Individual Submission
Internet-Draft
Intended status: Best Current Practice
Expires: December 25, 2008

G. Huston
R. Loomans
G. Michaelson
APNIC
June 23, 2008

A Profile for Resource Certificate Repository Structure
draft-huston-sidr-repos-struct-02.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a profile for the structure of repositories 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 possible internal structure of a Repository Cache that is intended to facilitate synchronization across a distributed collection of

repositories and facilitate certificate path construction.

Table of Contents

1. Introduction

To validate attestations made in the context of the Resource Public Key Infrastructure (RPKI) relying parties 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 replying parties 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 relying parties. 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 relying parties.

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 synchronization across a distributed collection of repositories and facilitate certificate path construction.

A Resource Certificate describes an action 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" [RFC3280], "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

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 uniquely associated with a single RPKI certificate's publication point, 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 of this certificate (or "verifiable via this certificate"). The certificate's Subject Information Authority (SIA) extension provides a set of URIs, each of which references this repository publication point and a supported access mechanism. Additionally, a certificate's Authority Information Authority (AIA) extension contains a URI that references the authoritative location for the 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 directory containing certificate B (see Figure 1).

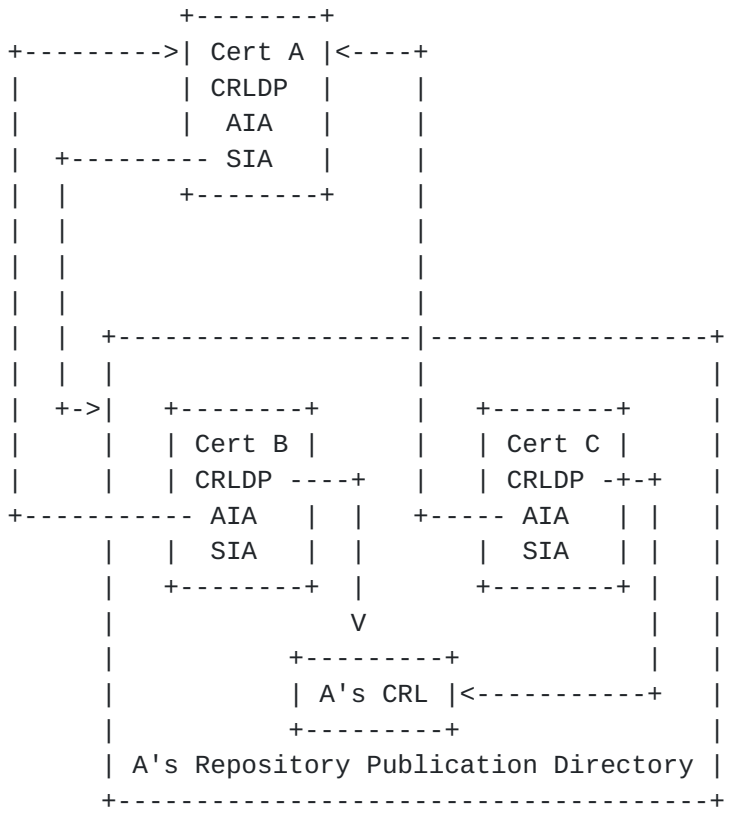

FIGURE 1: In this example, certificates B and C are issued under certificate A. Therefore, the AIA extensions of certificates B and C

point to A, and the SIA extension of certificate A points to the repository publication point containing certificates B and C, as well as A'a CRL.

The general intent is that an instance of a repository publication point contains all the signed products of a Certificate Authority, or all the objects signed by an End Entity (EE).

2.1. Manifests

All repository publication points MUST contain a manifest [I-D.ietf-sidr-rpki-manifests]. The manifest contains a list of the names of all objects contained in a repository publication point directory, as well as the hash value of each object's contents.

The collection of manifests across the entire RPKI is complete, in that all published objects are described in precisely one manifest.

2.2. CA Repository Publication Point

A CA Certificate has two accessMethods specified in its SIA field. The id-ad-caRepository accessMethod has an associated accessLocation that points to the the repository publication point of the products of this CA, as specified in [I-D.ietf-sidr-res-certs]. The id-ad-rpkiManifest accessMethod has an associated access location that points to the manifest object, as an object URL, that is associated with this repository publication point. This manifest describes all the objects that are to be found in that publication point and the hash value of each object (excluding the manifest itself) [I-D.ietf-sidr-rpki-manifests].

In the case of a CA's publication repository in the scope of the Resource Certificate PKI (RPKI) , the repository contains the current certificates issued by this CA, the most recent CRLs that are associated with the CA's non-revoked keypairs, the current manifest, and all objects that are signed using a "single-use" EE certificate, where the EE certificate was issued by this CA.

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 with a given key pair, implying that publication of successive instances of a CA's CRL may overwrite previous instances of CRLs signed by the same CA 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 that 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].

Manifest: When a new instance of a manifest is published by the CA, there is no requirement within the RPKI for any relying party to have continuing access to older instances of the CA's manifest. This implies that the name chosen for the manifest object in the publication repository may be a constant value, implying that publication of successive instances of the manifest overwrite the previous instance of the manifest within the context of each publication repository.

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 relying party has an interest only in the most recently published 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 series 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.

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 that are used to sign a single object, and "multi-use" EE Certificates that 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 EE certificate that was used to sign the object. The signed object name scheme for such objects can be derived from the associated EE certificate's public key, applying the algorithm described above. 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.

It is left as an implementation choice as to whether a CA is to use a single publication repository for all products of the CA across all non-retired keypairs, or to use one publication repository for each non-retired keypair.

It is not consistent with the specification that multiple CAs share a single repository publication point. Also it is not consistent with this specification that a CA repository pubcation point is shares with a "multi-use" EE repository publication point.

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 accessMethods specified in its SIA field. The id-ad-signedObjectRepository accessMethod has an associated accessLocation that points to the the repository publication point of the objects signed by this EE certificate, as specified in [I-D.ietf-sidr-res-certs]. The id-ad-rpkiManifest accessMethod has an associated access location 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 this EE certificate, and the hash value of each product (excluding the manifest itself) [I-D.ietf-sidr-rpki-manifests].

In the case of a EE's publication repository in the scope of the Resource Certificate PKI (RPKI) , the repository contains objects that have been signed by the EE's key pair, 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 certificates 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 certificate 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 inmplication is that all objects signed by a single EE certificate 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 per 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 should be available using RSYNC. Support of additional retrieval methods is the choice of the repository operator.

- Each CA publication directory in the publication repository should contain the products of a single issuer's CA instance. Aside from subdirectories, no other objects should be placed in a publication repository directory.

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

- Signed Objects are published in the location indicated by the SIA field of the EE certificate that has certified the key pair that 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 ofthe EE certificate. In the case of "single-use" EE certificates the signed object is published in the same repository publication point as the EE certificate itself, and the SIA extension references this object rather than the publication directory.

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 certification authority SHOULD use a persistent naming scheme for the certificates's repository publication point that is persistent across key rollover and other certificate reissuance 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 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 function is required, it is suggested that the relying party maintain a local repository containing a synchronized copy of all valid certificates, current certificate revocation lists, and all related signed objects that are stored in the local instances of components of the overall logical complete certificate repository.

The general approach to repository synchronization is one of a "top-down" walk of the distributed repository structure, commencing with the initial configured trust anchor certificates, and then populating the repository will all valid certificates that have been issued by these issuers, and then recursively applying the same approach to each of these subordinate certificates. Obviously a process would need to support some 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

[The text should reference the manifest draft to note that relying parties may use the manifest to ensure that they are receiving an authentic copy of the repository, and that the set of retrieved objects is complete. It is noted that with the exception of manifests themselves (which are mandatory to implement) all other objects of the RPKI are described in manifests.]

7. IANA Considerations

[There are no IANA considerations in this document.]

8. Normative References

[I-D.ietf-sidr-res-certs]
Huston, G., Loomans, R., and G. Michaelson, "A Profile for X.509 PKIX Resource Certificates",

draft-ietf-sidr-res-certs (work in progress),
November 2007.

[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 (work in progress),
January 2008.

[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.

[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.

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

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).