Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 30, 2017

T. Bruijnzeels
RIPE NCC
C. Martinez
LACNIC

June 28, 2017

RPKI signed object for TAL
draft-tbruijnzeels-sidrops-signed-tal-00

Abstract

Trust Anchor Locators (TALs) [RFC7730] are used by Relying Parties in the RPKI to locate and validate Trust Anchor certificates used in RPKI validation. This documents defines an RPKI signed object [RFC6488] for a Trust Anchor Locator (TAL) that can be published by Trust Anchor to communicate a new TAL to already deployed Relying Parties. The two primary use cases for this are that 1) a Trust Anchor may wish to change the locations where its TA certificate may be found, and 2) a Trust Anchor may wish to perform a planned migration to a new key. Note that unplanned key rolls are considered out of scope for this document.

Status of This Memo

Copyright Notice

Table of Contents

1. Requirements notation 2
2. Introduction 2
3. Signed TAL definition 3
   3.1. The Signed TAL Content Type 3
   3.2. The Signed TAL eContent 3
   3.3. Signed TAL Validation 4
4. Signed TAL Generation 4
5. Signed TAL Publication 5
6. Supporting a TA Key Roll 5
   6.1. Preparing a new TA key 5
   6.2. Staging period - Using both the old and the new TA key . 5
   6.3. Preserving the Signed TAL 6
   6.4. Retiring the old key 6
7. Supporting changing TA certificate publication point(s) . . . 6
   7.1. Adding a publication point 6
   7.2. Withdrawing a publication point 6
   7.3. Withdrawing the Signed TAL 7
8. Relying Party Use 7
9. IANA Considerations 7
   9.1. OID 7
   9.2. File Extension 7
10. Security Considerations 7
11. Acknowledgements 7
12. Normative References 8
Authors’ Addresses 9

1. Requirements notation

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].

2. Introduction

Trust Anchor Locator (TAL) files [RFC7730] are used in the Resource Public Key Infrastructure (RPKI) to help Relying Parties locate and verify a trust anchor certificate. A TAL file consists of:

- One or more rsync URIs [RFC5781]

- A subjectPublicKeyInfo [RFC5280] in DER format [X.509], encoded in Base64

The TAL can be distributed out-of-band to Relying Parties (RP), and it allows the RP to retrieve the most recent version of the Trust Anchor (TA) certificate from the cited location, and verify that public key of this certificate matches the TAL. This is useful as it allows selected data in the trust anchor to change, without needing to effect redistribution of the trust anchor per se. In particular the Internet Number Resources (INRs) extension [RFC3779] and the publication points defined in the Subject Information Access [RFC6487] may be updated this way.

The assumption is that both the URIs and key of the TA certificate remain stable. However, an organisation operating a TA may wish to change either of these properties, because of a need to:

- change one or more URIs

- perform a planned key roll

In this document we describe a method for TA operators to publish a an updated TAL in a secure a well-defined fashion, so that RPs can be alerted to these changes.

3. Signed TAL definition

A signed TAL is an RPKI signed object, as specified in [RFC6488]. The RPKI signed object template requires specification of the following data elements in the context of the manifest structure.

3.1. The Signed TAL Content Type

This document requests an OID for signed-Tal as follows:

```
signed-Tal OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
           rsadsi(113549) pkcs(1) pkcs9(9) 16 id-smime (1) TBD }
```

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]).

3.2. The Signed TAL eContent

The content of a Signed TAL is ASN.1 encoded using the Distinguished Encoding Rules (DER) [X.690], and is defined as follows:

```
SignedTalContent ::= IA5String
```

The "SignedTalContent" contains the content of the new TAL encoded in Base64 [RFC4648].

3.3. Signed TAL Validation

Before a Relying Party can use a Signed TAL, the relying party MUST first validate the Signed TAL. To validate a Signed TAL, the relying party MUST perform all the validation checks specified in [RFC6488] as well as the following additional specific validation step.

- The eContentType in the EncapsulatedContentInfo has OID 1.2.840.113549.1.9.16.1.TBD.

- The EE certificate of this Signed TAL is signed by a known Trust Anchor

- The decoded TAL content conforms to the format defined in [RFC7730]

If the above procedure indicates that the manifest is invalid, then the Signed TAL MUST be discarded and treated as though no Signed TAL were present.

4. Signed TAL Generation

A TA MAY choose to generate a single Singed TAL object to publish in its TA certificate publication point(s) in the RPKI. The TA MUST perform the following steps to generate the Signed TAL:

- Generate a key pair for a "one-time-use" EE certificate to use for the Signed TAL

- Generate a one-time-use EE certificate for the Signed TAL

- This EE certificate MUST have an SIA extension access description field with an accessMethod OID value of id-ad-signedobject, where the associated accessLocation references the publication point of the Sigend TAL as an object URL.

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

- This EE certificate MUST have a "notBefore" time that is before the moment that the Signed TAL will be published.

- This EE certificate MUST have a "notAfter" time that reflects the intended staging period, which MUST be at least 24 hours after the moment that the Signed TAL will be published.

5. Signed TAL Publication

A TA MAY publish a single Signed TAL object directly under its TA certificate publication point(s) in the RPKI. The object base filename SHOULD use a similar strategy as the base filename that is used to the determine the CRL and Manifest filenames for this TA certificate, and the extension part of the filename MUST be ".tal".

6. Supporting a TA Key Roll

A Signed TAL MAY be used to communicate a planned key roll for the TA.

6.1. Preparing a new TA key

Prior to publishing the Signed TAL for the new key the TA MUST perform the following steps:

- Generate a new key pair for the new TA certificate

- Generate a new TA Certificate, using a Subject Information Access for CA certificates (see section 4.8.8.1 of [RFC6487]) that references the URIs that will be used by the new key to publish objects, that are different from the URIs used by the TA certificate for the current key.

- ALL current signed certificates and other objects, with the exception of the old CRL, Manifest and Signed TAL, must be re-issued by the new key and published under the new publication point(s).

- The new TA certificate itself MUST be published in a (number of) new location(s) that are different from where the TA certificate for the current key is published.

After these steps are performed a new Signed TAL MUST be generated as described in Section 4, and published as described in Section 5.

6.2. Staging period - Using both the old and the new TA key

The staging period is initiated by the initial publication of a Signed TAL for the new key and must last at least 24 HOURS.

During the staging period the TA MUST continue to operate both the old and the new TA key.

6.3. Preserving the Signed TAL

The TA MAY preserve a Signed TAL for the old key after the staging period as a hint for RPs that missed the key roll. The following process can be used to achieve this:

- Produce a new long-lived CRL that revokes all previously signed certificates

- Produce a new long-lived Signed TAL

- Produce a new long-lived manifest that includes the CRL and Signed TAL

- Publish the CRL, MFT and Signed TAL

- Destroy the old TA key

6.4. Retiring the old key

The TA MAY retire and delete its old key after the staging period is over.

7. Supporting changing TA certificate publication point(s)

A signed TAL MAY be used to communicate an addition or removal of one or more publication locations where the TA certificate can be found.

7.1. Adding a publication point

When adding a publication point for a TA certificate, the TA MUST publish the certificate in the new location(s) prior to publication of the Signed TAL.

7.2. Withdrawing a publication point

When removing a publication point for TA certificate, the TA SHOULD observe a staging period of at least 24 Hours. The staging period is initiated by the publication of an updated Signed TAL where the publication point has been removed. During the staging period the TA SHOULD keep the old publication point up to date and available.

7.3. Withdrawing the Signed TAL

The TA MUST withdraw the Signed TAL after the chosen staging period, of at least 24 hours, is over.

8. Relying Party Use

When an RP discovers a new valid TAL signed under a trust anchor, it SHOULD substitute the current TAL immediately.

RP software MAY start using the new TAL thus found automatically without operator intervention, but it is RECOMMENDED that the software informs the operator of this event, and keeps a back-up of the old TAL.

Furthermore, it is RECOMMENDED that the RP software informs the operator whether the new TAL represents a key roll, or a change in URIs only.

9. IANA Considerations

9.1. OID

IANA is to add the following to the "RPKI Signed Objects" registry:

Decimal	Description	References
TBD	signed-Tal	[section 3.1]

9.2. File Extension

IANA is to add an item for the Signed TAL file extension to the "RPKI Repository Name Scheme" created by [RFC6481] as follows:

Extension	RPKI Object	Reference
.tal	Signed TAL	[this document]

10. Security Considerations

TBD

11. Acknowledgements

TBD

12. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <http://www.rfc-editor.org/info/rfc3779>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <http://www.rfc-editor.org/info/rfc4648>.

[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, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5781] Weiler, S., Ward, D., and R. Housley, "The rsync URI Scheme", RFC 5781, DOI 10.17487/RFC5781, February 2010, <http://www.rfc-editor.org/info/rfc5781>.

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

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, DOI 10.17487/RFC6487, February 2012, <http://www.rfc-editor.org/info/rfc6487>.

[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, <http://www.rfc-editor.org/info/rfc6488>.

[RFC7730] Huston, G., Weiler, S., Michaelson, G., and S. Kent, "Resource Public Key Infrastructure (RPKI) Trust Anchor Locator", RFC 7730, DOI 10.17487/RFC7730, January 2016, <http://www.rfc-editor.org/info/rfc7730>.

[X.509] ITU-T Recommendation X.509 (2000), "Recommendation X.509: The Directory - Authentication Framework", 2000.

[X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", 2002.

Authors’ Addresses

Tim Bruijnzeels
RIPE NCC

Email: tim@ripe.net

Carlos Martinez
LACNIC

Email: carlos@lacnic.net