‘Secure Device Identity’ Profile for TSN-IA

IEEE Plenary; March 07, 2022

Kai Fischer, Andreas Furch, Oliver Pfaff

Problem Statement

- This is a follow-up to the IEEE January plenary session *'Secure Device Identity' Profile for TSN-IA*, 2022-01-21 (https://www.ieee802.org/1/files/public/docs2022/60802-Pfaff-et-al-Secure-Device-Identity-Profile-0122-v01.pdf)
- Recap (2022-01-21):
  - IDevID EE certificate design variance: *identified the driving factors*
  - Different identity models (by different bodies) for the same physical entity. *sketched a co-existence model*
  - Home of this information: *preferred the SubjectAlternativeName extension*
- Next step (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*

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

LDevID-NETCONF/IDevID Use Cases

LDevID-NETCONF

- **Protect message exchanges** (NETCONF-over-TLS)
- **Authorize resource accesses** (NACM)

Note: solutions for these use cases are already specified in a comprehensive way:

- NETCONF-over-TLS: IETF RFC 7589
- NACM: IETF RFC 8341

IDevID

- **Prepare** for NETCONF-over-TLS i.e. set-up and manage LDevID-NETCONF credentials/trust anchors and certificate-to-name mappings
- **Verify** the original equipment **manufacturer** (*counterfeit protection*)
- **Check** whether an IA station is an **instance-in-class** (*system integrity/resilience*)
- …

Note: not all use cases already have solutions with comprehensive specifications

LDevID-NETCONF/IDevID Usage Models

LDevID-NETCONF

- **Frequently** used: see use cases above
- **Occasionally** updated (usually according a time schedule)
- Processed by verifiers in an **automated** fashion i.e. without human user-attention

IDevID

- **Rarely** used: see use cases above
- **Not** updated
- (May be) processed by verifiers in an **automated** fashion i.e. without human user-attention

➔ **Design variance** for LDevIDs-NETCONF *and* IDevIDs needs to be **limited** to facilitate automated processing in multi-vendor environments

*: IETF RFCs 7589 and 6125 do not detail IDevID contents

LDevID-NETCONF/IDevID Verification/Consumption

LDevID-NETCONF

1. *Certification path validation*: IETF RFC 5280
2. *Proof-of-Possession checking*: IETF RFC 5246
3. *Entity checking*:
   - Client identity:
     - IETF RFC 7589 (certificate-to-name mapping)
     - IETF RFC 8341 (authorization)
   - Server identity: IETF RFC 7589 (expected vs. actual based on addressing info [expected] and SAN extension content* [actual])

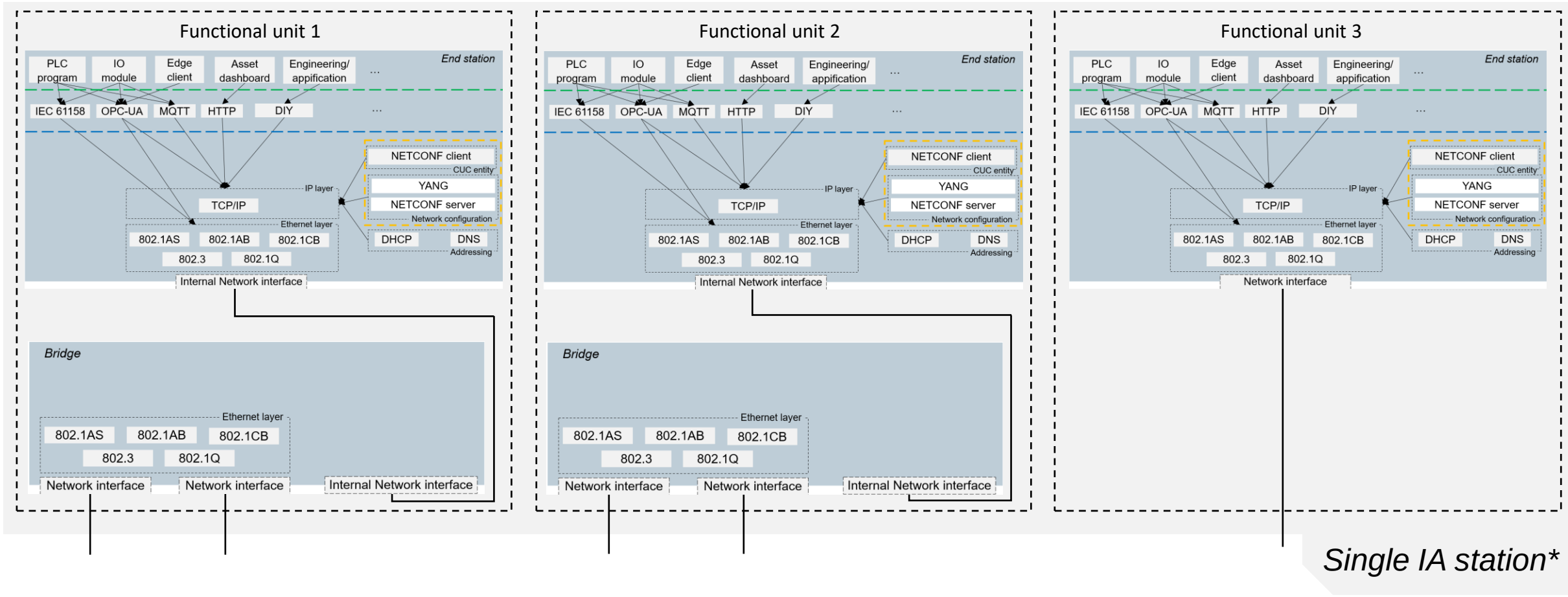
IDevID

1. *Certification path validation*: IETF RFC 5280
2. *Proof-of-Possession checking*: IETF RFC 5246**
3. *Entity checking*:
   - Client identity: n.a. in IEC/IEEE 60802
   - Server identity: expected vs. actual according owner/operator-selected strategies (tbd); upfront candidates:
     i. Any end station/bridge that can authenticate
     ii. …and that is from a dedicated manufacturer
     iii. …and that belongs to a dedicated type
     iv. …and that is a dedicated instance

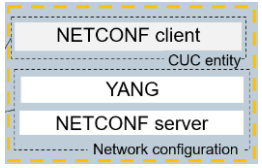
*: see IETF RFC 6125 for the details

**: for IDevID usage with NETCONF-over-TLS

Device Model: IA Stations



*Single IA station**



Represents a single NETCONF/YANG server which serves a single YANG info model that can be reached through multiple network interfaces. Also represents a single NETCONF client.

*: showing an exemplary composition by functional units as well as end stations and bridges

Device Model: LDevID-NETCONF/IDevID Implications

LDevID-NETCONF

- *Number of credentials in an IA station*: by default a **singleton**
  - This credential is used by the single NETCONF/YANG server on the IA station - independent from the IP address by which this server is addressed
  - Its EE certificate shall contain #1..n instance identifiers in form of #1 SAN extension providing #1..n `dNSName` (or `iPAddress`) values

IDevID

- *Number of in an IA station*: by default a **singleton** (per orderable item)
  - This credential is used by the single NETCONF/YANG server on the IA station - independent from the IP address by which this server is addressed
  - Its EE certificate can not contain instance identifiers in form of `dNSName` (or `iPAddress`); these values are not known by the manufacturer (in product business)

Device Identity Model: YANG Module `ietf-hardware`

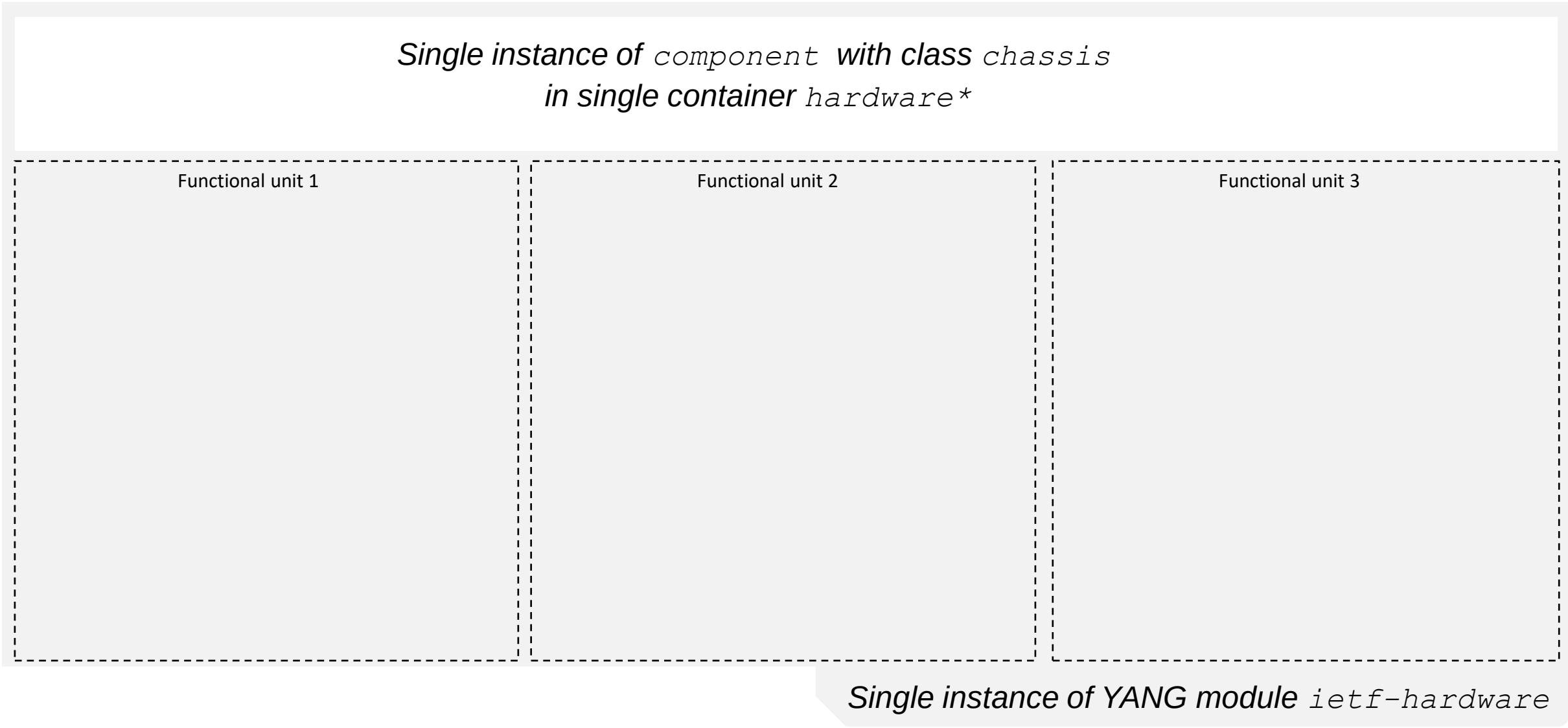
- This section uses IETF RFC 8348 to describe a ‘device identity’ model for IEC/IEEE 60802:
  - IETF RFC 8348 provides a “YANG data model for the management of hardware on a single server”
  - This helps to make the consideration of ‘secure device identity’ concrete. It is meant to be non-normative.
- IETF RFC 8348 defines the YANG modules `iana-hardware` and `ietf-hardware`
  - `iana-hardware` is a predefined and extensible enumeration of understood purposes for a piece of HW
    - Example values: `backplane`, `chassis`, `cpu`, `power supply`…
  - `ietf-hardware` provides a YANG information model to describe a variety of HW-based products in the interval [atomic...composite]
    - The container `hardware` incarnates an `ietf-hardware` info model. It provides a list of `component` items
    - A child object `component` describes a HW item that is classified by the `iana-hardware` enumeration. The management of its values is a shared concern between manufacturers and users:
      - `ro` items are manufacturer-assigned values that are part of the state data (can not be configured)
      - `rw` items are user-managed values that are part of the config data (may be configured)
  - See here for a HelloWorld example of an `ietf-hardware` object in JSON notation

Device Identity Model: `ro` Child* Elements in `component`

- **`physical-index`** (int32, 0..1): a manufacturer-assigned index value to refer to other `component` objects for Entity-MIBs
- **`description`** (string, 0..1) a manufacturer-assigned description
- **`contains-child`** (string, 0..n): a manufacturer-assigned reference to a `component` object in the same `hardware` object
- **`hardware-rev`** (string, 0..1): a manufacturer-assigned hardware revision for the `component`
- **`firmware-rev`** (string, 0..1): a manufacturer-assigned firmware revision for the `component`
- **`software-rev`** (string, 0..1): a manufacturer-assigned software revision for the `component`
- **`serial-num`**: (string, 0..1): a manufacturer-assigned serial number for the `component` (unique per `mfg-name`)
- **`mfg-name`** (string, 0..1): a manufacturer-assigned name for the `component` manufacturer (no registry authority resp. registration process is mentioned in IETF RFC 8348)
- **`model-name`** (string, 0..1): a manufacturer-assigned model name associated with the physical entity
- **`is-fru`** (boolean, 0..1): a manufacturer-assigned Boolean identifying if the physical entity described by this `component` is replaceable
- **`mfg-date`** (date-time, 0..1): a manufacturer-assigned date of manufacturing of the `component`
- **`uuid`**: (uuid, 0..1): a manufacturer-assigned universally unique identifier for this `component`

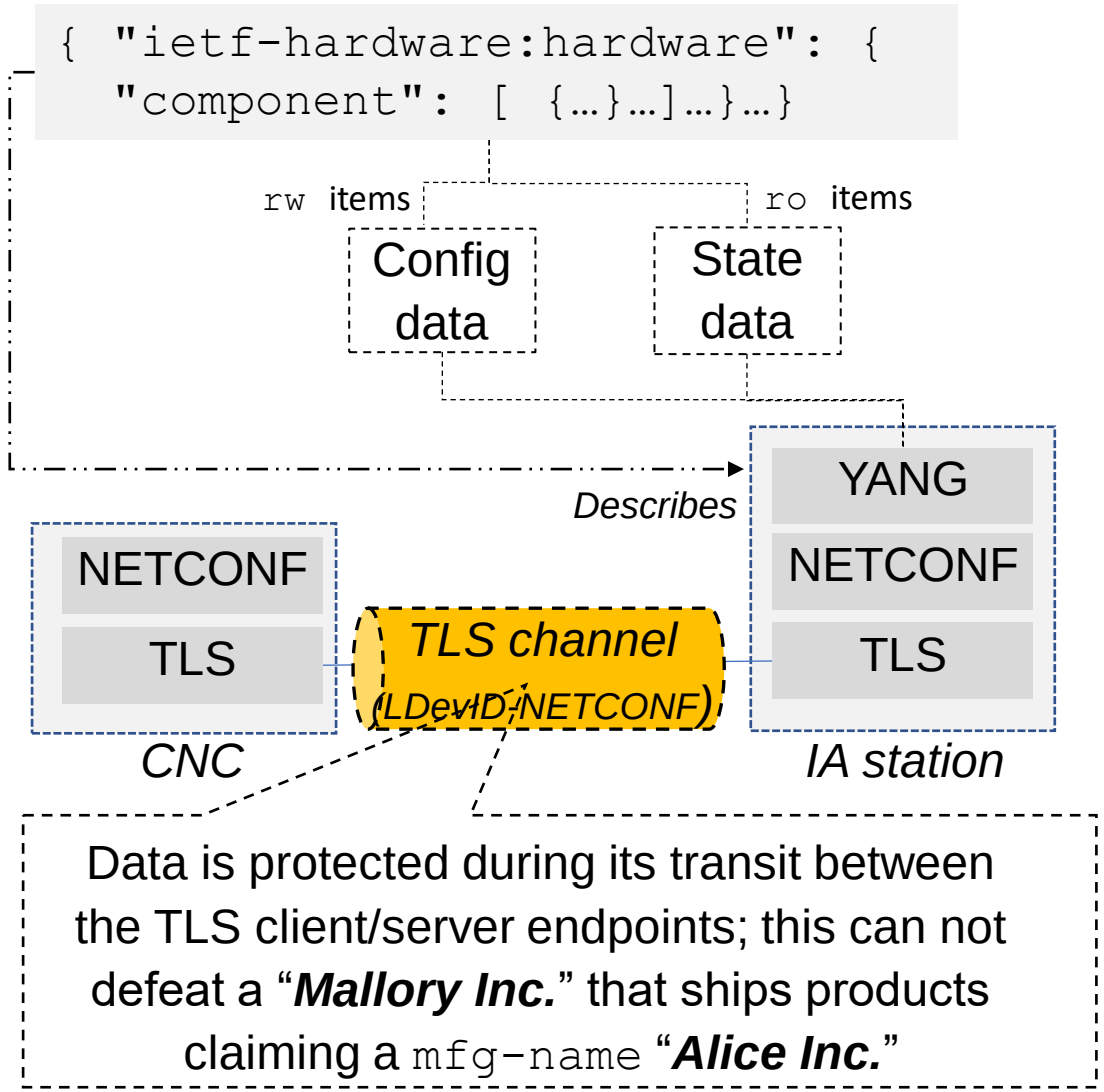
*: there are also `ro` grand-child elements in `component`. They are not considered for brevity

Device Identity Model: IA Stations



*: showing an exemplary `hardware` information model

Device Identity Model: Protection Level



- The information contained in a `hardware` container is not protected on **application-level**. This information is only protected during **transit** (NETCONF-over-TLS)
- Using LDevID-NETCONF credentials, clients (CNC):
  - Can **verify** whether a response to a `hardware` retrieval request was sent by an **authenticated endpoint** over an **authenticated transport**
  - Can **not verify** whether the passed information object is **genuine** i.e. whether or not its manufacturer-supplied subset of a `hardware` container originates from the claimed manufacturer and was not modified
- This creates risks such as **product counterfeiting** and **system integrity/resilience violations** resulting from manipulations such as:
  - False `mfg-name` values (illustrated)
  - False `model-name` values

Device Identity Model: LDevID-NETCONF/IDevID Implications

LDevID-NETCONF

- EE certificate contents for NETCONF/YANG servers:
  - SAN extension with `dNSName` and/or `iPAddress` (IETF RFC 7589, also see RFC 6125)

IDevID

- EE certificate contents for NETCONF/YANG servers:
  - Needs to bind identification information to safeguard manufacturer-specific information in the `ietf-hardware` info model (see below for details)

Secure Device Identity: ‘Device Identity’ Protection Demand

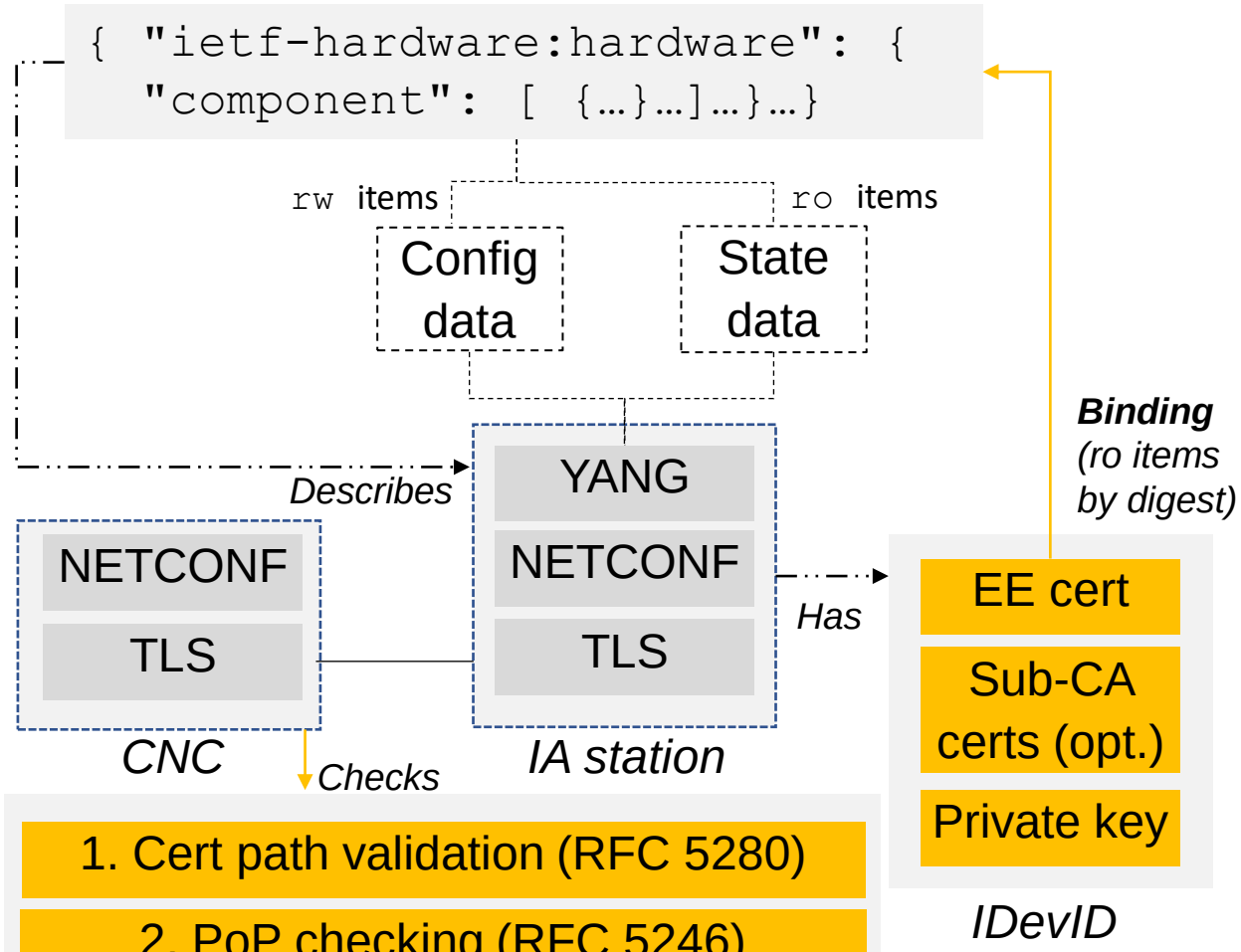
LDevID-NETCONF

- The protection of manufacturer-supplied content in `hardware` containers is **not necessary**
  - Rationale: manufacturer-supplied content in `hardware` containers is checked initially based on an IDevID (and might by re-checked later on this basis); no recurring checks are needed whenever LDevID-NETCONF credentials are used

IDevID

- The protection of manufacturer-supplied content in `hardware` containers **is needed** to address use cases such as:
  - Verify the original equipment manufacturer (*counterfeit protection*)
  - Check whether an IA station is an instance-in-class (*system integrity/resilience*)

Secure Device Identity: Protection Model



- This protection can be provided ***by-reference*** *i.e. an* `otherName` in the IDevID EE certificate carrying:
  - a **reference** to an instance of `ietf-hardware` information object or a part thereof (e.g. `component`)
  - an identification of **pre-digesting transform(s)** e.g. extraction of manufacturer-assigned information
  - an identification of the **digesting algorithm** e.g. SHA2-256 or SHA2-512
  - the **digest-value** of the referred and transformed information in an `ietf-hardware` instance

Notes:

- 'Secure device identity' additions are shown in bold
- The *by-reference* binding requires verifiers to obtain 2 objects (IDevID certification path via TLS and `hardware` container via NETCONF-over-TLS) and to assess these 2 objects in conjunction

Secure Device Identity: Alternative Binding Approaches

- *By-value*: the IDevID EE certificate becomes self-contained (no 2nd object needed). But this duplicates a potentially large set of information items (`hardware` with n>1 `component` child objects), requires YANG-to-ASN.1 syntax transformation for a complex information model (`ietf-hardware`) esp. its linking feature
  ➔ **not preferred**
- *By-URL* (pointing to a protected object)*:* requires verifiers to obtain 3 or more objects (IDevID certification path via TLS and `hardware` container plus a new object providing e.g. a detached signature for manufacturer-specific contents in `hardware` container via NETCONF-over-TLS) and to assess these objects in conjunction
  ➔ **not preferred**
- *By-URL* (pointing to an unprotected object)*:* not smart
  ➔ **not viable**
- *By-context* (`Issuer` field in IDevID EE certificate vs. `mfg-name` in `ietf-hardware` instance): does not protect other manufacturer-specific values in an `ietf-hardware` instance e.g. `model-name`. Introduces syntax-rooted issues: the `Issuer` field is an X.500 name (DN) e.g. `CN=TSN-IA Product CA,OU=IT Department,DC=Alice US,DC=COM`. The `mfg-name` could be a friendly name e.g. "*Alice Inc.*"
  ➔ **not preferred**

Secure Device Identity: Subject-Specific LDevID-NETCONF/ IDevID EE Certificate Contents

LDevID-NETCONF

- EE certificate contents for NETCONF/YANG servers:
  - SAN extension with `dNSName` and/or `iPAddress` (IETF RFC 7589, also see IETF RFC 6125)

IDevID

- EE certificate contents for NETCONF/YANG servers:
  - SAN extension with `otherName` carrying:
    - a **reference** to an instance of an `ietf-hardware` information object or a part thereof
    - an identification of **pre-digesting transform(s)**
    - an identification of the **digesting algorithm**
    - the **digest-value** of the referred and transformed information in an `ietf-hardware` instance

Summary, Follow-Ups

- Reminder: IDevID credentials are required to perform the security setup of an IA-station in factory default according the IETF-defined security model for NETCONF/YANG.
  - The automation of this security setup demands a common design for IDevID EE certificates
  - With some additions more use cases can be facilitated by the IDevID credentials. This includes counterfeiting protection and system integrity/resilience.
- Required follow-ups:
  - Further elaborate on the ‘secure device identity’ model for IEC/IEEE 60802:
    - By-reference details esp. reference mechanism
    - Pre-digesting transform(s) details
    - Details for assessing IDevID EE certificates and `ietf-hardware` information bound to it; supporting several assessment strategies
  - Further elaborate on the ‘device identity’ model for IEC/IEEE 60802 (note: this is at the boundary but not inside the security turf)

Abbreviations

ASN.1	Abstract Syntax Notation no. 1
CA	Certification Authority
Cert	Certificate
CNC	Centralized Network Configuration
CRL	Certificate Revocation List
CUC	Centralized User Configuration
DHCP	Dynamic Host Configuration Protocol
DIY	Do It Yourself
DNS	Domain Name Service
EE	End Entity
HTTP	HyperText Transfer Protocol
IA	Industrial Automation
ID	IDentifier
IDevID	Initial Device ID
IO	Input Output
IOC	IO Controller
IOD	IO Device
IP	Internet Protocol
JSON	JavaScript Object Notation
LDevID	Locally significant Device ID
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
NETCONF	NETwork CONFiguration
OID	Object ID
PLC	Programmable Logic Controller
PoP	Proof-of-Possession
RA	Registration Authority
ro	read only
rw	read write
SAN	Subject Alternative Name
SHA	Secure Hash Standard
STD	STandarD
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
URL	Uniform Resource Locator
UUID	Uniform Resource ID
YANG	Yet Another Next Generation

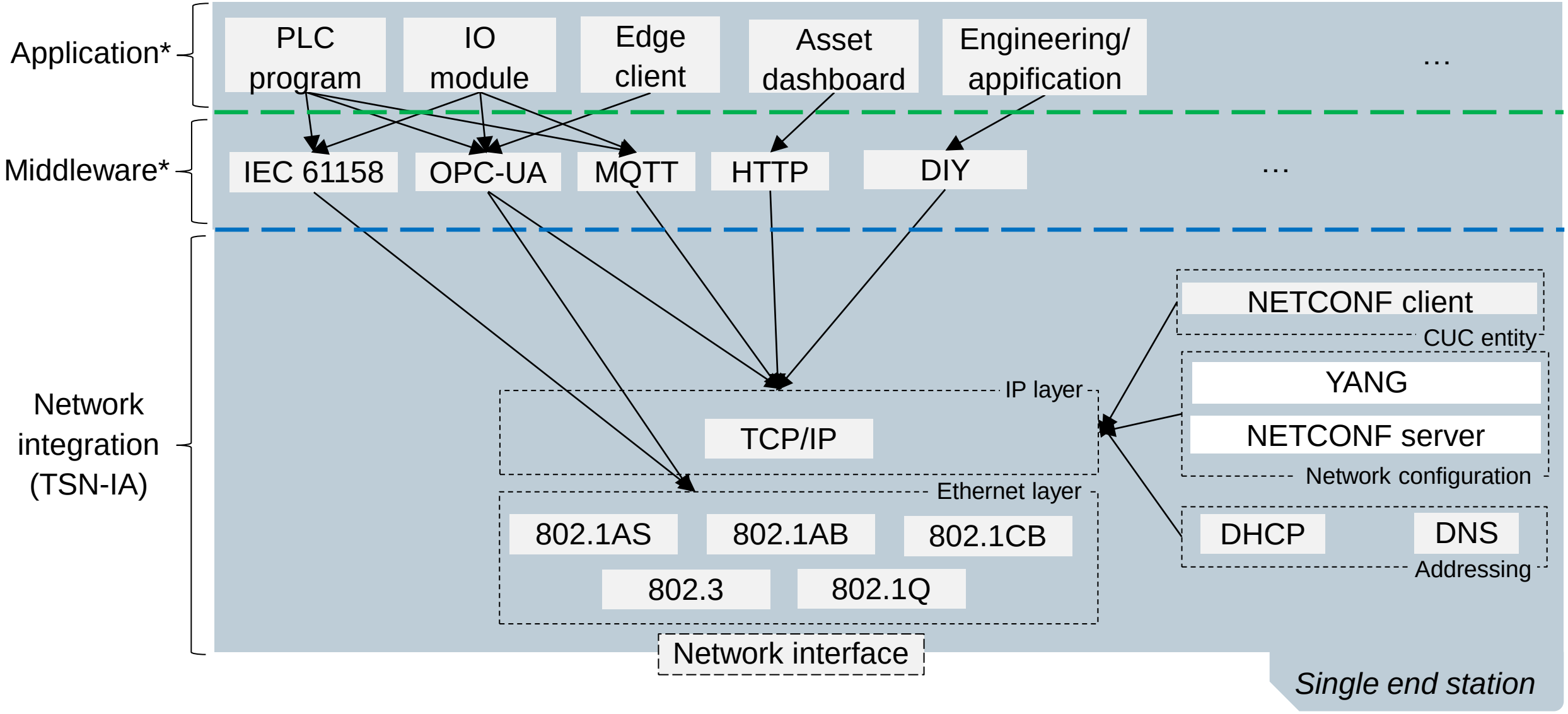
Contacts

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

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

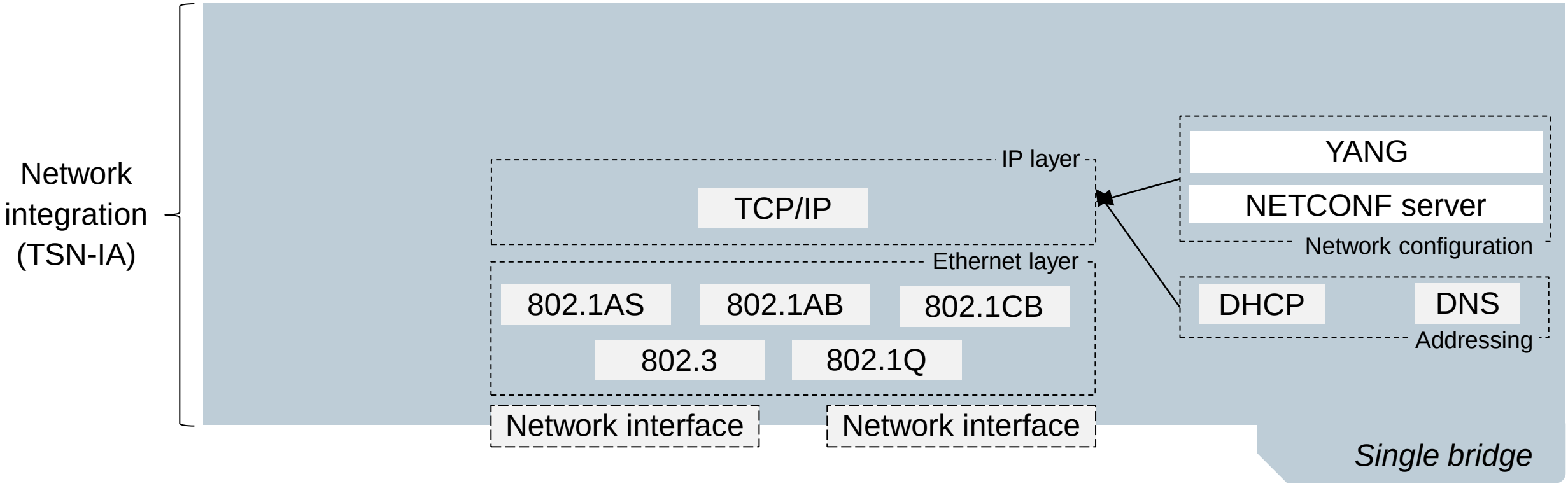
Oliver Pfaff, Siemens AG, DI FA CTR ICO PO, oliver.pfaff@siemens.com

Device Model: End Stations in IEC/IEEE 60802

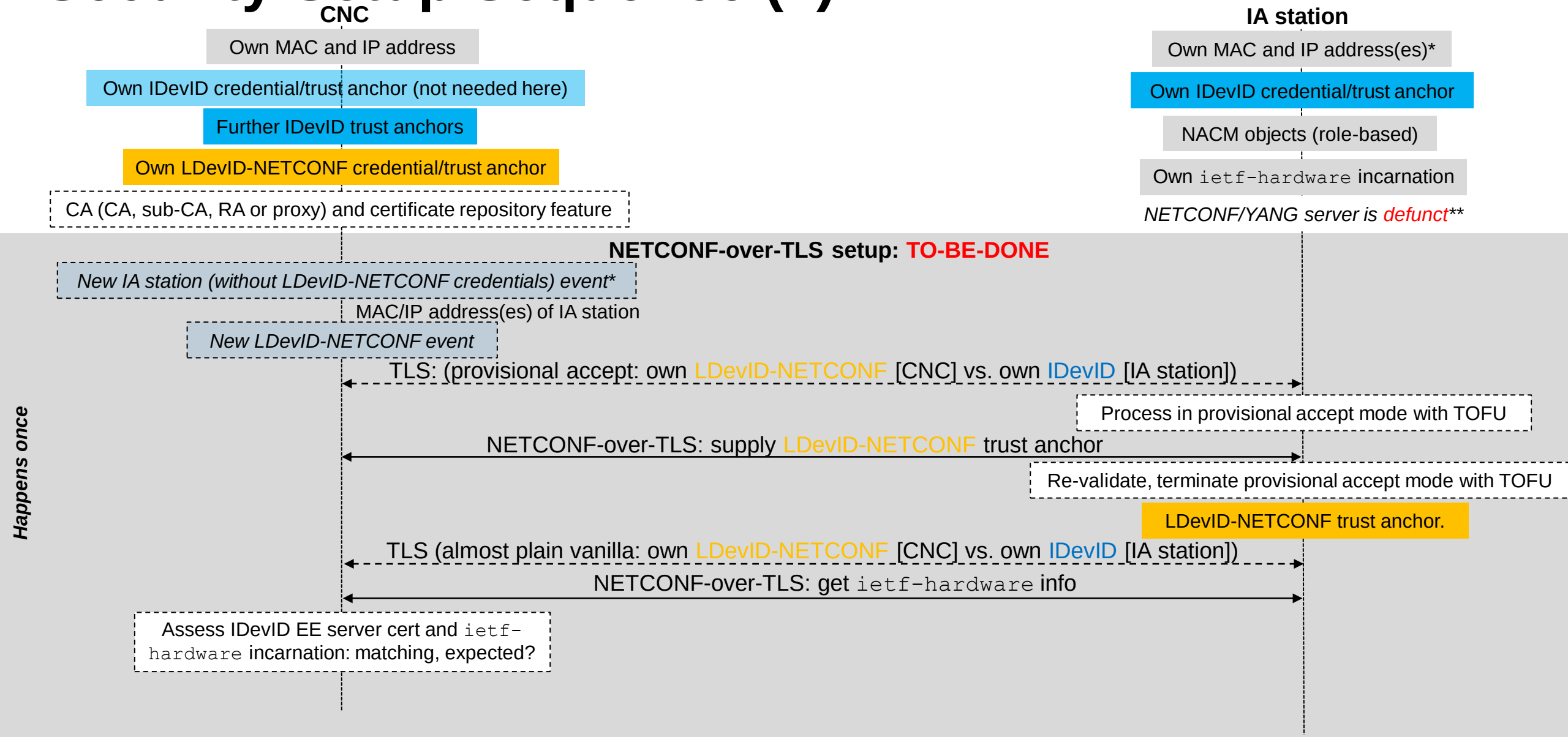


*: showing an exemplary/random suite of middleware/application modules

Device Model: Bridges in IEC/IEEE 60802



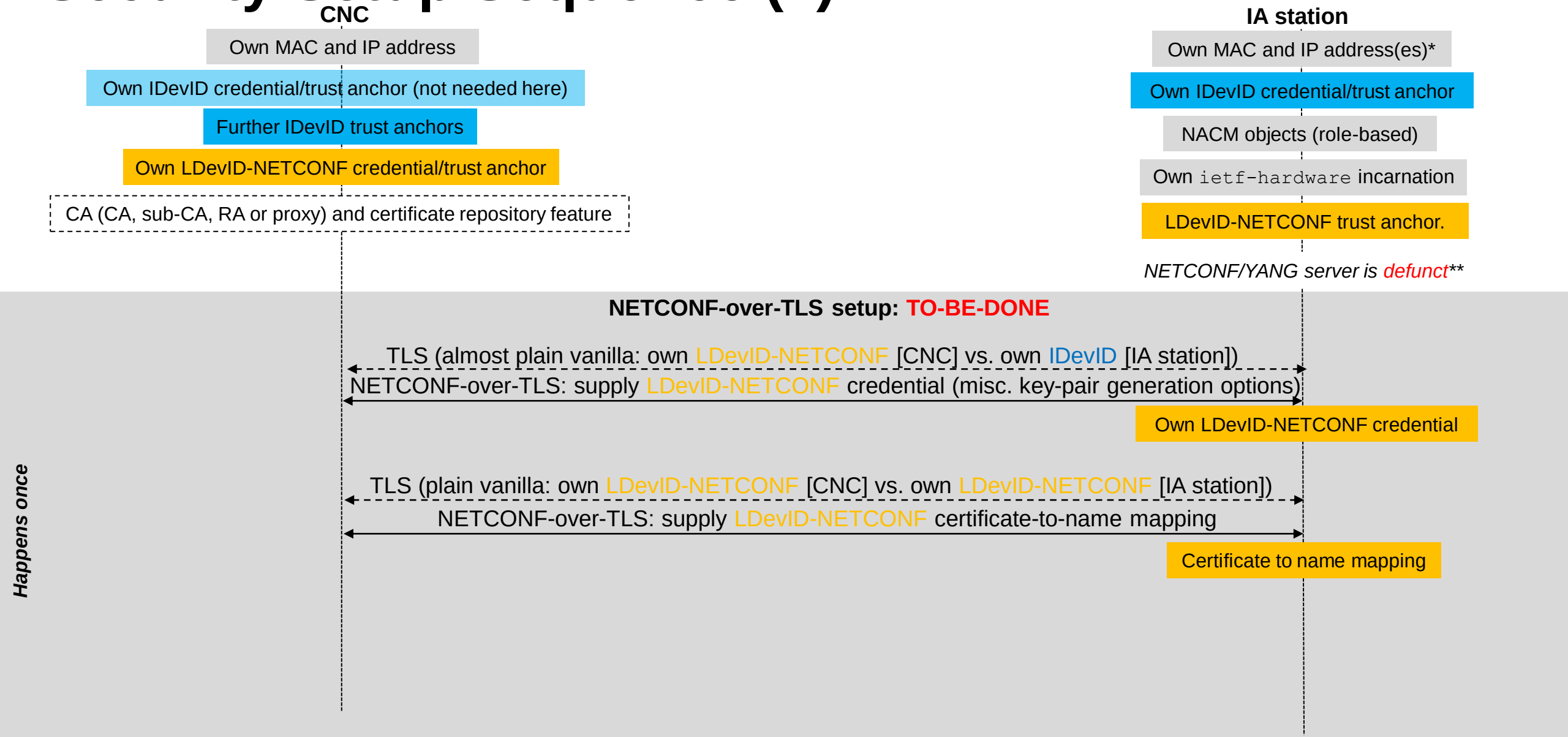
Security Setup Sequence (1)



*: Not detailed herein

**: Does not comply to NETCONF/YANG security rules set forth by IETF RFCs 6241, 7589

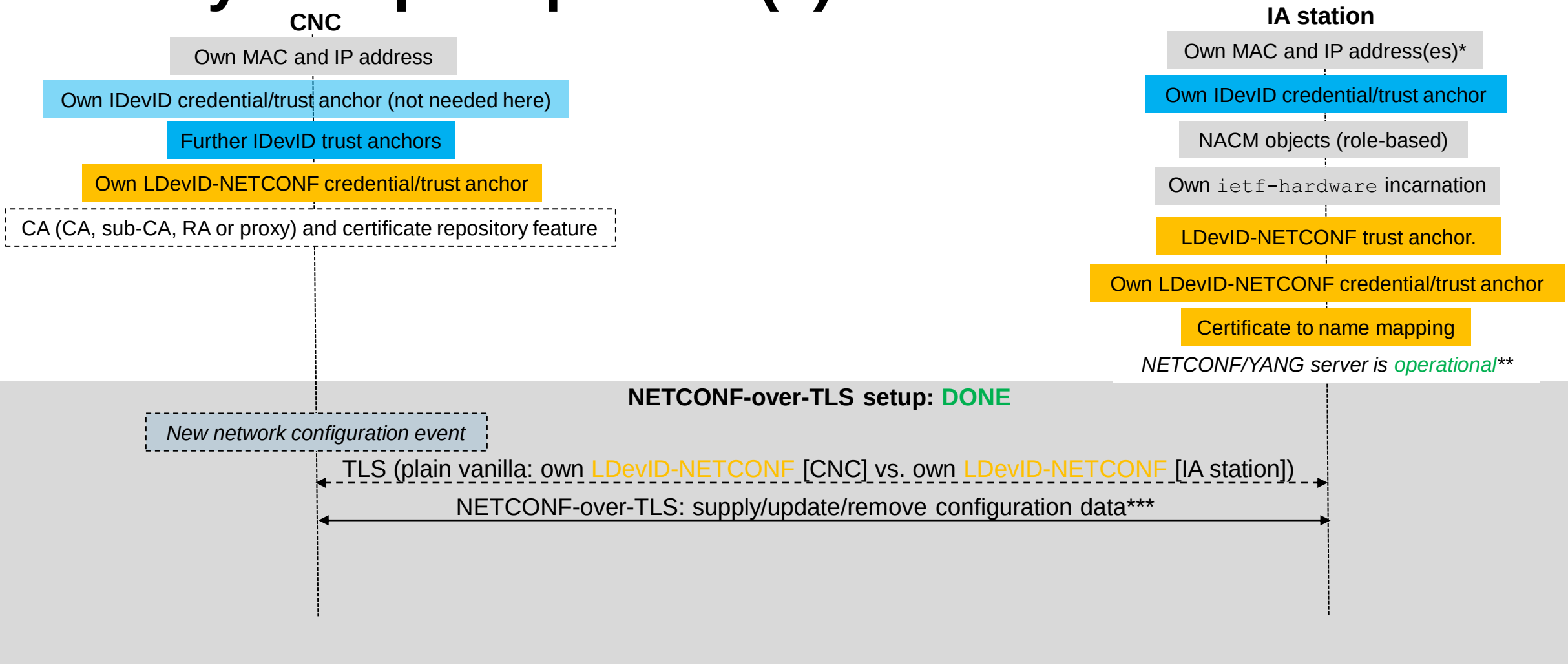
Security Setup Sequence (2)



*: Not detailed herein

**: Does not comply to NETCONF/YANG security rules set forth by IETF RFCs 6241, 7589

Security Setup Sequence (3)



*: Not detailed herein
**: Complies to NETCONF/YANG security rules set forth by IETF RFCs 6241, 7589
***: May encompass LDevID credentials/trust anchors (and further security settings) for middleware/applications

`GeneralName` Choices (IETF RFC 5280)

```
[0] otherName (asn1:OtherName)
[1] rfc822Name (asn1:IA5String)
[2] dNSName (asn1:IA5String)
[3] x400Address (asn1:ORAddress)
[4] directoryName (asn1:Name)
[5] ediPartyName (asn1:EDIPartyName)
[6] uniformResourceIdentifier (asn1:IA5String)
[7] iPAddress (asn1:OCTET STRING)
[8] registeredID (asn1:OBJECT IDENTIFIER)
```