Application for Test Account All-in Signing Service

1 Purpose of the document

This document serves as an information and application form for a test account for Swisscom's All-In Signing Service. This allows a subscriber to test the interaction of its subscriber application with the All-in Signing Service. Please find more details at https://trustservices.swisscom.com. Here you can also download the reference guide (https://trustservices.swisscom.com/downloads) with more information concerning the interface.

2 Access requirements: SSL/TLS Access Certificate

For secure communication (via https) to the AIS service, the subscriber generates a self-signed SSL client certificate with a key length of at least 2048 bits and transmits the certificate to Swisscom in advance (the same certificate can be used for several test accounts).
The structure of the certificate is as follows:

- Content of "subject" i.e. "distinguished name" of the certificate:
  - CN=<URL or DNS name of the customers system that communicates with AIS >
  - emailAddress=<E-mail address of the contact person for this connection >
  - O=<name of the organization >
  - C=<country in which the organisation is based >

The validity may not exceed 90 days. There are no specific requirements for the key usage.
Please mark your choice:

☐ The certificate has already been generated and is sent along with this application.

☐ The certificate will be forwarded to MSC.support@swisscom.com with reference to this application.

3 Identification Methods and Authentication Methods

The All-in Signing Service provides various standard procedures for identifying a signer and releasing the user's signature ("expression of will") in the case of a personal signature (on-demand). Organization signatures (static), on the other hand, are based on manual pre-identification of the organization and secure access to the all-in signing service without any further declaration of will. Depending on the different procedures different account names (claimed ID) can be used.

3.1 Identification with RA-App or Smart Registration Service

The RA-App procedure is available as standard for identification, i.e. an RA agent appointed by the customer collects the necessary data for registration in a face2face call and transmits it automatically to Swisscom's RA service. Also the identification methods of the Smart Registration Service import their evidences in the same way to Swisscom's RA-Service. Based on this data, the unique serial number of the signer for the certificate subject can be determined and it can be checked whether the signer has already been identified. (so-called "Verify Call", see documentation at https://trustservices.swisscom.com/downloads).

3.2 Own Registration Methods

The customer can also use other registration procedures, but these must then later be described in an "implementation concept" and approved by Swisscom and/or the auditor and the conformity assessment body. In this case the RA-Service and Smart Registration Service are not involved. Since the own registration methods are approved Swisscom All-in Signing Service assume that the transferred authentication means (mobile phone number) is correct registered.

3.3 Authentication Method Mobile ID

The Mobile ID can currently only be used with Mobile ID-enabled SIM cards from Swiss mobile phone providers. This enables the applicant to authenticate himself for a signature using direct 2-factor authentication and trigger a declaration of will for the signature. If the mobile ID is not available for the mobile phone number, the PWD/OTP procedure is automatically used.

3.4 Authentication Method Mobil ID Authenticator App

This App allows people who do not have a SIM card from a Swiss mobile operator, e.g. in the EU, to authenticate more conveniently. A mobile phone number is still required for registration (similar to a Whatsapp registration). The information is transmitted via the Internet. Depending on the ability of the phone, fingerprints or face recognition can then also be used for the expression of will.

3.5 Authentication Method PWD/OTP

The applicant authenticates himself via a website directly displayed by AIS to enter his password and an additional one-time password, which he receives by SMS. The website is accessed from the participant application. It is possible to incorporate the entry of the one time password or password by use of an iFrame. Please follow up the special documentation in the downloads area: https://trustservices.swisscom.com/downloads

3.6 Session Token/OTP

The declaration of intent is made by entering a one-time password generated by the AIS Service and sent to the applicant's mobile phone via SMS as soon as the applicant's data has been transmitted to the AIS Service. The applicant enters this in the participant application. It is possible to incorporate the entry of the one time password by use of an iFrame. Please follow up the special documentation in the downloads area: https://trustservices.swisscom.com/downloads

3.7 Own signature release procedures

Own signature release procedures can be used, also in combination with e.g. Session Token/OTP, by adding the 2nd missing factor (e.g. authentication at the beginning of the session). All these procedures must be described in an implementation concept before they can go live and must be approved beforehand by Swisscom.

4 Accounts and Test Scenarios (Claimed ID)

Please note: All test certificates are in principle of an "advanced" nature and marked as test certificates. These cannot therefore be tested as "qualified" in validators.

4.1 Personal signatures

Depending on the identification and signature release procedures mentioned above, your test account for personal signatures grants parallel access to several accounts in which you can test your subscriber application depending on the test situation. These also differ in the jurisdiction for which the certificate is to be issued: Swiss jurisdiction for signature certificates under the SigE legislation of Switzerland or EU jurisdiction for signature certificates under the eIDAS Regulation of the EU.

4.1.1 RA App or Smart Registration Service Identification and 2-Factor Authentication

Intentional use: Intended standard procedure when using the RA app or Smart Registration Service for qualified or advanced signature in combination with Mobile ID, Mobile ID Authenticator App or PWD/OTP expression of will. The All-in Signing Service automatically detects whether a mobile phone number (e.g. also foreign mobile IDs) is capable to use Mobile ID or Mobile ID Authenticator App and then selects the corresponding procedure.

Access to the test account jurisdiction CH (ZertES) with the following claimed ID:

`ais-90days trial-withRAservice:OnDemand-Advanced4`

Access to the test account jurisdiction EU (eIDAS) with the following claimed ID:

`ais-90days-trial-withRAservice:OnDemand-Advanced-EU`

4.1.2 Own Registration Method with Mobile ID/Mobile ID Authenticator App/Fallback PWD/OTP

Intentional use: No RA app or Smart Registration Service is used for identification, or you do not want test without identification of the RA app or Smart Registration Service during the test phase but first test the signature capability only. Signature release is based on 2 factors (Mobile ID or Mobile ID Authenticator App with fallback to PWD/OTP) as required for qualified signatures. The All-in Signing Service automatically detects whether a mobile phone number (e.g. also foreign mobile IDs) is capable for Mobile ID or Mobile ID Authenticator App and then selects the corresponding procedure.

Access to the test account jurisdiction CH (ZertES) with the following claimed ID:

`ais-90days-trial:OnDemand-Advanced4`

Access to the test account jurisdiction EU (eIDAS) with the following claimed ID:

`ais-90days-trial:OnDemand-Advanced-EU`

4.1.3 Own Registration Method with Session Token/OTP only

Intentional use: The easiest and fastest way to test the connection to the All-in-signing service. No RA app or Smart Registration Service is used for identification, or you do not want test without identification of the RA app or Smart Registration Service during the test phase and first test the signature connection only. A 1-factor procedure (SMS with one-time password) is used for signature release, which would only be suitable for the use of advanced signatures. Or you plan to use another second factor.

Access to the test account jurisdiction CH (ZertES) with the following claimed ID:

`ais-90days-trial-OTP:OnDemand-Advanced4`

Access to the test account jurisdiction EU (eIDAS) with the following claimed ID:

`ais-90days-trial-OTP:OnDemand-Advanced-EU`

4.2 Seals

4.2.1 Seals for Switzerland

Intentional use: Possibility to test the access to seals for Swiss jurisdiction.

Access to the test account with the following claimed ID:

`ais-90days-trial: static-saphir4-ch`

4.2.2 Seals for EU

Intentional use: Possibility to test the access to seals for EU jurisdiction.

Access to the test account with the following claimed ID:

`ais-90days-trial: static-saphir4-eu`

4.3 Timestamps

4.3.1 Timestamps for Switzerland/EU

Intentional use: Possibility to test the access to timestamps for Swiss and EU jurisdiction

Access to the test account with the following claimed ID:

```
ais-90days-trial
```

5 URL

Test account can be accessed via https://ais.swisscom.com .

6 Distinguished Name

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

6.1 Personal signatures (on-demand)

MUST/ OPTIONAL	Certificate parameter	Content	Example
MUST	CN	TEST <first name> <last name>	TEST Hans Mustermann
MUST	givenname	<First name(s)>[1]	Hans Urs
	surname	<Last name(s)>[1]	Mustermann
OPTIONAL (only after consultation)	O	TEST <Name of organization>	TEST ABC AG
OPTIONAL (only after consultation)	OU	<Information on the organizational unit or comment on the test, if O is set>	For Test purposes only, Test dept.
MUST	C	<Two-digit country code of the country of residence or home of the signatory (or of the organization, if O is set) >	CH
EITHER	emailaddress	<E-Mail of the signatory>	hans@swisscom.com
OR	serialnumber	<ID returned by the verify call if RA-App is used> or (only after consultation) <organization ID>: unique ID	RAS5b45b027c6d9370008072c48

Examples:

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=Muster, 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] Please note: using the RAS serialnumber, the names shall exactly match the names registered during the registration thus it could be necessary to add the 2nd or even 3rd name.

6.2 Seals (static)

For testing of seals we have added two certificates in the versions CH and EU to the test account, both have the same content

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

The certificates have already been set up by us and can be addressed according to the information in chapter 4.2.

7 Hints according the SLA

No availability is guaranteed for the test installation and Swisscom excludes any liability beyond the given liability by law. No service level is guaranteed.

If you have any problems, please contact MSC.support@swisscom.com. Technical training courses are also offered regularly for interested parties.

8 Instructions for use

The signatures obtained via this test account are test signatures and may only be used for technical implementation tests and demonstrations. They may not be used relating to contracts, certifications or agreements. The signatures are identified by the underlying signature certificate with the word "Test".

9 Contact data of the subscriber

9.1 Subscriber's address

Company name / organization name
Address
Postcode / Place

9.2 Technical main contact of the subscriber

First name, last name
Address
Phone number
Mobile number
E-Mail

9.3 Partner to be notified (optional)

First name, last name
Address
Phone number
Mobile number
E-Mail

10 Test access

After submitting this form to our fulfillment MSC.support@swisscom.com you will receive a confirmation with the activated test access (within 2 weeks). From then on you can use it until your access expires (90 days). Please order a prolongation afterwards if necessary.

11 Protection of the signature system

Despite "test access", this is a fully productive system which should be protected accordingly by the test participant application:

The private keys of the SSL/TLS certificate shall be either

- Encrypted on the system,
- Or stored on an external data stick/system,
- Or are managed encrypted by the subscriber application itself.

The participant application shall be protected against unauthorized access/manipulation and the operating system software and software components used shall be regularly kept up to date (update, patching).