

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: July 1, 2012

R. Bush  
Internet Initiative Japan  
December 29, 2011

**The RPKI Ghostbusters Record**  
**draft-ietf-sidr-ghostbusters-16**

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 which may be verified (indirectly) by a CA 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 [[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 July 1, 2012.

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.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Suggested Reading . . . . .	<a href="#">4</a>
<a href="#">3.</a>	RPKI Ghostbusters Record Payload Example . . . . .	<a href="#">4</a>
<a href="#">4.</a>	vCard Profile . . . . .	<a href="#">4</a>
<a href="#">5.</a>	CMS Packaging . . . . .	<a href="#">5</a>
<a href="#">6.</a>	Validation . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">8.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">8.1.</a>	OID . . . . .	<a href="#">6</a>
<a href="#">8.2.</a>	File Extension . . . . .	<a href="#">7</a>
<a href="#">8.3.</a>	Media Type . . . . .	<a href="#">7</a>
<a href="#">9.</a>	Acknowledgments . . . . .	<a href="#">7</a>
<a href="#">10.</a>	References . . . . .	<a href="#">8</a>
<a href="#">10.1.</a>	Normative References . . . . .	<a href="#">8</a>
<a href="#">10.2.</a>	Informative References . . . . .	<a href="#">8</a>
	Author's Address . . . . .	<a href="#">8</a>

Bush

Expires July 1, 2012

[Page 2]

## 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 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 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 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 [[I-D.ietf-sidr-signed-object](#)]. 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 may 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 an 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 4](#), is

Bush

Expires July 1, 2012

[Page 3]

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 [[RFC6350](#)].

## **3. 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
```

## **4. 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 which 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 which MUST be the first line in the vCard and MUST have the value "BEGIN:VCARD" as described in [[RFC6350](#)].

Bush

Expires July 1, 2012

[Page 4]

VERSION - pro forma packaging which MUST be the second line in the vCard and MUST have the value "VERSION:4.0" as described in 3.7.9 of [\[RFC6350\]](#).

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

ORG - an organization as described in 6.6.4 of [\[RFC6350\]](#).

ADR - a postal address as described in 6.3 of [\[RFC6350\]](#).

TEL - a voice and/or fax phone as described in 6.4.1 of [\[RFC6350\]](#).

EMAIL - an Email address as described in 6.4.2 of [\[RFC6350\]](#)

END - pro forma packaging which 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, zero or more of ADR, TEL, and EMAIL MUST be included. Other properties MUST NOT be included.

## 5. CMS Packaging

The Ghostbusters Record is a CMS signed-data object conforming to the Signed Object Template for the Resource Public Key Infrastructure, [\[I-D.ietf-sidr-signed-object\]](#).

The ContentType 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 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, 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 which contains the payload defined above.

This EE certificate MUST describe its internet number resources using



Bush

Expires July 1, 2012

[Page 5]

the "inherit" attribute, rather than explicit description of a resource set, see [[RFC3779](#)].

## 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 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.

## 8. IANA Considerations

### 8.1. OID

The IANA is requested to register the OID for the Ghostbusters Record in the registry created by [[I-D.ietf-sidr-signed-object](#)] as follows:

Name	OID	Specification
-----		
Ghostbusters	1.2.840.113549.1.9.16.1.35	[ This document ]



## 8.2. File Extension

Realizing the deep issues raised by [[RFC5513](#)], the IANA is requested to add an item for the Ghostbusters Record file extension to the RPKI Repository Name Scheme created by [[I-D.ietf-sidr-repos-struct](#)] as follows:

Filename Extension	RPKI Object	Reference
-----		
.gbr	Ghostbusters Record	[ This document ]

## 8.3. Media Type

The IANA is requested to register 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  
[this document].

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 [[I-D.ietf-sidr-signed-object](#)], 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>

## 9. Acknowledgments

The author wishes to thank Russ Housley, the authors of [[I-D.ietf-sidr-repos-struct](#)], Stephen Kent, Sandy Murphy, Rob Austein, Michael Elkins, and Barry Leiba for their contributions.

Bush

Expires July 1, 2012

[Page 7]

## **10. References**

### **10.1. Normative References**

- [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-09](#) (work in progress), July 2011.
- [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-04](#) (work in progress), May 2011.
- [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.

### **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-13](#) (work in progress), May 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-17](#) (work in progress), April 2011.
- [RFC5513] Farrel, A., "IANA Considerations for Three Letter Acronyms", [RFC 5513](#), April 1 2009.



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](mailto:randy@psg.com)