Internet Engineering Task Force (IETF)
Request for Comments: 9589
Updates: 6488
Category: Standards Track
ISSN: 2070-1721

J. Snijders
Fastly
T. Harrison
APNIC

May 2024

On the Use of the Cryptographic Message Syntax (CMS) Signing-Time Attribute in Resource Public Key Infrastructure (RPKI) Signed Objects

Abstract

In the Resource Public Key Infrastructure (RPKI), Signed Objects are defined as Cryptographic Message Syntax (CMS) protected content types. A Signed Object contains a signing-time attribute, representing the purported time at which the object was signed by its issuer. RPKI repositories are accessible using the rsync and RPKI Repository Delta protocols, allowing Relying Parties (RPs) to synchronize a local copy of the RPKI repository used for validation with the remote repositories. This document describes how the CMS signing-time attribute can be used to avoid needless retransfers of data when switching between different synchronization protocols. This document updates RFC 6488 by mandating the presence of the CMS signing-time attribute and disallowing the use of the binary-signing-time attribute.

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 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9589.

Table of Contents

1. Introduction

In the Resource Public Key Infrastructure (RPKI) [RFC6480], Signed Objects are defined as Cryptographic Message Syntax (CMS) [RFC5652] [RFC6268] protected content types by way of a standard template [RFC6488]. That template includes an optional CMS signing-time attribute, representing the time at which the object was signed by its issuer. At the time when the standard template was defined, rsync was the only distribution mechanism for RPKI repositories.

Since the publication of the standard template, a new, additional protocol for distribution of RPKI repositories has been developed: the RPKI Repository Delta Protocol (RRDP) [RFC8182]. While RPKI repository operators must provide rsync service, RRDP is typically deployed alongside it as well, and is preferred by default by most Relying Party (RP) implementations. However, RP implementations also support fallback to rsync in the event of problems with the RRDP service. As deployment experience with RRDP has increased, the usefulness of optimizing switchovers by RPs from one mechanism to the other has become apparent.

This document describes how Repository Operators [RFC6481] and RPs can use the CMS signing-time attribute to minimize the burden of switching over from RRDP to rsync. Additionally, this document updates [RFC6488] by mandating the presence of the CMS signing-time attribute and disallowing the use of the binary-signing-time attribute.

1.1. 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.

2. Optimized Switchover from RRDP to rsync

To avoid needless retransfers of unchanged files in consecutive rsync synchronizations, [RPKI-PUB-SERV] recommends the use of so-called 'deterministic' (normalized) timestamps for files. When the content of a file is unchanged, Repository Operators SHOULD ensure that the last modification timestamp of the file remains unchanged as well.

This document advances the aforementioned concept by describing a synchronization strategy through which needless transfers are also avoided upon first use of rsync, by leveraging data previously fetched via RRDP.

At the time of writing, all commonly used RP implementations will first attempt synchronization via RRDP, as described in [RPKI-REP-REQS]. If synchronization via RRDP fails for some reason (e.g., malformed XML, expired TLS certificate, HTTP connection timeout), the RP will attempt to synchronize via rsync instead.

In the rsync synchronization protocol, a file's last modification timestamp ('mod-time' from here on) and file size are used to determine whether the general-purpose rsync synchronization algorithm needs to be executed for the file. This is the default mode for both the original rsync implementation [rsync] and the OpenBSD implementation [openrsync]. If the sender's copy of the file and the receiver's copy of the file both have the same mod-time and file size, the files are assumed to contain the same content, and they will be omitted from the list of files to be transferred. Ensuring consistency with respect to mod-time for both senders and receivers helps to reduce the burden of rsync synchronization in terms of network bandwidth, disk I/O operations, and CPU usage.

In order to reduce the burden of the rsync synchronization (following an RRDP failure), Repository Operators and RPs SHOULD adhere to the following guidelines.

2.1. Guidance for Repository Operators

When serializing RPKI Signed Objects to a filesystem hierarchy for publication via rsync, the mod-time of the file containing the Signed Object SHOULD be set to the value of the CMS signing-time attribute contained within the Signed Object.

2.2. Guidance for Relying Parties

When serializing RPKI Signed Objects retrieved via RRDP to a filesystem hierarchy, the mod-time of the file containing the Signed Object SHOULD be set to the value of the CMS signing-time attribute contained within the Signed Object.

If an RP uses RRDP to synthesize a filesystem hierarchy for the repository, then synchronizing to the corresponding directory directly is an option. Alternatively, the RP can synchronize to a new (empty) directory using the --compare-dest=DIR rsync feature, in order to avoid retrieving files that are already available by way of the synthesized filesystem hierarchy stemming from previous RRDP fetches. The DIR component is to be substituted with the name of the directory containing previously fetched and validated RPKI data (in its original DER-encoded form, to ensure the file size parameter matches).

From the [rsync] man page for --compare-dest=DIR:

> This option instructs rsync to use DIR on the destination machine as an additional hierarchy to compare destination files against doing transfers (if the files are missing in the destination directory). If a file is found in DIR that is identical to the sender's file, the file will NOT be transferred to the destination directory. This is useful for creating a sparse backup of just files that have changed from an earlier backup.

From the [openrsync] man page for --compare-dest=directory:

> Use directory as an alternate base directory to compare files against on the destination machine. If file in directory is found and identical to the sender's file, the file will not be transferred.

3. Presence of the CMS Signing-Time Attribute in Public Repositories

Analyzing the [rpkiviews] archives containing millions of RPKI Signed Objects discovered via the five Regional Internet Registry (RIR) Trust Anchors (TAs) from 6 June 2022 to 29 January 2024, each Signed Object contained a CMS signing-time attribute.

The above means that all of the commonly used TAs and their subordinate Certification Authorities (CAs) produce Signed Objects that contain a CMS signing-time attribute. This means that making the CMS signing-time attribute mandatory would not cause any existing commonly used TA or CA to become non-compliant.

As of 29 January 2024, for 83.8% of Signed Objects, the CMS signing-time timestamp matches the file's mod-time observed via rsync. This means that it is already the case that RPs would see a significant reduction in the amount of processing required in rsync if they adopted the strategy outlined in Section 2.2.

In the above-mentioned period of time, no Signed Objects were discovered with a CMS binary-signing-time [RFC6019] attribute in the specified repositories. Therefore, disallowing the use of the CMS binary-signing-time attribute would not cause any existing commonly used TA or CA to become non-compliant.

4. Updates to RFC 6488

This section updates [RFC6488] to make the CMS signing-time attribute mandatory and to disallow the presence of the CMS binary-signing-time attribute.

* In Section 2.1.6.4, this paragraph is replaced as follows.

  OLD

  | The signedAttrs element MUST be present and MUST include the content- type and message-digest attributes [RFC5652]. The signer MAY also include the signing-time attribute [RFC5652], the binary-signing-time attribute [RFC6019], or both attributes. Other signed attributes MUST NOT be included.

  NEW

  | The signedAttrs element MUST be present and MUST include the content-type, message-digest, and signing-time attributes [RFC5652]. Other signed attributes MUST NOT be included.

* In Section 2.1.6.4.3, the first sentence is replaced as follows.

  OLD

  | The signing-time attribute MAY be present.

  NEW

  | The signing-time attribute MUST be present.

* In Section 2.1.6.4.3, the sentence "Note that the presence or absence of the signing-time attribute MUST NOT affect the validity of the signed object (as specified in Section 3)." is removed.

* Section 2.1.6.4.4 is removed in its entirety.

* In Section 3, item 1.f is replaced as follows.

  OLD

  | f. The signedAttrs field in the SignerInfo object is present and contains both the content-type attribute (OID 1.2.840.113549.1.9.3) and the message-digest attribute (OID 1.2.840.113549.1.9.4).

  NEW

| f. The signedAttrs field in the SignerInfo object is present
| and contains the content-type attribute (OID
| 1.2.840.113549.1.9.3), the message-digest attribute (OID
| 1.2.840.113549.1.9.4), and the signing-time attribute
| (1.2.840.113549.1.9.5).

* In Section 3, item 1.g is replaced as follows.

OLD

| g. The signedAttrs field in the SignerInfo object does not
| contain any attributes other than the following four: the
| content-type attribute (OID 1.2.840.113549.1.9.3), the
| message-digest attribute (OID 1.2.840.113549.1.9.4), the
| signing-time attribute (OID 1.2.840.113549.1.9.5), and the
| binary-signing-time attribute (OID
| 1.2.840.113549.1.9.16.2.46). Note that the signing-time
| and binary-signing-time attributes MAY be present, but they
| are not required.

NEW

| g. The signedAttrs field in the SignerInfo object does not
| contain any attributes other than the following three: the
| content-type attribute (OID 1.2.840.113549.1.9.3), the
| message-digest attribute (OID 1.2.840.113549.1.9.4), and
| the signing-time attribute (OID 1.2.840.113549.1.9.5).

* In Section 9 (Informative References), [RFC6019] is removed from the list.

5. Security Considerations

No requirement is imposed concerning the correctness of the signing time attribute. It does not provide reliable information on the time the signature was produced and it bears no relevance for seamless switchover between RRDP and rsync.

Although the Security Considerations in [RFC6019] mandate that the signing-time and binary-signing-time attributes (if both present) MUST provide the same date and time, there is still a chance that an object will have values for these attributes that do not represent the same date and time. Restricting the RPKI Signed Object profile to a single field for storing the signing time removes any potential for ambiguity.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[openrsync] "openrsync", 2023, <https://www.openrsync.org/>.

[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>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, DOI 10.17487/RFC6268, July 2011, <https://www.rfc-editor.org/info/rfc6268>.

[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>.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <https://www.rfc-editor.org/info/rfc6481>.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, DOI 10.17487/RFC6488, February 2012, <https://www.rfc-editor.org/info/rfc6488>.

[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>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

[rsync] "rsync", 2024, <https://rsync.samba.org/>.

7.2. Informative References

[RFC6019] Housley, R., "BinaryTime: An Alternate Format for Representing Date and Time in ASN.1", RFC 6019, DOI 10.17487/RFC6019, September 2010, <https://www.rfc-editor.org/info/rfc6019>.

[RPKI-PUB-SERV] Bruijnzeels, T., de Kock, T., Hill, F., and T. Harrison, "RPKI Publication Server Best Current Practices", Work in Progress, Internet-Draft, draft-timbru-sidrops-publication-server-bcp-02, 18 January 2024, <https://datatracker.ietf.org/doc/html/draft-timbru-sidrops-publication-server-bcp-02>.

[RPKI-REP-REQS] Bruijnzeels, T., Bush, R., and G. Michaelson, "Resource Public Key Infrastructure (RPKI) Repository Requirements", Work in Progress, Internet-Draft, draft-ietf-sidrops-prefer-rrdp-02, 23 December 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-prefer-rrdp-02>.

[rpkiviews] "rpkiviews", <https://www.rpkiviews.org/>.

Acknowledgements

The authors would like to thank Ties de Kock, Niels Bakker, Mikael Abrahamsson, Russ Housley, Zaheduzzaman Sarker, ric Vyncke, Mahesh Jethanandani, and Roman Danyliw, for their helpful review of this document.

Authors’ Addresses

Job Snijders
Fastly
Amsterdam
The Netherlands
Email: job@fastly.com

Tom Harrison
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane QLD 4101
Australia
Email: tomh@apnic.net