

RATS Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 5 November 2022

H. Birkholz  
Fraunhofer SIT  
T. Fossati  
Arm Limited  
W. Pan  
Huawei Technologies  
C. Bormann  
Universität Bremen TZI  
4 May 2022

Epoch Markers  
draft-birkholz-rats-epoch-markers-01

## Abstract

Abstract Text

## About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at  
<https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/>.

Discussion of this document takes place on the rats Working Group mailing list (<mailto:rats@ietf.org>), which is archived at  
<https://mailarchive.ietf.org/arch/browse/rats/>.

Source for this draft and an issue tracker can be found at  
<https://github.com/ietf-rats/draft-birkholz-rats-epoch-marker>.

## 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 5 November 2022.

Internet-Draft

Epoch Markers

May 2022

## Copyright Notice

Copyright (c) 2022 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 (<https://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 Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Requirements Notation . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Epoch IDs . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Interaction Models . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Epoch Marker CDDL . . . . .	<a href="#">4</a>
<a href="#">5.</a>	References . . . . .	<a href="#">6</a>
<a href="#">5.1.</a>	Normative References . . . . .	<a href="#">6</a>
<a href="#">5.2.</a>	Informative References . . . . .	<a href="#">6</a>
<a href="#">Appendix A.</a>	<a href="#">RFC 3161</a> TSTInfo . . . . .	<a href="#">7</a>
	Acknowledgements . . . . .	<a href="#">7</a>
	Authors' Addresses . . . . .	<a href="#">7</a>

[1.](#) Introduction

Systems that are required to interact via secure interactions often require a shared understanding of the freshness of conveyed information, especially in the domain of remote attestation procedures. Establishing a notion of freshness between various involved entities taking on roles that rely on information that is not outdated is not simple. In general, establishing a shared understanding of freshness in a secure manner is not simple. The RATS architecture [[I-D.ietf-rats-architecture](#)] dedicates an extensive appendix solely on the topic of freshness considerations and that fact alone should be considered a telltale sign on how necessary yet complex establishing a trusted and shared understanding of freshness between systems actually is.

This document provides a prominent way to establish a notion of freshness between systems: Epoch Markers. Epoch Markers are messages that are like time ticks produced and conveyed by a system in a freshness domain: the Epoch Bell. Systems that receive Epoch Markers do not have to track freshness with their own local understanding of

time (e.g., a local real time clock). Instead, each reception of a specific Epoch Marker rings in a new age of freshness that is shared between all recipients. In essence, the emissions and corresponding receptions of Epoch Markers are like the ticks of a clock where the ticks are conveyed by the Internet.

The layout of the freshness domain in which Epoch Markers are conveyed like the ticks of a clock, introduces a domain-specific latency -- and therefore a certain uncertainty about tick accuracy.

While all Epoch Markers share the common characteristic of being like clock ticks in a freshness domain, there are various payload types that can make up the content of an Epoch Marker. These different types of Epoch Marker payloads address several specific use cases and are laid out in this document. While Epoch Markers are encoded in CBOR and many of the payload types are encoded in CBOR as well, a prominent payload is the Time Stamp Token content as defined by [\[RFC3161\]](#): a DER-encoded TSTInfo value. Time Stamp Tokens (TST) produced by Time Stamp Authorities (TSA) are conveyed by the Time Stamp Protocol (TSP). At the time of writing, TSAs are the most common world-wide implemented secure timestamp token systems. Reusing the essential TST payload structure as a payload type for CBOR encoded Epoch Markers makes sense with respect to migration paths and general interoperability. But there is more than one way to represent a signed timestamp and other kinds of freshness ticks that can be used for Epoch Markers.

In this document, basic interaction models on how to convey Epoch Markers are illustrated as they impact the message design of a generic Epoch Marker. Then, the structure of Epoch Markers is specified using CDDL and the corresponding payload types are introduced and elaborated on. To increase the level of trustworthiness in the Epoch Bell and the system that produces them, Epoch Markers also provide the option to include (concise) remote attestation evidence or corresponding remote attestation results.

## [1.1.](#) Requirements Notation

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.](#) Epoch IDs

The RATS architecture introduces the concept of Epoch IDs that mark certain events during remote attestation procedures ranging from simple handshakes to rather complex interactions including elaborate freshness proofs. The Epoch Markers defined in this document are a solution that includes the lessons learned from TSAs, the concept of Epoch IDs and provides several means to identify a new freshness epoch. Some of these methods are introduced and discussed in Section 10.3 of [[I-D.ietf-rats-architecture](#)].

## [3.](#) Interaction Models

The interaction models illustrated in this section are derived from the RATS Reference Interaction Models. In general there are three of them:

- \* ad-hoc requests (e.g., via challenge-response requests addressed at Epoch Bells), corresponding to Section 7.1 in [[I-D.ietf-rats-reference-interaction-models](#)]
- \* unsolicited distribution (e.g., via uni-directional methods, such as broad- or multicasting from Epoch Bells), corresponding to Section 7.2 in [[I-D.ietf-rats-reference-interaction-models](#)]
- \* solicited distribution (e.g., via a subscription to Epoch Bells), corresponding to Section 7.3 in [[I-D.ietf-rats-reference-interaction-models](#)]

#### 4. Epoch Marker CDDL

```
epoch-marker = [  
    header,  
    $payload,  
]  
  
header = {  
    ? challenge-response-nonce,  
    ? remote-attestation-evidence, ; could be EAT or Concise Evidence  
    ? remote-attestation-results, ; hopefully EAT with AR4SI Claims  
}  
  
challenge-response-nonce = (1: "PLEASE DEFINE")  
remote-attestation-evidence = (2: "PLEASE DEFINE")  
remote-attestation-results = (3: "PLEASE DEFINE")  
  
;payload types independent on interaction model  
$payload /= native-rfc3161-TST-info
```

```
$payload /= TST-info-based-on-CBOR-time-tag  
$payload /= CBOR-time-tag  
$payload /= multi-nonce  
$payload /= multi-nonce-list  
$payload /= strictly-monotonically-increasing-counter  
  
native-rfc3161-TST-info = bytes ; DER-encoded value of TSTInfo  
  
; ~~~  
; ~~~ translation with a few poetic licenses of ASN.1 TSTInfo into CDDL  
; ~~~  
TST-info-based-on-CBOR-time-tag = {  
    &(version : 0) => int .default 1 ; obsolete?  
    &(policy : 1) => oid  
    &(messageImprint : 2) => MessageImprint  
    &(serialNumber : 3) => int  
    &(eTime : 4) => profiled-etime  
    ? &(accuracy : 5) => rfc3161-accuracy  
    &(ordering : 6) => bool .default false  
    ? &(nonce : 7) => int  
    ? &(tsa : 8) => GeneralName
```

```

    * $$TSTInfoExtensions
}

; based on COSE_Hash_Find (draft-ietf-cose-hash-algs)
MessageImprint = [
    hashAlg : int
    hashValue : bstr
]

rfc3161-accuracy = non-empty<{
    ? &(seconds : 0) => int
    ? &(millis: 1) => 1..999
    ? &(micros: 2) => 1..999
}>

; timeMap profiles etime from https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-04
profiled-etime = #6.1001(timeMap)
timeMap = {
    1 => #6.1(int / float) ; TIME_T
    * int => any
}

; Section 11.8 of I-D.ietf-cose-cbor-encoded-cert
GeneralName = [ GeneralNameType : int, GeneralNameValue : any ]

; stuff

```

```

oid = #6.111(bstr)
non-empty<M> = (M) .and ({ + any => any })

CBOR-time-tag = [
    time-tag,
    ? nonce
]

time-tag = "PLEASE DEFINE"
nonce = "PLEASE DEFINE"

multi-nonce = tstr / bstr / int

multi-nonce-list = [+ multi-nonce]

```

strictly-monotonically-increasing-counter = uint ; counter context? per issu

## [5. References](#)

### [5.1. 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>>.
- [RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", [RFC 3161](#), DOI 10.17487/RFC3161, August 2001, <<https://www.rfc-editor.org/info/rfc3161>>.
- [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>>.

### [5.2. Informative References](#)

- [I-D.ietf-rats-architecture]  
Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, [draft-ietf-rats-architecture-15](#), 8 February 2022, <<https://www.ietf.org/archive/id/draft-ietf-rats-architecture-15.txt>>.
- [I-D.ietf-rats-reference-interaction-models]  
Birkholz, H., Eckel, M., Pan, W., and E. Voit, "Reference Interaction Models for Remote Attestation Procedures", Work in Progress, Internet-Draft, [draft-ietf-rats-](#)

Birkholz, et al. Expires 5 November 2022 [Page 6]

---

Internet-Draft Epoch Markers May 2022

reference-interaction-models-05, 26 January 2022,  
<<https://www.ietf.org/archive/id/draft-ietf-rats-reference-interaction-models-05.txt>>.

## [Appendix A. \[RFC 3161\]\(#\) TSTInfo](#)

As a reference for the definition of TST-info-based-on-CBOR-time-tag the code block below depicts the original layout of the TSTInfo

structure from [\[RFC3161\]](#).

```
TSTInfo ::= SEQUENCE {
    version                INTEGER { v1(1) },
    policy                  TSAPolicyId,
    messageImprint          MessageImprint,
    -- MUST have the same value as the similar field in
    -- TimeStampReq
    serialNumber            INTEGER,
    -- Time-Stamping users MUST be ready to accommodate integers
    -- up to 160 bits.
    genTime                 GeneralizedTime,
    accuracy                Accuracy OPTIONAL,
    ordering                BOOLEAN   DEFAULT FALSE,
    nonce                   INTEGER   OPTIONAL,
    -- MUST be present if the similar field was present
    -- in TimeStampReq. In that case it MUST have the same value.
    tsa                     [0] GeneralName OPTIONAL,
    extensions              [1] IMPLICIT Extensions OPTIONAL }
```

## Acknowledgements

TBD

## Authors' Addresses

Henk Birkholz  
Fraunhofer SIT  
Rheinstrasse 75  
64295 Darmstadt  
Germany  
Email: [henk.birkholz@sit.fraunhofer.de](mailto:henk.birkholz@sit.fraunhofer.de)

Thomas Fossati  
Arm Limited  
United Kingdom  
Email: [Thomas.Fossati@arm.com](mailto:Thomas.Fossati@arm.com)



Huawei Technologies  
Email: [william.panwei@huawei.com](mailto:william.panwei@huawei.com)

Carsten Bormann  
Universität Bremen TZI  
Bibliothekstr. 1  
D-28359 Bremen  
Germany  
Phone: +49-421-218-63921  
Email: [cabo@tzi.org](mailto:cabo@tzi.org)