



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

Integration Guide

Smart Flows

V1.3.1

Integration Guide for Service Provider	
Scope	
Version	1.3.1
Status	Review
Replaces version	1.3
Issue date	08/012/2023
Document name	INT-GUIDE-Smart-Flows-SP-v1.3.1.docx
Server location	Swisscom Trust Services
Checklist of changes	

VER-SION	DATE	CHANGED BY	COMMENTS/NATURE OF THE CHANGE
0.9	14.11.2022	Joseph Koenig	Creation (Draft)
1.0	08.12.2022	Ionut Vacariu/Peter Amrhyn	API Description added
1.1	23.12.2022	Joseph Koenig	API Key Preprod updated
1.2	02.03.2023	Joseph Koenig	§6.1.3 updated with new status
1.3	17.03.2023	Joseph Koenig	§6.1.3 updated: deprecated status removed
1.3.1	08.12.2023	Ionut Vacariu	Authentication layer added §6.1.2

Table of Contents

1	Introduction	4
2	Benefits for the End Users	4
3	Benefits for the Platform partner	4
4	Generalities	5
4.1	Purpose of the Guide	5
4.2	Scope	5
4.3	Terms and Abbreviations.....	5
4.4	Referenced Documents	6
[1]	Service Description SRS.....	6
5	Smart Flow Features and sequence diagram	6
5.1	MVP Description	6
5.2	Front End	6
5.3	Library.....	6
5.4	Features available (Front End and Library).....	6
5.5	Integration.....	8
6	Onboarding of Service Providers.....	8
6.1	Standard Implementation	8
6.1.1	Integrate Smart Flow directly using the API of Smart Flows	8
6.1.2	Mobile number verification.....	9
6.1.3	Status Page display.....	9
6.1.4	T&C Acceptance	10
7	Testing environment.....	12
8	Support	13
8.1	Support Smart Flows	13
8.2	Support cases and limitations (for SRS).....	13

1 Introduction

The Smart Flows service (also called MFE i.e., Modular Front End) is an extension of the Smart Registration Service. With the Smart Registration Service Clients have the possibility to benefit from various Identification methods, depending on their specific need of jurisdiction and signature level.

Due to the various methods and identification partners the user is switching between different context, as signature platform, Identification platforms, Authentication platform etc... between Swisscom and Swisscom partners.

The clients can build their own flow based on the provided APIs, but Smart Flows provide an easy way to have a consistent End to End Flow including best practice and useful end customer information.

2 Benefits for the End Users

The end user would be able to easily:

- View what does Qualified Electronic Signature (QES) mean and how it works
- Check whether its phone number has its QES capabilities enabled or not

If QES is enabled:

- Check its current registration / assurance levels (i.e., whether it is allowed to sign a certain document or not)
- Upgrade its registration / assurance levels
- Check its signature method (e.g., MobileID, Password + SMS challenge, etc)
- Check whether there is an action required to maintain its status (e.g., accept the latest Terms of Use, etc)
- Check its status expiration date

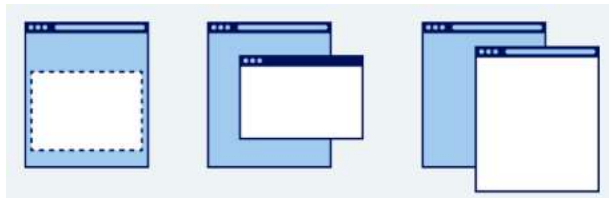
if QES is disabled (further releases):

- Enable QES for its phone number following as simple and guided process
- View all the methods available for its ID verification and the certificate / assurance levels to be granted
- View the different types of documents that can be e-signed with the different registrations / assurance levels

3 Benefits for the Platform partner

The platform partner would be able to easily:

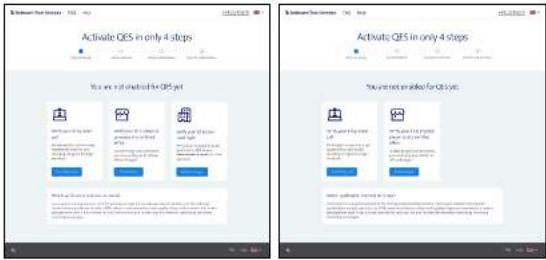
- Integrate the Modular Front End (MFE) solution to its platform
- Decide how the MFE would be integrated: widgets, embedded views, pop-ups, opening new tabs, etc



- Customize visual the elements of the MFE to match the platform look and feel via a simple CSS file



- Define which authentication methods to allow in its platform (view all, only video call id verification, etc)



- Define whether to allow the service to require user to accept latest Terms of Use or not
- Keep up to date with the service's latest functionalities, tutorials, documentation and FAQs for end users

4 Generalities

4.1 Purpose of the Guide

This integration guide is intended for developers of the service provider who would like to integrate the Smart Flows. The simplest Integration consist in the simple use of the libraries provided by Swisscom on the NPM platform. A Swagger documentation is also available for Partner who wants to integrate more specifically.

4.2 Scope

The document refers to Smart Flows integration. Prerequisite is a contract and integrated Smart Registration Service. This guide describes how to use the library to provide a consistent flow to the end user.

4.3 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
IPSP	Identity Proofing Service Provider
SP	Service Provider
RA database	Database of the Registration Service
RA	Registration Authority: Role responsible for user identification and registration.
T&C	Terms and Conditions
Verify call	to verify whether an evidence stored in the RA database enables the respective user for signing.

4.4 Referenced Documents

- [1] Service Description SRS
- [2] All-in Signing Service Reference Guide, Swisscom (Switzerland) Ltd.
- [3] Integration Guide Smart Registration Service (SRS) <https://trustservices.swisscom.com/wp-content/uploads/2022/09/INT-GUIDE-SRS-v1.7-en.pdf>

5 Smart Flow Features and sequence diagram

5.1 MVP Description

The MVP will contain two main components. The Smart Flows front end, intended for end user, to be able to check easily their identification Status. The Smart Flows Library (React) that can be used as is and integrated in any flow. The Smart Flows components interact with a back-end (Smart Flows back-end) which transfers the request to the different components involved in the Smart Flows features as RA Service APIs (Verify Call, Lookup Call etc...), Mobile ID API, SAS API (Serial for the Authentication method with PWD /OTP)

5.2 Front End

For the MVP the front End will provide the features listed below:

- Mobile number check
- Status page of a user:
 - Dashboard with the jurisdictions and signature level
 - Authentication method used and status
 - Explanation text about the QES
 - Status of the T&C Acceptance
- Button with T&C Acceptance possibility

Features planed for the next releases:

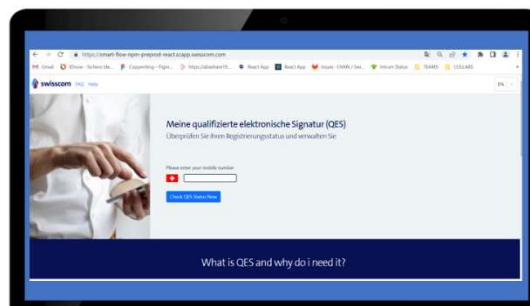
- Possibility to start a new identification
- Web components as Widgets

5.3 Library

Once integrated, the library will provide the standard flow to the user and guide the user to the next step for his successful registration.

5.4 Features available (Front End and Library)

Mobile Number verification



5.5 Integration

Download the Library: [Link to Library](#)

Then add the component in package.json :

```
"dependencies": {  
  "@swisscom/smart-flow-web-components": "^0.5.1-49"  
}
```

An alternative would be to run: `npm i --save @trustservices/smart-flow-web-components`

6 Onboarding of Service Providers

6.1 Standard Implementation

The clients will get access to the Smart Flows as soon as they will subscribe for an SRS contract. So Smart Flows is an additional Service of SRS.

The Artifactory can be found here:

[DEPRECATED] (From March 2024)

To be able to use

- **API Key**
- **Referer** (the URL where the FE application is hosted)

[NEW]

The client needs to have an SRS account for retrieving the JWT token.

Current Front-End Version (Example of Smart Flows integration) on Preprod environment:

<https://smart-flow-npm-preprod-react.scapp.swisscom.com/>

We recommend using the provided library to display the Smart Flows Screens. For more details, we provide here also the Swagger documentation the Smart Flows back end: See next section §6.2.

6.1.1 Integrate Smart Flow directly using the API of Smart Flows

Online API documentation:

<https://smart-flow-api-preprod.scapp.swisscom.com/swagger/index.html?urls.primaryName=Admin%20Doc#/>

6.1.2 Authentication layer

From version Smart Flow 1.3 a new authentication layer has been added. The current authentication for the SRS will be used also for accessing the Smart Flow API.

See here for more details:

<https://miss-backend-api-preprod.scapp.swisscom.com/swagger/index.html>

The authentication is done with:

- client ID
- Client secret

Scope: smartflow

[NEW]

With the client secret, the JWT token can be retrieved by the following CURL request:


```
curl --location --request POST 'https://xxxxx/oauth/token' \
--header 'Authorization: Basic CLIENT SECRET' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'scope=smartflow'
```

6.1.3 Mobile number verification

Use the Post Method

- 1) Post mobile number to Smart Flow Service to get OTP sent to mobile device of user for authentication

Request:

```
curl -X 'POST' \
'https://smart-flow-api-preprod.scapp.swisscom.com/api/public/confirm'\
-H 'accept: */*' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer *****'\
H 'X-Api-Key: *****'
-H 'Referer: https://smart-flow-api-preprod.scapp.swisscom.com'\
-d '{
  "msisdn": "4179999999",
  "code": "ABCD"
}'
```

Response: Status code: 200 OK

- 2) Post OTP from user to Smart Flow Service

Request:

```
curl -X 'POST' \
'https://smart-flow-api-preprod.scapp.swisscom.com/api/public/phone/verification/code' \
-H 'accept: */*' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer *****'\
H 'X-Api-Key: *****'
-H 'Referer: https://smart-flow-api-preprod.scapp.swisscom.com'\
-d '{
  "msisdn": "4179999999",
  "code": "ABCD"
}'
```

Response:

Status code: 200 OK – for the case when OTP is ok

Status code: 400 Bad Request – for the case when OTP is not ok

6.1.4 Status Page display

To display the entire status, you will need to gather the information about LOA, Jurisdiction and status of the linked authentication mean (Mobile ID or PWD OTP)

LOA, Jurisdiction, Status Authentication mean...

1) Lookup status of user evidence and Terms & Condition status

```
Request:
curl -X 'GET' \
  'https://smart-flow-api-preprod.scapp.swisscom.com/api/public/evidence/status?msisdn=417999999' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer *****\
-H 'X-Api-Key: *****\
-H 'Referer: https://smart-flow-api-preprod.scapp.swisscom.com'

Response:
{
  "status": [
    {
      "assuranceLevel": 3,
      "jurisdiction": "zertes"
    },
    {
      "assuranceLevel": 3,
      "jurisdiction": "eidas"
    }
  ],
  "loa4ExpiryDate": null,
  "signingStatus": "MISMATCH",
  "notFound": false
}
```

Call to action depending on status:

User evidence is active but serial number mismatch detected

Stats	Semantic
MID	User authenticated with Mobile ID and evidence is registered with RA Service and can sign QES.
SAS	User authenticated with PWD/OTP and evidence is registered with RA Service and can sign QES.
NOT_ABLE_TO_RETRIEVE	The API was not available, a retry should be done
NOT_REGISTERED_AT_ALL or NOT_RA_MID_SAS	User not registered not using PWD OTP not Using MID: get identified
MISSMATCH_SAS_BUT_MID	You have activated MID after you were registered with PWD OTP
MISSMATCH_SAS_CHANGE_SN	You have changed your Password after your Identification
MISSMATCH_MID	You have re-activated MID without recovery code after you were registered with MID

"

The T&C acceptance is asynchronous process based on three steps as described below:
To start the T&C acceptance you will need to fetch the link for the T&C acceptance.
Format of the link:

```
Request: /api/public/evidence/{msisdn}/tc
curl -X 'GET' \
  'https://smart-flow-api-preprod.scapp.swisscom.com/api/public/evidence/41*****/tc' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer *****\
-H 'X-Api-Key: *****\
-H 'Referer: https://smart-flow-api-preprod.scapp.swisscom.com'

Response:
{
  "link": "https://rasd.scapp.swisscom.com/t/xxxxxxx"
}
```

Response code 200 and T&C link is provided as attribute of response	<p>Partner should directly display T&Cs Website and let the user accept T&Cs.</p> <p>In case partner would like to integrate T&Cs page directly in its own portal, the following steps must be implemented:</p> <p>Get the T&Cs website and parse for the token</p> <p>Get links to T&Cs document with token</p> <p>Either user is directly redirected to T&Cs website of Swisscom Trust Services or partner implements custom flow, please check steps below (please be aware of contract obligation)</p> <p>Display links to user so that user can accept T&Cs</p> <p>If user confirms T&Cs, partner must submit confirm call to request service to accept T&Cs <i>/api/public/confirm</i></p> <p>(In case user has PWD/OTP as an authentication method, partner must show to user consent page so that user can enter password and OTP to accept T&Cs.)</p> <p>Partner must poll status of request to check if user has accepted T&Cs <i>/api/public/mobileid/status</i></p>
Response code 404	No T&C link can be found, and user must either have T&Cs accepted or there is no evidence registered.

1. With the token obtained from the step before, start the asynchronous process by calling the following API:

```
Request: /api/public/confirm
curl -X 'POST' \
  'https://smart-flow-api-preprod.scapp.swisscom.com/api/public/confirm' \
  -H 'Authorization: Bearer *****\
-H 'accept: */*' \
```

```
-H 'X-Api-Key: *****' \
-H 'Referer: https://smart-flow-api-preprod.scapp.swisscom.com/' \

-H 'Content-Type: application/json' \
-d '{
  "decizionZertes": true,
  "decisionEidas": true,
  "knowsTheRisk": true,
  "token": "*****"
}'
```

Response:
Status code: 200 OK – for the case when OTP is ok

2. After the step 2 is done, the user input is expected. In this step, pooling is done to the following API to get the status of the user.

```
Request: /api/public/mobileid/status
curl -X 'GET' \
  'https://smart-flow-api-preprod.scapp.swisscom.com/api/public/mobileid/status?token=*****' \
  -H 'accept: */*' \
  -H 'Authorization: Bearer *****\
-H 'X-Api-Key: *****' \
-H 'Referer: https://smart-flow-api-preprod.scapp.swisscom.com/'
```

```
Response:
{
  "token": xxxxx,
  "error": null,
  "consentUrl": null,
  "confirmed": false,
  "downgrade": false
}
```

token	The token for which the request was made
error	Not null if any error occurred
consentUrl	The consent url for the users that has to accept the T&C with PWD/OTP instead of MobileID. If this field is populated, this URL needs to be opened in a iframer. After the user enter the OTP, “confirmed”/”donwgrade” field will became true in the next pooling calls.
confirmed, downgrade	True when the user confirmed the T&C, false otherwise.

7 Testing environment

As for SRS 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)

Client Id: "missswaggerclient"

Client secret: "missswaggerclientsecret"

With this api key **3StDe481zPEI7nYMGR1FEQkTTtIKFasH** you can start the application at localhost:3000.
To start the attached application, use: npm run start

8 Support

8.1 Support Smart Flows

Swisscom will only provide support for general questions regarding the library, credentials problems or the access to the artifactory. Swisscom will not be able to support clients for specific integration needs. For this we recommend the clients to check the swagger documentation.

First level Support may be assured as usual by the partners for End User. Partner may use the same channel for getting support as for SRS (see below)

8.2 Support cases and limitations (for SRS)

We added here the support procedure for SRS. Customer with SRS contract can contact the support with Pro Number through the standard channel.

Our Hotline: +41 (0) 800 724 724, Menu selection "Datendienste" (Data services), use the word "All-in Signing Service".

Or per e-mail: ent.incident-data@swisscom.com

(please do not forget your PRO-number)

Your PRO-Number: is shown on the cover page of your contract.

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.

Pro- cess step	Issue with this process step	Successful	Support Team (Data to provide)
1	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none">▪ Status checking▪ Specific Implementation: see recommendations	Specific to SP	Service Provider Support
5	<ul style="list-style-type: none">▪ 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, ev- idence ID, Problem description, Con- tact)