Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2011

R. Bush
Internet Initiative Japan

March 11, 2011

The RPKI Ghostbusters Record
draft-ietf-sidr-ghostbusters-03

Abstract

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

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 RFC 2119 [RFC2119].

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 September 12, 2011.

Copyright Notice

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-owning certificate. An important example is when the owner of a Route Origin Authorization (ROA) sees a problem, or an impending problem, with a certificate or CRL in the path between the ROA and a trust anchor. E.g., 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 intentionally hashes which are not meaningful to humans, see [I-D.ietf-sidr-cp], there is no way to use a certificate itself to lead to the worrisome certificate's or CRL's maintainer. So, "Who do you call?"

This document specifies the RPKI Ghostbusters Record, an object signed, indirectly via an End Entity (EE) certificate, by the certificate whose maintainer may be contacted using the human usable payload information in the Ghostbusters Record.

The Ghostbusters Record conforms to the syntax defined in [I-D.ietf-sidr-signed-object].

Note that the Ghostbusters Record is not an identity certificate, but rather an attestation to the contact data made by the issuer of the certificate signing the Ghostbusters Record.

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

This specification has three main sections. The first, Section 4, is the format of the contact payload information, a severely profiled vCARD. The second, Section 5, profiles the packaging of the payload

as a profile of the RPKI Signed Object Template specification [I-D.ietf-sidr-signed-object]. The third, Section 6, describes the proper validation of the signed Ghostbusters Record.

2. Suggested Reading

It is assumed that the reader understands the RPKI, [I-D.ietf-sidr-arch], the RPKI Repository Structure, [I-D.ietf-sidr-repos-struct], Signed RPKI Objects, [I-D.ietf-sidr-signed-object], and vCARDs [RFC2426].

3. RPKI Ghostbusters Record Payload Example

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

```
BEGIN:vCard
VERSION:3.0
FN:Human's Name
N:Name;Human's;Ms.;Dr.;OCD;ADD
ORG:Organizational Entity
ADR;TYPE=WORK:;;42 Twisty Passage;Deep Cavern; WA; 98666;U.S.A.
TEL;TYPE=VOICE,MSG,WORK:+1-666-555-1212
TEL;TYPE=FAX,WORK:+1-666-555-1213
EMAIL;TYPE=INTERNET:human@example.com
END:vCard
```

4. vCARD Profile

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

The Ghostbusters vCARD payload is a minimalist subset of the vCARD as described in [RFC2426].

BEGIN - pro forma packaging which MUST be the first line in the vCARD and MUST have the value "BEGIN:vCARD" as described in

[RFC2426].

VERSION - pro forma packaging which MUST be the second line in the vCARD and MUST have the value "VERSION:3.0" as described in 3.6.9 of [RFC2426].

FN - the name, as described in 3.1.1 of [RFC2426], of a contactable person who responsible for the certificate.

N - the components of the name of the object the vCard represents, as described in 3.1.2 of [RFC2426].

ORG - an organization as described in 3.5.5 of [RFC2426].

ADR - a postal address as described in 3.2.1 of [RFC2426].

TEL - a voice and/or fax phone as described in 3.3.1 of [RFC2426].

EMAIL - an Email address as described in 3.3.2 of [RFC2426]

END - pro forma packaging which MUST be the last line in the vCARD and MUST have the value "END:vCARD" as described in [RFC2426].

Per [RFC2426], the BEGIN, VERSION, FN, N, and END types MUST be included in a record. To be useful, one or more of ADR, TEL, and EMAIL MUST be included. Other types MAY NOT be included.

5. CMS Packaging

The Ghostbusters Record is a CMS signed-data object conforming to the RPKI Signed Data Object Template, [I-D.ietf-sidr-signed-object].

The ContentType of a Ghostbusters Record is defined as rpkiGhostbusters, and has the numerical value of [TO BE ASSIGNED]. This OID MUST appear both within the eContentType in the encapContentInfo object as well as the ContentType signed attribute in the signerInfo object. See [I-D.ietf-sidr-signed-object].

eContent: The content of a Ghostbusters Record is described above in Section 4 above.

Similarly to a ROA, the Ghostbusters Record is verified using an EE certificate issued under the CA certificate associated with the resource-holding 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.

6. Validation

The validation procedure defined in Section 3 of [I-D.ietf-sidr-signed-object] 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 4 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.

7. Security Considerations

Though there is no on the wire protocol in this specification, there are attacks which 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 warned that the data in a Ghostbusters Record are self-asserted. These data have not been verified by the CA that issued a (CA) certificate to the entity that issued the EE

certificate used to validate the Ghostbusters Record.

8. IANA Considerations

This document has no IANA Considerations.

9. Acknowledgments

The author wishes to thank Russ Housley, the authors of [I-D.ietf-sidr-signed-object], Stephen Kent, and Michael Elkins for their contributions.

10. References

10.1. Normative References

[I-D.ietf-sidr-signed-object]
Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure", draft-ietf-sidr-signed-object-03 (work in progress), February 2011.

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

[RFC2426] Dawson, F. and T. Howes, "vCard MIME Directory Profile", RFC 2426, September 1998.

10.2. Informative References

[I-D.ietf-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch-12 (work in progress), February 2011.

[I-D.ietf-sidr-cp]

Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource PKI (RPKI)", draft-ietf-sidr-cp-16 (work in progress), December 2010.

[I-D.ietf-sidr-repos-struct]
Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", draft-ietf-sidr-repos-struct-07 (work in progress), February 2011.

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