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

AIACE-DE 21.05.2025 (Version 2)

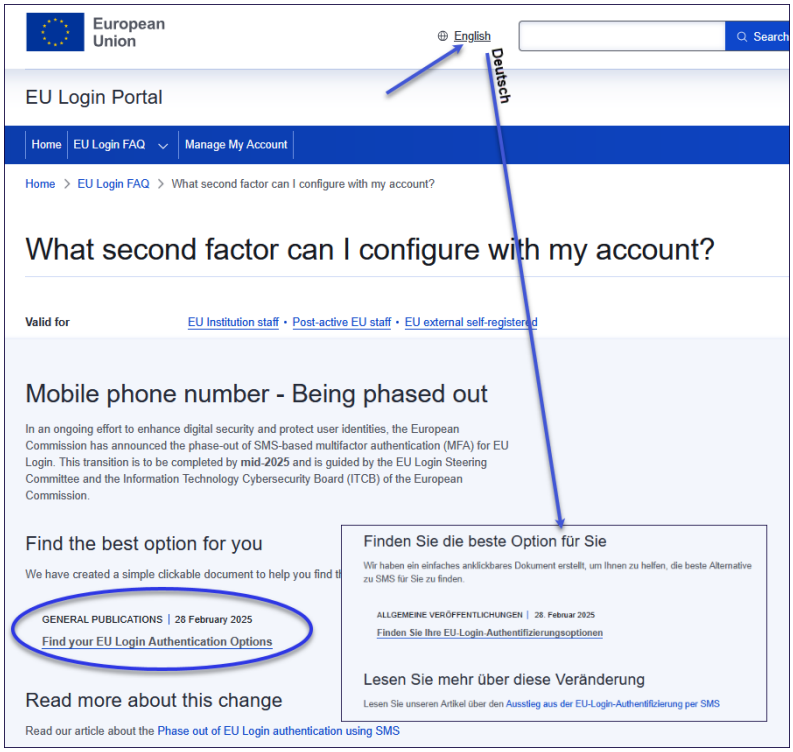
☞ **Achten Sie auf Aktualisierungen und neue Informationen auf der Website von AIACE-DE: http://www.aiace-de.eu/ und AIACE-INT@ec.europa.eu**

Sie haben ein EU-Login-Konto für Anwendungen wie GKFS-Online, MyPMO, SYSPER Post Activity oder Staff Matters? Sie verwenden als zweite Verifizierungsmethode **Mobiltelefon+SMS**? Dann droht seit einiger Zeit das PMO-Damoklesschwert „*Die Authentifizierung per SMS wird bis Mitte 2025 vollständig abgeschafft.*“

Hintergrund: Um die digitale Sicherheit zu verbessern und Benutzeridentitäten zu schützen, hat die Europäische Kommission die Abschaffung der SMS-Methode angekündigt. Daher wird dringend zur Umstellung auf eine andere Authentifizierungsmethode geraten. Unabhängig von dieser Notwendigkeit sollten Sie mindestens zwei verschiedene Methoden zur Verifizierung in Ihrem im EU Login Account einrichten, um bei Ausfall der einen auf die andere zurückgreifen zu können.

Zu Ihrer Beruhigung: Falls Sie die Umorientierung nicht schaffen (wollen), bleibt immer (noch) der althergebrachte Weg, mit der Kommission zu kommunizieren, also per Brief oder Telefon, soweit möglich auch per E-Mail, auch wenn dies zusehends schwieriger wird.

Handeln Sie: Es gibt eine Vielzahl von Anleitungen auf PMO- und AIACE-Webseiten. Zu empfehlen ist die interaktive Entscheidungshilfe, die von der Generaldirektion für Digitale Dienste (DIGIT) herausgegeben wurde: „SMS authentication phase-out in EU Login“. Diese ist zwar (bisher) nur auf Englisch verfügbar, aber die verlinkten Webseiten können durch Klicken auf die voreingestellte Sprache (siehe Pfeil im Bildschirmfoto) auf Deutsch angezeigt werden.



Alle Links in diesem Beitrag sind anklickbar.

Diese Entscheidungshilfe hilft Ihnen, eine oder mehrere der „sicheren Login-Alternativen“ einzurichten. Beachten Sie ggfs. die nachfolgend beschriebenen Tipps (Hinweis: „Smartphone“ beinhaltet auch „Tablet“).

Weitere Hilfen finden Sie auf der Website von AIACE INT[1].

☞ **Tipp:** Für die Registrierung und Verwaltung von Authentifizierungsmethoden müssen Sie sich immer zuerst mit Ihren Anmeldeinformationen in Ihr **EU Login-Konto** einloggen, entweder mit Ihrem Internet Browser: https://ecas.ec.europa.eu/cas/ oder durch Klicken auf „My Account / My Konto“ in der unteren blauen Menüleiste Ihrer MyPMO App (Smartphone). Wenn Sie unsicher sind, welche Methode(n) sie eingerichtet haben, öffnen Sie eine Übersicht im EU Login Account - „My Account – My account details“ (Mein Konto – Kontodaten).

☞ **Dieses Info ist am besten zu verstehen, wenn Sie auf den/die Link(s) klicken, um die gewünschten Informationen anzuzeigen.**

Sie haben folgende Optionen für sichere EU-Login-Authentifizierung:

1. **EU Login Mobile App PIN Code/QR code (für Smartphone; empfohlen).**
   - Eine einfache und sichere Option, entweder mit biometrischem Schutz / PIN-Code, Offline-QR-Code- oder Gesichtserkennung (je nach Einstellung in Ihrem Gerät).
   - Das Bildschirmfoto zeigt den Weg zur detaillierten DIGIT-Anleitung. Oder entsprechende Webseite direkt aufsuchen.
   - In einem Video-Tutorial zur Einrichtung Ihres Smartphones in Ihrem EU Login Account können die Untertitel auf Deutsch umgestellt werden: in unterer Video-Taskleiste das  Symbol links neben Zahnrad anklicken.
   - **VORSICHT:** Das Video warnt nicht, dass nach Vergabe eines PIN-Codes eine Nachricht nur ganz kurz am oberen Displayrand Ihres Mobilgeräts angezeigt wird. Auf diese Nachricht muss man unbedingt tippen, um die Anm… abzuschließen. Wischen Si… oberen Displayr… unten … Bei … auch ein orange-… auftauchen, das ignoriert …den sollte!

Dieser Fallstrick wurde inzwischen beseitigt. D.h. es wird keine Pushnachricht mehr gesendet.

   - **Authentifizierung auf einem Mobilgerät / On mobile authentication** ist eine Variante der EU Login Mobile App, wenn diese auf demselben mobilen Gerät installiert ist wie die gestartete Anwendung (z.B. MyPMO). Vorteil: Die EU Login Mobile App öffnet sich automatisch.

[1] Siehe https://aiace-europa.eu/de/tools/eu-login-app/

2. **Elektronische Ausweis-ID (eID) (PC mit Kartenlesegerät oder Smartphone. Einrichtung etwas komplizierter):** Authentifizierung über die Online-Ausweisfunktion Ihres Personalausweises[2] oder einer eID-Karte[3] für nichtdeutsche Angehörige der EU und des EWR. Voraussetzungen: siehe Websites in den genannten Fußnoten.
   - Voraussetzung: Online-Ausweis beantragen und registrieren; Ausweis-App des Bundes installieren oder Kartenleser verwenden
   - Anleitung zur Registrierung in Ihrem EU Login Account: siehe Leitfaden-Folie „Is your country on the list of those using an eID?“ oder direkte Webseite.
   - Smartphone fungiert als Kartenleser; die EU Login Mobile App öffnet automatisch die Ausweis-App und führt durch die weiteren Schritte (Ausweis-PIN eingeben und Personalausweis an Smartphones anlegen).
   - Alternativ (ohne App): Kartenlesegerät anschließen (Aber: Einschränkungen bei der Funktionalität nicht auszuschließen je Hardware und Software-Treibern.)

3. **Sicherheitsschlüssel / Security Key (sehr gut mit PC oder (nicht immer erfolgreich) mit Smartphone. Einfache Handhabung).** Physisches Gerät (Stick mit einem speziellen Chip), das über USB, Bluetooth oder NFC (Near Field Communication - Nahfeldkommunikation) eine Verbindung zu einem Computer, Smartphone herstellt.
   - Voraussetzung: Sicherheitsschlüssel erwerben: Googeln Sie nach „Sicherheits-schlüssel MFA“ (MFA = Multi-Faktor-Authentifizierung) und suchen Sie nach einem Stick, der FIDO2 unterstützt (FIDO = **F**ast **ID**entity **O**nline)
   - Anleitung zur Registrierung für EU-Login: siehe Leitfaden-Folie „My country does not use an eID – Security Key“ oder direkte Webseite.
   - Kurzanleitung: Sicherheitsschlüssel per USB an Ihr Gerät anschließen und entsprechend der DIGIT-Anleitung mit Ihrem EU-Login-Konto verknüpfen. Zur Verifizierung z.B. bei MyPMO oder JSIS Online den Schlüssel einfach einstecken, PIN oder Fingerabdruck und Sie sind drin.
   - ☞ **VORSICHT:** Wenn der Schlüssel (Stick) verloren geht, ist es zwar unwahrscheinlich, dass die PIN „geknackt“ werden kann, wenn sie nicht gerade „1234“ oder dergleichen vergeben haben, aber es empfiehlt sich, im EU Login Account unter „Manage my Security Keys“ (Meine Mobiltelefonnummern verwalten) den Schlüssel zu entfernen.

4. **Vertrauenswürdige Plattform / Trusted Platform Module (TPM) (für Fortgeschrittene; nur für PC)**. Ein Computerchip, der auf vielen Laptops und Desktop-Computern für eine nahtlose Authentifizierung verfügbar ist. Schneller, einfacher Zugang zu Diensten über PIN-Code, Fingerabdruck oder Gesichtserkennung. Kein separates Gerät erforderlich.
   - Anleitung zur Registrierung für EU-Login: siehe Leitfaden-Folie „Options for advanced users - Trusted Platform Module“ oder direkte Webseite.
   - Voraussetzung: Lesen Sie die technische Dokumentation Ihres Computers und stellen Sie sicher, dass das Trusted Platform Module (TPM) unter Windows oder die Secure Enclave auf Apple-Geräten unterstützt und aktiviert ist. Überprüfen Sie, ob Ihr Internet-browser konform ist, indem Sie die folgende Website konsultieren: https://caniuse.com/#search=webauthn
   - Dann das TPM unter Windows oder auf Apple einrichten. Siehe Schritt-für-Schritt-Anleitung von DIGIT.

---

[2] Siehe: https://www.personalausweisportal.de/Webs/PA/DE/startseite/startseite-node.html
[3] Siehe: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/eID-karte-der-EU-und-des-EWR/eid-karte-der-eu-und-des-ewr-node.html

- Richten Sie TPM als Authentifizierungsmethode im EU Login Account unter „Manage my Security Keys – Add a Trusted Platform“ ein. **Hinweis: Falls TPM nicht verfügbar ist, wird die Meldung angezeigt: „User verifying platform authenticator not available on your device.**“
- Beim ersten Einloggen in einer Anwendung (z.B. MyPMO) die Option „Security Keys and Trusted Platforms auswählen“ und entweder biometrisch (Fingerabdruck) oder mit Zugangskennwort authentifizieren.

5. **Passkey (nur für Smartphone; einfache Handhabung)**. Zu Deutsch: Hauptschlüssel. Passkeys sind lange, zufällig generierte Zeichenketten, offen und herstellerunabhängig. Statt mit einem Passwort loggt man sich per Fingerabdruck, Gesichtsscan oder mit einer PIN ein. Die Verifizierung erfolgt Im Hintergrund.
   - Anleitung zur Registrierung für EU-Login: siehe Leitfaden-Folie „Options for advanced users - Passkey“ oder direkte Webseite.
   - Im DIGIT-Leitfaden für fortgeschrittene Benutzer empfohlen. Die Einrichtung ist aber relativ simpel. Die Registrierung erfolgt analog wie für einen Sicherheitsschlüssel (siehe oben) mit dem Unterschied, dass „das Gerät“ kein externer Stick ist, sondern das Smartphone selbst. Geben Sie also einen entsprechenden Namen ein, z.B. „Smartphone“. Nach „Weiter“ muss entweder mit Fingerabdruck oder mit einer PIN bestätigt werden. Danach kommt die Meldung „Es wurde ein Passkey hinzugefügt.“
   - Wenn Sie eine Anwendung starten (z.B. MyPMO), wählen Sie die Option „Security Keys or Trusted Platforms“ („Passkey“ wird in der Auswahlliste nicht explizit angezeigt). Dann wählen Sie als Gerät den Namen des registrierten Smartphones aus und bestätigen mit Fingerabdruck oder PIN. Fertig!
   - **VORSICHT:** Wenn Sie Ihr EU-Login-Kennwort ändern (mindestens halbjährlich), muss der Passkey aktualisiert werden.

Fehlerbehebung / Troubleshooting

Hier ein paar Tipps, wenn es klemmt:

- **Server-Probleme:** Manchmal kann eine Anwendung „hängen“ oder lässt sich nicht aufrufen, weil es temporäre Probleme mit der Internetverbindung oder mit dem EU-Server gibt. Falls dieser Verdacht besteht, einfach etwas abwarten und später wieder versuchen.
- **EU Login-Probleme:**
  - ✓ Klicken Sie auf keinen Fall auf „Konto erstellen“, wenn bereits eines besteht!
  - ✓ Kennwort vergessen oder aktualisieren? Siehe Info hier.
  - ✓ Versuchen Sie es mit einem anderen kostenlosen Browser (z. B. Firefox, auf PC und Mac).
  - ✓ Schalten Sie ggfs. VPN aus, falls Sie diesen Dienst verwenden.
  - ✓ Verwenden Sie als Login nur Ihre von der Kommission anerkannte E-Mail-Adresse.
  - ✓ Leeren Sie den Cache (Puffer-Speicher) und den Verlauf Ihres Browsers: Strg+Umschalt+Entfern-Taste. Schließen Sie den Browser. Schalten Sie Ihren Arbeitsplatz (PC, Laptop, Tablet, Smartphone) aus und wieder ein. Wenn dann im EU-Login Ihre E-Mail-Adresse automatisch erscheint, haben Sie nicht alle gespeicherten Daten gelöscht, die möglicherweise nicht mehr aktuell sind und die Ursache für Ihr Verbindungsproblem sind.

- ✓ Wenn möglich, deaktivieren Sie Ihre Firewall für die Zeit der Registrierung, da die Verwendung einer Firewall Probleme verursachen kann

- **Probleme beim Aufruf von Anwendungen wie My PMO, JSIS Online:**
  - ✓ Stellen Sie sicher, dass Sie die richtige Webadresse (URL) verwenden, z.B. https://myremote.ec.europa.eu, https://webgate.ec.europa.eu/RCAM, oder https://mypmo.europa.eu
- **EU Login Mobile App: Wenn Sie Einrichtungsprobleme haben oder die App nicht wie gewünscht startet:**
  - ✓ Löschen Sie das mit Ihrem EU-Login-Konto verknüpfte Mobilgerät.
  - ✓ Mobilgerät (Android): In der EU Login mobile App alle Daten und den Cache (Puffer-Speicher) löschen: Einstellungen – Apps -> EU Login Mobile -> Speicher -> Daten/Cache löschen.
  - ✓ Dann die App deinstallieren und neu installieren.
  - ✓ Mobilgerät (iPhone): Einstellungen – Allgemein -> iPhone-Speicher -> EU Login Mobile -> App löschen. Dann die App neu installieren.
- **Elektronische Ausweis-ID (eID):**
  - ✓ Wenn Sie ein Kartenlesegerät verwenden, kann es Kompatibilitätsprobleme geben.
  - ✓ Installieren Sie ggfs. den neuesten Treiber.

Siehe auch: https://aiace-europa.eu/de/tools/eu-login/

Hilfe / EU-Login-Unterstützung

Im Falle eines nicht selbst lösbaren Problems können Sie sich wenden an:

AIACE-DE EU-Login-Helpdesk: Per E-Mail an eulogin.hilfe@aiace-de.eu mit kurzer Beschreibung des Problems und Angabe Ihrer Kontaktdaten

PMO: E-Mail senden an PMO-IT-APPLICATIONS@ec.europa.eu

PMO: Anmelden unter https://ec.europa.eu/newsroom/pmo/items/879194/en für eine **Individuelle oder Interaktive praxisbezogene Gruppensitzung** (auf Englisch oder Französisch)

PMO-Telefon: +32 (0)2 29 11111; Option 5 **(**Mo. bis Fr., 9:30 bis 12:30 Uhr)

Bei schriftlichen Anfragen geben Sie möglichst folgende Informationen an:

- ✓ den Benutzernamen oder die E-Mail-Adresse des betreffenden Kontos
- ✓ wie Sie auf die Anwendung zugreifen, einschließlich ihrer URL
- ✓ eine **detaillierte** Beschreibung des Problems
- ✓ wenn möglich, ein oder mehrere Screenshots, die das Problem mit der Adressleiste zeigen, auf der die aufgerufene Webseite und der vorherige Schritt angegeben sind
- ✓ Unbedingt angeben, ob und bis wann Ihr Zugang oder die Anwendung zuvor ordnungsgemäß funktioniert hat.