‘Secure Device Identity’ Profile for TSN-IA

IEEE Interim Session; September 13, 2022

Kai Fischer, Andreas Furch, Jiye Park, Oliver Pfaff

Problem Statement

- Deliver a fast-paced digest of the IEC/IEEE 60802 text contribution ‘Secure Device Identity Profile”,
  - Filename: 60802-Pfaff-et-al-Secure-Device-Identity-Profile-0922-v04.pdf
  - Date: 2022-09-06
- Highlight the main directions taken by this text – supporting its reading or even getting a rough picture without really reading it. Note: the slides do not aim at replacing the text
- Format:
  - One slide per level-4-headlines in the informative part
  - One slide per level-5-headlines in the normative part (with 2 exceptions)

Informative

Device Identity

a) Information to **talk about** a device, examples: *manufacturer name, model-name, serial-number*

b) Information **told by** the device about itself, same examples

c) Information to **talk to/address** a device, examples: *DNS names or IP addresses*

- Note: **IA-station = device**, the fundamental term of IEEE STD 802.1AR
- *Neighborhood*: the best-practice for “User Identity” (more precisely: IT’s perspective on Human User Identity) is documented in NIST SP 800-63-3 *Digital Identity Guidelines*

Informative

Verifiable Device Identity

- Identity information about a device that **can be verified** esp. communication-related device identity items
  b) Claims made by a device about itself, examples: *manufacturer name, model-name, serial-number*
  c) Expectations on a device, examples: *DNS names or IP addresses*
- Important: **verifiable ≠ verified**
- *Neighborhood*: the best-practice for “Verifiable User Identity” is documented in NIST SP 800-63A *Enrollment and Identity Proofing* along with NIST SP 800-63B *Authentication and Lifecycle Management*
  - Background: the NIST Digital Identity Guidelines aim at an authentication model with 3 parties (claimant=human user, verifier=online authentication authority, relying party=IT-service; the ‘online authentication authority’ decouples the relying party from complexity of authentication schemes/procedures)
  - Commonalities: various conceptual elements on an abstract level esp. “identity” and “authentication” of entities in a distributed system
  - Differentiators:
    - There is no human user in an IEC/IEEE 60802 system
    - There is no ‘online authentication authority’ in IEC/IEEE 60802

Informative

Verification Support Mechanisms

- Secure transports (of unsecured information): can help but provides **no full solution** for verifiable device identity
- Secure information: can provide a **solution** (using cryptographic checksums); introduces some small-print:
  - Validation keys are inevitable. They come in various forms:
    - Symmetric keys
    - Raw public keys
    - Self-signed public key certificates
    - CA-signed public key certificates
  - Their properties introduce details that matter for the scalability and security of the solution
- Important: **verifiable-by-network communications ≠ verifiable-by-something else** e.g. optically checking the body of a chassis; the latter is out-of-scope for IEC/IEEE 60802

Informative

IDevID and LDevID Credentials

- Objects defined by **IEEE STD 802.1AR** that facilitate verifiable device identity in form of:
  - Secure information using asymmetric schemes with CA-signed public key certificates (X.509v3)
  - Verifiable-by-network communications
- Object structure:
  - **Private key**
  - Certification path including a CA-signed public key certificate for the end entity (=device i.e. IA-station). This **EE certificate** (IETF RFC 5280) contains verifiable information about the device (accredited by the CA)
- Important: **IDevID ≠ LDevID**
  - IDevID (Initial Device Identity): issued by device manufacturers; contains information about the device known by time of its manufacturing, examples: *manufacturer name, model-name, serial-number*
  - LDevID (Locally significant Device Identity): issued by other entities esp. device users; contains information about the device known by time of its usage; examples: *DNS names or IP addresses*

Informative

IDevID Items Beyond IEEE STD 802.1AR

- Consider following cases for checking the initial device identity i.e. IA-stations in factory default state:
  - **Type check**:
    - Needs type information e.g. `model-name, hw-revision, description` in ietf-hardware YANG module
    - Not covered by IEEE STD 802.1AR ➔ *need to place additional requirements*
  - **Instance check**:
    - Needs instance information e.g. `serial-num` in ietf-hardware YANG module
    - IEEE STD 802.1AR has the product `serialNumber` as an option ➔ *need to place additional requirements*
  - **Manufacturer check**:
    - Needs manufacturer naming information e.g. `mfg-name` in ietf-hardware YANG module
    - IEEE STD 802.1AR requires `issuer` names, allows non-manufacturer `issuer` names ➔ *need to place additional requirements*
- Important:
  - Specifying “verifiable” device identity is regarded a task for the **IEC/IEEE 60802 specification** to facilitate an interoperable and automated verification of any IA-station by any CNC
  - Determining to-be-“verified” device identity is regarded a **responsibility of CNC users**; the whole interval [CheckNothing, CheckAllVerifiableItems] should be at user discretion

Informative

Device Identity Representation in IDevID/LDevID Credentials

- In the **EE certificate**
- In its **subjectAltName extension** (for naming information)
  - **By-value**
  - **By-ref**
- Note:
  - By-ref can introduce redundant information items
  - By-ref can increase the complexity (securely binding to the referred object)

Object Contents: IA-Station Identity (1)

- **Raw form**: no requirement beyond IEEE STD 802.1AR i.e. verifiable items as follows:
  - Appearance: `subject` resp. `issuer` fields in EE certificate
  - Contents: product serial-number in `serialNumber` (OID 2.5.4.5; optional) attribute in `subject` field; issuer name in `issuer` field (may but does not have to refer to the device manufacturer)
  - Representation: by-value
- **Extended form**: IEC/IEEE 60802-specific requirements i.e. verifiable items as follows:
  - Appearance: `subjectAltName` extension in EE certificate with a GeneralName of type `uniformResourceIdentifier` using a URN with `q-component` (IETF RFC 8141) to encode following contents in form of keyword/value pairs
  - Contents: `description`, `hardware-rev`, `serial-num`, `mfg-name`, `model-name` values from ietf-hardware YANG module (using the '`hardware`' container '`component`' child element that represents the management entity resp. NETCONF/YANG server of an IA-station)
  - Representation: by-value
  - Example: `urn:ieee:iec-ieee-60802#verifiable-device-identity?=mfg-name=xyz.com &model-name=SuperDuperDevice&hardware-rev=12.0&serial-num=0123456789& description=ServoDrive`

Object Contents: IA-Station Identity (2)

- Design rationale for the extended form:
  - Avoid conflicts: no overwriting of IEEE STD 802.1AR-defined items (see raw form) by IEC/IEEE 60802 items
  - Facilitate co-existence: allow other stakeholders e.g. middleware/application consortia or individual manufacturers to express their native device identity perception of an IA-station. Background:
    - 1 EE certificate has 1 `subject` field that is to be organized according X.501 (hierarchical naming tree underneath a single authority; can neither assume to fulfill “single authority” nor “hierarchical tree” in case of IA-stations)
    - 1 EE certificate can have 1 `subjectAltName` extension. 1 `subjectAltName` extension can carry 1..n `GeneralName` elements. One `GeneralName` provides a choice of various value types including but not limited to `uniformResourceIdentifier`
- Rationale for proposing two forms:
  - In order to make an educated decision between one-of vs. both it makes sense to see their implications
  - Both forms may make sense, scenario: manufacturers who have IDevIDs in place and who do not want to be obliged to change their infrastructure in order to ship IEC/IEEE 60802-compliant products

Normative – IDevID Profile

Object Contents: Signature Suites

- `RSA-2048/SHA-256` according to IEEE STD 802.1AR, clause 9.1
- `ECDSA P-256/SHA-256` according to IEEE STD 802.1AR, clause 9.2
- `ECDSA P-521/SHA-512`
- `ECDSA ed25519/SHA-256`
- `ECDSA ed448/SHA-512`
- `RSA-4096/SHA-512`

Normative – IDevID Profile

Information Model: Entries

- IDevID credentials (concerns IA-stations):
  - YANG module: `ietf-keystore`
  - NMDA: system state i.e. as YANG `config-false` entries
  - Note: uses `hidden-private-key` i.e. the IDevID private key is not retrievable by NETCONF/YANG exchanges
- Trust anchors for IDevID credentials (concerns CNCs):
  - YANG module: `ietf-truststore`
  - NMDA: applied configuration i.e. as YANG `config-true` entries
  - Note: built-in trust anchors are regarded out-of-scope for IEC/IEEE 60802. They serve manufacturer-domestic use cases such as SW/FW update which are not covered by IEC/IEEE 60802

Normative – IDevID Profile

Information Model: Entry Manifoldness and Naming

- IDevID credentials (concerns IA-stations):
  - 1..n, one per supported signature suite; if multiple IDevIDs are provided for one device then they shall contain the same device identity information
  - `/ietf-keystore:keystore/asymmetric-keys/asymmetric-key/name=IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfEECertificate>`
- Trust anchors for IDevID credentials (concerns CNCs):
  - 1..n
  - `/ietf-truststore:truststore/certificate-bags/certificate-bag/certificate/name=IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfCACertificate>`

Normative – IDevID Profile

Processing Model: Credentials

- Use cases:
  i. NETCONF/YANG security setup from factory default
  ii. Device identity verification (a subtask of i. that may also be performed independently)

  In both use cases: IA-stations act as claimant (equipped with IDevIDs); CNCs act as verifier (equipped with trust anchors for IDevIDs)

- Use:
  1. IDevID certification path validation (IETF RFC 5280): **compulsory**
  2. Proof-of-possession for IDevID private key (IETF RFC 5246 for TLS 1.2): **compulsory**
  3. Device identity verification for IDevID EE certificate contents: **situationally** i.e. subject to CNC user policy
     - Raw case:
       - Verifiable items: none from perspective of IEC/IEEE 60802
       - Verified items: none (the device identity verification at CNCs is passed with directive „No-Identity-Check“)
     - Extended case:
       - Verifiable items: `description, hardware-rev, serial-num, mfg-name, model-name`
       - Verified items: subject to CNC user policy

Normative – IDevID Profile

Processing Model: Trust Anchors

- Use cases: same as above, now focusing on fundamental objects needed by CNCs to fulfill their verifier role for the use cases i. and ii.
- Caveats:
  - *Offer&accept*: CAs resp. certificate issuers do not distribute “trust anchors”; They distribute “CA certificates”. These objects become (or not become) “trust anchors” at the discretion of relying parties i.e. CNC users.
  - *Anomaly*: the signature in self-signed (CA) certificates does not vouch for the authenticity of the object (in contrast to CA-signed certificates) – *Mallory can issue self-signed CA certificates in the name of Alice that can not be distinct from those of Alice*

Contacts

Kai Fischer, Siemens AG, T CST SES-DE, kai.fischer@siemens.com

Andreas Furch, Siemens AG, T CST SES-DE, andreas.furch@siemens.com

Jiye Park, Siemens AG, T CST SEA-DE, jiye.park@siemens.com

Oliver Pfaff, Siemens AG, DI FA CTR ICO PO, oliver.pfaff@siemens.com