MFA4Daimler - Handbuch für die Nutzung mit externen Authenticator Apps (Dealer/Supplier Community)

Inhaltsverzeichnis

1. Über dieses Dokument

In diesem Dokument wird die Einrichtung und Arbeit mit dem Multi-Faktor Authentifizierungsdienst "MFA4Daimler" in Kombination mit externen Authenticator Apps beschrieben.

Multi-Faktor-Authentifizierung (MFA) kombiniert mehrere Berechtigungsnachweise für mehr Sicherheit bei der Anmeldung von Benutzern an Applikationen.
Ziel dieser mehrstufigen Authentifizierung ist es, die Zugangsberechtigung des Benutzers bei der Anmeldung mit höherer Sicherheit verifizieren zu können und damit das Risiko von Accountübernahmen sowie unauthorisierten Zugriffen auf sensible Informationen zu minimieren.

Bei MFA wird bei der Anmeldung die Zugangsberechtigung durch mindestens zwei unabhängige Merkmale (Faktoren) überprüft.

Diese Faktoren können in folgende Kategorien eingeteilt werden:

- physische Besitzobjekte wie z.B. ein Hardware-Token
- geheimes Wissen wie z.B. ein Passwort oder eine PIN
- eindeutige physische Merkmale oder biometrische Daten wie z.B. der Fingerabdruck

MFA4Daimler unterstützt hierzu folgende Methoden für die Authentifizierung:

In diesem Guide beschrieben:

- Nutzung einer externen Authenticator App (z.B. Microsoft Authenticator, Google Authenticator, ...) mit einem Mobilgerät
- Nutzung einer externen Authenticator App (z.B. WinAuth) mit einem Desktop Gerät

Weitere Methoden:

- Nutzung der "PingID" App mit einem Mobilgerät (iOS/Android)
    - Für mehr Informationen siehe Handbuch "MFA4Daimler_Dealer_Supplier_UserGuide_Mobile"
- Nutzung eines kompatiblen FIDO2 Hardware-Sicherheitsschlüssel mit einem Mobil- oder Desktop Gerät
    - Für mehr Informationen siehe Handbuch "MFA4Daimler_UsersQuickGuide_HardwareSecKey"

Im Folgenden wird die Nutzung der Methode "externe Authenticator App" zur Anmeldung mit MFA4Daimler beispielhaft beschrieben.

2. Allgemeine Hinweise

Um eine Authenticator App mit MFA4Daimler verwenden zu können, muss die Authenticator-App zunächst mit dem MFA4Daimler Konto gekoppelt werden. Durch das Koppeln eines Geräts wird eine Vertrauensstellung zwischen Gerät und Konto hergestellt.

Das Einrichten einer Authenticator App zur Authentifizierung mit MFA4Daimler umfasst die folgenden Schritte:

- Download und Installation der gewünschten Authenticator App auf dem Gerät (z.B. Smartphone oder Desktop Gerät).
- Koppeln des Gerätes.

Nach erfolgreicher Einrichtung kann die Authenticator App zur Authentifizierung mit MFA4Daimler geschützten Anwendungen verwendet werden.

Koppeln Sie mehr als ein Gerät

Es wird empfohlen, wenn möglich mehr als ein Gerät mit MFA4Daimler zu koppeln. Damit wird gewährleistet, dass eine alternative Authentifizierungsmethode verfügbar ist, sollte Ihr primäres Gerät nicht verfügbar sein. Für weitere Informationen hierzu siehe Geräte verwalten.

Trennung von erstem und zweitem Faktor

Es wird empfohlen den ersten Faktor (z.B. UserID & Passwort) nach Möglichkeit vom zweiten Faktor (z.B. MFA4Daimler - Authenticator App) zu separieren, um ein Höchstmaß an Sicherheit zu gewährleisten.

Beispiel:
Bei der Authentifizierung an einer Anwendung mit einem Laptop wird empfohlen als zweiten Faktor eine mobile Authenticator App (z.B. Microsoft Authenticator) auf einem Mobilgerät zu verwenden.

3. Anwendungsfälle

Allgemein können alle Authenticator Apps mit MFA4Daimler verwendet werden, welche ein Standard Einmalkennwort (TOTP gemäß RFC6238) generieren können.
Dies bedeutet, dass die meisten allgemein bekannten Authenticator Apps unterstützt werden.

Im folgenden werden einige Beispiele für allgemein bekannte Authenticator Apps aufgelistet:

- iOS Geräte
  - Microsoft Authenticator
  - Google Authenticator
  - Authy
- Android Geräte
  - Microsoft Authenticator
  - Google Authenticator
  - Authy
- Desktop Geräte
  - WinAuth

In den folgenden Kapiteln werden diverse Anwendungsfälle beispielhaft beschrieben:

- Nutzung mit einem iOS Mobilgerät am Beispiel "Microsoft Authenticator"
- Nutzung mit einem Android Mobilgerät am Beispiel "Microsoft Authenticator"
- Nutzung mit einem Windows Desktop Gerät am Beispiel "WinAuth"

3.1. Nutzung mit einem Mobilgerät

In diesem Kapitel wird die Verwendung von MFA4Daimler mit einem mobilen Gerät am Beispiel der "Microsoft Authenticator" App beschrieben.

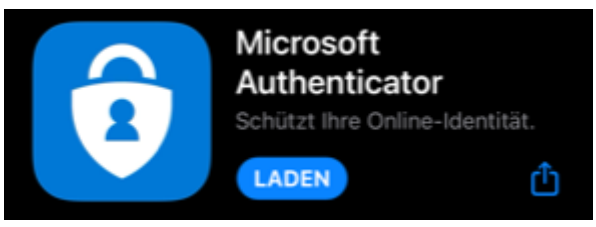
3.1.1. iOS Geräte

Installation

Installieren Sie die "Microsoft Authenticator" App auf ihrem iOS Gerät:

1. Starten Sie den App Store auf ihrem Gerät.

2. Suchen Sie nach der App "Microsoft Authenticator".



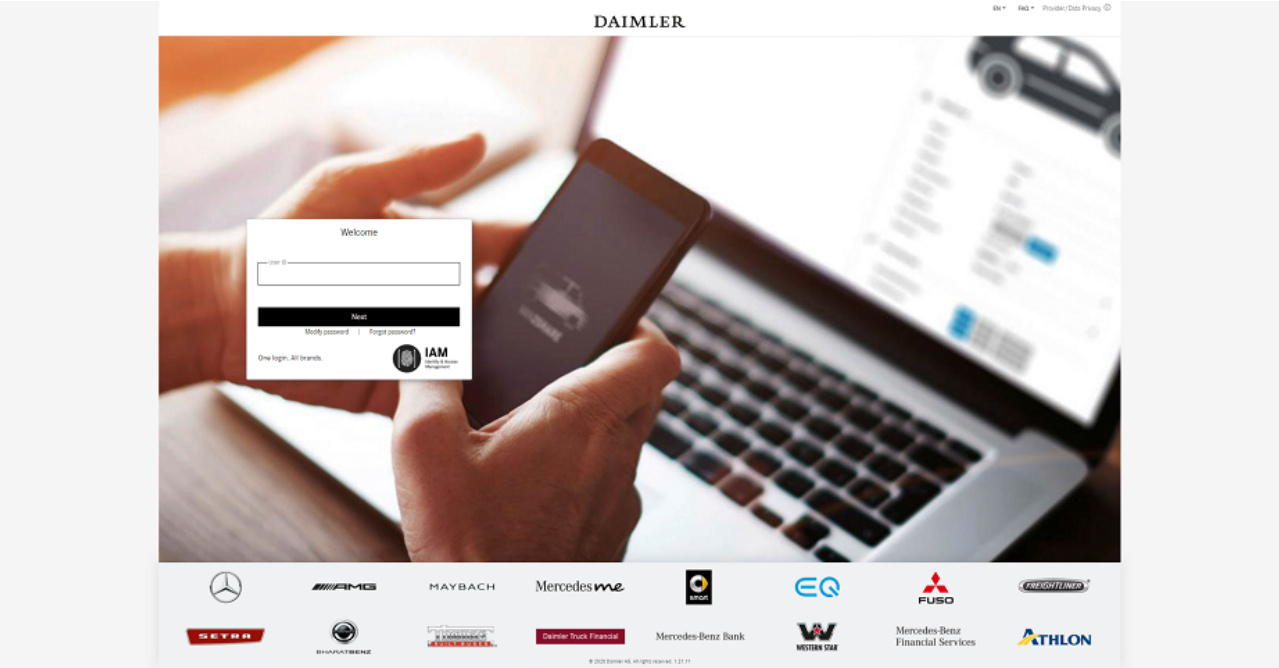
3. Installieren Sie die App auf Ihrem Gerät. Zusätzliche Informationen hierzu finden Sie hier.

Initiale Kopplung

Nachdem die "Microsoft Authenticator" App auf dem Gerät installiert wurde, wird die initiale Kopplung durchgeführt indem eine mit MFA4Daimler geschützte Anwendung aufgerufen wird.

1. Rufen Sie eine mit MFA4Daimler geschützte Applikation auf.

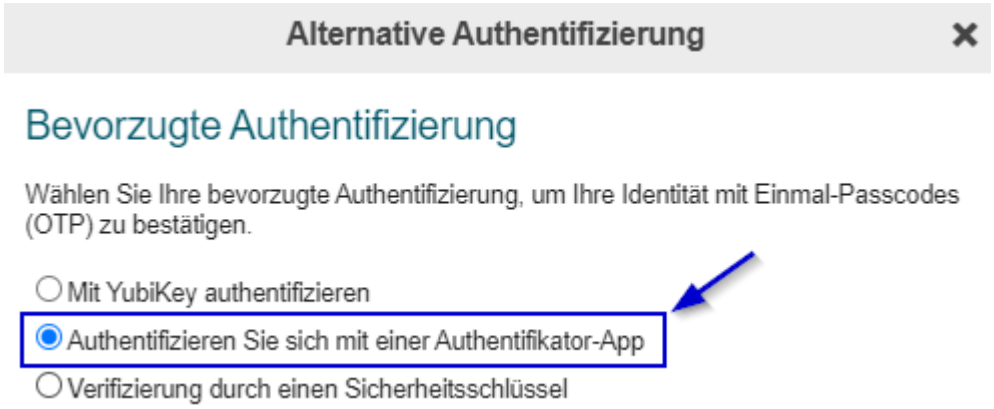
2. Melden Sie sich am Corporate Weblogin mit Ihrer UserID und Passwort an.



3. Nach erfolgreicher Anmeldung werden Sie durch den initialen Kopplungsprozess mit MFA4Daimler geführt.

   Für die Kopplung einer Authenticator App, wählen Sie den Link "Ich möchte eine alternative Authentifizierungsmethode verwenden".

4. Wählen Sie nun die Option "Authentifizieren Sie sich mit einer Authenticator-App".



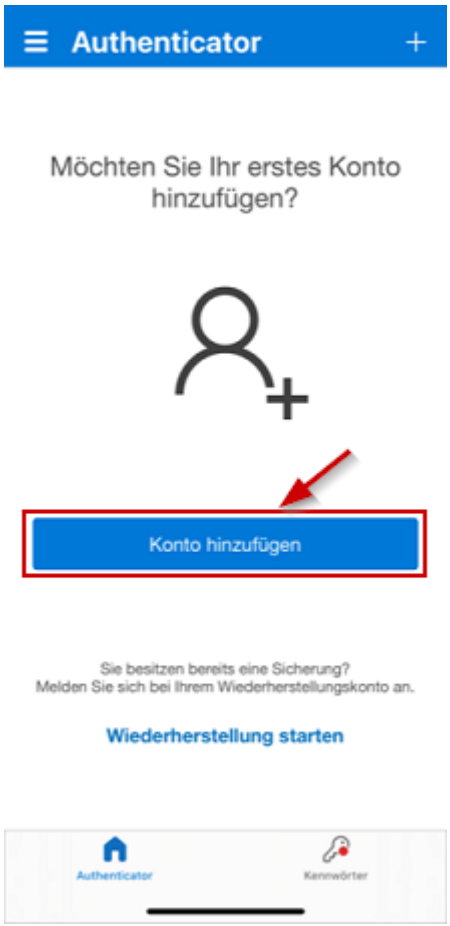
5. Kopplung Durchführen.

   Es wird nun ein QR Code für die Kopplung ihres Accounts mit einer Authenticator App angezeigt.
   Die Kopplung der "Microsoft Authenticator" App kann entweder durch das Scannen des angezeigten QR Codes mit ihrem Smartphone oder durch die manuelle Eingabe des Codes erfolgen.

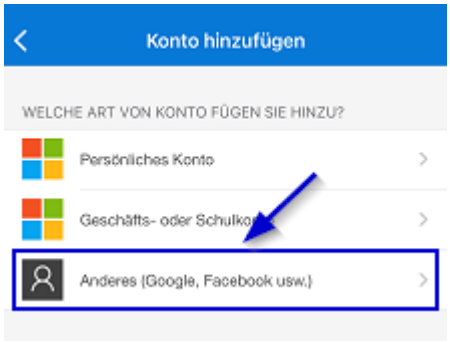
   Starten Sie die "Microsoft Authenticator" App um mit der Kopplung zu beginnen.
   Für Informationen zur manuellen Kopplung siehe "5.2".

5.1 QR Code scannen (Hierfür benötigt die "Microsoft Authenticator" App Kamerazugriff)

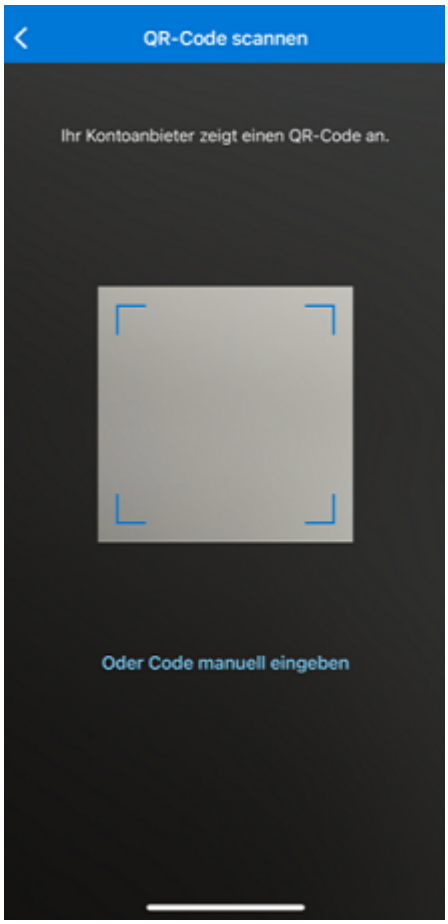
a) In der "Microsoft Authenticator" App wählen Sie "Konto hinzufügen".



b) Wählen Sie nun für die Art von Konto "Anderes (Google, Facebook usw.)".

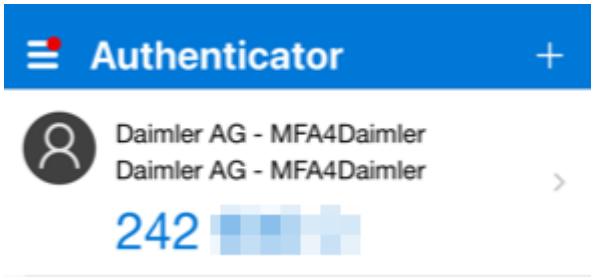


c) Die "Microsoft Authenticator" App erwartet nun, dass ein QR Code gescannt wird.



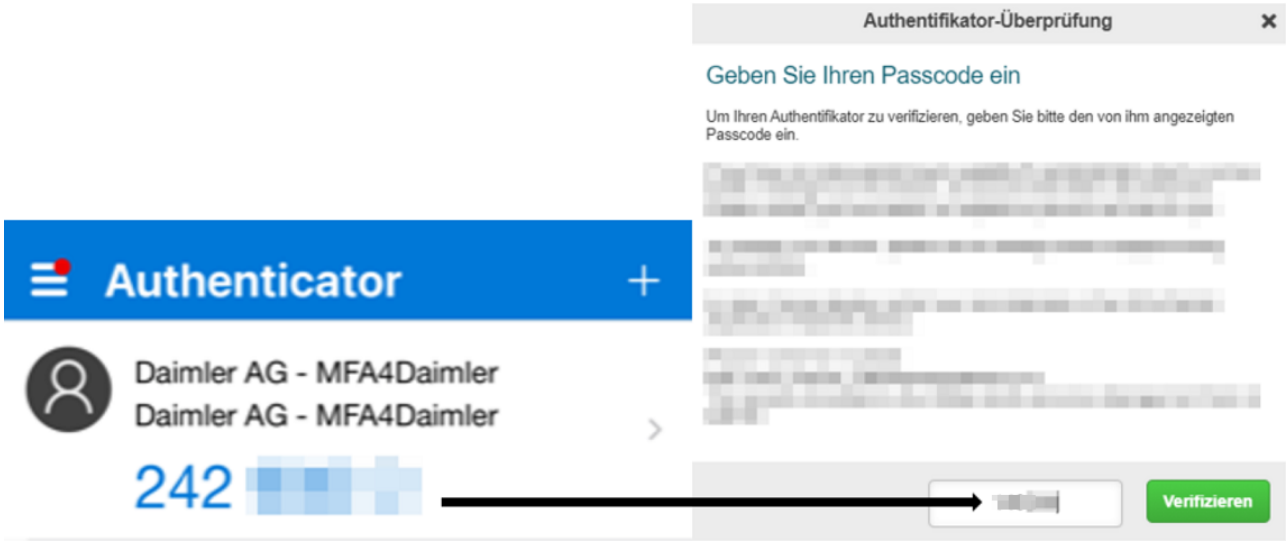
d) Scannen Sie den im Browser angezeigten QR Code mit ihrem Mobilgerät.

e) Es wird nun ein neuer Eintrag (in diesem Beispiel "Daimler AG - MFA4Daimler") in der "Microsoft Authenticator" App angezeigt.

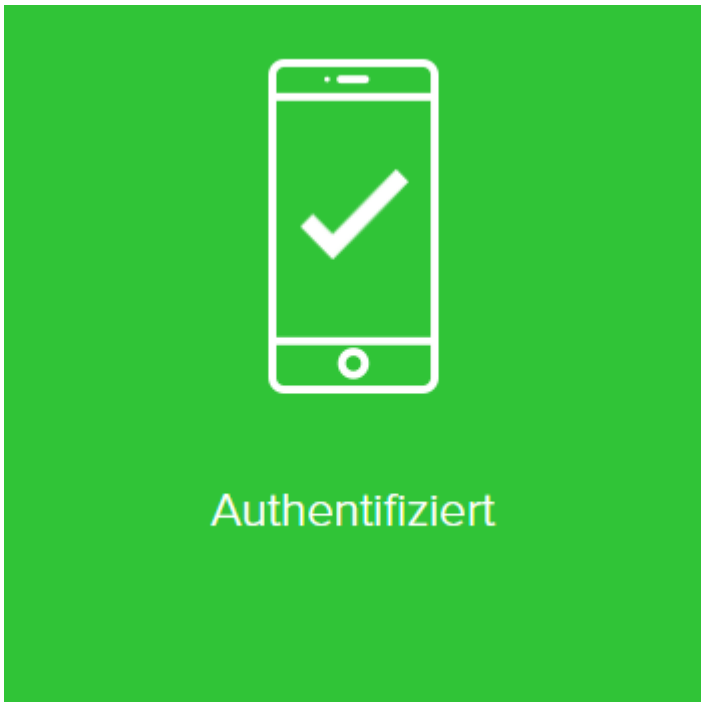


f) Wählen Sie nun im Browser "Weiter".

g) Geben Sie das in der "Microsoft Authenticator" App angezeigte Einmalkennwort im Eingabefeld des Browsers ein und wählen Sie "Verifizieren".

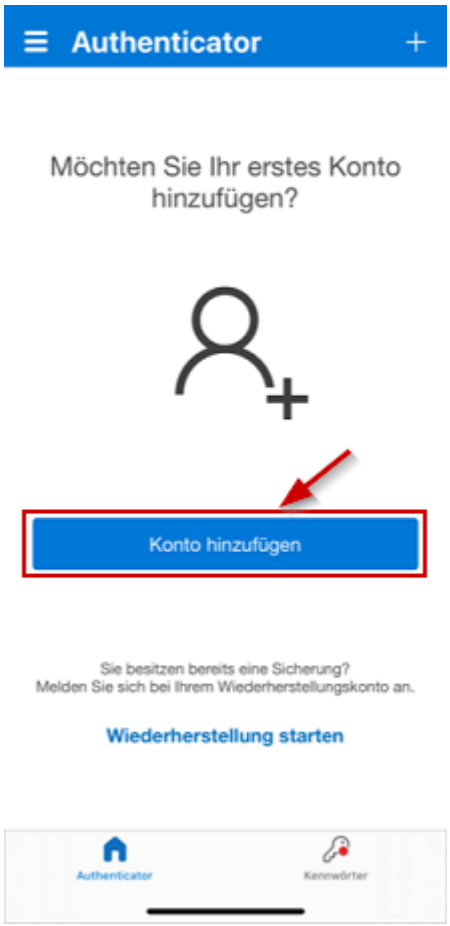


h) Die Kopplung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Sie können sich nun zukünftig mithilfe ihrer "Microsoft Authenticator" App mit MFA4Daimler anmelden.

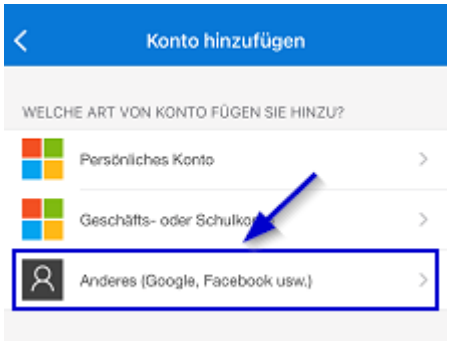


5.2 Manuelle Kopplung

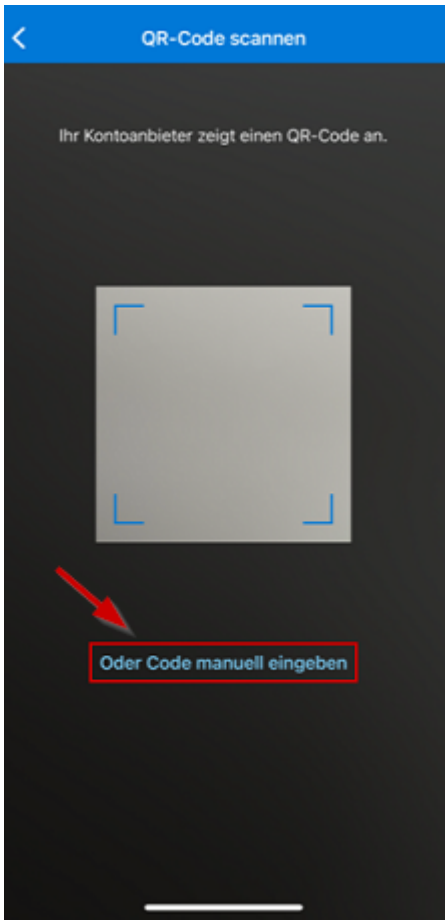
a) In der "Microsoft Authenticator" App, wählen Sie "Konto hinzufügen".



b) Wählen Sie nun für die Art von Konto "Anderes (Google, Facebook usw.)".

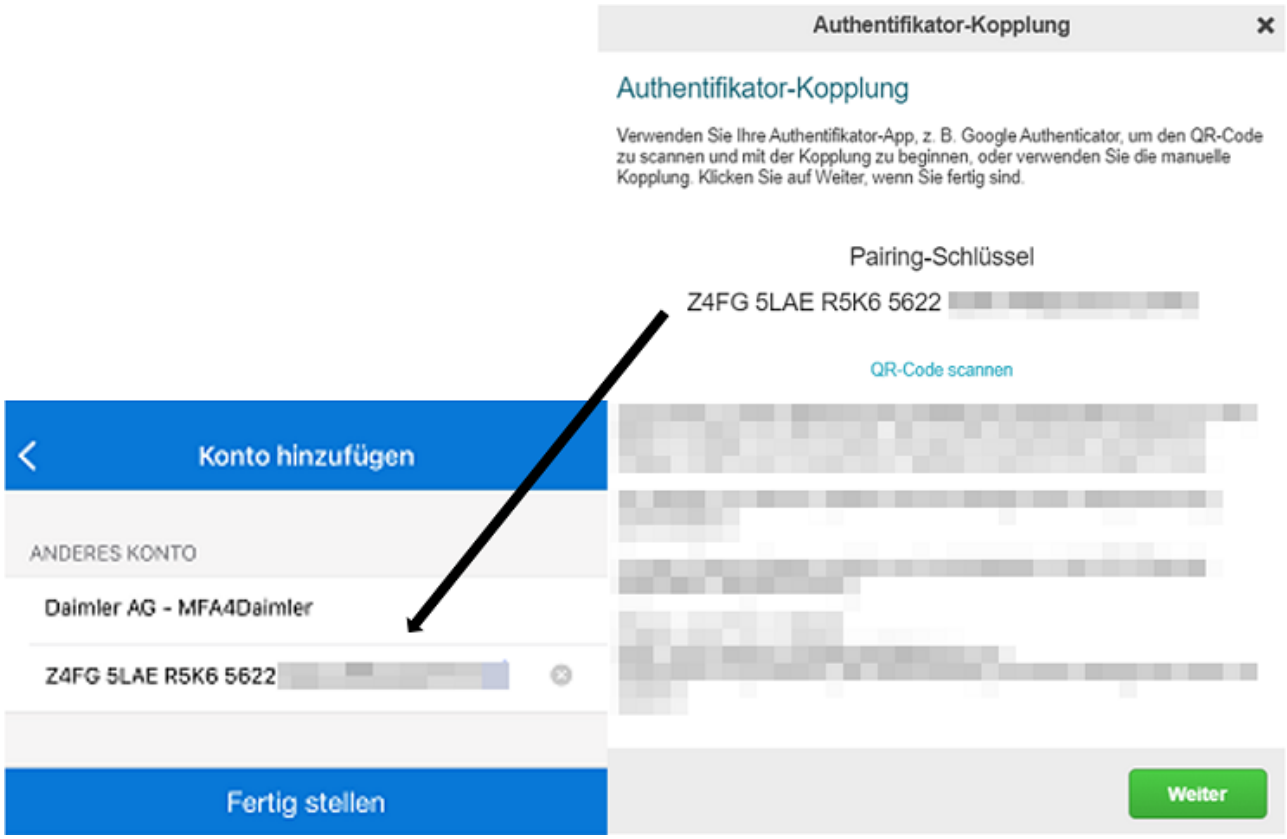


c) Die "Microsoft Authenticator" App erwartet nun, dass ein QR Code gescannt wird. Wählen Sie "Oder Code manuell eingeben" um den Pairing-Schlüssel manuell einzugeben.

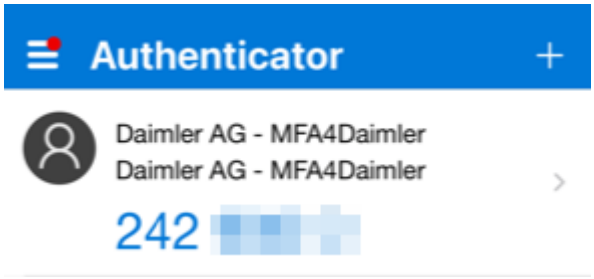


d) Wählen Sie bei MFA4Daimler "Manuelle Kopplung" um den manuellen Pairing-Schlüssel anzuzeigen.

e) Geben Sie in der "Microsoft Authenticator" App einen Kontonamen ein (z.B. "MFA4Daimler" und geben Sie den im Browser angezeigten Pairing-Schlüssel ein. Wählen Sie anschließend "Fertig stellen".

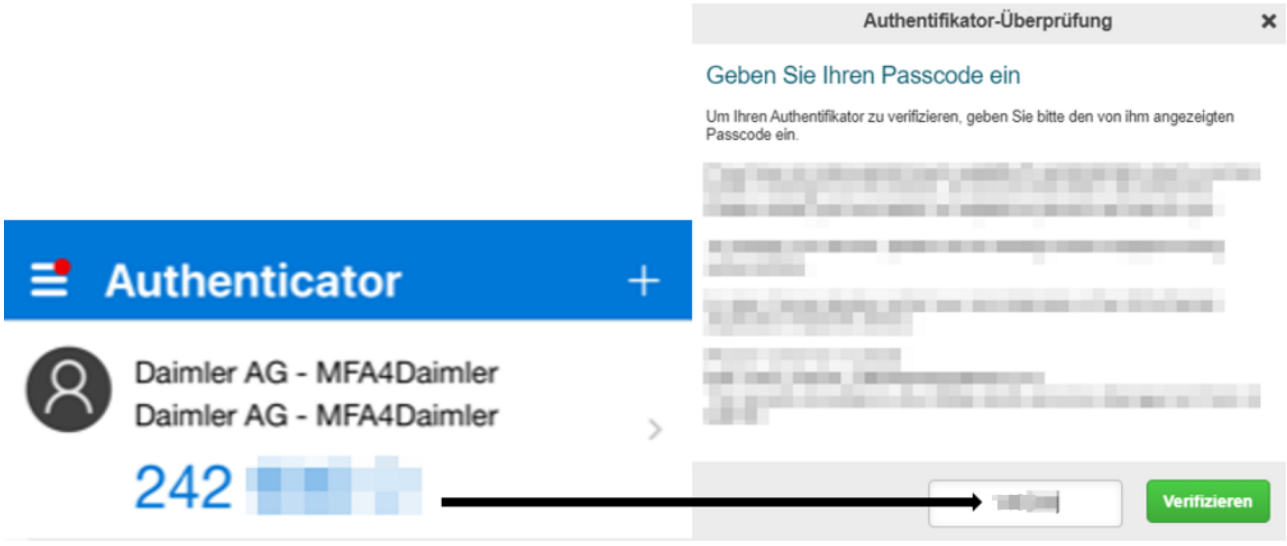


f) Es wird ein neuer Eintrag (in diesem Beispiel "Daimler AG - MFA4Daimler") in der "Microsoft Authenticator" App angezeigt.

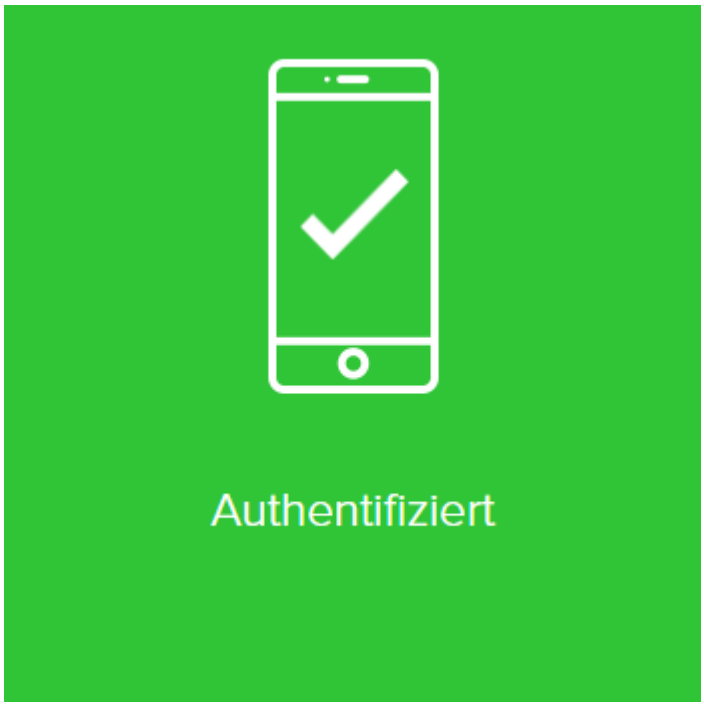


g) Wählen Sie nun im Browser "Weiter".

h) Geben Sie das in der "Microsoft Authenticator" App angezeigte Einmalkennwort im Eingabefeld des Browsers ein und wählen Sie "Verifizieren".



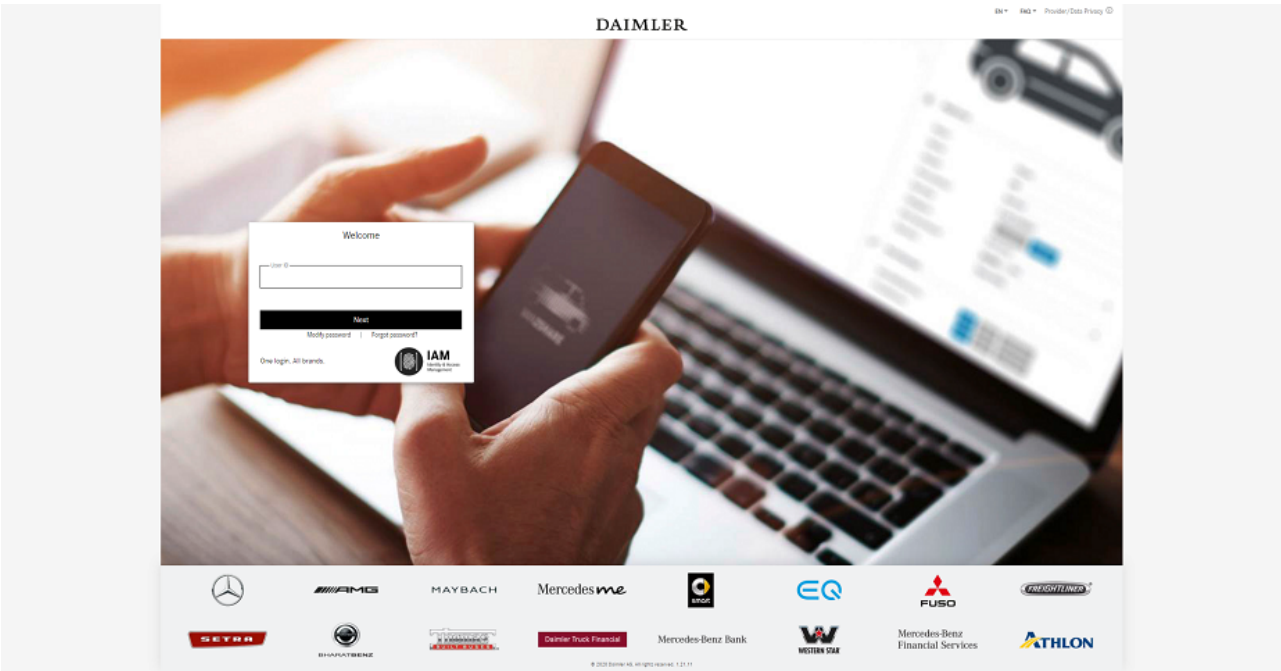
i) Die Kopplung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Sie können sich nun zukünftig mithilfe ihrer "Microsoft Authenticator" App mit MFA4Daimler anmelden.



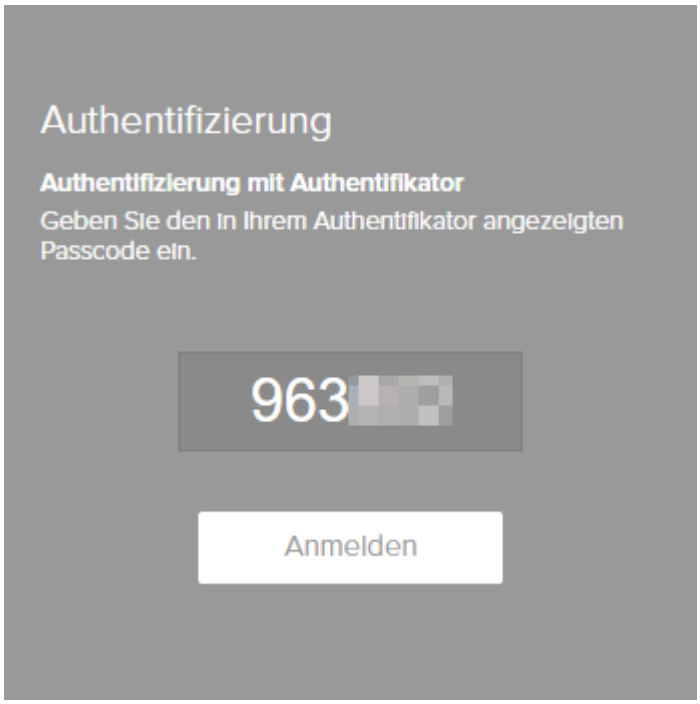
Authentifizierung

Nachdem Sie die "Microsoft Authenticator" App erfolgreich mit Ihrem Account gekoppelt haben, können Sie diese bei zukünftigen Authentifizierungen mit MFA4Daimler verwenden.

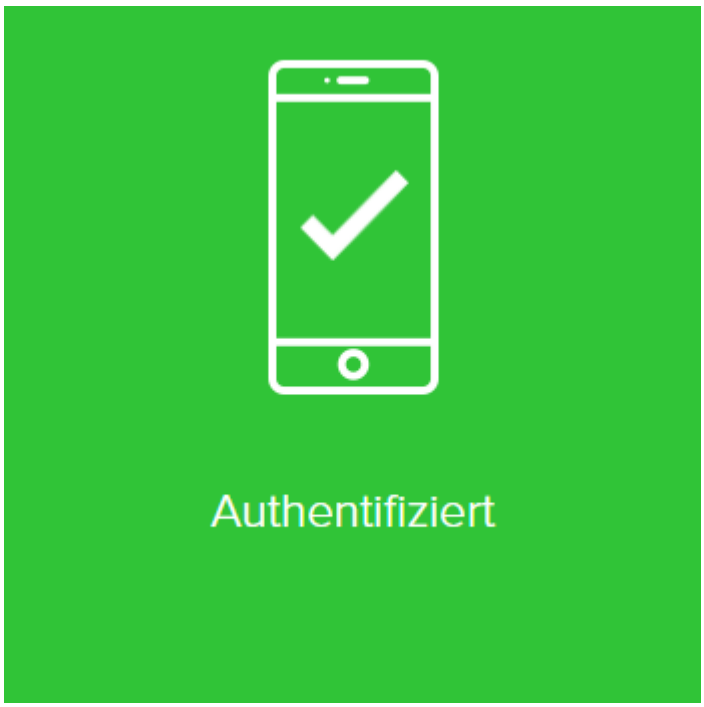
1. Rufen Sie eine mit MFA4Daimler geschützte Applikation auf.
2. Melden Sie sich am Corporate Weblogin mit Ihrer UserID und Passwort an.



3. Nach erfolgreicher Anmeldung werden Sie aufgefordert sich mit einer mit MFA4Daimler gekoppelten Methode zu authentifizieren. Öffnen Sie die "Microsoft Authenticator" App.
4. Geben Sie das in der "Microsoft Authenticator" App angezeigte Einmalkennwort in das Eingabefeld bei MFA4Daimler ein und wählen Sie "Anmelden".



5. Die Anmeldung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Anschließend werden Sie automatisch in die Applikation weitergeleitet.

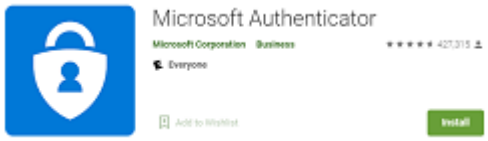


3.1.2. Android Geräte

Installation

Installieren Sie die "Microsoft Authenticator" App auf ihrem Android Gerät:

1. Starten Sie den App Store auf ihrem Gerät.
2. Suchen Sie nach der App "Microsoft Authenticator".

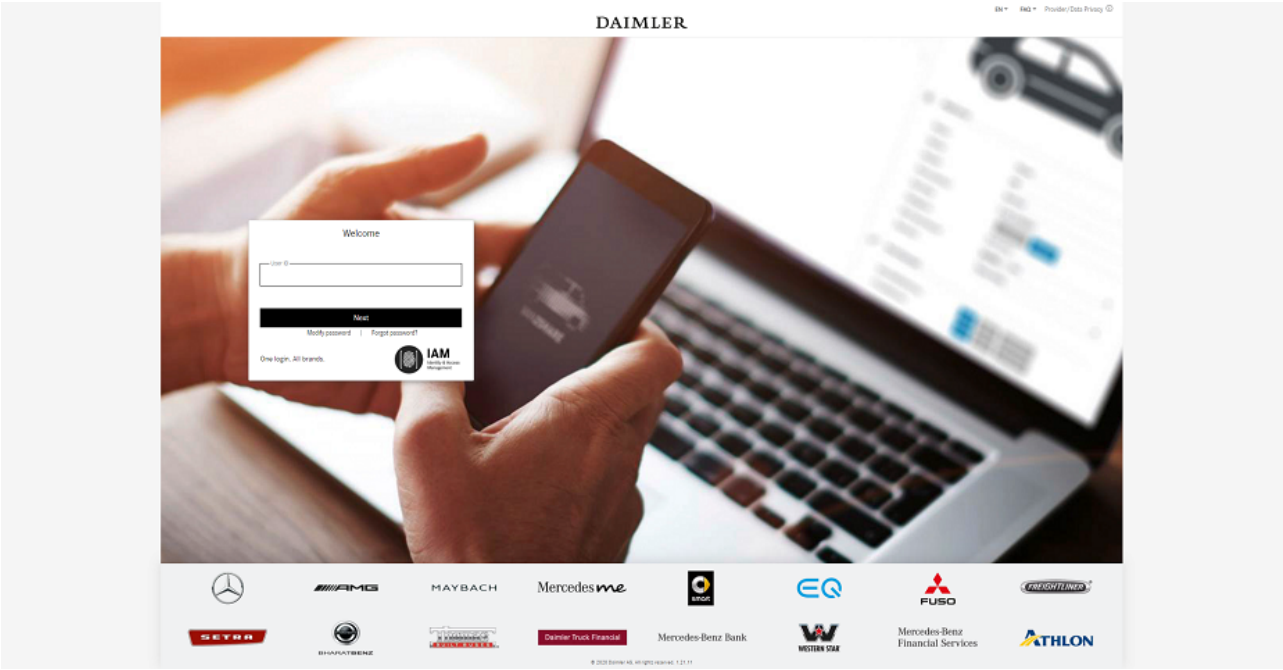


3. Installieren Sie die App auf Ihrem Gerät. Zusätzliche Informationen finden Sie hier.

Initiale Kopplung

Nachdem die "Microsoft Authenticator" App auf dem Gerät installiert wurde, wird die initiale Kopplung durchgeführt indem eine mit MFA4Daimler geschützte Anwendung aufgerufen wird.

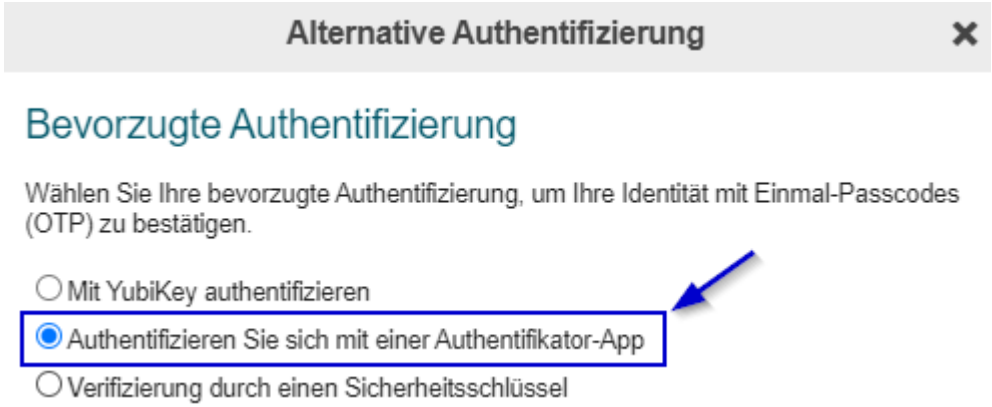
1. Rufen Sie eine mit MFA4Daimler geschützte Applikation auf.
2. Melden Sie sich am Corporate Weblogin mit Ihrer UserID und Passwort an.



3. Nach erfolgreicher Anmeldung werden Sie durch den initialen Kopplungsprozess mit MFA4Daimler geführt.

Für die Kopplung einer Authenticator App, wählen Sie den Link "Ich möchte eine alternative Authentifizierungsmethode verwenden".

4. Wählen Sie nun die Option "Authentifizieren Sie sich mit einer Authentifikator-App".



5. Kopplung Durchführen.

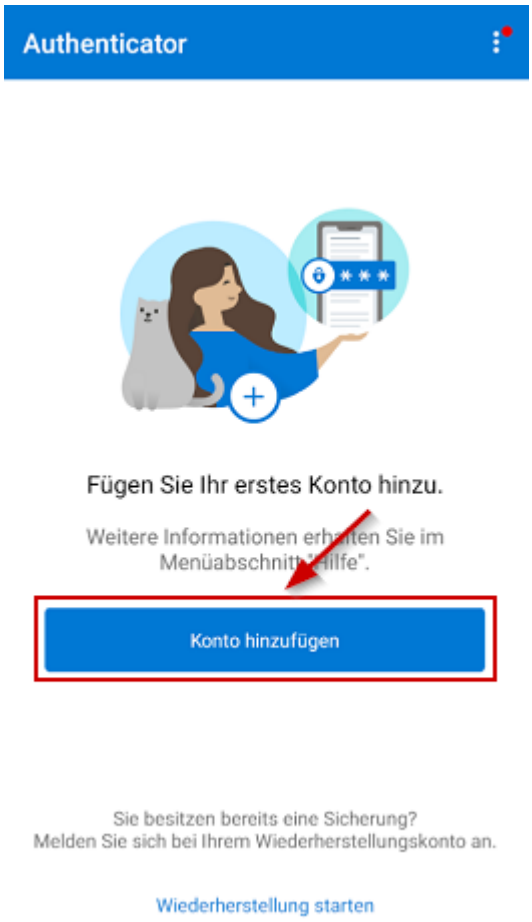
   Es wird nun ein QR Code für die Kopplung ihres Accounts mit einer Authenticator App angezeigt.

   Die Kopplung der "Microsoft Authenticator" App kann entweder durch das Scannen des angezeigten QR Codes mit ihrem Smartphone oder durch manuelle Eingabe des Codes erfolgen.

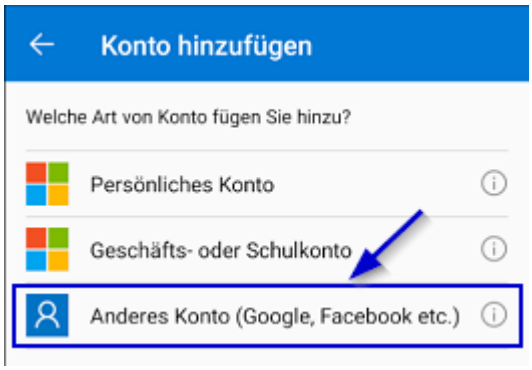
   Starten Sie die "Microsoft Authenticator" App um mit der Kopplung zu beginnen.

   5.1 QR Code scannen (Hierfür benötigt die "Microsoft Authenticator" App Kamerazugriff)

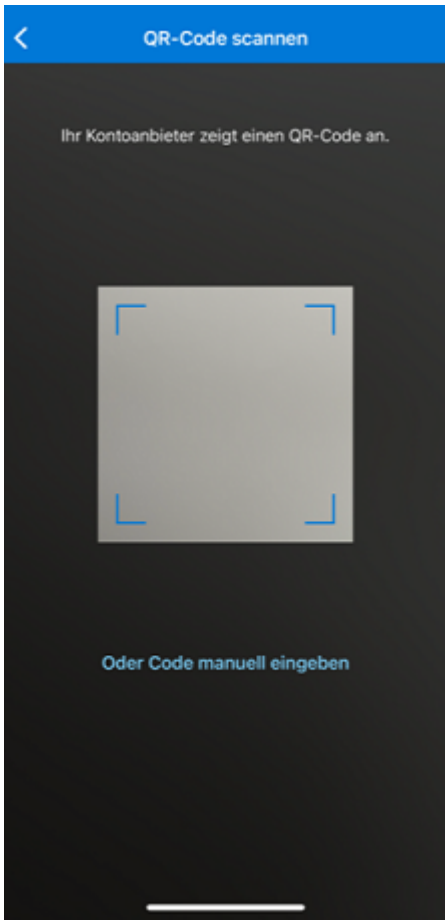
a) In der "Microsoft Authenticator" App, wählen Sie "Konto hinzufügen".



b) Wählen Sie nun für die Art von Konto "Anderes (Google, Facebook usw.)".

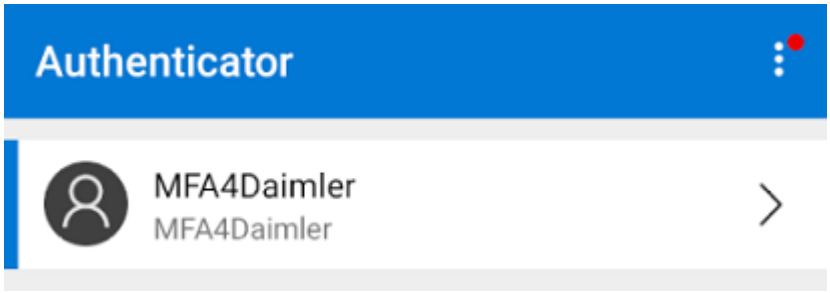


c) Die "Microsoft Authenticator" App erwartet nun, dass ein QR Code gescannt wird.



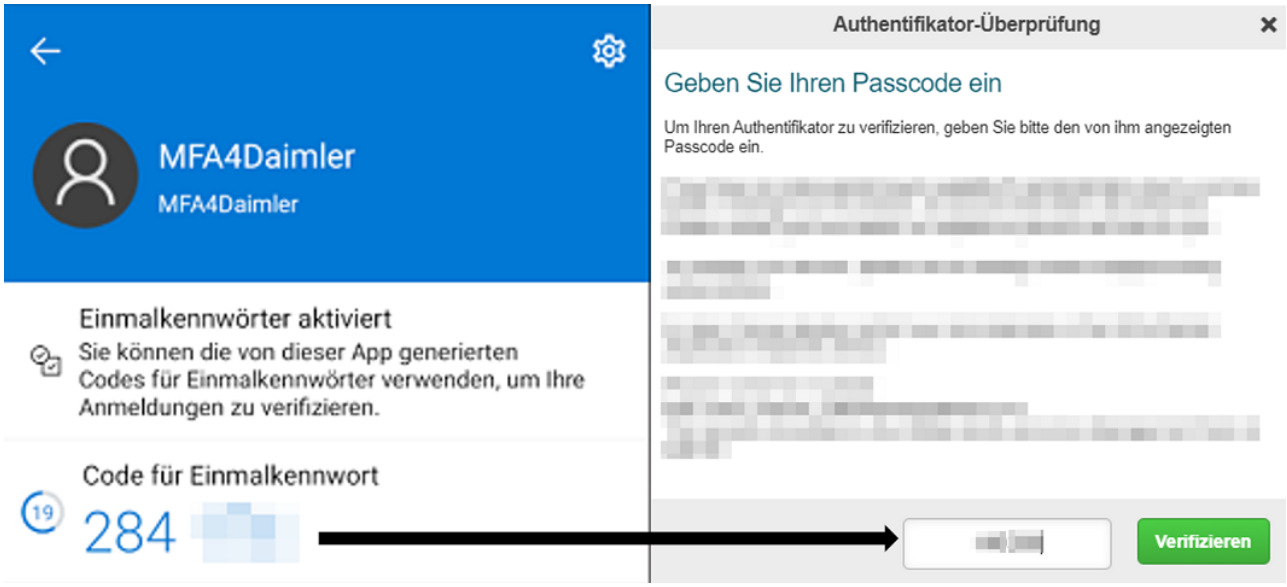
d) Scannen Sie den im Browser angezeigten QR Code mit ihrem Mobilgerät.

e) Es wird ein neuer Eintrag (in diesem Beispiel "MFA4Daimler") in der "Microsoft Authenticator" App angezeigt.

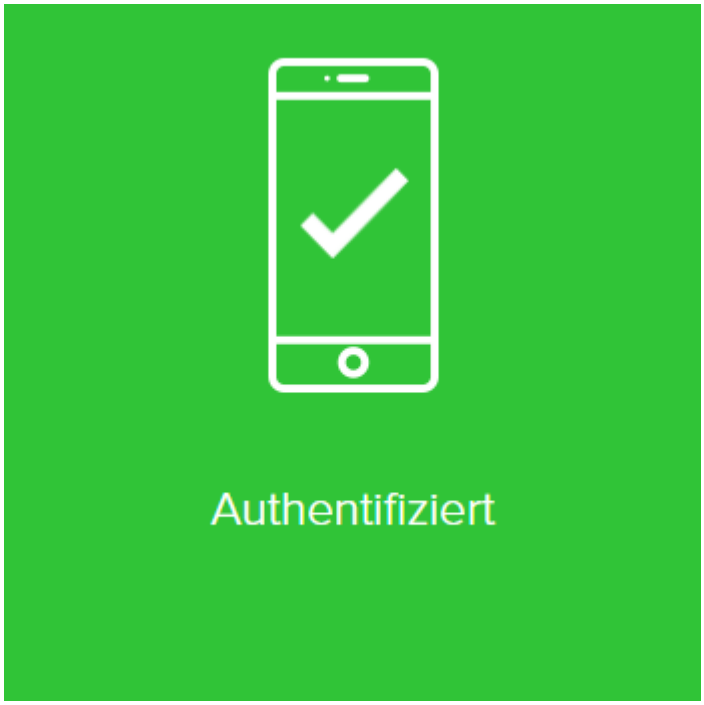


f) Wählen Sie nun bei MFA4Daimler auf "Weiter".

g) Geben Sie das in der "Microsoft Authenticator" App angezeigte Einmalkennwort im Eingabefeld des Browsers ein und wählen Sie "Verifizieren".

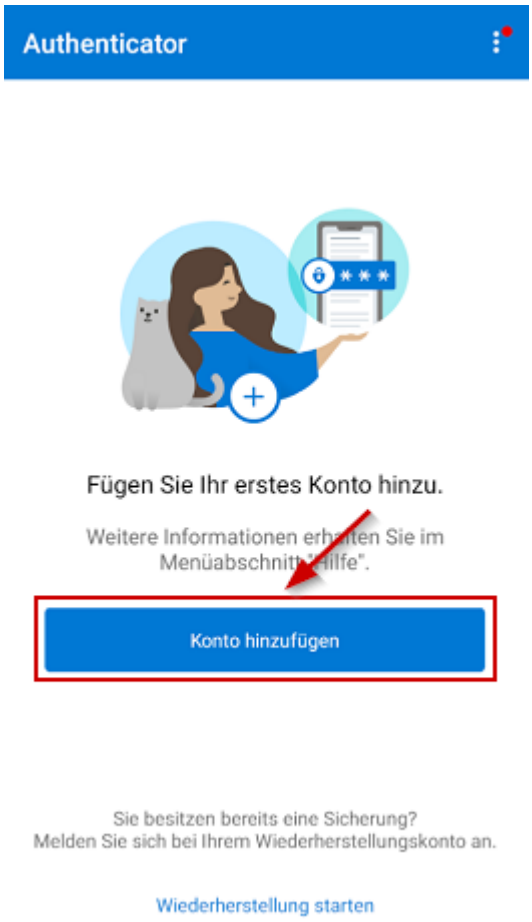


h) Die Kopplung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Sie können sich nun zukünftig mithilfe ihrer "Microsoft Authenticator" App mit MFA4Daimler anmelden.

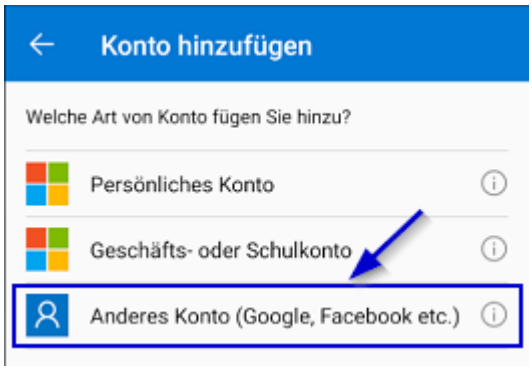


5.2 Manuelle Kopplung

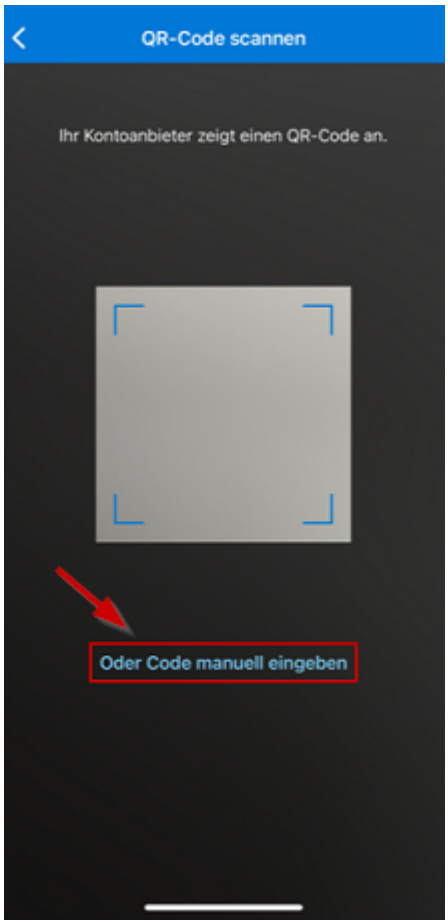
a) In der "Microsoft Authenticator" App, wählen Sie "Konto hinzufügen".



b) Wählen Sie nun für die Art von Konto "Anderes (Google, Facebook usw.)".

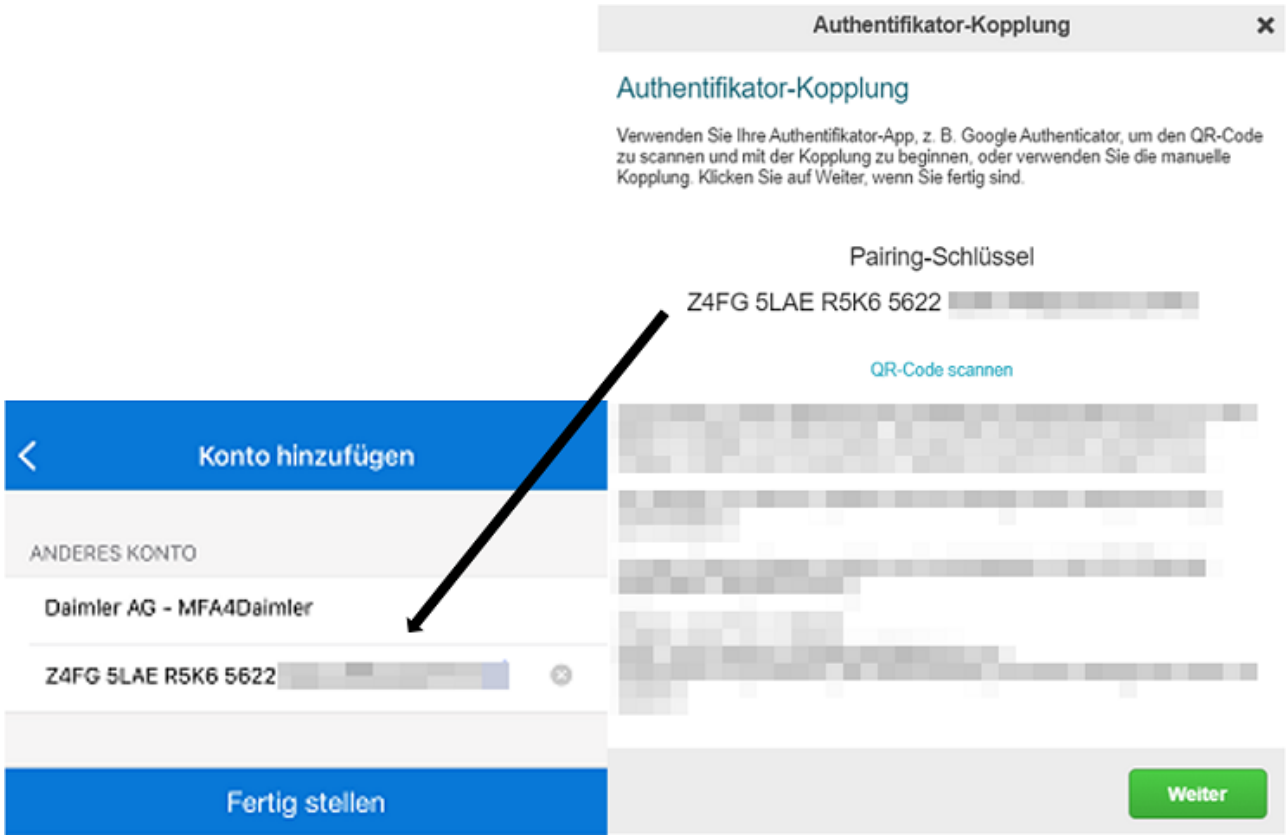


c) Die "Microsoft Authenticator" App erwartet nun, dass ein QR Code gescannt wird. Wählen Sie "Oder Code manuell eingeben" um den Pairing-Schlüssel manuell einzugeben.

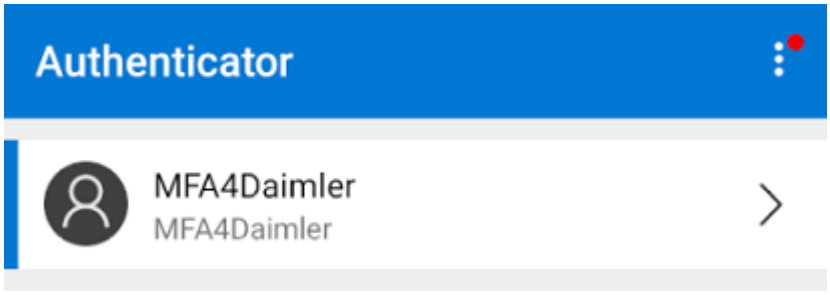


d) Wählen Sie bei MFA4Daimler "Manuelle Kopplung" um den manuellen Pairing-Schlüssel anzuzeigen.

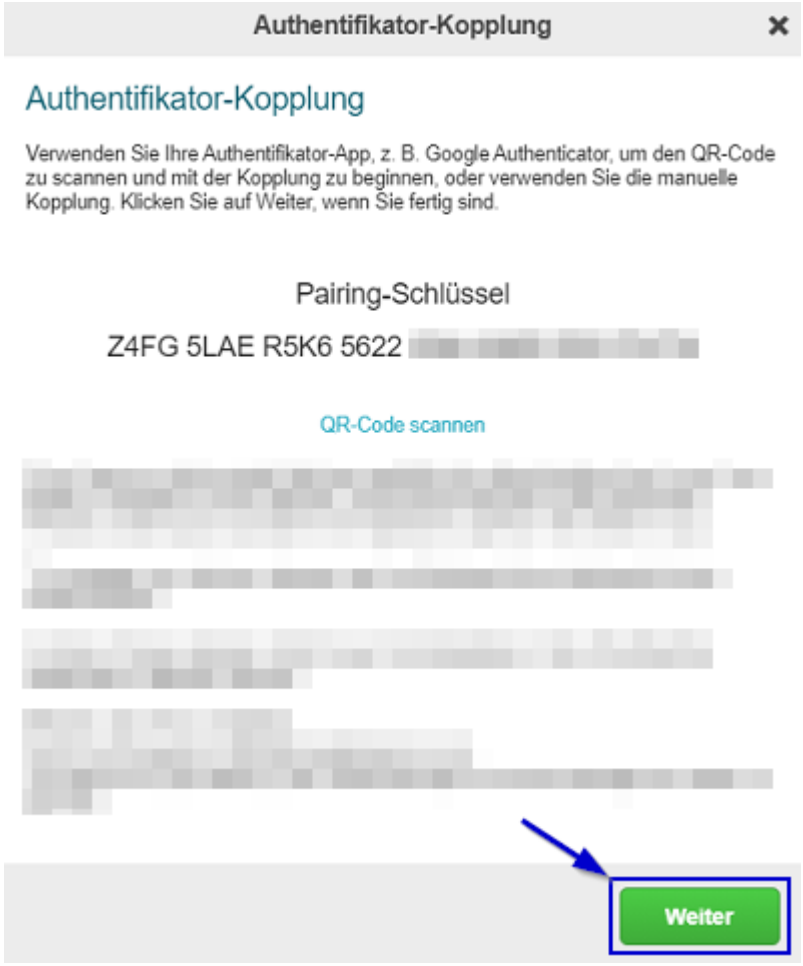
e) Geben Sie in der "Microsoft Authenticator" App einen Kontonamen ein (z.B. "MFA4Daimler" und geben Sie den im Browser angezeigten Pairing-Schlüssel ein. Wählen Sie anschließend "Fertig stellen".



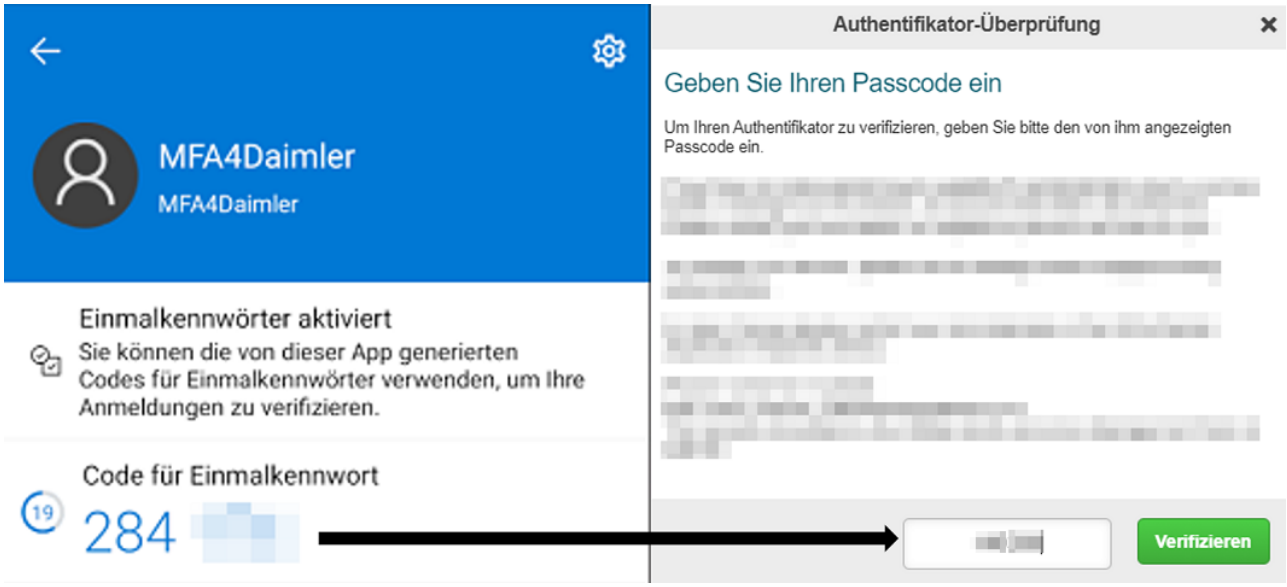
f) Es wird ein neuer Eintrag (in diesem Beispiel "Daimler AG - MFA4Daimler") in der "Microsoft Authenticator" App angezeigt.



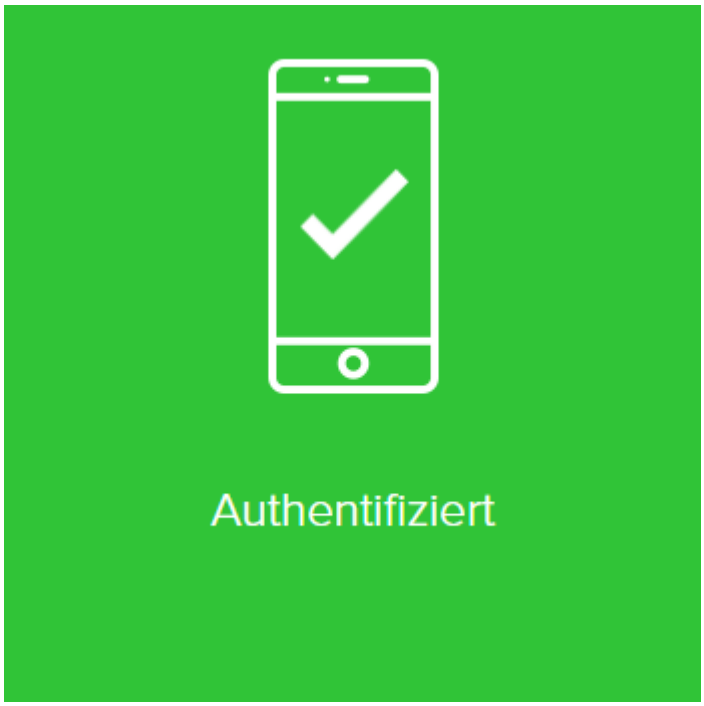
g) Wählen Sie nun bei MFA4Daimler auf "Weiter".



h) Geben Sie das in der "Microsoft Authenticator" App angezeigte Einmalkennwort im Eingabefeld des Browsers ein und wählen Sie "Verifizieren".



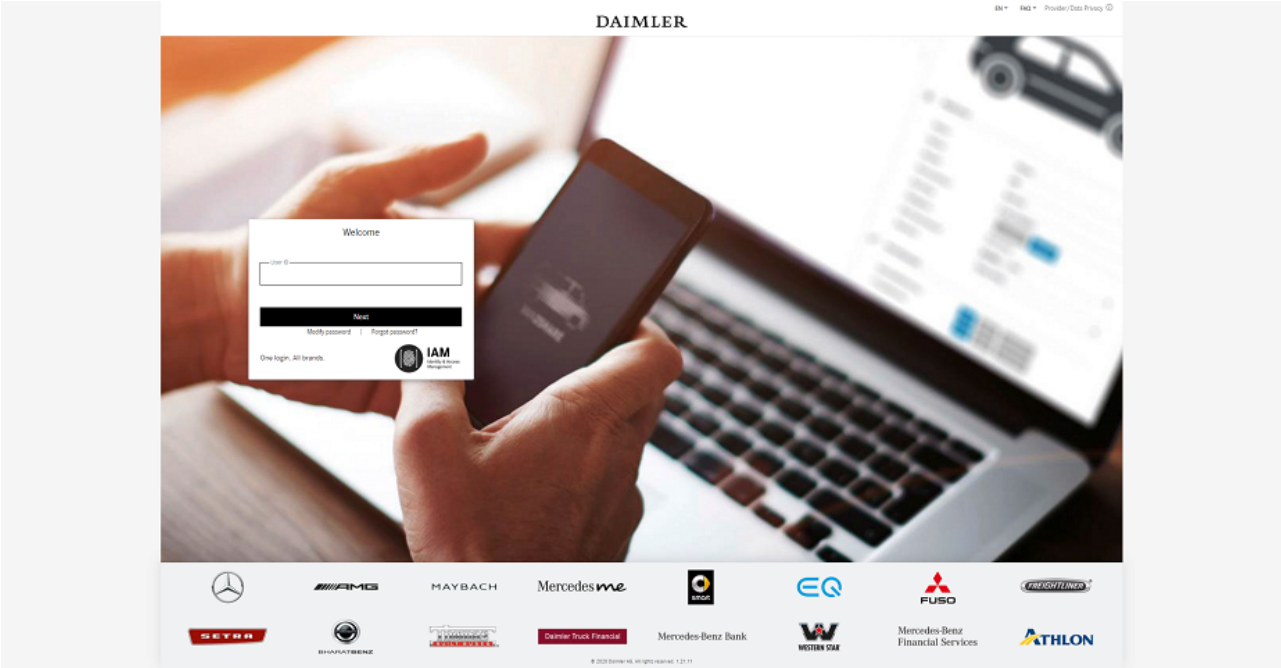
i) Die Kopplung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Sie können sich nun zukünftig mithilfe ihrer "Microsoft Authenticator" App mit MFA4Daimler anmelden.



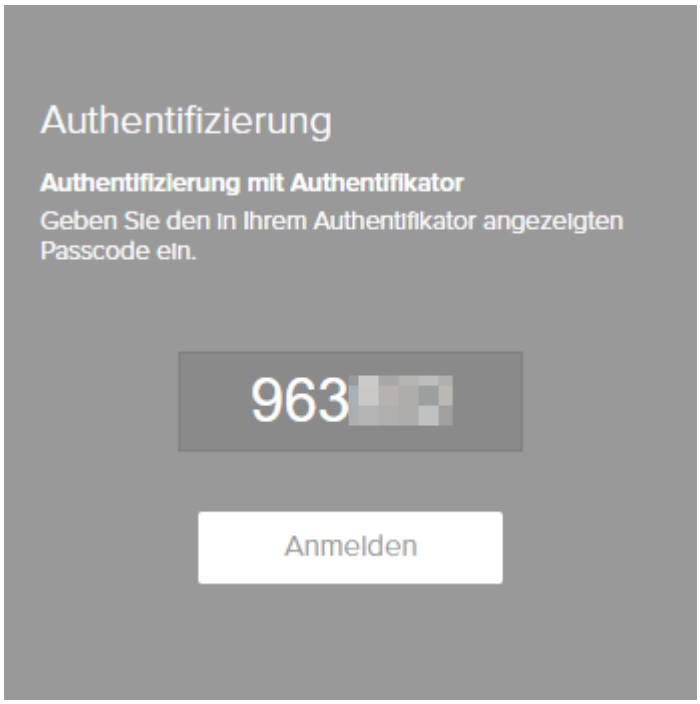
Authentifizierung

Nachdem Sie die "Microsoft Authenticator" App erfolgreich mit Ihrem Account gekoppelt haben, können Sie diese bei zukünftigen Authentifizierungen mit MFA4Daimler verwenden.

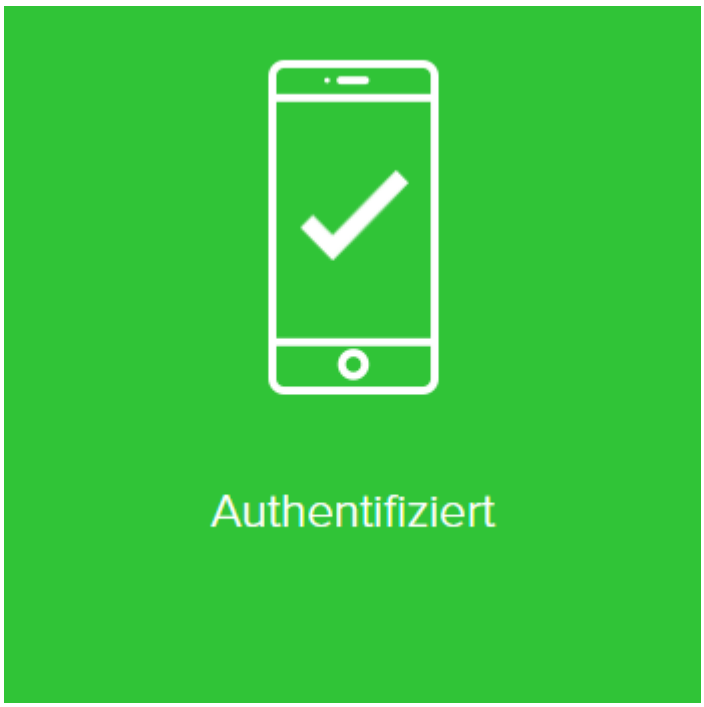
1. Rufen Sie eine mit MFA4Daimler geschützte Applikation auf.
2. Melden Sie sich am Corporate Weblogin mit Ihrer UserID und Passwort an.



3. Nach erfolgreicher Anmeldung werden Sie aufgefordert sich mit einer mit MFA4Daimler gekoppelten Methode zu authentifizieren. Öffnen Sie die "Microsoft Authenticator" App.
4. Geben Sie das in der "Microsoft Authenticator" App angezeigte Einmalkennwort in das Eingabefeld bei MFA4Daimler ein und wählen Sie "Anmelden".



5. Die Anmeldung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Anschließend werden Sie automatisch in die Applikation weitergeleitet.



3.2. Nutzung mit einem Desktop Gerät

In diesem Kapitel wird die Verwendung von MFA4Daimler mit einem Desktop Gerät am Beispiel der "WinAuth" App (Version 3.5.1) beschrieben.

3.2.1. Allgemeine Hinweise zu Remote-Desktop/Terminalserver Lösungen

Bei der Authentifizierung mit MFA4Daimler mit einer Remote-Desktop/Terminalserver Lösung wird die Nutzung einer externen Authenticator App mit einem Mobilgerät empfohlen (siehe Nutzung mit einem Mobilgerät).

Alternativ kann eine externe Authenticator App auf dem Desktop Gerät mit welchem auf die Remote-Desktop/Terminalserver Lösung zugegriffen wird verwendet werden.

Es wird sowohl aus Sicherheits- als auch Funktionalitätsgründen **nicht empfohlen**, eine externe Authenticator App auf der virtuellen Remote-Desktop/Terminalserver Lösung selbst zu verwenden.

Hinweis zur Nutzung der Authentifizierungsmethode "FIDO2 Hardware-Sicherheitsschlüssel":

- Aufgrund der Vielzahl an unterschiedlichen Implementierungen von Remote-Desktop/Terminalserver Lösungen kann es bei der Verwendung der Methode "FIDO2 Hardware-Sicherheitsschlüssel" in Verbindung mit Remote-Desktop/Terminalserver Lösungen mit MFA4Daimler zu Einschränkungen kommen. **Bevor Sie die Methode FIDO2 Hardware-Sicherheitsschlüssel in Verbindung mit einer Remote-Desktop/Terminalserver Lösung verwenden, wird dringend empfohlen die Funktionsfähigkeit im Einzelfall vorab zu testen und sicherzustellen. Im Fehlerfall kann in diesem Szenario nur eingeschränkt unterstützt werden.**

3.2.2. Installation der WinAuth Authenticator App

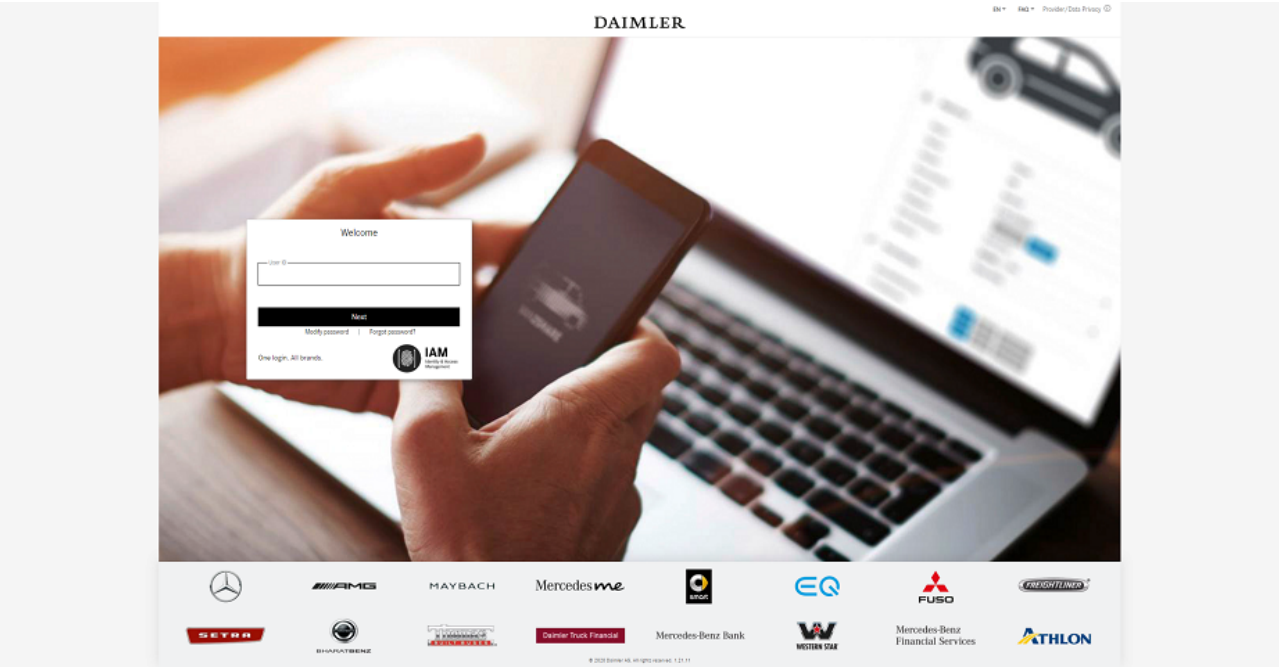
Laden Sie die "WinAuth" Authenticator App auf Ihr Desktop Gerät.

Für die Nutzung sind keine administrativen Rechte notwendig.

3.2.3. Initiale Kopplung

Nachdem Sie die "WinAuth" Authenticator App auf ihr Gerät geladen haben, wird die initiale Kopplung durchgeführt indem eine mit MFA4Daimler geschützte Anwendung aufgerufen wird.

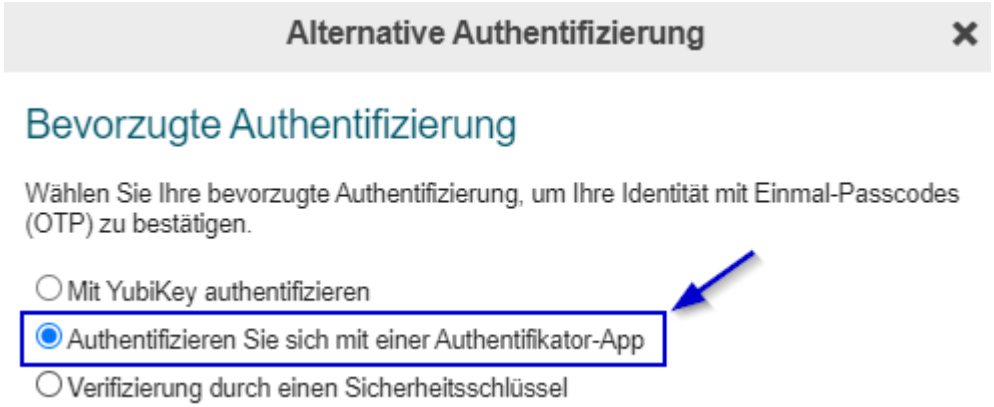
1. Rufen Sie eine mit MFA4Daimler geschützte Applikation auf.
2. Melden Sie sich am Corporate Weblogin mit Ihrer UserID und Passwort an.



3. Nach erfolgreicher Anmeldung werden Sie durch den initialen Kopplungsprozess mit MFA4Daimler geführt.

Für die Kopplung einer Authenticator App, wählen Sie den Link "Ich möchte eine alternative Authentifizierungsmethode verwenden".

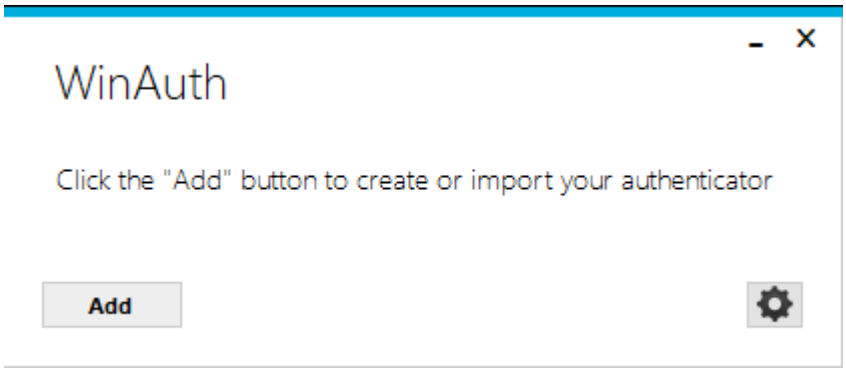
4. Wählen Sie nun die Option "Authentifizieren Sie sich mit einer Authenticator-App".



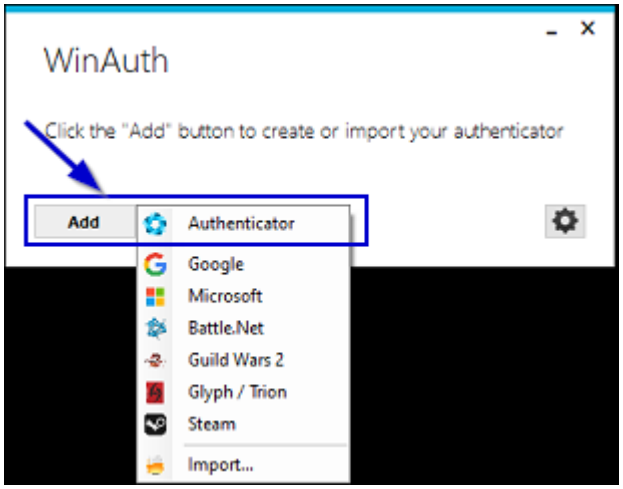
5. Kopplung Durchführen.

Es wird nun ein QR Code für die Kopplung ihres Accounts mit einer Authenticator App angezeigt. Wählen Sie bei MFA4Daimler "Manuelle Kopplung" um den manuellen Pairing-Schlüssel anzuzeigen.

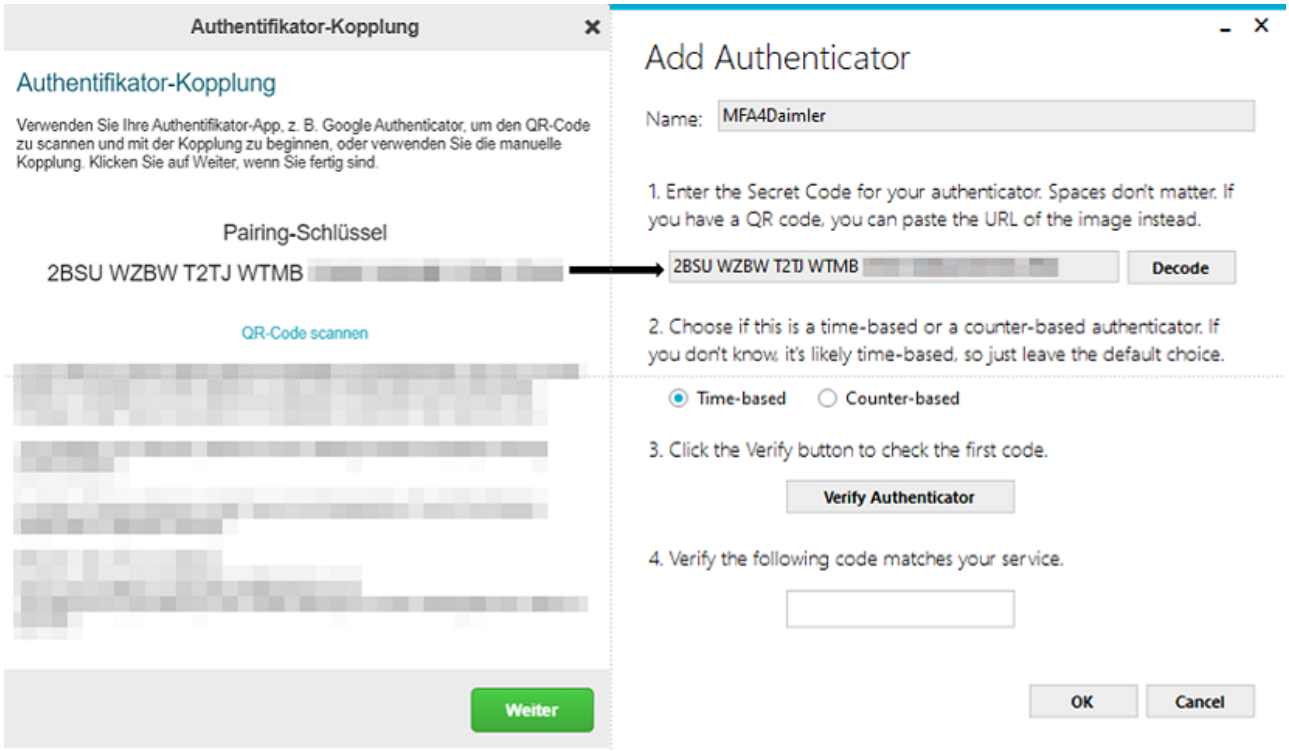
6. Öffnen Sie nun die "WinAuth" Authenticator App. Starten Sie dazu "WinAuth.exe".



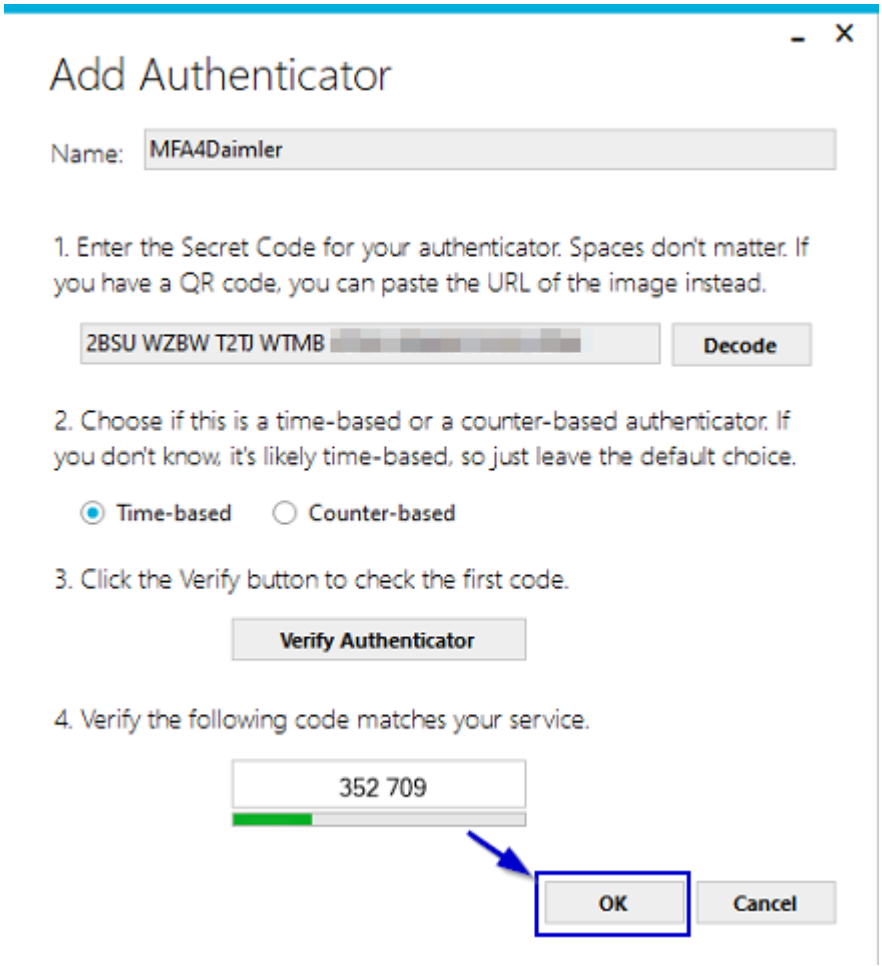
7. Um einen neuen Eintrag hinzuzufügen, wählen Sie "Add" und anschließend "Authenticator".



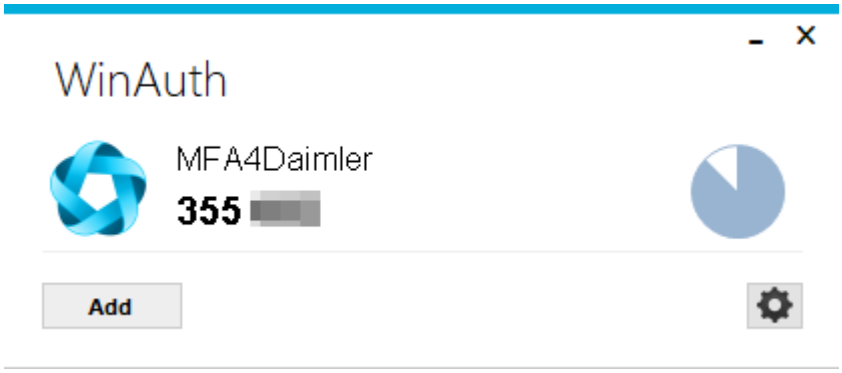
8. Geben Sie in der "WinAuth" Authenticator App einen Kontonamen ein (z.B. "MFA4Daimler") und geben Sie den im Browser angezeigten Pairing-Schlüssel ein (siehe Schritt 5.).



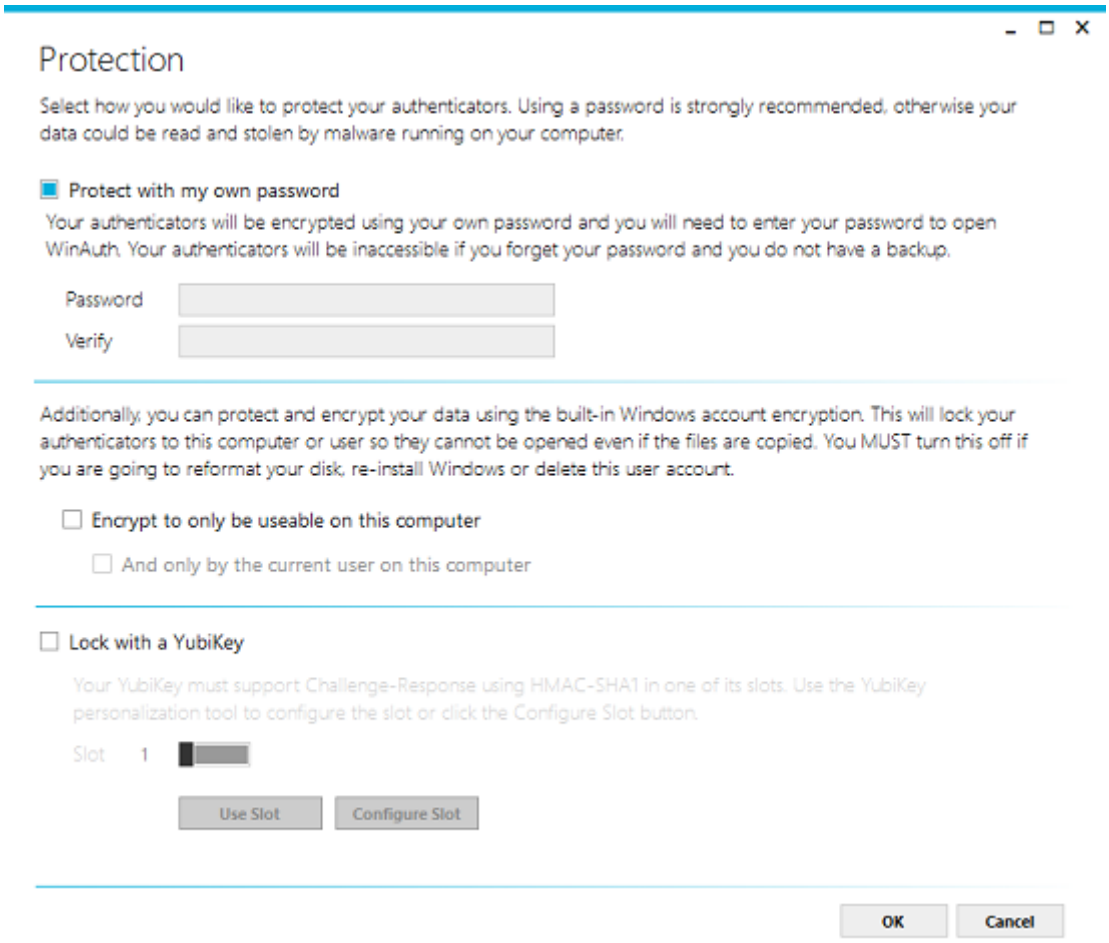
9. Wählen Sie nun in der "WinAuth" Authenticator App "OK", um Einmalkennwörter zu generieren.



10. Wählen Sie in der "WinAuth" Authenticator App erneut "OK". Es wird nun ein neuer Eintrag (in diesem Beispiel "MFA4Daimler") in der "WinAuth" Authenticator App angezeigt.

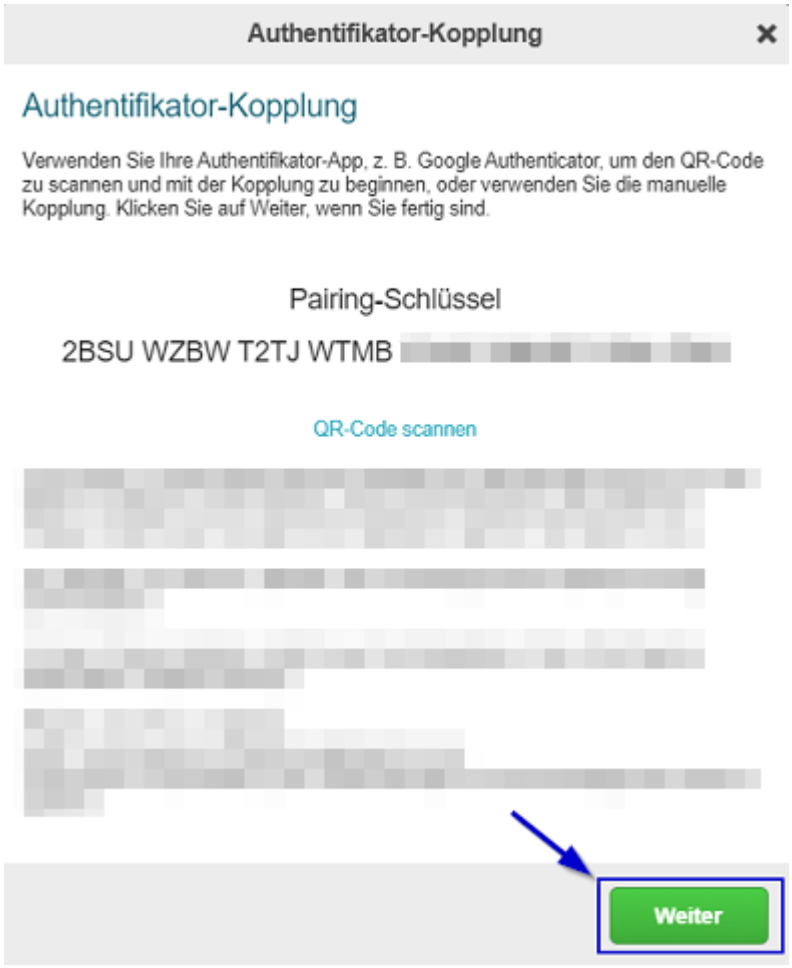


11. Gegebenfalls werden Sie aufgefordert, den Zugang zu Ihrer "WinAuth" Authenticator App zu schützen. Es wird empfohlen, eine der verfügbaren Methoden für den Zugangsschutz zu Ihrer "WinAuth" Authenticator App zu wählen. Zum Beispiel mit der Vergabe eines Passworts ("Protect with my own password"). Dieses Passwort wird dann für zukünftige Anmeldeversuche mit "WinAuth" benötigt.

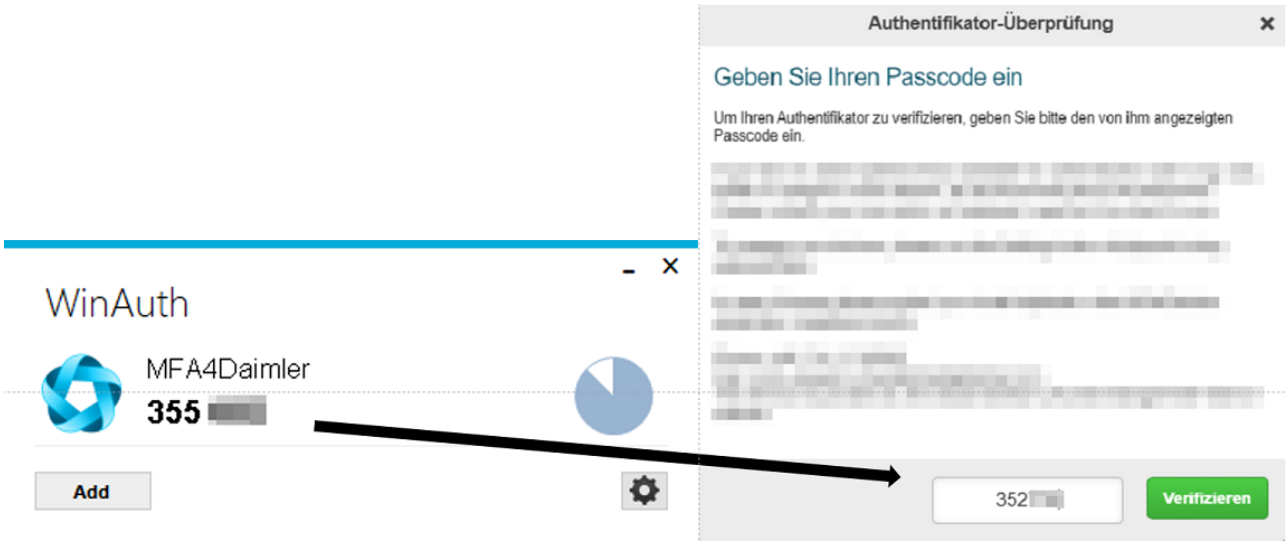


Wenn Sie keinen Schutz einrichten möchten, wählen Sie "Cancel".

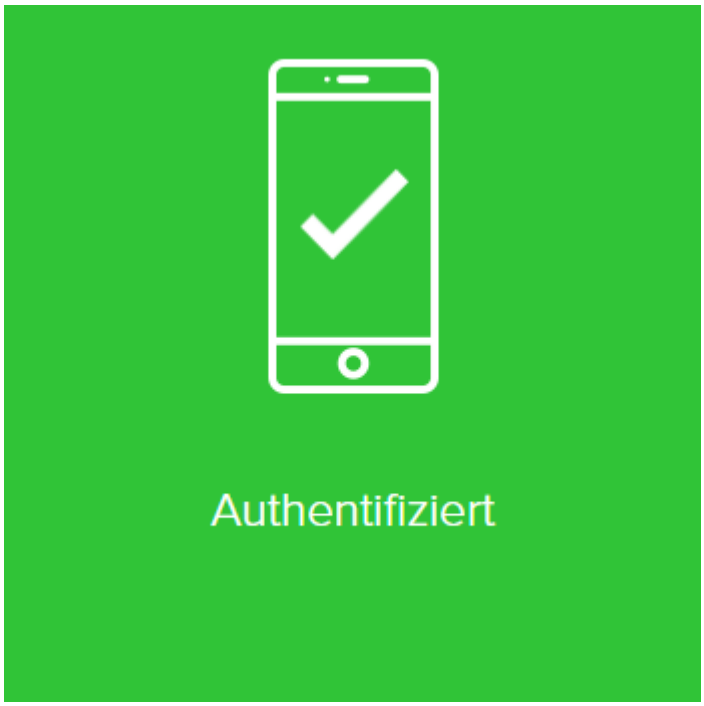
12. Wählen Sie nun im Browser "Weiter".



13. Geben Sie nun das in der "WinAuth" Authenticator App angezeigte Einmalkennwort im Eingabefeld des Browsers ein und wählen Sie "Verifizieren". Falls kein Einmalkennwort angezeigt wird, nutzen Sie in "WinAuth" die kreisförmige Pfeil-Schaltfläche auf der rechten Seite um ein Einmalkennwort anzuzeigen.



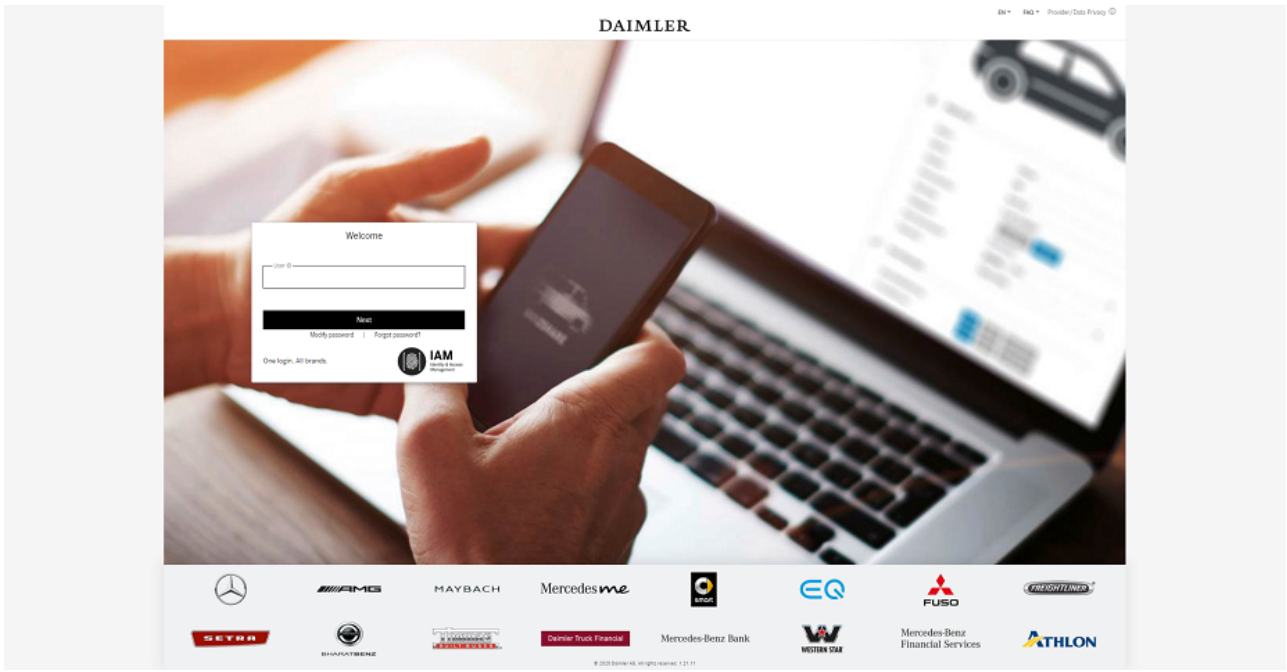
14. Die Kopplung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Sie können sich nun zukünftig mithilfe ihrer "Microsoft Authenticator" App mit MFA4Daimler anmelden.



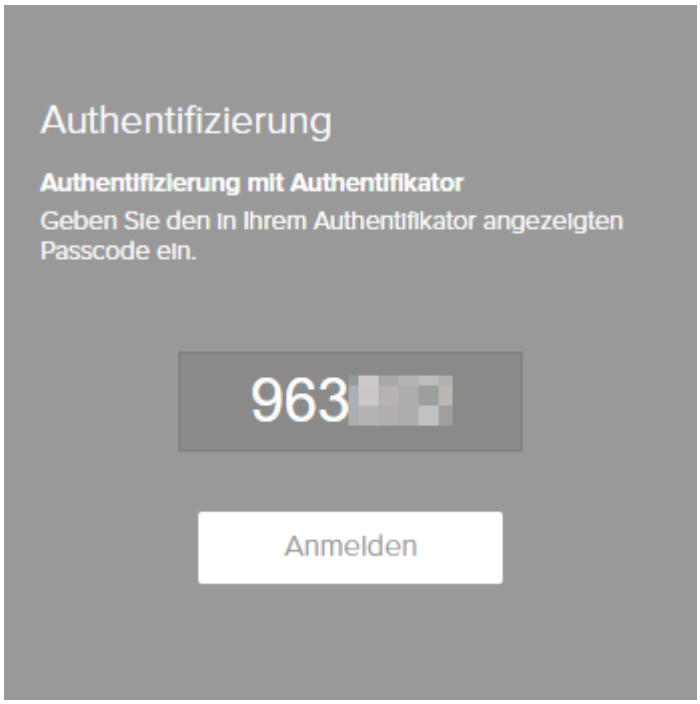
3.2.4. Authentifizierung

Nachdem Sie die "WinAuth" Authenticator App erfolgreich mit Ihrem Account gekoppelt haben, können Sie diese bei zukünftigen Authentifizierungen mit MFA4Daimler verwenden.

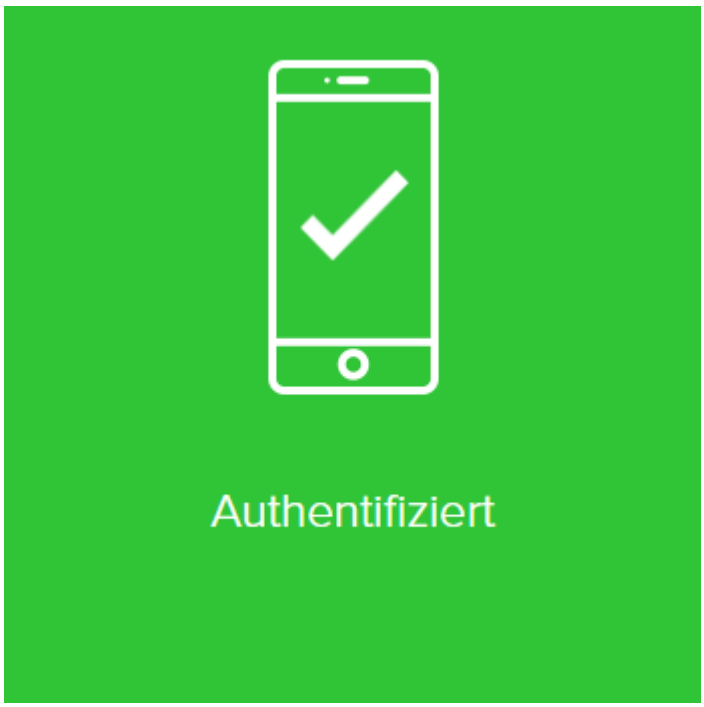
1. Rufen Sie eine mit MFA4Daimler geschützte Applikation auf.
2. Melden Sie sich am Corporate Weblogin mit Ihrer UserID und Passwort an.



3. Nach erfolgreicher Anmeldung werden Sie aufgefordert sich mit einer mit MFA4Daimler gekoppelten Methode zu authentifizieren. Öffnen Sie die "WinAuth" Authenticator App.
4. Kopieren Sie das in der "WinAuth" Authenticator App angezeigte Einmalkennwort in das Eingabefeld bei MFA4Daimler und wählen Sie "Anmelden". Falls kein Einmalkennwort angezeigt wird, nutzen Sie in "WinAuth" die kreisförmige Pfeil-Schaltfläche auf der rechten Seite um ein Einmalkennwort anzuzeigen.



5. Die Anmeldung ist erfolgreich abgeschlossen, wenn folgende Anzeige sichtbar ist. Sie werden automatisch in die Applikation weitergeleitet.



4. Account Reset und Allgemeine Self-Service-Funktionen

4.1. Account Reset

Ihr Konto muss zurückgesetzt werden, wenn sämtlicher Zugriff auf die mit Ihrem Konto gekoppelten Geräte nicht mehr möglich ist.

Um Ihr MFA4Daimler-Konto zurückzusetzen, wenden Sie sich an einen Ihrer zuständigen Administrationen (OrgAdmin/MarktAdmin), um das Zurücksetzen Ihres Kontos in GEMS für Sie durchzuführen.

Anschliessend können Sie beim nächsten Zugriff auf eine mit MFA4Daimler geschützte Applikation ein neues Gerät koppeln.

> Hinweis: Achten Sie darauf, ob Ihr Konto in der Produktions- oder Integrationsumgebung zurückgesetzt werden muss, da beide Umgebungen voneinander getrennt sind. Fügen Sie diese Information bei der Anfrage zum Reset hinzu.

4.2. Geräte verwalten

Wenn Sie ein Gerät zu Ihrem MFA4Daimler-Konto hinzufügen, ändern oder löschen möchten, besuchen Sie das Self Service Portal.

Sie können das Self Service Portal aufrufen, indem Sie während einer Authentifizierungsanforderung mit MFA4Daimler auf die Schaltfläche "Einstellungen" klicken.

Um Änderungen im Self Service Portal vornehmen zu können, ist eine Anmeldung mit MFA4Daimler notwendig.

4.2.1. Geräte hinzufügen

Öffnen Sie das MFA4Daimler Self Service Portal. Für Informationen hierzu siehe "4.2".

1. Unter "Meine Geräte" sehen Sie Ihre aktuell gekoppelten Geräte. Sie können bis zu vier verschiedene Geräte gleichzeitig mit Ihrem Konto koppeln. Wählen Sie "Hinzufügen", um den Registrierungsvorgang für ein neues Gerät zu starten.
2. Der Dialog „Neues Gerät hinzufügen“ wird angezeigt. Folgen Sie den angezeigten Schritten um Ihr neues Gerät zu koppeln.
3. Anschließend wird Ihr hinzugefügtes Gerät unter "Meine Geräte" angezeigt.

4.2.2. Ändern Sie Ihr primäres Authentifizierungsgerät

Wenn Sie mehr als ein Gerät zur Authentifizierung gekoppelt haben, können Sie ein primäres Gerät auswählen, mit dem Sie sich standardmäßig anmelden möchten.

Verwenden Sie die Schieberegler im MFA4Daimler Self Service Portal zur Auswahl Ihres primären Authentifizierungsgeräts.

4.2.3. Gerät entfernen

Wenn Sie ein Gerät aus Ihrem Konto entfernen möchten, verwenden Sie das MFA4Daimler Self Service Portal. Für Informationen hierzu siehe "4.2".

Um Änderungen im Self Service Portal vornehmen zu können, ist eine Anmeldung mit MFA4Daimler notwendig.

> **Warnung**
>
> Wenn Sie nur ein gekoppeltes Gerät haben, können Sie nach dem Entfernen des Geräts keine Authentifizierung mehr durchführen bis Sie erneut ein Gerät koppeln.

1. Wählen Sie im Self-Service-Portal das Gerät aus, das Sie entfernen möchten.
   Erweitern Sie das Menü des zu entfernenden Geräts mithilfe der Schaltfläche auf der rechten Seite.
2. Wählen Sie die Mülltonne Schaltfläche und bestätigen Sie, dass Sie dieses Gerät von Ihrem MFA4Daimler Konto entfernen möchten.
3. Nach dem erfolgreichen Entfernen des Geräts werden Ihre verbleibenden Geräte unter "Meine Geräte" angezeigt.

5. Support

Bei Fragen zu MFA4Daimler oder Problemen mit der Einrichtung wenden Sie sich bitte direkt an den Application Helpdesk von MFA4Daimler (Derzeit verfügbar in den Sprachen Englisch und Deutsch).

Bei produktspezifischen Fragen zu einzelnen externen Authenticator Apps wenden Sie sich bitte an die jeweiligen produktspezifischen Dokumentationen des Herstellers.

Kontaktdaten MFA4Daimler Application Helpdesk (AHD):

MFA4Daimler AHD	
Phone	+49 (711) 17-25005
Mail	cuhd_support_mfa4daimler@daimler.com

6. FAQ

6.1. Wie nutze ich MFA4Daimler an einem Rechner der von mehreren Personen abwechselnd genutzt wird?

Es wird dringend empfohlen, die "Logout" Funktion in der Anwendung durchzuführen bevor der Rechner von einer anderen Person genutzt wird.

Pro Benutzer und Browser ist die Sitzung für MFA4Daimler aktuell 8 Stunden gültig bevor eine neue starke Authentifizierung erforderlich ist.

6.2. Wie oft muss ich mich mit MFA4Daimler authentifizieren?

Pro Benutzer und Browser ist die Sitzung für MFA4Daimler aktuell 8 Stunden gültig bevor eine neue starke Authentifizierung erforderlich ist.
Das gilt auch, wenn Sie sich in der gleichen Browsers-Session an einer anderen mit MFA4Daimler geschützten Anwendung anmelden.

Wenn Sie in einer anderen Browser-Session (z.B. Anwendung A in Chrome, Anwendung B in Firefox) arbeiten oder einem anderen Gerät anmelden kann eine erneute MFA-Authentifizierung erforderlich sein.

6.3. Für welche Applikationen ist MFA4Daimler relevant?

Die Anforderung an eine starke Authentifizierung wie z.B. MFA4Daimler besteht für alle als "vertraulich" bzw. "integritäts-kritisch" klassifizierten Applikationen.

6.4. Kann MFA4Daimler mit einem privaten Gerät verwendet werden?

MFA4Daimler kann auch z.B. mit einem privaten Smartphone verwendet werden. Stimmen Sie die Nutzung eines privaten Geräts vorher mit Ihrem Arbeitgeber ab.

6.5. Was ist bei der Nutzung von MFA4Daimler mit Windows Gruppen-Accounts/Pool-Accounts zu beachten?

Sofern die Anmeldung mit MFA4Daimler an einem Desktop Client durchgeführt wird, der mit einem Windows Gruppen-Account von mehreren Personen genutzt wird, empfehlen wir eine mobile Authenticator App auf einem personalisierten Gerät wie z.B. einem Smartphone für die Anmeldung an MFA4Daimler geschützten Applikationen zu verwenden.

> Hinweis: Es wird aus Sicherheitsgründen nicht empfohlen, eine Authenticator App auf einem Client zu verwenden welcher von mehrern Benutzern genutzt wird.