

PKI-Manager Version 2.0

**Weboberfläche zur Zertifikatsbeantragung
für die RA-Stellen**

Nigus, Karina (BREKOM)

PKI-Manager – Weboberfläche zur Zertifikatsbeantragung

Es wurde eine Weboberfläche/Webanwendung entwickelt, um die Beantragung und Sperrung von User-Zertifikaten zu vereinfachen. Die Benutzung/Anwendung dieser Weboberfläche ist für die RA-Stellen (RA=Registrierungsstellen) vorgesehen. Übergeordnete RA-Stellen sind befugt untergeordnete RA-Stellen einzurichten.

Die RA-Stellen haben so die Möglichkeit die Zertifikate für ihre User eigenständig zu beantragen oder zu sperren.

Zusätzlich ist es möglich User-Zertifikaten verschiedene BVN-Dienste hinzuzufügen oder zu löschen.

Die Weboberfläche/Anwendung steht ausschliesslich den RA-Stellen ab den Juni **2016** zur Verfügung.

Voraussetzungen für den Zugriff auf die Webseite:

- Genehmigung von der übergeordneten RA-Stelle → die Senatorin für Finanzen Ref02, daß man die RA-Stelle Rolle ausüben kann
- Gültiges RA-Stellen-Zertifikat
- Browser
- Zugriff ist nur aus BVN erlaubt (ggf. VPN-Verbindung benutzen)

Zugangslink:

<https://pki-manager.bremen.intra/>

Ansicht für die RA-Stellen:

The screenshot shows a web browser window with the URL `https://pki-manager.bremen.intra/zertifikate.php`. The page title is "Zentrale RA: Freie Hansestadt Bremen" and the sub-RA is "Stadtbibliothek Bremen". There is a search bar labeled "Freitextsuche" with a "suchen" button. Below the search bar is a table with columns: "CN", "Email", "Ausgestellt", "beantragt durch", "Ausstellungsdatum", and "Laufzeit". The table contains one row of data for "Mustermann Max" with email "kniglus@brekom.de", status "ja", role "Import, Benutzer", issue date "06.04.2016 09:44", and validity "1 Jahr". Below the table are two buttons: "neues Zertifikat beantragen" and "Zertifikate als Excel exportieren".

Jede RA-Stelle bekommt die Auflistung der eigens ausgestellten/beantragten Zertifikate. Es können Zertifikate neu beantragt, gesperrt oder zu einem bestehenden, gültigen Zertifikat BVN-Dienste hinzugefügt oder gelöscht werden.

This screenshot is identical to the previous one, but a red arrow points to the button "Zertifikate als Excel exportieren", which is also circled in red.

RA-Stellen können alle ausgestellten Zertifikate in eine Excel-Tabelle exportieren.

So sieht die Maske für einen **Zertifikatsantrag** aus.

The screenshot shows a web browser window with the URL `https://pki-manager.bremen.intra/CertEdit.php`. The page title is "Zertifikatsantrag". On the left, there is a sidebar with "RA-Typ: sub" and a link to "Zertifikate". The main content area is divided into several sections:

- Personal and Organizational Data:** Fields for Land (DE), Bundesland (Bremen), Stadt (Bremen), Organisation (Freie Hansestadt Bremen), Organisationseinheit (Stadtbibliothek), Name (empty), Vorname (Der Name der Zertifikatsbesitzers.), Email (empty), and Gültigkeitsdauer (1 Jahr).
- Daten für das Anschreiben an den/die Zertifikatsbesitzer/in:** Fields for Anrede, Firma, Plz, Ort, Straße, and Alternative Rechnungsanschrift (highlighted with a red circle).
- Nutzung für folgende Dienste:** Checkboxes for BVN-Dienste, IPSec-Zugang, and OpenVPN.

Alternative Anschrift für die Rechnung, wenn diese von der beantragenden RA-Stelle abweichen sollte.

Man kann auch die BVN-Dienste hinzufügen/beatragen:

The screenshot shows a web browser window with the URL `https://pki-manages.bremen.intra/CertEdit.php`. The page title is "Zertifikatsantrag". The form is for a "sub" RA type, with the central RA being "Freie Hansestadt Bremen" and the sub RA being "Stadtbibliothek Bremen".

The form fields are as follows:

- Land: DE
- Bundesland: Bremen
- Stadt: Bremen
- Organisation: Freie Hansestadt Bremen
- Organisationseinheit: Stadtbibliothek
- Name: [Empty field]
- Vorname: Der Name der Zertifikatsbesitzers.
- Email: [Empty field]
- Gültigkeitsdauer: 1 Jahr

The "Daten für das Anschreiben an den/die Zertifikatsbesitzer/in:" section includes fields for:

- Anrede
- Firma
- Plz
- Ort
- Straße
- Alternative Rechnungsanschrift

The "Nutzung für folgende Dienste:" section is circled in red and contains:

- BVN-Dienste
- MIP, Exchange, Proxies, Standard

City: Bremen
Organization: Freie Hansestadt Bremen
Organizational Unit: Stadtbibliothek
Name: Teplerin
First Name: Claudia
Email: kniglus@brekom.de
Validity Duration: 1 Jahr

Daten für das Anschreiben an den/die Zertifikatsbesitzer/in:

Address: Frau
Company:
Postal Code: 28217
City: Bremen
Street: Am Weser-Terrain 1
Alternative Address:

Nutzung für folgende Dienste:

EVPN-Dienste
IPSec-Zugang
OpenVPN
Reverse-Proxy
Other Purpose:
CSG:

- stg
- stgweb
- gab
- kgg
- stgcert
- stgby
- stg

spec:chem

Beantragt am 12.04.2016 16:03
Ausgestellt am 06.04.2016 09:44

p12-Datei (gesperrt: nein)

Zertifikat nochmal versenden

Sperrung

Suspendierung anfordern

Daten für das Anschreiben an den/die Zertifikatsbesitzer/in:

Anrede

Firma

Plz

Ort

Straße

Alternative Rechnungsanschrift

Nutzung für folgende Dienste:

BVN-Dienste

IPSec-Zugang

OpenVPN

Reverse-Proxy

Anderer Verwendungszweck

CSG

Beantragt von

Import, Benutzer

Beantragt am

12.04.2016 16:03

Änderung der Zertifikat-Dienste beauftragen

Liste der Zertifikat-Dienste Änderungen

Oder die beantragten/zugewiesenen BVN-Dienste des Zertifikatsinhabers ansehen:

RA-Typ: sub
Zertifikate

Zertifikat

Mustermann Max
kniglus@brekom.de

[« zum Zertifikat](#)

| BVN-Dienste | IPSec-Zugang | OpenVPN | Reverse-Proxy | Anderer Verwendungszweck | CSG |
|-------------|--------------|---------|---------------|--------------------------|-------------------------|
| nein | nein | nein | nein | nein | 12.04.2016 15:26 Import |
| nein | nein | nein | nein | nein | 12.04.2016 16:42 Import |

men.intra/CertEdit.php?cer_id=18 FHB PKI

| | |
|----------------------------|---|
| Bundesland | Bremen |
| Stadt | Bremen |
| Organisation | <input type="text" value="FHB"/> |
| Organisationseinheit | <input type="text" value="BREKOM"/> |
| Name | <input type="text" value="Tester2"/> |
| Vorname | <input type="text" value="Heinz,CN1=BREKOM ERF"/> |
| Email | <input type="text" value="kniglus@brekom.de"/> |
| Gültigkeitsdauer | <input type="text" value="3 Jahre"/> |
| Beantragt von | Import, Benutzer |
| Beantragt am | 26.01.2016 16:47 |
| Ausgestellt am | 15.03.2013 10:42 |
| p12-Datei (gesperrt: nein) | Zertifikat nochmal versenden |

Daten für das Anschreiben an den Zertifikatsbesitzer:

| | |
|--------------------------------|----------------------|
| Anrede | <input type="text"/> |
| Firma | <input type="text"/> |
| Plz | <input type="text"/> |
| Ort | <input type="text"/> |
| Strasse | <input type="text"/> |
| Alternative Rechnungsanschrift | <input type="text"/> |

Nutzung für folgende Dienste:

| | | |
|--------------------------|-------------------------------------|-----------------------------------|
| IPSec-Zugang | <input type="checkbox"/> | <input type="text"/> |
| OpenVPN | <input type="checkbox"/> | <input type="text"/> |
| Reverse-Proxy | <input type="checkbox"/> | <input type="text"/> |
| Anderer Verwendungszweck | <input checked="" type="checkbox"/> | <input type="text" value="EGVP"/> |

Hinweise für das Feld CN, (Zusatz EGVP):

Namensaufbau: Dienststelle <Organisationskennzeichen> <Funktion(skürzel)>
(Beispiele: Senatorin fuer Finanzen Ref-02 Senatorin fuer Finanzen EGVP
Performa Nord ANO und ERF Universitaet Bremen ERF 1)

1. Angaben für die Nutzung mit dem EGVP

Die Angabe für das Feld CN muss für Eingangsstellen der Dienststellen identisch mit der Angabe „Name“ im EGVP sein. (Umlaute müssen umgewandelt werden)
Aus der „Tabelle der verantwortliche Stellen gemäß § 8 Abs. 1 Nr. 1 BremDSG“, zu finden im „Konzept für die Zugangseröffnung der FHB gemäß §3a
Verwaltungsverfahrensgesetz“ unter www.egvp.bremen.de.

Nicht aufgeführte Namen sind vor der Zertifikatsbeantragung bei der Senatorin für Finanzen Referat 02 zu beantragen. Die Ausstellung von Zertifikaten mit nicht zugelassenen Dienststellennamen ist untersagt und führt zur sofortigen Sperrung.

2. Angaben für die Übertragung von Anordnungs- / Zahlungsdaten zur Landeshauptkasse Funktionsrollen werden wie folgt im Feld CN (Zusatz EGVP) festgelegt:

ANO Anordnende Person

ERF sachlich/rechnerisch richtig zeichnende Person (Erfassende Person)

ANO und ERF Doppelfunktion

(Beispiele: Senator fuer Inneres und Sport ANO Universitaet Bremen ERF

Performa Nord ANO und ERF

Im CN-Feld bei Vorname wird hier wie folgt aufgebaut:

<Vorname>,CN1=<Dienststelle> >Funktion(skürzel)>

Beispiel: **Karina,CN1=BREKOM ERF**

Pro Person kann nur ein Zertifikat mit einer der drei Rollen (“ANO“; “ERF“; “ANO und ERF“) beantragt werden. Ein Zertifikat ist für ungültig zu erklären, wenn die Person die Funktion nicht mehr ausübt, welche mit dem Zertifikat verbunden ist. Wechselt eine Person zu einer anderen bremischen Organisationseinheit, für die wiederum ein Zertifikat beantragt werden soll, muss das bisherige Zertifikat für ungültig erklärt werden. Sofern es sich um eine anordnende Person handelt, muss auch die Anordnungsbefugnis gegenüber der Landeshauptkasse widerrufen werden.

Nachdem Ausfüllen der Felder muss noch die „Hinweise zum Auftrag“ bestätigt werden.
Mit „Auftrag abschließen“ wird das Zertifikat ausgestellt und eine Rechnung generiert.

The screenshot shows a web browser window with the URL `https://pki-manager.bremen.intra/CertReview.php?cer_id=2238`. The page title is "FHB PKI". On the left, a grey box displays "RA-Typ: sub" and a link for "Zertifikate". The main content area lists certificate details in a table format:

| | |
|---|---------------------|
| Land | DE |
| Bundesland | Bremen |
| Stadt | Bremen |
| Organisation | |
| Organisationseinheit | Stadtbibliothek |
| Name (CN) | Testern |
| Vorname (CN1) | Claudia |
| Email | kniglus@brekom.de |
| Gültigkeitsdauer | PKI-User-extern |
| Daten für das Anschreiben an den Zertifikatsbesitzer: | |
| Anrede | Frau |
| Firma | |
| Plz | 28217 |
| Ort | Bremen |
| Strasse | Am Weser-Terminal 1 |
| Nutzung für folgende Dienste: | |
| IPSec-Zugang | nein |
| Anderer Verwendungszweck | nein |
| CSG | |
| Alternative Rechnungsanschrift | |

Below the table, there is a section titled "Hinweise zum Auftrag" with a checkbox and a text box:

Die Bestellung eines Tickets kann nicht widerrufen werden. Die Daten eines Tickets können nachträglich nicht geändert werden. Ich habe mich vergewissert, daß die Daten des Zertifikats korrekt sind!

At the bottom of the form, there are two buttons: "Auftrag abschließen" on the left and "nochmal bearbeiten" on the right.

Zertifikatssperrung:

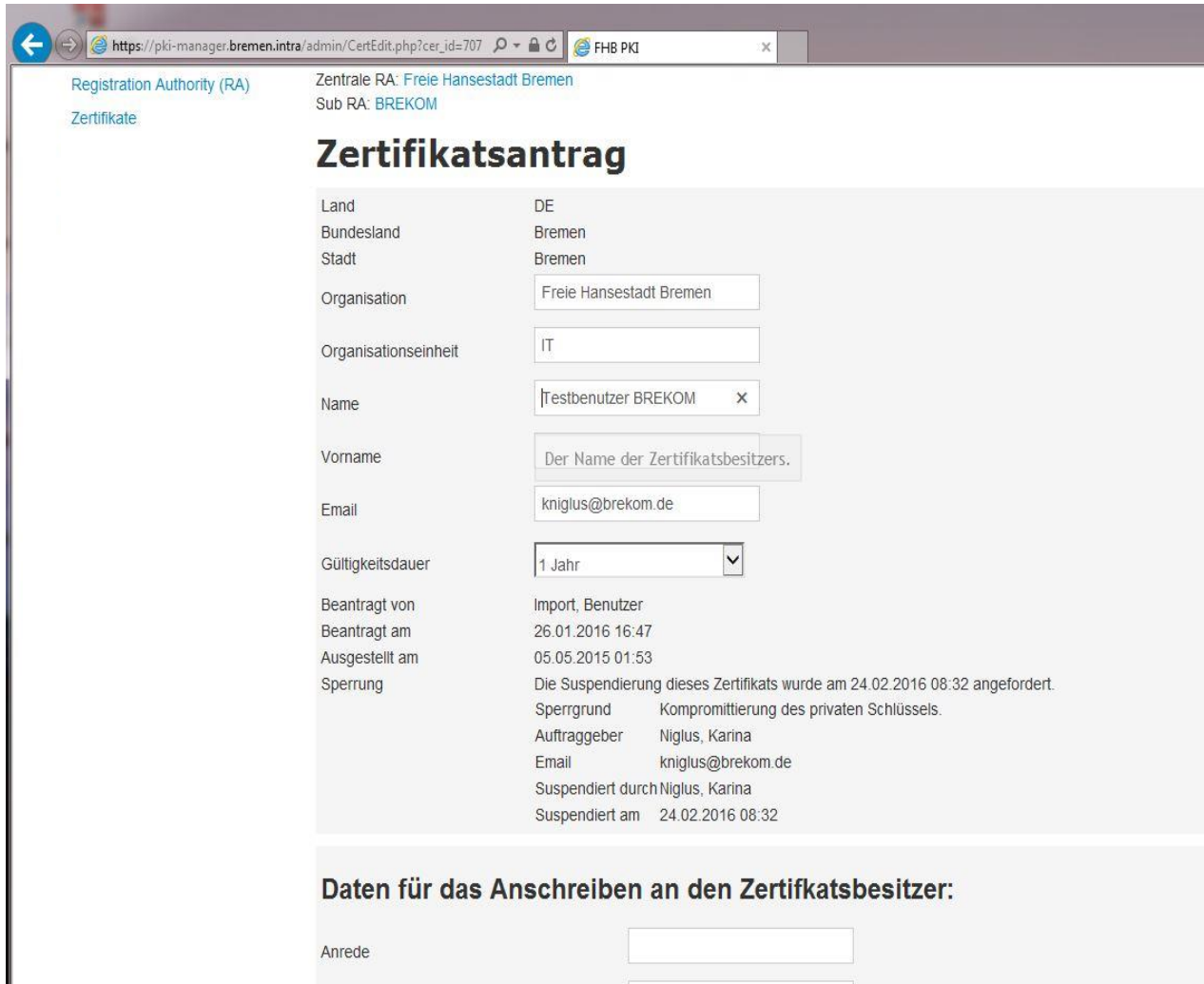
The screenshot shows a web browser window with the URL `https://pki-manager.bremen.intra/admin/CertSuspend.php?cer_id=-`. The page title is "ZertifikatsSuspendierung". On the left, there is a navigation menu with "Registration Authority (RA)" and "Zertifikate". The main content area contains the following fields and options:

- Name: Testbenutzer BREKOM
- Email: kniglus@brekom.de
- RequestID: 763
- SerialNumber: (empty)
- Sperrgrund: Kompromittierung des privaten Schlüssels. Der private Schlüssel könnte in fremde Hände gelangt sein.
- Auftraggeber: Niglus, Karina
- Email: kniglus@brekom.de
- Telefonnr.: 0421/24002336
- speichern

Wenn das zu sperrende Zertifikat ausgewählt ist, müssen die abgebildeten Felder für die Sperrung ausgefüllt werden. Nach dem „speichern“ muss der Sperrvorgang erneut bestätigt werden (siehe unten).

The screenshot shows a confirmation dialog box titled "Zertifikat sperren". It contains a warning icon (a triangle with an exclamation mark) and the text: "Soll das Zertifikat für Testbenutzer BREKOM suspendiert werden?". Below the text are two buttons: "suspendieren" and "abbrechen".

In der Übersicht „Zertifikatsantrag“ kann nachgesehen werden wann und von wem ein Zertifikat gesperrt wurde.



The screenshot shows a web browser window with the URL https://pki-manager.bremen.intra/admin/CertEdit.php?cer_id=707. The page title is "Zertifikatsantrag".

Registration Authority (RA): Zentrale RA: Freie Hansestadt Bremen
Sub RA: BREKOM

Zertifikatsantrag

| | |
|----------------------|--|
| Land | DE |
| Bundesland | Bremen |
| Stadt | Bremen |
| Organisation | Freie Hansestadt Bremen |
| Organisationseinheit | IT |
| Name | Testbenutzer BREKOM |
| Vorname | Der Name der Zertifikatsbesitzers. |
| Email | knigus@brekom.de |
| Gültigkeitsdauer | 1 Jahr |
| Beantragt von | Import, Benutzer |
| Beantragt am | 26.01.2016 16:47 |
| Ausgestellt am | 05.05.2015 01:53 |
| Sperrung | Die Suspendierung dieses Zertifikats wurde am 24.02.2016 08:32 angefordert. Sperrgrund: Kompromittierung des privaten Schlüssels. Auftraggeber: Nigus, Karina Email: knigus@brekom.de Suspendiert durch: Nigus, Karina Suspendiert am: 24.02.2016 08:32 |

Daten für das Anschreiben an den Zertifikatsbesitzer:

Anrede:

Zusätzlich besteht die Möglichkeit, die p12-Datei den Zertifikatinhaber erneut zu zusenden.

The screenshot shows a web browser window with the URL https://pki-manager.bremen.intra/CertEdit.php?cer_id=2187. The page title is "Zentrale RA: Freie Hansestadt Bremen" and "Sub RA: Stadtbibliothek Bremen". The main heading is "Zertifikatsantrag".

On the left, there is a sidebar with "RA-Typ: sub" and a link to "Zertifikate".

The main form contains the following fields and values:

| | |
|----------------------------|------------------------------------|
| Land | DE |
| Bundesland | Bremen |
| Stadt | Bremen |
| Organisation | Freie Hansestadt Bremen |
| Organisationseinheit | Stadtbibliothek |
| Name | Mustermann Max |
| Vorname | Der Name der Zertifikatsbesitzers. |
| Email | kniglus@brekom.de |
| Gültigkeitsdauer | 1 Jahr |
| Beantragt von | Import, Benutzer |
| Beantragt am | 12.04.2016 16:03 |
| Ausgestellt am | 08.04.2016 09:44 |
| p12-Datei (gesperrt: nein) | Zertifikat nochmal versenden |
| Sperrung | Suspendierung anfordern |

Below the form, there is a section titled "Daten für das Anschreiben an den/die Zertifikatsbesitzer/in:" with input fields for:

- Anrede
- Firma
- Plz
- Ort
- Straße
- Alternative Rechnungsanschrift

Massenbeantragung von User-Zertifikaten:

Für die Massenbeantragung von Zertifikaten wird es nach wie vor möglich sein eine festgelegte Excel-Tabelle, die mit den Daten befüllt ist, zu verwenden/schicken. (Vorgesehen ist hierfür ein UpLoad-Link (für die Excel-Tabelle) im PKI-Manager – nach 01.04.2016)

Beantragung von Maschinen-Zertifikaten:

Für die Server, die im BVN-Verzeichnisdienst der LAND-HB-Domäne sind brauchen Sie keine Anträge zu stellen. Für die Server-, Domänenkontroller, Notebooks und Rechner die Mitglieder im Land-HB-AD sind, werden die Zertifikate automatisch (per AutoEnrollment) verteilt.

Für andere Arten von Maschinen-Zertifikaten bitte das neue Zertifikatsantrag-Formular benutzen. Diesen bitte digital signiert per Email an: DataportNetzeHB@dataport.de senden.

Durch diese Form der Beantragung wird sichergestellt, dass für die betreffenden Domänen/SubDomänen die notwendigen Berechtigungen für Zertifikatsanträge vorhanden sind.

Hinweis/Bitte:

Wir sind sehr daran interessiert die Antragswege, das Verfahren und die dazu benötigten Tools/Arbeitsmittel zu verbessern, um Sie bei Ihrer Arbeit zu unterstützen. Deshalb möchten wir Sie dazu ermutigen uns Hinweise für mögliche Verbesserungen sowie Anregungen mitzuteilen. Vielen Dank!

Bitte schicken uns Ihre Meinung an: pki@brekom.de