

## **i-mpuls JMD**

Web-Anwendungs-Server für computergestützte Fallakten

# **Handbuch Authentifizierung mit Einmalpassworten (OTP)**

Stand: Oktober 2025

Projektbezeichnung	i-mpuls JMD	
Projektleiter (AG)	Ulrike Kiese (Servicebüro JMD)	
Projektleiter (AN)	Frank Koormann (Intevation)	
Verantwortlich	Katharina Schütze, Frank Koormann Intevation GmbH, Neuer Graben 17, 49074 Osnabrück	
Zuletzt geändert	9. Oktober 2025	
Bearbeitungszustand		in Bearbeitung
		vorgelegt
	x	fertig gestellt

## Inhaltsverzeichnis

1 Einleitung: 2-Faktor-Authentifizierung.....	3
2 Vorbereitungen.....	3
2.1 Aktivierung der Funktion OTP in i-mpuls JMD.....	3
2.2 Installation einer Authenticator-App.....	3
3 Initialisierung.....	4
3.1 Mit gültigem Funktionszertifikat.....	4
3.2 Ohne gültiges Funktionszertifikat.....	5
4 Zweiten Faktor OTP setzen.....	6
4.1 Für sich selbst.....	6
4.2 Für andere.....	7
5 Tägliche Arbeit: Login mit OTP.....	8
6 Support und Hilfen.....	8

## **1 Einleitung: 2-Faktor-Authentifizierung**

I-mpuls JMD setzt von Beginn an auf eine 2-Faktor-Authentifizierung: Neben der Anmeldekennung sind zwei Faktoren zur Authentifizierung notwendig:

- Etwas, dass man weiß (das Passwort) und
- etwas, dass man besitzt.

Besitz war bisher das Funktionszertifikat (für den gesamten JMD Träger); seit Oktober 2025 kann dies nun auch das initiale Geheimnis für zeit-basierte Einmalpassworte (time-base one-time passwords, TOTP oder kurz OTP) sein. Diese sind individuell pro Person.

Die Benutzung erfordert einen Passwort-Generator, meist eine Authenticator-App. Bei der Anmeldung an i-mpuls JMD wird dann neben Anmeldekennung und Passwort noch ein Einmalpasswort (OTP) als sechsstelliger Code abgefragt. Dieser wird durch die App generiert.

## **2 Vorbereitungen**

Zur Nutzung des OTP Verfahrens benötigen sie einen aktuellen und sicherheits-gepflegten Browser (Edge, Firefox oder Chrome) sowie ein mobiles Endgerät.

### **2.1 Aktivierung der Funktion OTP in i-mpuls JMD**

Für den Zugang zu i-mpuls JMD ist für jeden JMD Träger bereits aus dem bisherigen Verfahren „Funktionszertifikat“ eine verantwortliche Person festgelegt. Im Zuge der Erneuerung der zweiten Faktoren im Herbst 2025 wurde das Interesse an OTP abgefragt und entsprechend eingerichtet. Die verantwortlichen Personen werden für die weiteren Schritte angeschrieben.

Wenn Sie zusätzlich Interesse an der Nutzung von OTP haben, treten Sie bitte mit dem Servicebüro JMD in Kontakt.

### **2.2 Installation einer Authenticator-App**

Installieren Sie eine Authenticator-App auf ihrem mobilen Endgerät. Getestet haben wir mit Microsoft Authenticator und Google Authenticator, die in den App-Stores für Ihr Mobiltelefon verfügbar sind. Eine Open Source Alternative wäre z. B. FreeOTP von RedHat.

## 3 Initialisierung

### 3.1 Mit gültigem Funktionszertifikat

Sie haben noch Zugang zur i-mpuls JMD Anwendung - Dann können Sie nach der Freischaltung direkt mit der Initialisierung für die wichtigsten Zugänge (initiale Anmeldekennung (adm) und administrative Konten) starten:

1. Rufen Sie die i-mpuls JMD Startseite auf:  
<https://www.impuls-jmd.de>  
und
2. melden Sie sich mit dem Anmeldekonto „adm“ an.  
Sollte Ihnen das Passwort nicht (mehr) bekannt sein, nutzen Sie bitte einen anderen administrativen Account.
3. Öffnen Sie das Benutzerkonto, rechts oben neben dem Abmeldeknopf: Person-Icon und „adm (initiale Anmeldekennung)“ bzw. „Administration“
4. Wählen Sie neben der Überschrift „Mein Konto“ das QR-Code-Icon  (Titel: „Zweiter Faktor“) und
5. auf der folgende Seite „Zweiten Faktor setzen“.
6. Scannen Sie den QR-Code umgehend mit Ihrer Authenticator-App, drucken Sie die Seite mit der Druckfunktion des Browsers und verwahren Sie diese sicher.

Damit ist der initiale Zweite Faktor für das adm-Konto gesetzt und Sie verfügen über eine physische Sicherung. Kehren Sie zu den Kontoeinstellungen zurück.

Sie können nun für weitere von Ihnen genutzte Konten direkt im Menü „Administration - Benutzerkonto“ ebenfalls einen zweiten Faktor setzen (der ebenfalls gesichert werden muss) oder sich nun abmelden.

Kolleginnen und Kollegen, die ebenfalls mit i-mpuls JMD arbeiten, können wie unter Abschnitt 4 beschrieben vorgehen.

### **3.2 Ohne gültiges Funktionszertifikat**

Vorab:

- 1.** Bitte melden Sie sich bei Bedarf beim Servicebüro JMD, wenn Sie bei Ihrem Träger für die Zugänge zu i-mpuls JMD zuständig sind.
- 2.** Sie benötigen das gültige Kennwort für die initiale Anmeldekennung „adm“. Fordern Sie bitte zusätzlich über das Servicebüro ein neues Kennwort an, wenn dies Kennwort nicht (mehr) bekannt ist.
- 3.** Anschließend erhalten Sie einen Brief mit einem initialen QR-Code.
- 4.** Installieren Sie auf Ihrem Mobiltelefon eine Authenticator-App (s. Abschnitt 2.2).

Wenn Brief und Authenticator-App vorhanden sind:

- 5.** Scannen Sie den QR-Code mit Ihrer Authenticator-App ein.  
Vergeben Sie ggf. eine geeignete Bezeichnung.
- 6.** Rufen Sie die OTP-Startseite von i-mpuls JMD auf:  
<https://otp.impuls-jmd.de>
- 7.** Geben Sie Anmeldekennung „adm“ und Passwort ein und
- 8.** suchen Sie Ihren JMD Standort durch Eingabe des Namens in das JMD-Feld.  
Klicken Sie zur Auswahl auf den gewünschten Treffer.
- 9.** Klicken Sie „Anmelden“
- 10.** Öffnen Sie Ihre Authenticator-App auf dem Mobiltelefon:
  - wählen Sie die passende Anmeldekennung „adm“
  - geben Sie den angezeigten 6-stelligen Code in das OTP-Feld ein.  
Hinweis: Der Code ist maximal 30 Sekunden gültig und aktualisiert sich selbstständig.
- 11.** Klicken Sie „Anmelden“

Damit sind Sie an der i-mpuls JMD Anwendung angemeldet.

Das OTP muss nur einmal täglich eingegeben werden.

## 4 Zweiten Faktor OTP setzen

Solange das aktuelle Funktionszertifikat noch gültig ist, könnten Anwender\*innen selbst über ihr Benutzerkonto-Menü den initialen zweiten Faktoren setzen. Das Vorgehen entspricht den unter 4.1 beschriebenen Schritten. Bitte geben Sie die Informationen entsprechend weiter.

Wenn Sie entsprechend Abschnitt 3 als adm bzw. Administration bereits einen Zugang via OTP haben (oder noch das Zertifikat nutzen) können sie auch für andere Anwender\*innen in Ihrem Jugendmigrationsdienst den initialen zweiten Faktor setzen.

### 4.1 Für sich selbst

Sie können den zweiten Faktor **einmalig** für sich selbst setzen!

1. Rufen Sie die i-mpuls JMD Startseite auf:

<https://www.impuls-jmd.de>

und

2. melden Sie sich mit Ihrer Anmeldekennung und Passwort an.
3. Öffnen Sie das Benutzerkonto, rechts oben neben dem Abmeldeknopf:  
Person-Icon und „Bearbeitung“ bzw. „Administration“.
4. Wählen Sie neben der Überschrift „Mein Konto“ das QR-Code-Icon  (Titel: „Zweiter Faktor“) und
5. auf der folgende Seite „Zweiten Faktor setzen“.
6. Scannen Sie den QR-Code umgehend mit Ihrer Authenticator-App.

Eine zusätzliche Sicherung ist nicht notwendig:

- Beim Wechsel des mobilen Endgerätes oder Nutzung mehrerer Geräte können Sie den zweiten Faktor mit den Funktionen Ihrer Authenticator-App übertragen.
- Bei Verlust des mobilen Endgerätes muss der zweite Faktor aus Sicherheitsgründen durch die Administration neu gesetzt werden!

Sie können sich nun wie in Abschnitt 5 beschrieben anmelden, unter

<https://otp.impuls-jmd.de>

## 4.2 Für andere

Die folgenden Schritte können Sie mit einem administrativen Konto ausführen, entweder mit einem noch gültigen Funktionszertifikat oder mittel zweitem Faktor OTP. Mit den Schritten zur Anmeldung sind Sie bereits vertraut:

1. Rufen Sie die i-mpuls JMD Startseite auf:

<https://www.impuls-jmd.de>

oder

<https://otp.impuls-jmd.de>

und

2. melden Sie sich entsprechend des gewählten Verfahren mit ihrer Anmeldekennung für ein administratives Konto an.
3. Wählen Sie im Menü „Administration“ den Punkt „Benutzerkonto“ und wählen Sie aus der Liste der Benutzer\*innen das Konto, für das Sie einen zweiten Faktor setzen wollen.
4. Klicken Sie auf das „Bearbeiten“-Icon  und auf der folgenden Seite das QR-Code-Icon  (Titel: „Zweiter Faktor“).
5. auf der folgende Seite „Zweiten Faktor setzen“.
6. Es wird geprüft, ob für das gewählte Konto bereits ein zweiter Faktor konfiguriert wurde und ggf. entsprechend darauf hingewiesen. Sie haben die Berechtigungen, den zweiten Faktor neu zu setzen, müssen dies aber explizit bestätigen: Checkbox „Trotzdem zurücksetzen“  
Klicken Sie abschließend „Ja“
7. Es wird ein zweiter Faktor gesetzt und als QR-Code angezeigt.

Bitte sichern Sie diesen sofort, indem Sie

- den QR-Code direkt von der berechtigten Person scannen lassen oder
- die Seite ausdrucken / als PDF speichern und sicher weitergeben oder
- den QR-Code in die Zwischenablage kopieren und in internen Dokumenten weiter verarbeiten und sicher weitergeben.

## 5 Tägliche Arbeit: Login mit OTP

Für die Nutzung des zweiten Faktors:

1. Rufen Sie die OTP-Startseite von i-mpuls JMD auf:  
<https://otp.impuls-jmd.de>
2. Geben Sie Anmeldekennung und Passwort wie gewohnt ein und
3. suchen Sie Ihren JMD Standort durch Eingabe des Namens in das JMD-Feld.  
Klicken Sie zur Auswahl auf den gewünschten Treffer.
4. Klicken Sie „Anmelden“
5. Öffnen Sie Ihre Authenticator-App, wählen Sie die passende Anmeldekennung und geben Sie den angezeigten 6-stelligen Code in das OTP-Feld ein.  
Hinweis: Der Code ist maximal 30 Sekunden gültig und aktualisiert sich dann selbstständig.
6. Klicken Sie „Anmelden“

Damit sind Sie an der i-mpuls JMD Anwendung angemeldet.

Der ausgewählte JMD-Standort bleibt dabei bis zu einer erneuten Suche voreingestellt, das OTP muss bei erneuter Anmeldung am selben Tag nicht noch einmal eingegeben werden.

## 6 Support und Hilfen

Kontaktieren Sie uns per E-Mail

[jmd@support.intevation.de](mailto:jmd@support.intevation.de)

wenn Fragen oder Probleme mit dem Verfahren „Authentifizierung mit OTP“ haben.

Bitte haben Sie Verständnis, dass wir keine Unterstützung zu den unterschiedlichen Authenticator-Apps geben können.