

SAFE Zugangsadministration

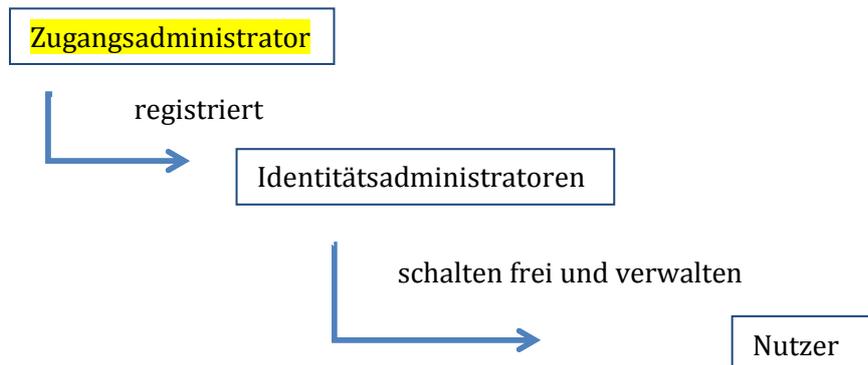
Registrierung und Verwaltung von Identitätsadministratoren

Leitfaden

für die Web-Anwendung für die Zugangsadministration

Version 1.0 (gültig ab SAFE V 1.8)

Die Verwaltung von Nutzern im SAFE-System erfolgt, wie in der Abbildung beschrieben, dreistufig. Die Nutzer registrieren sich immer selbst. Sie werden dann von einem Identitätsadministrator freigeschaltet und verwaltet. Die Identitätsadministratoren wiederum werden von Zugangsadministratoren freigeschaltet und verwaltet.



Für die Zugangsadministration steht eine Web-Anwendung zur Verfügung, die bei der Bundesnotarkammer betrieben wird. Dieser Leitfaden enthält Hinweise zur Nutzung dieser Web-Anwendung.

(Die Registrierung von Nutzern und die Freischaltung und Verwaltung von Nutzern erfolgen jeweils über separate Web-Anwendungen.)

Zugang zur Web-Anwendung für Zugangsadministratoren:

<https://safe.safe-justiz.de/safe-access-admin/>

Zugang zur Testumgebung:

Inhaltsverzeichnis

SAFE Zugangsadministration	1
1 Allgemeine Grundsätze	3
1.1 Einschränkung der Rechte der Zugangsadministratoren.....	3
1.2 Einschränkung der Rechte der Identitätsadministratoren.....	3
1.2.1 Einschränkung auf bestimmte Nutzergruppe.....	3
1.2.2 Einschränkung auf bestimmte Rollen.....	3
2 Anmeldung	4
2.1 Registrierung als Zugangsadministrator.....	5
2.2 Anmeldung an der Anwendung.....	5
3 Nutzungshinweise	6
3.1 Identitätsadministrator bearbeiten.....	6
3.1.1 Identitätsadministrator suchen.....	6
3.1.2 Persönliche Daten.....	8
3.1.3 Rechte für bestimmte Rollen vergeben.....	8
3.1.4 Eigenschaftseinschränkungen.....	11
3.2 Identitätsadministratoren löschen	13
3.3 Abmelden.....	15
3.4 Benutzerkonto löschen	14
4 Vorgaben für die Registrierung von Identitätsadministratoren für die Rollentypen	
ZenVG und JP-VP	15
5 Support.....	16
6 Anlagen	17
6.1 Rollen JP-VP und ZenVG	17
6.2 Rollen BNotK-ZTR.....	20

1 Allgemeine Grundsätze

Bei der Registrierung und Verwaltung von Identitätsadministratoren sind die in den nächsten Abschnitten beschriebenen Grundsätze zu beachten:

1.1 Einschränkung der Rechte der Zugangsadministratoren

SAFE-Identitäten haben in ihrer Rolle als Zugangsadministratoren keinen Zugriff auf andere SAFE-Identitäten (Nutzer). Ihre Aufgabe besteht einzig und allein in der Registrierung und Verwaltung von Identitätsadministratoren.

Zugangsadministratoren sind nur für ein bestimmtes Bundesland (oder den Bund) zuständig. Sie können nur für dieses Bundesland Identitätsadministratoren registrieren und verwalten. Sie haben weder lesenden noch schreibenden Zugriff auf Identitätsadministratoren anderer Bundesländer.

1.2 Einschränkung der Rechte der Identitätsadministratoren

1.2.1 Einschränkung auf bestimmte Nutzergruppe

Ein Zugangsadministrator kann die Administratorenrechte der Identitätsadministratoren, die er verwaltet, auf Nutzer mit bestimmten Eigenschaften (Attribute) beschränken. Hierfür wird bei der Freischaltung ein bestimmtes Attribut (z.B. „Justiz“ bei „Kennziffer-Präfix“) eingetragen. Der Identitätsadministrator kann dann nur solche Nutzer verwalten, die im Feld „Kennziffer-Präfix“ „Justiz“ eingetragen haben.

1.2.2 Einschränkung auf bestimmte Rollen

Ein Zugangsadministrator muss die Administratorenrechte der Identitätsadministratoren für bestimmte SAFE-Rollen freischalten.

Die SAFE-Rolle setzt sich zusammen aus dem „Rollentyp“ und dem „Rollenwert“.

- Der Rollentyp gibt die Anwendung an, auf die sich die Rolle bezieht (z.B. ZenVG).
- Der Rollenwert beschreibt die Rechtegruppen innerhalb dieses Rollentyps (z.B. ZenVG_GV).

Jede Identität kann mehrere Rollentypen und zu jedem Rollentyp einen oder mehrere Rollenwerte innehaben. Es ist möglich, dass ein Rollentyp für mehrere Anwendungen genutzt wird.

Jedem Identitätsadministrator **muss** mindestens eine bestimmte Rolle (Rollentyp + Rollenwert), die er verwalten darf, zugeordnet werden. Ihm können beliebig viele Rollen zugeordnet werden.

Der Identitätsadministrator kann nur solche Nutzer finden und verwalten, die über den/die entsprechende/n Rollentyp/en und Rollenwerte verfügen.

2 Anmeldung

Die Anmeldung ist nur mit Hardwarezertifikat über die sogenannte Clientauthentifizierung möglich.

Um das Hardwarezertifikat für die Anmeldung verwenden zu können, müssen folgende Anforderungen enthalten sein:

keyUsage = digitalSignature, keyEncipherment

extendedKeyUsage = clientAuth

Diese Funktionalitäten sind beispielsweise integriert in den Signaturkarten der TeleSec - Trust Center der Deutschen Telekom AG, DGN - Deutsches Gesundheitsnetz, Trustcenter der Bundesnotarkammer (einschließlich beA Karte), D-Trust Trustcenter der Bundesdruckerei, Bayern PKI sowie der DATEV Signaturkarte.

Die Anmeldung an der Web-Anwendung setzt voraus, dass der Zugangsadministrator im SAFE-System als solcher registriert ist.

Hierfür muss sich der Zugangsadministrator zunächst selbst über die SAFE-Registrierungsanwendung registrieren. Dies gilt sowohl für das SAFE-Echtsystem <https://safe.safe-justiz.de/safe-registration-client/> als auch für das SAFE-Testsystem <https://safetest.safe-justiz.de/safe-registration-client/>.

2.1 Registrierung als Zugangsadministrator

Bei der Registrierung muss er den Rollentyp „SAFE – Administrationsrollen für SAFE“ und den Rollenwert „Zugangsadmin“ auswählen - siehe Abbildung Bildschirmausschnitt SAFE-Registrierungsanwendung:

Neuen Rollentyp hinzufügen



Rollentyp auswählen
SAFE - Administrationsrollen für SAFE

Rollenwert auswählen
Ident-Admin
Zugangsadmin

Gewählte Rollenwerte

+ Rollentyp hinzufügen Abbrechen

Zwingend anzugeben sind die Pflichtfelder „Name“, „Vorname“, „Bundesland“ und „E-Mail-Adresse“. Zudem muss der öffentliche Schlüssel des Hardwarezertifikats hochgeladen werden. Einzelheiten sind im Leitfaden für die Registrierungsanwendung aufgeführt. Nach Abschluss der Registrierung wird eine Nutzer-ID angezeigt. Diese muss notiert werden.

Die Freischaltung der Zugangsadministratoren wird von der BLK-AG IT-Standards veranlasst. Bitte senden Sie die Nutzer-ID und Name, Vorname, Bundesland und E-Mail-Adresse des Zugangsadministrators mit der Bitte um Freischaltung an die Koordinatorin Daniela Freiheit, freiheit@it-justiz.de.

2.2 Anmeldung an der Anwendung

Die Anmeldung als Zugangsadministrator ist nur mittels Clientauthentifizierung per Hardwarezertifikat (SmartCard) möglich.

Für eine erfolgreiche Anmeldung muss Ihr Hardwarezertifikat im Browser hinterlegt sein.

Für die Einbindung eines Hardwarezertifikates (Kryptographie-Modul) im Browser gibt es keine allgemeingültige Beschreibung. Nutzen Sie bitte die Anleitung Ihres Kartenausstellers. Sie benötigen auf jeden Fall eine Treibersoftware.

Nach der automatischen Anmeldung gelangen Sie zur Hauptseite der Anwendung.

3 Nutzungshinweise

3.1 Identitätsadministrator bearbeiten

3.1.1 Identitätsadministrator suchen

Über die Suchmaske können die Identitätsadministratoren, die freigeschaltet oder bearbeitet werden sollen, gefunden werden.

The screenshot shows the user search interface in the SAFE system. At the top, there is a navigation bar with the SAFE logo and the text 'BEARBEITUNG / SUCHE'. Below this, there are tabs for 'Suche', 'Persönliche Daten', 'Rolleneinschränkungen', and 'Eigenschaftseinschränkungen'. The main area is divided into two columns: 'Nutzerdaten' and 'Persönliche Daten'. The 'Nutzerdaten' column contains input fields for 'Nutzer-ID', 'Benutzername', 'E-Mail', and 'Organisation', along with a radio button for 'Nur Nutzer mit unbearbeiteten Rollen'. The 'Persönliche Daten' column contains input fields for 'Name', 'Vorname', and 'Telefon'. A 'Suche' button is located at the bottom right of the form.

In jedem Suchfeld können Sie den gesamten Suchbegriff oder einen Teil eingeben. Geben Sie z.B. unter Name „Mayer“ ein, so werden alle Identitätsadministratoren gefunden, für die Sie berechtigt sind und deren Name „Mayer“ enthält. Also Mayer, Mayerhöffer, Müller-Mayer, etc... Groß- und Kleinschreibung hat auf die Suche keine Auswirkung. Die Suche wird ausgelöst, wenn Sie auf *Suche* klicken oder im Suchfeld die Eingabetaste (Enter) drücken.

Wenn Sie eine Übersicht über alle Nutzer erhalten möchten, klicken Sie ohne die Eingabe eines Suchbegriffs auf *Suche* oder Enter. Wird die Option „*Nur Nutzer mit unbearbeiteten Rollen*“ angewählt, so erscheinen nur die Identitätsadministratoren, die noch nicht freigeschaltet sind.

Das Ergebnis der Suche wird tabellarisch unter den Eingabefeldern angezeigt. Rot markierte Zeilen kennzeichnen Identitätsadministratoren, die noch nicht freigeschaltet sind.

Arbeitstypen / Identitäts in der Suche

Logo: Westfälische Wilhelms-Universität Münster

SAFE

BEARBEITUNG / SUCHE

Suche | Persönliche Daten | Rolleneinschränkungen | Eigenschaftseinschränkungen

Nutzerdaten

Nutzer-ID:

Benutzersname:

Adressdaten

E-Mail:

Organisation:

Nur Nutzer mit unbeschränkter Rolle:

Persönliche Daten

Name:

Vorname:

Kontaktdaten

Telefon:

Aktionen	Nutzer-ID	Benutzersname	Name	Vorname	Organisation	Email	Telefon
	safe_rg_dev-1447232024557-011379333	Flamena_0_111	Flamena	Dirnbrove	Organisationstest	flamena.dirnbrove@westfälischer.com	+491806545800
	safe_rg_dev-1447153230891-011379253	SAFE-618-TestUser	Test	User	WPS		
	safe_rg_dev-1447083363484-011379130	svetIn	Svetlin	Saev	Madame Toteauks Berlin	svetIn.saev@westfälischer.com	+491806545800
	safe_rg_dev-1447083363366-011379109	svetID	Svetlin	Saev	Madame Toteauks Berlin	svetIn.saev@westfälischer.com	+491806545800
	safe_rg_dev-1446048935063-011377477	idadmin@test					

1/1 Einträge

© 2024 SHAPSHOT | Hilfe | Impressum | Kontakt | Benutzerkonto löschen

Am unteren Ende der Tabelle wird die Gesamtzahl der gefundenen Einträge dargestellt. Besitzt eine Suche mehr als 50 Treffer, so werden die ersten 50 Datensätze angezeigt. Die restlichen Datensätze können über die Seitenzahlen oder die Navigationspfeile aufgerufen werden. Ein einfacher Navigationspfeil springt dabei zur nächsten oder vorgehenden Seite. Doppelte Navigationspfeile springen zur ersten oder letzten Seite.



1 - 47 von 47 Einträgen

Über das Bearbeiten-Symbol am Anfang jeder Zeile gelangen Sie zu den Detailangaben des jeweiligen Identitätsadministrators. Diese sind in die Reiter „Persönliche Daten“, „Rolleneinschränkung“ und „Eigenschaftseinschränkung“ unterteilt.

3.1.2 Persönliche Daten

Benutzername: Testuser

Vornamen: Max

Name: Mustermann

E-Mail: max@muster.de

Telefon: Telefon

Organisation: Behördenbezeichnung

Benutzernamen können in jeder SAFE-Instanz nur ein einziges Mal verwendet werden. Er muss mindestens fünf Zeichen lang sein.

Speichern Weiter > v1.11.7-SNAPSHOT Hilfe Impressum Benutzerkonto

Etwaige Änderungen können Sie direkt mit einem Klick auf **Speichern** übernommen oder Sie wechseln mit einem Klick auf *Weiter* zur Registerkarte *Rolleneinschränkungen*.

3.1.3 Rechte für bestimmte Rollen vergeben

Hier können Sie Administratorenrechte für bestimmte SAFE-Rollen freischalten (siehe auch unter 1.2.2). Der Identitätsadministrator kann später nur auf diejenigen Nutzer zugreifen, die mindestens einen dieser Rollenwerte innehaben. Er kann auch nur diese Rollen für Nutzer freischalten.

Einzelheiten zu den SAFE-Rollentypen und Rollenwerte finden Sie in der Anlage.

Bitte beachten Sie, dass die Rollenwerte egvp_anonym und ZenVG_Rollenabfrage **nicht** zugeordnet werden dürfen. Es handelt sich bei diesen Rollen um technische Rollen, die keinerlei Berechtigungen für Nutzer abbilden, sondern nur von speziellen Clients bzw. Fachanwendungen benötigt werden.

Suche Persönliche Daten **Rolleneinschränkungen** Eigenschaftseinschränkungen

+ Weiteren Rollentyp hinzufügen

Hier können Sie neue Rollentypen und -werte auswählen und hinzufügen. Es muss mindestens eine Rolle gesetzt sein.

Identitätsadministrationsrechte: ⓘ **freischalten** **verweigern**

Mit Hilfe der Steuerungselemente können Sie eine Identitätsadministrationsanfrage wahlweise freischalten oder ablehnen.

Über den Button „Weiteren Rollentyp hinzufügen“ räumen Sie dem Identitätsadministrator Administrationsrechte für die gewünschten Rollen ein.

Klicken Sie dafür auf *Weitere Rollentypen hinzufügen*. Damit öffnet sich ein neues Formular, mit dessen Hilfe Sie einen Rollentyp und Rollenwerte auswählen können.

Neuen Rollentyp hinzufügen

Rollentyp auswählen

ZenVG - Zentrale Vollstreckungsgerichte

Rollenwert auswählen

GV
Hoster
InsO
TechAdmin-Land
Test
VollG
VVB-EA
VVB-VV
ZenVG-Sachbearbeitung
ZenVG_Rollenabfrage

Gewählte Rollenwerte

+ Rollentyp hinzufügen **Abbrechen**

Wählen Sie in dem obersten Auswahlfeld einen Rollentyp aus.

Sobald Sie einen Rollentyp gewählt haben, werden Ihnen die zu dem Rollentyp verfügbaren Rollenwerte angezeigt. Sie wählen einen Rollenwert aus, in dem Sie auf den jeweiligen Rollenwert klicken. Nach dem Anklicken wird dieser Wert in die rechte Spalte verschoben. Sie können so mehrere Rollenwerte auswählen.

Eine Auswahl zurücksetzen können Sie, indem Sie in der rechten Spalte, den jeweiligen Rollenwert selektieren. Somit wird der Wert wieder in der linken Spalte (*Rollenwert auswählen*) hinzugefügt.

Wenn Sie Ihre Auswahl beendet haben, bestätigen Sie diese indem Sie auf *Rollentyp hinzufügen* klicken.

Der Button Rollentyp hinzufügen ist erst aktiviert und kann angeklickt werden, sobald Sie einen Rollentyp und mindestens einen Rollenwert ausgewählt haben.

Nach dem Klick auf *Rollentyp hinzufügen* schließt sich das Formular. Der Rollentyp und die ausgewählten Rollenwerte werden tabellarisch angezeigt:



Abbildung 1: Anzeigen des ausgewählten Rollentyps und -werte

Möchten Sie einen Rollenwert löschen, so klicken Sie auf das Minus hinter dem jeweiligen Rollenwert. Nach einer Bestätigung wird diese Rolle gelöscht. Wenn nur ein Rollenwert für den Rollentyp gewählt wurde, so wird die ganze Zeile gelöscht. Wenn mehr als ein Rollenwert dem Rollentyp zugeordnet wurden, so wird lediglich dieser Rollenwert gelöscht.

Möchten Sie den gesamten Rollentyp aus Ihrer Auswahl löschen, so klicken Sie auf das Löschen-Symbol in der Spalte „Aktionen“. Möchten Sie die Zuordnung der Rollenwerte bearbeiten, so klicken Sie auf das Bearbeiten-Symbol in der Spalte „Aktionen“.

Sie können beliebig viele Rollentypen und Rollenwerte hinzufügen, in dem Sie auf den Button *Neuen Rollentyp hinzufügen* klicken. Beachten Sie, die Rollentypen, die Sie bereits ausgewählt haben, werden Ihnen nicht mehr zur Auswahl gestellt.

Der Identitätsadministrator muss dann noch über den Button „freischalten“ aktiviert werden. Nach der Aktivierung kann der Identitätsadministrator sofort seine Arbeit aufnehmen. Ein zusätzliches Speichern ist nicht erforderlich. Der Status der Freischaltung wird direkt nach dem Textfeld „Identitätsadministrationsrechte“ angezeigt. Es können folgende Status unterschieden werden:

 bestätigt

 in Bearbeitung

 abgelehnt

Wenn Sie Ihre Auswahl abgeschlossen haben und den Identitätsadministrator mit dem Button „Freischalten“ bestätigt haben, gehen Sie entweder über *Weiter* oder direkt auf die Registerkarte *Eigenschaftseinschränkungen*.

3.1.4 Eigenschaftseinschränkungen

Wie unter Abschnitt 1.2.1 beschrieben, können Sie unter der Registerkarte *Eigenschaftseinschränkungen* angeben, welche Nutzergruppen der Identitätsadministrator verwalten darf.

Suche | Persönliche Daten | Rolleneinschränkungen | **Eigenschaftseinschränkungen**

Nutzerdaten

Nutzer-ID:

OSG-Manager:

Gruppe:

Externe-ID:

Adressdaten

E-Mail:

Organisation:

Behördenbezeichnung:

Ort:

Bundesland:

Straße:

Hausnummer:

PLZ:

Land:

De-Mail:

Persönliche Daten

Name:

Vorname:

Anrede:

Titel:

Kontaktdaten

Mobiletelefon:

Telefon:

Fax:

Kennziffer-Präfix:

Kennziffer:

Pflichtfeld v1.8.7-SNAPS

Dabei ist die Einschränkung auf das Bundesland bereits vorbelegt und kann nicht durch Sie geändert werden.

Sie können über diese Einschränkung hinaus beispielsweise durch Angabe eines Kennziffer-Präfixes (Justiz, Finanzen, Zoll, Kommunen) erreichen, dass der Identitätsadministrator nur Nutzer, die das von Ihnen angegebene Kennziffer-Präfix bei der Registrierung eingetragen haben, sehen und verwalten darf.

Bitte beachten Sie, dass sichergestellt ist, dass die von Ihnen ausgewählten Daten von den Nutzern auch exakt in der gewählten Schreibweise angegeben werden! Andernfalls kann der Identitätsadministrator die Nutzer nicht finden.

Die Felder „Externe-ID“ und „Gruppe“ dürfen nicht zur Einschränkung von Rechten genutzt werden, da diese Attribute ausschließlich von speziellen Anwendungen genutzt werden.¹

Zur Bearbeitung der Eigenschaften können Sie während der Bearbeitung des Identitätsadministrators, mit einem Klick auf *Weiter* zu der Registerkarte *Eigenschaftseinschränkung* navigieren oder direkt die Registerkarte anklicken.

Bestätigen Sie die Änderungen mit einem Klick auf *Speichern*.

3.2 Identitätsadministratoren löschen

Um einen Identitätsadministrator zu löschen, klicken Sie in der Suchergebnisliste auf das *Löschen*-Symbol.

Aktionen	Nutzer-ID	Benutzername	Name	Vorname	Organisation	Email	Telefon
[edit] [delete]	safe_ng_dev-1446046915063-011377427	IdAdminTest					
[edit] [delete]	safe_ng_dev-1447252024557-011379353	Plamena_D_111	Plamena	Dimitrova	OrganisationTest	plamena.dimitrova@westermacher.com	+491806545800
[edit] [delete]	safe_ng_dev-1448091776956-011374254	IdentityAdmin		IdentityAdmin		milan.milakov@westermacher.com	
[edit] [delete]	safe_ng_dev-1443770619559-011374707	IdentityAdmin	Utats	IdentityAdmin	org	Plamena@test.com	434343
[edit] [delete]	safe_ng_dev-1444986375230-011376007	anagarkonermann	Anagar	Konermann		anagarkonermann@westermacher.com	
[edit] [delete]	safe_ng_dev-1442418025204-011373967	autoidentityAdmin1442417407545	Vornamen	Name	Behördenbezeichnung	testMail@mail.com	0712507123
[edit] [delete]	safe_ng_dev-1442419643819-011373969	autoidentityAdmin1442419643618	Vornamen	Name	Behördenbezeichnung	testMail@mail.com	0712507123
[edit] [delete]	safe_ng_dev-1442420272949-011373984	autoidentityAdmin1442417407546	Vornamen	Name	Behördenbezeichnung	testMail@mail.com	0712507123
[edit] [delete]	safe_ng_dev-1442421545000-011373988	autoidentityAdmin1442417407548	Vornamen	Name	Behördenbezeichnung	testMail@mail.com	0712507123

¹ „Externe-ID“ wird für den Fachdatenimport im EGVP und „Gruppe“ von der Virtuellen Poststelle der DEHSt genutzt. Beide Felder sind derzeit nicht für Einschränkungen der Identitätsadministratoren geeignet.

Nach dem Klicken auf das *Löschen*-Symbol müssen Sie das Löschen bestätigen.



The image shows a confirmation dialog box titled "Löschen bestätigen" (Confirm Deletion). The text inside asks: "Der Benutzer 'idadmin4test' wird unwiderruflich gelöscht. Wollen Sie den Benutzer wirklich endgültig löschen?" (The user 'idadmin4test' will be permanently deleted. Do you really want to delete the user permanently?). There are two buttons: "Löschen" (Delete) and "Abbruch" (Cancel).

Nach dem Bestätigen wird der Identitätsadministrator gelöscht. Eine Statusmeldung bestätigt das Löschen.



3.3 Abmelden

Hinweis! Sie können sich aus einer SSL-authentifizierten Verbindung nur durch Schließen des Browsers abmelden. Bitte Schließen Sie den Browser, wenn Sie die Freischaltung oder Verwaltung der Identitätsadministratoren beendet haben.

3.4 Benutzerkonto löschen

Wenn Sie Ihr eigenes Benutzerkonto löschen möchten, klicken Sie unten rechts in der Anwendung auf *Benutzerkonto löschen*.

The screenshot shows a web browser window with the URL 'www.kstt-justiz.de'. The page title is 'BEARBEITUNG - SICHER'. The form is divided into several sections:

- Nutzerdaten:**
 - Nutzer-ID:
 - Berufskennzahl:
- Adressdaten:**
 - E-Mail:
 - Organisation:
 - Nur Nutzer mit unüberprüften Rollen:
- Persönliche Daten:**
 - Name:
 - Vorname:
 - Geburtsdatum:

At the bottom right, there is a 'Suche' button. The footer contains 'HERAUSGABER: Hilfe Impressum Kontakt Benutzerkonto löschen'.

Sie müssen das Löschen bestätigen. Beachten Sie, dass Ihr Account unwiderruflich gelöscht wird.

4 Vorgaben für die Registrierung von Identitätsadministratoren für die Rollentypen ZenVG und JP-VP

Es ist hilfreich - und wird dringend empfohlen – Identitätsadministratoren durch Eintragung

- eines Kennziffer-Präfix
 - a) Justiz
 - b) Finanzen
 - c) Kommunen
 - d) Zoll

auf ein Ressort zu beschränken und/oder

- der Behörden-Kennziffer (XJustiz – ID im Ressort Justiz) im Feld „Kennziffer“ auf eine bestimmte Behörde zu beschränken.

Beide Felder werden als Pflichtfelder im Registrierungsclient des gemeinsamen Vollstreckungsportals der Länder definiert.

5 Support

Eventuelle Supportfragen müssen innerhalb der einzelnen Länder gebündelt und, soweit möglich, landesintern beantwortet werden.

Der fachliche Support für die Identitätsadministratoren erfolgt durch die jeweiligen Zugangsadministratoren.

Für technische Supportanfragen der Zugangsadministratoren steht die Kontaktadresse technischersupport@safe-justiz.de zur Verfügung.

Beschreiben Sie dabei bitte Ihr Problem und geben Sie die genutzte Browserversion an. (Die Version Ihres Browsers finden Sie meist im Menü Hilfe unter dem Menüpunkt "über".)

Um eine effiziente Bearbeitung von Support-Anfragen gewährleisten zu können, ist für jedes Bundesland und den Bund jeweils der Zugangsadministrator nebst Vertreter als supportberechtigt benannt. Diese Supportberechtigten leiten Supportanfragen gebündelt an die angegebene Kontaktadresse weiter.

Oder per E-Mail.

Bitte geben Sie eine genaue Schritt für Schritt-Anleitung und die Browserversion, die Sie verwenden, an. Sie erhalten diese Information über *Kontakt*.

6 Anlagen

6.1 Rollen JP-VP und ZenVG

Zuordnung zu Rollentypen (falls unterschiedliche gewünscht)		Rollenwert	Beschreibung	Berechtigung im Verfahren	
				Portal	Landesverfahren
JP-VP	ZenVG				
X	X	GV	Gerichtsvollzieher	Einsicht in Schuldnerverzeichniseinträge	Einlieferung von Eintragungsanordnungen
				Einsicht in Vermögensverzeichnisregister	Einlieferung von Vermögensverzeichnissen
X	X	InsO	Insolvenzgerichte	Einsicht in Schuldnerverzeichniseinträge	Einlieferung von Eintragungsanordnungen
				(Einsicht in Vermögensverzeichnisregister)	
X	X	VVB-EA	Verwaltungsvollstreckungsbehörde mit Recht zur Einlieferung von Eintragungsanordnungen	Einsicht in Schuldnerverzeichniseinträge	Einlieferung von Eintragungsanordnungen
X	X	VVB-VV	Verwaltungsvollstreckungsbehörde mit Recht zur Einlieferung von Vermögensverzeichnissen	Einsicht in Vermögensverzeichnisregister	Einlieferung von Vermögensverzeichnissen

X	X	VollG	örtliches Vollstreckungsgericht	Einsicht in Schuldnerverzeichniseinträge	Eintrag/Einlieferung von Hemmnissen
				Einsicht in Vermögensverzeichnisregister	Zuordnung von Hemmnissen
					Bearbeitung und Löschung von Hemmnissen
					Bestätigung von Hemmnissen mit folgender Löschung eines Schuldneintrags
X	X	ZenVG-Sachbearbeitung	Sachbearbeiter im ZenVG	Einsicht in Schuldnerverzeichniseinträge	Verwaltung von Schuldneinträgen
				Einsicht in Vermögensverzeichnisregister	Verwaltung von Vermögensverzeichnissen
				Abdruckempfänger bearbeiten	Verwaltung von Hemmnissen
				Kosten bearbeiten	Statistik bearbeiten
				Revision bearbeiten	
X		Revision	Mitarbeiter, der zur Durchführung der internen Revision berechtigt ist	Rechte, die dazu notwendig sind, die Rechtmäßigkeit durchgeführter Einsichten zu überprüfen.	
X		Einsichtnehmer-SV		Einsicht in Schuldnerverzeichniseinträge	
X		Einsichtnehmer-VV		Einsicht in Vermögensverzeichnisregister	
X	X	Test	Rolle, die zum Test eines neu ausgerollten Software-Releases berechtigt (Test zur Abnahme)	Berechtigung zur Anmeldung während der Testphase	Berechtigung zur Anmeldung während der Testphase
X		Abdruckempfaenger	Abdruckempfänger	Berechtigung zum Empfang oder zum Download bereitgestellter Abdrucke	
X		Servicestelle	Mitarbeiter der Servicestelle des Vollstreckungsportals	Anlegen von Mandanten	
				Einsicht in Schuldnerverzeichniseinträge	
				Einsicht in	

				Vermögensverzeichnisregister	
				Kosten bearbeiten	
				Externe Einsichtnehmer verwalten	
	X	Hoster	Hoster des Landesverfahrens		Anlegen von Mandanten (mit Mandanten sind hierbei die Bundesländer gemeint, die die Anwendung nutzen)
	X	TechAdmin-Land	technische Administration des Landesverfahrens		Replikation konfigurieren, verwalten, kontrollieren
					Batchjobs konfigurieren, verwalten und kontrollieren
X		TechAdmin-Portal	technische Administration des Portalsystems	Replikation konfigurieren, verwalten, überprüfen	
				Batchjobs konfigurieren, verwalten, überprüfen	

6.2 Rollen BNotK-ZTR

Rollenwerte des Rollentyps BNotK-ZTR	Berechtigung im Verfahren
OLG-Admin	<ul style="list-style-type: none"> - Vornahme von Programmeinstellungen des ZTR und Pflege der Gerichtsdaten im Gerichtsverzeichnis der BNotK jeweils für die Amtsgerichte eines oder mehrerer Oberlandesgerichtsbezirke - Verwaltung der Gerichtsadmin-Rollen für die Amtsgerichte eines oder mehrerer Oberlandesgerichtsbezirke
Gerichtsadmin	<ul style="list-style-type: none"> - Vornahme von gerichtsweiten Einstellungen der Schnittstellen des ZTR für ein oder mehrere Amtsgerichte - Vornahme von Programmeinstellungen des ZTR und Pflege der Gerichtsdaten im Gerichtsverzeichnis der BNotK, jeweils für ein oder mehrere Amtsgerichte - Benutzerverwaltung für die anderen Rollen (außer der Gerichtsadmin-Rollen) für ein oder mehrere Amtsgerichte
ZTR-Sterbefallbearbeitung	Sterbefallbearbeitung (§ 78c BNotO)
ZTR-Registerabfrage	Registerabfragen (§ 78d Abs. 1 Satz 1 Nr. 1, Fall 2 BNotO)
ZTR-Meldung	Übermittlung von Verwahrangaben (§ 78b Abs. 1 Satz 1 BNotO) und Einsicht in eigene Registrierungen (§ 78d Abs. 2 BNotO)
ZTR-Eingangsbestätigung	Eingangsbestätigungen nach §§ 3 Abs. 3 Satz 2, 7 Abs. 4 Satz 1 ZTR-VO