As a leading trust service provider in Europe,
we enable the most innovative digital
business transaction models.

White Paper

Smart Registration Service

Swisscom Trust Services

Swisscom Trust Services

Content

Introduction

The electronic signature becomes more and more important. Online processes can now be fulfilled, as the last building block required for the conclusion of the contracts is now available: the online electronic signature. The added value of the electronic signature is quite clear: cost-saving, ecological and user-friendly.
Legally, the qualified electronic signature is the most legal binding signature, as defined by the legislator in the EU by eIDAS regulation or in Switzerland by ZertES legislation. All other signatures, such as advanced signatures or simple signatures like scanned signature images, can be used in certain legal processes, but the legal binding may have to be determined separately in court in case of any doubt.
The qualified signature is subject to strict requirements with regard to the identification of the signatory. It was up to now also the problem that the qualified signature was used very rarely. With the Smart Registration Service of Swisscom Trust Services, a bundle of alternative and very innovative methods for identification is offered, which makes online identification possible for everybody.

Identify once – sign multiple only based on authentication

The Smart Registration Service solves various problems:

- In the EU, different identification requirements apply as in Switzerland. Each identification method must be authorized for the chosen legal area. For example, video identification in Switzerland may only be used in connection with financial intermediaries.
- Certain methods, such as auto-identification without a human operator could be used for an advanced signature but not for a qualified signature.
- Organisations may use identification data not only for signature purposes but also for identification concerning the anti-money laundering.
- Only one offered identification method is not always sufficient. E.g. users using an insufficient camera or have limited internet bandwidth could have problems to use the video identification method or has no German eID. The choice of different identification methods which can be used in parallel could be helpful.
- Until now, an electronic signature was often always linked to the previous step of identification, i.e. three signatures within two weeks also required three identifications. Swisscom offers the link between unique identification with an authentication means: i.e. the signatory soon can sign only by use of a PIN, fingerprint, facial recognition without prior identification.

Definitions and Abbreviations

Identification partner (in the technical description defined as "Identification Service Provider" or „ISP“)
The provider of identification solutions is a Swisscom partner who has developed a solution for identifying a person. This solution provides a certain level of identification, i.e. a signatory can either only sign advanced or qualified. It is possible that one identification partner will provide multiple identification methods. For example, an identifier provides video identification or auto-online identification (OID) with self-registration of the user.

Swisscom Customer (in the technical description defined as „Service Provider“ or „SP“)
Service Provider is a Swisscom customer for the Smart Registration Service, which offers its future signatories a web portal or starting point for identification. This starting point can be completely detached from the signature portal. It may also be possible, for example, that the Swisscom customer does not offer a signature itself, but forwards the identified person to a signature portal of another Swisscom partner.

Just an example

Bob has received a PDF document and needs to **electronically sign** it. He's never done that before!
Bob chooses an online service provider that offers this option on its web portal. He quickly creates an account and transfers his document to the portal.

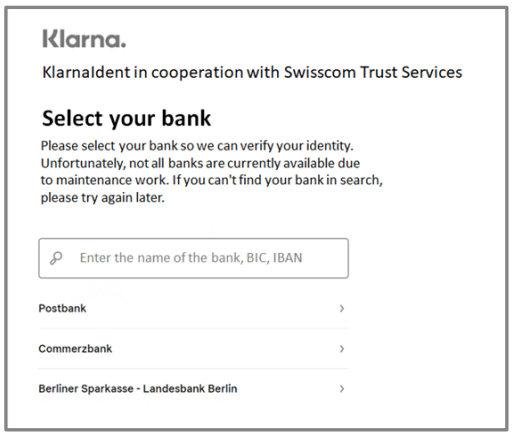
Ups! Bob hasn't been activated for the signature yet because he's never been identified before! No problem, Bob's now preferred signing portal leads him to a Swisscom identification partner, which in this case offers the video identification.
After a few minutes of contact with a nice operator Bob has to show his ID or passport. After identification he is ready to sign his document on the signature platform.

Bob is now able to sign!
He simply gives the declaration of will to the signature with his MobileID in Switzerland or a combination of password and one-time SMS code elsewhere or he soon uses the convenient MobileID app and gives consent with facial recognition or finger print. Finished! And so he signs next time likewise, without prior identification!

Swisscom Trust Services

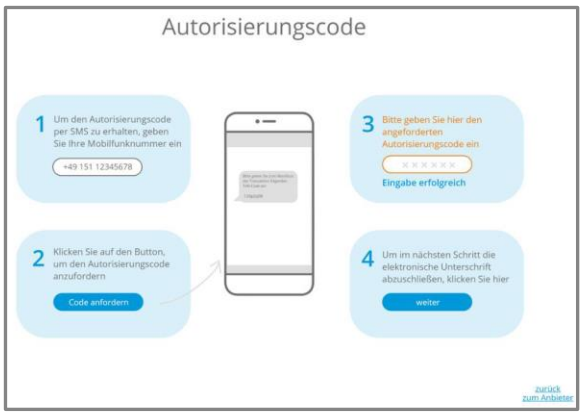
Available Identification Methods

In addition to the classic video identification, the KlarnaIdent bank identification is certainly interesting:



A short login to the online banking of a German bank enables the same level of identification for qualified electronic identification in Europe as video identification.
In addition, the electronic signature can also be used for identifications in the context of the fight against money laundering in accordance with German GWG law. The identifier Klarna enables a banking login with almost all German banks.

Also interesting is the German identity card with its eID functionality. With the Authada app, Authada enables direct easy identification from any NFC-enabled mobile device: put the ID in place near to the phone and enter the PIN code. Finished!



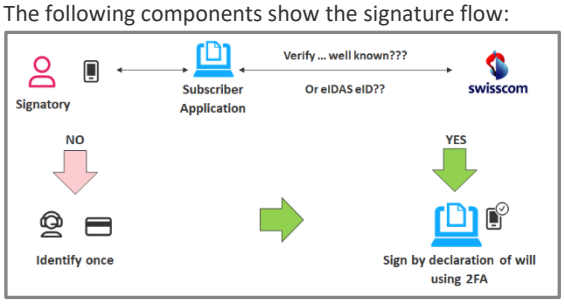
For advanced signatures, an online auto-identification is already available, i.e. an identification service, which usually works without an operator and biometrically compares the video image with the ID card and proves the lifeness in the video.

More methods for identification are planned:

- Courier service - rings up to 3x at the front door
- Point of Sales Identifikation – in your neighbourhood at selected places

How it works – technical description

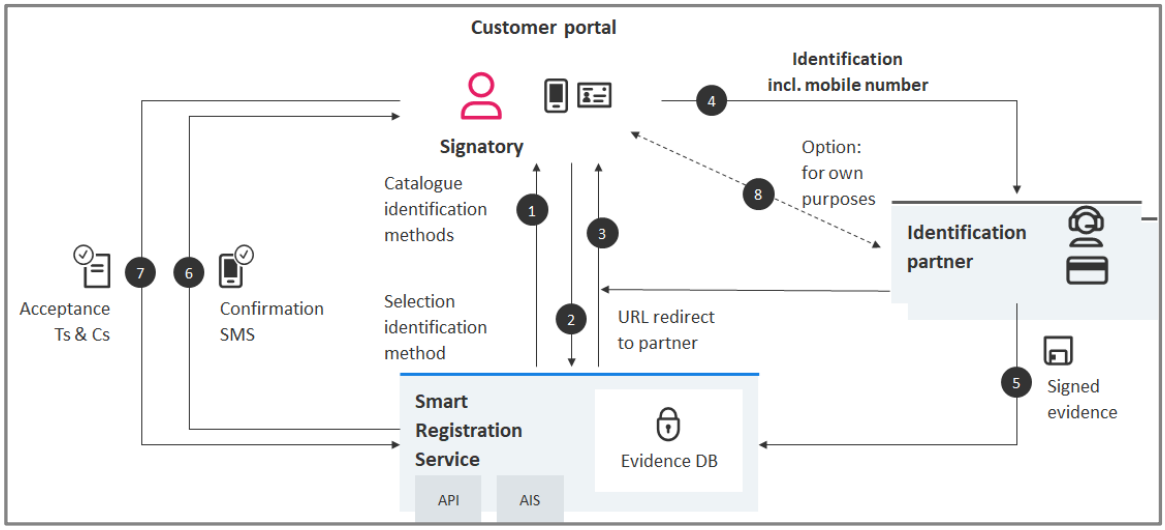
The following components show the signature flow:



legal area with the requested level (qualified or advanced signature) and if the person is already registered with Swisscom. If this is not the case, a one-time preidentification is necessary, otherwise the signature can be started immediately.

The signature application first checks (so-called "verify-call") whether a signature can be done in the respective

For identification, the Swisscom customer now offers in its portal a selection of identification methods for the future signatory:



The communication between Swisscom and the Customer is as follows:

(1) The customer gets a catalogue of the different available identification methods. The catalogue contains per method the correspondent legal area (eIDAS- EU/ ZertES – CH) and the level of assurance which allows to determine which signature quality is possible : qualified or advanced electronic signature.

(2) An identification method will be selected

(3) Swisscom opens an order with the identification partner and provides an URL redirecting the future signatory to the portal of the identification partner.

(4) The future signatory will now be forwarded to the portal of the identification partner and the registration takes place. The mobile number will be registered as authentication means. Based on this mobile number and a 2nd factor the future signatory can declare its will for all upcoming signatures.

(5) The identification partner will sign the evidence of the registration and import it to the evidence database of Swisscom.

(6) Swisscom uses the mobile number to ask the future signatory for the acceptance of terms and conditions by SMS.

(7) The future signatory accepts the terms and conditions on a portal of Swisscom by use of the URL found in the SMS.

(8) In the scope of AML it can be necessary that the customer wants also have the identification evidence. This is always based on an additional contract between customer and identification partner.

Service integration for the customer (Service Provider/SP)

The service implementation uses standard protocols.
The access and authorization of the service is based on an « access key » provided by Swisscom during the onboarding process.

- The service provider uses the OAUTH 2.0 protocol and JWT (« Jason Web Token »). They are used for later authorization on the system of the identification partner.
- A valid request for identification can be checked by use of the OAUTH introspection call.
- After proof of the validity of the token the identification can start.
- The customer can always check the status of the identification at the identification partner.
- Swisscom offers an interface description and integration guide which allows a short implementation cycle for the Service provider.
- The integration is possible after signing the Smart Registration Service contract with Swisscom.
- The interface is based on the “REST” call interfaces.
- Swisscom maintaines the interfaces to the identification partners thus the Service Provider has not to maintain those interfaces itself.

Is the user already registered? ("Verify Call")

This feature simply verifies that a user has already been properly registered for the signature. By specifying the appropriate parameters, it is possible to determine whether the user can sign in the scope of a specified jurisdiction and based on a certain signature quality: advanced electronic signature or qualified electronic signature. LOA - means "Level of Assurance".
In the following example, the service provider can determine whether the user can use the sample phone number and identification elements to perform a qualified electronic signature (LOA4) in accordance with eIDAS and ZertES

```
{
  "msisdn": "41791234567",
  "claimedIdentity": "test-client",
  "assuranceLevel": 4,
  "distinguishedName": "gn=Hans, sn=Müller, cn=Hans Müller, c=CH"
}
```

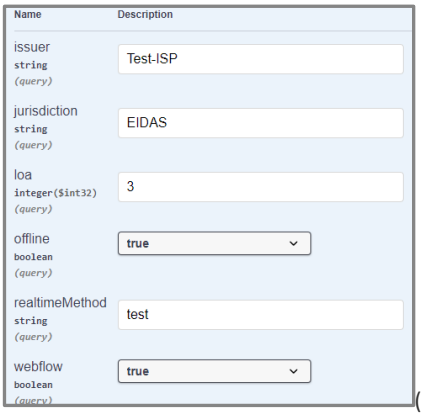
The positive response of the interface is shown. <string> contain the stored values of the Smart Registration Service, which can be used in the signature call: the evidenceID (uniquely stored serial number for the evidence), vetterMsisdn (the stored mobile number), serialNumber (unique serial number of the identified person based on the mobile number):

```
{
  "evidenceId": "string",
  "vetterMsisdn": "string",
  "serialNumber": "string"
}
```

Based on this positive or negative response, the Service Provider can initiate either the identification process or can directly sign.
Note that this interface does not require authentication.

List the available methods

This function allows to show a catalogue of all available identification methods. The Service Provider can filtert he responses for certain methods. For example the Service Provider can select only methods available from the identification partner « Test-ISP ».



(*)

Here the request oft he Service Provider:

```
curl -X GET "https://miss-backend-api-dev.scapp.swisscom.com/api/providers?issuer=Test-ISP&jurisdiction=EIDAS&loa=3&offline=true&realtimeMethod=test&webflow=true" -H "accept: application/vnd.sc.miss.provider.v1+json"
```

The response contains all methods with corresponding parameters in order to use this method :


```
[
  {
    "loa": 3,
    "issuer": "Test-ISP",
    "webflow": true,
    "jurisdiction": "ZERTES,EIDAS",
    "realtimeMethods": [
      "video",
      "test"
    ],
    "offline": true,
    "identificationData": [],
    "additionalData": [],
    "defaultLocale": "en"
  }
]
```


(*) Filter and parameters are subject to change

Possible filters:

Filter parameters	Definition	Example
loa	Level of Assurance	In case the Service Provider announces LOA 4 only identification methods with LOA 4 (QES) are listed an not LOA 3 (AES)
issuer	Identification partner	The preferred identification partner of Swisscom can be selected.
webflow	No breach of media	Identification methods without breach of media are used this means no courrier or POS registration.
jurisdiction	Legal area according the signature law of Switzerland or regulation of EU	Switzerland: «ZERTES», EU: «EIDAS»
realtimeMethods	Online methods available	e.g. “video” for video identification
Offline identification process	Offline process necessary	e.g. visit of POS or courier
Identification data /additional data	Pretransfer of identification data	Customer wants to transmit beforehand the existing customer data to the identification partner

Start of the identification process with the selected method

After selection of the method in the previous step, the Service Provider submits an identification request to start the process. The following parameters must be included in the application:

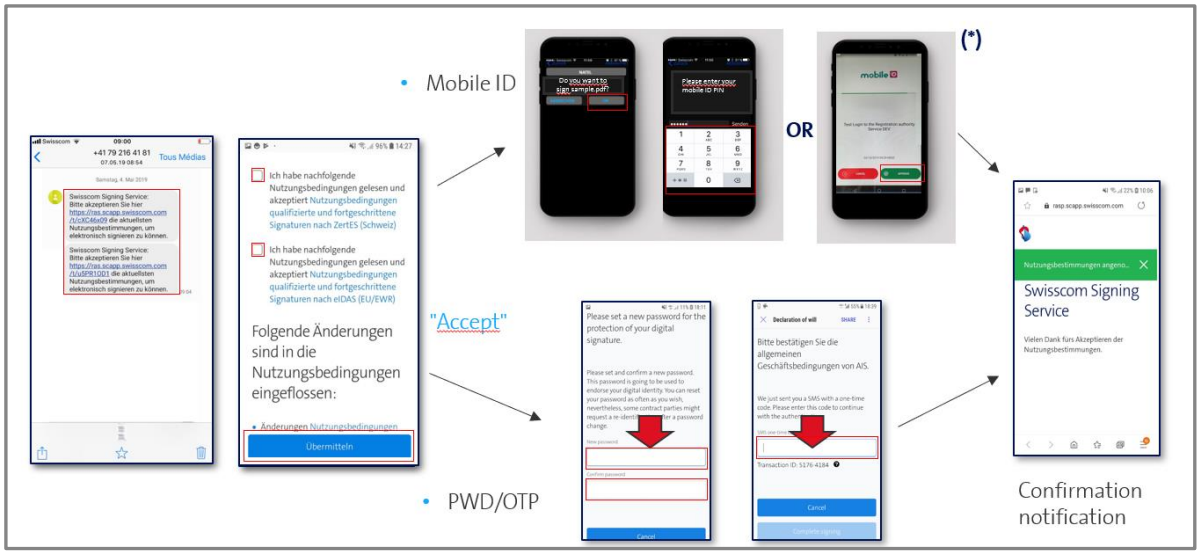

```
{
  "dob": "1978-02-28",
  "email": "hans.muster@swisscom.com",
  "firstName": "Hans",
  "language": "en",
  "lastName": "Muster",
  "mobile": "+41783478228"
}
```


The interface responds:


```
{
  "refId": "5c327977-a154-4747-b99d-c0733f7007c5",
  "error": null,
  "targetURL": "https://www.identity.tm/status_neu/1ABF5CD5DBEA405B20AEB9142448570D
}
```


Swisscom provides the link to start identification by the identification partner. The service provider redirects the user to this URL and the identification process can begin.

During identification, the user's mobile phone number is also checked because it is used for authentication at the time of signature. At the end of the identification process, the user receives an SMS on his mobile phone with a link to the terms and conditions of use of the Swisscom Signature Service (AIS).



After acceptance of the terms and conditions of use the user can electronically sign the document.

Determine the identification status

The service provider can ask for the status of an identification at any time. It can also determine if a problem occurred during identification.

Status request:


```
https://miss-backend-api-dev.scapp.swisscom.com/api/identifications/c3ee9d79-0250-4d1b-805b-e72d591b9f23
```


Status request answer of Swisscom:
The identification is done and the evidence is transmitted!

Response body

```
{
  "refId": "62c3ee9d79-0250-4d1b-805b-e72d591b9f23
  "orderId": "
  "issuer": "test",
  "adapter": "fake",
  "method": "video",
  "mobile": "+41775383140",
  "evidenceId": null,
  "statuses": [
    {
      "status": "created",
      "date": "2019-11-25T09:19:20.165Z",
      "reason": null,
      "kind": null
    },
    {
      "status": "created",
      "date": "2019-11-25T09:25:28.779991Z",
      "reason": null,
      "kind": null
    },
    {
      "status": "initialized",
      "date": "2019-11-25T09:19:20.192Z",
      "reason": null,
      "kind": null
    }
  ]
}
```

Other status messages (*) :

Status message	Meaning
"Waiting for Doc"	Swisscom is waiting for evidence data
"Identification done"	Identification already done but evidence data probably not already transmitted.
"Data Ready"	Evidence is transmitted and signature is possible after acceptance of terms of use
"Identification cancelled by user"	Identification was cancelled by the user with unknown reason.
Identification cancelled by ISP	Identification was cancelled by the identification partner with unknown reason.
Identification unsuccessful	Identification was cancelled due to insufficient or false identification cards/passports

(*) These messages are subject to change.

Additional identification data (e.g. in scope of AML)

In principle, the identification data remain with Swisscom for signature purposes. The signature itself shows the first name, name and home country of the identified person, unless a pseudonym has been chosen.
If the customer also wants to use the identification data for further purposes, an additional contract between the customer and the identification partner must be concluded. The identification partner will then allow the customer access to the data using Swisscom "orderID". The same identification process provides the data for signature purposes as well for e.g. anti-money laundering.
A separate white paper provides detailed information on the possibilities for the use of identification in the context of AML law in Germany ("GWG").

Setup Filter and Parameter

Swisscom will setup the Service Provider based on its requirements concerning identification and signature which will be described in the contract. The Service Provider can list the methods to be used, the legal area and the signature quality level.

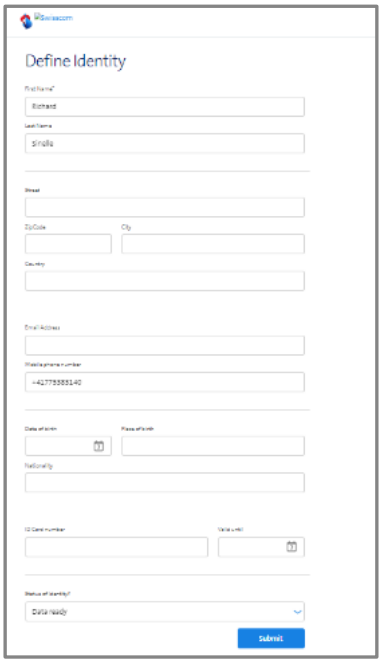
Example

Identification Service Provider	Identification Methods	LOA and jurisdiction
ISP 1	Video	LOA4/eIDAS
ISP2	BankIDent	LOA4/eIDAS

Test Environment

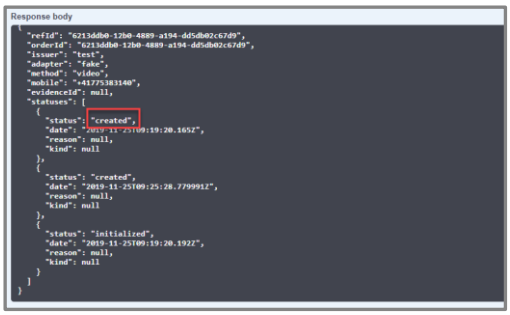
In order to simplify the integration Swisscom offers a test environment for the customer.
It is possible to test the end-to-end flow including the identification part. E.g. a sample session with the video identification partner can be done with live agents. By this the process can be testes in the same way as it will run later on in the production environment. Of course this should be done only in a limited manner since it causes extra costs.

This is the reason for Swisscom to offer the simulation of the interface of the identification partner and to return the different status of the identification. Swisscom offers a form which can be filled out with the identification values instead of the real identification values. (see figure on the right hand side).



In the case below the status of “complete identification” is chosen. It means the evidence data is already imported:

Following this example the following anwer will be shown: The identification is finished and the evidences are importet. In case the terms and conditions are accepted (to be checked by the verify call) the signatory can sign electronically.



The complete interface can be found here: https://miss-backend-api-dev.scapp.swisscom.com/swagger/index.html. An integration guide is available on request. Prerequisite of an access to the test environment is a signed service contract for the Smart Registration Service.

Service cost

A monthly fee occur for the provision of the service depending on the possible identification method. Each identification will be invoiced per transaction.

Advantage of the Service

The Smart Registration Service in its standard form enables a rapid implementation of an electronic qualified signature without regulatory effort. For the end user there is only one starting point and the customer enjoys only one single-sign-on contact for all identification methods by using evaluated methods and selected Swisscom partners. Swisscom ensures that the relevant methods are compliant with the law and in accordance with the relevant standards. Swisscom also bears full liability as a trust service provider for the reliability of identification.
The customer continuously benefits from the latest innovative identification options.

The best identification partners on the market are brought directly together with interested customers and can focus on their core competencies, identification.

We appreciate to answer your further questions!

Swisscom (Schweiz) AG
Enterprise Customers
Identification Service

Pfingstweidstrasse 51
8005 Zürich

Switzerland

https://trustservices.swisscom.com

Swisscom Trust Services