

EU Login Zwei-Faktor-Authentifizierung (2FA) - Erfahrungen / Tipps

AIACE-DE 21.05.2025 (Version 2)

Eine Übersicht über die möglichen Authentifizierungsmethoden als Ersatz für die SMS-Methode oder als zusätzliche Methode finden Sie auf der AIACE-DE-Webseite:

EU-Login: SMS fällt weg. Installieren Sie sichere Authentifizierungsmethode(n)!

Das vorliegende Info bietet Ihnen zusätzliche Entscheidungshilfe zur Auswahl der von Ihnen gewünschten (2FA) Authentifizierungsmethode sowie wichtige Tipps. Es basiert auf der Analyse der EU-Login-Tools und bisherigen Nutzererfahrungen.

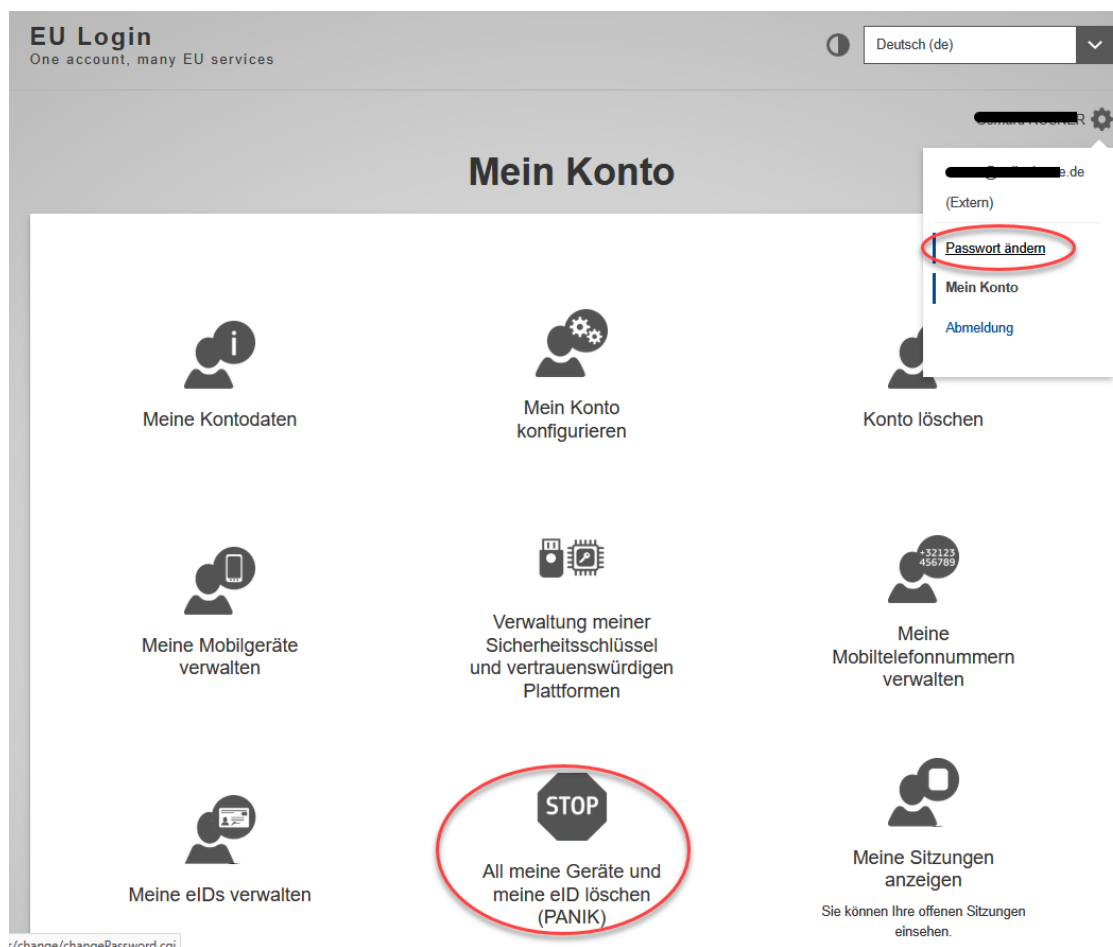
*Das Info erhebt keinen Anspruch auf Vollständigkeit und absolute Richtigkeit.
Kommentare können gerne gesandt werden an: gerhard.rosner@aiace-de.eu*

Wichtig: Für die Einrichtung jedes der möglichen Authentifizierungsmethoden ist **der erste Schritt der Aufruf Ihres EU-Login-Kontos**. Einen Leitfaden „EU Login für digitale EU-Dienste“ finden Sie ebenfalls auf der oben genannten AIACE-DE-Webseite.

Für das Einloggen in Ihr EU-Login-Konto genügt die Ein-Faktor-Authentifizierung (Benutzername + Passwort). Damit sind aber nur folgende Kontofunktionen ausführbar:

- **Passwort ändern**
- **All meine Geräte und meine eID löschen (PANIK):** siehe Leitfaden „EU Login für digitale EU-Dienste“.

Für alle anderen Kontoeinstellungen **und die meisten EU-Anwendungen** (wie MyPMO, JSIS Online) ist eine Zwei-Faktor-Authentifizierung erforderlich.



Wahl der Zwei-Faktor-Authentifizierungsmethode (2FA): Entscheidungshilfe

Die für EU-Pensionäre verfügbaren, nach Wegfall von „SMS“ als sicher geltenden Authentifizierungsmethoden sind im AIACE-DE-Leitfaden **EU-Login: SMS fällt weg....** beschrieben. **Sie müssen die Einrichtung einer 2FA-Methode nur einmal vornehmen.** Danach können Sie damit beim Aufruf einer Anwendung (z.B. RCAM/JSIS Online; siehe Bild) Ihre Identität bestätigen.



Die folgenden Empfehlungen beziehen sich jeweils darauf, mit welchem Gerätetyp Sie Ihre EU-Anwendungen (z.B. MyPMO) öffnen.

Aufruf von Anwendungen und 2FA mit demselben Mobilgerät (Smartphone/Tablet - Android/iOS):

- **EU Login Mobile App:** Gut geeignet trotz kompliziert erscheinender Einrichtung: Siehe Punkt A unten.
- **Elektronische Ausweis-ID (eID):** Geeignet: Siehe Punkt B unten.
- **Passkey:** Eignung unsicher: Siehe Punkt C unten.
- **Sicherheitsschlüssel / Security Key:** Eignung unsicher: Punkt D unten.

Aufruf von Anwendungen und 2FA mit demselben Computer (Windows/Apple) ohne Mobilgerät-Nutzung:

- **Sicherheitsschlüssel / Security Key:** Sehr gut geeignet. Siehe Punkt D unten.
- **Vertrauenswürdige Plattform / Trusted Platform Module (TPM/T1):** Gut geeignet für Windows-Computer mit TPM-Chip und Apple mit T1-Chip / etwas komplizierter einzurichten: Siehe Punkt E unten.
- **Elektronische Ausweis-ID (eID):** Geeignet: Siehe Punkt B unten.
- **Passkey:** Bedingt geeignet: Siehe Punkt C unten.

Aufruf von Anwendungen mit dem Computer (Windows/Apple), aber 2FA mittels Mobilgerät:

- **EU Login Mobile App:** Gut geeignet trotz kompliziert erscheinender Einrichtung: Siehe Punkt A unten.

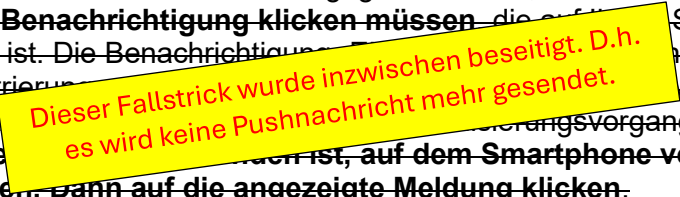
A. EU Login Mobile App

Detaillierte Schritt-für-Schritt-Anleitung von DIGIT:

[Wie kann ich meinem EU Login-Konto ein mobiles Gerät hinzufügen?](#)

Kurzanleitung: Falls Sie die DIGIT-Anleitung nicht verwenden möchten, finden Sie im Anhang eine „Kurz“anleitung (kürzer leider aufgrund der Komplexität nicht möglich).

Erfahrungen / Tipps:

- Beim Aufruf der EU-Anwendungen (wie MyPMO oder JSIS Online) verlangt die EU Login Mobile App die Verifizierung mittels Eingabe der festgelegten PIN oder mittels QR-Code. Wenn Sie für die Entsperrung Ihres Smartphones Gesichtserkennung (Face-ID) festgelegt haben, können Sie mit dieser Methode das Eintippen von Zahlen beim Login vermeiden.
- **VORSICHT (Häufige Hürde!):** Nachdem Sie als eine der letzten Schritte den QR-Code gescannt haben und die PIN eingegeben haben, erscheint die **Meldung, dass Sie auf eine Benachrichtigung klicken müssen**, die auf dem Smartphone eingegangen ist. Die Benachrichtigung, die auf dem Smartphone eingeht, liegt noch eine offene Registrierung vor. Viele übersehen diese. Wartet diese Benachrichtigung nicht auf, wird der Registrierungsvorgang abgebrochen. **Wenn die Meldung nicht kommt, ist es, auf dem Smartphone von oben nach unten wischen. Dann auf die angezeigte Meldung klicken.**

- Wenn der QR-Code wegen Zeitüberschreitung nicht mehr angezeigt wird, müssen Sie in Ihrem EU-Login-Konto das entsprechende Mobilgerät wieder löschen; dann erneut hinzufügen.
 - ✓ Dann auf **Initialisieren** in der EU Login Mobile App klicken.
 - ✓ Wenn dies wieder fehlschlagen sollte, die EU Login Mobile App deinstallieren und wieder neu installieren und Punkt 1 und 2 wiederholen.
- **Weitere mögliche Abhilfen bei fehlgeschlagener Initialisierung:**
 - ✓ Gehen Sie zu Ihrem EU Login-Konto und löschen Sie alle mobilen Geräte, die bereits mit Ihrem EU Login-Konto verknüpft sind.
 - ✓ Löschen Sie alle Daten und den Cache aus der mobilen EU Login-App:
 - i. Mobilgerät (Android): Einstellungen – Apps -> EU Login Mobile -> Speicher -> Daten/Cache löschen.
 - ii. Mobilgerät (iPhone): Einstellungen – Allgemein -> iPhone-Speicher -> EU Login Mobile -> App löschen.
 - ✓ Deinstallieren Sie die EU Login Mobile App und installieren Sie sie neu.
 - ✓ Vergewissern Sie sich, dass Sie kein Virtual Private Network (VPN) verwenden.
 - ✓ Deaktivieren Sie Ihre Firewall für die Zeit der Registrierung.

B. Elektronische Ausweis-ID (eID)

Detaillierte Schritt-für-Schritt-Anleitung von DIGIT:

[Wie kann ich meine eID meinem EU Login-Konto hinzufügen?](#)

Erfahrungen / Tipps:

- Diese Methode ist vor allem geeignet für Nutzer, die bereits Erfahrung mit der Verwendung des elektronischen Ausweises haben.
- Vorteil: I.d.R. keine Passworteingabe beim Login erforderlich, wenn Sie im Auswahlfeld für das Authentifizierungsverfahren die Methode **Elektronische ID (eID)** auswählen.

- Vereinzelt scheiterte die Einrichtung mit der Meldung „Authentifizierung fehlgeschlagen“. Der Fehler war nur vorübergehend. Nach einer gewissen Zeit konnte die Einrichtung erfolgreich wiederholt werden.
- Sie müssen zuerst Ihren Online-Ausweis im EU-Login-Konto einrichten. Danach können Sie sich damit für Anwendungen wie MyPMO verifizieren.
- **Einrichtung auf dem Computer:**
 - ✓ Verbinden Sie Ihre eID zunächst **mittels Kartenleser** mit Ihrem Computer
 - ✓ Oder verwenden Sie Ihr Smartphone als Kartenleser, wenn es NFC (=Near Field Communication; dt. Nahfeldkommunikation) unterstützt. Hierzu müssen Sie in der Ausweis-App in Ihrem Computer unter Einstellungen „Smartphone als Kartenleser“ anklicken und nach Anleitung eine Kopplung vornehmen. In der Ausweis-App Ihres Smartphones müssen Sie „Kartenleser“ aktivieren.
 - ✓ Überprüfen Sie ggfs. in der Ausweis-App unter "Meine Daten einsehen", dass die Ausweisfunktion mit diesem Gerät funktioniert.
 - ✓ Versichern Sie sich, dass die Ausweis-App auf Ihrem Computer gestartet wurde, öffnen Sie Ihr EU Login-Konto und folgen Sie der DIGIT-Anleitung.
- **Einrichtung auf dem Mobilgerät mit NFC (Smartphone/Tablet):**
 - ✓ Dieses fungiert dann gleichzeitig als Kartenleser. Alternativ können Sie einen externen Kartenleser für Android oder iOS anschließen.
 - ✓ Öffnen Sie **auf Ihrem Mobilgerät** Ihr EU Login-Konto und folgen Sie der DIGIT-Anleitung.

VORSICHT: Handschutzhüllen müssen vor dem Auflegen des Personalausweises entfernt werden, da NFC sonst nicht funktioniert.
- Es ist möglich, mindestens zwei Online-Ausweise zu registrieren (z.B. Ehemann / Ehefrau). Ob mehrere zulässig sind, habe ich nicht getestet.
- Im Menü **Meine Kontodaten** werden die verknüpften eIDs wie folgt angezeigt:

Liste verbundener Kennungen

STORK:DE/EU/32D [REDACTED] 65

STORK:DE/EU/EE [REDACTED] BE9

C. Passkey

Detaillierte Schritt-für-Schritt-Anleitung von DIGIT:

[Kann ich Passkey mit EU Login verwenden?](#)

Erfahrungen / Tipps:

- **VORSICHT:** Wenn Sie Passkey einrichten, sollten Sie bedenken, dass Sie diesen jedes Mal aktualisieren müssen, wenn Sie Ihr EU-Login-Kennwort ändern (zurzeit mindestens halbjährlich). Daher ist diese Methode nur bedingt sinnvoll.
- **Einrichtung auf dem Mobilgerät (Smartphone/Tablet):**
 - ✓ Bei Versuchen mit verschiedenen Smartphones funktionierte die Einrichtung gemäß DIGIT-Anleitung auf einem neueren Gerät, aber nicht bei einem älteren.
- **Einrichtung auf dem Computer:**
 - ✓ In der DIGIT-Anleitung wird suggeriert, dass diese Methode nur für Mobilgeräte geeignet sei. Sie kann aber auch bei den meisten Computern eingerichtet werden. Bei der Einrichtung müssen Sie auswählen wo der Passkey gespeichert werden soll:
 - **Wählen Sie:** iPhone, iPad oder Android-Gerät (Mobilgerät): Danach wird ein QR-Code angezeigt, den Sie mit Ihrem Mobilgerät scannen. Folgen Sie den im Display dann angezeigten Anweisungen.
 - **Alternativ:** Sicherheitsschlüssel. Dies ist aber nichts anderes als die in D beschriebene Methode.
 - ✓ Die Passkey-Methode (in Verbindung mit einem Mobilgerät) ist eine Möglichkeit, sich ohne die EU Login Mobile App zu authentifizieren.

D. Sicherheitsschlüssel (Security key)

Generell funktioniert die Einrichtung auf einem Computer problemlos. Die Installation ist einfach. Bei Mobilgeräten kann es Probleme geben. Nicht jeder Sicherheitsschlüssel ist hierfür geeignet.

Detaillierte Schritt-für-Schritt-Anleitung von DIGIT:

[Wie kann ich einen Sicherheitsschlüssel oder eine vertrauenswürdige Plattform hinzufügen?](#)

Erfahrungen / Tipps:

- Getestet wurden folgende Produkte:
 - ✓ YubiKey 5C NFC - Sicherheitsschlüssel für Zwei-Faktor-Authentifizierung (2FA) (Firma Yubico); Kosten ca. 60-70 €:
für Computer problemlos; für Mobilgerät fraglich.
 - ✓ Token2 T2F2-TypeC FIDO2 and U2F Security Key (Firma Token2); Kosten ca. 20-30 €: für Computer problemlos; für Mobilgerät fraglich.
- **Einrichtung auf dem Mobilgerät (Smartphone/Tablet):**
 - ✓ Bei Versuchen mit verschiedenen Smartphones funktionierte die Einrichtung gemäß DIGIT-Anleitung auf einem neueren Gerät, aber nicht bei einem älteren.
 - ✓ Beim Starten der Authentifizierung für die My PMO-App unter Verwendung eines Sicherheitsschlüssels (Yubikey) erscheint inzwischen die folgende Meldung: "No passkeys available...." Grund unbekannt. D.h. die Methode funktioniert nicht mehr. (Bisher nicht möglich, von PMO oder DIGIT Auskunft hierzu zu erhalten.)
- **Einrichtung auf dem Computer:**
 - ✓ Für die Festlegung eines PIN-Codes ist es erforderlich, dass der Sicherheitsschlüssel noch keinen PIN-Code gespeichert hat. Ggfs. Reset durchführen:
 - Windows: Windows-Taste im Suchfeld „Anmeldeoptionen“ eingeben → Sicherheitsschlüssel Verwalten → Sicherheitsschlüssel zurücksetzen
 - Apple: Einstellungen → [dein Name] → Anmeldung & Sicherheit → Sicherheitsschlüssel → ? (nicht getestet)

E. Vertrauenswürdige Plattform / Trusted Platform Module (TPM/T1)

Detaillierte Schritt-für-Schritt-Anleitung von DIGIT:

[Wie kann ich einen Sicherheitsschlüssel oder eine vertrauenswürdige Plattform hinzufügen?](#)

Erfahrungen / Tipps:

- Nur für Windows-Computer mit TPM-Chip oder Apple mit T1-Chip (Secure Enclave). Die Authentifizierung mittels TPM oder T1 ist jeweils an DIESEN Computer gebunden.
- Falls TPM nicht verfügbar ist, wird im EU-Login-Konto die Meldung angezeigt: „**User verifying platform authenticator not available on your device.**“
- Schneller, einfacher Zugang zu Anwendungen über PIN-Code, Fingerabdruck oder Gesichtserkennung. Kein separates Gerät erforderlich.
- Voraussetzung: Das Trusted Platform Module (TPM) muss unter Windows oder die Secure Enclave auf Apple-Geräten unterstützt und aktiviert werden.

Anhang: Einrichtung der EU Login Mobile App: siehe nächste Seite

Anhang: Einrichtung der EU Login Mobile App

Die folgende Schritt-für-Schritt-Anleitung lässt die Einrichtung dieser Methode als kompliziert erscheinen. Wenn Sie genau die Schritte befolgen, sollten Sie problemlos zum Ziel kommen.

- Gehen Sie auf Ihrem Mobilgerät zum Google Play Store (Android) oder zum App Store (iOS), suchen Sie nach der **EU Login Mobile App** und installieren Sie diese.
 - a. Öffnen Sie diese App, aber klicken **noch nicht** auf Initialisieren!
 - b. Wenn dies von der App verlangt wird, erlauben Sie Benachrichtigungen über die App und **den Zugriff auf die Kamera**.
 - c. VORSICHT:
 - i. Bei Meldung „Benachrichtigungen scheinen deaktiviert zu sein“: auf **Genehmigung zur Erteilung** und dann auf **Zulassen** klicken. Im unteren Bereich wird dann möglicherweise „Nein“ angezeigt – warum auch immer. Einfach ignorieren.
 - ii. Alternativ Einstellungen des Smartphones – Apps öffnen und dort die App EU Login Mobile auswählen. Dort Berechtigungen: Benachrichtigungen und Kamera zulassen
- Öffnen Sie Ihren Internet-Browser (Firefox, Chrome, Edge, Safari etc.) auf Ihrem Computer oder auf Ihrem Smartphone oder Tablet und gehen Sie zur EU Login-Homepage ecas.ec.europa.eu/cas. Loggen Sie sich dort ein und wählen ggfs. eine andere Sprache (Deutsch) aus.
 - a. Wählen Sie **Einstellungen** (Zahnradsymbol oben rechts),
 - b. dann **Mein Konto** und
 - c. klicken Sie auf **Meine Mobilgeräte verwalten**.
 - d. Dann klicken Sie auf **Mobilgerät hinzufügen**.
 - e. Geben Sie einen **Gerätenamen** (ohne Leerzeichen) ein, wählen Sie einen **PIN-Code** aus und klicken Sie auf **Senden**.
Auf Basis Ihrer Eingabe wird ein QR-Code generiert, der auf dem Computerbildschirm angezeigt wird. Den benötigen Sie in Schritt 3.
- Wenn Sie auf Ihrem Mobilgerät die **EU Login Mobile App** noch nicht geöffnet haben,
 - a. öffnen Sie diese und klicken Sie auf **Initialisieren** und dann auf **Weiter**. Ggfs. Zulassen, dass die App Bilder aufnehmen darf. Erforderlich für den QR-Scan!
 - b. Es öffnet sich der eingebaute QR-Code-Scanner.
 - c. Halten Sie Ihr Smartphone vor den auf dem Computer angezeigten QR-Code.
 - d. Geben Sie bei Aufforderung die in Schritt 2e vergebene PIN ein und ~~achten Sie auf die Benachrichtigung, die dann am oberen Rand erscheint.~~
 - e. ~~VORSICHT: Die Meldung, dass Sie auf die Benachrichtigung klicken müssen erscheint nur ganz kurz (!!!) mit der Meldung „EU Login Mobile: Von Ihnen liegt noch eine offene Registrierungsanfrage vor.~~
Wenn die Meldung verschwunden ist, auf dem Smartphone von oben nach unten wischen. Dann auf die angezeigte Meldung klicken.
 - f. Anzeige bei Erfolg: **Geräteregistrierung erfolgreich**
 - g. Ggfs. wird angezeigt **Biometrische Erfassung**. Hier können Sie festlegen, ob Fingerabdruck oder Gesichtserkennung zur Verifizierung erlaubt sein soll.
