RA-Agent

Table of Content

RA-Agent

What can I expect in this training?

Identification made easy!

The most important task of the RA agent is to record the **identity of a person**, because this is the only way to enable the identified person to **sign electronically**.

With the **RA App**, identification has never been easier!

In this training you will learn everything you need to know about electronic signatures and the RA App!

What do you guess: How long will it take you with the RA App to enable a person for electronic signatures?

Please click on the correct answer.

A) 2 minutes

B) 5 minutes

C) 15 minutes

Tania is working as a RA agent since 1 year and knows the RA-App very well. In this training she has many good tips for you as an upcoming RA agent, what you have to pay attention to when identifying ...

This is what you take from this training .....

After the training you know, ...

... what personal electronic signatures are and what the requirements are

... how the identification with the RA App works

... which documents you use for identification

... how to estimate your duties within the framework of identification

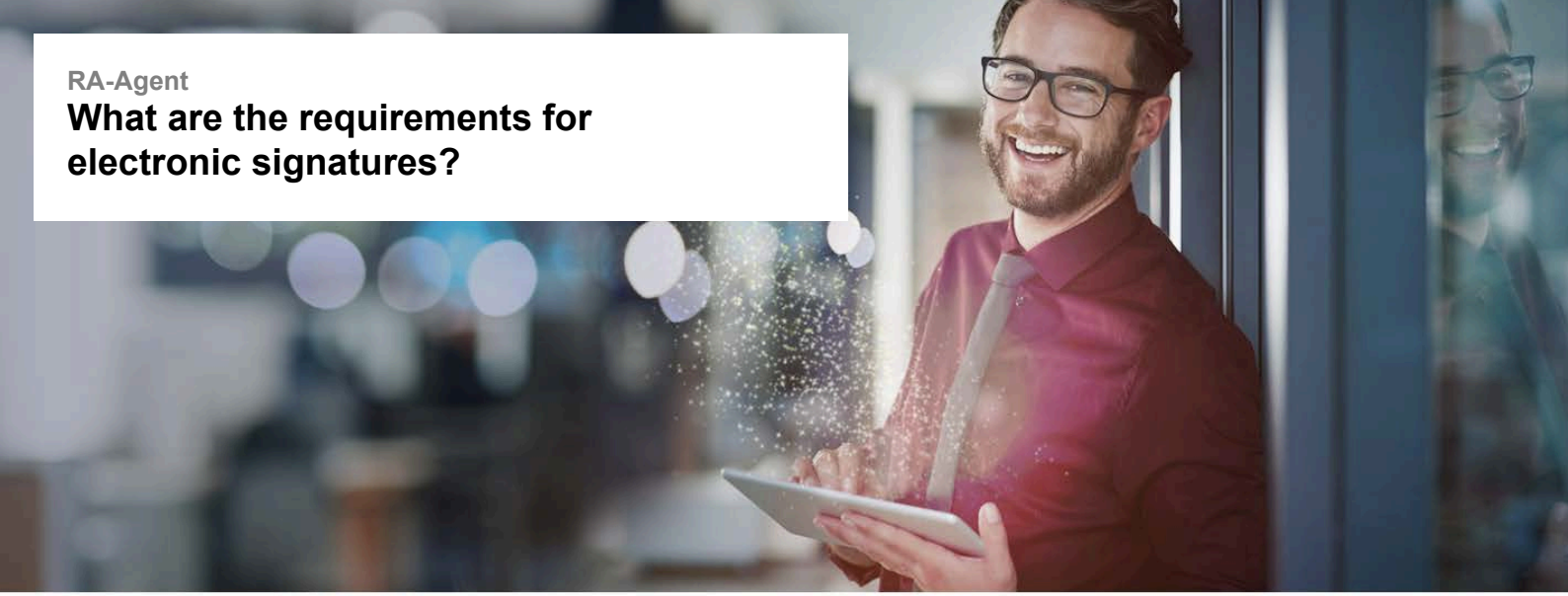
After the training you can …

... use the RA App to identify new people for electronic signing

... give the identified persons hints for electronic signing

... react to missing support by the RA App correctly, e.g. with an unknown identity card

For reasons of better legibility, the simultaneous use of male and female language forms is avoided. All personal designations naturally apply to both genders.



RA-Agent

What are the requirements for electronic signatures?

The Electronic Signature: Features and Requirements

What is an electronic signature?

An electronic signature contains **data in electronic form**. This data is attached to or logically linked to other electronic data. Thus, the signature guarantees the **integrity of the document** and the **identity of the signer**.

What are the different types of electronic signatures?

There are many different types of electronic signatures. As part of the RA Service, these **personal electronic signatures** are of interest:

- Advanced electronic signature (AdES)
- Qualified electronic signature (QES)

From the stomach: Which of the two signatures has evidence value in court?

Please choose the correct answer.

A) The Advanced Electronic Signature (AdES)

B) The Qualified Electronic Signature (QES)

The more important of the two is the **Qualified Electronic Signature (QES)**.

The identifications performed with the RA App enable the creation of **qualified** electronic signatures.

The **Qualified Electronic Signature** (QES) is the highest quality electronic signature and is the only signature that is **equivalent to a handwritten signature**. For Switzerland, this is regulated in the Swiss Code of Obligations (Art. 14 para 2 ^{bis} OR).

What's the difference bettween AdES and QES?

- The **AdES** has a certain probative force and is used in **contracts without formal regulation**.
- The **QES** has the highest evidential value and is used for contracts that **require the written form**. It is e**qual to a handwritten signature**.
- In court, **QES** are de facto accepted as evidence. Therefore the principle of shifting the burden of proof does not apply if a QES has been applied to a contract.

What are the requirements for electronic signatures?

What are Qualified Certificates...

Electronic signatures base on **digital certificates.** These certificates of Swisscom are created together with the key pairs used for signing and have a validity period of 10 minutes, i.e. they can only be used for a single signature at a time.

We distinguish between advanced certificates of the class **"Saphir"** and qualified certificates of the class **"Diamant"**.

Qualified Certificates ...

- ... in Switzerland must only be issued to **natural persons** and ...
- ... contain information that makes them a qualified certificate. Qualified Swisscom certificates contain the label " **Diamant**" in the issuer's name.

Who has what responsibility with this?

The RA Agent is responsible for these points:

- The RA Agent **conscientiously** identifies the person
- The RA Agent complies with the **specifications of Swisscom** and the **RA App**

➢ Make sure that you **really** identify the person who **claims to be** - and that the presented ID card or passport is **genuine** and the recorded data is **correct**!

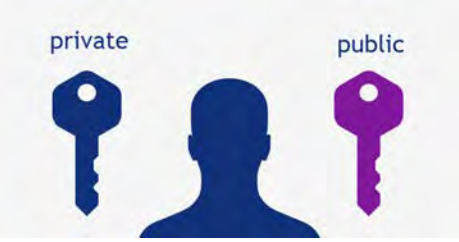
These points are met by Swisscom:

- Swisscom **enables the RA agents** to perform identifications.
- The signature is based on a **qualified electronic certificate**.
- The signature is generated by means which **the signer can keep under his sole control**.

"Only we as RA-Agents have the right to identify people, in order to enable them to sign. This is a privilege!
This is made possible with the Swisscom RA App that makes the identification process much easier."

What are the requirements for electronic signatures?

Public Key Infrastructure (PKI) – the basis of electronic signatures



Each user has two cryptographic keys (typically 384 characters long):

- a **private** key that no one else is allowed to know
- a **public** key that everyone can know

For the electronic signature you need these two keys:

- the **private** key for attaching a signature
- the **public** key to verify a signature

A Trust Service Provider (TSP) like Swisscom

- **identifies** the person (Registration Authority)
- associates the key-pair with the identified person

Swisscom as a Trust Service Provider (TSP):

- must be able to prove that she meets all **legal requirements**
- is **approved** by national authorities in Switzerland and in the EU

Various laws regulate the requirements for electronic signatures:

- in Switzerland this is the **ZertES** law with the corresponding ordinance (VZertES)
- in the EU, this is regulated by the **eIDAS** regulation and by country-specific laws

A qualified electronic signature is, ...

- ... according to ZertES, **only accepted in Swiss jurisdiction,** i.e. for contracts with applicable law and jurisdiction in Switzerland
- ... according to eIDAS Regulation, recognized in **every EU and EEA country**

What are the requirements for electronic signatures?

How to attach electronic signatures while keeping the private key secret?

Traditional approach

- The Trust Service Provider gives the user a **token** that contains his private and public keys
- The user carries the token **physically** with him
- The use of the token requires **special software** and a **card reader**

To trigger a signature, the signer **connects the token to the device** on which he wants to sign. For authentication he then enters the corresponding **PIN** .

Modern Approach

- The RA App registers the **cell phone number** of the user for later authentication.
- The signature keys are generated **at the time the signature** is triggered .
- The user can sign from any location and at any time

The signer can trigger a signature and authenticate with the **mobile phone**.

Question:

What kind of signatures can replace the handwritten signature?

Please select the correct answer.

A) The simple electronic signature (SES)

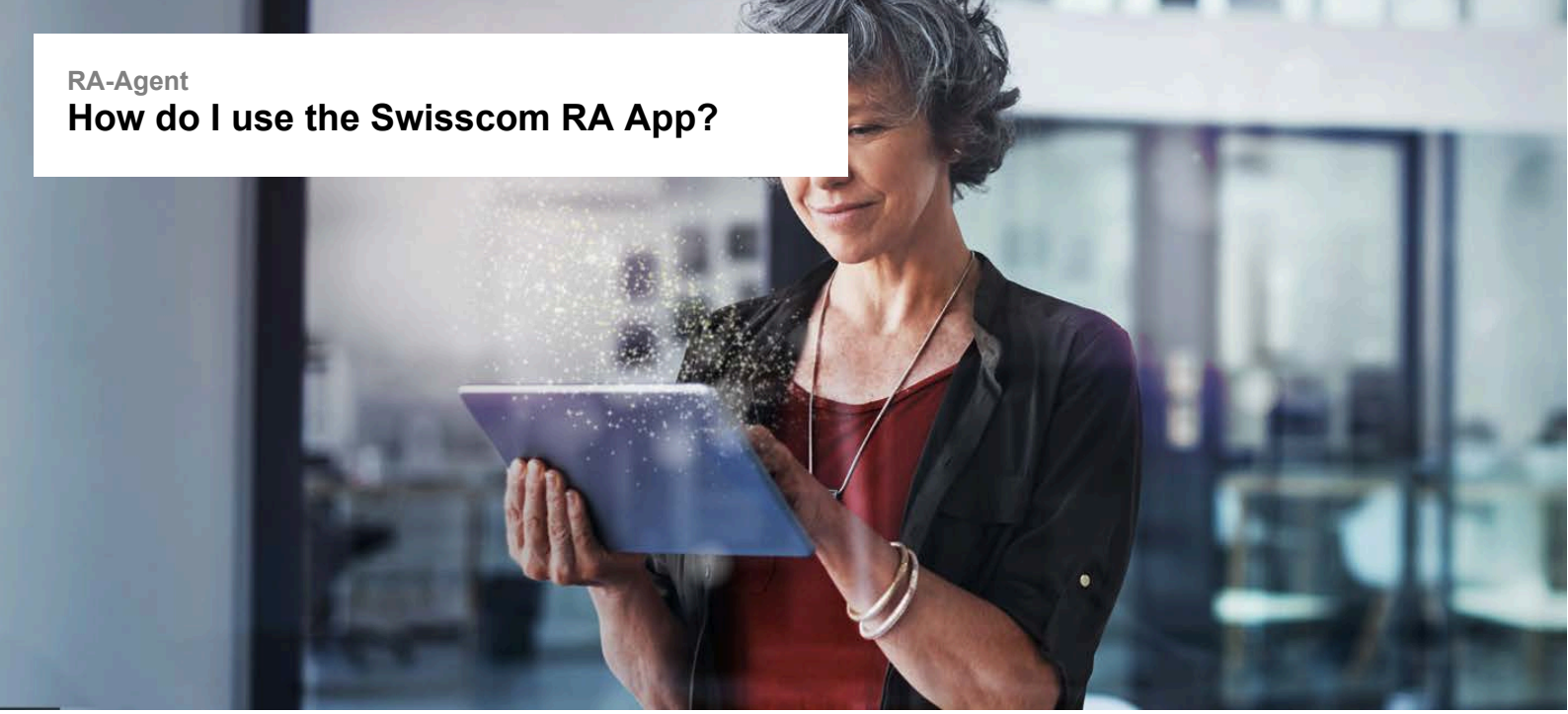
B) Advanced electronic signature (AdES)

C) Qualified elektronic signature (QES)

D) The handmade signature on a touchscreen

RA-Agent

How do I use the Swisscom RA App?



How does identification with the Swisscom RA App work?

What are the prerequisites?

- The **person to be identified** must always meet with the RA agent **in person.**
- The person to be identified has a **valid ID card** (from the Schengen area) or **passport** and a **mobile phone** with her.
- The RA agent must then ensure the **correct identification** with the presented ID document that has to be **available in the RA App**.
- Due to the data protection act, the person to be identified has to allow the RA agent to
  - take a **photo** of him and his ID (identity card or passport),
  - Swisscom stores her **mobile phone number**,
  - the data on the ID document (ID card or passport) is **read out and stored** at Swisscom in Switzerland

Tip

Ask the person to be identified to activate Mobile ID on her mobile phone **BEFORE** you start the identification with RA app. This makes the signature process even easier: a Mobile ID request is displayed on the mobile phone and the user confirms with his PIN or biometrics (e.g. fingerprint, Face-ID, etc.) .

How it works: navigate to www.mobileid.ch, enter your mobile phone number, click on "**Activate Mobile ID**", choose between **SIM** with a six-digit PIN or the **App version** with biometrics and follow the instructions for activation.

mobile ID

Important!

For the identification of a person with the RA-App only

- the **Swiss ID card**
- **ID cards of countries in the Schengen area**
- a **passport**

are permitted as identification documents, since the RA-App enables qualified electronic signatures and there are **strict legal requirements** for these.

➢ **Driving licences, foreigner's identity card, paper copies of ID documents** or **other documents** are **NOT** permitted for identification.

These ID documents must also have a **machine-readable code**, otherwise they **cannot** be used for identification. Therefore, for example, the **Italian identity card in paper form** is not suitable for identification.

Also important!

You must first ask the person to be identified for her consent to store her personal data. If the person agrees, please click the corresponding checkbox (see below: step 3 of the RA app 4.0 instructions). If the person refuses you have to cancel the identification immediately.

Good to know

According to the Swisscom's terms of use, the data is only used for the purpose of the signature. It is stored in encrypted form and kept for a certain period of time due to legal requirements (16 years under Swiss federal law and 35 years under European law).

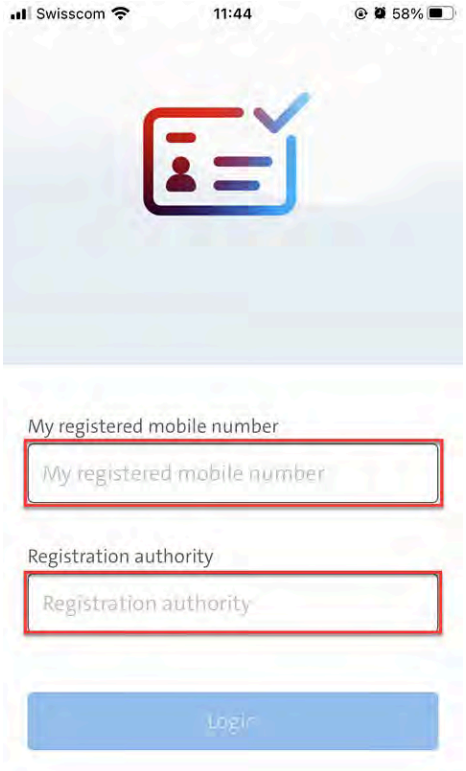
You are welcome to pass this information to the person to be identified.

How to use the RA App 4.0 step by step:

Instructions for the old RA App 3.x starting on page 13

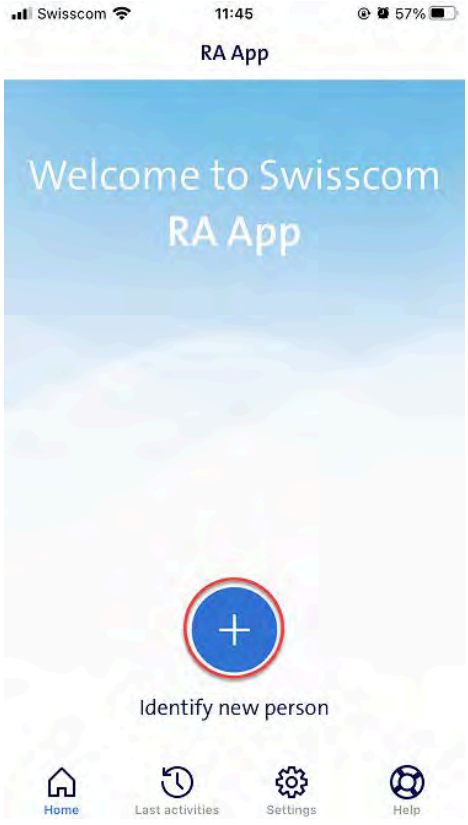
Step 1

Authenticate yourself in the RA App with your mobile number and the company name you received:



Step 2

You get to the start screen and start an identification with a click on the blue "+" sign.



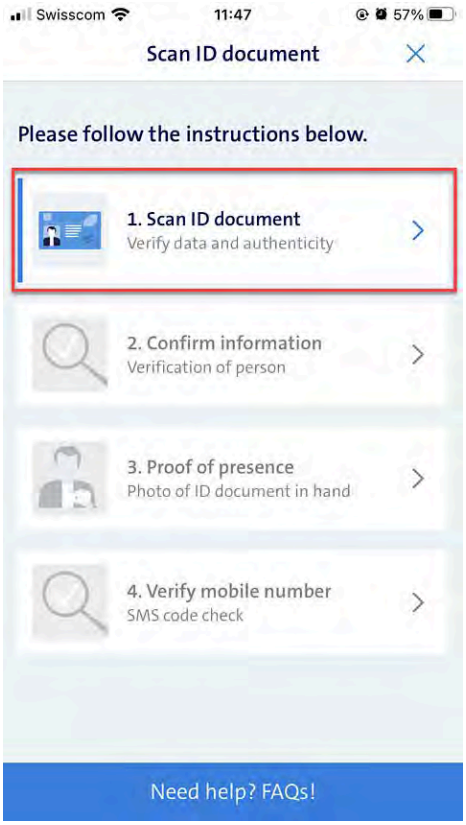
Step 3

Get the consent to store the data from the person to be identified and confirm it by clicking on the corresponding checkbox

Then click on "Confirm".

Step 4

Start the identification process by clicking on "Scan ID document".



Step 5

Now you scan the page of the ID document (ID or passport) that has an MRZ on it. The MRZ is sometimes on the front side under the photo and sometimes on the back side. Choose the correct side.

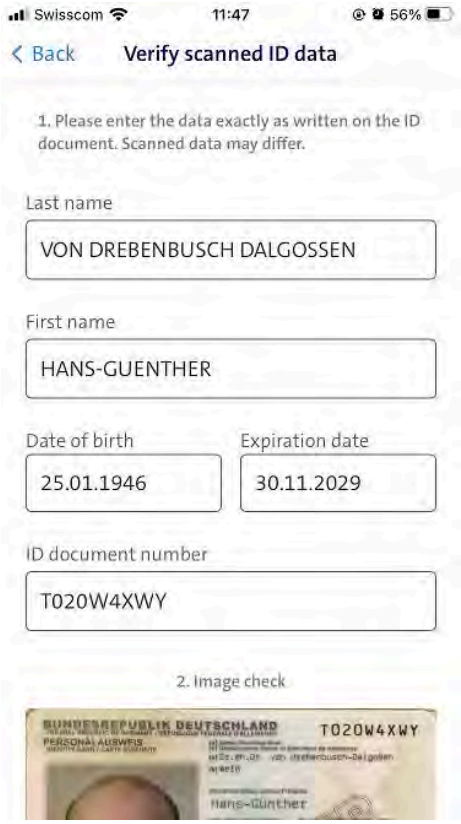
Tips:

- First hold the document a little further away from the camera and then slowly approach the lens.
- Choose a background that is not too bright so that the document is easily recognised by the scanning engine.
- Follow the instructions of the RA app at the top of the screen.

If the ID document presented has a reverse side (usually this is the case with ID cards), then turn the document over and scan the other side.

Step 6

Check the scanned ID information. If it does not match the with the information in the ID document, correct it manually.



In the example above, the data is not quite correct, the special characters were not scaned correctly: in the first name there is "ue" instead of "ü" and in the last name there is "ss" instead of "ß".

Please correct this so that the scanned data in the RA App matches the data in the ID document.

Please note:
missing or truncated parts of names must also be added.

- Please re-enter everything so that the information in the RA App exactly matches the data on the ID document.

But:

- Please **do not record titles** (e.g. Dr.) that are entered in the ID document, as they do not belong to the name.
- **Do not enter punctuation** such as dots "." or commas "," either, as these lead to errors.

Only minus signs "-" are allowed in names.

If everything is ok, then confirm this accordingly via the button at the very bottom of the screen or start the check again.

Step 7

A sample document is displayed. Check the security features according to the illustration in the RA app.

Also check that the person in the photograph is the person to be identified.

You should check the following characteristics:

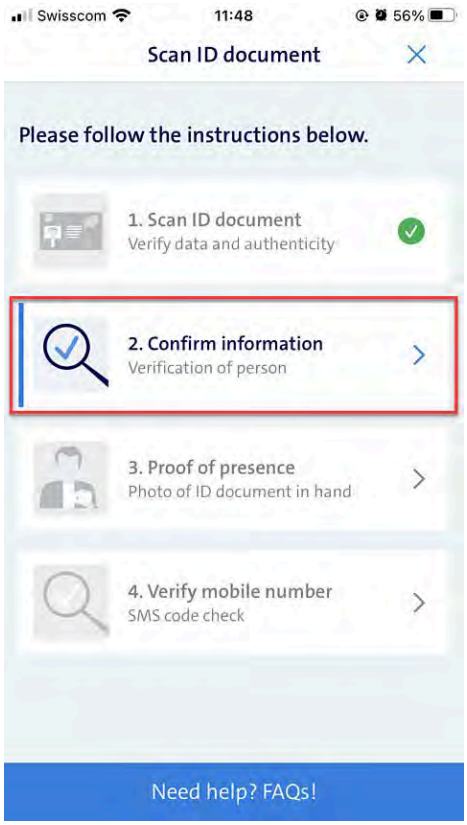
- Eye color
- Face shape and proportion
- Height and gender
- Age of the person

If everything is ok, select "Authenticity verified".

Step 8

Now you come to the next section: the person to be identified must confirm her data.

Please click on "Confirm information".



Step 9

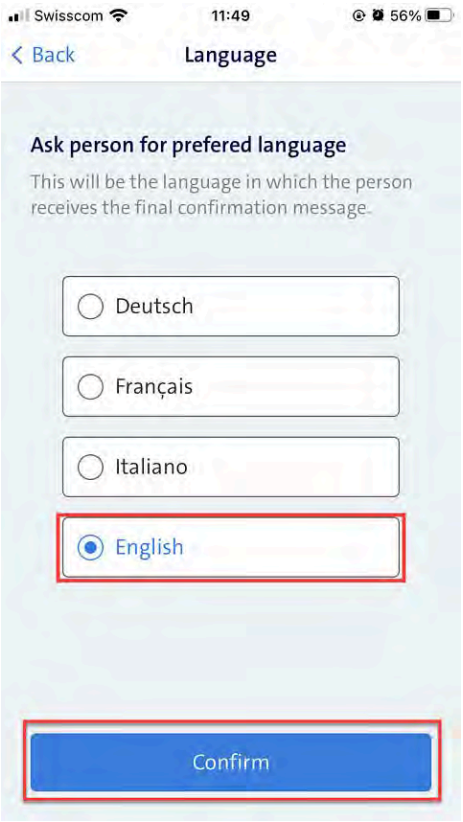
Show the person to be identified the data captured via the RA App and ask for his/her consent or correction.

If the person confirms that her data is correct, please click the "Confirm" button.

Otherwise open the editor via "Modify information" and repeat this step..

Step 10

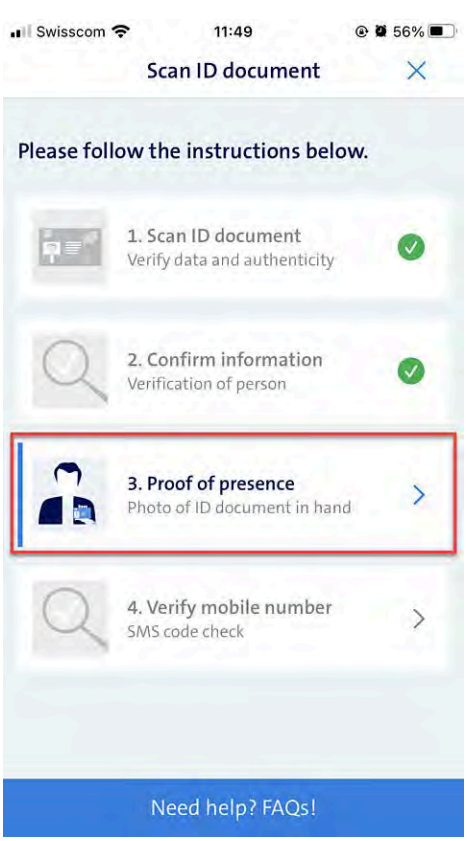
Now select the preferred language of the person to be identified and confirm the selection.



Step 11

The next section is about proving that the person is present in person.

Please click on "Proof of presence".



Step 12

Take a picture of the person, she should hold his/her ID document into the camera as shown in the screen.

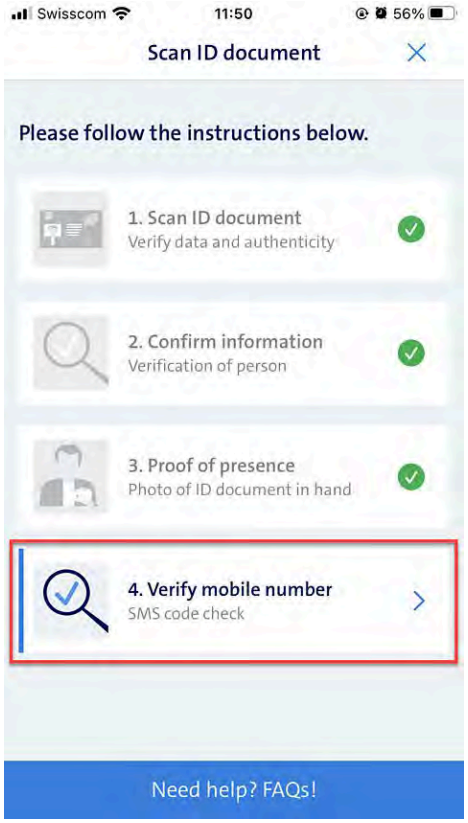
If the photo is ok, then you can "Confirm".

If the photo is bad, you can repeat this step as many times as you want.

Step 13

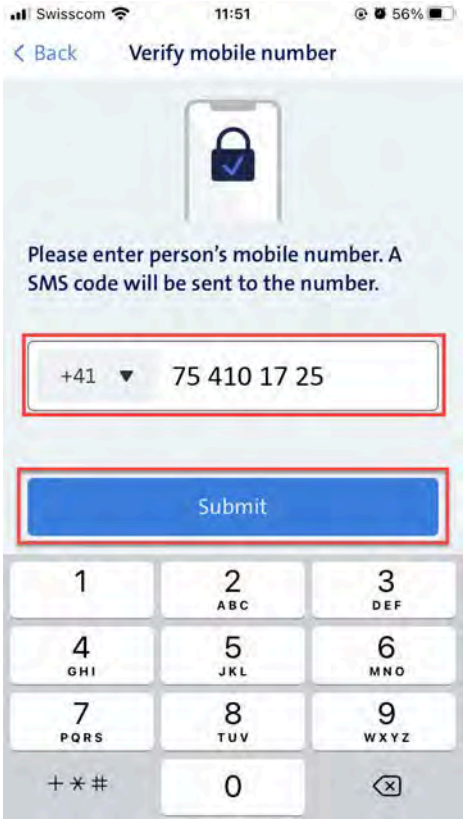
In the last section, the mobile number of the person to be identified is verified and the identification process is finished.

Please click on "Verify mobile number".



Step 14

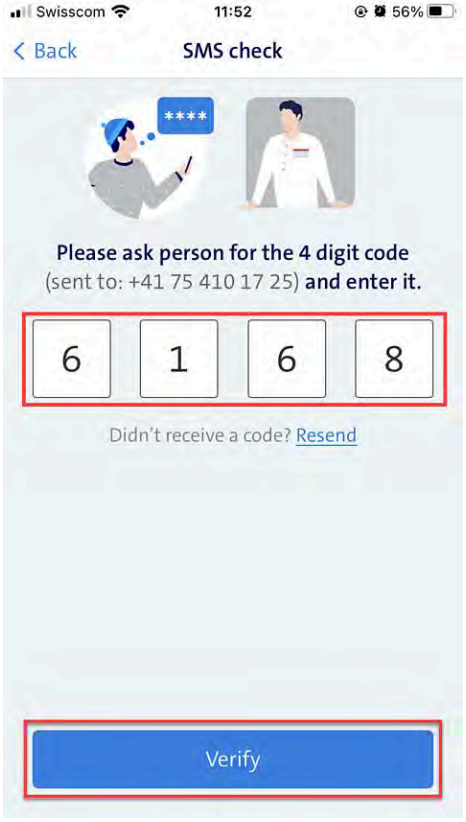
Enter the mobile number of the person to be identified in the corresponding field and then click on "Submit".



Step 15

The person to be identified will tell you the 4-digit code that was sent to him/her via SMS.

Enter this code in the appropriate fields and then click on "Verify".



Step 16

The last step is to sign the identification documents you have just created.

You do this via your cell phone using Mobile ID or password/SMS code procedure.

Step 17

The identification is now complete.

Tip: Please point out to the identified person that the whole process (the "registration") is only completed when he/she has also accepted the terms of use of the Swisscom Signing Service.

This is the instruction for the old RA App 3.x

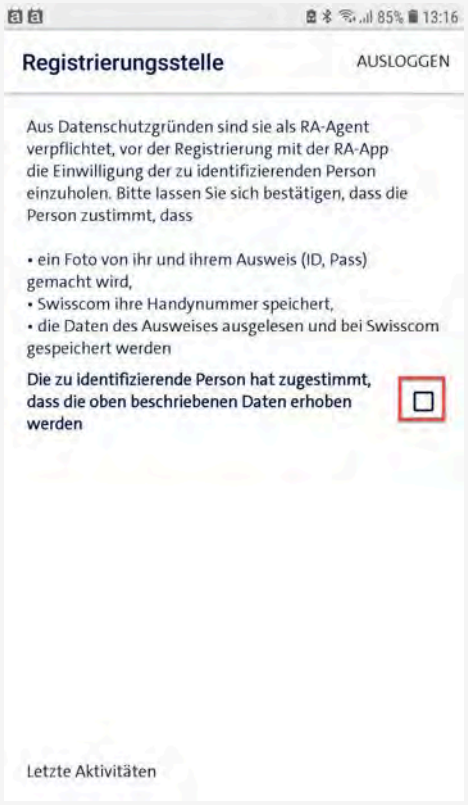
Step 1

Authenticate yourself in the RA App with your mobile number and the company name you received:

Step 2

First get the consent of the user that his data is taken and stored.

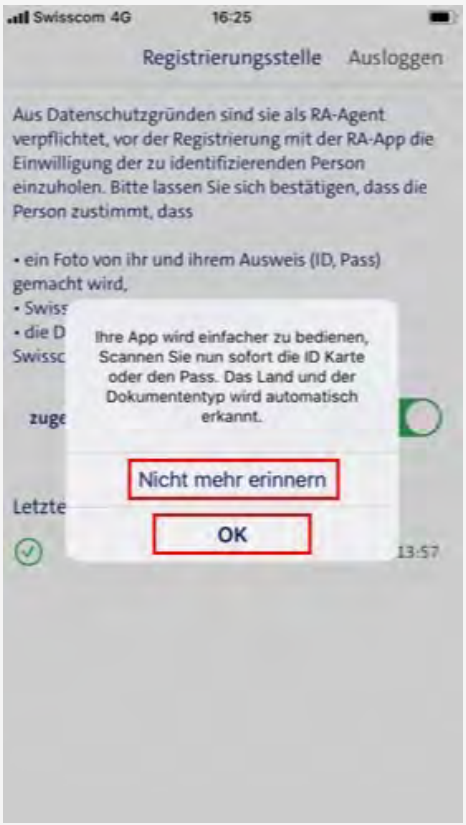
Then click on the appropriate checkbox.



The text disappears and you can go on.

Step 3

A message informs you about the new app. You can turn off this message for future identifications.



Step 4

Now you scan the page of the ID (ID or Pass) on which a MRZ can be seen.

Sometimes the MRZ is on the front under the photo and sometimes on the back. Select the correct page.

Tipp: Hold the document a little further away from the camera first and then slowly approach the lens.

Step 5

Check the scanned ID information.
If they do not match the information in the ID document, correct them manually.

Example 1: A letter of the name was read incorrectly.

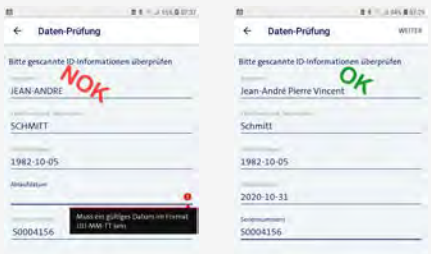
Please correct this letter.

Example 2: The name contains special characters such as umlauts.

Please **correct** so that the name matches the spelling in the ID document.

Example 3: The name has not been entered completely. In addition, an expiration date is missing.

Please **complete** everything so that the details correspond exactly to the data on the ID document.



Step 6

An example document is displayed.
Check the security features according to the image in the RA App.

Also make sure that the person in the photograph is actually the person to be identified.

Please check the following characteristics:

- Eye color
- Face shape and proportions
- Height and gender
- Age

If everything is ok check "Authenticity checked" and then "NEXT".

Step 7

Now take the other side of the ID card that does not contain a MRZ (only for ID/ Identity card). If you initially scanned a passport, this step is no longer necessary.

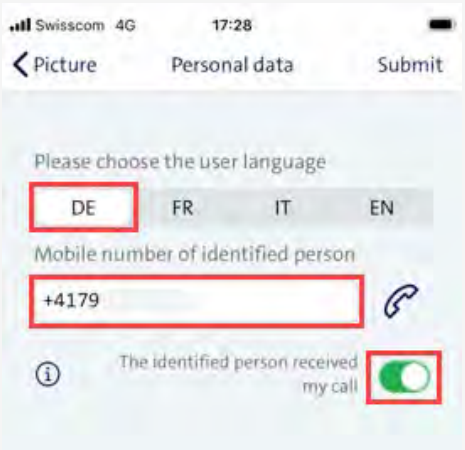
If everything's okay, then "Next". If the photo is bad, you can repeat this step as many times as you want

Step 8

Take a photo of the identified person (as proof of physical presence). The person should hold the ID document in the camera

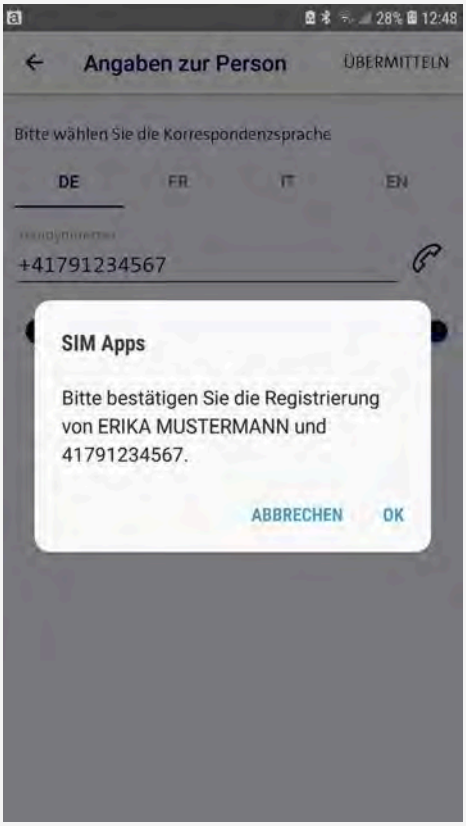
Step 9

Finally select the signers preferred language, get his mobile number and check by a call whether he really owns this mobile number.



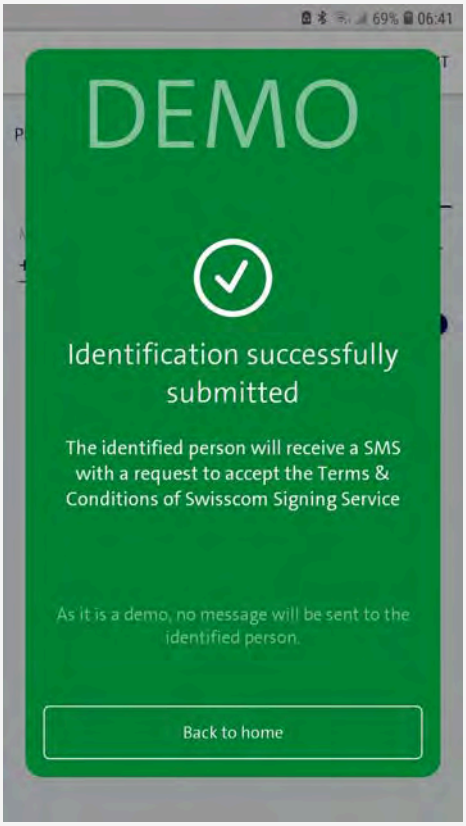
Step 10

After you have clicked on "Submit", you still have to sign the identification proofs you have just created. You do this via your mobile phone using Mobile ID or password/SMS-code.



Step 11

Finally the following message appears and you're done:



What does the RA agent need to be aware of when identifying?

The RA agent must check these 5 points:

Does the scanned ID information match the information in the presented ID document?

If not, the RA agent must **correct** or **add** this information.

Is the **photo on the ID document** a photo of the person you are currently identifying?

Is the **ID document still valid**, i.e. has it not expired?

Are there **no changes** to the ID document or **is it a forged ID document** (please check the security features, quality of the material, etc.)?

Were you able to verify that the person to be identified **actually owns** the given **mobile phone number**?

What do I do in any of the following situations?

If the person to be identified does not have a Swiss ID, identity card or passport with him/her,

- then you ask the person for such an ID document. If he/she does not have one, you cancel the identification and make a new appointment.
  Remember: Driving licences, working permits, foreigner's identity cards (Swiss permits B, C, G, etc.), paper copies of ID documents and other documents **ARE NOT PERMITTED** for the identification withthe RA app.

If the ID document presented is not stored in the RA app,

- then cancel the identification and inform your master RA agent.

If the scanned name of the person does not match the one in the ID document,

- then you correct or complete the incorrectly or incompletely scanned data in the RA App.

If the photo does not match the person in front of you,

- then you cancel the identification!

If the ID document presented is no longer valid, appears to be forged or stolen,

- then you cancel the identification!

If the call to the given cell phone number does not reach the person in front of you,

- then check the cell phone number and try again.

How does the authenticity check work?

In the Swisscom RA app you can see what an ID document **should look like**. During the authenticity check, the app shows you several **security features** that need to be checked **visually** or **palpable**.

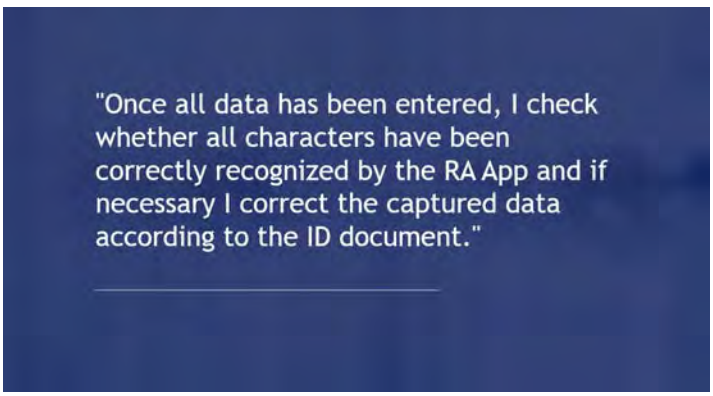
Move your mouse over the flashing hotspots to learn more about the individual fields.

1 Slightly incline the document. Then you will see that this area has a different appearance from different angles.

2 Move your finger over this area. You will notice that there is a palpable structure here.

1 Slightly incline the document. Then you will see that this area has a different appearance from different angles. You will also notice that there is a palpable structure when you move your finger over it.

What happens when all document data has been entered?



It's the responsibility of the RA Agent ...

- ... to enter the names and data **exactly** as they appear **in the ID document** and ...
- ... to **correct** the automatically entered data to exactly match the data in the ID document.

Notes

- No dots "." or commas "," may be entered in the names, as these lead to errors when signing. Simply replace dots and commas with spaces.
- Minus signs (hyphen "-") in names are allowed.
- Please do not enter titles (such as "Pd."), even if they are entered in the identity document, because titles are not part of names.

Why is the mobile phone number so important?

Do you have a spontaneous idea why the mobile phone number is so important?

Choose the right answer.

A) Because we can contact the person via WhatsApp.

B) Because the mobile phone number serves to identify the signing person.

C) Because we also access other personal data via the mobile phone number.

After completion of the identification, the mobile phone number is the **identity reference** of the signing person !

- It serves to **identify the user** before the electronic signature is triggered .
- The mobile phone number is used to obtain the **declaration of will** before signing.

After the identification ...

After the transmission of the ID data just recorded, the RA Agent confirms the **correctness of the data** by means of a digital signature.

The recorded data is stored securely and encrypted in a highly secure Swisscom data centre **in Switzerland**. This is an **audited process**.

No data from the identification process remains on the RA agent's mobile phone; all captured photos and data are **automatically deleted from the mobile phone**.

This is how you complete the process:

1. The identified person receives an **SMS** from Swisscom, which contains links to the t**erms of use of the Swisscom Signing Service** in the CH and EU versions.
2. The identified person **accepts** the terms of use with an **electronic signature**, which he/she confirms by means of **Mobile ID** or **password/ SMS code procedure**.

Can I try something with the RA App or show something?

Yes, you can, with

Demo-Mode

For the **login** to the RA App use the following data:

Mobile number: **+41 12 345 67 89**

Company identifier: **demo**

All other steps work exactly the same as described above. However, in demo mode, **no data** is transferred to Swisscom and **no SMS** is sent.

Questions:

Where is the data collected via the Swisscom RA App stored?

Choose the right Answer.

A) On the mobile phone of the RA agent
B) No data is stored
C) At Swisscom in a secure data centre
D) In a Public-Cloud

What do I have to check regarding the authenticity of the ID documents?

Choose the right answers.

A) The visual security elements (marked in red on the examples of ID documents in the RA app)
B) The checksum of the Machine Readable Zone (MRZ)
C) The haptic security elements (marked yellow on the examples of ID documents n the RA app)
D) Nothing. The Ra App checks everything automatically.

The scanned data does not match the data in the ID document, for example, the name is truncated or a date is incorrect. What are you doing?

Choose the right answers.

A) I'll leave it as it was scanned, so that's what it says in the MRZ.
B) I edit the name so that it exactly matches the information in the ID document.
C) I leave the possible abbreviation as it is in the MRZ.
D) I edit the date (date of birth or expiration date) so that it exactly matches the information in the ID document.

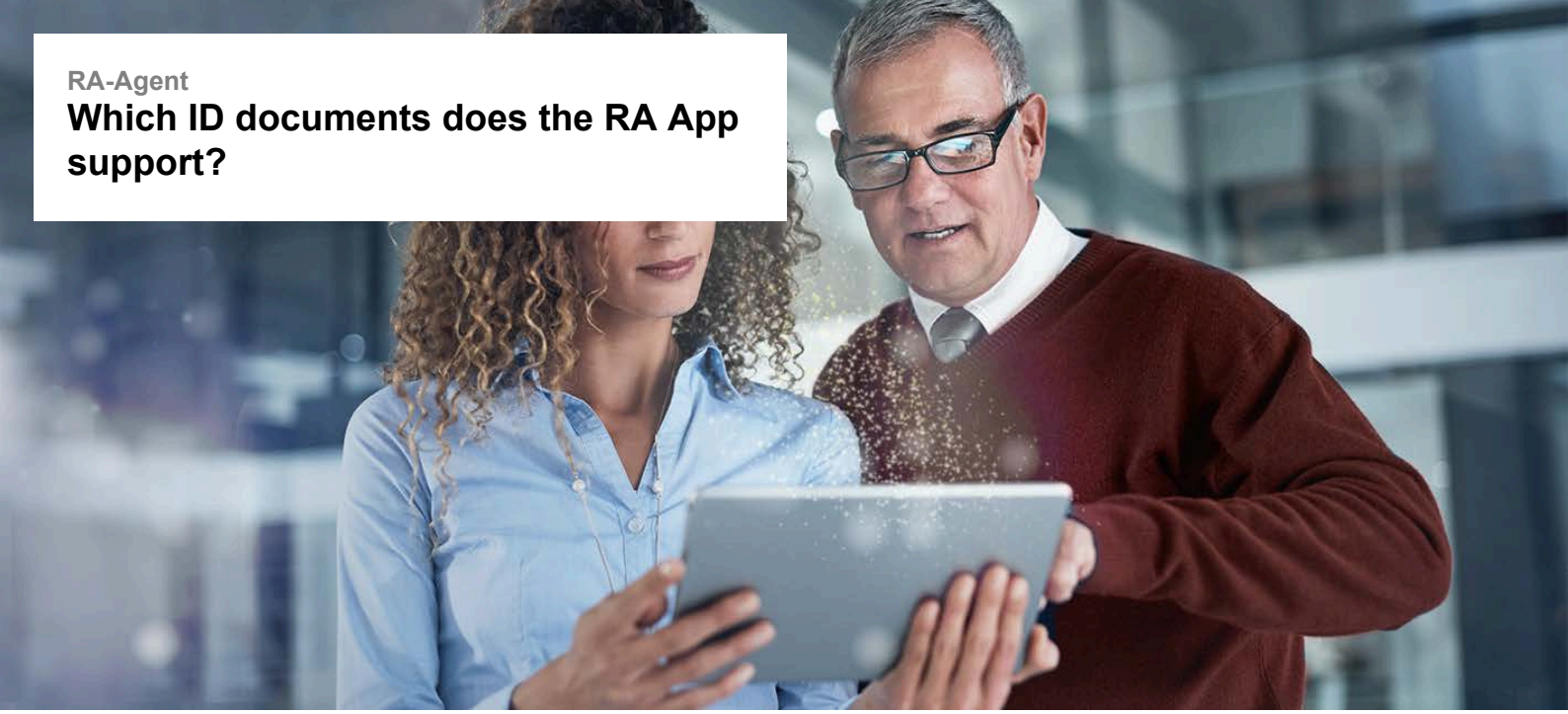
You identify a colleague and he asks you to enter his nick name as first name, for example "Mike" instead of "Michael". What do you do?

Choose the right answer.

A) I do him the favor, because I know him myself only under this name.
B) I refuse and point out to him that the names must be taken from the ID document.

RA-Agent

Which ID documents does the RA App support?



Which ID documents does the RA App support?

What do you think: Which ID documents must NOT be used for identification?

Please select the correct answers.

A) Foreigner's identity card
B) Passport
C) Driving License
D) Student card
E) Identity card
F) Refugee ID

The Swisscom RA App already supports **nearly all countries worldwide.** Nevertheless, it can happen that an ID document is **not listed in the RA App** .

If an ID document is presented for identification that is not available in the RA app, the RA agent must **reject it** and **cancel the identification!**

For the identification of a person with the RA-App only

- the **Swiss ID**
- **ID cards** of countries in the Schengen area
- **Passports**

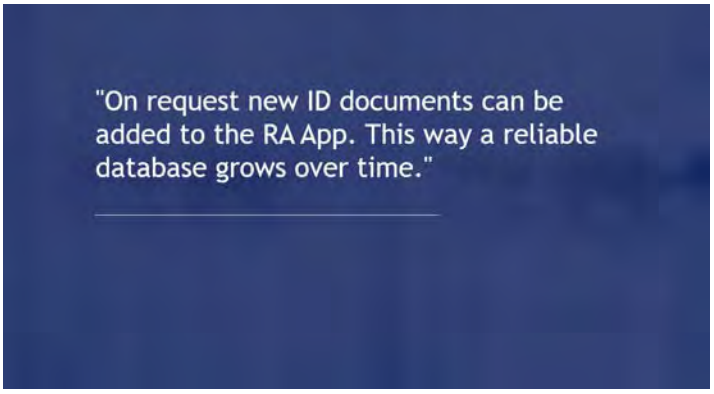
are permitted as ID documents, since the RA-App enables qualified electronic signatures and there are **strict legal requirements** for these.

- **Driving licences, foreigner's identity cards** or **other documents** are **NOT** permitted for the identification.
- Also **excluded** are **paper copies** of ID documents as well as identifications v**ia Teams or other online tools**.

These ID documents must also have a **machine-readable code (short MRZ)**, otherwise they **cannot** be used for identifications. Therefore, for example, the **Italian identity card in paper form** is not suitable for identification.

Which ID documents does the RA App support?

How does the RA Agent report ID documents that are not yet stored in the RA App?



- The RA Agent turns to the person who registered him as RA Agent (the so called **Master RA Agent**)
- The Master RA Agent contacts **Swisscom** via his well-known support channel.
- Only if the corresponding ID document is available in the RA App, the **applicant can be identified**.

Questions:

Which ID documents are supported by the RA App?

Please select the correct answer.

A) Only ID documents that are approved for identification for signing with QES: Swiss ID; ID cards from the Schengen area and passports.

B) All ID documents with a photo of the person.

C) The new foreigner's ID cards with biometric data.

What do I do if I the applicant presents an ID document that does not exist in the RA-App?

Please select the correct answer.

A) I select a similar ID document and try to capture the ID document with it.

B) I abort the identification and report the missing ID document in the RA App to my Master RA Agent.

RA-Agent

What should be done if the data of an identified person changes?

What happens if the data of an identified person changes?

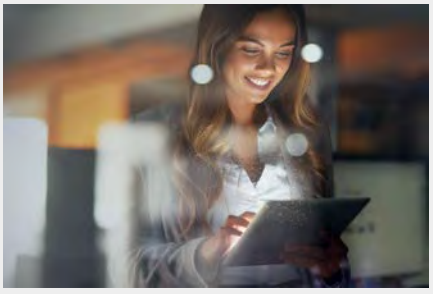
Then the person needs to be **re-identified**.

The data changes when ...

... the name changes.

... the ID document (ID Card or passport) expires.

... the mobile phone number or the provider changes.



... a new password for the password/ SMS-code procedure is set.

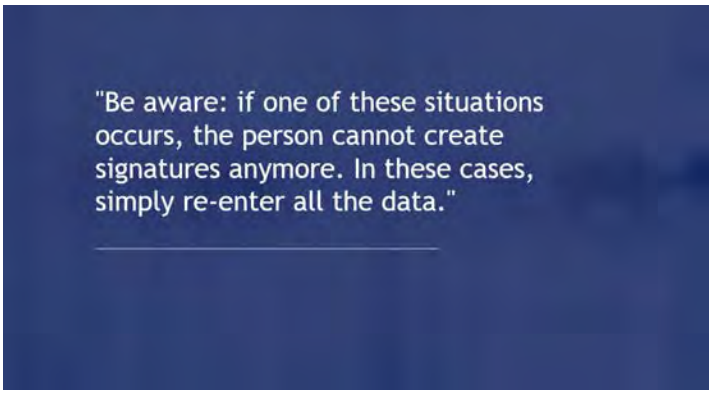
... a new SIM card is used or a new Mobile ID PIN (CH-SIM) is set *

... the Mobile ID app is activated *

What should be done if the data of an identified person changes? 27

***** When using **Mobile ID**, re-registration after password reset, after inserting a new SIM card or activating the Mobile ID app can be **avoided** if the user has a **Mobile ID recovery code**.

1. Ask the person you want to identify to activate the Mobile ID **BEFORE** the identification: https://www.mobileid.ch > " **Activate now**".
2. The person should then generate her recovery code: " **Generate recovery code**".
3. Now you can execute the identification
4. The recovery code must be **kept in a safe place** and used when activating or resetting the Mobile ID.



How will the data be newly recorded?

The new registration is quite simple:

- Repeat the identification with the Swisscom RA App. That is, perform all steps as if it were the **first identification** .
- Then all signatures of the user are based on the **new, updated data**.

Question:

In which event must the data of the identified person be newly recorded?

Please select the correct answer.

A) new mobile phone number
B) new surname (family name)
C) ID document expired or lost/stolen (a new ID document had to be issued)
D) for all above mentioned

RA-Agent

Information on data protection regulations and closure

Which data protection regulations apply to the Swisscom RA Service?

Which requirements result from data protection?

1. Only such personal data shall be processed that is **necessary to fulfil your tasks as a RA agent**.
2. In Switzerland, the ***Federal Act on Data Protection*** **FADP** applies.
   (according to Art. 2 (e) of the Swiss Signature Act)
3. In the EU the ***General Data Protection Regulation*** **GPDR** applies.

What does "data processing" actually mean?

Data processing includes ...

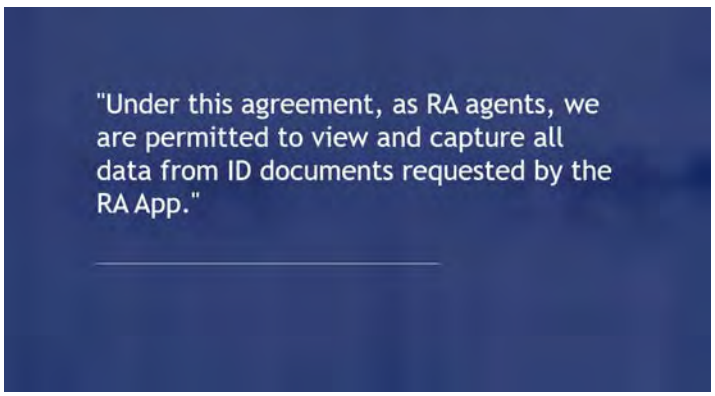
... any processing of **personal data**, independently from the methods or procedures used, in particular the **collection, storage, use, change, disclosure, archiving or deletion of data.**

(according Art. 3 (e) Federal Act on Data Protection)

The Swisscom RA Service ensures that the data is stored in accordance with the requirements of the **Swiss Signature Act** (ZertES) and the **FADP**.

The Service is also compliant with the **GPDR of the EU**. The organisation of the RA agent (the so-called RA agency) completes an agreement covering the data processing of the data that is relevant for the fullfilment of the service (ADV).

The so-called "Duties of the RA Agent" are the basis for the activity as a RA agent. All RA Agents are asked to accept these when they are appointed. By doing so, they confirm to comply with these "Duties of the RA Agent" at all times.



One last question:

After the identification process, is the information stored on the RA agent's mobile phone?

Please choose one response.

A) Sure, otherwise these data would be lost.

B) No, the data are directly transmitted to Swisscom.

No information from the identification process is stored on the RA agent's mobile phone, **not even the photos**.

In the RA app, a RA agent only sees the **anonymized mobile phone numbers** of the last persons he identified.

Well done!

If you have followed the suggested order of the learning cards, this will be your last one.

And now what?

1. Upon successful completion of the training, you will receive an SMS with a link through which you will have to accept your duities related your activity as a RA Agent.
2. After accepting the "Duties of the RA agent", you will receive a confirmation SMS, which will also tell you your company name.
3. Download the RA App ("Swisscom RA") from the App Store, start it and authenticate yourself with your cell phone number and the company name provided to you by SMS.

Now you can start identifying.