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

White Paper

Smart Registration Service

Swisscom Trust Services

Swisscom Trust Services

Inhaltsverzeichnis

Einführung

Die elektronische Signatur ist im Vormarsch. Immer mehr Online-Prozesse können nun erfolgreich abgeschlossen werden, da der letzte Baustein, der für die Vertragsabschlüsse benötigt wird, nun verfügbar ist: die Online-Signatur. Der Mehrwert der Durchgängigkeit von Online-Prozessen ist seit langem jedem eindeutig: kostensparend, ökologisch und benutzerfreundlich.
Rechtlich am sichersten ist immer noch die qualifizierte elektronische Signatur, wie sie der Gesetzgeber in der EU mit der eIDAS Verordnung oder in der Schweiz mit der ZertES Gesetzgebung definiert. Alle anderen Signaturen, wie fortgeschrittene Signaturen oder einfache Signaturen bis hin zu eingescannten Bildunterschriften können zwar in bestimmten Prozessen genutzt werden, die Beweiskraft muss aber gegebenenfalls vor Gericht gesondert festgestellt werden.

An die qualifizierte Signatur werden hohe Anforderungen gestellt in Bezug auf die Feststellung der Identität der Person. Das hat bisher auch die Ausbreitung verhindert. Mit dem Smart Registration Service der Swisscom Trust Services wird ein Bündel alternativer und sehr innovativer Methoden für die Identifikation angeboten, die eine online-Identifikation durch jedermann möglich machen.

Einmal passend identifizieren – beliebige Freigaben mit Authentisierung

Der Smart Registration Service löst dabei verschiedene Problematiken:

- In der EU gelten andere Anforderungen an die Identifikation wie in der Schweiz. Wenn jemand identifiziert werden soll, muss sicher sein, dass diese Identifikation auch für den gewählten Rechtsraum möglich ist. Beispielsweise darf die Videoidentifikation in der Schweiz nur im Zusammenhang mit Finanzintermediären eingesetzt werden.
- Bestimmte Verfahren – wie z.B. eine Autoidentifikation ohne menschlichen Operator – ermöglichen zwar eine fortgeschrittene Signatur aber keine qualifizierte Signatur.
- Organisationen müssen nicht nur für die elektronische Signatur identifizieren, sondern benötigen den Identifikationssatz auch noch selber, z.B. für die Bekämpfung der Geldwäsche.
- Nicht immer reicht eine Identifizierungsmethode aus, z.B. hat der zu identifizierende Benutzer zu wenig Bandbreite, um eine Videoidentifikation zu starten, oder er hat keine eID. Verschiedene Methoden aus einer Hand und ein Protokoll und Ansprechpartner ist hier die Antwort.
- Bisher war häufig eine elektronische Unterschrift immer mit dem vorherigen Schritt einer Identifikation verbunden, d.h. drei Unterschriften binnen zweier Wochen verlangten auch drei Identifikationen. Swisscom ermöglicht die Verbindung einer einmaligen Identifikation mit einer Authentisierung: d.h. demnächst kann mit einer PIN, Fingerprint, Gesichtserkennung ohne vorherige weitere Identifikation unterzeichnet werden.

Definitionen und Abkürzungen

Identifizierer (im technischen Protokoll "Identifizierung Service Provider" oder „ISP“ genannt)
Der Anbieter von Identifizierungslösungen ist ein Swisscom-Partner, der eine Lösung zur Identifizierung einer Person entwickelt hat. Diese Lösung bietet eine bestimmte Stufe der Identifikation, d.h. er kann entweder nur fortgeschritten oder qualifiziert unterzeichnen. Ein einziger Identifizierer wird in der Lage sein, mehrere Identifizierungsmethoden vorzuschlagen. Beispielsweise bietet ein Identifizierer Videoidentifikation oder eine Auto-Onlineidentifikation (OID) an, bei der sich der Benutzer selbst registriert.

Swisscom Kunde (Im technischen Protokoll „Service Provider“ oder „SP“ genannt)
Service Provider ist ein Swisscom Kunde für den Smart Registration Service, der seinen potentiell zu identifizierenden Personen ein Webportal oder Startpunkt für die Identifikation anbietet. Dieser Startpunkt kann völlig losgelöst von einer Signatur erfolgen. Es kann z.B. auch möglich sein, dass der Swisscom Kunde gar keine Signatur selber anbietet, sondern die identifizierte Person an ein Signaturportal eines anderen Partners von Swisscom weiterverweist.

Die Lösung an einem Beispiel erklärt

Bob hat ein PDF Dokument erhalten und muss es **digital unterschreiben**. Das hat er noch nie gemacht!
Bob wählt einen Online-Dienstleister, der diese Möglichkeit auf seinem Webportal anbietet. Er erstellt schnell ein Konto und überträgt sein Dokument.

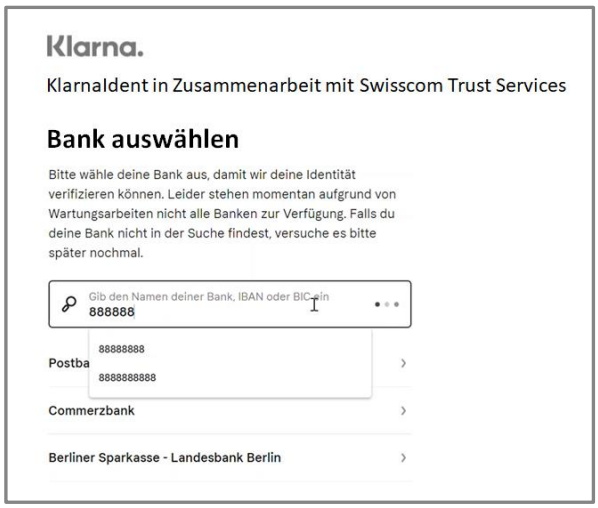
Ups! Bob wurde noch nicht für die Unterschrift aktiviert, da er noch nie zuvor identifiziert wurde! Kein Problem, Bobs nun bevorzugtes Signierportal führt ihn zu einem Swisscom Identifizierer, der in diesem Fall die Video Identifikation anbietet.
Nach ein paar Minuten Kontakt mit einem netten operator, der seinen gültigen Personalausweis gerne über die Webcam gezeigt bekommen möchte, wird Bob zurück zum Signaturportal geführt.

Nun kann Bob seine Signatur aktivieren!
Die Willensbekundung zur Signatur gibt er einfach mit seiner MobileID in der Schweiz oder einer Kombination von Passwort und Einmal-SMS Code anderswo oder er nutzt demnächst die bequeme MobileID App und gibt die Zustimmung mit Gesichtserkennung oder Fingerprint. Fertig! Und so signiert er beim nächsten Mal wieder, ohne vorherige Identifikation!

Swisscom Trust Services

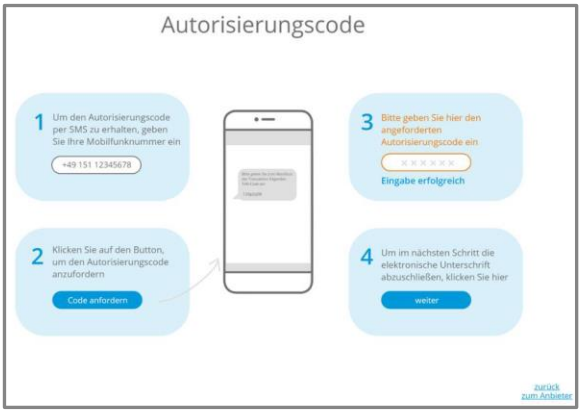
Verfügbare Identifizierungs Methoden

Neben der klassischen Videoidentifikation ist sicherlich die Bankidentifikation interessant:



Ein kurzes Login in das Online Banking einer deutschen Bank ermöglicht die gleiche Identifikationsstufe für die qualifizierte elektronische Identifikation in Europa wie die Videoidentifikation.
Zudem kann dann die elektronische Signatur auch für Identifikationen im Rahmen der Geldwäschebekämpfung nach deutschem GWG Gesetz genutzt werden. Der Identifizierer Klarna ermöglicht ein Banklogin mit fast allen deutschen Banken.

Ebenfalls interessant ist der deutsche Personalausweis mit seiner eID Funktionalität. Die Authada ermöglicht mit Ihrer App von jedem NFC fähigen Mobilgerät aus eine direkte einfache Identifikation: einmal Ausweis an das Gerät heranhalten und Freigabe PIN Code eingeben. Fertig!



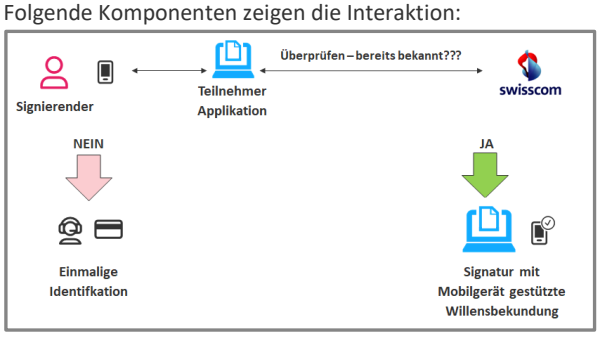
Für fortgeschrittene Signaturen steht bereits eine Online Auto Videoidentifikation zur Verfügung, d.h. ein Identifikationsdienst, der in der Regel ohne Operator arbeitet und biometrisch das Videobild mit dem Ausweis vergleicht und die Lebendigkeit im Video nachweist.

Weitere Methoden sind geplant:

- Kurierdienst – klingelt bis zu 3x an der Haustür
- Point of Sales Identifikation – vor Ort an ausgewählten Stationen

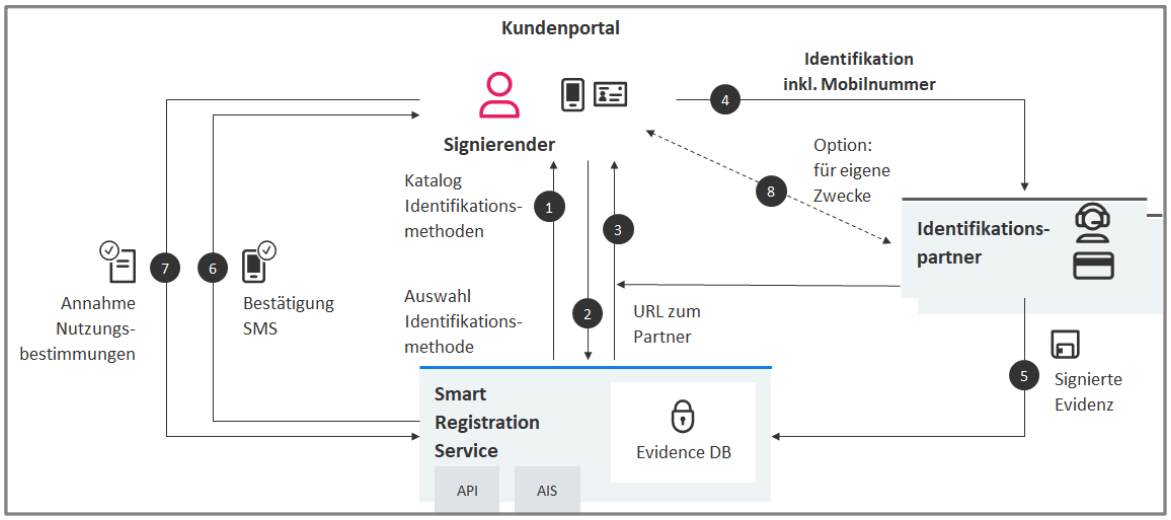
Funktionsweise – technische Beschreibung

Folgende Komponenten zeigen die Interaktion:



Die Signaturapplikation überprüft zunächst (sogenannter „verify-call"), ob ein Signierender die gewünschte Signatur im jeweiligen Rechtraum mit der Stufe fortgeschritten oder qualifiziert durchführen kann und bei Swisscom bereits registriert ist. Ist das nicht der Fall, ist eine einmalige Vorabidentifikation notwendig, ansonsten kann sofort identifiziert werden.

Für die einmalige Identifikation bietet der Swisscom Kunde nun z.B. in seinem Portal eine Möglichkeit für den zukünftig Signierenden an, mehrere Identifikationsmethoden auszuwählen:



Das Portal kommuniziert dabei wie folgt:

(1) Es fragt bei Swisscom den Katalog der möglichen Identifikationsmethoden an, diese werden mit dem zugelassenen Rechtsraum (eIDAS- EU/ ZertES – CH) übermittelt und der Identifikationsstufe, die besagt, welche Signatur möglich ist: Fortgeschritten (FES) oder Qualifiziert (QES)

(2) Eine Identifikationsmethode wird ausgewählt

(3) Swisscom eröffnet einen Auftrag beim Identifizierer und stellt eine URL bereit zum Portal des Identifizierers.

(4) Die zu identifizierende Person wird nun auf das Portal des Identifizierers weitergeleitet und identifiziert sich. Gleichzeitig wird die Mobilnummer registriert. Darauf basierend kann sie demnächst Willensbekundungen zur Signatur durchführen.

(5) Der Identifizierer übergibt Swisscom die Evidenz der Identifikation und des registrierten Authentifizierungsmittels.

(6) Über die angegebene Mobilnummer fragt Swisscom per SMS den zukünftig Signierenden an, den Nutzungsbestimmungen zuzustimmen.

(7) Der Nutzer öffnet den Link in der SMS und stimmt den Nutzungsbestimmungen auf einem Portal von Swisscom zu.

(8) Im Rahmen der Bekämpfung der Geldwäsche kann es notwendig sein, dass der Service Provider ebenfalls die Evidenz der Identifikationsdaten benötigt. Das geschieht aufgrund eines Zusatzvertrages zwischen Service Provider und Identifizierer.

Service Integration für den Kunden (Service Provider/SP)

Zur Implementierung der Lösung verwendet Swisscom Standardprotokolle.
Der Zugang und die Autorisierung des Dienstes erfolgt über einen von Swisscom bereitgestellten Zugangsschlüssel ("Access Key" - der Kunde als Service Provider wurde zuvor während des Onboardings registriert)

- Der Service Provider vewendet das OAUTH 2.0 Protokoll mit JWT („Jason Web Token“). Diese dienen später der Autorisierung beim Identifizierer.
- Mit einem OAUTH Introspect Aufruf wird die Anfrage zur Gültigkeit eines Antrages zur Identifikation angefragt.
- Nachdem die Gültigkeit des Tokens bestätigt wurde, kann die Identifizierung erfolgen.
- Am Ende der Identifizierung wird der Identifizierer einen Identifizierungsstatus angeben, der auf Anfrage jederzeit vom Kunden angefordert werden kann.
- Swisscom bietet eine Schnittstelle und eine detaillierte Anleitung, die es dem Service Provider ermöglicht, die Lösung einfach und in kürzester Zeit zu integrieren.
- Die Integration ist nach Abschluss eines Servicevertrages zum Smart Registration Service möglich.
- Die Schnittstelle orientiert sich am „REST“ Ansatz.
- Swisscom pflegt die Schnittstelle zum Identifizierer, so dass sich der Service Provider nicht um Schnittstellenanpassungen beim Identifizierer kümmern muss.

Ist ein Benutzer bereits registriert? ("Verify Call")

Diese Funktion überprüft einfach, ob ein Benutzer bereits ordnungsgemäß für die Signatur registriert wurde. Durch die Angabe der entsprechenden Parameter kann ermittelt werden, ob der Benutzer für die angegebene Rechtsraum unterschreiben kann und für welche Signatur Qualität: fortgeschrittene elektronische Signatur oder qualifizierte elektronische Signatur. LOA – bedeutet in Englisch "Level of Assurance".
Im folgenden Beispiel kann der Service Provider feststellen, ob der Benutzer mit der Beispieltelefonnummer und den Identitätselementen eine qualifizierte elektronische Signatur (LOA4) gemäß eIDAS und ZertES ausführen kann.

```
{
  "msisdn": "41791234567",
  "claimedIdentity": "test-client",
  "assuranceLevel": 4,
  "distinguishedName": "gn=Hans, sn=Müller, cn=Hans Müller, c=CH"
}
```

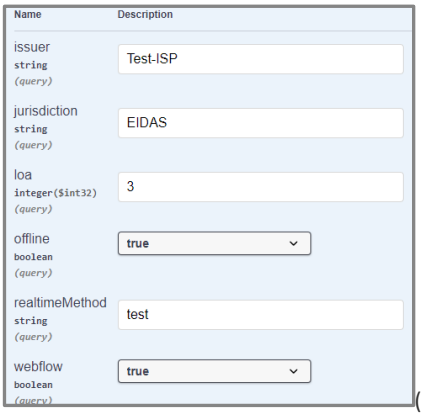
Hier ist z. B. die positive Antwort der Schnittstelle. Sie übergibt dabei in <string> die entsprechend hinterlegte Werte, die im Signaturaufruf genutzt werden: die evidenceID (eindeutig hinterlegte Seriennummer zur Evidenz), vetterMsisdn (die hinterlegte Mobilnummer), serialNumber (eineindeutige Seriennummer des Identifizierten aufgrund der Mobilnummer):

```
{
  "evidenceId": "string",
  "vetterMsisdn": "string",
  "serialNumber": "string"
}
```

Auf der Grundlage dieser positiven oder negativen Reaktion kann der Service Provider entweder den Identifizierungsprozess oder die direkte Signatur initiieren.
Beachten Sie, dass für diese Schnittstelle keine Authentifizierung erforderlich ist.

Abfrage der Liste der verfügbare Methoden

Diese Funktion enthält einen Katalog der verfügbaren Identifizierungsmethoden. Der Service Provider verfügt auch über einen Filter, um vorab Methoden auszufiltern. Hier ist ein Beispiel, in dem der Service Provider einen bestimmten Identifizierer (ISP) verwenden möchte ("Test-ISP" in unserem Beispiel)



(*)

Die Anforderung, die der Service Provider stellen wird, ist:

```
curl -X GET "https://miss-backend-api-dev.scapp.swisscom.com/api/providers?issuer=Test-ISP&jurisdiction=EIDAS&loa=3&offline=true&realtimeMethod=test&webflow=true" -H "accept: application/vnd.sc.miss.provider.v1+json"
```

Und die erhaltene Antwort wird in unserem Beispiel eine Methode mit den Elementen und Parametern sein, um diese Methode zu implementieren:


```
[
  {
    "loa": 3,
    "issuer": "Test-ISP",
    "webflow": true,
    "jurisdiction": "ZERTES,EIDAS",
    "realtimeMethods": [
      "video",
      "test"
    ],
    "offline": true,
    "identificationData": [],
    "additionalData": [],
    "defaultLocale": "en"
  }
]
```


(*) Filterdaten und Einstellungen können sich ändern

Folgende Filter sind hierbei möglich:

Filterparameter	Definition	Beispiel
loa	Level of Assurance	Wenn der Service Provider LOA 4 angibt dann erhält er nur die Methoden, die LOA 4 (QES) zulassen und nicht LOA 3 (FES)
issuer	Identifikationsprovider	Hier kann der Service Provider den Identifizierer auswählen falls er diesen Partner bevorzugt
webflow	Kein Medienbruch	Der Service Provider will hier Identifikationsmethoden ohne Medienbruch, z.B. kein Kurierdienst oder POS
jurisdiction	Rechtsraum gemäss Signaturgesetz der Schweiz oder Signaturverordnung in der EU	Schweiz: «ZERTES», EU: «EIDAS»
realtimeMethods	Onlinemethoden der Identifikation, die zur Verfügung stehen	Z.B. „video“ als Videoidentifikation
Offline identification process	Offlineprozess notwendig	z.B. Schalterbesuch oder Kurier
Identification data /additional data	Vorabidentifikationsdaten	Kunde möchte dem Identifizierer seine Bestandsdaten der zu identifizierenden Person mitgeben

Starten der Identifizierungsprozess mit der gewählten Methode

Nachdem die Methode aus den in der vorherigen Phase vorgeschlagenen Methoden ausgewählt wurde, wird ein Antrag auf Identifizierung gestellt, um den Prozess zu starten. Im Antrag müssen folgende Parameter mitgegeben werden:

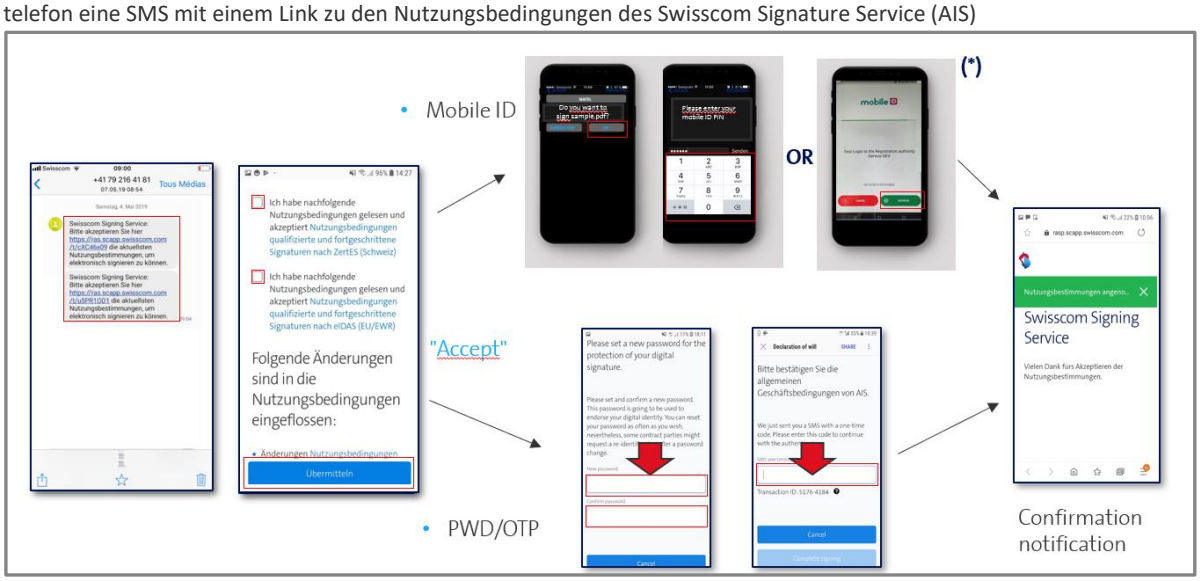

```
{
  "dob": "1978-02-28",
  "email": "hans.muster@swisscom.com",
  "firstName": "Hans",
  "language": "en",
  "lastName": "Muster",
  "mobile": "+41783478228"
}
```


Anbei die Antwort der Schnittstelle:


```
{
  "refId": "5c327977-a154-4747-b99d-c0733f7007c5",
  "error": null
  "targetURL": https://www.identity.tm/status_neu/1ABF5CD5DBEA405B20AEB9142448570D
}
```


Der Link zum Starten der Identifizierung durch den Identifizierer wird bereitgestellt. Der Serviceprovider muss die zu identifizierende Person auf diese URL leiten und der Identifizierungsprozess kann beginnen.

Während der Identifizierung wird auch die Mobiltelefonnummer des Benutzers überprüft, da sie zum Zeitpunkt der Signatur für die Authentifizierung verwendet wird. Am Ende des Identifizierungsprozesses erhält der Nutzer auf seinem Mobiltelefon eine SMS mit einem Link zu den Nutzungsbedingungen des Swisscom Signature Service (AIS)



Nach Zustimmung zu diesen Nutzungsbedingungen kann der Nutzer sein Dokument elektronisch signieren.

Identifizierungsstatus ermitteln

Der Service Provider kann jederzeit den Status erhalten, um festzustellen, ob der Benutzer die Identifizierung bereits abgeschlossen hat. Es kann auch feststellen, ob ein Problem während der Identifizierung aufgetreten ist.
Anforderung für Statusanforderung:

```
https://miss-backend-api-dev.scapp.swisscom.com/api/identifications/c3ee9d79-0250-4d1b-805b-e72d591b9f23
```

Hier ist die Antwort von Swisscom auf den Status der Identifizierung:
Die Identifikation ist abgeschlossen und die Evidenz ist erstellt!

Response body

```
{
  "refId": "62c3ee9d79-0250-4d1b-805b-e72d591b9f23
  "orderId": "
  "issuer": "test",
  "adapter": "fake",
  "method": "video",
  "mobile": "+41775383140",
  "evidenceId": null,
  "statuses": [
    {
      "status": "created",
      "date": "2019-11-25T09:19:20.165Z",
      "reason": null,
      "kind": null
    },
    {
      "status": "created",
      "date": "2019-11-25T09:25:28.779991Z",
      "reason": null,
      "kind": null
    },
    {
      "status": "initialized",
      "date": "2019-11-25T09:19:20.192Z",
      "reason": null,
      "kind": null
    }
  ]
}
```


Andere Statusmeldungen (*) :

Statusmeldung	Bedeutung
"Waiting for Doc"	Das System wartet auf den Import der Evidenz
"Identification done"	Die Identifikation wurde durchgeführt Die Daten der Identifikation (Evidenz) sind aber ggfs. noch nicht transferiert und bei Swisscom importiert.
"Data Ready »	Die Evidenz wurde importiert und eine Signatur ist nach Akzeptanz der Nutzungsbestimmungen möglich
"Identification cancelled by user"	Die Identifikation wurde durch den Benutzer abgebrochen. Der Grund ist nicht bekannt.
Identification cancelled by ISP	Die Identifikation wurde durch den Identifizierer abgebrochen. Der Grund ist nicht bekannt.
Identification unsuccessfull	Die Identifikation konnte nicht durchgeführt werden, weil die vorgelegten ID Dokumente (Videoidentifikation) nicht geprüft werden konnten oder fehlerhaft sind.

(*) Diese Meldungen können sich ändern und sind nur beispielhaft. Der Integrationsguide enthält die tatsächlich vorhandenen Meldungen.

Zusätzliche Identitätsdaten (z.B. im Rahmen der Geldwäschebekämpfung)

Grundsätzlich verbleiben die Identifizierungsdaten bei Swisscom zum Zwecke der Signatur. Im Rahmen der Signatur wird der Vorname, Name und das Heimatland der identifizierten Person sichtbar, sofern kein Pseudonym gewählt wurde. Möchte der Kunde ebenfalls die Identifizierungsdaten für weitere Zwecke nutzen, so muss hierfür ein Zusatzvertrag zwischen dem Kunden und dem Identifizierer abgeschlossen werden. Der Identifizierer wird dann dem Kunden einen Zugang zu den Daten ermöglichen unter Verwendung der Swisscom „orderID“. Hiermit ist es möglich, dass ein- und dieselbe Identifizierung sowohl für z.B. Geldwäscheidentifikationsüberprüfung und qualifizierte elektronische Signatur eingesetzt werden kann.
Ein gesondertes White Paper unterrichtet genau über Möglichkeiten zum Einsatz der Identifikation im GWG Umfeld der deutschen Rechtssprechung.

Setup Filter und Parameter

Basierend auf den Anforderungen des Service Providers, die er im Vertrag hinterlegt, wird der Service Provider bei Swisscom aufgeschaltet. Er kann dabei die Methoden angeben, die er für die Identifikation eingeben möchte und den entsprechenden Rechtsraum, in dem die Signatur eingesetzt werden soll sowie den LOA, der bestimmt, ob fortgeschritten oder qualifiziert signiert werden kann.

Konkretes Beispiel:

Identification Service Provider	Identifikationsmethoden	LOA und Rechtsraum
ISP 1	Video	LOA4/eIDAS
ISP2	BankIDent	LOA4/eIDAS

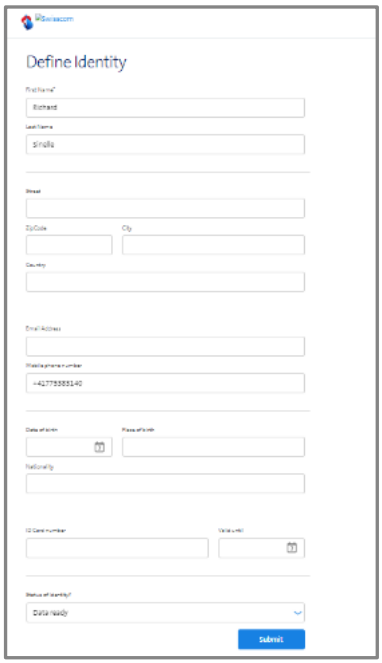
Testumgebung

Zur Erleichterung der Integration stellt Swisscom eine Testumgebung zur Verfügung, die es dem Kunden ermöglicht, den Smart Registration Service zu testen.

Er kann hierbei unter Einbezug des Identifizierers testen und damit den gesamten Prozess. Beispielsweise ist es möglich, die Video Identifizierung mit einem Videoidentifizierungsagenten zu testen, der den Prozess genauso durchführt wie später im produktiven Betrieb. Hiervon sollte nur beschränkt Gebrauch gemacht werden im Rahmen des Tests, um die Aufwände vorab gering zu halten.

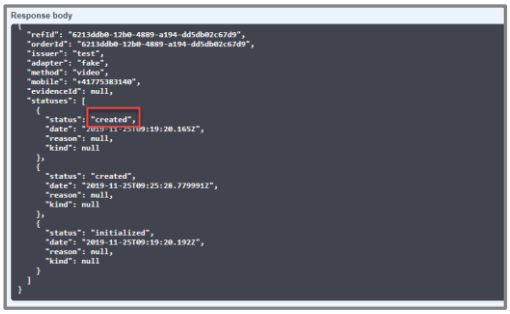
Daher bietet Swisscom die Möglichkeit die Identifizierer zu simulieren und die verschiedenen Stati der Identifizierer zurückzugeben. Das wird dadurch bewerkstelligt,

dass anstelle einer tatsächlich stattfindenden Identifikation ein Formular mit den Daten, die durch die tatsächliche Identifizierung validiert würden, ausgefüllt wird (siehe Abbildung rechts).



Zum weiteren Test wird dann z.B. der Fall ausgewählt, in dem die Identifizierung vollständig ist und die Evidenzen vorliegen:

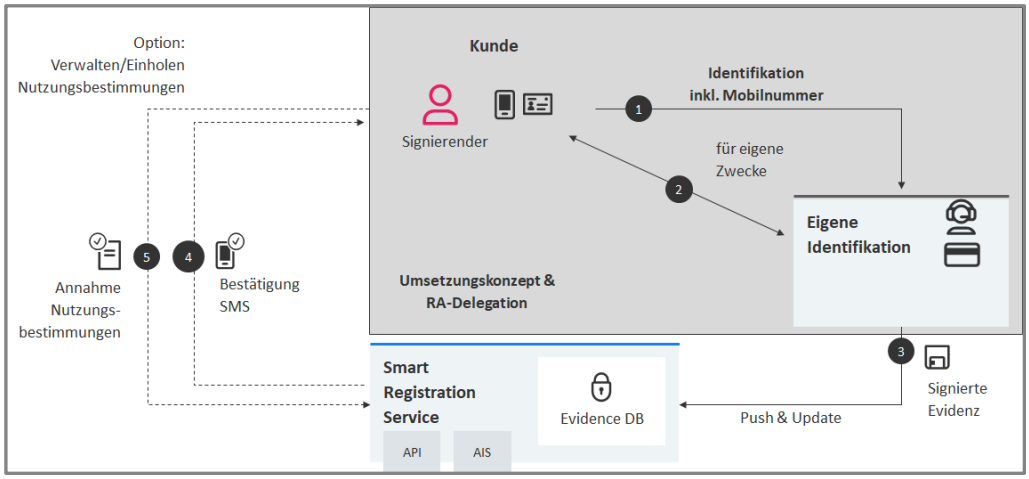
In diesem Beispiel wird folgende Antwort geliefert:
Die Identifizierung ist abgeschlossen und die Evidenzen wurden eingereicht. Mit anderen Worten, eine qualifizierte Unterschrift ist möglich, sofern die Nutzungsbestimmungen akzeptiert wurden. Das kann mit dem „verify“ Aufruf verifiziert werden.



Die genaue Schnittstelle ist unter https://miss-backend-api-dev.scapp.swisscom.com/swagger/index.html beschrieben. Es gibt hierzu auch einen Integration Guide. Voraussetzung für den Zugang zur Testumgebung ist ein abgeschlossener Servicevertrag zum Smart Registration Service.

Integration eines Identifizierers (eigene Identifikationsmethode)

Während die Integration des Dienstes für einen Service Provider extrem einfach und schnell ist, erfordert die Integration eines Identifizierers eine Reihe von Vorabaktivitäten.
Der Kunde nutzt hierbei seine eigene Identifikation für seine eigenen Prozesse und registriert den zukünftig Signierenden mit seiner Mobilnummer. Der Smart Registration Service unterstützt dabei die Archivierung der Registrierungsevidenzen und übernimmt auch die Verwaltung der Akzeptanz der Nutzungsbestimmungen:



Als Registrierungsstelle von Swisscom muss der Kunde mit seiner Identifizierung nachweisen können, dass seine Registrierung den Anforderungen an die Gesetzgebung und geltenden Regularien (z.B. den Normen von ETSI) entspricht. Hierzu legt der Identifizierer ein Umsetzungskonzept vor, in dem wesentliche Nachweise beschrieben werden, zum Beispiel:

- Governance (Serviceverantwortung, organisatorische Verankerung, Rollenkonzept):

  Es muss ein Rollenkonzept mit Sicherheitverantwortlichen, Systemverantwortlichen und Schulungsverantwortlichen vorweisbar sein. Insbesondere ist auch die Rollentrennung zu beachten.

- Prozesse (Identifikation, Rollen bei der Identifikation, Ablauf Signaturerstellung, Akzeptanz der Nutzungsbestimmungen im Prozess, Kontrolle der Signaturfreigabe, Verwaltung der Daten, Administration des Distinguished Names, Konformitätsprüfung, Auskunftspflicht):

  Die Identifikationsart und das Identifikationsverfahren sind genauestens zu beschreiben. Wichtig ist die physische Präsenz (oder gleichwertiges Verfahren) des Antragstellers für eine Signatur bei der Überprüfung der Identität und der Nachweis der Identität mit Lichtbildausweisen, also in der Regel Pass oder ID.
  Die Gültigkeit der Identifikation zum Signaturzeitpunkt ist sicher zu stellen.
  Sicherheitsaspekte in Bezug auf die sichere Kommunikation, Fehlversuche bei der Signatur etc. sind zu beschreiben.
  Im Identifikationsprozess muss auch das spätere Authentifizierungsmittel aufgenommen werden, d.h. bei Verwendung des Smart Registration Services zwingend die Mobilnummer. Das unteilbare Prüfverfahren von Identität und Mobilnummer muss beschrieben sein (one short session). Sofern nicht auf ein auditiertes Vefahren eines anerkannten Auditors zurückgegriffen wird, wird Swisscom die KPMG bitten, das Identifikationsverfahren in Verbindung mit dem Signaturservice gemäss CEN TS 419 241 mit Unterstützung des Kunden zu auditieren und die Bescheinigung der Konformität bei der Konformitätsbewertungsstelle einreichen.
- Schulung, Datenschutz und Auditiermöglichkeiten

  Für das eingesetzte Verfahren sind alle Mitarbeiter zu schulen. Die Schulung und der Nachweis der Schulung ist zu beschreiben. Alle Mitarbeiter müssen notwendige Datenschutzmassnahmen einhalten und Daten vertraulich behandeln.
  Möglichkeiten für den Auditor der Swisscom und Swisscom selber zur Überprüfung des Prozesses sind aufzuzeigen.

- Technische Details (Aufbau Distinguished Name, Willensbekundungsdetails, Schutz der Infrastruktur)

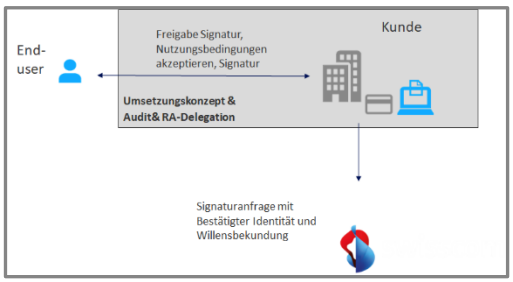
Das Umsetzungskonzept wird anschliessend von Swisscom gereviewed. Abhängig von der Konformitätsbewertungsstelle oder der Aufsichtsstelle kann ein zusätzliches Audit notwendig sein, insbesondere, wenn wesentliche Teile des Verfahrens vorab noch nicht auditiert wurden. Zusätzlich muss der Kunde im Falle eines eigenen Identifikations- oder Authentisierungsverfahrens einen Delegationsvertrag zur Delegation der Registrierungsstellentätigkeit unterzeichnen. Für das Einliefern der Evidenz kann die Swagger Schnittstelle beachtet werden: https://rasp.scapp.swisscom.com/swagger-ui.html

Verwendung eines anderen Authentisierungsverfahrens

Alternativ kann zu den Verfahren

- MobileID Schweiz (Nutzung der SIM eines Schweizer Mobilfunkanbieters)
- MobileID Authenticator App (Nutzung einer internationalen Authentication App auf Smartphone)
- Passwort / Einmalcode (Kombination einer Eingabe eines Passwortes für alle Signaturen und eines über SMS zugesendten Einmalcodes)

Auch ein eigenes, z.B. bestehendes Authentisierungsverfahren genutzt werden. Die Konformität muss allerdings noch zusätzlich in Verbindung mit der Identifikation nachgewiesen werden. Hierzu steht der Smart Registration Service dann nicht mehr oder nur noch eingeschränkt zur Verfügung. Es muss, wie oben beschrieben, ein Umsetzungskonzept erstellt werden. Auf Basis der Authentisierung kann dann direkt die Signaturanfrage bei Swisscom erfolgen:



Für den Authentisierungsprozess mit eigenen Authentisierungsmitteln muss zwingend der Kunde einen Auditbericht eines nach eIDAS zugelassenen Auditors für den Rechtsraum EU oder der KPMG Schweiz für den Rechtsraum Schweiz vorlegen. In dem Bericht muss beschrieben sein, wie der alleinige Zugriff des Signierenden auf den Signaturschlüssel (sogenanntes „sole control 2“ oder SCAL2 nach DIN EN 419241-1) und sichergestellt wird.
Zusätzlich für die Schweiz muss die Konformität mit dem schweizerischen Signaturgesetz beschrieben werden. Für den Einsatz im EU Raum muss der Auditor bescheinigen, dass das Authentisierungsmittel der Durchführungsverordnung der EU Kommission CIR 2015/1502 entspricht. Swisscom seinerseits muss prüfen, ob durch das Authentisierungsverfahren die Konformität der qualifizierten elektronischen Signaturerstellungseinheit nach eIDAS Art. 29 noch in der gleichen Art und Weise gegeben ist oder durch Anpassungen an das Authentisierungsverfahren in der Schnittstelle ein Änderungsantrag bei der Konformitätsbewertungsstelle eingereicht werden muss. In diesen Fällen fallen zusätzlich zu den Preispositionen in der Preisliste noch Projektkosten an.

Zusätzlich sind folgende Prozesse zu beschreiben, die der Smart Registration Service übernimmt:

- Daten der RA-Stelle (Archivierung der Dokumentation, Archivübergabe/-speicherung nach Vertragskündigung, Archivübergabe nach Einstellung der Geschäftstätigkeit, Datenschutz):

  Alle Nachweise zur Identifikation (z.B. ID/Passkopien) und zur Akzeptanz der Nutzungsbestimmungen müssen mindestens 11 bzw. 35 Jahre archiviert werden. Es müssen Verfahren beschrieben werden, wie diese Nachweise zu Swisscom transferiert werden, wenn der Geschäftsbetrieb oder der Vertrag nicht mehr aufrechterhalten wird. Ggfs. kann hierfür auf die Datenbank des Smart Registration Service zurückgegriffen werden.

- Verfahren zur Akzeptanz der Nutzungsbestimmungen von Swisscom
  Die Nutzungsbestimmungen für den Signaturservice von Swisscom müssen von der identifizierten Person bei der Identifikation nachweisbar akzeptiert werden.

Kosten des Service

Für die Bereitstellung des Service wird eine monatliche Grundgebühr fällig. Diese ist abhängig von den möglichen zugeschalteten Identifikationsverfahren. Pro durchgeführte Identifikation wird eine Transaktionsgebühr fällig.

Vorteile des Service

Der Smart Registration Service ermöglicht in seiner Standardausprägung eine schnelle Umsetzung einer elektronischen qualifizierten Signatur ohne regulatorischen Aufwand und alles aus einer Hand ohne weitere Untervergabe an Identifikationspartner. Er greift auf bewerte Methoden und auserwählte Swisscom Partner zurück. Swisscom sorgt dafür, dass die entsprechenden Methoden gesetzeskonform und normengerecht sind. Swisscom trägt auch für die Zuverlässigkeit der Identifikation die vollständige Haftung als Vertrauensdiensteanbieterin bzw. Zertifizierungsanbieter.
Laufend profitiert der Kunde von neuesten innovativen Identifikationsmöglichkeiten.
Die besten Identifikationspartner am Markt werden hierbei direkt mit interessierten Kunden zusammengebracht und können sich auf ihre Kernkompetenzen, dem Identifizieren, fokussieren.

Für weitere Auskünfte stehen wir gerne zur Verfügung:

Swisscom (Schweiz) AG
Enterprise Customers
Identification Service

Pfingstweidstrasse 51
8005 Zürich

Schweiz

https://trustservices.swisscom.com

Swisscom Trust Services