    **Multiple Repository Publication Points support in the Resource Public
                      Key Infrastructure (RPKI)**
            draft-ietf-sidr-multiple-publication-points-01

Abstract

   The Resource Public Key Infrastructure (RPKI) depends on Relying
   Parties (RP) ability to access its Trust Anchors' certificate
   specified in the different "Trust Anchor Locator (TAL)" files and the
   Repository Objects located at the Certificate Authorities (CA)
   repositories hosted in its respective publication point. This
   document updates [RFC6490] by allowing multiple URI associated to a
   single public key in a TAL file and introduces the concept of
   multiple repository publication point operators for every CA in the
   RPKI. This document provides also recommendation for the RP behavior
   when analyzing signed objects that include multiple publications
   points.

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 http://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 August 18, 2014.

Copyright Notice

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

2. **Introduction**

   The RPKI repository system described in [RFC6481] requires
   scalability and diversity in order to address challenges such as
   Distributed Denial of Service (DDoS) attacks, to secure the
   availability of the system when performing maintenance activities and
   against possible security incidents in one particular implementation.
   Additionally, when a single operator manages a RPKI Repository
   Publication Point, it is more probable to introduce circular
   dependencies when the Route Origin Authorization (ROA) signed objects
   for the Repository Publication Point IP addresses are hosted in
   servers that uses those same addresses.

   The current toolset for a CA to diversify its repository system is
   limited for both TA distribution and CA publication point management.
   In the case of trust anchors, [RFC6490] requires a unique URI per key
   on each TAL file. Conversely, in the case of the different
   publication points and although supported by [RFC6487] , there is no
   current guidance on how RPs should support multiple publication
   points for the same object.

   When using a single URI, the options for diversity and scalability
   are reduced to:

   1. Give the content to a Content Delivery Network (CDN) to have the
       content distributed (as long as the CDN supports the CA's access
       method , which is not currently the case for rsync). The
       implementation will typically require the configuration of a
       CNAME resource record in the authoritative server pointing to a
       server farm inside the CDN who will handle load-balancing by
       using a set of internally defined metrics. If, for the sake of
       diversity, a CA administrator would like to use two different
       CDNs for the same URI it will need to modify the authoritative
       name server behavior to break RFC1034 standard behavior and allow
       multiple CNAME records for the same alias. This modification is
       not available by default on most of the more widely deployed DNS
       servers.

   2. Copy the content to different Repository Publication Points
       around the globe (i.e. using [I-D.ietf-sidr-publication]) and
       load balance the content using different Domain Name System (DNS)
       techniques. The load balancing implementation will need to
       verify the availability of the target server before providing a
       DNS response to avoid blackholes caused by unavailable servers or
       clusters. This "feature" needs also be added to the
       authoritative name server or the full DNS resolution or
       outsourced to a third party (which would introduce another non-
       diversified element).

This document addresses this problem by enabling multiple operators for trust anchor material, and, while not making it mandatory, recommends the use of multiple publication points in signed objects.

The main idea is that the a CA will host its RPKI signed objects in different locations, using diverse routing paths and diverse DNS resolution. The RP will have more processing to perform to fetch the different objects when dealing with exceptions.

The first thing that is needed is to add multiple URIs support for each Trust Anchor. [RFC6490] requires that each TAL file includes a unique URI. This document removes this requirement by allowing one or more URI for each public key in a TAL file. In steady state, an RP should receive the same material from each of the different URI for the same root certificate. An exception could happen when the certificate is been updated or rolled-over, a process which should not have operational consequences.

For the root certificate trust anchor, this proposal has an additional consequence: it would create the idea of root-CA repository operators. This concept has worked well in the case of DNS, where one organization is responsible for creating the root zone material and a number of different organizations are responsible in running the root servers.

A CA can add support for multiple Repository Publication Points operators by adding more than one respective object for the Authority Information Access (AIA), the Subject Information Access (SIA) and the CRL Distribution Points (CRLDP) and which is supported by [RFC5280] and [RFC6487] . This document provides guidance on the RP expected behavior when analyzing signed objects with multiple Repository Publication Points in Section 4.

3. Multiple Operators support in TAL files

The idea of multiples operators support for a TA certificate
expressed on its TAL file is similar to the support for several Root
Server operators in a DNS hints file.

An example of such a TAL file with 3 operators would be:

```
rsync://rpki.operator1.org/rpki/hedgehog/root.cer
rsync://rpki.operator2.net/rpki/hedgehog/root.cer
rsync://rpki.operator3.biz/rpki/hedgehog/root.cer
```

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22gn/1oiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAjkk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueagpiLsFjwwpX6F+Ms8vqz45H+DKmYKvPSstZjCCq9
aJ0qANT9OtnfSDOS+aLRPjZryCNyvvBHxZXqj5YCGKtwIDAQAB

As we can see in this example, a RP would have different URI where to
fetch the self-signed certificate for the trust anchor. In each
location, the same result should be expected as all the URI share the
same public key.

In order to increase diversity, It is RECOMMENDED that the different
FQDN could be resolved to IP addresses included in ROA objects from
different CAs and hosted in diverse repository publication points.

3.1. Update to RFC 6490 Section 2.1

The following text will replace the last paragraph on Section 2.1 of
RFC 6490:

The TAL is an ordered sequence of:

1) One or more rsync URI [RFC5781],

2) A <CRLF> or <LF> line break after each URI,

3) A line containing a single <CRLF> or <LF> line break, and

4) A subjectPublicKeyInfo [RFC5280] in DER format [X.509], encoded in
Base64 (see Section 4 of [RFC4648]).A

3.2. Rules for Relying Parties (RP)

   A RP can use different rules to select the URI from where fetch the
   Trust Anchor certificate. Some examples are:

   o Using the order provided in the TAL file

   o Selecting the URI randomly from the available list

   o Creating a prioritized list of URIs based on RP specific
      parameters such as connection establishment delay

   If the connection to the preferred URI fails or the fetched
   certificate public key does not match the TAL public key, the RP
   SHOULD fetch the TA certificate from the next URI of preference.

4. Multiple Operators support in Certificates

   The support for multiple operators in the RPKI Certificate Authority
   (CA) and End Entity (EE) certificates is supported as the RFC 5082
   allows multiple repository publication point operators as the SIA,
   AIA and CRLDP are implemented as sequences. Consequently, no changes
   are needed on the existing RPKI standard and this section could be
   considered informative.

   In the case of the SIA extension, for each operator, the
   accessMethods for both the CA repository publication point and for
   the correspondent manifest needs to be added.

4.1. Rules for Relying Parties (RP)

   A RP can use different rules to select the URI to fetch the different
   repository objects and when performing the validation.

   When a RP needs to fetch one or more object from a list of possible
   URIs, it can chose the URI by adopting a locally defined rule that
   could be:

   o Using the order provided in the correspondent certificate

   o Selecting the URI randomly from the available list

   o Creating a prioritized list of URIs based on RP specific
      parameters such as connection establishment delay

   If the connection to the preferred URI fails , the RP SHOULD fetch
   the repository objects from the next URI of preference.

5. IANA Considerations

   No IANA requirements

6. Security Considerations

   TBA

7. Acknowledgements

   TBA.

8. Normative References

   [I-D.ietf-sidr-publication]
              "A Publication Protocol for the Resource Public Key
              Infrastructure (RPKI)", <http://www.ietf.org/id/
              draft-ietf-sidr-publication-02.txt>.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S.,
              Housley, R., and W. Polk, "Internet X.509 Public Key
              Infrastructure Certificate and Certificate Revocation List
              (CRL) Profile", RFC 5280, May 2008.

   [RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for
              Resource Certificate Repository Structure", RFC 6481,
              February 2012.

   [RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate
              Policy (CP) for the Resource Public Key Infrastructure
              (RPKI)", BCP 173, RFC 6484, February 2012.

   [RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for
              Use in the Resource Public Key Infrastructure (RPKI)",
              RFC 6485, February 2012.

   [RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for
              X.509 PKIX Resource Certificates", RFC 6487,
              February 2012.

   [RFC6490] Huston, G., Weiler, S., Michaelson, G., and S. Kent,
              "Resource Public Key Infrastructure (RPKI) Trust Anchor
              Locator", RFC 6490, February 2012.

   [RFC6492] Huston, G., Loomans, R., Ellacott, B., and R. Austein, "A
              Protocol for Provisioning Resource Certificates",
              RFC 6492, February 2012.

Authors' Addresses

    Roque Gagliano
    Cisco Systems
    Avenue des Uttins 5
    Rolle,   1180
    Switzerland

    Email: rogaglia@cisco.com

    Terry Manderson
    ICANN

    Email: terry.manderson@icann.org

    Carlos Martinez Cagnazzo
    LACNIC

    Email: carlos@lacnic.net