

DAIMLER

MFA4Daimler

Benutzerhandbuch MFA Mobile – Dealer & Supplier
Community



DAIMLER

Hinweis zu diesem Dokument

Wenn Sie eine Kopie dieses Handbuchs heruntergeladen haben, könnte diese veraltet sein. Stellen Sie sicher immer die neueste Version zu verwenden.

Inhaltsverzeichnis MFA4Daimler Benutzerhandbuch Mobile

Einleitung

Inhalt

1. Installation und Konfiguration
 - a) Installieren der MFA Mobile App “PingID”
 - b) Konfigurieren des mobilen Endgeräts / empfohlene Einstellungen
2. Aktivierung der MFA Mobile App “PingID”
 - a) mit Desktop basierten Anwendungen
 - b) mit mobile Anwendungen
3. Anmeldeverfahren
 - a) Arbeiten mit der MFA Mobile App “PingID”: Standard-Login-Verfahren
 - b) Anmeldeverfahren mit der PingID Mobile App im Detail (iOS und Android)
 - c) Fallback Optionen
4. Self Service Prozesse:
 - a) Ein weiteres mobiles Endgerät hinzufügen
 - b) Ändern des primären Endgeräts
 - c) Löschen eines mobilen Endgeräts
5. Self Service Prozesse in der MFA App
 - a) Das Optionen Menü
 - b) Migration eines mobilen Endgeräts
6. Service Prozess: Reset
7. Support

Klicken Sie auf die Unterstriche, um zu den Inhalten zu gelangen.

MFA4Daimler Benutzerhandbuch

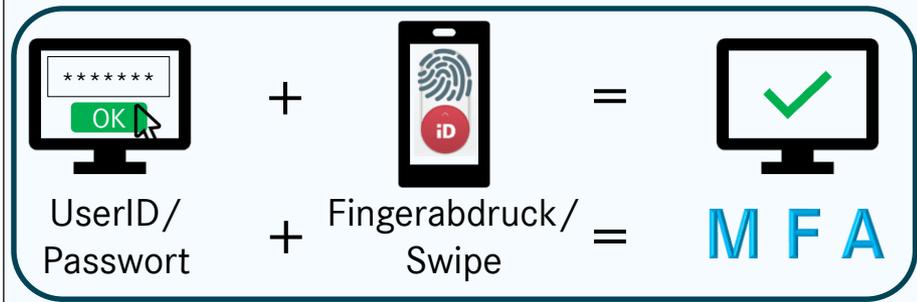
Der neue MFA Standard für Daimler

Eine zukunftssichere Lösung zur Multi-Faktor-Authentifizierung (MFA).

- Das Ziel dieser Lösung besteht darin, einen modernen, cloud-fähigen und hochmodernen Ersatz für die frühere Strong Authentication-Lösung „GAS - Confidential (SecurePIN)“ bereitzustellen.
- Die neue Lösung ist einfach zu bedienen und entspricht den heutigen Standards für sichere Authentifizierung.
- Die Informationssicherheitsrichtlinie von Daimler setzt voraus, dass vertrauliche Anwendungen die Multi-Faktor-Authentifizierung verwenden. Die neue MFA ist der „zweite Faktor“, wenn Sie sich bei einer solchen Anwendung anmelden.

Die neue MFA ist sicher und einfach

Die verschiedenen Faktoren (1 und 2) werden zu einer sicheren Authentifizierung zusammengefasst:



Die neue MFA bietet höchste Standards

Melden Sie sich an mit etwas, das Sie kennen UND etwas, das Sie haben.

- Der Zweck der mehrstufigen Authentifizierung besteht darin, mindestens zwei Anmeldeverfahren zu nutzen. Dies wird durch die Kombination verschiedener Authentifizierungstechnologien erreicht.
- Bei Daimler wird eine Kombination aus einem wissensbasierten ersten Faktor (Passwort) mit einem zweiten, auf Besitz basierenden Faktor kombiniert, der als zusätzlicher Nachweis der Authentifizierung dient (Fingerabdruck oder Zufallscode).

MFA4Daimler Benutzerhandbuch

Über dieses Handbuch

In diesem Dokument wird erläutert, wie Sie die neue MFA-4-Daimler-Lösung aktivieren und verwenden können. Es umfasst die Installation, die verschiedenen Authentifizierungsverfahren und Self-Service-Prozesse.

In dieser Anleitung sehen Sie zwei verschiedene Symbole.

Sie geben an, auf welchem Gerät der beschriebene Schritt durchgeführt werden muss :



Schritt auf iOS oder Android



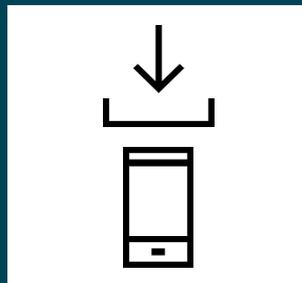
Schritt auf Windows / MacOS
Notebook oder Desktop

Quick Links zu den wichtigsten MFA-Schritten

Klicken Sie auf das entsprechende Bild, um fortzufahren

**Mit MFA
beginnen**

MFA nutzen - Teil 1
Installieren und Konfigurieren



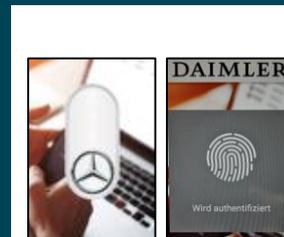
Folien 1a, 1b

MFA nutzen - Teil 2
Aktivierung und Kopplung



Folien 2, 2a, 2b

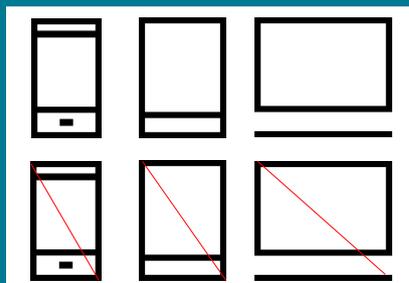
MFA nutzen - Teil 3
Mit MFA authentifizieren



Folien 3a, 3b, 3c

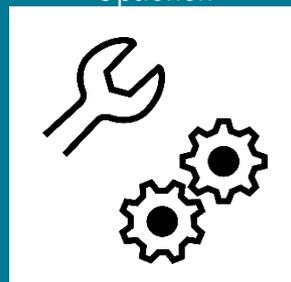
**MFA anpassen und
Fehler beheben**

Self Services - Teil 1
Geräte hinzufügen, ändern, löschen



Folien 4a, 4b, 4c

Self Services - Teil 2
Gerätemigration und andere
Optionen



Folien 5a, 5b

Self Services - Teil 3
4-Augen-Reset



Folie 6

1a Installieren der MFA Mobile App „PingID“

Installation für iOS und Android

Die MFA-App "PingID" muss vor der nächsten Verwendung einer vertraulichen Applikation auf Ihrem iOS- oder Android-Gerät installiert werden. Bitte laden Sie die „PingID“ App aus Ihrem AppStore (iOS/Android) auf Ihr Smartphone.

- a) Minimale Systemanforderungen für die Installation auf mobilen Endgeräten:
Für iOS: Version 11 und höher, oder Android Version 6 (Marshmallow) und höher.
- b) Auf iOS wird jeder Fingerabdrucksensor (TouchID) unterstützt. Auf Android wird jeder Fingerabdrucksensor ab der genannten Version unterstützt.

Hinweis: Während der Installation werden verschiedene Berechtigungen von der “PingID” App angefragt (Kamera, Standort, Benachrichtigungen). Für die beste Benutzererfahrung wird empfohlen den Zugriff zur Kamera sowie Benachrichtigungen zu erlauben. Die Standort Berechtigung ist nicht nötig.

1b Konfigurieren des mobilen Endgeräts

Empfohlene Einstellungen für iOS und Android

Um sicherzustellen, dass die in diesem Dokument erläuterte MFA-Funktion auf Ihrem mobilen Endgerät wie erwartet funktioniert, werden die empfohlenen Benachrichtigungseinstellungen nachstehend beschrieben. Die PingID-App funktioniert grundsätzlich auch mit anderen Einstellungen, dann kann jedoch bei Benachrichtigungen ein anderes als das in diesem Dokument beschriebene Verhalten auftreten. Die folgenden Einstellungen werden empfohlen, um sicherzustellen, dass Sie auf Ihrem gesperrten mobilen Endgerät benachrichtigt werden, wenn Sie sich mit MFA authentifizieren müssen.

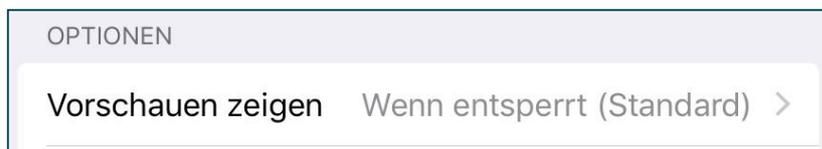
iOS Mitteilungen



- Starten Sie die iOS „Einstellungen“ App – Gehen Sie zu Mitteilungen



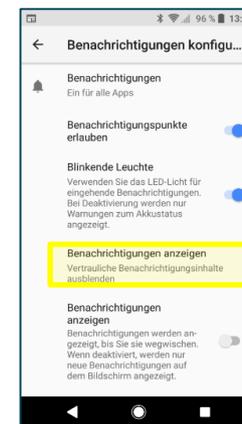
- Scrollen sie auf der linken Seite nach unten bis zu „PingID“.
- Wählen Sie rechts aus „Vorschauen anzeigen“ – „Wenn entsperrt“.
(könnte wie unten dargestellt bereits vorgelegt sein).



Android Benachrichtigungen*



- Starten Sie die Android „Einstellungen“ App – Gehen Sie zu Apps & Benachrichtigungen.
- Gehen sie zu „Benachrichtigungen konfigurieren“.
- Überprüfen Sie, dass bei „Benachrichtigungen anzeigen“ die Einstellung: „Vertrauliche Benachrichtigungsinhalte ausblenden“ steht.
- Wenn Sie für sich entschieden haben, keine systemweiten Benachrichtigungen für Ihr Gerät zuzulassen, gehen Sie bitte zu „Benachrichtigungen“ oben im selben Menü und wählen dort die App „PingID“ aus. Im dortigen Menü wählen Sie dann unter „Auf dem Sperrbildschirm“ „Vertrauliche Benachrichtigungsinhalte ausblenden“ aus.



- * Unterschiedliche Smartphones und Androidversionen können abweichende Menueinträge aufweisen.

2 Aktivierung der MFA Mobile App „PingID“

Es gibt zwei Möglichkeiten zur Aktivierung:

Für die Aktivierung der PingID Mobile App ist nur eine der folgenden Anweisungen erforderlich:

1. Wenn Sie eine vertrauliche Applikation auf dem Desktop oder Notebook nutzen wollen.
(gilt für Notebooks oder Desktops)

→ Bitte folgen Sie dem Abschnitt [2a](#)
(Seiten 10-12)



ODER

2. Wenn Sie eine vertrauliche Applikation auf einem mobilen Endgerät nutzen wollen.
(gilt für iOS- und Android-Geräte)

→ Bitte folgen Sie dem Abschnitt [2b](#)
(Seiten 13-14)



Nach der Aktivierung der App ist diese vollständig personalisiert und wird mit Ihrer persönlichen Daimler UserID verknüpft.
Die App darf aufgrund der Personalisierung nicht mit anderen Nutzern geteilt werden.

2a Aktivierung der MFA Mobile App „PingID“: Aktivierung mit Desktop-basierten Anwendungen 1/3

Die folgenden Schritte sind erforderlich, um die PingID-App zu aktivieren und zu koppeln, während Sie eine vertrauliche Desktopanwendung auf Ihrem Windows-Computer verwenden. Dies ist nur einmalig erforderlich. (Ausnahme: wenn Sie PingID auf neuen Geräten erstmalig einsetzen oder Ihr Gerät zurücksetzen müssen).

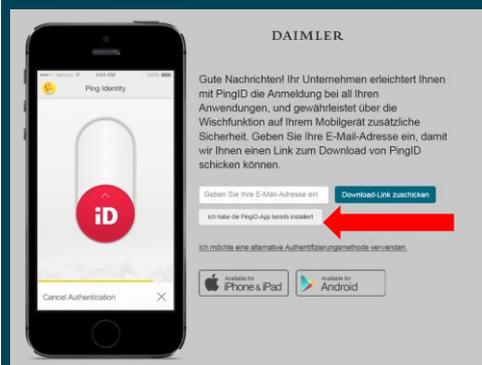
1. Starten Sie Ihre vertrauliche Desktop- oder Ihre Webanwendung.



Verwenden Sie Ihre Corporate Benutzer-ID und Ihr Corporate Passwort und klicken Sie auf "Anmelden".



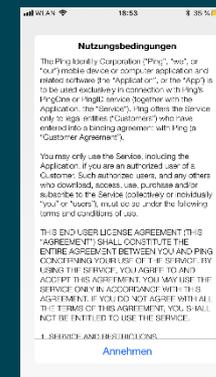
2. Nach einem erfolgreichen Login werden Sie zum MFA-Aktivierungsbildschirm weitergeleitet. Da die PingID-App zuvor installiert wurde, klicken Sie bitte auf "Ich habe die Ping-ID App bereits installiert" (im Screenshot unten mit rotem Pfeil markiert)



3. Nach einigen Sekunden werden Sie aufgefordert, die Kopplung Ihres Geräts abzuschließen. Ein QR-Code und ein Pairing-Schlüssel werden angezeigt. Sie können auf „Von vorne anfangen“ klicken, wenn Sie einen Schritt zurückgehen möchten.



4. Starten Sie die PingID-App auf dem mobilen Gerät. Bei der ersten Verwendung wird die Meldung "Nutzungsbedingungen" angezeigt. Bitte lesen Sie den Text und klicken Sie auf „Annehmen“, um fortzufahren.



2a Aktivierung der MFA Mobile App "PingID":

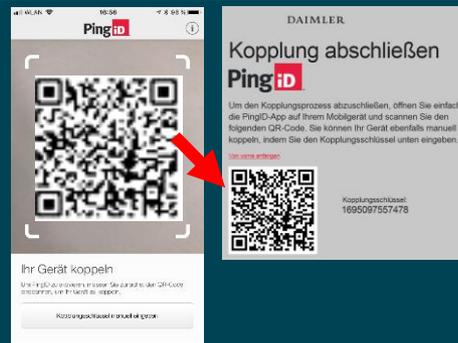
Aktivierung mit Desktop-basierten Anwendungen 2/3

Die Aktivierung ist durch einen QR-Scan möglich. Hierfür ist Zugriff auf die Kamera erforderlich. Alternative s. Kasten rechts. Befolgen Sie die Schritte 5 bis 7 auf dieser Seite und fahren Sie mit Schritt 11 auf der nächsten Seite fort.

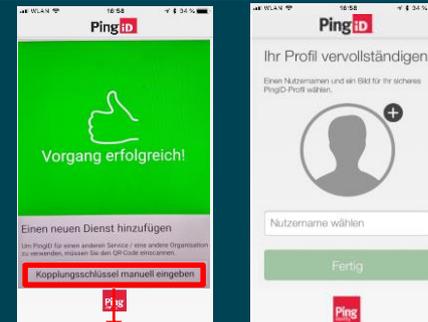
5. Die PingID bittet Sie um Berechtigungen für Kamera, Standort und Benachrichtigungen)*. Wenn Sie den Kamerazugriff akzeptiert haben, wird ein Kamerafenster in der App angezeigt. Wenn Sie keinen Zugriff auf die Kamera gewährt wollen, fahren Sie mit Schritt 8 fort.



6. Bitte scannen Sie mit Ihrem Handy den QR-Code auf der Webseite. Bewegen Sie Ihr Smartphone mit dem Kamerafenster zu Ihren Computerbildschirm, damit der QR-Code auf dem Display sichtbar wird. Ein Piepton bestätigt die erfolgreiche QR-Erkennung.



7. Bei Erfolg wird eine grüne Bestätigungsmeldung angezeigt. Anschließend werden Sie aufgefordert, einen Namen für Ihr Profil zu vergeben. Es wird empfohlen, Ihre Daimler UserID zu verwenden. Ein anderer Name ist aber zulässig. Ein Foto ist nicht erforderlich.



*** = Die Berechtigungen für die Kamera und für die Benachrichtigungen werden empfohlen. Die Standortberechtigung ist nicht erforderlich.**

Alternative Aktivierung ohne Kamera:

Ohne Kamera oder wenn Sie keinen Zugriff auf die Kamera erlauben, ist eine Aktivierung dennoch möglich. Wenn Sie dies vorziehen, führen Sie die Schritte 8 bis 10 auf der nächsten Seite aus.

Gehen Sie zu Schritt 11 auf der nächsten Seite

2a Aktivierung der MFA Mobile App "PingID":

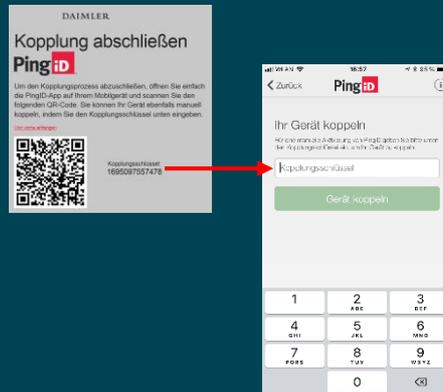
Aktivierung mit Desktop-basierten Anwendungen 3/3

Alternative Schritte 8 bis 10 ohne Kamera: Aktivierung durch Code statt QR-Scan
(Gehen Sie direkt zu Schritt 11, falls Sie die Schritte 5 bis 7 ausgeführt haben)

8. Wenn Sie keinen Zugriff auf Ihre Kamera gewähren und die PingID App lieber manuell aktivieren möchten, können Sie wie folgt vorgehen: Klicken Sie auf die Schaltfläche unterhalb des Kamerafensters (in der Abbildung gelb markiert): „Kopplungsschlüssel manuell eingeben“



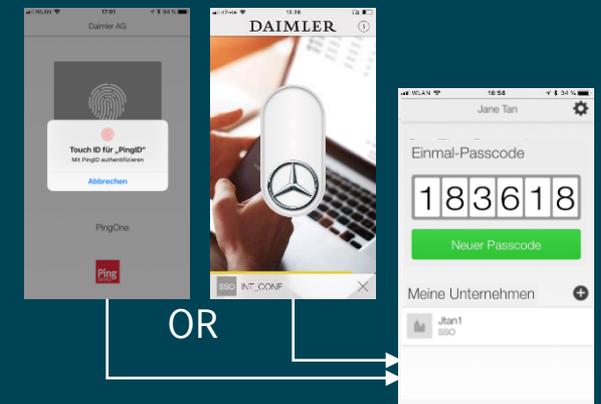
9. Bitte verwenden Sie den auf der Webseite angezeigten Kopplungsschlüssel (siehe auch Schritt 3.), der neben dem QR-Code angezeigt wird. Bitte geben Sie diesen Code in das leere Feld Ihres mobilen Geräts ein. Bestätigen Sie mit „Pair Device,,



10. Bei erfolgreicher Kopplung, werden Sie möglicherweise aufgefordert, den Zugriff auf Ihren Standort freizugeben. Dies kann abgelehnt werden. Danach müssen Sie einen Namen für Ihr App-Profil eingeben. Sie können einen beliebigen Namen verwenden. Ihre Daimler UserID wird als Möglichkeit empfohlen. Ein Foto ist nicht erforderlich.



11. Zum Abschluss der Kopplung verwenden Sie Ihren Fingerabdruck oder bewegen Sie das Icon nach oben. (je nach Verfügbarkeit eines Fingerabdrucksensors). Nach einer grünen Bestätigung schließen Sie den Bildschirm mit Klick auf das X. Die App zeigt dann wie rechts unten zu sehen einen Bildschirm mit einmaligem Passcode. Sie können die App jetzt ab sofort verwenden.



OR

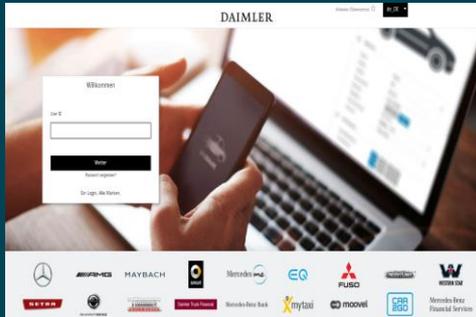


2b Aktivierung der MFA Mobile App "PingID": Aktivierung mit mobilen Applikationen 1/2

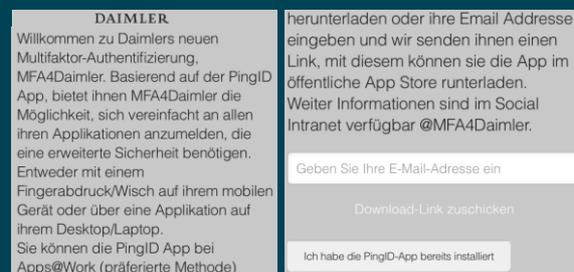
Die folgenden Schritte sind erforderlich, um die PingID-App während der Verwendung einer vertraulichen mobilen Daimler-Anwendung zu aktivieren.

1. Starten Sie die gewünschte vertrauliche mobile App.

Verwenden Sie Ihre corporate Benutzer-ID und Ihr Corporate Passwort und klicken Sie auf „Anmelden“.



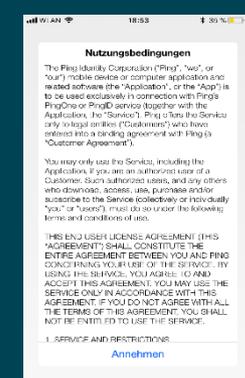
2. Nach einem erfolgreichen Login werden Sie zum MFA-Aktivierungsbildschirm weitergeleitet. Klicken Sie bitte auf „Ich habe die App bereits installiert!“ (mit rotem Pfeil markiert). Abhängig von Ihrem Gerät müssen Sie möglicherweise mit dem Text nach unten scrollen, um diese Option zu sehen.



3. Sie werden aufgefordert, die Kopplung Ihres Geräts fertigzustellen. Ein Kopplungsschlüssel wird am Ende des Bildschirms angezeigt. Notieren Sie sich diesen, da er für Schritt 6 erforderlich ist. Wenn Ihr Gerät ein Kopieren dieses Zahlencodes über den Touchscreen zulässt, können Sie dies auch tun.



4. Starten Sie die PingID-App auf dem mobilen Gerät. Beim ersten Aufruf der App wird die Meldung „Nutzungsbedingungen“ angezeigt. Bitte klicken Sie auf „Akzeptieren“, um fortzufahren.



2b Aktivierung der MFA Mobile App "PingID": Aktivierung mit mobilen Applikationen 2/2

Fortsetzung der mobilen Aktivierung:

5. Bei den Berechtigungen zum Ausführen von PingID (Kamera, Standort, Benachrichtigungen) akzeptieren Sie mindestens „Benachrichtigungen“. Unterhalb des Kamerafensters klicken Sie auf die Schaltfläche „Pairing Key manuell eingeben“ (unten gelb markiert):



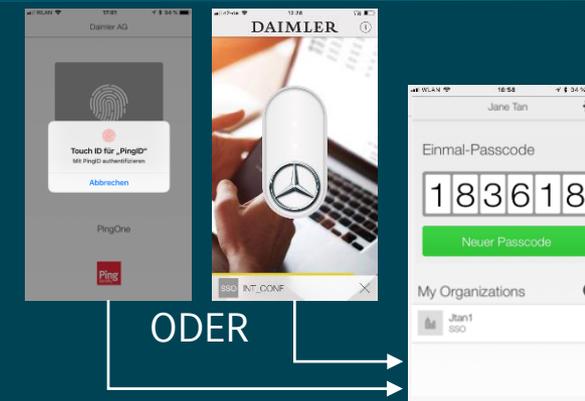
6. Bitte verwenden Sie den zuvor notierten oder kopierten Kopplungsschlüssel. (siehe auch Schritt 3.). Bitte geben Sie diesen oder fügen sie diesen Code in das leere Feld Ihres mobilen Geräts ein. Bestätigen Sie mit „Pair Device“.



7. Bei erfolgreicher Kopplung, werden Sie möglicherweise aufgefordert, den Zugriff auf Ihren Standort freizugeben. Dies kann abgelehnt werden. Danach müssen Sie einen Namen für Ihr App-Profil eingeben. Sie können einen beliebigen Namen verwenden. Ihre Daimler UserID wird als Möglichkeit empfohlen. Ein Foto ist nicht erforderlich.



8. Zum Abschluss der Kopplung verwenden Sie Ihren Fingerabdruck oder bewegen Sie das Icon nach oben. (je nach Verfügbarkeit eines Fingerabdrucksensors). Nach einer grünen Bestätigung schließen Sie den Bildschirm mit Klick auf das X. Die App zeigt dann wie rechts unten zu sehen einen Bildschirm mit einmaligem Passcode. Sie können die App jetzt ab sofort verwenden.



3a Arbeiten mit der MFA Mobile App „PingID“ 1/6

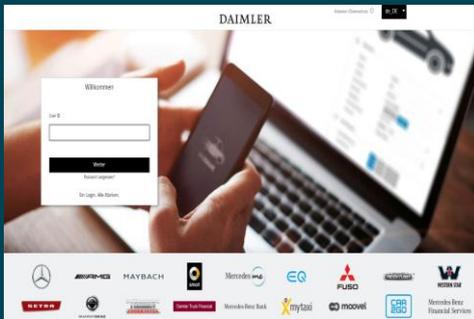
Standard Login mit einem aktivierten Mobilgerät

Dies ist die Standard-Anmeldung bei einer vertraulichen Anwendung. Alle weiteren Möglichkeiten finden Sie auf der nächsten Folie

1. Starten Sie Ihre Desktop- oder Webanwendung



Verwenden Sie Ihre Corporate Benutzer-ID und Ihr Corporate Passwort, um sich anzumelden:



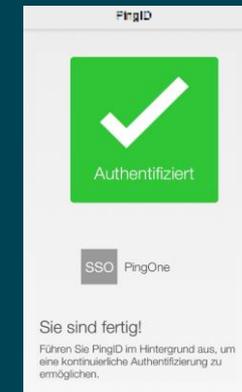
2. Nach erfolgreicher Anmeldung wird im Webbrowser eine Meldung angezeigt, dass PingID Ihr mobiles Gerät benachrichtigt.



3. Nach kurzer Zeit werden Sie von Ihrem gekoppelten Mobilgerät aufgefordert, die Anmeldung per Fingerabdruck bestätigen. Wenn Ihr Gerät keinen aktiven Fingerabdruckscanner hat, lesen Sie bitte weiter auf den nächsten Folien.



4. Nach erfolgreicher Bestätigung wird auf dem Desktop ein grünes Häkchen angezeigt. Sie werden jetzt automatisch in Ihre Anwendung weitergeleitet.



3b Arbeiten mit der MFA Mobile App „PingID“ 2/6

Anmeldeverfahren für iOS (vergleichen Sie auch Seite 18 für weitere Einstellungen)

Die PingID-App für iOS bietet verschiedene Optionen, um auf eine Anmeldung zu reagieren. Die Unterschiede sind abhängig vom aktuellen Status des Geräts: gesperrt, nicht gesperrt oder ob die PingID-App bereits im Vordergrund ausgeführt wird.

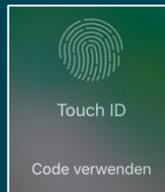
Wenn TouchID / Fingerprint bei Ihrem Gerät nicht aktiviert ist, muss der iOS-Entsperrcode verwendet werden.

1. Benachrichtigung bei gesperrtem iPhone: Kurz berühren.

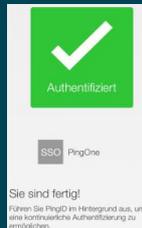
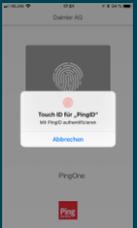
a) Berühren Sie die Nachricht kurz



b) Entsperren Sie mit Fingerabdruck oder Passcode um PingID zu starten



c) PingID öffnet sich: Bestätigen Sie mit dem Fingerabdruck*



* = Wenn Sie TouchID nicht aktiviert haben, erscheint an Stelle dessen der „Swipe“-Bildschirm (siehe rechts unter 4b)

2. Benachrichtigung bei gesperrtem iPhone: Lang berühren.

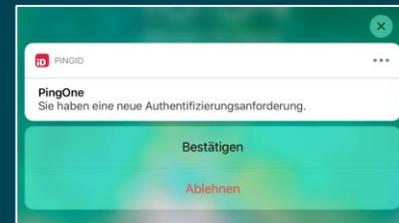
a) Berühren Sie die Nachricht lang



b) Bestätigen Sie die Anmeldung mit Fingerabdruck oder Passcode:

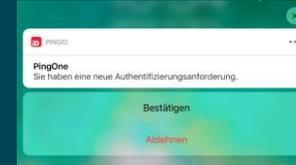


c) Wählen Sie aus, ob Sie die Anmeldung bestätigen oder nicht.



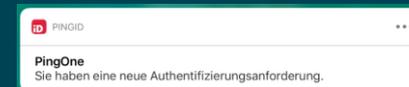
3. Benachrichtigung auf entsperrtem iPhone:

a) Berühren Sie die Benachrichtigung und ziehen Sie diese nach unten. Je nach Gerät können Sie auch „Force Touch“ verwenden (feste Berührung).

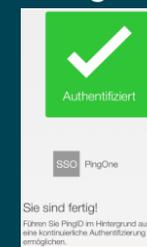


Bestätigen Sie die Anmeldung ODER

b) Sie berühren die Nachricht kurz



Dann öffnet sich die PingID App. Nutzen Sie Ihren Fingerabdruck.

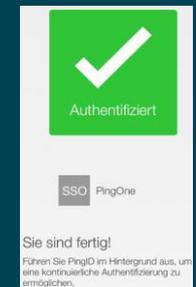


4. Benachrichtigung mit der PingID App im Vordergrund

a) Wenn Touch ID aktiv ist: Bestätigen mit Fingerabdruck:



b) Wenn das Gerät kein Touch ID hat oder dies nicht aktiv ist: Schieben Sie das Icon nach oben.

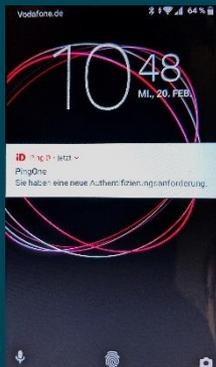


3b Arbeiten mit der MFA Mobile App „PingID“ 3/6

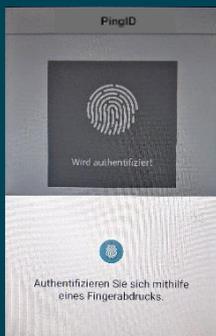
Anmeldeverfahren für Android (vergleichen Sie auch Seite 18 für weitere Einstellungen)

Die PingID-App für Android bietet verschiedene Optionen, um auf eine Anmeldung zu reagieren. Die Unterschiede sind abhängig vom aktuellen Status des Geräts: gesperrt, nicht gesperrt oder ob die PingID-App bereits im Vordergrund ausgeführt wird.

1. Benachrichtigung auf gesperrtem Android: - Berühren Sie die Benachrichtigung



a) Entsperren Sie Ihr Gerät mit Code oder Fingerabdruck



b) PingID öffnet sich. Bestätigen Sie die Anmeldung mit Ihrem Fingerabdruck oder schieben Sie das Icon nach oben, wenn Ihr Gerät keinen Fingerabdrucksensor hat.



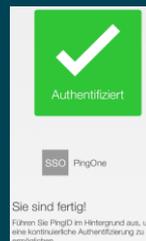
2. Benachrichtigung bei entsperrtem Android:

Bei entsperrten Android-Geräten wird bei jeder PingID-Benachrichtigung die PingID-App automatisch in den Vordergrund gebracht

a) PingID öffnet sich. Bestätigen Sie die Anmeldung mit Ihrem Fingerabdruck oder schieben Sie das Icon nach oben, wenn Ihr Gerät keinen Fingersensor hat.



b) Die PingID-App bestätigt die erfolgreiche Authentifizierung mit dem grünen Häkchen.



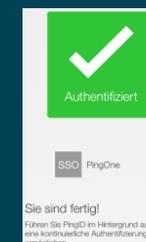
Sie sind fertig!
Führen Sie PingID im Hintergrund aus, um eine kontinuierliche Authentifizierung zu ermöglichen.

3. Benachrichtigung mit der PingID App im Vordergrund

a) Bestätigen Sie mit Ihrem Fingerabdruck oder indem Sie das Icon nach oben schieben (wenn Ihr Gerät keinen Fingerabdrucksensor hat).



b) Die PingID-App bestätigt die erfolgreiche Authentifizierung mit dem grünen Häkchen.



Sie sind fertig!
Führen Sie PingID im Hintergrund aus, um eine kontinuierliche Authentifizierung zu ermöglichen.

3b Arbeiten mit der MFA Mobile App „PingID“ 4/6 Einstellungen: Fingerprint, Swipe oder OTP

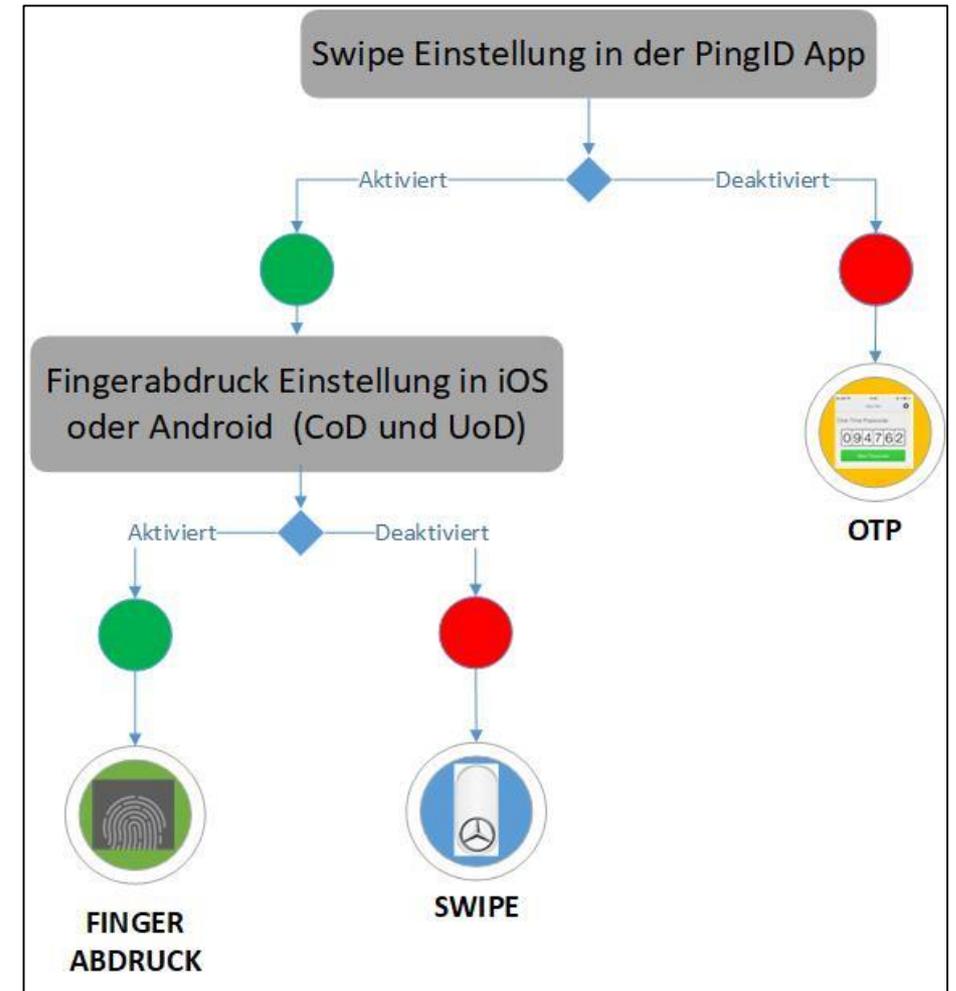
Zwei Einstellungen auf Ihrem Mobilgerät beeinflussen das Verhalten der PingID-App:

1. Ping-ID-App-Einstellung „Swipe“: Aktiviert oder deaktiviert.
2. Mobile Geräte-Einstellung „Fingerprint“: Aktiviert oder deaktiviert.

Abhängig von diesen Einstellungen fragt die PingID-App nach folgenden Authentifizierungstypen:

- Fingerabdruck
- Streichen / Swipe
- Einmalpasswort (OTP)

Wenn Sie beide Einstellungen aktiviert haben, verwenden Sie immer die Fingerabdruckauthentifizierung. (Empfehlung)
Für alle Optionen und Möglichkeiten schauen Sie sich bitte das Baumdiagramm auf der rechten Seite an.



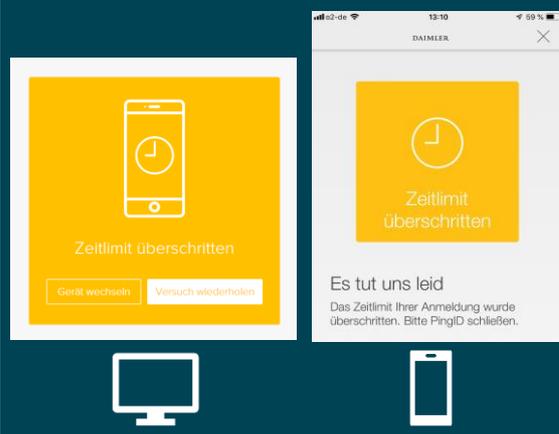
3c Arbeiten mit der MFA Mobile App „PingID“ 5/6 Hilfs-Optionen bei unterschiedlichen Problemen

Es gibt zwei mögliche Verfahren, wenn die Standardauthentifizierungsverfahren mit der Mobile App nicht sofort funktionieren:

1. Timeout der Anmeldung: Re-Authentifizierung

- Wenn Ihr Mobilgerät entsperrt ist, die PingID App im Vordergrund angezeigt wird und die Authentifizierung nicht innerhalb von 20 Sekunden bestätigt wird, wird im Webbrowser und kurz danach auch in der mobilen App eine gelbe Zeitüberschreitungs meldung angezeigt. Diese Nachricht enthält Schaltflächen zum Wiederholen der Authentifizierung (rechte Schaltfläche) oder zum Ändern des Authentifizierungsgeräts (linke Schaltfläche).
- Wenn das Gerät gesperrt ist oder von PingID nicht erreicht werden kann, wird nach ca. 30 Sekunden ein graues Feld zur Eingabe eines einmaligen Zugangscodes angezeigt. Fahren Sie in diesem Fall bitte mit Schritt 2 fort (siehe Beschreibung rechts).

Variante a)



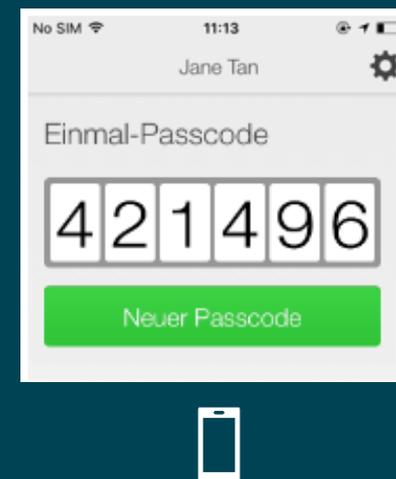
Nur bei Registrierung von mehr als einem MFA Gerät wird in den Dialogen die Möglichkeit des Gerätewechsels angezeigt.

Variante b)



2. Mobiles Gerät ist offline: Authentifizierung mit OTP

- Wenn Ihr Mobilgerät offline ist oder durch Verbindungsprobleme nicht von Push-Benachrichtigungen erreicht werden kann, kann die App für die Anzeige eines OTP-Codes (OTP = Einmalpasswort) manuell gestartet werden. Dieser Code wird dann für die Anmeldung genutzt. Starten sie die App mit dem roten ID Symbol und die App öffnet sich automatisch im OTP-Modus. 
- Geben Sie den angezeigten Nummerncode in das Feld auf der Webseite ein und bestätigen Sie mit "Anmelden".



3d Arbeiten mit der MFA Mobile App „PingID“ 6/6

Anmeldung mit verschiedenen MFA-Endgeräten

Achtung: dieses Anmeldeverfahren setzt voraus, dass sie bereits mehrere Endgeräte für sich aktiviert haben. s. hierzu Kapitel 4

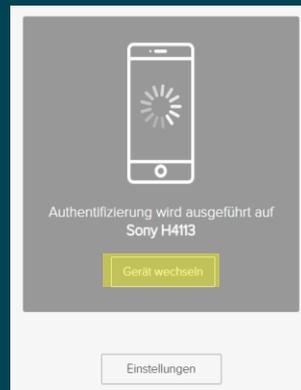
1. Starten Sie Ihre Desktop- oder Webanwendung.



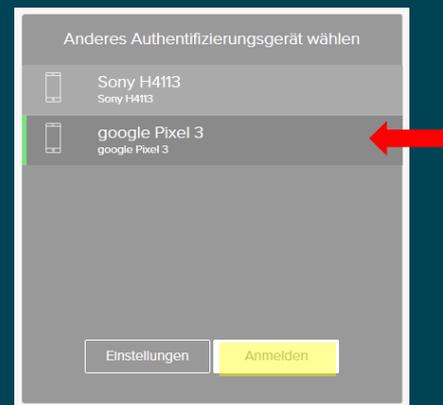
Verwenden Sie Ihre Corporate Benutzer-ID und Ihr Corporate Passwort, um sich anzumelden:



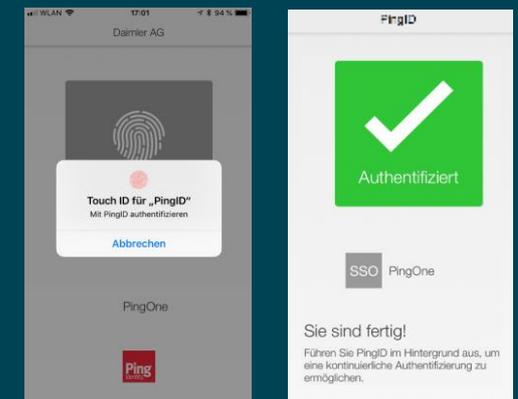
2. Wenn sie sich nicht mit ihrem primären Gerät anmelden wollen, können Sie, während die Authentifizierung schon läuft, zu einem anderen aktiven Gerät wechseln. Klicken Sie hierzu auf die Schaltfläche “Gerät wechseln”.



3. Es erscheint eine Übersicht mit Ihren registrierten MFA-Endgeräten. Klicken Sie auf das Gerät, mit dem Sie sich nun alternativ anmelden und welches dann zur Authentifizierung benachrichtigt werden soll. Bestätigen Sie ihre Auswahl mit “Anmelden”.



4. Der weitere Ablauf ist wie auf den vorstehenden Seiten beschrieben. Sie erhalten eine Benachrichtigung, nutzen den Fingerabdruck oder das Swipe Verfahren und sind dann erfolgreich mit Hilfe des alternativen Endgeräts authentifiziert.

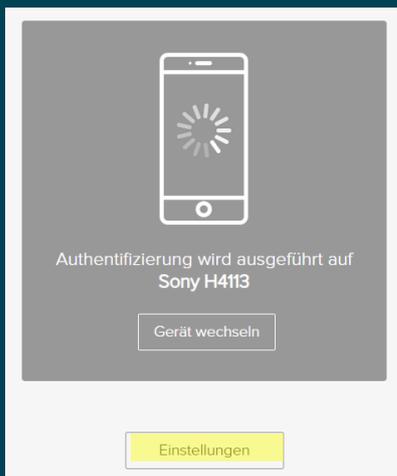


4a Self Service Prozesse mit MFA4Daimler

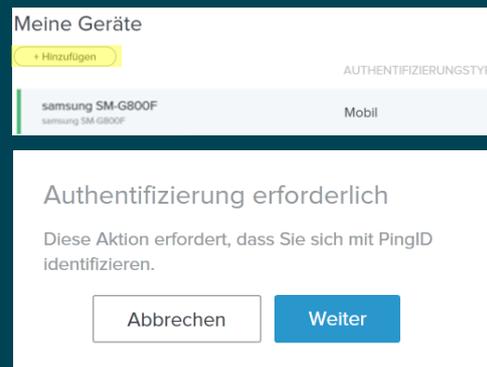
Ein weiteres Mobilgerät hinzufügen

Wenn Sie mit zwei Mobiltelefonen arbeiten, können Sie Ihrem MFA / PingID-Setup weitere Geräte hinzufügen:

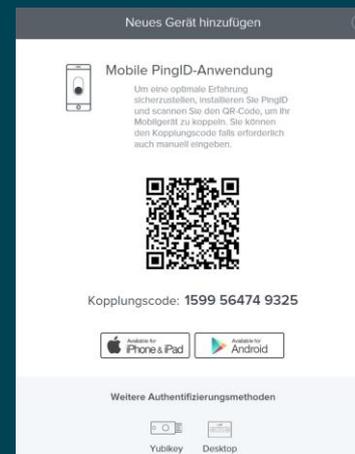
1. Melden Sie sich an einer vertraulichen Applikation an. Beim Erscheinen des PingID Dialogs bestätigen Sie jedoch nicht die Anmeldung auf ihrem aktiven Mobilgerät. Klicken Sie unten auf "Einstellungen", um zu Ihrer persönlichen PingID-Geräte-konfiguration zu gelangen.



2. Auf dem Bildschirm „Meine Geräte“ sehen Sie nun Ihr aktuell registriertes Mobiltelefon. Klicken Sie auf „Hinzufügen“, um den Registrierungsvorgang für ein neues Gerät zu starten. Bitte klicken Sie auf „Weiter“ und authentifizieren Sie sich mit Ihrem bereits aktiven Gerät.



3. Der Dialog "Neues Gerät hinzufügen" wird angezeigt. Fahren Sie nun mit der Registrierung Ihres zweiten Mobilgeräts fort, so wie auf den mit „2b“ bezeichneten Folien mit dem Titel: "Aktivieren der Ping ID Mobile App"



4. Danach sehen Sie Ihr neues Gerät in der Liste "Meine Geräte". Sie können sich abmelden oder einfach den Browser schließen, um den Vorgang zu beenden.

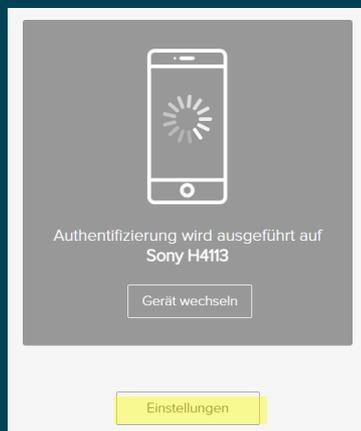


4b Self Service Prozesse mit MFA4Daimler

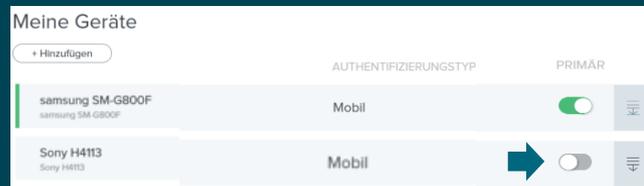
Ändern des primären Authentifizierungsgerätes

Wenn Sie mit zwei Mobiltelefonen arbeiten, können Sie das primäre Gerät auswählen, welches standardmäßig benachrichtigt werden soll:

1. Melden Sie sich an einer vertraulichen Applikation an. Beim Erscheinen des PingID Dialogs bestätigen Sie jedoch nicht die Anmeldung auf Ihrem aktiven Mobilgerät. Klicken Sie unten auf "Einstellungen", um zu Ihrer persönlichen PingID-Gerätekonfiguration zu gelangen.



2. Auf dem Bildschirm „Meine Geräte“ können Sie Ihre registrierten Geräte sehen, wobei Ihr aktuelles primäres Gerät grün angezeigt wird (Schaltfläche rechts). Wenn Sie Ihr primäres Gerät ändern möchten, bewegen Sie den Schalter für das andere Gerät nach rechts. Bitte klicken Sie auf "Weiter" und authentifizieren Sie sich mit dem noch aktuell primären Gerät.



Authentifizierung erforderlich

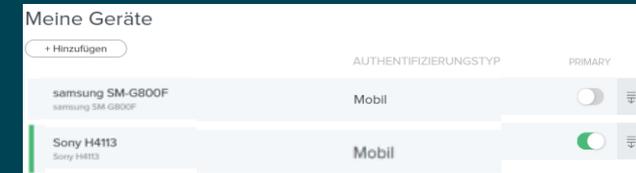
Diese Aktion erfordert, dass Sie sich mit PingID identifizieren.

Abbrechen

Weiter



3. Das Primärgerät sollte sich jetzt geändert haben, was durch den grünen aktiven Schalter angezeigt wird. Bei einer Standardauthentifizierung wird dieses Gerät benachrichtigt. (siehe Seite 15).
4. Sie können sich abmelden oder einfach den Browser schließen, um den Vorgang zu beenden.

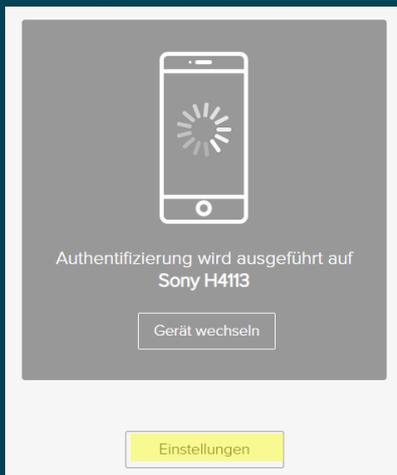


4c Self Service Prozesse mit MFA4Daimler

Löschen eines mobilen Geräts aus PingID

Wenn Sie ein Gerät aus PingID entfernen möchten, können Sie den folgenden Prozess verwenden:

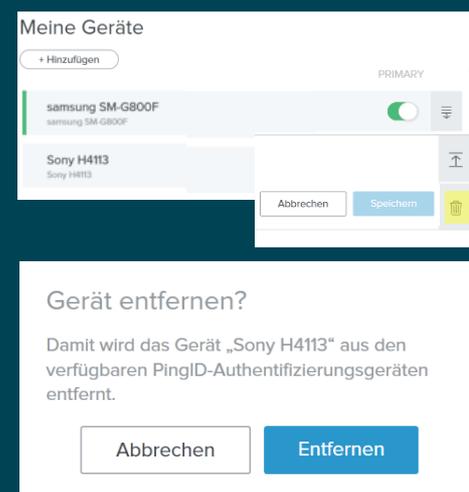
1. Melden Sie sich an einer vertraulichen Applikation an. Beim Erscheinen des PingID-Dialogs bestätigen Sie jedoch nicht die Anmeldung auf Ihrem aktiven Mobilgerät. Klicken Sie unten auf "Einstellungen", um zu Ihrer persönlichen PingID-Gerätekonfiguration zu gelangen.



2. Klicken Sie im Bildschirm „Meine Geräte“ am Ende der Zeile des Geräts, das Sie entfernen möchten. Authentifizieren Sie sich mit dem primären Gerät, wenn Sie dazu aufgefordert werden.



3. Klicken Sie auf das nun erscheinende Papierkorb-Symbol. Sie werden aufgefordert zu bestätigen, dass das Gerät aus Ping-ID entfernt wird.



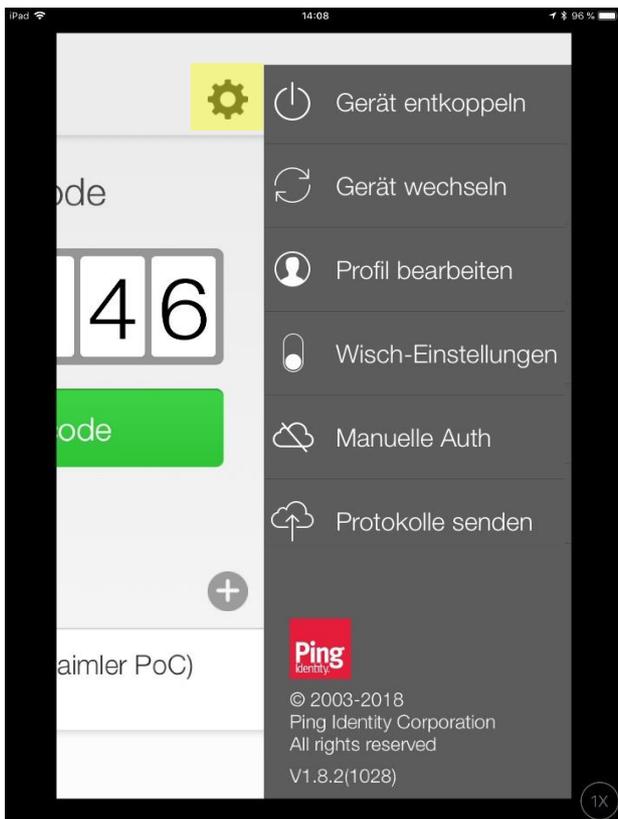
4. Nachdem Sie das Gerät entfernt haben, werden Ihre verbleibenden Geräte in der Übersicht "Meine Geräte" angezeigt. Sie können sich jetzt abmelden oder einfach den Browser schließen.



5a Self Service Prozesse in der MFA/PingID App 1/2

Das Optionen Menü

Die PingID-App für iOS / iPhone oder Android bietet verschiedene Optionen für Self-Services. Wenn Sie auf das Einstellungssymbol klicken (s. gelbe Markierung) öffnet sich ein Menü. Die Optionen werden nachfolgend erläutert.



Für das „Entkoppeln“= Deaktivieren dieses Geräts für PingID.
Sie können sich danach nicht mehr mit diesem Gerät authentifizieren (!)

Zur Übertragung der Authentifizierung auf ein neues Mobilgerät.
Führt zur Deaktivierung dieses Geräts (siehe Details hierzu auf der nächsten Seite)

Zum Bearbeiten Ihres Namens und zum Hinzufügen eines Fotos. Dies ist nur zur Anzeige innerhalb der App.

Zum Deaktivieren der Swipe- und Fingerprint-Funktion, z. B. wenn Sie eine langsame Internetverbindung nutzen oder wenn Sie nur OTP-Passcodes verwenden möchten. *

Zur App-Synchronisierung: Sehr selten werden Sie aufgefordert, sich manuell zu authentifizieren. Bitte klicken Sie hier, um dies mittels eines QR Codes oder eines Zahlencodes durchzuführen. Die Anmeldeseite wird ihnen mitteilen, ob diese Option genutzt werden muss.

Ausschließlich für Analysen. Verwenden Sie diese Option nur, wenn der Helpdesk darum bittet.

*= Sie können nicht die grundsätzliche Verwendung von „Swipe“ anstelle von „Fingerabdruck“ konfigurieren, wenn Ihr Gerät über einen aktiven Fingerabdruckscanner verfügt.
Sie können nur konfigurieren, dass Swipe und Fingerprint gemeinsam vollständig deaktiviert werden!

5b Self Service Prozesse in der MFA/PingID App 2/2

Migrieren der PingID Anmeldung zu einem neuen Mobilgerät

Um selber eine vollständige Migration der App von einem alten auf ein neues Gerät durchzuführen müssen beide Geräte gleichzeitig für Sie nutzbar sein. Wenn Ihr altes Gerät nicht für die Migration verfügbar ist, Sie jedoch ein neues Gerät registrieren müssen, wenden Sie sich an einen Ihrer zuständigen Administratoren (OrgAdmin/MarktAdmin), um Ihr Konto in GEMS für Sie zurückzusetzen.

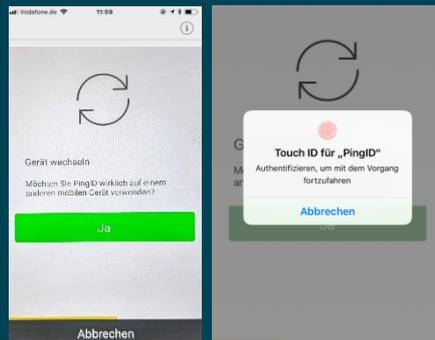
1. Starten Sie die PingID-App auf dem alten Mobilgerät.



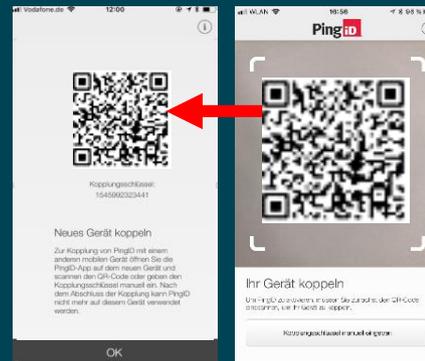
Klicken Sie auf das Einstellungssymbol oben rechts, um das Menü zu öffnen, und klicken Sie auf „Gerät wechseln“.



2. Das „alte“ Gerät fordert zur Bestätigung auf, wenn Sie die Authentifizierung auf ein anderes Gerät migrieren möchten. Bitte bestätigen Sie mit „Ja“ (linkes Bild). Sie werden aufgefordert dies mit Ihrem Fingerabdruck oder dem Entsperrcode Ihres Geräts zu bestätigen.



3. Bitte installieren Sie die PingID-App auf dem "neuen" Mobilgerät wie auf Folie 1a. Starten Sie die App und gewähren Sie Zugriff auf die Kamera. Scannen Sie den QR-Code des alten Geräts mit der Kamera des neuen Geräts oder geben Sie den Kopplungsschlüssel ein.



Altes Gerät

Neues Gerät



4. Bei erfolgreichem Pairing wird auf dem neuen Gerät eine grüne Bestätigungsmeldung angezeigt. Sie können jetzt die migrierte App verwenden.



Wenn das Pairing mit der Kamera fehlschlägt, klicken Sie auf „Kopplungsschlüssel manuell eingeben“ und geben Sie diesen ein. Er wird in Schritt 3 auf dem alten Gerät angezeigt.



Symbole:



Altes Gerät



Neues Gerät

6

Service Prozess mit MFA4Daimler – Account zurücksetzen

Anmerkung: Wenn Sie ein neues mobiles Gerät aktivieren oder migrieren wollen und Ihr altes Gerät steht aber noch zur Verfügung, nutzen Sie bitte den Self Service Migrations Process auf der vorherigen Seite. In diesem Fall ist ein Reset durch einen Administrator in GEMS nicht nötig.

Wenn Ihr MFA4Daimler Zugriff durch Ereignisse wie Verlust, Defekt oder eine Neuinstallation nicht mehr möglich ist, muss einer Ihrer Administratoren (OrgAdmin/MarktAdmin) Ihren Account in GEMS für Sie zurücksetzen. Er ist auch dann notwendig, wenn Sie Ihre MFA4Daimler neu aktivieren wollen, aber über kein aktives MFA Gerät verfügen.

7 Zusätzlicher Support

Bei zusätzlichen Fragen zum MFA4Daimler Service, wenden Sie sich bitte an den MFA4Daimler Application Helpdesk (Aktuell verfügbare Sprachen sind deutsch und englisch):

Tel/Fax: +49 (711) 17-25005

Mail: cuhd_support_mfa4daimler@daimler.com

DAIMLER

Versionsinformationen

Version	Datum	Änderungen
1.0	2021-02-17	Erste veröffentlichte Version des Handbuchs MFA Mobile für Dealer/Supplier Community in DE