COSE Receipts

draft-ietf-cose-merkle-tree-proofs

Orie Steele
IETF 120 Vancouver
23 July 2024

What does a Receipt do?

- Enables COSE to express proof types for **Verifiable Data Structures (VDS)**
- What's a VDS?
- Examples include:
  - Transparency Logs (Merkle Trees, etc)
  - Signed Inclusion Proofs (Receipts)
  - Signed Consistency Proofs (Checkpoints)

Signature with Receipts

```
18(                                 / COSE Sign 1                   /
    [
      h'a4012603...6d706c65',       / Protected                     /
      {                             / Unprotected                   /
        394: [                      / Receipts (2)                  /
          h'd284586c...4191f9d2'    / Receipt 1                     /
          h'c624586c...8f4af97e'    / Receipt 2                     /
        ]
      },
      nil,                          / Detached Payload              /
      h'79ada558...3a28bae4'        / Signature                     /
    ]
)
```


IETF

What do Receipts look like?

```
18([
  <<{
    1: -7, / Signed with ES256 /
    395: 1 / Stored in RFC9162_SHA256 Verifiable Data Structure /
  }>>,
  {
    396: { / Proofs /
      -1: [ / Inclusion Proof /
        <<[
          4, / Entries in the Log   /
          1, / Index of Entry /
          [  / Inclusion Path       /
            h'8aba0…4fdb8c4d',
            h'6c6c9…9051ac00'
          ]
        ]>>
      ]
    }
  },
  null,                  / Detached Payload /
  h'43b3b2fb…842613f03' / Signature /
])
```


IETF

CT style inclusion proofs

```
inclusion-proof = bstr .cbor [

    ; tree size at current merkle root
    tree-size: int

    ; index of leaf in tree
    leaf-index: int

    ; path from leaf to current merkle root
    inclusion-path: [ + bstr ]
]
```


IETF

Receipts = Signed Inclusion Proof

```
protected-header-map = {
  &(alg: 1) => int   ; Signature Algorithm
  &(vds: 395) => int ; Transparency Algorithm
  ; …
}

unprotected-header-map = {
  &(vdp: 396) => verifiable-proofs
  ; …
}

verifiable-proofs = {
  &(inclusion-proof: -1) => inclusion-proofs
}
```

Anatomy of a Receipt

```
18(                                 / COSE Sign 1                    /
    [
      h'a4012604...6d706c65',       / Protected                      /
      {                             / Unprotected                    /
        396: {                      / Proofs                         /
          -1: [                     / Inclusion proofs (1)           /
            h'83080783...32568964', / Inclusion proof 1              /
          ]
        },
      },
      nil,                          / Detached payload               /
      h'2e34df43...8d74d55e'        / Signature                      /
    ]
)
```


IETF

Why do it?

- SCITT Transparency Services needed it
  - Prove that a binary was included in an **append-only log**
  - Assert that policies were applied at the time the binary was included (**registered** in the VDS)

Status

- Recently published -05:
  - Need to request Early Allocations from IANA
  - Need to address Robin’s review

Next Steps

- Request WGLC?