‘Secure Device Identity’ Profile for TSN-IA

IEEE Interim Session; May 09, 2022

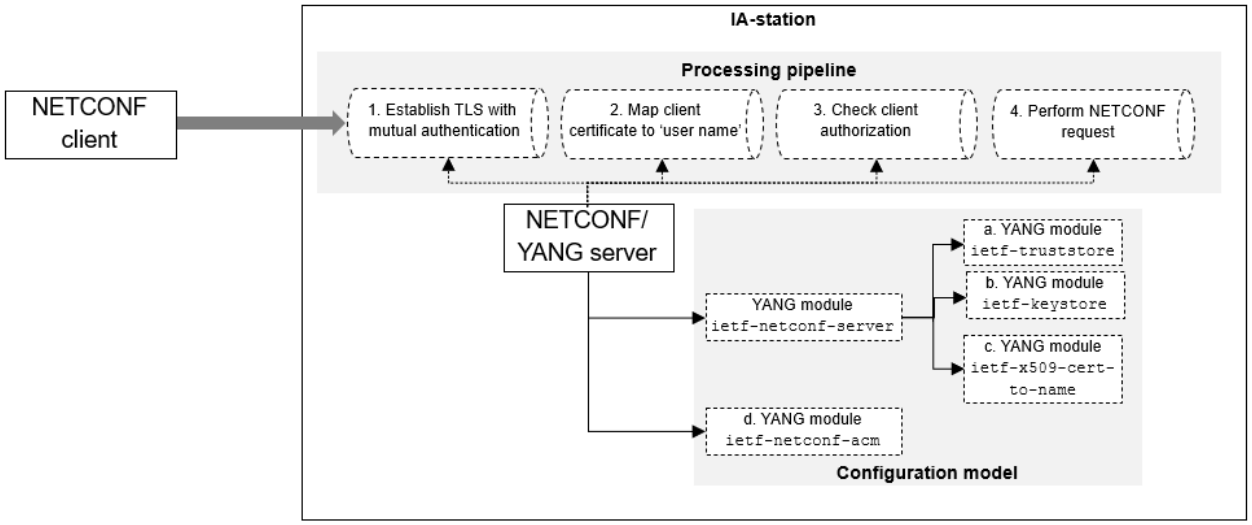
Kai Fischer, Andreas Furch, Oliver Pfaff

Problem Statement

- This is a follow-up to the IEEE March plenary session *'Secure Device Identity' Profile for TSN-IA*, 2022-03-07 (https://www.ieee802.org/1/files/public/docs2022/60802-Pfaff-et-al-Secure-Device-Identity-Profile-0322-v02.pdf)
- Recap (2022-03-07):
  - LDevID-NETCONF* and IDevID EE certificate design variance: *discuss the need for limitation*
  - 'Device' model in IEC/IEEE 60802: *discuss implications on the LDevID-NETCONF/IDevID incarnations (per 'device')*
  - 'Device identity' model in IEC/IEEE 60802: *discuss implications on LDevID-NETCONF/IDevID contents*
- Next step (2022-05-09):
  - NETCONF/YANG security paradigm: *describe the pattern for its fulfillment in TSN-IA*
  - TSN-IA fulfillment of the NETCONF/YANG security paradigm*: discuss actors, infrastructure and object layout*

*: short-hand term for an LDevID (IEEE 802.1AR) that complies with the IETF RFC 7589 rules for NETCONF-over-TLS

Recap: NETCONF/YANG Security Paradigm



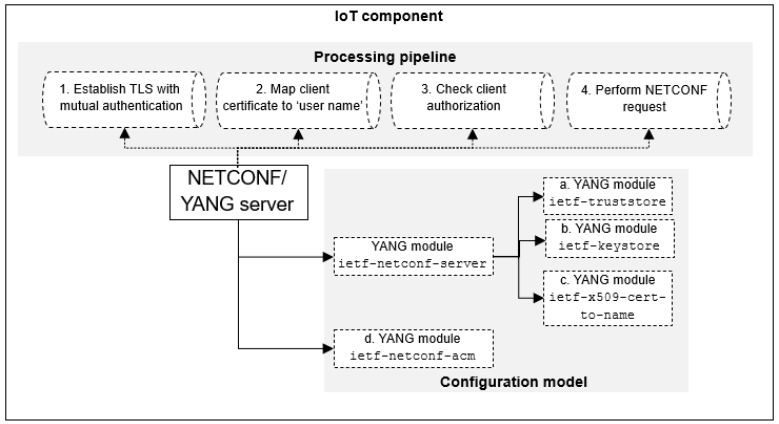
- The NETCONF/YANG security is characterized by:
  - *Security always-on*: all NETCONF exchanges (over the network) **must be protected**; the protection encompasses **mutual entity authentication** and **authorization**, see IETF RFC 6241
  - *Deployment-specific security*: **locally significant** credentials and trust anchors have to be employed, see IETF RFCs 7589 and 6125
- NETCONF/YANG servers implement this paradigm according a **processing pipeline** with steps 1-4 (shown for NETCONF-over-TLS)
- These steps are executed by the server upon the **current configuration** in its YANG modules a-d
  - a and b are used for step 1
  - c is used for step 2
  - d is used for step 3

  Note: step 4 may alter the contents in a-d

Conventional Fulfillment Pattern

- Fulfilling this paradigm is **challenging** for product components (which are hosting NETCONF/YANG servers) in **factory default state**: their NETCONF/YANG server must employ cryptographic protection (for exchanges in the network) but does not possess deployment-specific security objects. This is an ubiquitous challenge.
- The **conventional pattern** to fulfill the NETCONF/YANG security paradigm in e.g. IoT is:

0. Manufacturing



NETCONF/YANG server with *processing pipeline*=**present** *configuration*=**empty** (no LDevID-NETCONF)

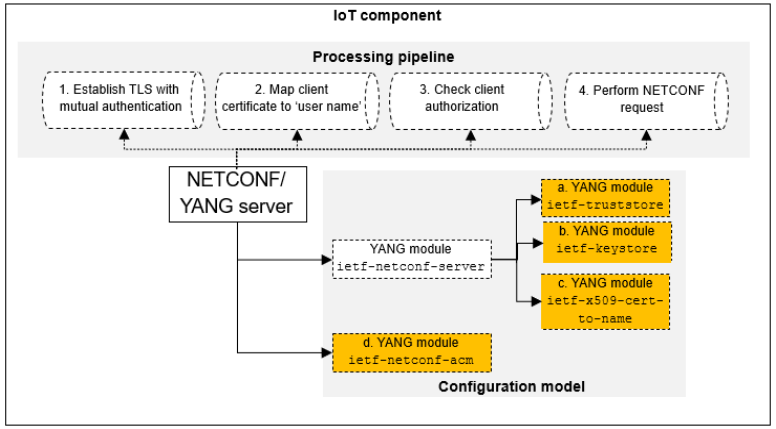
1. Bootstrapping

(incl. security set-up)

Beam LDevID-NETCONF

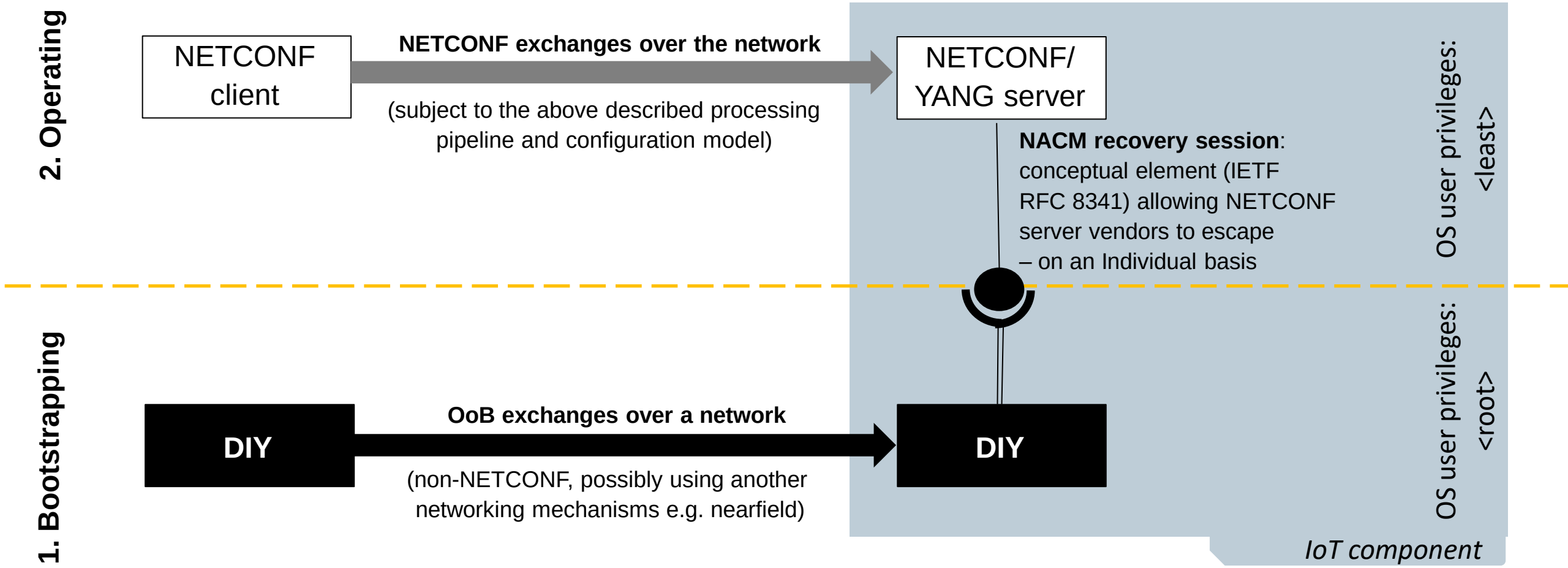
*Use 'NACM recovery session' (IETF RFC 8341) to populate configuration with LDevID-NETCONF - using **local security mechanisms** and **OoB communication means**; details incl. protection are DIY*

2. Operating

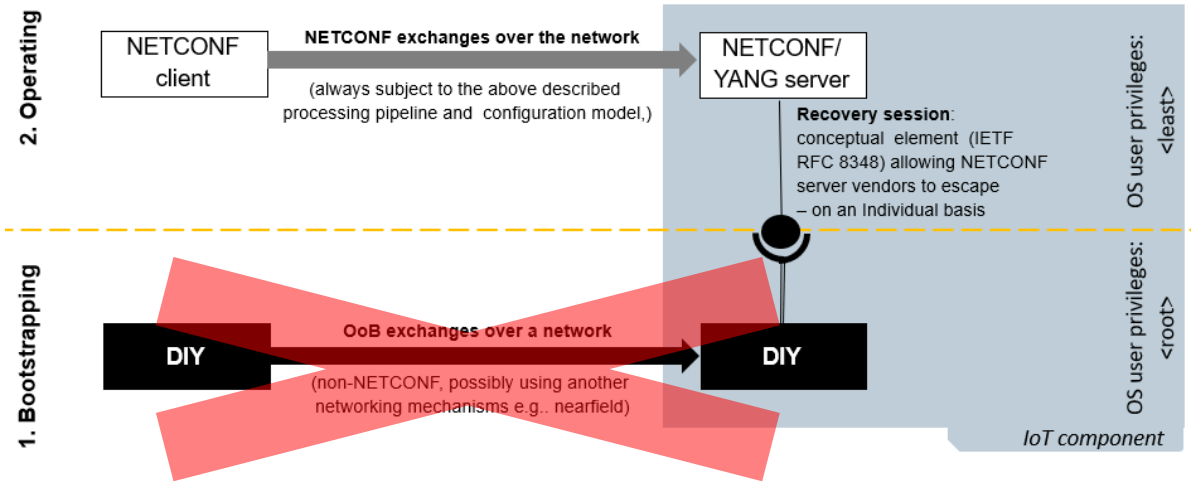


NETCONF/YANG server with *processing pipeline*=**present** *configuration*=**populated** (LDevID-NETCONF)

Conventional Fulfillment Pattern in More Detail



Conventional Pattern Fitness for TSN-IA



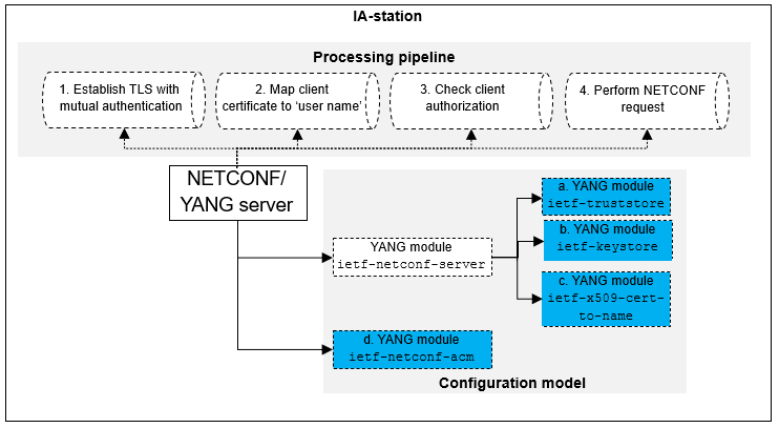
Not viable as an interoperable, manufacturer-independent solution in TSN-IA according given requirements

- The conventional pattern does not provide an interoperable, manufacturer-independent solution for IEC/IEEE 60802:
  - Can not assume a common **OoB communication means** in form of a secondary channel
  - Can not assume **local security mechanisms** such as the separation of system users and access control to system resources on OS-level
  - The security set-up of IA-stations can assume the capability to conduct **NETCONF exchanges** (over the network)
- The conventional pattern may be considered for custom, manufacturer-specific solutions

Proposed Fulfillment Pattern in TSN-IA

- *Idea*: IEC/IEEE 60802 actually is a post-manufacturing spec ➔ move the “OoB means” to the manufacturing environment; supply manufacturer credentials (IDevID) as part of an initial configuration (may be provided before the NETCONF server is deployed i.e. independently from the NACM recovery session); use them to protect initial NETCONF exchanges
- *Caveat*: IDevIDs can not contain deployment details ➔ need to **trade IDevID-for-LDevID-NETCONF** during the initial NETCONF-over-TLS exchange(s) before an operational use in the production environment

0. Manufacturing



NETCONF/YANG server with *processing pipeline*=**present** *configuration*=**pre-populated** (IDevID)

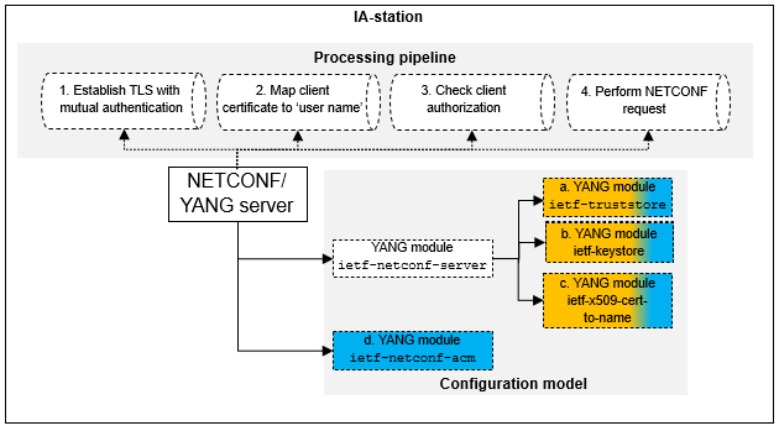
1. Bootstrapping

(incl. security set-up)

Trade IDevID-for-LDevID-NETCONF

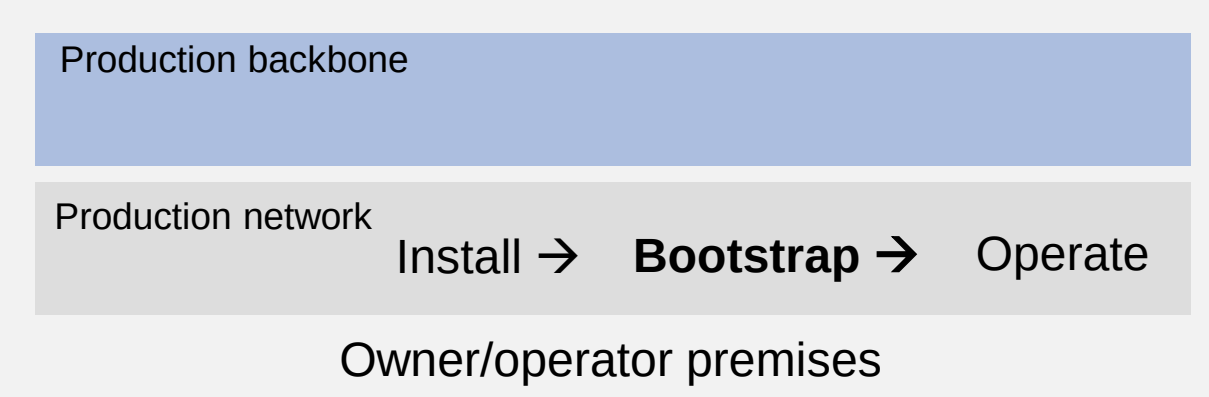
Use NETCONF/YANG exchanges - protected with IDevID (CD4 resp. D1.3) to supply LDevID-NETCONF

2. Operating

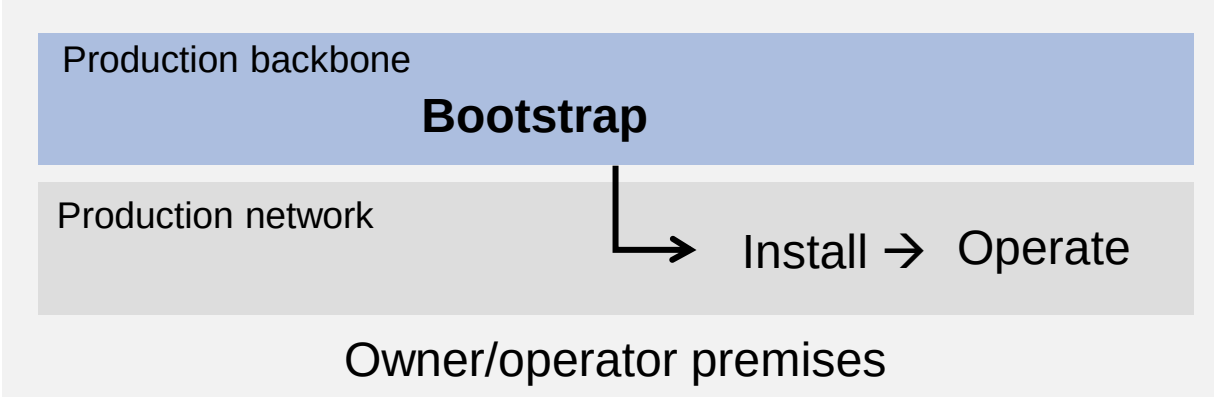


NETCONF/YANG server with *processing pipeline*=**present** *configuration*=**updated** (LDevID-NETCONF added)

Approaches for IDevID-to-LDevID-NETCONF Trading



a) **Directly in the production network** i.e. in an automated fashion; done by the CNC



b) **Outside the production network** in an operated fashion; done by an engineering tool

Assessing the IDevID-to-LDevID-NETCONF Trading Approaches

a) **Directly in the production network** i.e. in an automated fashion; done by the CNC

- Requires a common IDevID design - to facilitate the automated security setup of IA-stations by CNCs
- Matches the online engineering case, plug&produce

➢ Regarded as **default approach**

b) **Outside the production network** e.g. in an operated fashion; done by an engineering tool

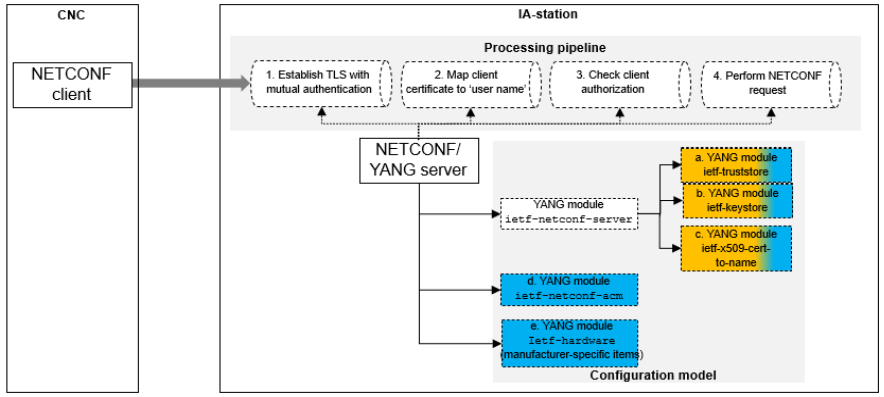
- Demands manufacturer-specific engineering tools – to be able to cope with the IA-station variety that can be encountered in a deployment e.g.
  - 1-2 digit number of manufacturers
  - 2-3 digit number of component types with
    - Specific means for human user interaction e.g. with/without screen, with/without keyboard
    - Specific form-factors e.g. Ethernet plug-types
  - 2-4 digit number of component instances
- Matches the offline engineering case

➢ Considered an **optional supported manufacturer-specific option**

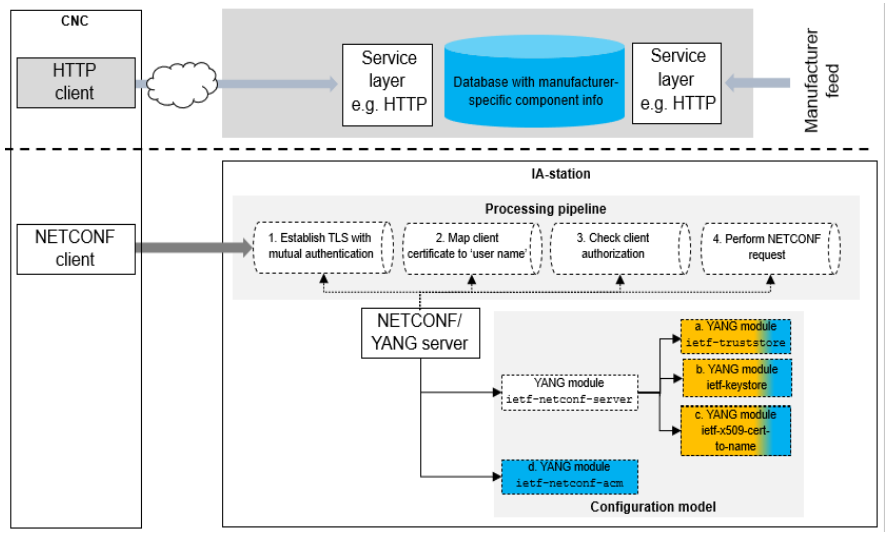
Need for Manufacturer Information

- The main IDevID use case in TSN-IA is the **protected imprinting** of LDevID-NETCONF
- The imprinting of LDevID-NETCONF is supplying **security objects** to an IA-station
  - This encompasses: trust anchor, credential and certificate-to-name mapping
- This is a critical step i.e. subject to **decision making** by owners/operators – same as with human beings; employee credentials (badges, cards…) are not issued to anybody in an AllowAll-mode
- In TSN-IA this decision making is assumed to be subject to the **validation** of information items including the following (details of the validation policy are owner/operator-specific):
  - Manufacturer name (e.g. mfg-name in ietf-hardware YANG module)
  - Component type (e.g. model-name in ietf-hardware YANG module)
  - Component instance (e.g. serial-num and/or uuid in ietf-hardware YANG module)
- The **verification** of this information is part of the validation process. Note:
  - IETF RFC 8348 (ietf-hardware) allows to provide manufacturer information that is required for validation. But it does not cover verification (sending this information via a protected channel does not provide verification)
  - IEEE 802.1AR allows to verify the product serial number and issuer in form of a X.500 DN (this is not equal to the real-world understanding of a manufacturer name)

Approaches to Source Manufacturer Information



c) **Supply by the IA-station itself**; provided by e.g. the YANG module ietf-hardware



d) **Supply by an external resource**; obtained by querying a product directory/registry e.g. as Web-based service outside the production environment

- Run by its manufacturer or on behalf of the manufacturer
- Supporting individual and/or bulk queries
- Supplying volatile and/or lasting media types
- Information retrieval by a separate tool

Assessing the Manufacturer Information Sourcing Approaches

c) **Supply by the IA-station itself;** provided by e.g. the YANG module ietf-hardware

- Requires IDevID EE certificate contents beyond IEEE 802.1AR (see below for form-factor options)
- Matches the online engineering case, plug&produce

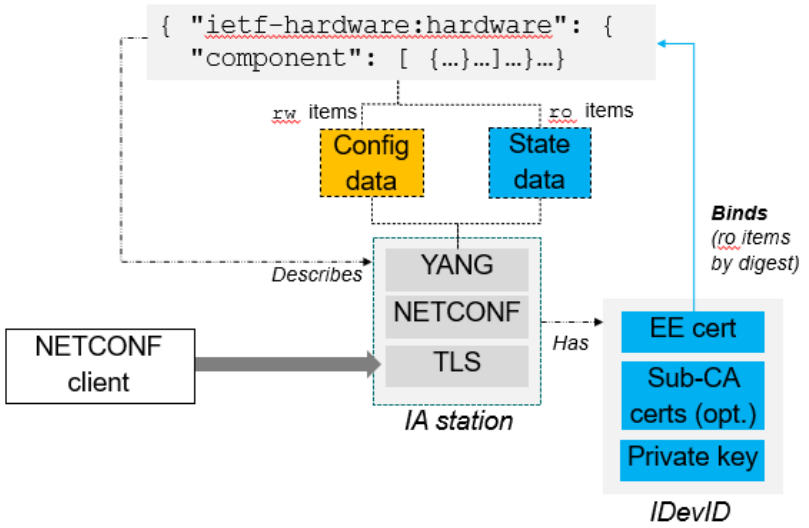
➢ Regarded as **default approach**

d) **Supply by an external resource;** obtained by querying a product directory/registry e.g. as Web-based service

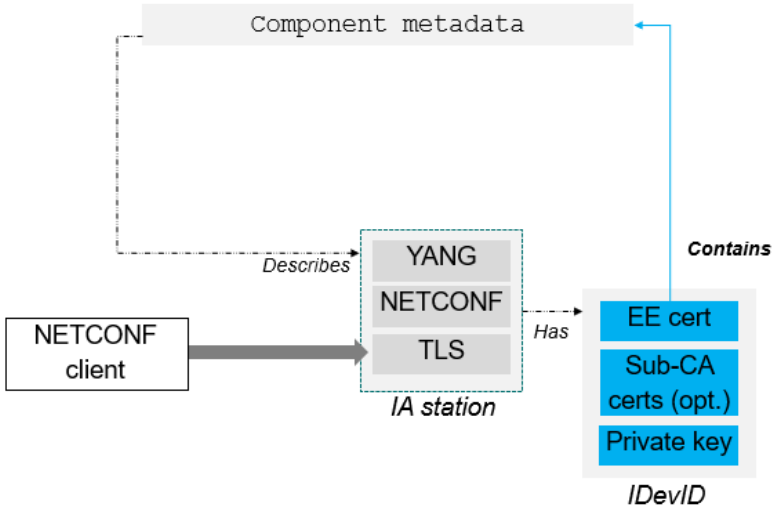
- Demands answers for an array of questions including:
  - Whether manufacturers are willing and in which (interoperable) form they would for expose such information (in a bulk fashion)?
  - Whether and how CNCs can discover responsible directory/registry services?
  - Whether and how CNCs can assume to establish connectivity?
  - How to solve the implied security problem (authenticity of provided information as owner/operator stake, secrecy of revealed information as manufacturer stake…)?
- Matches the offline engineering case

➢ Considered a **manufacturer-specific option**

Approaches to Self-Supply Manufacturer Information



e) **Supplied outside the IDevID EE certificate** in form of e.g. YANG module ietf-hardware - just bound by digest in the IDevID EE certificates (to establish verification of otherwise unverified data)



f) **Supplied inside the IDevID EE certificate** in form of e.g. a subjectAltName extension

Assessing the Self-Supply Approaches for Manufacturer Information

e) **Supplied outside the IDevID EE certificate** in form of e.g. YANG module ietf-hardware - just bound by digest in the IDevID EE certificates

- Requires a sequence that allows to read the ietf-hardware YANG information after provisionally establishing TLS (where an IA-station in factory default uses its IDevID credential)
- Matches the online and offline engineering cases; adds verification for the information in an ietf-hardware YANG module

➢ Regarded as **preferable approach for IEC/IEEE 60802**

f) **Supplied inside the IDevID EE certificate** in form of e.g. a subjectAltName extension

- Requires to duplicate (a subset of) ietf-hardware YANG information into IDevID EE certificates
- Matches the online and offline engineering cases; adds information (by-value) to verifiable objects

➢ Regarded a **fallback option**

Summary, Follow-Ups

- The NETCONF/YANG security paradigm is set forth in IETF RFC 6241 (and subsequent RFCs). It is characterized by: ***Security Always-On*** AND **deployment-specific security objects**
- Fulfilling this paradigm in TSN-IA is a challenge for IA-stations in **factory default state**. It can be fulfilled by **imprinting IDevIDs** (during manufacturing) and **trading them for LDevID-NETCONF** credentials/trust anchors (before operation). The basic trading mechanism is described in CD4 resp. D1.3
- This deck considered following questions for adopting this mechanism in TSN-IA :
  - Q1: *Where/how to trade IDevID for LDevID-NETCONF – a) and/or b)?*
  - Q2: *How to supply manufacturer information needed to fulfill industrial use cases – c) and/or d)?*
  - Q3: *Where to host such information - e) and/or f)?*
- The online engineering case (plug&produce) suggests the answers to comprise:
  - A1: a), directly in the production network i.e. in an automated fashion
  - A2: c), self-supplied by the IA-station
- The adoption of the ietf-hardware YANG module suggests:
  - A3: e), supplied outside the IDevID certificate - the IDevID EE certificate just binds (a subset of) this info

Abbreviations

ASN.1	Abstract Syntax Notation Nb. 1
CNC	Centralized Network Configuration
DIY	Do It Yourself
EE	End Entity
IA	Industrial Automation
ID	IDentifier
IDevID	Initial Device ID
IoT	Internet of Things
JSON	JavaScript Object Notation
LDevID	Locally significant Device ID
NACM	NETCONF Access Control Model
NMDA	Network Management Datastore Architecture
NETCONF	NETwork CONFiguration
OoB	Out-of-Band
ro	read-only
rw	read-write
TSN	Time-Sensitive Networking
XML	eXtensible Markup Language
YANG	Yet Another Next Generation

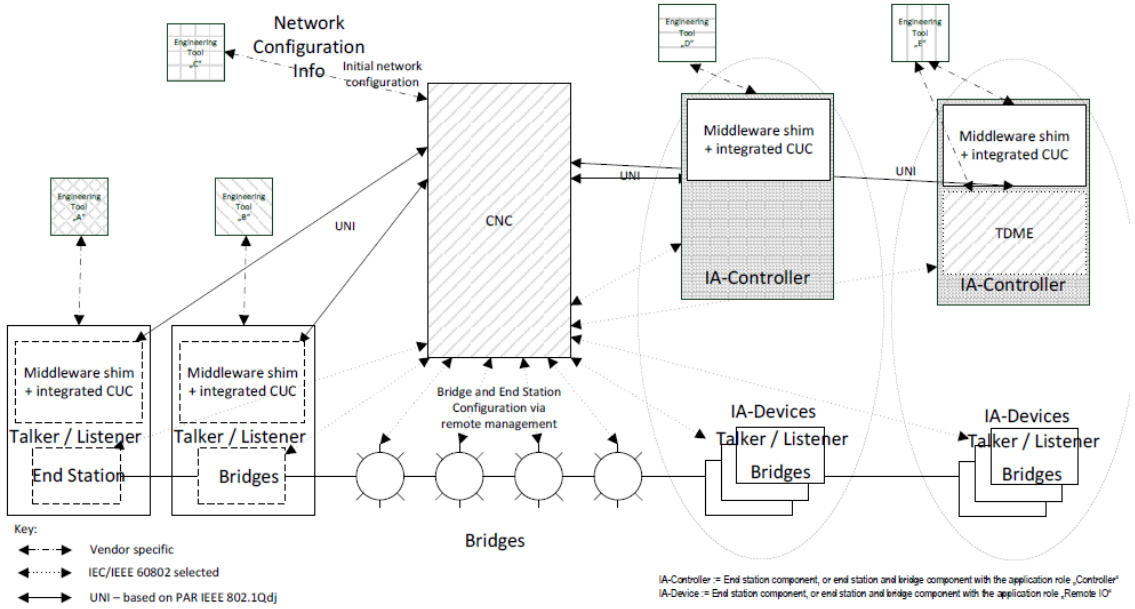
Contacts

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

Online/Offline Engineering, Plug&Produce



Source: Figure 27 – Operational Management Model in CD4 resp. D1.3

- **Online engineering, plug&produce**:
  - Is conducted between IA-stations and CNC
  - Happens in the production network
  - Is interoperable i.e. manufacturer independent
  - Needs specification coverage in IEC/IEEE 60802
- **Offline engineering**:
  - Is conducted between IA-stations and engineering tools
  - Happens outside the production network
  - Is manufacturer-dependent i.e. not interoperable
  - Is beyond the specification scope of IEC/IEEE 60802

Verification vs. Validation

- **Verification**: The evaluation of whether an information is an authentic and timely statement of an issuer or presenter.
  - In case of TLS server and client authentication this comprises: proof of private key possession (IETF RFC 5246) and checking EE certificate with local trust anchors (IETF RFC 5280)
- **Validation**: The assurance that a (verified) information meets the needs of a stakeholder
  - In case of TLS server authentication this comprises: actual vs. expected checking (IETF RFCs 7589 and 6125)
  - In case of TLS client authentication this comprises: certificate-to-name mapping (IETF RFC 7589) and client authorization (IETF RFC 8341)
- Note: this is based on https://www.w3.org/TR/vc-data-model/#terminology and was rephrased to retain the message and make it comprehensible outside this document as well as complemented by examples