As Europe's leading trust service provider, we enable the most innovative digital business models.

Integration Guide

Smart Registration Service

V1.41

Swisscom Trust Services

Scope	Integration Guide for Service Provider
Version	1.41
Status	Final
Replaces version	1.40
Issue date	13/05/2020
Document name	INT-GUIDE-SP-v0121.docx
Server location	Swisscom Trust Services

Checklist of changes

Version	Date	Changed by	Comments/nature of the change
1.0	24.01.2020	Joseph Koenig	Creation
1.1	02.03.2020	Joseph Koenig	Updated Identification status in §4
1.2	19.04.2020	Joseph Koenig	Status added in §4, §3 updated, appendix 1 updated
1.3	12.05.2020	Joseph Koenig	Appendix 1 updates, §6 Support added
1.4	10.07.2020	Joseph Koenig	Appendix 1 and 3 updates, Update &5.2
1.41	14.11.2020	Joseph Koenig	Appendix updated, Klarna method

Table of Contents

1 Introduction

The Smart Registration Service is a new service launched by Swisscom Trust Services in 2020 to enable Service Providers using electronic signature capabilities to use various efficient identification methods from selected Swisscom partners. Service providers can offer to the customers a signing process with on demand registration process with a selected authentication method based on the mobile number. The service consists of an API which can be used to get information about the different identification methods available and all necessary information to trigger the identification process itself. The Smart Registration Service is a complementary service to the Swisscom All-in Signing Service used to create electronic signatures and the Smart Registration Service that holds the registration data of the signatories. The identification process can be done independently from the signing process before the signing operation. During the signing operation only the registered authentication method is used.

1.1 Purpose

This integration guide is intended for developers of the service provider who would like to integrate the Smart Registration Service from Swisscom.
The technical documentation is mainly available on Swagger and this integration guide gives a big picture overview and helps the developer to go through the different steps.
The integration of the Smart Registration Service can be done within a very short time. The service uses well known protocols and does not require any special competencies.

- Estimation of integration time: 1 to 3 days
- Testing 1 to 3 days
- Productive within 1 to 2 weeks

1.2 Scope

The document refers to the Smart Registration Service. This guide describes how to perform the requests to get the available methods, how to set the filter and the semantic for its parameters. The guide will also give a catalogue (Appendix) with specific information or parameters for each identification method. It is recommended to check regularly the latest version of this Integration Guide to have the current overview of all possible methods.
Swisscom Trust Services adds new services constantly, according to new technological possibilities and regulations.

1.3 Terms and Abbreviations

AIS	All-in Signing Service: cloud-service provided by Swisscom to issue qualified and advanced electronic signatures, seals and timestamps
API	Application programming interface
Evidence	Signed personal identification data collected during the identification process and stored in the Smart Registration Service
LOA	Level of assurance, the identification method and the presented ID document enable a user either for LOA 3 (advanced signatures) or LOA 4 (qualified signatures)
SRS	Smart Registration Service
ISP	Identification Service Provider
SP	Service Provider
RA database	Database of the Registration Service
RA	Registration Authority: Role responsible for user identification and registration.
Verify call	Call to verify whether an evidence stored in the RA database enables the respective user for signing.

1.4 Referenced Documents

[1] Service Description SRS
[2] All-in Signing Service Reference Guide, Swisscom (Switzerland) Ltd.
[3] Description of how to perform a verify call, http://documents.swisscom.com/product/filestore/lib/5f4322cf-3530-4d6a-b26f-b8f685f8d069/VerifyID4Signing-en.pdf

2 SRS API Description

2.1 Online Documentation and Wiki

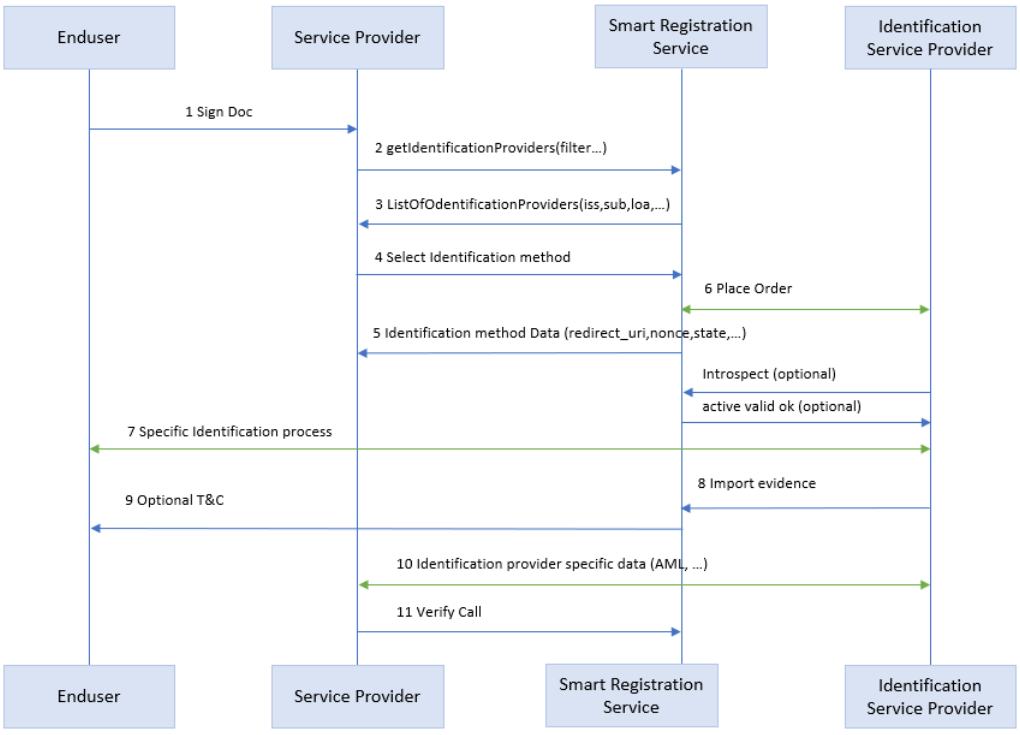
The API description is available on the Swagger platform on Swisscom Wiki.
https://miss-backend-api-preprod.scapp.swisscom.com/swagger/index.html

2.2 Steps for an end to end Identification process (High level)

The procedure in a nutshell:

- Service provider authenticates to the SRS
- Service provider submits a request to SRS API with an appropriate filter
- SRS response contains a list of available identification methods
- Service provider choses a method and submits a request for the specific method
- SRS provides the information to trigger the identification process (target URL and method specific information and data: see Appendix)
- Identification process is done
- Service provider can get the status of the successful identification while polling the status of a verify call to the Smart Registration Service

2.3 Main Flow and sequence diagram



The following flow and sequence diagram show the interface in detail:

(1) The user wants to sign a document and the Service Provider asks him to identify himself beforehand

(2) The Service Provider starts the identification process with the Smart Registration Service and asks for the list of the available ISPs using the bearer token.

(3) The Service Provider receives the list of the Identification Service Providers with the appropriate identification methods required for its process from the Smart Registration Service. Appropriate means for example: usable only for eIDAS or for ZertES signatures or only usable in a special country etc.

(4) The Service Provider selects (probably supported by the choice of the end user) the identification method and starts the identification process.

(5) Swisscom asks the Identification Service Provider for the personalized URL for the specific end user.

(6) The Smart Registration Service provides the personalized URL of the Identification Service Provider to the end user.

(7) The end user now calls up the URL to start the identification process directly with the ISP.

(8) The Identification Service Provider submits an OAuth2.0 introspection call to the Smart Registration Service in order to check the validity of the request.

(9) Swisscom analyses the bearer token and confirms the validity to the Identification Service Provider

(10) The Identification Service Provider imports the data taken during the identification process into the Smart Registration Service using the associated import interface (Smart Registration Service).

(11) Optionally the Service Provider can also fetch the evidence data from the Identification Service Provider, e.g. for AML check purposes using the Reference ID.

(12) Depending on the method used in (4) the Smart Registration Service sends out a SMS for the acceptance of the terms and conditions.

(13) The Smart Registration Service collects and archives the answer of the end customer concerning the terms and conditions.

(14) The Service Provider can verify that the evidence has been imported to the Smart Registration Service.

2.4 Authentication to the SRS

Aafter the onboarding process the SP can access the SRS Service with the OAuth2 – client credentials protocol. See chapter 3 and Swagger Documentation.

2.5 Initial Service Provider Information

The Service Provider may send initial information gathered from the user in advance, for example name, surname, mobile number etc. to speed up the identification process. This information will be verified by the Identification Service Provider during the identification process.
This is optional and depends on Identification Service Provider. For more details please refer to the Appendix "Initial Information".

3 Onboarding of Service Providers

The onboarding of a Service Provider is done after the contract for the use of SRS has been signed. Swisscom will configure the access to the SRS and send the credentials securely to the responsible person at the Service Provider (Username and Client Password). The protocol used for secure access to SRS is OAuth2.
To access the service the Service Provider shall provide:

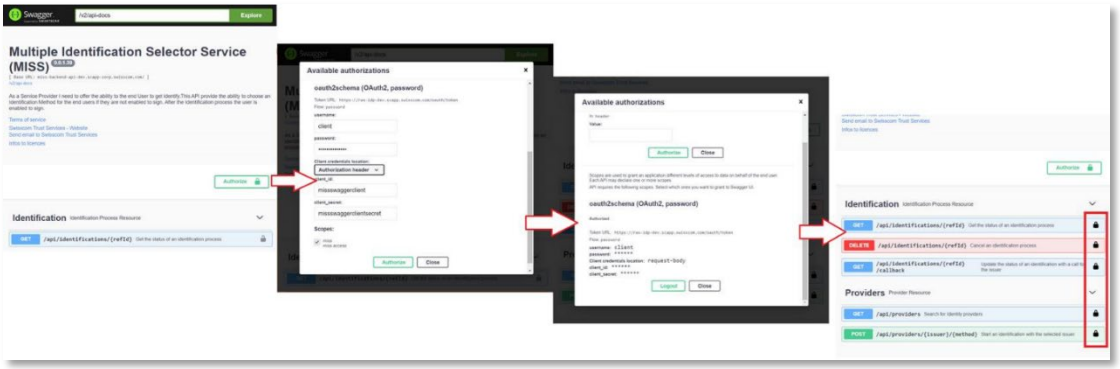
- Client ID
- Client Secret.

See Swagger documentation for more details:
https://miss-backend-api-preprod.scapp.swisscom.com/swagger/index.html

4 Testing environment

A test environment is available to Service Providers for test integration purposes. Service Providers can test integration end to end including the identification process.
Swisscom provides in its testing environment the possibility to simulate the different status of the identification method result. To use the test environment, use credentials below (without quotes)

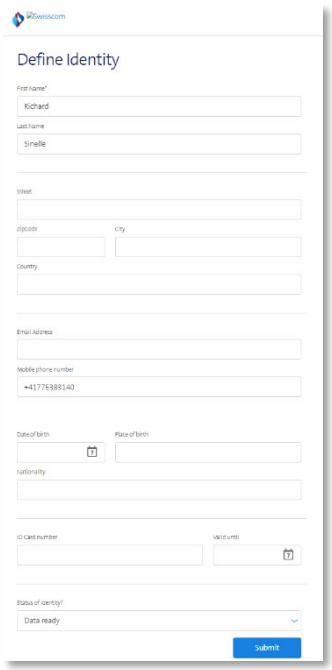
Username: "client" (needed only to access the test environment)
Password: "clientpassword" (needed only to access the test environment)
Client Id: "missswaggerclient"
Client secret: "missswaggerclientsecret"



The identification process can be mocked to facilitate testing. In the testing process the SP can simulate the status of the identification. In addition, the SP can enter its own testing data and then test the end to end process.

- Verify call: no valid evidence
- Test user identified
- Status set to data ready
- Verify call: Valid evidence found

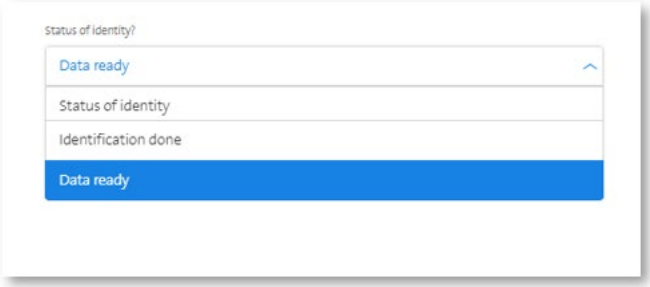
Typical end to end testing:

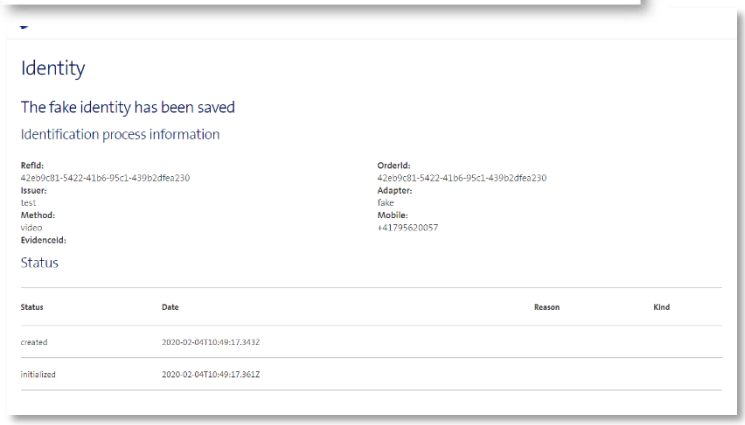


List of possible status:

Status	Semantic
Created	The identification data is collected and stored in order to initialize an order with the ISP
Initialized	The identification task has been ordered by the ISP. The identification task can now be started by the Service Provider by the use of the target URL.

Identification done	Identification process has been finished, evidence is in preparation
Data ready	The data is ready on ISP side and ready to be imported into the RA Database
Terminated	The evidence is present in the RA database and depending the identification process, the user must accept Terms and Conditions.
Error	The Identification data could not be imported in RA service for any reason like, fraud suspicion, negative identification in general, or due to insufficient means (bad camera, microphone) to identify. The response contains a string with the reason field provided by the ISP (not mandatory)





5 Additional Features of the SRS

5.1 Filter for Identification Methods

When requesting the list of available identification methods, the Service Provider can set a filter to get the relevant method for a specific process.

Filter parameter	Description	Remark
Issuer	Name of the ISP	When this parameter is set then the response will only contain identification methods from this specific ISP. Multiple issuers can be set.
Jurisdiction	Jurisdiction needed for the process	When this parameter is set the response contains only methods compatible with signatures for chosen jurisdiction. Multiple jurisdictions can be set. Jurisdiction available: EU (eIDAS), CH (ZertES)
LOA	Level of assurance (LOA) needed for the process. For example, LOA 4 if QES are needed, LOA 3 if AdES are needed.	When this parameter is set, the response contains only identification methods compatible with the chosen LOA.

Offline	Refers to an identification method where the user must follow a physical process offline, e.g. meeting a RA Agent, or going to a Post Office	The value can be true (include such methods in the response) or false (exclude such methods in the response)
Method Type	Name of the identification method (string)	The value is a string representing the method type (see list below) Only corresponding methods are included in the response
Webflow	Refers to an identification method where the user can follow the whole process in a web browser. For example, user will not need to download an app.	The value can be true (include such methods in the response) or false (exclude such methods in the response)
Real Time Method	Refers to a method where a user can sign immediately after finishing the identification process.	The value can be true (include such methods in the response) or false (exclude such methods in the response)

Identification method types:

- "**Video**"
- "**eID**": method is based on national eID concepts
- "**Bankident**": method is based on bank identification

This list will be updated regularly.

5.2 External ID

When choosing the identification method, the Service Provider has the possibility to provide a External ID. This External ID is a free text string defined by the Service Provider to be able to manage its own customer or partner requesting a signature where an identification is needed.
The External ID can be used by the SP for the billing of his customers.
(Note: This ID was named in the previous versions Customer ID)

6 Support

6.1 Overview

The whole identification process involves 3 parties: Swisscom, the service provider who wants to get a user enabled for the signature and the ISP.
The goal here is to clarify which support team has to be contacted, where are the limits and what data needs to be provided for a successful support process.

The whole process can be divided in 5 steps:

- Authentication to SRS and performing requests, receive appropriate response (Swisscom)
- Lead the end user to start the identification process (Service Provider)
- Identification process itself (Identification Service Provider)
- Leading the end user till identification is successful (Service Provider)
- Evidence is present in RA Service and user gets SMS for T&C to finalize the process (Swisscom)

As general rules we consider:

- The end user is in direct contact with the Service Provider for any business purpose. Thus, the 1st level support is ensured by the Service Provider who stay the SPOC for the end-user.
- If the analyze of the issue by 1st level Support reveals that some parameters are not fulfilled by Swisscom or the identification provider, then the Service Provider can contact through the right Support channel the Swisscom or identification provider Support by providing enough information (see table below in section 6.2).

6.2 Support cases and limitations

Issues may occur in each phase. The following table shows a list of possible issue, in each case the competent support team to be contacted. Also listed the parameter to check as fulfilled process step.

Process step	Issue with this process step	Successfull	Support Team (Data to provide)
1	▪ Server authentication to SRS Service ▪ Target URL not available, ▪ Order ID or Reference ID not available ▪ Unsuccessful response to correct request ▪ Service not responding	Target URL Ref ID Order ID	Swisscom Service Desk with PRO-Nr (Ref-ID, Order ID, method used, problem description Time)
2	▪ User redirect to Target URL ▪ User Identity data gathering ▪ User Identity data forwarding to identification provider ▪ Specific Implementation: see recommendations	Specific to SP	Service Provider Support
3	▪ Identification cannot be performed by officer ▪ Country not supported but in list ▪ Language not supported by Agent ▪ Timeouts ▪ Connection lost ▪ Specific identification app does not work (properly)	Officer confirms "Identification was successful" or "identification was unsuccessful" Final screen appears	Identification Service Provider via Swisscom Service Desk with PRO-Nr. (Ref-ID, Order ID, method used, problem description Time)
4	▪ Status checking ▪ Specific Implementation: see recommendations	Specific to SP	Service Provider Support
5	▪ Status is terminated but user does not get SMS for T&C ▪ Declaration of will (Mobile ID, PWD/OTP, etc.)	Evidence id Verify call successful	Swisscom Service Desk with PRO-Nr (Ref-ID, identification method used, MSISDN, evidence ID, Problem description, Contact)

7 Appendix – Identification Methods catalogue and specification

7.1 Overview and general recommendations

Hereafter you'll find the current list of identification methods available. For each method a description is given as a data sheet, that helps you to integrate the service in an efficient way.

Be aware about the specific recommendations for each method about the time taken for the identification process as the whole process is mainly composed of asynchronous single transactions. Please be also aware about the validity of the evidences that can be different from one method to another.

We recommend providing some useful information for the end-users about the steps they will have to pass to get a better understanding on the webpage of the Service Provider.

In order to increase the usability by the user we recommend informing the end-user to activate Mobile ID (MID or MID App) in advance. Doing so, the end-user will be able to use its MID or MID App for signing in a very easy way. Otherwise, the user will need to use the Password/OTP process (2-step authentication)

Before the start of the ISP's URL the user shall be notified that he will be redirected to an external identification service provider and shall be informed by the Service Provider about the usage of the personal data, e.g.:

- German: Durch den Aufruf der URL "https://xxx..." werden Sie zum Identifikationsportal unseres Identifikationspartners weitergeleitet, bei dem Sie sich im Auftrag der Swisscom Trust Services identifizieren können. Ihre hierfür erhobenen Personendaten werden ausschliesslich für die ordnungsgemässe Identifizierung im Rahmen der elektronischen Signatur verwendet.

- English: After the call of the URL "https://xxx.." You will be redirected to the identification portal of our identification partner which will identify you on behalf of Swisscom Trust Services. Your personal data collected for this purpose will be used exclusively for proper identification within the scope of the electronic signature.

In case you closed an additional contract with the Identification Service Provider for use of the identification data for own purposes (e.g. in the scope of the AML protection) you shall notify this like:

- German: Durch den Aufruf der URL "https://xxx..." werden Sie zum Identifikationsportal unsere Identifikationspartners weitergeleitet, bei dem Sie sich im Auftrag von uns und Swisscom Trust Services identifizieren können. Ihre hierfür erhobenen Personendaten werden ausschliesslich für die ordnungsgemässe Identifizierung im Rahmen der Überprüfung gegen die Bekämpfung der Geldwäsche und im Rahmen der elektronischen Signatur verwendet.

- English: By calling the URL "https://xxx..." you will be forwarded to the identification portal of our identification partners, where you can identify yourself on behalf of us and Swisscom Trust Services. Your personal data collected for this purpose will be used exclusively for proper identification in the context of the anti-money laundering review and in the context of electronic signatures.

7.2 Appendix 1 – Video Identification by Identity.tm

- Identification method name: VIDEO IDENTITY.TM
- Identification Service Provider: Identity.tm
- Signature capability for User Identified with this method: QES (AES)/eIDAS, AES/ZertES
  - Validity of the evidence: 5 years max
  - Language possible for video calls German, English
  - List of supported countries Link
- User Flow

  User starts identification – Video session is started (mobile phone or web) – Officer asks for information and scans ID documents - Mobile number is verified with a SMS Challenge - Video Session is terminated and Backoffice check is done - User can sign. Please note the special requirements that people to be identified can use the proprietary identity.tm app below.

- Method filter specification

Filter Parameter	Value	Value
Issuer	IDENTITY.TM	IDENTITY.TM
Jurisdiction	EIDAS	ZERTES
LOA	4	4 (from April 2nd, 2020 due to New decision of the Federal Council in the context of the Corona Crisis)
Offline	FALSE	FALSE
Method Type	Video	video
Web flow	TRUE	TRUE
Realtime Method	TRUE	TRUE

- **Initial Identity Data submission(optional)**: When initiating the process, the Service Provider can submit identity Data gathered from the user in advance. This is not mandatory, i.e. the identification process can be started with an empty payload.
  - **Attention**: To be able to use the identity.TM Mobile App, at least the **Surname** must be provided. Otherwise only the flow in the browser can be used for identification.
  - In case of identity data is provided, this data must match with the real data of the user as this data will be verified during the identification process by the RA Agent (small typos are allowed and will be corrected by the RA Agent). Otherwise the identification will be rejected as fraud attempt.

Recommended implementation:

- Prior integration, it is useful that the SP think about the data match: It is possible to collect all the data that the SP has about the end user and send it to identity.tm. But only in case of an additional contract with identity.tm to use the data for own purposes (e.g. AML check) the SP gets back a data set of matched. Otherwise the SP will only get back a "failed" without knowing which data was wrong and the SP will have to ask the end user to check the correct spelling or to correct the mistakes.
- If it is not needed to do a matching between the data in the Service Provider account and the Data in RA Service, then we suggest submitting only the Surname (also called Last name or Family name, necessary for the mobile App) an none of the other attributes listed below in the table. This submitted surname must correspond exactly to the real data of the user as written in the Pass or ID document (without typo).
- If a matching is needed, the SP should provide only the data he wants to be verified. If the identification is successful, the data is verified. If not, suggest your user to check all the entered data (all first names entered? no typos? accents? etc....).

- If the verification fails in the beginning of the Identification process, then the Status "IDENTIFICATION_NEGATIVELY_CONDUCTED", and the identification must be started again. The service provider will have to place a new order to get a new target URL

List of initial Identity Data that can be submitted

Attributes	Can be submitted to SRS (*)
First name, Surname	Yes
Mobile number	Yes
Postal Address data	No
Date of birth	Yes
Place of birth	Yes
Nationality	Yes
Artist Name	No
Title	No
Serial ID Document	No
Issuer Country	No
Issuing city	No
Validity	Yes

(*) see Swagger documentation

- **Connection lost during the Video Call**

The call can take some time (usually several minutes). Within this time the connection can be lost, independently to the SRS Service or identity.TM service (e.g. bad signal quality), or something can happen on user side that breaks the process. In this case we recommend the service provider to inform the end user how he should proceed. The target URL can be reused for example and the customer could start again the identification.
In case the service provider has announced a new target URL to the end user, the service provider must ensure that all previous pending orders are properly cancelled according to the Swagger documentation. Otherwise the service provider has a lot of pending orders.
Ideally, we would recommend the Service Provider to send to the end user the Target URL and all needed information to start over again by use of a separate communication channel (email for instance)
The Target URL is valid until cancellation. The service Provider can cancel the order if needed after a while (See Swagger documentation)

- **Specific identification method response Information**

	Description
Target URL	URL to the Identification Service Provider to start
Swisscom Reference to the transaction	Ref ID
Identity.TM Reference to the transaction	Order ID

- **Recommended implementation**

The video Identification process can take between **10 to 20 Minutes** (including back office 4-eyes principle check by compliance officer). After video identification is triggered by the Service Provider, the Service Provider should wait for this period before checking through a Verify Call whether the identification has been successful. Please note that the verify call can fail due to two reasons:

- Identification evidence data not yet transmitted to Swisscom (Status is not "Terminated", see §4 List of possible Status)
- User did not accept the terms of use

- **System Requirement:**
    - If the browser is not supported, a message prompted
    - Chrome, Firefox, Opera, Safari and Edge are supported.
    - Internet Explorer is not supported.
    - Known issues with current version of Safari.

- Desktop Browser: Chrome, Opera, Firefox, Safari, Edge - latest versions (official) or
- Mobile Device: for native Android (5+) and iOS Apps (13+)
    - Internet Explorer is not supported. Known issues with current version of Safari.

- Bandwidth: Minimum 0,5 MB/s up/down
- Microphone: Enabled
- Camera: Enabled with minimum resolution 640 x 480 px
- Network requirements:
    - Minimum: The minimum Requirement is that TCP port 443 is open. Some firewall/proxy rules only allow for SSL traffic over port 443. You will need to make sure that non-web traffic can also pass over this port. TLS1.2
    - Better Experience: In addition to the minimum requirements being met, we also recommend that UDP port 3478 is open. TLS1.2
    - Best Experience: For the best possible experience, we recommend that UDP ports 1025 - 65535 be open. TLS1.2
- WebRTC: Outbound TCP, non-SSL web traffic on port 443 and the following domains must be accessible:
    - *.tokbox.com (static IP blocks also available)
    - static.opentok.com
    - enterprise.opentok.com
    - api.opentok.com
    - anvil.opentok.com
- WebSocket: In some situations, WebSocket connections are blocked over port 80. In this case a secure SSL connection using WSS over port 443 should successfully connect. The destinations and ports used by Pusher clients are as follows:
    - ws://ws.pusherapp.com on port 80

wss://ws.pusherapp.com on port 443

7.3 Appendix 2 – Identification with bank account login, by Klarna

- Identification method name: Bank
- Identification Service Provider: Klarna
- Language of the front End App: German, English
- Signature capability for User Identified with this method: QES (AES) /eIDAS, AES /ZertES
- Validity of the evidence: 2 years
- Countries/Documents: N/A
- Supported Banks: German banks except Listed here: Link
- User flow

  Precondition: User is owner of a bank account from a bank supported by Klarna Process.
  User starts identification – chooses his bank – User performs login to his bank account and small transaction – mobile phone is checked through SMS challenge – Checks are done – User gets an SMS to accept the T&C. After the T&C Are accepted, the user can sign.

- Method filter specification

Filter Parameter	Value
Issuer	KLARNA
Method Name	Bank
Jurisdiction	EIDAS/ZertES
LOA	LOA3 LOA4
Offline	FALSE
Method Type	Bankident
Webflow	TRUE
Realtime Method	TRUE

- Initial Information: Information that can be provided while triggering the identification method:

M *List of initial Identity Data that are submitted*

Attributes	
Firstname (Given Names)	**Mandatory***
Lastname (Surname)	**Mandatory***
Date of birth	**Mandatory***
Mobile number	**Mandatory***
Place of birth	Optional
Country	**Mandatory***
Email address	Optional
Language	Optional
External ID	Optional

(*) This data must match with the personal data linked to the bank account.

- Specific identification method response Information

	Description
Target URL	URL to the Identification Service Provider to start
Ref. ID	Reference to the transaction

- Recommended implementation

After the Identification process is started, a Session is active for 60 Minutes to finish the Process.

The Identification is finished when status "Terminated" is reached.

If the Timeout is reached (60 Minutes) without status "Terminated", then the Identification gets the Status Negative Identification.

After the identification process is terminated, we recommend starting with Verify Call after a delay of **30 Seconds to 2 minutes**. After the verify call is successful, the user is correctly registered and can sign.

- **Connection lost during the Process**

If the connection is lost during the process or something goes wrong **the target URL can be used again 5 Times within the session time of 60 Minutes**.