Secure Device Identity' Profile for TSN-IA: DevID Signature Suites

IEEE 802 Wireless Interim Session; January 19, 2023

Kai Fischer, Andreas Furch, Oliver Pfaff

Problem Statement

- During the Sept. 2022 Interim Session, we presented the **digest** of the **IEC/IEEE 60802 text contribution "Secure Device Identity Profile"** (see 60802-Pfaff-et-al-Secure-Device-Identity-Profile-0922-v04.pdf)
- **Remaining task** from this session was to find a consensus for the number and choice of IEC/IEEE 60802 supported DevID signature suites
- Goal of this presentation: **Propose the DevID signature suite selection/definition for IEC/IEEE 60802** as part of the secure device identity profile of IEC/IEEE 60802
- Note: the secure device identity profile of IEC/IEEE 60802 shall be **IEEE802.1AR-2018 compliant**

Given Things

- IEEE 802.1AR uses the concept of "**DevID Signature Suites**" to specify cryptographic algorithms used for **signing** use cases in an interoperable manner
- IEEE 802.1AR-2018 specifies 3 instances of "DevID Signature Suites"
  - **RSA-2048/SHA-256**
  - **ECDSA P-256/SHA-256**
  - **ECDSA P-384/SHA-384**
- IEC/IEEE 60802 aims at using IDevIDs according IEEE 802.1AR-2018 to

  i. **Protect** the initial NETCONF/YANG exchange(s) with IA stations that are in factory default state

  ii. **Safeguard** identity claims made (via NETCONF/YANG) by IA stations that are in factory default state
- IEC/IEEE 60802 needs to profile its "DevID Signature Suites" instances to achieve objectives i. and ii. in an **interoperable** manner

Key Questions for IEC/IEEE 60802

Q1: **number** of **required** “DevID Signature Suite(s)”

- n=1
- n>1

Q2: **name and description** of the **required** “DevID Signature Suite(s)”

Q3: **number** of **optional** “DevID Signature Suite(s)”

- m=0
- m>0

Q4: **name and description** of the **optional** “DevID Signature Suite(s)”

IEC/IEEE 60802 Impact of these Questions

Specification impact: **minor**

- No conceptual impact on informative text in 4.8 (Security for TSN-IA)
- No conceptual impact on normative text in 6.3 (Security model)
- They matter for the following normative text (in a very obvious way)
  - 5.5.6 (IA-station requirements for security)
  - 5.6.3 (IA-station options for security)

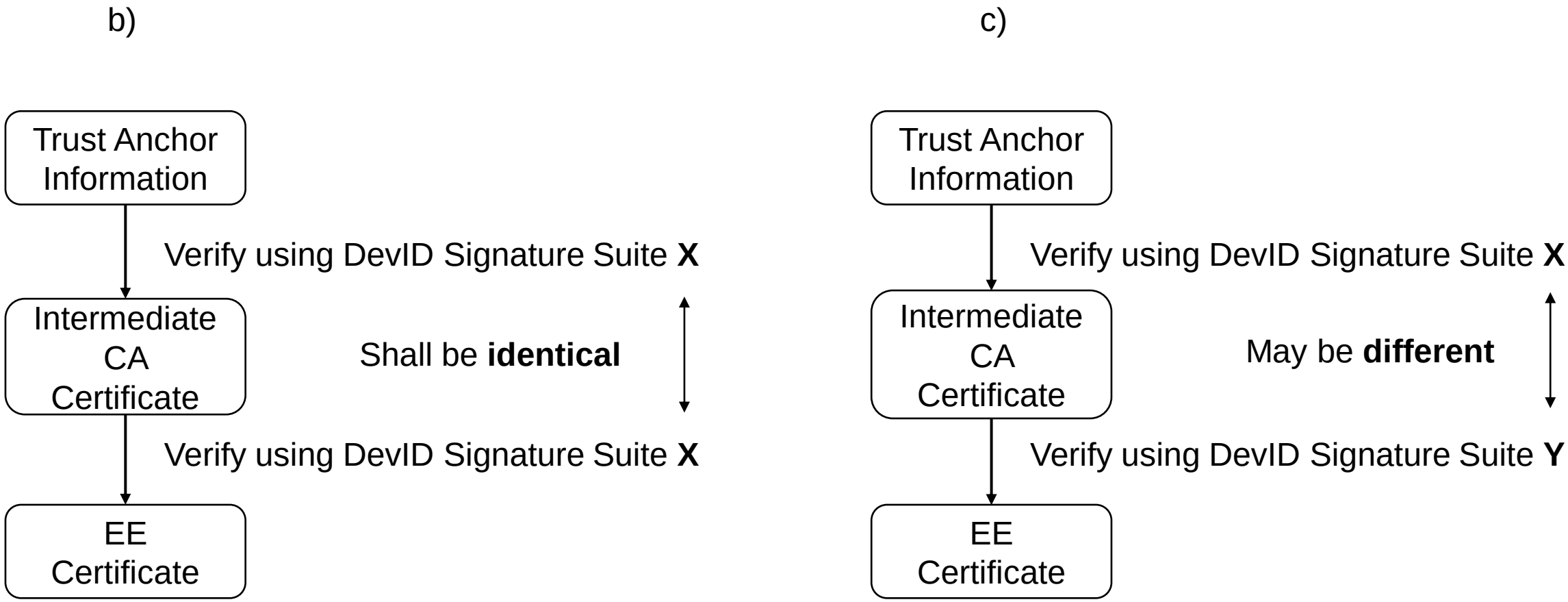
Implementation impact: **major**

- They matter for the realization of IEC/IEEE 60802-compliant and interoperable products

How to Interpret Required and Optional According to IEEE 802.1AR-2018

- Goal: achieve **interoperability** on the one hand, do not prohibit **variety** on the other hand
- Proposal:
  - DevID signature suite x is **required**:
    a) IA-station has a DevID module that supports the DevID signature suite x
    b) IA-station has an IDevID credential with certification path plus trust anchor information issued under DevID signature suite x as part of its factory default state
    c) IA-station may have additional IDevID credential(s) with certification path plus trust anchor information issued under a combination of any required or any optional DevID signature suites
  - DevID signature suite y is **optional**:
    a) IA-station may have a DevID module that supports the DevID signature suite y
    b) IA-station has an IDevID credential with certification path plus trust anchor information issued under DevID signature suite y as part of its factory default state
    c) IA-station may have additional IDevID credential(s) with certification path plus trust anchor information issued under a combination of any required or any optional DevID signature suites

DevID Signature Suite: Fundamental Difference Items b) and c)



A1: Number of Required “DevID Signature Suite(s)”

- *Facts*:
  - Pro n=1: clear focus and minimal complexity
  - Pro n>1: choice for users e.g. desired security strength for protecting the initial security setup
- *Suggestion*: n=1
- *Argument*: IEC/IEEE 60802-compliant products still have to be created, ‘choice’ is a concern that will matter for subsequent editions of the standard

A2: Names and Description of the Required “DevID Signature Suite(s)”

- *Plan A*: **ECDSA P-256/SHA-256**
  - *Reason*:
    - Covered by IEEE 802.1AR-2018
    - Tentative requirement for NETCONF-over-TLS for v1.3 (draft-ietf-netconf-over-tls13-01)
  - *Handicap*: supports 128 bit security strength only, this limitation applies for EE certificates, intermediate CA certificates and trust anchors under the interoperability clause b)
- *Plan B*: **ECDSA P-521/SHA-512**
  - *Reason*: mitigate the plan A handicap
  - *Handicap*: ECDSA P-521/SHA-512 is not yet covered by IEEE 802.1AR
  - *Approach*: temporarily document this DevID Signature Suite in IEC/IEEE 60802; text (ca. 1 page) shall be created in cooperation with IEEE 802.1 Security Taskgroup and moved into an 802.1AR update asap

A3: Number of Optional “DevID Signature Suites”

- *Facts*:
  - Pro m=0: clear focus and minimal complexity
  - Pro m>0: support manufacturers that worry about cryptographic agility (at their own discretion)
- *Suggestion*: m>0
- *Argument*: do not prohibit variety especially allow to address cryptographic agility

A4: Names of the Optional “DevID Signature Suite(s)”

- *Plan A**: **ECDSA P-521/SHA-512, EdDSA instance Ed25519****, **EdDSA instance Ed448****
  - *Reason*:
    - Do not prohibit variety, facilitate cryptographic agility
    - Support of 128, 224 and 256 bit security strengths
  - *Handicap*:
    - ECDSA P-521/SHA-512, EdDSA instance Ed25519, EdDSA instance Ed448 are not yet covered by IEEE 802.1AR
    - EdDSA instance Ed448 introduces a new hash algorithm family (SHAKE)
  - *Approach*: temporarily document this DevID Signature Suite in IEC/IEEE 60802; text (ca. 1 page) shall be created in cooperation with IEEE 802.1 Security Taskgroup and moved into an 802.1AR update asap
- *Plan B*: anything else

*: this plan A suggestion assumes that Plan A is chosen in A2
**: notation according IETF RFC 8032

Concluding Remarks

- RSA was not included in this proposal because of excessive key lengths (3072 bits or more) as well as to reduce the complexity for implementation and testing
- Implications for TLS cipher suites are (in the Plan A/A case):
  - TLSv1.2 according IEC/IEEE 60802 D1.4 profile: no impact; all combinations are feasible
  - TLSv1.3 according draft-ietf-netconf-over-tls13-01: no impact; TLS cipher suite is separated from the digital signature algorithms*

*: TLSv1.3 changed the cipher suite concept to separate the authentication and key exchange mechanisms from the record protection algorithm, which also resulted in a different naming concept for cipher suites.

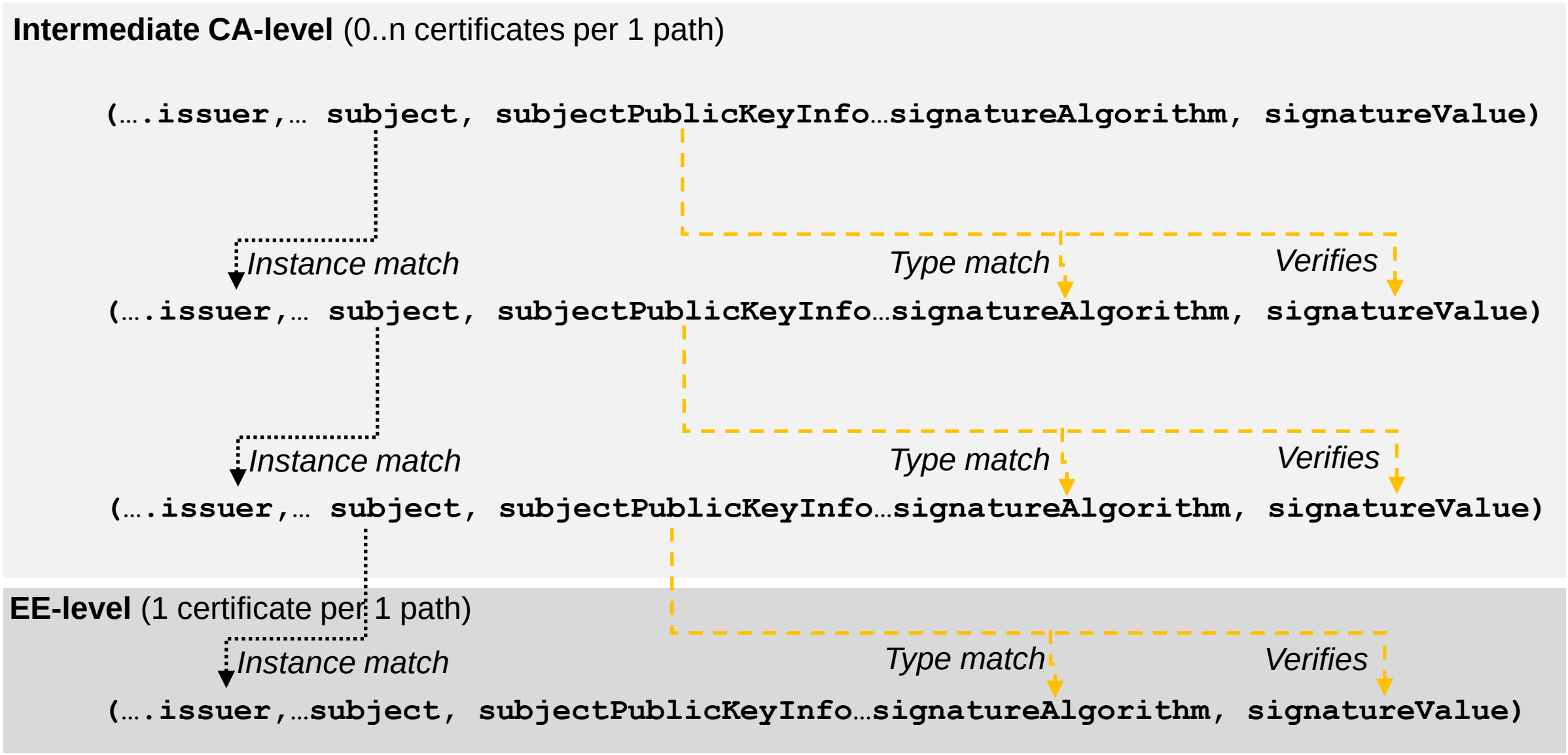
Contacts

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

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

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

Certification Path: IETF RFC 5280, 6.1.1 (a)



Trust Anchor Information: IETF RFC 5280, 6.1.1 (d)

Trust anchor information (1..n objects per certification path validation algorithm instantiation)

Certificate object
(….issuer,… subject, subjectPublicKeyInfo…signatureAlgorithm, signatureValue)
or

Raw public key
(subjectPublicKeyInfo)
or

Fingerprint value for certificate object
Hash(certificate object**)**
or

Fingerprint value for raw public key
Hash(subjectPublicKeyInfo)
or

…