Introducing

JDR.jl:

Interactively Analyzing the RPKI

MAT-WG @RIPE 82 - virtual

Luuk Hendriks

luuk@nlnetlabs.nl

NLNETLABS

JDR.jl: Interactively Analyzing the RPKI

TL;DR:
we want to explore data published in the RPKI in an interactive, iterative and somewhat performant way.

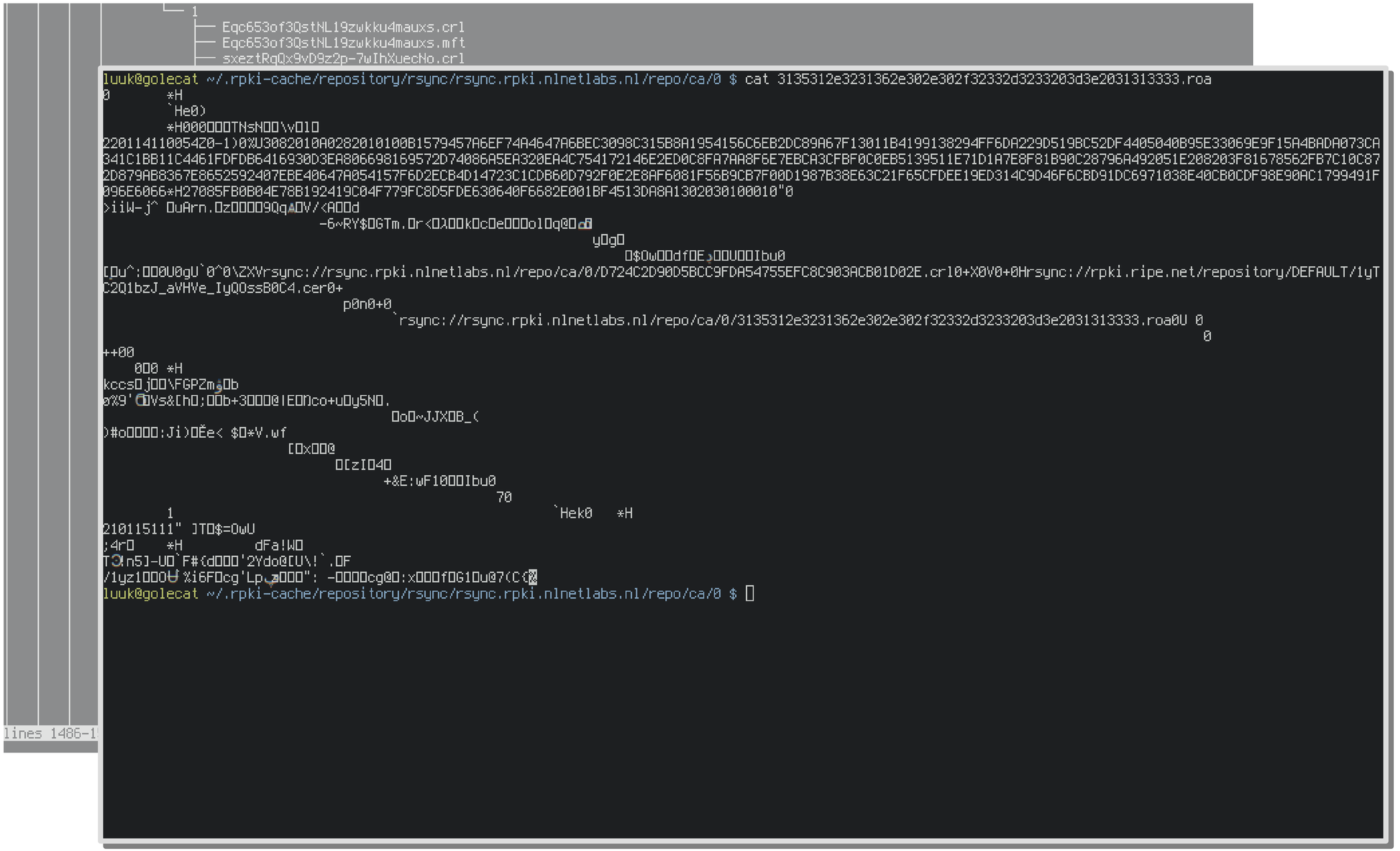
JDR.jl: Interactively Analyzing the RPKI

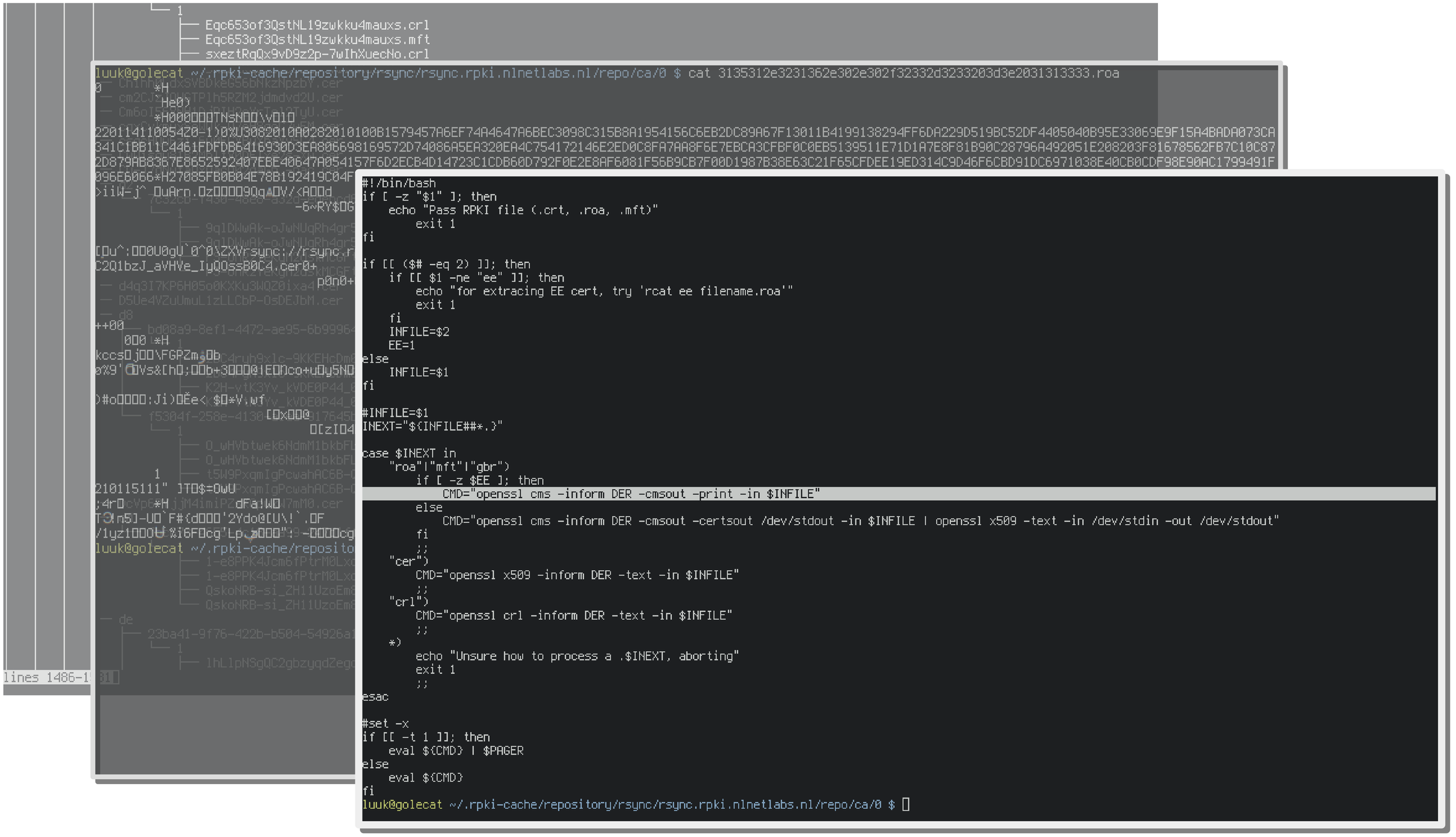
Resource **P**ublic **K**ey **I**nfrastructure, a public, distributed repository containing attestations with regards to routing intents.

“ASN 211321 is authorized to announce prefix 2001:db8:123::/48”

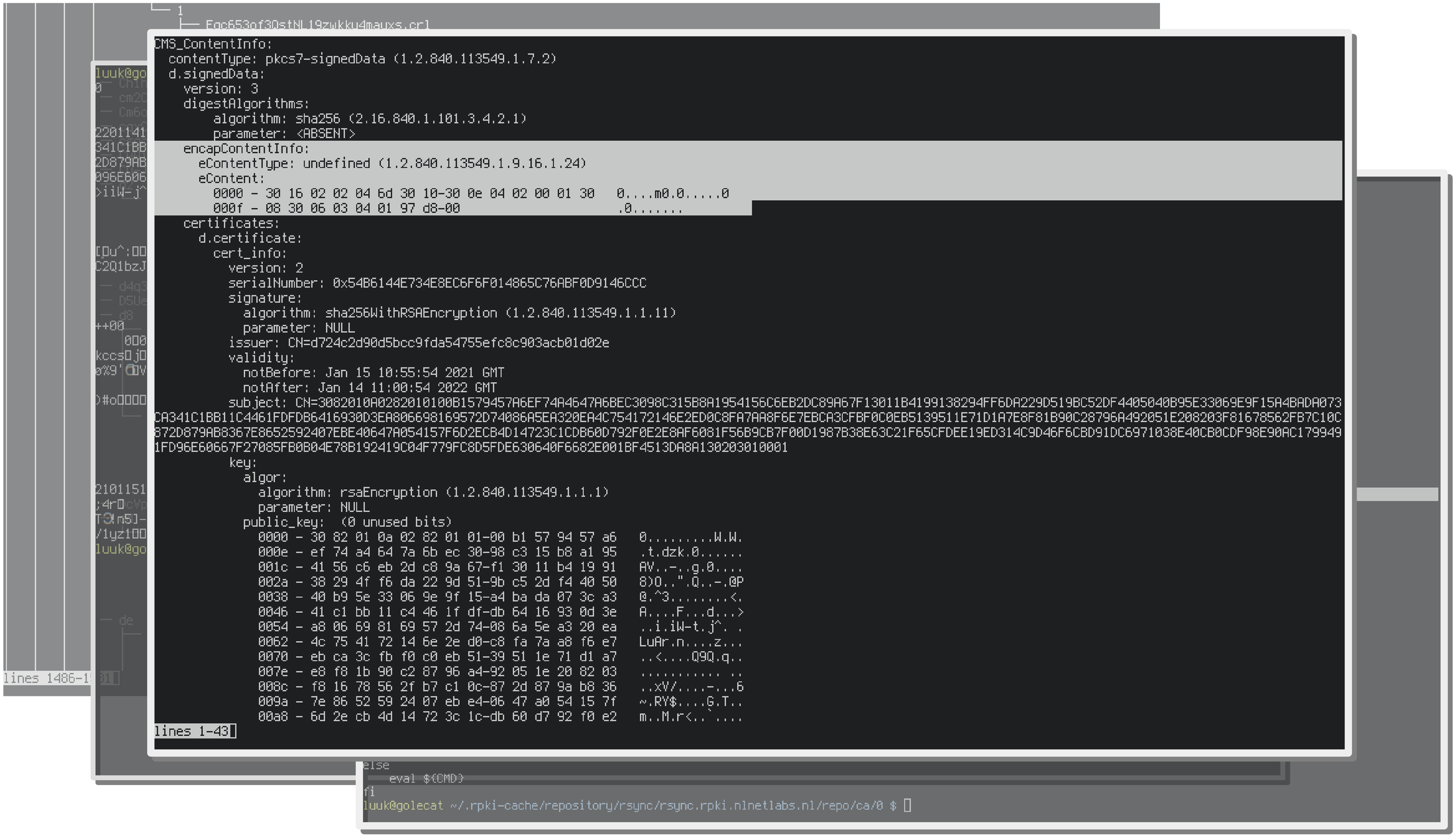
Comprised of X509 certificates (listing INR resources), CMS manifests (listing files), X509 CRLs, and ROAs (also CMS format).

```
│   │   │   │   │   │   └── 1
│   │   │   │   │   │       ├── Eqc653of3QstNL19zwkku4mauxs.crl
│   │   │   │   │   │       ├── Eqc653of3QstNL19zwkku4mauxs.mft
│   │   │   │   │   │       ├── sxeztRqQx9vD9z2p-7wIhXuecNo.crl
│   │   │   │   │   │       └── sxeztRqQx9vD9z2p-7wIhXuecNo.mft
│   │   │   │   │   ├── Chihh0LdxSVBDkeG56bNkzNpzbY.cer
│   │   │   │   │   ├── cm2CJzJQWGTP1h5RZM2jdmdvd2U.cer
│   │   │   │   │   ├── Cm6oI56VNH1DjPIH2eYrTel2TyU.cer
│   │   │   │   │   ├── cqxCvkmyxSoWUk-O7eH8goC7wEM.cer
│   │   │   │   │   ├── csqcHQu6zi_6u0EGYBuXbaYv5C4.cer
│   │   │   │   │   ├── CwWisqu81B2MbltV0DElxe2s-Xw.cer
│   │   │   │   │   ├── Cy-J7dNwfaQxuacD02qaGh_-pac.cer
│   │   │   │   │   ├── d2
│   │   │   │   │   │   └── 7c32cb-f430-48e8-a32d-edebcd6e0662
│   │   │   │   │   │       └── 1
│   │   │   │   │   │           ├── 9qlDWwAk-oJwNUqRh4gr5Weh6Mc.crl
│   │   │   │   │   │           ├── 9qlDWwAk-oJwNUqRh4gr5Weh6Mc.mft
│   │   │   │   │   │           ├── rS-UnR2YeKyM2dskMCGFtZfDH-I.crl
│   │   │   │   │   │           └── rS-UnR2YeKyM2dskMCGFtZfDH-I.mft
│   │   │   │   │   ├── d4q3I7KP6H05o0KXKu3WQZ0ixa4.cer
│   │   │   │   │   ├── D5Ue4VZuUmuL1zLLCbP-OsDEJbM.cer
│   │   │   │   │   ├── d8
│   │   │   │   │   │   ├── bd08a9-8ef1-4472-ae95-6b999643b922
│   │   │   │   │   │   │   └── 1
│   │   │   │   │   │   │       ├── 2bC4ryh9xlc-9KKEHcDm0XdLCK8.crl
│   │   │   │   │   │   │       ├── 2bC4ryh9xlc-9KKEHcDm0XdLCK8.mft
│   │   │   │   │   │   │       ├── K2H-vtK3Yv_kVDE0P44_0JoMN6A.crl
│   │   │   │   │   │   │       └── K2H-vtK3Yv_kVDE0P44_0JoMN6A.mft
│   │   │   │   │   │   └── f5304f-258e-4130-a1ea-917645b3976f
│   │   │   │   │   │       └── 1
│   │   │   │   │   │           ├── O_wHVbtwek6NdmM1bkbFLiGGxk4.crl
│   │   │   │   │   │           ├── O_wHVbtwek6NdmM1bkbFLiGGxk4.mft
│   │   │   │   │   │           ├── t5W9PxqmIgPcwahAC6B-QbT87Oo.crl
│   │   │   │   │   │           └── t5W9PxqmIgPcwahAC6B-QbT87Oo.mft
│   │   │   │   │   ├── DcVp6PYjjM4imiPZsK0pukW7mM0.cer
│   │   │   │   │   ├── dd
│   │   │   │   │   │   └── fbc673-4655-4c18-aa99-247d1ff8d335
│   │   │   │   │   │       └── 1
│   │   │   │   │   │           ├── 1-e8PPK4Jcm6fPtrM0Lxqnhv1Pm8.crl
│   │   │   │   │   │           ├── 1-e8PPK4Jcm6fPtrM0Lxqnhv1Pm8.mft
│   │   │   │   │   │           ├── QskoNRB-si_ZH11UzoEm8OEfwR4.crl
│   │   │   │   │   │           └── QskoNRB-si_ZH11UzoEm8OEfwR4.mft
│   │   │   │   │   ├── de
│   │   │   │   │   │   ├── 23ba41-9f76-422b-b504-54926a10f649
│   │   │   │   │   │   │   └── 1
│   │   │   │   │   │   │       ├── lhLlpNSgQC2gbzyqdZego9Mt6dg.crl
lines 1486-1531
```


└── 1
├── Eqc653of3QstNL19zwkku4mauxs.crl
├── Eqc653of3QstNL19zwkku4mauxs.mft
├── sxeztRqQx9vD9z2p-7wIhXuecNo.crl
luuk@golecat ~/.rpki-cache/repository/rsync/rsync.rpki.nlnetlabs.nl/repo/ca/0 $ cat 3135312e3231362e302e302f32332d3233203d3e2031313333.roa
0 *H
`He0)
*H000TNsN\v0l
220114110054Z0-1)0%U3082010A0282010100B1579457A6EF74A4647A6BEC3098C315B8A1954156C6EB2DC89A67F13011B4199138294FF6DA229D519BC52DF4405040B95E33069E9F15A4BADA073CA
341C1BB11C4461FDFDB6416930D3EA806698169572D74086A5EA320EA4C754172146E2ED0C8FA7AA8F6E7EBCA3CFBF0C0EB5139511E71D1A7E8F81B90C28796A492051E208203F81678562FB7C10C87
2D879AB8367E8652592407EBE40647A054157F6D2ECB4D14723C1CDB60D792F0E2E8AF6081F56B9CB7F00D1987B38E63C21F65CFDEE19ED314C9D46F6CBD91DC6971038E40CB0CDF98E90AC1799491F
096E6066*H27085FB0B04E78B192419C04F779FC8D5FDE630640F6682E001BF4513DA8A1302030100010"0
>iiW-j^ DuArn.OzOOOO9Qq▲OV/<AOOd
-6~RY$OGTm.Or<OλOOkOcOeOOOolOq@O◻O
yOgO
O$OwOOdfOE;OOUOOIbu0
[Du^:OO0U0gU`0^0\ZXVrsync://rsync.rpki.nlnetlabs.nl/repo/ca/0/D724C2D90D5BCC9FDA54755EFC8C903ACB01D02E.crl0+X0V0+0Hrsync://rpki.ripe.net/repository/DEFAULT/1yT
C2Q1bzJ_aVHVe_IyQOssB0C4.cer0+
p0n0+0
`rsync://rsync.rpki.nlnetlabs.nl/repo/ca/0/3135312e3231362e302e302f32332d3233203d3e2031313333.roa0U 0
0
++00
0O0 *H
kccsOjOO\FGPZm;Ob
2%9'O1Vs&[hO;OOb+3OOOO@!EONco+uOy5NO.
OoO~JJXOB_(
)#oOOOO:Ji)OĚe< $O*V.wf
[OxOO@
OzIO4O
+&E:wF10OOIbu0
70
1 `Hek0 *H
210115111" JTO$=OwU
;4rO *H dFa!WO
TO!n5]-UO`F#{dOOO'2Ydo@CU\!`.OF
/1yz1OOOU %i6FOcg'Lp;OOO": -OOOOcg@O:xOOOfOG1Ou@7(C{
luuk@golecat ~/.rpki-cache/repository/rsync/rsync.rpki.nlnetlabs.nl/repo/ca/0 $
lines 1486-1


└── 1
├── Eqc653of3QstNL19zwkku4mauxs.crl
├── Eqc653of3QstNL19zwkku4mauxs.mft
├── sxeztRqQx9vD9z2p-7wIhXuecNo.crl
luuk@golecat ~/.rpki-cache/repository/rsync/rsync.rpki.nlnetlabs.nl/repo/ca/0 $ cat 3135312e3231362e302e302f32332d3233203d3e2031313333.roa
2201141110054Z0-1)0%U3082010A0282010100B1579457A6EF74A4647A6BEC3098C315B8A1954156C6EB2DC89A67F13011B4199138294FF6DA229D519BC52DF4405040B95E33069E9F15A4BADA073CA
341C1BB11C4461FDFDB6416930D3EA806698169572D74086A5EA320EA4C754172146E2ED0C8FA7AA8F6E7EBCA3CFBF0C0EB5139511E71D1A7E8F81B90C28796A492051E208203F81678562FB7C10C87
2D879AB8367E8652592407EBE40647A054157F6D2ECB4D14723C1CDB60D792F0E2E8AF6081F56B9CB7F00D1987B38E63C21F65CFDEE19ED314C9D46F6CBD91DC6971038E40CB0CDF98E90AC1799491F
096E6066*H27085FB0B04E78B192419C04F
>iiW-j^_DuArn.OzOOOO9QqAOV/<AOOd
-6~RY$OG
└── 1
├── 9q1DWuAk-oJwNUqRh4gr
[Du^:OO0U0gU`0^0\ZXVrsync://rsync.r
C2Q1bzJ_aVHVe_IyQOssB0C4.cer0+
p0n0+
├── d4q3I7KP6H05o0KXKu3WQZ0ixa4
├── D5Ue4VZuUmuL1zLLCbP-OsDEJbM.cer
├── d8
++00
bd08a9-8ef1-4472-ae95-6b9996
0O0!*H
kccsOjOO\FGPZm;Ob
ø%9'OVs&[hO;OOb+3OOO@!EOOco+uOy5NO
K2H-vtK3Yv_kVDE0P44_
)#oOOOO:Ji)OĚe<$O*V,wf
f5304f-258e-4130
OxOO@
OzIO4
├── O_wHVbtwek6NdmM1bkbF
├── O_wHVbtwek6NdmM1bkbF
├── t5W9PxqmIgPcwahAC6B-
1
210115111"]TO$=OwU
;4rOcVp6*H
T!n5J-UO`F#{dOOO'2Ydo@[U\!`,OF
/1yz1OOOU%i6FOcg'Lp>OOO"
-OOOOcg
luuk@golecat ~/.rpki-cache/reposito
├── 1-e8PPK4Jcm6fPtrM0Lx
├── 1-e8PPK4Jcm6fPtrM0Lx
├── QskoNRB-si_ZH11UzoEm
└── QskoNRB-si_ZH11UzoEm
de
├── 23ba41-9f76-422b-b504-54926a
└── 1
├── lhL1pNSgQC2gbzyqdZeg
lines 1486-1
#!/bin/bash
if [-z "$1"]; then
echo "Pass RPKI file (.crt, .roa, .mft)"
exit 1
fi
if [[($# -eq 2)]]; then
if [[$1 -ne "ee"]]; then
echo "for extracing EE cert, try 'rcat ee filename.roa'"
exit 1
fi
INFILE=$2
EE=1
else
INFILE=$1
fi
#INFILE=$1
INEXT="${INFILE##*.}"
case $INEXT in
"roa"|"mft"|"gbr")
if [-z $EE]; then
CMD="openssl cms -inform DER -cmsout -print -in $INFILE"
else
CMD="openssl cms -inform DER -cmsout -certsout /dev/stdout -in $INFILE | openssl x509 -text -in /dev/stdin -out /dev/stdout"
fi
;;
"cer")
CMD="openssl x509 -inform DER -text -in $INFILE"
;;
"crl")
CMD="openssl crl -inform DER -text -in $INFILE"
;;
*)
echo "Unsure how to process a .$INEXT, aborting"
exit 1
;;
esac
#set -x
if [[-t 1]]; then
eval ${CMD} | $PAGER
else
eval ${CMD}
fi
luuk@golecat ~/.rpki-cache/repository/rsync/rsync.rpki.nlnetlabs.nl/repo/ca/0 $


CMS_ContentInfo:
contentType: pkcs7-signedData (1.2.840.113549.1.7.2)
d.signedData:
version: 3
digestAlgorithms:
algorithm: sha256 (2.16.840.1.101.3.4.2.1)
parameter: <ABSENT>
encapContentInfo:
eContentType: undefined (1.2.840.113549.1.9.16.1.24)
eContent:
0000 - 30 16 02 02 04 6d 30 10-30 0e 04 02 00 01 30 0....m0.0.....0
000f - 08 30 06 03 04 01 97 d8-00 .0.......
certificates:
d.certificate:
cert_info:
version: 2
serialNumber: 0x54B6144E734E8EC6F6F014865C76ABF0D9146CCC
signature:
algorithm: sha256WithRSAEncryption (1.2.840.113549.1.1.11)
parameter: NULL
issuer: CN=d724c2d90d5bcc9fda54755efc8c903acb01d02e
validity:
notBefore: Jan 15 10:55:54 2021 GMT
notAfter: Jan 14 11:00:54 2022 GMT
subject: CN=3082010A02820101100B1579457A6EF74A4647A6BEC3098C315B8A1954156C6EB2DC89A67F13011B4199138294FF6DA229D519BC52DF4405040B95E33069E9F15A4BADA073
CA341C1BB11C4461FDFDB6416930D3EA806698169572D74086A5EA320EA4C754172146E2ED0C8FA7AA8F6E7EBCA3CFBF0C0EB5139511E71D1A7E8F81B90C28796A492051E208203F81678562FB7C10C
872D879AB8367E8652592407EBE40647A054157F6D2ECB4D14723C1CDB60D792F0E2E8AF6081F56B9CB7F00D1987B38E63C21F65CFDEE19ED314C9D46F6CBD91DC6971038E40CB0CDF98E90AC179949
1FD96E60667F27085FB0B04E78B192419C04F779FC8D5FDE630640F6682E001BF4513DA8A130203010001
key:
algor:
algorithm: rsaEncryption (1.2.840.113549.1.1.1)
parameter: NULL
public_key: (0 unused bits)
0000 - 30 82 01 0a 02 82 01 01-00 b1 57 94 57 a6 0.........W.W.
000e - ef 74 a4 64 7a 6b ec 30-98 c3 15 b8 a1 95 .t.dzk.0......
001c - 41 56 c6 eb 2d c8 9a 67-f1 30 11 b4 19 91 AV..-..g.0....
002a - 38 29 4f f6 da 22 9d 51-9b c5 2d f4 40 50 8)O.."Q..-.@P
0038 - 40 b9 5e 33 06 9e 9f 15-a4 ba da 07 3c a3 @.^3........<.
0046 - 41 c1 bb 11 c4 46 1f df-db 64 16 93 0d 3e A....F...d...>
0054 - a8 06 69 81 69 57 2d 74-08 6a 5e a3 20 ea ..i.iW-t.j^. .
0062 - 4c 75 41 72 14 6e 2e d0-c8 fa 7a a8 f6 e7 LuAr.n....z...
0070 - eb ca 3c fb f0 c0 eb 51-39 51 1e 71 d1 a7 ..<....Q9Q.q..
007e - e8 f8 1b 90 c2 87 96 a4-92 05 1e 20 82 03 ....
008c - f8 16 78 56 2f b7 c1 0c-87 2d 87 9a b8 36 ..xV/....-...6
009a - 7e 86 52 59 24 07 eb e4-06 47 a0 54 15 7f ~.RY$....G.T..
00a8 - 6d 2e cb 4d 14 72 3c 1c-db 60 d7 92 f0 e2 m..M.r<..`....
lines 1-43
else
eval ${CMD}
fi
luuk@golecat ~/.rpki-cache/repository/rsync/rsync.rpki.nlnetlabs.nl/repo/ca/0 $


CMS_ContentInfo:
contentType: pkcs7-signedData (1.2.840.113549.1.7.2)
d.signedData:
version: 3
digestAlgorithms:
algorithm: sha256 (2.16.840.1.101.3.4.2.1)
parameter: <ABSENT>
encapContentInfo:
eContentType: undefined (1.2.840.113549.1.9.16.1.24)
eContent:
0000 - 30 16 02 02 04 6d 30 10-30 0e 04 02 00 01 30 0....m0.0.....0
000f - 08 30 06 03 04 01 97 d8-00 .0.......
certificates:
d.certificate:
cert_info:
version: 2
serialNumber: 0x54B6144E734E8EC6F6F014865C76ABF0D9146CCC
signature:
algorithm: sha256WithRSAEncryption (1.2.840.113549.1.1.11)
parameter: NULL
issuer: CN=d724c2d90d5bcc9fda54755efc8c903acb01d02e
validity:
notBefore: Jan 15 10:55:54 2021 GMT
notAfter: Jan 14 11:00:54 2022 GMT
subject: CN=3082010A02820101100B1579457A6EF74A4647A6BEC3098C315B8A1954156C6EB2DC89A67F13011B4199138294FF6DA229D519BC52DF4405040B95E33069E9F15A4BADA073
CA341C1BB11C4461FDFDB6416930D3EA806698169572D74086A5EA320EA4C754172146E2ED0C8FA7AA8F6E7EBCA3CFBF0C0EB5139511E71D1A7E8F81B90C28796A492051E208203F81678562FB7C10C
872D879AB8367E8652592407EBE40647A054157F6D2ECB4D14723C1CDB60D792F0E2E8AF6081F56B9CB7F00D1987B38E63C21F65CFDEE19ED314C9D46F6CBD91DC6971038E40CB0CDF98E90AC179949
1FD96E60667F27085FB0B04E78B192419C04F779FC8D5FDE630640F6682E001BF4513DA8A130203010001
key:
algor:
algorithm: rsaEncryption (1.2.840.113549.1.1.1)
parameter: NULL
public_key: (0 unused bits)
0000 - 30 82 01 0a 02 82 01 01-00 b1 57 94 57 a6 0.........W.W.
000e - ef 74 a4 64 7a 6b ec 30-98 c3 15 b8 a1 95 .t.dzk.0......
001c - 41 56 c6 eb 2d c8 9a 67-f1 30 11 b4 19 91 AV..-..g.0....
002a - 38 29 4f f6 da 22 9d 51-9b c5 2d f4 40 50 8)O.."Q..-.@P
0038 - 40 b9 5e 33 06 9e 9f 15-a4 ba da 07 3c a3 @.^3........<.
0046 - 41 c1 bb 11 c4 46 1f df-db 64 16 93 0d 3e A....F...d...>
0054 - a8 06 69 81 69 57 2d 74-08 6a 5e a3 20 ea ..i.iW-t.j^. .
0062 - 4c 75 41 72 14 6e 2e d0-c8 fa 7a a8 f6 e7 LuAr.n....z...
0070 - eb ca 3c fb f0 c0 eb 51-39 51 1e 71 d1 a7 ..<....Q9Q.q..
007e - e8 f8 1b 90 c2 87 96 a4-92 05 1e 20 82 03 ....
008c - f8 16 78 56 2f b7 c1 0c-87 2d 87 9a b8 36 ..xV/....-...6
009a - 7e 86 52 59 24 07 eb e4-06 47 a0 54 15 7f ~.RY$....G.T..
00a8 - 6d 2e cb 4d 14 72 3c 1c-db 60 d7 92 f0 e2 m..M.r<..`....
lines 1-43
eval ${CMD}
fi
luuk@golecat ~/.rpki-cache/repository/rsync/rsync.rpki.nlnetlabs.nl/repo/ca/0 $

JDR.jl: Interactively Analyzing the RPKI

Fetch all the data from the RPKI,
plow through it locally/offline in an iterative, explorative manner.
E.g. in an interactive shell (REPL), notebooks (Jupyter)

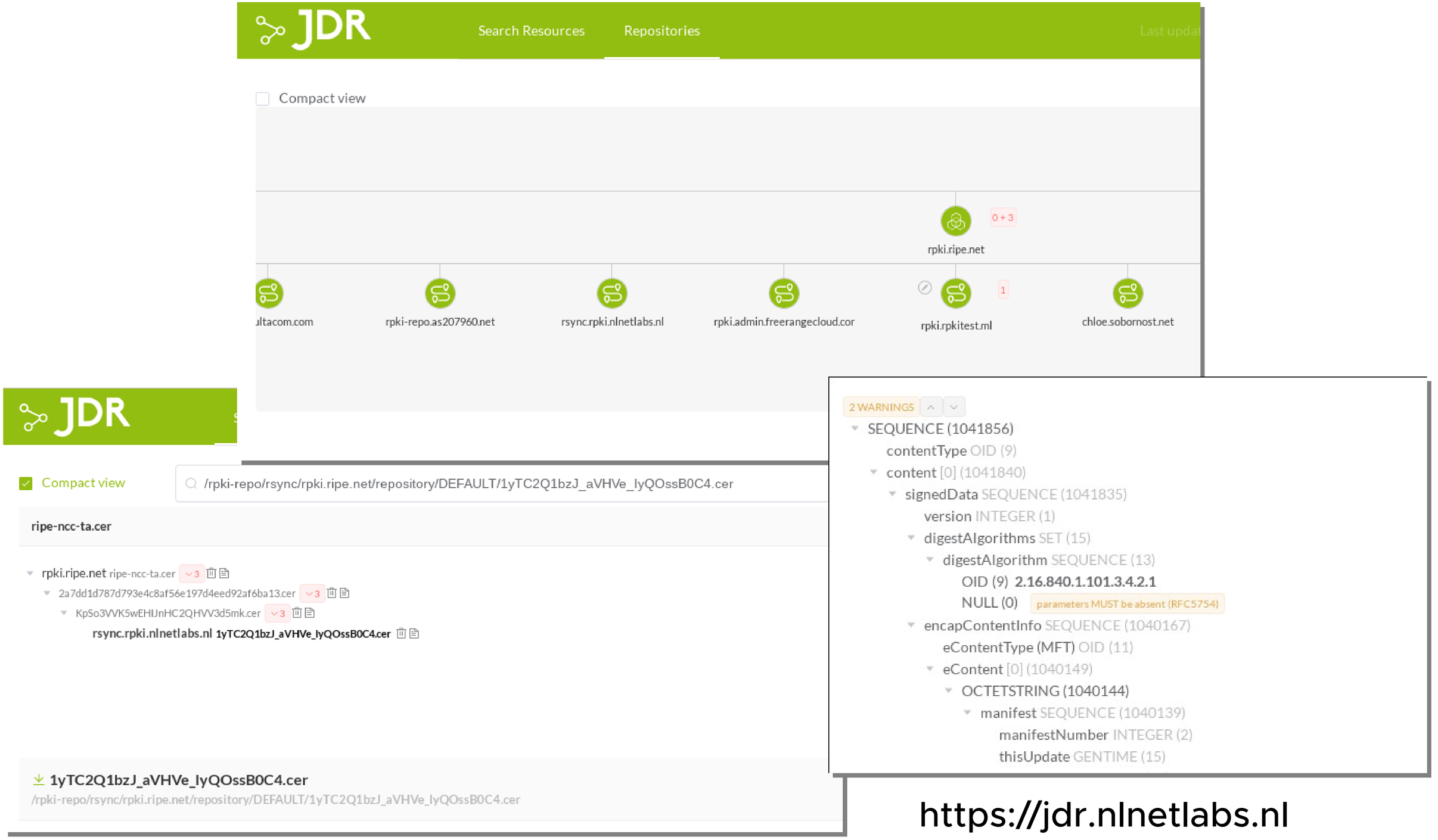
Imagine: RP software giving a non-descriptive error ‘some.mft is kaputt’. Find the MFT. Then how to find its CER? And then how to find all the ROAs below that CER, possibly via subordinate CAs?

JDR.jl: Interactively Analyzing the RPKI

A Julia (.jl) package allowing to do all these things.

Julia is an interpreted-JIT-compiled language, enabling the interactive part (and thus notebooks) while still offering great performance.

We'll see what components make up JDR.jl, and how they convert plain RPKI files into something we can easily analyse.



https://jdr.nlnetlabs.nl

JDR.jl `tree -L 3 src/`

- ASN1
- PKIX
- RPKI
- Common
- Webservice

JDR.jl `tree -L 3 src/`

- ASN1: decoding the RPKI files, creating ASN.1 structures
- PKIX : validate and enrich the ASN.1 structures (X509 and CMS), highlighting errors and extracting information, all RPKI specific
- **RPKI: datastructures/types/functions to work with the results of the two modules above**
- Common: Helper types and functions
- Webservice: API endpoints for jdr.nlnetlabs.nl

Demo / notebook

1) Determining all affected prefixes under a broken manifest

2) Finding unused resources/entitlements

3) Historical analysis

Follow along at https://jdr.nlnetlabs.nl/notebook

What’s coming

- Processing files (likely) belonging to *missing* manifests
- Fetching RPKI files without depending on Routinator, add RRDP support
- Focus on the ‘time’ aspect, e.g. seeing changes between two points in time, or processing historical data with a custom `now()`
- More docs, increase test coverage, more docs

References

code + docs: https://github.com/NLnetLabs/JDR.jl

notebook: https://jdr.nlnetlabs.nl/notebook

RPKI: https://rpki.readthedocs.io/en/latest/

Julia: https://julialang.org/

a big *Thank you !*

to the RIPE NCC Community Projects Fund,
enabling us to carry out this work.

JDR.jl:
Interactively Analyzing the RPKI

MAT-WG @RIPE 82 - virtual

Luuk Hendriks

luuk@nlnetlabs.nl

NLNETLABS