



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

White Paper QES Ident

Use of the qualified electronic signature and the
associated processes within the scope of
identity verification according to
§ 12 GwG / German law



Content

Introduction 3

Purpose of the document and exclusion clause 3

Identification processes in the context of combating money laundering 3

Integration of the QES Ident Service 4

The customer experience 5

Data protection according to GDPR 5

The role of the ID card or Passport document 6

Advantages of the process 6

Further information on this topic 6



Introduction

With the QES Ident Service, Swisscom Trust Services supports the process of verifying the identity of natural persons, particularly in the context of the provisions of the [German Anti Money Laundering Act \("AML"\)](#). Swisscom Trust Services is considerably simplifying the process of identity verification for anti-money laundering purposes for its customers. Previously a physical on-site identification or video identification, which always has high abort rates, was necessary according to the AML. With Swisscom QES Ident only electronic access to a German bank account is required.

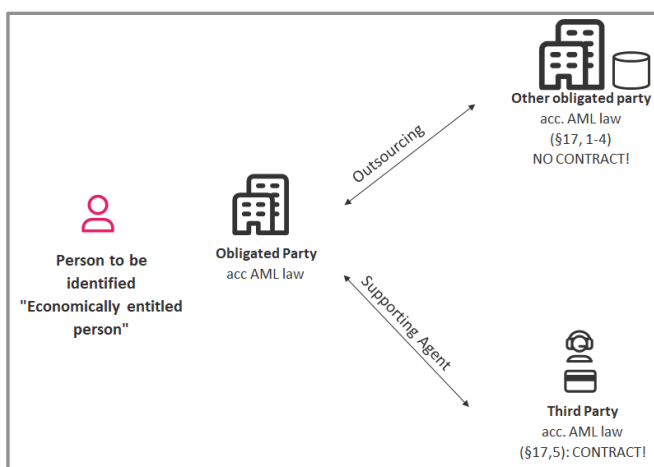
Purpose of the document and exclusion clause

This document serves as a basis for discussion with the various parties concerned - it does not claim to be complete or error-free. It does not constitute an offer and is not intended to have any other legal effect, in particular not for existing or future contracts.

In this document, Swisscom Trust Services expresses its opinion and view, also regarding legal assessments - such as those concerning the German Anti Money Laundering Act (AML) - but without any guarantee or liability. It is the sole responsibility of each party concerned to carefully study the circumstances themselves and draw their own conclusions. Swisscom Trust Services recommends that each party consult experts as necessary to clarify any questions that arise, particularly in areas of special legislation, such as the AML.

Identification processes in the context of combating money laundering

In the context of the fight against money laundering, the focus is on compliance with due diligence obligations about the identification and collection of identification data of its contractual partner. An obligated party under the AMLA must ensure that it assures its contractual partner to be checked and knows with whom it is doing business. To this end, the contractual partners must be clearly identified in accordance with the law.



The current approach is to personally inspect the contractual partner and identify him by means of an official identification document or to use an approved video identification. Particularly in the case of video identification, special conditions, such as the prohibition of sub-delegation, must be observed, as well as the strict requirements of [§17 \(5\) GWG](#) with regard to "other suitable persons and companies" as third parties who have to fulfil duties of care in the context of identification.

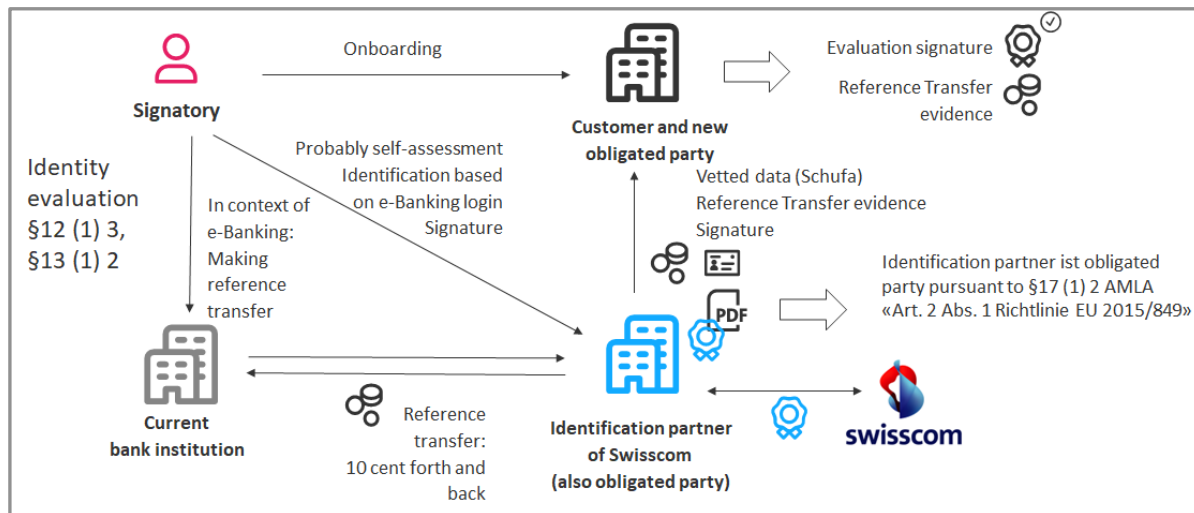
However, in [§12 \(1\) 3](#) or [§12 \(1\) 2](#), the AMLA also permits an identity check using a qualified electronic signature in accordance with the eIDAS Regulation, provided that there is also a validation of the signature and a reference transfer from an account in the

name of the person to be identified. The reference transfer must be made "directly" within the framework of the signature creation. By this, contracts requiring the written form (BGB §126a) can be signed digitally with the signature. If only an identity check is to be carried out, the signature can be applied, for example, to a self-disclosure document from the customer or an account application form. In this way, the contractual partner identifies itself as a natural person vis-à-vis the obligated party, with the support of the Swisscom identification partner, who is itself an obligated party within the meaning of the AMLA and provides the necessary data from the identification check according to eIDAS. The identification method approved for Swisscom IT Services Finance S.E. for this purpose by means of e-banking login requires the same proof within the meaning of the "eIDAS Regulation" as is later required in the context of the AMLA:

- Verification of the necessary (own) data of the person to be identified (name, address, place of birth, birthday, nationality)
- E-Banking Login to a German account, e.g. (previous) house bank, additional checks distinguish here between account owner and account authorised representatives or shared accounts
- Triggering of a transfer (10 cents) to a recipient account of the identification partner and thus triggering of strong authentication at the house bank's account. The amount will be refunded later.
- Completion of the identification with a second factor for authentication (one-time password via SMS).



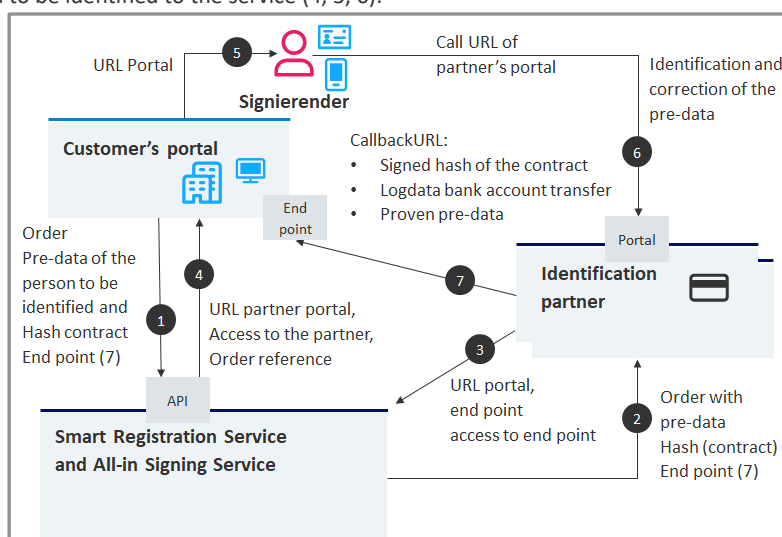
In this respect, Swisscom provides these eIDAS identification proofs via its identification partner following the identification and signature, so that the customer can also use these as proof of identification in the sense of the GWG. The customer as the obligated party then only has to validate the signature against the [EU Trust List](#) and provide proof of a reference transfer from a verified account made by the verified person, which it has received as proof from the Swisscom identification partner.



Since the identification partner itself is the obligated party pursuant to [Section 17 \(1\) 2 GWG](#) (banking institution), special contracts on due diligence are not required, which would otherwise be necessary pursuant to [Section 17\(5\)GWG](#) with "other suitable persons and companies" as supporting third parties.

Integration of the QES Ident Service

The QES Ident Service with its proof of identification and signature is completely integrated into the customer workflow. It would be conceivable, for example, that the customer shows the person to be identified a document for electronic signature, e.g. a self-disclosure or account opening. The customer then opens an order (1) for a QES Ident with Swisscom and forwards the person to be identified to the service (4, 5, 6).



With the order opening, the customer already transfers the known personal data (1) to the QES Ident Service, which the person can then check and correct again (optionally) in the portal of Swisscom's identification partner:

- First name and surname,
- Home address,
- Date of birth,
- Place of birth
- and nationality.

All data except the place of birth are checked by a well-known German credit agency and compared with the data from the e-Banking login. The verified person then makes the reference transfer from his or her account in Germany to the account of the identification partner and thus also fulfils the GWG requirement of "immediacy" (here: same session) of



the transfer to be made. Likewise, the hash of the document is now also electronically signed in a qualified manner, which the customer also transmitted to Swisscom when placing the order (1). The signed hash is returned to the customer by the identification partner (8). The customer can create a signed document from the signed hash. This ensures that the content of the document cannot be read by either Swisscom or the identification partner.

The customer can now check the permissibility of the signature of Swisscom IT Services Finance S.E. using the [EU trust list](#) and the signature certificate or by querying a [validator](#). In addition, the customer receives log data of the reference transfer directly from Swisscom's identification partner (8). This means that identification within the meaning of §12 (1) 3 or §12 (1) 2 has been carried out by checking a qualified electronic signature. Further data is collected and transmitted without the strict requirements of an identification check, as described in the [Interpretation and Application Instructions of the BAFIN pursuant to Section 51 \(8\) GwG, as of December 2018](#), in chapter 5.1.3.2 d). It says here literally:

"For the identification of natural persons, the information pursuant to Section 11 (4) No. 1 AMLA shall be collected regularly by asking the person concerned or by taking over from an identification document submitted by the person concerned. (...)

The following options are available for verifying the identity of natural persons: (...)

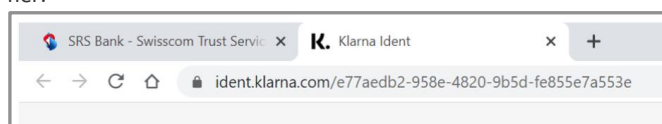
d. Qualified electronic signature pursuant to [Section 12 \(1\) sentence 1 no. 3 GwG](#)

An appropriate examination of the above-mentioned identification documents and evidence shall be based on the risks of money laundering and terrorist financing in each individual case. This also applies in view of the fact that some of these documents and evidence do not contain all the information specified in [Section 11 \(4\) No. 1 AMLA](#). Nevertheless, this circumstance does not exclude the suitability of the document or evidence for verifying the identity of the natural person to be identified (nor does it expressly exclude Section 4 (4) sentence 1 GwG aF). Insofar as individual details mentioned in [Section 11 \(4\) No. 1 GwG](#) are not contained in the document, no verification is required with regard to these details. "

Here, Bafin even relies on self-disclosure or "no verification", nevertheless, one is on the safe side with any other careful collection of these data, such as based on identification collection for a qualified eIDAS signature as done within QES Ident.

The customer experience

The signatory is forwarded from the customer workflow to a special identification URL of Swisscom's identification partner:



After confirming the terms of use, he enters his data, selects the banking institution and gives the authorization for the reference transfer:

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

First name

Ingolf

Last name

Rauh

DD

MM

YYYY

02

02

1965

Street

City

Zip code

Country

Germany

Mobile number

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

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

DKB

Deutsche Kreditbank - DKB

Kreis- und Stadtparkasse Dinkelsbühl

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.

chipTAN optisch (Flickercode)

-

+

□

◀

▶

Finally, the contract is signed with a one-time password, which is received via SMS.

Data protection according to GDPR

Within the meaning of the GDPR, all parties are independent controllers in this scenario. This means that the customer asks the person to be checked for consent to the data transfer to Swisscom and the identification partner. The person to be verified enters into a separate contractual relationship with Swisscom regarding the conditions of use for the signature. The identification partner is the delegated registration authority office and is itself under obligation. It obtains the customer's consent to data processing. All parties are visible to the customer during the screens or during the interactions. In this



respect, no order processing is concluded. Swisscom will keep the data for 35 years in accordance with the Austrian Signature Act (SVG).

The role of the ID card or Passport document

Again and again the question arises to what extent also identity card or passport data or copies must be included in the case of the bank login identification procedure.

In the May 2020 version, the application and interpretation instructions of the Bafin point out:

" According to Section 8 (2) sentence 2 GwG, **in particular**, a copy of the documents submitted for identity verification in accordance with Section 12 (1) sentence 1 number 1 or 4 GwG or their complete optical digital recording must always be made (see in detail below under Chapter 9).

Reference is made here to [§8 Paragraph 2 Sentence 2 GwG](#), which, for example, also excludes the document copy itself for the eID:

"Insofar as documents pursuant to Section 12 (1) sentence 1 number 1, 4 or 5 are submitted for the purpose of verifying the identity of a natural person or documents pursuant to Section 12 (2) are submitted for the purpose of verifying the identity of a legal entity" or insofar as documents determined on the basis of a statutory instrument pursuant to Section 12 (3) are submitted or used, the obligors have the right and the obligation to make copies of these documents or records or to record them in optically digitised form or, in the case of on-site readout in accordance with Section 18a of the Identity Card Act, Section 78(5), second sentence, of the Residence Act or Section 13 of the eID Card Act, to record the service- and card-specific identifier and the fact that the data were taken over by means of on-site readout These shall be deemed to be recordings within the meaning of sentence 1."

The basis of the bank login procedure is the verified transmitted data of the person, the transaction that took place and the proof that this person holds an account. This means that the "documents" (data) used here are transmitted accurately. They are expressly considered as records in the sense of the required diligence.

This means that the term "document" in the law and also in the Bafin documents is not always the same as an identity document.

Advantages of the process

Compared to a physical on-site inspection, this procedure can be carried out online within one or two minutes without media discontinuity. High abort rates, sometimes up to 20-30%, which can occur in connection with video identification because the camera resolution or bandwidth is insufficient, are not to be expected here. In contrast to a video identification, no outsourcing contract according to [§17\(5\)ff. AMLA](#), which transfers the duties of care to the video service provider, does not have to be concluded. As Swisscom's identification partner is also a bank itself and thus also an obligated party within the meaning of the AMLA, it can provide verification information, such as the verification of the reference transfer, without the need for a further individual contract. By linking the possibility of a bank transfer with an identification verification and signature, the legally required immediacy is also given (see [§12 \(1\) AMLA](#) according to subsection 5). In addition, the procedure is also considerably cheaper than video identification due to the lower abort rates.

After conclusion of the service contract, the Swisscom customer only has to comply technically with the Swisscom protocol and is then automatically connected to the Swisscom identification partner. The "one-stop shopping" without any further contract with the identification partner enables him to continue to use the signature only on the basis of authentication in the future regardless of any further identification (up to a maximum of 2 years).

Further information on this topic

Further information and contact details can be found on our homepage <https://trustservices.swisscom.com>