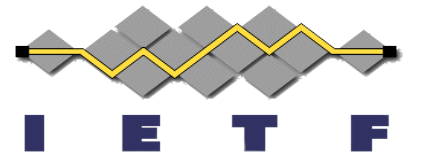


# Concise Encoding of Signed Merkle Tree Proofs (CoMETRE)

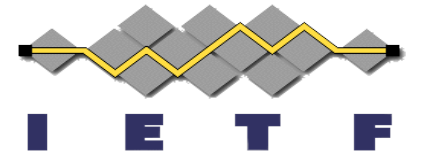
[draft-steele-cose-merkle-tree-proofs](#)

O. Steele, H. Birkholz, A. Delignat-Lavaud, C. Fournet

IETF 117, San Francisco  
July 24, 2023

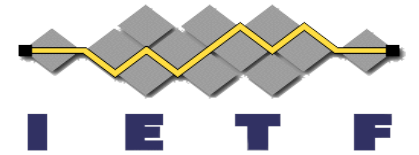


# What Does It Do?



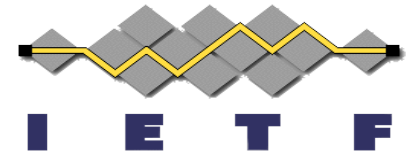
- Describes verifiable data structures in CBOR, encoding various proof types for binary merkle trees, merkle search trees, cryptographic accumulators, etc...
- Provides COSE building blocks for transparency logs, and other verifiable data structures.

# Why Do It?



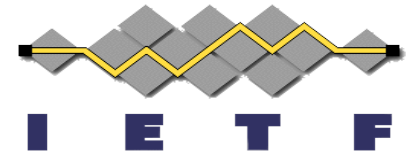
- Establishes interoperability across various verifiable data systems:
  - CBOR inclusion and consistency proofs for RFC9162
  - Enable offline verification
  - Gives COSE the ability to understand “proof types” beyond signatures, macs and ciphers.
  - There are other transparency use cases, such as “key transparency” & “certificate transparency”.

# Status



- Recently published [-01](#):
  - Updated to support generic “verifiable data structures” and “proof type”.
  - Updated IANA Registry Request to accommodate more than Merkle trees, correspondingly.
  - More proof types in the future! (beyond consistency, e.g., freshness)
  - Need to improve CDDL examples (stay tuned).
  - Will monitor proof type output of KT and render it COSE interoperable.
  - Need to improve CDDL examples (stay tuned).

# Application Example (SCITT Receipt)



See also <https://github.com/ietf-scitt/draft-birkholz-cose-cometre-ccf-profile>

```
# COSE_Sign1
18([

# Protected Header
h'a2012...43833633531',
# {
#  "alg" : "ES256",
#  1 : -7,
#  "verifiable-data-structure" : "RFC9162_SHA256",
#  TBD_1 : 1,
#  ... additional application specific headers ...
# }

# Unprotected Header
{
# "inclusion-proof" : "h'313...c3932"
TBD_2 : h'3133...52c3932'
},

# Detached Payload

# Signature
h'486...7f77ea'
])
```

```
# COSE_Sign1
18([

# Protected Header
h'a2012...43833633531',
# {
#  "alg" : "ES256",
#  1 : -7,
#  "verifiable-data-structure" : "RFC9162_SHA256",
#  TBD_1 : 1,
#  ... additional application specific headers ...
# }

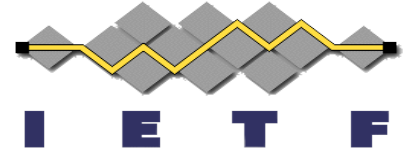
# Unprotected Header
{
# "consistency-proof" : "h'4525...4234"
TBD_3 : h'412413...386752'
},

# Protected Payload
h'fe802...75c',

# Signature
h'3786...5133a'
])
```

# Demo Example (SCITT Transparency Service)

See also <https://scitt.xyz>



scitt.xyz/demo/log/entries/0

Demo

Exit Demo

Authenticate

did:jwk:eyJraWQ...

Inclusion

Consistency

Identity

Sign

Verify

API

scitt.io

Tree 3 Leaf 0 Merkle inclusion proofs prove a leaf is present in a tree.

INCLUSION PATH ↑

`_k0Lz9I1idVIIhSMuHRHzX1_FJ_XRDx1cThFN8XnWs`

INCLUSION PATH ↑

`R20pxx1Pi8mq0xwSrtnJUCxd2_e_8jniQoXNu5i1Vc`

Demo

Signed Inclusion Proof

DOWNLOAD

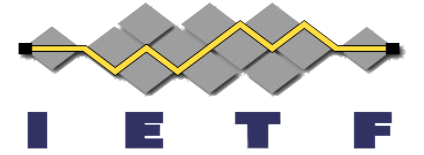
```
1 # COSE_Sign1
2 18([
3
4 # Protected Header
5 h'a3013822036a696d6167652f6a7065670459017e469643a6a776b3a65794a72615751694f694a31636d3436615756305a6a707759584a6862584d366232463164476736616e64724c58526f6457316963484a70626e513663326868
4c5449314e6a70324f4735424f5546575a484649624668485a546c525357733465445a315132465654334e6c525646724e456b744c566732554464a535746524969776961335235496a6f6952554d
694c434a6a636e59694f694a514c544d344e434973496d46735a794936496b56544d7a67304969776965434936496d4e425133426e64554a7a656c5535626c3966535774586245684e54475678567a
5130536c51324d30704761464e56556c4e51613249786258647a63586c52626c5a765546395a546c564857444a4d536c464e63576f694c43a35496a6f695a6d7453566b52465a6d67314f46396f5a6c4
6c4e514e5749744e5842324e6d356865485271536d6850587a6c71537a5178636d744b5a3146325a576c5251585a5954323158636a6879534331324d32396665574a495643a4392330',
6
7 # {
8 #   "alg": "ES384",
9 #   "1": -35,
10 #   "content-type": 'h'696d6167652f6a706567',
11 #   "kid": 'h'6469643a6a776b3a65794a72615751694f694a31636d3436615756305a6a707759584a6862584d366232463164476736616e64724c58526f6457316963484a70626e5136633268684c54
49314e6a70324f4735424f5546575a484649624668485a546c525357733465445a315132465654334e6c525646724e456b744c566732554464a535746524969776961335235496a6f6952554d694c
434a6a636e59694f694a514c544d344e434973496d46735a794936496b56544d7a67304969776965434936496d4e425133426e64554a7a656c5535626c3966535774586245684e54475678567a5130
536c51324d30704761464e56556c4e51613249786258647a63586c52626c5a765546395a546c564857444a4d536c464e63576f694c43a35496a6f695a6d7453566b52465a6d67314f46396f5a6c4
514e5749744e5842324e6d356865485271536d6850587a6c71537a5178636d744b5a3146325a576c5251585a5954323158636a6879534331324d32396665574a495643a4392330',
12
13 # 4 : did: jwk:eyJraWQ0Ij1cm46aWV0ZjpwYXJhbW62F1dGg6andRlXRoadW11cHJpbmQ6c2hhLTI1Nj02G580UWFZFIjFmZjZlR1R3W54eDZlQ2FV3N1RVFNeKtLVg2UdDJWFRlRiwiY3R5Tjo1RUMLLC
JjcnY01JOLTMANCiImFszYiG1KVTMz0IiwicCI6ImNB038ndUJzeU5019FSWEbXNHTGVxvz0S1Q2M0p6aFVNUlN0Qz2lXbXZxc3R1b3ZlVUF9ZlVHMDJmLWoiLCJ0Ij01Zm50UkRFRm90F90ZLNQ
NWItcXh02Nm5hRq5mhpXz1q5ZqcmXZ1F2Z1R1QXZlY2ZLXChyS1C2M29FmJ1VC39#0
14 # }
15 # Unprotected Header
16 {
17 # "inclusion-proof": "h'3133312c332c302c3133302c3231362c36342c38382c3332c3235342c37372c33372c313032c35332c3133372c3231332c37322c33342c32372c31322c3
8322c32302c37312c32302c3132352c3132372c32302c3135392c3231352c36382c36302c3130312c3131322c33362c3232352c32302c323232c32332c3135372c3130372c3231362c36342
c38382c33322c37312c39392c3136392c3139392c32392c37392c3133392c3230312c3234312c3231302c313712c3137362c37342c3138372c3130332c33372c36342c3137372c3131392c313932c313
032c3139312c323432c35372c3230302c3136392c332c3137372c35342c3233382c39382c3231332c3837'"
18 # 100 : h'150a839a8f6625008fee139fe8c18fd6da92fbb0a68ec16d6e715912b9d08a11bad914cb08a34620f460e2b14a3566f5b1b3da7494fe7d9405100b54e0b08934ed51f96801522bc85fb3d57a5c2
320352c3132352c3132372c32302c3135392c3231352c36382c36302c3130312c3131322c33362c3232352c32302c323232c32332c3135372c3130372c3231362c36342c38382c33322c3731
2c39392c3136392c3139392c32392c37392c3133392c3230312c3234312c3231302c313712c3137362c37342c3138372c3130332c33372c36342c3137372c3131392c313932c3139312c3234
322c35372c3230302c3136392c332c3137372c35342c3233382c39382c3231332c3837'"
19 # }
20 # Detached Payload
21 # Signature
22 h'150a839a8f6625008fee139fe8c18fd6da92fbb0a68ec16d6e715912b9d08a11bad914cb08a34620f460e2b14a3566f5b1b3da7494fe7d9405100b54e0b08934ed51f96801522bc85fb3d57a5c2
eb6831d94c64fda02fala2c630f90e5'
```

Signed Statement

```
1 # COSE_Sign1
2 18([
3
4 # Protected Header
5 h'a3013822036a696d6167652f6a7065670459017e469643a6a776b3a65794a72615751694f694a31636d3436615756305a6a707759584a6862584d366232463164476736616e64724c58526f6457316963484a70626e513663326868
4c5449314e6a70324f4735424f5546575a484649624668485a546c525357733465445a315132465654334e6c525646724e456b744c566732554464a535746524969776961335235496a6f6952554d
694c434a6a636e59694f694a514c544d344e434973496d46735a794936496b56544d7a67304969776965434936496d4e425133426e64554a7a656c5535626c3966535774586245684e54475678567a
5130536c51324d30704761464e56556c4e51613249786258647a63586c52626c5a765546395a546c564857444a4d536c464e63576f694c43a35496a6f695a6d7453566b52465a6d67314f46396f5a6c4
6c4e514e5749744e5842324e6d356865485271536d6850587a6c71537a5178636d744b5a3146325a576c5251585a5954323158636a6879534331324d32396665574a495643a4392330',
6
7 # {
8 #   "alg": "ES384",
9 #   "1": -35,
10 #   "content-type": 'h'696d6167652f6a706567',
11 #   "kid": 'h'6469643a6a776b3a65794a72615751694f694a31636d3436615756305a6a707759584a6862584d366232463164476736616e64724c58526f6457316963484a70626e5136633268684c54
49314e6a70324f4735424f5546575a484649624668485a546c525357733465445a315132465654334e6c525646724e456b744c566732554464a535746524969776961335235496a6f6952554d694c
434a6a636e59694f694a514c544d344e434973496d46735a794936496b56544d7a67304969776965434936496d4e425133426e64554a7a656c5535626c3966535774586245684e54475678567a5130
536c51324d30704761464e56556c4e51613249786258647a63586c52626c5a765546395a546c564857444a4d536c464e63576f694c43a35496a6f695a6d7453566b52465a6d67314f46396f5a6c4
514e5749744e5842324e6d356865485271536d6850587a6c71537a5178636d744b5a3146325a576c5251585a5954323158636a6879534331324d32396665574a495643a4392330',
12
13 # 4 : did: jwk:eyJraWQ0Ij1cm46aWV0ZjpwYXJhbW62F1dGg6andRlXRoadW11cHJpbmQ6c2hhLTI1Nj02G580UWFZFIjFmZjZlR1R3W54eDZlQ2FV3N1RVFNeKtLVg2UdDJWFRlRiwiY3R5Tjo1RUMLLC
JjcnY01JOLTMANCiImFszYiG1KVTMz0IiwicCI6ImNB038ndUJzeU5019FSWEbXNHTGVxvz0S1Q2M0p6aFVNUlN0Qz2lXbXZxc3R1b3ZlVUF9ZlVHMDJmLWoiLCJ0Ij01Zm50UkRFRm90F90ZLNQ
NWItcXh02Nm5hRq5mhpXz1q5ZqcmXZ1F2Z1R1QXZlY2ZLXChyS1C2M29FmJ1VC39#0
14 # }
15 # Unprotected Header
16 {
17 # "content-type": 'h'696d6167652f6a706567',
18 # Detached Payload
19
20 # Signature
21 h'aF4f2c641ef13fad47fdb2929fd2c9551e0068e89b85376a960c9253c8f0457afeb8580e05b0a42be7aec458f4d9d7bc9c61224237f94273d7898331ec96c560524fa0ab877cbe3cb11870fc21
bec63e74388a0eb636d3326cf90118e'
```

Statement

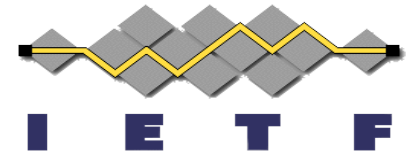
# Profiling CoMETRE



- First addition to “verifiable data structures”:
  - Confidential Computing Framework (CCF) Tree Algorithm
  - Base CDDL:

```
Receipt = [  
  version: int,  
  ts_identifier: tstr,  
  proof: SignedMerkleTreeProof  
]
```

# CCF Profiling CDDL



```
CCF-leaf = [  
  internal-hash: bstr ; a string of HASH_SIZE bytes;  
  internal-data: bstr; a string of at most 1024 bytes; and  
  data_hash: bstr ; the serialization of the element stored at this leaf.  
]
```

```
CCF-inclusion-proof: [+ proof-element],
```

```
proof-element = [  
  left: bool
```

```
  hash: bstr
```

```
]
```

# Next Steps

- Adoption Time?
- Profit!

