

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 4, 2021

M. Candela
NTT
R. Bush
IIJ & Arrcus
W. Kumari
Google
August 31, 2020

Finding and Using Geofeed Data
draft-ymbk-opsawg-finding-geofeeds-00

Abstract

This document describes how to find and to prudently use 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 4, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

Finding Geofeeds

August 2020

Table of Contents

1.	Introduction	2
1.1.	Requirements Language	2
2.	Geofeed Files	2
3.	inet-num: Class	3
4.	Authenticating Geofeed Data	3
5.	Operational Considerations	4
6.	Security Considerations	5
7.	IANA Considerations	5
8.	Acknowledgements	5
9.	Normative References	5
	Authors' Addresses	6

[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. Additionally, 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](#)] inet-num: 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 prefix '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.](#) inet-num: Class

RPSL, [[RFC2622](#)], as used by the Regional Internet Registries (RIRs), has been augmented with the inet-num: class [[INETNUM](#)].

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

```
inet-num: 192.0.2.0/24 #example
remarks: Geofeed https://example.com/geofeed/
```

[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 inet-num: 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 prefix. 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.

As the signer would need to specify the covered RPKI resources relevant to the signature, the RPKI certificate covering the inet-num: object's prefix 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.

Candela, et al.

Expires March 4, 2021

[Page 3]

Internet-Draft

Finding Geofeeds

August 2020

Until [\[RFC8805\]](#) is updated to formally define such an appendix, it may be 'hidden' as a series of "#" comments at the end of the geofeed file.

```
# RPKI Signature: 192.0.2.0/24
# MIIgugYJKoZIhvcNAQcCoIDTALBgghkgBZQMEAgEwKQYLKoZIhvcNAQkQARig
# GgQYMBYCAhzRMBAwDgQCAAoIIeUDCCBLQwggOcoAMCAQICAwDe4TANBgkqhkiG
# 9w0BAQsFADAzMTEwLWYDVQQ0VBREI5Mzk2MTFDOTFGMDI3REI1NjNGQ0NDNUI5
# REUxMB4XDTE5MTIxOTE4NDMDAxMDEwMzExMC8GA1UEAxMoNjdBMDEwLWYDV
# RkeE2MDhCRjI0NjZjZjU0NTRDREOTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
# AQoCggEBALqRj0peHKFr4RuEo86/Pw7LZLkQVBeBI5UrcLSMjPttLLfz02dD3
# hNA2EnLMCPmMbh0kwCmsNsJ0+nbKyZJwbRmqpcnTJjndjxGY+ZnVkJXpPd4/S0o
# dvJi72LsU0lK4JVRI+wPTU0qqvB0gwYcTtTPEesyR/3ZJpA9sLPAQHUsCr9sGH
# 3DE0j0Qh2ub4pr6mR63497EwSLZYK5Q7xBAiYo0jfa0G3Ni7eqKfgvLyJe+bPD
# YMa4uuKhSYedIy+ubDnxglwNZ8lgGF9IECAwEAAa0CAc8wggHLMBOGA1UdDgQW
# BBRnoJw+H6YIvyRp01RYBQHSMEGDAWgBQjJt5c6tuTlhHJHwJ9tWP8zFud4TAY
# BgNVHSABAF8EDjAMMAoGCCA1UdHwRJMecwRaBDoEGGP3JzeW5j0i8vY2EwLnJw
# a2kubmV0L3Jwa2kvUkduZXNVlSeVI4Q2ZiVmpfTXhibmVFLmNybDBBbGgrBgEF
# BQcBAQRPMEOwSwYIKwYBBQOi8vY2EwLnJwa2kubmV0L3Jwa2kvYXV0Q0EvSXli
# ZVhPcmJrNVlSeVI4Q2ZiVmcjA0BgNVHQ8BAf8EBAMCB4AwgY4GCCsGAQUFBwEL
# BIGBMH8wSwYIKwYBBQUHMAY2EwLnJwa2kubmV0L3Jwa2kvUkduZXQvWjZDY1Bo
# LW1DThrhYVR0VVdBUU1iY1BggrBgEFBQcwDYYkaHR0cHM6Ly9jYTAucnBraS5u
# ZXQvcnJkcC9ub3RpZnkueGBwEHAQH/BBAwDjAMBAlAATAGAwQARaYlMA0GCSqG
# SIb3DQEBCwUAA4IBAQc+Cx9LN8dxjFFcohFRBRMnraXZjKhAaccKZ1v0PaG7iU
# lz6q1k37f0FuTSn7/eX/j9UZBMwQOQGZF87bGT3+Sh7qQCV0W0qB/V+Jknqrzk
# n9mL+ZwPw7fgVw4I8xBD7mVQoZhTPiGdLEUhhM7dP0moBNV8YdfLrB5fV1byWJ
# sE+LKDo3I+fJEt7imDo0gbqKWSS+1bpTTB5+V1Qc1rcKyZK7rp8tmsEQCxe2JM
# EWPML3do016M8ctjGUCXxT8dRhS047Z9e1drPCsd+rMYIBqjCCAaYCAQ0AFGeg
# nD4fpgi/JGk7VFgFDG3ENNAwQCAaBrMBoGCSqGSIB3DQEJAZENBgsqhkiG9w0B
```

```
# CRABGDACBgkqhkiG9w0BCQMTg0NjE0WjAvBgkqhkiG9w0BCQQxIgQgfEXq+Mbk
# 85Ro9ZcGTfrGLPRIpiqRIzDQYJKoZIhvcNAQEBBQAEggEAIa8unm8JGfiiTHXY
# HIiNNmZ8zIpR+AkWqZIpDRMgBzWxHyBVsmL01zce441FCJBgEr+TR36/uGvNes
# tV/35qkeykYxvBPhylSrwnKt6HHzfCE9wT6BIpiQPGLUdMGguUisG+hSaoZPG
# 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 inet-num: object's prefix range.

If no data in a geofeed file are signed per [Section 4](#), then multiple inet-num:s MAY refer to the same geofeed file, and the consumer MUST

Candela, et al.

Expires March 4, 2021

[Page 4]

Internet-Draft

Finding Geofeeds

August 2020

use only those covered by the prefix in the inet-num: 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 inet-num: objects pointing to malicious geofeed files. [Section 4](#) suggests an overly 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 and Russ Housley 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>>.

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