



E-Justiz
Koordinierungsstelle
Europa

Handbuch – Registrierung zur JUDEX- Benutzerverwaltung (für Haupt- und Behördenadministratoren)

Stand: 07/2026

Inhalt

Einleitung.....	3
Meldung an die zuständigen Stellen.....	4
Ablauf der Freischaltung.....	4
a. Nutzung einer Smartphone-App	6
b. Nutzung der Desktop-App.....	6
Abschluss der Registrierung.....	8

Einleitung

Das **JUstice Digital EXchange** System (JUDEX oder auch Referenzimplementierung, vormals eEDES genannt) ist eine von der Europäischen Kommission entwickelte und von IT.NRW bereitgestellte Browseranwendung, die es ermöglicht, digital, sicher und schnell über das e-CODEX System bei anderen Mitgliedstaaten der Europäischen Union um Rechtshilfe im Zivil- und Strafbereich zu ersuchen (z.B. Europäische Ermittlungsanordnungen oder Zustellungs- und Beweisaufnahmeersuchen).

JUDEX ist dabei kein eigenständiges e-Akten-System.

Für die Nutzung von JUDEX ist eine Registrierung der einzelnen Nutzenden und Erteilung ihrer Berechtigungen erforderlich. Damit wird sichergestellt, dass nur auf Daten, für die die entsprechende Berechtigung vorliegt, zugegriffen werden kann.

Für die Verwaltung der Zugänge wurden zwei Administrationsebenen eingerichtet:

- Die Ebene der sog. **Hauptadministratoren** auf Landes- bzw. Bundesebene und
- die Ebene der sog. **Behördenadministratoren** auf Behördenebenen innerhalb der Länder- und Bundesbehörden.

Die Hauptadministratoren sind für die Anlage und Verwaltung der Behördenadministratoren ihres Landes oder auf Bundesebene zuständig. Die Behördenadministratoren wiederum verwalten die Nutzenden der ihnen zugeordneten Behörde(n). Sie haben die Möglichkeit, Nutzerinnen und Nutzer in den ihnen zugewiesenen Behörden anzulegen, ihre Rollen anzupassen, zu löschen oder die Kennwörter zurückzusetzen.

Für Haupt- und Behördenadministratoren ist eine 2-Faktor-Authentifizierung notwendig.

Gegenstand dieses Handbuchs ist der vorgelagerte **Registrierungsvorgang** für die JUDEX Benutzerverwaltung.

Meldung an die zuständigen Stellen

Die Registrierung und Verwaltung aller Hauptadministratoren der Länder und des Bundes erfolgt durch die am Ministerium der Justiz NRW angesiedelten E-Justiz Koordinierungsstelle Europa (EKE). Die Registrierung und Verwaltung aller Behördenadministratoren erfolgt sodann über die zuständigen Hauptadministratoren. Neue Kennungen oder Anpassungen können die Hauptadministratoren bei der EKE und die Behördenadministratoren bei ihren jeweiligen Hauptadministratoren anfragen (z.B. vergessenes Kennwort, Änderung des zweiten Faktors, Zuständigkeit für Behörden).

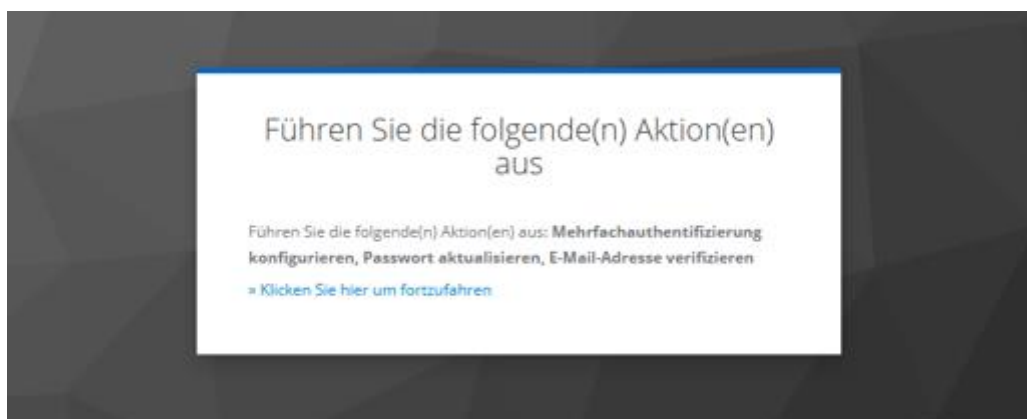
Ablauf der Freischaltung

Nach entsprechender Eintragung erhalten Sie eine E-Mail von prod-auth@no-reply.nrw.de für die Anmeldung zur Benutzerverwaltung.

Klicken Sie hier auf „Link zur Aktualisierung/Vervollständigung“, um den Prozess zu starten. Bitte beachten Sie, dass die Gültigkeit des Links zeitlich begrenzt ist. Kann eine Registrierung innerhalb der in der E-Mail angegebenen Zeit nicht erfolgen, muss der Vorgang erneut angestoßen werden.

Einen neuen Link erhalten die Hauptadministratoren über die EKE und die Behördenadministratoren über ihre zuständigen Hauptadministratoren.

Nach dem Klick auf den Link erscheint die nachfolgende Ansicht im Browser.



Klicken Sie hier bitte ebenfalls auf den Link „Klicken Sie hier um fortzufahren“.

Anschließend werden Sie zur Einrichtung eines zweiten Faktors aufgefordert. Diesen werden Sie aus Sicherheitsgründen bei jeder künftigen Anmeldung in der Benutzerverwaltung benötigen. Mögliche Anwendungen sind die Smartphone-Applikationen FreeOTP, Google Authenticator und Microsoft Authenticator.

Alternativ kann eine von IT.NRW entwickelte Desktop-Anwendung verwendet werden, die hier abgerufen werden kann:

<https://membox.nrw.de/index.php/s/1xAWSOoZylvjkao> (Kennwort: 2FA).

Ebenso ist die Nutzung von Keepass möglich.

Bitte halten Sie in Zweifelsfällen vor der Auswahl und Installation immer Rücksprache mit Ihren lokalen IT-Verantwortlichen.

Weiterhin beachten Sie bitte, dass im Falle der Nutzung der von IT.NRW entwickelten Desktop-App weder die EKE noch IT.NRW Support hierfür leisten.

Mehrfachauthentifizierung konfigurieren

 **Sie müssen eine Mehrfachauthentifizierung einrichten, um das Benutzerkonto zu aktivieren.**

1. Installieren Sie eine der folgenden Applikationen auf Ihrem Smartphone:
FreeOTP
Google Authenticator
Microsoft Authenticator
2. Öffnen Sie die Applikation und scannen Sie den QR-Code:

[Sie können den QR-Code nicht scannen?](#)
3. Geben Sie den von der Applikation generierten One-time Code ein und klicken Sie auf Absenden.
Geben Sie einen Gerätenamen an, um die Verwaltung Ihrer OTP-Geräte zu erleichtern.

One-time Code *

Gerätename

☒ Von anderen Geräten abmelden

Absenden

a. Nutzung einer Smartphone-App

Sofern Sie eine Smartphone-Anwendung nutzen, müssen Sie den QR-Code innerhalb der Anwendung abschnappen. Nach Einrichtung sollte Ihnen eine sechsstellige Zahl angezeigt werden. Diese muss in das Feld „One-time Code“ eingegeben werden.

Im Feld „Gerätename“ sollte eine Bezeichnung eingegeben werden, die es Ihnen erlaubt, sich an Ihren zweiten Faktor zu erinnern (z.B. „Dienst-iPhone“ etc.).

Es ist möglich, falls gewünscht, mehr als einen zweiten Faktor zu hinterlegen. Hierfür ist aber erforderlich, dass der Prozess erneut angestoßen wird.

b. Nutzung der Desktop-App

Entscheiden Sie sich zur Nutzung einer Desktop-App (von IT.NRW oder Keepass), klicken Sie auf „Sie können den QR-Code nicht scannen?“.

Mehrfachauthentifizierung konfigurieren

**Sie müssen eine Mehrfachauthentifizierung einrichten, um das Benutzerkonto zu aktivieren.**

1. Installieren Sie eine der folgenden Applikationen auf Ihrem Smartphone:
FreeOTP
Google Authenticator
Microsoft Authenticator
2. Öffnen Sie die Applikation und scannen Sie den QR-Code:

Sie können den QR-Code nicht scannen?
3. Geben Sie den von der Applikation generierten One-time Code ein und klicken Sie auf Absenden.
Geben Sie einen Gerätenamen an, um die Verwaltung Ihrer OTP-Geräte zu erleichtern.

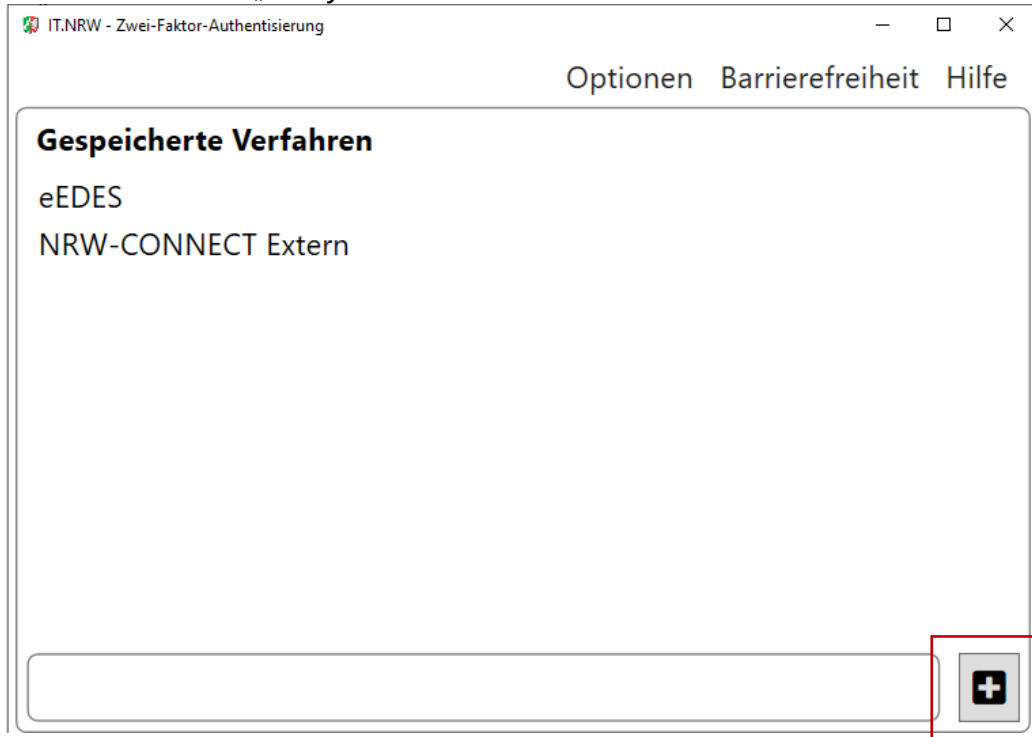
One-time Code *

Gerätename

☒ Von anderen Geräten abmelden

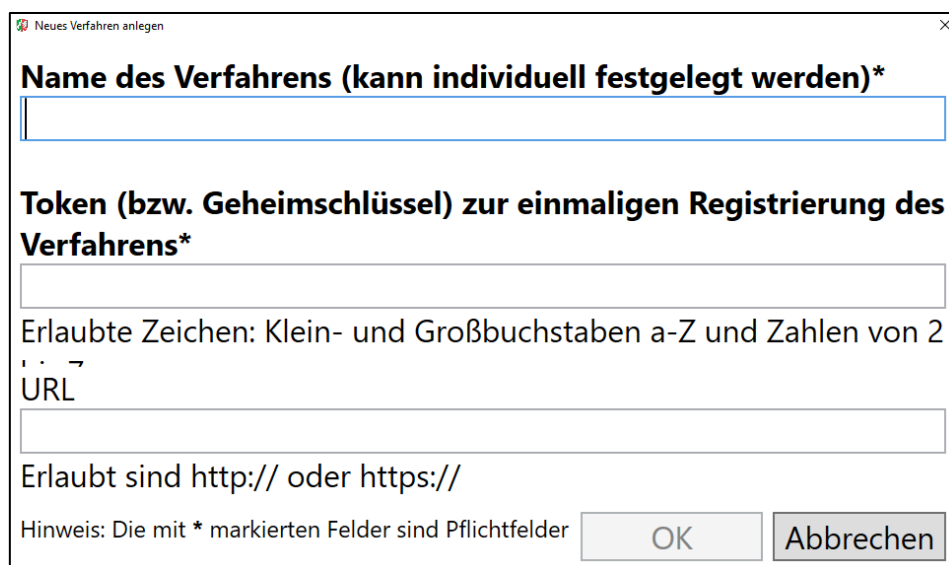
Absenden

Ihnen wird sodann ein längerer Token/Geheimschlüssel angezeigt, den Sie in der Desktop-App eingeben müssen. Klicken Sie dafür in der Desktop-App nach Eingabe des Kennworts auf das „+“-Symbol in der unteren rechten Ecke.



Anschließend können Sie den Namen des Verfahrens (frei wählbar) und den bei der Registrierung angezeigten Token eingeben.

Wichtig: Der Token muss ohne Leerzeichen eingegeben werden. Das Feld URL kann frei bleiben.



Neues Verfahren anlegen

Name des Verfahrens (kann individuell festgelegt werden)*

Token (bzw. Geheimschlüssel) zur einmaligen Registrierung des Verfahrens*

Erlaubte Zeichen: Klein- und Großbuchstaben a-Z und Zahlen von 2

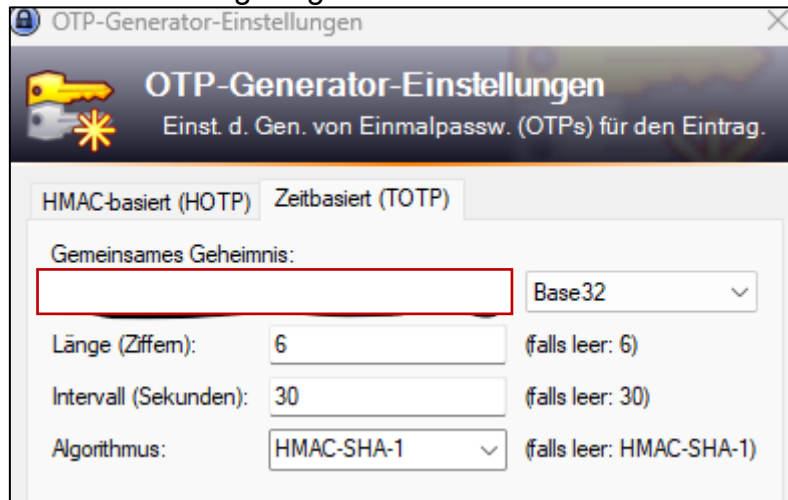
URL

Erlaubt sind http:// oder https://

Hinweis: Die mit * markierten Felder sind Pflichtfelder

OK Abbrechen

Sofern Keepass genutzt wird muss der Token (ebenfalls ohne Leerzeichen) in das Feld „gemeinsames Geheimnis“ eingetragen werden.



Abschluss der Registrierung

Wurde der zweite Faktor erfolgreich eingerichtet, werden Sie aufgefordert, ein neues Passwort zu vergeben. Ist auch dies erfolgt, gelangen Sie zur Login-Seite und können die Benutzerverwaltung aufrufen.

Bitte wenden Sie sich bei Problemen mit der Einrichtung der 2-Faktor-Authentifizierung direkt an Ihren lokalen IT-Service. IT.NRW und die EKE können diesbezüglich keinen Support leisten.