schnittstelle, die mit einer Teilnehmerapplikation zur Auslösung der Signatur verbunden wird. Die Teilnehmerapplikation ist nicht Bestandteil dieser Leistungsbeschreibung, sie wird ausserhalb des Signing Service z.B. durch Partner bereitgestellt.
Token	Siehe Access Token.
Umsetzungskonzept	Im Falle von kundeneigenen Identifikationsmethoden für die Registrierung oder im Falle der Verwendung kundeneigener Signaturfreigabemethoden für die Signaturfreigabe müssen diese Methoden und weitere regulatorisch relevante Punkte in einem Umsetzungskonzept beschrieben und von Swisscom Trust Services freigegeben werden. Das Umsetzungskonzept dient auch als Grundlage für die Beantragung des Audits dieser Methoden.
URL	Uniform Resource Locator bezeichnet typischerweise die http(s) Adresse, die im Browser für eine Webseite aufgerufen wird.
Vertrauensdienst	In der eIDAS Verordnung verwendeter Begriff für den Anbieter von vertrauenswürdigen Signaturen, Siegel und Zeitstempel sowie Zertifikaten. Im Schweizer Signaturgesetz wird analog der Begriff der «Anbieterin von Zertifizierungsdiensten» gebraucht.
WebAuthn	WebAuthn ist ein vom World Wide Web Consortium (W3C) unter enger Einbeziehung der FIDO-Allianz im Rahmen des FIDO2-Projekts veröffentlichter Standard für eine Programmierschnittstelle (API), mit der Benutzer von Webanwendunge eine direkte Authentifikation mittels Public-Key-Verfahren im Webbrowser nutzen können.
Webview	Mit Hilfe eins Webviews wird eine Ansicht gezeigt oder in einer App/Anwendung eingebettet, die Webinhalte – in diesem Fall von Swisscom Trust Services – anzeigt.
ZertES	Schweizerisches Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate
Zertifikat	Das Zertifikat ordnet den öffentlichen Schlüssel einem Inhaber zu, z.B. einem Signierenden oder einem Siegelersteller. Ein Zertifizierungs- oder Vertrauensdienst überprüft den Inhaber und signiert selber diese Zuordnung. Das Zertifikat ist einem Wurzelzertifikat zugeordnet, welches dem Zertifizierungs- oder

Begriff	Beschreibung
	Vertrauensdienst gehört und in allen Validierungen als vertrauenswürdig eingestuft wird.
Zertifizierungsdienst	Im Schweizer Signaturgesetz ZertES genutzter Begriff für Bereitstellung von Signaturen, Siegel, Zeitstempel inklusive der Zertifikate. Der Vertrauensdienst ist dabei der Anbieter von Zertifizierungsdiensten.
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

4.1 Zugänge zu den Registrierungsverfahren und/oder Siganturfreigabemethoden

Die Registrierungsverfahren werden über mehrere Zugänge zur Verfügung gestellt:

Standardausprägung	Angebot
Registrierungsportal: Die zu identifizierende Person besucht die Webseite https://srsident.trustservices.swisscom.com und wählt das passende Verfahren für die Registrierung gegen Einlösung eines Gutscheincodes oder gegen Bezahlung mit Kreditkarte. Die Registrierungsportallösung ist weiter unten beschrieben.	●
Zugang zu den Stores: Parallel gibt es das Konzept der sogenannten "Stores" bei denen die Verfahren direkt im Signaturflow angeboten werden. Die ausgewählten Verfahren, mit denen sich ein Signierender registrieren kann, werden für den Kunden jeweils nach Bestellung konfiguriert. Mit den Verfahren im Store können auch andere Signaturfreigabemethoden genutzt werden, die nicht mobilfunkgestützt sind.	●

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

Darüber hinaus gibt es noch die Möglichkeit, offline eine Identifikation über RA-App durchzuführen. Diese ist ein einer eigenen Leistungsbeschreibung beschrieben. Die RA-App wird auch in zahlreichen Swisscom Shops und anderen Vor-Ort Identifikationsstellen genutzt.

4.2 Registrierungsverfahren

Im Folgenden sind alle Identifikations- und Registrierungsverfahren tabellarisch gelistet:

- Standardausprägung: Methode des eingesetzten Verfahrens
- Partner: Partner der Swisscom Trust Services, die diesen Service als delegierte Identifikationspartner/Registrierungsstelle der Swisscom Trust Services bereitstellen
- Gültig: Maximaler Gültigkeitszeitraum in Jahren (J). Verfahren, die während der Registrierung auf Identifikationsdokumente zurückgreifen, bestimmen die maximale Gültigkeit bis zu diesem Zeitraum an Jahren, oder kürzer, sofern das vorgelegte Identifikationsdokument vorher abläuft. Ein Ausweisdokument wird als gültig angesehen, sofern der Datumsaufdruck auf dem Dokument diese Gültigkeit dokumentiert. Sonderdekrete oder Gesetze aus einigen nationalen Staaten, die auch abgelaufene Ausweise als gültig deklarieren, können nicht anerkannt werden.
- Rechtliche Einschränkung für Signaturtyp: Zulassung des Verfahrens im Einsatz für die Qualifizierte Elektronische Signatur (QES) oder Fortgeschrittene Elektronische Signatur (FES) im Rechtsraum der eIDAS Verordnung (EU) oder im Rechtsraum Schweiz (CH)
- Sprachen: Sprachführungen in den Sprachen: D=Deutsch, E=Englisch, F=Französisch, I=Italienisch, PL=Polnisch

Die Verfahren werden wie folgt angeboten:

- Über das Identifikationsportal auf der Homepage ("Portal").
- Über den Store je nach Bestellung und Konfiguration ("Store").

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. Pro ClaimedID können verschiedene Verfahren während des Setups konfiguriert werden.

Standardausprägung	Partner	Gültig	Hinweise	Rechtsraum Sprachen	Portal / Store
Bestätigung der Nutzungsbestimmungen	Swisscom (Schweiz) AG und Swisscom IT Services Finance S.E., Österreich			EU: QES/FES CH: QES/FES EU: D,E CH: D,E,I,F	●
Standard-Identifikationspartner					
Videoidentifikation, App basiert	IDNow GmbH, Deutschland	5J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores **Über Portal:** nur Mobile ID, Mobile ID App oder PWD/OTP als Signaturfreigabe	EU: QES/FES CH: FES D, E	○ (Store, Portal)
		Zugelassene Dokumente unter: https://go.idnow.de/bafin2017/documents			
eID-Identifikation (Deutschland), App basiert	IDNow GmbH, Deutschland	5J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores **Über Portal:** nur Mobile ID, Mobile ID App oder PWD/OTP als Signaturfreigabe	EU: QES/FES CH: FES D, E	○ (Portal)
		Zugelassene Dokumente unter: Deutscher Personalausweis, Deutscher Aufenthaltstitel oder Unionsbürgerkarte			
Autoidentifikation, Browser basiert	Fidentity AG, Schweiz	2J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores	EU: QES/FES CH: QES/FES	○ (Store)
		Zugelassene Dokumente unter: https://fidentity.ch/fidentity/wp-content/uploads/2023/11/List-of-allowed-documents-v13_neu.pdf			
NFC-Identifikation, Browser basiert	Fidentity AG, Schweiz	2J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores	EU: QES/FES CH: QES/FES D, E, F, I	○ (Store)
		Zugelassene Dokumente unter: https://fidentity.ch/fidentity/wp-content/uploads/2023/11/List-of-allowed-documents-v13_neu.pdf			
Autoidentifikation, App basiert	Nect GmbH, Deutschland	2J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores **Über Portal:** nur Mobile ID, Mobile ID App oder PWD/OTP als Signaturfreigabe	EU: QES/FES CH: FES D, E	○ (Portal)
		Zugelassene Dokumente unter: https://nect.com/support/faqcontent/documents/general?			
Videoidentifikation, App basiert	Intrum AG, Schweiz	5J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores **Über Portal:**	EU: FES CH: QES/FES D, E, F, I	○ (Portal, Store)

Standardausprägung	Partner	Gültig	Hinweise	Rechtsraum Sprachen	Portal / Store
			nur Mobile ID, Mobile ID App oder PWD/OTP als Signaturfreigabe		
		Zugelassene Dokumente unter https://go.online-ident.ch/swisscomsrsch/documents			
Autoidentifikation, App basiert	Intrum AG, Schweiz	2J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores **Über Portal:** nur Mobile ID, Mobile ID App oder PWD/OTP als Signaturfreigabe	EU: FES CH: QES/FES D, E, F, I	○ (Portal, Store)
		Zugelassene Dokumente unter https://go.online-ident.ch/swisscomsrsch/documents			
Autoidentifikation, App basiert	ti&m AG, Schweiz	2J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores	EU: QES/FES CH: QES/FES D, E, F, I	○ (Store)
		Alle ICAO 9303 Identifikationsdokumente, die gemäss ZertES zugelassen sind.			
NFC-Identifikation, App basiert	ti&m AG, Schweiz	2J	**Über Store:** alle Signaturfreigabeverfahren des Signaturfreigabe-Stores	EU: QES/FES CH: QES/FES D, E, F, I	○ (Store)
		Alle ICAO 9303 Identitätsdokumente, die gemäss ZertES zugelassen sind und aus denen der Chip ausgelesen werden kann (www.icao.int)			
Kundeneigene Identifikation	Nutzer, bzw. Bereitsteller des IDP	Nur nach Akzeptanz eines Umsetzungskonzeptes durch Swisscom Trust Services und Freigabe durch die Konformitätsbewertungsstelle und Aufsichtsstelle. Gültigkeit und Umfang werden im Umsetzungskonzept vereinbart.			○ (Store)
IdP-Identifikationen					
IdP-Identifikation mit Postfinance App	Postfinance AG, Schweiz	1J	Nur in Verbindung mit der Signaturfreigabemethode der Postfinance für Postfinance Kunden	CH: QES/FES D, E, F, I	○ (Store)
Kundeneigener IDP	Nutzer, bzw. Bereitsteller des IDP	Nur nach Akzeptanz eines Umsetzungskonzeptes durch Swisscom Trust Services und Freigabe durch die Konformitätsbewertungsstelle und Aufsichtsstelle. Gültigkeit und Umfang werden im Umsetzungskonzept vereinbart.			○ (Store)
Weitere Leistungen					
Nutzung des Self-Service Portals	Swisscom (Schweiz) AG		nur Mobile ID, Mobile ID App oder PWD/OTP als Signaturfreigabe	D, E	○ (SRS)
Darstellung der Registrierungsverfahren im Store mit Swisscom Views	Swisscom (Schweiz) AG		Von Swisscom konfigurierte Views zur Auswahl der bestellten und konfigurierten Registrierungsmethoden werden angeboten. Preise werden nicht angezeigt.	D, E	○ (Store)
Einbindung der Registrierungsmethoden des Stores im eigenen Look & Feel (UX)	Teilnehmer		Teilnehmerspezifisches UX für die Darstellung der gewählten Registrierungsmethoden über die OIDC-PAR Schnittstelle, z.B. auch zur preislichen Auszeichnung der verschiedenen Verfahren.	N/A	○ (Store)

● = Standard (im Preis inbegriffen) ○ = Gegen Aufpreis nur im SRS, nur im Store oder im SRS und Store erhältlich.

Verfahren die mit dem veralteten SRS Service von Swisscom Trust Services können weiterhin genutzt werden in Verbindung mit den Signaturfreigabemethoden Mobile ID und Passwort / Einmalcode.

4.3 Signaturfreigabemethoden

Im Folgenden sind alle Signaturfreigabemethoden tabellarisch gelistet. Diese müssen bereits während der Registrierung mindestens einmal verwendet bzw. überprüft worden sein:

- Standardausprägung: Charakter des eingesetzten Verfahrens
- Partner: Partner der Swisscom Trust Services, die diesen Service als delegierten Signaturfreigabeservice der Swisscom Zertifizierungs- und Vertrauensdienste bereitstellt
- Rechtliche Einschränkung für Signaturtyp: Zulassung des Verfahrens im Einsatz für die Qualifizierte Elektronische Signatur (QES) oder Fortgeschrittene Elektronische Signatur (FES) im Rechtsraum der eIDAS Verordnung (EU) oder im Rechtsraum Schweiz (CH)
- Sprachen: Sprachführungen in den Sprachen: D=Deutsch, E=Englisch, F=Französisch, I=Italienisch

Die Signaturfreigabemethoden werden im Store während des Signaturflusses je nach Bestellung und Konfiguration angeboten. Sofern nicht in den Hinweisen anders angegeben, können die Verfahren im Store auch nur mit den Identifikationsverfahren im Store eingesetzt werden. Pro ClaimedID können verschiedene Verfahren während des Setups konfiguriert werden.

Standardausprägung	Partner	Hinweise	Rechtsraum Sprachen	Store
Standard-Signaturfreigabemethoden in Verbindung mit Standard-Identifikation:				
Passwort / Einmalcode via SMS	Swisscom (Schweiz) AG	Nur in Ländern mit SMS-Empfang und Roaming Abkommen mit CH/Deutschland Einsetzbar mit allen Store und Portal Identifikationen, bzw. RA-App/Shop	EU: QES/FES CH: QES/FES D, E, F, I	○ (Store, Portal, RA-App)
Einmalcode via SMS	Swisscom (Schweiz) AG		EU: FES CH: FES D, E, F, I	○ (Store, Portal)
Mobile ID	Swisscom (Schweiz) AG		EU: QES/FES CH: QES/FES D, E, F, I	○ (Store, Portal, RA-App)
Mobile ID App	Swisscom (Schweiz) AG		EU: QES/FES CH: QES/FES D, E, F, I	○ (Store, Portal, RA-App)
Swisscom Signaturfreigabe App	Swisscom (Schweiz) AG	In Verbindung mit Store Identifikationen.	EU: QES/FES CH: QES/FES D, E, F, I	○ (Store)
Passkeys	Android, Apple, Microsoft, yubikey und andere FIDO Allianz Mitglieder	In Verbindung mit Store Identifikationen.	EU: QES/FES CH: QES/FES Alle lokalen Sprachen	○ (Store)
Signaturfreigabe SDK	Swisscom (Schweiz) AG in Verbindung mit Futurae AG	Konfigurierbares SDK für eine App-gesteuerte Signaturfreigabe (Biometrie/PIN) im Rahmen einer eigenen App, z.B. zur Kontoführung. In Verbindung mit Store Identifikationen.	EU: QES/FES CH: QES/FES Sprache konfigurierbar	N/A
Kundeneigene Signaturfreigabe methode	Nutzer, bzw. Bereitsteller des IDP	Nur nach Akzeptanz eines Umsetzungskonzeptes durch Swisscom Trust Services und Freigabe durch die Konformitätsbewertungsstelle und Aufsichtsstelle. Gültigkeit und Umfang werden im Umsetzungskonzept vereinbart.		○ (Store)

Standardausprägung	Partner	Hinweise	Rechtsraum Sprachen	Store
Fasttrack Verfahren	Swisscom (Schweiz) AG	Diese Methode greift auf die gesetzliche Regelung zurück, dass alls Schweizer Mobilnummern nur nach Identifikation des Mobilfunkanschlussinhabers vergeben werden können. Es können nur FES innerhalb der Schweiz ausgestellt werden, diese Signaturen beinhalten nur die Mobilnummer.	CH: FES	○ (Store)
Signaturfreigaben durch den IdP:				
Authentisierung mit Postfinance App	Postfinance AG, Schweiz	Nur in Verbindung mit einer Registrierung beim gleichen IdP	EU: FES CH: QES/FES D, E, F, I	○ (Store)
Einmalsignaturen ohne Freigabeverfahren:				
Freigabe durch eine Store Identifikationsmethode aus Ziffer 4.2	Jeweiliger Anbieter aus 4.2	Die Signaturfreigabe geschieht in der gleichen Sitzung wie die Identifikation und Bestätigung der Nutzungsbestimmungen. Die Anwendung einer besonderen Signaturfreigabemethode entfällt. Der Nutzer muss bei einer weiteren Signatur sich wieder neu registrieren lassen.	EU: FES CH: QES/FES D, E, F, I	○ (Store)
Sonstige Leistungen:				
Darstellung der Signaturfreigabeverfahren im Store mit Swisscom Views	Swisscom (Schweiz) AG	Von Swisscom konfigurierte Views zur Auswahl der bestellten Signaturfreigabemethoden werden angeboten. Preise werden nicht angezeigt.	D.E	○ (Store)
Einbindung der Signaturfreigabemethoden des Stores im eigenen Look & Feel (UX)	Teilnehmer	Teilnehmerspezifisches UX für die Darstellung der gewählten Signaturfreigabemethoden über die OIDC-PAR und/oder CIBA-Schnittstelle, z.B. auch zur preislichen Auszeichnung der verschiedenen Verfahren.	N/A	○ (Store)

● = Standard (im Preis inbegriffen) ○ = Gegen Aufpreis im Store erhältlich.

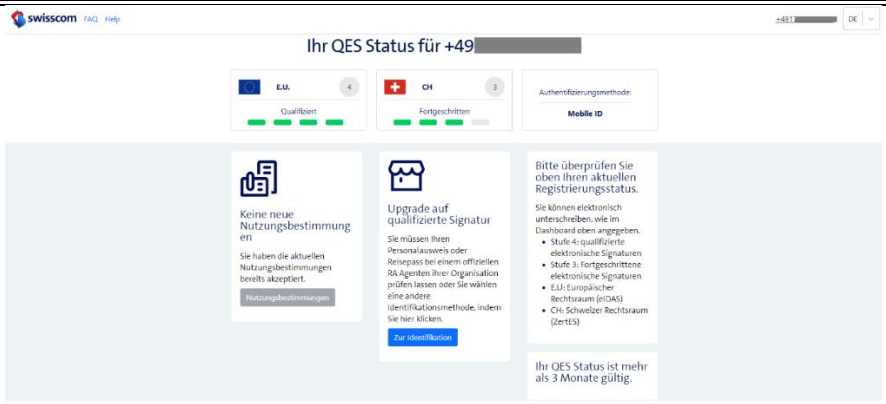
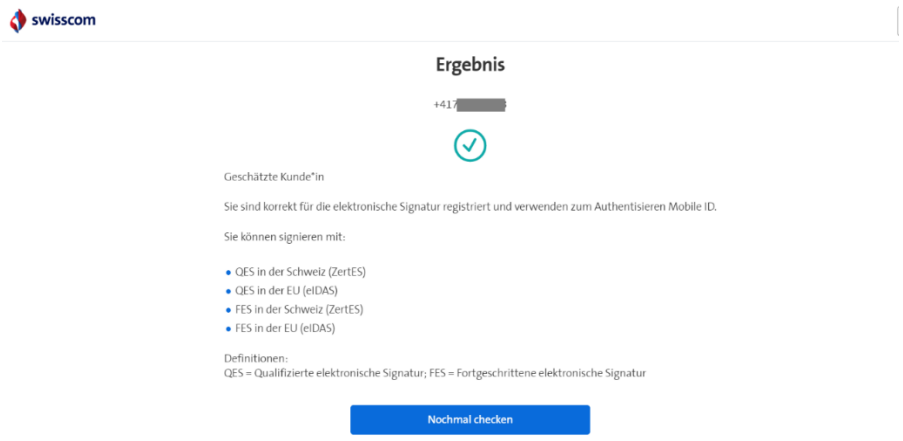
4.4 Definition der Leistungsausprägungen und Optionen

Nachfolgend werden mögliche zugelassene Verfahren erläutert. Nur die im Bestellformular oder Vertrag benannten Verfahren sind auch bestellbar, bzw. werden durch einen Identifikationspartner zum Zeitpunkt der Bestellung angeboten.

Leistungsausprägung/ Option	Definition
Akzeptanz der Nutzungsbestimmungen	Im Vorfeld der Registrierung müssen die Nutzungsbestimmungen der Swisscom Trust Services akzeptiert werden. Der Signierende hat die Möglichkeit, die Nutzungsbestimmungen der Swisscom (Schweiz) AG und/oder der Swisscom IT Services Finance S.E. einzeln oder direkt für beide Rechtsräume zu akzeptieren. Die Nutzungsbestimmungen gelten jeweils für sowohl fortgeschrittene als auch qualifizierte elektronische Signaturen. Die Bestätigung der Nutzungsbestimmungen erfolgt: • Entweder im Registrierungsprozess selbst, wo die entsprechenden Nutzungsbestimmungen angezeigt werden, und mit Häkchen bestätigt werden müssen. Hierzu bietet Swisscom Trust Services oder ein Identifizierungspartner einen "Webview" an, den eine Teilnehmerapplikation in ihren Workflow einbetten kann. • Oder im Falle einer Identifikation via Portal oder RA-App im Nachgang zur Registrierung durch Zusendung einer SMS mit einer URL zu einer Webseite, auf der die Bestätigung stattfinden muss. Diese SMS wird von Swisscom Trust Services ausgesendet, nachdem die Evidenzen der Registrierung eingeliefert wurden und zuvor keine Nutzungsbestimmungen bestätigt wurden. • Oder im Self-service Portal https://smart-flow.trustservices.swisscom.com/ auf der nach Prüfung der

Leistungsausprägung/ Option	Definition
	Mobilnummer die Nutzungsbestimmungen für Mobilnummer gestützte Signaturfreigabemethode geprüft werden können
Videoidentifikation, App basiert	Mit der Videoidentifikation erhält der Nutzer eine URL auf eine Webseite und einen Verweis auf eine App (QR-Code), die er herunterladen und auf seinem Smartphone installieren muss. Mit der installierten App nimmt er einen weiteren QR-Code auf der Webseite an oder gibt die vorgegebenen Parameter zum Start des Identifikationsvorganges ein. Ggfs. sind noch weitere Daten (z.B. Name) vorab einzugeben. Dann startet der Videoidentifikationsdienst mit einem Operator, der im Dialog den Nutzer durch den Vorgang durchführt. Hierfür ist es notwendig, ein Smartphone mit Kamera zu haben. Im Rahmen einer Websession muss die zu identifizierende Person benutzergeführt durch einen Operator des Video-Identifikationspartners ihren Ausweis zeigen und Fragen zur Bestätigung der Ausweisdaten beantworten und die Lebenderkennung nachweisen. Anschliessend werden die so ermittelten Daten an den Swisscom Zertifizierungs- und Vertrauensdienst übertragen.
eID-Identifikation, App basiert	Der Nutzer erhält eine URL zu einer Webseite, auf der er gebeten wird, eine App auf seinem Android oder Apple Smartphone zu installieren und zu nutzen, mit welchen folgenden Schritten durchgeführt wurden: - Foto der Vorder- und Rückseite des deutschen Personalausweises oder eines elektronischen deutschen Aufenthaltstitels/eID Card mit eID-Funktion - Der Ausweis wird an die NFC-Schnittstelle des Smartphones gehalten und über NFC wird die Chipinformationen des Ausweisdokumentes ausgelesen - Die Mobilnummer wird bestätigt mittels eines Einmalpasswortes, welches per SMS übergeben wird. Der Ergebnisdatensatz der Identitätsprüfung wird dann dem Swisscom Zertifizierungs- und Vertrauensdienst zur Verfügung gestellt.
Autoidentifikation, App basiert	Die zu identifizierende Person wird zu einer Webseite weitergeleitet und muss zunächst eine App für die Autoidentifikation herunterladen und installieren und die Anweisungen der App befolgen: • 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 einem Selfie (Foto) der zu signierenden Person mittels der Frontkamera. • Es findet ein "Liveness Check" (Lebenderkennung) 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 KI-Algorithmen (Dauer bis zu 15 Minuten). Der Ergebnisdatensatz wird dann an den Swisscom Zertifizierungs- und Vertrauensdienst übermittelt. Da keine persönliche Benutzerführung erfolgt, ist der Nutzer selbst dafür verantwortlich, die korrekten Ausweise, ein Pass- oder ID Dokument gemäss der Länderliste, die beim Kauf angezeigt wurde zu zeigen und korrekte Beleuchtungsverhältnisse und Kameraschärfe einzuhalten. Führerausweis/Führerschein reichen beispielweise nicht aus für die Registrierung zur QES.
NFC-Identifikation, App basiert	Funktioniert wie die oben beschriebene App-basierte Autoidentifikation mit folgenden Abweichungen: • Anstelle der Ausweisprüfung (z.B. Hologramm etc.) wird der NFC-Chip des Ausweises ausgelesen. Hierbei wird der Ausweis einige Sekunden über die Stelle des NFC-Lesers des Smartphones gehalten, so dass alle Informationen ausgelesen werden können. • Die manuelle Hintergrundprüfung kann im Allgemeinen entfallen und verkürzt damit den Prozess.
Auto- und NFC-Identifikation, Browser basiert	Die zu identifizierende Person wird zu einer Webseite weitergeleitet und wird über QR-Code an den Browser ihres Mobiltelefons weitergeleitet. Eine App Installation ist nicht

Leistungsausprägung/ Option	Definition
	notwendig und die Browsersession des Smartphones übernimmt nun die weitere Benutzerführung: • Mit der Kamera des Smartphones nimmt man einen QR Code auf und startet so eine Browsersitzung auf dem Smartphone • Sofern das Dokument NFC fähig ist (chip basiertes Ausweisdokument) und die Methode die NFC-Identifikation unterstützt, wird eine NFC Erweiterung des Browsers nachgeladen und installiert. In diesem Fall muss dann das Dokument an die Rückseite des Smartphones gehalten werden, um via NFC die Dokumentenchipdaten auszulesen. • Sofern NFC nicht möglich, muss die Vorder- und ggfs. Rückseite des zugelassenen Ausweisdokumentes zunächst mit der rückwärtigen Kamera des Smartphones erfasst werden. o Das Ausweisdokument muss dabei so gekippt und bewegt werden, dass im Lichtschein alle optischen Sicherheitsmerkmale (z.B. Hologramme) erkannt werden können. • Das Ausweisfoto wird abgeglichen mit einem Selfie (Foto) der zu signierenden Person mittels der Frontkamera. • Es findet ein "Liveness Check" (Lebenderkennung) statt, indem z.B. in einer Videoaufnahme eine bestimmte Bewegung gefordert wird. • Sofern kein NFC zum Einsatz kam, findet die Prüfung der Identifikationsdaten im Hintergrund statt mit Hilfe von KI-Algorithmen (Dauer bis zu 15 Minuten). Der Ergebnisdatensatz wird dann an den Swisscom Zertifizierungs- und Vertrauensdienst übermittelt. Da keine persönliche Benutzerführung erfolgt, ist der Nutzer selbst dafür verantwortlich, die korrekten Ausweise, ein Pass- oder ID Dokument gemäss der Länderliste, die beim Kauf angezeigt wurde zu zeigen und korrekte Beleuchtungsverhältnisse und Kameraschärfe einzuhalten. Führerausweis/Führerschein funktioniert beispielweise nicht.
Kundeneigener IdP	Kundeneigene IdPs, die auf Benutzerdaten zurückgreifen, die im Sinne der Signaturgesetzgebung bereits ausreichend identifiziert wurden, können in den Store mit aufgenommen werden. Die Nutzung der Methode kann entweder nur für den kundeneigenen Signaturbetrieb erfolgen oder sie kann (gegen Entgelt) auch anderen Signaturdiensten angeboten werden. Die zugrundeliegende Identifikation muss den Anforderungen von EN 119 461 genügen. Der Nachweis, dass eine Person bei einem IdP registriert wurde, wird immer über das vom IdP herausgegebene Authentifizierungsmittel erfolgen. Das Authentifizierungsmittel ist demnach später auch die einzige Möglichkeit zur Signaturfreigabe und muss den Anforderungen des Standards CEN/TS 419 241 genügen.
Kundeneigene Identifikation	Kundeneigene Identifikationsmethoden, z.B. weitere Auto- oder Videoidentifikationsmethoden, können in den Brokerflow eingebunden werden, sofern diese konformitätsgeprüft sind. Hierfür müssen sie den Anforderungen von EN 119 461 genügen. Die Identifikationsmethode kann mit beliebigen Standardsignaturfreigabemethoden oder einer kundeneigenen Signaturfreigabemethode kombiniert werden. Die Nutzung der Methode kann entweder nur für den kundeneigenen Signaturbetrieb erfolgen oder sie kann (gegen Entgelt) auch anderen Signaturdiensten angeboten werden.
Nutzung des Self-Service Portals	Das Self-Service Portal bietet sich insbesondere für Nutzer des Registrierungsportals und des Smart Registration Service an, die offline ihre Registrierung durchgeführt haben und vor der Signatur Gewissheit darüber haben möchten, ob die Registrierung ordnungsgemäss verlaufen ist bzw. sie signieren können. Es wird derzeit von Swisscom betrieben, es könnte zukünftig aber auch durch einen Partner betrieben werden mit gleicher Funktionalität. **Überprüfung des Registrierungsstatus** 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 auf diesem Portal ausgelöst werden, wenn z.B. die SMS mit den Nutzungsbestimmungen nicht den Empfänger erreicht hat. Das Portal ist aufrufbar unter: https://smart-flow.trustservices.swisscom.com/

Leistungsausprägung/ Option	Definition
	 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 Signaturfreigabemethode 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-Identifikations-seite kann über den Button "Zur Identifikation" erreicht werden. **Überprüfung der Signaturfähigkeit** Darüber hinaus kann auf einem zweiten Portal überprüft werden, ob eine Signatur möglich ist: https://check-signature.scapp.swisscom.com/ Hierzu ist ein Text "Hello World" testhalber mit der registrieren Signaturfreigabemethode zu signieren. Nach der Signatur wird das Ergebnis angezeigt:  Die Nutzung der Portale ist kostenfrei.
IdP Identifikation	Verschiedene IdPs ermöglichen die Registrierung mit ihren eigenen Apps und Logins. Hierbei müssen sich die Nutzer zunächst mit der IdP eigenen App oder dem IdP eigenen Zugang authentisieren und bestätigen, dass sie beim IdP registriert sind. Je nach Art der Registrierung können Nutzer von der Nutzung des Signaturdienstes abgelehnt werden (z.B., wenn eine Identifikation zwar nach dem Bankengesetz korrekt verlaufen ist, aber das Identifikationsdokument im Rahmen des Signaturgesetzes nicht ausreichend ist). D.h. der Nutzer durchläuft beim IdP einen Abgleich und wird ggfs. dadurch herausgefiltert. Sofern die Signatur möglich ist, muss der Nutzer die Nutzungsbestimmungen des jeweiligen Swisscom Zertifizierungs- bzw. Vertrauensdienstes bestätigen und kann fortan mit einer dafür eingerichteten Signaturfreigabemethode beim IdP Signaturen freigeben. Der Einsatz anderer Signaturfreigabemethoden ist mit einer IdP Registrierung in der Regel nicht möglich.

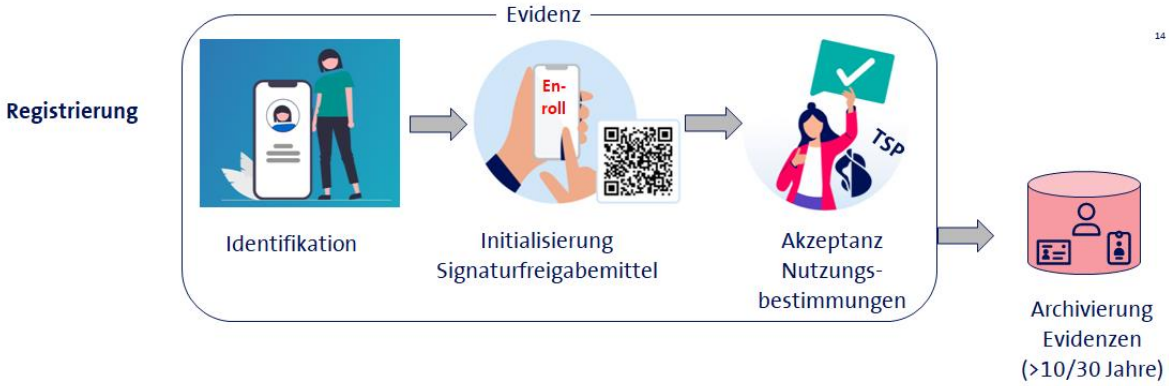
Leistungsausprägung/ Option	Definition
Darstellung der Registrierungsverfahren im Store mit Swisscom Views	Für die schnelle Integration der Registrierungsstrecke im Browser offeriert Swisscom Views mit Swisscom Logo und eigenem UX-Design für die Auswahl der geeigneten Registrierungsmethode. Im webgeführten Browser-Flow wird dem Signierenden dann eine auf einem Swisscom System gehostete Seite angezeigt im Swisscom Look & Feel. Hier werden keine Preise für die unterschiedlichen Registrierungsverfahren angezeigt, d.h. der Besteller der Leistungen erhält abhängig von dem vom Kunden gewählten Verfahren eine Rechnung gemäss dem vom Nutzer gewählten Verfahren für die Identifikation. Es werden nur die Verfahren angezeigt, die der Besteller der Leistung auch wirklich bestellt hat und die für den Signaturauftrag Sinn machen (z.B. fortgeschritten oder qualifiziert, Jurisdiktion EU oder Schweiz). Einzelne Ikonen zeigen die verschiedenen Verfahren an und bieten über Hilfe-Symbole auch weitergehende Informationen an (z.B. Art des Verfahrens etc.). Auch die Jurisdiktion, für die das Verfahren anwendbar ist, wird angezeigt.
Einbindung der Registrierungsmethoden des Stores im eigenen Look & Feel (UX)	Sofern die Teilnehmerspezifische UX für die Auswahl der Registrierungsmethoden zur Anwendung kommen soll und z.B. zusätzliche Informationen zu den einzelnen Verfahren platziert werden sollen, wie z.B. unterschiedliche Preisinformationen, bietet sich die OIDC-PAR Schnittstelle an, um die zur Verfügung stehenden und bestellten Verfahren einzubinden. Hier ist Integrationsaufwand auf Seiten der Teilnehmerapplikation notwendig sowie beidseitiger Testaufwand.
Passwort / Einmalcode via SMS	Password (-eingabe), für die Authentisierung am Service oder für Signaturfreigaben zu verwendendes Password, welches den Faktor «Wissen» bietet. Diese Passwort Eingabe wird kombiniert mit einem Einmalcode, der für eine einfache Nutzung via SMS an ein Mobilfunkgerät übertragen wird. Damit wird der Faktor „Besitz“ eines Mobilfunkgerätes mit der angegebenen Mobilnummer überprüft.
Einmalcode via SMS	Einmalcode, der für eine einfache Nutzung via SMS an ein Mobilfunkgerät übertragen wird. Damit wird der Faktor „Besitz“ eines Mobilfunkgerätes mit der angegebenen Mobilnummer überprüft. Damit wird nur ein Faktor überprüft – das Verfahren ist dementsprechend nur für Fortgeschrittene Elektronische Signaturen einsatzfähig.
Mobile ID	Managed Service für die sichere Benutzer-Authentisierung basierend auf eine Push Message und PIN-Eingabe. Mobile ID kann von verschiedenen Mobilfunk Providern der Schweiz, unter anderem Swisscom (Schweiz) AG, für Schweizer SIM-Karten bezogen werden. Für die Initialisierung benötigt es eine SMS. Siehe https://mobileid.ch
Mobile ID App	Managed Service App (Applikation), die vom Google Play Store oder Apple Store herunter geladen werden kann zur sicheren Benutzer-Authentisierung. Diese basiert auf Authentisierungsmöglichkeiten des Mobilgerätes wie z.B. Fingerprint oder Face Recognition. Die Mobile ID App wird über eine internationale Mobilnummer per SMS initialisiert und funktioniert mit einer laufenden Internetverbindung. https://mobileid.ch
Swisscom Signaturfreigabe App	App im Google oder Apple Store für das Smartphone, welches eine Signaturfreigabe mit biometrischen Merkmalen (z.B. Fingerprint oder Face Recognition) ermöglicht und als Rückfalllösung eine 6-stellige PIN hat. Dieses Signaturfreigabemethode ist nicht an eine Mobilnummer oder SIM-Karte gebunden und damit auch nicht auf den Empfang einer SMS angewiesen.
Passkeys	Passkeys sind eine Erweiterung des FIDO-Standards für eine 2-Faktor Authentisierung, die typischerweise von Webdiensten auch für die Anmeldung genutzt wird. Es handelt sich dabei um Paare von privaten und öffentlichen Schlüsseln, die auf dem jeweiligen Gerät gespeichert werden und innerhalb einer Android/Apple oder Windows Umgebung auch in der jeweiligen Umgebung auf mehreren Geräten synchronisiert werden. Typischerweise wird zur Aktivierung der Passkeys die Methode zu dem Entsperren des Bildschirms verwendet (z.B. Fingerprint, Gesichtserkennung oder PIN). Alternativ können auch FIDO2 kompatible USB- oder NFC Sticks via webauthn Schnittstelle genutzt werden. Damit ist eine Signaturfreigabe unabhängig von einer Mobilnummer oder sogar unabhängig von einem Smartphone möglich.
Signaturfreigabe SDK	Software Development Kit für den Einsatz der Signaturfreigabemöglichkeiten der Signaturfreigabe App im Rahmen einer eigenen App. Damit kann in eine eigene Kundenapp die Signaturfreigabe eingebaut werden, so dass hier stark reduzierte Auditaufwände anfallen, da der entsprechende Freigabeprozess im Prinzip auditiert ist und auf Swisscom Systemen läuft und lediglich in der Kunden App eingebunden ist. Es muss hierfür ein Einsatzkonzept in Absprache mit Swisscom Trust Services erstellt werden und eine Abnahme durch die Konformitätsbewertungsstelle (Auditor) erfolgen.

Leistungsausprägung/ Option	Definition
Fasttrack Verfahren	Die Fasttrack Methode bezeichnet eine Signaturfreigabe ohne vorgängige Registrierung bei Swisscom Trust Services. Hierbei wird die Gesetzgebung der Schweiz herangezogen, die Teilnehmer an Mobilfunkdiensten dazu verpflichtet, sich vorab identifizieren zu lassen. Die Mobilfunkanbieter speichern die Teilnehmerdaten hinter einer Mobilnummer. Im Rahmen des Fasttrack-Verfahrens ist somit keine erneute Identifikation oder Registrierung notwendig und die Signaturfreigabe kann direkt durch einen Einmalcode erfolgen, der per SMS an einer in der Schweiz registrierten Mobilnummer erfolgt. Es können nur fortgeschrittene elektronische Signaturen auf Basis dieses Verfahrens ausgestellt werden und das Zertifikat dieser Signaturen beinhaltet lediglich die Mobilnummer als überprüftes Datum und das Land Schweiz.
Kundeneigene Signaturfreigabe	Neben kundeneigene Signaturfreigaben, die auf dem Signaturfreigabe SDK beruhen, können auch weitere kundeneigene Signaturfreigaben in den Signaturflow eingebunden werden, die nicht das SDK nutzen. Die Nutzung der Methode kann entweder nur für den kundeneigenen Signaturbetrieb erfolgen oder sie kann (gegen Entgelt) auch anderen Signaturdiensten angeboten werden. Die zugrundeliegende Freigabe (Authentisierung) muss den Anforderungen von CEN/TS 419 241 genügen.
Authentisierung mit Postfinance App	Das Login bei der eBanking App der Postfinance kann für die Freigabe einer Signatur verwendet werden. Siehe IdP Identifikationen.
Freigabe durch eine Store Identifikationsmethode aus Ziffer 4.2	Die sogenannte One-Shot Signatur ermöglicht eine Signaturfreigabe ohne Installation, Initialisierung und Nutzung eines Signaturfreigabemittels. Hierbei findet die Identifikation und die Signaturfreigabe (hierzu reicht ein "OK" Knopf) mit der Signatur in einer Sitzung statt, die vom Broker initiiert wird. Es können alle Store Methoden aus Kapitel 4.2 dafür genutzt werden.
Darstellung der Signaturfreigabeerfahren im Store mit Swisscom Views	Für die schnelle Integration der Registrierungs- und Signaturfreigabestrecke offeriert Swisscom Views mit Swisscom Logo und eigenem UX-Design für die Auswahl der geeigneten Signaturfreigabemethode. Im webgeführten Browser-Flow wird dem Signierenden dann eine auf einem Swisscom System gehostete Seite angezeigt im Swisscom Look & Feel. Hier werden keine Preise für die unterschiedlichen Verfahren angezeigt, d.h. der Besteller der Leistungen erhält abhängig von dem vom Kunden gewählten Verfahren für die Signaturfreigabe eine Rechnung gemäss gewählter Signaturfreigabe, sofern überhaupt Gebühren für das Verfahren erhoben werden. Es werden nur die Verfahren entscheidungsbasiert angezeigt, die der Besteller der Leistung auch wirklich bestellt hat und die für den Signaturauftrag Sinn machen (z.B. fortgeschritten oder qualifiziert, Jurisdiktion EU oder Schweiz). Einzelne Ikonen zeigen die verschiedenen Verfahren an und bieten über Hilfe-Symbole auch weitergehende Informationen an (z.B. Art des Verfahrens etc.). Auch die Jurisdiktion, für die das Verfahren anwendbar ist, wird angezeigt.
Einbindung der Signaturfreigabe-methoden des Stores im eigenen Look & Feel (UX)	Sofern die Teilnehmerspezifische UX für die Auswahl der Signaturfreigabemethoden zur Anwendung kommen soll und z.B. zusätzliche Informationen zu den einzelnen Verfahren platziert werden sollen, wie z.B. unterschiedliche Preisinformationen, bietet sich die OIDC-PAR Schnittstelle, um die zur Verfügung stehenden und bestellten Verfahren einzubinden. QR Code Elemente können über den Standard OpenID Connect Client Initiated Backchannel Authentication Flow (OIDC CIBA) eingebunden werden. Hier ist Integrationsaufwand auf Seiten der Teilnehmerapplikation notwendig sowie beidseitiger Testaufwand.

4.5 Ablauf der Identifikation und Registrierung

4.5.1 Genereller Ablauf des Registrierungsverfahrens

Die Registrierung wird entweder vom Teilnehmer im Rahmen des Angebotes der Teilnehmerapplikation angeboten und in den Workflow der Signaturapplikation integriert. Ausserdem besteht für Signierende die Möglichkeit sich direkt online gegen Bezahlung mit Kreditkarte oder Gutscheincode auf der Seite der Swisscom Trust Services zu registrieren: https://srsident.trustservices.swisscom.com



Eine Registrierung besteht immer aus folgenden Schritten:

- Eine Signaturfreigabemethode muss gewählt und ggfs. vorab installiert werden. Die möglichen Signaturfreigabemethoden sind aus dem Angebot unter Ziffer 4.3 zu wählen. Nicht jede Identifikationsmethode unterstützt auch alle Signaturfreigabemethoden. Ein IdP, wie z.B. eine Bank, wird in der Regel nur seine eigene App zur Signaturfreigabe erlauben.
- Die Nutzungsbestimmungen des jeweiligen Swisscom Zertifizierungsdienstes bzw. Vertrauensdienstes müssen akzeptiert werden. Das geschieht entweder während der Registrierung oder im Nachgang durch Zusendung einer SMS mit einem Link zu einer Webseite mit den Nutzungsbestimmungen von Swisscom.
- Das Signaturfreigabemethode muss erstmalig verwendet werden, man muss z.B. zeigen, dass man im Besitz einer Signaturfreigabemethode oder im Besitz der Mobilnummer ist. Hierbei wird eine eindeutige ID der Signaturfreigabemethode erzeugt, die dem Nutzer dann zugeordnet wird (z.B. Kennzeichen des Smartphones oder Mobilnummer, etc.).
- Die Identifikation, die bei den Standard-Identifikationspartner z.B. mittels Videoidentifikation oder mittels Abgleichs mit einem Bankkonto durchgeführt wird. Im Falle des IdP authentifiziert man sich, d.h. man loggt sich beim IdP ein und bestätigt, dass man bereits vom IdP identifiziert wurde. Im Rahmen der Identifikation wird geprüft, ob man für das Verfahren der elektronischen Signatur zugelassen werden kann und alle gesetzlichen Voraussetzungen dafür erfüllt sind (z.B. Besitz des korrekten Identitätsdokumentes etc.).
- Zum Schluss wird ein Ergebnisdatensatz als "Evidenz" in der Swisscom Registrierungsdatenbank (RA System) eingeliefert und vom Swisscom Zertifizierungs- und Vertrauensdienst im Rahmen der gesetzlichen Aufbewahrungsfrist archiviert. Diese Evidenz wird z.B. auch bei Gerichtsverfahren in Bezug auf die elektronische Signatur oder anderen Überprüfungen bei Zweifeln an der Signatur herangezogen.

Für den Ablauf der Registrierung werden Swisscom eigene Webviews angeboten, die in den jeweiligen Workflow der Teilnehmerapplikation eingebunden werden können. Alternativ kann der Nutzer Webviews erstellen, die mittels OIDC PAR bzw. OIDC CIBA die einzelnen Schritte nacheinander durchführen.

Identifikationsverfahren können kombiniert sein, d.h. es kann zum Beispiel zunächst versucht werden, eine Person anhand eines NFC fähigen Ausweisdokumentes zu identifizieren. Sollte das nicht vorhanden sein, oder nicht gelingen, so wird die Person dann in einen Autoidentifikaitonsprozess weitergeleitet.

4.6 Nutzung des Registrierungsportals der Swisscom Trust Services

4.6.1 Ablauf der Registrierung mit Gutscheincode oder Kreditkartenzahlung

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 für den 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.
- Das Signaturniveau muss stimmen: In der Regel verlangen qualifizierte elektronische Signaturen, eine aufwändigere Registrierung als fortgeschrittene elektronische Signaturen. 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, welche Voraussetzungen gegeben sein müssen. Für eine eID oder NFC-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. Für Identifikation bei einem IdP/Bank müssen bei diesem IdP auch Kundenbeziehungen existieren.
- Sprache: Nicht alle Verfahren bieten in der Benutzerkommunikation jede Sprache.
- Die Gültigkeiten der Registrierungen, d.h. der Zeitraum in denen ohne eine weitere Registrierung signiert werden kann, ist von Verfahren zu Verfahren unterschiedlich.
- 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 beschränkt sein. Hierbei ist ggfs. eine Rückfrage erforderlich mit der Partei, die den Gutscheincode übergeben hat.

4.6.2 Bezahlung

Nachdem das passende Verfahren gewählt wurde, kann der Nutzer die Identifikation mittels 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.

4.6.3 Optional: Installation der Signaturfreigabemethode

Bevor der Installationsprozess gestartet wird, muss die Signaturfreigabemethode, welche später für die Signaturfreigabe genutzt werden soll, installiert werden. Zu beachten ist, dass nur Mobile ID und Passwort mit Einmalcode via SMS als Methode bereitstehen. Wird vorab keine Signaturfreigabemethode installiert, könnte der Nutzer gezwungen werden, eine Kombination von selbstgewähltem Passwort und Einmalcode via SMS zu nutzen.

4.6.4 Identifikationsprozess

Zum Start des Identifikationsprozesses wird der Nutzer zum Identifikationspartner oder IdP weitergeleitet. Parallel dazu erhält der Nutzer 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 Identifikationspartners 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:

- die notwendigen Mittel bereit zu haben, z.B. eine ausreichende Kamera, ausreichende Beleuchtungssituation oder einen NFC-Leser oder NFC-Zugang am Mobilgerät 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 zum Swisscom Zertifizierungs- und Vertrauensdienst überträgt und den Prozess nicht vorzeitig abzubrechen.

In vielen Situationen können Sie bei der Identifikation vorab eine E-Mail-Adresse mitteilen. Sie erhalten dann eine E-Mail mit einem Link, mit dem 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 bspw. die Ausweisbilder verwaschen, nicht lesbar, ein (vermeintlich) falscher Ausweis vorgelegt worden sein, oder ein Ausweis als nicht ausreichend sicher eingestuft werden, so kann die Registrierung zurückgewiesen werden. Eine begonnene Registrierung führt nicht zwangsläufig zum Erfolg. Daher bedeutet die Zahlung nicht automatisch einen Anspruch auf eine erfolgreiche Registrierung, sondern legitimiert den Käufer lediglich für einen Versuch im Rahmen eines Identifikationsverfahrens.

4.6.5 Nutzungsbestimmungen

Im Prozess müssen die Nutzungsbestimmungen der Swisscom Trust Services akzeptiert werden. Für die Akzeptanz wird erstmalig die Signaturfreigabemethode eingesetzt. Sofern dieses ein Passwort beinhaltet, muss das Passwort zum ersten Mal gesetzt werden. Häufig werden die Nutzungsbestimmungen bereits im Prozess des Identifikationspartners 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 Authentisierungsmittel bestätigt werden. Sofern der Anweisung in der SMS nicht Folge geleistet wird, wird die SMS binnen 15 Tage alle 3 Tage zugestellt. Sollte danach keine Zustimmung erfolgen, so wird der Registrierungsvorgang gelöscht und es muss für eine Signatur eine neue Registrierung durchgeführt werden. Sofern nur einer Nutzungsbestimmung anstelle von beiden Nutzungsbestimmungen (CH/EU) zugestimmt wird, kann nachfolgend nur in dem betreffenden Rechtsgebiet signiert werden.

4.6.6 Signatur

Erst nach Akzeptanz der Nutzungsbestimmungen und der Einlieferung der Evidenz durch den Identifikationspartner kann der Nutzer bei den Teilnehmerapplikationen und Signaturanwendungen signieren.
Die Registrierungen haben je nach eingesetztem Verfahren Ablaufdaten, z.B. können sie am Ablaufdatum des Ausweises gebunden sein oder sind generell nur für 1, 2 oder 5 Jahre gültig (siehe oben). Vor Ablauf wird der Nutzer nochmals mit einer SMS gewarnt, dass er sich neu registrieren lassen muss, sofern die Mobilnummer bekannt ist.

4.6.7 Rückerstattung

Sollte ein Fehler aufgrund von Fehlern im Registrierungsprozess entstanden sein, besteht bei einer Kreditkartenzahlung das Anrecht auf eine Rückerstattung und bei der Verwendung eines Vouchers die Möglichkeit eines Ersatzvouchers.
Gründe sind insbesondere:

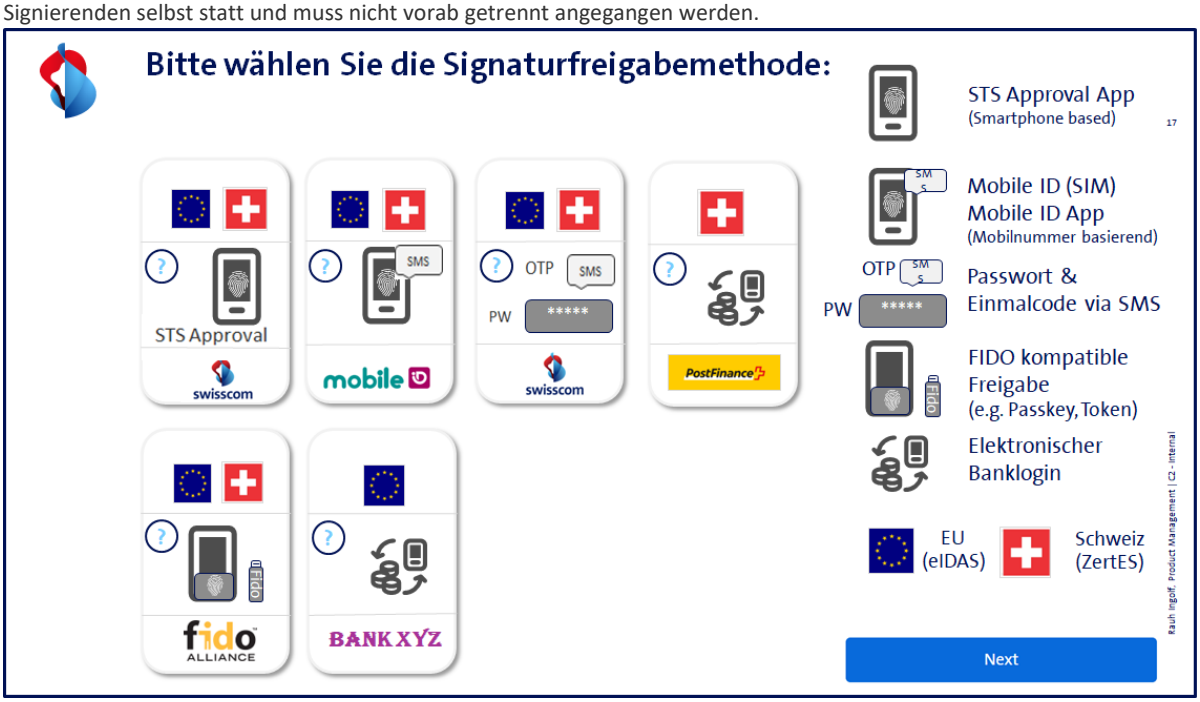
- Nicht erhaltene SMS auf Mobilnummern innerhalb der EU, Schweiz und EWR
- Abbrüche in der App oder des Prozesses aufgrund von Fehlverhalten
- "Hängenbleiben" des Prozesses länger als 15 Minuten

Des Weiteren können Vouchers für Verfahren rückerstattet werden, 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 Hängenbleiben des Prozesses.
- Einsatz von nicht zugelassener 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.
- Fehlende Akzeptanz der Nutzungsbestimmungen

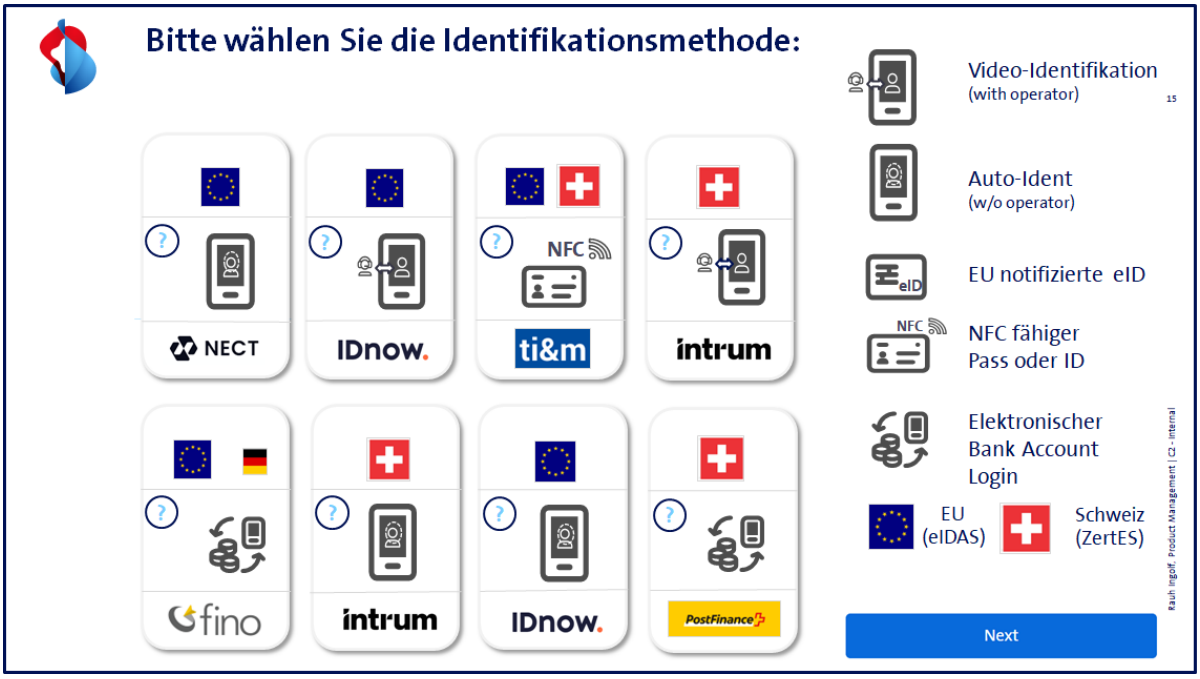
4.7 Nutzung des Stores im Rahmen der Teilnehmerapplikationen

Teilnehmer, die im Rahmen der Signaturapplikationen (Teilnehmerapplikationen) einen Signaturworkflow anbieten, erhalten gemäss Bestellung und Konfiguration Zugang zu allen im Store (Marktplatz) angebotenen und bestellten Registrierungsverfahren. Damit findet die Registrierung und Auswahl der Signaturfreigabemethode im Signaturworkflow durch den Signierenden selbst statt und muss nicht vorab getrennt angegangen werden.



(Prinzipbild – die Verfahren sind teilweise noch nicht im Store erhältlich)

Diese Verfahren müssen bestellt und entsprechend der Bestellung konfiguriert werden. Im Bestellformular ist ersichtlich, welches Verfahren für einen Store konfiguriert werden kann. Es kann ein monatliches Bereitstellungsentgelt oder eine Gebühr pro erfolgte Identifikation verlangt werden, die an die Swisscom Trust Services entrichtet wird, sofern nicht pauschal abgegolten wird. Swisscom Trust Services tritt als Reseller der Identifikationsleistung auf. Der Partner preist die Kosten in sein Angebot an den Endkunden ein.
Genauso werden auch die Registrierungsmethoden im Signaturflow angeboten:

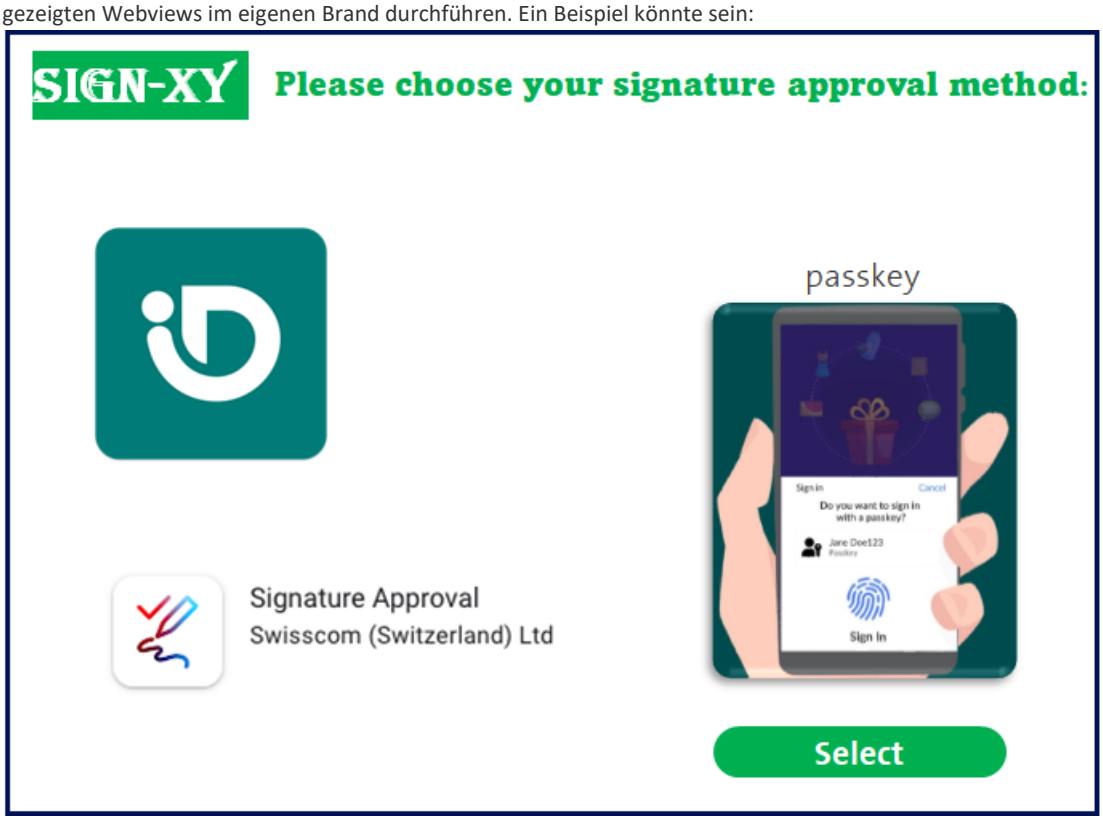


(Prinzipbild – die Verfahren sind teilweise noch nicht im Store erhältlich)

Auch hier werden nur die gewünschten und bestellten Verfahren in die Auswahl konfiguriert.

Swisscom Trust Services stellt im Signaturflow sicher, dass Personen, die nicht registriert wurden und im Store der Signaturfreigabemethoden eine nicht registrierte Methode wählen oder deren Signaturfreigabe scheitert, zum Store für die Registrierungsmethoden weitergeleitet werden. Hier sind je nach Rechtsraum und Signaturniveau die passenden Registrierungsverfahren im Angebot.
Signaturflows sind aber auch so konfigurierbar, dass z.B. nur eine Signaturfreigabemethode oder Registrierungsverfahren verfügbar ist. Als spezielle Konfiguration ist auch die sogenannte Einmalsignatur möglich. Bei dieser werden nur Identifikationsmethoden angezeigt und in der gleichen Sitzung erfolgt auch die Signatur. Eine spezielle Signaturfreigabe entfällt, führt aber dazu, dass bei zukünftigen Signaturen zuvor wieder eine Registrierung notwendig ist.

Über die OIDC-PAR Schnittstelle und mit Hilfe von OIDC CIBA kann der Nutzer selber die Ansteuerung anstelle der oben gezeigten Webviews im eigenen Brand durchführen. Ein Beispiel könnte sein:



4.8 Eigene Identifikations- und Signaturfreigabemethode

IdPs haben die Möglichkeit eigene Identifikations- oder Signaturfreigabemethode einzubinden. Hierfür ist ein Umsetzungskonzept und ein Audit durch eine Konformitätsbewertungsstelle und eventuell eine entsprechende Meldung an die Aufsichtsstelle notwendig. Die einzelnen Schritte werden im Rahmen des Onboarding Supports angeboten und sind in der entsprechenden Leistungsbeschreibung zum Onboarding Support beschrieben. Die Verfahren können dann nach Freigabe – sofern gewünscht – auch für andere Teilnehmer im Store angeboten werden.

4.9 Service Desk

Swisscom Trust Services stellt ein Servicedesk (1st Level Support) für die Identifikationen zur Verfügung, die mit Kreditkarten erworben wurden oder für Nutzer, die in ihren Applikationen die oben genannten Schnittstellen zu den Swisscom Systemen nutzen. Nutzer, die die Identifikationen per Voucher durchführen, wenden sich an die Stelle, die ihnen die Voucher übergeben hat. Entsprechend den Anfragen löst Swisscom Trust Services bei Bedarf die Incidents direkt mit den Servicestellen der Identifikationspartner, sofern kein eigenes Identifikationsverfahren eingesetzt wird.
Über das Registrierungsportal erworbene Identifikationen garantieren keine Registrierung. Sollte eine Registrierung nicht funktionieren, so wird dem Benutzer ein weiterer Versuch mit der gleichen und abschliessend mit einer anderen Methode angeboten. Führt das nicht zum Erfolg, haben Benutzer mit Kreditkartenzahlung Anspruch auf eine Rückerstattung der Kosten.

5 Leistungsdarstellung und Verantwortlichkeiten

Einmalige Leistungen

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Bereitstellung des Registrierungsmethoden im Rahmen Registrierungsportal		
1. Registrierung über das Online-Portal der Swisscom Trust Services: Der Nutzer kann auf https://srsident.trustservices.swisscom.com die geeignete Registrierung aufrufen und mit Voucher oder Kreditkarte bezahlen	✓	
2. Erwerb der Registrierungsmöglichkeit über das Online-Portal entweder durch Vertragsabschluss über einen oder mehrere Voucher oder direkt durch Kreditkartenzahlung.		✓
Bereitstellung der Registrierungsmethoden und Signaturfreigabemethoden in den Stores (im Signatur-Flow)		
3. Nutzer (in diesem Fall also Teilnehmer), die Signaturapplikationen für den Signaturservice bereitstellen, können die Stores zur Auswahl der Registrierungsmethode und zur Wahl der Signaturfreigabe mit einbinden. Swisscom Trust Services stellen im Rahmen der Registrierung die Prozesse zum Aufruf des Signaturfreigabemethode und zur Akzeptanz der Nutzungsbestimmungen als konfigurierbarer Webview zur Verfügung.	✓	
4. Einbindung der Webviews im Signaturflow. Errichtung einer eigenen Abrechnung und Verrechnung der Leistungen gegenüber den identifizierten Personen (Signierende).		✓
Bereitstellung der Store Registrierungsmethoden und Signaturfreigabemethoden via OIDC-Schnittstellen, PAR/CIBA		
5. Implementierung der Views basierend auf den angebotenen Schnittstellen		✓
6. Gemeinsamer Schnittstellentest	✓	
Beendigung des Service		
1. Löschen der Berechtigungen und Zugänge zum Smart Registration Service	✓	
2. Einstellen des Betriebes von Identifikationsverfahren oder Signaturfreigabeverfahren, die den regulatorischen oder gesetzlichen Ansprüchen nicht mehr genügen, oder vom Anbieter nicht mehr unterstützt werden.	✓	

Wiederkehrende Leistungen

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Standardleistungen allgemein		
1. Bereitstellung und Pflege der Service Infrastruktur und des Zugangs sowie Betrieb.	✓	
2. Sicherstellung der Konformität der Identifikationsverfahren zu den jeweiligen angebotenen Arten der elektronischen Signatur und dem angebotenen Rechtraum für dieses Verfahren	✓	
3. Auswahl des geeigneten, mit der gewünschten elektronischen Signatur und sonstigen Voraussetzungen kompatiblen Identifikationsverfahrens gemäss Ziffer 4.		✓
4. Bereitstellung und Pflege der Schnittstelle zu den von Swisscom Trust Services 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 im Falle der Swisscom eigenen Webviews	✓	
6. Information an die zu identifizierende Person über die anstehende Identifikation, den Zweck der Identifikation und das zu befolgende Vorgehen im Rahmen der Identifikation im Falle der Nutzung der OIDC PAR oder CIBA APIs		✓
6. Bereitstellung eines Zugangs zum Identifikationspartner bzw. IdP für die zu identifizierende Person	✓	
7. Einsammeln der Evidenzdaten bzw. Ergebnissen von den externen Identifikationspartner oder IdPs.	✓	
8. Melden von Sicherheitsvorfällen, die die Identifikation oder Signaturfreigabe betreffen		✓
9. Gesetzeskonforme Archivierung aller erhaltenen Evidenzen, die verwendeten Signaturfreigabemethode und Zustimmungen zu den Nutzungsbestimmungen	✓	
10. Support, Koordinierung und Beauftragung der Supportfälle beim jeweiligen Identifikationspartner unter Nennung der Vertragsnummer, Multiple Authentication Broker Transaction ID (sogenannte	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
"rax_id"), ggfs. Mobilnummer oder UUID (falls bekannt), Zeitpunkt der Identifikation und genutzter Identifikationsmethode sowie ggfs. Mobilnummer		
11. Nennung der Auftragsreferenz (sofern vorhanden), Zeitpunkt der Identifikation, genutzte Identifikationsmethode und verwendetes Signaturfreigabemethode oder andere geforderte Daten im Falle eines Support Cases.		✓
12. Der zu identifizierende Person stellt sicher, dass er seinen ständigen Wohnsitz in der Schweiz, dem EWR oder einem Land der EU hat oder einem anderen Land, welches explizit im Auftrag an Swisscom Trust Services benannt wurde.		✓
13. Eigene Kommunikationskosten des Nutzers zur Inanspruchnahme von Supportdienstleistungen (z.B. Telefon, Porto, etc.)		✓
14. Der Nutzer akzeptiert, dass er oder die zu identifizierende Person keinen Anspruch auf eine Registrierung hat. Diese kann aus verschiedenen Gründen, z.B. Risikogründen, abgelehnt werden. Die einzige Entschädigung ist hierbei eine Rückzahlung der Kosten, die er oder die betreffende Person für diese Registrierung bezahlt hat. Alternativ kann Swisscom Trust Services auch einen Gutschein für eine weitere Registrierungsmethode zustellen.		✓
15 Abrechnung der Leistungen gegenüber dem Besteller der Leistungen unter Auflistung der summarischen Nutzung der Methoden. (B2B Abrechnung)	✓	
16. Benutzer- bzw. Endkundenspezifisch Nutzungserfassung und Abrechnung, welche Methode wie häufig genutzt wurde.		✓
17. Kommunikation mit den Apps, Browser, Schlüssel (z.B. Passkeys) und Endgeräten des Signierenden bzw. der zu identifizierenden Person, sofern • Die Geräte und Apps per Internet mit ausreichender Bandbreite erreichbar sind oder Mobilfunkfunktionalitäten per Mobilfunk • Für Einmalcodes SMS durch den lokalen Provider von Swisscom empfangen werden können • Keinerlei lokal bei den Signierenden oder der zu identifizierenden Person installierte Viren oder störende Software die Kommunikation stört • Immer die aktuellen Versionen der benötigten Apps und Browser verwendet werden • Bei Betriebssystemfunktionen (z.B. Passkeys) immer die aktuellen Versionen der Betriebssysteme oder entsprechender Software verwendet wird.	✓	
Standardleistungen bei Aufruf der Registrierungs- oder Signaturfreigabemethoden aus dem Store mit OIDC PAR		
1. Hinweis an die zu identifizierende Person, dass diese zu einem Portal oder Dienst eines Identifikationspartners weitergeleitet wird (Beispiel: "Durch den Aufruf der URL http://xxx werden Sie zum Identifikationsportal unseres Identifikationspartners weitergeleitet, bei dem Sie sich identifizieren können"). Einholen von Einwilligungen im Sinne der geltenden Datenschutzgesetzgebung, sofern Vorabdaten gesendet werden.		✓
2. Verantwortung für die Vorbereitung der Identifikation der zu identifizierenden Person vor Bereitstellung des Zugangs zum Identifikationspartner durch Aufforderung oder Benutzerführung im geeigneten Portal und Einhalten aller Vorschriften für das gewählte Identifikationsverfahren, d.h. insbesondere Hinweis auf Bereitstellung der erforderlichen Mittel (z.B. Kamera, NFC Zugang am Mobilgerät) und der notwendigen Identifizierungsmittel (Kontonummer mit Kontozugang, korrekte geforderte ID/Pass Dokumente, etc.), Akzeptanz der Nutzungsbestimmungen, genügende Ausleuchtung bei Videoverfahren, Installation der notwendigen Identifikationsapps/-programme, notwendige Eingaben oder Aussagen zu gestellten Fragen.		✓
3. Behandlung von Fehlern während der Registrierung und/oder Signaturfreigabe z.B. durch Bereitstellung eines weiteren Versuches oder alternativer Registrierungs- oder Signaturfreigabeverfahren.		✓
Standardleistungen bei Bereitstellung der Methoden über das Registrierungsportal		
1. Zur Verfügung stellen des Vouchersystems und Einlösemöglichkeiten von Voucher sowie Abwicklung von Kreditkartenzahlungen über Zahlungsdienstleister.	✓	
2. Eingabe der exakten persönlichen Daten für ordentliche Rechnungsstellung bzw. Zahlungsbeleg		✓
3. Rechnungstellung (per E-Mail) an Firmenkunden oder Zahlungsbeleg an den Privatnutzer	✓	
4. Kostenübernahme für abgebrochene Identifikationen (z.B. Videoidentifikation) sofern diese aufgrund eines fehlerhaften Prozesses bei Swisscom Trust Services erfolgte unter Einhaltung der Mitwirkungsleistungen des Nutzers.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
5. Online-Identifikation über das Portal von Swisscom Trust Services: 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. Identifikation im Rahmen der Stores: Support über die im Bestellformular/Vertrag erwähnten Möglichkeiten. Ein Registrierungsproblem wird generell über Kostenerstattung oder eine ersatzweise durchgeführte Identifikation gelöst. Es besteht generell kein Anspruch auf eine detaillierte Analyse eines Identifikationsproblems.	✓	
6. Internationale Abführung der gesetzliche Abgaben im Privatkundengeschäft.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Video-Identifikation per App		
1. Download der angegebenen App aus dem App-Store des Smartphones und Installation auf dem Smartphone. Die App kann ggfs. nicht in jedem länderspezifischen App-Store verfügbar sein.		✓
2. Download und Installation/Aktivierung der Signaturfreigabemethode, sofern notwendig		✓
3. Nutzung auf einem Smartphone mit einer ausreichenden Kamera (Minimum Auflösung 1024 x 768 Pixel) bei ordentlichen Lichtverhältnissen (Lampe, Tageslicht)		✓
4. Verwendung von ID aus ausgewählten EU/EWR Ländern und Schweiz bzw. Pässen. Keine Aufenthaltsberechtigungen oder Führerscheine. Siehe Ziffer 4.2 für die Liste der berechtigten Dokumente.		✓
5. Sprachauswahl des Operators durch die Sprachwahl der Benutzeroberfläche/Smartphone, sofern keine extra Sprachwahl angegeben ist.		✓
6. Beantwortung aller vom Operator gestellte Fragen in den angegebenen zugelassen Sprachen der Sprachwahl bzw. Befolgung der Anweisungen des Operators. Diese dienen der zusätzlichen Sicherheitsüberprüfung des Dokumentes bzw. auch der Sicherstellung, dass eine nicht zuvor aufgenommene Videositzung bei der Registrierung abgespielt wird (sogenannte Lebenderkennung).		✓
7. Durchführung der Identifikation und Übermittlung der Evidenz an den Swisscom Zertifizierungs- und/oder Vertrauensdienst.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Auto-Identifikation per App		
1. Download der angegebenen App aus dem App-Store des Smartphones und Installation auf dem Smartphone. Die App kann ggfs. nicht in jedem länderspezifischen App-Store verfügbar sein.		✓
2. Download und Installation/Aktivierung der Signaturfreigabemethode, sofern notwendig		✓
3. Nutzung auf einem Smartphone mit einer Kamera (Minimalauflösung 1024 x 768 Pixel) bei ordentlichen Lichtverhältnissen (Lampe, Tageslicht)		✓
4. Verwendung von ID aus ausgewählten EU/EWR Ländern und Schweiz bzw. Pässen. Die Verwendung von Aufenthaltsberechtigungen oder Führerscheine ist nicht möglich. Siehe Ziffer 4.2 für die Liste der berechtigten Dokumente.		✓
5. Sprachauswahl der Benutzerführung durch die Sprachwahl der Benutzeroberfläche/Smartphone, sofern keine extra Sprachwahl angegeben ist.		✓
6. Beantwortung aller von der App gestellte Fragen bzw. Befolgung der Anweisungen der App. Diese dienen der zusätzlichen Sicherheitsüberprüfung des Dokumentes bzw. auch der Sicherstellung, dass eine nicht zuvor aufgenommene Videositzung bei der Registrierung abgespielt wird (sogenannte Lebenderkennung).		✓
7. Durchführung der Identifikation und Übermittlung der Ergebnisdaten an den Swisscom Zertifizierungs- und/oder Vertrauensdienst.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
NFC-Identifikation per App		
1. Download der angegebenen App aus dem App-Store des Smartphones und Installation auf dem Smartphone. Die App kann ggfs. nicht in jedem länderspezifischen App-Store verfügbar sein.		✓

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
2. Download und Installation/Aktivierung der Signaturfreigabemethode, sofern notwendig		✓
3. Nutzung auf einem Smartphone mit einer Kamera (Minimalauflösung 1024 x 768 Pixel) bei ordentlichen Lichtverhältnissen (Lampe, Tageslicht). Smartphone muss mit einem NFC-Chip-Leser ausgestattet und für die Auslesung vorbereitet sein.		✓
4. Verwendung von Chip basierten ID aus ausgewählten EU/EWR Ländern und Schweiz bzw. Pässen. Die Verwendung von Aufenthaltsberechtigungen oder Führerscheine ist nicht möglich. Siehe Ziffer 4.2 für die Liste der berechtigten Dokumente.		✓
5. Sprachauswahl der Benutzerführung durch die Sprachwahl der Benutzeroberfläche/Smartphone, sofern keine extra Sprachwahl angegeben ist.		✓
6. Beantwortung aller von der App gestellte Fragen bzw. Befolgung der Anweisungen der App. Diese dienen der zusätzlichen Sicherheitsüberprüfung des Dokumentes bzw. auch der Sicherstellung, dass eine nicht zuvor aufgenommene Videositzung bei der Registrierung abgespielt wird (sogenannte Lebenderkennung).		✓
7. Durchführung der Identifikation und Übermittlung der Ergebnisdaten an den Swisscom Zertifizierungs- und/oder Vertrauensdienst.	✓	

Tätigkeiten (S = STS/ N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Auto- und NFC Identifikation per Browser		
1. Aufruf einer Browser Session auf dem Smartphone des Nutzers z.B. via QR code.		✓
2. Download und Installation/Aktivierung der Signaturfreigabemethode, sofern notwendig.		✓
3. Nutzung auf einem Smartphone mit einer Kamera (Minimalauflösung 1024 x 768 Pixel) bei ordentlichen Lichtverhältnissen (Lampe, Tageslicht). Für die Nutzung von NFC-Identifikationen muss das Smartphone mit einem NFC-Chip-Leser ausgestattet sein und für die Auslesung vorbereitet sein.		✓
4. Installation der Browsererweiterung für das NFC-Auslesen, sofern die NFC-Schnittstelle und ein chip basierter Ausweis verwendet werden soll.		✓
5. Beantwortung aller von der App gestellte Fragen bzw. Befolgung der Anweisungen der App. Diese dienen der zusätzlichen Sicherheitsüberprüfung des Dokumentes bzw. auch der Sicherstellung, dass eine nicht zuvor aufgenommene Videositzung bei der Registrierung abgespielt wird (sogenannte Lebenderkennung).		✓
6. Durchführung der Identifikation und Übermittlung der Ergebnisdaten an den Swisscom Zertifizierungs- und/oder Vertrauensdienst.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
eID-Identifikation		
1. Download der angegebenen App aus dem App-Store des Smartphones und Installation auf dem Smartphone. Ggfs. müssen weitere nationale Apps dazu installiert werden (je nach Land). Die App kann ggfs. nicht in jedem länderspezifischen Appstore verfügbar sein.		✓
2. Download und Installation/Aktivierung der Signaturfreigabemethode, sofern notwendig.		✓
3. Nutzung auf einem Smartphone mit einer NFC-Schnittstelle.		✓
4. Verwendung von ID aus ausgewählten EU/EWR Ländern und Schweiz. Siehe Kapitel 4.2 für die Liste der berechtigten Dokumente.		✓
5. Sprachauswahl der Benutzerführung durch die Sprachwahl der Benutzeroberfläche/Smartphone, sofern keine extra Sprachwahl angegeben ist.		✓
6. Beantwortung aller von der App gestellte Fragen bzw. Befolgung der Anweisungen der App. Diese dienen der zusätzlichen Sicherheitsüberprüfung.		✓
7. Durchführung der Identifikation und Übermittlung der Ergebnisdaten an den Swisscom Zertifizierungs- und/oder Vertrauensdienst.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
IdP Identifikation		
1. Geschäftsverhältnis mit dem anbietenden IdP und Besitz und Einsatz der nötigen Zugangsmittel, um sich beim IdP zu authentifizieren. Der Aufruf und die Verwendung der Zugangsmittel ist ggfs. beim IdP zu erfragen.		✓
2. Die Identifikation beim IdP muss so (in der Historie) erfolgt sein, dass sie auch kompatibel zu den Regularien und Gesetzen der geforderten elektronischen Signatur ist.		✓
3. IdP muss nicht gesetzeskonforme Identitätsfeststellungen herausfiltern und ablehnen	✓	
4. Die Nutzungsbestimmungen der Swisscom Trust Services müssen bei der erstmaligen Registrierung für den Signaturservice akzeptiert werden.		✓
5. Durchführung der Identifikation und Übermittlung der Ergebnisdaten an den Swisscom Zertifizierungs- und/oder Vertrauensdienst, sofern nicht vom IdP archiviert.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Kundeneigener IdP, Kundeneigene Identifikationsmethode und Signaturfreigabemethode		
1. Bestellung der entsprechenden Leistungen aus dem Onboarding Support zur Erlangung der Konformität für den betreffenden Rechtsraum und Signaturart. Abschluss eines Vertrages zur Delegation der Registrierungsstellentätigkeit.		✓
2. Erstellung eines Umsetzungskonzeptes und Meldung aller Konzeptänderungen und in diesem Fall Bestellung eines neuen Reviews für das geänderte Umsetzungskonzept		✓
3. Review des Umsetzungskonzeptes, Erstellung der Auditanfrage, Planung des Audits, Diskussion des Auditabschlussberichtes, Einreichung der neuen Methode bei den Aufsichtsstelle(n) zur Erlangung der Freigabe für den Einsatz.	✓	
4. Beseitigung aller Nichtkonformitäten, laufende Anpassung an neue Standards und Regularien, Einhalten aller für dieses Verfahren angewandten Regularien und Gesetze, regelmässige Wiederholungsaudits und Vollaudits (alle zwei Jahre). Bestellung über Swisscom Trust Services.		✓
5. Bereitstellung aller Informationen durch den Bereitsteller der Methode als Zulieferer zum Zertifizierungs- bzw. Vertrauensdienst als kritische Infrastruktur im Rahmen der NIS2 Direktive und entsprechenden nationalen Gesetzen. Selbstprüfung der relevanten Prüfpositionen zur Cybersecurity und Teilnahme am gemeinsamen jährlichen Audit mit Swisscom Trust Services.		✓
6. Durchführung der notwendigen Audits mit dem Bereitsteller der Methode im Rahmen der kritischen Infrastrukturen.	✓	
7. Verantwortung für die konforme Durchführung der Identifikation und Bereitstellung der Evidenz, Meldung aller Verstösse und Auffälligkeiten sehr zeitnah an Swisscom Trust Services.		✓

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Password – Einmalcode Signaturfreigabemethode		
1. Setzen und sicheres Vermerken/Notieren des für die Signatur zu verwendenden Passworts. Dieses kann während der Nutzungsdauer nicht mehr zurückgesetzt werden! In diesem Falle ist eine neue Registrierung notwendig.		✓
2. Verwendung einer SIM-Karte eines Netzbetreibers, der SMS (ggfs. Roaming) aus dem Netz der Swisscom (Schweiz) AG oder des Anbieters seven.io oder Horisen empfangen kann. Das kann in einigen ausländischen Staaten problematisch sein, bestimmte Staaten lassen keinen SMS-Empfang aus dem Ausland ohne Anmeldung zu. Über die Mobilnummer der SIM-Karte wird der Einmalcode zugesendet.		✓
3. Eingabe von Passwort und Einmalcode in die vorgesehenen Eingabefenster.		✓
4. Bereitstellen der Eingabefenster. Im Rahmen eines Workflows der Teilnehmerapplikation werden die Fenster als parametrisierbare iFrames angeboten. Die Parametrisierung kann unter https://github.com/SwisscomTrustServices/AIS/wiki/SAS-Documentation eingesehen werden	✓	
5. Nutzung der 2-Faktoreingabe von Passwort und Einmalcode zur Signaturauslösung, sowie Protokollierung und Archivierung dieser Willensbekundung.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Mobile ID-Verfahren		
1. Nutzung einer Schweizer SIM-Karte, die Mobile ID ermöglicht		✓
2. Initialisierung der Mobile ID auf dem Smartphone mit der Mobile ID fähigen SIM-Karte auf https://mobileid.ch . Sicheres Archivieren des während der Aktivierung angezeigten Wiederherstellcodes für eine Aktivierung auf einem anderen Smartphone. Wird Mobile ID auf einem anderen Smartphone verwendet ohne den Wiederherstellcode muss der Nutzer sich neu registrieren.		✓
3. Setzen und sicheres Merken/Verwahren der 6-stelligen PIN, die beim Aufruf der Mobile ID immer eingegeben werden muss.		✓
4. Verwendung einer SIM-Karte eines Netzbetreibers, der SMS (ggfs. Roaming) aus dem Netz der Swisscom (Schweiz) AG oder des Anbieters seven.io bzw. Horisen empfangen kann. Das kann in einigen ausländischen Staaten problematisch sein, bestimmte Staaten lassen keinen SMS-Empfang aus dem Ausland ohne Anmeldung zu. Über die Mobilnummer der SIM-Karte wird der Einmalcode zugesendet. Die SMS wird für die Initialisierung der Mobile ID verwendet. Schweizer Mobilfunkanbieter akzeptieren alle Swisscom SMS.		✓
5. Eingabe der PIN zur Signaturfreigabe.		✓
6. Aufruf der Mobile ID auf dem Gerät des Signierenden zur Signaturauslösung, sowie Protokollierung und Archivierung dieser Willensbekundung.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Mobile ID App Verfahren		
1. Download der Mobile ID App aus dem App-Store des Smartphones und Installation auf dem Smartphone. Die App ist nicht in jedem Land im App Store verfügbar.		✓
2. Initialisierung der Mobile ID App auf dem Smartphone und Einrichten eines zweiten Faktors, z.B. einer Gesichtserkennung oder eines Fingerprints. Sicheres Archivieren des während der Aktivierung angezeigten Wiederherstellcodes für eine Aktivierung auf einem anderen Smartphone. Wird Mobile ID App auf einem anderen Smartphone verwendet ohne den Wiederherstellcode, muss der Nutzer sich neu registrieren.		✓
3. Verwendung einer SIM-Karte eines Netzbetreibers, der SMS (ggfs. Roaming) aus dem Netz der Swisscom (Schweiz) AG oder des Anbieters seven.io oder Horisen empfangen kann. Das kann in einigen ausländischen Staaten problematisch sein, bestimmte Staaten lassen keinen SMS-Empfang aus dem Ausland ohne Anmeldung zu. Über die Mobilnummer der SIM-Karte wird der Einmalcode zugesendet. Die SMS wird für die Initialisierung der Mobile ID App verwendet.		✓
5. Aktivierung des biometrischen Faktors zur Signaturfreigabe.		✓
6. Aufruf und Nutzung der Mobile ID zur Signaturauslösung, sowie Protokollierung und Archivierung dieser Willensbekundung.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
FIDO2 Verfahren (z.B. Passkey)		
1. Verwendung eines Gerätes (PC, Smartphone, USB Stick FIDO2 kompatibel, etc.) bzw. einer Software auf einem Gerät, welche den FIDO2 Standard oder Passkey unterstützt.		✓
2. Erstmalige Erstellung des FIDO2 Schlüssels/passkey. Danach Nutzung auf allen Geräten, auf denen dieser Key (ggfs. synchronisiert durch Systemdienste der Betriebssystemhersteller oder Softwarehersteller) bereitsteht. Verantwortlichkeit für die Sicherheit des Passkeys, des privaten FIDO2 Schlüssels und etwaiger Synchronisation.		✓

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
IdP Signaturfreigabe		
1. Geschäftsverhältnis mit dem anbietenden IdP und Besitz und Einsatz der nötigen Zugangsmittel, um sich beim IdP zu authentifizieren. Der Aufruf und die Verwendung ist ggfs. beim IdP zu erfragen.		✓

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
2. Für die Nutzung der IdP Signaturfreigabe muss die Registrierung zwingend beim IdP erfolgen.		✓
3. Aufruf und Nutzung der gewählten IdP Signaturfreigabe zur Signaturauslösung, sowie Protokollierung und Archivierung dieser Willensbekundung.	✓	

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Signaturfreigabe SDK		
1. Einbettung des Software Development Kits in eine eigen gestaltete App zur Signaturfreigabe. Berücksichtigung der Initialisierungsparameter (z.B. PIN-Länge, biometrische Faktoren etc.). Diese werden von Swisscom Trust Services zur Verfügung gestellt.		✓
2. Erstellung eines Einsatzkonzeptes für das SDK, welches konforme Nutzung und die App Veröffentlichung beschreibt. (Vorlage wird von Swisscom zur Verfügung gestellt)		✓
3. Abnahme des Konzeptes und Freischaltung zur Nutzung.	✓	
4. Initialisierung der App und damit des SDK auf dem Smartphone und Einrichten eines zweiten Faktors, z.B. einer Gesichtserkennung oder eines Fingerprints sowie eines PINs als Rückfalllösung. Ggfs. sicheres Archivieren des während der Aktivierung angezeigten Wiederherstellcodes für eine Aktivierung auf einem anderen Smartphone. Wird das SDK mit der zugehörigen App auf einem anderen Smartphone verwendet ohne den Wiederherstellcode muss der Nutzer sich neu registrieren.		✓
5. Aktivierung des biometrischen Faktors zur Signaturfreigabe.		✓
6- Aufruf und Nutzung der Signaturfreigabe SDK zur Signaturauslösung, sowie Protokollierung und Archivierung dieser Willensbekundung.	✓	
7. Bestellung eines Walkthroughs durch den Auditor (geschätzt 2 Personentage) an STS		✓
8. Platzierung des Auditauftrages zum Walkthrough beim Auditor	✓	
9. Update des Einsatzkonzeptes bei jeder Änderung. Befolgung der Freigabeprozeduren für jedes Update gemäss freigegebenen Einsatzkonzept.		✓
10 Abnahme des geänderten Konzeptes, ggfs. Auditbeauftragung und Freischaltung zur Nutzung.	✓	
11 Kosten des Auditors durch Swisscom in Rechnung gestellt		✓

Tätigkeiten (S = STS/N = Nutzer, d.h. Besteller dieser Leistung)	S	N
Swisscom Signaturfreigabe App		
1. Download der Signaturfreigabe App aus dem App-Store des Smartphones und Installation auf dem Smartphone. Die App ist nicht in jedem Land im App Store verfügbar.		✓
2. Initialisierung der Signaturfreigabe App auf dem Smartphone und Einrichten eines zweiten Faktors, z.B. einer Gesichtserkennung oder eines Fingerprints und eines PINs als Rückfallposition. Falls ein Wiederherstellcode angeboten wird, auch sicheres Archivieren des während der Aktivierung angezeigten Wiederherstellcodes für eine Aktivierung auf einem anderen Smartphone. Wird die Signaturfreigabeapp auf einem anderen Smartphone verwendet ohne den Wiederherstellcode, muss der Nutzer sich neu registrieren.		✓
3. Aktivierung des biometrischen Faktors zur Signaturfreigabe.		✓
4. Aufruf und Nutzung der Signaturfreigabe App zur Signaturauslösung, sowie Protokollierung und Archivierung dieser Willensbekundung.	✓	

6 Service Level

6.1 Service Level

6.1.1 Genereller Service Level der Swisscom Trust Services für alle Dienste

Die nachfolgenden Service Levels beziehen sich grundsätzlich auf die vereinbarte Monitored Operation Time für die Bereitstellung der Services inklusive der Services der Partner. Damit sind insbesondere die Services der Bereitstellung der Verfahren in den Stores und auf der Registrierungswebseite gemeint, sowie die Supportzeiten für die allgemeine Ticketentgegennahme 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			Registrierung & Signaturfreigabe
Operation Time			
Monitored Operation Time	Mo-So	00:00-24:00	●
Provider Maintenance Window	PMW-DC	PMW Data Center Swisscom (Schweiz) AG	●
	PMW-S: mit Vorankündigung für sicherheits- und systemkritische Updates	Täglich 19:00-07:00, nur für angekündigte Wartungen	●
Support Time			
Support Time [1]	Mo-Fr	08:00-17:00[2]	●
Störungsannahme	Mo-So	00:00-24:00	●
Availability			
Service Availability			
• 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

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

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

6.1.2 Besondere SLAs pro verwendetes Verfahren

Die Tabelle unten enthält pro Verfahren weitere SLA Werte:

- Standardausprägung und Partner: spezifisches Verfahren, für das SLA-Werte angegeben werden
- Operation Time: Zeit, während der Registrierungen stattfinden können. Bei Services mit menschlicher Bearbeitung (auch im Hintergrund) benötigt es einige Zeit, bis die Ergebnisse validiert wurden
- Bearbeitungszeit bis zur Einlieferung: Aufgrund von Backgroundchecks können sich nach Abschluss der Identifikation weitere Bearbeitungszeiten ergeben, bis dass das Ergebnis der Identifikation Swisscom Trust Services übergeben wurde und die erste Signatur geleistet werden kann. Die Zeiten beziehen sich nur auf die Operation Time.
- Link Verfallszeiten: Im Falle einer Registrierung über das Registrierungsportal der Swisscom Trust Services erhalten die Nutzer Links mit den Weiterleitungen zu den Identifikationspartner, so dass im Falle eines Fehlers oder Abbruchs die Identifikation kostenfrei wiederholt werden kann. Die Links werden nach Bezahlung oder Einlösung des Gutscheins per E-Mail dem Empfänger zugesendet. Sie unterliegen Verfallsdaten und müssen zeitnah genutzt werden. 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. Bei Methoden, die im Store angeboten werden, spielen diese Parameter keine Rolle.

- Zu beachten sind die Feiertage der Partner, die sich in der Regel wie Sonntage auswirken:
  Schweiz: 1. Und 2. Januar, Karfreitag, Ostermontag, Pfingstmontag, Auffahrt, 1. August, 25. Und 26. Dezember

Standardausprägung	Partner	Operation Time	Bearbeitungszeit bis Einlieferung	Link Verfallszeiten (Tage)	Anzahl Wiederholungen	Sonstige SLA
Standardidentifizierungen						
Videoidentifikation, App basiert	IDNow Gmbh, Deutschland	Mo.-So. 7h00-24h00	Max. 20 Minuten	90	Keine Begrenzung	Gemessene Aufnahme der Calls auf Monatsbasis: 80% während der ersten 90 Sekunden 90%, während der ersten 120 Sekunden, 95% während der ersten 180 Sekunden.
eID Identifikation (Deutschland), App basiert	IDNow Gmbh, Deutschland	Mo.-So. 7h00-24h00	Binnen Sekunden	90	Keine Begrenzung	
Auto-Identifikation, Browser basiert	Fidentity AG, Schweiz	Autoident: Mo.-Fr. 8h00-18h00 Sa. 8h00-12h00 (erweitertes SLA auf Anfrage)	Max. 3 Minuten	Diese Parameter spielen im Store Modell keine Rolle		
NFC Identifikation, Browser basiert	Fidentity AG, Schweiz	7 Tage/24h	Max. 3 Minuten	Diese Parameter spielen im Store Modell keine Rolle		
Autoidentifikation, App basiert	Nect GmbH, Deutschland	7 Tage / 24 Stunden	Max. 2 Minuten	30	5	

Standardausprägung	Partner	Operation Time	Bearbeitungszeit bis Einlieferung	Link Verfallszeiten (Tage)	Anzahl Wiederholungen	Sonstige SLA
Auto Identifikation, App basiert	ti&m AG, Schweiz	Mo.-Fr. 8h00-20h00 Sa. 8h00-16h00 7 Tage/24 Stunden auf Anfrage und Aufpreis	Max. 5 Minuten	Diese Parameter spielen im Store Modell keine Rolle		Techn. Verfügbarkeit auf Jahresbasis 99.5%
NFC Identifikation, App basiert	ti&m AG, Schweiz	7 Tage / 24 Stunden	Max. 5 Minuten	Diese Parameter spielen im Store Modell keine Rolle		Techn. Verfügbarkeit auf Jahresbasis 99.5%
Videoidentifikation, App basiert	Intrum AG, Schweiz	Mo. – Sa. 7h00 – 22h00	Max. 15 Minuten	90 Bei der Verwendung im Store spielen diese Parameter keine Rolle	Keine Begrenzung	
Autoidentifikation, App basiert	Intrum AG, Schweiz	Mo. – Sa. 7h00 – 22h00	Max. 15 Minuten	90 Bei der Verwendung im Store spielen diese Parameter keine Rolle	Keine Begrenzung	
IdP Identifikationen						
IdP Identifikation mit Postfinance App	Postfinance AG, Schweiz	7 Tage / 24 Stunden	Binnen Sekunden			

6.1.3 Gültigkeit von Gutscheincodes

Für das Registrierungsportal der Swisscom Trust Services 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.

7 Rechnungsstellung und Mengenreport

Der Nutzer erhält per E-Mail im Falle der Kreditkartenzahlung einen Zahlungsbeleg inklusive Höhe der Mehrwertsteuer. Gutscheinkunden erhalten eine Rechnung. Alle anderen Nutzer erhalten Reports über die erfolgreichen Registrierungen und Signaturfreigaben, für die sie bezahlt haben. Die Preise ergeben sich aus den Preisankündigungen auf der Webseite oder dem Bestellformular für die Gutscheine.

8 Besondere Regelungen

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

Die Archivierung der von den Identifikationspartnern übermittelten Identifikationsdaten findet ausschliesslich auf Swisscom Servern in der Schweiz statt. Je nach vom Nutzer gewählter Identifikationsmethode werden im Servicevertrag benannte Identifikationspartner aus der EU und der Schweiz beigezogen, die die jeweilige Identifikation durchführen. Diese Identifikationspartner sind im Rahmen der Übertragung der Datenverarbeitung vertraglich zum Datenschutz gemäss DSGVO bzw. DSG verpflichtet.
Swisscom (Schweiz) AG bzw. Swisscom ITSF schliesst mit den externen Identifikationspartnern 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.

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

Das Angebot der Signaturen und Registrierungen der 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.

8.3 Austausch von Methoden, Abschaltung von Methoden

Swisscom bietet die Registrierungs- und Signaturfreigabemethoden unter folgenden Voraussetzungen an:

- Die Methoden sind auditiert und für die Signaturerstellung regulatorisch und gesetzlich freigegeben.
- Die Anbieter halten die Auflagen entsprechend ein.

Sollte sich die Regulatorik ändern oder Ereignisse eintreten, die den Fortbestand der Identifikation oder Signaturfreigabe nicht mehr weiter ermöglichen (z.B. nicht bestandenes Audit, Aufgabe der Geschäftstätigkeit des Anbieters, etc.) so steht es Swisscom frei, die angebotene Methode durch eine gleichwertige Methode zu ersetzen oder die Methode komplett aus dem Angebot herauszunehmen. In letzterem Fall besteht ein ausserordentliches Kündigungsrecht durch den Kunden.

Im Rahmen von Pauschalangeboten, die in einem Preis sowohl Registrierung, Signaturfreigabe und Signatur ermöglichen ist der Austausch von Anbietern gleichartiger Methoden jederzeit möglich.

8.4 Abgrenzung bei der Nutzung der Identifikationsdaten, Identifikationspartner für weitere, eigene Zwecke

Grundsätzlich hat der Nutzer mit verschiedenen Identifikationsverfahren nach Anfrage und Absprache die Möglichkeit, für die Erfüllung eines eigenen Zwecks direkt mit dem Identifikationspartner ebenfalls einen Vertrag zur Durchführung desselben Identifikationsprozesses und zur Nutzung der dadurch gewonnen Evidenz abzuschliessen (z.B. im Rahmen der Geldwäschebekämpfung), sofern der Identifikationspartner das anbietet. In diesem Fall wird der aus diesem Vertrag erstellte Identifikationsdatensatz mit den signaturrelevanten Daten nicht nur dem Swisscom Zertifizierungs- und/oder Vertrauensdienst zur Verfügung gestellt, sondern auch – ggfs. noch angereichert mit weiteren Daten – dem Nutzer.
Dieser Prozess setzt den Abschluss von zusätzlichen, untereinander abgestimmten Verträgen voraus (einerseits zwischen Nutzer und Identifikationspartner und andererseits zwischen Identifzierer und Swisscom Trust Services oder dem Swisscom Zertifizierungs- und Vertrauensdienst), die nicht Gegenstand dieser Leistungsbeschreibung sind.
Falls der Nutzer von dieser Möglichkeit Gebrauch macht und es zum Abschluss dieser Verträge kommt,

- ist der Nutzer im Rahmen der vorliegenden Leistungsbeschreibung dafür verantwortlich, seinen Signierenden Geschäftsbedingungen vorzulegen, in denen das Konstrukt, zusammen mit einer transparenten Datenschutzregelung, dargelegt wird.
- ist der Nutzer verpflichtet, Swisscom Trust Services vor der Aufschaltung eines Registrierungsverfahrens auf das Bestehen eines Vertrags mit einem Identifikationspartner hinzuweisen.