Please find the English version below

iCust System - Aktivierung der Multi Faktor Authentifizierung MFA4 (PingID)

Alle iCust Nutzer müssen die Multi Faktor Authentifizierung (PingID) aktiviert haben

*** Wichtig – Ihre Aktion ist erforderlich ***

Um was geht es?

- PingID ist ein erweiterter Authentifizierung-Prozess, der verbindlich seitens Daimler für vertrauliche und integritäts kritische Applikationen vorgeschrieben ist.
- Das Einloggen in einer Applikation erfordert dadurch einen sogenannten “Zweiten Faktor” der über die cloud-basierte Lösung PingID abgefragt wird. Dies geschieht mittels der kostenloses Smartphone/Desktop App oder einem FIDO zertifizierten USB Stick.

Wer ist betroffen?

- Alle iCust User.

Was müssen Sie einrichten?

- Alle iCust Anwender müssen Ihren Account für die Nutzung mit PingID einrichten.

  Die MFA4Daimler Management Seite https://login.daimler.com/password/mfa-settings können Sie bereits jetzt verwenden um Ihren Logon einzurichten und zu testen.
  Ebenso lassen sich dort zusätzliche MFA-Devices als Backup hinterlegen. Sie müssen nichts unternehmen, wenn Sie PingID bereits nutzen, müssen Sie diese nicht noch einmal einrichten.

- Sie haben folgende Möglichkeiten: Installieren der Mobile PingID Smartphone App, die Desktop App oder einen FIDO-zertifizierten USB stick, wie z.B. Yubikey. Unter folgendem Link finden Sie den PingID Guide:

  https://www.pingidentity.com/de/resources/downloads/pingid.html

Bei Fragen bezüglich der Aktivierung der Multi Faktor Authentifizierung MFA (PingID) wenden Sie sich bitte an den MFA4Daimler Application Helpdesk:
Email: cuhd_support_mfa4daimler@daimler.com
Telefon: +49 (0) 711 17 25 00 5

Servicezeiten: Montag bis Freitag 06:00-22:00 Uhr
(kein Support an bundeseinheitlichen Feiertagen)

iCust System - Activation of Multi Factor Authentication MFA4 (PingID)

All iCust users must have Multi Factor Authentication (PingID) enabled

*** Important – your action is required ***

What's it about?

- PingID is the additional authentication process which is mandatory for confidential and integrity critical applications within Daimler.
- A logon will then require a second factor via the cloud-based solution PingID using the cost free smartphone/desktop app or a FIDO compliant USB stick.

Who's affected?

- All iCust users.

What's to do?

- All internal and external iCust users must set up and test their account for use with PingID:

  The MFA4Daimler management web page https://login.daimler.com/password/mfa-settings could be used for setup/logon even before.
  You can also configure other MFA-devices as backup there. There is no ToDo on your end, in case you are already using PingID for another Daimler application (e.g. CISM).

- users need to install the mobile PingID smartphone app, the desktop app or a FIDO-compatible USB stick, such as Yubikey, to enable their Daimler account for MFA4Daimler.
  See the attached MFA Supplier Guide:

  https://www.pingidentity.com/de/resources/downloads/pingid.html

For questions regarding the activation of the Multi Factor Authentication MFA4 (PingID), please contact the MFA4Daimler Application Helpdesk:
Email: cuhd_support_mfa4daimler@daimler.com
Phone: +49 (0) 711 17 25 00 5

service times: Monday to Friday 6:00am-10:00pm
(no support on national holidays)