



RPKI MIRO & RTRlib

RIPE 74, Budapest

Andreas Reuter, Matthias Wählisch
Freie Universität Berlin

`{andreas.reuter,m.waehlich}@fu-berlin.de`

Thomas Schmidt
HAW Hamburg

`t.schmidt@haw-hamburg.de`

RPKI Overview

RPKI Overview

- Resource Certificate attests Internet-Resource ownership

RPKI Overview

- Resource Certificate attests Internet-Resource ownership
- Route Origin Authorizations (ROAs) authorize AS to legitimately announce prefixes

RPKI Overview

- Resource Certificate attests Internet-Resource ownership
- Route Origin Authorizations (ROAs) authorize AS to legitimately announce prefixes
- ROAs are issued using Resource Certificates

RPKI Overview

**Global
RPKI**

RIPE



ARIN



...

LIR



NIR



ROA
ASN: 65535
Prefix:
192.168.1.0/24



RPKI Overview

Global RPKI



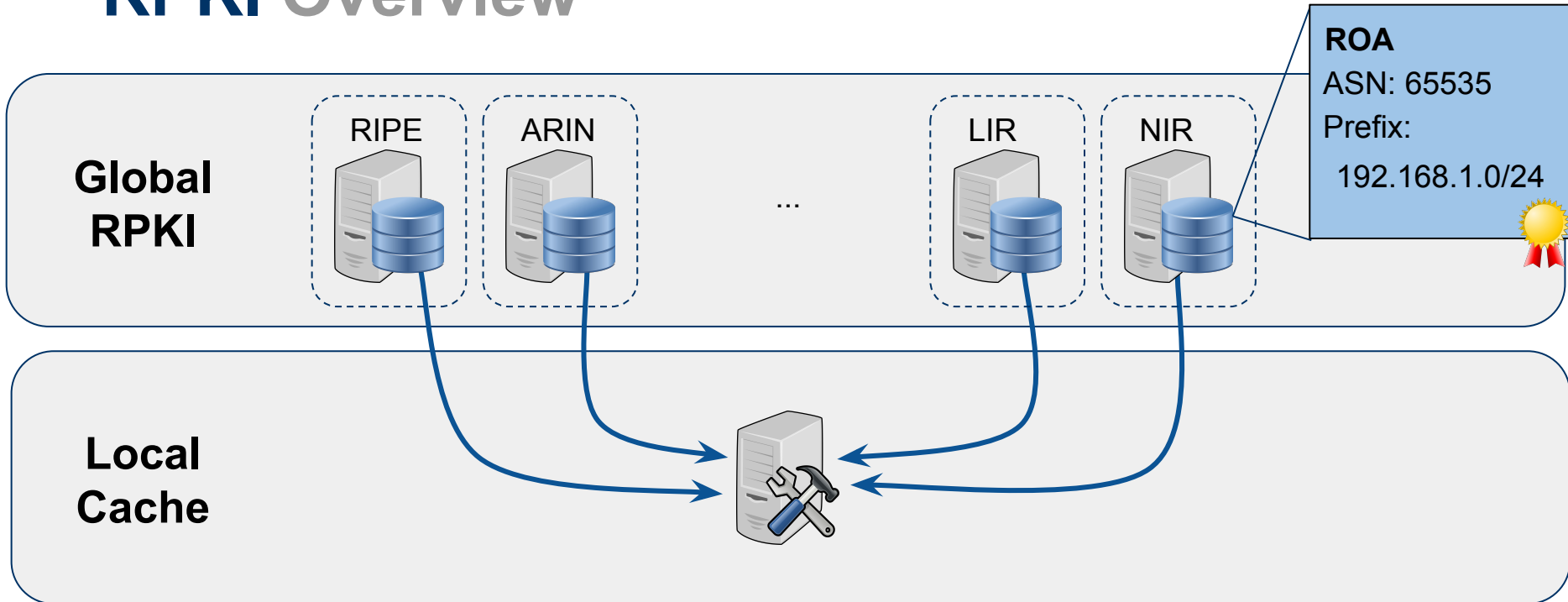
ROA
ASN: 65535
Prefix:
192.168.1.0/24



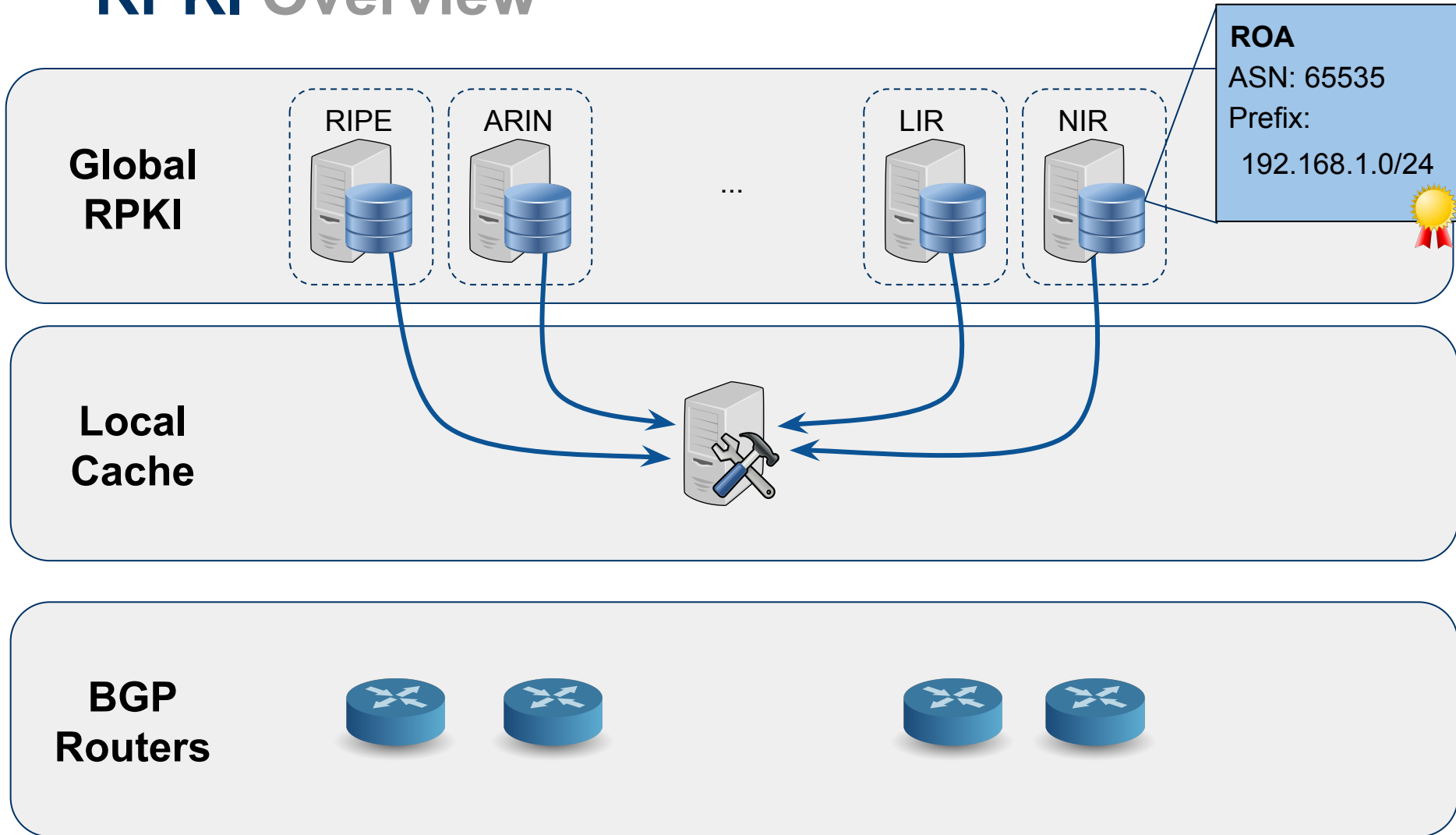
Local Cache



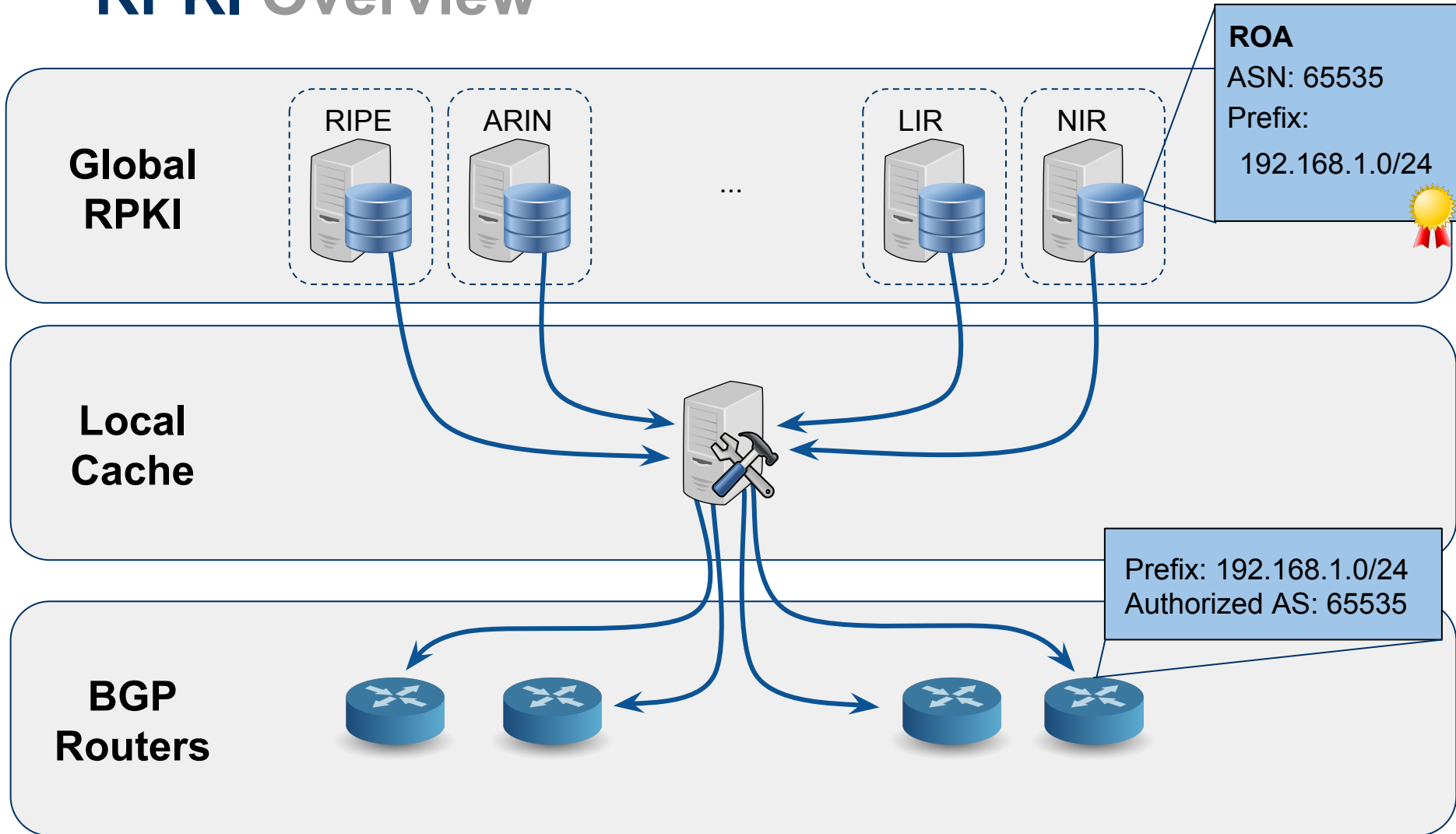
RPKI Overview



RPKI Overview



RPKI Overview



MIRO Overview

Monitoring and Inspection of **RPKI** Objects

MIRO Overview

Monitoring and Inspection of RPKI Objects

- **Validator**: Downloads, validates, and exports the global RPKI (not just ROAs)
 - ◆ Export to JSON, or use Java API

MIRO Overview

Monitoring and Inspection of RPKI Objects

- **Validator:** Downloads, validates, and exports the global RPKI (not just ROAs)
 - ◆ Export to JSON, or use Java API

- **Browser:** Web application that allows inspection and filtering of RPKI objects
 - ◆ Can deploy yourself, or use version hosted by us

MIRO Overview

Monitoring and Inspection of RPKI Objects

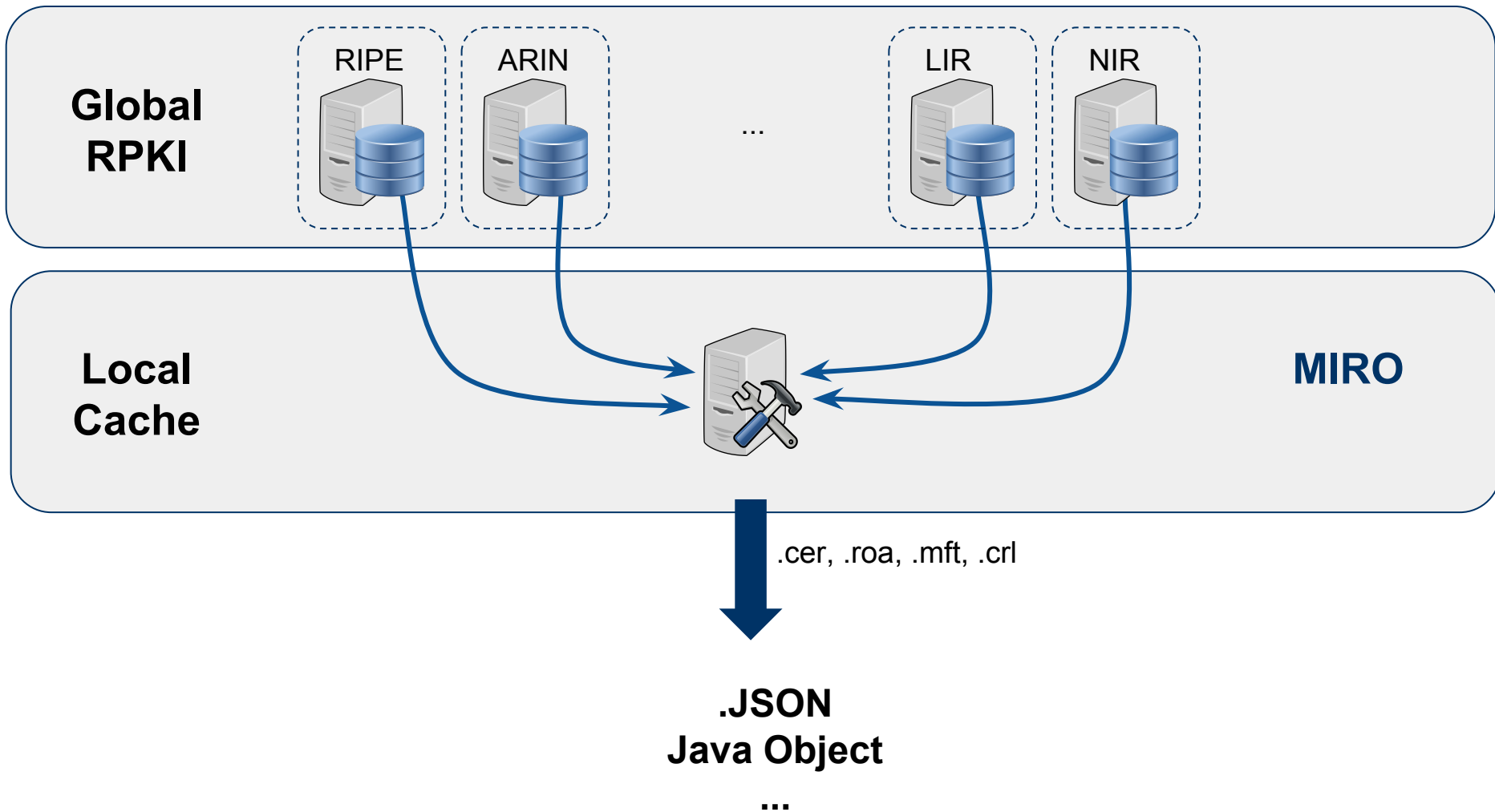
- **Validator:** Downloads, validates, and exports the global RPKI (not just ROAs)
 - ◆ Export to JSON, or use Java API

- **Browser:** Web application that allows inspection and filtering of RPKI objects
 - ◆ Can deploy yourself, or use version hosted by us

MIRO uses the *rpki-commons* library from RIPE NCC:

 github.com/RIPE-NCC/rpki-commons

RPKI Overview



RPKI Browser: Overview

RPKI Repository Browser RPKI Browser Statistics About

Filter Clear Filter List View RIPE Download (JSON)

2017-05-10T13:00:38.359+02:00

- ripencc-ta.cer
 - b1314c89c8803a127d62c83f01292a0474b9e6.cer
 - nb3vJ8Y2osQK65MPYzB1FVDVisA.cer
 - VtOacghft9GFjzVE1rd6Fe6FeHs.roa
 - FyOGwXr4TejAN1WQwc96Moll_U8.cer
 - 63_SFzkM2JkJEPAbyEETIbBnAQM.cer
 - ETW8vZudAxfyRLRFXE5Z4fwuHBE.cer
 - gPBfgxtObD4GUrPLrVWVhionLCg.cer
 - hWdd9pqB77wcl2Nc_cRqM8nvoA.cer
 - cxeUNuJgY5kxHPwsT_o3ITRDrYM.cer
 - gdXIZQzVmGw9svwfmC3f44pBzBs.cer
 - Xd26J7F3ZSDRHYRjyEVFiYSc23Q.cer
 - 1-7rdwb8Pxp2W-u3wQqs1Ka-8AM.cer
 - l6rxYswnmaJyu-uhm7aO0lezoQ.cer
 - T-kEiOzqi_jq0LJVPhFGvVP9ab8.cer
 - tuLyNdH6Cw5Wws-PfvCDOUzHDMU.cer
 - dyFv2Lm0i4JwDczQPSZM3KR0_s.cer
 - 1ah40CeqmR-KI4aWIBR7FrfSpDs.cer
 - ghoZ50_u51_qwmZcq1s_QfxmL4.cer
 - ClqAWfCu9wGXne5Q9G8277QsHZE.cer
 - JBRF2fpkLQT2MtECH4V1Yt1hs3k.cer
 - efWBYsDkn9HXmAEVfN_nXM6Ti8.cer
 - RedSIVoUMKmD5pom1wVyRro5NKc.cer
 - EfnUyEhjfVSczGjllrnkqVcAOG4.cer
 - ouefFASocCHq65LaNDiySmZ_kus.cer

Certificate Manifest CRL

Validation Status: PASSED

Validity Period: 2017-05-09T13:26:32.000Z - 2022-05-09T13:26:32.000Z

Errors: None

Warnings: None

Subject: CN=ripencc-ta

SKI: E8552B1FD6D1A4F7E404C6D8E5680D1EBC163FC3

Issuer: [CN=ripencc-ta](#)

AKI: None

SerialNr: 192

Filename: ripencc-ta.cer

Location: rsync://rpk.ripe.net/ta/ripencc-ta.cer

EE: false

CA: true

TA: true

Public Key: Sun RSA public key, 2048 bits
 modulus: 26417507841994249002335275349968358018749945254465391
 205926068761009836723958150757643247386671351211774764234956599
 2964744256283187220710001310255363564818053828507479750269602219
 4674983906433456463101948831121153251689906051382334679573755633
 0511479452362395992462127370296320200221247954188869800688659247
 3360864501955776640541896515995072787220387140217946690313140685
 1684699020876306818620333780378379873013155080509726827201218992
 5782711757466803649446547687051295032345991523376592529203855820
 3290181443214927346958843948631267452037556758611980929057196232
 6274886722691631406065925764413315144468359192704599
 public exponent: 65537

[ASCII download](#)

- Resources**
- AS7
 - AS28
 - AS137
 - AS224
 - AS248-AS251
 - AS261
 - AS286
 - AS288
 - AS294
 - AS375
 - AS378
 - AS513
 - AS517
 - AS528-AS529
 - AS544
 - AS553
 - AS559
 - AS565
 - AS590
 - AS593
 - AS669

RPKI Browser: Control Bar

RPKI Repository Browser RPKI Browser Statistics About

Filter Clear Filter List View RIPE Download (JSON) 2017-05-10T13:00:38.359+02:00

ripe-ncc-ta.cer Certificate Manifest CRL

Validation Status: PASSED
 Validity Period: 2017-05-09T13:26:32.000Z - 2022-05-09T13:26:32.000Z
 Errors: None

Resources
 AS28
 AS137

Filter Clear Filter List View RIPE Download (JSON)

AKI: None
 SerialNr: 192
 Filename: ripe-ncc-ta.cer
 Location: rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer
 EE: false
 CA: true
 TA: true
 Public Key: Sun RSA public key, 2048 bits
 modulus: 26417507841994249002335275349968358018749945254465391
 2059260687610098367239581507576432473866713512117774764234956599
 2964744256283187220710001310255363564818053828507479750269602219
 4674983906433456463101948831121153251689906051382334679573755633
 0511479452362395992462127370296320200221247954188869800688659247
 3360864501955776640541896515995072787220387140217946690313140685
 1684699020876306818620333780378379873013155080509726827201218992
 5782711757466803649446547687051295032345991523376592529203855820
 3290181443214927346958843948631267452037556758611980929057196232
 6274886722691631406065925764413315144468359192704599
 public exponent: 65537

[ASCII download](#)

AS288
 AS294
 AS375
 AS378
 AS513
 AS517
 AS528-AS529
 AS544
 AS553
 AS559
 AS565
 AS590
 AS593
 AS669

RPKI Browser: Certificate Tree

RPKI Repository Browser RPKI Browser

Filter Clear Filter List View RIPE Download (OFF)

ripe-ncc-ta.cer

- ▶ b1314c89c8803a127d62c83f3f01292a0474b9e6.cer
 - ▶ nb3vJ8Y2osQK65MPYzB1FVDVisA.cer
 - ▶ VtOacghft9GFjzVE1rd6Fe6FeHs.roa
 - ▶ FyOGwXr4TejAN1WQwc96Moll_U8.cer
 - ▶ 63_SFzkM2JkJEPAbYEETIbBnAQM.cer
 - ▶ ETW8vZudAxfyRLRFXE5Z4fwuHBE.cer
 - ▶ gPBfgxtObD4GUrpLirWVhionLCg.cer
 - ▶ hWdd9pqB77wcl2Nc__cRqM8nvoA.cer

Certificate

Validation Status: Validity Errors: Warning Subject: SKI: Issuer: AKI: Serial Number: File Name: Location: E: C: TA: Public Key

▶ **ripe-ncc-ta.cer**

- ▶ b1314c89c8803a127d62c83f3f01292a0474b9e6.cer
 - ▶ nb3vJ8Y2osQK65MPYzB1FVDVisA.cer
 - ▶ VtOacghft9GFjzVE1rd6Fe6FeHs.roa
 - ▶ FyOGwXr4TejAN1WQwc96Moll_U8.cer
 - ▶ 63_SFzkM2JkJEPAbYEETIbBnAQM.cer
 - ▶ ETW8vZudAxfyRLRFXE5Z4fwuHBE.cer
 - ▶ gPBfgxtObD4GUrpLirWVhionLCg.cer
 - ▶ hWdd9pqB77wcl2Nc__cRqM8nvoA.cer

1684699020876306818620333780378379873013155080509726827201218992
 5782711757466803649446547687051295032345991523376592529203855820
 3290181443214927346958843948831267452037556758611980929057196232
 6274886722691631406065925764413315144468359192704599
 public exponent: 65537

[ASCII download](#)

AS565
AS590
AS593
AS669

RPKI Browser: ROA Content

RPKI Repository Browser RPKI Browser Statistics About

Filter Clear Filter List View RIPE Download (JSON) 2017-05-10T14:02:45.021+02:00

- ripencc-ta.cer
 - b1314c89c8803a127d62c83f3f01292a0474b9e6.cer
 - nb3vJ8Y2osQK65MPYzB1FVDVisA.cer
 - VtOacghf9GFjzVE1rd6Fe6FeHs.roa**
 - FyOGwXr4TejAN1WQwc96Moll_U8.cer
 - 63_SFzkM2JkJEPAbYEEETibBnAQM.cer
 - ETW8vZudAxfyRLRFXE5Z4fwuHBE.cer
 - gPBfgxtObD4GUrpLirWVhionLCg.cer
 - hWdd9ppqB77wcl2Nc_cRqM8nvoA.cer
 - cxeUNuJgY5kxHPwsT_o3ITRDryM.cer
 - gdXIZQzVmGw9svwfmC3f44pBzBs.cer
 - Xd26J7F3ZSDRHyrjyEVFiYSc23Q.cer
 - 1-7rdwb8Pxp2W-u3wQqs1Ka-8AM.cer
 - l6rxYswnmaJyu-uhm7aO0lezoQ.cer
 - T-kEiOzqi_jq0LJVPhFGvVP9ab8.cer
 - tuLyNdH6Cw5Wws-PfvCDOUzHDMU.cer
 - dyFv2Lm0Oi4JwDCzQPSZM3KR0_s.cer
 - 1ah40CeqmR-KI4aWIBR7FrfSpDs.cer
 - ghoZ50_u51_qwmZcq12s_QfxmL4.cer
 - ClqAWfCu9wGXne5Q9G8277QsHZE.cer
 - JBRF2fplQT2MECH4V1Yt1hs3k.cer
 - efWBYsDkN9HXmAEVfN_nXM6Tl8.cer
 - RedSIVoUMKmD5pom1wVyRro5NKc.cer
 - EfnUyEhjfvSczGjilmkqVcAOG4.cer

ROA EE Certificate

Filename: VtOacghf9GFjzVE1rd6Fe6FeHs.roa
 Location: rsync://rpk.ripe.net/repository/ARIN/2B/8aba71-3ba8-4b8d-8eb6-346a3ec1868c/1/

Validation Status: PASSED
 Errors: None
 Warnings: None
 Validity Period: 2017-03-01T16:10:52.000Z - 2018-07-01T00:00:00.000Z
 Signing Time: 2017-03-01T16:10:52.000Z
 ASN: AS8758

[ASCII download](#)

Prefix	Max. Length
146.185.64.0/19	19

RPKI Browser: ROA Content

RPKI Repository Browser RPKI Browser Statistics About

Filter Clear Filter List View RIPE

- ripe-ncc-ta.cer
 - b1314c89c8803a127d62c83f3f01292a0474b...
 - nb3vJ8Y2osQK65MPYzB1FVDVisA.cer
 - VtOacghf9GFjzVE1rd6Fe6FeHs.roa**
 - FyOGwXr4TejAN1WQwc96Moll_U8.cer
 - 63_SFzkM2JkJEPAbYEETibBnAQM.cer
 - ETW8vZudAxfyRLRFXE5Z4fwuHBE.cer
 - gPBfgxtObD4GUrpLirWVhionLCg.cer
 - hWdd9pqB77wcl2Nc_cRqM8nvoA.cer
 - cxeUNuJgY5kxHPwsT_o3ITRDryM.cer
 - gdXIZQzVmGw9svwfmC3f44pBzBs.cer
 - Xd26J7F3ZSDRHyrjyEVFiYSc23Q.cer
 - 1-7rdwb8Pxp2W-u3wQqs1Ka-8AM.cer
 - l6xrxYswmaJyu-uhm7aO0lezoQ.cer
 - T-kEiOzqi_jq0LJVPhFGvVP9ab8.cer
 - tuLyNdH6Cw5Wws-PfvCDOUzHDMU.cer
 - dyFv2Lm0Oi4JwDCzQPSZM3KR0_s.cer
 - 1ah40CeqmR-KI4aWIBR7FrSpDs.cer
 - ghoZ50_u51_qwmZcq12s_QfxmL4.cer
 - ClqAWfCu9wGXne5Q9G8277QsHZE.cer
 - JBRF2fpkLQT2MECH4V1Yt1hs3k.cer
 - efWBYsDkN9HXmAEVfvN_nXM6Tl8.cer
 - RedSIVoUMKmD5pom1wVyRro5NKc.cer
 - EfnUyEhjfvSczGjilmkqVcAOG4.cer

Validation Status: PASSED

Errors: None

Warnings: None

Validity Period: 2017-03-01T16:10:52.000Z - 2018-07-01T00:00:00

Signing Time: 2017-03-01T16:10:52.000Z

ASN: AS8758

[ASCII download](#)

Prefix	Max. Length
146.185.64.0/19	19

02:45.021+02:00

MIRO Links

Monitoring and Inspection of RPKI Objects

- Try it at **rpki-browser.realmv6.org**
- To deploy it yourself, check out:
github.com/rpki-miro/MIRO.Browser
- MIT Licence

For bug reports and feature requests:

 **github.com/rpki-miro**

For direct contact:

andreas.reuter@fu-berlin.de

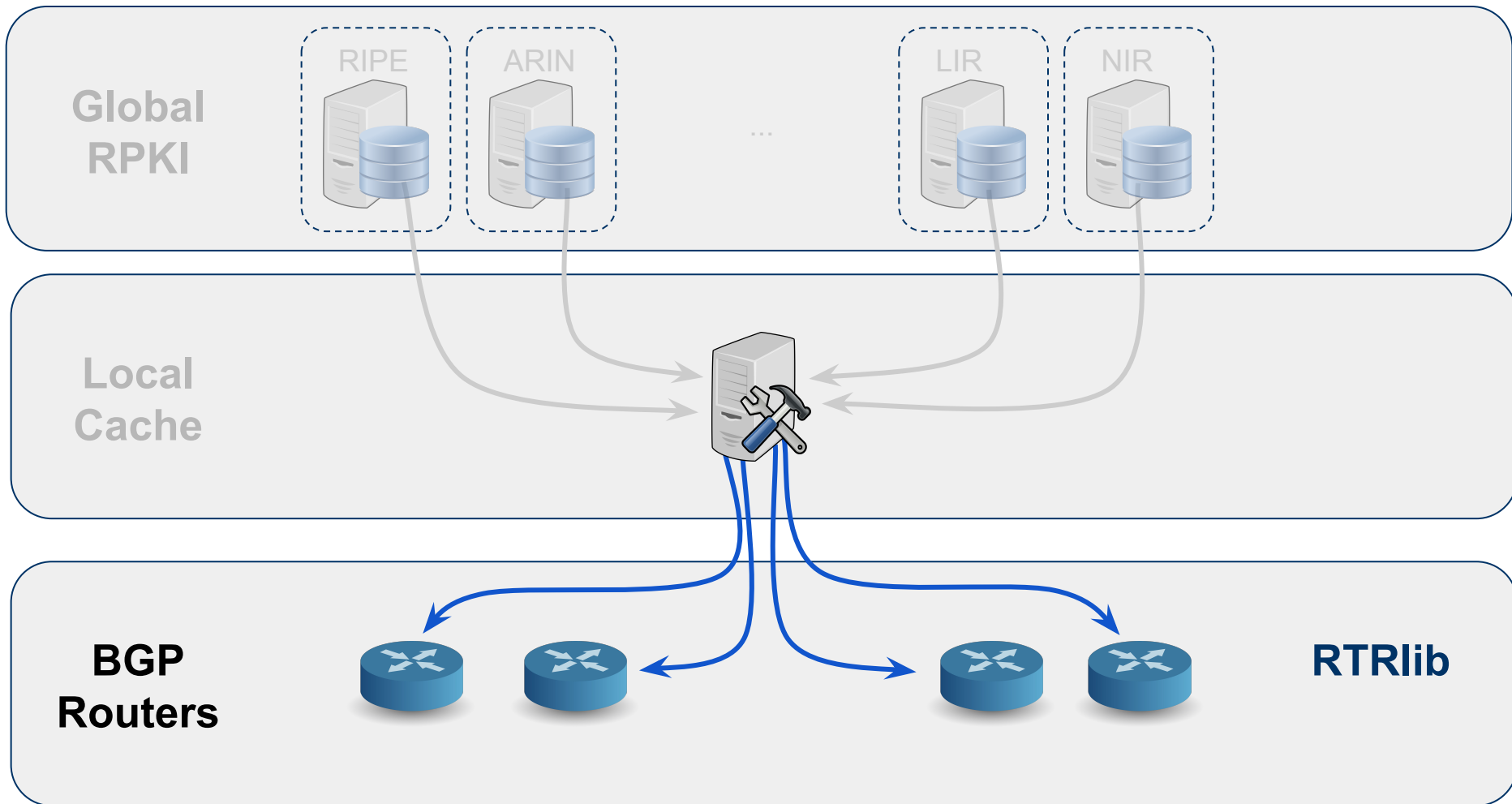
RTRlib Overview

→ Lightweight, open-source C library

RTRlib Overview

- Lightweight, open-source C library
- Implements client part of RPKI/RTR protocol
 - ◆ Origin Validation: RFC 6810, RFC 6811
 - ◆ Prepared for BGPsec: draft-ietf-sidr-rpki-rtr-rfc6810-bis

RPKI Overview



RTRlib Overview

- Lightweight, open-source C library

- Implements client part of RPKI/RTR protocol
 - ◆ Origin Validation: RFC 6810, RFC 6811
 - ◆ Prepared for BGPsec: draft-ietf-sidr-rpki-rtr-rfc6810-bis

- Provides fresh ROA data w/o bound to a specific cache server implementation
 - ◆ Useful for routing software developers

RTRlib Overview

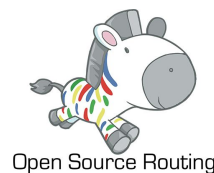
- Lightweight, open-source C library

- Implements client part of RPKI/RTR protocol
 - ◆ Origin Validation: RFC 6810, RFC 6811
 - ◆ Prepared for BGPsec: draft-ietf-sidr-rpki-rtr-rfc6810-bis

- Provides fresh ROA data w/o bound to a specific cache server implementation
 - ◆ Useful for routing software developers
 - ◆ Useful when developing monitoring tools

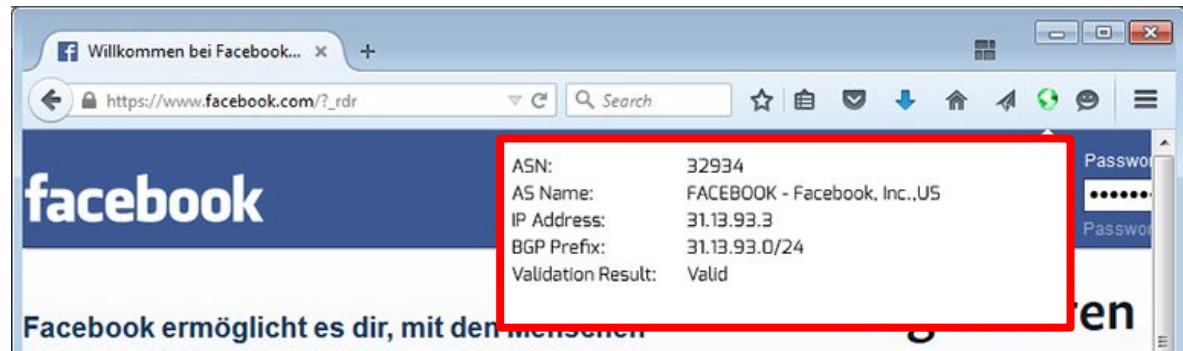
RTRlib Overview

- Lightweight, open-source C library
- Implements client part of RPKI/RTR protocol
 - ◆ Origin Validation: RFC 6810, RFC 6811
 - ◆ Prepared for BGPsec: draft-ietf-sidr-rpki-rtr-rfc6810-bis
- Provides fresh ROA data w/o bound to a specific cache server implementation
 - ◆ Useful for routing software developers
 - ◆ Useful when developing monitoring tools

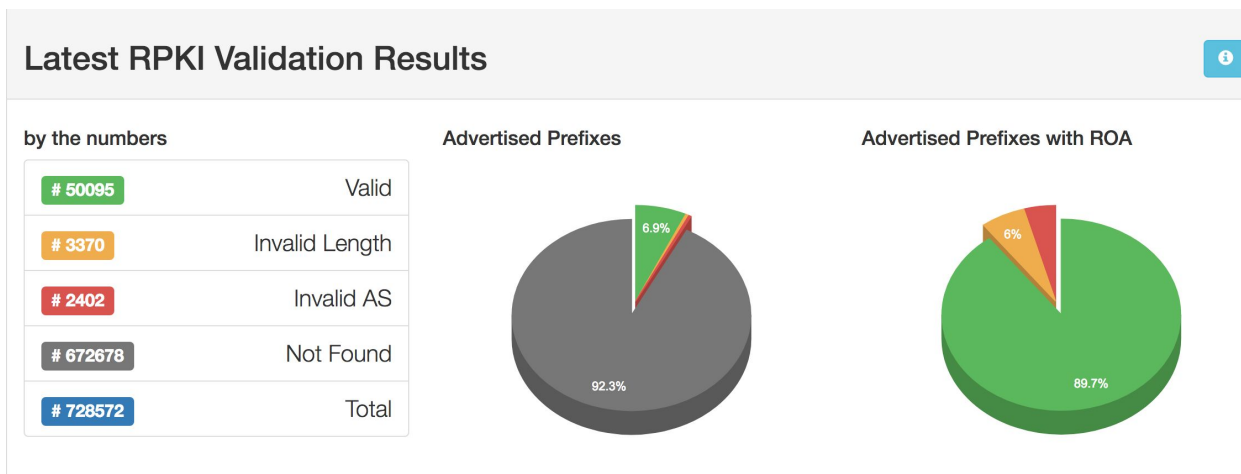


RTRlib Tools

RPKI Browser Plugin



RPKI Realtime Dashboard



RTRlib Links

- More information at **rtrlib.realmv6.org**
- Find the code, and tools using the RTRLib:
 - 🔗 **github.com/rtrlib**
- MIT Licence

Summary

RPKI MIRO

rpki-miro.realmv6.org

 github.com/rpki-miro

RTRlib

rtrlib.realmv6.org

 github.com/rtrlib

Thanks to our supporters and contributors

SPONSORED BY THE



Federal Ministry
of Education
and Research



Fabian Holler, Nils Bars,
Sebastian Meiling, Colin Sames,
Michael Roethke, Martin Winter,
Mehmet Ceyran, Robert Schmidt,
Pavel Tvrdík