White Paper „Identifikation durch eine RA-Agentur mit der RA-App“.

1 Einleitung

Um fortgeschrittene oder qualifizierte elektronische Signaturen mit dem „All-in Signing Service“ von Swisscom erstellen zu können, müssen die Personen vorgängig durch Swisscom identifiziert werden. Diese Identifikation ist sowohl im Rahmen der Schweizer Gesetzgebung (ZertES) als auch in jenem der EU-Gesetzgebung (eIDAS) erforderlich. Laut Gesetz kann diese Tätigkeit an einen vertrauenswürdigen Dritten delegiert werden (eine Rechtseinheit, ein Unternehmen oder eine Organisation), der die Identifikation vornimmt. Damit diese Delegation korrekt organisiert und ihre Qualität sichergestellt werden kann, wird zwingend ein Vertrag zwischen Swisscom und dem betreffenden vertrauenswürdigen Dritten unterzeichnet (RA-Agenturvertrag). Der vertrauenswürdige Dritte, der im Folgenden als „RA-Agentur“ bezeichnet wird, kümmert sich um die Identifikation.

So handeln Organisationen ausserhalb von Swisscom aber auch Einheiten innerhalb von Swisscom als RA-Agenturen, die ermächtigt sind, die Verifizierung der Identität der Personen vorzunehmen, denen qualifizierte oder fortgeschrittene digitale Zertifikate ausgehändigt werden müssen. Diese Organisationen oder Einheiten halten sich an den von Swisscom festgelegten Prozess und die entsprechenden Regeln sowie die Gesetzgebung.

2 Wie funktioniert die Identifikation?

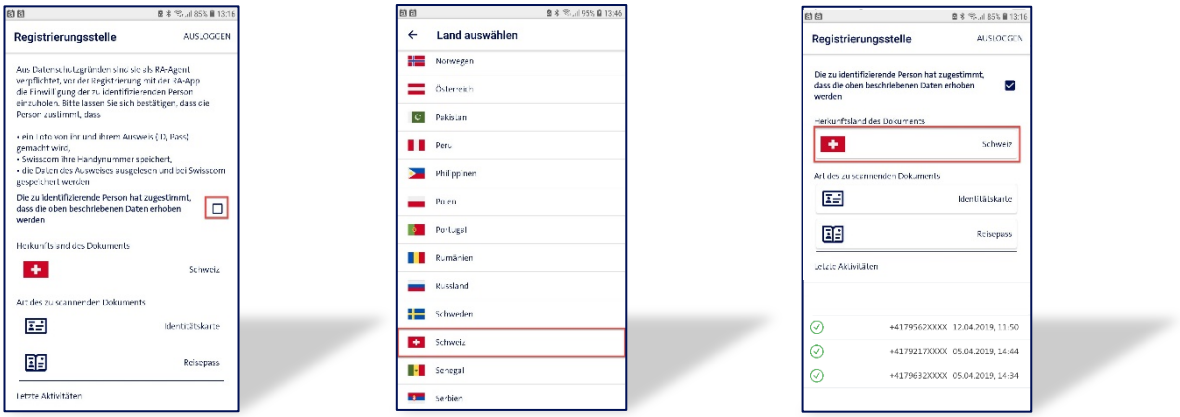
Die RA-Agentur ist für den Identifikationsprozess von Swisscom zuständig, dem natürliche Personen unterzogen werden, bevor sie bei Swisscom die Erzeugung elektronischer Unterschriften beantragen können. Für diesen Identifikationsprozess bezeichnet die RA-Agentur die Personen, die den Prozess mit Hilfe einer mobilen Applikation (der Swisscom RA-App) durchführen. Diese Personen werden als RA-Agenten bezeichnet (Agenten der Registrierungsstelle / "Registration Authority"). Die RA-Agenten sind also zugelassene Anwender der Swisscom RA-App und gehören zwingend der Organisation der RA-Agentur an. Die RA-App ist auf den Plattformen Android und OS verfügbar. Nach der Identifikation übermittelt die mobile Applikation die im Verlauf des Identifikationsprozesses erhobenen Daten direkt an Swisscom.

Damit ein Agent ermächtigt werden kann, eine Identifikation vorzunehmen, muss er vorgängig zwingend eine Schulung absolvieren. Dafür stellt Swisscom eine Online-Schulung in Form eines E-Learning zur Verfügung, zu der der zukünftige RA-Agent aufgeboten wird. Die Schulung enthält zentrale Informationen, die für die Identifikation bekannt sein und angewendet werden müssen, sowie verschiedene Fragen, die der zukünftige RA-Agent korrekt beantworten muss.

Nur ein RA-Agent, der den Test am Ende der Schulung bestanden hat, wird von Swisscom ermächtigt, Identifikationen vorzunehmen. Dies ist auch die Voraussetzung, damit er sich mit der Swisscom RA-App verbinden kann.

Vorgehen:

Nach dem Start der mobilen Applikation muss sich der RA-Agent zunächst mit seiner Mobiltelefonnummer und seiner Mobile ID authentifizieren. Falls er keine Mobile ID hat, kann er sich auch mit dem Authentifizierungsprozess Passwort + einmaliger Code via SMS verbinden.



Bevor er mit dem Identifikationsprozess beginnt, muss der RA-Agent die Zustimmung der zu identifizierenden Person einholen, dass seine Identitätsdaten von Swisscom registriert werden, wie dies das Datenschutzgesetz verlangt.

Nachdem er die Zustimmung erhalten und in der mobilen Applikation bestätigt hat, wird der RA-Agent aufgefordert, das Ausstellungsland und die Art des Identifikationsdokuments (Identitätskarte, Pass) auszuwählen. Über 80 Länder stehen heute zur Verfügung und die Datenbank wird laufend erweitert. Gemäss ZertES sind nur Identitätskarten oder Pässe zulässig.

Nachdem er das Land und die Ausweisart gewählt hat, wird dem RA-Agent ein Beispieldokument präsentiert. Dieser kann nun das angezeigte Beispiel mit dem ihm vorgelegten Ausweis vergleichen. Dies ist ein erster Echtheitstest. Wenn der vorgelegte Ausweis stark vom am Bildschirm angezeigten Ausweis abweicht, ist der RA-Agent verpflichtet, die Identifikation zu verweigern.

Auf dem Beispieldokument werden auch gewisse leicht kontrollierbare Sicherheitselemente hervorgehoben. Dabei handelt es sich einerseits um visuelle, andererseits um taktile Elemente. Die visuellen Elemente werden rot, die taktilen gelb umrahmt. So kann der RA-Agent in einigen Sekunden die Echtheit des im vorgelegten Ausweises sicherstellen, indem er das Vorhandensein dieser Sicherheitselemente überprüft.

Nach dieser Kontrolle überprüft der RA-Agent, dass das Foto auf dem Ausweis mit der Person, die vor ihm steht, übereinstimmt. Angesichts der Gültigkeitsdauer der Ausweise kann das Foto deutlich von der zu identifizierenden Person abweichen. Im Zweifelsfall kann der RA-Agent die Identifikation ablehnen oder der Person vorschlagen, einen anderen, neueren Ausweis vorzulegen.

Falls die Identität bestätigt ist, fotografiert der RA-Agent direkt mit der mobilen Applikation den Teil des Ausweises. Dafür muss er die mobile Applikation berechtigen, auf die Kamerafunktion des Telefons zuzugreifen. Er wird auch angeleitet, welchen Teil des Ausweises er fotografieren muss (Vor- oder Rückseite). In einer zweiten Phase muss er den Teil des Ausweises scannen, der einen maschinenlesbaren Bereich (MRZ) enthält. Diese Daten werden in der Folge dem RA-Agent angezeigt, damit er sie überprüfen kann.

Hinweis: Ausweise ohne maschinenlesbaren Bereich können nicht berücksichtigt werden. Zum Beispiel wird für Personen italienischer Nationalität empfohlen, nicht die Papierversion der Identitätskarte vorzulegen oder den Pass zu verwenden.

Hinweis: Die mobile Applikation akzeptiert nur Identitätskarten oder Pässe bei der maschinellen Lesung. Angesichts der Vielfalt der weltweit bestehenden Ausweise kann es jedoch vorkommen, dass ein nicht zulässiger Ausweis irrtümlicherweise gescannt wird (Fahrausweis). Der RA-Agent muss in diesem Fall die Identifikation unmittelbar verweigern.

Nach dem Scan des maschinenlesbaren Bereichs fotografiert der RA-Agent die Person, die ihren Ausweis deutlich sichtbar präsentiert. Dieses Foto dient als Beweis der Präsenz der Person, was eine Anforderung des ZertES ist.

Schliesslich nimmt der RA-Agent nun die Registrierung der identifizierten Person vor und präzisiert dazu die gewünschte Korrespondenzsprache (DE, FR, IT, EN) sowie die Mobiltelefonnummer der identifizierten Person. Um Fehler zu vermeiden, tätigt der RA-Agent einen Anruf auf die von der zu identifizierenden Person angegebene Nummer und stellt somit sicher, dass die Person die Inhaberin dieser Nummer ist, indem er überprüft, dass der Anruf das entsprechende Mobiltelefon erreicht.

Danach bestätigt der RA-Agent den erfolgreichen Abschluss dieser Überprüfung mit einer Unterschrift. Eine Nachricht auf dem Bildschirm bestätigt ihm anschliessend den erfolgreichen Abschluss.

Die erfassten Daten sowie die Fotos werden an Swisscom übermittelt und gesichert und verschlüsselt als Beweise gespeichert. Die Daten werden nur zu Beweiszwecken im Rahmen der elektronischen Signaturen verwendet und dürfen nicht für andere Zwecke genutzt werden.

Nach der Registrierung erhält die identifizierte Person vom RA-Service von Swisscom ein SMS mit einem Link zu den Nutzungsbedingungen des Signaturdienstes. Diese werden dem Nutzer für die Gerichtsbarkeiten der Schweiz und der EU präsentiert. Der Nutzer kann die gewünschte Gerichtsbarkeit wählen oder auch beide. Es wird empfohlen, die Nutzungsbedingungen für beide Gerichtsbarkeiten zu akzeptieren, da dies dem Nutzer mehr Möglichkeiten bietet.

Eine auf diese Weise identifizierte Person wird damit ein „Mitglieder der Gemeinschaft“ der Unterzeichner von Swisscom. Sie kann nun während der vollen Gültigkeitsdauer der Identifikation auf allen von den Partnern und Kunden Signaturlösungen signieren, welche den All In Signing Service nutzen. Eine neue Identifikation ist dazu nicht erforderlich. Die auf diese Weise durchgeführte Identifikation hat eine Gültigkeitsdauer von 5 Jahren. 3 Monate vor Ablauf dieser Frist und ein zweites Mal 1 Monat vor Ablauf erhält der Nutzer eine Nachricht, die ihn darauf aufmerksam macht, dass er seine Identifikation erneuern muss. Für die Erneuerung der Identifikation kann er genau denselben Prozess bei einem RA-Agenten seiner Wahl durchlaufen.

Hinweis: Es ist empfehlenswert, wenn möglich einen Ausweis mit einer Gültigkeitsdauer von mindestens 5 Jahren zu verwenden. Die Identifikation muss auch erneuert werden, wenn der Ausweis vor Ablauf der 5-Jahresfrist nach der ersten Identifikation seine Gültigkeit verliert.

Tipp: "Demo-Modus"

Die Swisscom RA-Applikation bietet einen Demo-Modus an, der es dem Nutzer ermöglicht, sich mit den Funktionalitäten der Applikation vertraut zu machen, ohne das Risiko einzugehen, einen Fehler zu machen. Dieser Demo-Modus kann von jedermann verwendet werden, auch ohne zuvor zum RA-Agenten ernannt worden zu sein.
Für die Aktivierung des Demo-Modus kann man sich mit den folgenden Daten verbinden:
Meine registrierte Mobiltelefonnummer: +41001234567
Mein Unternehmensidentifikator: demo
In diesem Modus werden keine Daten an Swisscom weitergeleitet.

3 Wie kann ich ein RA-Agentennetz aufbauen?

Die erste Etappe besteht darin, einen RA-Agenturvertrag zwischen Swisscom und dem Unternehmen abzuschliessen, das Identifikationen durchführen möchte und das zur RA-Agentur wird.

Aus rechtlichen Gründen kann die RA-Agentur nur Personen ihrer eigenen Organisation als RA-Agenten vorschlagen. Drittorganisationen können jedoch mit Swisscom einen Vertrag als zusätzliche RA-Agentur abschliessen.

Es gibt zwei Arten von RA-Agenten:

Der Standard-RA-Agent: Er ist ermächtigt, innerhalb des Unternehmens Identifikationen vorzunehmen (in der Regel die Mehrzahl).
Der Master-RA-Agent: Er hat dieselben Rechte wie die Standard-RA-Agenten, kann jedoch zudem neue Agenten ernennen und das Agentennetz verwalten (in der Regel nur wenige Personen innerhalb des Unternehmens). Für seine Aufgaben erhält er Zugang zu einem dedizierten Portal für die Verwaltung der Agenten innerhalb der Organisation.

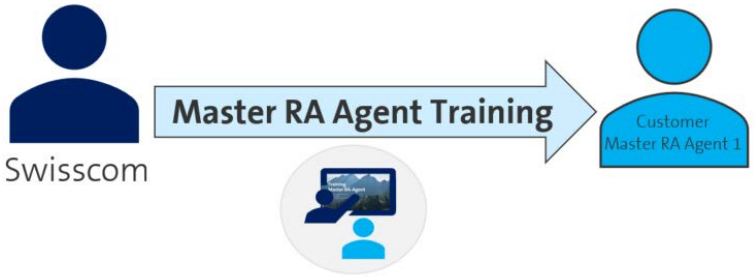
Nach Abschluss des Vertrags beantragt die RA-Agentur zunächst bei Swisscom die Ernennung eines Master-RA-Agenten mit dem dafür vorgesehenen Formular. Die RA-Agentur muss sicherstellen, dass der bezeichnete Master-RA-Agent zuvor durch einen RA-Agenten von Swisscom für die qualifizierte elektronische Signatur mit Swisscom identifiziert wurde (z.B. im Vertrag bestimmte Kontaktperson oder Swisscom-Partner).

Swisscom prüft den Antrag der RA-Agentur. Falls er akzeptiert wird, organisiert Swisscom eine Schulung zum Master-RA-Agenten. Diese Schulung erfolgt in direktem Kontakt und ist ein wichtiger Schritt für die Erstellung des RA-Agenturvertrags. Es handelt sich nämlich um die erste Person innerhalb des Kundenunternehmens, die Identifikationen vornehmen kann. Nach dieser Schulung muss der Master-RA-Agent noch eine Online-Schulung (Grundschulung des RA-Agenten) absolvieren und erhält dabei einen Zugang zum Portal für die Verwaltung der RA-Agenten.

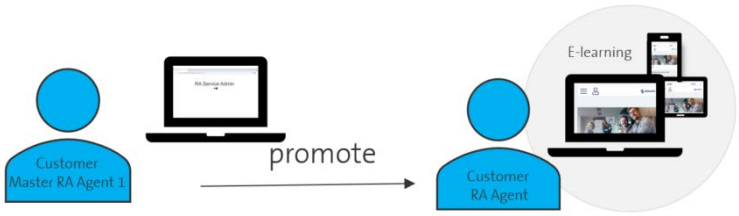
Der Master-RA-Agent ist auch dafür zuständig, die weiteren Master-RA-Agenten oder Standard-RA-Agenten, die ernannt werden, korrekt zu schulen und zu betreuen. Das anzuwendende Verfahren kann also wie folgt beschrieben werden:

1. Master-RA-Agent: Schulung direkt durch Swisscom

2. Master-RA-Agent: Schulung durch den 1. Master-RA-Agenten des Unternehmens



Der Master-RA-Agent ernennt die Standard-RA-Agenten:



Die Master-RA-Agenten können im Verwaltungsportal weitere RA-Agenten ernennen und ihren Status verwalten. Falls dies für die Erfüllung der Verpflichtungen der RA-Agentur erforderlich ist, können sie ausserdem die folgenden Daten zu allen durch die RA-Agentur identifizierten Personen einsehen:

- Vorname(n) und Name(n) der Person(en)
- Referenz des Identifikationsnachweises (die Daten der Identitätskarte sind mit Ausnahme des Gültigkeitsdatums nicht einsehbar, die bei der Identifikation gemachten Fotos auch nicht)
- Mobiltelefonnummer
- Trust-Identifizierungsniveau (zwischen 1 und 4, wobei Niveau 4 die qualifizierte elektronische Signatur und Niveau 3 die fortgeschrittene elektronische Signatur ermöglicht)
- Zeichnungsberechtigung: global oder kontextuell (1)
- Identifikationsdatum
- Ablauf der Gültigkeit der Signaturermächtigung (Identifikation + 5 Jahre oder Gültigkeitsdauer des Ausweises, falls dieser vorher ablaufen sollte)
- Status der Identifikation

Die RA-Agenten können ihrerseits nur Identifikationsaufgaben vornehmen. Sie haben keinen Zugriff auf das Verwaltungstool.

Nachdem er die Online-Schulung erfolgreich absolviert hat, wird jeder RA-Agent und jeder Master-RA-Agent über seine Pflichten als RA-Agent informiert. Diese bestehen aus ihrer Kooperations- und Vertraulichkeitsverpflichtung, die sie bei ihrer Identifikationstätigkeit einzuhalten haben. Der zukünftige RA-Agent hat diese Verpflichtungen sorgfältig durchzulesen und zu akzeptieren, indem er eine qualifizierte elektronische Signatur vornimmt. Falls er sich weigert, wird der RA-Agent nicht zur Durchführung von Identifikationen ermächtigt und kann sich nicht mit der Swisscom RA-Applikation verbinden. Diese Verpflichtungen bilden integrierenden Bestandteil des RA-Agenturvertrags, den die RA-Agentur vorgängig mit Swisscom abschliesst.

Somit kann der Aufbau eines effizienten Netzes von RA-Agenten für die Identifikation automatisch verwaltet und vollständig durch die RA-Agentur (den Kunden) realisiert werden. Dies ist besonders interessant für einen Aufbau über mehrere Standorte oder über zahlreiche Abteilungen hinweg.

(1) Global bedeutet der Signierender kann in alle Applikationen signieren die den AIS nutzen. Kontextual Nutzer können innerhalb spezifische Applikationen signieren (zum Beispiel Finanzinstitute)

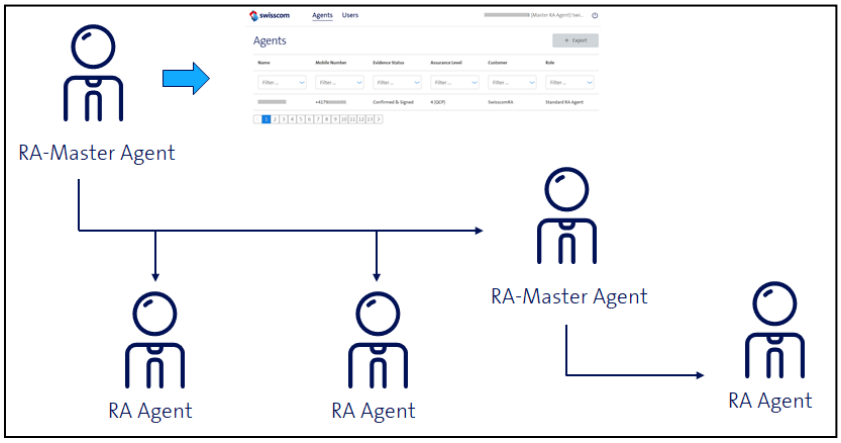


Bild: Typischer RA Agenten Aufbau

Als zugelassener und geprüfter TSP (Trust Service Provider) behält sich Swisscom und / oder ihre Zertifizierungsstelle das Recht vor, stichprobenmässige Prüfungen der Arbeit der RA-Agentur auf Anfrage der Zertifizierungsbehörde vorzunehmen. Mit Ausnahme von ausserordentlichen Fällen erfolgt diese Prüfung nicht vor Ort, sondern ausschliesslich auf dokumentarischer Grundlage mittels der Beschreibung der übermittelten und gespeicherten Daten.

Swisscom unterstützt die RA-Agentur weiterhin durch ihren Support. Die RA-Agentur erhält eine Supportnummer (PRO-Nummer) bei Abschluss des Vertrags und kann sich rund um die Uhr unter der Nummer +41 (0) 800 724 724 724, Menü „Data Services“, Stichwort „All-in Signing Service“ an den Swisscom Support wenden.

Swisscom (Schweiz) AG
Enterprise Customers
Identification Service

Pfingstweidstrasse 51
8005 Zürich

www.swisscom.com/signing-service