linaro™ Arm Solutions at Lightspeed

EAT Profile for Device Attestation

Mathieu Poirier
Thomas Fossati

This Presentation

1. Some introduction material
2. The presentation of the EAT Profile
3. An example of how the EAT Profile fits in the bigger picture on Arm
4. Remaining work and open questions

Some Details

Currently 7 (short) CDDL files

Concise Data Definition Language (CDDL)

GitHub: https://github.com/rats-device-attestation/draft-poirier-rats-eat-da

Data Tracker: https://datatracker.ietf.org/doc/html/draft-poirier-rats-eat-da

EAT Profile for Device Attestation

Goals and Motivations:

- About formalizing the representation of claims generated by devices
- Architecture agnostic → SPDM and TDISP are the same regardless of architecture
- Simple representation of the information yielded by SPDM - nothing more, nothing less
- Targeted scenarios: CMA and Confidential Computing
- Linaro has no commercial gain in this specification

The Specification

spdm-claims.cddl:

```
da-token = {
  &(eat_profile: 265) => "tag:linaro.org,2025:device#1.0.0"
  &(eat_nonce: 10) => bytes .size 64
  &(eat_submods: 266) => {
    + device-name => $device-claims-set
  }
}

device-name = text .regexp "dev-[A-Za-z0-9]+"

$device-claims-set /= spdm-claims
$device-claims-set /= cxl-claims
$device-claims-set /= chi-claims
$device-claims-set /= pcie-legacy-claims
```

The Specification

pci-legacy-claims.cddl

```
pcie-legacy-claims = {
 &(eat_profile: 265) => "tag:linaro.org,2025:device-pcie-legacy#1.0.0"
 &(legacy-header: 3805) => pcie-type-0-1-config-space
 ? $$pcie-legacy-claim-extension
}

pcie-type-0-1-config-space = {
  &(vendorID: 1) => bytes .size 2
  &(deviceID: 2) => bytes .size 2
  ? &(command: 3) => bytes .size 2
  ? &(status: 4) => bytes .size 2
  ? &(revisionID: 5) => bytes .size 1
  ? &(classCode: 6) => bytes .size 3
  ? &(cacheLineSize: 7) => bytes .size 1
  ? &(latencyTimer: 8) => bytes .size 1
  ? &(headerType: 9) => bytes .size 1
  ? &(BITS: 10) => bytes .size 1
}
```

spdm-claims.cddl

```
spdm-claims = {
  &(eat_profile: 265) => "tag:linaro.org,2025:device-spdm#1.0.0"
  spdm-artefacts
  ? &(vca: 3804) => bytes
}

spdm-artefacts //= (
  &(measurements: 3802) => spdm-measurements
  &(certificates: 3803) => spdm-certificates
)

spdm-artefacts //= (
  &(measurements: 3802) => spdm-measurements
)

spdm-artefacts //= (
  &(certificates: 3803) => spdm-certificates
)
```

The Specification

spdm-certificates.cddl

```
spdm-certificates = {
  default-cert-slot => cert-chain
  ? aux-cert-slots => cert-chain
}

; ASN.1 DER-encoded certificates concatenated with no intermediate
; padding.
cert-chain = bytes

default-cert-slot = 0
aux-cert-slots = 1..7
```

spdm-measurements.cddl

```
spdm-measurements = {
  + block-id => spdm-measurement
  ? "signature" => spdm-measurement-blocks-signature
}

block-id = 1..239
```

The Specification

spdm-measurement.cddl

```
spdm-measurement = {
  &(component-type: 1) => component-type
  measurement
}

measurement //= ( &(digest-measurement: 2) => digest-measurement )
measurement //= ( &(raw-measurement: 3) => raw-measurement )

component-type /= &(immutable-rom: 0)
component-type /= &(mutable-firmware: 1)
...
component-type /= &(informational: 9)
component-type /= &(structured-measurement-manifest: 10)

raw-measurement = bytes
digest-measurement = digest
digest = [
  alg: uint / text
  val: bytes
]
```

The Specification

spdm-measurement-block-signature.cddl

```
hash-algorithm-type /= &(tpm_alg_sha_256: 0)
hash-algorithm-type /= &(tpm_alg_sha_384: 2)
...
hash-algorithm-type /= &(tpm_alg_sm3_256: 64)

spdm-measurement-blocks-signature = {
  &(slot: 1) => 0..7, ; Slot of the certificate chain used to
                      ; authenticate the measurement.  Default
                      ; should be 0.
  &(requester-nonce: 2) => bytes .size 32,
  &(responder-nonce: 3) => bytes .size 32,
  &(combined-spdm-prefix: 4) => bytes .size 100,
  &(IL1: 5) => bytes, ; L1 (see comment on the right)
  &(base-hash-algo: 6) => hash-algorithm-type,
  &(signature: 7) => bytes
}
```

```
;
; See signature generation and verification algorithms for
; MEASUREMENTS messages on page 126.
;
; L1 = Concatenate(VCA, GET_MEASUREMENTS_REQUEST1,
;                  MEASUREMENTS_RESPONSE1, ...,
;                  GET_MEASUREMENTS_REQUESTn-1,
;                  MEASUREMENTS_RESPONSEn-1,
;                  GET_MEASUREMENTS_REQUESTn,
;                  MEASUREMENTS_RESPONSEn)
;
```

```
{
  "__cmwc_t": "tag:github.com,2025:veraison/ratsd/cmw",
```

```
01  "tsm": [
02    "application/vnd.veraison.tsm-report+cbor"',
03    <<
04      / CCA Token /
05      399({
06        / realm token /
07        44241: << 18([
08          << {1: -35} >>,
09          {},
10          << {10: h'D4ACABFA...', ... } >>,
11          h'5190…'
12      ]),
13     / platform token /
14      44234: << 18([...]) >>
15     })
16   >>
17  ],
```

```
  "dev": [
    'application/eat-ucs+cbor;
eat_profile="tag:linaro.org,2025:device#1.0.0"',
 01    << {
 02     / eat_profile / 265: "tag:linaro.org,2025:device#1.0.0",
 03      / eat_nonce / 10: h'D4ACABFA...',
 04     / submod / 266: {
 05       "/sys/devices/pci0000:00/0000:00:00.0": { / spdm-claims /
 06        / eat_profile / 265:"tag:linaro.org,2025:device-spdm#1.0.0",
 07          / spdm-measurements / 3802: {
 08           / block-id 1 / 1: {
 09              / component type / 1: 0, / immutable ROM /
 10             / digest measurement / 2: [ 1, h'8D531D77...' ]
 11            },
 12           / block-id 2 / 2: {
 13              / component type / 1: 1, / mutable FW /
 14              / digest measurement / 2: [ 1, h'9EFFD8A6...' ]
 15            },
 16           / block-id 3 / 3: {
 17              / component type / 1: 2, / HW config /
 18              / digest measurement / 2: [ 1, h'FFDE4248...' ]
 19            }
 20         },
 21          / spdm-certificates / 3803: {
 22            / default-cert-slot / 0: h'308201D4...' / cert chain /
 23          }
 24       }
 25     }
 26   } >>
 27 ]
}
```

```
{
  "__cmwc_t": "tag:github.com,2025:veraison/ratsd/cmw",
```

```
"tsm": [
    "application/vnd.veraison.tsm-report+cbor"',
    <<
      / CCA Token /
      399({
        / realm token /
        44241: << 18([
          << {1: -35} >>,
          {},
          << {10: h'D4ACABFA...', ... } >>,
          h'5190…'
      ]),
      / platform token /
      44234: << 18([...]) >>
    })
    >>
  ],
```

```
"dev": [
    'application/eat-ucs+cbor;
eat_profile="tag:linaro.org,2025:device#1.0.0"',
    << {
      / eat_profile / 265: "tag:linaro.org,2025:device#1.0.0",
      / eat_nonce / 10: h'D4ACABFA...',
      / submod / 266: {
        "/sys/devices/pci0000:00/0000:00:00.0": { / spdm-claims /
          / eat_profile / 265: "tag:linaro.org,2025:device-spdm#1.0.0",
          / spdm-measurements / 3802: {
            / block-id 1 / 1: {
              / component type / 1: 0, / immutable ROM /
              / digest measurement / 2: [ 1, h'8D531D77...' ]
            },
            / block-id 2 / 2: {
              / component type / 1: 1, / mutable FW /
              / digest measurement / 2: [ 1, h'9EFFD8A6...' ]
            },
            / block-id 3 / 3: {
              / component type / 1: 2, / HW config /
              / digest measurement / 2: [ 1, h'FFDE4248...' ]
            }
          },
          / spdm-certificates / 3803: {
            / default-cert-slot / 0: h'308201D4...' / cert chain /
          }
        }
      }
    } >>
  ]
}
```

```
{
  "__cmwc_t": "tag:github.com,2025:veraison/ratsd/cmw",

  "tsm": [
    "application/vnd.veraison.tsm-report+cbor"',
    <<
      / CCA Token /
      399({
        / realm token /
        44241: << 18([
          << {1: -35} >>,
          {},
          << {10: h'D4ACABFA...', ... } >>,
          h'5190...'
        ]),
        / platform token /
        44234: << 18([...]) >>
      })
    >>
  ],

  "dev": [
    'application/eat-ucs+cbor; eat_profile="tag:linaro.org,2025:device#1.0.0"',
    << {
      / eat_profile / 265: "tag:linaro.org,2025:device#1.0.0",
      / eat_nonce / 10: h'D4ACABFA...',
      / submod / 266: {
        "/sys/devices/pci0000:00/0000:00:00.0": { / spdm-claims /
          / eat_profile / 265: "tag:linaro.org,2025:device-spdm#1.0.0",
          / spdm-measurements / 3802: {
            / block-id 1 / 1: {
              / component type / 1: 0, / immutable ROM /
              / digest measurement / 2: [ 1, h'8D531D77...' ]
            },
            / block-id 2 / 2: {
              / component type / 1: 1, / mutable FW /
              / digest measurement / 2: [ 1, h'9EFFD8A6...' ]
            },
            / block-id 3 / 3: {
              / component type / 1: 2, / HW config /
              / digest measurement / 2: [ 1, h'FFDE4248...' ]
            }
          },
          / spdm-certificates / 3803: {
            / default-cert-slot / 0: h'308201D4...' / cert chain /
          }
        }
      }
    } >>
  ]
}
```

Remaining Work

Add support for “spdm-challenge”:

- Very similar to the specification in spdm-measurement-blocks-signature.cddl
- Allows this specification to be used for CMA scenarios

Introduce support for new bus technology when needed:

- “cxl-claims”, “chi-claims”

Add a section to describe how the EAT Profile for Device Attestation binds with the CCA Attestation Token

- We want other architectures to do the same

Open Questions

How do we keep up with upcoming versions of the SPDM specification?

Is there a need to describe TDISP artefacts?

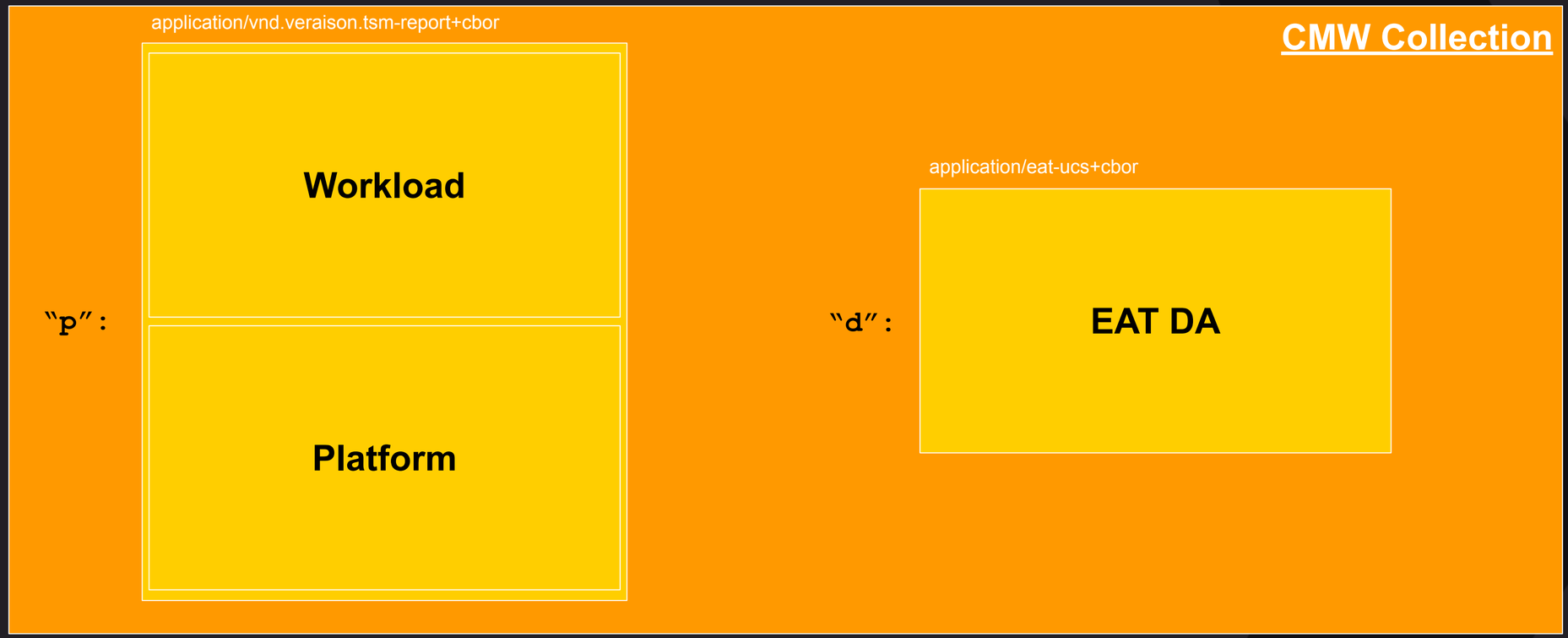
The only one that would make sense is the Interface Report but very HW oriented

Can you use this specification? If not, what needs to change?

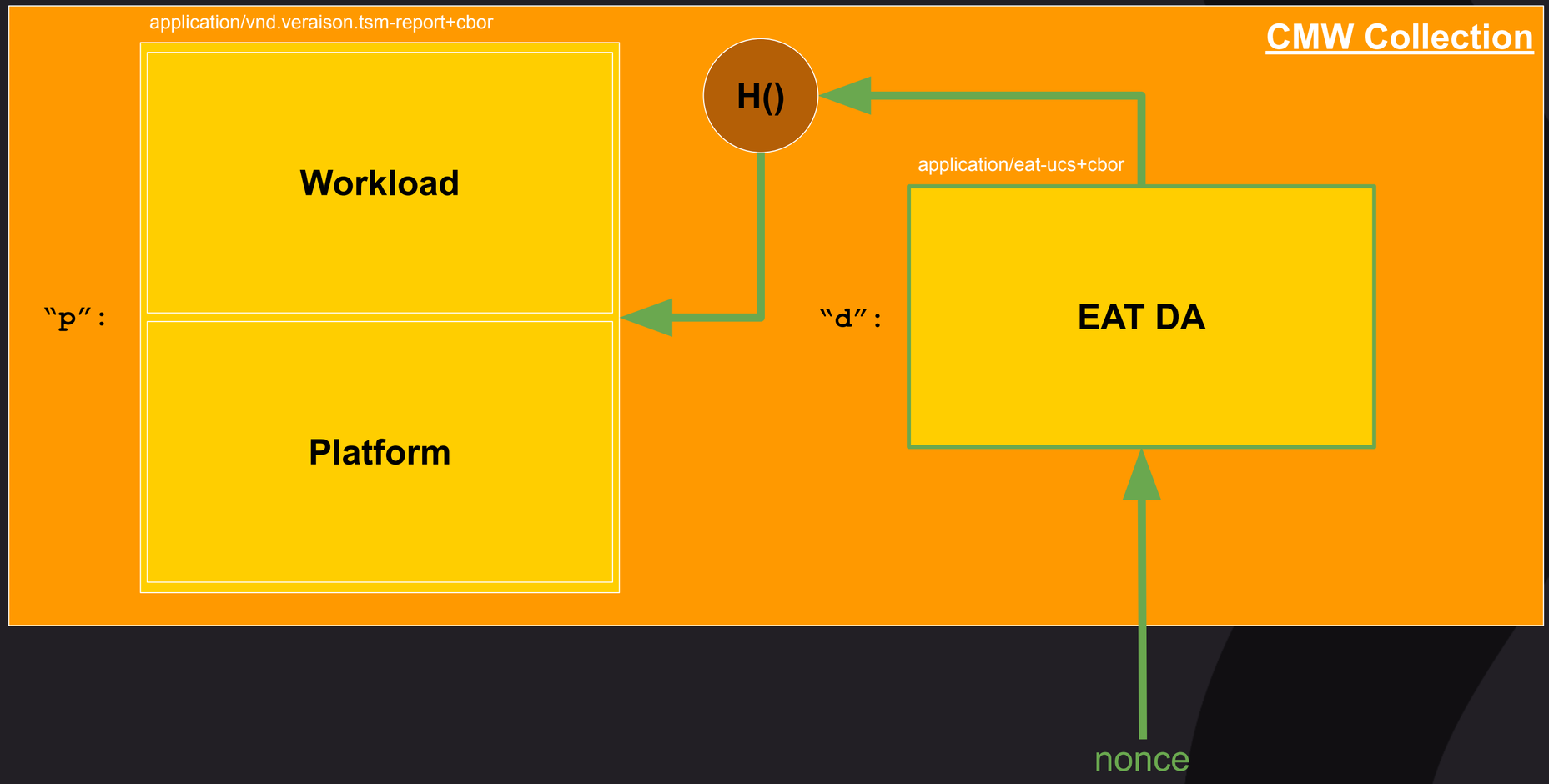
Backup

How to Combine the Pieces

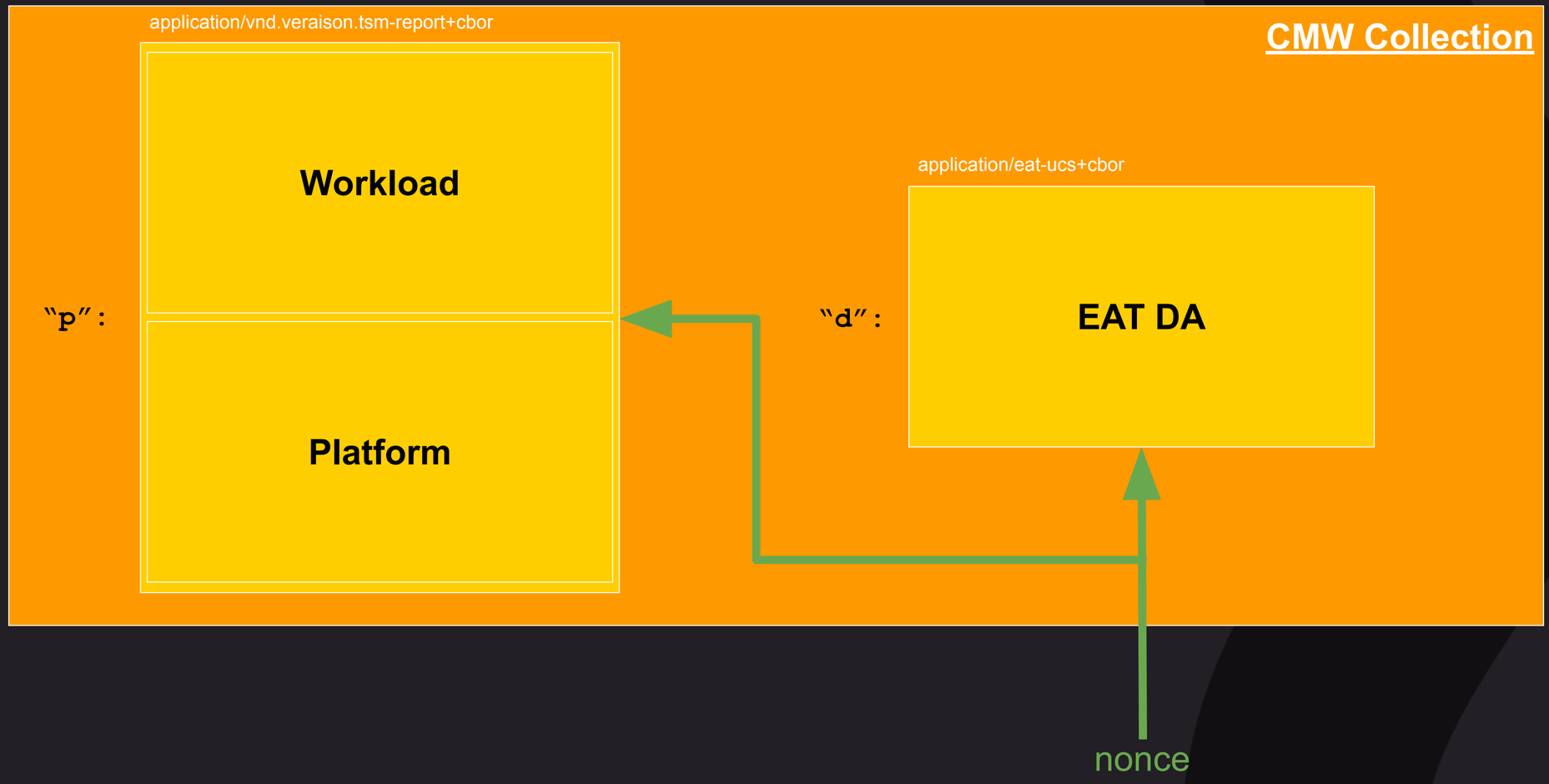
Composition



Binding (Hash Lock)



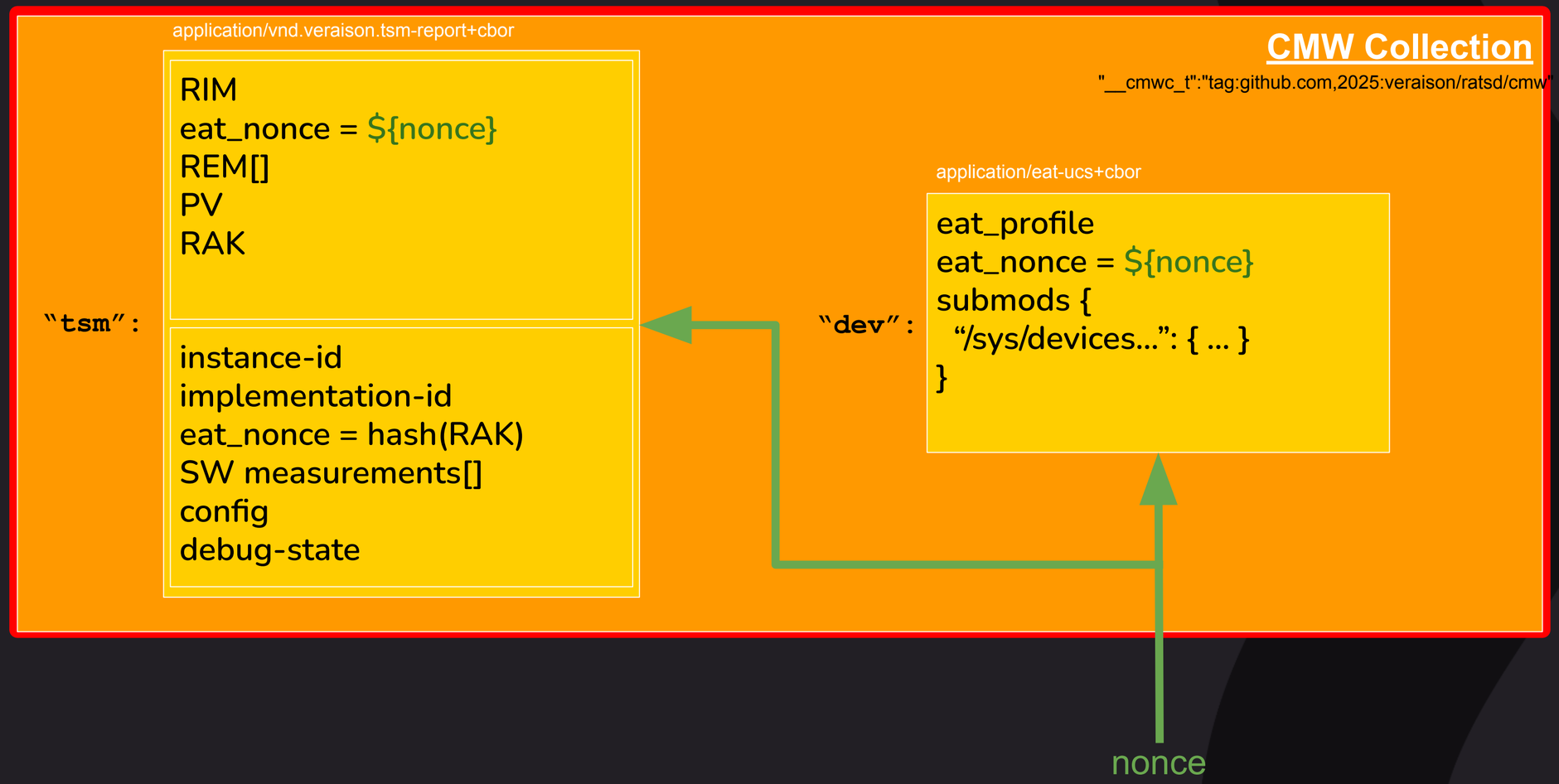
Binding (Nonce Fan-out)



Sealing

Lead attester signs the CMW collection

Prototype (ratsd)



Lead attester signs the CMW collection

```
{
  "__cmwc_t": "tag:github.com,2025:veraison/ratsd/cmw",

  "tsm": [
    "application/vnd.veraison.tsm-report+cbor"',
    <<
      / CCA Token /
      399({
        / realm token /
        44241: << 18([
          << {1: -35} >>,
          {},
          << {10: h'D4ACABFA...', ... } >>,
          h'5190...'
        ]),
        / platform token /
        44234: << 18([...]) >>
      })
    >>
  ],

  "dev": [
    'application/eat-ucs+cbor; eat_profile="tag:linaro.org,2025:device#1.0.0"',
    << {
      / eat_profile / 265: "tag:linaro.org,2025:device#1.0.0",
      / eat_nonce / 10: h'D4ACABFA...',
      / submod / 266: {
        "/sys/devices/pci0000:00/0000:00:00.0": { / spdm-claims /
          / eat_profile / 265: "tag:linaro.org,2025:device-spdm#1.0.0",
          / spdm-measurements / 3802: {
            / block-id 1 / 1: {
              / component type / 1: 0, / immutable ROM /
              / digest measurement / 2: [ 1, h'8D531D77...' ]
            },
            / block-id 2 / 2: {
              / component type / 1: 1, / mutable FW /
              / digest measurement / 2: [ 1, h'9EFFD8A6...' ]
            },
            / block-id 3 / 3: {
              / component type / 1: 2, / HW config /
              / digest measurement / 2: [ 1, h'FFDE4248...' ]
            }
          },
          / spdm-certificates / 3803: {
            / default-cert-slot / 0: h'308201D4...' / cert chain /
          }
        }
      }
    } >>
  ]
}
```