Secure Inter-Domain Routing
Working Group
Internet Draft
Intended status: Informational
Expires: November 23, 2011

M. Lepinski
S. Kent
BBN Technologies
May 23, 2011

An Infrastructure to Support Secure Internet Routing
draft-ietf-sidr-arch-13.txt

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on November 23, 2011.

Copyright Notice

Copyright (c) 2011 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.

Abstract

This document describes an architecture for an infrastructure to support improved security of Internet routing. The foundation of this architecture is a resource public key infrastructure (RPKI) that represents the allocation hierarchy of IP address space and Autonomous System (AS) Numbers; and a distributed repository system for storing and disseminating the data objects that comprise the RPKI, as well as other signed objects necessary for improved routing security. As an initial application of this architecture, the document describes how a legitimate holder of IP address space can explicitly and verifiably authorize one or more ASes to originate routes to that address space. Such verifiable authorizations could be used, for example, to more securely construct BGP route filters.

Table of Contents

1. Introduction

This document describes an architecture for an infrastructure to support improved security for BGP routing [RFC 4271] for the Internet. The architecture encompasses three principle elements:

. a resource public key infrastructure (RPKI)

. digitally-signed routing objects to support routing security

. a distributed repository system to hold the PKI objects and the signed routing objects

The architecture described by this document enables an entity to verifiably assert that it is the legitimate holder of a set of IP addresses or a set of Autonomous System (AS) numbers. As an initial application of this architecture, the document describes how a legitimate holder of IP address space can explicitly and verifiably authorize one or more ASes to originate routes to that address space. Such verifiable authorizations could be used, for example, to more securely construct BGP route filters. In addition to this initial application, the infrastructure defined by this architecture also is intended to provide future support for security protocols such as S-BGP [S-BGP] or soBGP [soBGP]. This architecture is applicable to the routing of both IPv4 and IPv6 datagrams. IPv4 and IPv6 are currently the only address families supported by this architecture. Thus, for example, use of this architecture with MPLS labels is beyond the scope of this document.

In order to facilitate deployment, the architecture takes advantage of existing technologies and practices. The structure of the PKI element of the architecture corresponds to the existing resource allocation structure. Thus management of this PKI is a natural extension of the resource-management functions of the organizations that are already responsible for IP address and AS number resource allocation. Likewise, existing resource allocation and revocation practices have well-defined correspondents in this architecture. Note that while the initial focus of this architecture is routing security applications, the PKI described in this document could be used to support other applications that make use of attestations of IP address or AS number resource holdings.

To ease implementation, existing IETF standards are used wherever possible; for example, extensive use is made of the X.509 certificate profile defined by the Public Key Infrastructure using X.509 (PKIX) working group [RFC 5280] and the extensions for IP Addresses and AS numbers representation defined in RFC 3779 [RFC 3779]. Also Cryptographic Message Syntax (CMS) [RFC 5652] is used as the syntax for the newly-defined signed objects [SIGN-OBJ] required by this infrastructure.

As noted above, the architecture is comprised of three main components: an X.509 PKI in which certificates attest to holdings of IP address space and AS numbers; non-certificate signed objects (including route origination authorizations and manifests) used by the infrastructure; and a distributed repository system that makes all of these signed objects available for use by ISPs in making routing decisions. These three basic components enable several security functions; most notably the cryptographic validation that an autonomous system is authorized to originate routes to a given prefix [ROA-VALID].

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" [RFC 5280], and "X.509 Extensions for IP Addresses and AS Identifiers" [RFC 3779].

Throughout this document we use the terms "address space holder" or "holder of IP address space" interchangeably to refer to a legitimate holder of IP address space who has received this address space through the standard IP address allocation hierarchy. That is, the address space holder has either directly received the address space as an allocation from a Regional Internet Registry (RIR) or IANA; or else the address space holder has received the address space as a sub-allocation from a National Internet Registry (NIR) or Local Internet Registry (LIR). We use the term "resource holder" to refer to a legitimate holder of either IP address or AS number resources.

Throughout this document we use the terms "registry" and ISP to refer to an entity that has an IP address space and/or AS number allocation that it is permitted to sub-allocate.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC 2119].

2. Public Key Infrastructure for Internet Number Resources

Because the holder of a block of IP address space is entitled to define the topological destination of IP datagrams whose destinations fall within that block, decisions about inter-domain routing are inherently based on knowledge of the allocation of the IP address space. Thus, a basic function of this architecture is to provide cryptographically verifiable attestations as to these allocations. In current practice, the allocation of IP addresses is hierarchical. The root of the hierarchy is IANA. Below IANA are five Regional Internet Registries (RIRs), each of which manages address and AS number allocation within a defined geopolitical region. In some regions the third tier of the hierarchy includes National Internet Registries (NIRs) as well as Local Internet Registries (LIRs) and subscribers with so-called provider-independent ("portable") allocations. (The term LIR is used in some regions to refer to what other regions define as an ISP. Throughout the rest of this document we will use the term LIR/ISP to simplify references to these entities.) In other regions the third tier consists only of LIRs/ISPs and subscribers with provider-independent allocations.

In general, the holder of a block of IP address space may sub-allocate portions of that block, either to itself (e.g., to a particular unit of the same organization), or to another organization, subject to contractual constraints established by the registries. Because of this structure, IP address allocations can be described naturally by a hierarchic public-key infrastructure, in which each certificate attests to an allocation of IP addresses, and issuance of subordinate certificates corresponds to sub-allocation of IP addresses. The above reasoning holds true for AS number resources as well, with the difference that, by convention, AS numbers may not be sub-allocated except by RIRs or NIRs. Thus allocations of both IP addresses and AS numbers can be expressed by the same PKI. Such a PKI, which is henceforth referred to as the Resource Public Key Infrastructure (RPKI), is a central component of this architecture.

2.1. Role in the overall architecture

Certificates in this PKI are called Resource Certificates, and conform to the certificate profile for such certificates [RES-CERT]. Resource certificates attest to the allocation by the (certificate) issuer of IP addresses or AS numbers to the subject. They do this by binding the public key contained in the Resource Certificate to the IP addresses or AS numbers included in the certificate's IP Address Delegation or AS Identifier Delegation Extensions, respectively, as defined in RFC 3779 [RFC 3779].

An important property of this PKI is that certificates do not attest to the identity of the subject. Therefore, the subject names used in certificates are not intended to be "descriptive." That is, the resource PKI is intended to provide authorization, but not authentication. This is in contrast to most PKIs where the issuer ensures that the descriptive subject name in a certificate is properly associated with the entity that holds the private key corresponding to the public key in the certificate. Because issuers need not verify the right of an entity to use a subject name in a certificate, they avoid the costs and liabilities of such verification. This makes it easier for these entities to take on the additional role of Certificate Authority (CA).

Most of the certificates in the PKI assert the basic facts on which the rest of the infrastructure operates. CA certificates within the PKI attest to IP address space and AS number holdings. End-entity (EE) certificates are issued by resource holder CAs to delegate the authority attested by their allocation certificates. The primary use for EE certificates is the validation of Route Origination Authorizations (ROAs), signed objects which provide an explicit authorization by an address holder that a given AS is permitted to originate routes to a set of addresses (see Section 3). End Entity certificates are also used to verify other signed objects, such as manifests which will be used to help ensure the integrity of the repository system (see Section 5).

2.2. CA Certificates

Any resource holder who is authorized to sub-allocate these resources must be able to issue Resource Certificates to correspond to these sub-allocations. Thus, for example, CA certificates will be associated with IANA and each of the RIRs, NIRs, and LIRs/ISPs. A CA certificate also is required to enable a resource holder to issue ROAs, because it must issue the corresponding end-entity certificate used to validate each ROA. Thus some entities that do not sub-allocate their resources also will need to have CA certificates for their allocations, e.g., a multi-homed subscriber with a provider-independent allocation, to enable them to issue ROAs. (A subscriber who is not multi-homed, whose allocation comes from an LIR/ISP, and who has not moved to a different LIR/ISP, need not be represented in the PKI. Moreover, a multi-homed subscriber with an allocation from an LIR/ISP may or may not need to be explicitly represented, as discussed in Section 7.2.2)

Unlike in most PKIs, the distinguished name of the subject in a CA certificate is chosen by the certificate issuer. The subject's distinguished name must not attempt to convey the identity of the

subject in a descriptive fashion. The subject's distinguished name must include the common name attribute and may additionally include the serial attribute.

In this PKI, the certificate issuer, being an RIR, NIR, or LIR/ISP, is not in the business of verifying the legal right of the subject to assert a particular identity. Therefore, selecting a distinguished name that does not convey the identity of the subject in a descriptive fashion minimizes the opportunity for the subject to misuse the certificate to assert an identity, and thus minimizes the legal liability of the issuer. Since all CA certificates are issued to subjects with whom the issuer has an existing relationship, it is recommended that the issuer select a subject name that enables the issuer to easily link the certificate to existing database records associated with the subject. For example, an authority may use internal database keys or subscriber IDs as the subject common name in issued certificates.

Although the subject's common name in a certificate does not convey identity, it is still the case that the common name must be unique among all subjects to whom a certification authority issues certificates. That is, a CA must not issue certificates to two different entities which use the same common name for the subject.

Each Resource Certificate attests to an allocation of resources to a resource holder, so entities that have allocations from multiple sources will have multiple CA certificates. Note that when an entity receives multiple certificates from different issuers that the subject names in these certificates will generally be different. A CA also may issue distinct certificates for each distinct allocation to the same entity, if the CA and the resource holder agree that such an arrangement will facilitate management and use of the certificates. For example, an LIR/ISP may have several certificates issued to it by one registry, each describing a distinct set of address blocks, because the LIR/ISP desires to treat the allocations as separate.

2.3. End-Entity (EE) Certificates

The private key corresponding to a public key contained in an EE certificate is not used to sign other certificates in a PKI. The primary function of end-entity certificates in this PKI is the verification of signed objects that relate to the usage of the resources described in the certificate, e.g., ROAs and manifests.

For ROAs and manifests there will be a one-to-one correspondence between end-entity certificates and signed objects, i.e., the private key corresponding to each end-entity certificate is used to sign

exactly one object, and each object is signed with only one key. This property allows the PKI to be used to revoke these signed objects, rather than creating a new revocation mechanism. When the end-entity certificate used to sign an object has been revoked, the signature on that object (and any corresponding assertions) will be considered invalid, so a signed object can be effectively revoked by revoking the end-entity certificate used to sign it.

A secondary advantage to this one-to-one correspondence is that the private key corresponding to the public key in a certificate is used exactly once in its lifetime, and thus can be destroyed after it has been used to sign its one object. This fact should simplify key management, since there is no requirement to protect these private keys for an extended period of time.

The EE certificate used to verify a signed object appears in the Cryptographic Message Syntax (CMS) wrapper (see [SIGN-OBJ]) of the signed object. Therefore, it is not necessary to transmit the EE certificate separately from the signed object. Likewise, it is not necessary for the EE certificate to appear in the RPKI repository system except as part of the corresponding signed object.

Although this document describes only two uses for end-entity certificates, additional uses will likely be defined in the future. For example, end-entity certificates could be used as a more general authorization for their subjects to act on behalf of the specified resource holder. This could facilitate authentication of inter-ISP interactions, or authentication of interactions with the repository system. These additional uses for end-entity certificates may require retention of the corresponding private keys, even though this is not required for the private keys associated with end-entity certificates keys used for verification of ROAs and manifests, as described above.

2.4. Trust Anchors

In any PKI, each relying party (RP) chooses its own set of trust anchors. This general property of PKIs applies here as well. There is an extant IP address space and AS number allocation hierarchy, and thus IANA and/or the five RIRs are obvious candidates to be default TAs here. Nonetheless, each RP ultimately chooses the set of trust anchors it will use for certificate validation.

For example, a RP (e.g., an LIR/ISP) could create a trust anchor to which all address space and/or all AS numbers are assigned, and for which the RP knows the corresponding private key. The RP could then issue certificates under this trust anchor to whatever entities in

the PKI it wishes, with the result that the certification paths terminating at this locally-installed trust anchor will satisfy the RFC 3779 validation requirements. A large ISP that uses private (i.e., RFC 1918) IP address space and runs BGP internally will need to create this sort of trust anchor to accommodate a CA to which all private (RFC 1918) address space is assigned. The RP could then issue certificates under this CA that correspond to the RP's internal use of private address space.

Note that a RP who elects to create and manage its own set of trust anchors may fail to detect allocation errors that arise under such circumstances, but the resulting vulnerability is local to the RP.

It is expected that some parties within the extant IP address space and AS number allocation hierarchy may wish to publish trust anchor material for possible use by relying parties. A standard profile for the publication of trust anchor material for this public key infrastructure can be found in [SIDR-TA].

3. Route Origination Authorizations

The information on IP address allocation provided by the PKI is not, in itself, sufficient to guide routing decisions. In particular, BGP is based on the assumption that the AS that originates routes for a particular prefix is authorized to do so by the holder of that prefix (or an address block encompassing the prefix); the PKI contains no information about these authorizations. A Route Origination Authorization (ROA) makes such authorization explicit, allowing a holder of IP address space to create an object that explicitly and verifiably asserts that an AS is authorized originate routes to a given set of prefixes.

3.1. Role in the overall architecture

A ROA is an attestation that the holder of a set of prefixes has authorized an autonomous system to originate routes for those prefixes. A ROA is structured according to the format described in [ROA-FORM]. The validity of this authorization depends on the signer of the ROA being the holder of the prefix(es) in the ROA; this fact is asserted by an end-entity certificate from the PKI, whose corresponding private key is used to sign the ROA.

ROAs may be used by relying parties to verify that the AS that originates a route for a given IP address prefix is authorized by the holder of that prefix to originate such a route. For example, an ISP might use validated ROAs as inputs to route filter construction for

use by its BGP routers. (See [ROA-VALID] for information on the use of ROAs to validate the origination of BGP routes.)

Initially, the repository system will be the primary mechanism for disseminating ROAs, since these repositories will hold the certificates and CRLs needed to verify ROAs. In addition, ROAs also could be distributed in BGP UPDATE messages or via other communication paths, if needed to meet timeliness requirements.

3.2. Syntax and semantics

A ROA constitutes an explicit authorization for a single AS to originate routes to one or more prefixes, and is signed by the holder of those prefixes. Conceptually, the ROA syntax consists of two parts, a general CMS template common to all RPKI signed objects [SIGN-OBJ] and an encapsulated content specific to the ROA which expresses the authorization [ROA-FORM].

At a high level, the ROA's content contains (1) an AS number; (2) a list of IP address prefixes; and, optionally, (3) for each prefix, the maximum length of more specific (longer) prefixes that the AS is also authorized to advertise. (This last element facilitates a compact authorization to advertise, for example, any prefixes of length 20 to 24 contained within a given length 20 prefix.)

Note that a ROA contains only a single AS number. Thus, if an ISP has multiple AS numbers that will be authorized to originate routes to the prefix(es) in the ROA, an address space holder will need to issue multiple ROAs to authorize the ISP to originate routes from any of these ASes.

A ROA is signed using the private key corresponding to the public key in an end-entity certificate in the PKI. In order for a ROA to be valid, its corresponding end-entity (EE) certificate must be valid and the IP address prefixes of the ROA must exactly match the IP address prefix(es) specified in the EE certificate's RFC 3779 extension. Therefore, the validity interval of the ROA is implicitly the validity interval of its corresponding certificate. A ROA is revoked by revoking the corresponding EE certificate. There is no independent method of revoking a ROA. One might worry that this revocation model could lead to long CRLs for the CA certification that is signing the EE certificates. However, routing announcements on the public internet are generally quite long lived. Therefore, as long as the EE certificates used to verify a ROA are given a validity interval of several months, the likelihood that many ROAs would need to revoked within that time is quite low.

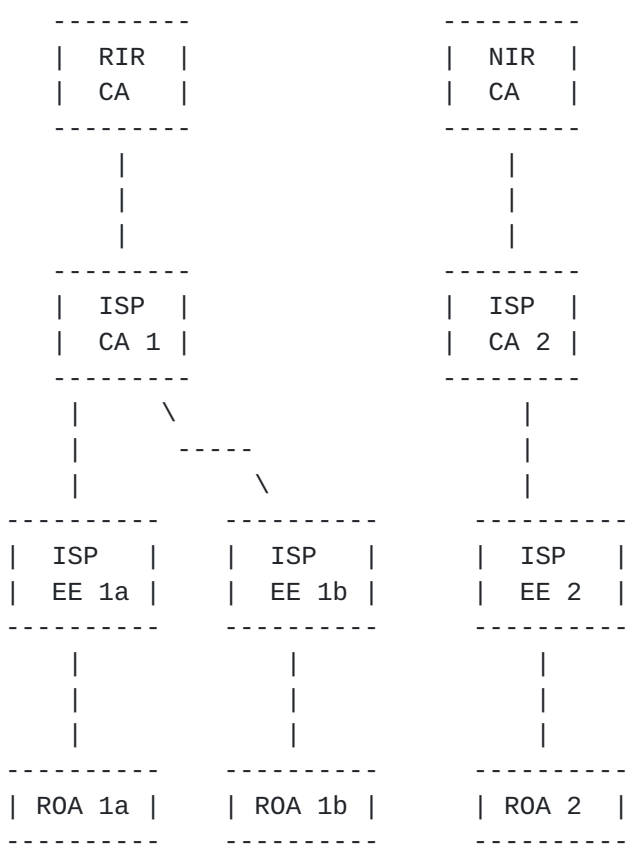

FIGURE 1: This figure illustrates an ISP with allocations from two sources (an RIR and an NIR). It needs two CA certificates due to RFC 3779 rules.

Because each ROA is associated with a single end-entity certificate, the set of IP prefixes contained in a ROA must be drawn from an allocation by a single source, i.e., a ROA cannot combine allocations from multiple sources. Address space holders who have allocations from multiple sources, and who wish to authorize an AS to originate routes for these allocations, must issue multiple ROAs to the AS.

4. Repositories

Initially, an LIR/ISP will make use of the resource PKI by acquiring and validating every ROA, to create a table of the prefixes for which each AS is authorized to originate routes. To validate all ROAs, an LIR/ISP needs to acquire all the certificates and CRLs. The primary function of the distributed repository system described here is to store these signed objects and to make them available for download by LIRs/ISPs. Note that this repository system provides a mechanism by which relying parties can pull fresh data at whatever frequency they deem appropriate. However, it does not provide a mechanism for

pushing fresh data to relying parties (e.g. by including resource PKI objects in BGP or other protocol messages) and such a mechanism is beyond the scope of the current document.

The digital signatures on all objects in the repository ensure that unauthorized modification of valid objects is detectable by relying parties. Additionally, the repository system uses manifests (see Section 5) to ensure that relying parties can detect the deletion of valid objects and the insertion of out of date, valid signed objects.

The repository system is also a point of enforcement for access controls for the signed objects stored in it, e.g., ensuring that records related to an allocation of resources can be manipulated only by authorized parties. The use of access controls prevents denial of service attacks based on deletion of or tampering to repository objects. Indeed, although relying parties can detect tampering with objects in the repository, it is preferable that the repository system prevent such unauthorized modifications to the greatest extent possible.

4.1. Role in the overall architecture

The repository system is the untrusted clearing-house for all signed objects that must be globally accessible to relying parties. When certificates and CRLs are created, they are uploaded to this repository, and then downloaded for use by relying parties (primarily LIRs/ISPs). ROAs and manifests are additional examples of such objects, but other types of signed objects may be added to this architecture in the future. This document briefly describes the way signed objects (certificates, CRLs, ROAs and manifests) are managed in the repository system. As other types of signed objects are added to the repository system it will be necessary to modify the description, but it is anticipated that most of the design principles will still apply. The repository system is described in detail in [REPOS].

4.2. Contents and structure

Although there is a single repository system that is accessed by relying parties, it is comprised of multiple databases. These databases will be distributed among registries (RIRs, NIRs, LIRs/ISPs). At a minimum, the database operated by each registry will contain all CA and EE certificates, CRLs, and manifests signed by the CA(s) associated with that registry. Repositories operated by LIRs/ISPs also will contain ROAs. Registries are encouraged to maintain copies of repository data from their customers, and their customer's customers (etc.), to facilitate retrieval of the whole

repository contents by relying parties. Ideally, each RIR will hold PKI data from all entities within its geopolitical scope.

For every certificate in the PKI, there will be a corresponding file system directory in the repository that is the authoritative publication point for all objects (certificates, CRLs, ROAs and manifests) verifiable via this certificate. A certificate's Subject Information Authority (SIA) extension [RFC 5280] contains a URI that references this directory. Additionally, a certificate's Authority Information Authority (AIA) extension [RFC 5280] contains a URI that references the authoritative location for the CA certificate under which the given certificate was issued. That is, if certificate A is used to verify 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 2).

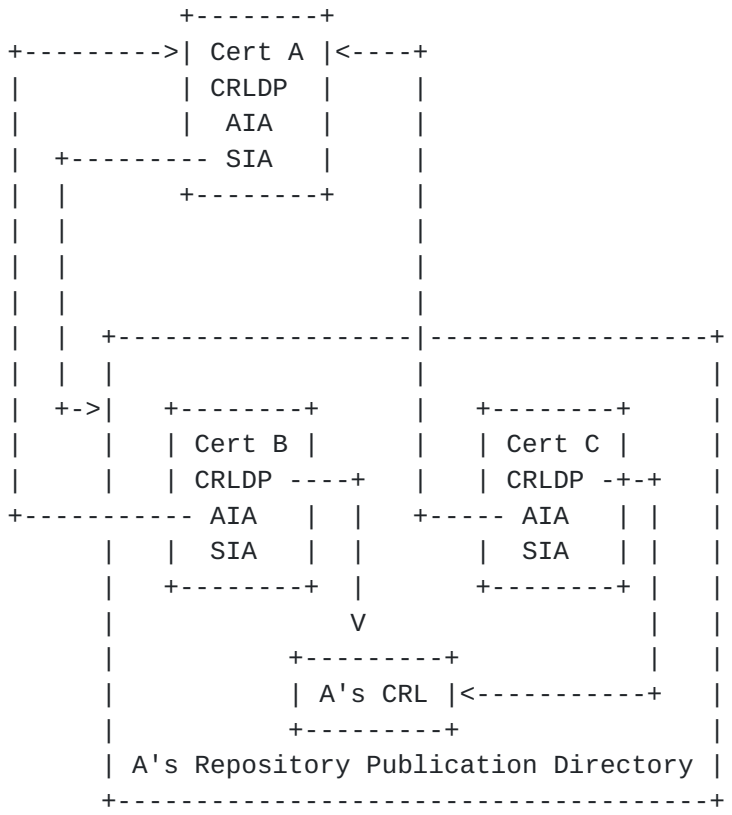

FIGURE 2: Use of SIA and AIA extensions in the RPKI

In Figure 2, certificates B and C are issued by (CA) A. Therefore, the AIA extensions of certificates B and C point to (certificate) A, and the SIA extension of certificate A points to the repository publication point of CA A's subordinate products, which includes

certificates B and C, as well as the CRL issued by A. The CRL Distribution Points (CRLDP) extension in certificates B and C both point to the Certificate Revocation List (CRL) issued by A.

If a CA certificate is reissued with the same public key, it should not be necessary to reissue (with an updated AIA URI) all certificates signed by the certificate being reissued. Therefore, a certification authority SHOULD use a persistent URI naming scheme for issued certificates. That is, reissued certificates should use the same publication point as previously issued certificates having the same subject and public key, and should overwrite such certificates.

4.3. Access protocols

Repository operators will choose one or more access protocols that relying parties can use to access the repository system. These protocols will be used by numerous participants in the infrastructure (e.g., all registries, ISPs, and multi-homed subscribers) to maintain their respective portions of it. In order to support these activities, certain basic functionality is required of the suite of access protocols, as described below. No single access protocol need implement all of these functions (although this may be the case), but each function MUST be implemented by at least one access protocol deployed by a repository operator.

Download: Access protocols must support the bulk download of repository contents and subsequent download of changes to the downloaded contents, since this will be the most common way in which relying parties interact with the repository system. Other types of download interactions (e.g., download of a single object) may also be supported.

Upload/change/delete: Access protocols must also support mechanisms for the issuers of certificates, CRLs, and other signed objects to add them to the repository, and to remove them. Mechanisms for modifying objects in the repository may also be provided. All access protocols that allow modification to the repository (through addition, deletion, or modification of its contents) must support verification of the authorization of the entity performing the modification, so that appropriate access controls can be applied (see Section 4.4).

To ensure all relying parties are able to acquire all RPKI signed objects, all publication points MUST be accessible via RSYNC (see [RFC 5781] and [RSYNC]), although other download protocols MAY also be supported. A repository publication point may provide update/change/delete functionality via (set of) access protocols that

it desires, provided that the supported protocols are clearly communicated to all certification authorities publishing data at a given publication point.

4.4. Access control

In order to maintain the integrity of information in the repository, controls must be put in place to prevent addition, deletion, or modification of objects in the repository by unauthorized parties. The identities of parties attempting to make such changes can be authenticated through the relevant access protocols. Although specific access control policies are subject to the local control of repository operators, it is RECOMMENDED that repositories allow only the issuers of signed objects to add, delete, or modify them. Alternatively, it may be advantageous in the future to define a formal delegation mechanism to allow resource holders to authorize other parties to act on their behalf, as suggested in Section 2.3 above.

5. Manifests

A manifest is a signed object listing of all of the signed objects (except for the manifest itself) issued by an authority responsible for a publication in the repository system. For each unexpired certificate, CRL, or ROA issued by the authority, the manifest contains both the name of the file containing the object, and a hash of the file content.

As with ROAs, a manifest is signed by a private key, for which the corresponding public key appears in an end-entity certificate. This EE certificate, in turn, is signed by the CA in question. Since the private key in an EE certificate is used to sign only a single manifest, then the manifest can be revoked by revoking the EE certificate. In such a case, to avoid needless CRL growth, the EE certificate used to validate a manifest SHOULD expire at the same time that the manifest expires.

Manifests may be used by relying parties when constructing a local cache (see Section 6) to mitigate the risk of an attacker who deletes files from a repository or replaces current signed objects with stale versions of the same object. Such protection is needed because although all objects in the repository system are signed, the repository system itself is untrusted.

5.1. Syntax and semantics

A manifest constitutes a list of (the hashes of) all the files in a repository point at a particular point in time. A detailed specification of the manifest's content is provided in [MANIFEST] but, at a high level, a manifest consists of (1) a manifest number; (2) the time the manifest was issued; (3) the time of the next planned update; and (4) a list of filename and hash value pairs.

The manifest number is a sequence number that is incremented each time a manifest is issued by the authority. An authority is REQUIRED to issue a new manifest any time it alters any of its items in the repository, or when the specified time of the next update is reached. A manifest is thus valid until the specified time of the next update or until a manifest is issued with a greater manifest number, whichever comes first. (Note that when an EE certificate is used to sign only a single manifest, whenever the authority issues the new manifest, the CA MUST also issue a new CRL which includes the EE certificate corresponding to the old manifest. The revoked EE certificate for the old manifest will be removed from the CRL when it expires, thus this procedure ought not to result in significant CRLs growth.)

6. Local Cache Maintenance

In order to utilize signed objects issued under this PKI, a relying party must first obtain a local copy of the valid EE certificates for the PKI. To do so, the relying party performs the following steps:

1. Query the repository system to obtain a copy of all certificates, manifests and CRLs issued under the PKI.

2. For each CA certificate in the PKI, verify the signature on the corresponding manifest. Additionally, verify that the current time is earlier than the time indicated in the nextUpdate field of the manifest.

3. For each manifest, verify that certificates and CRLs issued under the corresponding CA certificate match the hash values contained in the manifest. Additionally, verify that no certificate or manifest listed on the manifest is missing from the repository. If the hash values do not match, or if any certificate or CRL is missing, notify the appropriate repository administrator that the repository data has been corrupted.

4. Validate each EE certificate by constructing and verifying a certification path for the certificate (including checking relevant CRLs) to the locally configured set of TAs. (See [RES-CERT] for more details.)

Note that since relying parties will perform these operations regularly, it is more efficient for the relying party to request from the repository system only those objects that have changed since the relying party last updated its local cache.

Note also that by checking all issued objects against the appropriate manifest, the relying party can be certain that it is not missing an updated version of any object.

7. Common Operations

Creating and maintaining the infrastructure described above will entail additional operations as "side effects" of normal resource allocation and routing authorization procedures. For example, a subscriber with provider-independent ("portable") address space who enters a relationship with an ISP will need to issue one or more ROAs identifying that ISP, in addition to conducting any other necessary technical or business procedures. The current primary use of this infrastructure is for route filter construction; using ROAs, route filters can be constructed in an automated fashion with high assurance that the holder of the advertised prefix has authorized the origin AS to originate an advertised route.

7.1. Certificate issuance

There are several operational scenarios that require certificates to be issued. Any allocation that may be sub-allocated requires a CA certificate, e.g., so that certificates can be issued as necessary for the sub-allocations. Holders of provider-independent IP address space allocations also must have certificates, so that a ROA can be issued to each ISP that is authorized to originate a route to the allocation (since the allocation does not come from any ISP). Additionally, multi-homed subscribers may require certificates for their allocations if they intend to issue the ROAs for their allocations (see Section 7.2.2). Other resource holders need not be issued CA certificates within the PKI.

In the long run, a resource holder will not request resource certificates, but rather receive a certificate as a side effect of the allocation process for the resource. However, initial deployment of the RPKI will entail issuance of certificates to existing resource holders as an explicit event. Note that in all cases, the authority

issuing a CA certificate will be the entity who allocates resources to the subject. This differs from most PKIs in which a subject can request a certificate from any certification authority.

If a resource holder receives multiple allocations over time, it may accrue a collection of resource certificates to attest to them. If a resource holder receives multiple allocations from the same source, the set of resource certificates may be combined into a single resource certificate, if both the issuer and the resource holder agree. This is accomplished by consolidating the IP Address Delegation and AS Identifier Delegation Extensions into a single extension (of each type) in a new certificate. However, if these certificates attest to allocations which are valid for different periods of time, creating a certificate that combines them might create problems as the combined certificate can only express a single validity interval.

If a resource holder's allocations come from different sources, they will be signed by different CAs, and cannot be combined. When a set of resources is no longer allocated to a resource holder, any certificates attesting to such an allocation MUST be revoked. A resource holder SHOULD NOT use the same public key in multiple CA certificates that are issued by the same or differing authorities, as reuse of a key pair complicates path construction. Note that since the subject's distinguished name is chosen by the issuer, a subject who receives allocations from two sources generally will receive certificates with different subject names.

7.2. CA Key Rollover

Whenever a certification authority wishes to change the public key (and corresponding private key) associated with its RPKI CA certificate, it MUST perform a key rollover procedure. Key rollover is typically performed on a periodic basis, where the frequency of key rollovers is specified in the certification practice statement of the given CA. Additionally, unscheduled rollovers may be required in the event of suspected key compromises.

Note that rollover is only required when the CA's key actually changes, it is not required in cases where a new CA certificate is issued with the same key as the previous certificate for this CA. For example, a new CA certificate must be issued if the CA gains or relinquishes resource, or if the validity period of the resource allocation is extended. However, in such a cases the new certificate will generally use the same public (and private) key as the previous certificate and thus key rollover is not required.

The document [KEY-ROLL] specifies a conservative key rollover procedure that should be used by a certification authority when it changes the public (and private) keys associated with its RPKI CA certificate. At a high level, the two key properties of the rollover procedure are as follows. First, as data from RPKI signed objects may be used in routing operations, the procedure ensures that at any point in the rollover procedure a relying party will never reach incorrect conclusions about the validity of a signed object. Note in particular, that the CA cannot assume that a relying party will use any particular algorithm for constructing a certificate path from an EE certificate to (one of) the relying party's trust anchor(s), therefore, the key rollover procedure is designed to preserve the integrity of the SIA and AIA points within the RPKI hierarchy to the greatest extent possible. Second, the key rollover procedure is design so that the reissuance of all certificates below the CA in the RPKI hierarchy is not required. Of course, it is necessary to re-sign all certificates issued directly under the CA whose key is changing. However, the SIA and AIA pointers within the certificates are populated so that no further re-issuance is required.

7.3. ROA management

Whenever a holder of IP address space wants to authorize an AS to originate routes for a prefix within his holdings, he MUST issue an end-entity certificate containing that prefix in an IP Address Delegation extension. He then uses the corresponding private key to sign a ROA containing the designated prefix and the AS number for the AS. The resource holder MAY include more than one prefix in the EE certificate and corresponding ROA if desired. As a prerequisite, then, any address space holder that issues ROAs for a prefix must have a resource certificate for an allocation containing that prefix. The standard procedure for issuing a ROA is as follows:

1. Create an end-entity certificate containing the prefix(es) to be authorized in the ROA.

2. Construct the payload of the ROA, including the prefixes in the end-entity certificate and the AS number to be authorized.

3. Sign the ROA using the private key corresponding to the end-entity certificate (the ROA is comprised of the payload encapsulated in a CMS signed message [RFC 5652]).

4. Upload the end-entity certificate and the ROA to the repository system.

The standard procedure for revoking a ROA is to revoke the corresponding end-entity certificate by creating an appropriate CRL and uploading it to the repository system. The revoked ROA and end-entity certificate SHOULD be removed from the repository system.

Care must be taken when revoking ROAs in that revoking a ROA may cause a relying party to treat routing advertisements corresponding to the prefixes and origin AS number in the ROA as unauthorized (and potentially even change routing behavior to no longer forward packets based on those advertisements). In particular, resource holders should adhere to the principle of "make before break" as follows. Before revoking a ROA corresponding to a prefix which the resource holder wishes to be routable on the Internet, it is very important for the resource holder to ensure that there exists another valid alternative ROA that lists the same prefix (possibly indicating a different AS number). Additionally, the resource holder should ensure that the AS indicated in the valid alternative ROA is actually originating routing advertisements to the prefixes in question. Furthermore, a relying party must fetch new ROAs from the repository system before taking any routing action in response to a ROA revocation.

7.3.1. Single-homed subscribers

In BGP, a single-homed subscriber with Provider Aggregatable (PA) address space does not need to explicitly authorize routes to be originated for the prefix(es) it is using, since its ISP will already advertise a more general prefix and route traffic for the subscriber's prefix as an internal function. Since no routes are originated specifically for prefixes held by these subscribers, no ROAs need to be issued under their allocations; rather, the subscriber's ISP will issue any necessary ROAs for its more general prefixes under resource certificates from its own allocation. Thus, a single-homed subscriber with an IP address allocation from his service provider is not included in the RPKI, i.e., it does not receive a CA certificate, nor issue EE certificates or ROAs.

7.3.2. Multi-homed subscribers

Here we consider a subscriber who receives Provider Aggregatable (PA) IP address space from a primary ISP (i.e., the IP addresses used by the subscriber are a subset of ISP A's IP address space allocation) and receives redundant upstream connectivity from one or more secondary ISPs, in addition to the primary ISP. The preferred option for such a multi-homed subscriber is for the subscriber to obtain an AS number (from an RIR or NIR) and run BGP with each of its upstream providers. In such a case, there are two ways for ROA management to

be handled. The first is that the primary ISP issues a CA certificate to the subscriber, and the subscriber issues a ROA to containing the subscriber's AS number and the subscriber's IP address prefixes. The second possibility is that the primary ISP does not issue a CA certificate to the subscriber, and instead issues a ROA on the subscriber's behalf that contains the subscriber's AS number and the subscriber's IP address prefixes.

If the subscriber is unable or unwilling to obtain an AS number and run BGP, the other option is that the multi-homed subscriber can request that the primary ISP create a ROA for each secondary ISP that authorizes the secondary ISP to originate routes to the subscriber's prefixes. The primary ISP will also create a ROA containing its own AS number and the subscriber's prefixes, as it is likely in such a case that the primary ISP wishes to advertise precisely the subscriber's prefixes and not an encompassing aggregate. Note that this approach results in inconsistent origin AS numbers for the subscriber's prefixes which are considered undesirable on the public Internet; thus this approach is NOT RECOMMENDED.

7.3.3. Provider-Independent Address Space

A resource holder is said to have provider-independent (portable) address space if the resource holder received its allocation directly from a RIR or NIR. Because the prefixes represented in such allocations are not taken from an allocation held by an ISP, there is no ISP that holds and advertises a more general prefix. A holder of a portable IP address space allocation MUST authorize one or more ASes to originate routes to these prefixes. Thus the resource holder MUST generate one or more EE certificates and associated ROAs to enable the AS(es) to originate routes for the prefix(es) in question. This ROA is required because none of the ISP's existing ROAs authorize it to originate routes to the subscriber's provider-idependent allocation.

8. Security Considerations

The focus of this document is security; hence security considerations permeate this specification.

The security mechanisms provided by and enabled by this architecture depend on the integrity and availability of the infrastructure it describes. The integrity of objects within the infrastructure is ensured by appropriate controls on the repository system, as described in Section 4.4. Likewise, because the repository system is structured as a distributed database, it should be inherently resistant to denial of service attacks; nonetheless, appropriate

precautions should also be taken, both through replication and backup of the constituent databases and through the physical security of database servers.

9. IANA Considerations

Instructions for IANA's participation in the RPKI are provided in [IANA-OBJ].

10. Acknowledgments

The architecture described in this draft is derived from the collective ideas and work of a large group of individuals. This work would not have been possible without the intellectual contributions of George Michaelson, Robert Loomans, Sanjaya and Geoff Huston of APNIC, Robert Kisteleki and Henk Uijterwaal of the RIPE NCC, Tim Christensen and Cathy Murphy of ARIN, Rob Austein of ISC and Randy Bush of IIJ.

Although we are indebted to everyone who has contributed to this architecture, we would like to especially thank Rob Austein for the concept of a manifest, Geoff Huston for the concept of managing object validity through single-use EE certificate key pairs, and Richard Barnes for help in preparing an early version of this document.

11. References

11.1. Normative References

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

[RFC 4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006

[RFC 5280] 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.

[RFC 5652] Housley, R., "Cryptographic Message Syntax", RFC 5652, September 2009.

[RFC 3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

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

[RES-CERT] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs, May 2011.

[ROA-FORM] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROA)", draft-ietf-sidr-roa-format, February 2011.

[SIGN-OBJ] Chi, A., Kent, S., and M. Lepinski, "Signed Object Template for the Resource Public Key Infrastructure", draft-ietf-sidr-signed-object, May 2011.

[MANIFEST] Austein, R., et al., "Manifests for the Resource Public Key Infrastructure", draft-ietf-sidr-rpki-manifests, May 2011.

[REPOS] Huston, G., Michaelson, G., and R. Loomans, "A Profile for Resource Certificate Repository Structure", draft-ietf-sidr-repos-struct, February 2011.

[IANA-OBJ] Manderson, T., Vegoda, L. and S. Kent, "RPKI Objects issued by IANA", draft-ietf-sidr-iana-objects, May 2011.

11.2. Informative References

[KEY-ROLL] Huston, G., Michaelson, G., and S. Kent, "CA Key Rollover in the RPKI", draft-huston-sidr-keyroll, February 2011.

[ROA-VALID] Huston, G., et al., "Validation of Route Origination in BGP using the Resource Certificate PKI", draft-ietf-sidr-roa-validation, April 2011.

[SIDR-TA] Michaelson, G., Kent, S., and Huston, G., "A Profile for Trust Anchor Material for the Resource Certificate PKI", draft-ietf-sidr-ta, April 2011.

[S-BGP] Kent, S., Lynn, C., and Seo, K., "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications Vol. 18, No. 4, April 2000.

[soBGP] White, R., "soBGP", May 2005, <ftp://ftp-eng.cisco.com/sobgp/index.html>

[RSYNC] Tridgell, A., "rsync", March 2008, <http://rsync.samba.org/>

Authors' Addresses

Matt Lepinski
BBN Technologies
10 Moulton St.
Cambridge, MA 02138

Email: mlepinski@bbn.com

Stephen Kent
BBN Technologies
10 Moulton St.
Cambridge, MA 02138

Email: kent@bbn.com