COSE Receipts

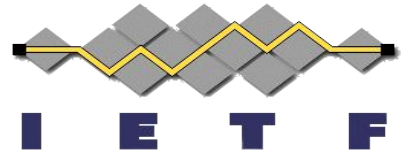
formerly known as:
Concise Encoding of Signed Merkle Tree Proofs (CoMETRE)

draft-ietf-cose-merkle-tree-proofs

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

IETF 119, Brisbane
March 19, 2024

What Does It Do?



- Enables a “kind of counter signature”, that includes the ability to provide addition proof types
  - Proof of Inclusion
  - Proof of Consistency
  - Proof of Non Inclusion

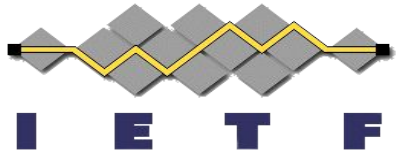
Why Do It?

- SCITT needed it.
- Enables COSE interoperability for use cases such as:
  - Supply Chain Transparency
  - Key Transparency

Status

- Recently published -04:
  - Changes to the abstract … not limited to merkle trees.
  - Changes to COSE registry structure…
    - Like COSE Key and COSE Key Params
  - Updates to the IANA registry requests

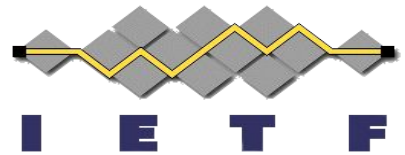
Example: SCITT Transparent Statement




```
18(                                 / COSE Sign 1                    /
    [
      h'a4012603...6d706c65',       / Protected                      /
      {                             / Unprotected                    /
        394: [                      / Receipts (1)                   /
          h'd284586c...4191f9d2'    / Receipt 1                      /
        ]
      },
      nil,                          / Detached payload               /
      h'79ada558...3a28bae4'        / Signature                      /
    ]
)
```

394 to be registered by SCITT Architecture
… should it be registered by this draft instead?

Example: SCITT Receipt



```
18(                                   / COSE Sign 1                    /
    [
      h'a4012604...6d706c65',         / Protected                      /
      {                               / Unprotected                    /
        -222: {                       / Proofs                         /
          -1: [                       / Inclusion proofs (1)           /
            h'83080783...32568964', / Inclusion proof 1                /
          ]
        },
      },
      nil,                            / Detached payload               /
      h'10f6b12a...4191f9d2'          / Signature                      /
    ]
)
/ Decoded Protected /
{                                   / Protected                      /
  1: -7,                            / Algorithm                      /
  4: h'50685f55...50523255',        / Key identifier                 /
  -111: 1,                          / Verifiable Data Structure      /
  15: {                             / CWT Claims                     /
    1: transparency.vendor.example, / Issuer                         /
    2: vendor.product.example,      / Subject                        /
  }
}
```

Next Steps

- Consistency Proofs need feedback on design.
  - https://github.com/cose-wg/draft-ietf-cose-merkle-tree-proofs/issues/13
- Request early allocation of COSE Header Parameters?
  - https://github.com/cose-wg/draft-ietf-cose-merkle-tree-proofs/issues/15
- Request early directorate reviews?
  - https://github.com/cose-wg/draft-ietf-cose-merkle-tree-proofs/issues/16
- ….WGLC by IETF 120 ?