Secure Inter-Domain Routing
Internet-Draft
Intended status: BCP
Expires: November 16, 2010

G. Huston
R. Loomans
G. Michaelson
APNIC

May 15, 2010

A Profile for Resource Certificate Repository Structure
draft-ietf-sidr-repos-struct-04.txt

Abstract

This document defines a profile for the structure of repository publication points that contain X.509 / PKIX Resource Certificates, Certificate Revocation Lists and signed objects. This profile contains the proposed object naming scheme, the contents of repository publication points, the contents of publication point manifests and a suggested internal structure of a local repository cache that is intended to facilitate synchronisation across a distributed collection of repository publication points and facilitate certification path construction.

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 November 16, 2010.

Copyright Notice

Table of Contents

1. Introduction

To validate attestations made in the context of the Resource Public Key Infrastructure (RPKI) [I-D.sidr-arch] Relying Parties (RPs) need access to all the X.509 / PKIX Resource Certificates, Certificate Revocation Lists (CRLs), and signed objects that collectively define the RPKI.

Each issuer of a certificate, CRL or a signed object makes it available for download to RPs through the publication of the object in a RPKI repository.

The repository system is the central clearing-house for all signed objects that must be globally accessible to all RPs. When certificates, CRLs and signed objects are created, they are uploaded to a repository publication point, from whence they can be downloaded for use by RPs.

This document defines a profile for the structure of RPKI repositories. This profile contains the proposed object naming scheme, the contents of repository publication points, the contents of publication point manifests and a possible internal structure of a Repository Cache that is intended to facilitate synchronisation across a distributed collection of repositories and facilitate certificate path construction.

A Resource Certificate describes an attestation by an Issuer that binds a list of IP address blocks and AS numbers to the Subject of a certificate, identified by the unique association of the Subject's private key with the public key contained in the Resource Certificate.

1.1. Terminology

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" [RFC5280], "X.509 Extensions for IP Addresses and AS Identifiers" [RFC3779], and related regional Internet registry address management policy documents.

2. RPKI Repository Publication Point Content and Structure

The RPKI does not use a single repository publication point to publish RPKI objects. Instead, the RPKI repository system is comprised of multiple repository publication points. Each repository publication point is associated with one or more RPKI certificates'

publication points, as defined in the certificate's Subject Information Authority (SIA) extension.

This section describes the collection of objects (RPKI certificates, CRLs, manifests and signed objects) held in repository publication points.

For every certificate in the PKI, there will be a corresponding repository publication point file system directory that is the authoritative publication point for all objects signed by the private key part of the key pair whose public key part is the subject public key of this certificate.

Objects are added to the publication point when issued by the associated CA, or when signed by the private key part of a key pair whose subject public key is described in an EE certificate that is associated with the repository publication point, and are removed when expired or revoked.

The certificate's Subject Information Authority (SIA) extension provides a URI that references this repository publication point and supported repository access mechanisms. Additionally, a certificate's Authority Information Authority (AIA) extension contains a URI that references the authoritative location for the Certification Authority (CA) certificate under which the given certificate was issued. That is, if the subject of certificate A has issued certificate B, then the AIA extension of certificate B points to certificate A, and the SIA extension of certificate A points to a repository publication point file system directory containing

certificate B (see Figure 1).

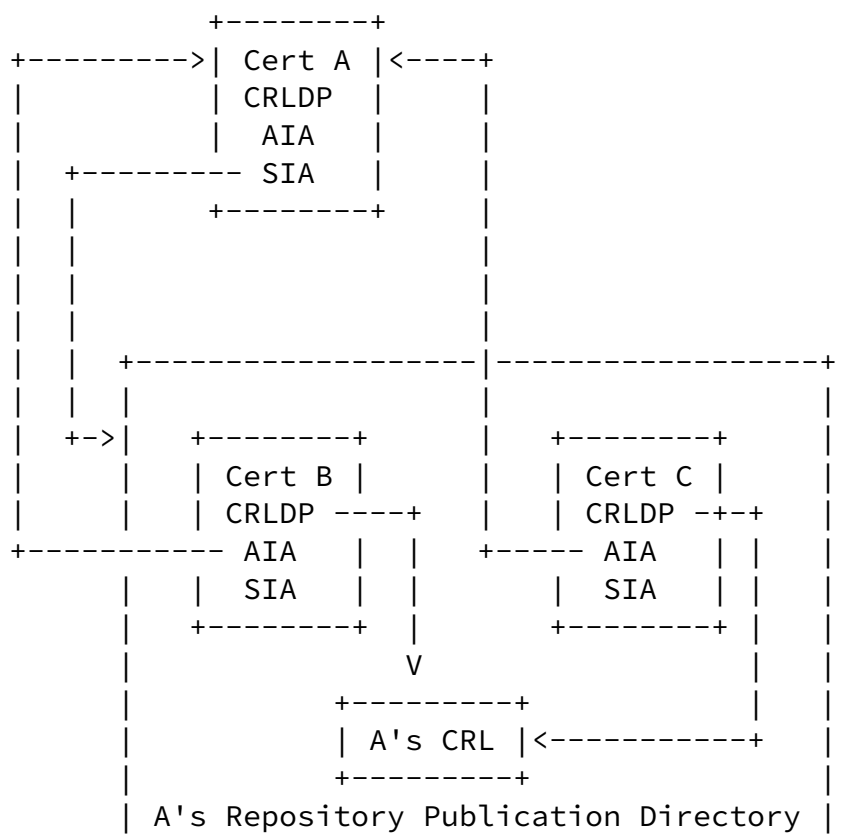

Figure 1: Example Repository Structure.

In the example shown in Figure 1, certificates B and C are issued by CA A. Therefore, the AIA extensions of certificates B and C point to the object publication point where Certificate A is published, and the SIA extension of certificate A points to the repository publication point of CA A's subordinate products, including certificates B and C, as well as A's CRL.

The general intent of this distributed repository structure is that an instance of a CA's repository publication point contains all the signed products of that CA, and an End Entity's (EE's) repository publication point contains all the objects that have been signed by the private key part of a key pair whose public key is described in the subject public key of the associated EE certificate.

2.1. Manifests

All CA's and all EE's that have repository publication points ("multi-use" EE certificates, as defined in [I-D.sidr-res-certs]) MUST maintain a manifest [I-D.sidr-rpki-manifests] of their published subordinate products. The manifest contains a list of the names of all objects issued by that CA, or signed by the private key part of a key pair whose public key is the subject public key of the associated

EE certificate, and published in a repository publication point file system directory, as well as the hash value of each object's contents.

An authority MAY perform a number of object operations on a publication repository within the scope of a repository change before issuing a single manifest that covers all the operations within the scope of this change. Repository operators SHOULD implement some form of synchronisation function on the repository to ensure that relying parties who are performing retrieval operations on the repository are not exposed to intermediate states during changes to the repository and the associated manifest.

2.2. CA Repository Publication Point

A CA Certificate has two accessMethod elements specified in its SIA field. The id-ad-caRepository accessMethod element has an associated accessLocation element that points to the repository publication point of the products of this CA, as specified in [I-D.sidr-res-certs]. The id-ad-rpkiManifest accessMethod element has an associated accessLocation element that points to the manifest object, as an object URL, that is associated with this CA.

In the case of a CA's publication repository in the scope of the RPKI, the repository contains the current unrevoked certificates issued by this CA, the most recent CRL that is associated with the CA's non-revoked key pairs, the current unrevoked manifest, and all current objects that are signed using the private key of a key pair whose public key is the subject public key of a current unrevoked "single-use" EE certificate, where the EE certificate was issued by this CA.

The CA's manifest describes all the current unrevoked objects that are to be found in that publication point that were issued by this CA, and all published objects signed using the private key of a key pair whose public key is the subject public key of a current unrevoked "single-use" EE certificate that has been issued by this CA, and the hash value of each object (excluding the manifest itself) [I-D.sidr-rpki-manifests].

Because an instance of a CA is associated with a single key pair, an entity performs the equivalent of a key rollover operation by generating a new CA instance as well as a new key pair. In such cases the entity may chose to continue the use of a single repository publication point for both CA instances. In such cases the repository publication point will contain the CRL, manifest, subordinate certificates and signed objects of both CA instances.

Some guidelines for naming objects in a CA's repository publication point are as follows:

CRL: The scope of a CRL in the RPKI is all objects issued by a CA, implying that publication of successive instances of a CA's CRL should overwrite previous instances of CRLs signed by the same CA's private key in the publication repository. It is consistent with this objective that the name chosen for the CRL in the

publication repository be a value derived from the public key part of the CA's key pair whose private key was used to sign the CRL. One such method of generating a CRL publication name is described in section 2.1 of [RFC4387], converting the 160-bit hash of the CA's public key value into a 27-character string using a modified form of Base64 encoding, with an additional modification as proposed in section 5, table 2, of [RFC4648]. A CRL MAY use a filesystem name extension of ".crl" to denote the object as a CRL.

Manifest: When a new instance of a manifest is published by the CA, there is no requirement within the RPKI for any RP to have continuing access to older instances of the CA's manifest. When multiple CA's share a common repository publication point their respective manifests must be distinct. It is consistent with this objective that the name chosen for the manifest in the publication repository be a value derived from the public key part of the CA's key pair, using the algorithm described above for CRL object names. A manifest MAY use a filesystem name extension of ".mft" to denote the object as a manifest.

Certificates: Within the RPKI framework it is possible that a CA may issue a series of certificates for the same subject name, the same subject public key, and the same resource collection. Within the context of each such series of certificates a RP has an interest only in the most recently published current certificate. The publication repository object name scheme for the CA may use a unique name for each such series of certificates, thereby ensuring that each successive issued certificate in such a series effectively overwrites the previous instance of the certificate in the publication repository. If the CA adopts a local policy that each subject uses a unique key pair for each unique instance of a certified resource collection then the CA can use a certificate object name scheme that is derived from the subject's public key, applying the algorithm described above for CRL object names to the subject's public key value. A certificate MAY use a filesystem name extension of ".cer" to denote the object as a certificate.

Signed Objects: Within the RPKI framework there are two kinds of EE

certificates that are used in conjunction with digital certificates: "single-use" EE certificates, where the private key of the key pair whose public key is the subject public key of the EE certificate is used to sign a single object, and "multi-use" EE Certificates, whose private key of the key pair whose public key is the subject public key of the EE certificate may be used to sign multiple objects. In the case of "single-use" EE certificates, the single signed object is to be published in the same repository publication point as the associated EE certificate. The signed object name scheme for such objects can be derived from the associated EE certificate's subject public key, applying the algorithm described above for CRL object names to the EE certificates's subject public key value. The signed object is listed in the manifest associated with this repository publication point. In the case of "multi-use" EE certificates the repository publication point is described in the following section.

2.3. EE Repository Publication Point

EE repository publication points are used in conjunction with "multi-use" EE Certificates. In this case the EE Certificate has two accessMethod elements specified in its SIA field. The id-ad-signedObjectRepository accessMethod element has an associated accessLocation element that points to the repository publication point of the objects signed by the private key of a key pair whose public key is the subject public key of this EE certificate, as specified in [I-D.sidr-res-certs]. The id-ad-rpkiManifest accessMethod element has an associated accessLocation element that points to the manifest object as an object URL, that is associated with this repository publication point. This manifest describes all the signed objects that are to be found in that publication point that have been signed by the private key of a key pair whose public key is the subject public key of this EE certificate, and the hash value of each product (excluding the manifest itself) [I-D.sidr-rpki-manifests].

In the case of an EE's publication repository in the scope of the RPKI, the repository contains objects that have been signed by the private key of the key pair whose public key is the subject public key of the EE certificate, and a manifest of all such signed objects.

The objects published in a EE repository publication point do not form a logical sequence, and must be named uniquely in the context of the publication repository.

It is consistent with this specification, but not recommended

practice, that all subordinate EE's of a given CA share a common publication repository. In this case the repository publication point would contain multiple manifest objects, one for each EE that has placed objects into this common publication point. Each manifest is limited in scope to listing the objects signed by the EE certificate. The implication is that all objects signed by the private key of a key pair whose public key is the subject key of a single EE certificate, including the EE's manifest, share a base name element that is generated from the public key of the EE certificate. The choice of whether to use a common single publication repository or a dedicated publication repository for each EE certificate is an implementation choice.

3. Resource Certificate Publication Repository Considerations

Each issuer may publish their issued certificates and CRL in any location of their choice. However, there are a number of considerations which guide the choice of a suitable repository publication structure.

- The publication repository SHOULD be hosted on a highly available service and high capacity publication platform.

- The publication repository MUST be available using RSYNC [RFC5781][I-D.sidr-res-certs] Support of additional retrieval mechanisms is the choice of the repository operator. The supported retrieval mechanisms should be consistent with the accessMethod element value(s) specified in the SIA of the associated CA or EE.

- Each CA repository publication point file system directory in the publication repository should contain the products of this CA, including those objects signed by single-use EE certificates that have been issued by this CA. The signed products of related CA's that are operated by the same entity may share the CA repository publication point file system directory. Aside from subdirectories, no other objects should be placed in a repository publication point file system directory.

  Any such subdirectory should be the repository publication point file system directory of a CA or EE certificate that is contained in the CA's repository publication point file system directory. There are no constraints on the name of a repository publication point file system subdirectory. These considerations also apply recursively to subdirectories of these repository publication

point file system subdirectories directories.

- Signed Objects are published in the location indicated by the SIA field of the EE certificate that has certified the public key part of the key pair whose private key part was used to sign the object. The choice of the repository publication point is determined by the nature of the signing EE certificate. In the case of "multi-use" EE certificates the signed object is published in an EE repository publication point as referenced by the SIA extension of the EE certificate. In the case of "single-use" EE certificates the signed object is published in the repository publication point of the CA certificate that issued the EE certificate, and the SIA extension of the single use EE certificate references this object rather than the repository publication point file system directory[I-D.sidr-res-certs].

4. Certificate Reissuance and Repositories

If a CA certificate is reissued, it should not be necessary to reissue all certificates signed by the certificate being reissued. Therefore, a CA SHOULD use a persistent naming scheme for the certificate's repository publication point that is persistent across certificate re-issuance events. That is, reissued certificates SHOULD use the same repository publication point as previously issued certificates having the same subject and subject public key, and SHOULD overwrite previously issued certificates within the repository publication point file system directory.

5. Synchronising Repositories

It is possible to perform the validation-related task of certificate path construction using retrieval of individual certificates and certificate revocation lists using online retrieval of individual certificates, sets of candidate certificates and certificate revocation lists based on the Authority Information Access, Subject Information Access and CRL Distribution Points certificate fields. This is not recommended in circumstances where speed and efficiency are relevant considerations. Where an efficient validation operation is required, it is RP MAY maintain a local repository containing a

synchronised copy of all current valid certificates, current certificate revocation lists, and all related signed objects, maintained as a local current copy of the complete distributed RPKI repository collection.

The general approach to repository synchronisation is one of a "top-down" walk of the distributed repository structure, commencing with the initial configured trust anchor certificates, and then populating the local repository cache will all valid certificates that have been

issued by these issuers, and then recursively applying the same approach to each of these subordinate certificates. Such a repository traversal process would need to support some locally configured maximal chain length from the initial trust anchors to the current working validation point in order to ensure that the process does not follow a loop or a non-terminating certificate chain.

6. Security Considerations

Repositories are not "protected" structures, and repository retrieval operations are vulnerable to various forms of "man-in-the-middle" attacks. Corruption of retrieved objects is detectable by a RP through the RPKI validation of the retrieved object. Insertion of older objects is detectable by the CRL, assuming that the older object has been revoked by the issuer. However, certain forms of substitution and removal attacks are not directly detectable. For this reason all published RPKI objects are described in a manifest [I-D.sidr-rpki-manifests]. The manifest can improve the level of assurance that a RP is receiving an authentic copy of the repository, and that the set of retrieved objects is complete.

7. IANA Considerations

[There are no IANA considerations in this document.]

8. Normative References

[I-D.sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support

Secure Internet Routing", draft-ietf-sidr-arch-08.txt (work in progress), July 2009.

[I-D.sidr-res-certs]
Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs-16.txt (work in progress), February 2008.

[I-D.sidr-rpki-manifests]
Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure", draft-ietf-sidr-rpki-manifests (work in progress), August 2009.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP

Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC4387] Gutmann, P., "Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP", RFC 4387, February 2006.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[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.

[RFC5781] Weiler, S., Ward, D., and R. Housley, "The rsync URI Scheme", RFC 5781, February 2010.

Authors' Addresses

Geoff Huston
Asia Pacific Network Information Centre

Email: gih@apnic.net
URI: http://www.apnic.net

Robert Loomans
Asia Pacific Network Information Centre

Email: robertl@apnic.net
URI: http://www.apnic.net

George Michaelson
Asia Pacific Network Information Centre

Email: ggm@apnic.net
URI: http://www.apnic.net