Internet Engineering Task Force (IETF)
Request for Comments: 6493
Category: Standards Track
ISSN: 2070-1721

R. Bush
Internet Initiative Japan

February 2012

The Resource Public Key Infrastructure (RPKI) Ghostbusters Record

Abstract

In the Resource Public Key Infrastructure (RPKI), resource certificates completely obscure names or any other information that might be useful for contacting responsible parties to deal with issues of certificate expiration, maintenance, roll-overs, compromises, etc. This document describes the RPKI Ghostbusters Record containing human contact information that may be verified (indirectly) by a Certification Authority (CA) certificate. The data in the record are those of a severely profiled vCard.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6493.

Table of Contents

1. Introduction

In the operational use of the RPKI, it can become necessary to contact, human to human, the party responsible for a resource-holding CA certificate, AKA the certificate's maintainer, be it the holder of the certificate's private key or an administrative person in the organization, a NOC, etc. An important example is when the operator of a prefix described by a Route Origin Authorization (ROA) sees a problem, or an impending problem, with a certificate or Certificate Revocation List (CRL) in the path between the ROA and a trust anchor. For example, a certificate along that path has expired, is soon to expire, or a CRL associated with a CA along the path is stale, thus placing the quality of the routing of the address space described by the ROA in jeopardy.

As the names in RPKI certificates are not meaningful to humans, see [RFC6484], there is no way to use a certificate itself to lead to the worrisome certificate's or CRL's maintainer. So, "Who you gonna call?"

This document specifies the RPKI Ghostbusters Record, an object verified via an end-entity (EE) certificate, issued under a CA certificate, the maintainer of which may be contacted using the payload information in the Ghostbusters Record.

The Ghostbusters Record conforms to the syntax defined in [RFC6488]. The payload of this signed object is a severely profiled vCard.

Note that the Ghostbusters Record is not an identity certificate, but rather an attestation to the contact data made by the maintainer of the CA certificate issuing the EE certificate whose corresponding private key signs the Ghostbusters Record.

This record is not meant to supplant or be used as resource registry whois data. It gives information about an RPKI CA certificate maintainer, not a resource holder.

The Ghostbusters Record is optional; CA certificates in the RPKI can have zero or more associated Ghostbuster Records.

Given a certificate, to find the closest Ghostbuster Record, go up until a CA certificate is reached, which may be the object itself of course. That CA certificate will have Subject Information Access (SIA) to the publication point where all subsidiary objects (until you hit a down-chain CA certificate's signed objects) are published. The publication point will contain zero or more Ghostbuster Records.

This specification has three main sections. The first, Section 5, is the format of the contact payload information, a severely profiled vCard. The second, Section 6, profiles the packaging of the payload as a profile of the RPKI Signed Object Template specification [RFC6488]. The third, Section 7, describes the proper validation of the signed Ghostbusters Record.

2. Requirements Language

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 [RFC2119].

3. Suggested Reading

It is assumed that the reader understands the RPKI [RFC6480], the RPKI Repository Structure [RFC6481], Signed RPKI Objects [RFC6488], and vCards [RFC6350].

4. RPKI Ghostbusters Record Payload Example

An example of an RPKI Ghostbusters Record payload with all properties populated is as follows:

```
BEGIN:VCARD
VERSION:4.0
FN:Human's Name
ORG:Organizational Entity
ADR;TYPE=WORK:;;42 Twisty Passage;Deep Cavern;WA;98666;U.S.A.
TEL;TYPE=VOICE,TEXT,WORK;VALUE=uri:tel:+1-666-555-1212
TEL;TYPE=FAX,WORK;VALUE=uri:tel:+1-666-555-1213
EMAIL:human@example.com
END:VCARD
```

5. vCard Profile

The goal in profiling the vCard is not to include as much information as possible, but rather to include as few properties as possible while providing the minimal necessary data to enable one to contact the maintainer of the RPKI data that threatens the ROA[s] of concern.

The Ghostbusters vCard payload is a minimalist subset of the vCard as described in [RFC6350].

BEGIN - pro forma packaging that MUST be the first line in the vCard and MUST have the value "BEGIN:VCARD" as described in [RFC6350].

VERSION - pro forma packaging that MUST be the second line in the vCard and MUST have the value "VERSION:4.0" as described in Section 3.7.9 of [RFC6350].

FN - the name, as described in Section 6.2.1 of [RFC6350], of a contactable person or role who is responsible for the CA certificate.

ORG - an organization as described in Section 6.6.4 of [RFC6350].

ADR - a postal address as described in Section 6.3 of [RFC6350].

TEL - a voice and/or fax phone as described in Section 6.4.1 of [RFC6350].

EMAIL - an Email address as described in Section 6.4.2 of [RFC6350]

END - pro forma packaging that MUST be the last line in the vCard and MUST have the value "END:VCARD" as described in [RFC6350].

Per [RFC6350], the BEGIN, VERSION, FN, and END properties MUST be included in a record. To be useful, at least one of ADR, TEL, and EMAIL MUST be included. Other properties MUST NOT be included.

6. CMS Packaging

The Ghostbusters Record is a CMS signed-data object conforming to the "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", [RFC6488].

The content-type of a Ghostbusters Record is defined as id-ct-rpkiGhostbusters, and has the numerical value of 1.2.840.113549.1.9.16.1.35. This OID MUST appear both within the eContentType in the encapContentInfo object as well as the content-type signed attribute in the signerInfo object. See [RFC6488].

eContent: The content of a Ghostbusters Record is described in Section 5.

Similarly to a ROA, a Ghostbusters Record is verified using an EE certificate issued by the resource-holding CA certificate whose maintainer is described in the vCard.

The EE certificate used to verify the Ghostbusters Record is the one that appears in the CMS data structure that contains the payload defined above.

This EE certificate MUST describe its Internet Number Resources using the "inherit" attribute, rather than explicit description of a resource set; see [RFC3779].

7. Validation

The validation procedure defined in Section 3 of [RFC6488] is applied to a Ghostbusters Record. After this procedure has been performed, the Version number type within the payload is checked, and the OCTET STRING containing the vCard data is extracted. These data are checked against the profile defined in Section 5 of this document. Only if all of these checks pass is the Ghostbusters payload deemed valid and made available to the application that requested the payload.

8. Security Considerations

Though there is no on-the-wire protocol in this specification, there are attacks that could abuse the data described. As the data, to be useful, need to be public, little can be done to avoid this exposure.

Phone Numbers: The vCards may contain real world telephone numbers, which could be abused for telemarketing, abusive calls, etc.

Email Addresses: The vCards may contain Email addresses, which could be abused for purposes of spam.

Relying parties are hereby warned that the data in a Ghostbusters Record are self-asserted. These data have not been verified by the CA that issued the CA certificate to the entity that issued the EE certificate used to validate the Ghostbusters Record.

9. IANA Considerations

9.1. OID

The IANA has registered the OID for the Ghostbusters Record in the registry created by [RFC6488] as follows:

Name	OID	Specification
Ghostbusters	1.2.840.113549.1.9.16.1.35	[RFC6493]

9.2. File Extension

Realizing the deep issues raised by [RFC5513], the IANA has added an item for the Ghostbusters Record file extension to the "RPKI Repository Name Scheme" created by [RFC6481] as follows:

Filename Extension	RPKI Object	Reference
.gbr	Ghostbusters Record	[RFC6493]

9.3. Media Type

The IANA has registered the media type application/rpki-ghostbusters as follows:

```
Type name: application
Subtype name: rpki-ghostbusters
Required parameters: None
Optional parameters: None
Encoding considerations: binary
Security considerations: Carries an RPKI Ghostbusters Record
                         [RFC6493].
Interoperability considerations: None
Published specification: This document.
Applications that use this media type: RPKI administrators.
Additional information:
  Content: This media type is a signed object, as defined
      in [RFC6488], which contains a payload
      of a profiled vCard as defined above in this document.
  Magic number(s): None
  File extension(s): .gbr
  Macintosh file type code(s):
Person & email address to contact for further information:
  Randy Bush <randy@psg.com>
Intended usage: COMMON
Restrictions on usage: None
Author: Randy Bush <randy@psg.com>
Change controller: Randy Bush <randy@psg.com>
```

10. Acknowledgments

The author wishes to thank Russ Housley, the authors of [RFC6481], Stephen Kent, Sandy Murphy, Rob Austein, Michael Elkins, and Barry Leiba for their contributions.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC6350] Perreault, S., "vCard Format Specification", RFC 6350, August 2011.

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

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, February 2012.

11.2. Informative References

[RFC5513] Farrel, A., "IANA Considerations for Three Letter Acronyms", RFC 5513, April 1 2009.

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

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)"", RFC 6484, February 2012.

Author’s Address

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

Phone: +1 206 780 0431 x1
EMail: randy@psg.com