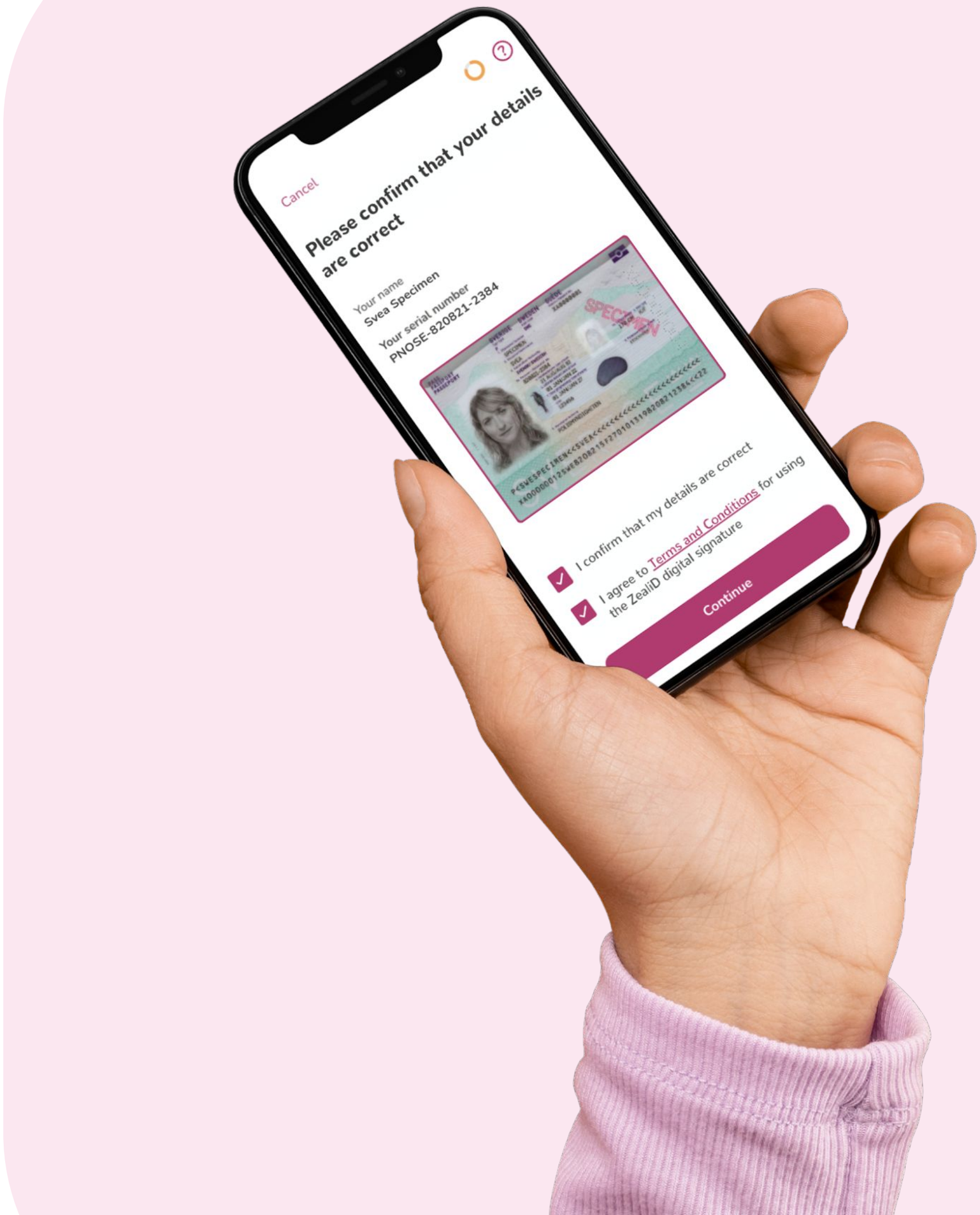
ZealiD

ZealiD Handbook

In this handbook you will find information about ZealiD, how to get a qualified certificate, how it works and answers to frequently asked questions.



www.zealid.com

ZealiD

Table of Contents

ZealiD

1. Qualified Trust Services

Electronic trust services guarantee secure and trustworthy electronic transactions. These transactions are legally valid and are recognized at the European level.

Qualified Trust Services include:

1. Certificates for electronic signatures or for electronic seals;
2. Certificates for website authentication;
3. Electronic time stamps;
4. The validation of electronic signatures or electronic seals;
5. The preservation of electronic signatures or electronic seals;
6. Electronic registered delivery.

1.1. Electronic Identification, Authentication and Trust Services (eIDAS)

The regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, which is commonly known as the “eIDAS-Regulation”, was introduced in 2014 and has been fully in force since 1st July 2016. On 29th September 2018 a major milestone was reached, as the EU-wide recognition of notified eID-schemes started.

Qualified Trust Service Providers (QTSP) comply with the eIDAS framework to ensure secure electronic transactions.

eIDAS

1.2. Trusted List

The Member States of the European Union and the European Economic Area publish a list of specifically accredited qualified trust service providers and information related to the qualified trust services provided by them.

EU Trusted List

1.3. EU Trust Mark

According to the European Commission, the EU trust mark gives assurance that the providers of electronic trust services and the trust services offered by them are qualified and comply with the rules set out in the eIDAS Regulation. This ensures a high quality of trust services which are regulated throughout the EU.

ZealiD

2. ZealiD Service

2.1. What is ZealiD?

ZealiD is a Qualified Trusted Service Provider specializing in issuing eIDAS qualified certificates, signatures, and time stamps. Qualified electronic signatures are legally binding and accepted EU-wide.

In addition, ZealiD is certified as a Registration Authority (RA), meaning that we provide identification services. Identification services are provided remotely.

ZealiD is supervised by three main authorities:

1. Swedish Post and Telecoms Authority (PTS);
2. Swedish Authority for Privacy Protection (IMY);
3. our Conformity Assessment Body (CAB).

2.2. Qualified Electronic Signatures

ZealiD issues qualified electronic signatures (QES) which are legally binding and have the same legal effect as handwritten signatures. Qualified electronic signatures ensure the highest level of identity verification since they are hard to forge in contrast to handwritten signatures and other digital signature types, which do not have qualified status. ZealiD's qualified certificates carry a Qualified Time Stamp (QTS). It serves as reliable proof to the relying party, indicating at what time a document was signed.

2.2.1. Expiration

The maximum certificate validity is two years. Documents signed before the expiration date of a signature are still valid, but a user will not be able to sign new ones. In that case, a user should register once again to obtain a new and valid electronic signature.

2.2.2. Qualified Electronic Signature on a Document

A qualified electronic signature is a digital signature. Adobe Reader is a commonly used and easily accessible tool. Besides their main functionality, it also gives information on whether a file contains any signature(s). Such information can be found under the Signature Panel section. It allows a user to check the validity and integrity of an electronic signature and see all details about the certificate, Trusted Service Provider, etc.

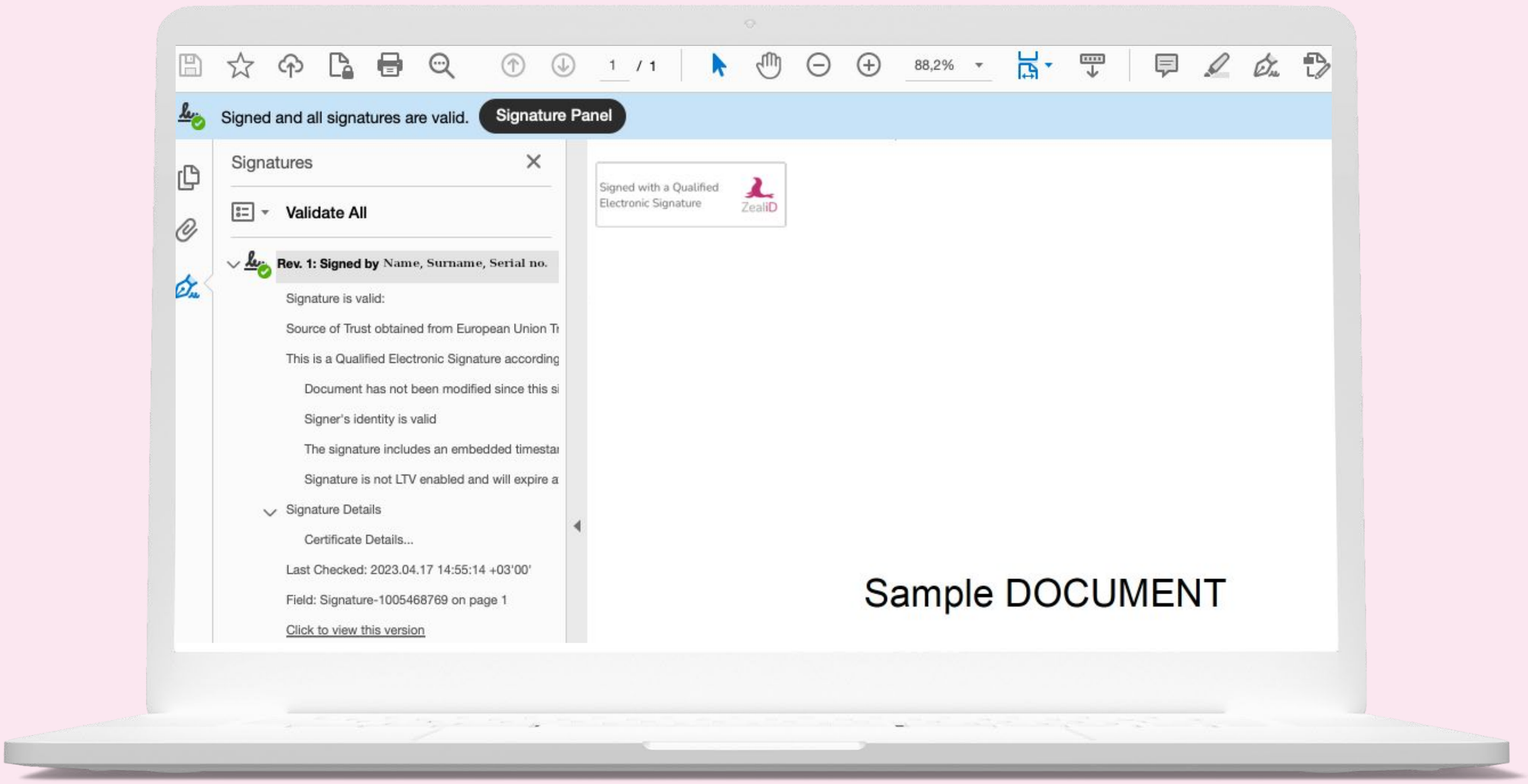
2.2.3. Validity

There are certain practices for checking the validity of qualified electronic signatures. The two main practices are provided next.

ZealiD

1 Adobe Reader

When a user opens a file containing qualified electronic signatures via Adobe Reader, the system automatically indicates whether the document and qualified electronic signatures are valid.



A signed file preview via Adobe Reader

ZealiD

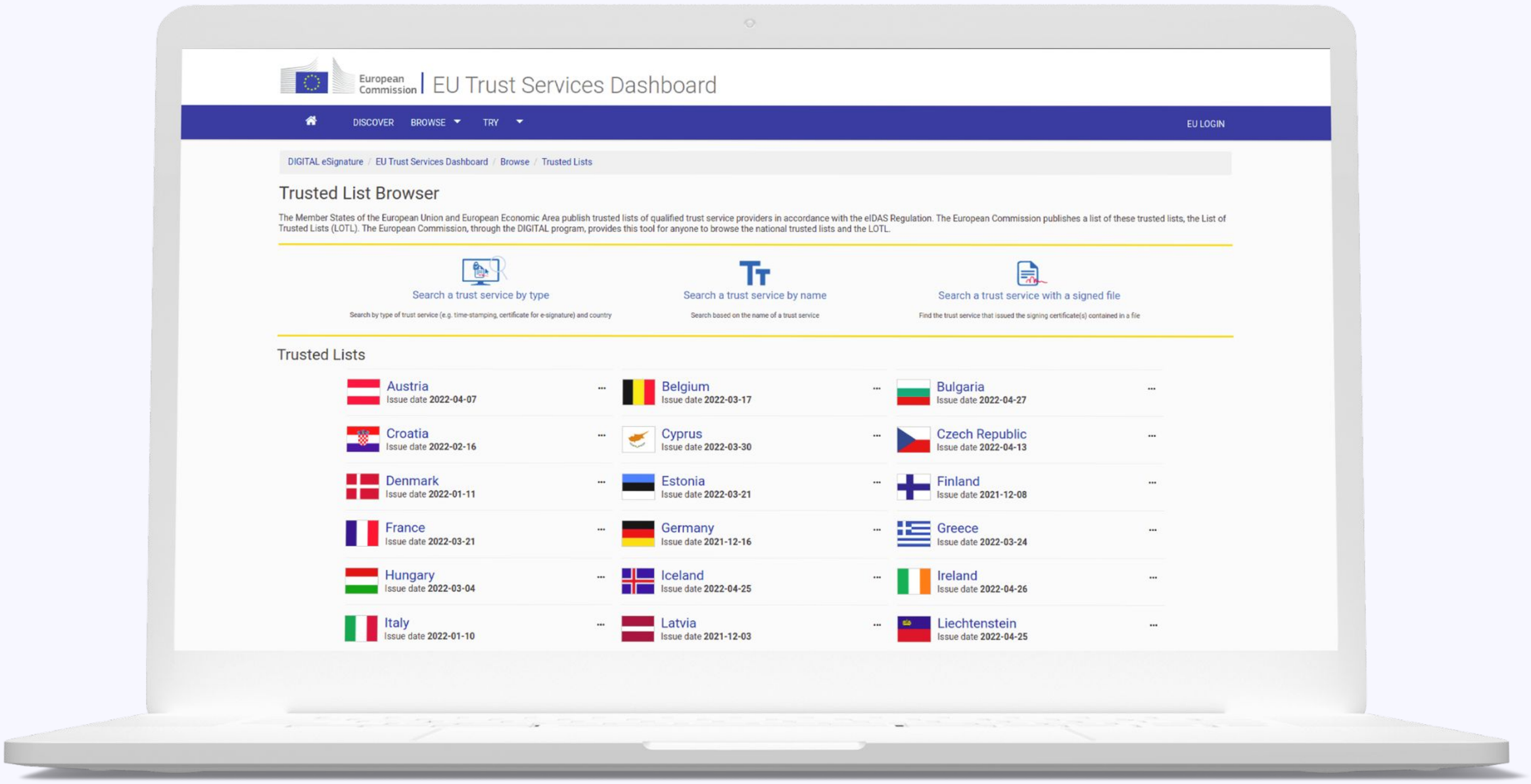
2 Qualified Validation Services

Article 32 of the eIDAS Regulation describes the requirements for the validation of qualified electronic signatures. There are certain steps included in the validation process:

- The verification of the integrity of the data;
- The verification of the validity of the certificate;
- The verification of the qualified status of the certificate;
- The verification if the signature was created by a qualified electronic signature creation device.

Some qualified trust service providers specialize in validation services. QTSP status granted to certain providers guarantees that the provider follows eIDAS requirements; therefore, the user of the service benefits from higher legal certainty.

By using the Trusted List browser, a user can find a provider for the validation of qualified electronic signatures.



EU Trust Services Dashboard

Once the Trusted List Browser is opened, a user selects which services they would like to see. The qualified validation service for qualified electronic signatures can be filtered accordingly.

2.2.4. Revocation

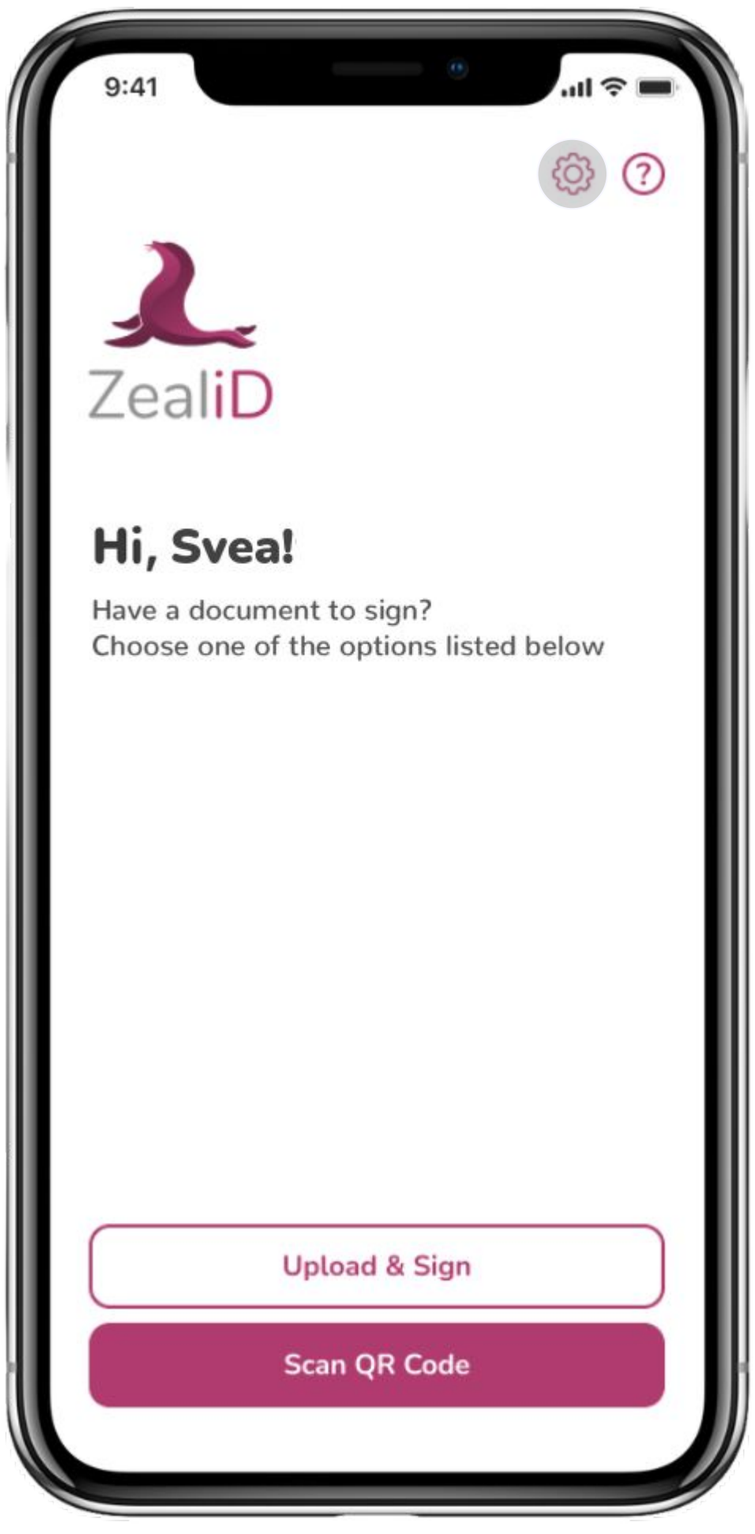
A qualified certificate may be revoked for a variety of reasons. Such situations include changes in one's name, mobile device theft, losing a mobile device, or replacing it with a new one.

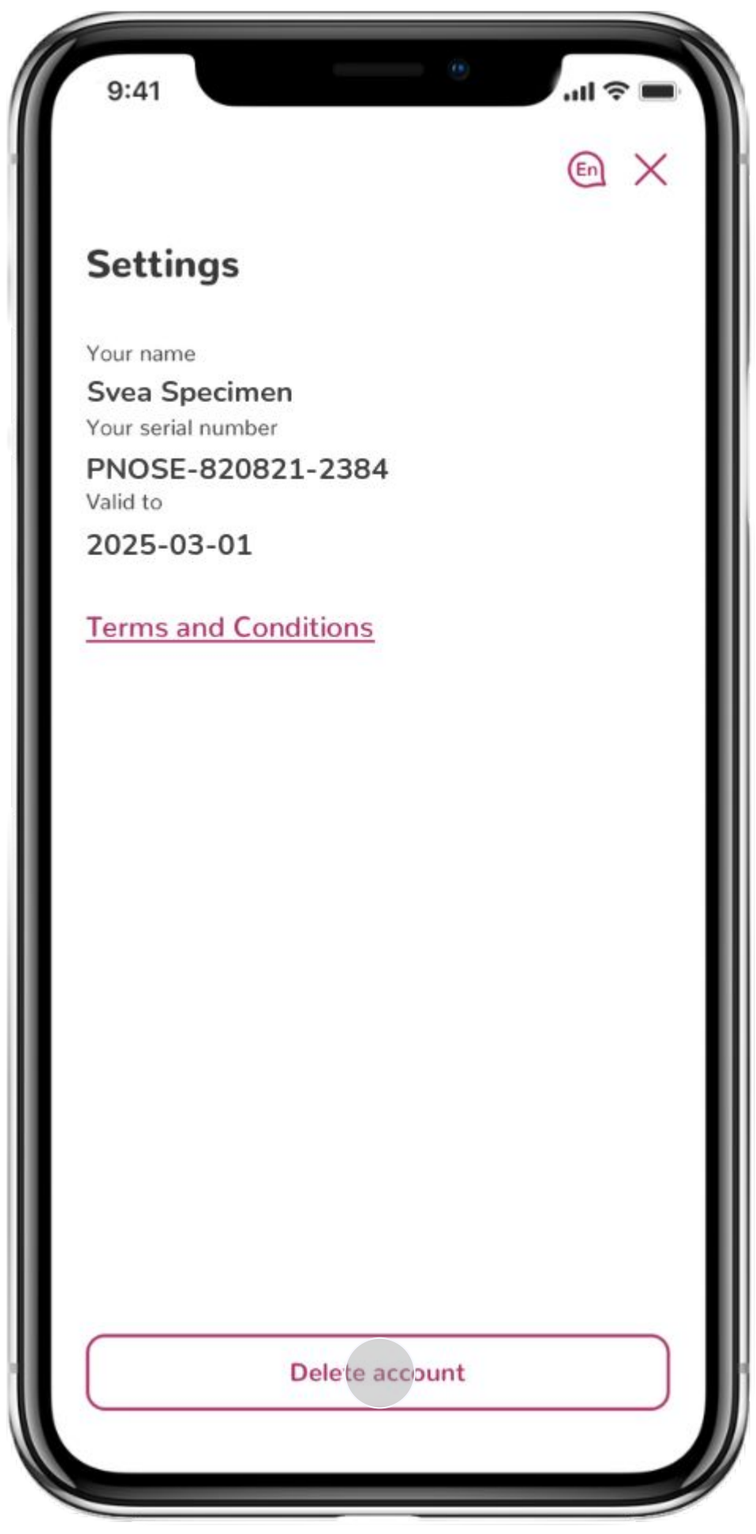
It is important to highlight that once a certificate is revoked, it will no longer be possible to reinstate it. However, the documents that have been previously signed using a qualified electronic signature will remain valid.

There are three possible ways to revoke a qualified certificate issued by ZealiD:

1 Revocation via ZealiD mobile app

- Open the ZealiD mobile app and click on the “Settings” icon (marked in gray);
- Tap on “Delete account” (marked in gray);
- Click “Ok” in a pop-up table;
- Confirm revocation with biometric authentication (Face ID or Touch ID).





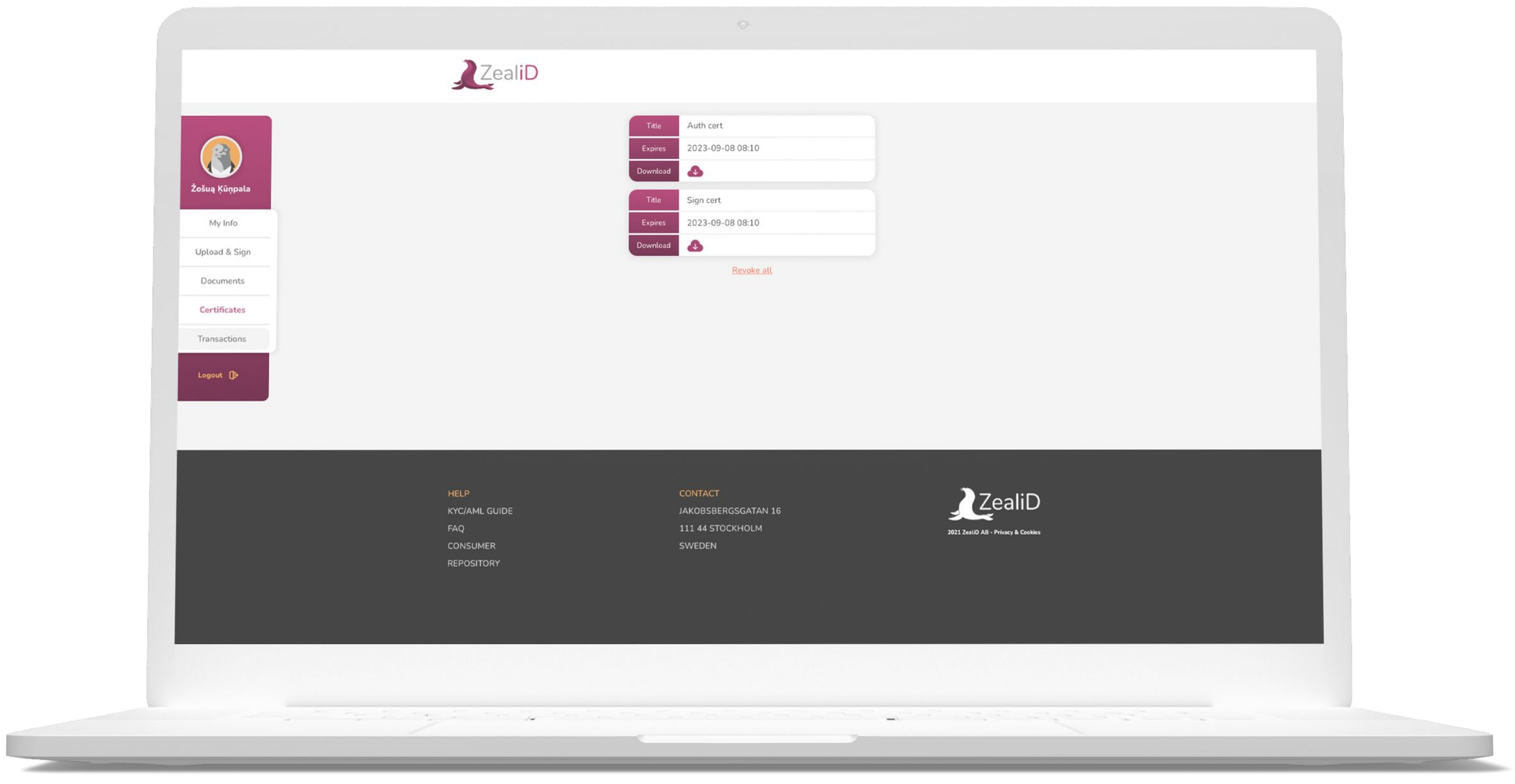
ZealiD

2 Revocation via My ZealiD portal

My ZealiD

- Open the ZealiD mobile app on your phone and go to my.zealid.com on another device (e.g., laptop);
- Press the “Scan QR code” button in the mobile app and scan the QR code presented at my.zealid.com to access the user’s portal;

- Click on “Certificates” and select “Revoke all”;
- Confirm revocation by clicking “Revoke all” in a pop-up table.



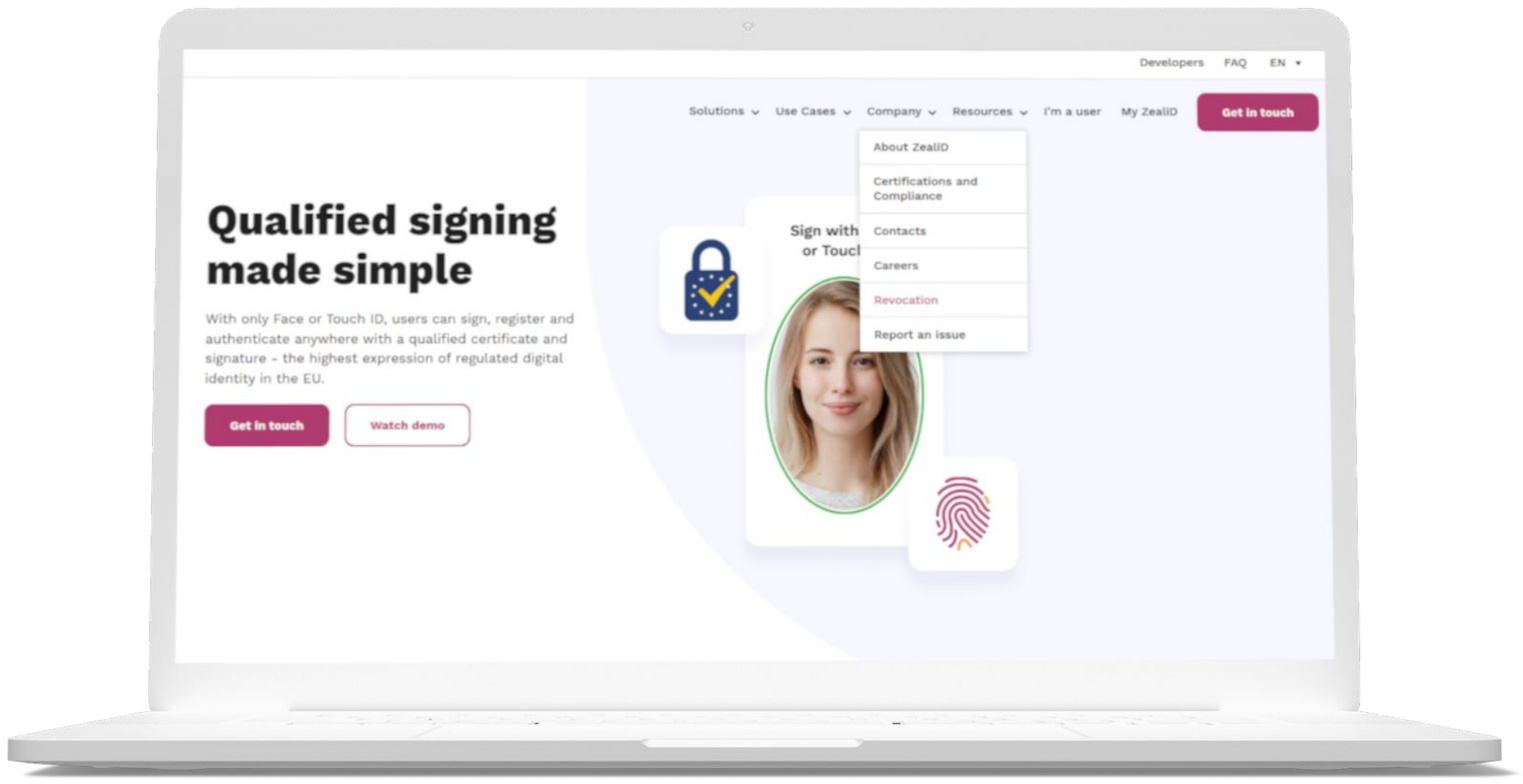
ZealiD

3 Revocation form online

Revocation

There is a way to revoke a certificate online. It is recommended in cases where access to the mobile device that was used to obtain a certificate is no longer available.

- Go to zealid.com, click on “Company“ and select “Revocation”;
- Fill in and submit the Revocation Request form;
- The request will be carried out within 24 hours by the ZealiD Team;
- Once the revocation process is complete, a confirmation of certificate revocation will be sent via email.



Revocation form online

www.zealid.com

ZealiD

2.3. Coverage

While supporting 26 countries in the EU, ZealiD is expanding its global coverage to support as many users as possible.

Coverage

2.3.1. Supported Identity Documents

ZealiD supports passports, ID cards, and residence permits. Currently, over 150 different document models are accepted.
ID documents are removed from the supported list when they are out of circulation and new models are added.

Supported ID

2.4. Registration

Registration is performed remotely. Two things are required to obtain a qualified electronic signature from ZealiD:

- Mobile device with biometric authentication (Face ID or Touch ID);
- Supported ID document.

Being a non-EU citizen, a user is required to have:

- Mobile device with biometric authentication (Face ID or Touch ID);
- European or American phone number;
- Supported ID document.

2.4.1. How long does the registration take?

Self in-app registration typically takes around 3 minutes. Additionally, each application has to go through a manual review process that may take up to 5 minutes.

2.4.2. Service Hours

Users can download the ZealiD mobile app and register at any time. However, our manual vetting service is available:

Monday-Friday 7:00-19:00 CET
Saturday-Sunday 11:00-16:00 CET

Users will not be able to receive final approval outside of service hours. If users have already registered via the ZealiD mobile app, they can use it for authentication and signing at any time.

ZealiD

3. Security

- Infrastructure is hosted on our own hardware and servers, located in certified data centers with 24x7 guards on site and video monitoring;
- Signing operations are performed on dedicated servers;
- The actual cryptographic key operations are performed on certified Hardware Security Modules;
- Administration of the cryptographic devices requires physical presence of multiple authorized users, with credentials on individual smart cards;
- During registration, a secure TLS channel based on cryptographic certificates is established between the app and our back-end servers;
- This communication is encrypted and verified;
- Cryptographic secrets on the mobile phone are stored in its native local secure hardware storage.

4. Privacy and Data

4.1. Data Processing

Data categories	Purpose for data processing	Purpose for data processing
Users of ZealiD Mobile App	Obtain contact data	Consent & necessity for compliance with a legal obligation
Users applying for the qualified certificates and electronic signatures	Identify and verify user's identity	
Subscribers to whom the qualified certificates and electronic signatures are being issued	Ensure compliance for the evidence package	

4.2. Data Retention Periods

Registration Authority:

- Registration data - 12 years from the registration date;
- Events' logs of service usage - 10 years since the event.

Certificate Authority:

- No less than 14 years from the registration;
- In case certificate validity terminated - no less than 12 years since the certificate termination date;
- In case ZealiD activity terminated - no less than 12 years from the termination date.

ZealiD

5. ZealiD Mobile App

Purpose

ZealiD, as a Qualified Trust Service Provider, is obliged to identify people to whom it issues certificates. This requirement is known as “Know Your Customer” (KYC) and it is an essential process for a business verifying the identity of its clients.

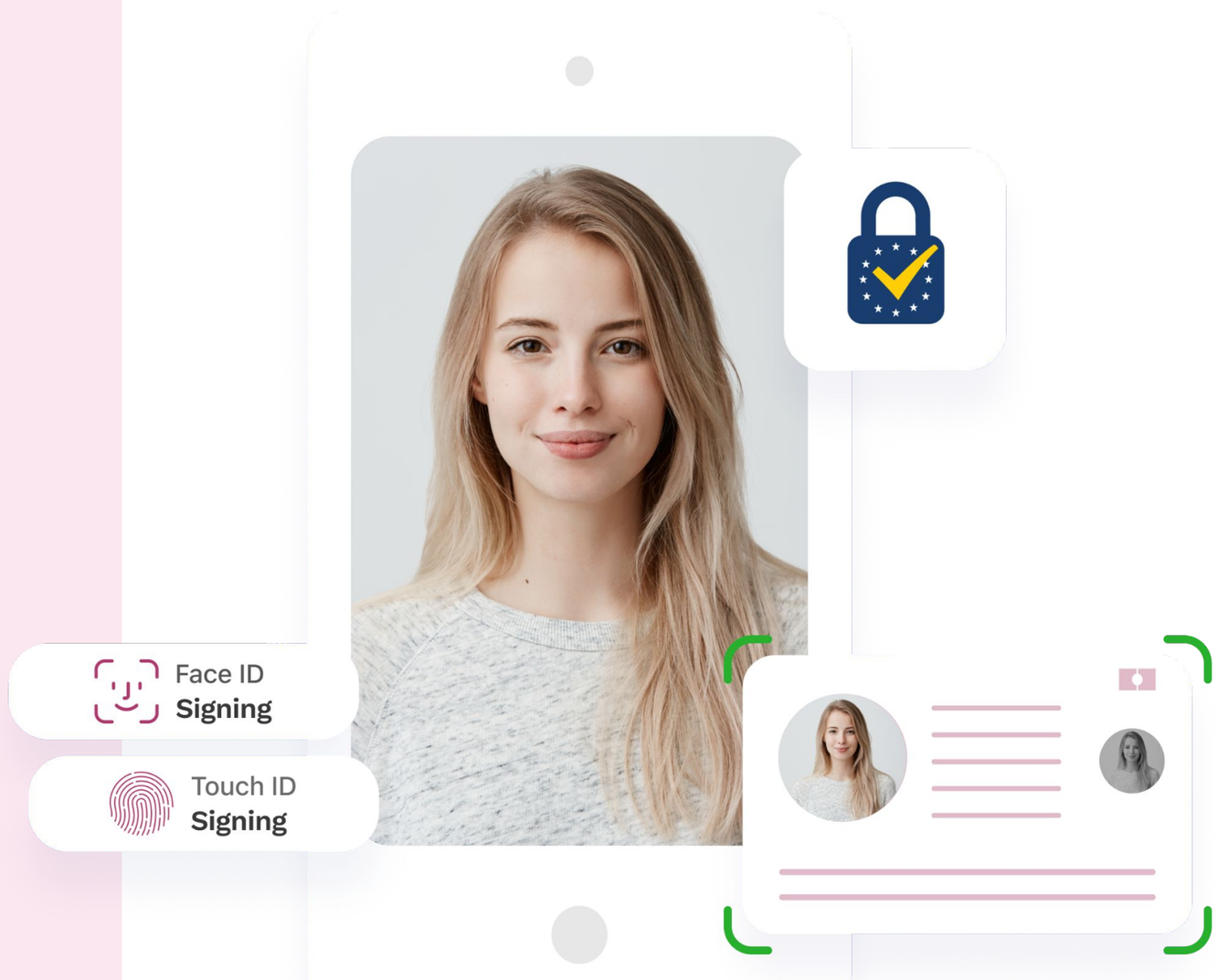
Registration Process

The registration process is performed remotely within the ZealiD mobile app. First-time users need to perform the registration process to identify themselves (registration process for iPhone users is pictured next). A registered user will be able to use qualified electronic signatures right away.

Download your ZealiD

GET IT ON Google Play

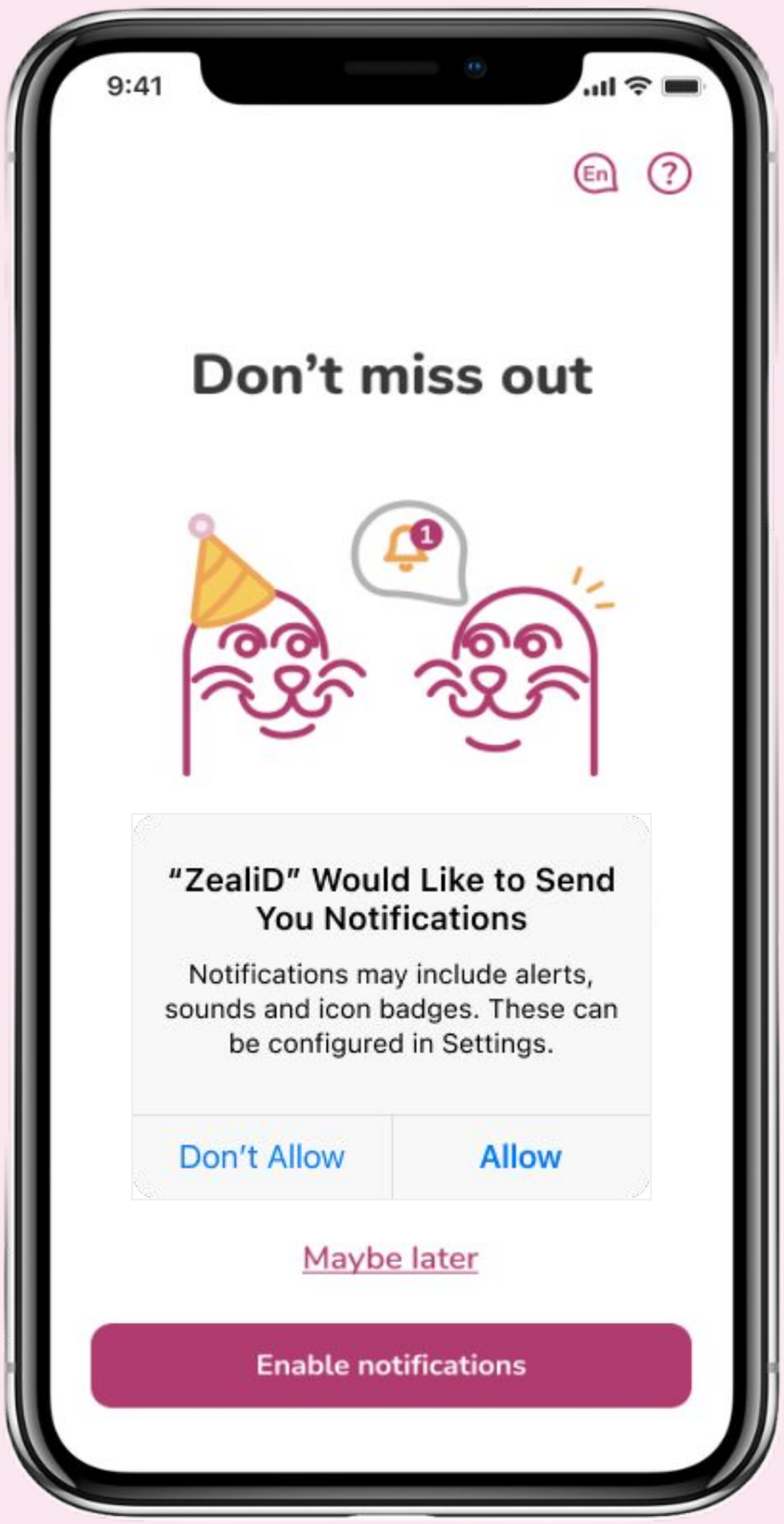
Download on the App Store



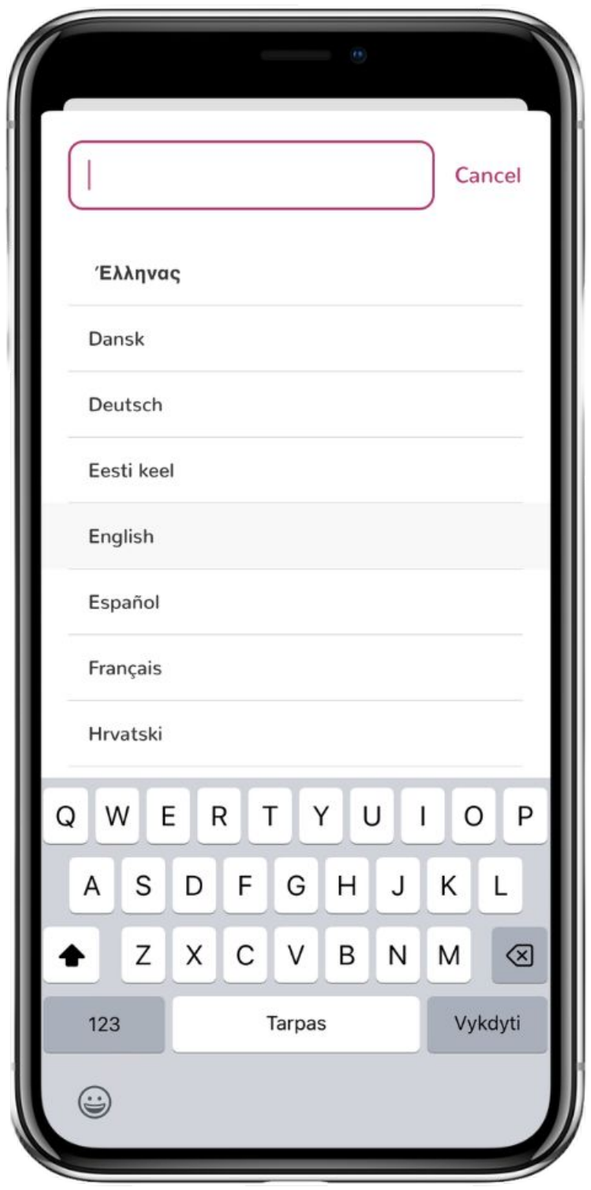
ZealiD

1 Enable Notifications

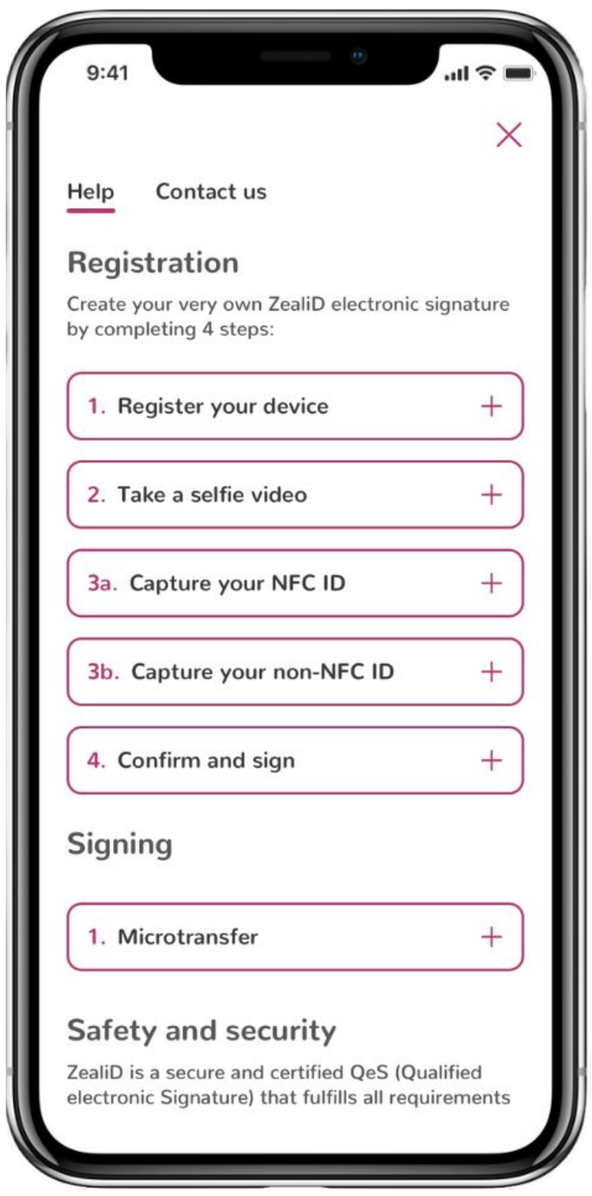
Open the ZealiD mobile app. Get ready to register by enabling push notifications to receive them once a submitted application is reviewed and a qualified electronic signature is ready to be activated.



Select Language



Help Center and Contact Page

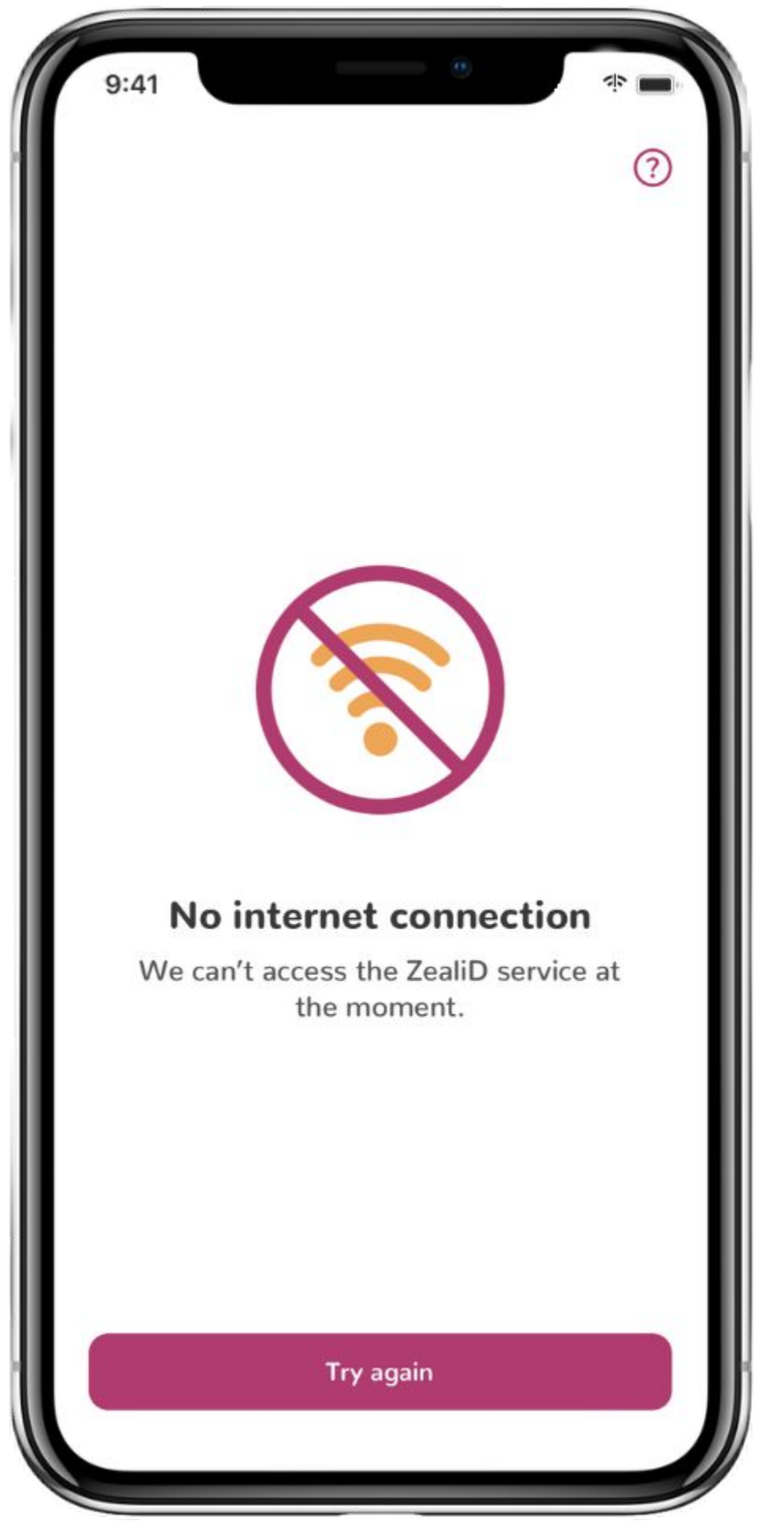


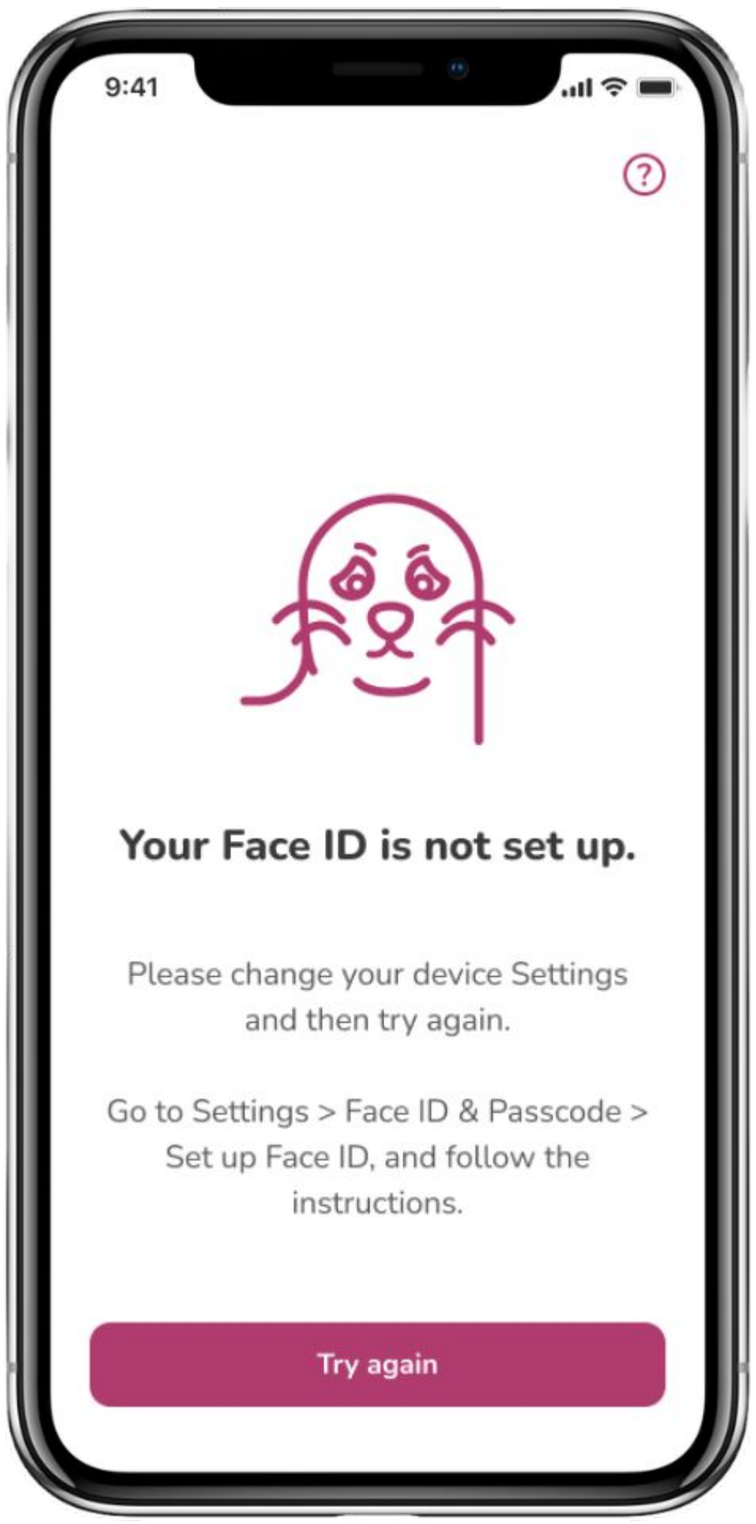
ZealiD

Possible errors

No internet connection

To use the ZealiD mobile app, an internet connection must be available (mobile data or Wi-Fi). Enable it to proceed with registration.





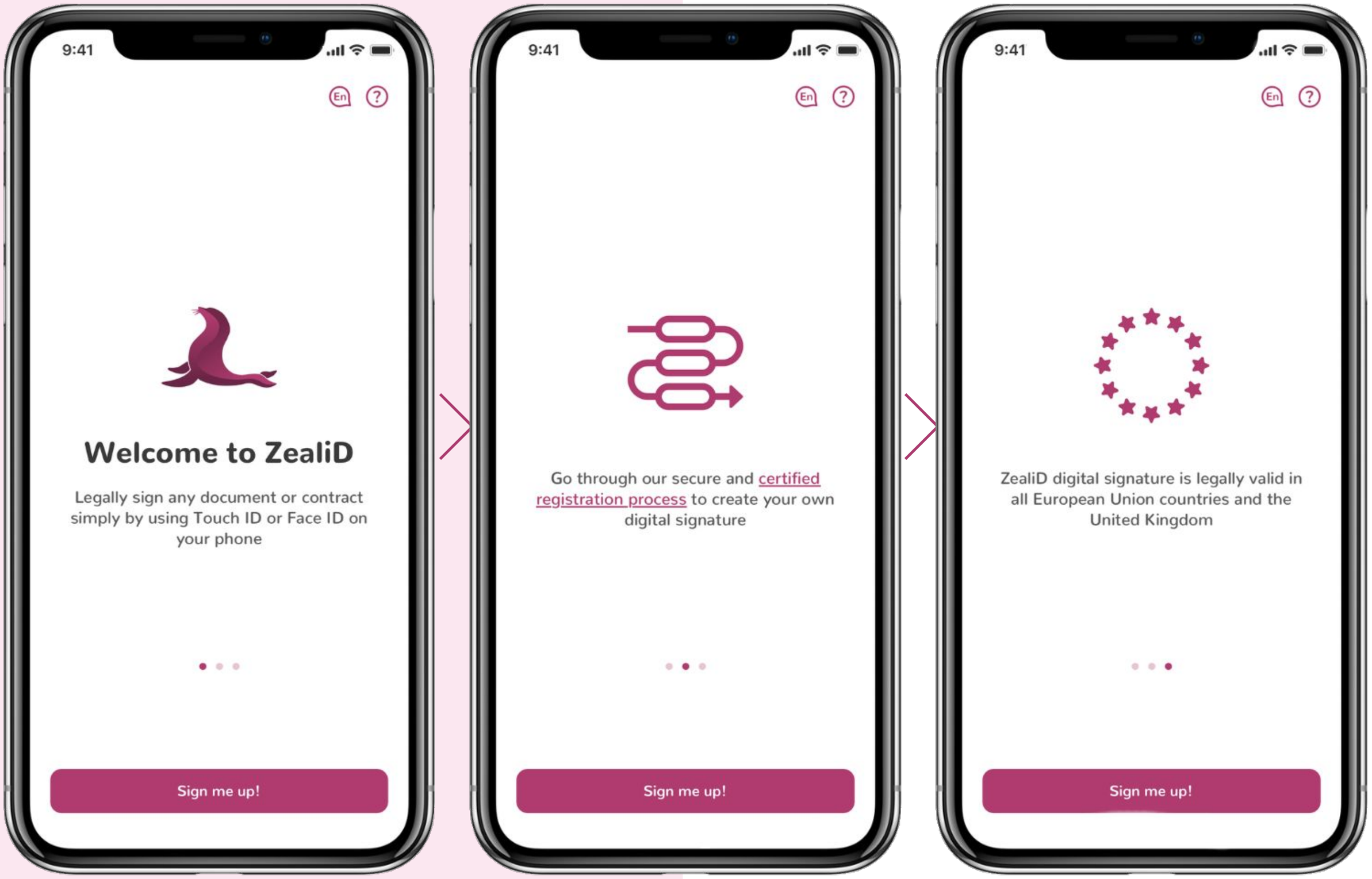
Biometrics are not set up

To be able to use the ZealiD mobile app and authorize qualified signatures, Face ID or Touch ID must be enabled and functional on the mobile device. Enable biometric authentication on your device and continue with the registration process.

ZealiD

2 Get to know ZealiD

Get familiar with ZealiD, qualified electronic signature, and its benefits. Click “Sign me up!”

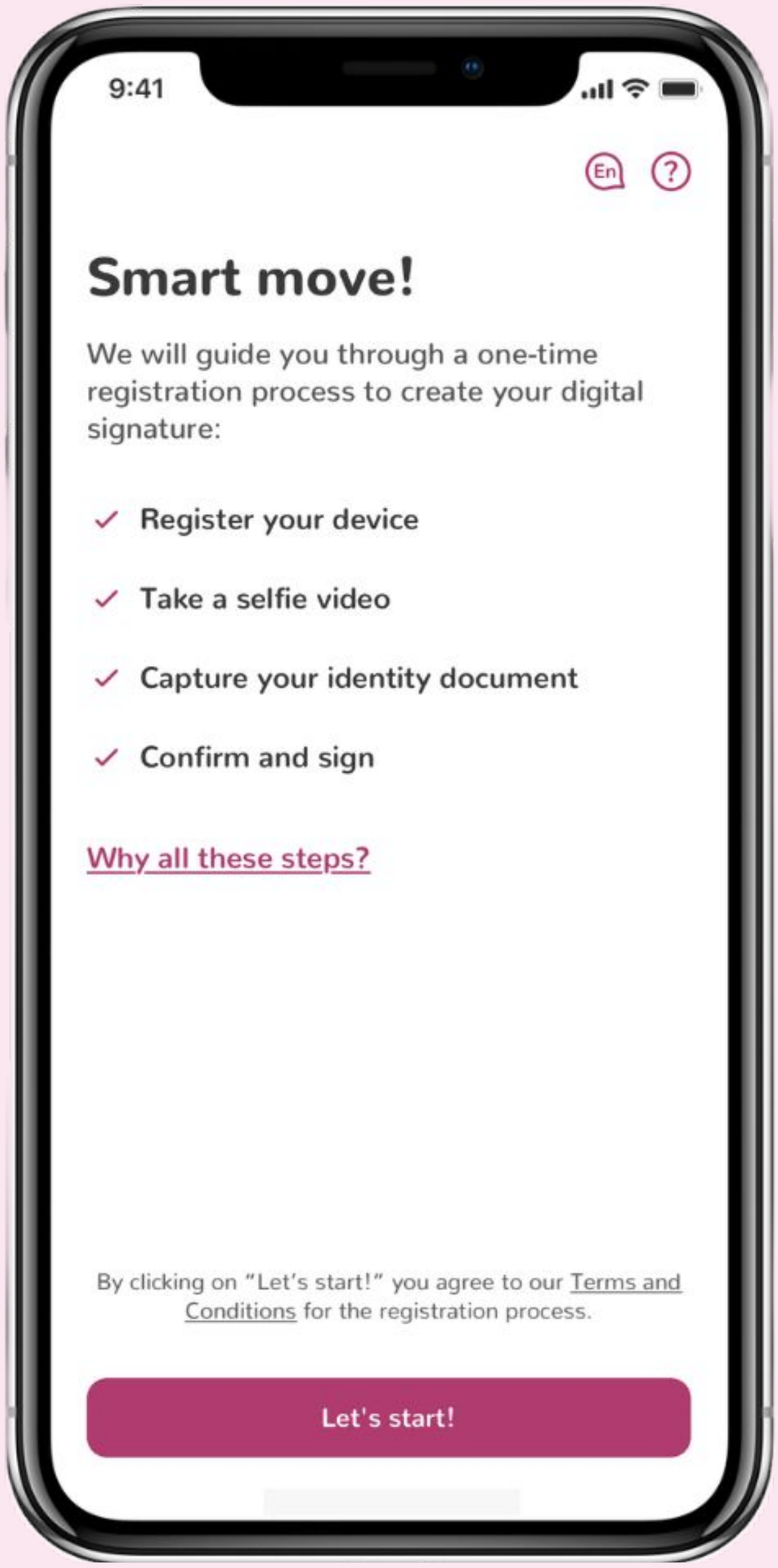


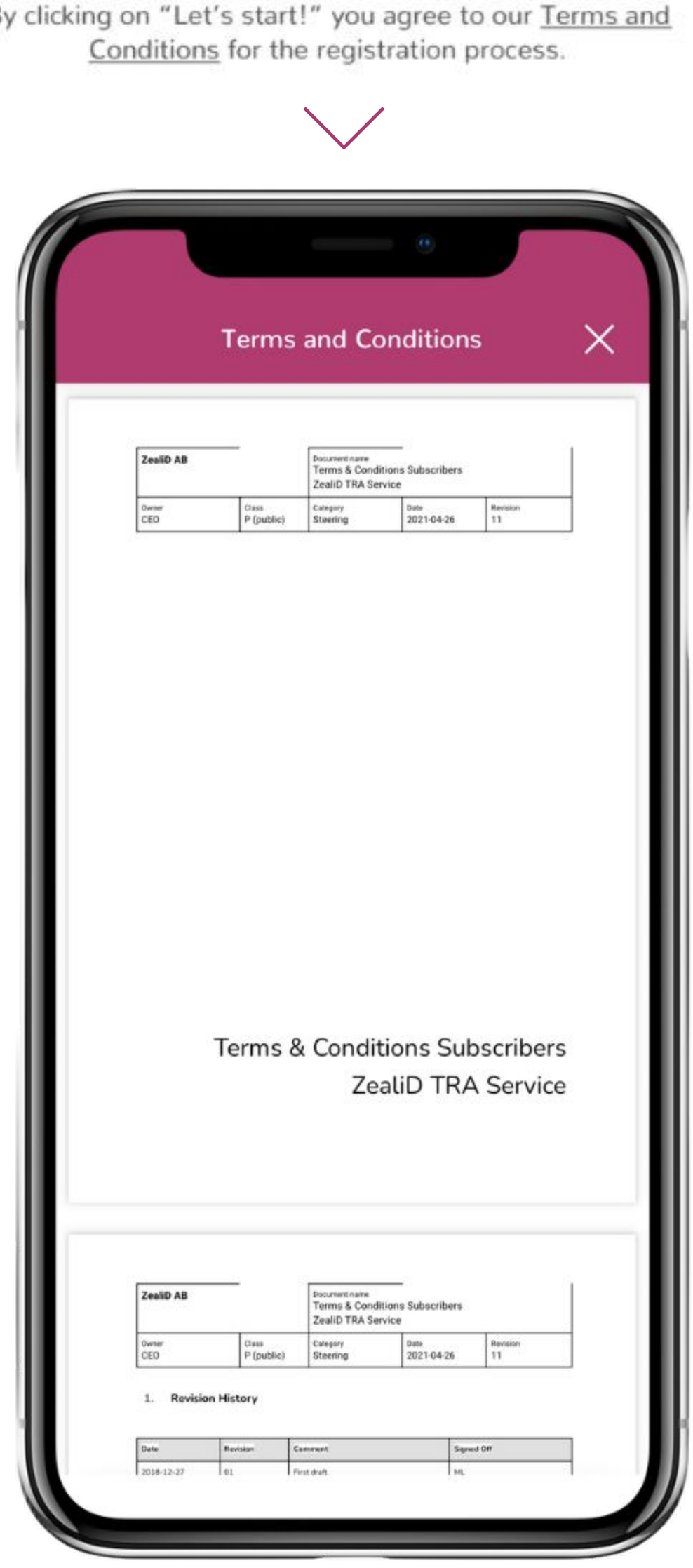
ZealiD

3 Get to know the registration process

By clicking “Why all these steps?”, you will be redirected to the Help Center.

Get familiar with the Terms & Conditions and click “Let’s start!”.



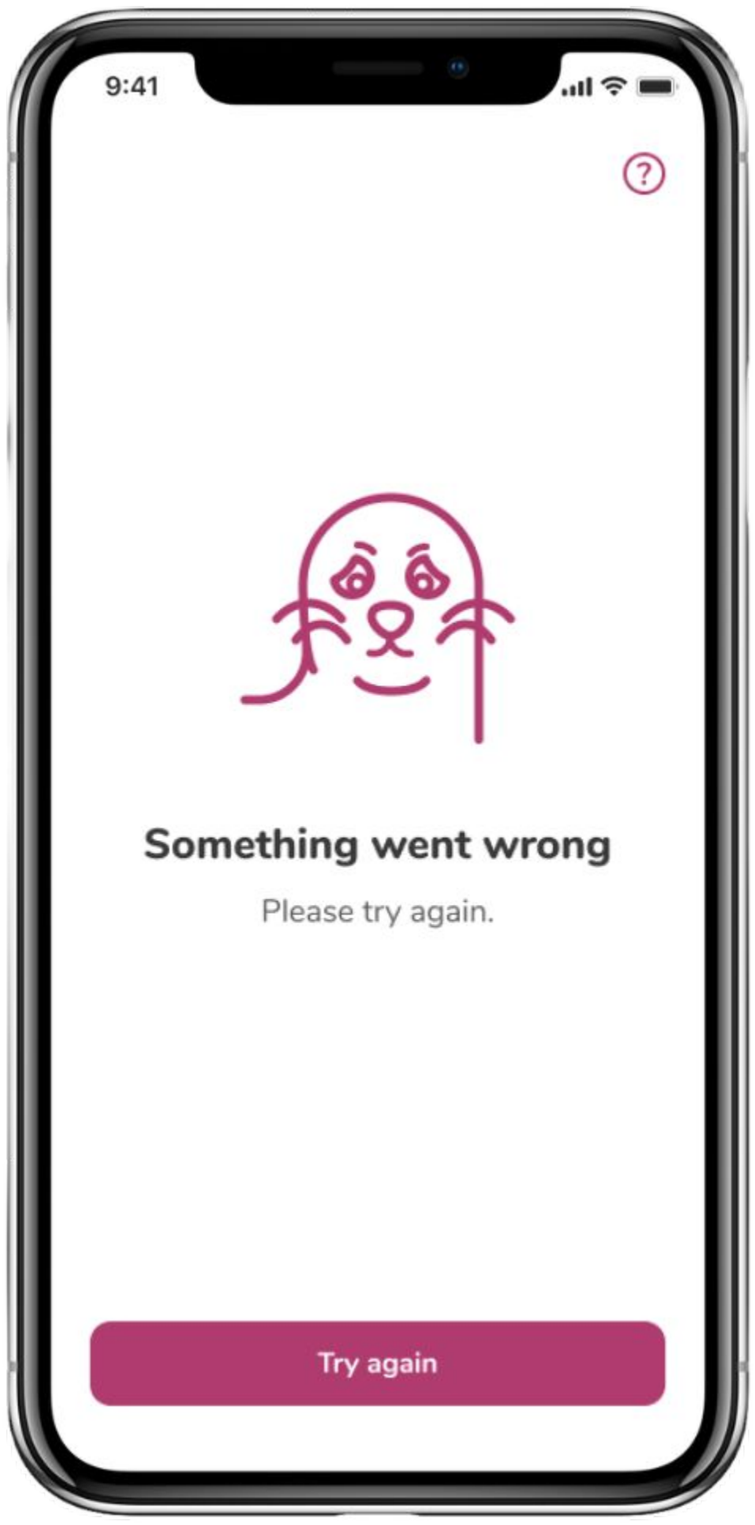


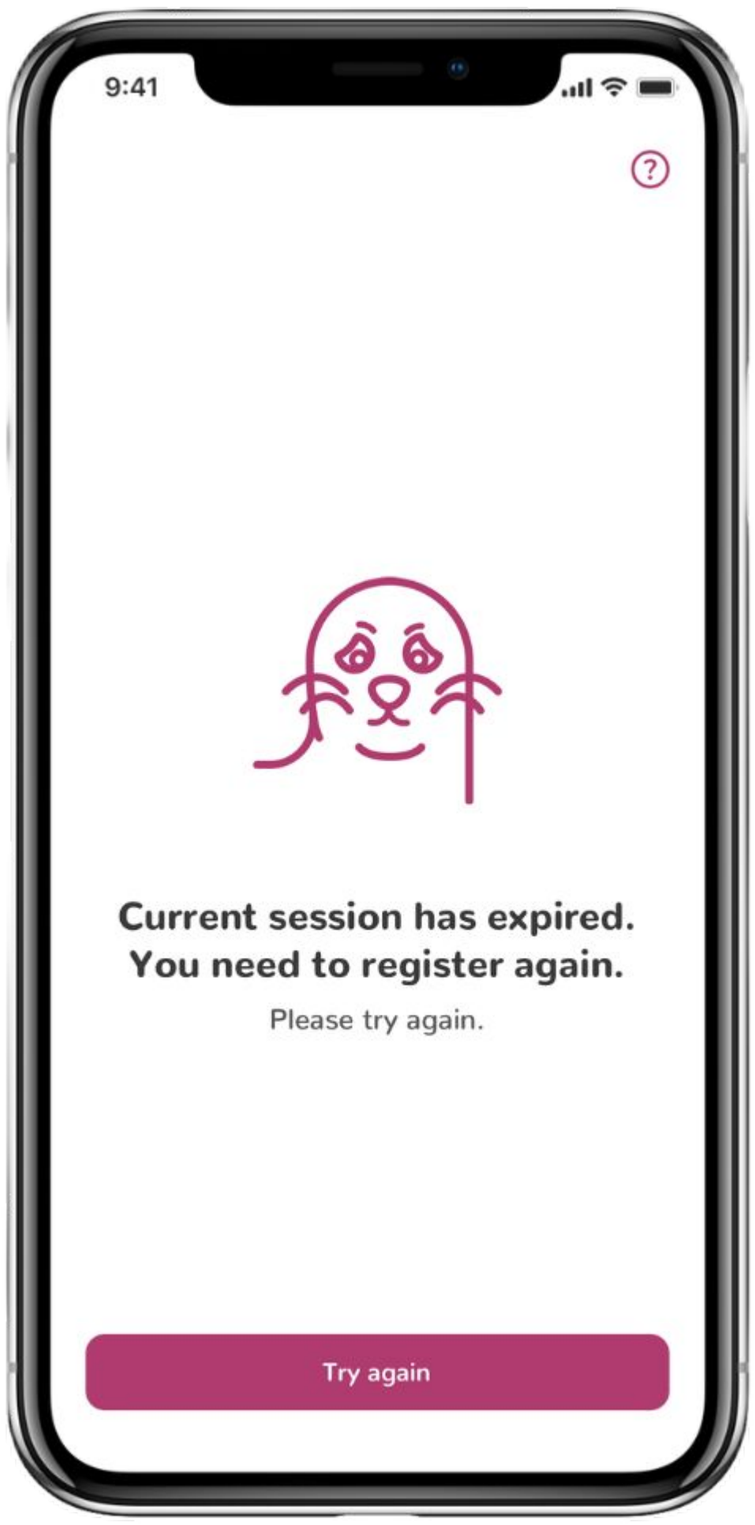
ZealiD

Possible errors at any point in the registration process

Something went wrong

Generic error message requiring to retry your last action.





Session has expired

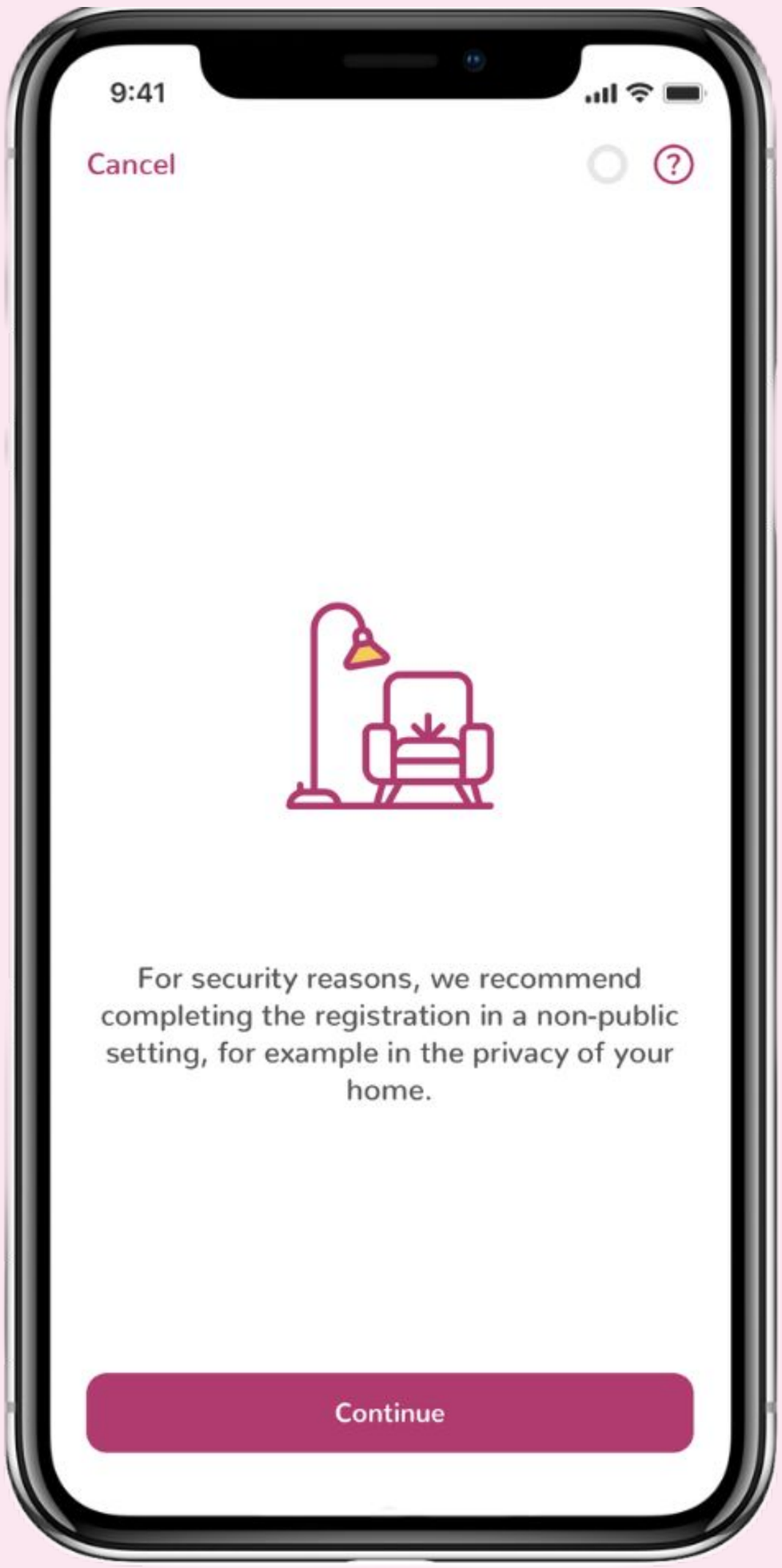
There is a 120 min. time limit to complete the registration process. If the limit is exceeded, you will need to restart the registration process from the beginning.

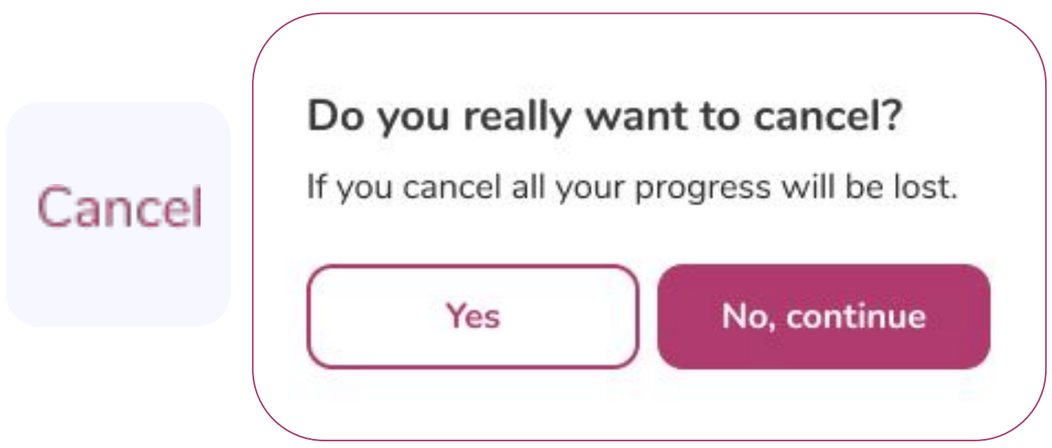
www.zealid.com

ZealiD

4 Ensure secure environment

We recommend registering in a private and secure setting, as the registration process requires the use of an ID document. Therefore, it is important to keep personal data safe and away from strangers in a public environment.



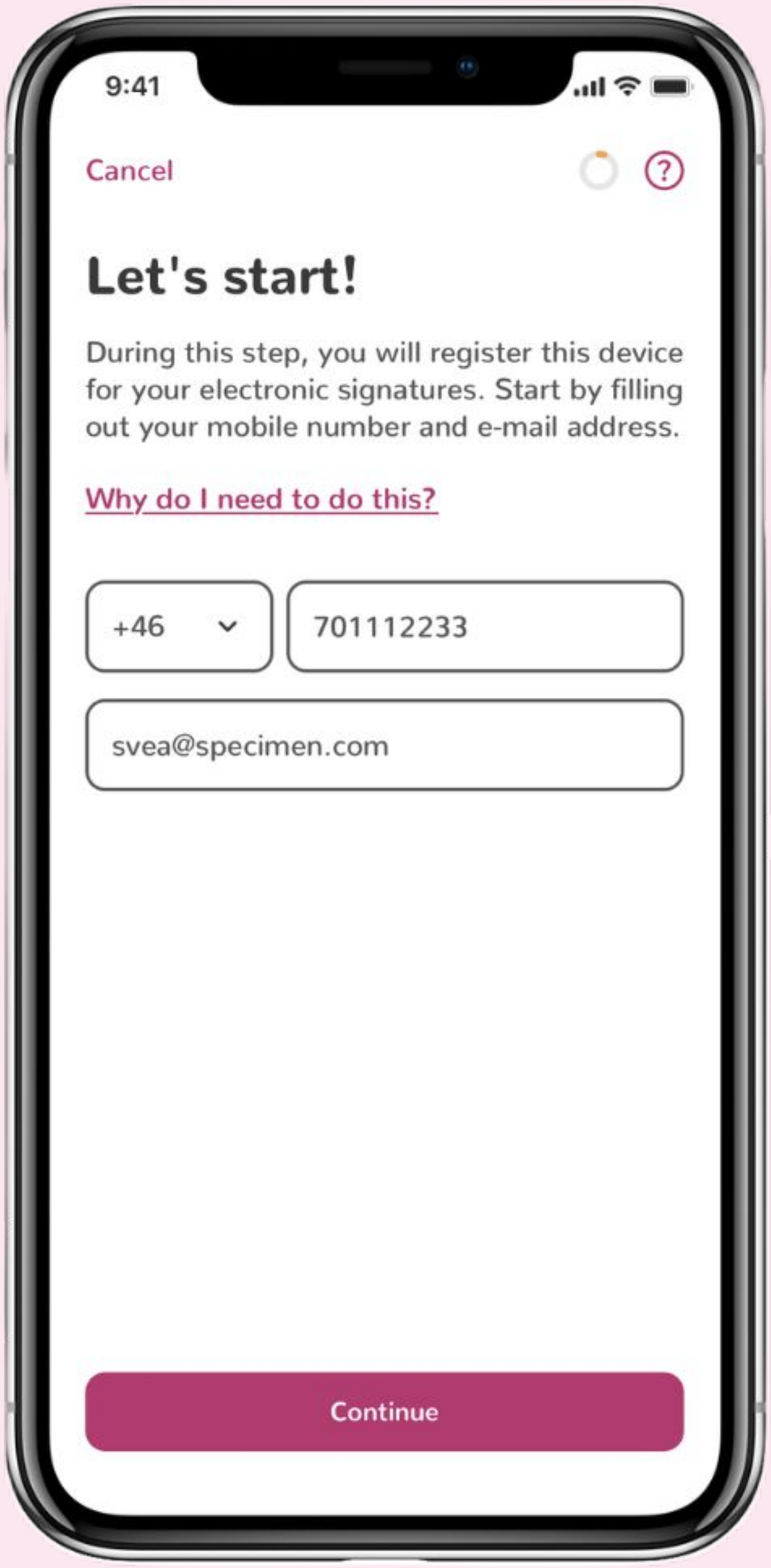


Registration progress bar and Help Center

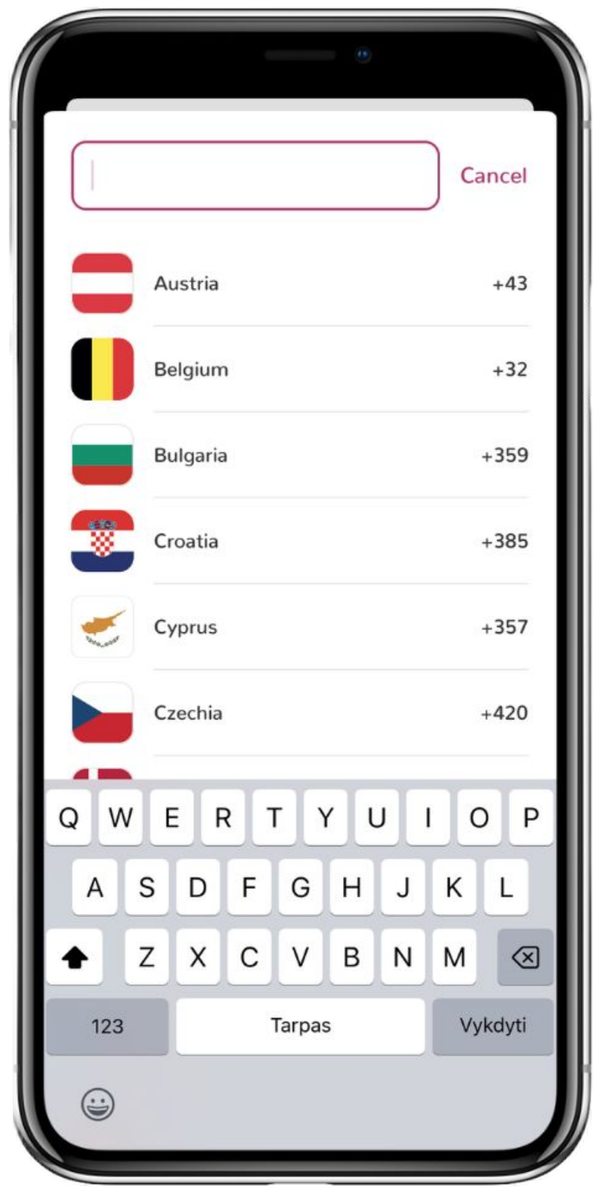
ZealiD

5 Device registration: contact input

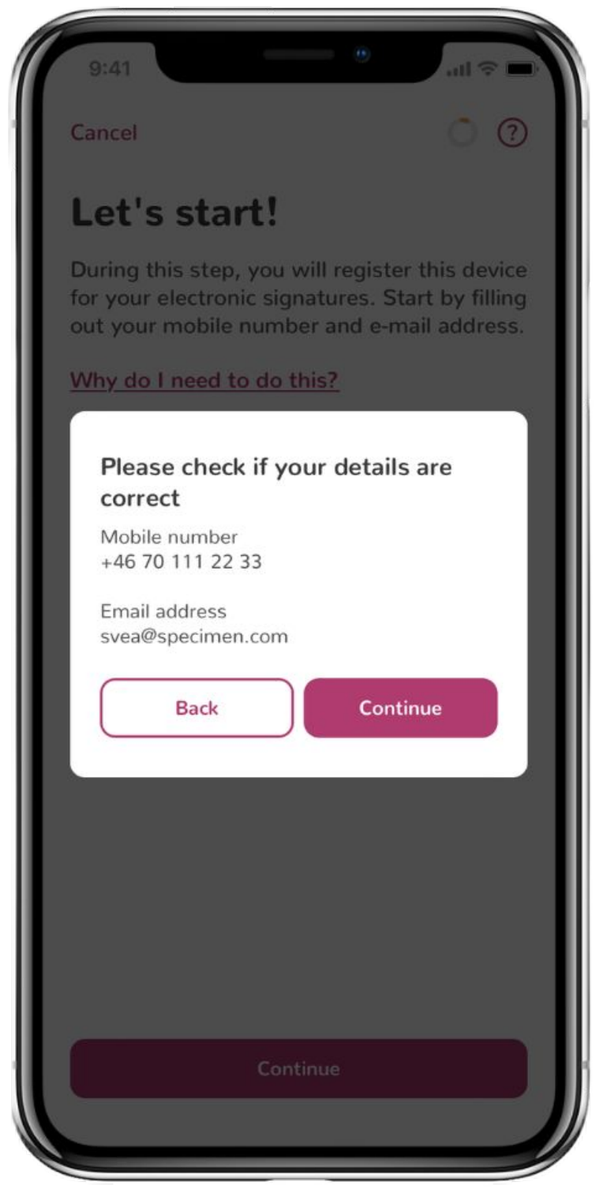
Enter your phone number and email address to receive one-time passwords (OTP). The OTP will be received via SMS and email. The mobile device will be registered as a Trusted device for qualified signing in the next step.



Select country code



Check details and click “Continue”.

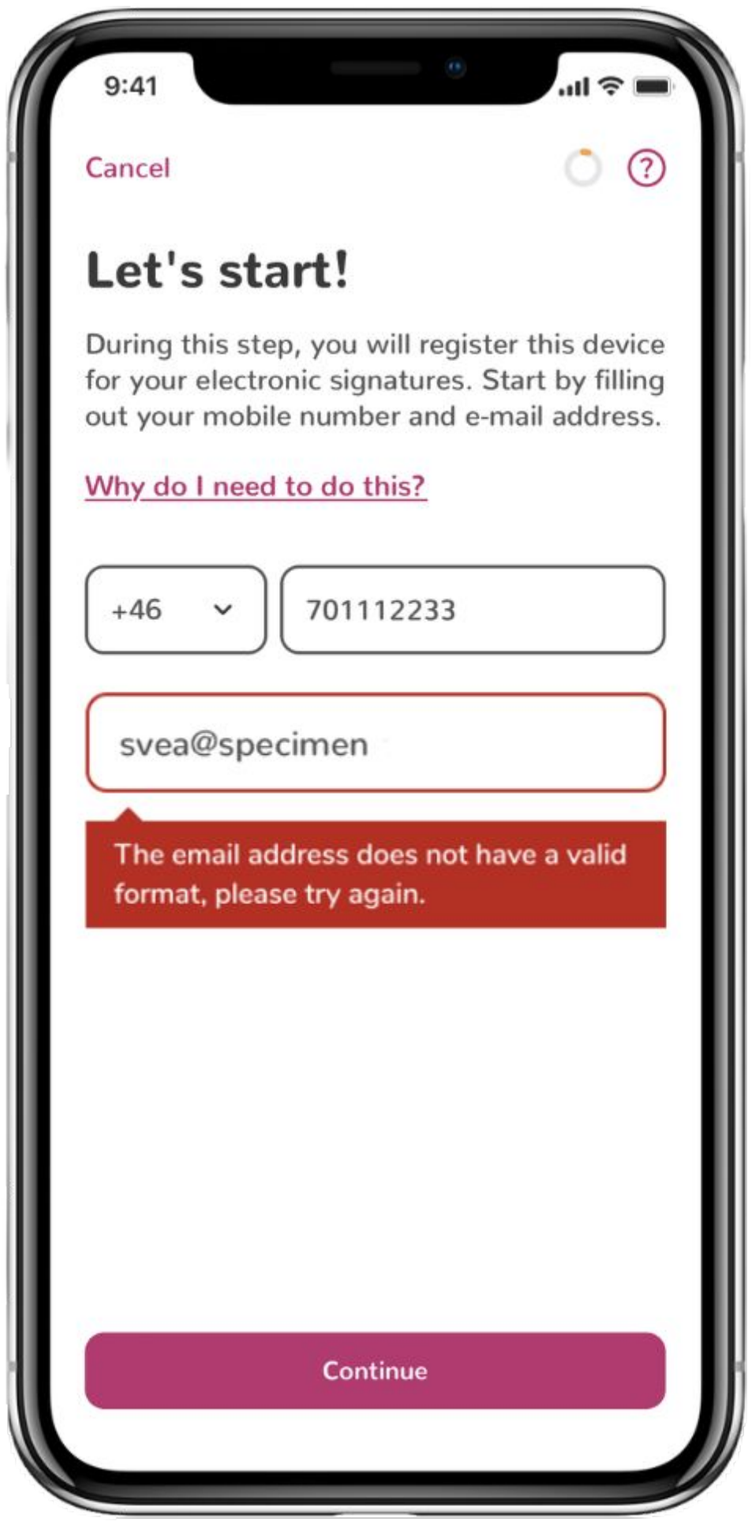


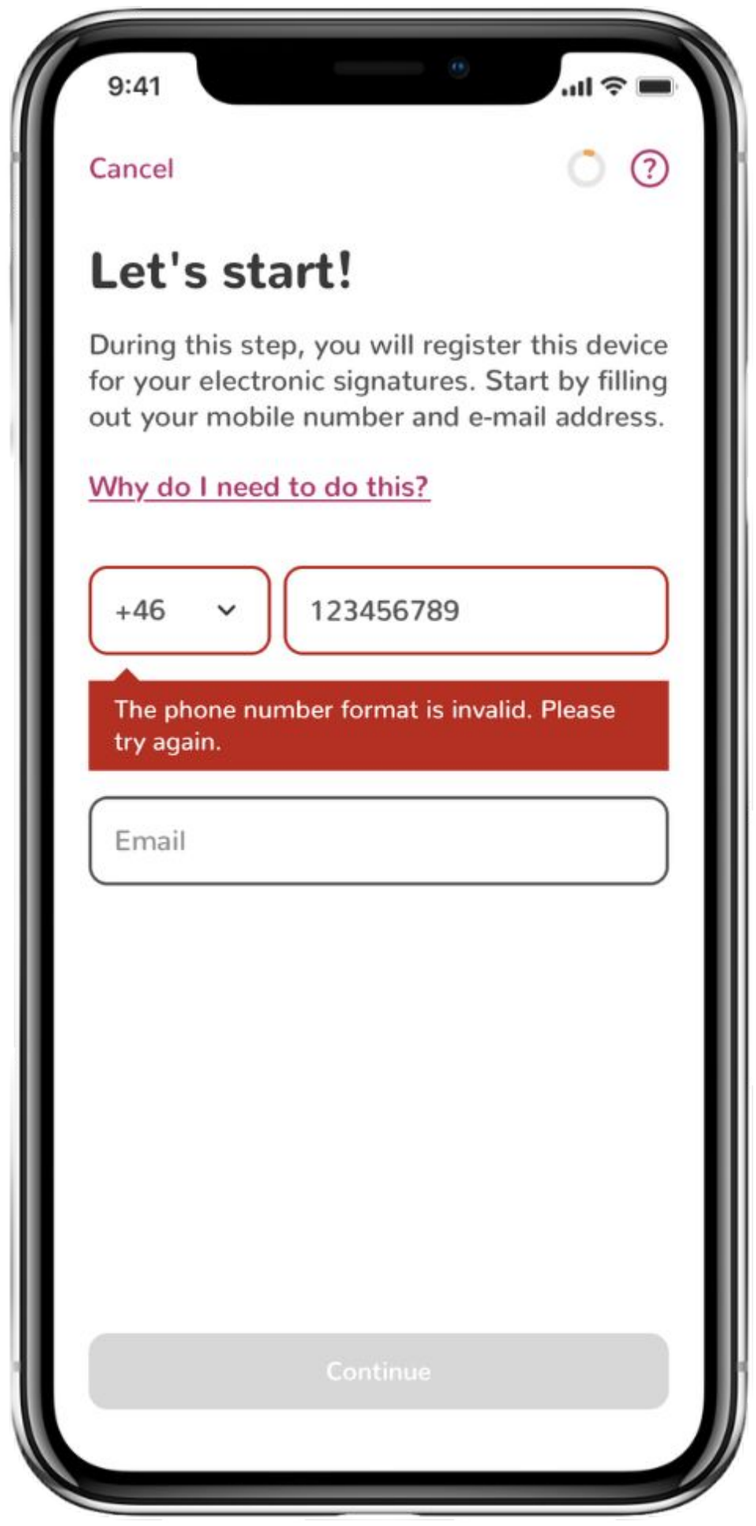
ZealiD

Device registration: errors

Incorrect phone number format

Enter a valid phone number. For example, the correct amount of digits or international format.





Incorrect email format

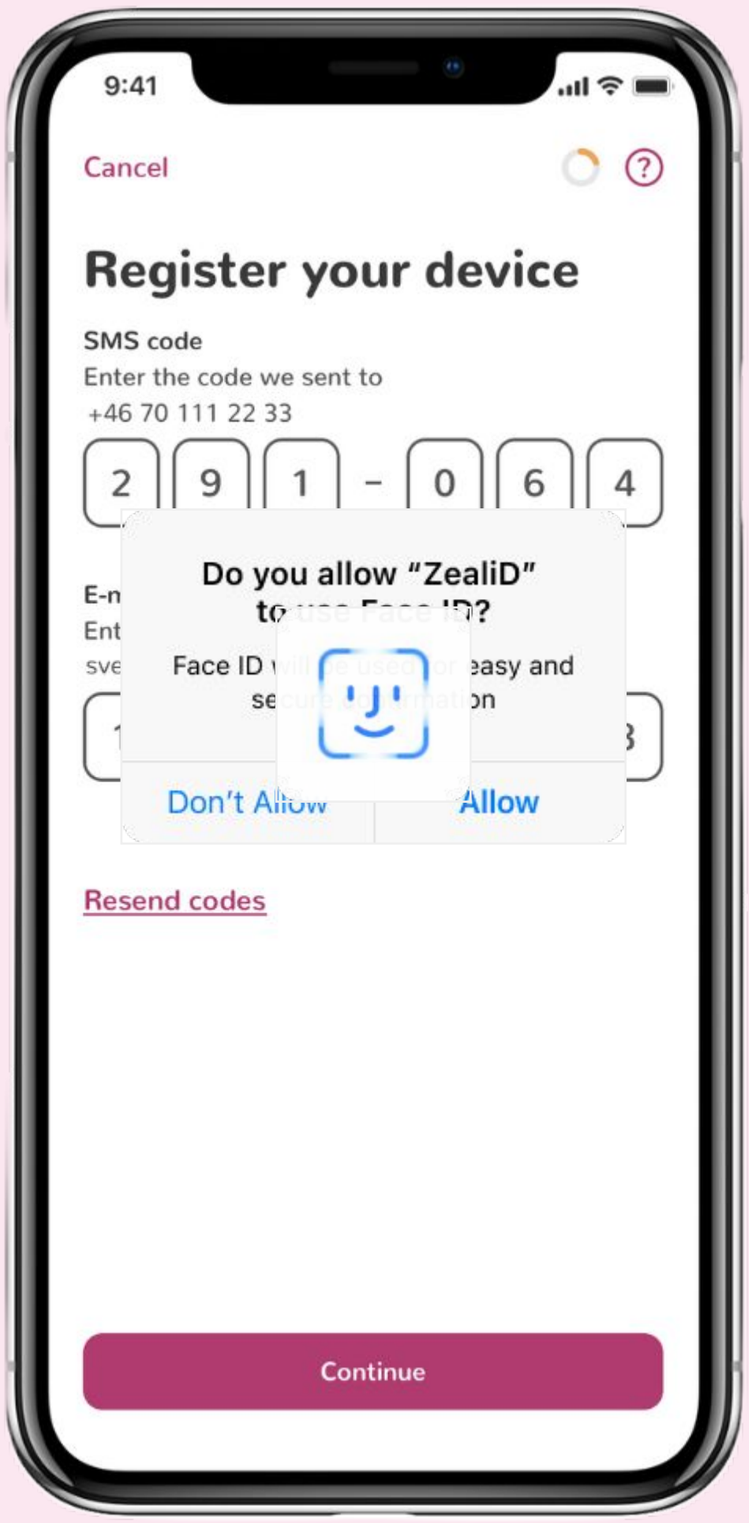
Enter an email address in a valid format.

www.zealid.com

ZealiD

5 Device registration: code entry

Enter the received codes and confirm with Face ID or Touch ID. A mobile device will be registered for qualified signing. Biometric authentication ensures that only the mobile device owner is able to authorize signatures.



Resend codes

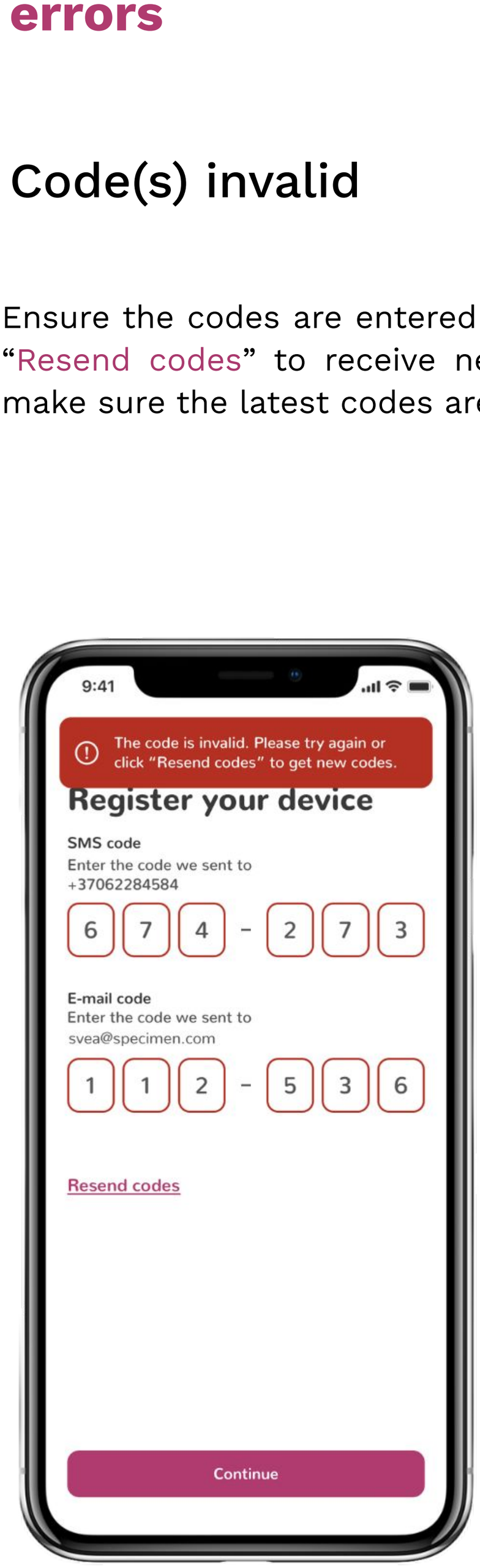
Use this option if receiving one of the codes takes longer than a couple of minutes.

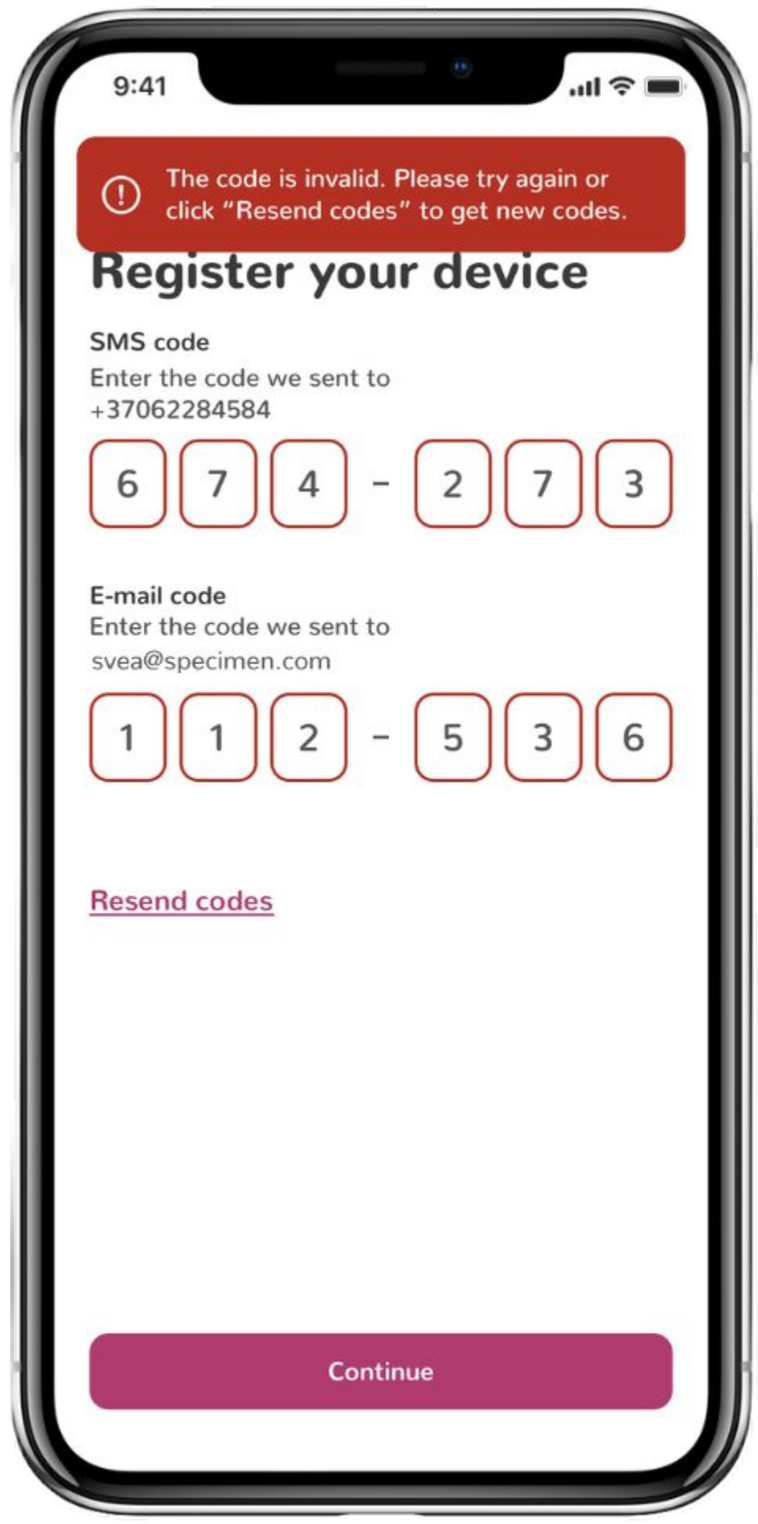
ZealiD

Device registration: errors

Code(s) invalid

Ensure the codes are entered correctly. Use “Resend codes” to receive new codes and make sure the latest codes are entered.





OTP Codes have expired

Codes are valid for 10 minutes. If they’re expired, click “Resend codes” to receive the new ones.

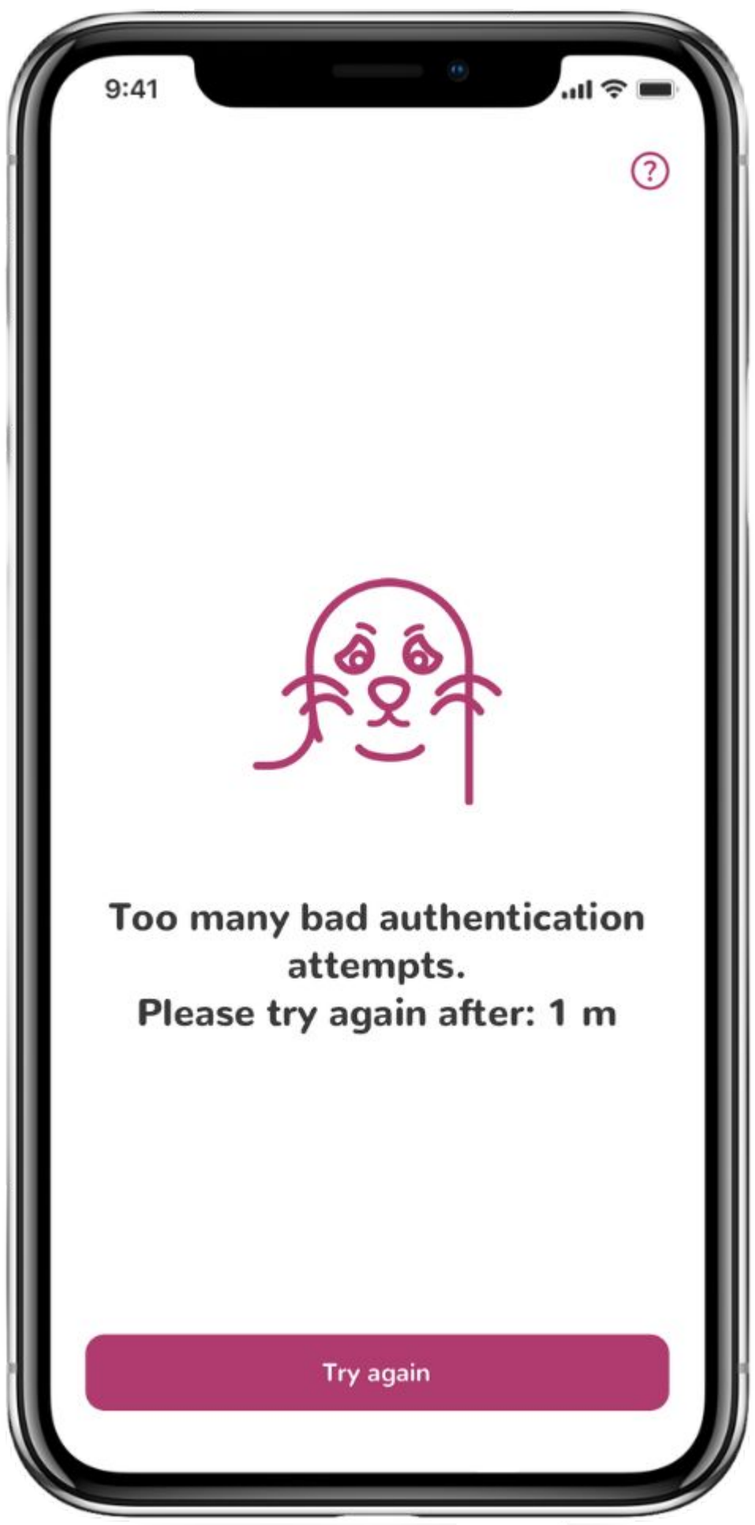
www.zealid.com

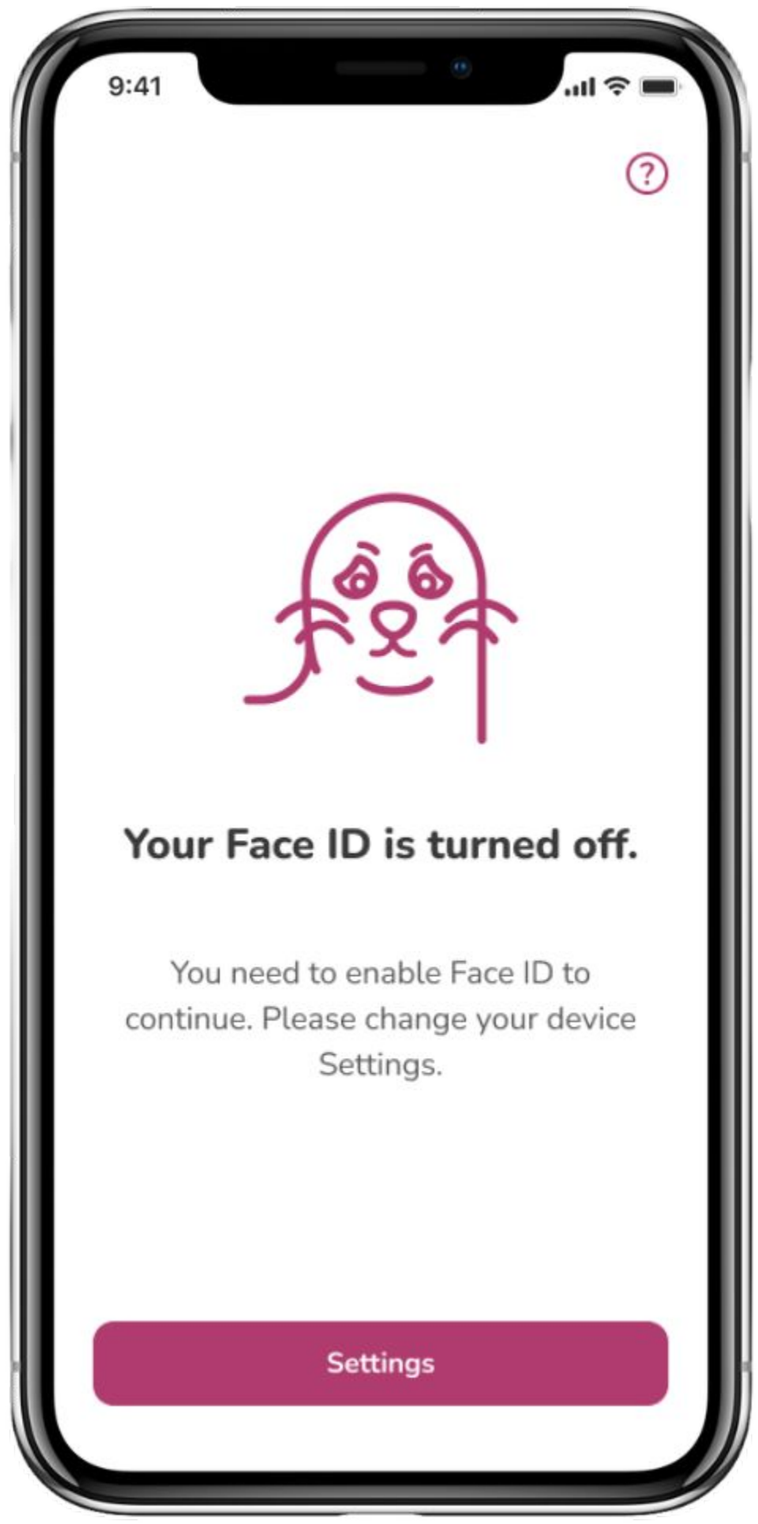
ZealiD

Device registration: errors

Biometrics were turned off

Biometric authentication is a crucial part of authorizing qualified electronic signatures. Click “Try again” to receive new OTP codes and allow the app to use Face ID or Touch ID to proceed with the registration.





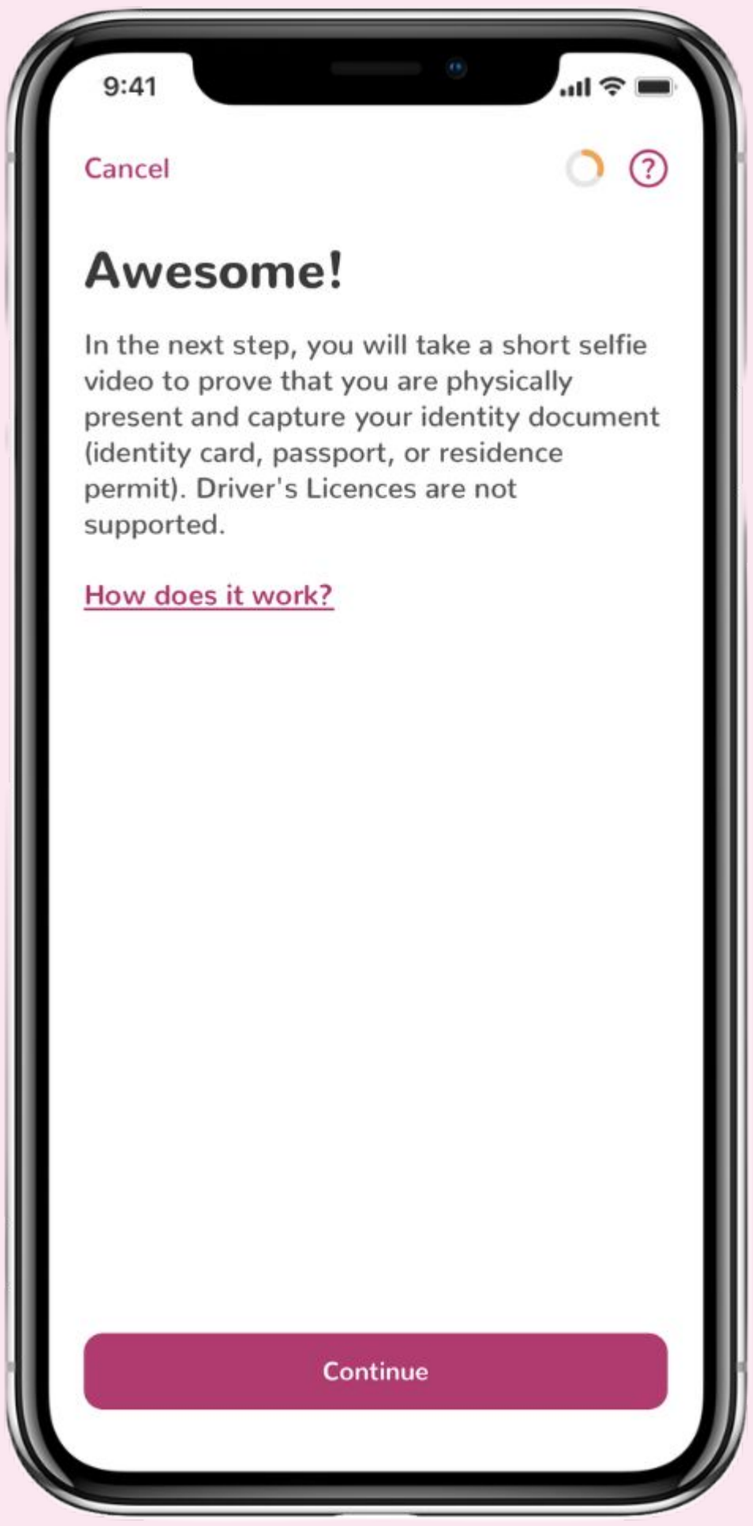
Too many bad authentication attempts

Face ID/Touch ID was not recognized 3 times in a row. Wait the specified time and try again. If biometric authentication fails again, you will need to wait 5 minutes. If biometrics fail again, you will be redirected to the “Let’s start!” screen and will be asked to re-enter your contact details. Make sure that Face ID/Touch ID is set up properly.

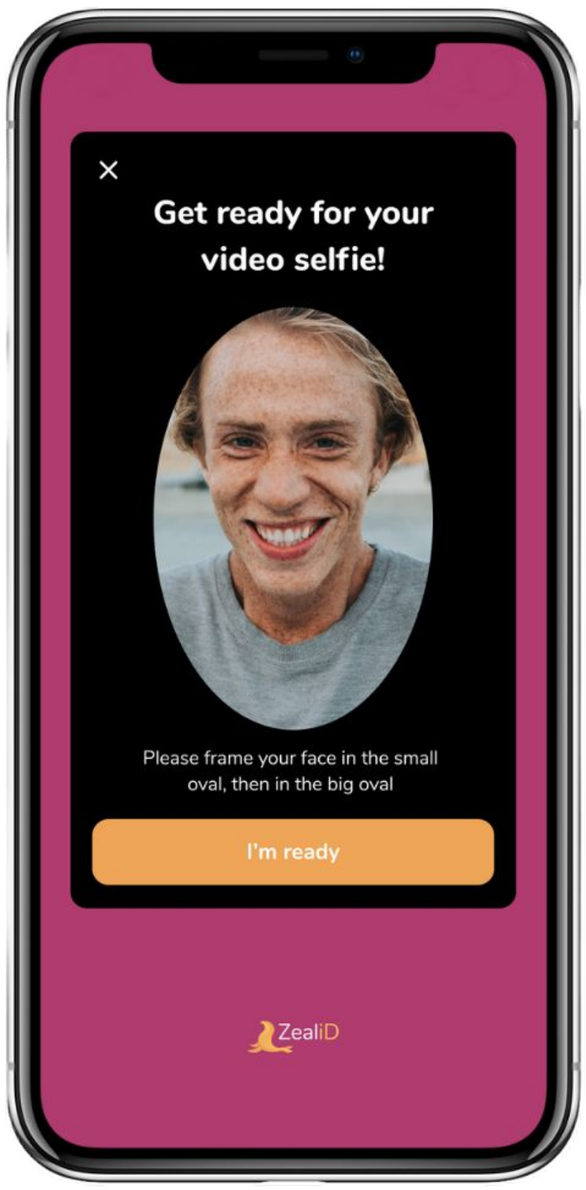
ZealiD

6 Liveness check

A video selfie will be taken to establish your physical presence. Make sure the surroundings don't have extreme lighting. Improper lighting can affect the quality of a selfie. Enable the camera, center the face in the oval frame and follow the instructions. Once completed, you will be redirected to the ID check step automatically.

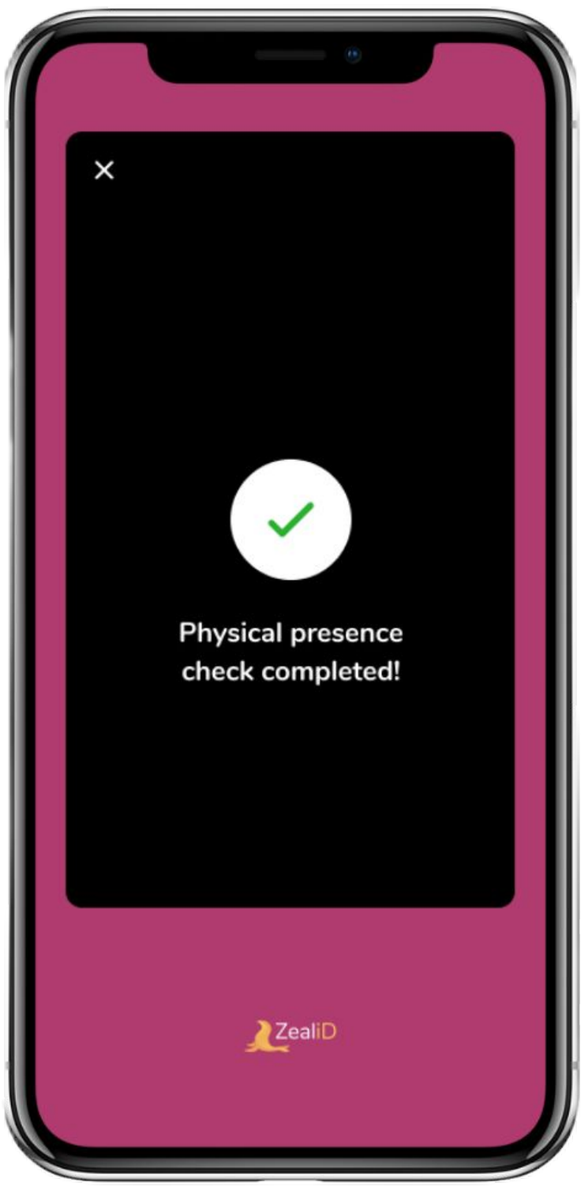


1



2

3

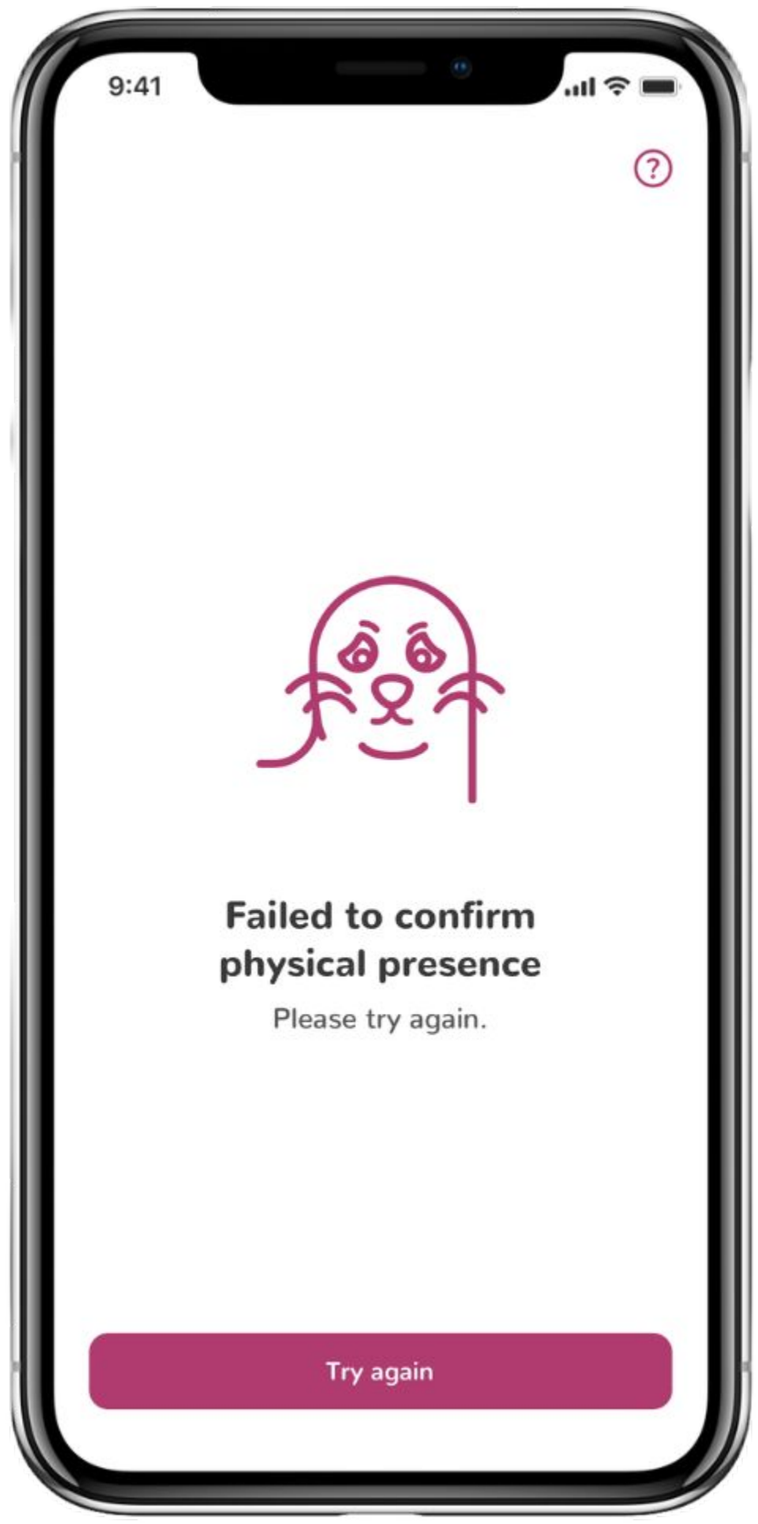


ZealiD

Liveness check: errors

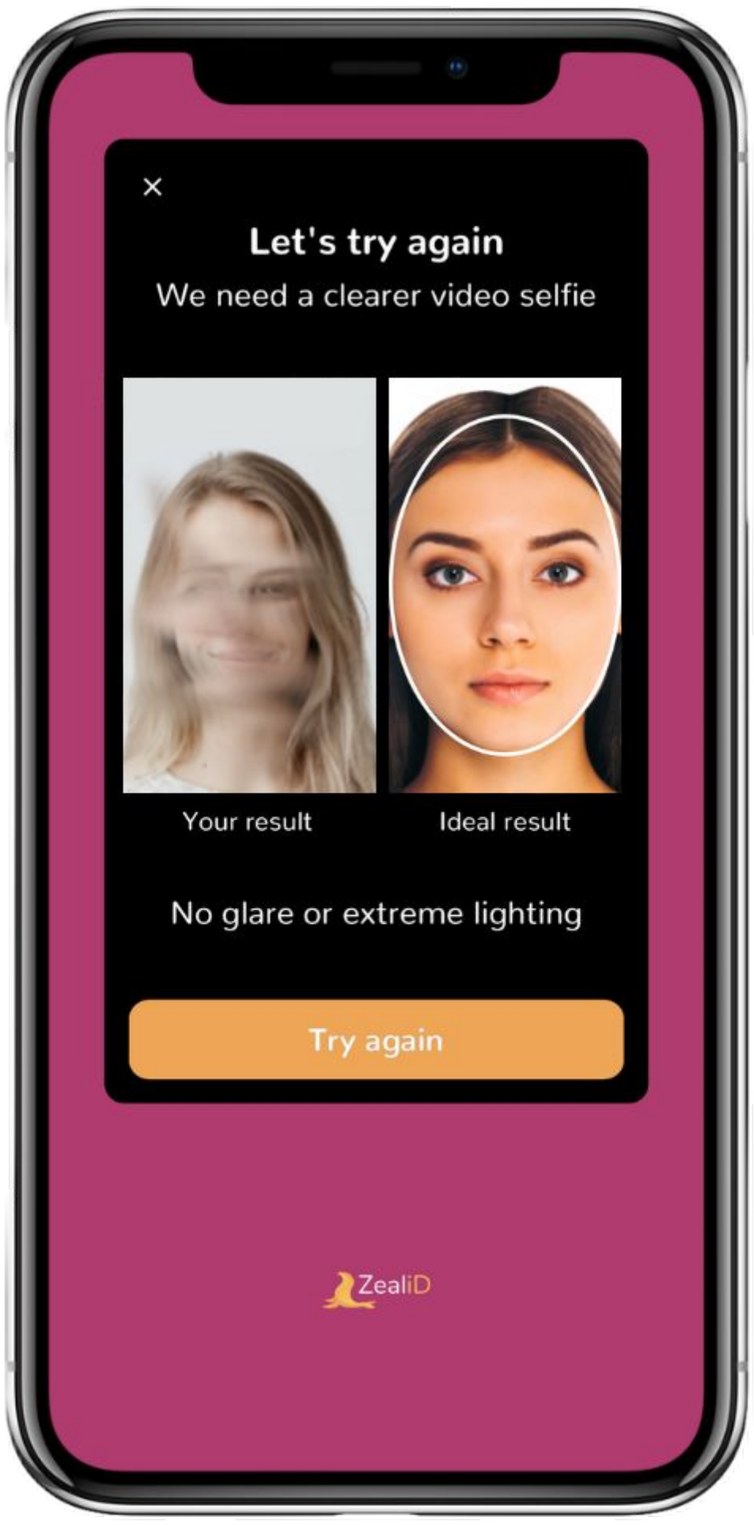
Failed to confirm physical presence

While a selfie video was being taken, a significant part of your face was covered or other circumstances prevented confirming if you were physically present. You can retry the liveness check step.



Redo liveness check

The liveness check resulted in a bad quality selfie (photo shows glare, extreme lighting, or is blurry). Your selfie is shown next to the good quality example photo. You can try the liveness check again.



www.zealid.com

ZealiD

7 ID check: photo

Place an ID document on a flat surface and fit it into a frame. Take a photo of the biodata page. Make sure the photo is sharp, no crucial information is covered by other objects or light. The photo should be representable as it will be held for evidentiary purposes.

At this step, the ZealiD mobile app will recognize if your ID document contains an NFC chip:

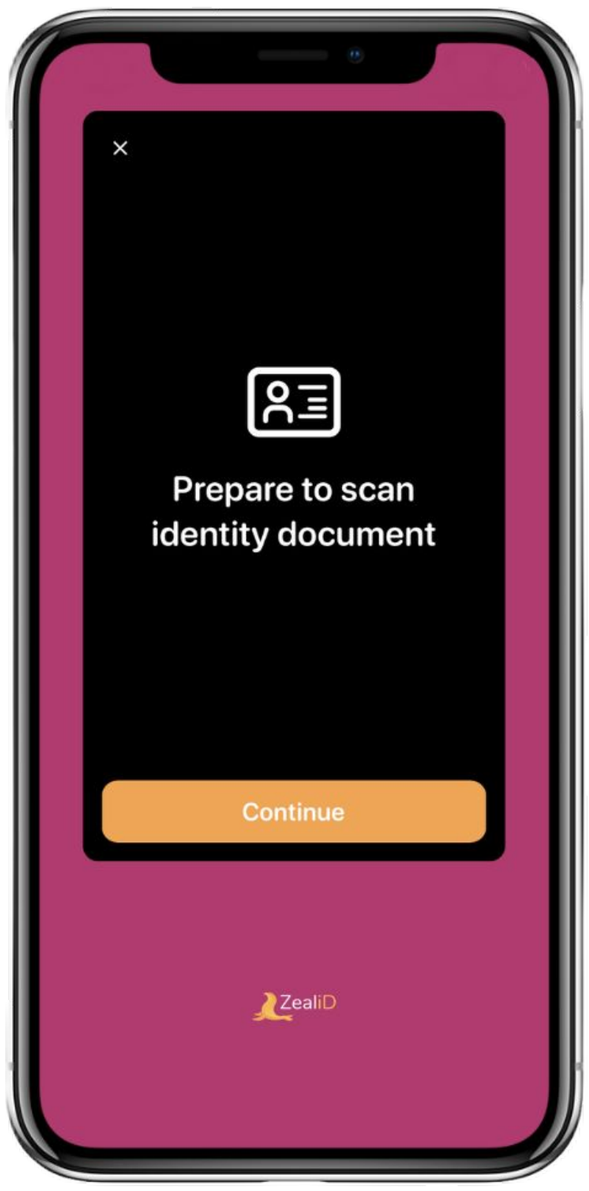
If the chip is present, you will be redirected to scan your ID document (see step 8a).

If the NFC chip is not present, you will be redirected to make a video of your ID document (see step 8b).

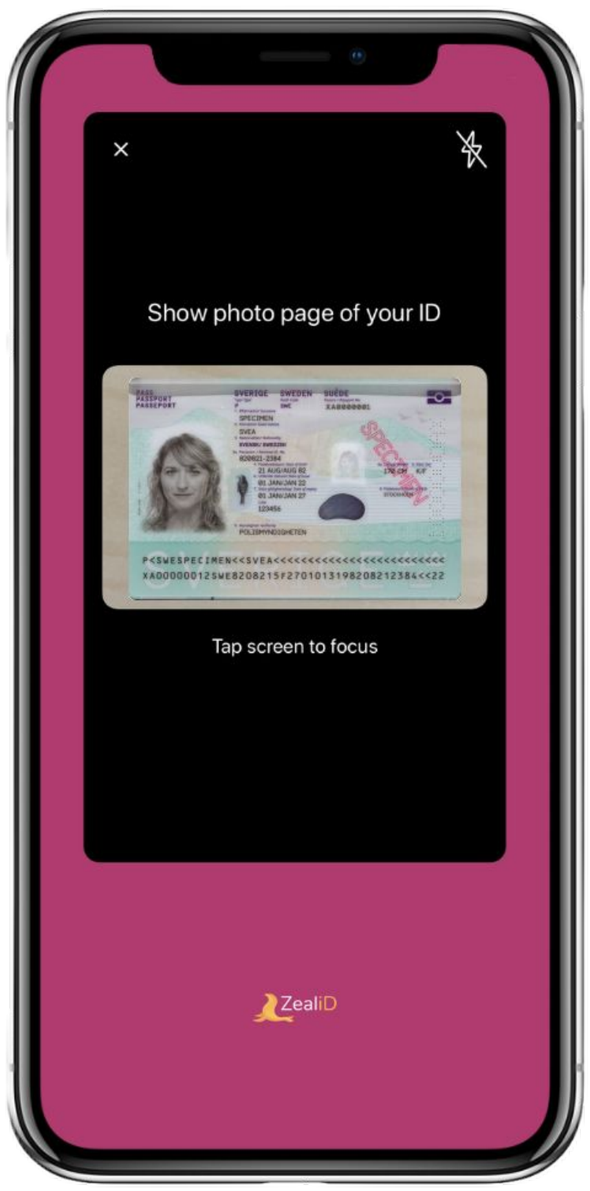
Passports

Required photo: biodata page

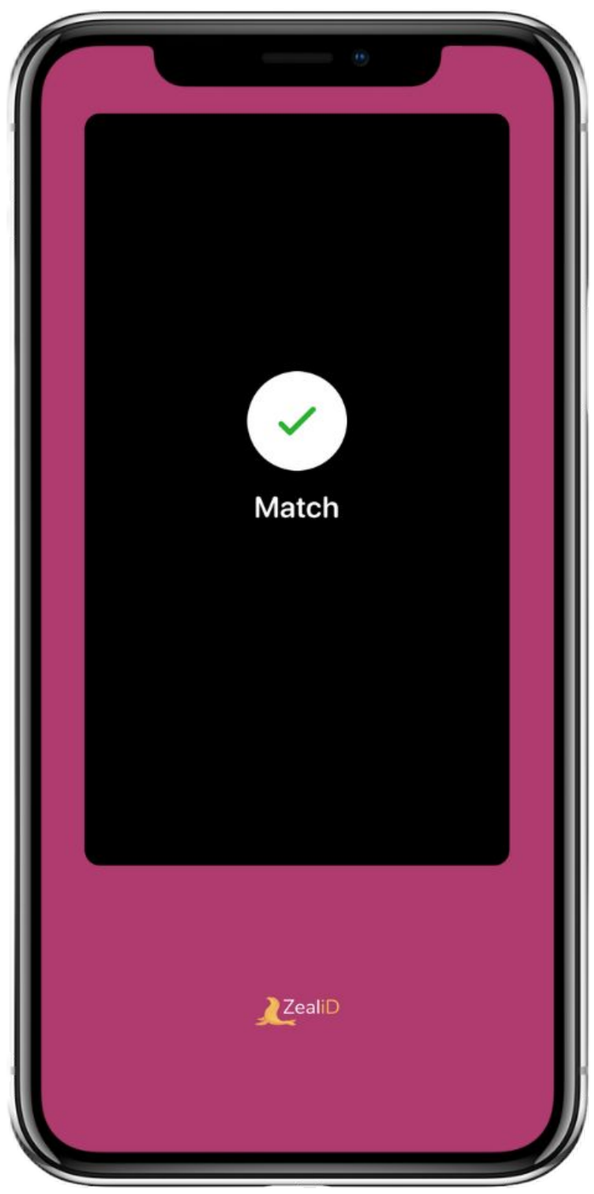
1



2



3



Step 7 for ID Cards and Residence Permits

ZealiD

7 ID check: photo

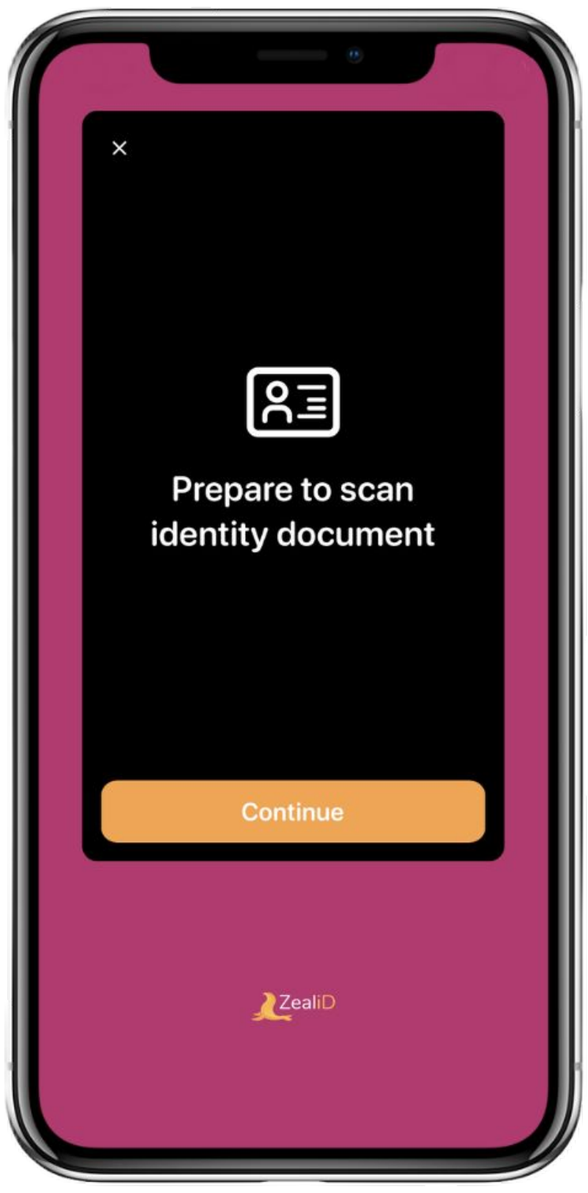
ID Cards

Required photos: front and back

Residence Permits

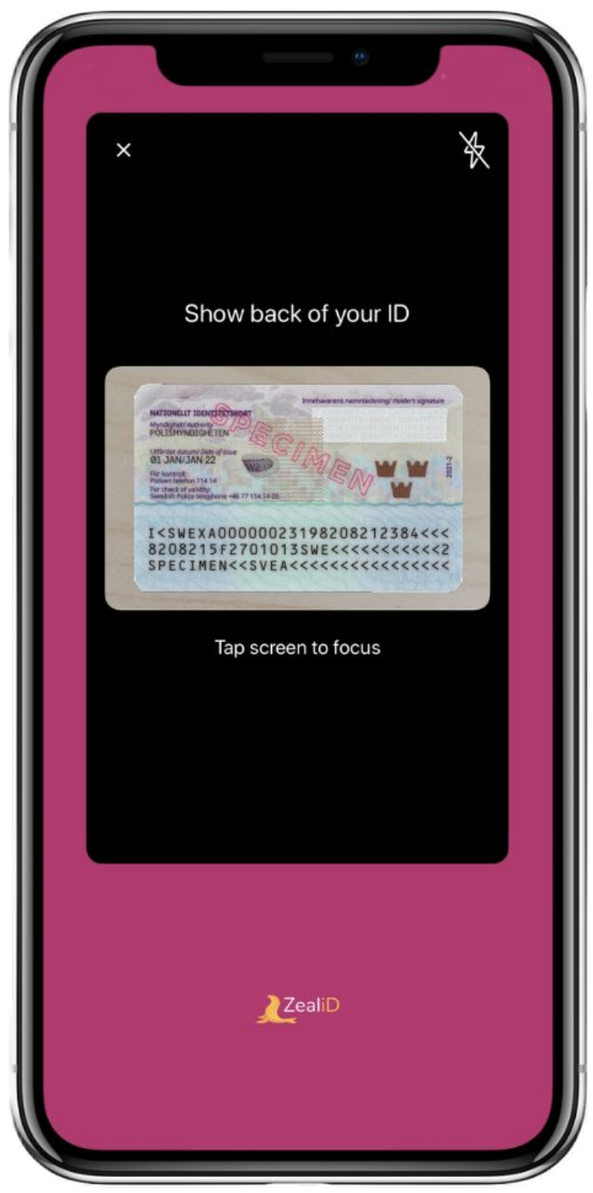
Required photos: front and back

1

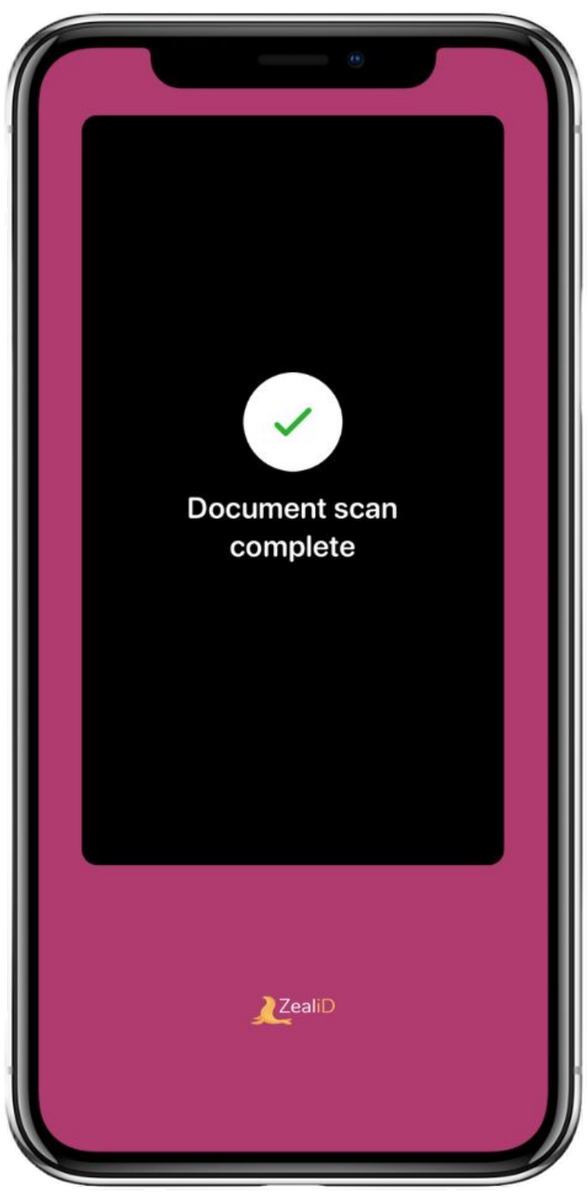


2

3



4

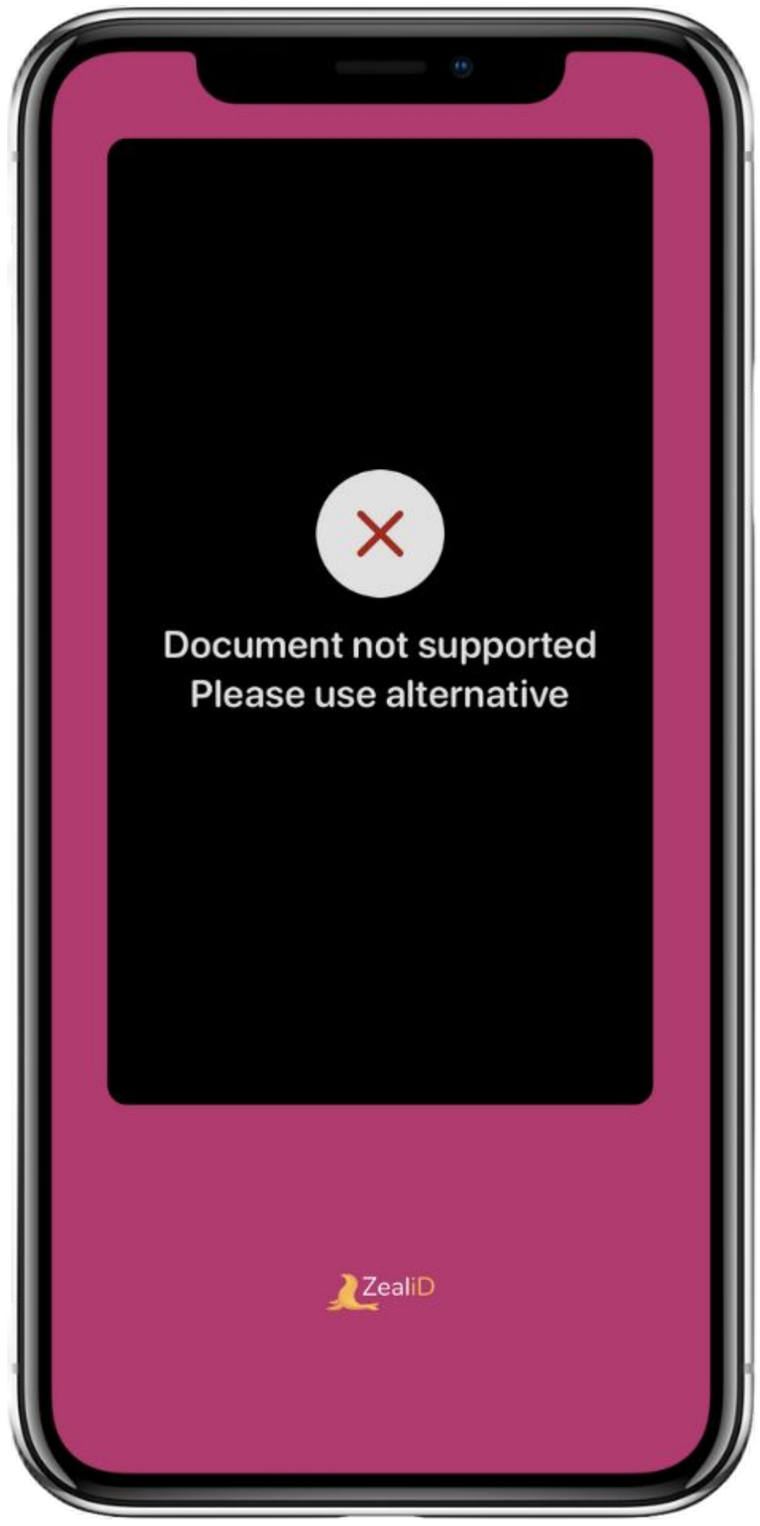


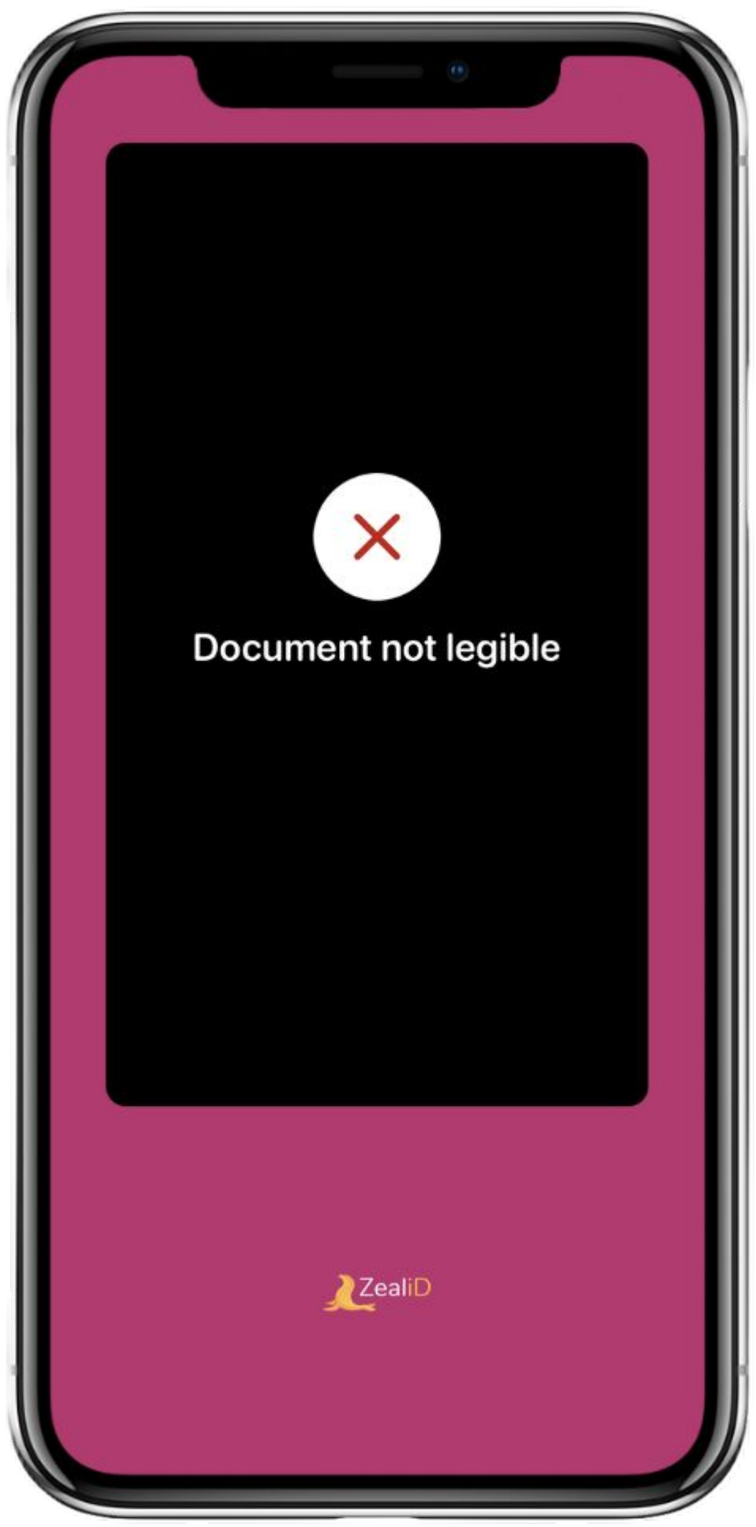
ZealiD

ID check: errors

Document not supported

A document in use is not supported. Check the supported ID list and try an alternative.





Document not legible

The document was not recognized because of bad ID photo quality. Retry taking the document photos.

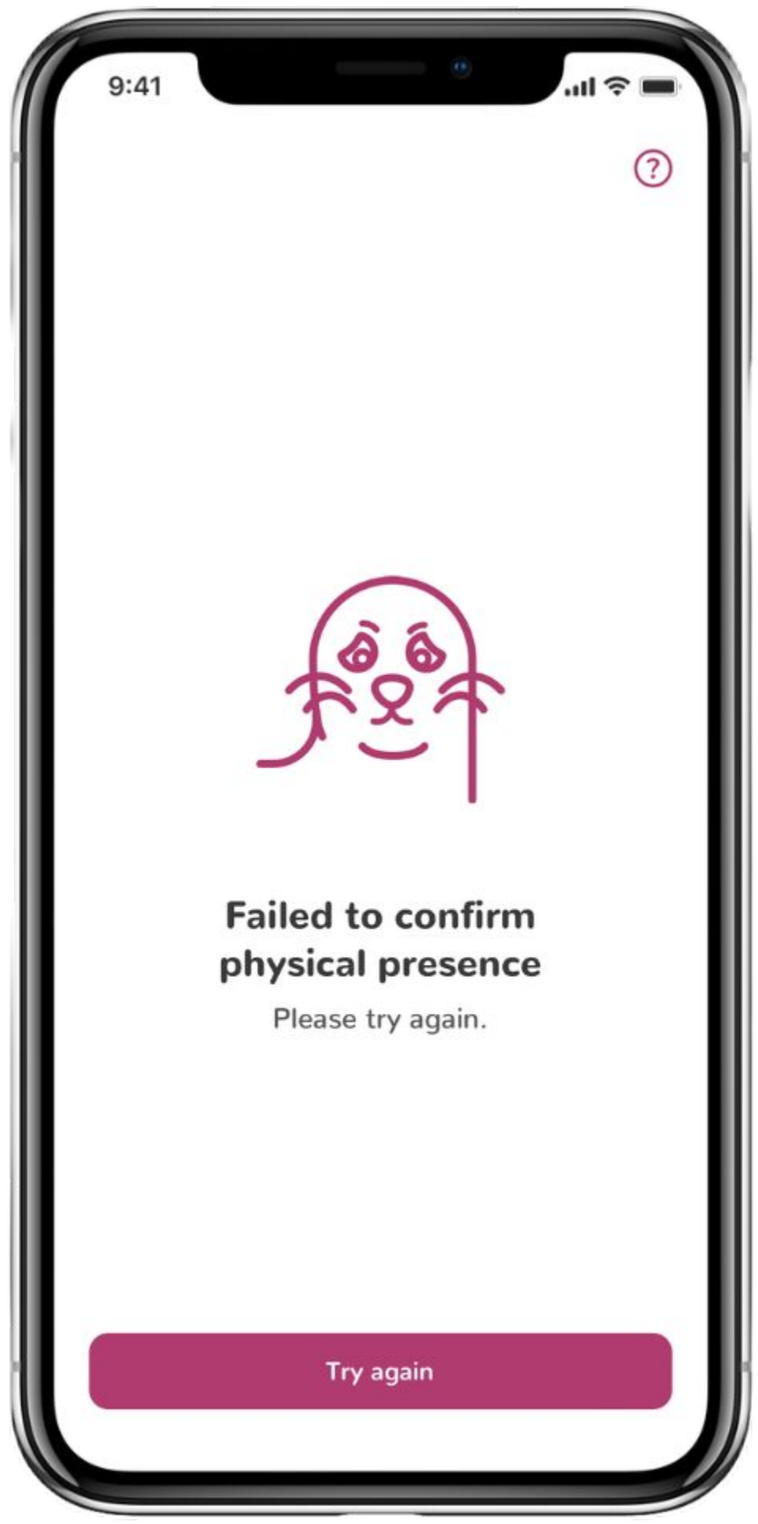
www.zealid.com

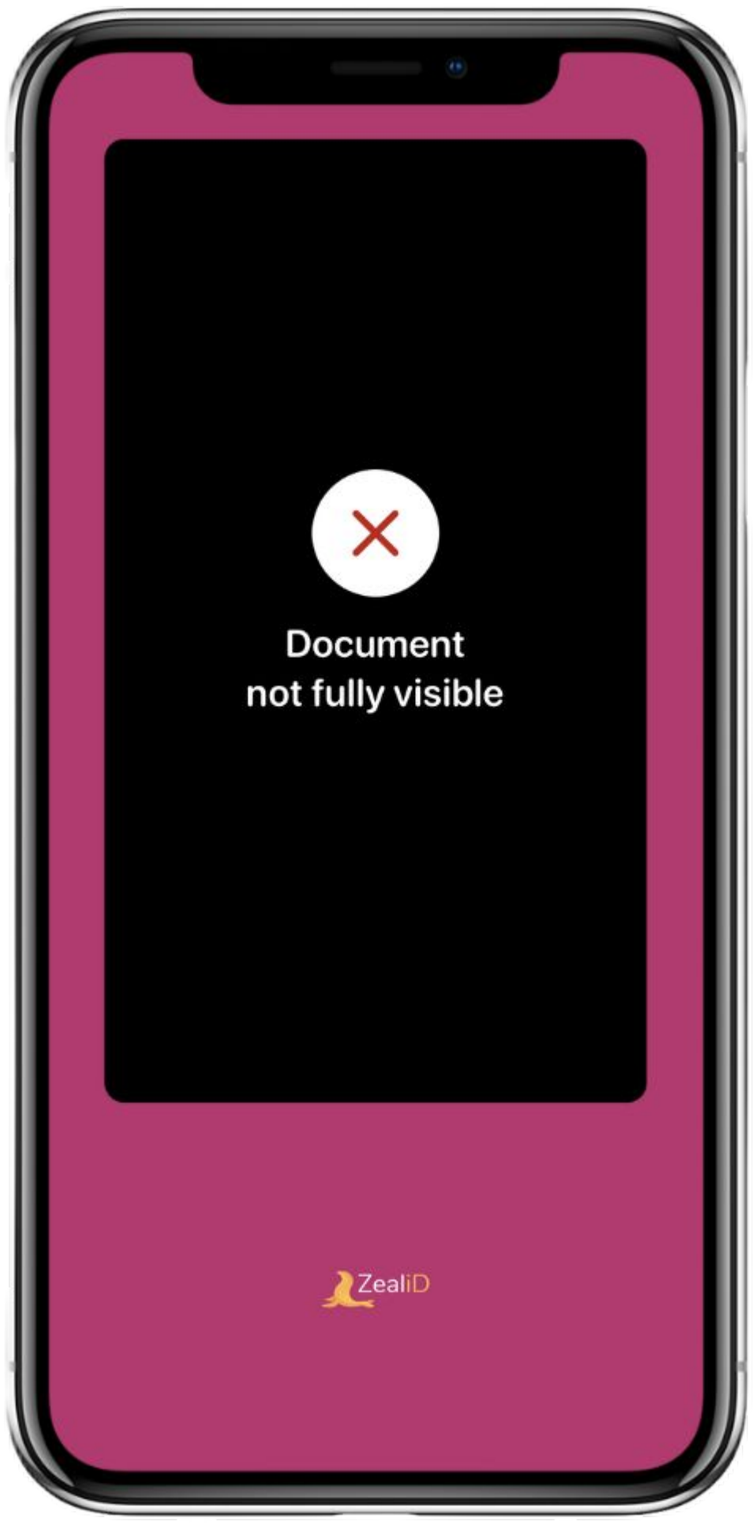
ZealiD

ID check: errors

Failed to confirm physical presence

Low match between your selfie and the document holder’s image. Ensure good lighting while taking a photo of the document. Photo angle might impact face recognition and low match.





Document not fully visible

The document was out of frame or some parts were obscured while taking a photo of the ID document.

www.zealid.com

ZealiD

8a ID check: NFC scan

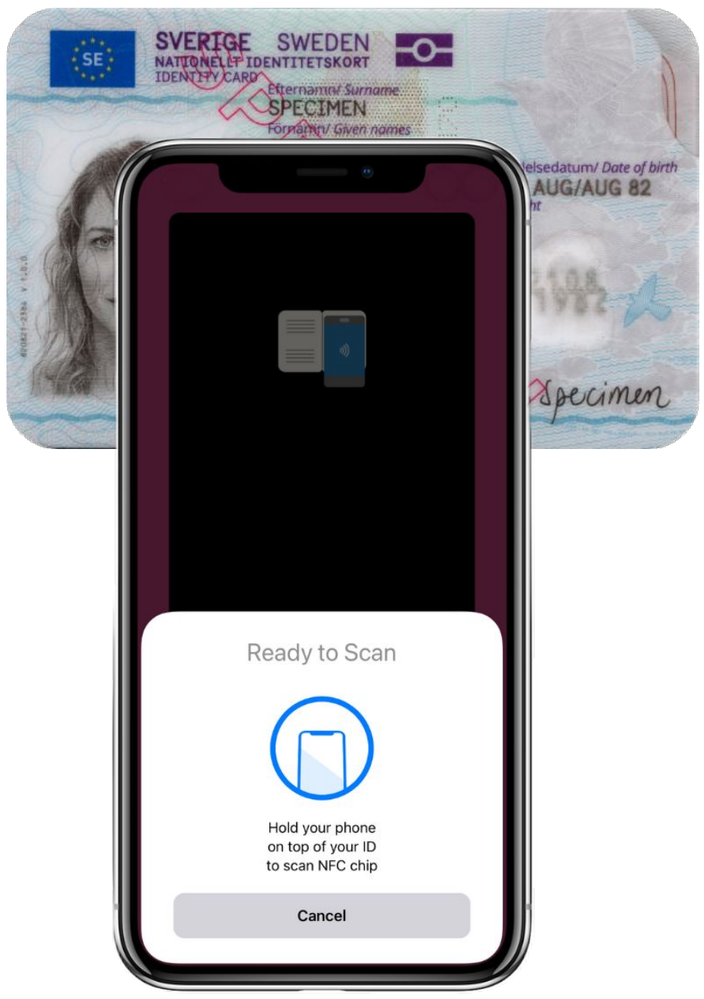
If an NFC chip is embedded in your ID document, the ZealiD mobile app will guide you to scan your ID document with a mobile device for data extraction. Once a scan is complete, your application will be submitted for manual review.

Scanning a chip can be impacted by thick phone cases and additional items in them or by moving the phone while scanning is in progress. If the NFC scan is unsuccessful, the app will redirect you to make a video of the ID document instead.

NFC chip location on a document

PASSPORTS: NFC chips in passports are usually located on the front cover of the passport, with several exceptions in different countries. For example, an NFC chip is inserted in the back cover page of the American and Italian passports.

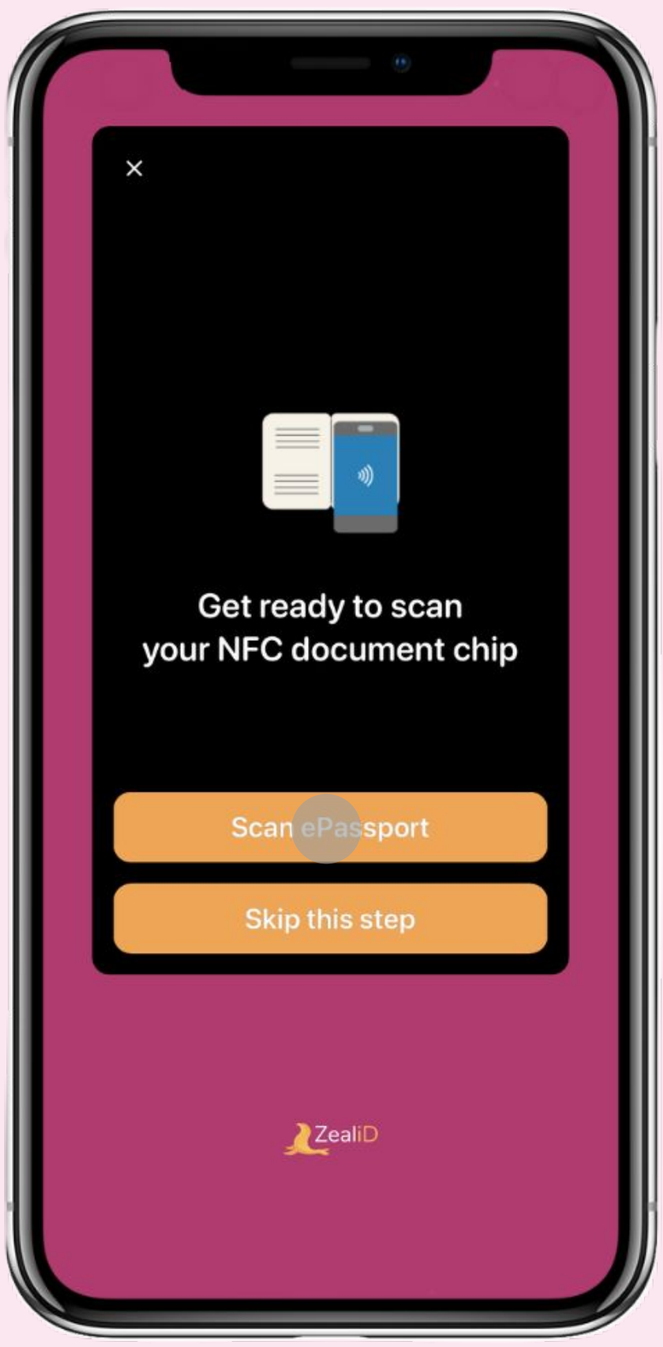
ID CARDS and RESIDENCE PERMITS: Chips are located mostly in the middle of the cards.



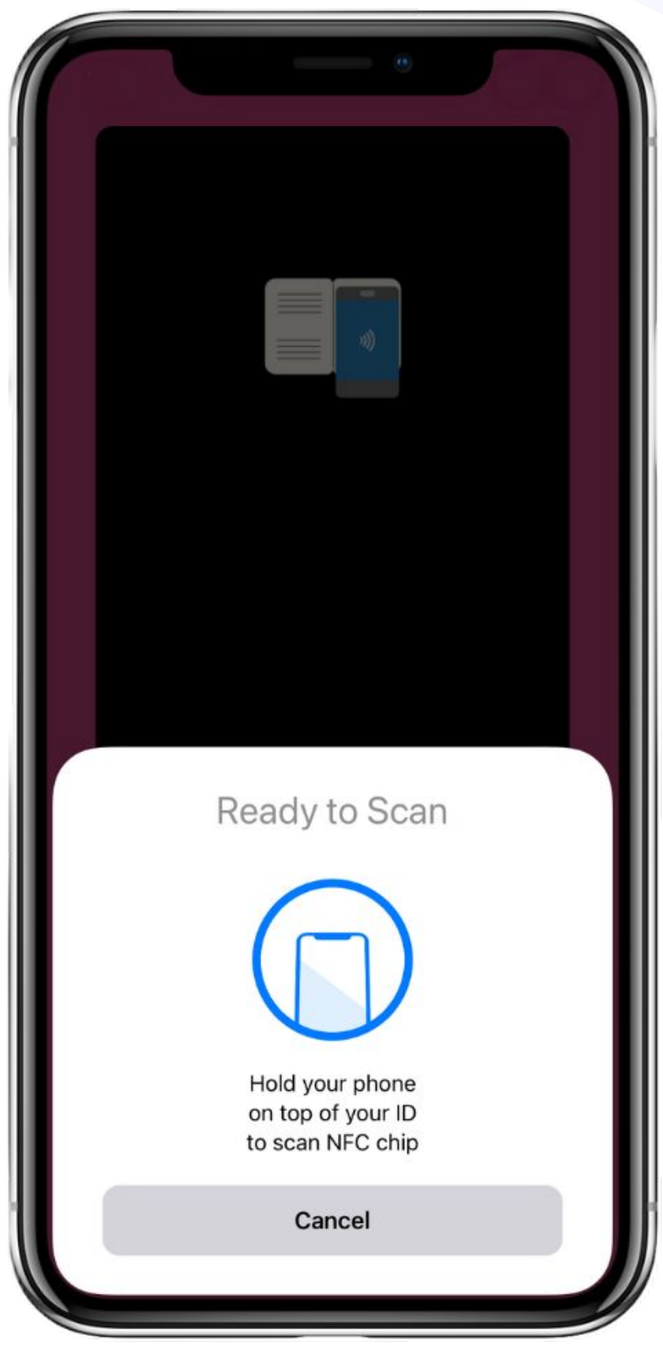
ZealiD

8a ID check: NFC scan

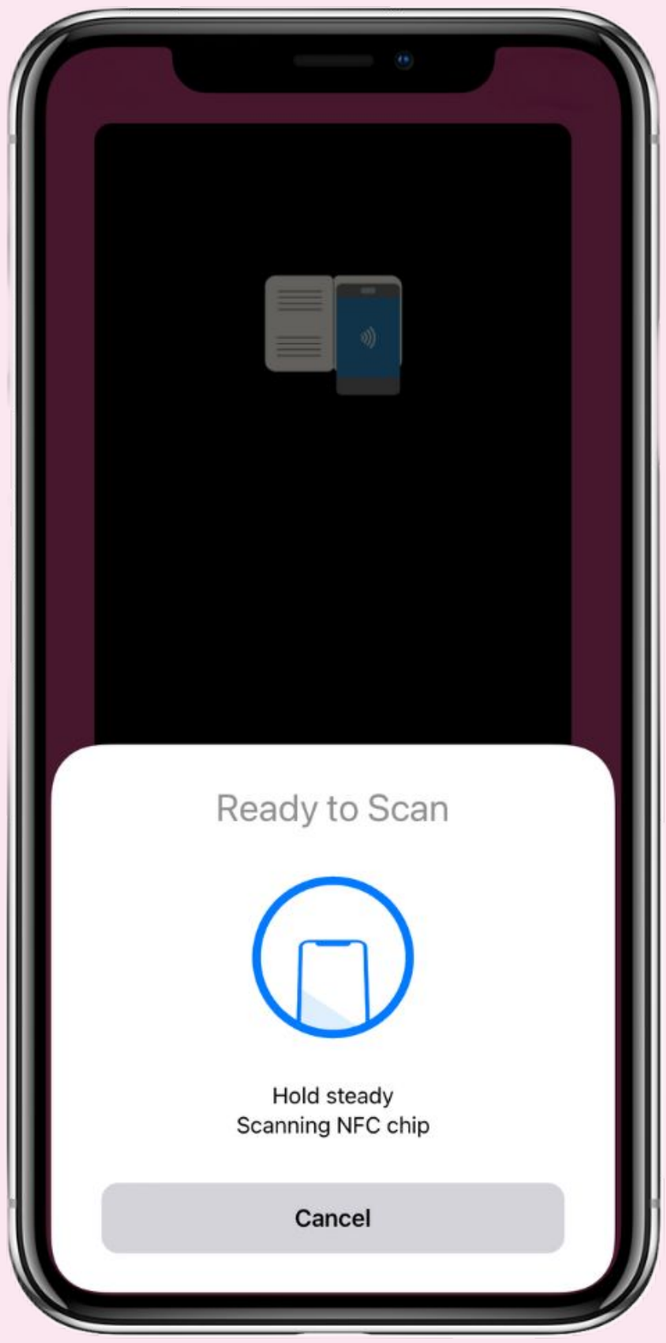
1



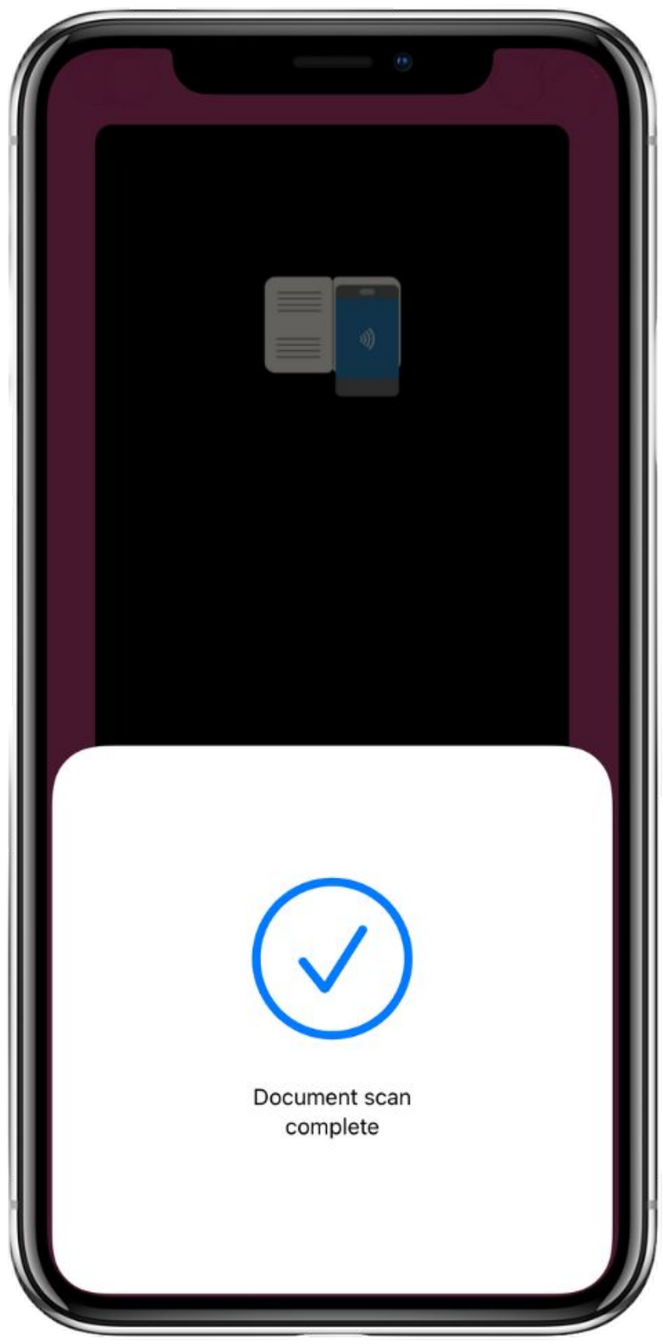
2



3



4

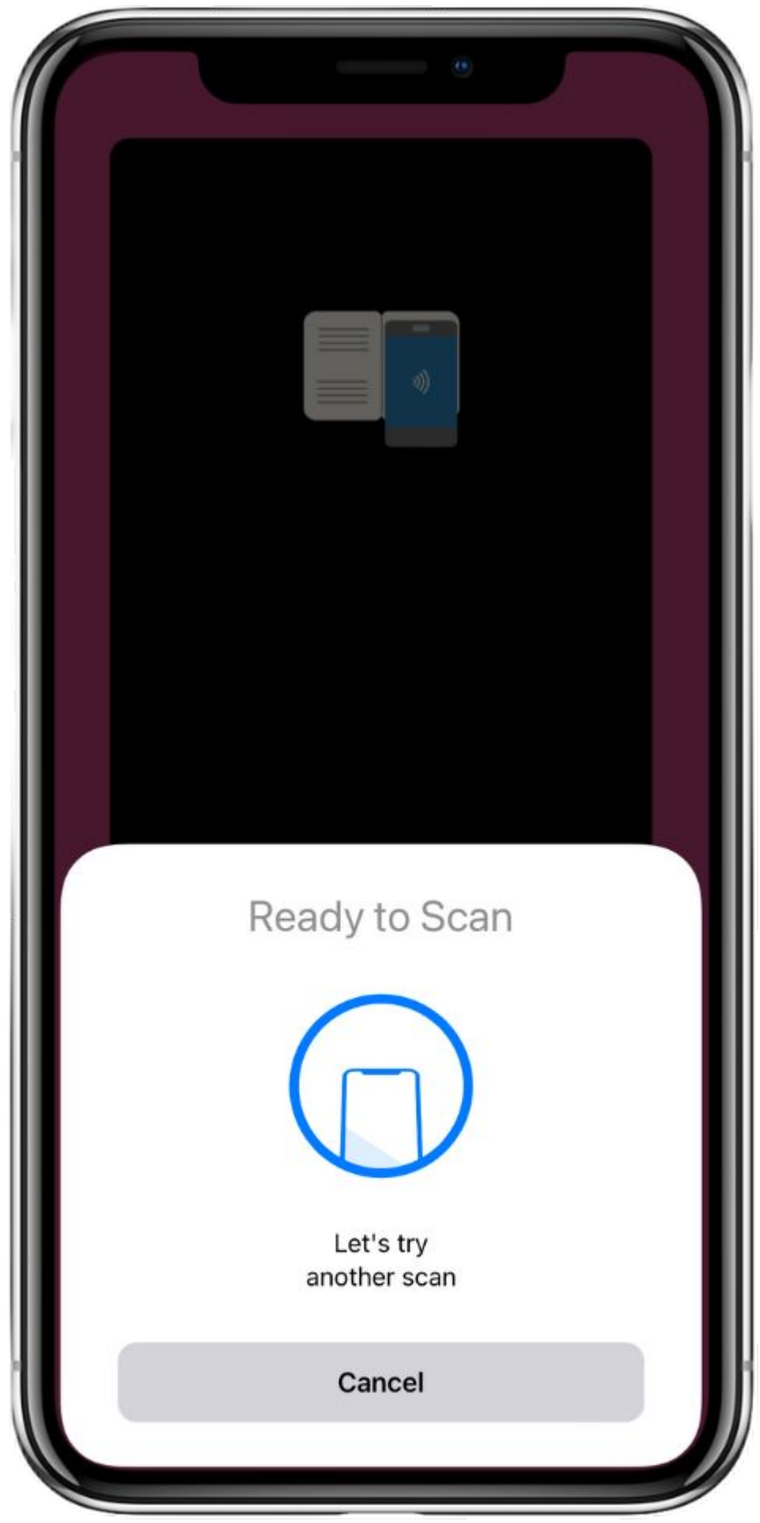


ZealiD

NFC scan: errors

Try another scan

Hold the phone steady while the NFC scan is in progress. You will be able to retry the NFC scan.



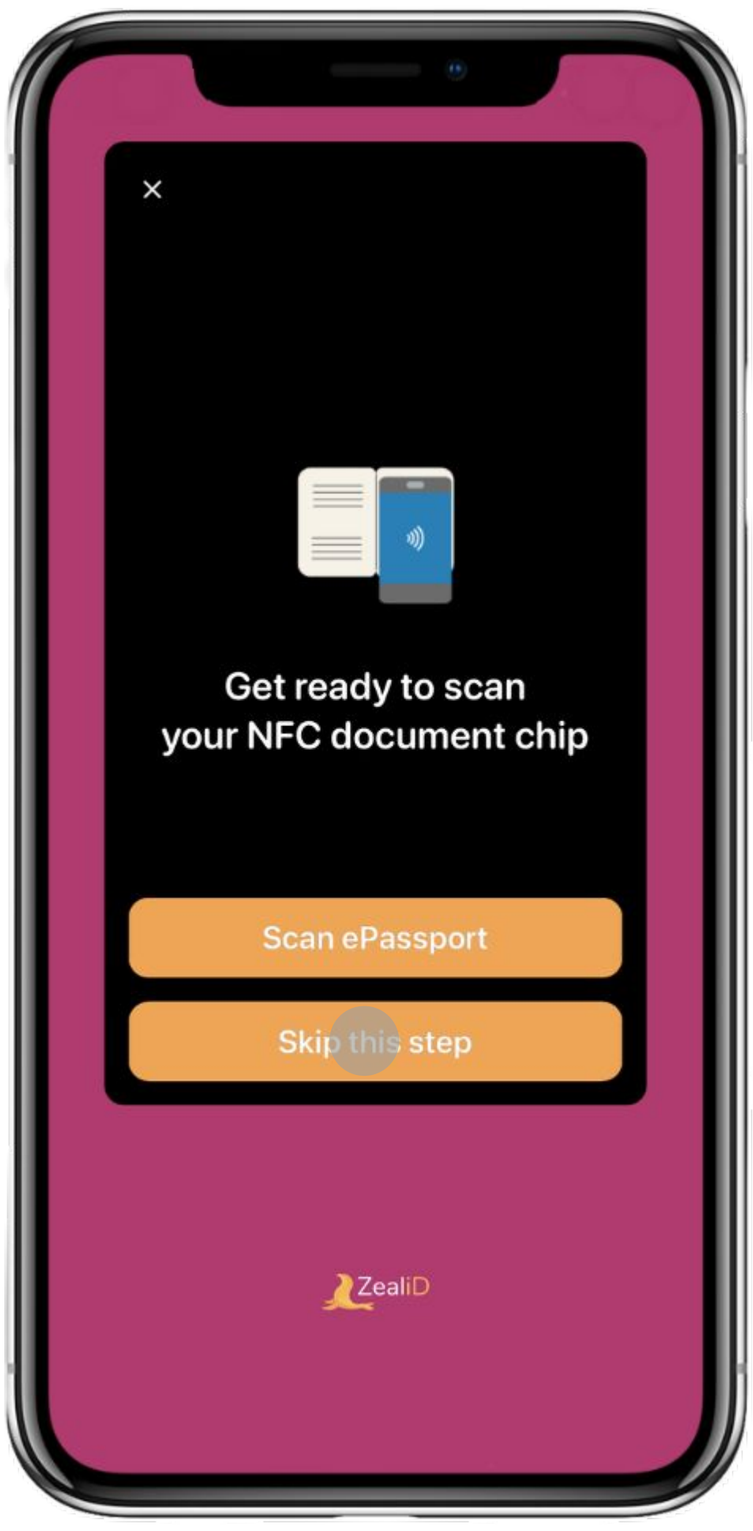
NFC chip unreadable

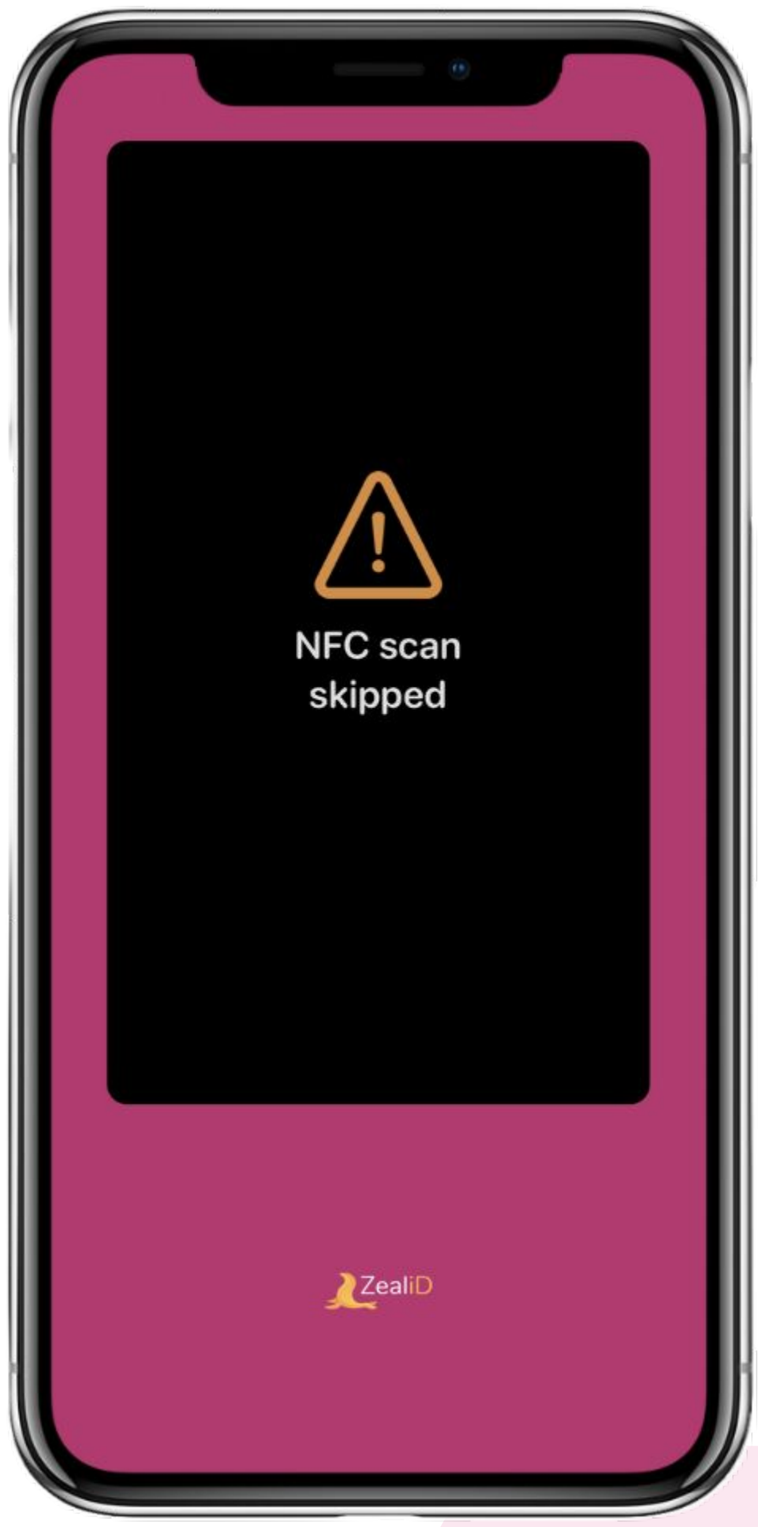
There was an error accessing the chip, or the chip might be damaged. You will be redirected to film a video of the document instead. See step 8b.

NFC scan: warning

NFC scan skipped

You chose to skip the NFC scan and film your ID document instead. See step 8b.





ZealiD

8b ID check: video

This step is applicable if the NFC chip is not embedded in an ID document or if NFC scanning was unsuccessful. Make sure to follow the recommendations provided. It helps to ensure that your application is received in good quality and meets the registration requirements.

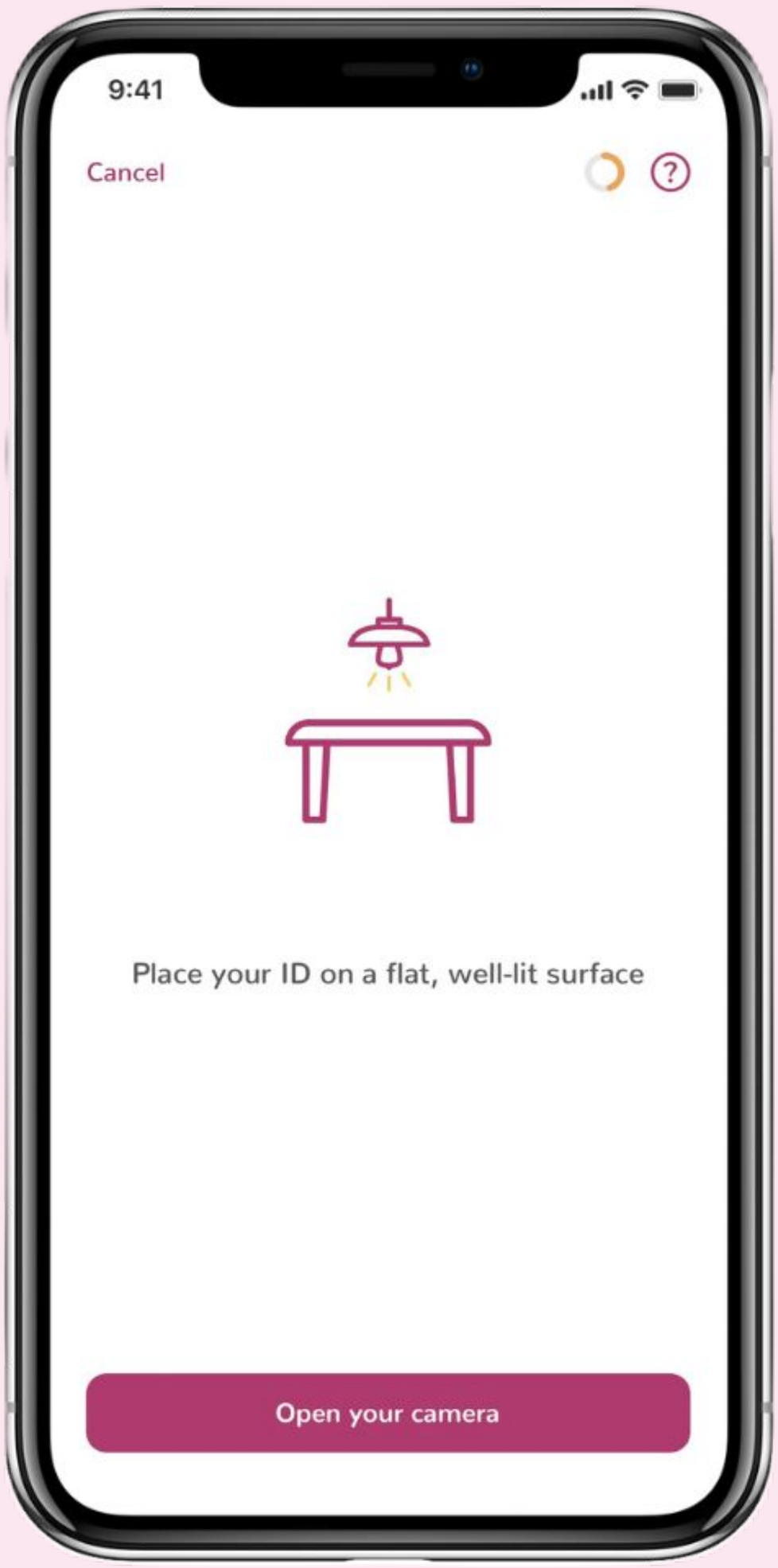
Passports

Place the biodata page of a passport on a flat surface and repeat the pattern shown in the application's instructions. Move the phone to follow the line as shown on the app. To ensure adequate lighting, the camera's flash will activate automatically.

Step 8b for ID Cards and Residence Permits

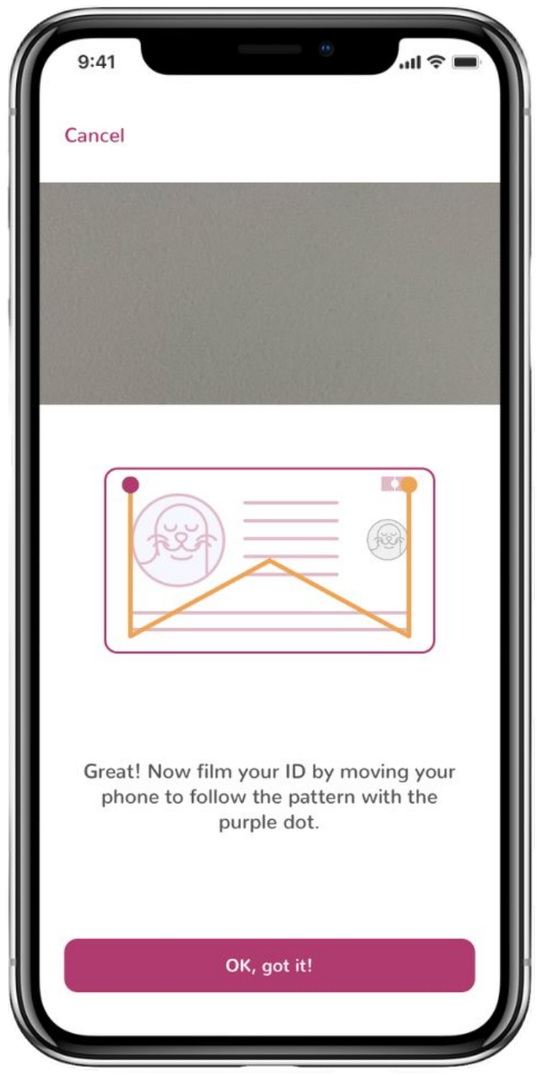
ZealiD

8b ID check: video

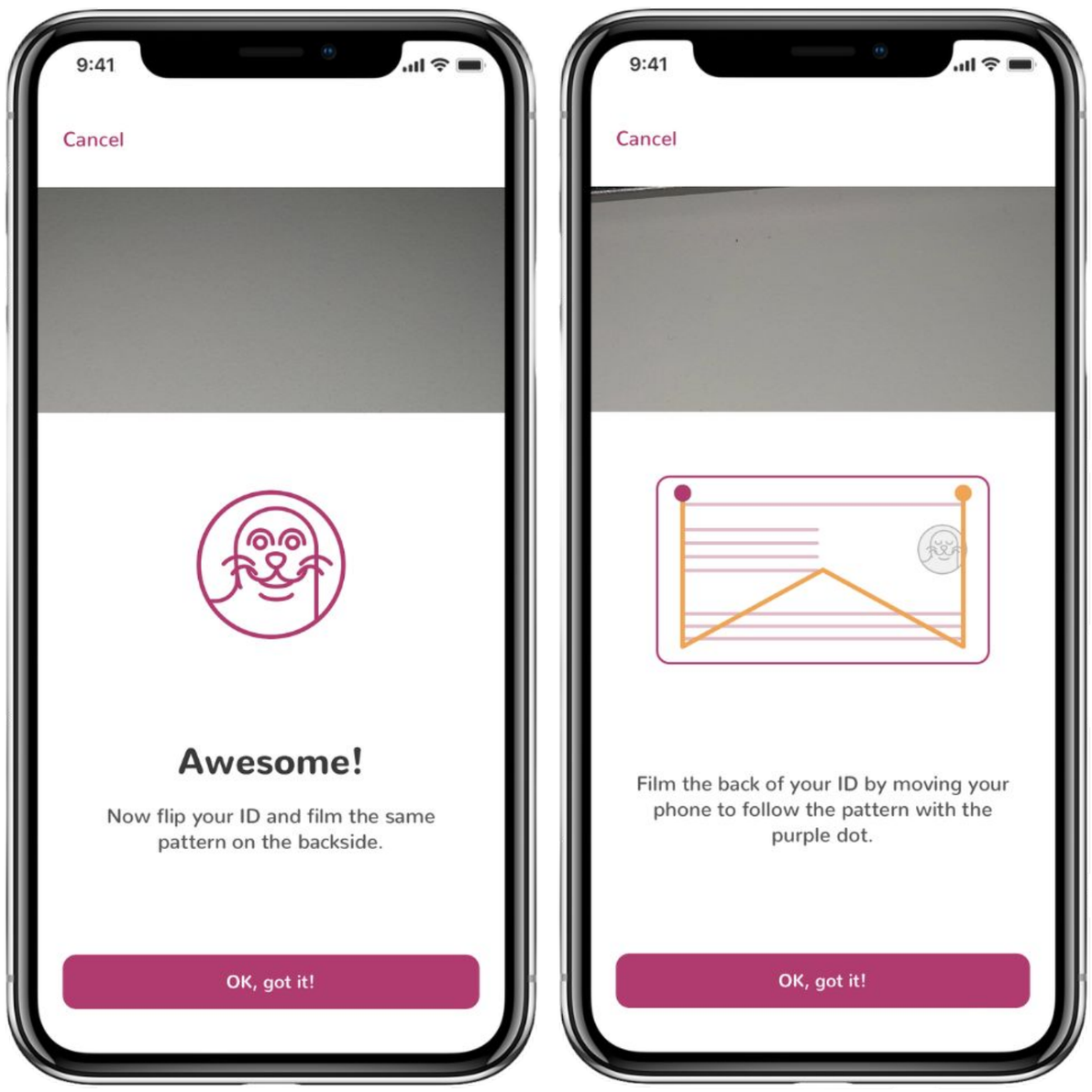


ID Cards and Residence Permits

Film the front side repeating the pattern shown in the app.



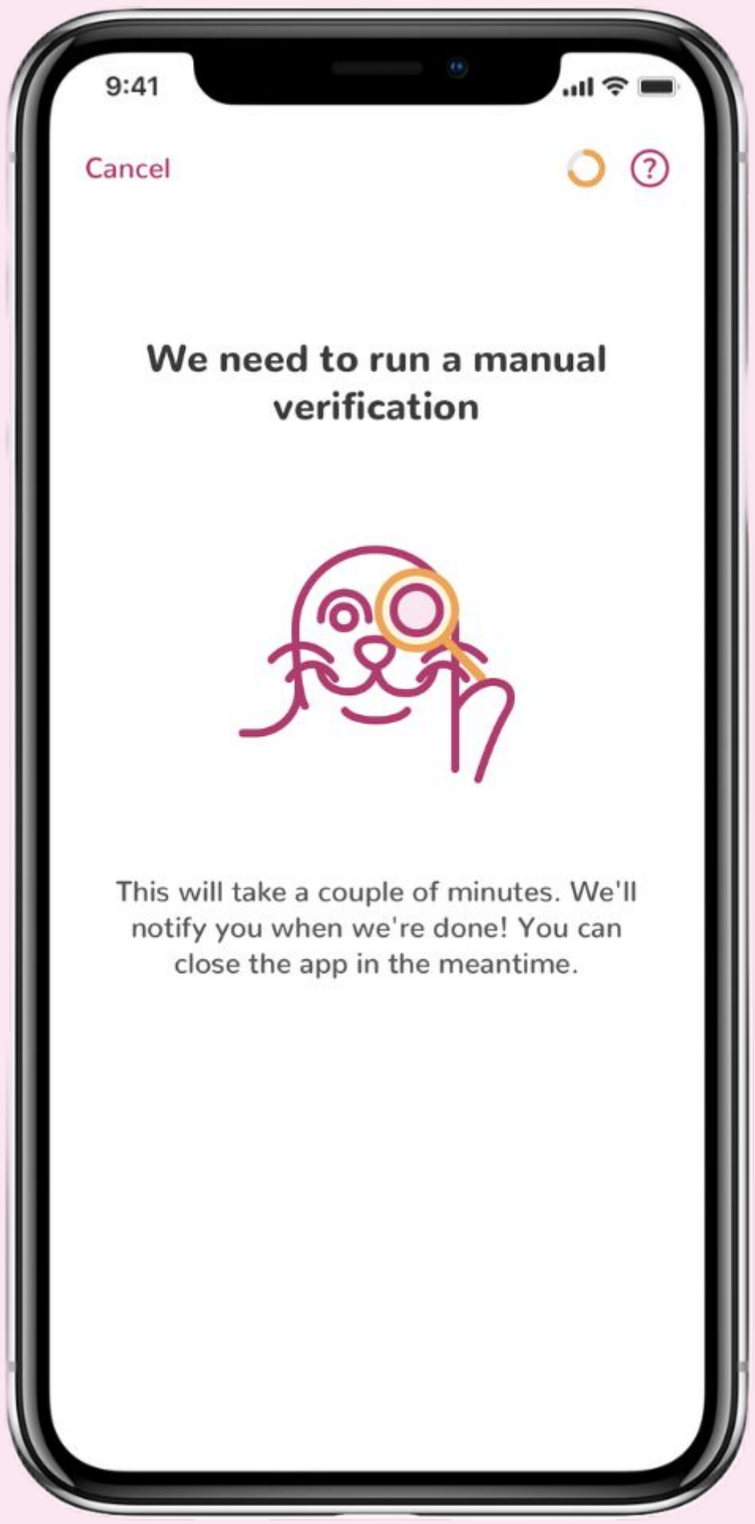
Flip the card to film the back side.



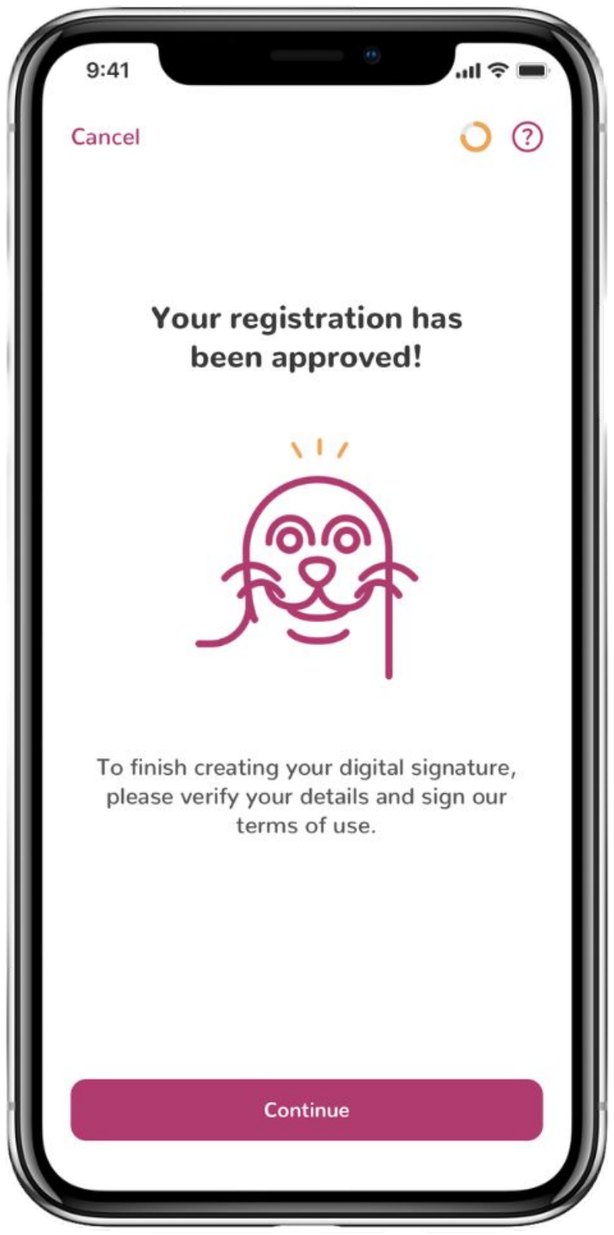
ZealiD

9 Manual Vetting

Every application is reviewed by the Manual Vetting Team. A highly trained Specialist will check the received data, inspect the document validity and authenticity to prevent fraud. Manual review takes up to 5 minutes. Once the review is complete, a push notification is received (if enabled). Alternatively, application status can be seen in the mobile app.

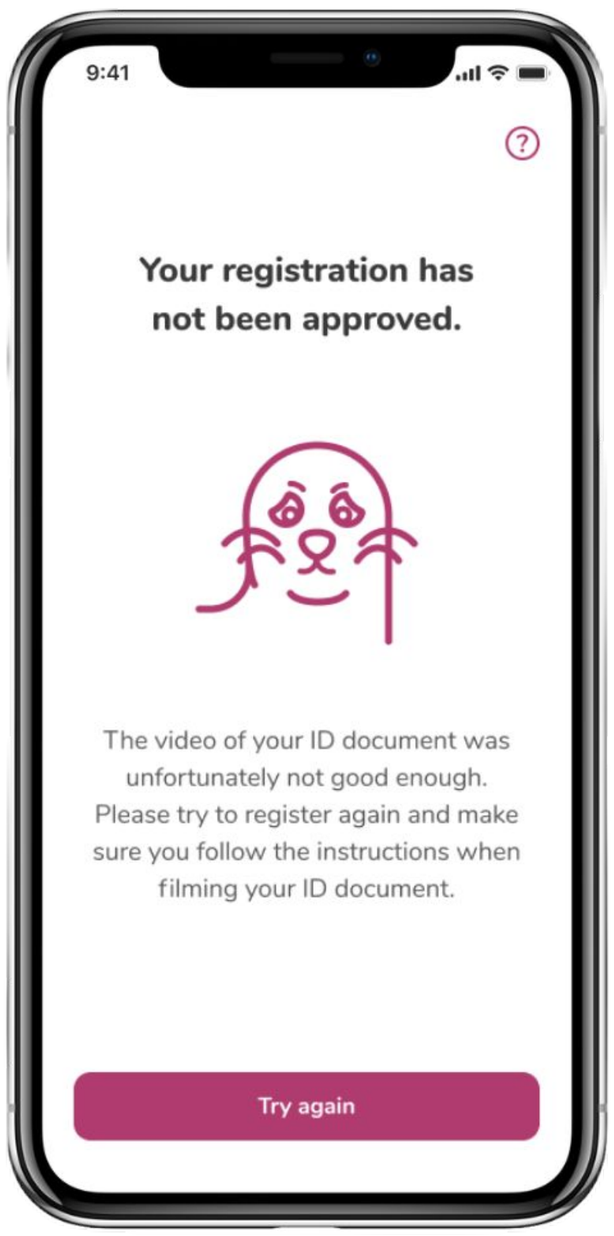


Approved



Declined

(see the next page for possible reasons)



ZealiD

Reasons to decline an application

Video pattern was not followed	During the registration process the assigned pattern was not followed
Identification process cancelled	The user has cancelled the registration process by selecting the “cancel” button
Document photo was not in frame	The ID document does not fit into the frame and not all the provided information in the document is visible
Document was blurry	The ID document is too blurry and essential information is not readable
Document is damaged	The ID document has significant damage
Document is expired	The ID document used during the registration process is expired
Document is not supported	The document used during the registration process is not supported
Facial image and document photo mismatch	The person in the selfies and the document holder’s image of the document do not match
Improper lighting	Some parts of the document were unverifiable or unreadable due to light reflections on the document
Missing document photos	One of the photos of the ID document is missing. E.g. only front side of ID card provided

ZealiD

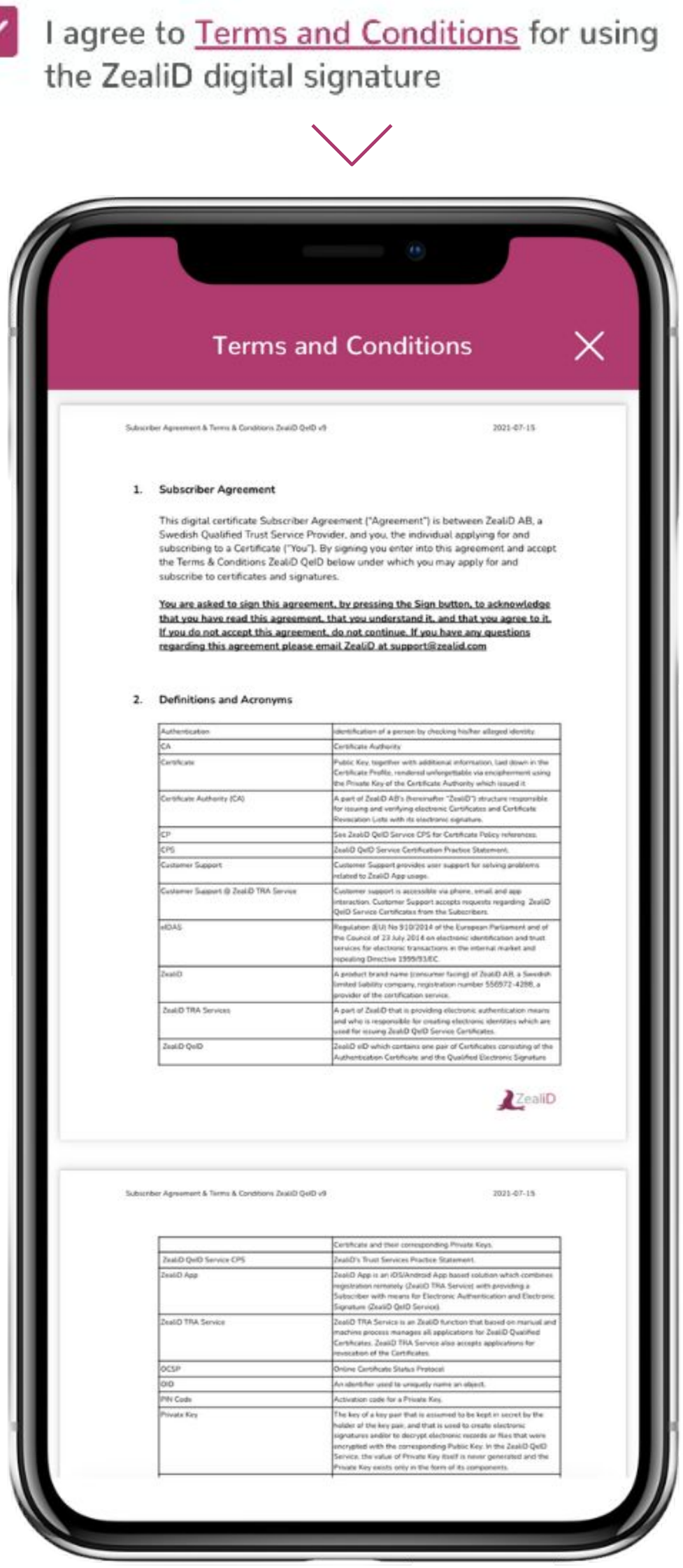
Reasons to decline an application

We couldn't detect an original document	The ID document used during the registration process is not in its original form
Obscured parts of the document	Some information is unverifiable due to some parts of the ID document being covered or hidden
Unverified document security features	Application was declined because some of the security elements of the ID document could not be verified
You are a minor (under 18 years old)	In order to use ZealiD services, a natural person must be 18+ years old
More than one person visible in the photo	More than one person was identified during the registration process
Document is invalid	After searching the public records, it is identified that the ID document is reported as lost or stolen
Only one side of ID document filmed	Application is declined when only one side (the front or back side) of the ID card or residence permit is filmed

ZealiD

10 Confirm details

A full name and serial number will be provided on the screen. Check and confirm that the details are correct, agree to the terms and conditions of signature usage. A qualified certificate will be generated automatically.



ZealiD

Structure of Serial Number

ETSI EN 319 412-1

1. 3 character natural identity type reference:

- "PAS" for identification based on passport number.
- "IDC" for identification based on national identity card number.
- "PNO" for identification based on (national) personal number (national civic registration number).
- Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).

2. 2 character ISO 3166 [2] country code

3. hyphen-minus "-"

4. identifier (according to country and identity type reference)

E.g., A user has registered with a Swedish Passport:

PNO ([1]identification based on personal number) SE ([2]country code for Sweden) - ([3]hyphen-minus) [4]personal number 820821-2384

Serial Number: PNOSE-820821-2384

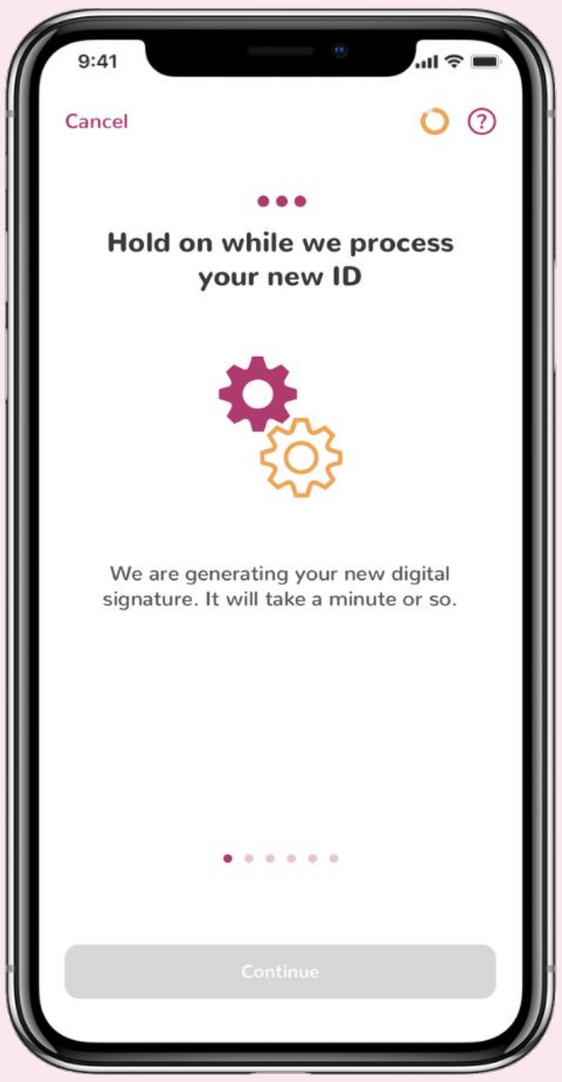
www.zealid.com

ZealiD

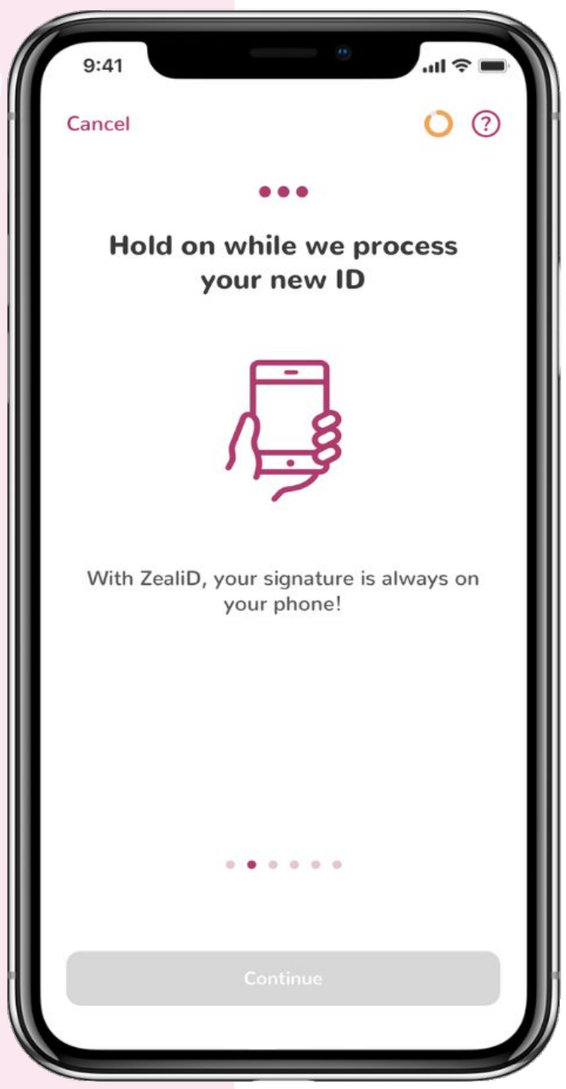
11 Certificate generation

A qualified certificate will be generated automatically. Wait until the app loads and proceed further.

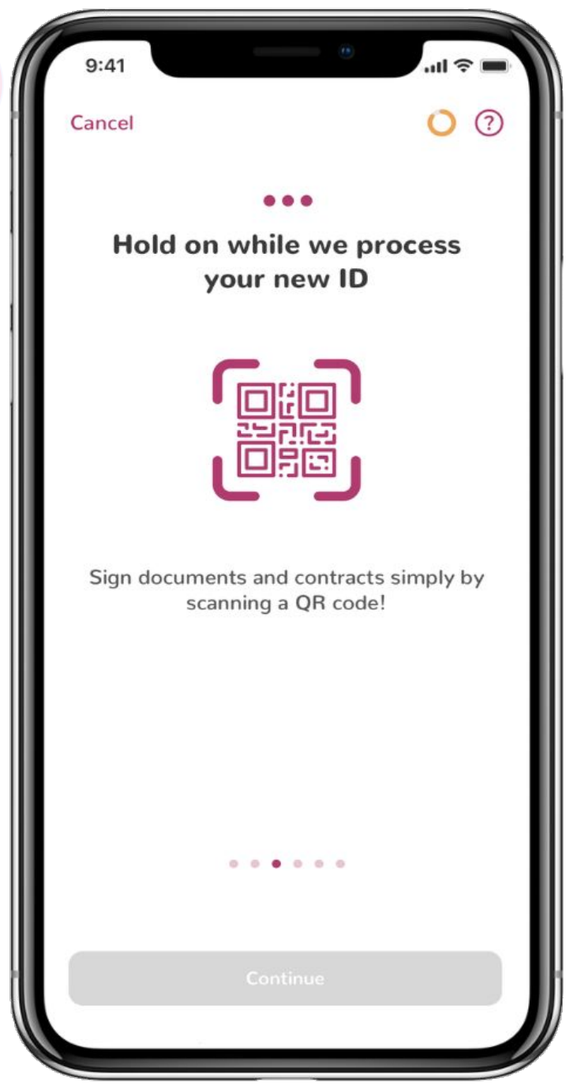
1



2

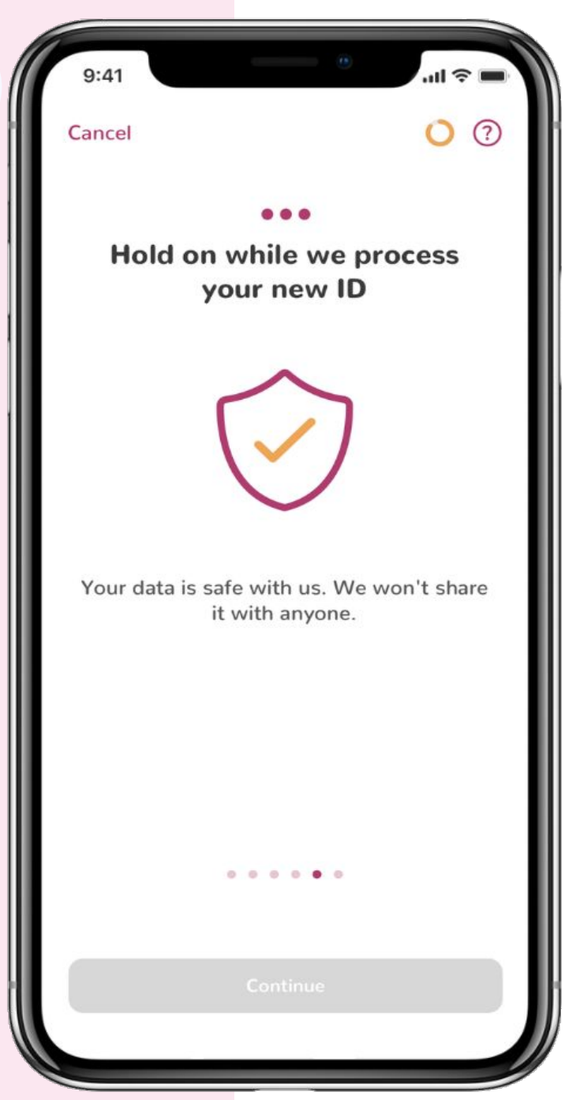


3

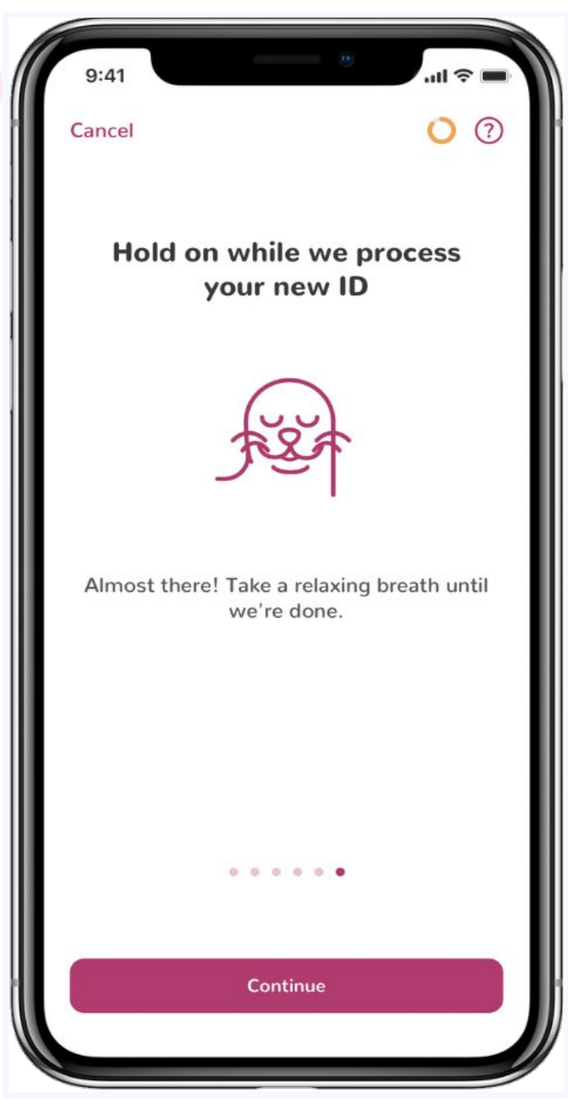


4

5



6

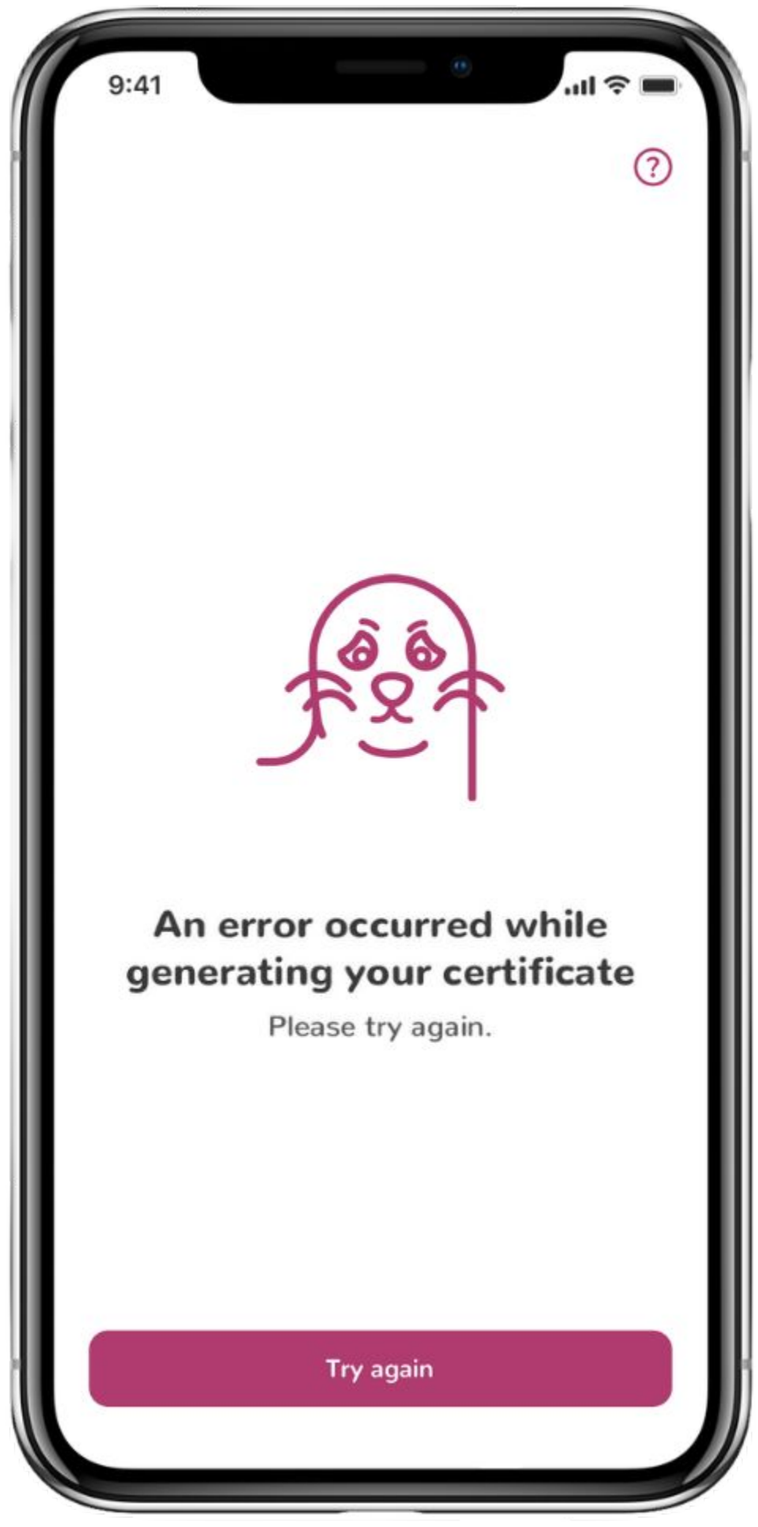


ZealiD

Certificate generation: errors

Error while generating certificate

You have successfully passed the registration process, but an error occurred in the certificate generation process. Click “Try again”. to repeat the certificate generation.

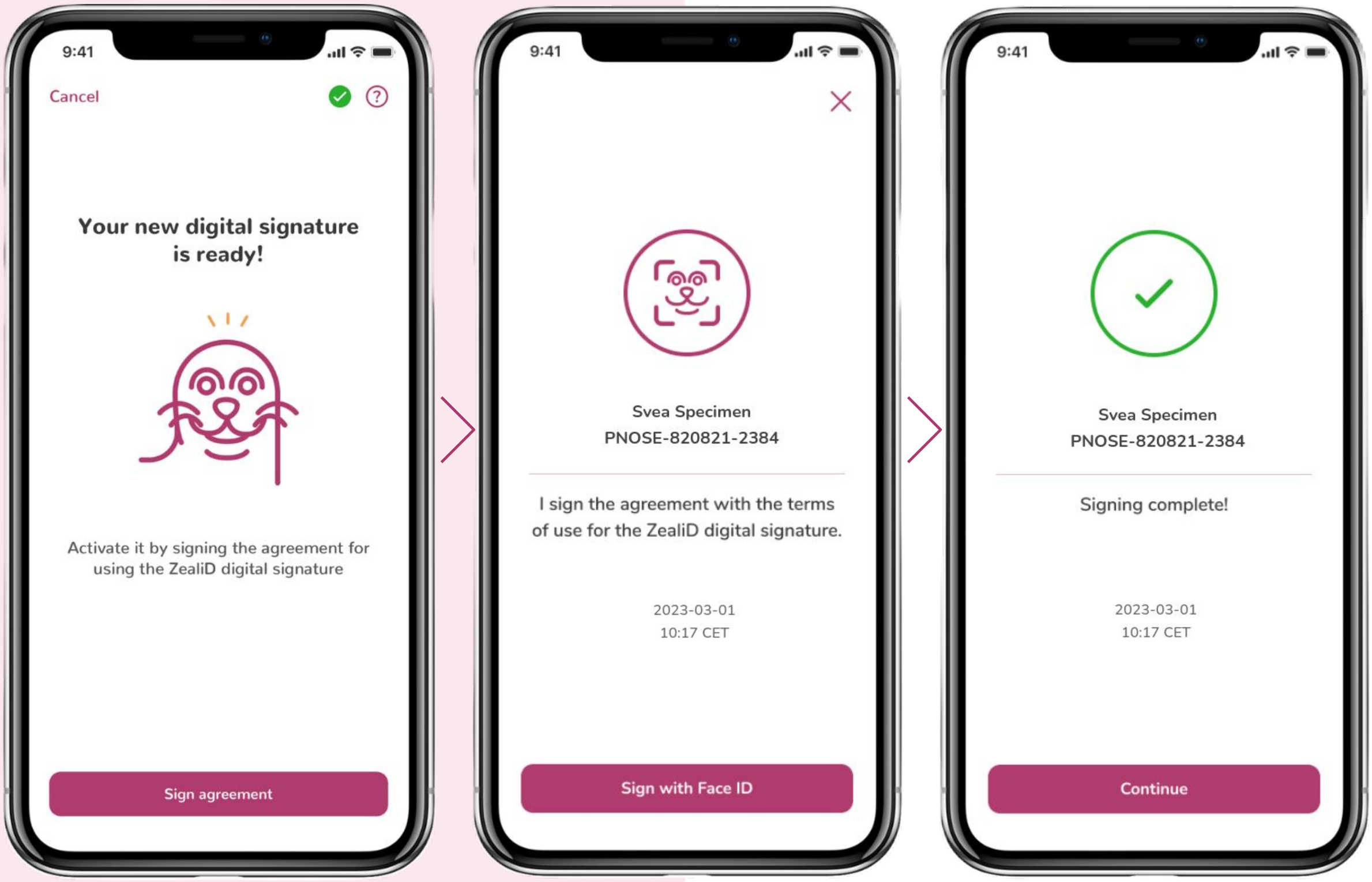


www.zealid.com

ZealiD

12 Activate signature

A qualified electronic signature is ready. Activate it by using Face ID or Touch ID.

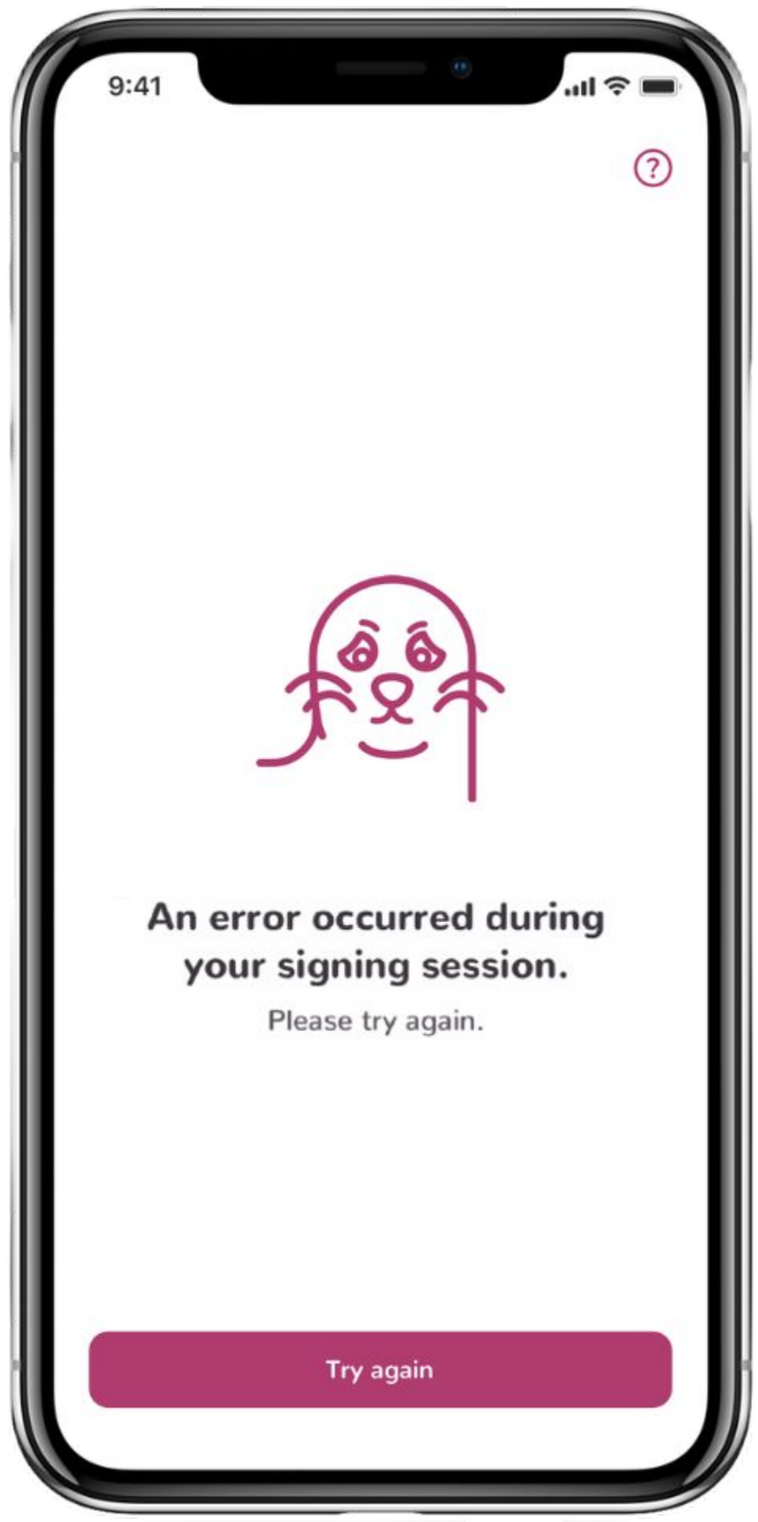


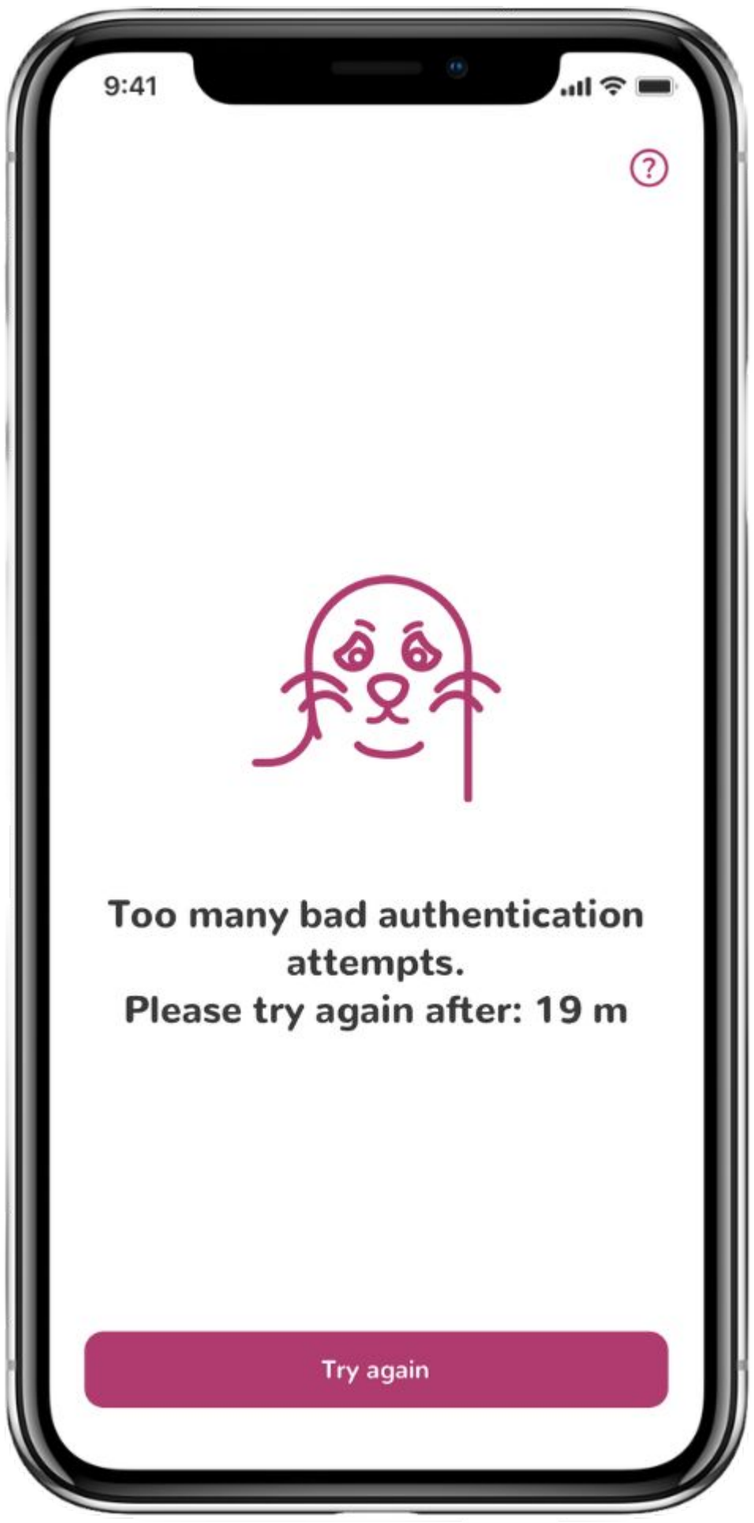
ZealiD

Activate signature: errors

Error during the signing session

There was an error during the agreement signing process. Click “Try again”.





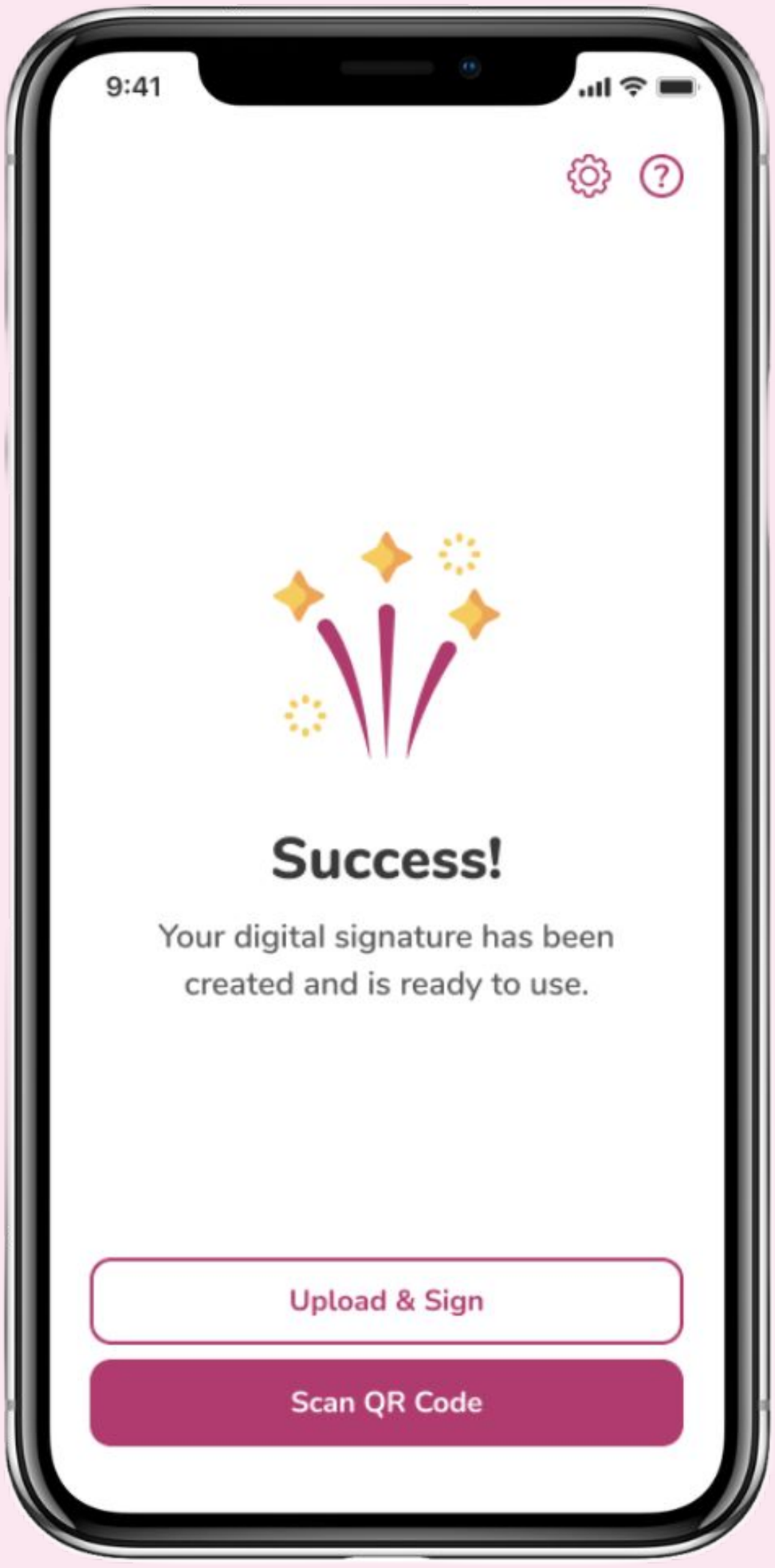
Too many bad authentication attempts

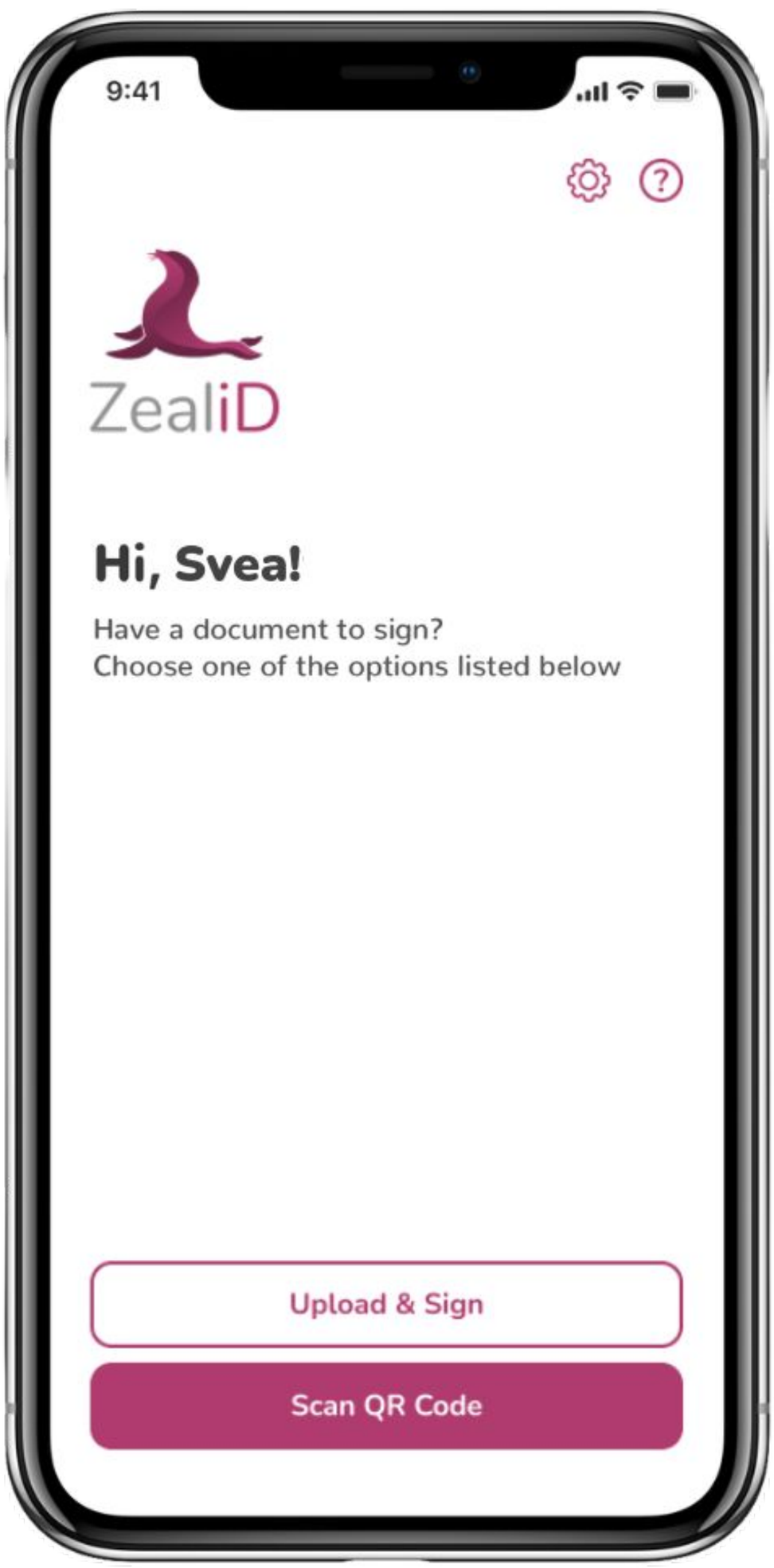
Face ID/Touch ID was not recognized 3 times in a row. Wait the specified time and try again. If biometric authentication fails again, you will need to wait 12 hours and retry biometric authentication. If biometrics fail again, you will be asked to redo the registration process.

ZealiD

13 Success

The registration process is now complete. Click “Scan QR code” in the mobile app and scan a QR code provided in the signing platform to authorize qualified electronic signatures.



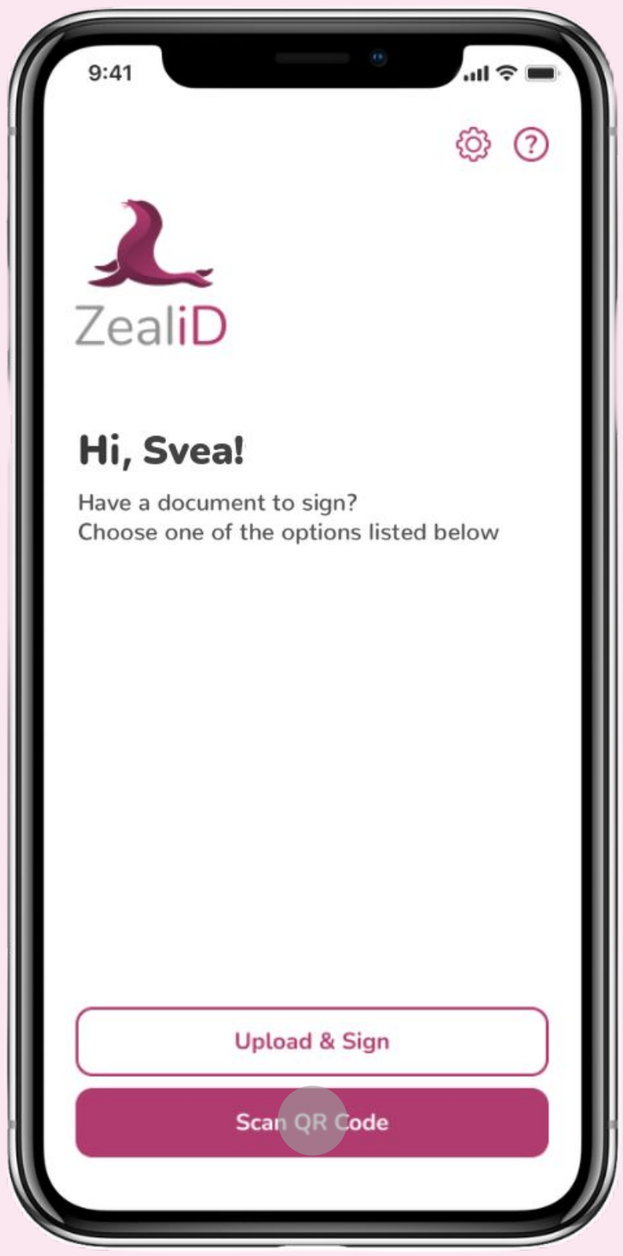


ZealiD

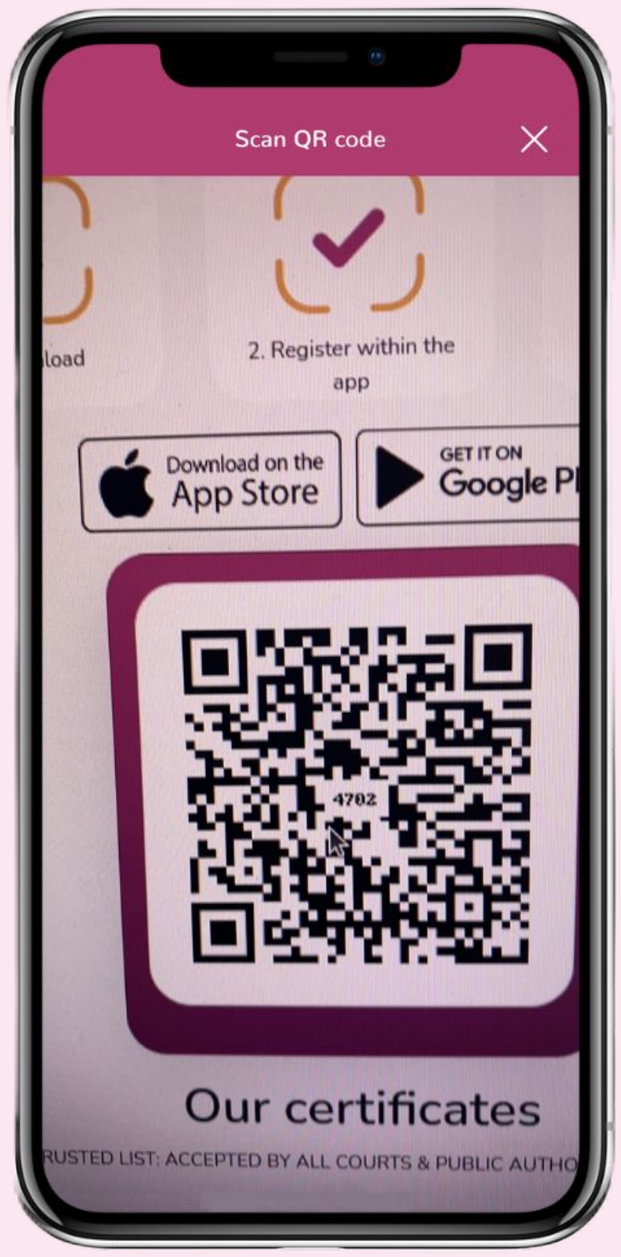
QR code scanning

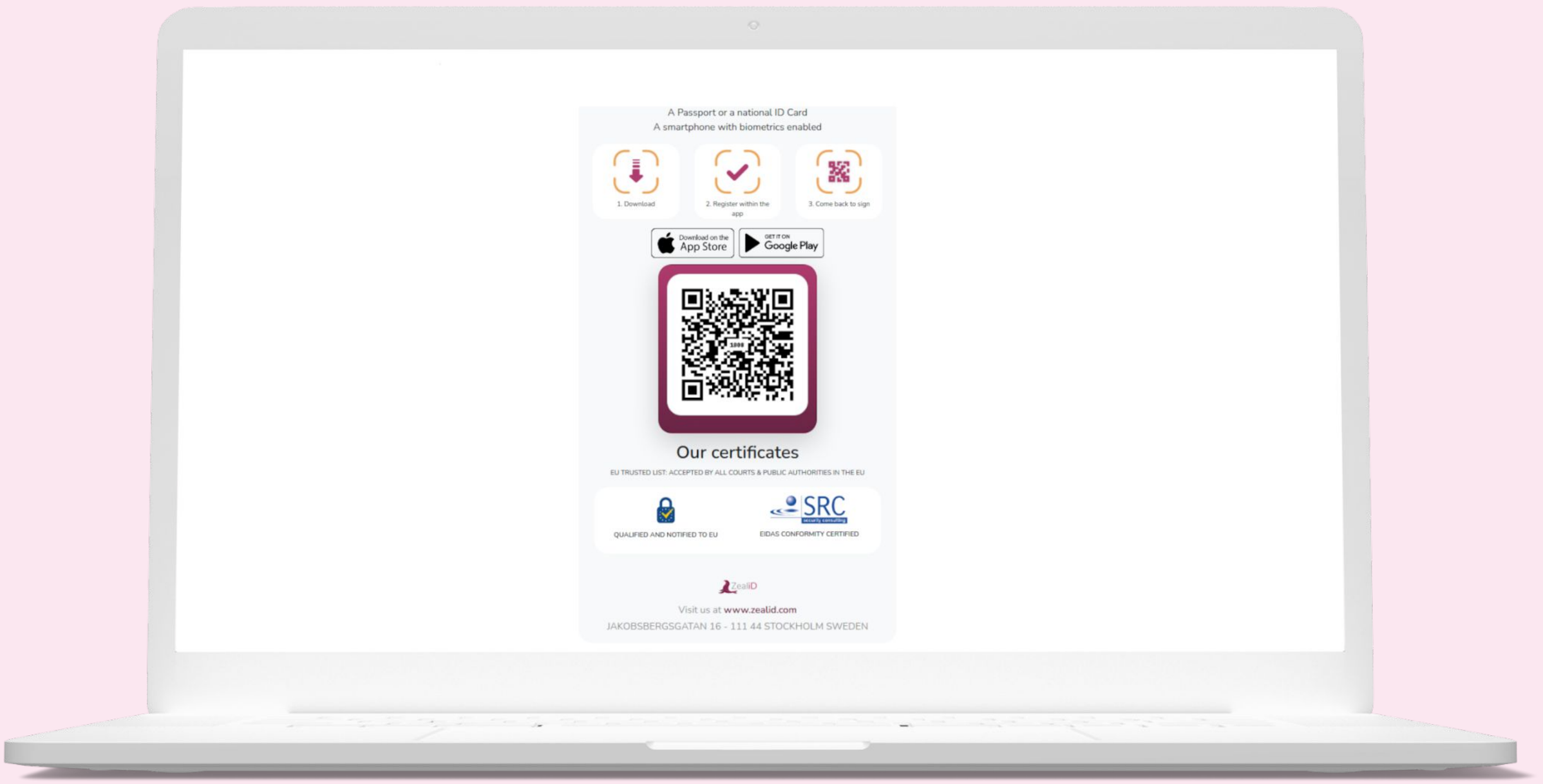
Open the ZealiD app, tap “Scan QR Code” button to scan a QR code which is presented in your signing platform. You will be asked to authorize your login attempts and signatures with Face ID/Touch ID.

1



2





A preview of a QR code in a signing platform

ZealiD

References

1. eIDAS
2. eSignature FAQ
3. EU Trusted List
4. DSS Demo WebApp
5. ZealiD Repository
    5.1. Service Certificate Practice Statement
    5.2. Privacy Policy
    5.3. Terms & Conditions Subscribers ZealiD TRA Service
6. Certificate Revocation
7. ZealiD Coverage
8. Supported ID documents
9. Registration Demo
10. ZealiD Help Center

ZealiD

APEX

Term	Definition
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 20 ZealiD AB Document name ZealiD QeID Certificate Practice Statement (CPS) Owner CEO Class P Category Steering Date 2021-10-01 Revision 17 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
EU Trusted List	A publicly available tool provided by the European Commission. It allows the user to browse through the information present in the Member States national Trusted Lists (TLs), as well as in the European Commission central list (named List of Trusted Lists (LOTL)).
DSS WebApp	An open-source software library for digital signature creation, validation, and extension, designed to help digital solutions achieve compliance with the eIDAS Regulation.
Qualified Trust Service Provider	A TSP who provides one or more qualified trust services (QTS) and is granted the qualified status by the national supervisory body.
Certificate Authority	A part of the trust service provider’s structure responsible for issuing and verifying electronic Certificates and Certificate Revocation Lists with its electronic signature.
Registration Authority	Entity that is responsible for identification and Authentication of Subjects of Certificates. Additionally, the Registration Authority may accept Certificate applications, check the applications and/or forward the applications to the Certificate Authority.
Qualified Certificate	A certificate for electronic signatures that is issued by the qualified trust service provider and meets the requirements laid down in Annex I of the eIDAS Regulation.
Qualified Electronic Signature	Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a Qualified Certificate for electronic signatures.
Biometric authentication	Touch ID or Face ID used to access a mobile device.
Biodata page	A page in a passport containing personal data such as name and surname, date of birth, document number, etc.
Valid ID Document	One of the supported ID documents by ZealiD that includes passports, identification cards and residence permits.
Manual Vetting	Manual review of submitted applications by ZealiD users.

Contacts

Sales
sales@zealid.com

Customer Care
support@zealid.com

Germany

ZealiD GmbH
c/o Bird & Bird
Maximiliansplatz 22
80333 Munich
HRB 122732

Sweden

ZealiD AB
Reg. no. 556972-4288
Box 3437
10368 Stockholm

Lithuania

Identitrade UAB
Reg. no.304478730
Saltoniškių 2C
Vilnius 08126