Workgroup: Network Working Group
Internet-Draft:
draft-ietf-sidrops-rpki-has-no-identity-06
Published: 14 April 2022
Intended Status: Standards Track
Expires: 16 October 2022
Authors: R. Bush
Arrcus & Internet Initiative Japan
R. Housley
Vigil Security

The I in RPKI does not stand for Identity

Abstract

There is a false notion that Internet Number Resources (INRs) in the RPKI can be associated with the real-world identity of the 'holder' of an INR. This document attempts to put that notion to rest.

Requirements Language

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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 https://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 16 October 2022.

Copyright Notice

Table of Contents

1. Introduction

The Resource Public Key Infrastructure (RPKI), see [RFC6480], "Represents the allocation hierarchy of IP address space and Autonomous System (AS) numbers," which are collectively known as Internet Number Resources (INRs). Since initial deployment, the RPKI has grown to include other similar resource and routing data, e.g. Router Keying for BGPsec, [RFC8635].

In security terms, the phrase "Public Key" implies there is also a corresponding private key [RFC5280]. The RPKI provides strong authority to the current holder of INRs; however, some people a have a desire to use RPKI private keys to sign arbitrary documents as the INR 'holder' of those resources with the inappropriate expectation that the signature will be considered an attestation to the authenticity of the document content. But in reality, the RPKI certificate is only an authorization to speak for the explicitly identified INRs; it is explicitly not intended for authentication of the 'holders' of the INRs. This situation is emphasized in Section 2.1 of [RFC6480].

It has been suggested that one could authenticate real-world business transactions with the signatures of INR holders. E.g. Bill's Bait and Sushi could use the private key attesting to that they are the holder of their AS in the RPKI to sign a Letter of Authorization (LOA) for some other party to rack and stack hardware owned by BB&S. Unfortunately, while this may be technically possible, it is neither appropriate nor meaningful.

The I in RPKI actually stands for "Infrastructure," as in Resource Public Key Infrastructure, not for "Identity". In fact, the RPKI does not provide any association between INRs and the real world holder(s) of those INRs. The RPKI provides authorization to make assertions only regarding named IP address blocks, AS numbers, etc.

In short, avoid the desire to use RPKI certificates for any purpose other than the verification of authorizations associated with the delegation of INRs or attestations related to INRs. Instead, recognize that these authorizations and attestations take place irrespective of the identity of a RPKI private key holder.

2. The RPKI is for Authorization

The RPKI was designed and specified to sign certificates for use within the RPKI itself and to generate Route Origin Authorizations (ROAs), [RFC6480], for use in routing. Its design intentionally precluded use for attesting to real-world identity as, among other issues, it would expose the Certification Authority (CA) to liability.

That the RPKI does not authenticate real-world identity is by design. If it tried to do so, aside from the liability, it would end in a world of complexity with no proof of termination, as X.400 learned.

Registries such as the Regional Internet Registries (RIRs) provide INR to real-world identity mapping through WHOIS, [RFC3912], and similar services. They claim to be authoritative, at least for the INRs which they allocate.

PKI operations MUST NOT be performed with RPKI certificates other than exactly as described, and for the purposes described, in [RFC6480]. That is, RPKI-based credentials of INRs MUST NOT be used to authenticate real-world documents or transactions without some formal external authentication of the INR and the authority for the actually anonymous INR holder to authenticate the particular document or transaction.

I.e., RPKI-based credentials of INRs MUST NOT be used to authenticate real-world documents or transactions without some formal external authentication of the INR and the authority for the actually anonymous INR holder to authenticate the particular document or transaction.

Given sufficient external, i.e. non-RPKI, verification of authority, the use of RPKI-based credentials seems superfluous.

3. Discussion

The RPKI base document, [RFC6480], Section 2.1 says explicitly "An important property of this PKI is that certificates do not attest to the identity of the subject."

The Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI) [RFC7382] Section 3.1, Naming, makes very clear that "The Subject name in each certificate SHOULD NOT be meaningful;" and goes on to do so at some length.

Normally, the INR holder does not hold the private key attesting to their resources; the Certification Authority (CA) does. The INR holder has a real-world business relationship with the CA for which they have likely signed real-world documents.

As the INR holder does not have the keying material, they rely on the CA, to which they presumably present credentials, to manipulate their INRs. These credentials may be userid/password (with two factor authentication one hopes), a hardware token, client browser certificates, etc.

Hence schemes such as [I-D.ietf-sidrops-rpki-rta] and [I-D.ietf-sidrops-rpki-rsc] must go to great lengths to extract the supposedly relevant keys from the CA.

For some particular INR, say Bill's Bait and Sushi's Autonomous System (AS) number, someone out on the net probably has the credentials to the CA account in which BB&S's INRs are registered. That could be the owner of BB&S, Roberto's Taco Stand, an IT vendor, or the Government of Elbonia. One simply can not know.

In large organizations, INR management is often compartmentalized with no authority over anything beyond dealing with INR registration. The INR manager for Bill's Bait and Sushi is unlikely to be authorized to conduct bank transactions for BB&S, or even to authorize access to BB&S's servers in some colocation facility.

Then there is the temporal issue. The holder of that AS may be BB&S today when some document was signed, and could be the Government of Elbonia tomorrow. Or the resource could have been administratively moved from one CA to another, likely requiring a change of keys. If so, how does one determine if the signature on the real-world document is still valid?

While Ghostbuster Records [RFC6493] may seem to identify real-world entities, their semantic content is completely arbitrary, and does not attest to holding of any INRs. They are merely clues for operational support contact in case of technical RPKI problems.

Usually, before registering INRs, CAs require proof of an INR holding via external documentation and authorities. It is somewhat droll that the CPS Template, [RFC7382], does not mention any diligence the CA must, or even might, conduct to assure the INRs are in fact owned by a registrant.

That someone can provide 'proof of possession' of the private key signing over a particular INR should not be taken to imply that they are a valid legal representative of the organization in possession of that INR. They could be just an INR administrative person.

Autonomous System Numbers do not identify real-world entities. They are identifiers some network operators 'own' and are only used for loop detection in routing. They have no inherent semantics other than uniqueness.

4. Security Considerations

Attempts to use RPKI data to authenticate real-world documents or other artifacts requiring identity are invalid and misleading.

When a document is signed with the private key associated with an RPKI certificate, the signer is speaking for the INRs, the IP address space and Autonomous System (AS) numbers, in the certificate. This is not an identity; this is an authorization. In schemes such as [I-D.ietf-sidrops-rpki-rta] and [I-D.ietf-sidrops-rpki-rsc] the signed message further narrows this scope of INRs. The INRs in the message are a subset of the INRs in the certificate. If the signature is valid, the message content comes from a party that is authorized to speak for that subset of INRs.

Control of INRs for an entity could be used to falsely authorize transactions or documents for which the INR manager has no authority.

5. IANA Considerations

This document has no IANA Considerations.

6. Acknowledgments

The authors thank George Michaelson and Job Snijders for lively discussion, Geoff Huston for some more formal text, Ties de Kock for useful suggestions, and last but not least, Biff for the loan of Bill's Bait and Sushi.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] 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, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[RFC7382] Kent, S., Kong, D., and K. Seo, "Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)", BCP 173, RFC 7382, DOI 10.17487/RFC7382, April 2015, <https://www.rfc-editor.org/info/rfc7382>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8635] Bush, R., Turner, S., and K. Patel, "Router Keying for BGPsec", RFC 8635, DOI 10.17487/RFC8635, August 2019, <https://www.rfc-editor.org/info/rfc8635>.

7.2. Informative References

[I-D.ietf-sidrops-rpki-rsc] Snijders, J., Harrison, T., and B. Maddison, "Resource Public Key Infrastructure (RPKI) object profile for Signed Checklist (RSC)", Work in Progress, Internet-Draft, draft-ietf-sidrops-rpki-rsc-06, 12 February 2022, <https://www.ietf.org/archive/id/draft-ietf-sidrops-rpki-rsc-06.txt>.

[I-D.ietf-sidrops-rpki-rta] Michaelson, G. G., Huston, G., Harrison, T., Bruijnzeels, T., and M. Hoffmann, "A profile for Resource Tagged Attestations (RTAs)", Work in Progress, Internet-Draft, draft-ietf-sidrops-rpki-rta-00, 21 January 2021, <https://www.ietf.org/archive/id/draft-ietf-sidrops-rpki-rta-00.txt>.

[RFC3912] Daigle, L., "WHOIS Protocol Specification", RFC 3912, DOI 10.17487/RFC3912, September 2004, <https://www.rfc-editor.org/info/rfc3912>.

[RFC6493]
Bush, R., "The Resource Public Key Infrastructure (RPKI) Ghostbusters Record", RFC 6493, DOI 10.17487/RFC6493, February 2012, <https://www.rfc-editor.org/info/rfc6493>.

Authors' Addresses

Randy Bush
Arrcus & Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, WA 98110
United States of America

Email: randy@psg.com

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA, 20170
United States of America

Email: housley@vigilsec.com