

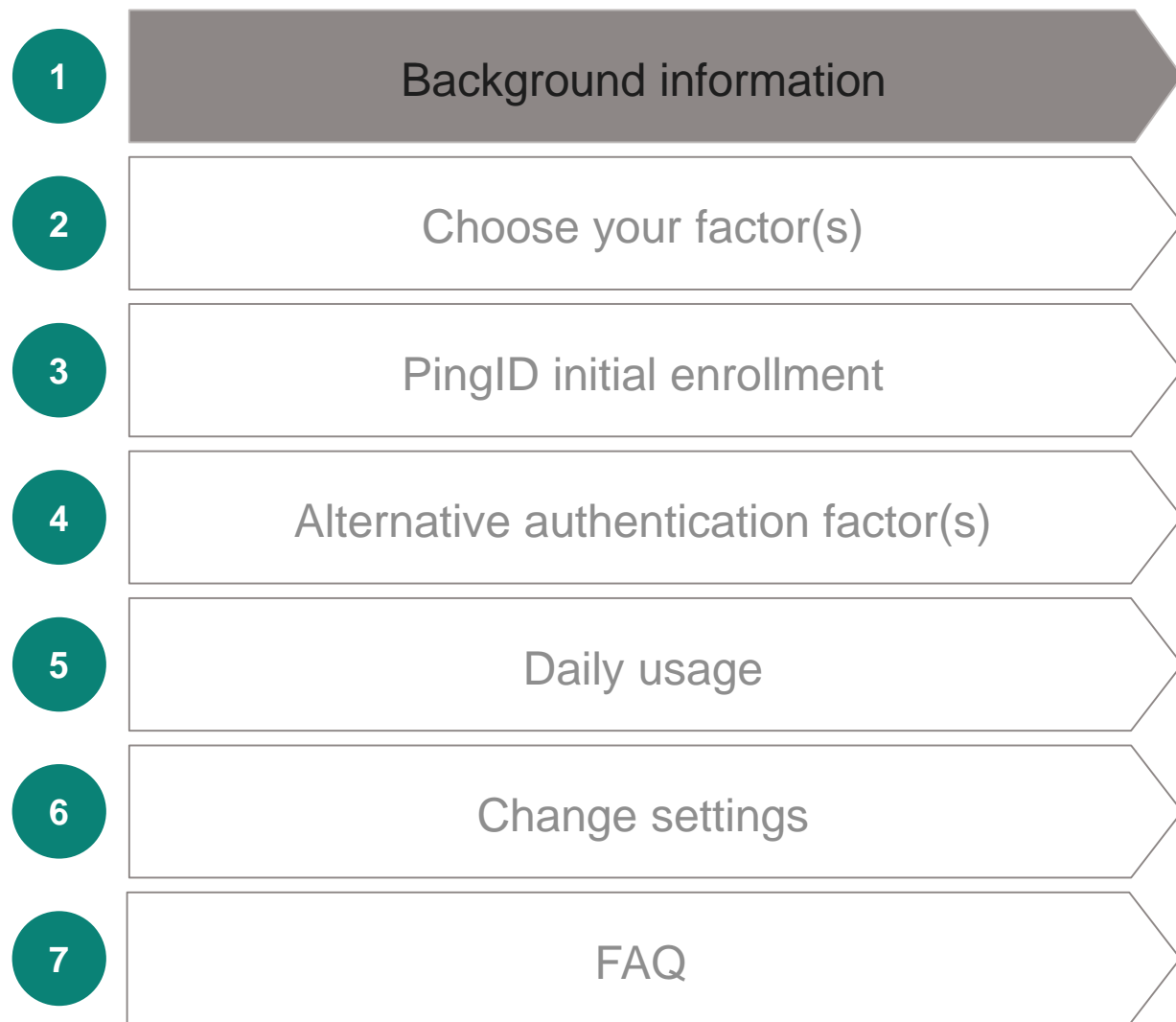


Step-by-Step guide to enroll Multifactor Authentication (MFA) for Customers

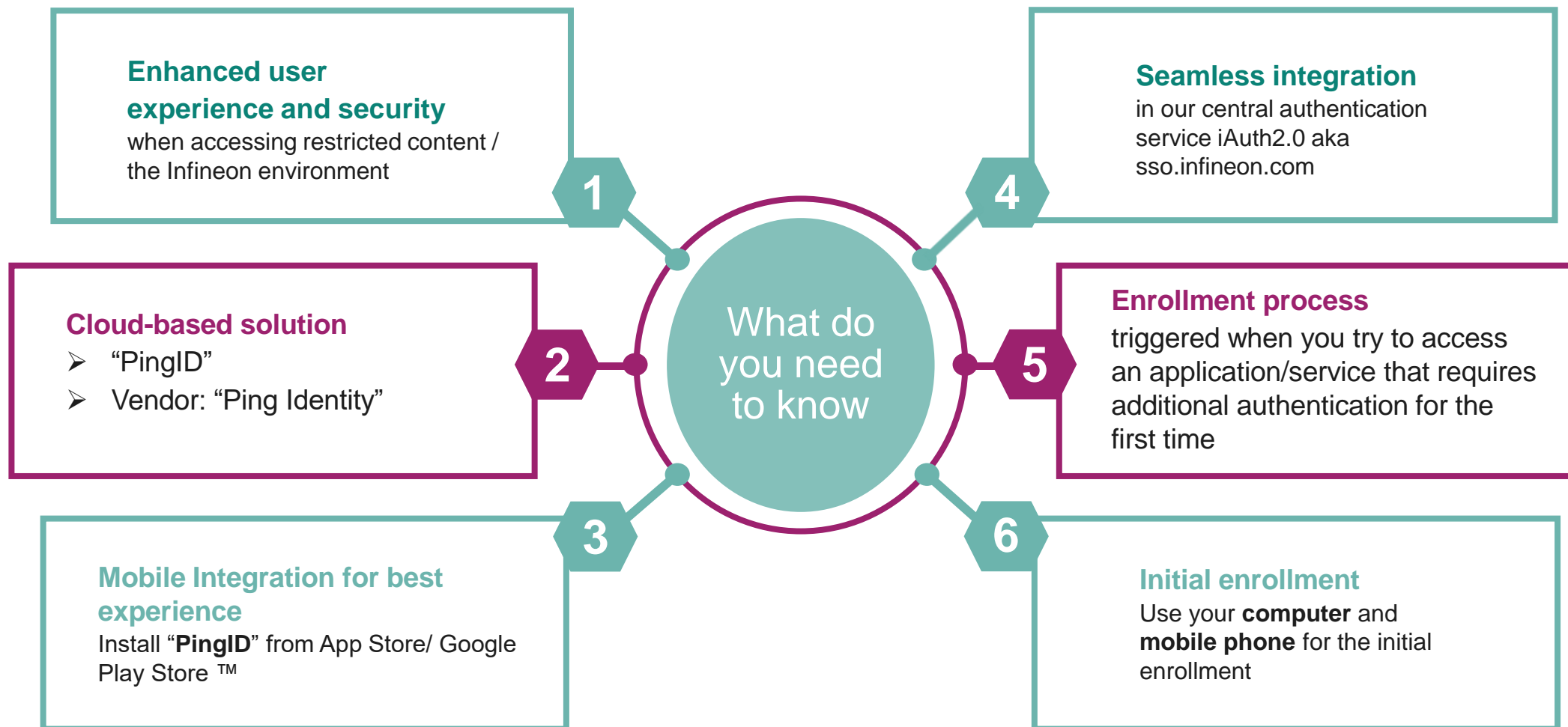
Infiniteon Technologies AG



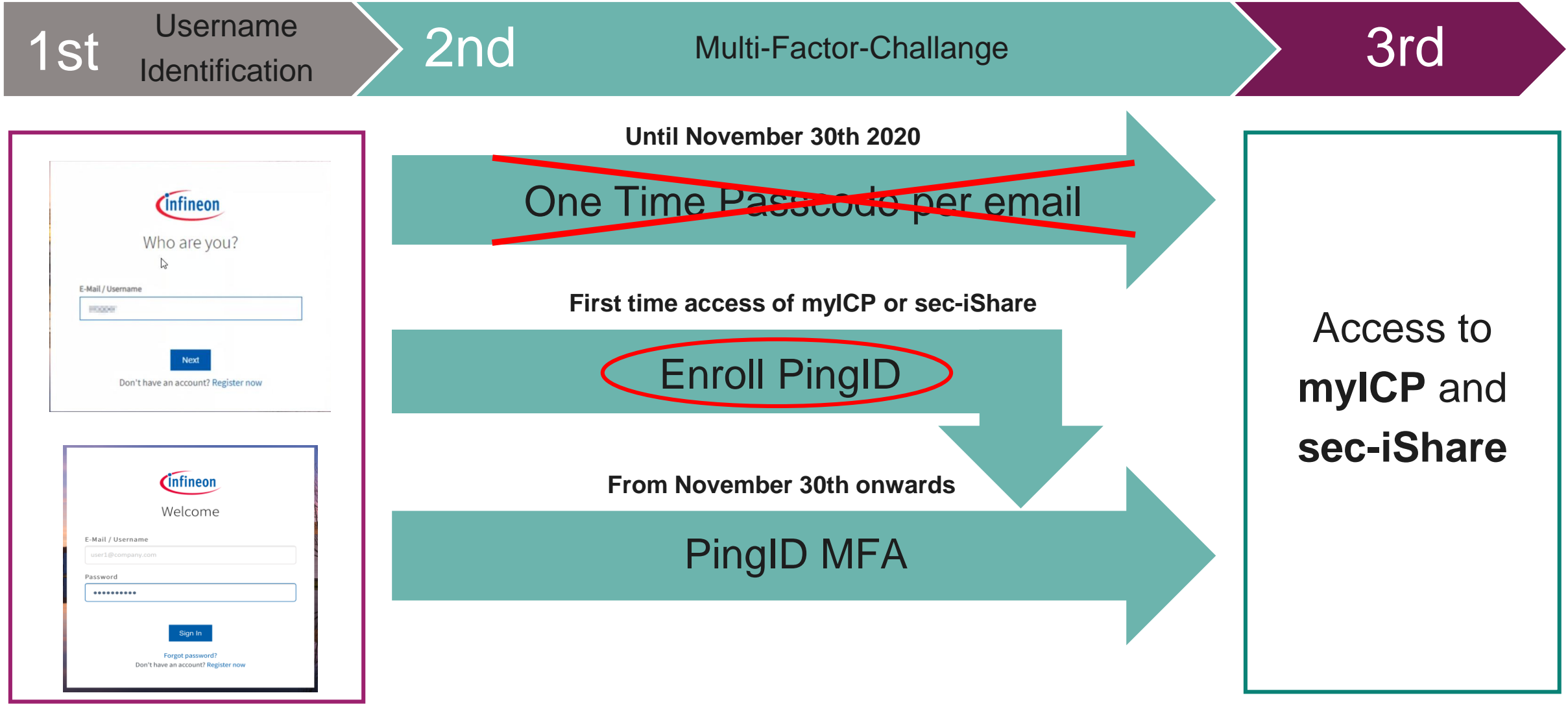
Overview



The six key infos about the new MFA solution



What will change



Motivation



One-Time-Password (OTP) via email caused a lot of problems

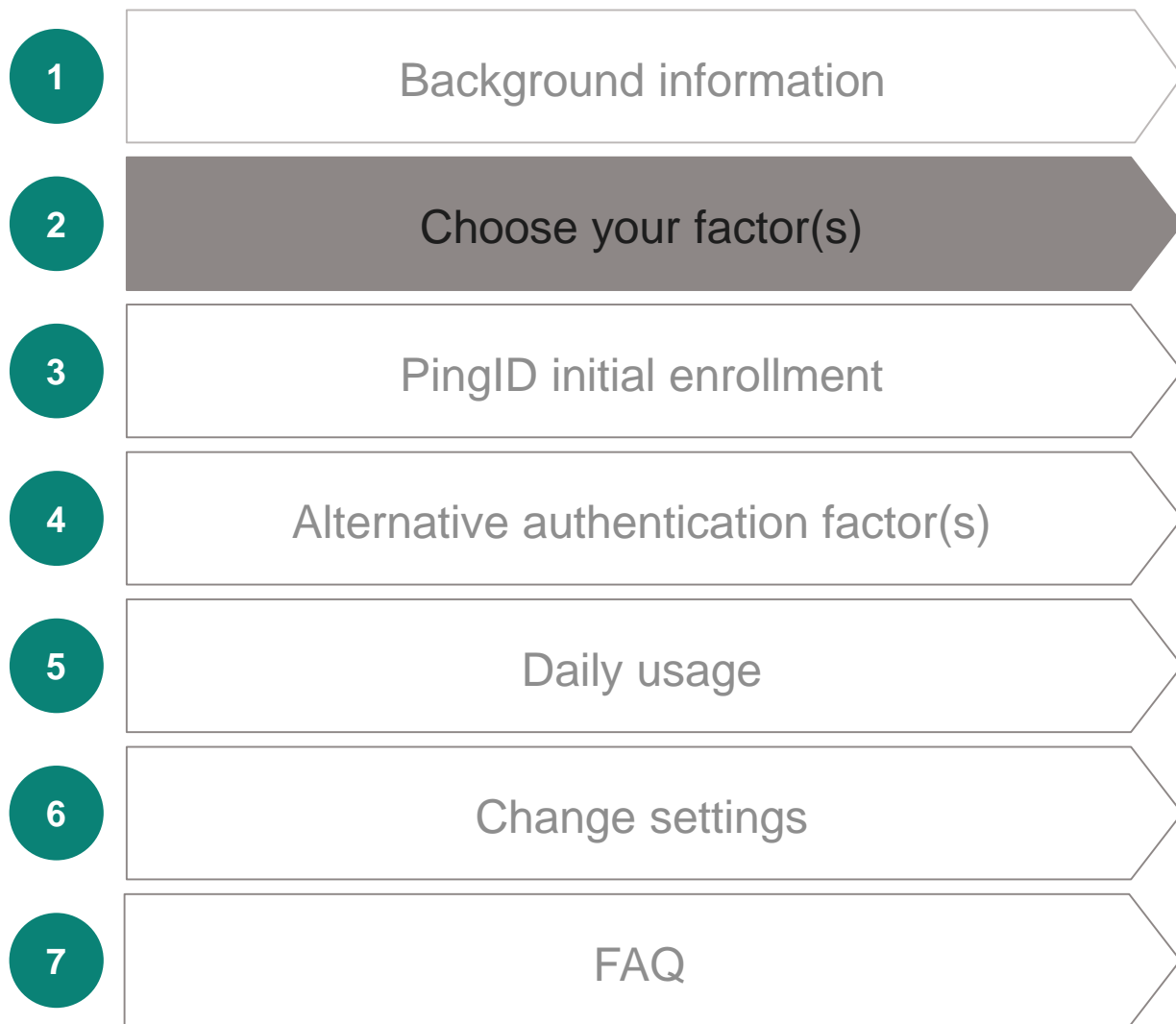


Modern Multi-Factor-Authentication solution with flexibility and improved user-experience



Modern Multi-Factor-Authentication solution with flexibility and improved user-experience

Overview



What factor fits?

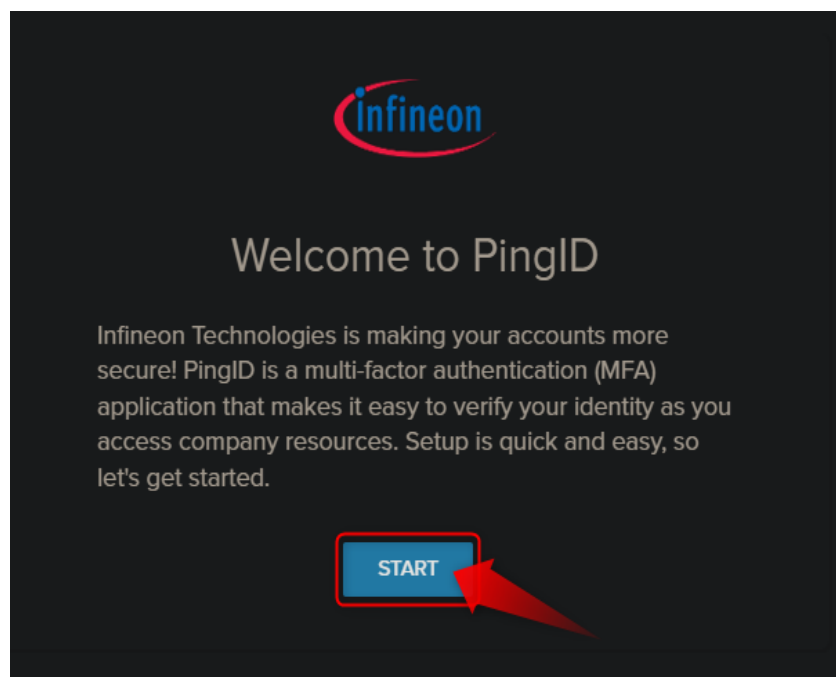
I want to use my I take the factor	Smart-Phone 	Cell-Phone 	Wired-Phone 	Yubikey Token 	Hardware Security Token (e.g. FIDO2)	Personal Computer (e.g. Windows OS)
PingID App*						
SMS		*				
Voice						
Yubikey						
Security Key/ Passkey						
Authenticator						**

* Provider needs to support this

** Installation of Authenticator Software is needed (e.g. 2 Factor Authenticator)

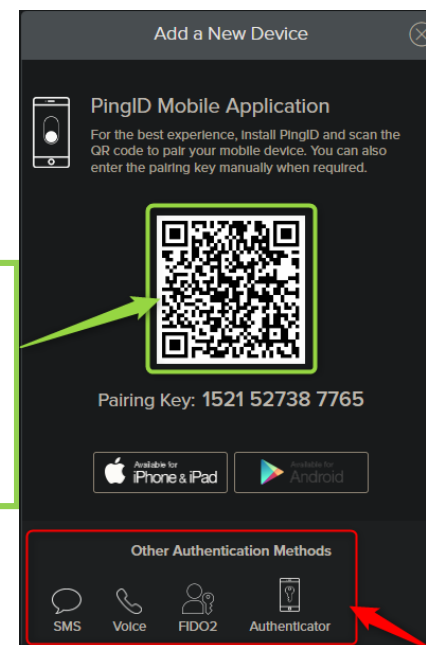
PingID Multifactor Authentication solution lets you choose

When you login the first time to the **myInfineon Collaboration Platform** (MyICP) or an **Secure-iShare**, you will be redirected to the **PingID** system



It will help you to choose your 2nd factor to login, while the **PingID-App** is the preferred way in terms of security and usability. However you can also choose an alternative method* (for options and setup please look [here](#))

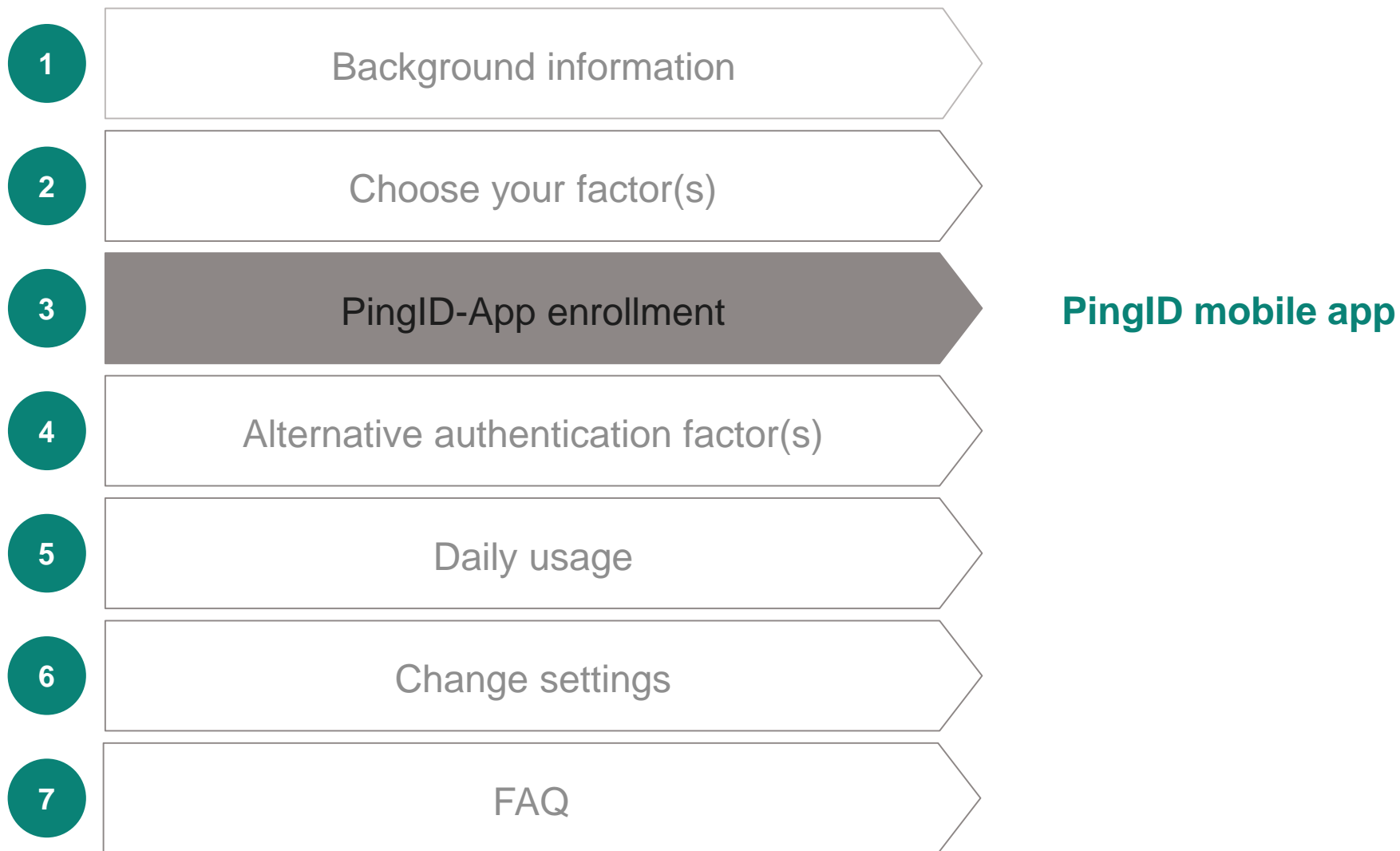
QR-Code to enroll with the PingID-App (preferred)



Select other authentication method: SMS, Voice, FIDO2 or Authenticator App

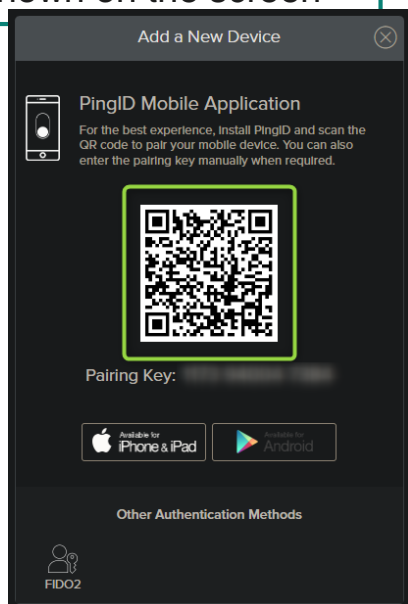
* You can enroll up to 10 methods/devices

Overview

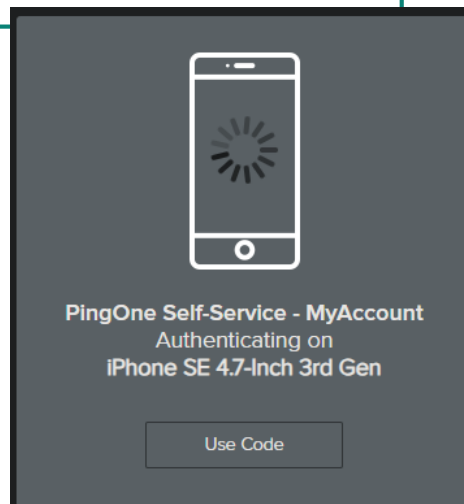


Initial enrollment PingID App

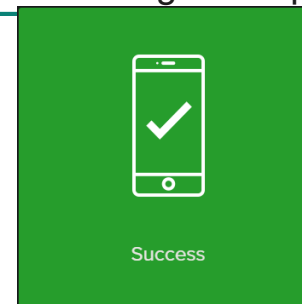
1. Open the PingID-App on your mobile device and scan the QR-Code shown on the screen



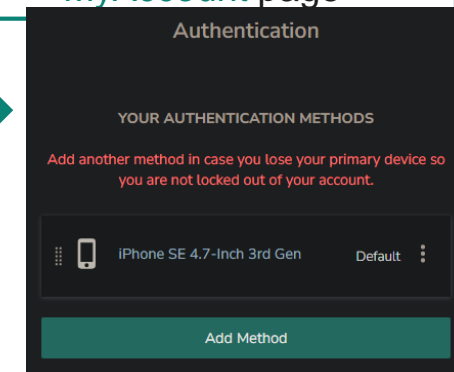
2. Confirm authentication on your phone with TouchID or FaceID



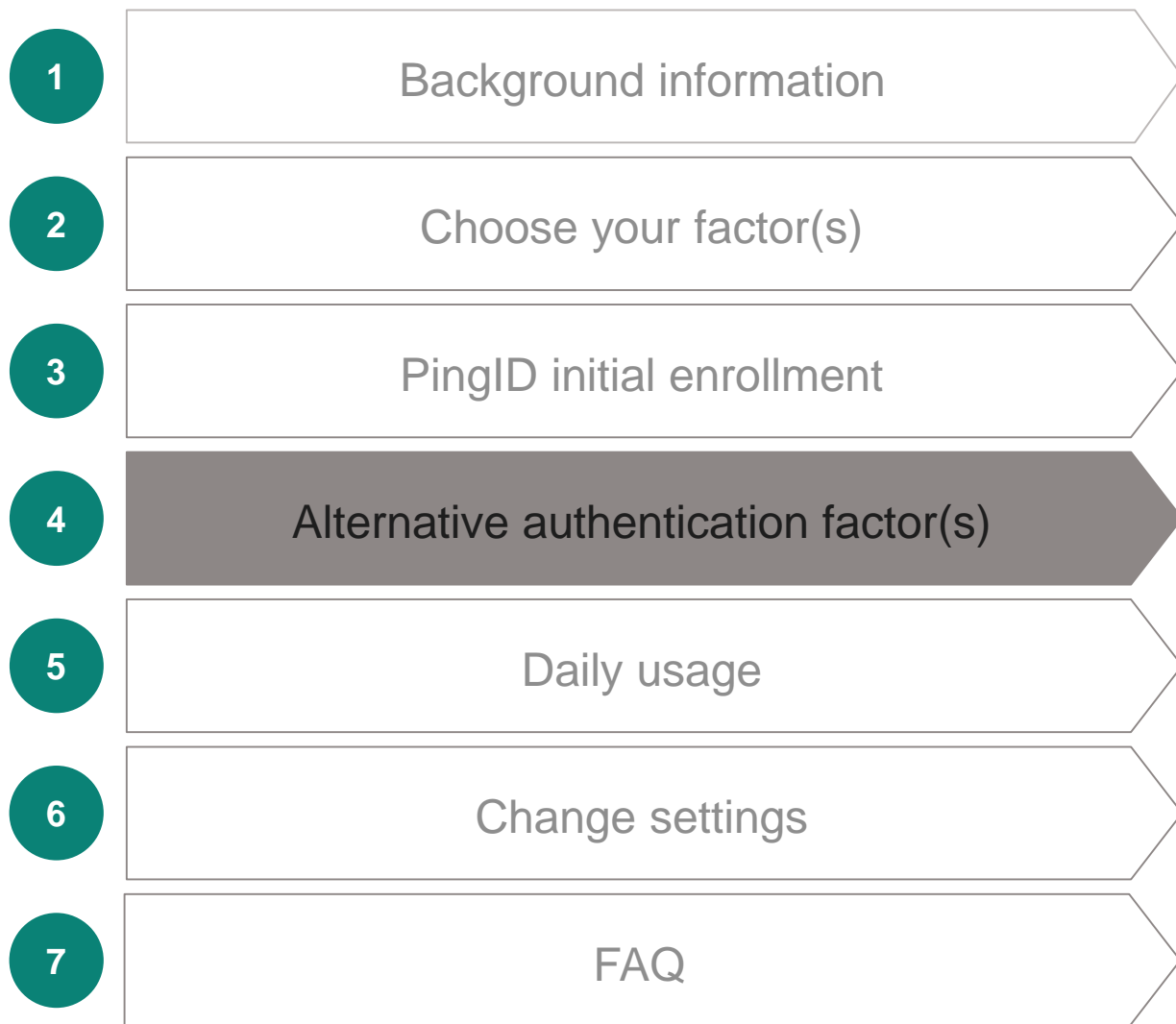
3. „Success“ message will appear



4. You will be redirected to your PingID Self-Service – MyAccount page









Overview



SMS
Voice
FIDO2
Authenticator
Windows Hello

Alternative Factors for MFA

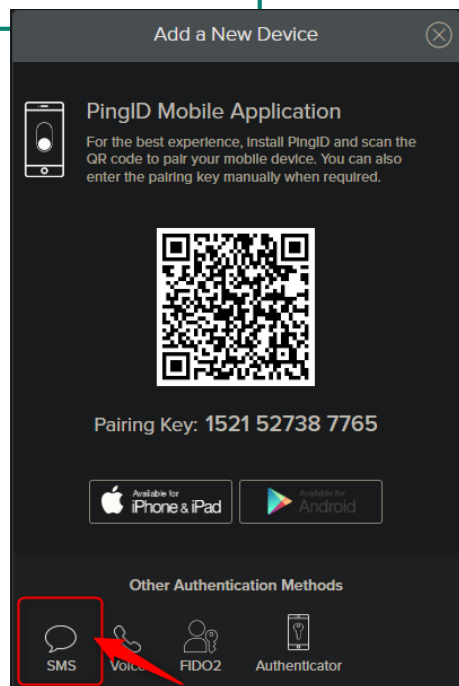
Click on the icon of the alternative factor you have chosen to directly jump to the instructions

 SMS	Sends an OTP* via SMS, for instructions please click here
 Voice	Calls you and tells you an OTP*, for instructions please click here
 Yubikey	Uses your existing security hardware, for instructions please click here
 Security Key/ Passkey	
 Authenticator	For instructions to enroll SMS, for instructions please click here
 Windows Hello	Uses your Windows Hello method, for instructions please click here

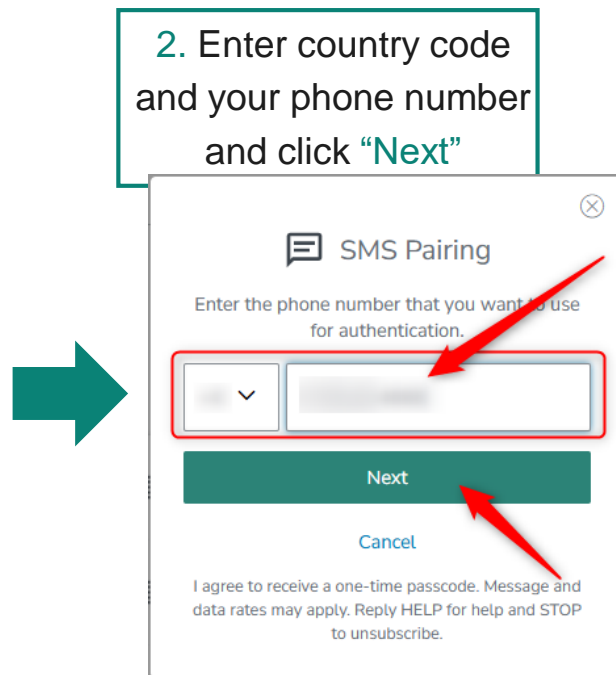
*OTP = One-time passcode

Enroll SMS for MFA

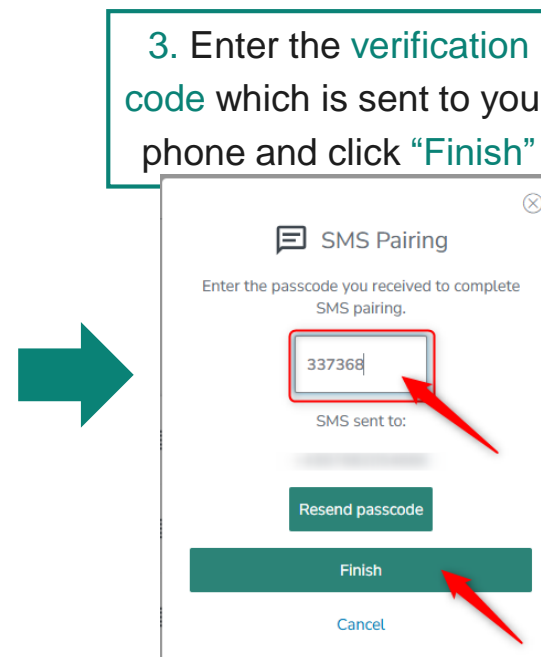
1. Choose method **SMS**



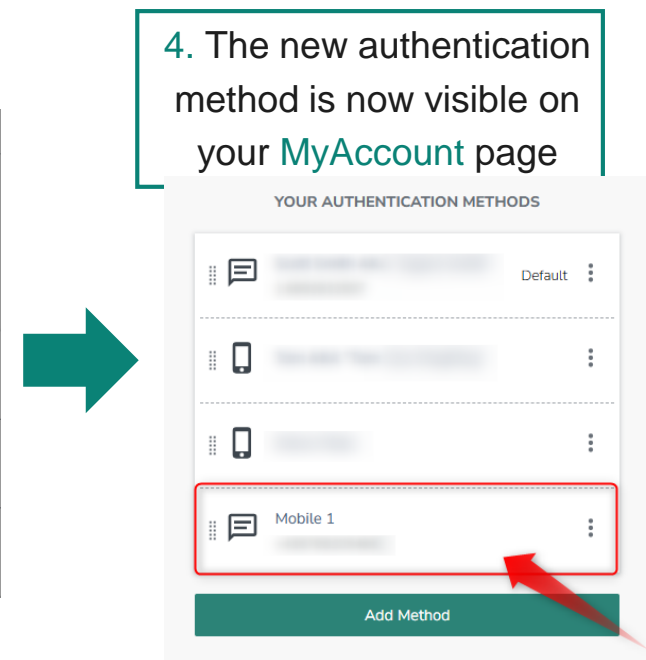
2. Enter country code and your phone number and click **"Next"**



3. Enter the **verification code** which is sent to your phone and click **"Finish"**

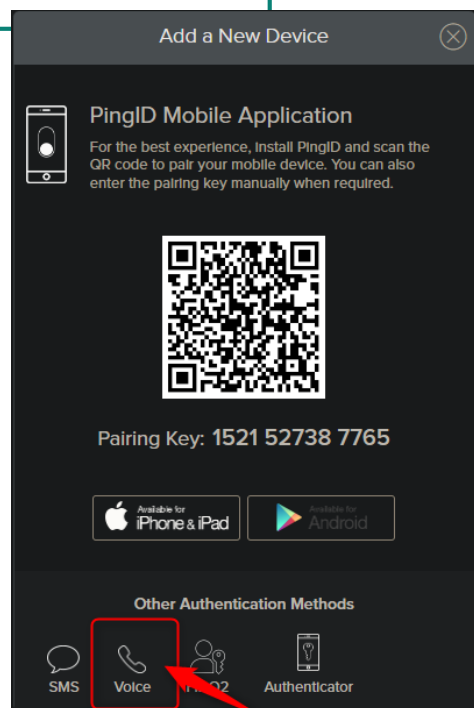


4. The new authentication method is now visible on your **MyAccount** page

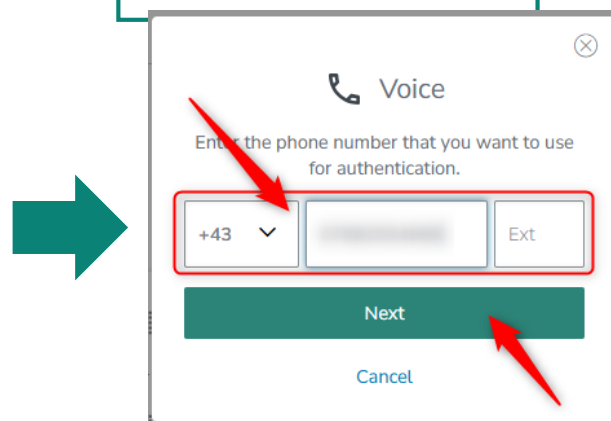


Enroll Voice for MFA

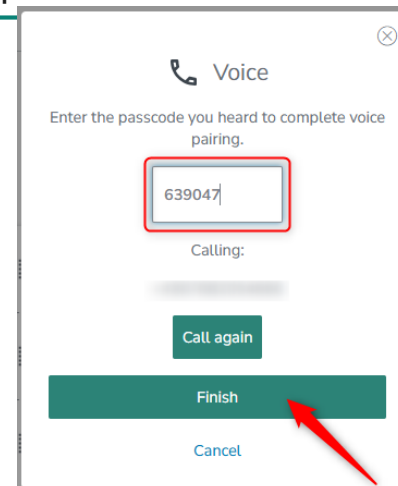
1. Choose method **Voice**



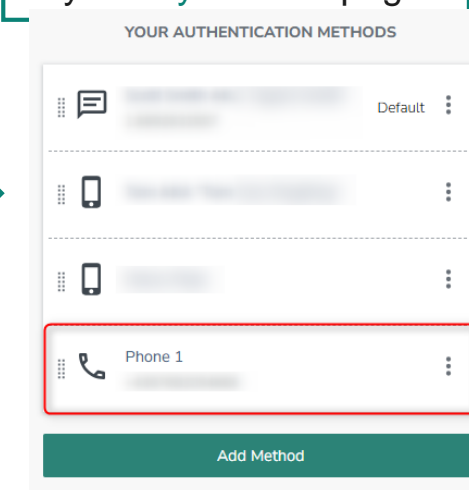
2. Enter country code and your phone number and click **"Next"**



3. Enter the **verification code** which is sent to your phone and click **"Finish"**



4. The new authentication method is now visible on your **MyAccount** page

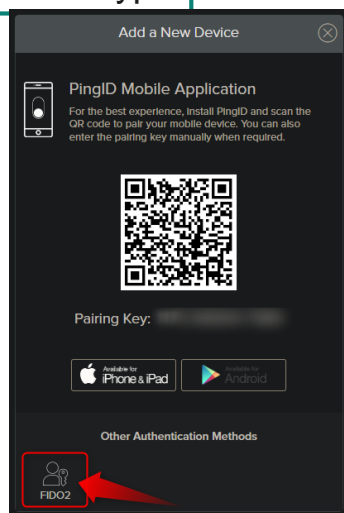


Enroll FIDO2 hardware token for MFA

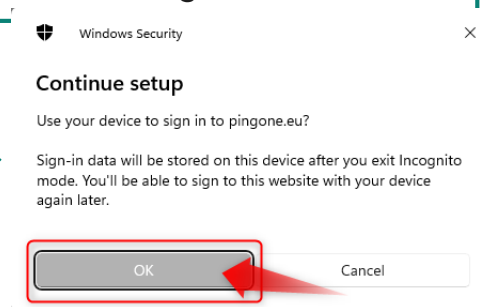
1. Connect the security key to your notebook



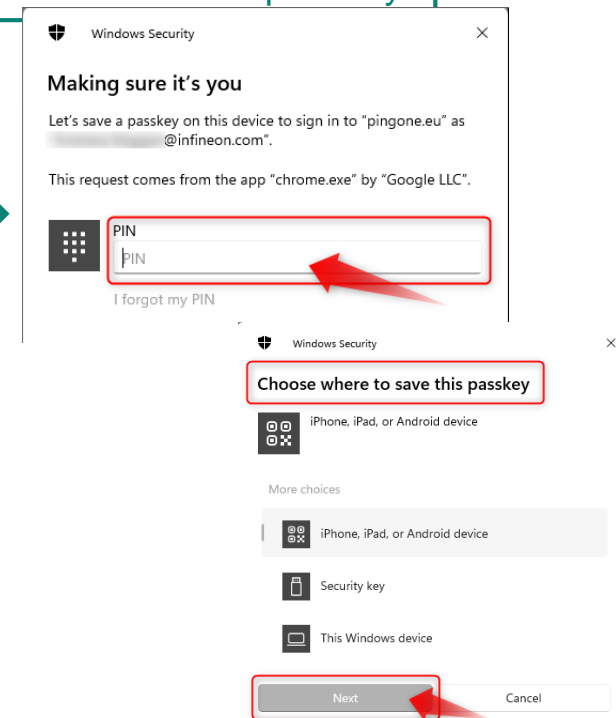
2. Choose FIDO2 as device type



3. Start the pairing process by clicking „OK“



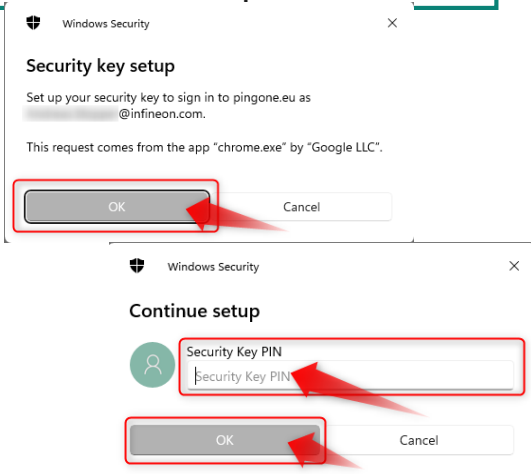
4. Create a PIN and choose where to save the passkey



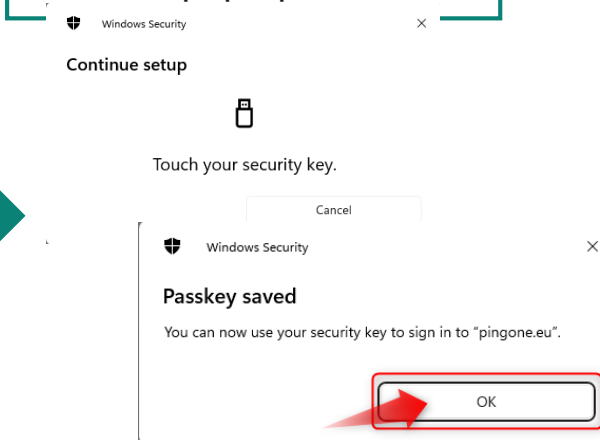
Please continue on the next slide

Enroll FIDO2 hardware token for MFA

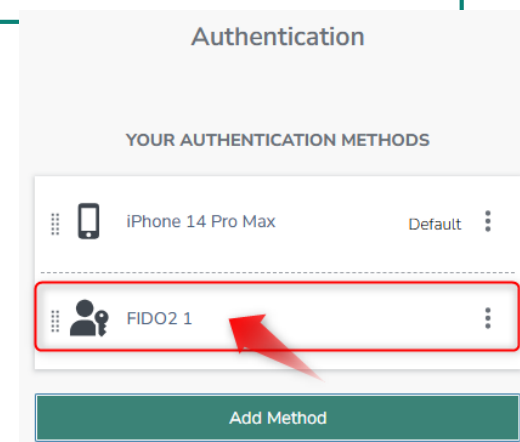
5. Click „OK“ and confirm in the next pop-up with your **PIN** you have created in step 4



6. Touch your FIDO2 key and click „OK“ on the next pop-up.



6. Your new authentication method should be now visible on your **MyAccount** page

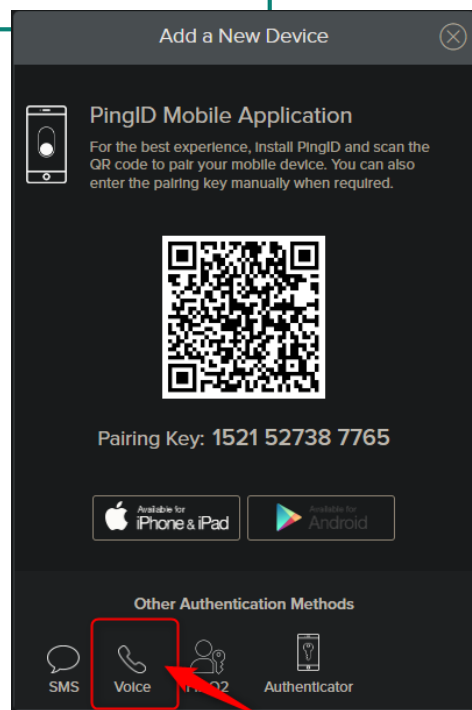


Enroll Authenticator for MFA

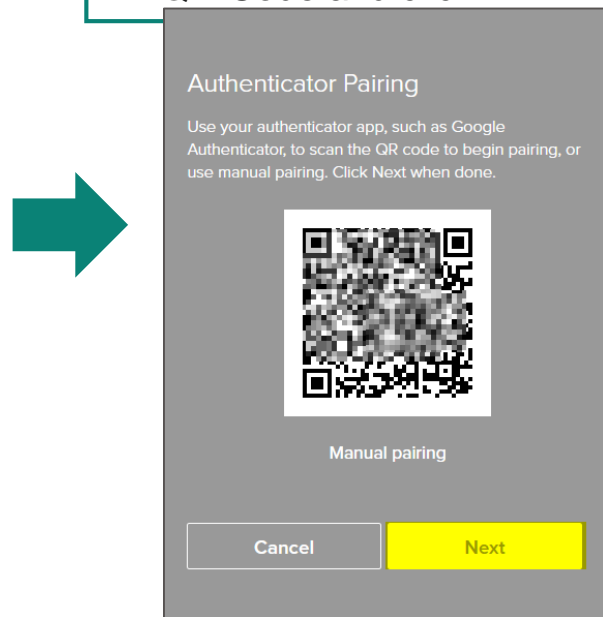
Pre-requisite: existence of an Authenticator App* that supports RFC6238 standard (e.g. Google Authenticator, 2 Factor Authenticator for Windows)

Attention: PingID Desktop App is **not** suitable!

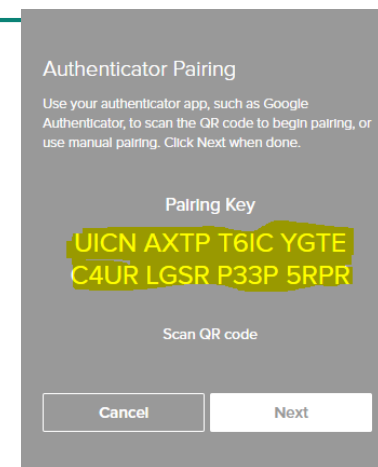
1. Choose method **Voice**



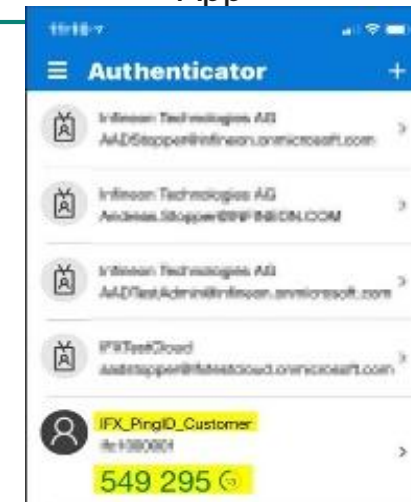
2. Choose your Authenticator App on your phone, scan the QR-Code and click **"Next"**



3. If needed choose **"Manual pairing"** to get a readable code



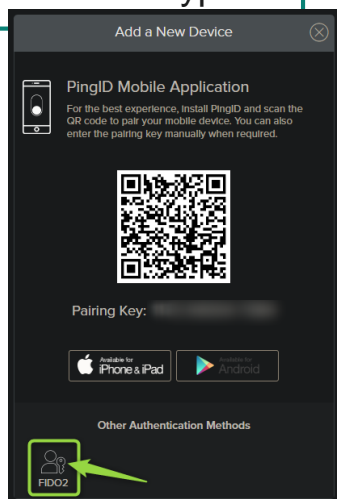
4. Use given information to enroll in your Authenticator App*



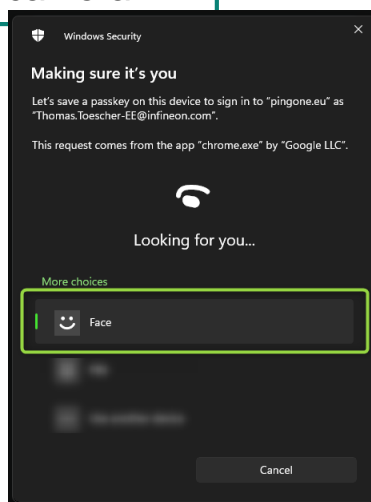
Enroll FIDO2 Windows Hello for MFA

Important: To use this option for MFA, you need to setup Windows Hello as login option on your notebook !!!

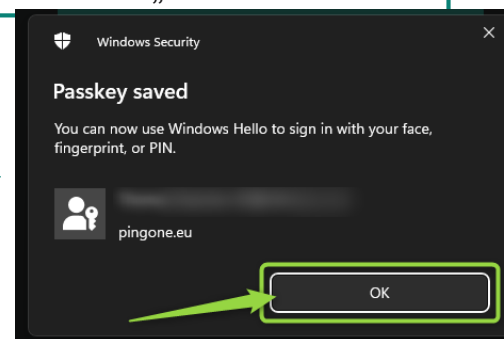
1. Choose FIDO2 as device type



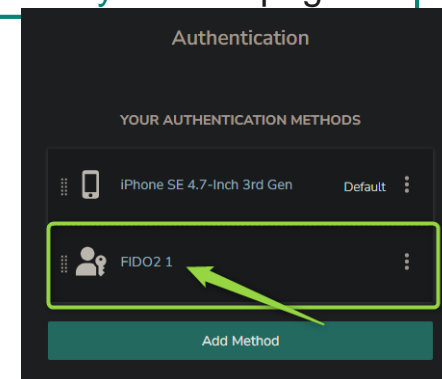
2. Select „Face“ and look in your notebooks camera



3. Follow the instructions on the screen, to finish the enrolment click „OK“

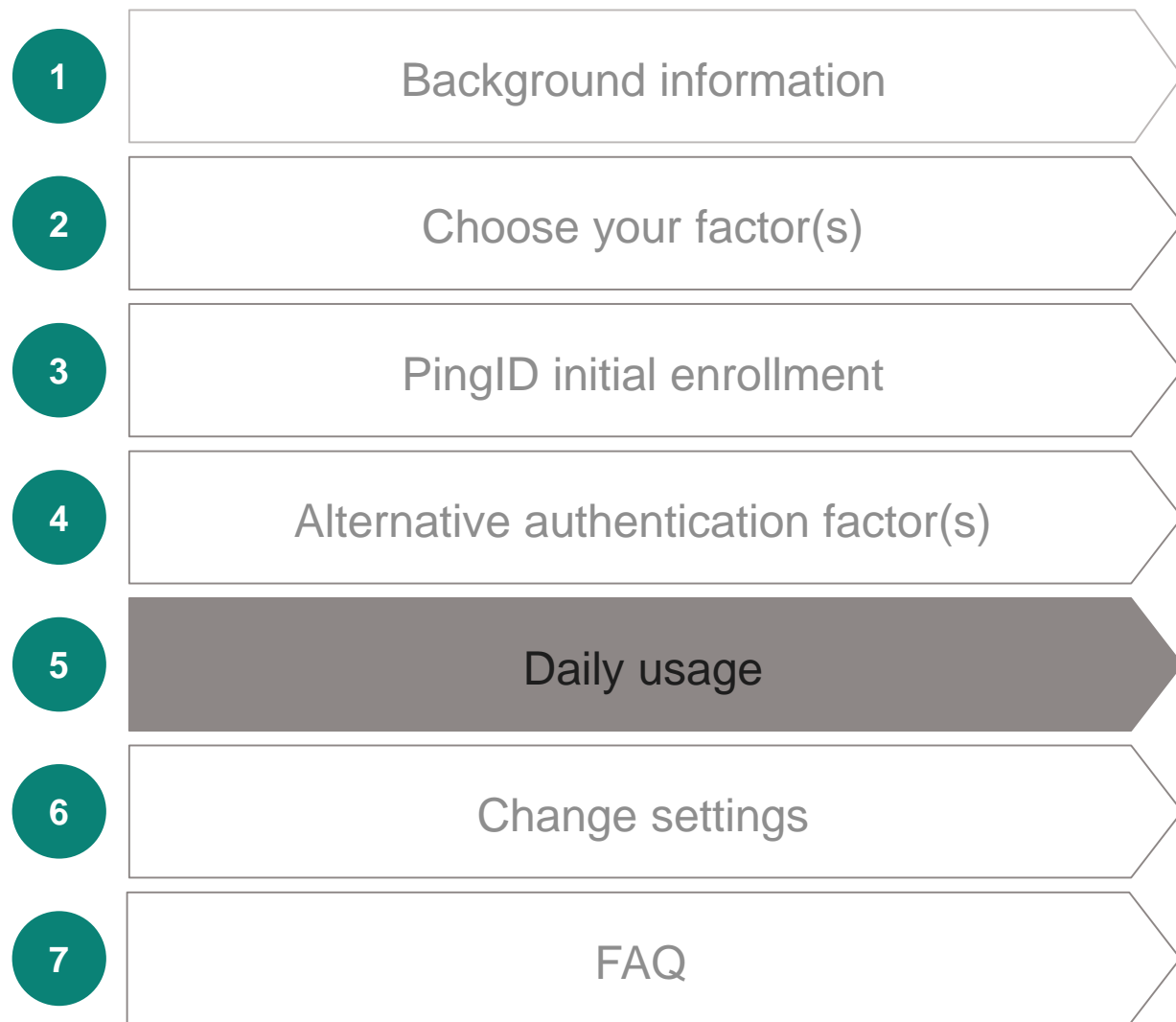


4. The new authentication method is now visible on your [MyAccount](#) page

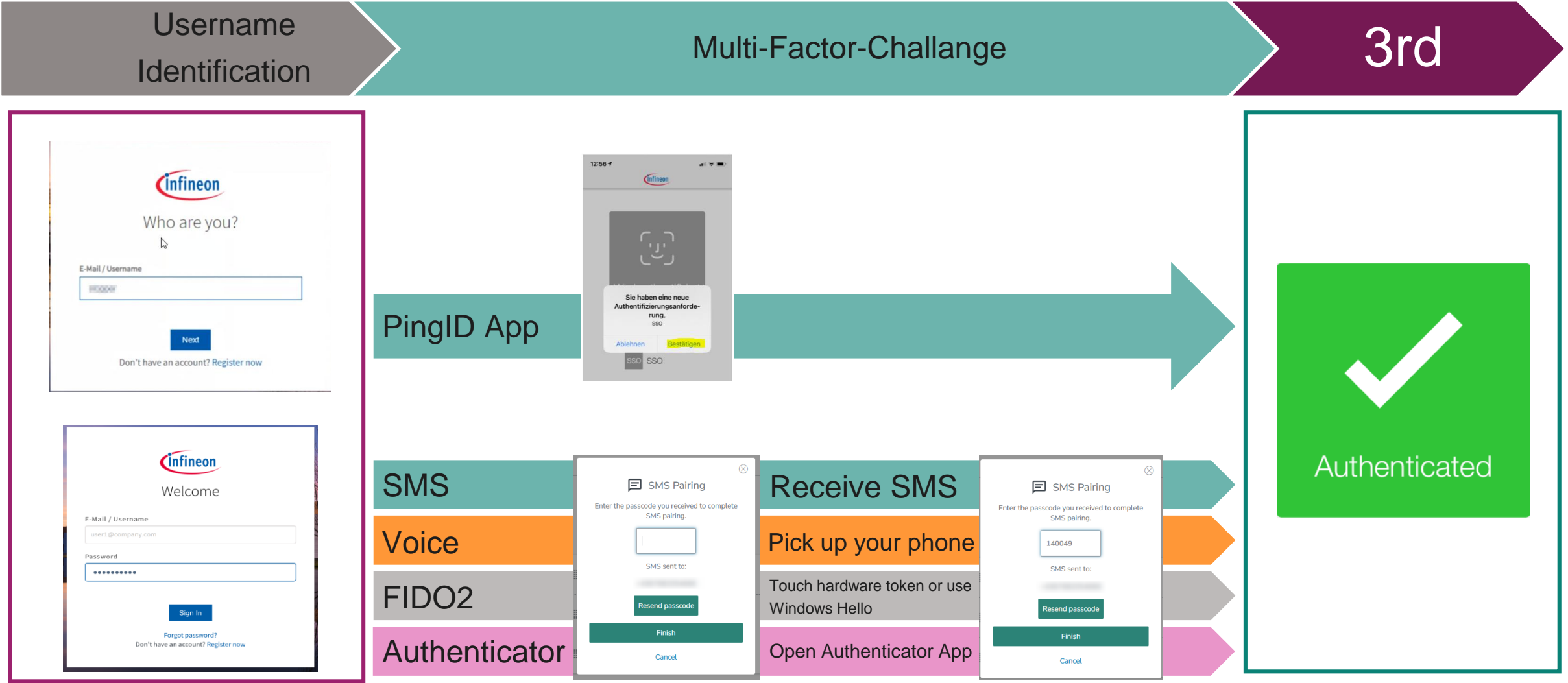


Important: It is recommended to rename this authentication method to separate it from other FIDO2 variants

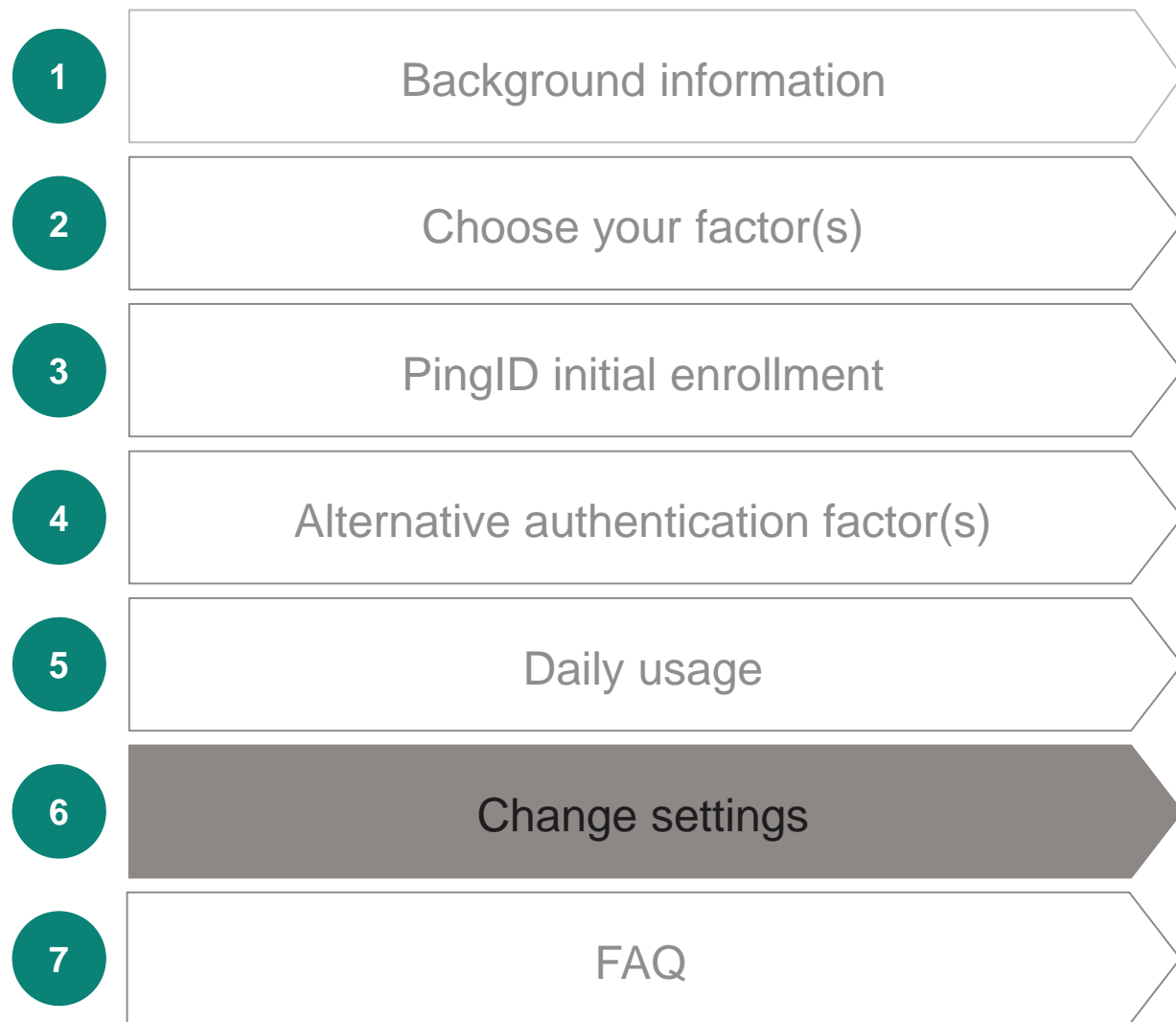
Overview



Daily usage



Overview



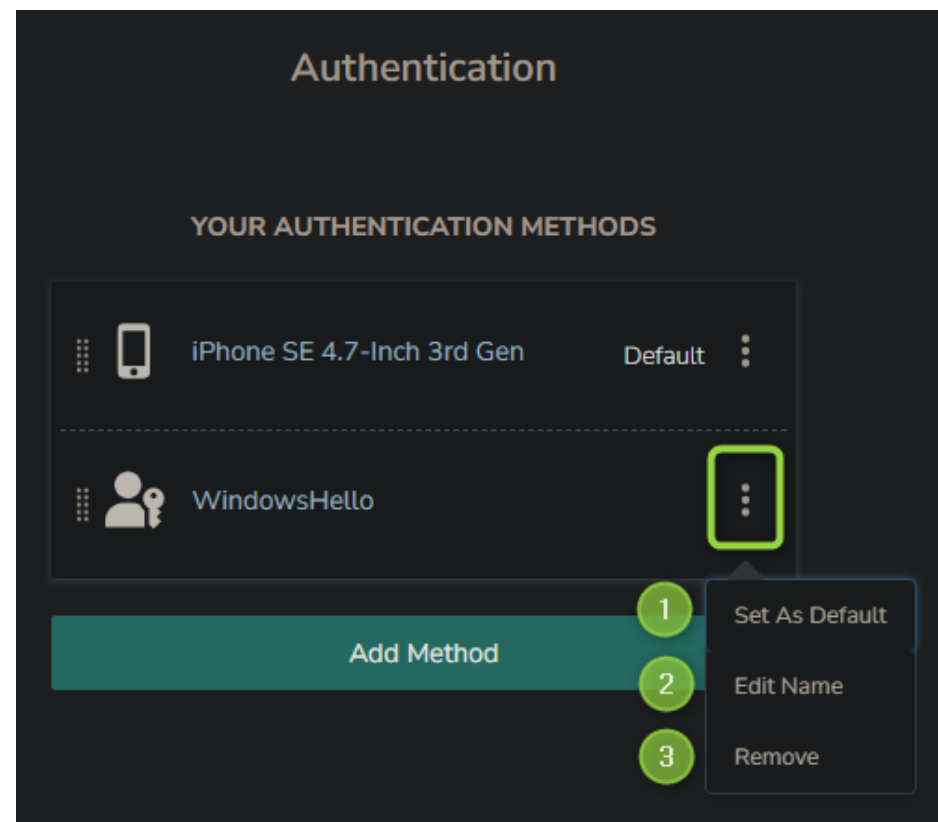
Change device or factor

1. Login to the [PingID Self Service Portal](#) to see your connected authentication methods

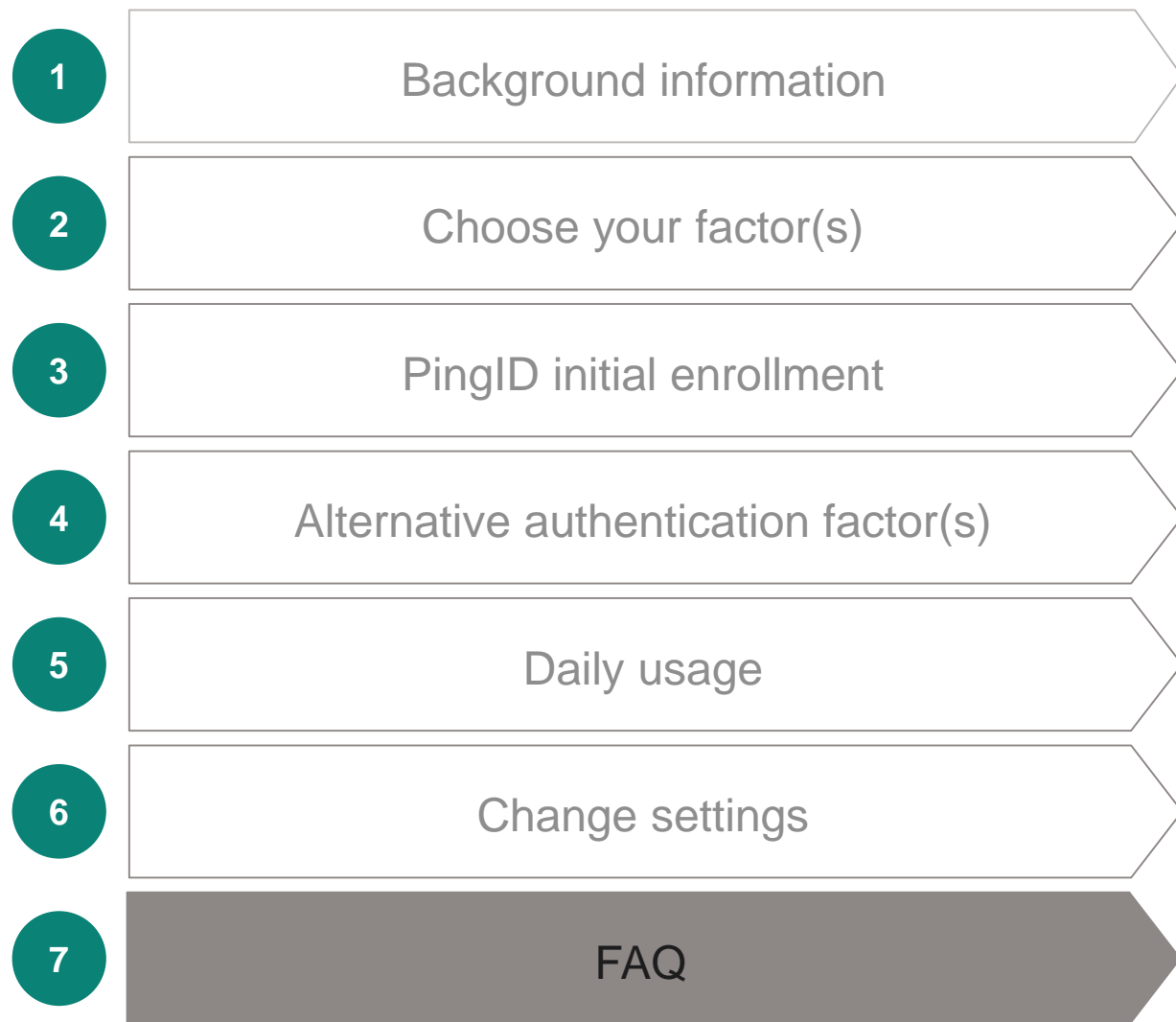


2. By clicking on  following changes can be done at any time:

1. Set a method as default
2. Edit the name of the selected method
3. Remove the selected method



Overview





Which devices can be enrolled?

- PingID App (recommended)
- SMS
- Voice call
- FIDO2 devices/methods
- OATH Token to be integrated in alternate Authenticator Apps (e.g. Microsoft/Google Authenticator)



Why is one-time-password (OTP) via Mail not allowed?

- E-Mail is reserved for password reset functionality



Who can I contact in case of problems?

- Please contact the [Infineon Support Center](#)

