Remote ATtestation ProcedureS
Internet-Draft
Intended status: Informational
Expires: 26 September 2026

M. Poirier
T. Fossati
Linaro

25 March 2026

An EAT Profile for Trustworthy Device Assignment
draft-poirier-rats-eat-da-06

Abstract

In confidential computing, device assignment (DA) is the method by which a device (e.g., network adapter, GPU), whether on-chip or behind a PCIe Root Port, is assigned to a Trusted Virtual Machine (TVM). For the TVM to trust an assigned device, the device must provide the TVM with attestation Evidence confirming its identity and the state of its firmware and configuration.

Since Evidence claims can be processed by 3rd party entities (e.g., Verifiers, Relying Parties) external to the TVM, there is a need to standardize the representation of DA-related information in Evidence to ensure interoperability. This document defines an attestation Evidence format for DA as an EAT (Entity Attestation Token) profile.

About This Document

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

The latest revision of this draft can be found at https://rats-device-attestation.github.io/draft-poirier-rats-eat-da/draft-poirier-rats-eat-da.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-poirier-rats-eat-da/.

Discussion of this document takes place on the Remote ATtestation ProcedureS Working Group mailing list (mailto:rats@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/rats/. Subscribe at https://www.ietf.org/mailman/listinfo/rats/.

Source for this draft and an issue tracker can be found at https://github.com/rats-device-attestation/draft-poirier-rats-eat-da.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Copyright Notice

Table of Contents

1. Introduction

In confidential computing, device assignment (DA) is the method by which a device (e.g., network adapter, GPU), whether on-chip or behind a PCIe Root Port, is assigned to a Trusted Virtual Machine (TVM). Most confidential computing platforms (e.g., Arm CCA, AMD SEV-SNP, Intel TDX) provide DA capabilities. Such capabilities prevent execution environments or software components that are untrusted by the TVM (including other TVMs and the host hypervisor) from accessing or controlling a device that has been assigned to the TVM. This includes, for example, protection of device MMIO interfaces and device caches. From a trust perspective, DA allows a device to be included in the TVM's Trusted Computing Base (TCB). For the TVM to trust the device, the device must provide the TVM with attestation Evidence confirming its identity and the state of its firmware and configuration.

This document defines an attestation Evidence format for DA as an EAT [RFC9711] profile. The format is designed to be generic, extensible and architecture-agnostic. Ongoing work on DA concentrates on PCIe devices that support the SPDM protocol [SPDM], but other bus architectures and protocols are expected to be supported as the technology gains wider adoption. As such, this document focuses on the formalization of an Evidence format for SPDM-compliant devices while leaving room for the definition of other Evidence formats such as Compute Express Link (CXL) and the Coherent Hub Interface (CHI). This list is by no means exhaustive and is expected to expand.

2. Conventions and Definitions

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.

3. Device Assignment Token (DAT) Claims

The Device Assignment Token (DAT) is the encompassing envelope for the individual device claims to be presented. A DAT can be used as a standalone entity but can also be embedded in a larger, platform-specific attestation token. A DAT consists of an EAT profile identifier, a nonce and an EAT submodule (Section 4.2.18 of [RFC9711]) that contains any number of individual device claims. Each individual device claim is the combination of a device name and a standard claims format based on the bus or protocol the device supports. The syntax of the device name depends on the type of bus or protocol used. Each name consists of two parts joined by a semicolon: a namespace and a bus-specific name. See Section 3.1.5 for SPDM devices, and Section 3.2.1 for legacy PCIe devices. As previously mentioned, this draft currently defines the claims set for SPDM compliant devices and PCIe legacy devices that do not support the SPDM protocol. Careful condideration was also given to the overall design in order to leave room for future expansion.

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

device-name = text .regexp "(legacy-pcie|spdm):.+"

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

3.1. SPDM Claims

A SPDM claim instance is expected to be present for each SPDM compatible device to be attested. Each instance consists of a measurements section, a certificates section, or both. These can be supplemented with an additional section that contains information from the TEE Device Information Security Protocol (TDISP) Device Interface Report. TDISP messages are embedded in the VENDOR_DEFINED_REQUEST and VENDOR_DEFINED_RESPONSE messages of the SPDM protocol. Optionally, the Negotiated State preamble (version, capabilities and algorithms) bytes can be included to present the full negotiated state between the SPDM requester and responder.

```
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
  ? &(device-interface-report: 3807) => tdisp-device-interface-report
)

spdm-artefacts //= (
  &(measurements: 3802) => spdm-measurements
  ? &(device-interface-report: 3807) => tdisp-device-interface-report
)

spdm-artefacts //= (
  &(certificates: 3803) => spdm-certificates
  ? &(device-interface-report: 3807) => tdisp-device-interface-report
)
```

3.1.1. Measurements Claim

There can be up to 239 measurements per device with the entire measurement log optionally signed by the certificate populated in one of the 8 certificate slots. It should be noted that measurements formalized herein follow the DMTF measurement specification.

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

block-id = 1..239
```

3.1.1.1. Measurement

SPDM measurements start with a component type that reflects one of the 10 categories defined by the SPDM specification. Following is the measurement itself represented by either a raw bitstream or a digest. The size of the digest value is derived from the measurement hash algorithm conveyed by the SPDM ALGORITHMS message response.

```
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 /= &(hardware-config: 2)
component-type /= &(firmware-config: 3)
component-type /= &(freeform-measurement-manifest: 4)
component-type /= &(device-mode: 5)
component-type /= &(mutable-firmware-version: 6)
component-type /= &(mutable-firmware-svn: 7)
component-type /= &(hash-extend-measurement: 8)
component-type /= &(informational: 9)
component-type /= &(structured-measurement-manifest: 10)

raw-measurement = bytes
digest-measurement = digest

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

3.1.1.2. Measurements Signature

SPDM compliant devices can optionally support the capability to sign measurements. Included in the measurement claim signature are all the elements needed by a third party entity to reconstruct the original measurement log signed by the device. Those elements include L1 (see CDDL below), the combined SPDM prefix, the hash algorithm used to generate a digest of the measurement log and nonces provided by the requester and responder. The slot number of the leaf certificate used to sign the measurement log is also provided.

```
   ;
   ; What follows is based on SPDM v1.3.2 (DSP0274_1.3.2.pdf)
   ;

   ;
   ; Algorithms currently supported by SPDM.
   ; See "MeasurementHashAlgo", table 21, page 79.
   ;
   hash-algorithm-type /= &(tpm_alg_sha_256: 0)
   hash-algorithm-type /= &(tpm_alg_sha_384: 2)
   hash-algorithm-type /= &(tpm_alg_sha_512: 4)
   hash-algorithm-type /= &(tpm_alg_sha3_256: 8)
   hash-algorithm-type /= &(tpm_alg_sha3_384: 16)
   hash-algorithm-type /= &(tpm_alg_sha3_512: 32)
   hash-algorithm-type /= &(tpm_alg_sm3_256: 64)

   ;
   ; 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)
   ;
   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 above)
      &(base-hash-algo: 6) => hash-algorithm-type,
      &(signature: 7) => bytes
   }
```

3.1.2. Certificate Claims

According to the specification, SPDM compliant devices should support at most 8 slots, with slot 0 populated by default. Slot 0 SHALL contain a certificate chain that follows the Device certificate model or the Alias certificate model. Regardless of the certificate model used, a certificate chain comprises one or more DER-encoded X.509 v3 certificates [RFC5280]. The certificates MUST be concatenated with no intermediate padding.

```
spdm-certificates = {
  default-cert-slot => cert-chain
  ? aux-cert-slot-1 => cert-chain
  ? aux-cert-slot-2 => cert-chain
  ? aux-cert-slot-3 => cert-chain
  ? aux-cert-slot-4 => cert-chain
  ? aux-cert-slot-5 => cert-chain
  ? aux-cert-slot-6 => cert-chain
  ? aux-cert-slot-7 => cert-chain
}

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

default-cert-slot = 0

aux-cert-slot-1 = 1
aux-cert-slot-2 = 2
aux-cert-slot-3 = 3
aux-cert-slot-4 = 4
aux-cert-slot-5 = 5
aux-cert-slot-6 = 6
aux-cert-slot-7 = 7
```

3.1.3. TDISP Device Interface Report

A TDISP Device Interface Report begins with various bitfields indicating the state and characteristics of the PCIe device interface. Next are 3 register fields pertaining to MSI-X (Message Signalled Interrupts), LNR (Lightweight Notification Requester) and TPH (TLP Processing Hints) capabilities. MMIO ranges are assigned from PCIe BAR(s) and provide information about the memory areas a device is working with. More information on the MMIO range bitfields and the ones defined as part of the device interface field (above) can be found in the TDISP section of the PCI Express specification. The last field is device-specific and optionally included to convey additional configuration information about the device.

```
tdisp-device-interface-report = {
  ? &(interface-info: 1) => interface-info-bits
  ? &(msi-x-message-control: 2) => bytes .size 2
  ? &(lnr-control: 2) => bytes .size 2
  ? &(tph-control: 3) => bytes .size 4
  ? &(mmio-ranges: 4) => mmio-ranges
  ? &(device-specific-info: 5) => bytes
}

interface-info-bits = bytes .bits interface-info-flags
interface-info-flags = &(bit0: 0,
                         bit1: 1,
                         bit2: 2,
                         bit3: 3,
                         bit4: 4,
                         bit5: 5,
                        )

mmio-ranges = {
  + &(mmio-range: 1) => mmio-range
}

mmio-range = {
  &(first-4k-page: 1) => bytes .size 8
  &(number-of-4k-pages: 2) => bytes .size 4
  &(attributes: 3) => range-attributes
}

range-attributes = {
  &(range-attribute-bits: 1) => range-attribute-bits
  &(range-attribute-range-id: 2) => bytes .size 2
}

range-attribute-bits = bytes .bits range-attributes-flags
range-attributes-flags = &(bit0: 0,
                           bit1: 1,
                           bit2: 2,
                           bit3: 3,
                          )
```

3.1.4. Negotiated State Preamble (Version, Capabilities and Algorithms)

The Negotiated State Preamble (i.e., vca) claim contains the concatenation of messages GET_VERSION, VERSION, GET_CAPABILITIES, CAPABILITIES, NEGOTIATE_ALGORITHMS, and ALGORITHMS last exchanged between the SPDM Requester and Responder.

3.1.5. Submodule Naming

The namespace used for SPDM submodules is "spdm".

The name associated with an SPDM submodule is extracted from the leaf certificate of the relevant device.

* If the leaf certificate contains a Subject Alternative Name of type DMTFOtherName, the submodule name is the value contained in ub-DMTF-device-info. For example: "spdm:ACME:WIDGET:0123456789".

* Otherwise, the submod name is the string representation of the certificate Subject, as described in [RFC4514]. For example: "spdm:C=CA,O=ACME,OU=Widget,CN=0123456789".

3.2. PCIe Legacy Device Claims

The definition of a device claims set for PCIe legacy devices that do not implement the extensions needed to attest for their provenance and configuration is provided, making it is possible to keep using current assets as secures ones are being provisioned. This legacy device claims set simply mirrors the type 0/1 common registers of the PCIe configuration space, mandating only that the vendor and device identification code be provided. Other fields of the configuration space header may optionally be included should they add value. A binary format of the PCIe configuration space is made available for processing by existing PCIe configuration space tools. Implementers may optionally choose to include both text and binary versions should there be a use case to support this representation.

```
   =============== NOTE: '\' line wrapping per RFC 8792 ================

   pcie-legacy-claims = {
     &(eat_profile: 265) => "tag:linaro.org,2025:device-pcie-legacy#1.0\
                                                                    .0"
     pcie-legacy-artefacts
     ? $$pcie-legacy-claim-extension
   }


   pcie-legacy-artefacts //= (
     &(artefacts-text: 3805) => pcie-type-0-1-config-space-text
     &(artefacts-bytes: 3806) => pcie-type-0-1-config-space-bytes
   )

   pcie-legacy-artefacts //= (
     &(artefacts-text: 3805) => pcie-type-0-1-config-space-text
   )

   pcie-legacy-artefacts //= (
     &(artefacts-bytes: 3806) => pcie-type-0-1-config-space-bytes
   )

   pcie-type-0-1-config-space-bytes = bytes .size 256

   pcie-type-0-1-config-space-text = {
     &(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
   }
```

3.2.1. Submodule Naming

The namespace used for legacy PCIe submodules is "legacy-pcie".

The name is any arbitrary string chosen by the implementation. For example, "legacy-pcie:0000:01:02.0" where "0000" is the domain, "01" the PCI bus id, "02" the device on the bus and "0" the device function.

4. Collated CDDL

```
================ NOTE: '\' line wrapping per RFC 8792 ================

dat = {
  &(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 "(legacy-pcie|spdm):.+"
$device-claims-set /= spdm-claims / cxl-claims / chi-claims / pcie-\
                                                        legacy-claims
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,
        ? &(device-interface-report: 3807) => tdisp-device-interface\
                                                        -report,
      ) // (
        &(measurements: 3802) => spdm-measurements,
        ? &(device-interface-report: 3807) => tdisp-device-interface\
                                                        -report,
      ) // (
        &(certificates: 3803) => spdm-certificates,
        ? &(device-interface-report: 3807) => tdisp-device-interface\
                                                        -report,
      ))
spdm-measurement = {
  &(component-type: 1) => component-type,
  measurement,
}
measurement //= (&(digest-measurement: 2) => digest-measurement // &\
                            (raw-measurement: 3) => raw-measurement)
component-type /= &(immutable-rom: 0) / &(mutable-firmware: 1) / &(\
hardware-config: 2) / &(firmware-config: 3) / &(freeform-measurement\
-manifest: 4) / &(device-mode: 5) / &(mutable-firmware-version: 6) \
/ &(mutable-firmware-svn: 7) / &(hash-extend-measurement: 8) / &(\
           informational: 9) / &(structured-measurement-manifest: 10)
raw-measurement = bytes
digest-measurement = digest
digest = [
  alg: uint / text,
  val: bytes,
]
```

```
   spdm-certificates = {
     default-cert-slot => cert-chain,
     ? aux-cert-slot-1 => cert-chain,
     ? aux-cert-slot-2 => cert-chain,
     ? aux-cert-slot-3 => cert-chain,
     ? aux-cert-slot-4 => cert-chain,
     ? aux-cert-slot-5 => cert-chain,
     ? aux-cert-slot-6 => cert-chain,
     ? aux-cert-slot-7 => cert-chain,
   }
   cert-chain = bytes
   default-cert-slot = 0
   aux-cert-slot-1 = 1
   aux-cert-slot-2 = 2
   aux-cert-slot-3 = 3
   aux-cert-slot-4 = 4
   aux-cert-slot-5 = 5
   aux-cert-slot-6 = 6
   aux-cert-slot-7 = 7
   spdm-measurements = {
     + block-id => spdm-measurement,
     ? "signature" => spdm-measurement-blocks-signature,
   }
   block-id = 1 .. 239
   hash-algorithm-type /= &(tpm_alg_sha_256: 0) / &(tpm_alg_sha_384: 2\
   ) / &(tpm_alg_sha_512: 4) / &(tpm_alg_sha3_256: 8) / &(\
   tpm_alg_sha3_384: 16) / &(tpm_alg_sha3_512: 32) / &(tpm_alg_sm3_256\
                                                                  : 64)
   spdm-measurement-blocks-signature = {
     &(slot: 1) => 0 .. 7,
     &(requester-nonce: 2) => bytes .size 32,
     &(responder-nonce: 3) => bytes .size 32,
     &(combined-spdm-prefix: 4) => bytes .size 100,
     &(IL1: 5) => bytes,
     &(base-hash-algo: 6) => hash-algorithm-type,
     &(signature: 7) => bytes,
   }
   cxl-claims = {&(eat_profile: 265) => "tag:linaro.org,2025:device-cxl\
                                                          #1.0.0"}
   chi-claims = {&(eat_profile: 265) => "tag:linaro.org,2025:device-chi\
                                                          #1.0.0"}
   pcie-legacy-claims = {
     &(eat_profile: 265) => "tag:linaro.org,2025:device-pcie-legacy#1.0\
                                                            .0",
     pcie-legacy-artefacts,
     ? $$pcie-legacy-claim-extension,
   }
   pcie-legacy-artefacts //= ((
```

```
          &(artefacts-text: 3805) => pcie-type-0-1-config-space-text,
          &(artefacts-bytes: 3806) => pcie-type-0-1-config-space-bytes,
        ) // &(artefacts-text: 3805) => pcie-type-0-1-config-space-\
   text // &(artefacts-bytes: 3806) => pcie-type-0-1-config-space-bytes)
   pcie-type-0-1-config-space-bytes = bytes .size 256
   pcie-type-0-1-config-space-text = {
     &(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,
   }
   tdisp-device-interface-report = {
     ? &(interface-info: 1) => interface-info-bits,
     ? &(msi-x-message-control: 2) => bytes .size 2,
     ? &(lnr-control: 2) => bytes .size 2,
     ? &(tph-control: 3) => bytes .size 4,
     ? &(mmio-ranges: 4) => mmio-ranges,
     ? &(device-specific-info: 5) => bytes,
   }
   interface-info-bits = bytes .bits interface-info-flags
   interface-info-flags = &(
     bit0: 0,
     bit1: 1,
     bit2: 2,
     bit3: 3,
     bit4: 4,
     bit5: 5,
   )
   mmio-ranges = {+ &(mmio-range: 1) => mmio-range}
   mmio-range = {
     &(first-4k-page: 1) => bytes .size 8,
     &(number-of-4k-pages: 2) => bytes .size 4,
     &(attributes: 3) => range-attributes,
   }
   range-attributes = {
     &(range-attribute-bits: 1) => range-attribute-bits,
     &(range-attribute-range-id: 2) => bytes .size 2,
   }
   range-attribute-bits = bytes .bits range-attributes-flags
   range-attributes-flags = &(
     bit0: 0,
     bit1: 1,
```

```
    bit2: 2,
    bit3: 3,
  )
```

5. Security Considerations

TODO Security

6. IANA Considerations

6.1. New CWT Claims Registrations

IANA is requested to register the following claims in the "CBOR Web Token (CWT) Claims" registry [IANA.cwt].

6.1.1. SPDM Measurements Claim

* Claim Name: spdm-measurements
* Claim Description: SPDM Measurements
* JWT Claim Name: N/A
* Claim Key: 3802
* Claim Value Type(s): map
* Change Controller: IETF
* Specification Document(s): Section 3.1.1 of RFCthis

6.1.2. SPDM Certificates Claim

* Claim Name: spdm-certificates
* Claim Description: SPDM Certificates
* JWT Claim Name: N/A
* Claim Key: 3803
* Claim Value Type(s): map
* Change Controller: IETF
* Specification Document(s): Section 3.1.2 of RFCthis

6.1.3. SPDM VCA Claim

* Claim Name: spdm-vca
* Claim Description: SPDM Version, Capabilities and Algorithms
* JWT Claim Name: N/A
* Claim Key: 3804
* Claim Value Type(s): bytes
* Change Controller: IETF
* Specification Document(s): Section 3.1.4 of RFCthis

6.1.4. PCIe Legacy Device Text Claim

* Claim Name: pcie-legacy-device-text
* Claim Description: PCIe Legacy Device Textual Representation
* JWT Claim Name: N/A
* Claim Key: 3805
* Claim Value Type(s): map
* Change Controller: IETF
* Specification Document(s): Section 3.2 of RFCthis

6.1.5. PCIe Legacy Device Binary Claim

* Claim Name: pcie-legacy-device-binary
* Claim Description: PCIe Legacy Device Binary Representation
* JWT Claim Name: N/A
* Claim Key: 3806
* Claim Value Type(s): bytes
* Change Controller: IETF
* Specification Document(s): Section 3.2 of RFCthis

6.1.6. TDISP Device Interface Report

* Claim Name: tdisp-device-interface-report
* Claim Description: TDISP Device Interface Report
* JWT Claim Name: N/A
* Claim Key: 3807
* Claim Value Type(s): bytes
* Change Controller: IETF
* Specification Document(s): Section 3.1.3 of RFCthis

7. References

7.1. Normative References

[IANA.cwt] IANA, "CBOR Web Token (CWT) Claims", <https://www.iana.org/assignments/cwt>.

[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/rfc/rfc2119>.

[RFC4514] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names", RFC 4514, DOI 10.17487/RFC4514, June 2006, <https://www.rfc-editor.org/rfc/rfc4514>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[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/rfc/rfc8174>.

[RFC9711] Lundblade, L., Mandyam, G., O'Donoghue, J., and C. Wallace, "The Entity Attestation Token (EAT)", RFC 9711, DOI 10.17487/RFC9711, April 2025, <https://www.rfc-editor.org/rfc/rfc9711>.

7.2. Informative References

[SPDM] DMTF, "Security Protocol and Data Model (SPDM) Specification Version: 1.3.2", 21 August 2024, <https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.3.2.pdf>.

Appendix A. Examples

```
   =============== NOTE: '\' line wrapping per RFC 8792 ================

   {
     / profile / 265: "tag:linaro.org,2025:device#1.0.0",
     / nonce / 10: h'\
   f9efc3341597f75f8d94432ad39566a8c5704b2004ba001c094f475bfc057f9f25d7\
          aa40cd86cd30ebaae746fb19f008c1e6a1f23ad6a178e18dceda918f7f6e',
     / submods / 266: {
       "spdm:ACME:WIDGET-A:0123456789": {
         / profile / 265: "tag:linaro.org,2025:device-spdm#1.0.0",
         / measurements / 0x0eda: {
           1: {
             / component-type /  1: 2, / hardware config /
             / raw-measurement / 3: h'4f6d616861'
           }
         },
         / certificates / 0x0edb: {
           / device certs / 0: h'\
                             676f616e6e6174726164974696f6e6d6f6e676572'
           / no aux certs /
         }
       },
       "spdm:C=CA,O=ACME,OU=Widget-B,CN=9876543210": {
         / profile / 265: "tag:linaro.org,2025:device-spdm#1.0.0",
         / measurements / 0x0eda: {
           1: {
             / component-type / 1: 1, / mutable firmware /
             / digest-measurement / 2: [
               / alg / 1,
               / val / h'6b656e6e656c6c79'
             ]
           },
           6: {
             / component-type / 1: 2, / hardware config /
             / digest measurement / 2: [
               / alg / 0,
               / val / h'756e646572637279'
             ]
           }
         },
         / certificates / 0x0edb: {
           / device certs / 0: h'61746865697A656178696C6C6172',
           / aux certs (slot=2) / 2: h'23451576923AE99106783948598A'
         }
       }
     }
   }
```

Acknowledgments

Thank you Basma El Gaabouri, Henk Birkholz, James Bottomley, Lukas Wunner, Simon Frost and Yousuf Sait for your comments and suggestions.

Authors' Addresses

Mathieu Poirier
Linaro
Email: mathieu.poirier@linaro.org

Thomas Fossati
Linaro
Email: thomas.fossati@linaro.org