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

Integration Guide

Smart Registration Service

V1.8

Swisscom Trust Services

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

Scope	Integration Guide for Service Provider
Version	1.8
Status	Final
Replaces version	1.7
Issue date	30/09/2022
Document name	INT-GUIDE-SP-v018.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
1.42	24-08.2021	Joseph Koenig	Appendix updated video; Appendix added for eID
1.5	15-12-2021	Joseph Koenig	Appendix 4 added Nect §8.5, review §4, added §5
1.6	12-06-2022	Joseph Koenig	Updated Appendix 4, added Appendix 5 and 6 for SRS video and Auto Ident CH
1.7	30-09-2022	Joseph Koenig	SRS Auto ident CH and SRS Video Ident CH updated – Appendix 7 added for the SRS ident web flow
1.8	15-06-2023	Joseph Koenig	§6.3 Silent SMS mode added

Table of Contents

1 Introduction 4
1.1 Purpose 4
1.2 Scope 4
1.3 Terms and Abbreviations 4
1.4 Referenced Documents 4
2 SRS API Description 5
2.1 Online Documentation and Wiki 5
2.2 Steps for an end to end Identification process (High level) 5
2.3 Main Flow and sequence diagram 5
2.4 Authentication to the SRS 6
2.5 Initial Service Provider Information 6
3 Onboarding of Service Providers 6
4 Testing environment 7
8
5 Recommended Integration – Best Practice 9
5.1 Verify Call – Lookup Call 9
5.2 Status tracking end-to-end and method selection 9
6 Additional Features of the SRS 10
6.1 Filter for Identification Methods 10
6.2 External ID 10
7 Support 11
7.1 Overview 11
7.2 Support cases and limitations 11
8 Appendix – Identification Methods catalogue and specification 13
8.1 Overview and general recommendations 13
8.2 Appendix 1 – Video Identification by Identity.tm 14
8.3 Appendix 2 – Identification with bank account login, by Klarna 18
8.4 Appendix 3 –Identification with nPA (eID) by Identity.tm 20
8.5 Appendix 4 –Identification with Robo-Ident (SRS-Selfie-Ident) by Nect 23
8.6 Appendix 5 –Identification with SRS Video-Ident-CH by INTRUM 31
8.7 Appendix 6 –Identification with SRS Auto-Ident-CH by INTRUM 34
8.8 Appendix 7 – Identification over the Swisscom Trust Services Identification page 37

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
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.

1.4 Referenced Documents

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

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

[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

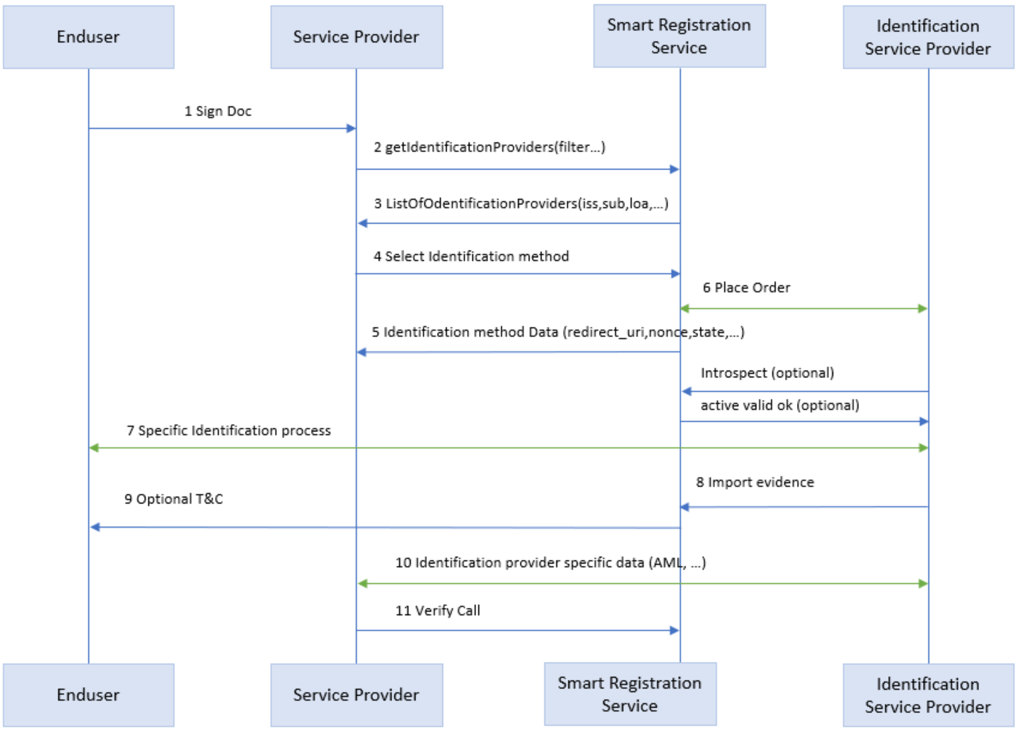
The API description is available on the Swagger platform on Swisscom Wiki.
https://miss-backend-api-preprod.scapp.swisscom.com/swagger/index.html

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


Enduser
Service Provider
Smart Registration Service
Identification Service Provider
1 Sign Doc
2 getIdentificationProviders(filter...)
3 ListOfOdentificationProviders(iss,sub,loa,...)
4 Select Identification method
6 Place Order
5 Identification method Data (redirect_uri,nonce,state,...)
Introspect (optional)
active valid ok (optional)
7 Specific Identification process
8 Import evidence
9 Optional T&C
10 Identification provider specific data (AML, ...)
11 Verify Call
Enduser
Service Provider
Smart Registration Service
Identification Service Provider

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 IPSP (Identification Service Provider on the diagram) 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 IPSP.

(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

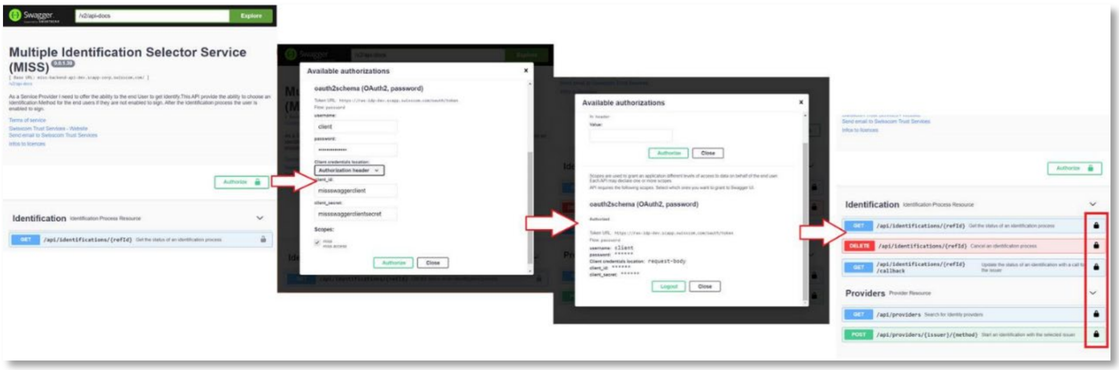
The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

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)

Client Id: "missswaggerclient"
Client secret: "missswaggerclientsecret"


Swagger
/v2/api-docs
Explore
Multiple Identification Selector Service (MISS)
Terms of service
Swisscom Trust Services - Website
Send email to Swisscom Trust Services
Infos to licences
Authorize
Identification Identification Process Resource
GET /api/identifications/{refId} Get the status of an identification process
Available authorizations
oauth2schema (OAuth2, password)
username:
client
password:
Client credentials location:
Authorization header
client_id:
missswaggerclient
client_secret:
missswaggerclientsecret
Scopes:
Authorize
Close
Logout
DELETE /api/identifications/{refId} Cancel an identification process
GET /api/identifications/{refId}/callback Update the status of an identification with a call to the issuer
Providers Provider Resource
GET /api/providers Search for identity providers
POST /api/providers/{issuer}/{method} Start an identification with the selected issuer

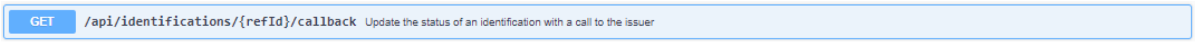
The identification process can be mocked to facilitate testing. In the testing process the SP can simulate the status of the identification. In addition, the SP can enter its own testing data and then test the end-to-end process.

To trigger a mocked Identification, the request must be done with:

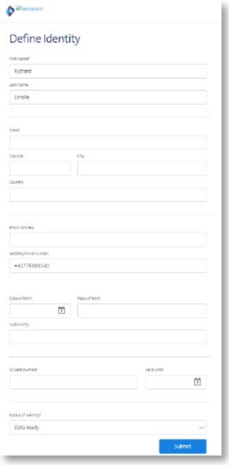
- **Issuer**="Test"
- **Method**="Video"

Store the Reference ID for further use.
After redirecting to the target URL, a form can be filled out to mock the result for the desired use case.

- Status can be set according testcase (see example below for a successful video identification)
- **Important**: use the **call back** method with the reference ID to update the status (only for test)

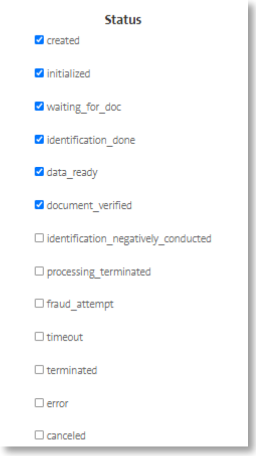

GET /api/identifications/{refId}/callback Update the status of an identification with a call to the issuer

- After the evidence is created the status "Terminated " can be checked with the method "get status"
- After this step a Verify call or a lookup call can be done to check the successful end-to-end process


Define Identity

First Name*: Richard
Last Name: Sinelle
Street:
zipcode:
city:
Country:
E-mail address:
Mobile phone number: +41775388140
Date of birth:
Place of birth:
Nationality:
ID Card number:
valid until:
Status of identity*: Data ready

Submit


Status

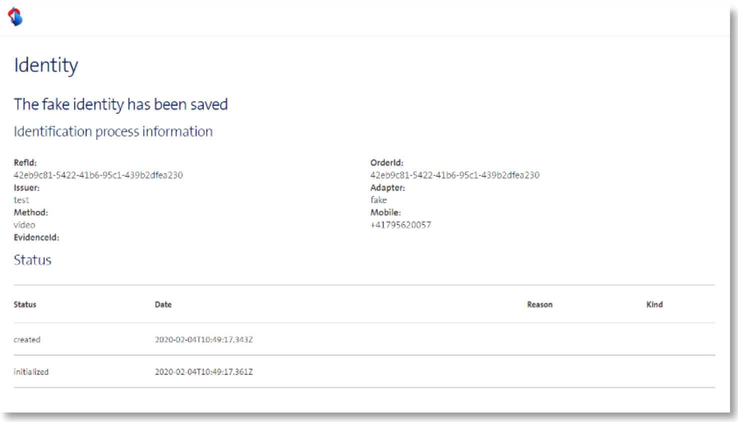
☑ created
☑ initialized
☑ waiting_for_doc
☑ identification_done
☑ data_ready
☑ document_verified
☐ identification_negatively_conducted
☐ processing_terminated
☐ fraud_attempt
☐ timeout
☐ terminated
☐ error
☐ canceled

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

List of possible status: (The status should apply for all methods - see also Appendix for specific status handling for each method)

Status	Semantic	Recommended action
Created	The identification data is collected and stored in order to initialize an order with the IPSP	Retrieve the target URL, store the Ref ID and specific IPSP ID (order ID, ident ID, Case ID….) for support purpose
Initialized	The identification task has been ordered by the IPSP. The identification task can now be started by the Service Provider using the target URL.	User starts identification with the target URL
Identification done	Identification process has been finished; evidence is in preparation	
Data ready	The data is ready on IPSP 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.	For all methods except SRS Selfie Ident, start polling with a lookup call till user has accepted T&C. For SRS Selfie Ident user can already sign if this status is reached
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 IPSP (not mandatory)	Restart a new process from the beginning with a new target URL
Negatively conducted	This Status is returned for SRS Video EU or SRS eID DE or SRS Selfie Ident EU if the Identification was unsuccessful for some reason (not a valid or expired document used, rejected by the back-office Agent user stopped before accepting the T&C in the app for SRS Selfie Ident)	Check the reason and restart a new process from the beginning with a new target URL
Timeout	The identification method was not finished or used in the defined Timeframe.	Restart a new process from the beginning with a new target URL
Canceled	User cancelled the identification process	Restart a new process from the beginning with a new target URL



Identity

The fake identity has been saved

Identification process information

RefId: 42eb9c81-5422-41b6-95c1-439b2dfea230

Issuer: test

Method: video

EvidenceId:

OrderId: 42eb9c81-5422-41b6-95c1-439b2dfea230

Adapter: fake

Mobile: +41795620057

Status

Status	Date	Reason	Kind
created	2020-02-04T10:49:17.343Z		
initialized	2020-02-04T10:49:17.361Z		

5 Recommended Integration – Best Practice

5.1 Verify Call – Lookup Call

The verify call should be used by the integration partner before and/or after any identification process to be able to guide a user correctly through an end-to-end process.
If successful, the semantic of the Verify call is the confirmation that for a specified mobile number and its attached parameter a valid evidence exist, and user should be able to sign if the user did not reset his authentication method since the identification process*.
The verify call is interesting for matching purpose.
Online documentation for the verify call: https://rasp.scapp.swisscom.com/swagger/index.html

(*) for example, password change if user uses the Password/OTP authentication or Mobile ID reset or reactivation without recovery code.

The lookup call is easier to use as no personal data (DN) is needed and will be sufficient for most use cases.
The Semantic of the Lookup call is the same as for Verify call.
Online documentation fort the lookup call: https://rasp.scapp.swisscom.com/swagger/index.html
Note: if the evidence will "expire" within 90 days, this information will also be available in the response. This is useful to inform the user of the need of a new identification

5.2 Status tracking end-to-end and method selection

It is recommended to track the status through the SRS API along the identification process. After the Identification process is done (in general Status "Terminated" or "Timeout" or "negatively conducted" is reached). Then it is recommended to poll the status for T&C acceptance* with a verify call or lookup call depending on your use case to guide the end user.

> "*Serial Mismatch*": even if the tracking of the identification status and T&C status is done properly, this error can happen in the final signature process in some cases. Please refer to the integration guide of the signing service for more details about this error that should be handled in the user flow by the Service Provider. The user needs to get identified again if this error occurs.

SRS offers the possibility to choose the right method depending the use case. SRS does not provide any backup logic to send the send user automatically to an alternative method if one method is not successful. But SRS provides through the correct tracking of the different status the possibility for the Service Provider to choose an alternative method at any time.
Example: User started the SRS-Bank identification, but the process could not be achieved for some reason, then the user can be redirected to SRS-Video or SRS-eID to be able to try another way.

Note: The creation of a target URL is never Billed. Swisscom will only bill the successful identifications.
(*) this is not needed for the robo-ident method

6 Additional Features of the SRS

6.1 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 IPSP	When this parameter is set then the response will only contain identification methods from this specific IPSP. 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
Web flow	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
- "**Bank**": method is based on bank identification
- "**Robo-ident**": method is based on a selfie and liveness check
- "**Autoident**": method based on a selfie and liveness check, with additional back-office check

This list will be updated regularly.

6.2 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.
(Note: This ID was named in the previous versions Customer ID)

6.3 Silent SMS

The Silent SMS Feature is a very useful feature for customer using the Smart Flows component. See also the integration guide for Smart Flows (Link)
To activate the Silent SMS mode the "disabledSmsAlerts" field must be set to "True" in the place order request.
Once set, the IPSP will transfer this information to Swisscom when the import is done, and no SMS will be sent out for the acceptance of the Terms & Conditions.

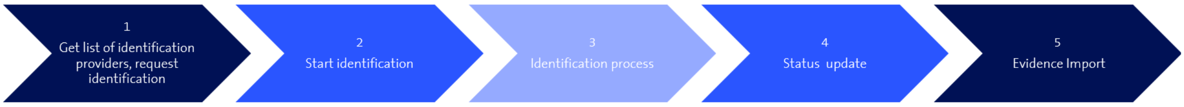
- **Attention**: please use this feature carefully, and only if you plan to get the Terms & Condition accepted through the Smart Flows process. Otherwise the user will not be able to finish the registration and the identification even if successful will be lost

- **Note**: please be aware that the life cycle SMS and potentially the Terms and Condition renewal will be sent out.

7 Support

7.1 Overview

The whole identification process involves 3 parties: Swisscom, the service provider who wants to get a user enabled for the signature and the IPSP.
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).

7.2 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	Successful	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)

The information in this document is of a non-binding nature and is subject to change.

8 Appendix – Identification Methods catalogue and specification

8.1 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 evidence 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 IPSP’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.

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

8.2 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 (see also Language below) 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 gets SMS with link to the T&C of Swisscon. After T&C are accepted, user can sign. Please note the special requirements that people to be identified can use the proprietary identity.tm app below.

- Language: a language parameter can be set in the request to be led to an Agent speaking this language (Croatian "HR", French "FR", Spanish "ES"). Please be aware that the front end takes the language of the browser of the user agent. From beginning of September 2021, the additional language mentioned above will be available on a best effort basis.
- Method filter specification

Filter Parameter	Value	Value
Issuer	IDENTITY.TM	IDENTITY.TM
Jurisdiction	EIDAS	ZERTES
LOA	4	3 (since 2nd Oct. 2020)
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.

  - **Attention:** Mobile Number update - please be aware that in some case the user asks to change his mobile number within the Identification process. This is possible but, in this case, you must be aware that the number you potentially stored on SP side is wrong. Please inform the user to inform you in case of change.

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) and 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….).
  - Attention: do not provide titles in the surname field. Special characters or punctuation (".""," etc.) will also lead to an error that will end in a negatively conducted identification.
- 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

- **Domains to be whitelisted (User will be redirected to our identification partner)**

	Description
Identity.tm	Main domain for the video identification
Example of target URL	https://www.identity.tm/status/649C6099931C4BBE2B34

- **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

The information in this document is of a non-binding nature and is subject to change.

- 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

- **Miscellaneous**

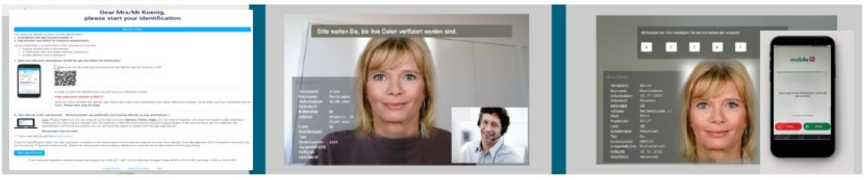
Generally, for better conversion, we recommend end-user to use the mobile App of identity or a **mobile browser** directly on the smartphone if user wants to use a web browser.
We also recommend using preferably a **Mobile Network** and avoid in general company WLAN.

- **Service Times**

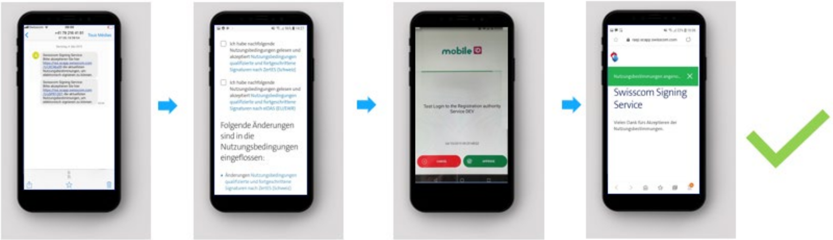
  The service times is displayed on the start page. Please check especially the service times for specific languages.

- **Screenshots**

- The Video identification is done with our partner identity.TM


Dear Mrs/Mr Koenig,
please start your identification
Bitte warten Sie, bis Ihre Daten verifiziert worden sind.
mobile

- After the identification the user gets a SMS to accept T&C


Folgende Änderungen sind in die Nutzungsbedingungen eingeflossen:
mobile
Swisscom Signing Service

Swisscom Trust Services

8.3 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	Bank
Web flow	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

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

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.

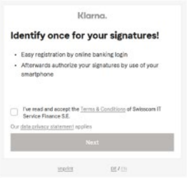
After the identification process is terminated, we recommend starting with Verify Call after a delay of **30 Seconds to 2 minutes**. After the verify call is successful, the user is correctly registered and can sign.

- **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**.

- **Note**: The Target URL contains additionally a Token so the length of the target URL will contain around 700 Characters. Typical Format: https://ident.playgroud.klarna.com/SESSION_ID?access_token=ey*******
  We recommend not to limit the target URL and not to encode it in the further process.

- **Screenshots**



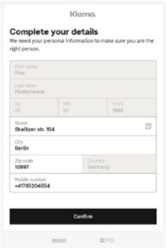
Klarna.

Identify once for your signatures!

- Easy registration by online banking login
- Afterwards authorize your signatures by use of your smartphone

□ I've read and accept the Terms & Conditions of Swisscom IT Service Finance S.E.

Our data privacy statement applies

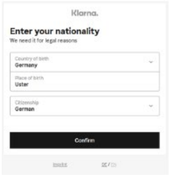


Klarna.

Complete your details

We need your personal information to make sure you are the right person.

First name: Max
Last name: Mustermann
DD: 01
MM: 01
YYYY: 1986
Street: Skalitzer str. 104
City: Berlin
Zip code: 10997
Country: Germany
Mobile number: +41765204554

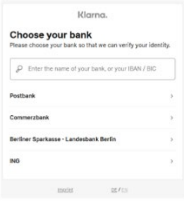


Klarna.

Enter your nationality

We need it for legal reasons

Country of birth: Germany
Place of birth: Uster
Citizenship: German



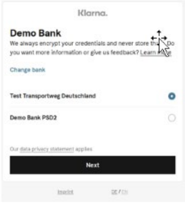
Klarna.

Choose your bank

Please choose your bank so that we can verify your identity.

Enter the name of your bank, or your IBAN / BIC

Postbank ›
Commerzbank ›
Berliner Sparkasse - Landesbank Berlin ›
ING ›



Klarna.

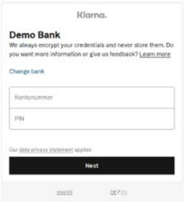
Demo Bank

We always encrypt your credentials and never store them. Do you want more information or give us feedback? Learn more

Change bank

Test Transportweg Deutschland ●
Demo Bank PSD2 ○

Our data privacy statement applies



Klarna.

Demo Bank

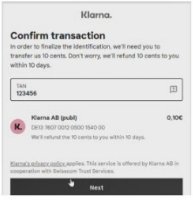
We always encrypt your credentials and never store them. Do you want more information or give us feedback? Learn more

Change bank

Kontonummer
PIN

Our data privacy statement applies

• • •



Klarna.

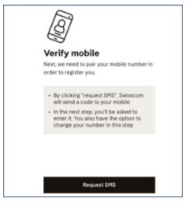
Confirm transaction

In order to finalize the identification, we'll need you to transfer us 10 cents. Don't worry, we'll refund 10 cents to you within 10 days.

TAN: 123456

Klarna AB (publ) 0,10€
DE13 7607 0012 0500 1540 00
We'll refund the 10 cents to you within 10 days.

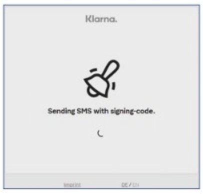
Klarna's privacy policy applies. This service is offered by Klarna AB in cooperation with Swisscom Trust Services.



Verify mobile

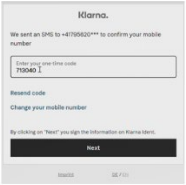
Next, we need to pair your mobile number in order to register you.

- By clicking "request SMS", Swisscom will send a code to your mobile
- In the next step, you'll be asked to enter it. You also have the option to change your number in this step



Klarna.

Sending SMS with signing-code.

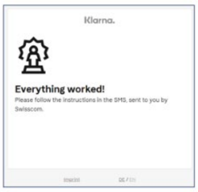


Klarna.

We sent an SMS to +41795620*** to confirm your mobile number

Enter your one-time code: 713040

By clicking on "Next" you sign the information on Klarna Ident.



Klarna.

Everything worked!

Please follow the instructions in the SMS, sent to you by Swisscom.

8.4 Appendix 3 –Identification with nPA (eID) by Identity.tm

• Identification method name:	**identity-tm-eid**
• Identification Service Provider:	Identity.tm
• Signature capability for User Identified with this method:	QES (AES)/eIDAS, AES/ZertES
➢ Validity of the evidence:	5 years (or ID expiration date)
➢ Language possible for the process	German, English
➢ List of supported countries/documents	according eIDAS Regulation

- User Flow

  User starts identification – User chooses desktop process or identity.TM App.

- Identity.TM App: user follows the steps in the app, enters his PIN* for the eID process, user confirms his mobile number by entering a TAN
- Desktop version: user is asked first to verify his mobile number by entering a TAN. User starts the official Ausweiss-App2 and follows the steps. User confirms the identification with his PIN*

(*) The PIN is a code set by the user and known only by him to access the data on the nPA chip. This is done separately by the user typically when he receives the nPA from the official office of "Bundesrepublik Deutschland". To do so, the user gets a document containing a unique so called "Transport PIN" to activate the eID function of his nPA. Note that if the user didn't do this before then he will have the possibility to do it within the identity.TM app flow.

- Method filter specification

Filter Parameter	**Value**	**Value**
Issuer	Identity-tm-eid	Identity-tm-eid
Method Name	eID (case sensitive)	eID
Jurisdiction	EIDAS	ZertEs
LOA	LOA4	LOA3
Offline	FALSE	FALSE
Method Type	eID	eID
Web flow	TRUE	TRUE
Realtime Method	TRUE	TRUE

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

List of initial Identity Data that are submitted

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

Attributes	
Firstname (Given Names)	Mandatory*
Lastname (Surname)	Mandatory*
Date of birth	Mandatory*
Mobile number	Mandatory*

Place of birth	Optional
Country	Optional
Email address	Optional
Language	Optional
External ID	Optional

(*) This data must match with the personal data on the nPA

- specific identification method response Information

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

- **Recommended implementation**

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

If the status "Negatively conducted" is reached then there was a problem that didn't permit to confirm the identification (typically, wrong name or surname, fraud attempt, mobile number not verified etc...)

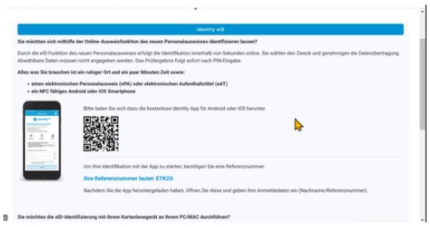
After the identification process is terminated, we recommend starting with Verify Call or lookup call after a delay of **30 Seconds to 2 minutes**. After the verify call is successful, the user is correctly registered and can sign.

For the browser version, we recommend following the same recommendations as for the video identification process by identity.TM (see § Appendix 1)

- **Connection lost during the Process**

If the connection is lost during the process or something goes wrong the target URL can be used again as long as the identification was not flagged "negatively conducted"

- **Screenshots**



Sie möchten sich mithilfe der Online-Ausweisfunktion des neuen Personalausweises identifizieren lassen?

Durch die eID-Funktion des neuen Personalausweises erfolgt die Identifikation innerhalb von Sekunden online. Sie wählen den Zweck und genehmigen die Datenübertragung. Abwählbare Daten müssen nicht angegeben werden. Das Prüfergebnis folgt sofort nach PIN-Eingabe.

Alles was Sie brauchen ist ein ruhiger Ort und ein paar Minuten Zeit sowie:

- **einen elektronischen Personalausweis (nPA) oder elektronischen Aufenthaltstitel (eAT)**
- **ein NFC fähiges Android oder iOS Smartphone**

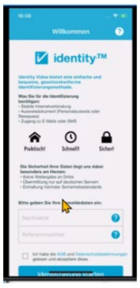
Bitte laden Sie sich dazu die kostenlose identity App für Android oder iOS herunter

Um Ihre Identifikation mit der App zu starten, benötigen Sie eine Referenznummer.

Ihre Referenznummer lautet: ETK2G

Nachdem Sie die App heruntergeladen haben, öffnen Sie diese und geben Ihre Anmeldedaten ein (Nachname/Referenznummer).

Sie möchten die eID-Identifizierung mit Ihrem Kartenlesegerät an Ihrem PC/MAC durchführen?



identity Video bietet eine einfache und bequeme, gesetzeskonforme Identifizierungsmethode.

Was Sie für die Identifizierung benötigen:
• Stabile Internetverbindung
• Ausweisdokument (Personalausweis oder Reisepass)
• Zugang zu E-Mails oder SMS

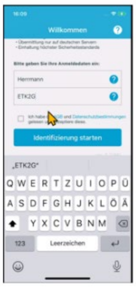
Die Sicherheit Ihrer Daten liegt uns dabei besonders am Herzen:
• Keine Weitergabe an Dritte
• Übermittlung nur auf deutschen Servern
• Einhaltung höchster Sicherheitsstandards

Bitte geben Sie Ihre Anmeldedaten ein:

Nachname

Referenznummer

□ Ich habe die AGB und Datenschutzbestimmungen gelesen und akzeptiere diese.



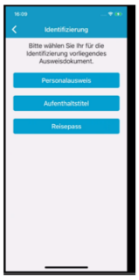
• Übermittlung nur auf deutschen Servern
• Einhaltung höchster Sicherheitsstandards

Bitte geben Sie Ihre Anmeldedaten ein:

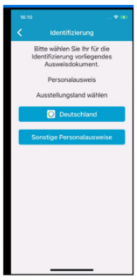
Herrmann

ETK2G

□ Ich habe die AGB und Datenschutzbestimmungen gelesen und akzeptiere diese.



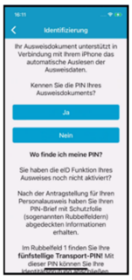
Bitte wählen Sie Ihr für die Identifizierung vorliegendes Ausweisdokument.



Bitte wählen Sie Ihr für die Identifizierung vorliegendes Ausweisdokument.

Personalausweis

Ausstellungsland wählen



Ihr Ausweisdokument unterstützt in Verbindung mit Ihrem iPhone das automatische Auslesen der Ausweisdaten.

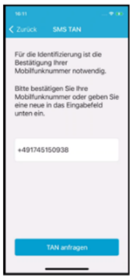
Kennen Sie die PIN Ihres Ausweisdokuments?

Wo finde ich meine PIN?

Sie haben die eID Funktion Ihres Ausweises noch nicht aktiviert?

Nach der Antragstellung für Ihren Personalausweis haben Sie Ihren PIN-Brief mit Schutzfolie (sogenannten Rubbelfeldern) abgedeckten Informationen erhalten.

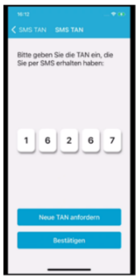
Im Rubbelfeld 1 finden Sie Ihre **fünfstellige Transport-PIN!** Mit dieser PIN können Sie Ihre Identitätsprüfung abschließen



Für die Identifizierung ist die Bestätigung Ihrer Mobilfunknummer notwendig.

Bitte bestätigen Sie Ihre Mobilfunknummer oder geben Sie eine neue in das Eingabefeld unten ein.

+491745150938

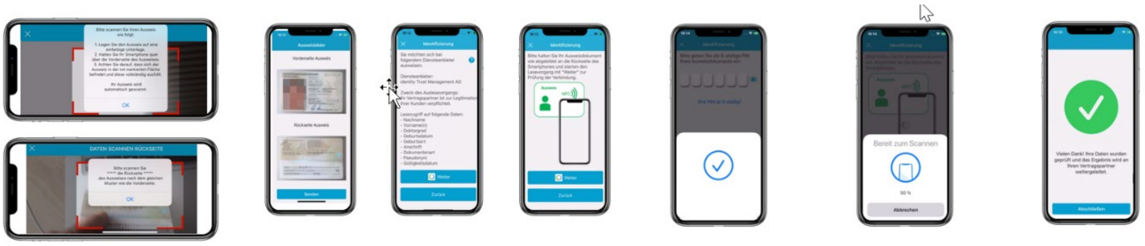


Bitte geben Sie die TAN ein, die Sie per SMS erhalten haben:

1 6 2 6 7

The information in this document is of a non-binding nature
and is subject to change.

Swisscom Trust Services



Bitte scannen Sie Ihren Ausweis wie folgt:

1. Legen Sie den Ausweis auf eine einfarbige Unterlage.
2. Halten Sie Ihr Smartphone quer über die Vorderseite des Ausweises.
3. Achten Sie darauf, dass sich der Ausweis in der rot markierten Fläche befindet und diese vollständig ausfüllt.

Ihr Ausweis wird automatisch gescannt.

OK

DATEN SCANNEN RÜCKSEITE

Bitte scannen Sie ***** die Rückseite ***** des Ausweises nach dem gleichen Muster wie die Vorderseite.

OK

Ausweisbilder

Vorderseite Ausweis

Rückseite Ausweis

Senden

Identifizierung

Sie möchten sich bei folgendem Diensteanbieter ausweisen:

Diensteanbieter: identity Trust Management AG

Zweck des Auslesevorgangs: Ihr Vertragspartner ist zur Legitimation Ihrer Kunden verpflichtet.

Lesezugriff auf folgende Daten:
- Nachname
- Vorname(n)
- Doktorgrad
- Geburtsdatum
- Geburtsort
- Anschrift
- Dokumentenart
- Pseudonym
- Gültigkeitsdatum

Weiter

Zurück

Identifizierung

Bitte halten Sie Ihr Ausweisdokument wie abgebildet an die Rückseite des Smartphones und starten den Lesevorgang mit "Weiter" zur Prüfung der Verbindung.

Weiter

Zurück

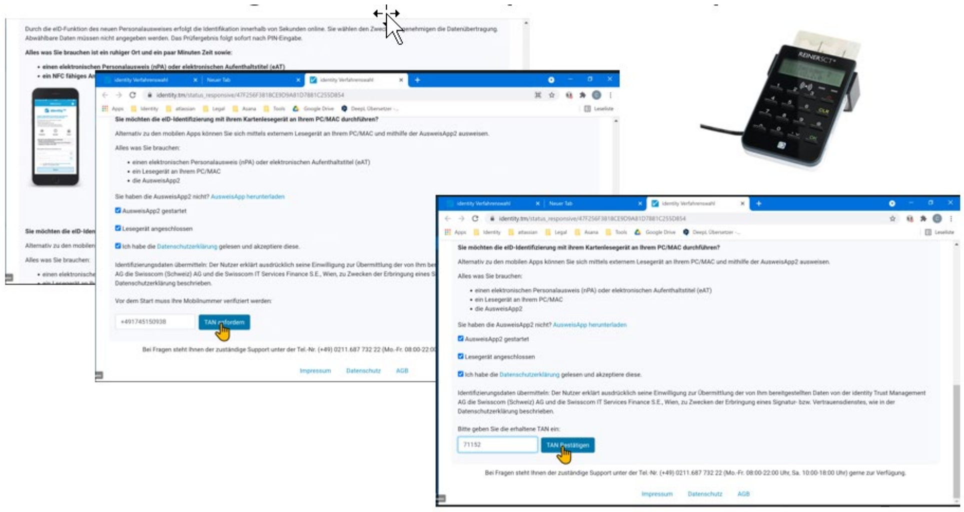
Bereit zum Scannen

50 %

Abbrechen

Vielen Dank! Ihre Daten wurden geprüft und das Ergebnis wird an Ihren Vertragspartner weitergeleitet.

Abschließen



Durch die eID-Funktion des neuen Personalausweises erfolgt die Identifikation innerhalb von Sekunden online. Sie wählen den Zwec[…] genehmigen die Datenübertragung. Abwählbare Daten müssen nicht angegeben werden. Das Prüfergebnis folgt sofort nach PIN-Eingabe.

Alles was Sie brauchen ist ein ruhiger Ort und ein paar Minuten Zeit sowie:

- **einen elektronischen Personalausweis (nPA) oder elektronischen Aufenthaltstitel (eAT)**
- **ein NFC fähiges An**

identity Verfahrenswahl | Neuer Tab | identity Verfahrenswahl

identity.tm/status_responsive/47F256F3818CE9D9A81D7881C255D854

Sie möchten die eID-Identifizierung mit Ihrem Kartenlesegerät an Ihrem PC/MAC durchführen?

Alternativ zu den mobilen Apps können Sie sich mittels externem Lesegerät an Ihrem PC/MAC und mithilfe der AusweisApp2 ausweisen.

Alles was Sie brauchen:

- einen elektronischen Personalausweis (nPA) oder elektronischen Aufenthaltstitel (eAT)
- ein Lesegerät an Ihrem PC/MAC
- die AusweisApp2

Sie haben die AusweisApp2 nicht? AusweisApp herunterladen

☑ AusweisApp2 gestartet

☑ Lesegerät angeschlossen

☑ Ich habe die Datenschutzerklärung gelesen und akzeptiere diese.

Identifizierungsdaten übermitteln: Der Nutzer erklärt ausdrücklich seine Einwilligung zur Übermittlung der von Ihm bereitgestellten Daten von der identity Trust Management AG die Swisscom (Schweiz) AG und die Swisscom IT Services Finance S.E., Wien, zu Zwecken der Erbringung eines Signatur- bzw. Vertrauensdienstes, wie in der Datenschutzerklärung beschrieben.

Vor dem Start muss Ihre Mobilnummer verifiziert werden:

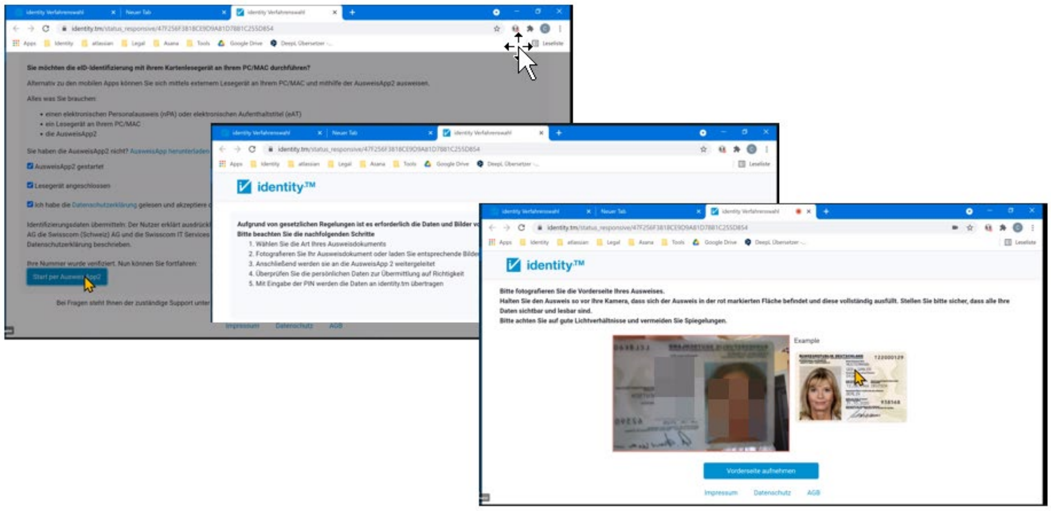
+491745150938 | TAN anfordern

Bitte geben Sie die erhaltene TAN ein:

71152 | TAN bestätigen

Bei Fragen steht Ihnen der zuständige Support unter der Tel.-Nr. (+49) 0211.687 732 22 (Mo.-Fr. 08:00-22:00 Uhr, Sa. 10:00-18:00 Uhr) gerne zur Verfügung.

Impressum Datenschutz AGB



Ihre Nummer wurde verifiziert. Nun können Sie fortfahren:

Start per AusweisApp2

Aufgrund von gesetzlichen Regelungen ist es erforderlich die Daten und Bilder v[…]
Bitte beachten Sie die nachfolgenden Schritte

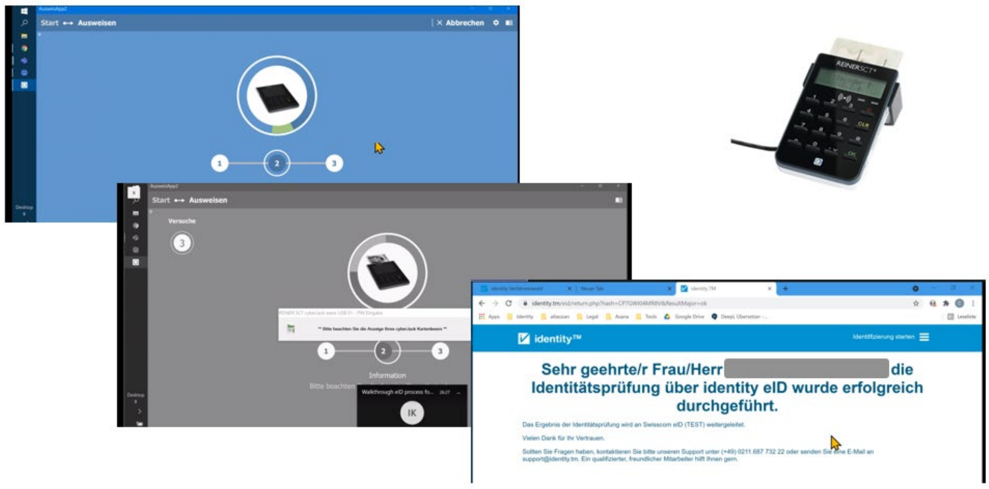
1. Wählen Sie die Art Ihres Ausweisdokuments
2. Fotografieren Sie Ihr Ausweisdokument oder laden Sie entsprechende Bilder
3. Anschließend werden sie an die AusweisApp 2 weitergeleitet
4. Überprüfen Sie die persönlichen Daten zur Übermittlung auf Richtigkeit
5. Mit Eingabe der PIN werden die Daten an identity.tm übertragen

Bitte fotografieren Sie die Vorderseite Ihres Ausweises.
Halten Sie den Ausweis so vor Ihre Kamera, dass sich der Ausweis in der rot markierten Fläche befindet und diese vollständig ausfüllt. Stellen Sie bitte sicher, dass alle Ihre Daten sichtbar und lesbar sind.
Bitte achten Sie auf gute Lichtverhältnisse und vermeiden Sie Spiegelungen.

Example

Vorderseite aufnehmen

Impressum Datenschutz AGB



AusweisApp2

Start ⟷ Ausweisen | ✕ Abbrechen

Versuche 3

** Bitte beachten Sie die Anzeige Ihres cyberJack Kartenlesers **

Information

identity.tm/eid/return.php?hash=CP7GW04MR8V&ResultMajor=ok

identity™ | Identifizierung starten

Sehr geehrte/r Frau/Herr [redacted] die Identitätsprüfung über identity eID wurde erfolgreich durchgeführt.

Das Ergebnis der Identitätsprüfung wird an Swisscom eID (TEST) weitergeleitet.

Vielen Dank für Ihr Vertrauen.

Sollten Sie Fragen haben, kontaktieren Sie bitte unseren Support unter (+49) 0211.687 732 22 oder senden Sie eine E-Mail an support@identity.tm. Ein qualifizierter, freundlicher Mitarbeiter hilft Ihnen gern.

8.5 Appendix 4 –Identification with Robo-Ident (SRS-Selfie-Ident) by Nect

- Identification method name: robo-ident
- Identification Service Provider: nect
- Signature capability for User Identified with this method: QES (AES)/eIDAS, AES/ZertES
    - ➢ Validity of the evidence: 2 years (or ID expiration date)
    - ➢ Language possible for the process German, English
    - ➢ List of supported countries/documents ICAO compliant Passports, German ID

- User Flow (check out the explanation video: LINK

  User starts identification with a target URL and open the page with the QR Code – User downloads and installs the Nect app (mandatory) and scans the QR Code with the Nect App.

- Nect App: user follows the steps in the app, scans his ID document, takes a selfie, and is asked to pronounce some random words appearing on the screen.
- After these steps the data is analyzed, and the result is displayed.
- In some cases, the user must repeat the pronunciation of new random words.

- Method filter specification

Filter Parameter	Value	Value
Issuer	nect	nect
Method Name	robo-ident	robo-ident
Jurisdiction	EIDAS	ZertES
LOA	LOA4	LOA3
Offline	FALSE	FALSE
Method Type	Robo-ident	Robo-ident
Web flow	TRUE	TRUE
Realtime Method	TRUE	TRUE

- Initial Information: no initial data is needed while triggering the identification method: We recommend providing an empty payload as no matching is done by this method.

Attributes	
Firstname (Given Names)	Optional
Lastname (Surname)	Optional
Date of birth	Optional
Mobile number	Optional

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

Place of birth	Optional
Country	Optional
Email address	Optional
Language	Optional
External ID	Optional

- Specific identification method response Information

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

- **Recommended implementation**

The Identification is finished and successful when status **"Terminated"** is reached.

If the status **"error"** is reached with the reason **"Timeout"** then the target URL cannot be used anymore, and the process is finished. This happens after **30 days** if Target URL was not used or **60 minutes** if the process was started in the App and T&C were accepted.

After the user has passed the step of accepting the Terms and Conditions of Nect then the timeout occurs after **60 Minute** inactivity or unsuccessful identification. Overall, the user can retry **5 times with the same target URL**.

If status "error" is reached without reason, this means the Identification was unsuccessful for an unknown reason.

Attention: identification on production environment should only be done with real and valid documents. Wrong or faked documents or "Tests" on production could be flagged as Fraud suspicion and the mobile number could be blacklisted.

If the identification is flagged unsuccessful in the app, there was a problem that didn't permit to confirm the identification (typically, wrong name or surname, fraud attempt, mobile number not verified etc.)

After the identification process is "terminated", and the confirmation appeared in the Nect app the user should be able to sign only after accepting the T&C of Swisscom successfully. We recommend making a polling with a lookup call anyway to ensure that the T&C were accepted correctly.

Please note that there is no additional need to get an SMS for T&C for the user.

- **Connection lost or problems during the Process**

If the connection is lost during the process or something goes wrong the target URL can be used again as long as the identification was not flagged "negatively conducted" or "error" or "timeout".

- **Possible reason for unsuccessful identification**

Additionally to the Status error or negatively conducted, the reason is added to the status for support purpose. The reason describes the problem occurred and contains the information if user can start again or not.

> *Example*:
> "The user tried identifying with an unapproved document."
> "The case result is final, i.e. no further attempts are possible."

In this example the user tried identifying with a document that is not supported and the user cannot try again with the same target URL.

- **Miscellaneous**

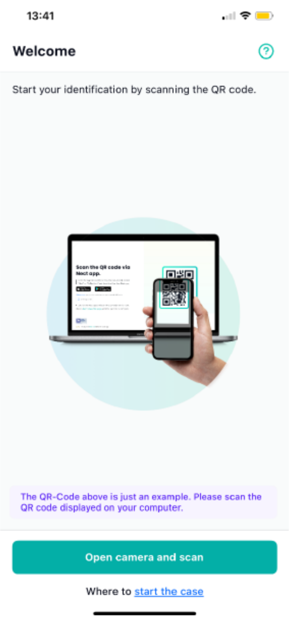
- The Target URL is available 30 Days (Status created and initialized)
- Once the process is started the Timeout is reached after 60 minutes

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

- The process of ID verification takes in general around 2 minutes but can take up to 6 Minutes in some cases depending on the quality of the photos, taken, light conditions etc. and if there is a manual check.
- The method does not provide a matching if initial data is provided and there are no check criteria at the initial step. All data gathered during the identification process are verified but not compared to the initial data.
- Support is offered by Nect via email within the app: user should not the **Case ID**

- **Screenshots**



13:41

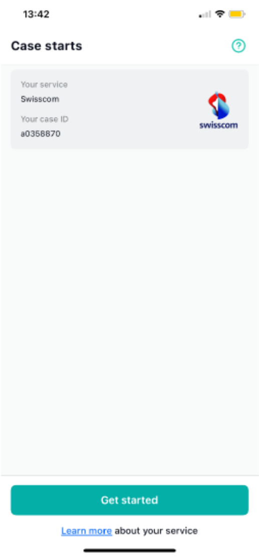
Welcome

Start your identification by scanning the QR code.

The QR-Code above is just an example. Please scan the QR code displayed on your computer.

Open camera and scan

Where to start the case



13:42

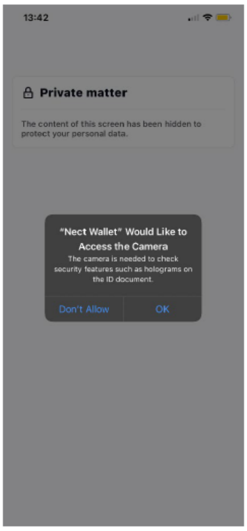
Case starts

Your service
Swisscom

Your case ID
a0358870

Get started

Learn more about your service



13:42

Private matter

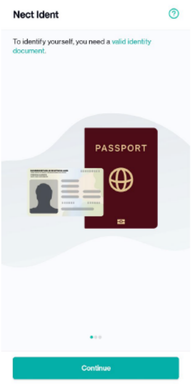
The content of this screen has been hidden to protect your personal data.

"Nect Wallet" Would Like to Access the Camera

The camera is needed to check security features such as holograms on the ID document.

Don't Allow | OK

User has to select "Get started" to start the identification process.

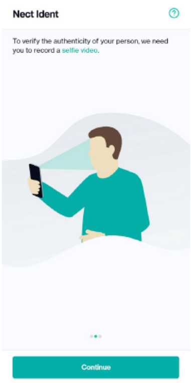


Nect Ident

To identify yourself, you need a valid identity document.

Continue

The user is informed that a valid identiy document is needed for the process. Please select 'Continue'.

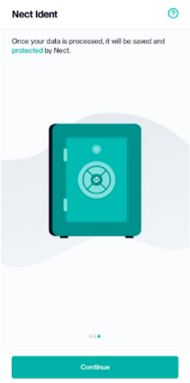


Nect Ident

To verify the authenticity of your person, we need you to record a selfie video.

Continue

The user is informed that a is taken during the process. Please select 'Continue'.

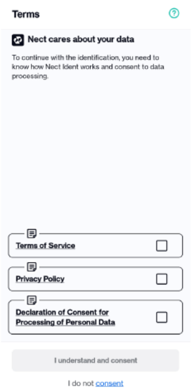


Nect Ident

Once your data is processed, it will be saved and protected by Nect.

Continue

The user is informed that the data is safely prossed by Nect. Please select 'Continue'.



Terms

Nect cares about your data

To continue with the identification, you need to know how Nect Ident works and consent to data processing.

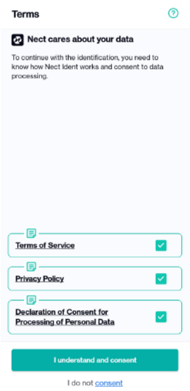
Terms of Service □

Privacy Policy □

Declaration of Consent for Processing of Personal Data □

I understand and consent

I do not consent



Terms

Nect cares about your data

To continue with the identification, you need to know how Nect Ident works and consent to data processing.

Terms of Service ☑

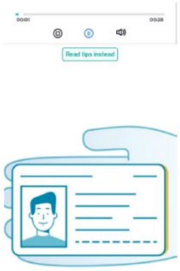
Privacy Policy ☑

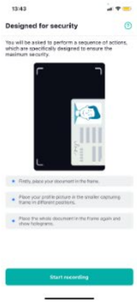
Declaration of Consent for Processing of Personal Data ☑

I understand and consent

I do not consent

Before the identification process begins, the user must agree to the General Terms of Service, the privacy policy, and the processing of his or her data. Please select 'I understand and consent'.

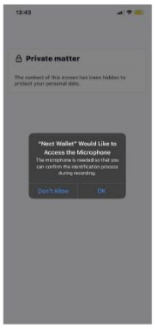



13:43

Designed for security

You will be asked to perform a sequence of actions, which are specifically designed to ensure the maximum security.

- Firstly, place your document in the frame.
- Place your profile picture in the smaller capturing frame in different positions.
- Place the whole document in the frame again and show holograms.

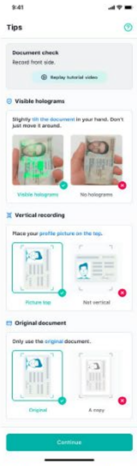

13:43

Private matter

The content of this screen has been hidden to protect your personal data.

"Nect Wallet" Would Like to Access the Microphone

The microphone is needed so that you can confirm the identification process during recording.


9:41

Tips

Document check
Record front side.

Visible holograms

Slightly tilt the document in your hand. Don't just move it around.

Vertical recording

Place your profile picture on the top.

Original document

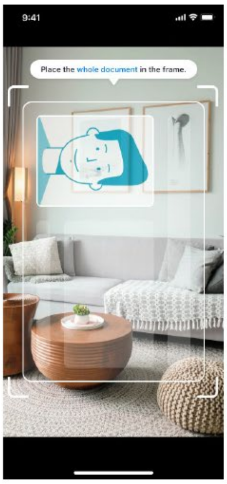
Only use the original document.

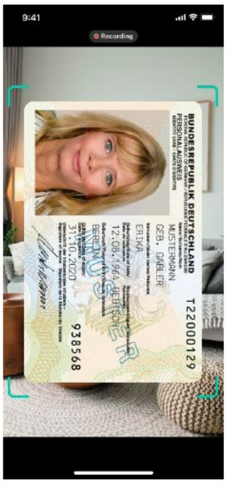
A video is played which visualizes the video taking of the ID front. Please make sure that:

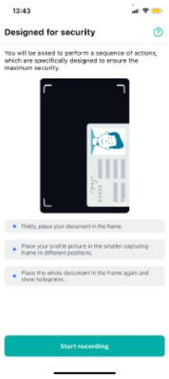
- You place your profile picture on the top
- Slightly tilt the document that you can see the holograms
- Good lightning conditions

Android specific: As the Nect Wallet app needs permission to take pictures, record video and record audio, please select 'While using the app'.

Tips are shown after the video. Please check them and if you are ready select 'Continue'.





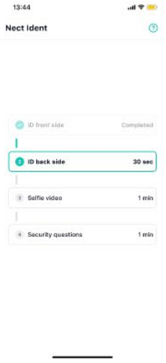

13:43

Designed for security

You will be asked to perform a sequence of actions, which are specifically designed to ensure the maximum security.

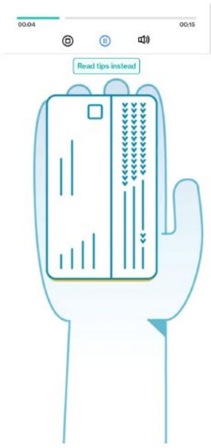
- Firstly, place your document in the frame.
- Place your profile picture in the smaller capturing frame in different positions.
- Place the whole document in the frame again and show holograms.

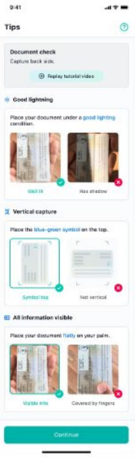
Recording of the front side starts automatically as soon as the ID document is held in the app's designated frame. By panning the document, holograms and other security features are made visible.


13:44

Nect Ident

ID front side	Completed
2 ID back side	30 sec
3 Selfie video	1 min
4 Security questions	1 min




9:41

Tips

Document check
Capture back side.

Good lightning

Place your document under a good lighting condition.

Vertical capture

Place the blue-green symbol on the top.

All information visible

Place your document flatly on your palm.

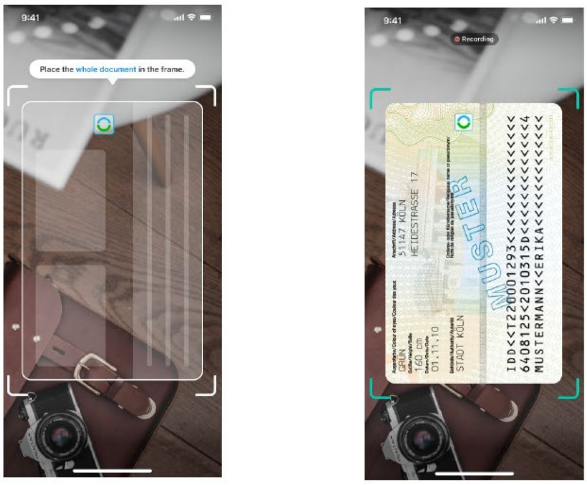
A photo of the back of the ID document is then taken. **If a passport is used for identification, no photo of the back is required.**

A video is played which visualizes the recording of the ID back side.

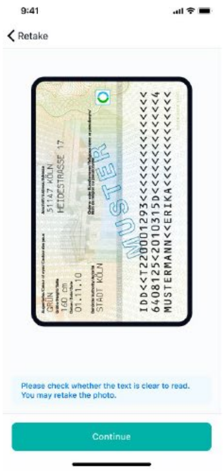
Please make sure that you have good lightning conditions, the ID card is placed correctly and all information is visible. Please select 'Continue'.

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

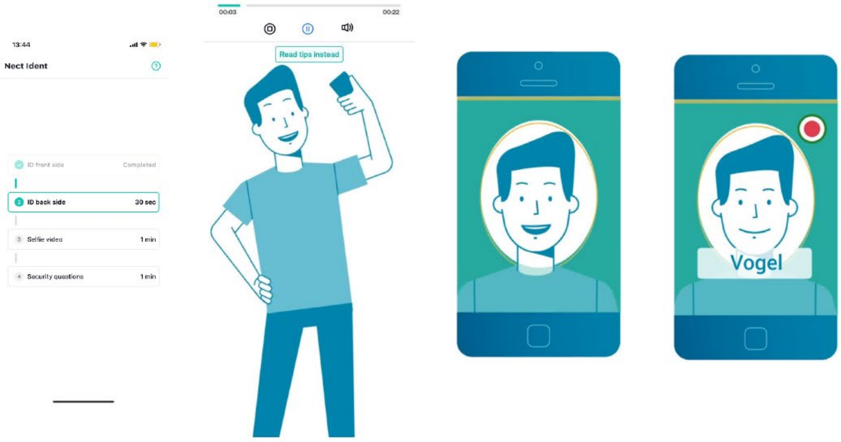


A photo of the back of the ID document is taken automatically.



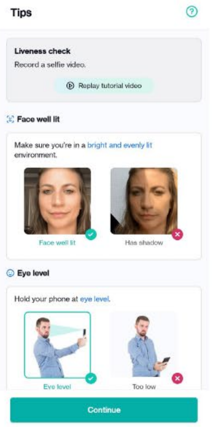
Please check whether the text is clear to read. You may retake the photo.

Please re-check the picture if the text is clear to read. If you have the option to re-take the picture or 'continue'.



- ID front side Completed
- 2 ID back side 30 sec
- 3 Selfie video 1 min
- 4 Security questions 1 min

The third step of the identification is the recording of a selfie video.


Tips

Liveness check
Record a selfie video.

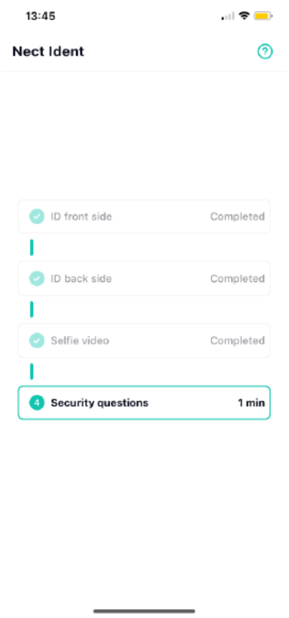
Face well lit

Make sure you're in a bright and evenly lit environment.

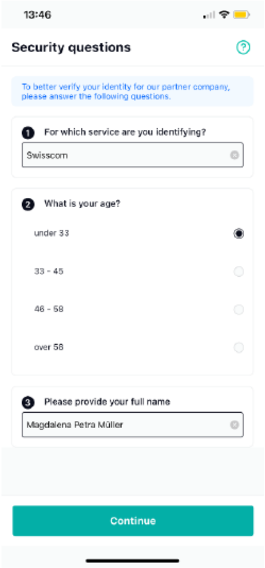
Eye level

Hold your phone at eye level.

Tips are shown after the video. Please check them and if you are ready select 'Continue'.



- ID front side Completed
- ID back side Completed
- Selfie video Completed
- 4 Security questions 1 min



Security questions

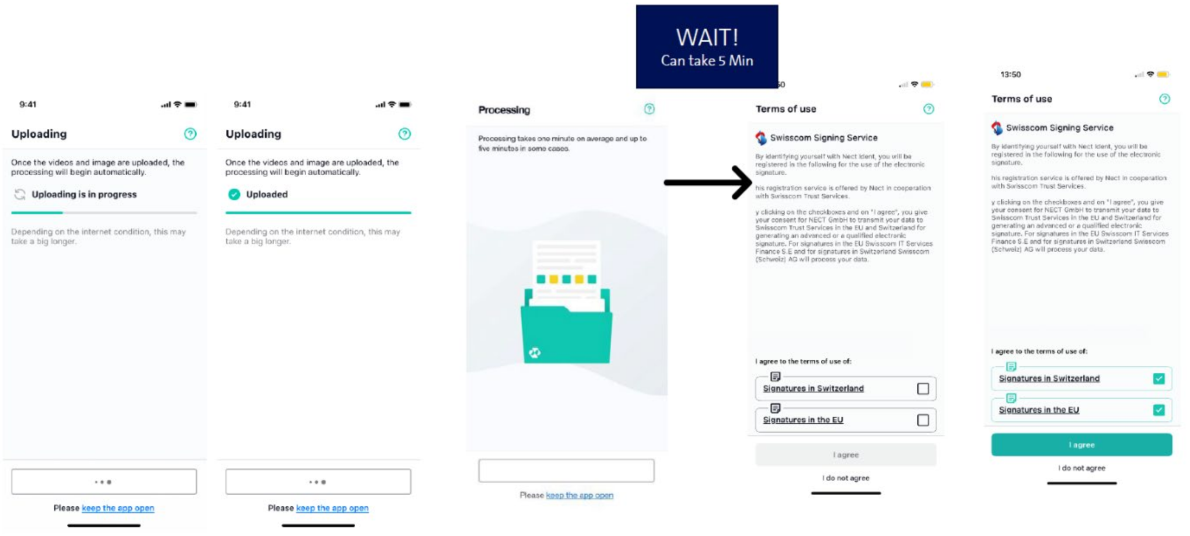
To better verify your identity for our partner company, please answer the following questions.

1 For which service are you identifying?
Swisscom

2 What is your age?
- under 33 ●
- 33 - 45 ○
- 46 - 58 ○
- over 58 ○

3 Please provide your full name
Magdalena Petra Müller

The information in this document is of a non-binding nature and is subject to change.


WAIT!
Can take 5 Min

Uploading

Once the videos and image are uploaded, the processing will begin automatically.

Uploading is in progress

Depending on the internet condition, this may take a big longer.

Please keep the app open

Uploading

Once the videos and image are uploaded, the processing will begin automatically.

✓ Uploaded

Depending on the internet condition, this may take a big longer.

Please keep the app open

Processing

Processing takes one minute on average and up to five minutes in some cases.

Please keep the app open

Terms of use

Swisscom Signing Service

By identifying yourself with Nect Ident, you will be registered in the following for the use of the electronic signature.

his registration service is offered by Nect in cooperation with Swisscom Trust Services.

y clicking on the checkboxes and on "I agree", you give your consent for NECT GmbH to transmit your data to Swisscom Trust Services in the EU and Switzerland for generating an advanced or a qualified electronic signature. For signatures in the EU Swisscom IT Services Finance S.E and for signatures in Switzerland Swisscom (Schweiz) AG will process your data.

I agree to the terms of use of:

Signatures in Switzerland □

Signatures in the EU □

I agree

I do not agree

Terms of use

Swisscom Signing Service

By identifying yourself with Nect Ident, you will be registered in the following for the use of the electronic signature.

his registration service is offered by Nect in cooperation with Swisscom Trust Services.

y clicking on the checkboxes and on "I agree", you give your consent for NECT GmbH to transmit your data to Swisscom Trust Services in the EU and Switzerland for generating an advanced or a qualified electronic signature. For signatures in the EU Swisscom IT Services Finance S.E and for signatures in Switzerland Swisscom (Schweiz) AG will process your data.

I agree to the terms of use of:

Signatures in Switzerland ☑

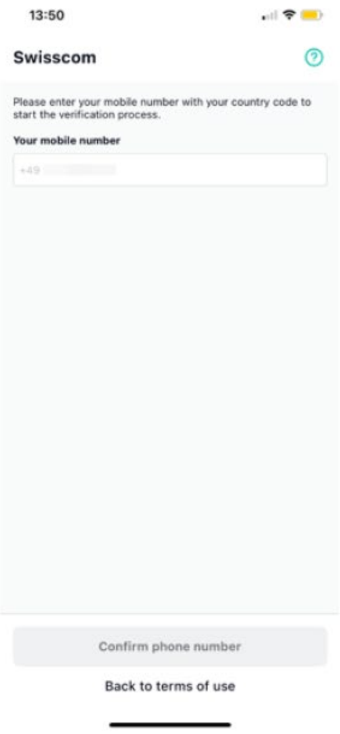
Signatures in the EU ☑

I agree

I do not agree

Swisscom Terms of use

The information in this document is of a non-binding nature and is subject to change.



13:50

Swisscom

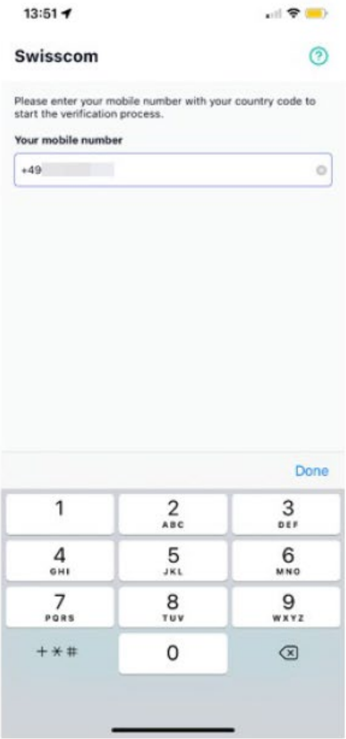
Please enter your mobile number with your country code to start the verification process.

Your mobile number

+49 [redacted]

Confirm phone number

Back to terms of use



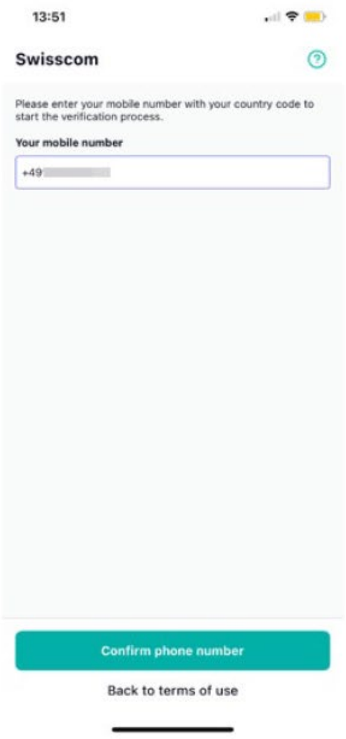
13:51

Swisscom

Please enter your mobile number with your country code to start the verification process.

Your mobile number

+49 [redacted]



13:51

Swisscom

Please enter your mobile number with your country code to start the verification process.

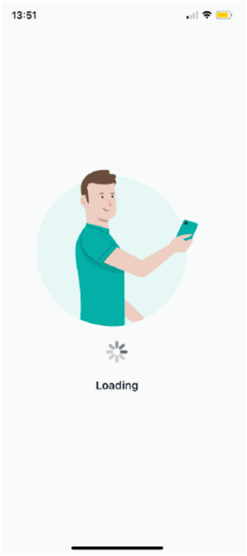
Your mobile number

+49 [redacted]

Confirm phone number

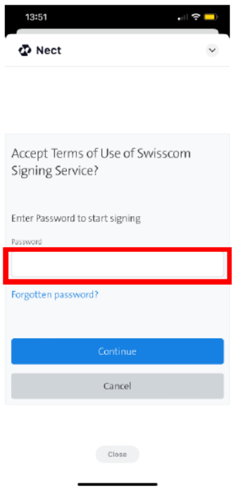
Back to terms of use

If user accepts T&C with Password and OTP:



13:51

Loading



13:51

Nect

Accept Terms of Use of Swisscom Signing Service?

Enter Password to start signing

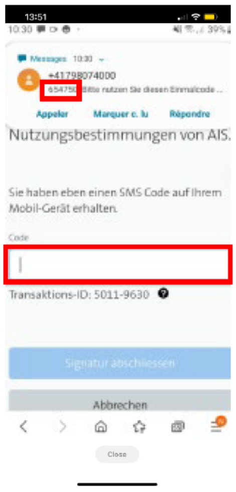
Password

Forgotten password?

Continue

Cancel

Close



13:51

10:30

Messages 10:30

+41798074000

654750 Bitte nutzen Sie diesen Einmalcode ...

Appeler Marquer c. lu Répondre

Nutzungsbestimmungen von AIS.

Sie haben eben einen SMS Code auf Ihrem Mobil-Gerät erhalten.

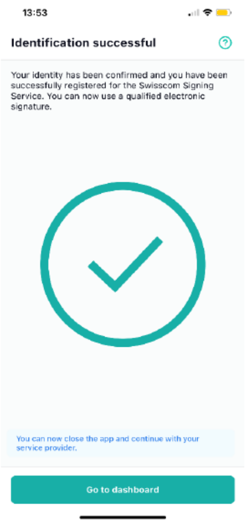
Code

Transaktions-ID: 5011-9630

Signatur abschliessen

Abbrechen

Close



13:53

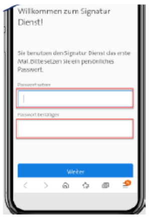
Identification successful

Your identity has been confirmed and you have been successfully registered for the Swisscom Signing Service. You can now use a qualified electronic signature.

You can now close the app and continue with your service provider.

Go to dashboard

Enter Password if not first registration, otherwise set password



Willkommen zum Signatur Dienst!

Sie benutzen den Signatur Dienst das erste Mal. Bittesetzen Sie ein persönliches Passwort.

Passwort setzen

Passwort bestätigen

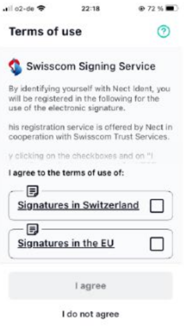
Weiter

Swisscom Trust Services

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

If user accepts T&C with Mobile ID APP:


Terms of use

Swisscom Signing Service

By identifying yourself with Nect Ident, you will be registered in the following for the use of the electronic signature.

his registration service is offered by Nect in cooperation with Swisscom Trust Services.

y clicking on the checkboxes and on "I

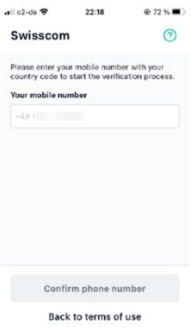
I agree to the terms of use of:

Signatures in Switzerland □

Signatures in the EU □

I agree

I do not agree


Swisscom

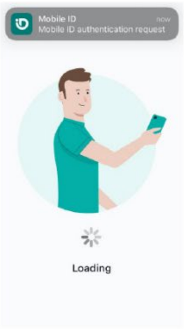
Please enter your mobile number with your country code to start the verification process.

Your mobile number

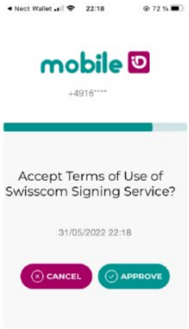
+49 1[redacted]

Confirm phone number

Back to terms of use


Mobile ID now
Mobile ID authentication request

Loading

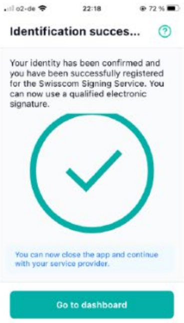

mobile ID

+4916****

Accept Terms of Use of Swisscom Signing Service?

31/05/2022 22:18

CANCEL APPROVE

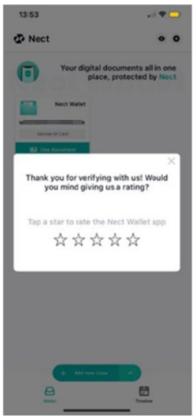

Identification succes...

Your identity has been confirmed and you have been successfully registered for the Swisscom Signing Service. You can now use a qualified electronic signature.

You can now close the app and continue with your service provider.

Go to dashboard

Identification is successful:

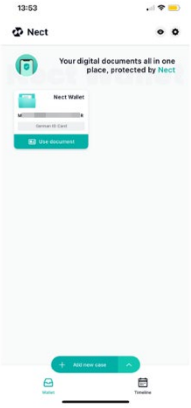

Nect

Your digital documents all in one place, protected by Nect

Thank you for verifying with us! Would you mind giving us a rating?

Tap a star to rate the Nect Wallet app

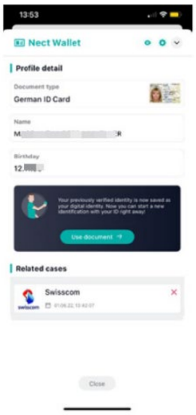
☆☆☆☆☆


Nect

Your digital documents all in one place, protected by Nect

Nect Wallet

Use document


Nect Wallet

Profile detail

Document type
German ID Card

Name
M[redacted]R

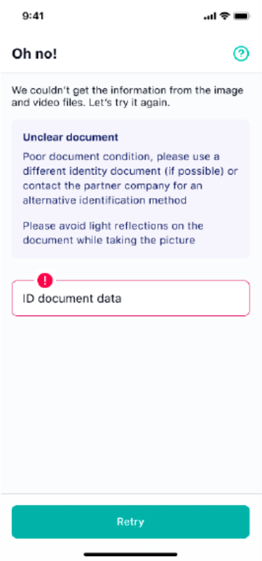
Birthday
12.[redacted]

Related cases

Swisscom

Close

Identification is unsuccessful:


Oh no!

We couldn't get the information from the image and video files. Let's try it again.

Unclear document

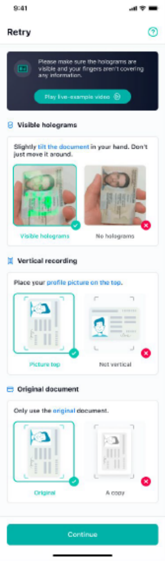
Poor document condition, please use a different identity document (if possible) or contact the partner company for an alternative identification method

Please avoid light reflections on the document while taking the picture

ID document data

Retry

If the machine could not read out all necessary information from video of the front side, the picture of the back side or your selfie video – this page and a detailed explanation in English is shown. Please select 'Retry'.


Retry

Please make sure the holograms are visible and your fingers aren't covering any information.

Play live-example video

Visible holograms

Slightly tilt the document in your hand. Don't just move it around.

Visible holograms ✓ No holograms ✗

Vertical recording

Place your profile picture on the top.

Picture top ✓ Not vertical ✗

Original document

Only use the original document.

Original ✓ A copy ✗

Continue

Tips are shown on what might be the issue. Please select 'Continue'.

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

8.6 Appendix 5 –Identification with SRS Video-Ident-CH by INTRUM

- Identification method name: video
- Identification Service Provider : intrum-video
- Signature capability for User Identified with this method: AES/eIDAS, AES/QES/ZertES
  - Validity of the evidence: 5 years max
  - Language possible for video calls (Agent language) German, English, French, Italian
  - 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 gets an SMS with a link to the T&C – User accepts T&C and User can sign.

- Language: a language parameter can be set in the request to be led to an Agent speaking this language Please be aware that the front end takes the language of the browser of the user agent.
- Method filter specification

Filter Parameter	Value	Value
Issuer	Intrum-video	Intrum-video
Jurisdiction	eIDAS	ZertES
LOA	3	4
Offline	FALSE	FALSE
Method Type	Video	video
Web flow	TRUE	TRUE
Realtime Method	TRUE	TRUE

- Initial data provided: the data provided in the request must match exactly the data on the ID document. If there is an error in the Last name, the identification will be negative. If Surname and at least one given name is provided correctly in case of multiple given names, the identification is positive.

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

The information in this document is of a non-binding nature and is subject to change.

- **Miscellaneous**

- The Target URL is available 90 Days (Status created and initialized)
- The process of ID verification takes in general 5 to 10 minutes. (max 15 min)
- If no SMS is received after 15 min the identification is negative. Check the status.

- **Possible reason for unsuccessful identification**

Additionally to the SRS Status "error", "canceled" or "aborted", the reason is added to the status for support purpose. The reason describes the problem occurred.

Examples:
"User does not allow camera permission in the app."
"User does not accept the terms and conditions.")
"User is not ready for a selfie.")
"User aborts as the app is not scanning the document.")
"User cancels as the phone number is specified incorrectly.")
"User wants to identify later.")
"User is not interested in performing the identity verification.")
"User aborts because the app is not responding.")
...

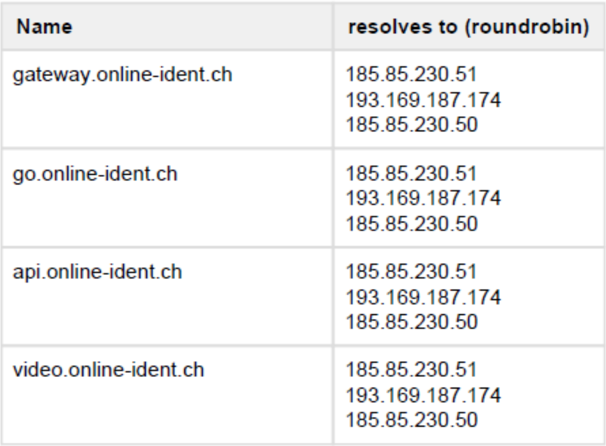
Note: Please note that if Status is "aborted" the user can retry with the same IdentID.
If Status is "cancelled" or "error" then User cannot retry and needs a new Target URL.

- **Hardware/Device**

The identification can be done through a mobile APP or directly in a desktop modern browser (not internet Explorer). The mobile app is available in all Appstore's worldwide. The identification is not possible on a mobile browser.
If using a desktop browser, the camera and microphone must have a good quality than permits a correct conversation and scanning of documents.
Check here the compatibility:
https://www.idnow.io/wp-content/uploads/Compatibility_Matrix_31012022-1.pdf
Technical requirements

UDP: 3478 (STUN)
UDP: 6000-7000 (for Video/Audio/Data Stream) (set when connection is initiated)
TCP: 443 (HTTPS)
TCP: 80 (if URL is entered "go.online-ident.ch" instead of https:// redirect to 443 (HTTPS)

The following server names must be resolved to the following IPs (round robin). the server names should be used if possible.



Name	resolves to (roundrobin)
gateway.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50
go.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50
api.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50
video.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50

The information in this document is of a non-binding nature and is subject to change.

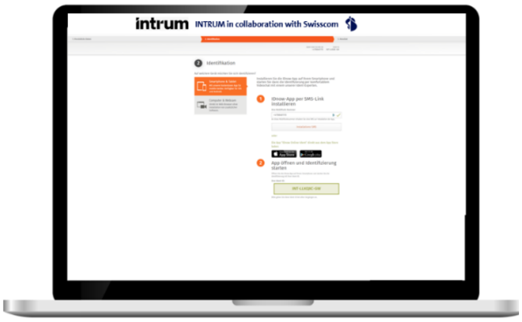
Swisscom Trust Services

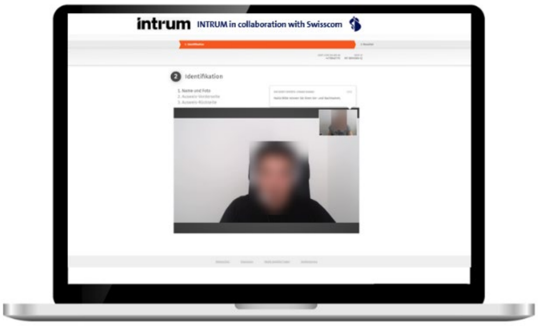
Target	Protocol	Comment
185.85.230.51:443 193.169.187.174:443 185.85.230.50:443	TCP / HTTPS	User frontend
185.85.230.51:443 193.169.187.174:443 185.85.230.50:443	TCP / HTTPS	API calls video server
185.85.230.51:3478 193.169.187.174:3478 185.85.230.50:3478	UDP / STUN	Video communication
185.85.230.51:6000-7000 193.169.187.174:6000-7000 185.85.230.50:6000-7000	UDP / RTP, RTCP, TURN	Video communication

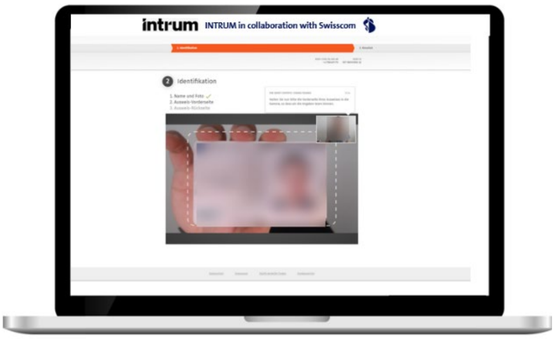
- **Service Times**

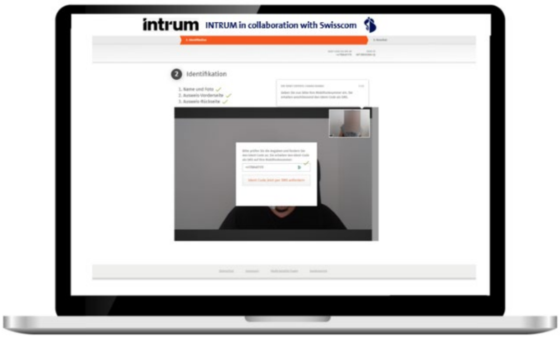
Monday-Saturday 7:00-22:00

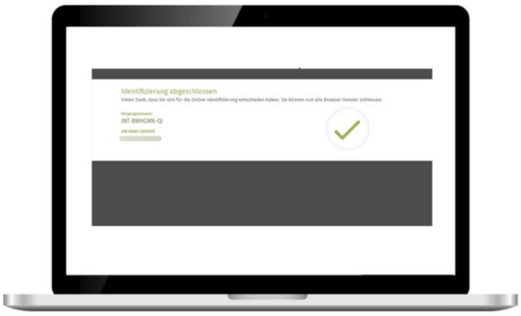
- **Screenshots**









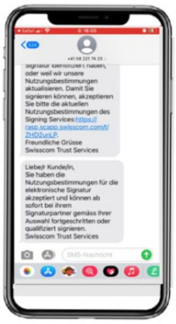


Identifizierung abgeschlossen

Vielen Dank, dass Sie sich für die Online-Identifizierung entschieden haben. Sie können nun alle Browser-Fenster schliessen.

Vorgangsnummer

INT-BWHGNN-QJ



+41 58 221 74 23

Signatur identifiziert haben, oder weil wir unsere Nutzungsbestimmungen aktualisieren. Damit Sie signieren können, akzeptieren Sie bitte die aktuellen Nutzungsbestimmungen des Signing Services:https://rasp.scapp.swisscom.com/t/ZHD2unLP.
Freundliche Grüsse
Swisscom Trust Services

Liebe/r Kunde/in,
Sie haben die Nutzungsbestimmungen für die elektronische Signatur akzeptiert und können ab sofort bei ihrem Signaturpartner gemäss Ihrer Auswahl fortgeschritten oder qualifiziert signieren.
Swisscom Trust Services

The information in this document is of a non-binding nature and is subject to change.

Swisscom Trust Services

8.7 Appendix 6 –Identification with SRS Auto-Ident-CH by INTRUM

- Identification method name: autoident
- Identification Service Provider : intrum-autoident
- Signature capability for User Identified with this method: AES/eIDAS, AES/QES/ZertES
  - Validity of the evidence: 2 years max
  - Language possible German, English, French, Italian
  - List of supported countries LINK
- User Flow

  User starts identification in the browser or in the mobile app – user scans ID documents - Mobile number is verified with a SMS Challenge – User makes a selfie video that is analysed by an AI – A back-office check is done – **User gets an SMS with a link to the T&C** – User accepts T&C and User can sign.

- Language: language of the user agent (browser language or mobile phone language)
- Method filter specification

Filter Parameter	**Value**	**Value**
Issuer	Intrum-autoident	Intrum-autoident
Jurisdiction	eIDAS	ZertES
LOA	3	4
Offline	FALSE	FALSE
Method Type	Video	Video
Web flow	TRUE	TRUE
Realtime Method	TRUE	TRUE

- Initial data provided: the data provided in the request must match exactly the data on the ID document. If there is an error in the Last name, the identification will be negative. If Surname and at least one given name is provided correctly in case of multiple given names, the identification is positive.

Attributes	
Firstname (Given Names)	Mandatory

Lastname (Surname)	Mandatory
Date of birth	Optional
Mobile number	Mandatory
Place of birth	Optional
Country	Optional
Email address	Optional
Language	Optional
External ID	Optional

- **Miscellaneous**

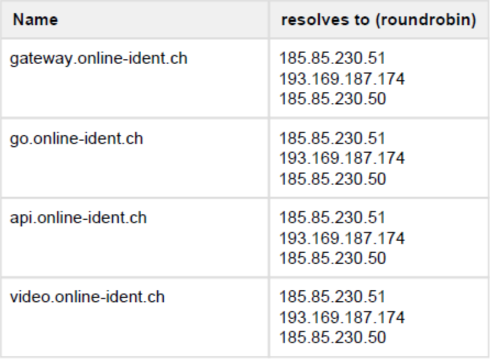
- The Target URL is available 90 Days (Status created and initialized)
- The process of ID verification takes in general 5 to 10 minutes. (max 15 min)
- If no SMS is received after 15 min the identification is negative. Check the status.

- **Hardware/Device**

The identification can be done through a mobile APP or directly in a desktop modern browser (not internet Explorer). The mobile app is available in all Appstore's worldwide. The identification is not possible on a mobile browser.
If using a desktop browser, the camera and microphone must have a good quality than permits a correct conversation and scanning of documents.
Check here the compatibility:
https://www.idnow.io/wp-content/uploads/Compatibility_Matrix_31012022-1.pdf
Technical requirements

UDP: 3478 (STUN)
UDP: 6000-7000 (for Video/Audio/Data Stream) (set when connection is initiated)
TCP: 443 (HTTPS)
TCP: 80 (if URL is entered "go.online-ident.ch" instead of https:// redirect to 443 (HTTPS)

The following server names must be resolved to the following IPs (round robin). the server names should be used if possible.



Name	resolves to (roundrobin)
gateway.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50
go.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50
api.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50
video.online-ident.ch	185.85.230.51 193.169.187.174 185.85.230.50

The information in this document is of a non-binding nature and is subject to change.

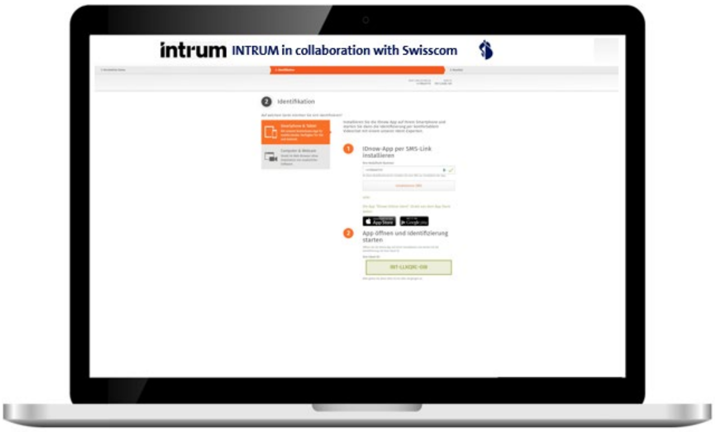
Swisscom Trust Services

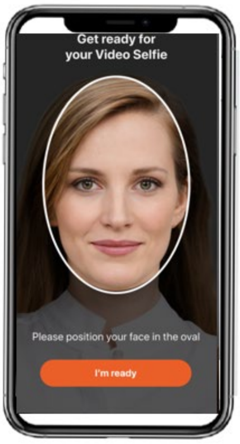
Target	Protocol	Comment
185.85.230.51:443 193.169.187.174:443 185.85.230.50:443	TCP / HTTPS	User frontend
185.85.230.51:443 193.169.187.174:443 185.85.230.50:443	TCP / HTTPS	API calls video server
185.85.230.51:3478 193.169.187.174:3478 185.85.230.50:3478	UDP / STUN	Video communication
185.85.230.51:6000-7000 193.169.187.174:6000-7000 185.85.230.50:6000-7000	UDP / RTP, RTCP, TURN	Video communication

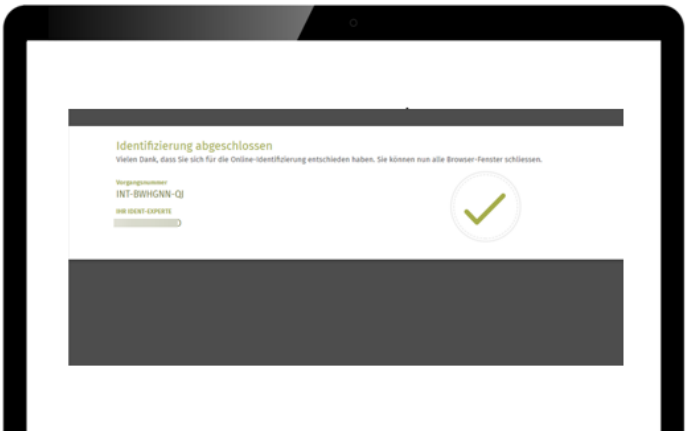
- **Service Times**

Monday-Saturday 7:00-22:00

- **Screenshots**




Get ready for your Video Selfie
Please position your face in the oval
I'm ready


Identifizierung abgeschlossen

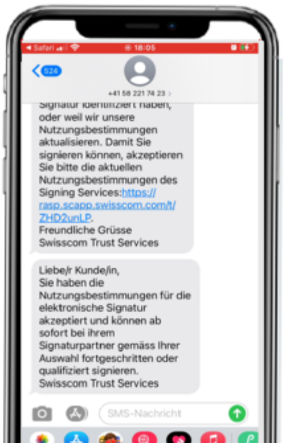
Vielen Dank, dass Sie sich für die Online-Identifizierung entschieden haben. Sie können nun alle Browser-Fenster schliessen.

Vorgangsnummer

INT-BWHGNN-QJ

IHR IDENT-EXPERTE

[redacted]



Signatur identifiziert haben, oder weil wir unsere Nutzungsbestimmungen aktualisieren. Damit Sie signieren können, akzeptieren Sie bitte die aktuellen Nutzungsbestimmungen des Signing Services:https://rasp.scapp.swisscom.com/t/ZHD2unLP.
Freundliche Grüsse
Swisscom Trust Services

Liebe/r Kunde/in,
Sie haben die Nutzungsbestimmungen für die elektronische Signatur akzeptiert und können ab sofort bei ihrem Signaturpartner gemäss Ihrer Auswahl fortgeschritten oder qualifiziert signieren.
Swisscom Trust Services

8.8 Appendix 7 – Identification over the Swisscom Trust Services Identification page

Technical requirements:
Java script should not be blocked on the browser

Browser: Chrome, Firefox, Edge, Safari
In enterprise Network, ensure that no proxy Firewall restriction apply or whitelist following needed domains:

Domain used in the whole Identification process

Domain List	Purpose
https://srsident.trustservices.swisscom.com/	SRS Identification web flow
https://fonts.gstatic.com/	SRS Identification web flow
https://www.google-analytics.com/	SRS Identification web flow
https://www.google.com/	SRS Identification web flow
https://www.googletagmanager.com/	SRS Identification web flow
https://www.gstatic.com/	SRS Identification web flow
https://go.online-ident.ch/	SRS Video ident CH
https://go.online-ident.ch/	SRS Auto ident CH
https://www.identity.tm/	SRS Video Ident EU
https://www.identity.tm/	SRS eID DE
https://ident.klarna.com/	SRS Bank DE
https://jump.nect.com/	SRS Selfie Ident EU
https://maps.googleapis.com/	SRS Direct

Swisscom Trust Services

The information in this document is of a non-binding nature
and is subject to change.