Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 7, 2021

M. Candela
NTT
R. Bush
IIJ & Arrcus
W. Kumari
Google
R. Housley
Vigil Security

September 3, 2020

Finding and Using Geofeed Data
draft-ymbk-opsawg-finding-geofeeds-01

Abstract

This document describes how to find and authenticate geofeed data.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 7, 2021.

Table of Contents

1. Introduction

Providers of Internet content and other services may wish to customize those services based on the geographic location of the user of the service. This is often done using the source IP address used to contact the service. Also, infrastructure and other services might wish to publish the locale of their services. [RFC8805] defines geofeed, a syntax to associate geographic locales with IP addresses. But it does not specify how to find the relevant geofeed data given an IP address.

This document specifies how to augment the Routing Policy Specification Language (RPSL), [RFC2622] inetnum: class, [INETNUM] to refer to geofeed data, and how to prudently use them.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Geofeed Files

Geofeed files are described in [RFC8805]. They provide a facility for an IP address resource 'owner' to associate those IP addresses to geographic locale(s).

Content providers and other parties who wish to locate an IP address to a geographic locale need to find the relevant geofeed data. In Section 3 this document specifies how to find the relevant geofeed file given an IP address.

This document also suggests optional data for geofeed files to provide stronger authenticity to the data.

3. inetnum: Class

RPSL, [RFC2622], as used by the Regional Internet Registries (RIRs), has been augmented with the inetnum: class [INETNUM]. inetnum: objects, each of which which describes an IP address range and its attributes.

Ideally, RPSL would be augmented to define a new RPSL geofeed: attribute in the inetnum: class. Until such time, this document defines the syntax of a Geofeed remarks: attribute which contains a URL of a geofeed file. The format MUST be as in this example, "remarks: Geofeed " followed by a URL which will vary.

```
inetnum: 192.0.2.0/24 # example
remarks: Geofeed https://example.com/geofeed.csv
```

Any particular inetnum: object MAY have, at most, one geofeed reference.

inetnum: objects form a hierarchy, see [INETNUM] Section 4.2.4.1, Hierarchy of INETNUM Objects. Geofeed references SHOULD be at the lowest applicable inetnum: object. When fetching, the most specific inetnum: object with a geofeed reference MUST be used.

When geofeed references are provided by multiple inetnum: objects which have identical address ranges, then the geofeed reference on the inetnum: with the most recent last-modified: attribute SHOULD be preferred.

4. Authenticating Geofeed Data

The question arises on whether a particular geofeed data set is authentic, i.e. authorized by the 'owner' of the IP address space and is authoritative in some sense. The inetnum: which points to the geofeed file provides some authentication. Unfortunately the RPSL in many repositories is weakly authenticated at best.

An optional authenticator MAY be appended to a geofeed file. It would essentially be a digest of the main body of the file signed by the private key of the relevant RPKI certificate for the covering

address range. One needs a format that bundles the relevant RPKI certificate with the signature and the digest of the geofeed text.

Borrowing detached signatures from [RFC5485], after text file canonicalization (Sec 2.2), the Cryptographic Message Syntax (CMS) [RFC3852] would be used to create a detached DER encoded signature which is then BASE64 encoded and line wrapped to 72 or fewer characters.

Both the address ranges of the signing certificate and of the inetnum: MUST cover all prefixes in the geofeed file; and the address range of the signing certificate must cover that of the inetnum:.

An address range A 'covers' address range B if the range of B is identical to or a subset of A. 'Address range' is used here because inetnum: objects and RPKI certificates need not align on CIDR prefix boundaries, while those of geofeed lines must.

As the signer would need to specify the covered RPKI resources relevant to the signature, the RPKI certificate covering the inetnum: object's address range would be included in the [RFC3852] CMS SignedData certificates field.

Identifying the private key associated with the certificate, and getting the department with the HSM to sign the CMS blob is left as an exercise for the implementor. On the other hand, verifying the signature requires no complexity; the certificate, which can be validated in the public RPKI, has the needed public key.

Until [RFC8805] is updated to formally define such an appendix, it MUST be 'hidden' as a series of "#" comments at the end of the geofeed file. This is a cryptographically incorrect, albeit simple example. A correct and full example is in Appendix A.

```
# RPKI Signature: 192.0.2.0/24
# MIIGugYJKoZIhvcNAQcCoIDTALBglghkgBZQMEAgEwKQYLKoZIhvcNAQkQARig
# GgQYMBYCAhzRMBAwDgQCAAoIIEuDCCBLQwggOcoAMCAQICAwDe4TANBgkqhkiG
# 9w0BAQsFADAzMTEwLwYDVQQ0VBREI5Mzk2MTFDOTFGMDI3REI1NjNGQ0NDNUI5
# ...
# w+nU1q1VSZDvw/YVpyaWAu99SjHTxpIBdwp3avpZ84Daxy4h4v084xFvjnqAAg
# ukYLIfBPdZiuvtLaLR/vjZR4s7mR4L4SNj0WSNPYKwad9cs+ozQpymByDL8VW8
# pUXCTD5sPYzBKsTpAbiDsQ==
# END Signature: 192.0.2.0/24
```


5. Operational Considerations

Geofeed data SHOULD be fetched using https [RFC2818].

When using data from a geofeed file, one MUST ignore data outside of the inetnum: object's inetnum: attribute's address range.

Iff the geofeed file is not signed per Section 4, then multiple inetnum: objectss MAY refer to the same geofeed file, and the consumer MUST use only geofeed lines where the prefix is covered by the address range of the inetnum: object they have followed.

An entity fetching geofeed data through these mechanisms MUST NOT do frequent real-time look-ups to prevent load on RPSL servers. And do not fetch at midnight, because everyone else may.

6. Scurity Considerations

It would be generally prudent for a consumer of geofeed data to also use other sources to cross-validate the data. All of the Security Considerations of [RFC8805] apply here as well.

As mentioned in Section 4, many RPSL repositories have weak if any authentication. This would allow spoofing of inetnum: objects pointing to malicious geofeed files. Section 4 suggests an sadly complex method for stronger authentication based on the RPKI.

7. IANA Considerations

No action is requested of the IANA.

8. Acknowledgements

Thanks to Rob Austein for CMS and detached signature clue. Also to Erik Kline who was too shy to agree to co-authorship.

9. Normative References

[INETNUM] RIPE, "Description of the INETNUM Object", <https://www.ripe.net/manage-ips-and-asns/db/support/documentation/ripe-database-documentation/rpsl-object-types/4-2-descriptions-of-primary-objects/4-2-4-description-of-the-inetnum-object>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2622] Alaettinoglu, C., Villamizar, C., Gerich, E., Kessens, D., Meyer, D., Bates, T., Karrenberg, D., and M. Terpstra, "Routing Policy Specification Language (RPSL)", RFC 2622, DOI 10.17487/RFC2622, June 1999, <https://www.rfc-editor.org/info/rfc2622>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[RFC3852] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, DOI 10.17487/RFC3852, July 2004, <https://www.rfc-editor.org/info/rfc3852>.

[RFC5485] Housley, R., "Digital Signatures on Internet-Draft

Documents", RFC 5485, DOI 10.17487/RFC5485, March 2009, <https://www.rfc-editor.org/info/rfc5485>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8805] Kline, E., Duleba, K., Szamonek, Z., Moser, S., and W. Kumari, "A Format for Self-Published IP Geolocation Feeds", RFC 8805, DOI 10.17487/RFC8805, August 2020, <https://www.rfc-editor.org/info/rfc8805>.

Appendix A. Example

This appendix provides an example, including a trust anchor, a CA certificate subordinate to the trust anchor, an end-entity certificate subordinate to the CA for signing the geofeed, and a detached signature.

The trust anchor is represented by a self-signed certificate. As usual in the RPKI, the trust anchor has authority over all IPv4 address blocks, all IPv6 address blocks, and all AS numbers.

-----BEGIN CERTIFICATE-----
MIIEPjCCAyagAwIBAgIUPsUFJ4e/7pKZ6E14aBdkbYzms1gwDQYJKoZIhvcNAQEL
BQAwFTETMBEGA1UEAxMKZXhhbXBsZS10YTAeFw0yMDA5MDMxODU0NTRaFw0zMDA5
MDExODU0NTRaMBUxEzARBgNVBAMTCmV4YW1wbGUtdGEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCelMmMDCGBhqn/a3VrNAoKMr1HVLKxGoG7VF/13HZJ
0twObUZlh3Jz+XeD+kNAURhELWTrsgdTkQQfqinqOuRemxTl55+x7nLpe5nmwaBH
XqqDOHubmkbAGanGcm6T/rD9KNk1Z46Uc2p7UYu0fwNO0mo0aqFL2FSyvzZwziNe
g7ELYZ4a3LvGn81JfP/JvM6pgtoMNuee5RV6TWaz7LV304ICj8Bhphy/HFpOA1rb

```
O9gs8CUMgqz+RroAIa8cV8gbF/fPCz9Ofl7Gdmib679JxxFrW4wRJ0nMJgJmsZXq
jaVc0g7ORc+eIAcHw7Uroc6h7Y7lGjOkDZF75j0mLQa3AgMBAAGjggGEMIIBgDAd
BgNVHQ4EFgQU3hNEuwvUGNCHY1TBatcUR03pNdYwHwYDVR0jBBgwFoAU3hNEuwvU
GNCHY1TBatcUR03pNdYwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYw
GAYDVR0gAQH/BA4wDDAKBggrBgEFBQcOAjCBuQYIKwYBBQUHAQsEgawwgakwPgYI
KwYBBQUHMAqGMnJzeW5jOi8vcnBraS5leGFtcGxlLm5ldC9yZXBvc2l0b3J5L2V4
YW1wbGUtdGEubWZ0MDUGCCsGAQUFBzANhilodHRwczovL3JyZHAuZXhhbXBsZS5u
ZXQvbm90aWZpY2F0aW9uLnhtbDAwBggrBgEFBQcwBYYkcnN5bmM6Ly9ycGtpLmV4
YW1wbGUubmV0L3JlcG9zaXRvcnkvMCcGCCsGAQUFBwEHAQH/BBgwFjAJBAIAATAD
AwEAMAkEAgACMAMDAQAwHgYIKwYBBQUHAQgEEjAQoA4wDDAKAgEAAgUA/////zAN
BgkqhkiG9w0BAQsFAAOCAQEAgZFQ0Sf3CI5Hwev61AUWHYOFniy69PuDTq+WnhDe
xX5rpjSDRrs5L756KSKJcaOJ36lzO45lfOPSY9fH6x30pnipaqRA7t5rApky24jH
cSUA9iRednzxhVyGjWKnfAKyNo2MYfaOAT0db1GjyLKbOADI9FowtHBUu+60ykcM
Quz66XrzxtmxlrRcAnbv/HtV17qOd4my6q5yjTPR1dmYN9oR/2ChlXtGE6uQVguA
rvNZ5CwiJ1TgGGTB7T8ORHwWU6dGTc0jk2rESAaikmLi1roZSNC21fckhapEit1a
x8CyiVxjcVc5e0AmS1rJfL6LIfwmtive/N/eBtIM92HkBA==
-----END CERTIFICATE-----
```

The CA certificate is issued by the trust anchor. This certificate grants authority over one IPv4 address block (192.0.2.0/24) and two AS numbers (64496 and 64497).


```
-----BEGIN CERTIFICATE-----
```

```
MIIFBzCCA++gAwIBAgIUcyCzS10hdfG65kbRq7toQAvRDKowDQYJKoZIhvcNAQEL
BQAwFTETMBEGA1UEAxMKZXhhbXBsZS10YTAeFw0yMDA5MDMxOTAyMTlaFw0yMTA5
MDMxOTAyMTlaMDMxMTAvBgNVBAMTKDNBQ0UyQ0VGNEZCMjFCN0QxMUUzRTE4NEVG
QzFFMjk3QjM3Nzg2NDIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDc
zz1qwTxC2ocw5rqp8ktm2XyYkl8riBVuqlXwfefTxsR2YFpgz9vkYUd5Az9EVEG7
6wGIyZbtmhK63eEeaqbKz2GHub467498BXeVrYysO+YuIGgCEYKznNDZ4j5aaDbo
j5+4/z0Qvv6HEsxQd0f8br6lKJwgeRM6+fm7796HNPB0aqD7Zj9NRCLXjbB0DCgJ
liH6rXMKR86ofgll9V2mRjesvhdKYgkGbOif9rvxVpLJ/6zdru5CE9yeuJZ59l+n
YH/r6PzdJ4Q7yKrJX8qD6A60j4+biaU4MQ72KpsjhQNTTqF/HRwi0N54GDaknEwE
TnJQHgLJDYqww9yKWtjjAgMBAAGjggIvMIICKzAdBgNVHQ4EFgQUOs4s70+yG30R
4+GE78Hil7N3hkIwHwYDVR0jBBgwFoAU3hNEuwvUGNCHY1TBatcUR03pNdYwDwYD
VR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwGAYDVR0gAQH/BA4wDDAKBggr
BgEFBQcOAjBhBgNVHR8EWjBYMFagVKBShlByc3luYzovL3Jwa2kuZXhhbXBsZS5u
ZXQvcmVwb3NpdG9yeS8zQUNFMkNFRjRGQjIxQjdEMTFFM0UxODRFRkMxRTI5N0Iz
Nzc4NjQyLmNybDBOBggrBgEFBQcBAQRCMEAwPgYIKwYBBQUHMAKGMnJzeW5jOi8v
cnBraS5leGFtcGxlLm5ldC9yZXBvc2l0b3J5L2V4YW1wbGUtdGEuY2VyMIG5Bggr
BgEFBQcBCwSBrDCBqTA+BggrBgEFBQcwCoYycnN5bmM6Ly9ycGtpLmV4YW1wbGUu
bmV0L3JlcG9zaXRvcnkvZXhhbXBsZS1jYS5tZnQwNQYIKwYBBQUHMA2GKWh0dHBz
Oi8vcnJkcC5leGFtcGxlLm5ldC9ub3RpZmljYXRpb24ueG1sMDAGCCsGAQUFBzAF
hiRyc3luYzovL3Jwa2kuZXhhbXBsZS5uZXQvcmVwb3NpdG9yeS8wHwYIKwYBBQUH
AQcBAf8EEDAOMAwEAgABMAYDBADAAAIwHgYIKwYBBQUHAQgEEjAQoA4wDDAKAgMA
+/ACAwD78TANBgkqhkiG9w0BAQsFAAOCAQEAnLu+d1ZsUTiX3YWGueTHIalW4ad0
Kupi7pYMV2nXbxNGmdJMol9BkzVz9tj55ReMghUU4YLm/ICYe4fz5e0T8o9s/vIm
cGS29+WoGuiznMitpvbS/379gaMezk6KpqjH6Brw6meMqy09phmcmvm3x3WTmx09
mLlQneMptwk8qSYcnMUmGLJs+cVqmkOa3sWRdw8WrGu6QqYtQz3HFZQojF06YzEq
V/dBdCFdEOwTfVl2n2XqhoJl/oEBdC4uu2G0qRk3+WVs+uwVHP0Ttsbt7TzFgZfY
yxqvOg6QoldxZVZmHHncKmETu/BqCDGJot9may31ukrx34Bu+XFMVihm0w==
-----END CERTIFICATE-----
```

The end-entity certificate is issued by the CA. This certificate grants signature authority for one IPv4 address block (192.0.2.0/24). Signature authority for AS numbers is not needed for geofeed data signatures, so no AS numbers are included in the certificate.

```
-----BEGIN CERTIFICATE-----
MIIErTCCA5WgAwIBAgIUJ605QIPX8rW5m4Zwx3WyuW7hZuMwDQYJKoZIhvcNAQEL
BQAwMzExMC8GA1UEAxMoM0FDRTJDRUY0RkIyMUI3RDExRTNFMTg0RUZDMUUyOTdC
Mzc3ODY0MjAeFw0yMDA5MDMxOTA1MTdaFw0yMTA2MzAxOTA1MTdaMDMxMTAvBgNV
BAMTKDkxNDY1MkEzQkQ1MUMxNDQyNjAxOTg4ODlGNUM0NUFCRjA1M0ExODcwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCycTQrOb/qB2W3i3Ki8PhA/DEW
yii2TgGo9pgCwO9lsIRI6Zb/k+aSiWWP9kSczlcQgtPCVwr62hTQZCIowBN0BL0c
K0/5k1imJdi5qdM3nvKswM8CnoR11vB8pQFwruZmr5xphXRvE+mzuJVLgu2V1upm
BXuWloeymudh6WWJ+GDjwPXO3RiXBejBrOFNXhaFLe08y4DPfr/S/tXJOBm7QzQp
tmbPLYtGfprYu45liFFqqP94UeLpISfXd36AKGzqTFCcc3EW9l5UFE1MFLlnoEog
qtoLoKABt0IkOFGKeC/EgeaBdWLe469ddC9rQft5w6g6cmxG+aYDdIEB34zrAgMB
AAGjggG3MIIBszAdBgNVHQ4EFgQUkUZSo71RwUQmAZiIn1xFq/BToYcwHwYDVR0j
BBgwFoAUOs4s70+yG30R4+GE78Hil7N3hkIwDAYDVR0TAQH/BAIwADAOBgNVHQ8B
Af8EBAMCB4AwGAYDVR0gAQH/BA4wDDAKBggrBgEFBQcOAjBhBgNVHR8EWjBYMFag
VKBShlByc3luYzovL3Jwa2kuZXhhbXBsZS5uZXQvcmVwb3NpdG9yeS8zQUNFMkNF
RjRGQjIxQjdEMTFFM0UxODRFRkMxRTI5N0IzNzc4NjQyLmNybDBsBggrBgEFBQcB
AQRgMF4wXAYIKwYBBQUHMAKGUHJzeW5jOi8vcnBraS5leGFtcGxlLm5ldC9yZXBv
c2l0b3J5LzNBQ0UyQ0VGNEZCMjFCN0QxMUUzRTE4NEVGQzFFMjk3QjM3Nzg2NDIu
Y2VyMCEGCCsGAQUFBwEHAQH/BBIwEDAGBAIAAQUAMAYEAgACBQAwRQYIKwYBBQUH
AQsEOTA3MDUGCCsGAQUFBzANhilodHRwczovL3JyZHAuZXhhbXBsZS5uZXQvbm90
aWZpY2F0aW9uLnhtbDANBgkqhkiG9w0BAQsFAAOCAQEABR2T0qT2V1ZlsZjj+yHP
TArIVBECZFSCdP+bJTse85TqYiblMsNS9yEu2SNbaZMNLuSSiAffYooh4nIYq/Rh
6+xGs1n427JZUokoeLtY0UUb2fIsua9JFo8YGTnpqDMGe+xnpbJ0SCSoBlJCIj+b
+YS8WXjEHt2KW6wyA/BcNS8adS2pEUwC2cs/WcwzgbttnkcnG7/wkrQ3oqzpC1ar
Kelyz7PGIIXJGy9nF8C3/aaaEpHd7UgIyvXYuCY/lqWTm97jDxgGIYGC7660mtfO
MkB8YF6kUU+td2dDQsMztcOxbzqiGnicmeJfBwG2li6O0vorW4d5iIOTKpQyqfh4
5Q==
-----END CERTIFICATE-----
```

The end-entity certificate is displayed below in detail. For brevity, the other two certificates are not.

```
   0 1197: SEQUENCE {
   4  917:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2
        :       }
  13   20:     INTEGER 27AD394083D7F2B5B99B8670C775B2B96EE166E3
  35   13:     SEQUENCE {
  37    9:       OBJECT IDENTIFIER
        :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
  48    0:       NULL
        :       }
  50   51:     SEQUENCE {
  52   49:       SET {
  54   47:         SEQUENCE {
```

```
     56    3:      OBJECT IDENTIFIER commonName (2 5 4 3)
     61   40:      PrintableString
```



```
          :       '3ACE2CEF4FB21B7D11E3E184EFC1E297B3778642'
          :       }
          :      }
          :     }
    103   30:   SEQUENCE {
    105   13:    UTCTime 03/09/2020 19:05:17 GMT
    120   13:    UTCTime 30/06/2021 19:05:17 GMT
          :     }
    135   51:   SEQUENCE {
    137   49:    SET {
    139   47:     SEQUENCE {
    141    3:      OBJECT IDENTIFIER commonName (2 5 4 3)
    146   40:      PrintableString
          :       '914652A3BD51C144260198889F5C45ABF053A187'
          :       }
          :      }
          :     }
    188  290:   SEQUENCE {
    192   13:    SEQUENCE {
    194    9:     OBJECT IDENTIFIER rsaEncryption
          :      (1 2 840 113549 1 1 1)
    205    0:     NULL
          :      }
    207  271:    BIT STRING, encapsulates {
    212  266:     SEQUENCE {
    216  257:      INTEGER
          :       00 B2 71 34 2B 39 BF EA 07 65 B7 8B 72 A2 F0 F8
          :       40 FC 31 16 CA 28 B6 4E 01 A8 F6 98 02 C0 EF 65
          :       B0 84 48 E9 96 FF 93 E6 92 89 65 8F F6 44 9C CE
          :       57 10 82 D3 C2 57 0A FA DA 14 D0 64 22 28 C0 13
          :       74 04 BD 1C 2B 4F F9 93 58 A6 25 D8 B9 A9 D3 37
          :       9E F2 AC C0 CF 02 9E 84 75 D6 F0 7C A5 01 70 AE
          :       E6 66 AF 9C 69 85 74 6F 13 E9 B3 B8 95 4B 82 ED
          :       95 D6 EA 66 05 7B 96 96 87 B2 9A E7 61 E9 65 89
          :       F8 60 E3 C0 F5 CE DD 18 97 05 E8 C1 AC E1 4D 5E
          :       16 85 2D ED 3C CB 80 CF 7E BF D2 FE D5 C9 38 19
          :       BB 43 34 29 B6 66 CF 2D 8B 46 7E 9A D8 BB 8E 65
          :       88 51 6A A8 FF 78 51 E2 E9 21 27 D7 77 7E 80 28
          :       6C EA 4C 50 9C 73 71 16 F6 5E 54 14 4D 4C 14 B9
```

```
         :       67 A0 4A 20 AA DA 0B A0 A0 01 B7 42 24 38 51 8A
         :       78 2F C4 81 E6 81 75 62 DE E3 AF 5D 74 2F 6B 41
         :       FB 79 C3 A8 3A 72 6C 46 F9 A6 03 74 81 01 DF 8C
         :       EB
  477     3:      INTEGER 65537
         :       }
         :      }
         :     }
  482   439:   [3] {
```



```
  486   435:    SEQUENCE {
  490    29:     SEQUENCE {
  492     3:      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
  497    22:      OCTET STRING, encapsulates {
  499    20:       OCTET STRING
         :        91 46 52 A3 BD 51 C1 44 26 01 98 88 9F 5C 45 AB
         :        F0 53 A1 87
         :       }
         :      }
  521    31:     SEQUENCE {
  523     3:      OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
  528    24:      OCTET STRING, encapsulates {
  530    22:       SEQUENCE {
  532    20:        [0]
         :         3A CE 2C EF 4F B2 1B 7D 11 E3 E1 84 EF C1 E2 97
         :         B3 77 86 42
         :        }
         :       }
         :      }
  554    12:     SEQUENCE {
  556     3:      OBJECT IDENTIFIER basicConstraints (2 5 29 19)
  561     1:      BOOLEAN TRUE
  564     2:      OCTET STRING, encapsulates {
  566     0:       SEQUENCE {}
         :       }
         :      }
  568    14:     SEQUENCE {
  570     3:      OBJECT IDENTIFIER keyUsage (2 5 29 15)
  575     1:      BOOLEAN TRUE
  578     4:      OCTET STRING, encapsulates {
  580     2:       BIT STRING 7 unused bits
         :        '1'B (bit 0)
```

```
          :         }
          :       }
    584   24:     SEQUENCE {
    586    3:      OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
    591    1:      BOOLEAN TRUE
    594   14:      OCTET STRING, encapsulates {
    596   12:       SEQUENCE {
    598   10:        SEQUENCE {
    600    8:         OBJECT IDENTIFIER
          :          resourceCertificatePolicy (1 3 6 1 5 5 7 14 2)
          :          }
          :         }
          :        }
          :       }
    610   97:     SEQUENCE {
    612    3:      OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
```



```
    617   90:      OCTET STRING, encapsulates {
    619   88:       SEQUENCE {
    621   86:        SEQUENCE {
    623   84:         [0] {
    625   82:          [0] {
    627   80:           [6]
          :           'rsync://rpki.example.net/repository/3ACE2CEF4F'
          :           'B21B7D11E3E184EFC1E297B3778642.crl'
          :            }
          :           }
          :          }
          :         }
          :        }
          :       }
    709  108:     SEQUENCE {
    711    8:      OBJECT IDENTIFIER authorityInfoAccess
          :       (1 3 6 1 5 5 7 1 1)
    721   96:      OCTET STRING, encapsulates {
    723   94:       SEQUENCE {
    725   92:        SEQUENCE {
    727    8:         OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
    737   80:         [6]
          :          'rsync://rpki.example.net/repository/3ACE2CEF4F'
          :          'B21B7D11E3E184EFC1E297B3778642.cer'
          :          }
```

```
          :         }
          :        }
          :       }
    819   33:     SEQUENCE {
    821    8:      OBJECT IDENTIFIER ipAddrBlocks (1 3 6 1 5 5 7 1 7)
    831    1:      BOOLEAN TRUE
    834   18:      OCTET STRING, encapsulates {
    836   16:       SEQUENCE {
    838    6:        SEQUENCE {
    840    2:         OCTET STRING 00 01
    844    0:         NULL
          :          }
    846    6:        SEQUENCE {
    848    2:         OCTET STRING 00 02
    852    0:         NULL
          :          }
          :         }
          :        }
          :       }
    854   69:     SEQUENCE {
    856    8:      OBJECT IDENTIFIER subjectInfoAccess
          :       (1 3 6 1 5 5 7 1 11)
    866   57:      OCTET STRING, encapsulates {
```



```
    868   55:       SEQUENCE {
    870   53:        SEQUENCE {
    872    8:         OBJECT IDENTIFIER '1 3 6 1 5 5 7 48 13'
    882   41:         [6]
          :          'https://rrdp.example.net/notification.xml'
          :          }
          :         }
          :        }
          :       }
          :      }
          :     }
          :    }
    925   13:  SEQUENCE {
    927    9:   OBJECT IDENTIFIER sha256WithRSAEncryption
          :    (1 2 840 113549 1 1 11)
    938    0:   NULL
          :    }
    940  257:  BIT STRING
```

```
:   05 1D 93 D2 A4 F6 57 56 65 B1 98 E3 FB 21 CF 4C
:   0A C8 54 11 02 64 54 82 74 FF 9B 25 3B 1E F3 94
:   EA 62 26 E5 32 C3 52 F7 21 2E D9 23 5B 69 93 0D
:   2E E4 92 88 07 DF 62 8A 21 E2 72 18 AB F4 61 EB
:   EC 46 B3 59 F8 DB B2 59 52 89 28 78 BB 58 D1 45
:   1B D9 F2 2C B9 AF 49 16 8F 18 19 39 E9 A8 33 06
:   7B EC 67 A5 B2 74 48 24 A8 06 52 42 22 3F 9B F9
:   84 BC 59 78 C4 1E DD 8A 5B AC 32 03 F0 5C 35 2F
:   1A 75 2D A9 11 4C 02 D9 CB 3F 59 CC 33 81 BB 6D
:   9E 47 27 1B BF F0 92 B4 37 A2 AC E9 0B 56 AB 29
:   E9 72 CF B3 C6 20 85 C9 1B 2F 67 17 C0 B7 FD A6
:   9A 12 91 DD ED 48 08 CA F5 D8 B8 26 3F 96 A5 93
:   9B DE E3 0F 18 06 21 81 82 EF AE B4 9A D7 CE 32
:   40 7C 60 5E A4 51 4F AD 77 67 43 42 C3 33 B5 C3
:   B1 6F 3A A2 1A 78 9C 99 E2 5F 07 01 B6 96 2E 8E
:   D2 FA 2B 5B 87 79 88 83 93 2A 94 32 A9 F8 78 E5
:   }
```

To allow reproduction of the signature results, the end-entity private key is provided. For brevity, the other two private keys are not.


```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAsnE0Kzm/6gdlt4tyovD4QPwxFsootk4BqPaYAsDvZbCESOmW
/5Pmkollj/ZEnM5XEILTwlcK+toU0GQiKMATdAS9HCtP+ZNYpiXYuanTN57yrMDP
Ap6EddbwfKUBcK7mZq+caYV0bxPps7iVS4LtldbqZgV7lpaHsprnYellifhg48D1
zt0YlwXowazhTV4WhS3tPMuAz36/0v7VyTgZu0M0KbZmzy2LRn6a2LuOZYhRaqj/
eFHi6SEn13d+gChs6kxQnHNxFvZeVBRNTBS5Z6BKIKraC6CgAbdCJDhRingvxIHm
gXVi3uOvXXQva0H7ecOoOnJsRvmmA3SBAd+M6wIDAQABAoIBAQCyB0FeMuKm8bRo
18aKjFGSPEoZi53srIz5bvUgIi92TBLez7ZnzL6Iym26oJ+5th+lCHGO/dqlhXio
pI50C5Yc9TFbblb/ECOsuCuuqKFjZ8CD3GVsHozXKJeMM+/o5YZXQrORj6UnwT0z
ol/JE5pIGUCIgsXX6tz9s5BP3lUAvVQHsv6+vEVKLxQ3wj/1vIL8O/CN036EV0GJ
mpkwmygPjfECT9wbWo0yn3jxJb36+M/QjjUP28oNIVn/IKoPZRXnqchEbuuCJ651
```

```
IsaFSqtiThm4WZtvCH/IDq+6/dcMucmTjIRcYwW7fdHfjplllVPve9c/OmpWEQvF
t3ArWUt5AoGBANs4764yHxo4mctLIE7G7l/tf9bP4KKUiYw4R4ByEocuqMC4yhmt
MPCfOFLOQet71OWCkjP2L/7EKUe9yx7G5KmxAHY6jOjvcRkvGsl6lWFOsQ8p126M
Y9hmGzMOjtsdhAiMmOWKzjvm4WqfMgghQe+PnjjSVkgTt+7BxpIuGBAvAoGBANBg
26FF5cDLpixOd3Za1YXsOgguwCaw3Plvi7vUZRpa/zBMELEtyOebfakkIRWNm07l
nE+lAZwxm+29PTD0nqCFE91teyzjnQaLO5kkAdJiFuVV3icLOGo399FrnJbKensm
FGSli+3KxQhCNIJJfgWzq4bE0ioAMjdGbYXzIYQFAoGBAM6tuDJ36KDU+hIS6wu6
O2TPSfZhF/zPo3pCWQ78/QDb+Zdw4IEiqoBA7F4NPVLg9Y/H8UTx9r/veqe7hPOo
Ok7NpIzSmKTHkc5XfZ60Zn9OLFoKbaQ40a1kXoJdWEu2YROaUlAe9F6/Rog6PHYz
vLE5qscRbu0XQhLkN+z7bg5bAoGBAKDsbDEb/dbqbyaAYpmwhH2sdRSkphg7NiwC
DNm9qWa1J6Zw1+M87I6Q8naRREuU1IAVqqWHVLr/ROBQ6NTJ1Uc5/qFeT2XXUgkf
taMKv61tuyjZK3sTmznMh0HfzUpWjEhWnCEuB+ZYVdmO52ZGw2A75RdrILL2+9Dc
PvDXVubRAoGAdqXeSWoLxuzZXzl8rsaKrQsTYaXnOWaZieU1SL5vVe8nK257UDqZ
E3ng2j5XPTUWli+aNGFEJGRoNtcQvO60O/sFZUhu52sqq9mWVYZNh1TB5aP8X+pV
iFcZOLUvQEcN6PA+YQK5FU11rAI1M0Gm5RDnVnUl0L2xfCYxb7FzV6Y=
    -----END RSA PRIVATE KEY-----
```

Signing of "192.0.2.0/24,US,WA,Seattle," (terminated by CR and LF), yields the following detached CMS signature.


```
# RPKI Signature: 192.0.2.0/24
# MIIGlwYJKoZIhvcNAQcCoIIGiDCCBoQCAQMxDTALBglghkgBZQMEAgEwDQYLKoZI
# hvcNAQkQARugggSxMIIErTCCA5WgAwIBAgIUJ605QIPX8rW5m4Zwx3WyuW7hZuMw
# DQYJKoZIhvcNAQELBQAwMzExMC8GA1UEAxMoM0FDRTJDRUY0RkIyMUI3RDExRTNF
```

```
   # MTg0RUZDMUUyOTdCMzc3ODY0MjAeFw0yMDA5MDMxOTA1MTdaFw0yMTA2MzAxOTA1
   # MTdaMDMxMTAvBgNVBAMTKDkxNDY1MkEzQkQ1MUMxNDQyNjAxOTg4ODlGNUM0NUFC
   # RjA1M0ExODcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCycTQrOb/q
   # B2W3i3Ki8PhA/DEWyii2TgGo9pgCwO9lsIRI6Zb/k+aSiWWP9kSczlcQgtPCVwr6
   # 2hTQZCIowBN0BL0cK0/5k1imJdi5qdM3nvKswM8CnoR11vB8pQFwruZmr5xphXRv
   # E+mzuJVLgu2V1upmBXuWloeymudh6WWJ+GDjwPXO3RiXBejBrOFNXhaFLe08y4DP
   # fr/S/tXJOBm7QzQptmbPLYtGfprYu45liFFqqP94UeLpISfXd36AKGzqTFCcc3EW
   # 9l5UFE1MFLlnoEogqtoLoKABt0IkOFGKeC/EgeaBdWLe469ddC9rQft5w6g6cmxG
   # +aYDdIEB34zrAgMBAAGjggG3MIIBszAdBgNVHQ4EFgQUkUZSo71RwUQmAZiIn1xF
   # q/BToYcwHwYDVR0jBBgwFoAUOs4s70+yG30R4+GE78Hil7N3hkIwDAYDVR0TAQH/
   # BAIwADAOBgNVHQ8BAf8EBAMCB4AwGAYDVR0gAQH/BA4wDDAKBggrBgEFBQcOAjBh
   # BgNVHR8EWjBYMFagVKBShlByc3luYzovL3Jwa2kuZXhhbXBsZS5uZXQvcmVwb3Np
   # dG9yeS8zQUNFMkNFRjRGQjIxQjdEMTFFM0UxODRFRkMxRTI5N0IzNzc4NjQyLmNy
   # bDBsBggrBgEFBQcBAQRgMF4wXAYIKwYBBQUHMAKGUHJzeW5jOi8vcnBraS5leGFt
   # cGxlLm5ldC9yZXBvc2l0b3J5LzNBQ0UyQ0VGNEZCMjFCN0QxMUUzRTE4NEVGQzFF
   # Mjk3QjM3Nzg2NDIuY2VyMCEGCCsGAQUFBwEHAQH/BBIwEDAGBAIAAQUAMAYEAgAC
   # BQAwRQYIKwYBBQUHAQsEOTA3MDUGCCsGAQUFBzANhilodHRwczovL3JyZHAuZXhh
   # bXBsZS5uZXQvbm90aWZpY2F0aW9uLnhtbDANBgkqhkiG9w0BAQsFAAOCAQEABR2T
   # 0qT2V1ZlsZjj+yHPTArIVBECZFSCdP+bJTse85TqYiblMsNS9yEu2SNbaZMNLuSS
   # iAffYooh4nIYq/Rh6+xGs1n427JZUokoeLtY0UUb2fIsua9JFo8YGTnpqDMGe+xn
   # pbJ0SCSoBlJCIj+b+YS8WXjEHt2KW6wyA/BcNS8adS2pEUwC2cs/WcwzgbttnkcN
   # G7/wkrQ3oqzpC1arKelyz7PGIIXJGy9nF8C3/aaaEpHd7UgIyvXYuCY/lqWTm97j
   # DxgGIYGC7660mtfOMkB8YF6kUU+td2dDQsMztcOxbzqiGnicmeJfBwG2li6O0vor
   # W4d5iIOTKpQyqfh45TGCAaowggGmAgEDgBSRRlKjvVHBRCYBmIifXEWr8FOhhzAL
   # BglghkgBZQMEAgGgazAaBgkqhkiG9w0BCQMxDQYLKoZIhvcNAQkQARswHAYJKoZI
   # hvcNAQkFMQ8XDTIwMDkwMzE5MTQzMVowLwYJKoZIhvcNAQkEMSIEICvi8p5S8ckg
   # 2wTRhDBQzGijjyqs5T6I+4VtBHypfcEWMA0GCSqGSIb3DQEBAQUABIIBABsRae94
   # 8DGcnE2230IavoT4xIzeJ6/ldy9FE9xx8oUsNrw7+dUf4pef7y5WmBiLxOWCmR/a
   # ovDUBqhERXLWTVfO9Y3DnPkY/DsAJGm7dA8vyfiODpvaoVr0Kjybjj60LSEtnEsW
   # 2CvR5fNvFX56Uh2bKdjp53uoIS+WESSo8T9RNwfRE758/iBvOoF8nvW0/r1GTh7Z
   # 68i0YHrQ0yW/cG59wac2F02B66024xuYF3Pd3R4L1cUDY8BORfF/1RJQnly0tet0
   # zjDBPfsQT4c7h62/ieL0LOkjzub+aCWSFt5yKcbG2eL4qERw6hAgWwxSqypy6kPp
   # Jn4hFJ0tmYWcKZM=
   # End Signature: 192.0.2.0/24
```

Authors' Addresses

Massimo Candela
NTT
Siriusdreef 70-72
Hoofddorp 2132 WT
Netherlands

Email: massimo@ntt.net

Randy Bush
IIJ & Arrcus
5147 Crystal Springs
Bainbridge Island, Washington 98110
United States of America

Email: randy@psg.com

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: warren@kumari.net

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA 20170
USA

Email: housley@vigilsec.com