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

Integration Guide

QES Ident Service

V1.0

Swisscom Trust Services

Swisscom Trust Services

Scope	Integration Guide for Service Provider
Version	1.0
Status	Final
Replaces version	N/A
Issue date	18/11/2020
Document name	INT-GUIDE-QES-v0100.docx
Server location	Swisscom Trust Services

Checklist of changes

Version	Date	Changed by	Comments/nature of the change
1.0	18.11.2020	Joseph Koenig	Creation

Table of Contents

1 Introduction

The QES-Ident-Service is a new service launched by Swisscom Trust Services in 2020 to enable Service Providers using electronic signature capabilities to use an efficient identification method in collaboration with our partner Klarna as Identification Service Provider. Service providers can offer to the customers to sign a document with a qualified electronic signature based on e-Banking login and authentication by the mobile number. The service consists of an API which is also used in the context of other registration possibilities and offers some optional API calls which may be not necessary for the QES Ident Service. The QES-Ident-Service is a complementary service to the Swisscom All-in Signing Service used to create electronic signatures and provides the link to the needed identification process. Typically, the signing process is done in the context of the identification process.

1.1 Purpose

This integration guide is intended for developers of the service provider who would like to integrate the QES-Ident-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 QES-Ident-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 QES-Ident-Service. This guide describes how to perform the requests to get the right Identification method.

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
ISP	Identification Service Provider
JWT	Jason Web Tokens
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
RA	Registration Authority: Role responsible for user identification and registration.
RA database	Database of the Registration Service
SP	Service Provider
Verify call	Call to verify whether an evidence stored in the RA database enables the respective user for signing.

1.4 Referenced Documents

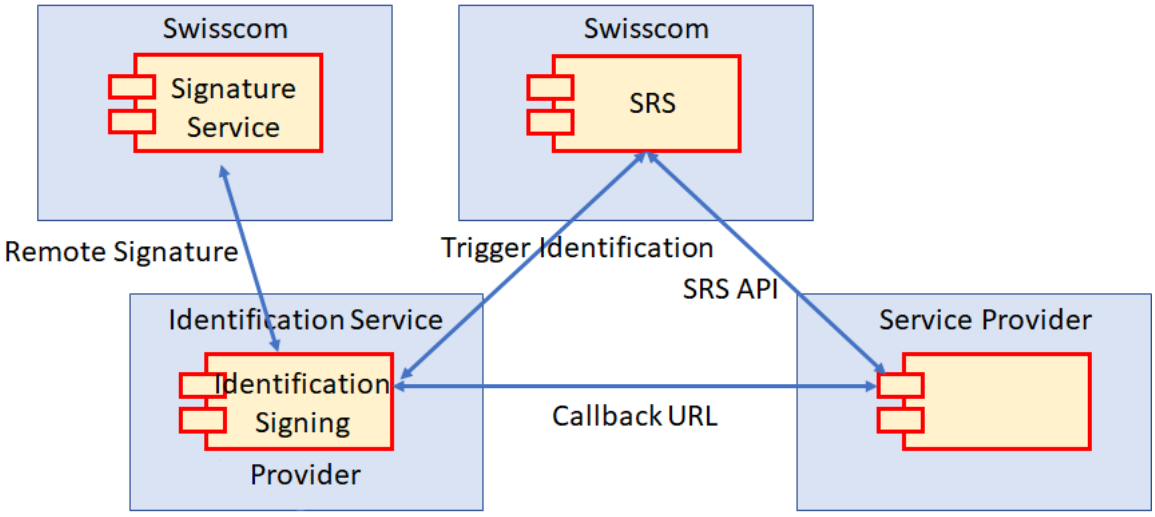
[1]	Service Description QES Ident Services
[2]	All-in Signing Service Reference Guide, Swisscom (Switzerland) Ltd.

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
As the QES-Ident-Service uses functionalities of the Smart Registration Service (usable through the SRS API), we will describe in the next descriptions the use of the SRS API.

2.2 Overview components



2.3 Role concept

We have the following actors:

- Service Provider (SP) is the customer of the QES Ident Service which offers the QES Ident Service to its end customers the signatories of a document.
- Identification Service Provider (ISP) is the Swisscom partner and delegated registration authority which performs the identification process for the future signatory and provides the identification data to Swisscom and the Service Provider

2.4 Prerequisite for the SP to use QES-Ident Service

In order to use QES-Ident Service the SP will need to setup an endpoint for the ISP in order to receive the identification data. The SP will provide for each identification a call-back URL used then by the ISP to provide the identification data. JWT's that can be signed to check the authenticity of the provider will secure the information exchange. Additionally, as the JWT's signature is calculated using the header and the payload, this can be used to check that the content was not tampered.
(The detailed description and use of JWT's is out of scope of this integration guide)

2.5 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 selects the identification method for QES Ident service in the communication with the Smart Registration Service and starts the identification process based on a set of (optional) initial identification data of the person to be identified and the hash of the document to be signed.

3- Swisscom opens an order at the Identification Service Provider and asks the Identification Service Provider for the personalized URL in order to identify the specific end user.

4- The Smart Registration Service provides the personalized URL of the Identification Service Provider to the Service Provider for his end user.

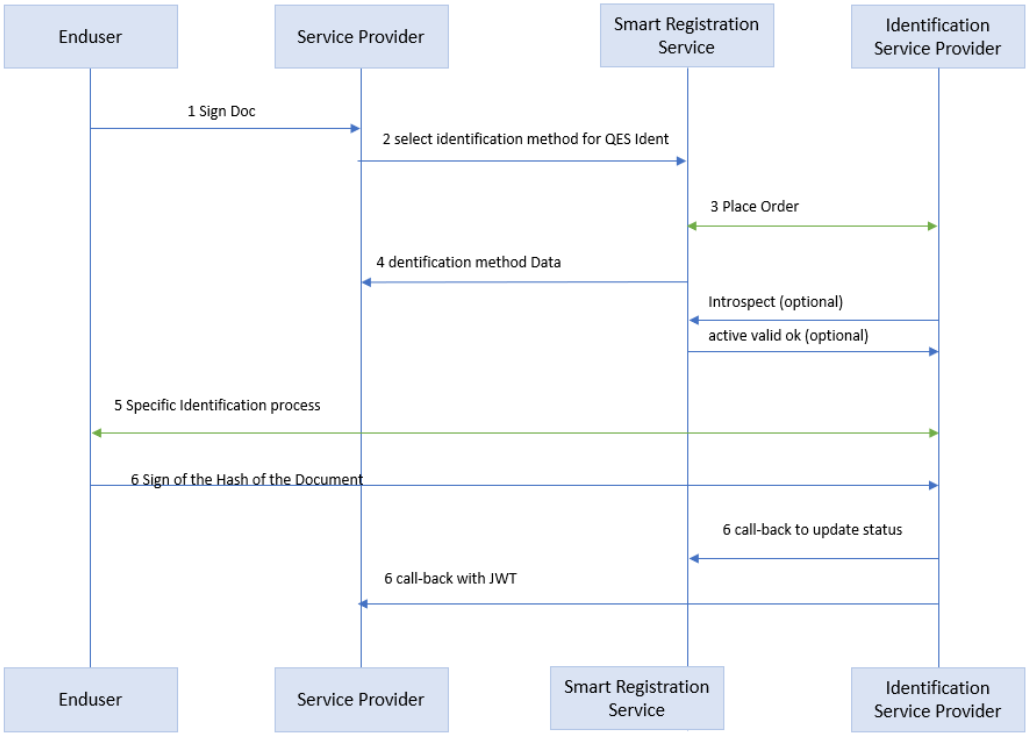
   Optional: The Identification Service Provider submits an OAuth2.0 introspection call to the Smart Registration Service in order to check the validity of the request. Swisscom analyses the bearer token and confirms the validity to the Identification Service Provider

5- The end user now enters the URL in his browser to start the identification process directly with the ISP.

6- The end user signs the hash of the document via the ISP and the remote Signature Service of Swisscom

7- The ISP makes a call-back to SRS to update the status about the identification process

8- The ISP makes a call-back to SP with a JWT after identification in order to get the collected identification data and evidence and the signed hash



2.6 Authentication to the SRS

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

2.7 Initial Service Provider Information

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

3 Onboarding of the Service Provider

The onboarding of a Service Provider is done after the contract for the QES-Ident-Service 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:

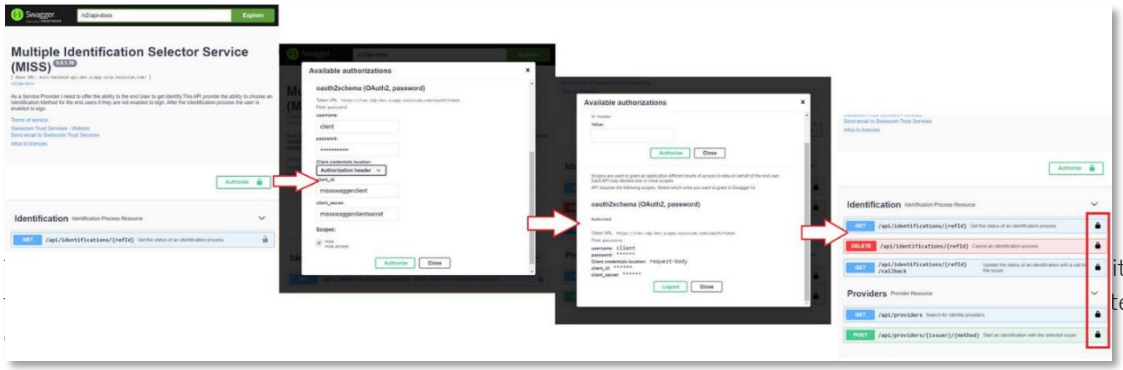
- Client ID
- Client Secret.

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"



itate
ter its

Typical end to end testing:

- Create Target URL
- Test user gets identified and performs signature

- Check Status until status is terminated

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.
Terminated	The Identification is finished, and the identification provider performed the callback on SRS API
Error	No callback was performed by the ISP

5 Additional Features of the SRS

5.1 Filter for Identification Methods)

This feature generally not necessary for QES Ident. For more details please refer to the integration Guide of SRS Service: linkExternal ID

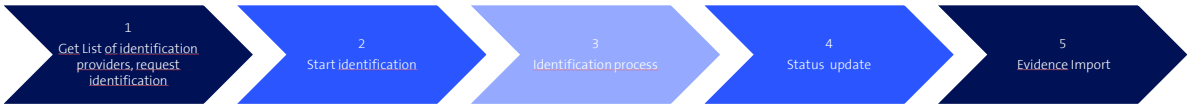
5.2 External ID

When choosing the identification method, the Service Provider has the possibility to provide an 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. Swisscom will associate the identification request with this External 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:

1. Authentication to SRS and performing requests, receive appropriate response (Swisscom)
2. Prompt the end user to start the identification process (Service Provider)
3. Identification process itself (Identification Service Provider) combined with the signature process
4. Guide the end user till identification is successful (Service Provider)

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, 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 ISP ▪ Timeouts ▪ Connection lost ▪ Signature not placed on hash	ISP confirms successful or unsuccessful identification with Information on the Final screen.	Identification Service Provider via Swisscom Service Desk with PRO-Nr. (Ref-ID, method used, problem description Time)
4	▪ Status checking ▪ Specific Implementation: see recommendations	Specific to SP	Service Provider Support

7 Appendix – Details Identification Method for QES-Ident-Service

- Identification method name: aml-bank
- Identification Service Provider: Klarna
- Signature capability for User Identified with this method: QES/eIDAS
- Countries/Documents: N/A
- User flow

  Precondition: User is owner of a bank account supported by Klarna Process
  User starts identification – chooses his bank – User performs login to his bank account and signs the contract– mobile phone is checked through SMS challenge – Checks are done –

Method filter specification

Filter Parameter	Value
Issuer	KLARNA
Method Name	aml-bank
Jurisdiction	EIDAS
LOA	4
Offline	FALSE
Method Type	Bankident
Webflow	TRUE
Realtime Method	TRUE

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

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
Nationality	**Mandatory***
Email address	Optional
Language	Optional
External ID	Optional
documentHash (**)	**Mandatory***
callbackUrl (***)	**Mandatory***

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

(**) Hash of the document that needs to be signed

(***) The service provider needs to setup an endpoint for the Identification provider to send the Callback when identification is done (Out of scope, see integration Guide ISP)

Specific identification method response Information

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