

1. How to submit a BPKI request?	1
1.1 Administrative contact	1
1.2 Non-administrative contact	2
2. How to enrol BPKI certificate?	3
on Linux:	3
On Windows:	3
3. BPKI Renewal	5
4. How to add ROAs?	5
5. How to manage ROAs?	6

1. How to submit a BPKI request?

To request a BPKI certificate, connect to <https://my.afrinic.net> and navigate to "My Account > BPKI".

NOTE: *AFRINIC shall assist you only if you provide the below requested information/document and you have NO outstanding balances.*

1.1 Administrative contact

If you are an administrative contact, kindly send us your identification information on service-support@afrinic.net :

1. Full name
2. E-mail address
3. NIC-HANDLE
4. Organisation's name
5. Scanned copy of an official, Government/State-issued, ID, passport, driver's license or company ID card.

Certificate Requests

To enrol a digital certificate from the Member CA used by AFRINIC to issue BPKI certificates, we first need to verify your identity.

In order to do this you will need to send scanned copies of the following documents to our Registration Services team for approval at :

- Government- or State-issued ID card
 - Passport
 - Drivers' license
- Company ID card

1.2 Non-administrative contact

If you are a technical, billing, abuse or general contact, you will be asked to request a BPKI certificate by clicking on the "Request BPKI certificate" button.

Request BPKI Certificate

Please click the button below to request your BPKI certificate which is required to access this section of the site.


Request BPKI certificate

Your request will be sent to all the Administrative contacts of your organisation. Only if the admin contact already has a valid BPKI certificate, the system will grant him access to accept

the BPKI request made by non-admin contacts of the organisation. If this is not the case, ask the admin contact to go back to step 1.1 above.

How an admin contact can approve BPKI sent by a non-admin contact?

Log on to <https://my.afrinic.net> and navigate to "My Account > BPKI".

Click on  .

Full Name	Approved	Pending	Rejected	
		✓		 

The non-admin contact shall receive an email with the credentials approximately 30 minutes after the admin contact has approved.

Once the credentials received, non-admin contact to follow step 2. below on how to enrol BPKI certificate.

2. How to enrol BPKI certificate?

AFRINIC recommends CSR generations on either Chrome or Firefox browser.

1. It is highly advised to have a new folder where all the generated files will be stored. This will facilitate the enrollment process.
2. Generate a new private key and Certificate Signing Request. You require openssl to do this.

on Linux/Mac:

Download and install openssl "*yum install openssl*"

openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key

On Windows:

download this OpenSSL package (<http://gnuwin32.sourceforge.net/packages/openssl.htm>) and use the same commands as above.

2. Go to the enrolment page

<https://externalra.afrinic.net/externalra-gui/facelet/enroll-csccert.xhtml>.



The screenshot shows a web form titled "Enroll" with a sub-header "Create certificate from CSR". Below this, there are several input fields: "Entity identifier (username)", "Shared secret (password)", and "Show secret". A "Send Certificate Request" button is visible. Below the button is a "Choose File" button and a "No file chosen" message. A large text area contains the following text: "-----BEGIN CERTIFICATE REQUEST-----", "...base 64 encoded request...", and "-----END CERTIFICATE REQUEST-----". At the bottom, there are radio buttons for "Response type" with options "PEM", "DER", and "DER encoded PKCS#7". A "Send Certificate Request" button is also present at the bottom.

3. Enter your credentials.

4. On choose file, use the generated .csr file from step 1.

5. Select the PEM option and click on Send Certificate Request; Download and save the PEM file.

6. The next step is to generate a .p12 file to install in your browser.

First, download CA certificate here

<https://v2.afrinic.net/images/bpki/memberca.pem.txt>

Next, use openssl to create the p12 file: `openssl pkcs12 -export -out <NIC-HANDLE>.p12 -inkey privateKey.key -in <NIC-HANDLE>.pem -certfile memberca.pem.txt`

Note: The <NIC-HANDLE.pem> should be the file name downloaded from step 5 and NIC-HANDLE should be replaced by your own NIC-HANDLE.

7. Install the p12 on your browser.

On Firefox: Go to Privacy and Security > View Certificates > Import certificate and insert the password which was used to encrypt the certificate.

Certificate Manager ×


Your Certificates People Servers Authorities

You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On	
▼ NMB1-AFRINIC				
NMB1-AFRINIC	Software Security ...	55:C8:0A:63:95:...	21 May 2020	

View... Backup... Backup All... Import... Delete...

OK

 **Password Required**

Please enter the password that was used to encrypt this certificate backup:

3. BPKI Renewal

BPKI Certificates are valid for 2 years and when it expires, the ROAs will not be visible from MyAFRINIC. In case your BPKI certificate has expired, kindly follow step 1.1 and step 2 above to renew it.

4. RPKI - How to add ROAs?

1. Login to <https://my.afrinic.net>
2. Go to Resources
3. Resource Certification
4. Select Issue ROA's
5. Create ROA by providing the following:
 - Enter a unique ROA name
 - Select the originating ASN
 - Select the IPv4 Prefix
 - Select the IPv6 Prefix where applicable
 - Select the ROA validity start date
 - Select the ROA expiry date

Add ROA

* Name:	Please enter a unique ROA name. Spaces will be replaced by "_".
Your AS Numbers:	Please select your ASN from this list or enter any other valid ASN in the field below.
* AS Number:	ASN must be between 0 - 4294967295 in ASPLAIN format. "Reserved" and "Unallocated" ASNs will be rejected.
IPv4 address range:	Please select your prefix in the drop down list and click the "+" button, then you can specify the details.
IPv6 address range:	Please select your prefix in the drop down list and click the "+" button, then you can specify the details.
* Not Valid Before (YYYY-MM-DD):	
* Not Valid After (YYYY-MM-DD):	

Add ROA | **Cancel**

6. Click "add ROA"

5. How to manage ROAs?

While adding or editing ROA specifications, you can see the effect on the validity of your BGP announcements in the "View ROA's" section. Ensure the following sections have valid dates and the ROA's remain validity with status "NO" to indicate that it is not revoked.

List ROAs

Not before	Not after	Revoked?
2015-05-27 13:23:46	2020-05-27 13:23:46	Yes
2015-05-27 13:27:49	2015-05-29 13:27:49	Yes