Contributors

Fischer, Kai <kai.fischer@siemens.com>

Furch, Andreas <andreas.furch@siemens.com>

Park, Jiye <jiye.park@siemens.com>

Pfaff, Oliver <oliver.pfaff@siemens.com>

Log

v0.1	2022-01-21	IEEE January 2022 Interim Session presentation
v0.2	2022-03-07	IEEE March 2022 Plenary presentation
v0.3	2022-05-09	IEEE May 2022 Interim Session presentation
v0.4	2022-09-06	Initial version in text form

Secure Device Identity Profile

4

4.8.6 Secure Device Identity

Note to editor: this covers the informative aspects of a ‘Secure Device Identity’ profile for IEC/IEEE 60802. This text is meant to replace D1.4, chapter 4.8.6 Secure device identity.

4.8.6.1 Device Identity

The term ‘device’ originates from IEEE STD 802.1AR (Secure Device Identity). It matches an IA-station in IEC/IEEE 60802.

The device identity refers to a set of information items about a device resp. IA-station that:

- Describes a device as a physical or virtual entity in a distributed system (identifier and/or attribute information).
- Is used by a device to describe itself as such entity (identifier and/or attribute information).
- Allows to interact with this device (addressing information i.e., a specific identifier class).

The targeted use case e.g., application data exchanges, configuration exchanges, inventory or ordering determines the required amount of identity information about a device resp. IA-station.

The device identity of any single IA-station encompasses:

- MAC addresses, IP addresses, TCP ports, DNS names
- ietf-hardware YANG module contents (IETF RFC 8348)

4.8.6.2 Verifiable Device Identity

Certain aspects of device identity demand verification before relying on them during online interactions. Examples are:

- DNS names or IP addresses are used to call the management entity of an IA-station i.e., its NETCONF/YANG server. Their value represents the caller's expectation on the identity of their responder in network communications. Its verification allows to defeat DNS spoofing, component impersonation and man-in-the-middle attacks. This is mandated by IETF RFC 7589 and described in IETF RFC 6125. Passing this check is a prerequisite before NETCONF application exchanges can happen.
- mfg-name values in instances of the ietf-hardware YANG module. They make claims about the IA-station manufacturer. Their verification is a means to protect against counterfeiting.

The verification of IA-station identity happens according to a model that is fully specified by IEC/IEEE 60802 and whose checking can be done in a manufacturer-agnostic manner. This verification is important before supplying locally significant credentials especially LDevID-NETCONF to IA-stations that are in factory-default state.

Note to editor: there is ongoing work to analyze attack vectors for layer 2 communications in IEC/IEEE 60802. Depending on its outcome, MAC addresses or other items might additionally appear in the set of verifiable device identity items.

4.8.6.3 Verification Support Mechanisms

4.8.6.3.1 General

This section considers mechanisms that support device identity verification during online interactions with IA-stations.

4.8.6.3.2 Secure Transports

Sending information in plain form over a protected channel, e.g., ietf-hardware YANG module contents via NETCONF-over-TLS protects the transferred information during its transit through the network but does not vouch for the correctness of the received information e.g., the mfg-name value.

4.8.6.3.3 Secure Information

Protecting information objects by means of cryptographic checksums allows to verify the authenticity and integrity of the provided information. Cryptographic checksums may use symmetric or asymmetric schemes. In case of asymmetric schemes, raw and self-signed public keys need to be distinguished from CA-signed public keys.

Asymmetric schemes with CA-signed public keys are preferable for the verifiable device identity use case: claimants and verifiers share a public key; the claimant possesses the corresponding private key. The establishment and storage of the shared public keys uses public key certificates. For this approach self-signed CA certificates are to be established in an authentic manner. Their amount is independent from the number of verifiers (CNCs) as well as claimants (IA-stations). It may be a 1-digit number.

4.8.6.4 IDevID and LDevID Credentials

IDevID and LDevID credentials are specified by IEEE STD 802.1AR. These objects are comprised of a certification path and a private key. The certification path encompasses an end entity certificate which contains verifiable device identity in a CA-signed form. The device identity verification happens after validating the certification path (IETF RFC 5280) and checking the proof-of-possession for the private key (IETF RFC 5246 in case of TLS 1.2). The certification path validation demands trust anchors as input arguments (IETF RFC 5280, section 6.1.1 input argument (d)).

Two types of credentials are distinguished by IEEE STD 802.1AR:

- IDevIDs are issued by device manufacturers. They represent an initial identity as it is known at device production-time. The initial device identity is not locally significant: it cannot contain deployment-specific information such as DNS names or IP addresses.
- LDevIDs are issued by other actors e.g., a device user. They represent a locally significant device identity: they can contain deployment-specific information e.g., DNS names or IP addresses.

IEEE STD 802.1AR uses signature suites to describe the subject public key and the signature fields in IDevID and LDevID certification paths. This notion is different from TLS cipher suites.

Note: IDevID and LDevID credentials also serve purposes beyond secure device identity, for instance the realization of secure transports. This facilitates the use case of NETCONF/YANG security setup from factory default state.

4.8.6.5 IDevID Items Beyond IEEE STD 802.1AR

IEEE STD 802.1AR represents the initial device identity as serialNumber (OID 2.5.4.5) attribute in the subject field of the EE certificate. Its value provides the serial number of the device. This value is required to be unique within the domain of significance of the EE certificate issuer. The serialNumber attribute is an optional capability. This allows to verify following identity items:

- Certificate issuer (not necessarily: manufacturer) by issuer field (data type: ASN.1 Name)
- If present: device instance by serialNumber value (data type: ASN.1 PrintableString)

Note: this verification can happen after certification path validation (IETF RFC 5280) and the proof-of-possession checking for the private key (IETF RFC 5246 in case TLS 1.2).

The following describes options for verifying the device identity of IA-stations in factory default state. It also identifies informational items needed for the corresponding checks:

- IA-station manufacturer check: using names that identify IA-station manufacturers e.g., mfg-name in ietf-hardware YANG module.

Note: IEEE STD 802.1AR does not require issuer names to refer to a manufacturer.

- IA-station type check: using attributes that identify IA-station types e.g., model-name, hw-revision, description in ietf-hardware YANG module.
- IA-station instance check: using values that identify IA-station instances e.g., serial-num in ietf-hardware YANG module.

Note: the product serialNumber is optional in IEEE STD 802.1AR

Following model applies to the verification of the initial device identity of IA-stations:

- The set of to-be-conducted checks is determined by IA-station and CNC users.
- An IA-station uses IDevID credentials to prove its device identity. The checking happens by means of online interactions in the operational network. It happens automatically and is done by CNCs. This does not depend on configuration-domain external repositories.
- Other stakeholders e.g., middleware/application consortia or individual manufactures are allowed to additionally express information items in IDevID credentials to reflect their device identity model. CNCs do not assess such additional information.

4.8.6.6 Device Identity Representation in IDevID and LDevID Credentials

The best practices for representing verifiable device identity information in IDevID and LDevID credentials are:

- Corresponding information (actual values or references to them) appears in EE certificates:
    - IDevID EE certificates bind initial device identity items that are known by the device manufacturer at production time e.g., mfg-name.
    - LDevID EE certificates bind locally significant device identity items that are known by other actors such as device users e.g., DNS names or IP addresses. They may also bind initial device identity information.
- Items that encode device naming information appear in the subjectAltName extension.

Note: this is required by IETF RFC 5280 (section 4.2.1.6). It is also backed by IETF RFC 6125 (section 2.3).

- A binding can take one of following forms. Multiple forms can appear in one EE certificate:
    - By-value: the verifiable device identity information is represented by its value inside the IDevID resp. LDevID EE certificate. Examples are:
        - The product serialNumber in IDevID credentials (IEEE STD 802.1AR)
        - The hostname of the NETCONF/YANG server in LDevID-NETCONF credentials (IETF RFC 7589 and 6125)
    - By-ref: the verifiable device identity information is represented by a reference inside the IDevID resp. LDevID EE certificate, not by its value:
        - The actual value may be provided by the device itself or by a device-external source.
        - If it is provided in form of an unprotected information object, then the reference object that is embedded to EE certificates should include a digest value.

6

6.3

6.3.3 IDevID Profile

Note to editor: this covers the normative aspects of a 'Secure Device Identity' profile for IEC/IEEE 60802. This text is meant to replace D1.4, chapter 6.3.3 Factory default state.

6.3.3.1 General

IA-stations shall possess IDevID credentials according to the profile in this clause. CNCs shall contain trust anchors for validating IDevID credentials.

6.3.3.2 Object Contents

6.3.3.2.1 General

The IDevID credential contents shall comply to IEEE STD 802.1AR and the profile in this clause.

6.3.3.2.2 IA-Station Identity

Any IDevID EE certificate of an IA-station shall take one of the following forms:

- Raw form: the IDevID EE certificate complies to IEEE STD 802.1AR
- Extended form: the IDevID EE certificate complies to IEEE STD 802.1AR and the requirements provided in this clause.

The extended form of an IDevID EE certificate shall be constructed as follows:

- The verifiable device identity shall appear as a URN in a GeneralName of type uniformResourceIdentifier in the subjectAltName extension.
- The URN value shall be constructed according to IETF RFC 8141 and as follows:
  - Namespace identifier: ieee (IETF RFC 8069)
  - Namespace-specific string: iec-ieee-60802#verifiable-device-identity
  - q-component (see IETF RFC 8141, 2.3.2) to parameterize the named resource: an ampersand-separated list of keyword=value tuples with following keywords and values. These tuples can appear in any order inside the q-component:
    - The keywords: description, hardware-rev, serial-num, mfg-name, model-name
    - Their corresponding values from the single 'component' list entry in the ietf-hardware YANG module that represents the management entity of the IA-station resp. from its pre-material form in percent-encoding (IETF RFC 3986).

Note: these are the items with the YANG property config-false from the 'component' list entry that represents the management entity of the IA-station. The config-false items firmware-rev and software-rev are excluded to avoid IDevID credential updates in case of FW or SW updates.

Note: an object looks like urn:ieee:iec-ieee-60802#verifiable-device-identity?=mfg-name=<mfg-name>&model-name=<model-name>&hardware-rev=<hardware-rev>&serial-num=<serial-num>&description=<description>

Note: one IDevID EE certificate can have one subjectAltName extension which can have one or more GeneralName entries. In particular: there can be one or more GeneralName entries of type uniformResourceIdentifier. This allows other organizations e.g., middleware and application consortia or individual manufacturers to also represent their perception of verifiable device identity in addition to the IEC/IEEE 60802 perception.

Note to editor: additional normative references (IETF RFC 3986, 8069 and 8141) are needed

Note to editor: in case of IA-stations whose functional units cannot change after manufacturing more ietf-hardware items (other child elements) may be included. If this results in increased structural complexity the embedding approach might change (by-ref).

6.3.3.2.3 Signature Suites

An IDevID shall utilize one signature suite from the following list of signature suite names:

- 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

Note: the utilization of RSA for the establishment of shared secret keys is deprecated by IETF RFC 7525 and discontinued by IETF RFC 8446. (TLS 1.3).

Note to editor: additional normative references (IETF RFC 7525, 8446) are needed

Note to editor: signature suite descriptions are required for ECDSA P-521/SHA-512, ECDSA ed25519/SHA-256, ECDSA ed448/SHA-512, RSA-4096/SHA-512. This should be provided in IEC/IEEE 60802 until they get covered by IEEE STD 802.1AR.

Note to editor: to support signing according to RSA additional TLS cipher suites are needed:
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

6.3.3.3 Information Model

6.3.3.3.1 General

The information model for IDevID credentials and trust anchors shall comply to YANG and NMDA, in particular the YANG modules ietf-keystore and ietf-truststore, as well as the profile in this clause.

6.3.3.3.2 Entries

IDevID credentials shall be provided in form of built-in keys of an IA-station by its manufacturer. In YANG they are modeled as config-false nodes and are represented in the ‘keystore’ container that is instantiated by the YANG module ietf-keystore. The private key shall use the private-key-type choice hidden-private-key i.e., the IDevID private key is not presented in NETCONF/YANG. The details of storing and protecting IDevID private keys as well as using them for signing purposes are implementation-specific.

Trust anchors for IDevID credentials are CNC user-configured data objects: these objects shall be available as applied configuration (IETF RFC 8342) upon CNCs. In YANG they are modeled as config-true nodes and are represented in the ‘truststore’ container that is instantiated by the YANG module ietf-truststore.

Note: IA-station built-in trust anchors for use cases such as FW/SW update are out-of-scope in IEC/IEEE 60802.

6.3.3.3.3 Entry Manifoldness

An IA-station shall support at least one IDevID credential, one per supported signature suite. If an IA-station possesses multiple IDevID credentials, then they shall be issued by the same organization (the IA-station manufacturer). Their EE certificates shall contain the same device identity information.

A CNC shall support at least one trust anchor for IDevID credentials per supported IA-station manufacturer.

6.3.3.3.4 Entry Naming

IDevID credentials shall be present in an ‘asymmetric-key’ entry that is identified as follows:

/ietf-keystore:keystore/asymmetric-keys/asymmetric-key/name=
IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfEECertificate>

IDevID trust anchors shall be present in ‘certificate’ entries that are identified as follows:

/ietf-truststore:truststore/certificate-bags/certificate-bag/certificate/name=
IDevID-<SignatureSuiteName>-<CertificateSerialNumberOfCACertificate>

Such entries shall be present underneath a ‘certificate-bag’ entry that is identified as follows:

/ietf-truststore:truststore/certificate-bags/certificate-bag/name=IDevID

6.3.3.4 Processing Model

6.3.3.4.1 General

The processing model for IDevID credentials and trust anchors shall comply to IEEE STD 802.1AR as well as the profile in this clause.

6.3.3.4.2 Credentials

6.3.3.4.2.1 General

IDevID credentials are used in following use cases:

- NETCONF/YANG security setup from factory default; the number of such events scales with the number of factory resets i.e., this use case is performed sporadically. It is conducted by CNCs and encompasses a device identity verification.
- Device identity verification happens as a subtask during NETCONF/YANG security setup from factory default. It may also happen additionally according to CNC user discretion. The details of device identity verification are also subject to given policy.

In these use cases, IA-stations act in claimant role and CNCs act in verifier role:

- IA-stations shall present the certification path of and prove private key possession for an IDevID credential.
- CNCs shall validate the certification path, check the proof-of-possession for the private key, and verify the obtained device identity information.

6.3.3.4.2.2 Creation

IA-station manufacturers select the form factor for representing verifiable device identity in IDevID credentials: raw or extended form. The details of the IDevID credential issuance process are manufacturer-specific and out-of-scope for IEC/IEEE 60802.

IA-station manufacturers are not required to offer an update feature for IDevID credentials.

6.3.3.4.2.3 Distribution

IA-stations shall supply IDevID credentials in form of built-in keys, see 6.3.3.3.

6.3.3.4.2.4 Use

Verifiers (CNCs) shall perform the following checks when they challenge claimants (IA-stations) to authenticate themselves by means of an IDevID credential:

- IDevID certification path validation according to IETF RFC 5280. Whether this validation happens with or without revocation checks is at the discretion of the CNC user.
  - It is the responsibility of the CNC user to supply a trust anchor configuration (set of trusted certificates or trusted public keys), a revocation check instruction (Boolean) and optionally CRL objects to CNCs.

Note: the certification path validation is passed if and only if the IDevID EE certificate is the leaf of a valid certification path that ends with a CA certificate which is signed by a configured trust anchor and which is not revoked (if revocation check is enabled).

- Proof-of-possession checking for the private key according to IETF RFC 7589 and 5246.

Note: the proof-of-possession check is passed if and only if the IA-station possesses the private key which matches the public key in the IDevID EE certificate.

- Device identity verification:
  - It is the responsibility of the CNC user to establish and supply to CNCs: a device identity verification policy which determines the verifiable device identity subset that shall be checked by the CNC for the IA-stations in a configuration domain. This is a subset of {description, hardware-rev, serial-num, mfg-name, model-name}. The empty subset (“no-identity-check”) as well as the whole set are allowed.
  - The device identity verification for an IA-station instance shall behave as follows:

  - If this subset is empty, then the device identity check is passed.
  - If this subset is non-empty, then the CNC performs following expected vs. actual check for each verifiable device identity item in this subset:
    - The check for any item in this subset is passed if the expected value (from ietf-hardware YANG module) matches the actual value (from the verifiable device identity URN value for IEC/IEEE 60802 in the subjectAltName extension of the IDevID EE certificate).

Note: this check fails if the IDevID has raw form.

    - The device identity check is passed if it is passed for all items in the subset.

Note: the device identity verification is passed if and only if all values in the verifiable device identity URN for IEC/IEEE 60802 match the values in the ietf-hardware YANG module – for all items in the device identity verification policy (unless “no-identity-check” is configured). This protects against accidental or intentional ietf-hardware YANG module content modifications – to an extent that is subject to CNC user policy.

IDevIDs in raw form (without IEC/IEEE 60802 verifiable device identity URN) may be used if the device identity verification setting option “no-identity-check” is employed. This allows to perform the NETCONF/YANG security setup from factory default for IA-stations with IDevID credentials in raw form. From CNC perspective these IA-stations remain anonymous.

Note: this document does not specify a mechanism for device identity verification for IDevIDs in raw form. Whether and how device identity checks for such IA-stations are done in an offline mode is at the discretion of CNC users.

6.3.3.4.2.5 Storage

IDevID credentials shall be stored persistently upon an IA-station. The details for implementing this persisted storage are IA-station manufacturer-specific and out-of-scope for IEC/IEEE 60802.

6.3.3.4.2.6 Revocation

It is the responsibility of IA-station manufacturers to report revocation for the IDevID credentials issued by them in form of X.509 CRL objects. These objects are made available in a form that allows relying parties i.e., CNC users to retrieve them at their own discretion.

CNC users decide whether they support IDevID certification path validation with or without revocation:

- If revocation checks are disabled, then certificate path validation shall be performed according to IETF RFC 5280, 6.1 Basic Path Validation.
- If revocation checks are enabled, then certificate path validation shall be performed according to IETF RFC 5280, 6.1 Basic Path Validation and 6.3 CRL Validation.

Note: it is the responsibility of CNC users to obtain up-to-date X.509 CRL objects from manufactures and make them locally available for verifiers.

6.3.3.4.3 Trust Anchors

6.3.3.4.3.1 General

Trust anchors are input arguments for certification path validation according to IETF RFC 5280, section 6.1.1 input argument (d). Relying parties decide about these input arguments in a discretionary fashion i.e., these objects are not created and distributed as literal trust anchor objects but in a pre-material form of self-signed certificate objects.

Note: the digital signature in self-signed certificates do not vouch for authenticity of this object: Actor X can issue self-signed certificates featuring the name of actor A that cannot be distinguished from self-signed certificates issued by A. Out-of-band mechanisms are needed to verify the authenticity of self-signed certificates.

The trust anchors for use cases where IA-stations act in claimant role are determined by CNC users.

6.3.3.4.3.2 Creation

The details of the issuance and update processes for self-signed root certificates for validation of IDevID credentials are out-of-scope for IEC/IEEE 60802.

6.3.3.4.3.3 Distribution

With respect to use cases where IA-stations act in claimant role e.g., NETCONF/YANG security setup and device identity verification the following model applies:

- Issuers (IA-station manufacturers) create and distribute self-signed root certificates. Issuers also provide out-of-band means that allow relying parties to check the authenticity of these objects.
- Relying parties (CNC users) check the authenticity of self-signed root certificates by out-of-band means and decide about their acceptance as trust anchors for certification path validation in a discretional manner and configure their verifiers (CNCs) accordingly.

Specifying details of out-of-band distribution and validation of self-signed root certificates is out-of-scope for IEC/IEEE 60802.

6.3.3.4.3.4 Use

Trust anchors for IDevID credentials are used for certification path validation according to IETF RFC 5280. This concerns CNCs with respect to the use cases NETCONF/YANG security setup from factory default, device identity verification.

6.3.3.4.3.5 Storage

Trust anchors for IDevID credentials shall be stored persistently upon CNCs. The details for implementing this persisted storage are out-of-scope for IEC/IEEE 60802.

6.3.3.4.3.6 Revocation

IA-station manufacturers are not required to support an authority revocation feature for IDevID credential certification authorities.

Note to editor: an adoption of this contribution is meant to have following impact on the D1.4:

- Chapter 4.8.6 in this contribution replaces the chapter 4.8.6 Secure device identity

- Chapter 6.3.3 in this text contribution replaces the chapter 6.3.3 Factory default state

- Additional normative references (D1.4 clause 2): IETF RFC 3986, 7525, 8069, 8141 and 8446

- Additional TLS cipher suites to support RSA-based signing as an option (D1.4 clauses 5.6.3, 6.3.2.1.1):
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256