Secure Inter-Domain Routing	T. Manderson
Internet-Draft	G. Michaelson
Intended status: Standards Track	APNIC
Expires: December 25, 2008	June 23, 2008

TOC

Alternative RPKI Repository Retrieval Mechanism
draft-sidr-fetch-00

Status of this Memo

Abstract

This document proposes a mechanism for a relying party to synchronise a local cache of the RPKI repository using a HTTP retrieval mechanism.

Table of Contents

---

1. Introduction

TOC

This document details a mechanism and algorithm for a relying party to synchronise a local cache of RPKI objects against the collection of original publication points.

1.1. Terminology

TOC

It is assumed that the reader is familiar with the terms and concepts described in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (Housley, R., Polk, W., Ford, W., and D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” April 2002.) [RFC3280], "A Profile for X.509 PKIX Resource Certificates" (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” September 2009.) [I-D.ietf-sidr-res-certs] "Manifests for the Resource Public Key Infrastructure" (Austein, R., Huston, G., Kent, S., and M. Lepinski, “Manifests for the Resource Public Key Infrastructure,” December 2009.) [I-D.ietf-sidr-rpki-manifests], "X.509 Extensions for IP Addresses and AS Identifiers" (Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers,” June 2004.) [RFC3779], "Hypertext Transfer Protocol -- HTTP/1.1" (Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, “Hypertext

Transfer Protocol -- HTTP/1.1," June 1999.) [RFC2616], "HTTP Over TLS" (Rescorla, E., "HTTP Over TLS," May 2000.) [RFC2818], and related regional Internet registry address management policy documents.

1.2. Requirements Language

TOC

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 RFC 2119.

---

2. Overview

TOC

2.1. RPKI Repository

TOC

An RPKI Repository is a collection of RPKI Publication Points.

2.2. Publication Points

TOC

A Publication Point is the location where RPKI objects exist for public use. The Publication Point also contains a manifest of all the RPKI objects that are published at that location. The Publication Point URI is held in the SIA of the RPKI Certificate that signed the objects at that Publication Point.

2.3. RPKI Manifests

TOC

A manifest is a signed object, listing of all of the RPKI objects at a publication point in the RPKI Repository, excluding the manifest itself. The manifest contains the file name and a hash of the contents of the RPKI object file.
The URI to the manifest exists in the manifest SIA from the Certificate that signed the manifest.
Manifest validation SHOULD be done according to "Manifests for the Resource Public Key Infrastructure" (Austein, R., Huston, G., Kent, S.,

and M. Lepinski, “Manifests for the Resource Public Key Infrastructure,” December 2009.) [I-D.ietf-sidr-rpki-manifests].

2.4. Object URI

TOC

The object location URI is constructed by using the Publish Point from the Signing RPKI Certificate SIA and the File (name) in the manifest signed by the Signing RPKI Certificate. The exception to this is the Certificate Authority (CA) certificate and manifest relationship.

2.5. CA and Manifest Relationship

TOC

In the situation that the certificate in focus is the Certificate Authority (CA) certificate:

- Like all RPKI certificates (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” September 2009.) [I-D.ietf-sidr-res-certs] the CA contains a SIA that identifies a Publish Point and a Manifest.

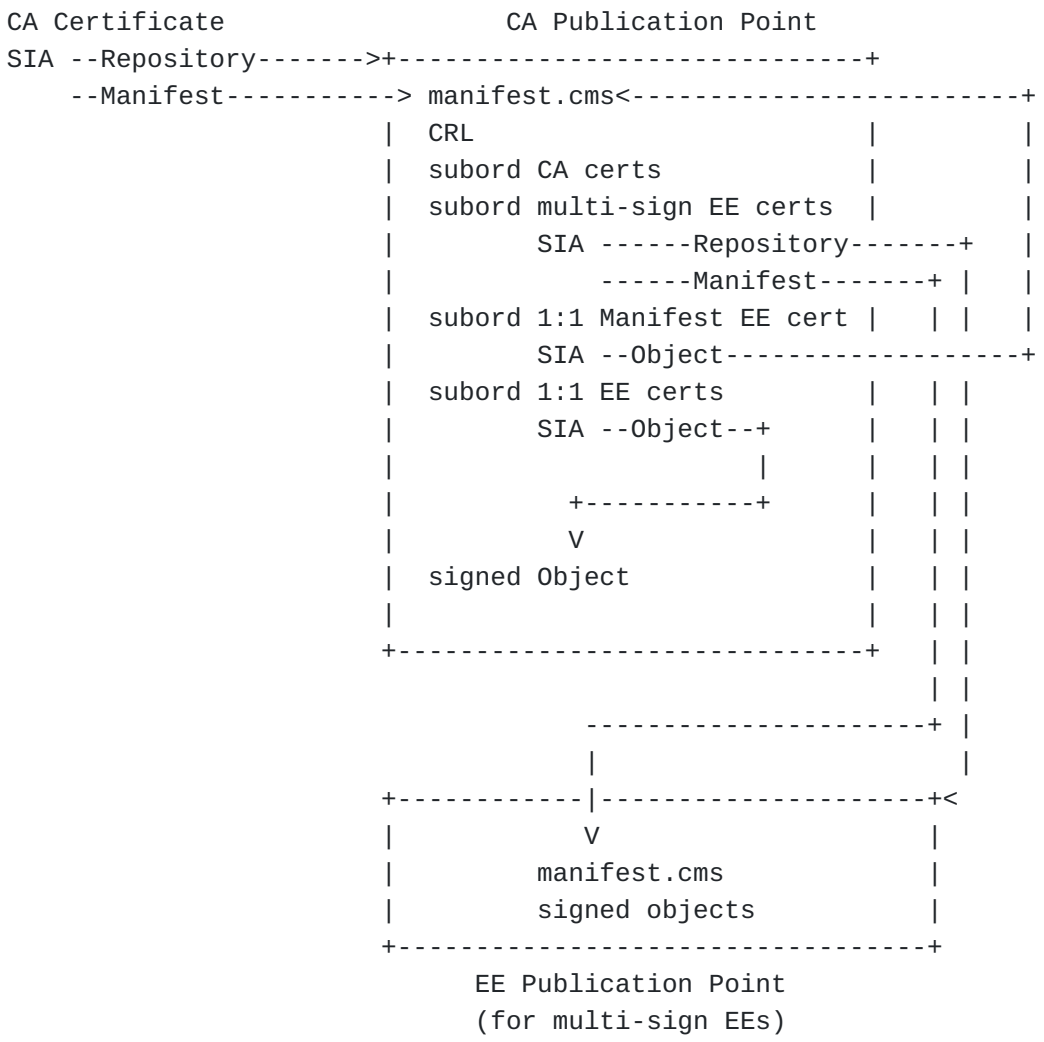
- The CA signs an End Entity (EE) Certificate for the single purpose of signing the CA manifest.

- The EE certificate has an SIA that also identifies the manifest.

2.6. Traversing a RPKI Repository

TOC

A generalised RPKI hierarchy structure of a resource repository, including the out of band collected Trust Anchor (CA), can be represented as:



The following broad algorithm MAY be used to traverse the hierarchy, starting with the Trust Anchor or CA RPKI Certificate.

1. Collect the manifest referenced in the id-ad-rpkiManifest (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X. 509 PKIX Resource Certificates,” September 2009.) [I-D.ietf-sidr-res-certs] Manifest AccessMethod of the SIA of the Certificate.

2. Collect, from the Publication Point, every valid object listed in the manifest.

3. For each subordinate object with id-ad-signedObjectRepository (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X. 509 PKIX Resource Certificates,” September 2009.)

[I-D.ietf-sidr-res-certs] and id-ad-rpkiManifest access method SIA values repeat fom step 1.

Processing of each subordinate Publish Point MAY be done in parallel, provided sufficient RPKI material has been collected for Manifest and RPKI validation.

---

3. Transport Protocol

TOC

3.1. HTTP

TOC

When transferring a RPKI objects HTTP 1.1 (Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.) [RFC2616]SHOULD be used as the underlying transport mechanism, as specified by the URI in the SIA field. Various HTTP methods MAY be used to minimise the number of fetches and data transfers over the transport connection.

3.2. HTTPS

TOC

HTTPS (Rescorla, E., "HTTP Over TLS," May 2000.) [RFC2818] based transfers MAY be used in order to ensure the integrity of the repository site or to encrypt the retrieval of the RPKI objects. It is therefore up to the resource certificate issuer to understand any potential operational performance issues associated with using A HTTPS URI in the RPKI certificate SIA fields.

3.3. Other Protocols

TOC

The retrieval algorithm specified in this document can also be used by other protocols as an effecient way to synchronise the RPKI repository with a local cache, provided HTTP specifics such as (but not limited to) redirects, http pragma, connection behaviours and pipe-lining are addresed.

TOC

4. Retrieval

4.1. Retrieval Algorithm

TOC

If the SIA for the Publish Point of the RPKI Certificate Authority (CA) Certificate or End Entity Certificate defines a HTTP or HTTPS access method in the URI then the following algorithm MAY be used by a Retrieval Client for any initial and subsequent fetch of certificates and signed outcomes (objects) from an RPKI Repository Server (RRS).

4.1.1. Post RPKI Validated (PRV)

TOC

a. Fetch the appropriate manifest (Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure," December 2009.) [I-D.ietf-sidr-rpki-manifests] from the RRS. The RC MAY maintain the connection to the RRS with a persistent connection.

b. Confirm the manifest's validity.

- *If the manifest is invalid, or the manifest is empty, terminate processing and close any RRS connections

c. Construct a list of URIs to be retrieved by comparing hash values in the downloaded manifest, with the hash values of the locally cached object:

- *If a local manifest does not exist then all objects contained in the manifest MUST be listed for retrieval.
- *If an object entry in the downloaded manifest does not exist locally, the URI SHOULD be added to the retrieval list.
- *If an object exists locally and does not appear in the manifest, it SHOULD be deleted from the local cache.
- *If the hash value of the object in the downloaded manifest does not match the hash value of the local copy of the object, the URI of the object SHOULD be added to the retrieval list.
- *If the retrieval list is empty, terminate processing and close any RRS connections.

d.
Fetch the list of objects using pipe-lined GET requests.

*HTTP redirects SHOULD be honoured by the client and followed using a separate RRS connection for the object.

e. Confirm that all of the objects listed in the downloaded manifest have been retrieved.

f. Confirm the hash of the downloaded object file contents matches the hash stored in the downloaded manifest

*If the hash does not match, the object MAY be newer than the manifest and the object SHOULD be RPKI validated.

g. Close any RRS connections.

h. RPKI Validate the retrieved objects and store the validated objects in the local cache.

---

5. Client Considerations

TOC

5.1. Hash Comparison

TOC

As described in the PRV algorithm, if the hash does not match, the object may be newer than the manifest. It is RECOMMENDED that suitable warnings be generated by the retrieval client to alert to any issues of a hash mismatch.

5.2. Hash Mismatch

TOC

To minimise the occurrences of hash values that do not match, the RC MAY consider postponing retrieval of a RPKI Repository for some period of time either side of the "nextUpdate" time detailed in the manifest.

TOC

6. Acknowledgements

Due recognition needs to be given to all the individuals involved in the inter-RIR Resource Certificate working group.

---

7. IANA Considerations

TOC

This memo includes no request to IANA.

---

8. Security Considerations

TOC

8.1. RC to RRS Channel Attacks

TOC

Using an unencrypted channel could expose the relying party to either man-in-the-middle or remote Denial of Service (DoS) HTTP/TCP attacks against the channel between the RC and the RRS.
The certificate issuer should consider the potential for disruption to the relying party operations in selecting the preferred SIA access methods.

8.2. RRS and Manifest Integrity

TOC

A scenario exists where a malicious attack could place an invalid RPKI certificate on the RRS in the Publication Point prior to the manifest creation. While this does not represent a high risk to the overall Resource Certificate system as the object will fail to validate, it may affect the Relying Party as:

- An object is extremely large and RC retrieves the object this may cause resource network or other types of congestion.

- Many invalid objects, which the RC must download, may affect overall performance or the RC or the overall Resource Certificate system.

---

9. Normative References

TOC

[I-D.huston-sidr-repos-struct]	Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure," draft-huston-sidr-repos-struct-01 (work in progress), February 2008 (TXT).
[I-D.ietf-sidr-res-certs]	Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," draft-ietf-sidr-res-certs-17 (work in progress), September 2009 (TXT).
[I-D.ietf-sidr-rpki-manifests]	Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure," draft-ietf-sidr-rpki-manifests-06 (work in progress), December 2009 (TXT).
[RFC2616]	Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," RFC 2616, June 1999 (TXT, PS, PDF, HTML, XML).
[RFC2818]	Rescorla, E., "HTTP Over TLS," RFC 2818, May 2000 (TXT).
[RFC3280]	Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280, April 2002 (TXT).
[RFC3779]	Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers," RFC 3779, June 2004 (TXT).

Authors' Addresses

TOC

	Terry Manderson
	APNIC
	AU
Phone:	+61 7 3858 3100
Email:	terry@apnic.net
	George Michaelson
	APNIC
	AU
Phone:	+61 7 3858 3100
Email:	ggm@apnic.net

Full Copyright Statement

TOC

Intellectual Property