



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

Protecting Your RIPE Data

A Simple Guide

Gerardo Viviers | 28 October 2024 | RIPE 89

What We'll Explore Today



- Why secure your RIPE Database objects?
- Maintainers
- Notification of updates
- Controlling references to your objects
- Protecting references to SET objects
- AS-SETs and the AUT-NUM object
- *Extra*: New INETNUM object statuses
- Additional Demos?





Why Secure Your RIPE Database Objects?

“ASN alert: Avoid the network's blooper reel”

The Importance of an Accurate Registry



Fundamental to maintaining a stable, secure, and efficient Internet

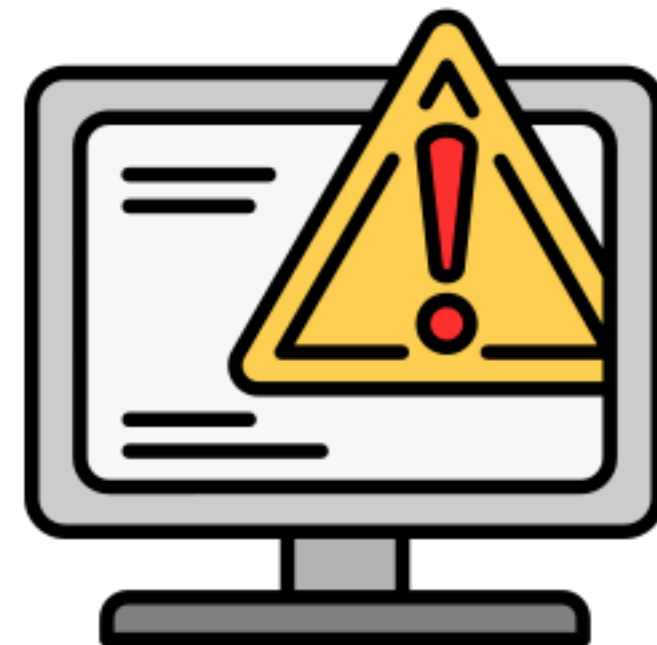
An accurate registry supports:

- Troubleshooting
- Resource management and future planning
- Facilitating peering and network interconnection
- Abuse prevention and mitigation
- Routing efficiency
- Compliance and legal obligations
- Automation



Operational Impact

- Some RIPE Database objects have an **operational impact**
- They can affect **routing, security,** and **inter-network** operations
- Key objects: **route, route6, as-set, domain**
- Keeping them secure is critical!





route and route6 Objects

- Define **authorised origin AS** for prefixes
- Critical for preventing route hijacking
- Used in building router filters
- Aid in troubleshooting and outage resolution

```
route:      193.0.24.0/21
descr:     RIPE-MEETINGS
origin:    AS2121
mnt-by:    RIPE-NCC-MNT
created:   2008-04-09T11:04:18Z
last-modified: 2012-04-24T10:09:25Z
source:    RIPE
```

```
route6:    2001:67c:2e8::/48
descr:     RIPE-NCC
origin:    AS3333
mnt-by:    RIPE-NCC-MNT
created:   2010-09-27T12:14:23Z
last-modified: 2010-09-27T12:14:23Z
source:    RIPE
```

Tip: Update them when announcing new prefixes or changing the originating AS



as-set Object

- Represents a **set of ASNs** for an organisation and customers
- Used in peering automation
- Influences route acceptance policies
- Enables hierarchical filtering
- Streamlines BGP session set up

```
as-set:      AS-RIPENCC
descr:      RIPE NCC
members:    AS3333
members:    AS2121
members:    AS12654
tech-c:     OPS4-RIPE
admin-c:    BRD-RIPE
mnt-by:     RIPE-NCC-MNT
created:    2005-10-31T10:58:55Z
last-modified: 2017-12-04T14:56:33Z
source:     RIPE
```

Tip: Regularly review and update to reflect current network structure



domain Object

- Essential for reverse DNS set up
- Impacts email deliverability
- Used in ENUM for VoIP/telephony services
- Aids in abuse handling and contact identification
- Supports certain security checks

Tip: Keep updated, especially after network architecture changes

```
domain:      24.0.193.in-addr.arpa
descr:      RIPE MEETING
nserver:    manus.authdns.ripe.net
nserver:    ns3.afrinic.net
nserver:    ns3.lacnic.net
nserver:    ns4.apnic.net
nserver:    rirns.arin.net
admin-c:    BRD-RIPE
tech-c:     OPS4-RIPE
zone-c:     OPS4-RIPE
mnt-by:     RIPE-NCC-MNT
mnt-by:     RIPE-GII-MNT
created:    2016-11-10T13:11:14Z
last-modified: 2024-03-19T07:01:58Z
source:    RIPE
```


Things to Consider



Consistency

Ensure consistency across all objects. E.g., origin AS in route objects should match AS-SET contents.

Automation

Implement automation for creating and updating objects to maintain accuracy as your network evolves.

Regular Audits

Periodically review all objects to ensure they reflect your current network state, especially after changes or acquisitions.

Change Management

Update relevant RIPE Database objects as part of your change management process for network changes.

Impact Assessment

Assess potential impact on peers and customers before making changes. Coordinate significant changes with other operators.



Maintainers

“When 'please don't touch' isn't enough for your objects”

Which “auth:” Mechanism?



MD5 Hash Password

auth: MD5-PW

Will be deprecated in 2025

Low Security



SSO Authentication

auth: SSO

Uses RIPE NCC Access account

Medium Security



PGP/X.509 Certificate

auth: PGPKEY-#####

auth: X509-#####

Uses public key cryptography

High Security

MD5 Hash Password



- Oldest authentication method
- Uses a hashed password for authentication
- **Will be deprecated in 2025** due to security concerns
- If currently in use, plan to transition before deprecation

```
mntner:      EXAMPLE-MNT
descr:      Example maintainer
admin-c:    JOE1-RIPE
upd-to:     joe@example.net
auth:    MD5-PW $1$Hi8Qqg
mnt-by:     EXAMPLE-MNT
created:    2024-5-26T11:38:51Z
last-modified: 2024-5-26T11:38:51Z
source:     RIPE
```

SSO Authentication



- **Uses RIPE NCC Access account** for authentication
- More convenient than MD5 - no separate passwords for each maintainer
- Offers better security features like two-factor authentication
- Good balance of **security** and **convenience**
- **Cannot be used for automation**, only interactive updates using the website

```
mntner:      EXAMPLE-MNT
descr:      Example maintainer
admin-c:    JOE1-RIPE
upd-to:     joe@example.net
auth:    SSO joe@example.net
mnt-by:     EXAMPLE-MNT
created:    2024-5-26T11:38:51Z
last-modified: 2024-5-26T11:38:51Z
source:     RIPE
```

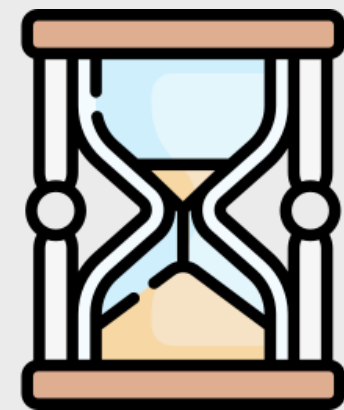
PGP/X.509 Certificate Authentication



- Considered the **most secure** method
- Uses public key cryptography
- Can use either **PGP** (Pretty Good Privacy) or **X.509** certificates
- Provides maximum security for critical objects
- There is no shared secret between the client and server that could be exposed
 - This is as long as the private key is kept safe

```
mntner:      EXAMPLE-MNT
descr:      Example maintainer
admin-c:    JOE1-RIPE
upd-to:     joe@example.net
auth:    PGPKEY-7A3F2E9C
auth:    X509-9182
mnt-by:     EXAMPLE-MNT
created:    2024-5-26T11:38:51Z
last-modified: 2024-5-26T11:38:51Z
source:     RIPE
```

Recommendations



If using MD5, plan to transition before 2025



Consider moving to SSO for a balance of security and convenience



Use PGP / X.509 for maximum security on critical objects



Regularly review and update your authentication methods



How To Create a KEY-CERT

DEMO



1. Generate a Self-signed Certificate

- First generate a self-signed x509 certificate, along with a private key
- Ensure the certificate is **at least 2048 bits**

```
$ openssl req -x509 -days 365 -newkey rsa:4096  
-sha384 -subj "/C=NL/CN=ripe.net" -keyout  
client-key.pem -nodes -out client-cert.pem
```

2. Convert Certificate to ASCII



```
$ openssl x509 -in client-cert.pem
-----BEGIN CERTIFICATE-----
MIIFITCCAwmgAwIBAgIUHD8QpV+IvEVs/pDVK3Ml63TNJUgWdQYJKoZIhvcNAQEM
BQAwIDELMAkGA1UEBhMCTkwXETAPBgNVBAMMCHJpcGUubmV0MB4XDTI0MDUxNDEz
NDQyNl0XDTI1MDUxNDEzNDQyNl0wIDELMAkGA1UEBhMCTkwXETAPBgNVBAMMCHJp
cGUubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAssEU+sbcX9YB
UH/qX9qbF63e1L1LmYFZ2LR119qgqQqYQUR06onCimEJF1bL90c7TDkRcBoyMtzm
KP3kSuiIW0ZpxGcmUtGnoiry9q5thxp60lZNad/Yi59PyTrs8DRo24ebPSKCa1FS
edpFYwP1b0o61ipDARGldx0qtbSXZ0ujxgicQTZxLjakMUKltjLczGN6lXpbLM0a
.
.
.
u+sqCr5eP2DZKmTrUEJPf5NW0k5FBKtmVzkBDXobL7ipctmlmehvEzF9gLgJhnL
lekKdyWrgbunHTfeRF11jxC8js1p4t9BNQ+wpqgom8/V1F9pNRGDzVDS5arok00U
xoAThRqS22DX6JMSDmvTF/DnRZ71j1quL7eUVjdLA8J1Dwvz4YfiYseQEvGAxvY
u3+ZrA1qScImHv1WERETskiAgy5GxpxMW19WIZtBJ3d3QTo4wIrsd050F9ecF2Zs
Up7/pcv+vNxr/Tgf0119yuJzzDjyklaumke0wWvqHz/t6SIisgxAMMF1vAiYvYgC
uh3UhrPEVG/x4Z5RNBqSb+7Mk08jGrVj5qUhtD6FyeJ53u0M1jQQEAZ+G1zsZZzw
x80fSveD5QXj5pzgzLvP0nlk3m5cJEu4FILtzVol1TX4QQXDdeYOCwNK2393ac56
vCxGxD4oqaYyZa3Fz0rjWSDlBwhynd+0Cq2PvIw7wLIYxq7UuZ77W3QL6/LRRzrs
X17yf8Ux8feNjWkKe/L3mq6QBZ9wzoadK+XjTQYWQCb6WlH9QEYpmFS/XCz5kfQ
sUI9iChbKvcW0FFPID+XMbzKMgbSvP6aBz0hbUz3b9Tn4qfn9Yp2YwPci7RrvlK
lECvj7YuYAysqbZKiulSN6N30KHd
-----END CERTIFICATE-----
```

3. Prepare the KEY-CERT object



(a) Open a text editor and paste the certificate

(b) Start with "**key-cert:**" followed by the keyword **AUTO-1**

(c) Add "**certif:**" at the beginning of each certificate line

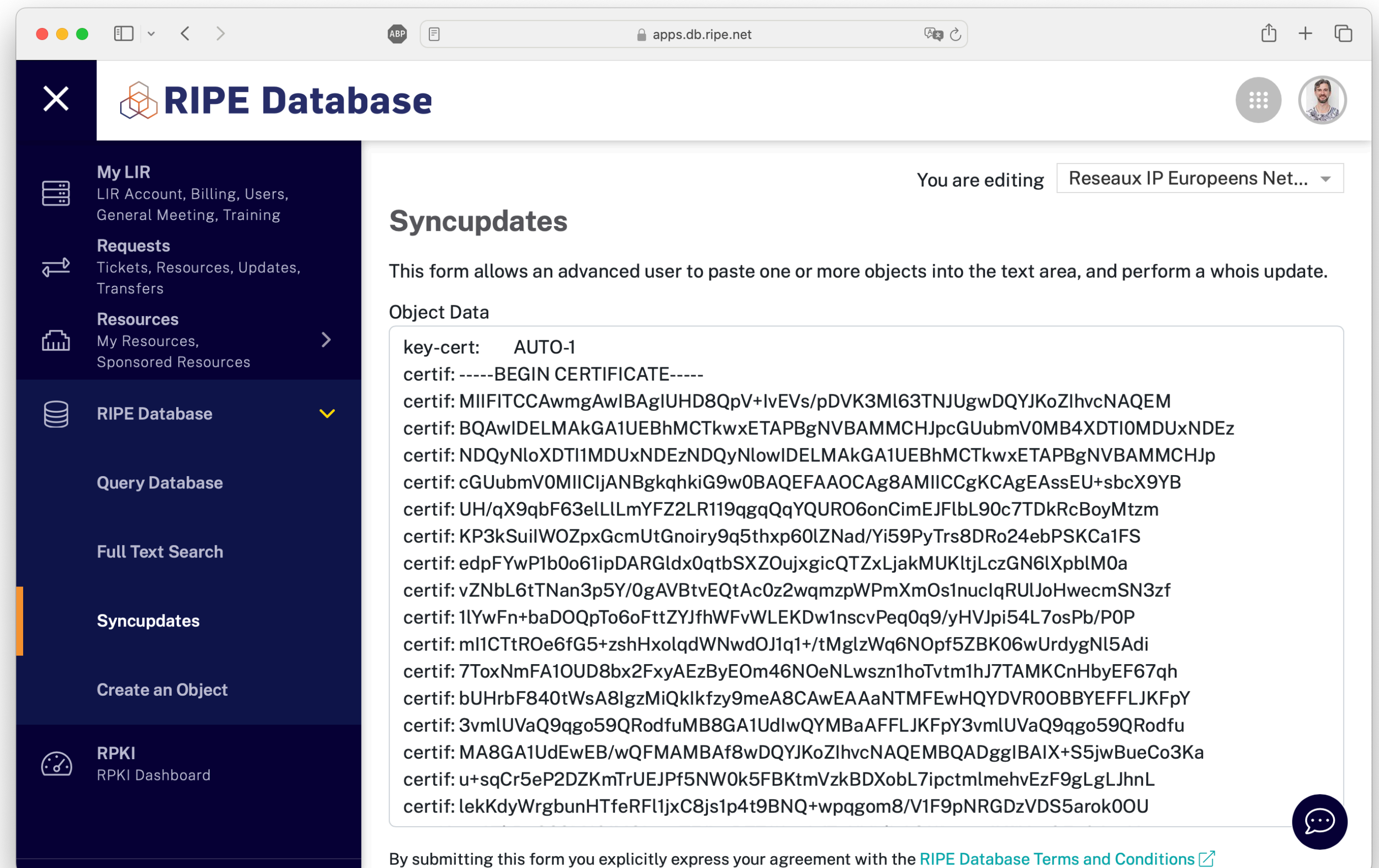
(d) End with the "**mnt-by:**" and the "**source:**"

```
key-cert:          AUTO-1
certif:  -----BEGIN CERTIFICATE-----
certif:  MIIFITCCAwmGAWIBAgIUHD8QpV+IvEVs/pDVk3Ml63TNJUgWdQYJKoZIhvcNAQEM
certif:  BQAwIDELMAkGA1UEBhMCTkwETAPBgNVBAMMCHJpcGUubmV0MB4XDTE0MDUxNDEz
certif:  NDQyNloXDTI1MDUxNDEzNDQyNlowIDELMAkGA1UEBhMCTkwETAPBgNVBAMMCHJp
certif:  cGUubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAsEU+sbC9YB
certif:  UH/qX9qbF63eLLlMqYFZ2LR119qqgQqYQUR06onCimEJF1bL90c7TDkRcBoyMtzm
certif:  KP3kSuiIW0ZpxGcmUtGnoiry9q5thxp60lZnad/Yi59PyTrs8DRo24ebPSKCa1FS
certif:  edpFYwP1b0o61ipDARGldx0qtbSXZ0ujxgicQTZxLjakMUKltjLczGN6lXpbLM0a
certif:  vZNB6tTnan3p5Y/0gAVBtvEQtaC0z2wqmpzPmXm0s1nucIqRUlJoHwecmSN3zf
certif:  1lyWfn+baD0QpTo6oFttZYJfhWfVLEKdW1nscvPeq0q9/yHVJpi54L7osPb/P0P
certif:  mI1CTtR0e6fG5+zshXo1qdWNwd0J1q1+/tMglzWq6N0pf5ZBK06wUrdygNl5Adi
certif:  7ToxNmFA10UD8bx2FxyAEzByE0m46N0eNLwszn1hoTvtm1hJ7TAMKcNHyEF67qh
.
.
certif:  bUHrbF840tWsA8IgzMiQkIkfzy9meA8CAwEAAaNTMFewHQYDVR00BBYEFLJKFpY
certif:  3vmlUVaQ9qgo59QRodfuMB8GA1UdIwQYMBaAFFLJKFpY3vmlUVaQ9qgo59QRodfu
certif:  MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEMBQADggIBAIX+S5jwBueCo3Ka
certif:  u+sqCr5eP2DZKmTrUEJPF5NW0k5FBKtmVzkBDXobL7ipctmlmehvEzF9gLGJhnl
certif:  lekKdyWrgbunHTfeRf1jx8js1p4t9BNQ+wpqgom8/V1F9pNRGDzVDS5arok00U
certif:  xoAThRqS22DX6JMSDmvTF/DnRZ71j1quL7eUVjdLA8J1Dwvz4YfiYseQEvGAxvY
certif:  u3+ZrA1qScImHv1WERETskiAjy5GxpxMW19WIZtBJ3d3QTo4wIrsd050F9ecF2Zs
certif:  Up7/pcv+vNxr/Tgf01l9yuJzzDJyKlaumke0wWvqHz/t6SIisgxAMMFlvAiYvYgC
certif:  uh3UHrPEVG/x4Z5RNBqSb+7Mk08jGrVj5qUhtD6FyeJ53u0M1jQQEAZ+G1zsZZzw
certif:  x80fSveD5QXj5pzgzLvP0nlk3m5cJEu4FILtzVol1TX4QQXDdeY0CwNK2393ac56
certif:  vCxGxD4oqaYyZa3Fz0rjWSDlBwhynd+0Cq2PvIw7wLIYxq7UuZ77W3QL6/LRRzrs
certif:  X17yf8Ux8feNjWkKe/L3mq6QBZ9wzoadK+XjTQYwQCb6wLH9QEYpmFS/XCz5kfQ
certif:  sUI9iChbKvcW0FFPID+XMbzKMgbSvP6aBz0hbUz3b9Tn4qfn9Yp2YwPci7RrvlK
certif:  lECvj7YuYAysqbZKiulSN6N30KHd
certif:  -----END CERTIFICATE-----
mnt-by:  SOME-OTHER-MNT
source:  RIPE
```

4. Create Object With Syncupdates



- Copy/paste the object into Syncupdates
- Send the update to the RIPE Database



The screenshot shows the RIPE Database web interface. The browser address bar displays 'apps.db.ripe.net'. The page title is 'RIPE Database'. A dark blue sidebar on the left contains navigation links: 'My LIR', 'Requests', 'Resources', 'RIPE Database' (selected), 'Query Database', 'Full Text Search', 'Syncupdates', 'Create an Object', and 'RPKI'. The main content area is titled 'Syncupdates' and shows 'You are editing Reseaux IP Europeens Net...'. Below the title, there is a text area containing the following object data:

```
key-cert: AUTO-1
certif: -----BEGIN CERTIFICATE-----
certif: MIIFITCCAwmGAWlBAglUHD8QpV+lvEVs/pDVK3MI63TNJUgWdQYJKoZIhvcNAQEM
certif: BQAwIDELMAkGA1UEBhMCTkwxETAPBgNVBAMMCHJpcGUubmV0OMB4XDTI0MDUxNDEz
certif: NDQyNloXDTI1MDUxNDEzNDQyNlowIDELMAkGA1UEBhMCTkwxETAPBgNVBAMMCHJp
certif: cGUubmV0MIIICjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAssEU+sbcX9YB
certif: UH/qX9qbF63elLlLmYFZ2LR119qgqQqYURO6onCimEJFlbL90c7TDkRcBoyMtzm
certif: KP3kSuiW0ZpxGcmUtGnoiry9q5thxp60lZNad/Yi59PyTrs8DRo24ebPSKCa1FS
certif: edpFYwP1b0o61ipDARGldx0qtbSXZOujxgicQTZxLjakMUKltjLczGN6lXpblM0a
certif: vZnbl6tTNan3p5Y/0gAVBtvEQtAc0z2wqmzpWpMxmOs1nuclqRUIJoHwecmSN3zf
certif: 1lywFn+baDOQpTo6oFttZYJfhWFvWLEKdW1nscvPeq0q9/yHVJpi54L7osPb/P0P
certif: ml1CTtROe6fG5+zshHxolqdWNwdOJ1q1+/tMglzWq6NOpf5ZBK06wUrDygnI5Adi
certif: 7ToxNmFA10UD8bx2FxyAEzByEOm46NOeNLwszn1hoTvtm1hJ7TAMKcNhbYEF67qh
certif: bUHrbF840tWsA8lgzMiQkIkfzy9meA8CAwEAAaNTMFEwHQYDVR0OBBYEFFLJKFpY
certif: 3vmlUVaQ9qgo59QRodfuMB8GA1UdlwQYMBaAFFLJKFpY3vmlUVaQ9qgo59QRodfu
certif: MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEMBQADggIBAIX+S5jwBueCo3Ka
certif: u+sqCr5eP2DZKTrUEJPf5NW0k5FBKtmVzkBDXobL7ipctmlmehvEzF9gLgJhnl
certif: lekKdyWrgbunHTfeRFl1jxC8js1p4t9BNQ+wpqgom8/V1F9pNRGDzVDS5arok00U
```

At the bottom of the form, there is a disclaimer: 'By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)'.



5. Take Note of the Primary Key

- If **successful**, you will get a confirmation
- Write down or copy the **primary key**
 - e.g. X509-3574

```
~~~~~  
The following object(s) were processed SUCCESSFULLY:  
  
---  
Create SUCCEEDED: [key-cert] X509-3574  
~~~~~
```

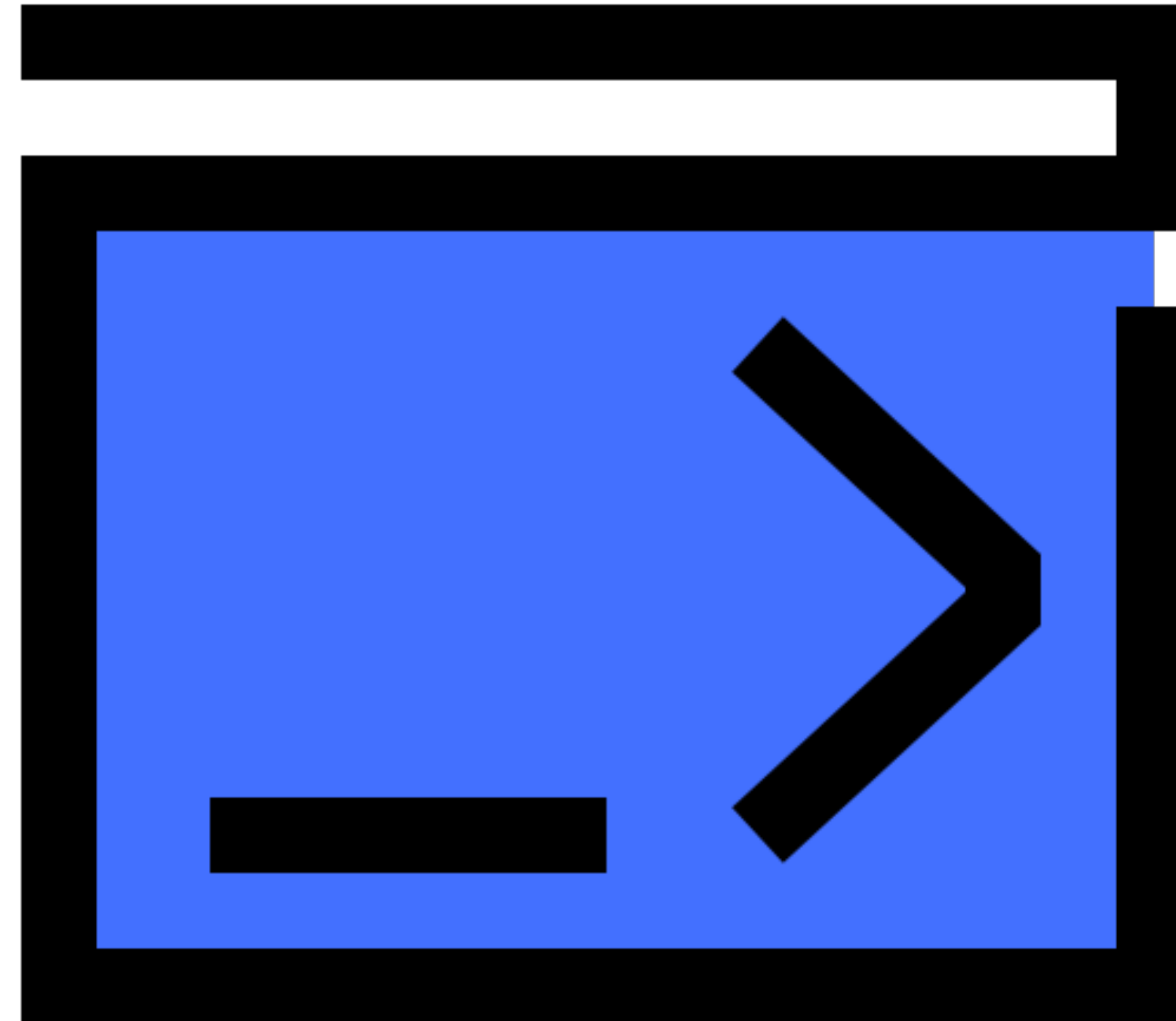


5. Take Note of the Primary Key

- If **successful**, you will get a confirmation
- Write down or copy the **primary key**
 - e.g. X509-3574

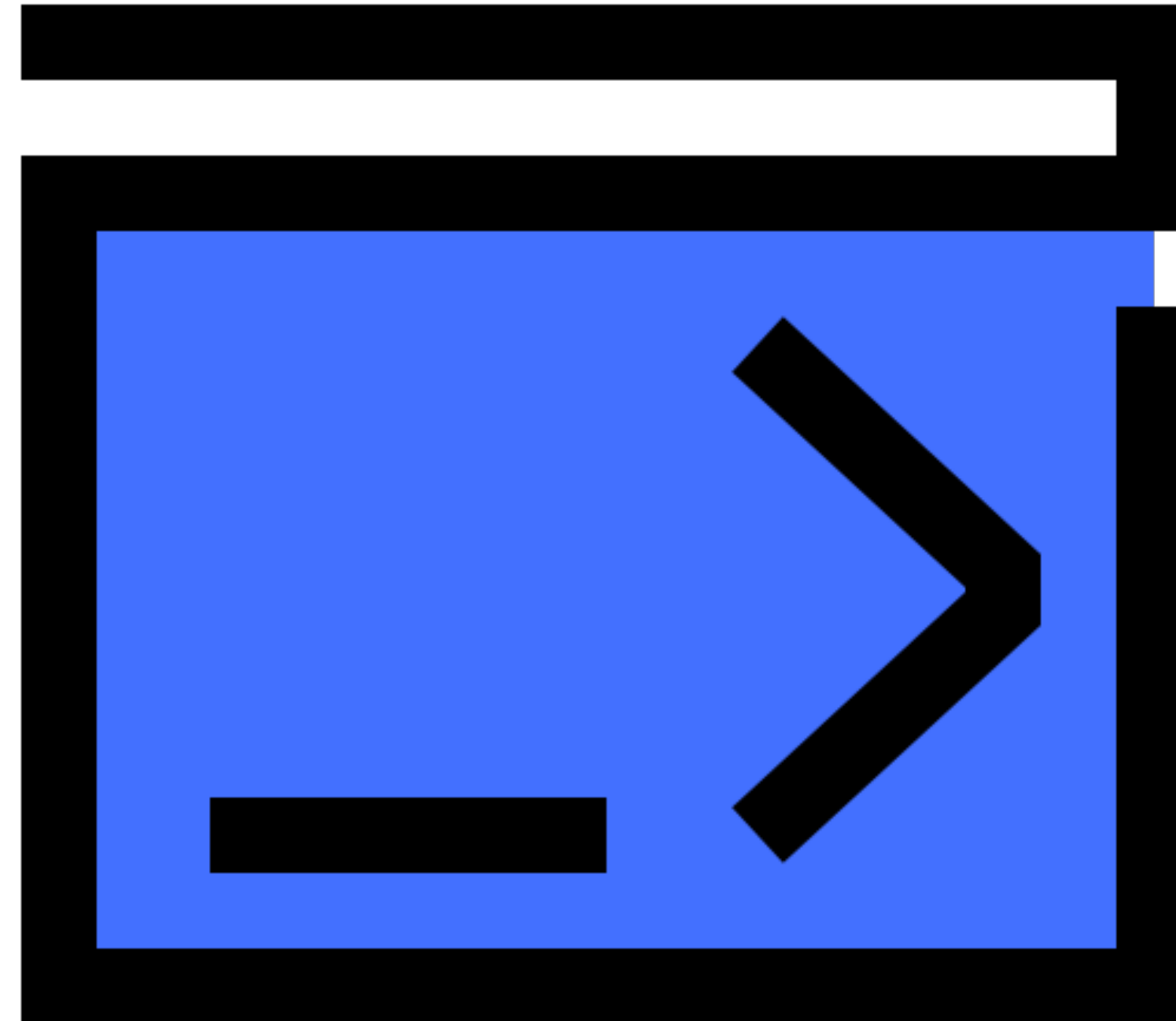
```
~~~~~  
The following object(s) were processed SUCCESSFULLY:  
  
---  
Create SUCCEEDED: [key-cert] X509-3574  
~~~~~
```

Let's do it!



Open Terminal

Let's do it!



Open Terminal



Add New “auth:” to MNTNER

DEMO

1. Search for your Maintainer



The screenshot shows the RIPE Database search interface. The browser address bar is `apps.db.ripe.net`. The page title is "Webupdates — RIPE Network Coordination Centre". The left sidebar contains navigation options: My LIR, Requests, Resources, RIPE Database (selected), Query Database, Full Text Search, Syncupdates, Create an Object, and RPKI. The main content area shows a search for "GAV-MNT". The search results display the following RPSL object:

```
mntner: GAV-MNT
descr: A Maintainer to Remember
admin-c: GAV
auth: SS0
auth: MD5-PW
mnt-by: GAV-MNT
created: 2009-03-13T08:02:12Z
last-modified: 2022-10-13T11:32:47Z
source: RIPE# Filtered
```

Below the search results, it says "RIPE Database Software Version 1.113.2".

1. Search for your Maintainer



The screenshot shows the RIPE Database search interface. The search bar contains the text "GAV-MNT", which is circled in orange. Below the search bar, there are several filter buttons: "Types", "Hierarchy flags", "Inverse lookup", and "Advanced filter". To the right of these filters are two buttons: "APPLY FILTERS" and "RESET FILTERS". Below the filters, there is a disclaimer: "By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)". To the right of this disclaimer, it says "You are editing" followed by a dropdown menu showing "Reseaux IP Europeens Net...". Below this, the "Search results" section is displayed. It contains the following RPSL format text:

```
mntner:      GAV-MNT
descr:      A Maintainer to Remember
admin-c:    GAV
auth:       SS0
auth:       MD5-PW
mnt-by:     GAV-MNT
created:    2009-03-13T08:02:12Z
last-modified: 2022-10-13T11:32:47Z
source:     RIPE# Filtered
```

To the right of this text is a button labeled "Update object". At the bottom of the search results section, it says "RIPE Database Software Version 1.113.2".

1. Search for your Maintainer



The screenshot shows the RIPE Database search interface. The search term "GAV-MNT" is entered in the search bar. The search results show the following details for the maintainer:

mntner:	GAV-MNT	Update object
descr:	A Maintainer to Remember	
admin-c:	GAV	
auth:	SS0 [redacted]	
auth:	MD5-PW [redacted]	
mnt-by:	GAV-MNT	
created:	2009-03-13T08:02:12Z	
last-modified:	2022-10-13T11:32:47Z	
source:	RIPE# Filtered	

RIPE Database Software Version 1.113.2

1. Search for your Maintainer



The screenshot shows the RIPE Database web interface. The browser address bar is 'apps.db.ripe.net'. The page title is 'Webupdates — RIPE Network Coordination Centre'. The main header includes the RIPE Database logo and a user profile picture. A search bar contains the text 'GAV-MNT'. Below the search bar are filter buttons: 'Types', 'Hierarchy flags', 'Inverse lookup', and 'Advanced filter', along with 'APPLY FILTERS' and 'RESET FILTERS' buttons. A disclaimer states: 'By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)'. The user is editing the object 'Reseaux IP Europeens Net...'. The search results section shows the following RPSL object details:

```
mntner: GAV-MNT
descr: A Maintainer to Remember
admin-c: GAV
auth: SSO
auth: MD5-PW
mnt-by: GAV-MNT
created: 2009-03-13T08:02:12Z
last-modified: 2022-10-13T11:32:47Z
source: RIPE# Filtered
```

An 'Update object' button is visible next to the search results. The footer indicates 'RIPE Database Software Version 1.113.2'.

2. Add a New "auth:" Attribute



Modify "mntner" object EDIT IN TEXT AREA

Please enter the maintainers you would like to use as mnt-by

GAV-MNT ☆

mntner
GAV-MNT + ?

descr
A Maintainer to Remember ↓ + ?

admin-c
GAV ↓ + ?

upd-to
gviviers@ripe.net ↓ + ?

mnt-nfy
gviviers@ripe.net ↓ + ?

auth
SSO [redacted] ↓ + ?

2. Add a New "auth:" Attribute



Modify "mntner" object EDIT IN TEXT AREA

Please enter the maintainers you would like to use as mnt-by

GAV-MNT ☆

mntner
GAV-MNT + ?

descr
A Maintainer to Remember ↓ + 🗑️ ?

admin-c
GAV ↓ + ?

upd-to
gviviers@ripe.net ↓ + ?

mnt-nfy
gviviers@ripe.net ↓ + 🗑️ ?

auth
SSO [redacted] ↓ + 🗑️ 🔒 ?

auth

X509-3574 ↓ + 🗑️ 🔒 ?

3. Update It



Your object has been successfully modified DISMISS

mntner "GAV-MNT"

mntner:	GAV-MNT
descr:	A Maintainer to Remember
admin-c:	GAV
upd-to:	gviviers@ripe.net
mnt-nfy:	gviviers@ripe.net
auth:	SSO [REDACTED]
auth:	MD5-PW [REDACTED]
+ auth:	X509-3574
notify:	gviviers@ripe.net
mnt-by:	GAV-MNT
created:	2009-03-13T08:02:12Z
- last-modified:	2022-10-13T11:32:47Z
+ last-modified:	2024-08-02T11:45:28Z
source:	RIPE

MODIFY BACK TO CREATE OBJECT

Let's do it!



Open Webupdates

Let's do it!



Open Webupdates



X.509 and the REST API

EXAMPLE

Example: Update an object



```
$ curl -v --header "Content-type: application/json"  
-d @file.json -X PUT  
--key client-key.pem  
--cert client-cert.pem  
https://rest-cert.db.ripe.net/ripe/person/XY12345-RIPE.json
```

Example: Update an object



Sends the request with a header specifying the data format as JSON

```
$ curl -v --header "Content-type: application/json"
```

```
-d @file.json -X PUT
```

```
--key client-key.pem
```

```
--cert client-cert.pem
```

```
https://rest-cert.db.ripe.net/ripe/person/XY12345-RIPE.json
```

Example: Update an object



Sends the request with a header specifying the data format as JSON

```
$ curl -v --header "Content-type: application/json"
```

```
-d @file.json -X PUT
```

```
--key client-key.pem
```

```
--cert client-cert.pem
```

```
https://rest-cert.db.ripe.net/ripe/person/XY12345-RIPE.json
```

Sends the content of
"file.json" using the
PUT method

Example: Update an object



Sends the request with a header specifying the data format as JSON

```
$ curl -v --header "Content-type: application/json"
```

```
-d @file.json -X PUT
```

```
--key client-key.pem
```

```
--cert client-cert.pem
```

```
https://rest-cert.db.ripe.net/ripe/person/XY12345-RIPE.json
```

Sends the content of "file.json" using the PUT method

Use "client-key.pem" file for authentication

Example: Update an object



Sends the request with a header specifying the data format as JSON

```
$ curl -v --header "Content-type: application/json"
```

```
-d @file.json -X PUT
```

```
--key client-key.pem
```

```
--cert client-cert.pem
```

```
https://rest-cert.db.ripe.net/ripe/person/XY12345-RIPE.json
```

Sends the content of "file.json" using the PUT method

Use "client-key.pem" file for authentication

Use "client-cert.pem" file for client certificate verification

Example: Update an object



Sends the request with a header specifying the data format as JSON

```
$ curl -v --header "Content-type: application/json"
```

Sends the content of "file.json" using the PUT method

```
-d @file.json -X PUT
```

Use "client-key.pem" file for authentication

```
--key client-key.pem
```

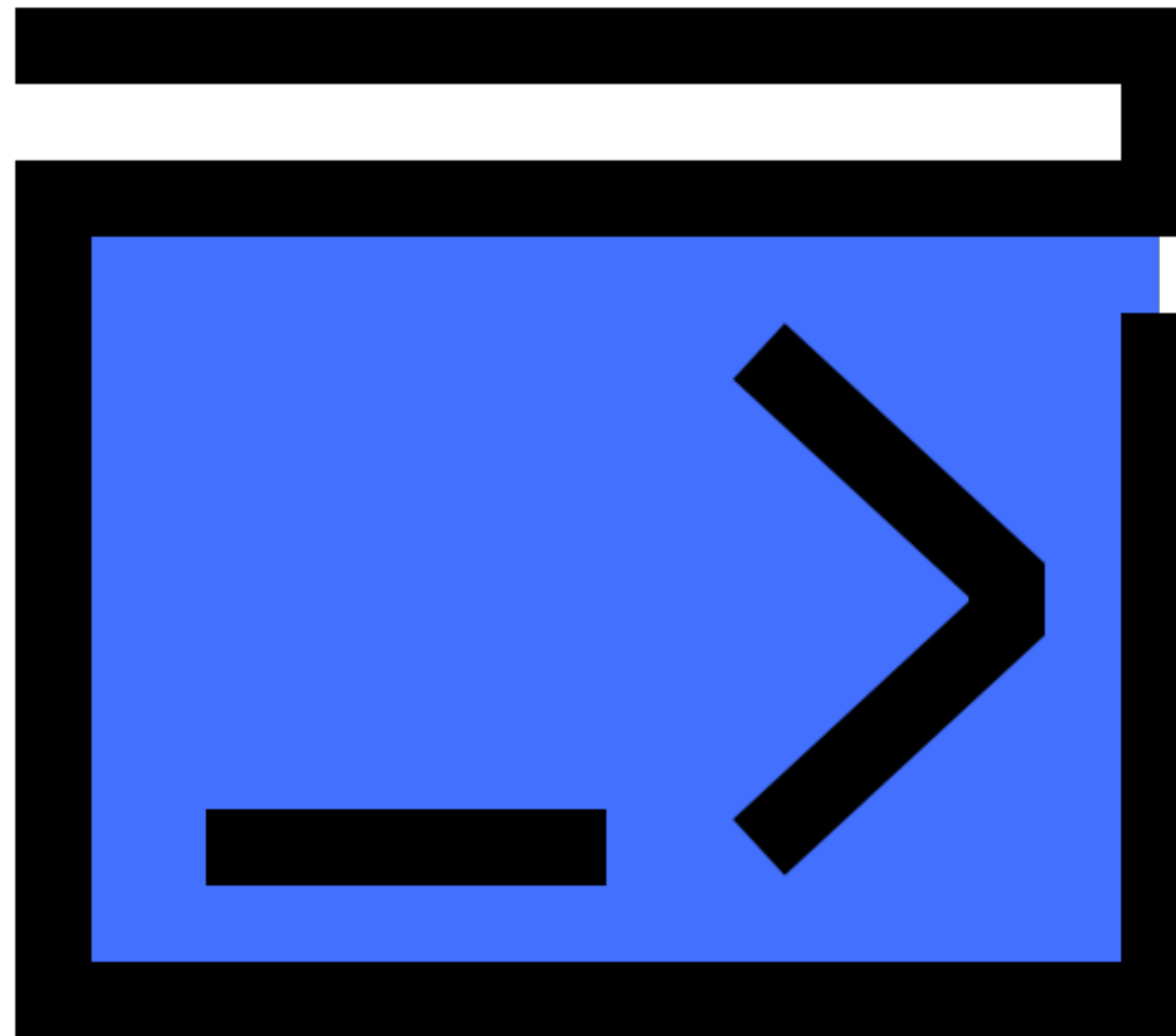
Use "client-cert.pem" file for client certificate verification

```
--cert client-cert.pem
```

```
https://rest-cert.db.ripe.net/ripe/person/XY12345-RIPE.json
```

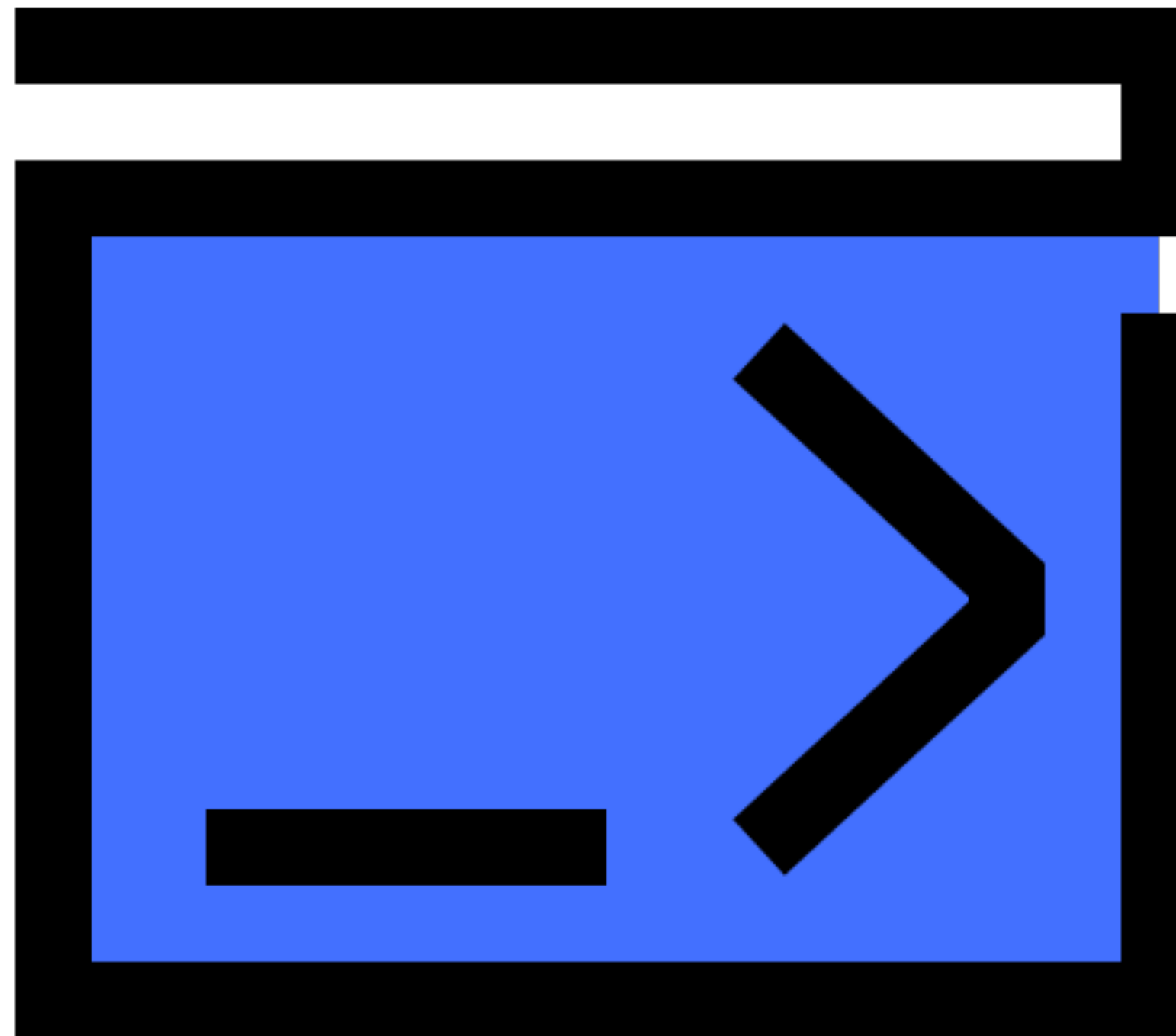
Specifies the REST API endpoint to interact with

Let's do it!



Open Terminal

Let's do it!



Open Terminal



Notification of Updates

“The only notifications you can't swipe away”

RIPE Database Update Notifications



- **Essential** for maintaining accurate and secure records
- Different attributes for **different notification needs**
- Helps **monitor changes** to your objects



What Notifications Can You Get?



upd-to:

Notifications for
failed updates



mnt-nfy:

Notifications for
successful updates

```
mntner:      EXAMPLE-MNT
admin-c:    ADM123-RIPE
upd-to:    updates@example.com
mnt-nfy:  notifications@example.com
auth:      SSO admin@example.com
mnt-by:    EXAMPLE-MNT
created:   2023-07-30T12:00:00Z
last-modified: 2023-07-30T12:00:00Z
source:    RIPE
```

In this example, '**updates@example.com**' will receive notifications for failed update attempts, while '**notifications@example.com**' will only receive notifications for successful updates.



What do the Notifications Contain?

- Type of update (creation, modification, deletion)
- Object type and primary key
- Changes made to the object
- Timestamp of the update
- IP address and SSO account

Notification of RIPE Database changes

1 message

RIPE Database Administration local <unread@ripe.net>

Reply-To: gviviers@ripe.net

To: gviviers@ripe.net

This is to notify you of changes in RIPE Database or object authorisation failures.

This message is auto-generated.
You can reply to this message to contact the person who made this change.

If you do not understand why we sent you this message, or for assistance or clarification please visit <https://www.ripe.net/s/notify>.

Change requested from:

- From-Host: 2001:67c:2e8:9::c100:14e6
- Date/Time: Tue Jun 20 08:49:51 2023Z

Some object(s) in RIPE Database that you either maintain or you are listed in as to-be-notified have been added, deleted or changed.

OBJECT BELOW MODIFIED:

```
@@ -7,5 +7,6 @@
nic-hdl:      GAV
+mnt-ref:    GAV-MNT
mnt-by:      GAV-MNT
created:     2009-03-13T07:58:22Z
-last-modified: 2017-09-06T11:32:09Z
+last-modified: 2023-06-20T08:49:51Z
source:      RIPE
```



The "notify:" Attribute

- Receive notifications for **any updates** to your objects
- Notifications sent **regardless** of who made the changes
- Useful for **monitoring** all activities related to your objects

```
person: Gerardo Viviers-Alink
remarks: "Where's the coffee?"
e-mail: gviviers@ripe.net
address: Stationsplein 11
address: 1012 AB Amsterdam
phone: +31 20 5354444
notify: alerts@ripe.net
nic-hdl: GAV123-RIPE
mnt-by: GAV-MNT
created: 2009-03-13T07:58:22Z
last-modified: 2023-06-20T08:49:51Z
source: RIPE
```


Special Notification Attributes



ref-nfy: (ORG)

Notification when the **ORG** is referenced



irt-nfy: (IRT)

Notification when the **IRT** is referenced or dereferenced

organisation: ORG-EX123-RIPE

ref-nfy: db-alerts@example.com

inetnum: 192.0.2.0 - 192.0.3.255
netname: EXAMPLE-NETWORK
country: XL
org: ORG-EX123-RIPE
admin-c: ADMIN-RIPE
tech-c: TECH-RIPE
status: ASSIGNED PA
mnt-by: EXAMPLE-MNT
mnt-irt: IRT-EXAMPLE-RIPE
created: 2023-07-30T12:00:00Z
last-modified: 2023-07-30T12:00:00Z
source: RIPE

irt: IRT-EXAMPLE-RIPE

irt-nfy: db-alerts@example.com

Unreachable Mailbox



- If the email address is unreachable, it is **added** to a list
- The RIPE Database **will not send** any more notifications
- To **remove** your address from the list, contact support:
 - Email: ripe-dbm@ripe.net
 - Through the contact form:
<https://www.ripe.net/about-us/support/contact/contact-us/>





Best Practices

- Use appropriate **notification attributes** for your needs
- **Regularly check** and **update** your contact information
- **Monitor notifications** to stay informed about changes to your objects
- **Use different attributes** for different levels of notification granularity



Let's do it!



Open Webupdates

Let's do it!



Open Webupdates



Controlling References to your Objects

“Your objects' restraining order against unwanted admirers”



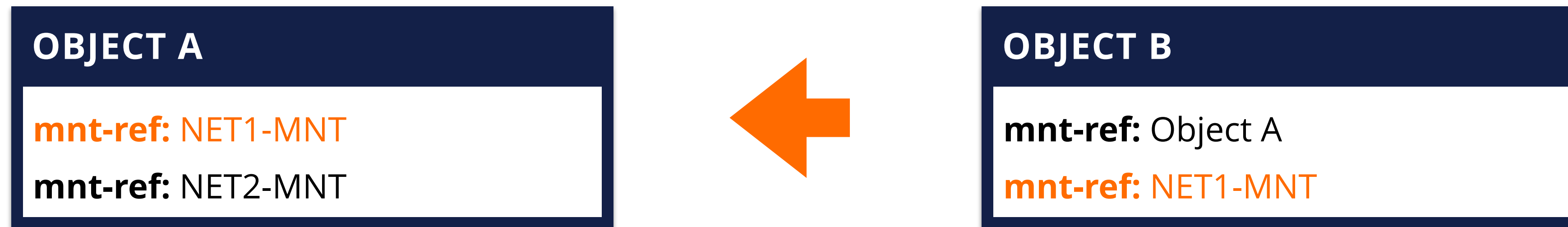
The "mnt-ref:" Attribute

- Controls **which maintainers** can reference your objects
- Applicable to **ORGANISATION, PERSON, ROLE, MNTNER**, and **IRT** objects
- **Enhances security** and **control** over your RIPE Database objects

```
person:          Gerardo Viviers-Alink
remarks:        "Where's the coffee?"
e-mail:         gviviers@ripe.net
address:        Stationsplein 11
address:        1012 AB Amsterdam
phone:          +31 20 5354444
mnt-ref:      GAV-MNT
nic-hdl:        GAV123-RIPE
mnt-by:         GAV-MNT
created:        2009-03-13T07:58:22Z
last-modified: 2023-06-20T08:49:51Z
source:        RIPE
```



How "mnt-ref:" Works

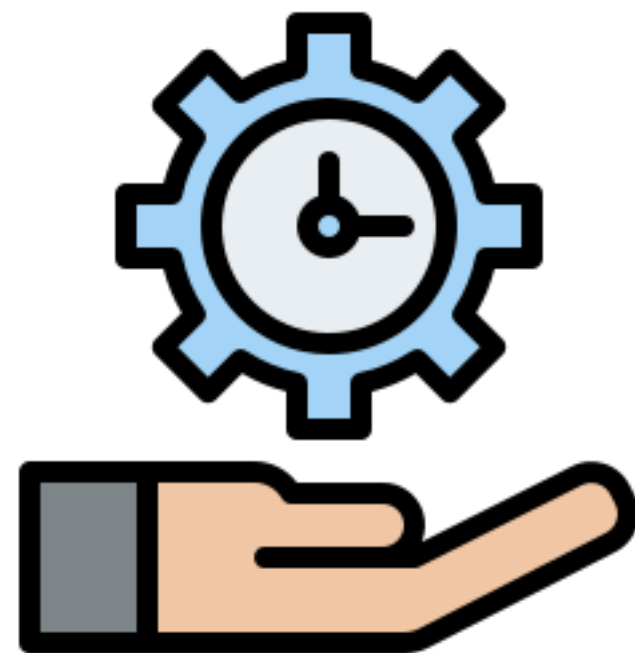


- Object B can reference Object A because NET1-MNT is listed in Object A's "mnt-ref:"
- If Object B's "mnt-by:" was not listed in Object A's "mnt-ref:", the reference would be rejected



Using "mnt-ref:" Effectively

- **Add to your objects** to restrict who can reference them
- Include collaborators' maintainers for joint projects
- **Regularly review** and **update** for security
- Align with your overall RIPE Database management strategy



Example: ORGANISATION Object



```
organisation:  ORG-EXAMPLE-RIPE
org-name:      Example Organisation
org-type:      LIR
address:       123 Example Street
address:       Exampleville
mnt-ref:       EXAMPLE-MNT
mnt-ref:       PARTNER-MNT
mnt-by:        RIPE-NCC-HM-MNT
mnt-by:        EXAMPLE-MNT
source:        RIPE
```

In this example, only **EXAMPLE-MNT** and **PARTNER-MNT** can create references to this ORGANISATION object.

Best Practices



- Use "mnt-ref:" on important objects (**ORG, PERSON, ROLE, MNTNER, IRT**)
- Be selective of **which maintainers** you include
- Keep your "mnt-ref:" list **up-to-date** as partnerships change
- Consider the implications before leaving "mnt-ref:" **unspecified**
- Use along with **other security measures** in the RIPE Database





Protecting References in SET Objects

“Teaching your objects to be picky about their friends”

"member-of:" and "mbrs-by-ref:" Attributes



- **SET objects**

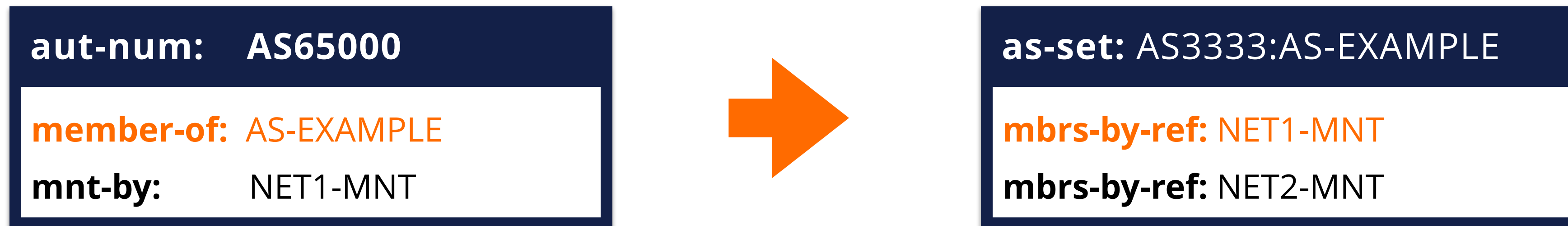
- Collections of other objects
- AS-SET, ROUTE-SET, RTR-SET, PEERING-SET, FILTER-SET

- "**member-of:**" used in objects wanting to join a SET

- "**mbrs-by-ref:**" used in SET objects to control membership

```
as-set: AS3333:as-exampleset
members: AS65001
members: AS65002
members: AS65003
members: AS65004
members: AS65005
admin-c: EXAMPLE-ADMIN
tech-c: EXAMPLE-TECH
mnt-by: EXAMPLE-MNT
source: RIPE
```

How it Works



- aut-num AS65000 **requests membership** in AS3333:AS-EXAMPLE
- AS-EXAMPLE **allows it** because NET1-MNT is in “mbrs-by-ref:”



"member-of:" Attribute

- Used in: **AUT-NUM**, **ROUTE**, **ROUTE6**, **INET-RTR** objects
- Indicates desire to be part of a SET
- Can reference multiple SETs

```
aut-num:      AS65000
member-of:    AS3333:as-example
member-of:    AS65050:as-customer
mnt-by:       EXAMPLE-MNT
source:       RIPE
```

```
route6:       2001:db8::/32
origin:       AS65020
member-of:    AS65090:ROUTE6-SET
mnt-by:       EXAMPLE-MNT
source:       RIPE
```



"mbrs-by-ref:" Attribute





- Used in: **AS-SET, ROUTE-SET, RTR-SET** objects
- Lists maintainers allowed to add members
- Acts as a protection mechanism

```
as-set: AS3333:as-example
mbrs-by-ref: EXAMPLE-MNT
mbrs-by-ref: PARTNER-MNT
mnt-by: EXAMPLE-MNT
source: RIPE
```






```
route-set: RS-EXAMPLE-SET
mbrs-by-ref: AS65030
mbrs-by-ref: AS65031
mbrs-by-ref: AS65032
mnt-by: EXAMPLE-MNT
source: RIPE
```




Benefits

-  Enhanced control over SET membership
-  Prevention of unauthorised additions
-  Distributed management of SET membership
-  Improved security for your network resources

Best Practices

-  Use "mbrs-by-ref:" in all of your SET objects
-  Only list trusted maintainers in "mbrs-by-ref:"
-  Use "member-of:" when adding objects to a SET
-  Regularly review and update your SET memberships
-  Keep documentation of your SET structure and policies



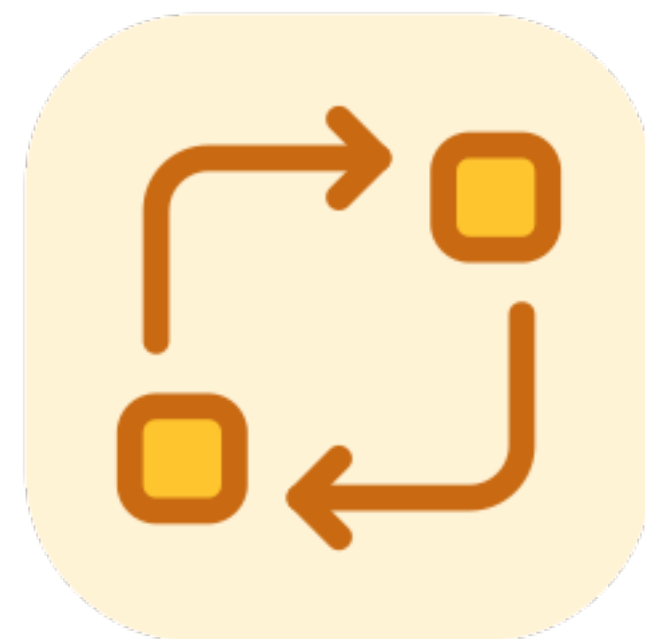
AS-SETs and the AUT-NUM object

“The bouncer deciding who gets into the AS-SET party”



AS-SETs and AUT-NUM Objects

- **AS-SET:** Collection of Autonomous System Numbers (ASNs)
- **AUT-NUM:** Represents individual Autonomous Systems
- Relationship between AS-SETs and AUT-NUM objects
- Naming requirements and authorisation process



AS-SET Naming Requirements



- Must start with "as-" (lowercase)
- Can contain letters, digits, underscores: "_", and hyphens: "-"
- Last character must be a letter or digit
- **Hierarchical names are mandatory**
- Total length should not exceed 80 characters

```
as-set: AS64496:as-customers
members: AS64497, AS64498, AS64499
members: AS64496:as-gold-customers
members: AS64496:as-silver-customers
mbrs-by-ref: EXAMPLE-MNT
mnt-by: EXAMPLE-MNT
source: RIPE
```



Hierarchical AS-SET Names

- Start with an AS number, followed by a colon: ":"
- End with a name
- At least one part must be an actual SET name (starting with "as-")
- Components separated by colons: ":"
- All set name components must be AS-SET names

Valid examples:

```
AS3333:as-customers
```

```
AS3333:as-transit:as-copper
```

```
AS1234:AS5678:as-peer
```

Authorisation from AUT-NUM



```
AS [number] : as- [name]
```

- The AS-SET name must start with the authorising AS number
- This AS number is followed by a colon (:) and the as-set name
- The as-set name must begin with "as-" (lowercase)
- This convention links the AS-SET to its authorising ASN
- Only the AS holder can create and manage this AS-SET



Best Practices

- Use **clear, descriptive** hierarchical names for AS-SETs
- Maintain **a logical structure** in your AS-SET hierarchy
- Regularly **review** and **update** AS-SET memberships
- Ensure proper **authorisation** before adding ASNs to AS-SETs
- **Document** your AS-SET structure and policies

```
AS3333:as-root
├── AS3333:as-customers
│   ├── AS3333:as-customer1
│   └── AS3333:as-customer2
└── AS3333:as-peers
```



What's New in the RIPE Database?

“Teaching an old database new bits”



Two New inetnum Status

- **AGGREGATED-BY-LIR**

- Allows you to group multiple assignments under a single INETNUM object
- Same as in INET6NUM (IPv6) objects, but “assignment-size:” is optional

- **ALLOCATED-ASSIGNED PA**

- Allows holders of very small PA allocations (i.e. /24) to register the whole allocation as one assignment
- Reduces the amount of objects to maintain for these LIRs

Benefits of AGGREGATED-BY-LIR



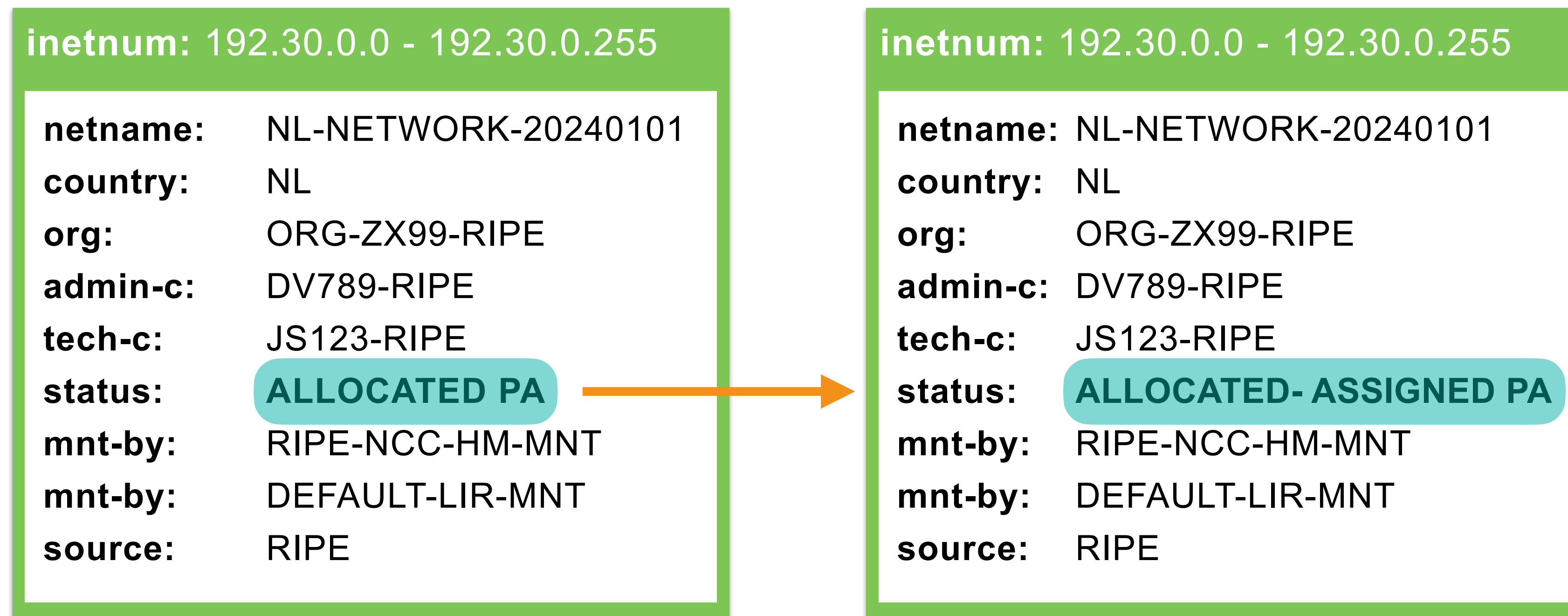
- Reduces administrative workload for LIRs
- Simplifies registration of multiple small assignments
- Encourages proper assignment registration
- Helps with GDPR compliance

```
inetnum:      192.0.2.0 - 192.0.3.255
netname:      EXAMPLE-NET-AGGR
descr:        Aggregated assignments
country:      NL
org:          ORG-EISP1-RIPE
admin-c:      ADMIN-EXAMPLE
tech-c:       TECH-EXAMPLE
status:    AGGREGATED-BY-LIR
mnt-by:       EXAMPLE-MNT
created:      2023-08-15T10:00:00Z
last-modified: 2023-08-15T10:00:00Z
source:       RIPE
```



Status: ALLOCATED-ASSIGNED PA

- Registers a whole assignment for small IPv4 allocations
- LIR changes status in the RIPE Database
- It is seen both as ALLOCATED PA *and* ASSIGNED PA





Any Demos You Want To See?

DEMOS



Questions



academy@ripe.net

gviviers@ripe.net



Useful Links

- **RIPE Database Documentation**
 - <https://apps.db.ripe.net/docs>
- **RIPE Database Syncupdates**
 - <https://apps.db.ripe.net/db-web-ui/syncupdates>
- **OpenSSL**
 - <https://docs.openssl.org/3.2/man7/openssl-guide-introduction/>