Leonardo Identity Provider - Multi-factor Authentication

QUICK GUIDE: First access configuration

Context

In the process of identifying and authenticating users to access critical and confidential services, Leonardo has introduced a multi-factor authentication process that provides more secure access and protection of user identities.

The MFA authentication enabled by Leonardo for the services offered to its stakeholders involves "2-factor" authentication:

- 1st authentication factor: User-Name and Password
- 2nd authentication factor: a "method" of identity confirmation chosen initially by the user and manageable during the course of use of the service by the user himself (self-service management).

The following guide will describe the procedures for choosing the method for the 2nd authentication factor and registering the device used for the chosen method.

The methods made available by Leonardo for the 2nd authentication factor are:

- **SMS Method:** For receiving a single-use code (OTP)
- **Voice Call method:** for voice reception of a disposable code (OTP)
- **Mobile App Method**: Using application on smartphone via Push-Notification, when the mobile device is connected to Internet network, or passcode, when the mobile device is offline

Prerequisites configuration mode of MFA

> “SMS” method:

The user must have provided, when registering contact information on Leonardo Customer Portal in the Business Phone field, their cell phone number on which to receive the OTP code via SMS.

Note how, if no mobile number has been provided, the "SMS" icon will not be visible and available for selection. Contact your Leonardo contact person for more information on how to request number entry.

> “Voice Call”method:

The user must have provided, when registering contact information on Leonardo Customer Portal in the Telephone field, the landline number or cell phone number on which to receive the call.

Note how, if no number has been provided, the "Voice call" icon will not be visible and available for selection. Contact your Leonardo contact person for more information on how to request number entry.

> Mobile App “Ping ID”:

- Internet-connected cellular device: The device on which the application will be installed must be connected to an Internet network and have a biometric factor (e.g., face or fingerprint recognition) in order to complete the authentication.
- Offline device: The OTP code authentication method is possible if the device is not connected to an Internet network or if the user chooses to use it by disabling the notifications, when the device is connected to an Internet network, from the settings of the application installed on the cellular device.

First access configuration

Click on the > to access the guide for the chosen method:

> **First MFA configuration with SMS**

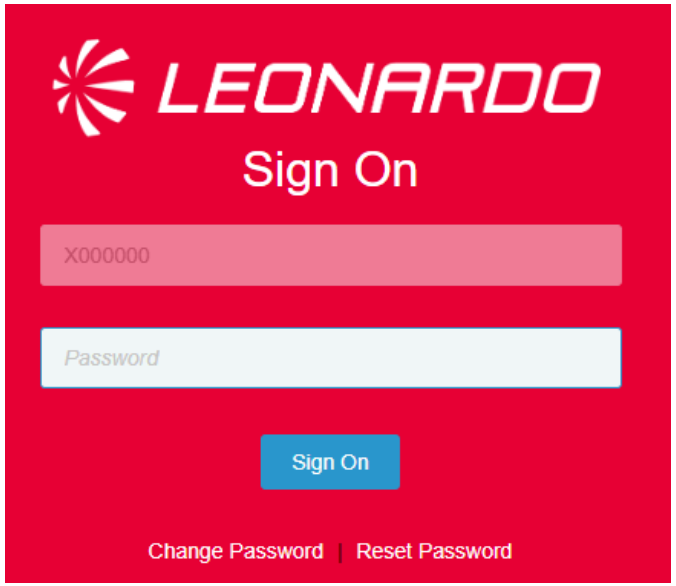
> **First MFA configuration via Voice Call**

> **First MFA configuration on MobileApp**

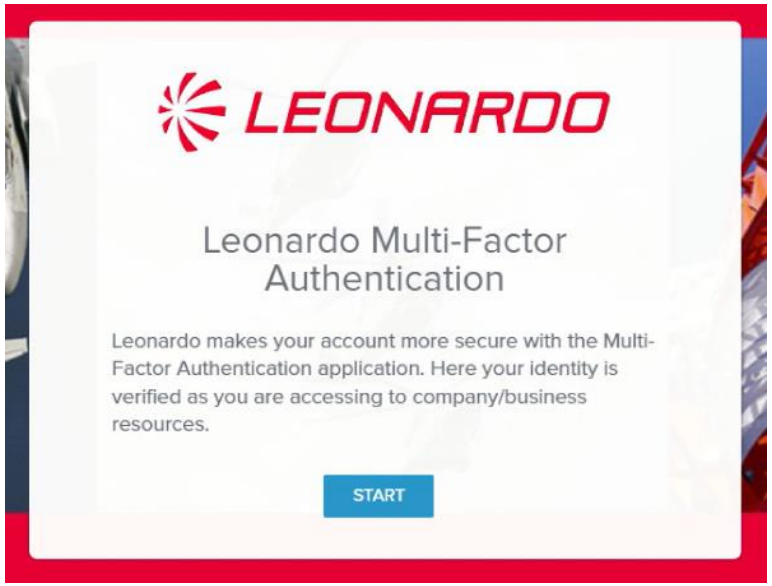
First MFA configuration with SMS - step 1/2

When accessing a Leonardo service protected by MFA you are asked, as the 1st authentication factor to enter your credentials (user-name and password) that you already have.

At this stage you are presented with the screens below in which you must enter your credentials and proceed with the **[Sign On]** button.



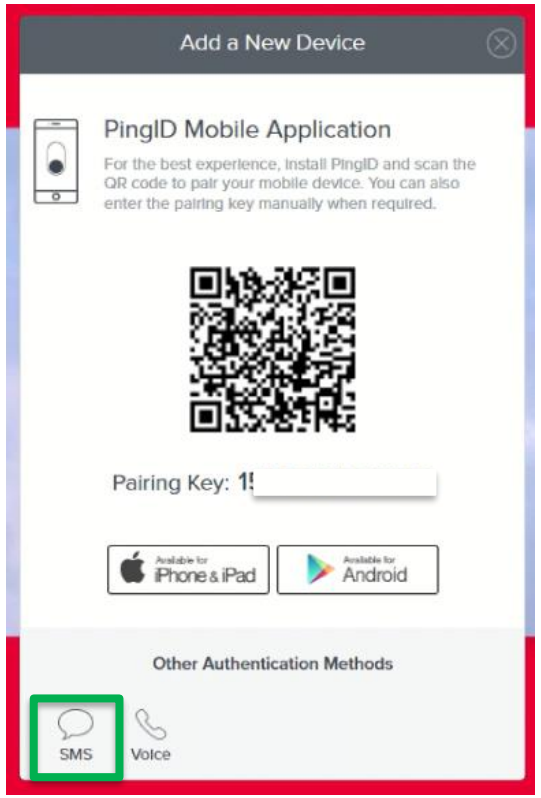
Next, the user will be prompted to proceed with configuring at least one of the Multi-Factor Authentication methods made available by Leonardo. Click on **[START]** to begin:

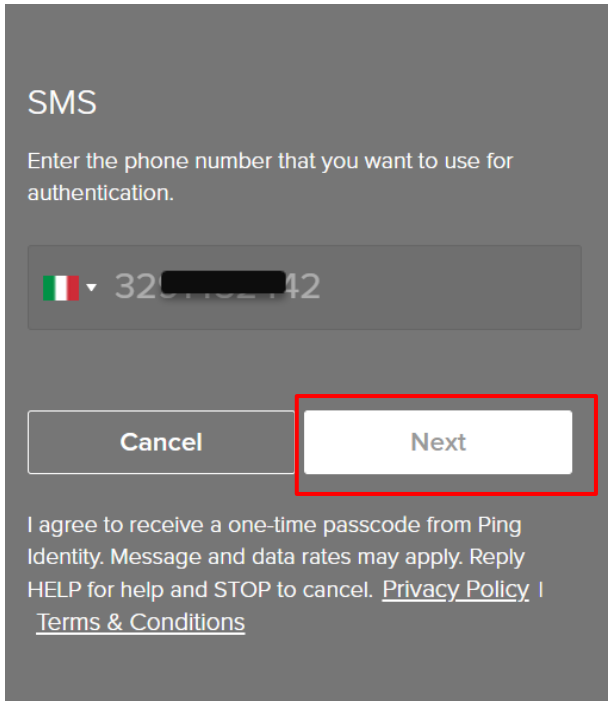


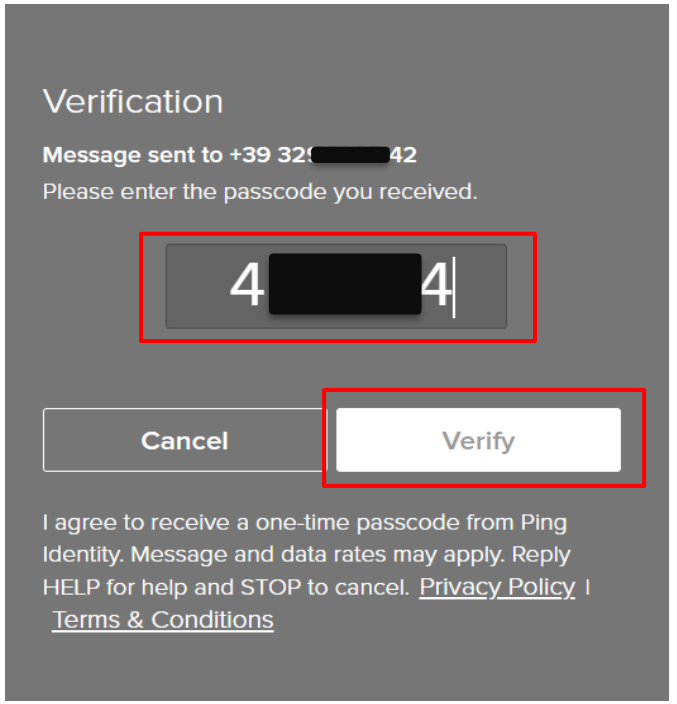
First MFA configuration with SMS - step 2/2

Click on the **SMS** icon in the "Other authentication methods" section: you will see on screen the mobile phone number provided in the Business Phone field on Leonardo Customer Portal. Then confirm the phone number by clicking on "Next".

The 6-digit OTP received on the mobile number associated with the user must be entered in the appropriate field.





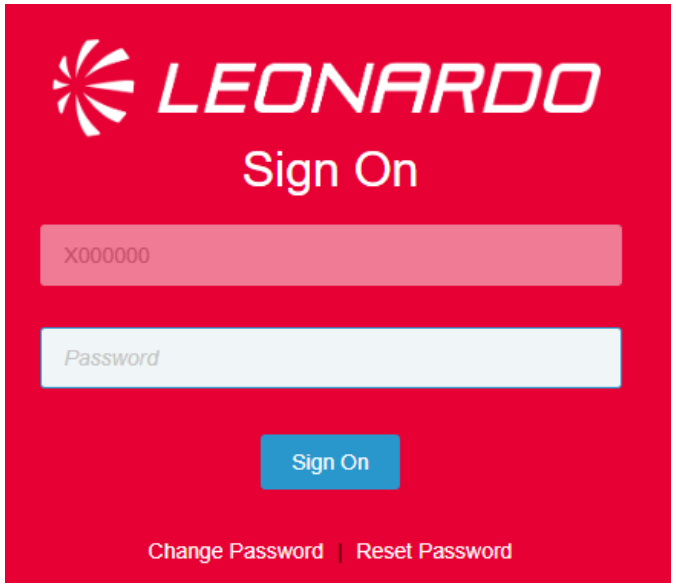


The second authentication factor configuration via SMS is complete.

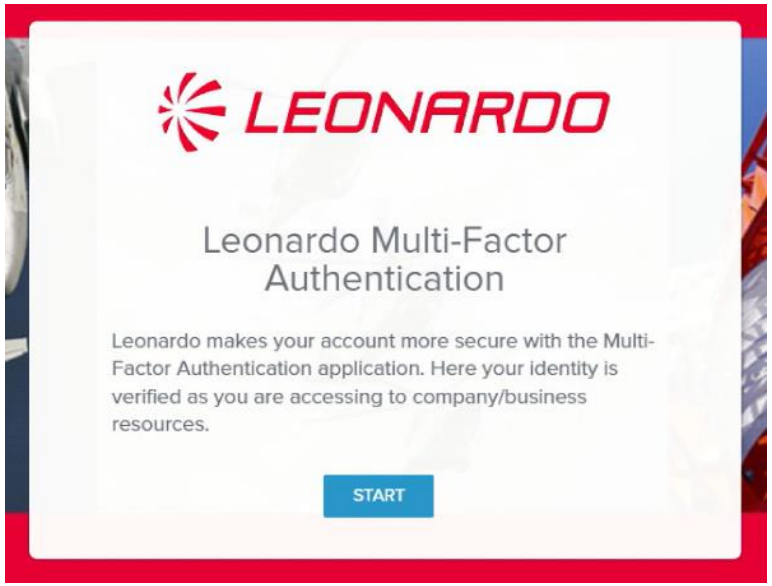
First MFA configuration via Voice Call - step 1/2

When accessing a Leonardo service protected by MFA you are asked, as the 1st authentication factor to enter your credentials (user-name and password) that you already have.

At this stage you are presented with the screens below in which you must enter your credentials and proceed with the **[Sign On]** button.

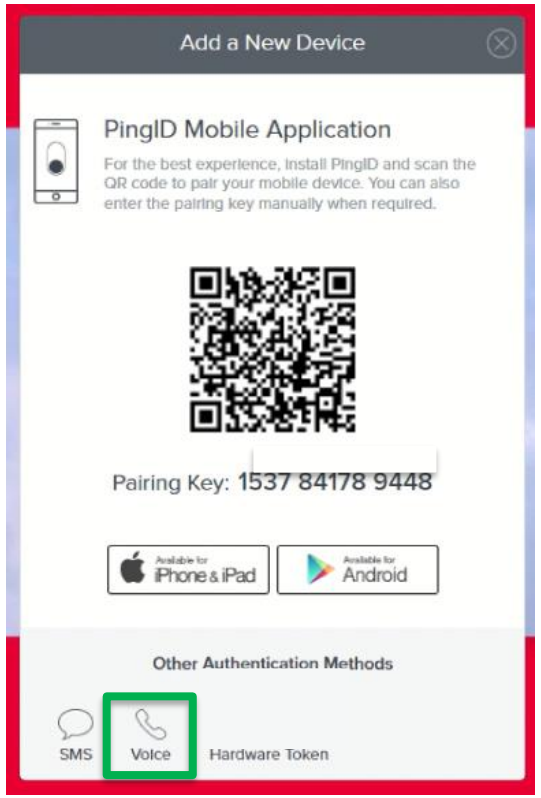


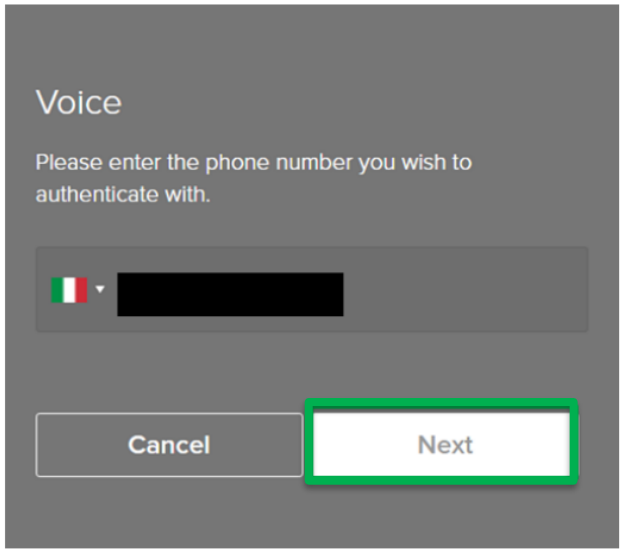
Next, the user will be prompted to proceed with configuring at least one of the Multi-Factor Authentication methods made available by Leonardo. Click on **[START]** to begin:

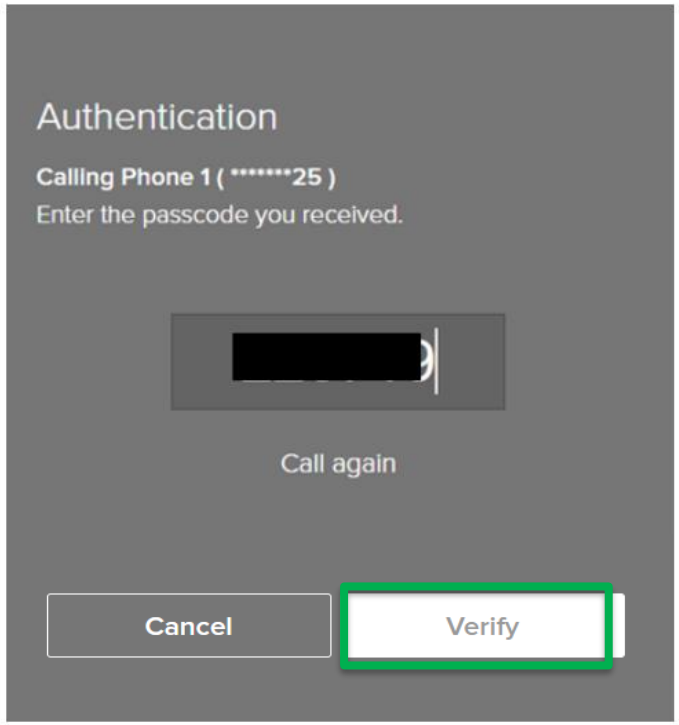


First MFA configuration via Voice Call - step 2/2

Click on the **Voice** icon in the "Other authentication methods" section: you will see on screen the phone number provided in the Telephone field on Leonardo Customer Portal. Then confirm the phone number by clicking on "Next“ to receive the call providing by voice the OTP code to authenticate. The user should enter the OTP code received in the appropriate field and then click on "Verify”:





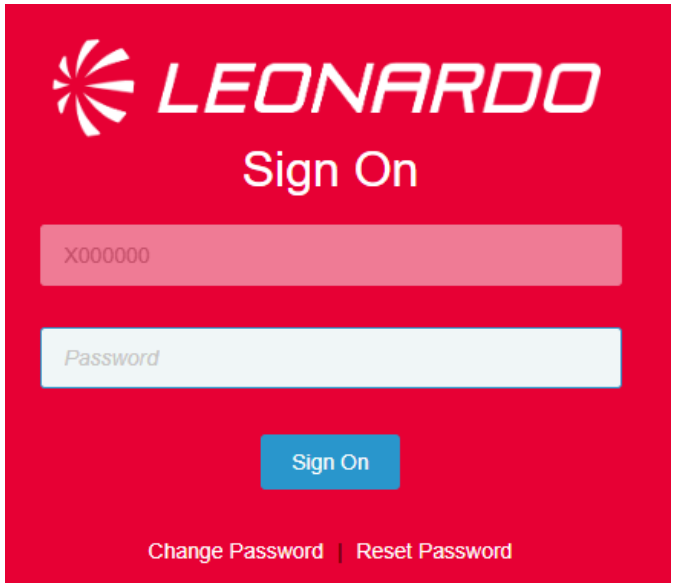


The second authentication factor configuration via Voice Call is complete.

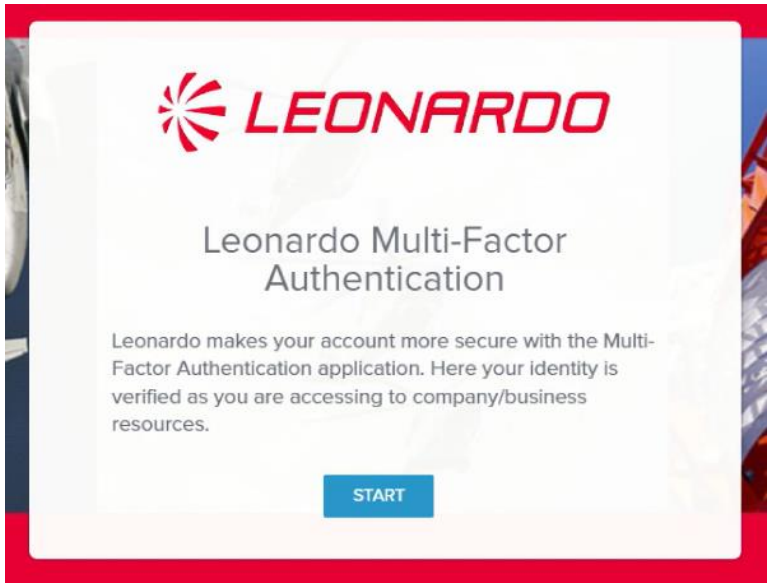
First MFA configuration via Mobile App “PingID” (Push-Notification or OTP) - step 1/3

When accessing a Leonardo service protected by MFA you are asked, as the 1st authentication factor to enter your credentials (user-name and password) that you already have.

At this stage you are presented with the screens below in which you must enter your credentials and proceed with the **[Sign On]** button.



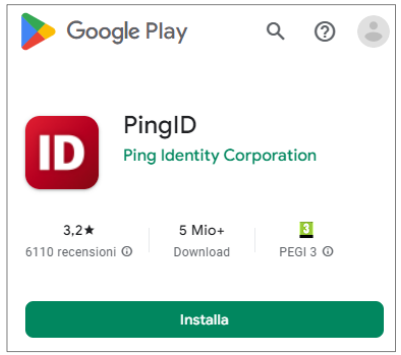
Next, the user will be prompted to proceed with configuring at least one of the Multi-Factor Authentication methods made available by Leonardo. Click on **[START]** to begin:

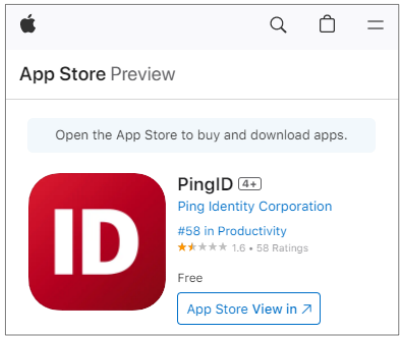


First MFA configuration via Mobile App “PingID” (Push-Notification or OTP) - step 2/3

To configure the MFA via Mobile App, it is necessary to install the "PingID" application on the user's cell phone or tablet.

Download «PingID» MobileApp from Google Play Store (Android) or App Store (iOS)

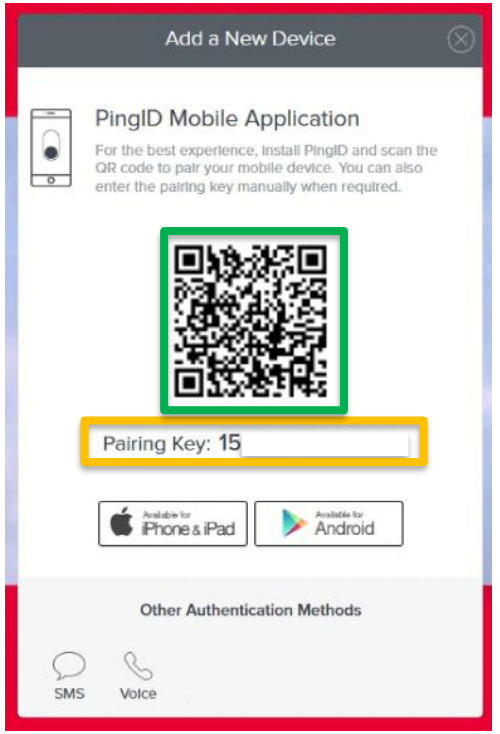




After the Mobile App has been installed, accept the terms of service, camera and location permissions and push notifications (required to use the service).

Complete the configuration of the «PingID» MobileApp on your device by choosing between:

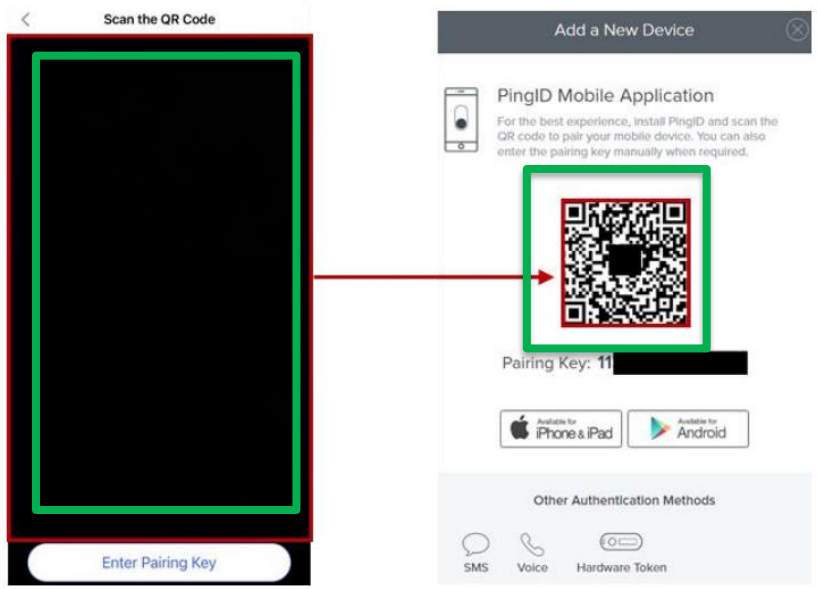
A. Scanning with the MobileApp the QR code shown on the screen
B. Entering the Pairing Code by clicking on «enter pairing code manually» on the MobileApp



First MFA configuration via Mobile App “PingID” (Push-Notification or OTP) - step 3/3

A. Scanning the QR code with the MobileApp:

To complete the association, the user must use the Mobile App "PingID" on the mobile device by scanning the QRcode on the web screen. Below are the screens that the user will see simultaneously on the mobile device (Mobile App "PingID") and on the browser (web) where the MFA configuration phase is taking place:

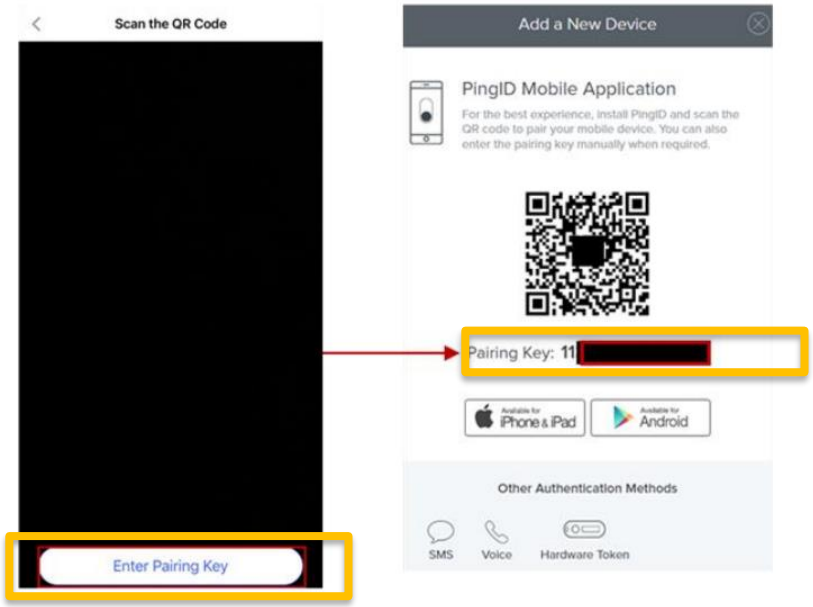


Initial screen "PingID" on mobile device

Web screen for device association

B. Entering the Pairing Code on the MobileApp:

Alternatively, the user can complete the device pairing by entering the pairing key found on the web screen. The following are the screens that the user will simultaneously see on the mobile device (Mobile App "PingID") and the browser (web) where the MFA configuration phase is in progress:



"PingID" screen by pairing key

Web screen to read pairing key

The second authentication factor configuration via Mobile App is complete.

THANK **YOU**
FOR YOUR ATTENTION

leonardocompany.com