Bestellung und Anleitung Testaccount All-in Signing Service für Vertragspartner

1 Zweck des Dokumentes

Dieses Dokument dient als Informations- und Bestellformular für einen langfristigen Partnervertrags-Testaccount für den All-In Signing Service von Swisscom. Damit kann ein Partner das Zusammenspiel seiner Teilnehmerapplikation mit dem All-in Signing Service testen oder für seinen Endkunden einen weiteren Testaccount bestellen. Nähere Informationen unter https://trustservices.swisscom.com. Hier finden Sie auch den Reference Guide (https://trustservices.swisscom.com/downloads), der nähere Informationen zur Schnittstelle bietet.

2 Zugangsvoraussetzung: SSL/TLS Zugangszertifikat

Zum Schutz der Verbindung (über https) zum AIS Service generiert der Teilnehmer ein selbst signiertes SSL/TLS-Client-Zertifikat mit einer Schlüssellänge von mindestens 2048 Bit und übermittelt dieses vorgängig an Swisscom. (Ein Zugangszertifikat kann für mehrere Test-Accounts genutzt werden).

Der Aufbau des Zertifikates ist wie folgt:

- Inhalt des "Subject" bzw. "Distinguished Name" des Zertifikates:
  - CN=<URL oder DNS-Name des Teilnehmersystems, das mit dem AIS kommuniziert>
  - emailAddress=<E-Mail Adresse der Kontaktperson für diese Verbindung>
  - O=<Name der Organisation>
  - C=<Land, in dem die Organisation ihren Sitz hat>

Die Gültigkeit darf 2 Jahre nicht überschreiten. Es werden keine besonderen Anforderungen an die Schlüsselverwendungen (key usage) gestellt. Bitte ankreuzen:

☐ Das Zertifikat ist bereits erzeugt und wird parallel zu dieser Erklärung mitgesendet.

☐ Das Zertifikat wird unter Bezug auf diese Bestellung an die Adresse MSC.support@swisscom.com nachgesendet.

3 Identifikations- und Signaturfreigabeverfahren

Im Rahmen des All-in Signing Service stehen verschiedene Standardverfahren bereit für die Identifizierung eines Signierenden und die Signaturfreigabe des Nutzers im Falle einer Personensignatur (on-demand). Organisationssignaturen (static) basieren hingegen auf eine manuelle Vorabidentifizierung der Organisation und eines gesicherten Zugangs zum All-in Signing Service ohne weitere Willensbekundung. In Abhängigkeit der verschiedenen Verfahren werden später die passenden Kontenbezeichnungen (Claimed ID) genutzt.

3.1 Identifikation mit RA-App und Smart Registration Service

Für die Identifikation steht standardmässig das Verfahren mit RA-App zur Verfügung, d.h. ein vom Kunde benannter RA-Agent erhebt in einem face2face Gespräch die notwendigen Daten zur Registrierung per App und übermittelt diese automatisch an den RA-Service der Swisscom. Auch die Identifikationsverfahren des Smart Registration Service importieren ihre Evidenzdaten in gleicher Weise in den RA-Service. Basierend auf diesen Daten kann die eindeutige Seriennummer des Signierenden für das Zertifikatssubjekt ermittelt werden und überprüft werden, ob der Signierende bereits identifiziert wurde. (sogenannter "Verify Call", siehe Dokumentation unter https://trustservices.swisscom.com/downloads).

3.2 Eigene Registrierungsverfahren

Der Kunde kann auch andere Registrierungsverfahren nutzen, hingegen müssen diese dann später in einem "Umsetzungkonzept" beschrieben und von Swisscom und/oder dem Auditor und/oder der Konformitätsbewertungsstelle freigegeben werden. Da hier auf eine auditierte Registrierung aufgesetzt

wird, geht die Fernsignatur dabei von der Richtigkeit der übertragenen Authentisierungsinformation (Mobilnummer) aus.

3.3 Authentisierungsmethode Mobile ID

Die Mobile ID ist derzeit nur einsetzbar mit Mobile ID fähigen SIM Karten von Schweizer Mobilfunkanbietern. Hierdurch kann sich der Antragsteller für eine Signatur mittels direkter 2-Faktor Authentisierung authentisieren und eine Willensbekundung zur Signatur auslösen. Sollte Mobile ID bei der Mobilfunknummer nicht vorhanden sein, wird automatisch auf das PWD/OTP Verfahren zurückgegriffen.

3.4 Authentisierungsmethode Mobile ID Authenticator App

Diese App gibt denjenigen Personen die Möglichkeit, bequemer eine Authentisierung durchzuführen, die nicht über eine SIM Karte eines Schweizer Mobilfunkanbieters verfügen, z.B. in der EU. Für die Registrierung ist weiterhin eine Mobilfunknummer (ähnlich der Whatsapp Registrierung) notwendig. Die Information wird per Internet übertragen. Für die Willensbekundung können dann je nach Fähigkeit des Telefons z.B. auch Fingerprint oder Face Recognition genutzt werden.

3.5 Authentisierungsmethode PWD/OTP

Hierbei authentifiziert sich der Antragsteller über eine von AIS direkt angezeigte Webseite zur Eingabe seines Passworts und eines zusätzlichen Einmalpasswortes, das er per SMS erhält. Die Webseite wird von der Teilnehmerapplikation aufgerufen. Es ist möglich das Eingabefenster für das Einmalpasswort oder das Passwort als iFrame in die eigene Webseite einzubinden. Bitte beachten Sie hierfür die spezielle Dokumentation im Downloadbereich: https://trustservices.swisscom.com/downloads.

3.6 Authentisierungsmethode Session Token/OTP

Die Willensbekundung erfolgt durch die Eingabe eines Einmalpasswortes, das vom AIS Service generiert wird und das über SMS an das Handy des Antragstellers übermittelt wird sobald die Daten des Antragsstellers an den AIS Service übermittelt wurden. Dieses gibt der Antragsteller in der Teilnehmeranwendung ein. Es ist möglich das Eingabefenster für das Einmalpasswort als iFrame in die eigene Webseite einzubinden. Bitte beachten Sie hierfür die spezielle Dokumentation im Downloadbereich: https://trustservices.swisscom.com/downloads

3.7 Eigene Signaturfreigabeverfahren

Eigene Signaturfreigabeverfahren können verwendet werden, auch in Kombination z.B. mit Session Token/OTP, indem man selber den 2ten fehlenden Faktor (z.B. Authentisierung durch Login am Beginn der Session) hinzugibt. Alle diese Verfahren müssen vor produktivem Start in einem Umsetzungskonzept beschrieben werden und vorgängig freigegeben werden.

4 Kontenbezeichnung und Testausprägungen (Claimed ID)

Bitte beachten Sie: Alle Testzertifikate sind prinzipiell «fortgeschrittener» Natur und als Testzertifikate gekennzeichnet. Diese können also nicht in Validatoren als «qualifiziert» geprüft werden.

4.1 Personensignaturen

In Abhängigkeit von den zuvor genannten Identifizierungs- und Signaturfreigabeverfahren werden mit ihrem Testaccount für Personensignaturen parallel Zugang zu mehreren Konten eingeräumt, in denen Sie je nach Testsituation ihre Teilnehmerapplikation testen können. Diese unterscheiden sich auch durch den Rechtsraum, für den das Zertifikat ausgestellt werden soll: Rechtsraum Schweiz für Signaturzertifikate nach der ZertES Gesetzgebung der Schweiz oder Rechtsraum EU für Signaturzertifikate nach der eIDAS Verordnung der EU.

4.1.1 RA App oder Smart Registration Service Identifikation und 2-Faktor Authentisierung

Einsatz: Vorgesehenes Standardverfahren bei Nutzung der RA-App oder den Identifikationsverfahren des Smart Registration Service für die qualifizierte oder fortgeschrittene Signatur in Verbindung mit Mobile ID, MobileID Authenticator App oder PWD/OTP als Methode zur Willensbekundung. Der All-in Signing Service erkennt automatisch, ob eine Mobilfunknummer (z.B. auch ausländische) Mobile ID/MobileID Authenticator App fähig ist und wählt danach das entsprechende Verfahren.

Zugang zum Testaccount Rechtsraum CH (ZertES) mit folgender Claimed ID:
`ais-90days-trial-withRAservice:OnDemand-Advanced4`

Zugang zum Testaccount Rechtsraum EU (eIDAS) mit folgender Claimed ID:
`ais-90days-trial-withRAservice:OnDemand-Advanced-EU`

4.1.2 Eigene Registrierungsmethode mit Mobile ID/Mobile ID Authenticator App/Fallback PWD/OTP

Einsatz: Zur Identifizierung ist keine RA-App oder Smart Registration Service vorgesehen, oder Sie wollen während der Testphase noch nicht auf die Identifizierung der RA-App bzw. Smart Registration Service aufbauen und erstmal die Signaturanbindung testen. Die Signaturfreigabe basiert auf 2 Faktoren (Mobile ID oder Mobile ID Authenticator App mit Rückfall auf PWD/OTP), wie bei qualifizierten Signaturen erforderlich. Der All-in Signing Service erkennt automatisch, ob eine Mobilfunknummer (z.B. auch ausländische) Mobile ID oder Mobile ID Authenticator App fähig ist und wählt danach das entsprechende Verfahren.

Zugang zum Testaccount Rechtsraum CH (ZertES) mit folgender Claimed ID:
`ais-90days-trial:OnDemand-Advanced4`

Zugang zum Testaccount Rechtsraum EU (eIDAS) mit folgender Claimed ID:
`ais-90days-trial:OnDemand-Advanced-EU`

4.1.3 Eigene Registrierungsmethode mit Session Token/OTP only

Einsatz: Einfachste und schnellste Testmöglichkeit, um die Anbindung an den All-in-Signing Service zu testen. Zur Identifizierung ist keine RA-App oder Smart Registration Service vorgesehen, oder sie wollen während der Testphase noch nicht auf die Identifizierung der RA-App oder Smart Registration Service aufbauen und erst mal die Signaturanbindung testen. Für die Signaturfreigabe wird ein 1-Faktor Verfahren (SMS mit one-time Passwort) verwendet, was nur für den Einsatz von fortgeschrittenen Signaturen geeignet wäre. Oder Sie haben vor, einen eigenen 2ten Faktor einzusetzen.

Zugang zum Testaccount Rechtsraum CH (ZertES) mit folgender Claimed ID:
`ais-90days-trial-OTP:OnDemand-Advanced4`

Zugang zum Testaccount Rechtsraum EU (eIDAS) mit folgender Claimed ID:
`ais-90days-trial-OTP:OnDemand-Advanced-EU`

4.2 Kontenbezeichnung (Claimed ID) Siegel

4.2.1 Siegel für die Schweiz

Einsatz: Testmöglichkeit für die Anbindung an Siegel für den Schweizer Rechtsraum.

Zugang zum Testaccount mit folgender Claimed ID:
`ais-90days-trial: static-saphir4-ch`

4.2.2 Siegel für EU

Einsatz: Testmöglichkeit für die Anbindung an Siegel für den Rechtsraum EU.

Zugang zum Testaccount mit folgender Claimed ID:
`ais-90days-trial: static-saphir4-eu`

4.3 Kontenbezeichnung (Claimed ID) Zeitstempel

4.3.1 Zeitstempel für die Schweiz und EU

Einsatz: Testmöglichkeit für die Anbindung an Zeitstempel für den Schweizer und EU Rechtsraum.

Zugang zum Testaccount mit folgender Claimed ID:
`ais-90days-trial`

5 URL

Der Testzugang wird über https://ais.swisscom.com angesprochen.

6 Distinguished Name

Der Distinguished Name ist in der Schnittstelle zum AIS Service wie folgt anzugeben:

6.1 Personensignaturen (on-demand)

MUST/ OPTIONAL	Zertifikats-parameter	Inhalt	Beispiel
MUST	CN	TEST <Vorname> <Nachname>	TEST Hans Mustermann
MUST	givenname	<Vorname(n)>[1]	Hans Urs
	surname	<Nachname(n)>[1]	Mustermann
OPTIONAL (nur nach Rücksprache)	O	TEST <Name der Organisation>	TEST ABC AG
OPTIONAL (nur nach Rücksprache)	OU	<Information zur Organisationseinheit oder Bemerkung zum Test, falls O gesetzt>	For Test purposes only, Testabteilung
MUST	C	<zweistelliger Ländercode des Wohnsitz- oder Heimatlandes des Signierenden (oder der Organisation, falls O gesetzt)>	CH
ENTWEDER	emailaddress	<E-Mail des Signierenden>	hans@swisscom.com
ODER	serialnumber	<ID aus dem verify call bei Verwendung der RA-App> oder (nur nach Absprache) <Unternehmens ID>: eindeutige ID	RAS5b45b027c6d9370008072c48

Beispiele:

cn=TEST Max Muster, givenname=Max, surname=Muster, c=CH, emailaddress=maximus34@gmail.com

cn=TEST Max Muster, givenname=Max, surname=Muster, c=CH, serialnumber=RAS5b45b027c6d9370008072c48

cn=TEST Max Muster, givenname=Max, surname=Musterr, o=TEST ABC AG, c=CH, emailaddress=maximus34@gmail.com

cn=TEST Max Muster, givenname=Max, surname=Muster, o=TEST ABC AG, ou=bluewin signer, c=CH, serialnumber=RAS5b45b027c6d9370008072c48

[1] Bitte beachten: bei der Verwendung der RAS-serialnumber müssen die Namen so eingegeben werden, wie sie bei der Registrierung aufgenommen wurden, d.h. es kann ein zweiter oder auch dritter Vorname, etc. notwendig sein.

6.2 Organisationssignaturen (Siegel)

Zum Testen von Siegeln haben wir zwei Zertifikate in den Ausprägungen CH und EU auf dem Testaccount hinterlegt, beide haben den gleichen Inhalt:

```
commonName                = All-in Signing Service TEST account
organizationName          = TEST - Swisscom (Switzerland) Ltd.
organizaionIdentifier     = VATCH-CHE-101.654.423
countryName               = CH
```

Die Zertifikate wurden von uns bereits so eingerichtet und können gemäss den Angaben unter Kapitel 4.2 angesprochen werden.

7 Hinweise zum Service Level

Für die Teststellung werden keine Verfügbarkeiten zugesagt und jegliche Haftung ausserhalb der gesetzlichen Haftung ist seitens Swisscom ausgeschlossen. Es besteht kein Anspruch auf einen Service Level.
Bei Problemen können Sie sich gerne an MSC.support@swisscom.com wenden. Es werden auch regelmässig für Interessierte technische Schulungen angeboten.

8 Hinweise zum Einsatz

Die über diesen Testaccount bezogenen Signaturen sind Testsignaturen und dürfen auch nur für technische Implementierungstests und Vorführungen genutzt werden. Sie dürfen nicht im Zusammenhang mit Verträgen, Beurkundungen oder Vereinbarungen genutzt werden. Die Signaturen werden durch das zugrundeliegende Signaturzertifikat mit dem Wort "Test" gekennzeichnet.

9 Kontaktdaten des Teilnehmers

9.1 Anschrift des Teilnehmers

Firmenname / Organisationsname	
Adresse	
PLZ/Ort	

9.2 Technischer Hauptkontakt des Teilnehmers

Name, Vorname	
Anschrift	
Telefonnummer	
Mobile	
E-Mail	

9.3 Zu benachrichtigender Partner (optional)

Name, Vorname	
Anschrift	
Telefonnummer	
Mobile	
E-Mail	

10 Testzugang

Sie erhalten nach Einsenden dieses Formulars an unser Fulfillment MSC.support@swisscom.com eine Bestätigung mit dem aufgeschalteten Testzugang (i.d.R. binnen 2 Wochen). Von da an können Sie diesen bis zum Ablauf Ihres Zugangs (2 Jahre) nutzen. Verlängerungen sind explizit zu beantragen.

11 Schutz des Signatursystems

Trotz "Testzugang" handelt es sich hier um ein voll produktives System, welches durch die Testteilnehmerapplikation entsprechend geschützt werden sollte:

Die privaten Schlüssel des SSL/TLS Zertifikates müssen entweder

- Verschlüsselt auf dem System aufbewahrt werden,
- Oder auf einem externen Datenträger aufbewahrt werden,
- Oder werden durch die Teilnehmerapplikation selber verschlüsselt verwaltet.

Die Teilnehmerapplikation muss vor unberechtigtem Zugriff/Manipulation geschützt sein und die Betriebssystemsoftware und verwendeten Softwarekomponenten regelmässig auf neuestem Stand gehalten werden (Update, Patching).