Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 26, 2015

R. Bush
Internet Initiative Japan

June 24, 2015

RPKI Local Trust Anchor Use Cases
draft-ietf-sidr-lta-use-cases-03

Abstract

There are a number of critical circumstances where a localized routing domain needs to augment or modify its view of the Global RPKI. This document attempts to outline a few of them.

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 December 26, 2015.

Copyright Notice

Copyright (c) 2015 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 (http://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.

Table of Contents

1. Introduction

Today RPKI-based Origin Validation, [RFC6811], relies on widespread deployment of the Global Resource Public Key Infrastructure (RPKI), [RFC6480]. In the future, RPKI-based Path Validation, [I-D.lepinski-bgpsec-overview], will be even more reliant on the Global RPKI.

But there are critical circumstances in which a local, clearly-scoped, administrative and/or routing domain will want to augment and/or modify their internal view of the Global RPKI.

This document attempts to lay out a few of those use cases. It is not intended to be authoritative, complete, or to become a standard. It merely tries to lay out a few critical examples to help frame the issues.

2. Suggested Reading

It is assumed that the reader understands the RPKI, see [RFC6480], the RPKI Repository Structure, see [RFC6481], Route Origin Authorizations (ROAs), see [RFC6482], and GhostBusters Records, see [RFC6493].

3. What is 'Local'

The RPKI is a distributed database containing certificates, CRLs, manifests, ROAs, and GhostBusters Records as described in [RFC6481]. Policies and considerations for RPKI object generation and maintenance are discussed elsewhere.

Like the DNS, the Global RPKI tries to present a single global view, although only a loosely consistent view, depending on timing,

updating, fetching, etc. There is no 'fix' for this, it is not broken, it is the nature of distributed data with distributed caches.

There are critical uses of the RPKI where a local administrative and/or routing domain, e.g. an end-user site, a particular ISP or content provider, an organization, a geo-political region, ... may wish to have a specialized view of the RPKI.

For the purposes of this exploration, we refer to this localized view as a 'Local Trust Anchor', mostly for historical reasons, but also because implementation would likely require the local distribution of one or more specialized trust anchors, [RFC6481].

4. Example Uses

We explore this space using three examples.

Carol, a RIPE resource holder (LIR, PI holder, ...), operates outside of the Netherlands. Someone convinces a Dutch court to force the RIPE/NCC to remove or modify some or all of Carol's certificates, ROAs, etc. or the resources they represent, and the operational community wants to retain the ability to route to Carol's network(s). There is need for some channel through which operators can exchange local trust, command, and data collections necessary to propagate patches local to all their RPKI views.

Bob has a multi-AS network under his administration and some of those ASs use private ([RFC1918]) or 'borrowed' address space which is not announced on the global Internet, and he wishes to certify them for use in his internal routing.

Alice is responsible for the trusted routing for a large organization, commercial or geo-political, in which management requests routing engineering to redirect their competitors' prefixes to socially acceptable data, and Alice is responsible for making the CA hierarchy have validated certificates for those redirected resources as well as the rest of the Internet.

5. Notes

In these examples, it is ultimately the ROAs, not the certificates, which one wants to modify or replace. But one probably can not simply create new ROAs as one does not have the private keys needed to sign them. Hence it is likely that one has to also do something about the [RFC6480] certificates.

The goal is to modify, create, and/or replace ROAs and GhostBuster Records which are needed to present the localized view of the RPKI data.

One wants to reproduce only as much of the Global RPKI as needed. Replicating more than is needed would amplify tracking and maintenance.

One can not reissue down from the root trust anchor at the IANA or from the RIRs' certificates because one do not have the private keys required. So one has to create a new trust anchor which, for ease of use, will contain the new/modified certificates and ROAs as well as the unmodified remainder of the Global RPKI.

Because Alice, Bob, and Carol want to be able to archive, reproduce, and send to other operators the data necessary to reproduce their modified view of the global RPKI, there will need to be a formally formally defined set of data which is input to a well-defined process to take an existing Global RPKI tree and produce the desired modified re-anchored tree.

It is possible that an operator may need to accept and process modification data from more than one source. Hence modification 'recipes' should be mergable.

6. Security Considerations

These use cases are all about violating global security, albeit within a constrained local context.

Authentication of modification 'recipes' will be needed.

7. IANA Considerations

This document has no IANA Considerations.

8. Acknowledgments

The author wishes to thank Rob Austein, Steve Kent, and Karen Seo.

9. References

9.1. Normative References

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

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

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012.

[RFC6493] Bush, R., "The Resource Public Key Infrastructure (RPKI) Ghostbusters Record", RFC 6493, February 2012.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, January 2013.

9.2. Informative References

[I-D.lepinski-bgpsec-overview]
Lepinski, M. and S. Turner, "An Overview of BGPSEC", draft-lepinski-bgpsec-overview-00 (work in progress), March 2011.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

Author's Address

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, Washington 98110
US

Email: randy@psg.com