MFA4Daimler – Quick Guide for Hardware Security Keys

Before you begin

- Make sure your browser supports this method of authentication.
- Make sure you are using a security key which is suitable for your device (e.g. USB-A, USB-C, NFC, BLE).

When using security keys with MFA4Daimler, the following requirements and limitations apply:

- MFA4Daimler supports FIDO2 and U2F security keys.
  - **Note:** U2F security keys can only generate a single credential per domain. A device can only be paired by one user per domain.
- Security keys can be used for web-based authentication through WebAuthn supporting browsers only

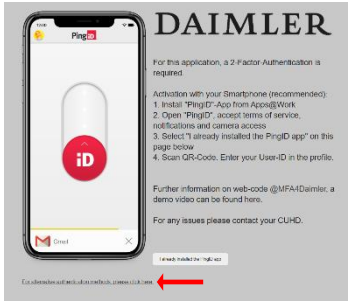
- Registration and authentication must be performed with a WebAuthn supported browser, such as the latest versions of Google Chrome or Microsoft Edge.

Register your security key with MFA4Daimler

1 Start an application protected with MFA4Daimler

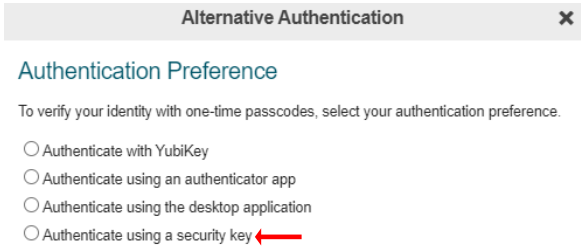
Log on using your corporate UserID and password.

On the registration page, select the link **„For alternative authentication methods, click here“**.



2 Select your authentication method

Select „security key“ and click **Next**.



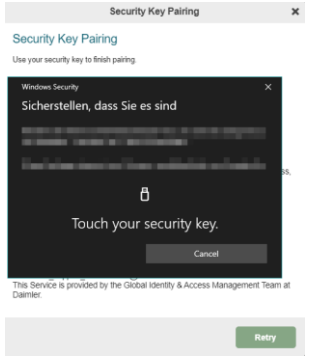
3 Perform authentication

You are prompted to authenticate with your security key.

Insert the security key into your computer USB port and then tap the contact.

This triggers authentication with your security key. A green check mark appears, indicating the pairing request is successful.

You might be asked to setup a user verification for your security key during this step (e.g. a PIN code). If so, this PIN will be requested with every authentication attempt to unlock your key.



4 Use your security key for authentication

Whenever you are required to authenticate with MFA4Daimler, insert your security key into your computer USB port and then tap the contact to authenticate.