DAIMLER

MFA4Daimler
User Guide MFA Mobile – Dealer & Supplier Communities

DAIMLER

Advice for this document

If you have downloaded a copy of this document, it may be out of date by now.
Make sure to always use the latest version.

Version 1.3

Table of contents MFA4Daimler User Guide Mobile

Introduction

Content

All underlined content can be clicked to jump to the corresponding slide

MFA4Daimler User Guide - Dealer & Supplier Communities

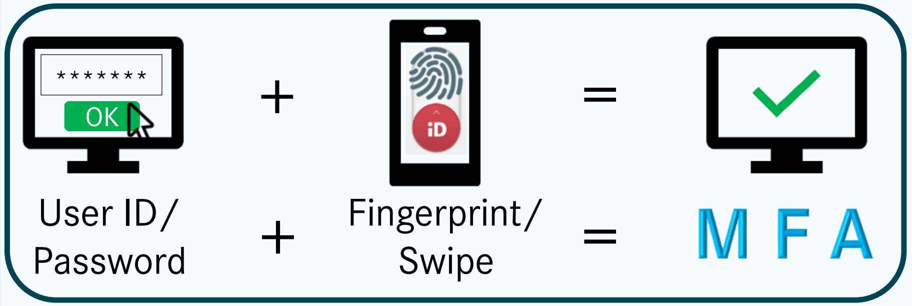
The new MFA Standard for Daimler

A future proof Multi-Factor-Authentication (MFA) solution

- The overall goal is to provide a modern, cloud ready, state-of-the-art replacement for the former Strong Authentication Solution “GAS – Confidential (SecurePIN)”
- The new solution is easy to use and conforms with today’s standards for secure authentication
- Daimler’s Information Security Policy requires that confidential applications have to use Multi-Factor-Authentication. The new MFA will be the “second factor” authentication check when logging into such an application.

The new MFA is secure & convenient to use

The different factors (first and second) are combined into one secure authentication:



The new MFA offers highest standards

Authentication with something you know <u>AND</u> something you have

- The purpose of Multi-Factor-Authentication is to secure logins by using more than one factor of authentication. This is achieved by combining **different** authentication technologies.
- At Daimler, a combination of a knowledge-based first factor (Password) is combined with a second factor based on possession, which serves as additional proof of authentication (Fingerprint or One-Time Password (OTP)).

MFA4Daimler User Guide

About this manual

This document explains how to activate and work with the new MFA4Daimler solution.
It covers installation, different authentication methods and Self Service processes.

Throughout this guide you will see two different icons.
They indicate, on which device the described step has to be taken:

📱	Step to be taken on iOS or Android
🖥	Step to be taken on Windows or MacOS computer

Quick Links to the most important MFA steps

Click on the appropriate picture to continue

Start using MFA

Using MFA - Part 1
Installing and Configuring

Slides 1a, 1b

Using MFA - Part 2
Activating and Pairing

Slides 2, 2a, 2b

Using MFA – Part 3
Authenticating with MFA

Slides 3a, 3b, 3c

Modify & troubleshoot MFA

Self Services - Part 1
Add, Change, Delete Device

Slides 4a, 4b, 4c

Self Services – Part 2
Self-Migrate and other options

Slides 5a, 5b

Self Services – Part 3
4-Eyes-Reset

Slide 6

1a Installing the MFA Mobile App PingID

Installation on iOS and Android

The MFA app PingID must be installed on your iOS or Android device before the next usage of a confidential application. Please download and install the App "PingID" from the respective AppStore (iOS/Android).

a) Minimum system requirements for installation on mobile devices:
For iOS: Version 11 and higher, or Android Version 6 (Marshmallow) and higher.
b) Every fingerprint scanner on iOS (TouchID) and Android is supported with the above minimal system requirements.

Hint: During the installation process you will be asked for permissions for the PingID App (camera, location and notifications). For the best user experience, we recommend allowing access for camera and notifications. The location permission is not necessary.

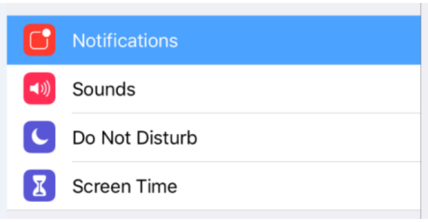
1b Configuring the mobile device

Recommended settings for iOS and Android

To ensure that the MFA functionality described in this document works as expected, recommended notification settings are documented below.
The PingID app will work also with other settings, however you may experience a different behaviour when being notified.
The settings are recommended to ensure you are being notified on your locked mobile device when you have to authenticate yourself.

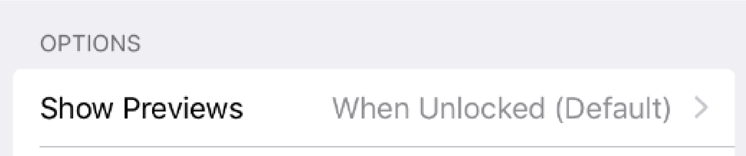
iOS Notifications

- Start the iOS settings
- Go to „Notifications“



Notifications
Sounds
Do Not Disturb
Screen Time

- Scroll down to „PingID“
- Choose „Show Previews“
- Set „When unlocked“ (may be set as default already, like shown in the screenshot below).

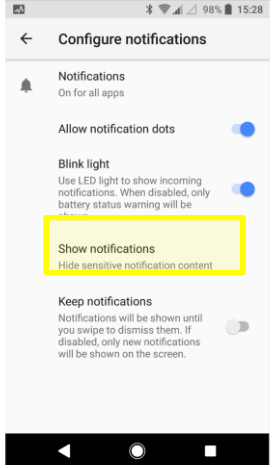


OPTIONS

Show Previews When Unlocked (Default) >

Android Notifications*

- Start the Android settings app
  - Go to „Apps & Notifications“
- Go to „Configure notifications“
- Check that „Show Notifications“ is set to „Hide sensitive notification content“.
- When you have selected to not show notifications at all, you have to go to „Notifications“ in the same menu, select the „PingID “ app and set the „Show Notifications“ in this menu to „Hide sensitive notification content“.



98% 15:28

Configure notifications

Notifications
On for all apps

Allow notification dots

Blink light
Use LED light to show incoming notifications. When disabled, only battery status warning will be shown

Show notifications
Hide sensitive notification content

Keep notifications
Notifications will be shown until you swipe to dismiss them. If disabled, only new notifications will be shown on the screen.

* Depending on your Android device and version this menu may differ due to vendor specific implementation.

2 Activation of the MFA Mobile App PingID

Two options for activation

For the activation of the PingID Mobile app only one of the following instructions is required:

1. **When you are using a Desktop or Notebook as your main device to work with applications (applies to Notebooks or Desktops)**

   → Please follow the steps described in 2a) (Slides 10-12)

OR

2. **When you are using a Mobile Device as your main device to work with applications (applies to iOS and Android devices)**

   → Please follow the steps described in 2b) (Slides 13-14)

By using the activation, the app gets fully personalized and will be linked to your personal Daimler UserID.
The app must not be shared in any way due to this personalization.

2a Activating the MFA Mobile App PingID

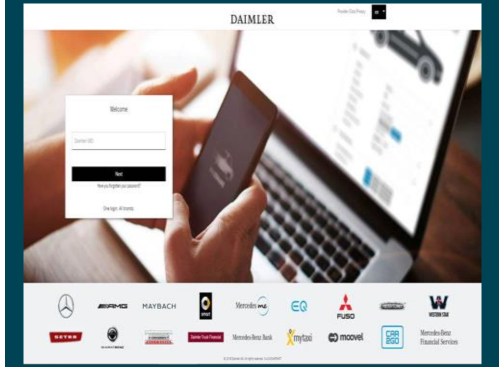
Activation using Desktop based Applications 1/3

The following steps are required to activate and pair the PingID app while using a confidential Daimler desktop application on your Windows computer.
Only required once (or if you have to reactivate PingID on new or reset devices).

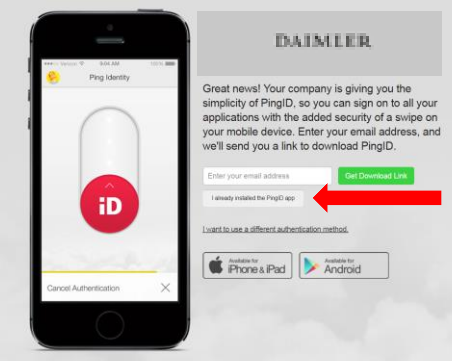
1. **Launch your intended confidential desktop or web application.**

   Your Daimler Windows Application

   You will be forwarded to the new Daimler Web-Login. Use your corporate User ID and Corporate password and click "Sign In"



2. **After a successful login, you will be forwarded to the MFA Activation Screen. As the PingID app was installed before, please click on "I have installed the app already"! (marked with red arrow in the screenshot below)**



Great news! Your company is giving you the simplicity of PingID, so you can sign on to all your applications with the added security of a swipe on your mobile device. Enter your email address, and we'll send you a link to download PingID.

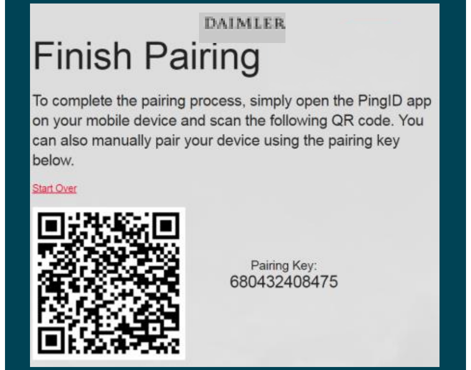
Enter your email address | Get Download Link

I already installed the PingID app

I want to use a different authentication method.

3. **After a few seconds you will be asked to finalize the pairing of your device. A QR code and a Pairing Key is displayed.**

   You can click on "Start Over", if you want to go back one step.



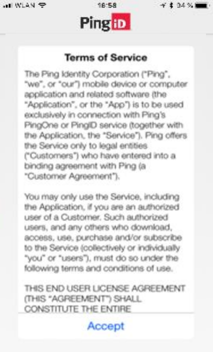
Finish Pairing

To complete the pairing process, simply open the PingID app on your mobile device and scan the following QR code. You can also manually pair your device using the pairing key below.

Start Over

Pairing Key:
680432408475

4. **Start the PingID app on the mobile device. On first time use the "Terms of Service" message is displayed. Please read and click "Accept" to continue.**



Terms of Service

The Ping Identity Corporation ("Ping", "we", or "our") mobile device or computer application and related software (the "Application", or the "App") is to be used exclusively in connection with Ping's PingOne or PingID service (together with the Application, the "Service"). Ping offers the Service only to legal entities ("Customers") who have entered into a binding agreement with Ping (a "Customer Agreement").

You may only use the Service, including the Application, if you are an authorized user of a Customer. Such authorized users, and any others who download, access, use, purchase and/or subscribe to the Service (collectively or individually "you" or "users"), must do so under the following terms and conditions of use.

THIS END USER LICENSE AGREEMENT (THIS "AGREEMENT") SHALL CONSTITUTE THE ENTIRE

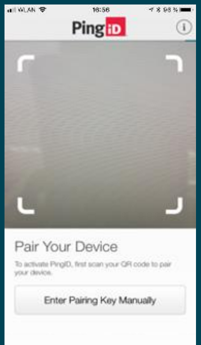
Accept

2a Activating the MFA Mobile App PingID

Activation using Desktop based Applications 2/3

The activation is possible by a QR scan and requires access to the camera. For an alternative see the red box on the right.
Follow the steps 5 to 7 on this page and continue with step 11 on the next page

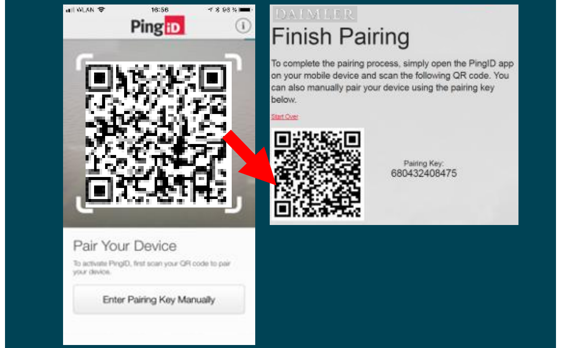
5. You will be asked for permissions to run PingID (camera, location and notifications)*. When you have accepted the camera access a camera window is shown inside the app. If you did not allow camera access, skip to step 8.



Pair Your Device

To activate PingID, first scan your QR code to pair your device.

6. Please use your mobile phone to scan the QR code on the webpage. Just move your smartphone with the camera window towards your computer screen, so that the QR code can be seen on the display. A beep confirms a successful QR reading.



Pair Your Device

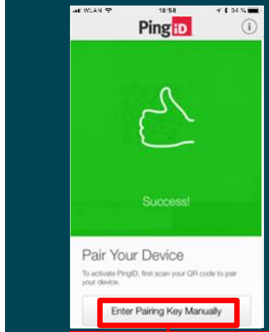
To activate PingID, first scan your QR code to pair your device.

Finish Pairing

To complete the pairing process, simply open the PingID app on your mobile device and scan the following QR code. You can also manually pair your device using the pairing key below.

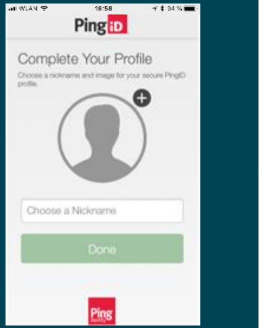
Pairing Key: 680432408475

7. If pairing was successful, a green confirmation message will be shown. Afterwards, you are asked to enter a name for your profile. You can use any name here, but it is recommended to use your Daimler UserID. A photo is not required.



Pair Your Device

To activate PingID, first scan your QR code to pair your device.



Complete Your Profile

Choose a nickname and image for your secure PingID profile.

If pairing by camera fails, click on „Enter Pairing Key Manually“ and enter the pairing key displayed in step 6. See next slide for details.

*** = The permissions for camera and for notifications are highly recommended, the location permission is not required.**

Alternative activation without camera:

Without a camera or if you declined the access to the camera, an activation of MFA is still possible. If you prefer this, please use the steps 8 to 10 on the next page.

→ **Go to Step 11 on next page**

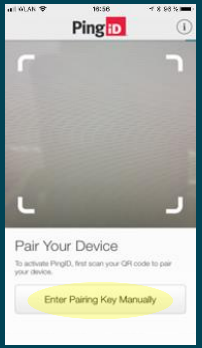
2a Activating the MFA Mobile App PingID

Activation & Pairing using Desktop based Applications 3/3

Alternative steps 8 to 10: Activation by code instead of QR scan
(Please go directly to step 11, if you already followed the steps 5 to 7 on the page before)

Step 11 is the final step for both types of activation

8. If you did not allow access to your camera or prefer to activate the app manually, you can activate PingID as follows: Click the button below the camera window (marked yellow in screenshot): ‘Enter Pairing Key Manually’



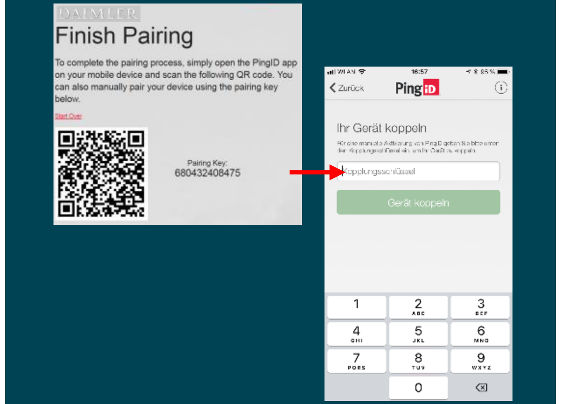
16:56

Pair Your Device

To activate PingID, first scan your QR code to pair your device.

Enter Pairing Key Manually

9. Please use the code shown on the webpage (see step 3), which is displayed beside the QR code. Please enter this code into the input field on your mobile device. Confirm with “Pair Device”.



DAIMLER

Finish Pairing

To complete the pairing process, simply open the PingID app on your mobile device and scan the following QR code. You can also manually pair your device using the pairing key below.

Start Over

Pairing Key:
680432408475

16:57

Zurück

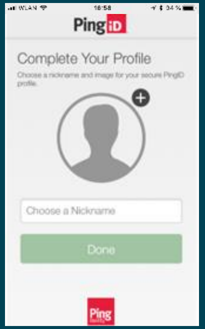
Ihr Gerät koppeln

Für eine manuelle Aktivierung von PingID geben Sie bitte unten den Kopplungsschlüssel ein, um Ihr Gerät zu koppeln.

Kopplungsschlüssel

Gerät koppeln

10. If pairing is successful, you may be asked to allow access to your location. This is not required and can be refused. Afterwards, you are asked to enter a name for your app profile. You can use any name here, but it is recommended to use your Daimler UserID. A photo is not required.



16:58

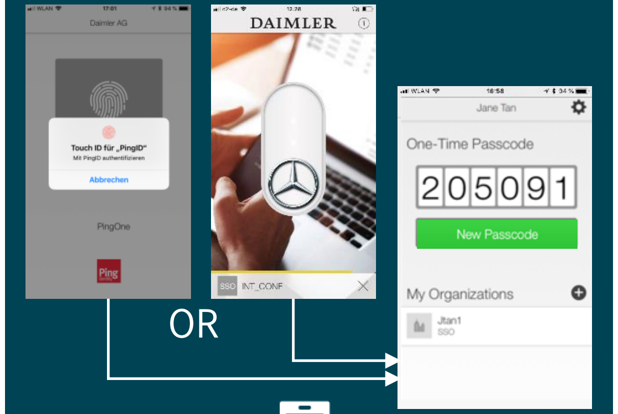
Complete Your Profile

Choose a nickname and image for your secure PingID profile.

Choose a Nickname

Done

11. To finish the pairing you are asked to use your fingerprint or to swipe the icon up. Fingerprint authentication is only enabled, if you have a mobile device with an activated fingerprint scanner. A green checkmark confirms this. Close the screen by clicking on “X”. Afterwards, the app shows a One-Time Password as seen on the right screen below. You are now ready to use the app.



17:01

Daimler AG

Touch ID für „PingID“
Mit PingID authentifizieren

Abbrechen

PingOne

DAIMLER

SSO INT_CONF

OR

16:58

Jane Tan

One-Time Passcode

205091

New Passcode

My Organizations

Jtan1
SSO

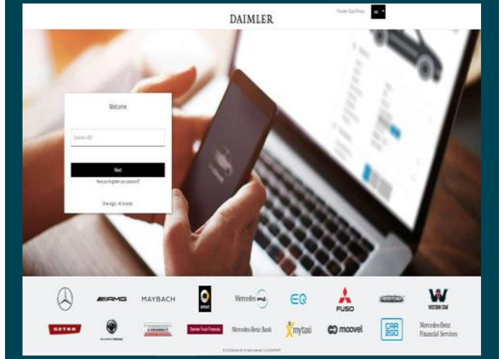
2b Activating the MFA Mobile App PingID

Activation using Mobile Applications 1/2

The following steps are required to activate and pair the PingID app while using a confidential mobile Daimler application.

1. **Launch the intended confidential mobile app.**

   Use your corporate UserID and your Corporate password and click "Sign In".



DAIMLER

Welcome

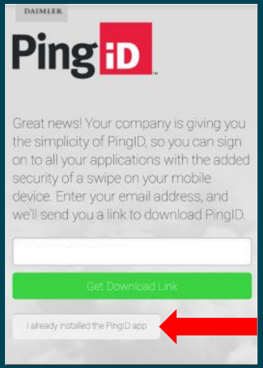
Daimler ID

Next

Have you forgotten your password?

One login. All brands.

2. **After a successful login, you will be forwarded to the MFA activation screen. As the PingID app was installed before, please click on "I have installed the app already"! (marked with red arrow in the screenshot below). Depending on your device you might have to scroll down to see this option.**



DAIMLER

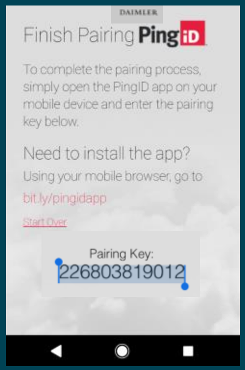
PingID

Great news! Your company is giving you the simplicity of PingID, so you can sign on to all your applications with the added security of a swipe on your mobile device. Enter your email address, and we'll send you a link to download PingID.

Get Download Link

I already installed the PingID app

3. **After a few seconds you will be asked to finish the pairing of your device. A Pairing Key is displayed at the end of the shown screen. Please make a note of the pairing key, since it is required for step 6. If your device allows to copy the key using the touch screen, you can also do so.**



DAIMLER

Finish Pairing PingID

To complete the pairing process, simply open the PingID app on your mobile device and enter the pairing key below.

Need to install the app?

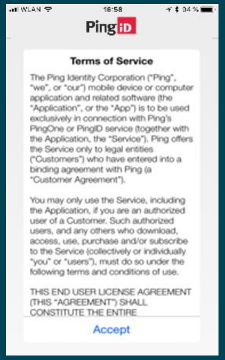
Using your mobile browser, go to

bit.ly/pingidapp

Start Over

Pairing Key:
226803819012

4. **Start the PingID app on the mobile device. On first time use the "Terms of Service" message is displayed. Please click "Accept" to continue.**



WLAN 16:58 34 %

PingID

Terms of Service

The Ping Identity Corporation ("Ping", "we", or "our") mobile device or computer application and related software (the "Application", or the "App") is to be used exclusively in connection with Ping's PingOne or PingID service (together with the Application, the "Service"). Ping offers the Service only to legal entities ("Customers") who have entered into a binding agreement with Ping (a "Customer Agreement").

You may only use the Service, including the Application, if you are an authorized user of a Customer. Such authorized users, and any others who download, access, use, purchase and/or subscribe to the Service (collectively or individually "you" or "users"), must do so under the following terms and conditions of use.

THIS END USER LICENSE AGREEMENT (THIS "AGREEMENT") SHALL CONSTITUTE THE ENTIRE

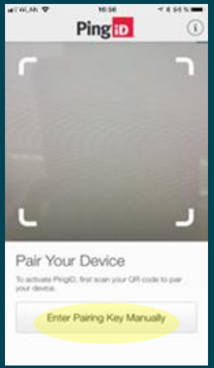
Accept

2b Activating the MFA Mobile App PingID

Activation using Mobile Applications 2/2

The following steps are required to activate and pair the PingID app while using a confidential mobile Daimler application.

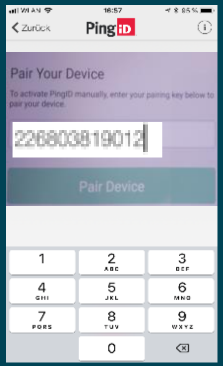
5. You will be asked for permissions to run PingID (camera, location and notifications). Accept at least notifications. Afterwards a camera window is shown. Click the button below the camera window (marked yellow in screenshot): “Enter Pairing Key Manually”



Pair Your Device

To activate PingID, first scan your QR code to pair your device.

6. Now the app shows a screen to enter the activation code. Please use the key you copied before in step 3 and paste it into the empty field. You can also enter it manually here and confirm it with the green button.

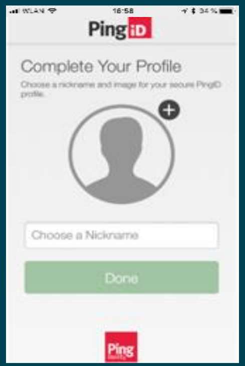


Pair Your Device

To activate PingID manually, enter your pairing key below to pair your device.

226803819012

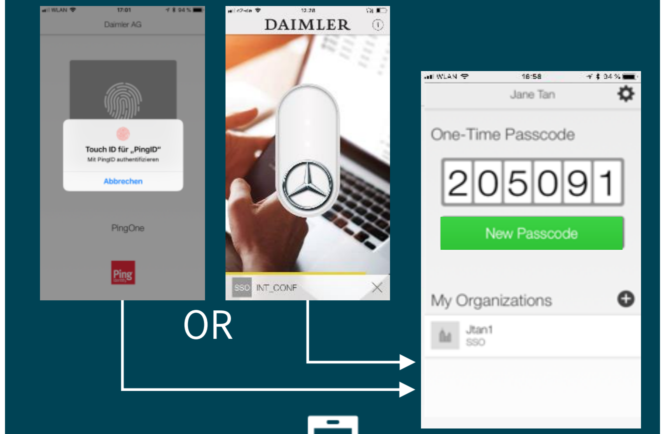
7. If pairing is successful, you may be asked to allow access to your location. This is not required and can be refused. Afterwards you are asked to enter a name for your app profile. You can use any name here, but it is recommended to use your Daimler UserID. A photo is not required.



Complete Your Profile

Choose a nickname and image for your secure PingID profile.

8. To finish the pairing you are asked to use your fingerprint or to swipe the icon up. (Fingerprint only when you have a mobile device with an activated fingerprint scanner). A green checkmark confirms this. Close the screen by clicking on “X”. Afterwards the app shows a One-Time Passcode screen like shown below. You are now ready to use the app for authentication.



Touch ID für „PingID“

Mit PingID authentifizieren

One-Time Passcode

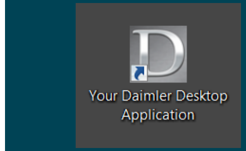
205091

3a How to work with the MFA Mobile App PingID 1/6

Default Login Process using an activated mobile device

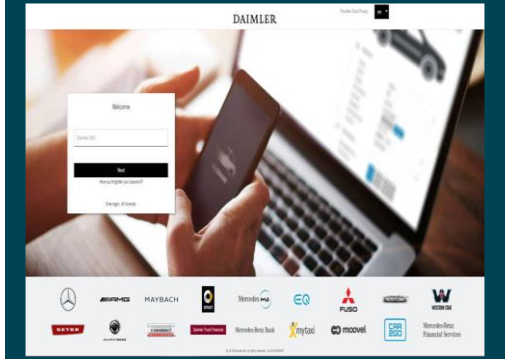
This is the standard procedure for login into a confidential application. All other cases see next slide.

1. Launch your intended desktop or web application:



Your Daimler Desktop Application

Use your Corporate User ID and your Corporate password to log in:



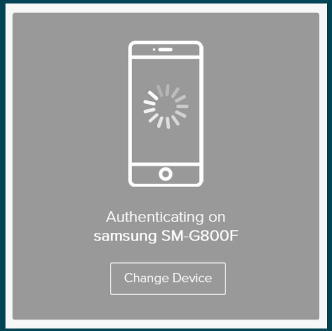
DAIMLER

Welcome

Next

One login. All brands.

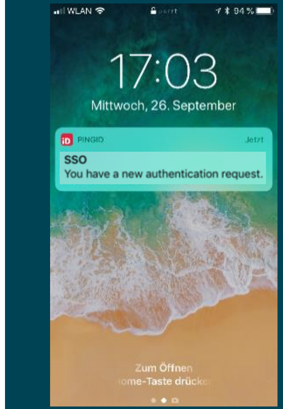
2. After successful login, a message will be shown in the web browser, that PingID notifies your mobile device. (see below)



Authenticating on samsung SM-G800F

Change Device

3. After a few seconds your paired mobile device will ask you to confirm your authentication by fingerprint or by swiping your finger. (If your device has no active fingerprint scanner please see next slides)



17:03

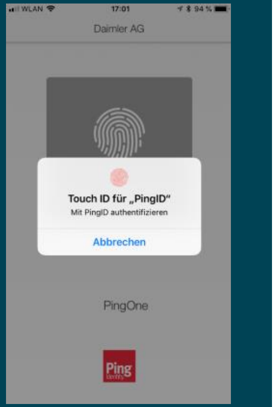
Mittwoch, 26. September

PINGID Jetzt

SSO

You have a new authentication request.

Zum Öffnen ome-Taste drück



Daimler AG

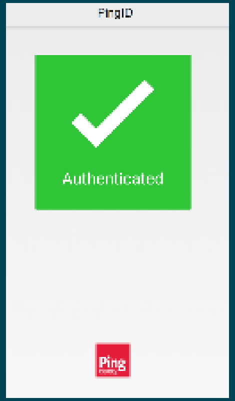
Touch ID für „PingID“

Mit PingID authentifizieren

Abbrechen

PingOne

4. After a successful confirmation a green checkmark is displayed on the desktop. You will be transferred automatically to your application.



PingID

Authenticated

3b How to work with the MFA Mobile App PingID 2/6

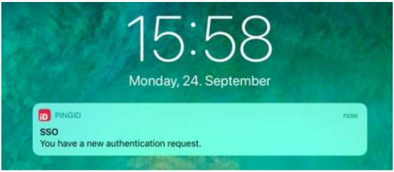
Authentication methods for iOS (see page 18 for further settings and their effects)

The PingID app for iOS offers different options to respond to an authentication request. The differences depend on the current state of the device: locked, unlocked or if the PingID app is already running in the foreground.

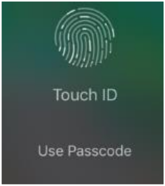
If your TouchID/Fingerprint is not activated, the unlock action is replaced with using the iOS unlock code

1. Notification on locked iPhone: - Touch quickly

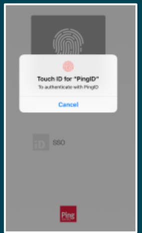
a) Touch the received message quickly

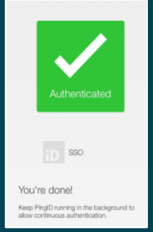

15:58
Monday, 24. September
PINGID now
SSO
You have a new authentication request.

b) Use your fingerprint or passcode to unlock and to open PingID



c) PingID opens.
Use your fingerprint to confirm*



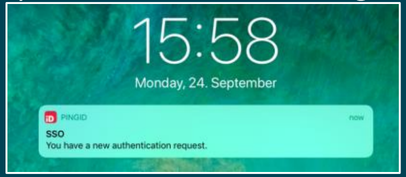


You're done!
Keep PingID running in the background to allow continuous authentication.

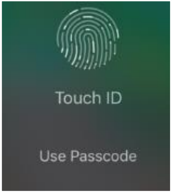
* = If your device has TouchID disabled there is a slider to swipe over the screen instead (see to the right in 4b)

2. Notification on locked iPhone: - Touch long

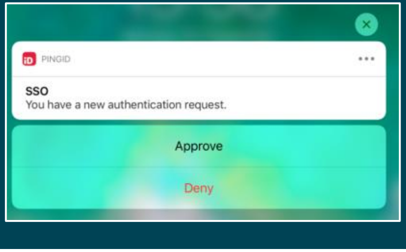
a) Touch the received message long


15:58
Monday, 24. September
PINGID now
SSO
You have a new authentication request.

b) Confirm with TouchID or Passcode:

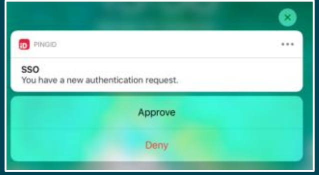


c) Decide to approve or to deny the request


PINGID
SSO
You have a new authentication request.

3. Notification on unlocked iPhone:

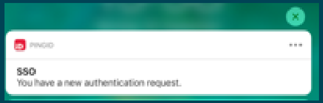
a) Touch and swipe down message (on some iOS devices „Force Touch" is available instead of „Swipe down"


PINGID
SSO
You have a new authentication request.

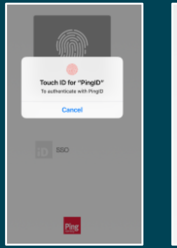
Click „Approve" to confirm

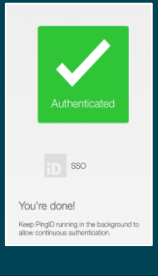
OR

b) If you touch the message quickly


PINGID
SSO
You have a new authentication request.

The PingID app opens.
Use your fingerprint to confirm.

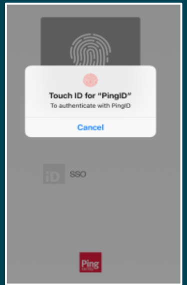


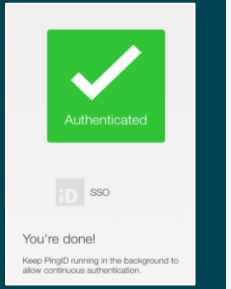


You're done!
Keep PingID running in the background to allow continuous authentication.

4. Message with PingID app running in foreground:

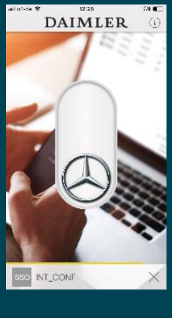
a) When Touch ID is active:
Confirm with your fingerprint

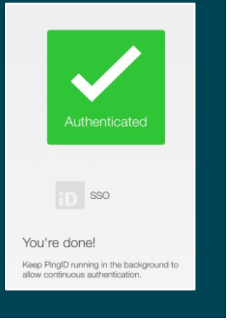




You're done!
Keep PingID running in the background to allow continuous authentication.

b) Device without or with disabled TouchID:
Swipe the icon up.





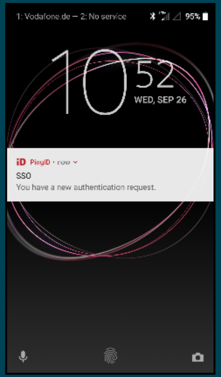
You're done!
Keep PingID running in the background to allow continuous authentication.

3b How to work with the MFA Mobile App PingID 3/6

Authentication methods for Android (see page 18 for further settings and their effects)

The PingID app for Android offers different options to respond to an authentication request. This depends on the Android version and the current device state: locked, unlocked or if the PingID app is already running in the foreground.

1. On locked Android:
- Touch the notification



1: Vodafone.de – 2: No service

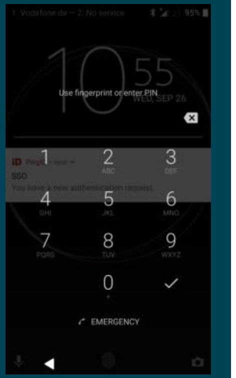
10 52 WED, SEP 26

PingID • now

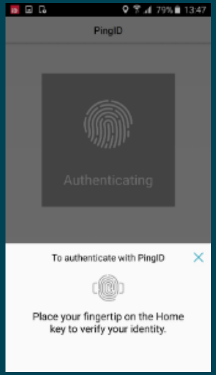
SSO

You have a new authentication request.

a) Unlock the device by code or fingerprint



Use fingerprint or enter PIN



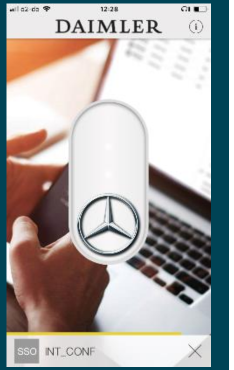
PingID

Authenticating

To authenticate with PingID

Place your fingertip on the Home key to verify your identity.

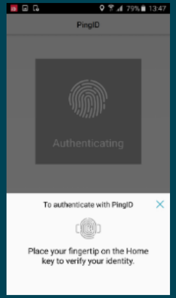
b) PingID opens. Confirm by using your fingerprint or by swiping the iconup (if your device has no fingerprint scanner)



2. On unlocked Android:

→ On unlocked Android devices any PingID notification will bring the PingID app automatically to the foreground

a) PingID opens. Confirm by using your fingerprint or by swiping the icon up (if your device has no fingerprint scanner)

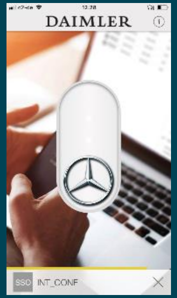


PingID

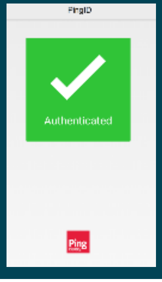
Authenticating

To authenticate with PingID

Place your fingertip on the Home key to verify your identity.

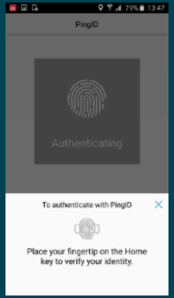


b) The PingID app confirms successful authentication with the green checkmark.



3. Message with PingID app running in foreground:

a) PingID starts authentication. Confirm by using your fingerprint or by swiping the icon up (if your device has no fingerprint scanner)

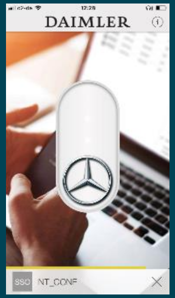


PingID

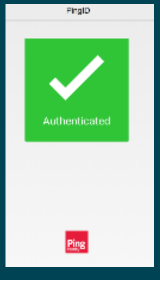
Authenticating

To authenticate with PingID

Place your fingertip on the Home key to verify your identity.



b) The PingID app confirms successful authentication with the green checkmark.



3b How to work with the MFA Mobile App PingID 4/6

Authentication Settings: Fingerprint/Swipe or OTP

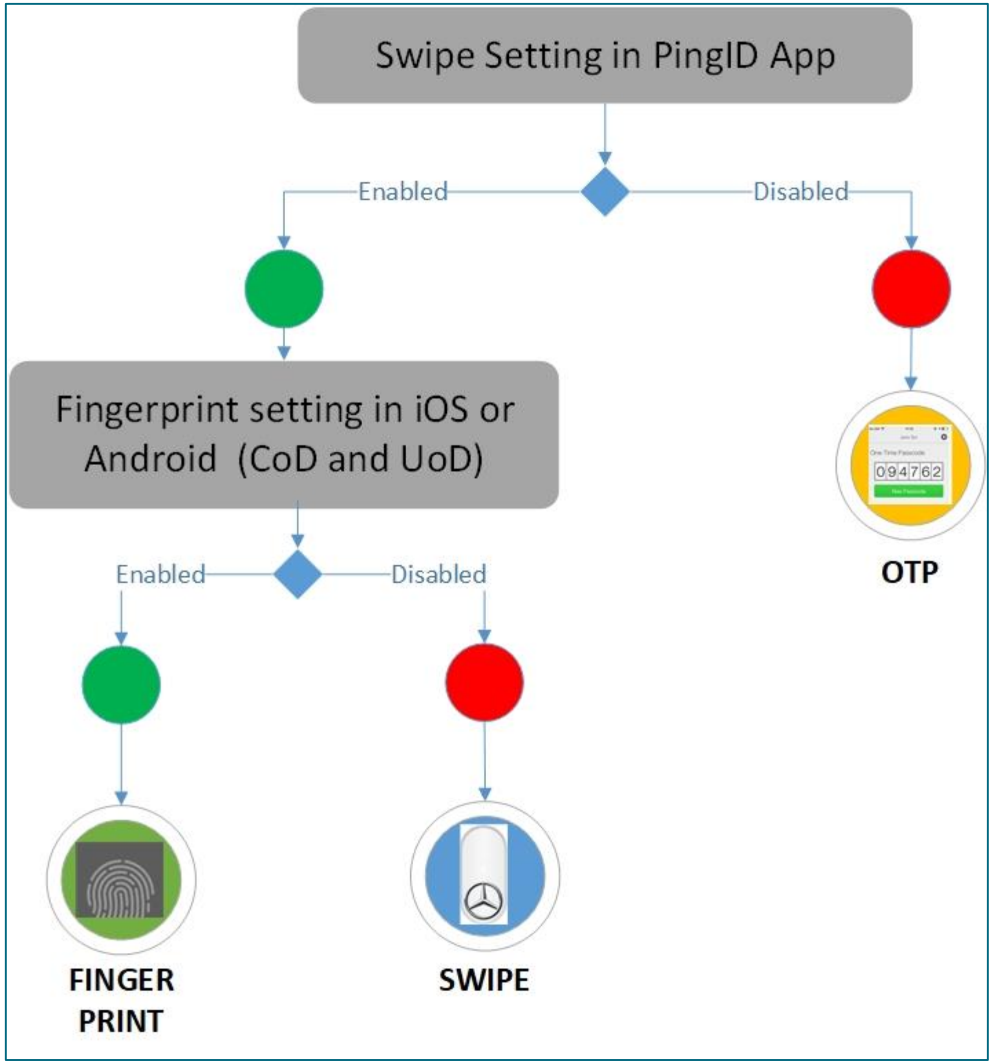
Two settings on your mobile device are influencing the behavior of the PingID app:

1. **Ping ID app setting "Swipe": Enabled or Disabled.**
2. **Mobile device setting "Fingerprint": Enabled or Disabled**

Depending on these settings, the PingID App will ask for different types of authentication:

- **Fingerprint**
- **Swipe**
- **One-Time Password (OTP)**

If you have enabled both settings you will always use the fingerprint authentication. (Recommendation)
For all options please check the tree chart on the right.


Swipe Setting in PingID App
Enabled
Disabled
Fingerprint setting in iOS or Android (CoD and UoD)
Enabled
Disabled
094762
OTP
FINGER PRINT
SWIPE

3c How to work with the MFA Mobile App PingID 5/6

Fallback options in case of different problems

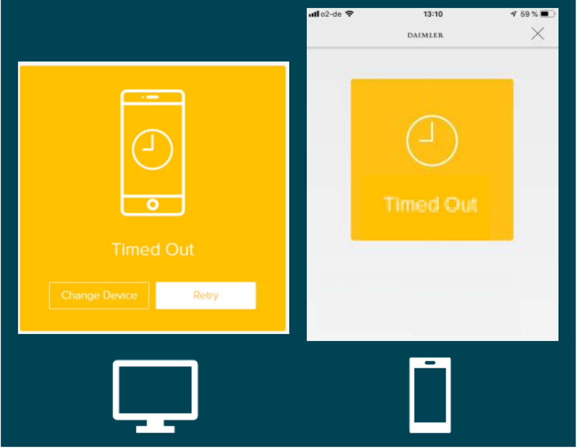
There are two fallback options if the standard authentication procedures with the mobile app do not work immediately:

1. Timeout of request: Re-Authentication

a) If you have an unlocked mobile device and the authentication is not confirmed within 20 seconds, a yellow timeout message is displayed in the web browser and also shortly in the mobile app.
This message contains buttons to repeat the authentication (right button "Retry") or to change the authentication device (left button)

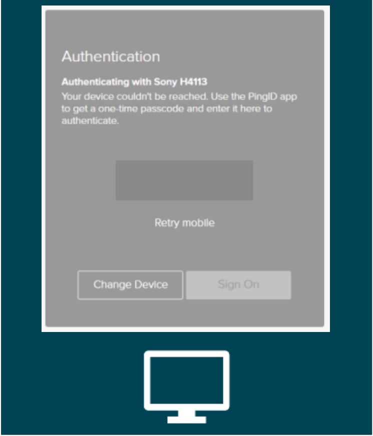
b) If the device is locked or cannot be reached by PingID, a grey field to enter a one-time passcode appears after 30 seconds.
Please continue with step 2 in this case. (See description on the right)

Variant a)



Only when registering more than one MFA device these dialogues will show the option „Change Device

Variant b)



Authentication

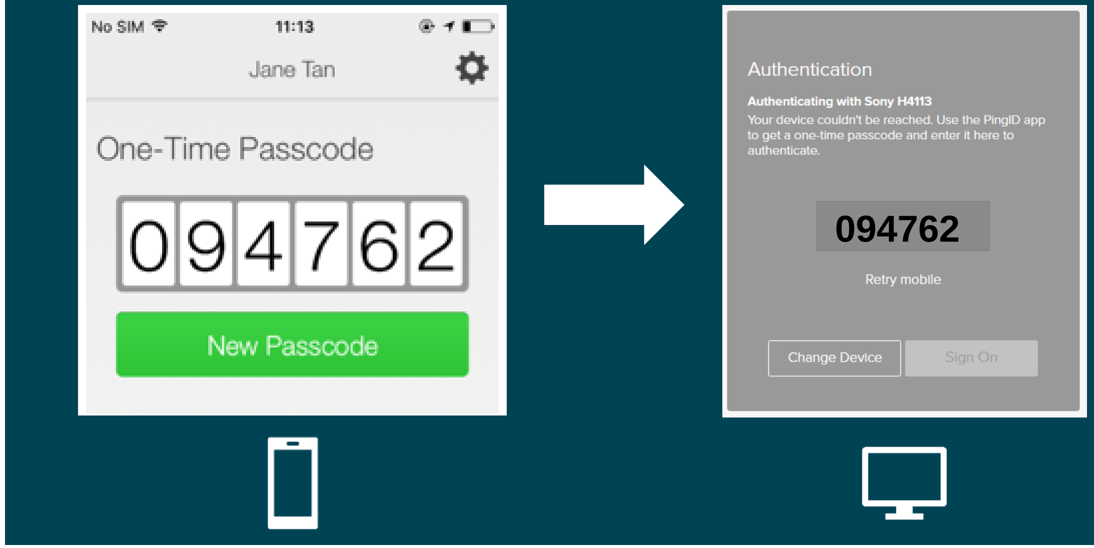
Authenticating with Sony H4113

Your device couldn't be reached. Use the PingID app to get a one-time passcode and enter it here to authenticate.

2. Mobile device is offline: Authentication with OTP

a) In cases where your mobile device is offline or cannot be reached by Push notifications due to connectivity issues, the PingID mobile can be started for displaying an OTP code (OTP=One-Time Password). This can be used for login. When you manually start the app on the mobile device by clicking on the red PingID icon, the app is started in OTP mode right away: iD

b) Enter the displayed number code into the field on the webpage and confirm with "Sign On"



Authentication

Authenticating with Sony H4113

Your device couldn't be reached. Use the PingID app to get a one-time passcode and enter it here to authenticate.

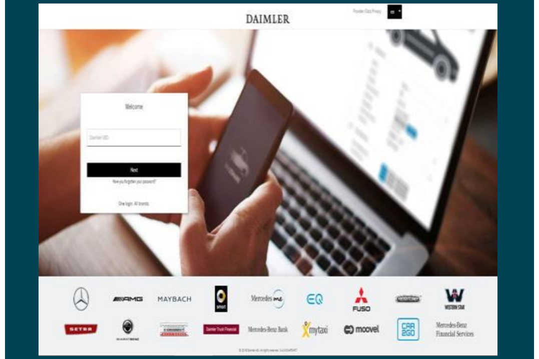
3d How to work with the MFA Mobile App PingID 6/6

Login with different MFA Devices

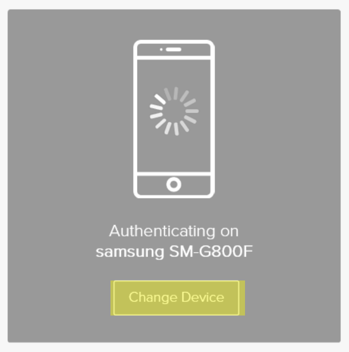
Caution: This type of login is only possible, if you have more than one active MFA device. See Chapter 4 for details.

1. Launch your intended desktop or web application:

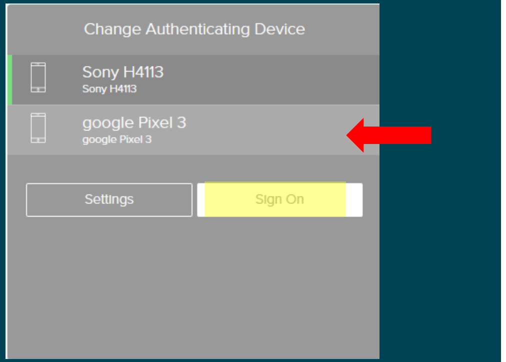
Use your Corporate User ID and your Corporate password to sign in:



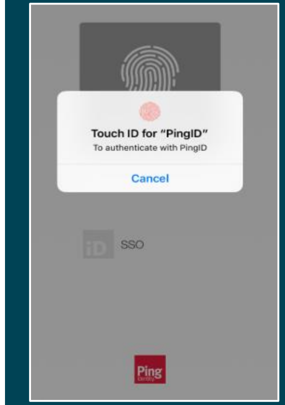
2. If you want to login with another MFA device than your primary, you can change this during the started authentication process. Just click on the "Change Device" button in the lower part of the authentication screen:

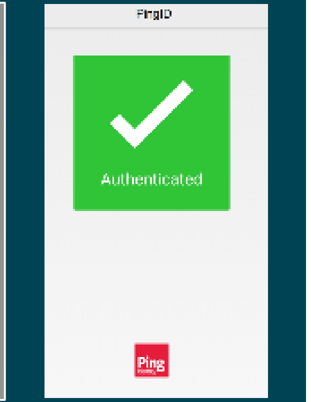

Authenticating on samsung SM-G800F

3. An overview of your currently registered MFA devices will be displayed. Please click on the device, which you intend to login with now. This device will then be notified next. Please confirm your choice with „Login".



4. The further procedure of the login process is as described on the pages before. You will get a notification, use your fingerprint or swipe and get logged in this way with the usage of your other MFA device.



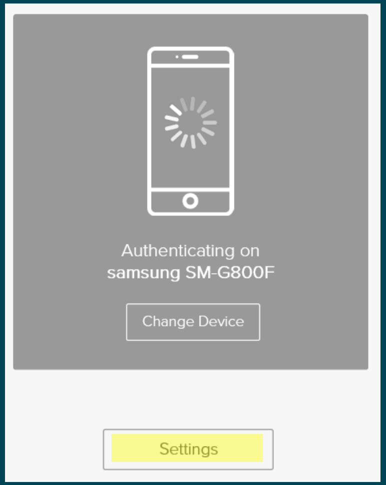


4a Self Service Processes with MFA4Daimler

Add another mobile device

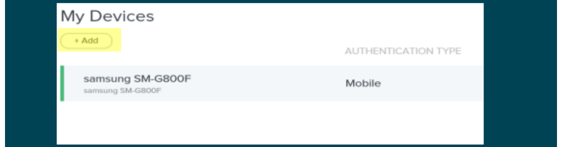
If you have more than one mobile device, you can add additional devices to your MFA/PingID setup.

1. Begin your authentication to a confidential app. When the PingID dialogue pops up, do not confirm the authentication on your mobile. Click “Settings” at the bottom of the page to go to your personal PingID device configuration.



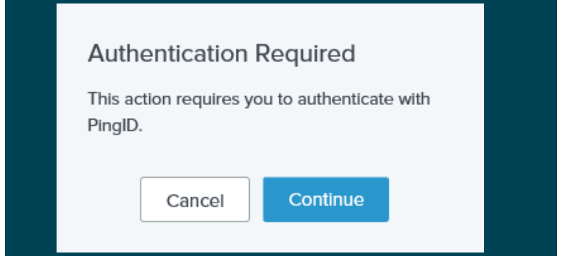
Authenticating on samsung SM-G800F

2. On the “My Devices” screen you will see your currently registered mobile phone. Click on “Add” to start the registration process for a new device. Please click continue and authenticate with the already registered device.



My Devices

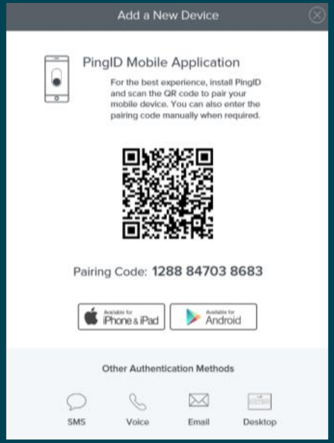
	AUTHENTICATION TYPE
samsung SM-G800F samsung SM-G800F	Mobile



Authentication Required

This action requires you to authenticate with PingID.

3. The “Add a new device” dialogue appears. Carry on with the registration of your second phone as explained on the slides 1b: “Activating the Ping ID Mobile App”



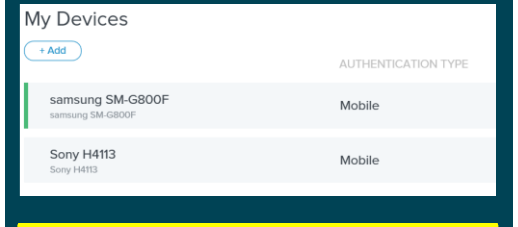
Add a New Device

PingID Mobile Application

For the best experience, install PingID and scan the QR code to pair your mobile device. You can also enter the pairing code manually when required.

Pairing Code: 1288 84703 8683

4. Afterwards you will see the your new device in the “My Devices” list. You can sign off or just close the browser.



My Devices

	AUTHENTICATION TYPE
samsung SM-G800F samsung SM-G800F	Mobile
Sony H4113 Sony H4113	Mobile

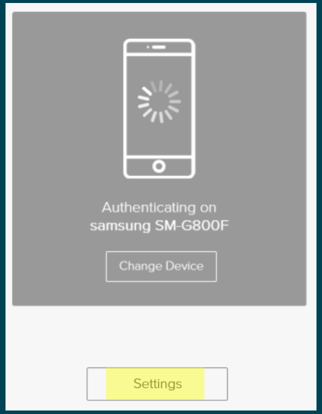
- **You can register 4 devices as a maximum.**

4b Self Service Processes with MFA4Daimler

Change your primary authentication device

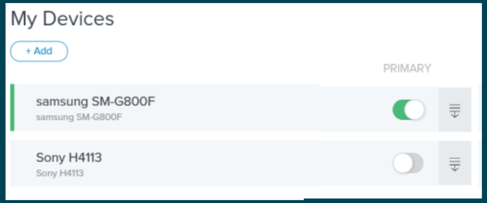
If you work with two mobile phones you can change the primary device, which should be notified by default.

1. Authenticate to a confidential app and when the PingID dialogue is shown, please click “Settings” to go to your personal PingID configuration page.



Authenticating on samsung SM-G800F

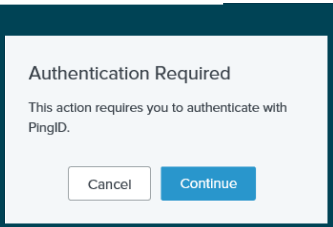
2. On the “My Devices” screen you can see your registered devices with your current primary device shown in green (button is swiped to the right).
If you want to change your primary device, swipe the button next to the desired device to the right.
Please click continue and authenticate with the current primary device.



My Devices

samsung SM-G800F
samsung SM-G800F

Sony H4113
Sony H4113

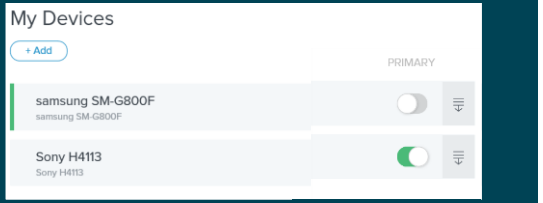


Authentication Required

This action requires you to authenticate with PingID.

3. The primary device has now been changed, indicated by the green button. From now on, it will be notified first, when you use the standard authentication process 3a (see page 13).

4. You can sign off or just close the browser now.



My Devices

samsung SM-G800F
samsung SM-G800F

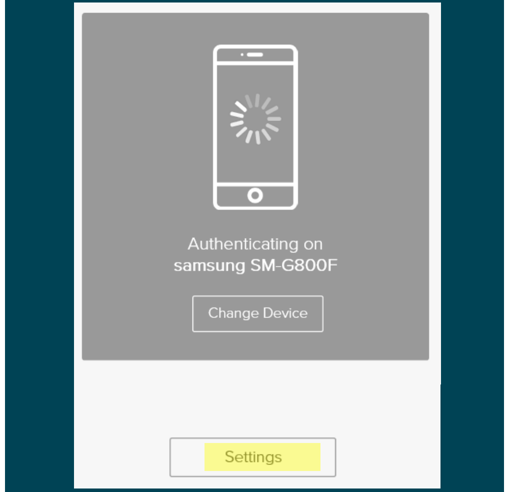
Sony H4113
Sony H4113

4c Self Service Processes with MFA4Daimler

Delete a mobile device from PingID

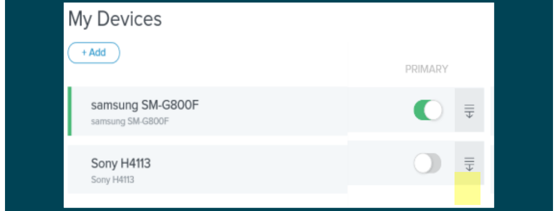
If you want to remove a device from PingID, you can use the following process.

1. Authenticate to a confidential app and when the PingID dialogue is shown, click “Settings” to go to your personal PingID configuration page.



Authenticating on samsung SM-G800F

2. On the “My Devices” screen, click on the lines of the device you want to remove. Please authenticate with the primary device if prompted.

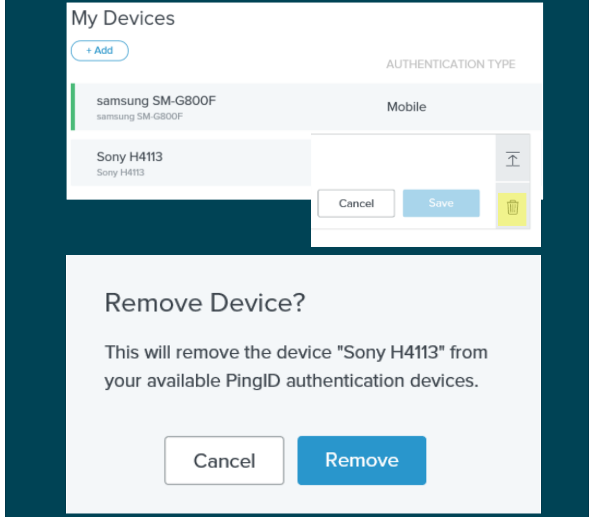


My Devices

samsung SM-G800F
samsung SM-G800F

Sony H4113
Sony H4113

3. Click on the bin icon. You are prompted to confirm the removal of that device from Ping ID.



My Devices

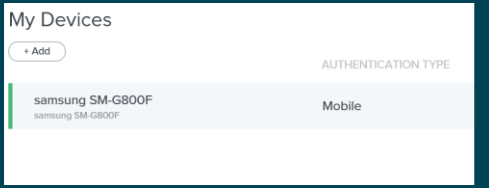
samsung SM-G800F
samsung SM-G800F
Mobile

Sony H4113
Sony H4113

Remove Device?

This will remove the device "Sony H4113" from your available PingID authentication devices.

4. After removing the device you will see your remaining devices in the “My Devices” overview. You can sign off or just close the browser now.



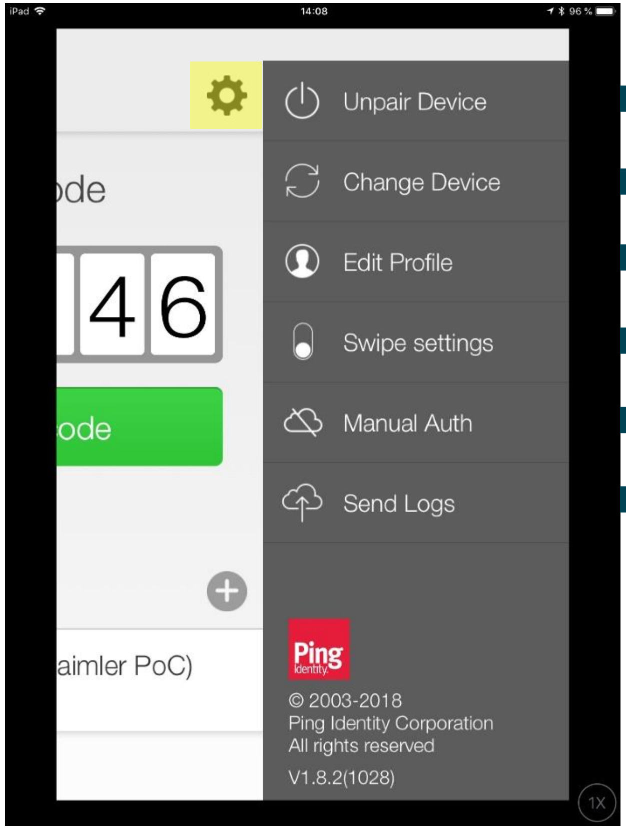
My Devices

samsung SM-G800F
samsung SM-G800F
Mobile

5a Self Service Processes in the MFA/PingID App 1/2

The options menu

The PingID app for iOS or Android devices offers several options for self-services.
When clicking on the settings icon on the upper right corner, an additional menu appears. The options are explained below.



For deactivating the device from PingID. You cannot authenticate with this device afterwards anymore (!)

For transferring the authentication to a new mobile device. Deactivates this device. (see next page)

For editing your name and add a photo. This is just for display purposes inside the app.

For disabling the swipe and fingerprint feature,
i.e. if you are on a slow internet line or if you prefer the usage of OTP passcodes only.*

For app synchronization: On very rare occasions you may be asked to authenticate manually.
Please click here to authenticate with a QR code or number. The login page will tell you when and how.

For analysis purposes only. Do not use unless asked for by the Helpdesk.

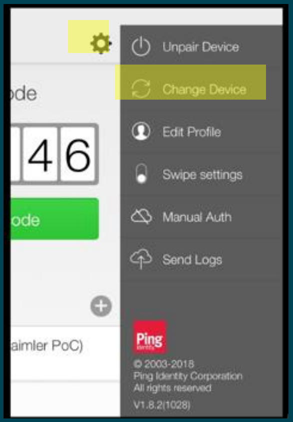
*= You cannot configure to use swipe instead of fingerprint, if your device has an active fingerprint scanner.
You can only configure to deactivate Swipe and fingerprint completely !

5b Self Service Process in the MFA/PingID App 2/2

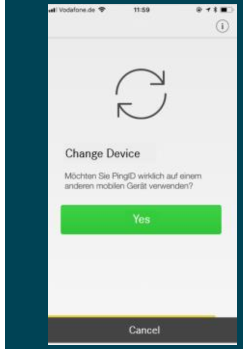
Migrate the PingID authentication to a new mobile device

Your old and your new mobile device have to be available simultaneously to do a complete migration of the app. If your old device is not available, but you need to register a new device, please contact your administration to reset your account in GEMS..

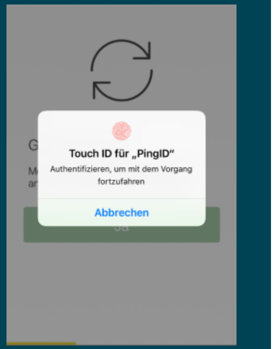
1. Start the PingID app on the "old" mobile device.
   Click on the settings icon on the upper right to open the menu and click on "Change Device"



2. The "old" device will ask for confirmation, if you want to change the service and move it to another device. Please confirm with "Yes" (left picture). You are asked to confirm with your fingerprint or with the unlock code of your device.

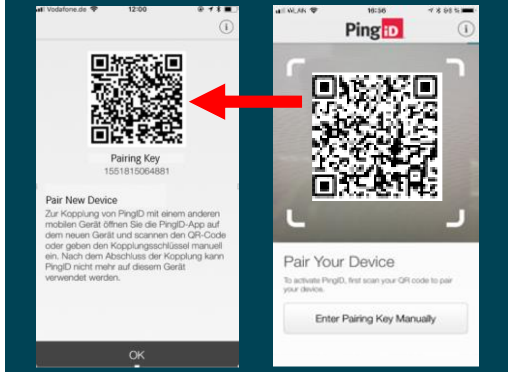

Change Device

Möchten Sie PingID wirklich auf einem anderen mobilen Gerät verwenden?


Touch ID für „PingID"

Authentifizieren, um mit dem Vorgang fortzufahren

3. Please install the PingID app on the "new" mobile device like on slide 1a. Start the app and allow access to the camera.
   Scan the QR code of the old device with the camera of the new mobile device or enter the pairing key.


Pairing Key
1551815064881

Pair New Device

Zur Kopplung von PingID mit einem anderen mobilen Gerät öffnen Sie die PingID-App auf dem neuen Gerät und scannen den QR-Code oder geben den Kopplungsschlüssel manuell ein. Nach dem Abschluss der Kopplung kann PingID nicht mehr auf diesem Gerät verwendet werden.

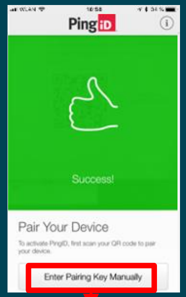
Pair Your Device

To activate PingID, first scan your QR code to pair your device.

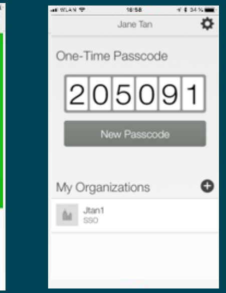
Old device

New device

4. If pairing is successful, a green confirmation message will be shown on the new device. You are now ready to use the migrated app for authentication.


Pair Your Device

To activate PingID, first scan your QR code to pair your device.



If pairing with the camera fails, click on „Enter Pairing Key Manually" and enter the pairing key displayed in step 3 on the old device (displayed below the QR code.)

Symbols:

▯ Old Device

▯ New Device

6 Service Process with MFA4Daimler – Account Reset

**Remark: If you want to activate or migrate to a new mobile device and your old device is still accessible,
please use the Self Service migration process explained before. In this case a reset through your data administration is not required.**

If the access to your MFA4Daimler access has been interrupted by events like loss, break, or reinstallation of your currently paired device and you have no access to additionally paired devices, your data administration has to reset MFA4Daimler for your account.

In this case, please contact your helpdesk or data administration to furter assist you with the reset.

7 Additional Support

For any additional support issues regarding the MFA4Daimler service, please contact the MFA4Daimler Application Helpdesk (Supported languages currently english and german):

Tel/Fax: +49 (711) 17-25005
Mail: cuhd_support_mfa4daimler@daimler.com

Version Information

Version	Date	Major Changes
1.0	2019-09-17	1st version of Daimler Handbook MFA mobile for Dealer and Supplier Communities
1.1	2019-11-08	Added section for the usage of hardware security keys
1.2	2020-06-30	Added hint regarding camera and notification access for the PingID App
1.3	2021-02-17	Minor Updates, removal of hardware security key section due to dedicated available guide