

# Afterthoughts for D1.3/1.4 Security – Impact of TLSv1.3, Alternatives, Risk

IEEE Plenary; July 15, 2022

Kai Fischer, Andreas Furch, Oliver Pfaff

# Problem Statement

- Think again about D1.3 resp. D1.4 security
- This rethinking has the following triggers:
  - The recent appearance of an Internet draft for NETCONF-over-TLSv1.3
  - The question “*is there a cheaper alternative for the NETCONF/YANG security setup than the procedure described in D1.3/1.4?*” that was raised during the F2F in Frankfurt (June 13-15, 2022)
  - The question “*could the NETCONF/YANG security setup procedure in D1.3/1.4 be screwed?*” that was raised during the IEEE May Interim Session presentation about ‘*Secure Device Identity*’ Profile for TSN-IA (May 09, 2022)
- Considered topics:
  - *Impact of **TLSv1.3** as a secure transport for NETCONF*
  - *Alternatives to setting-up security for NETCONF/YANG with an **in-band**\* mechanism*
  - *Risk of screwing something by setting-up security for NETCONF/YANG with an **in-band**\* mechanism*

# Recap of D1.3/1.4 Security

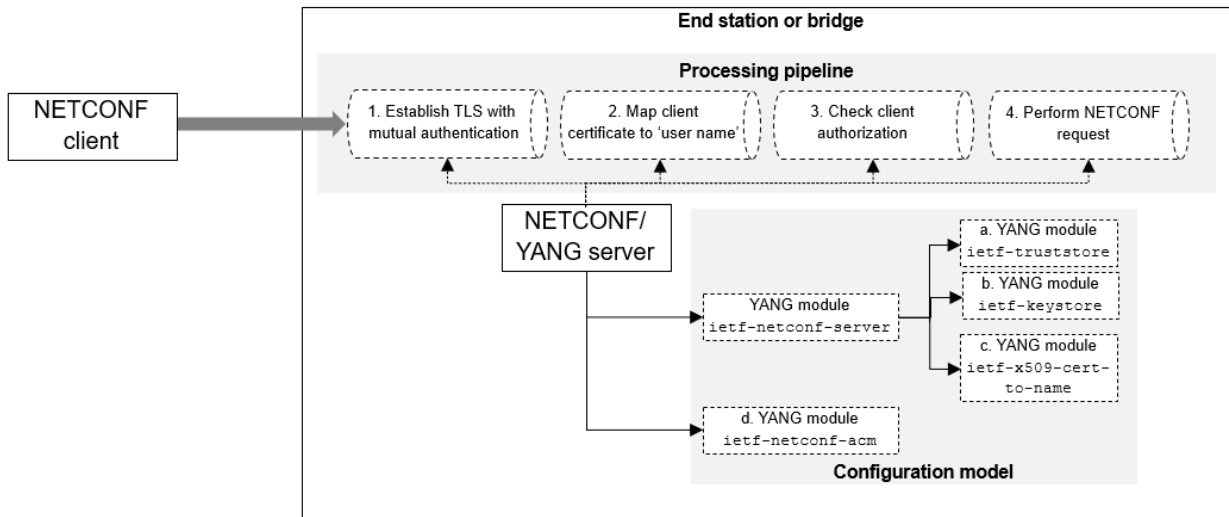
- Already covered in IEC/IEEE 60802 D1.3/1.4; all mentioned items concern NETCONF/YANG:
- **TLS profile** for message exchange protection
- **NACM profile** for resource access authorization - covering security resources different from the YANG module ietf-netconf-acm
- **In-band security setup** utilizing IDevID credentials and trust anchors
- Current backlog (numbering indicates the planned sequence-of-work):
  1. Secure Device Identity (esp. IDevID) profile for TSN-IA
  2. Access authorization for TSN-IA resources beyond the above
    - i. YANG module ietf-netconf-acm
    - ii. Non-security resources in NETCONF/YANG
    - iii. Non-NETCONF/YANG resources
  3. Security for layer 2 protocols in TSN-IA

# Basic Facts (for TLS as NETCONF Secure Transport)

- TLSv1.2 and v1.3 (IETF RFC 5246 and 8446) are in **good standing**; TLSv1.0 and v1.1 are deprecated (IETF RFC 8996). TLSv1.3 is not just an update of TLSv1.2; it is a **full redesign**:
  - It alters some fundamental concepts in TLS esp. ‘cipher suite’
    - TLSv1.3: identifies a 2-tuple (msg encryption and authentication [AEAD], key derivation [HKDF]).  
Example: `TLS_AES_128_GCM_SHA256`
    - TLSv1.2: identifies a 4-tuple (key agreement/establishment, digital signature, msg encryption, msg authentication)\*. Example: `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
  - It adds new conceptual elements such as ‘early data’ aka ‘0-RTT data’
- NETCONF-over-TLS is specified for TLSv1.2 by **IETF RFC 7589**
- An IETF draft document for NETCONF-over-TLSv1.3 was published 2022-06-17 as an **individual submission** ([draft-turner-netconf-over-tls13-00](#)), not yet a WG draft or an IETF RFC. This is a delta-spec to IETF RFC 7589:
  - It adopts things that have to be adopted esp. [cipher suites](#) and [early data](#)
  - It retains the remainders of IETF RFC 7589 including [certificate validation](#), [server identity](#) and [client identity](#)

\*: interpretation varies across classical (described above) and AEAD schemes

# Impact of TLSv1.3 Hit-Pattern

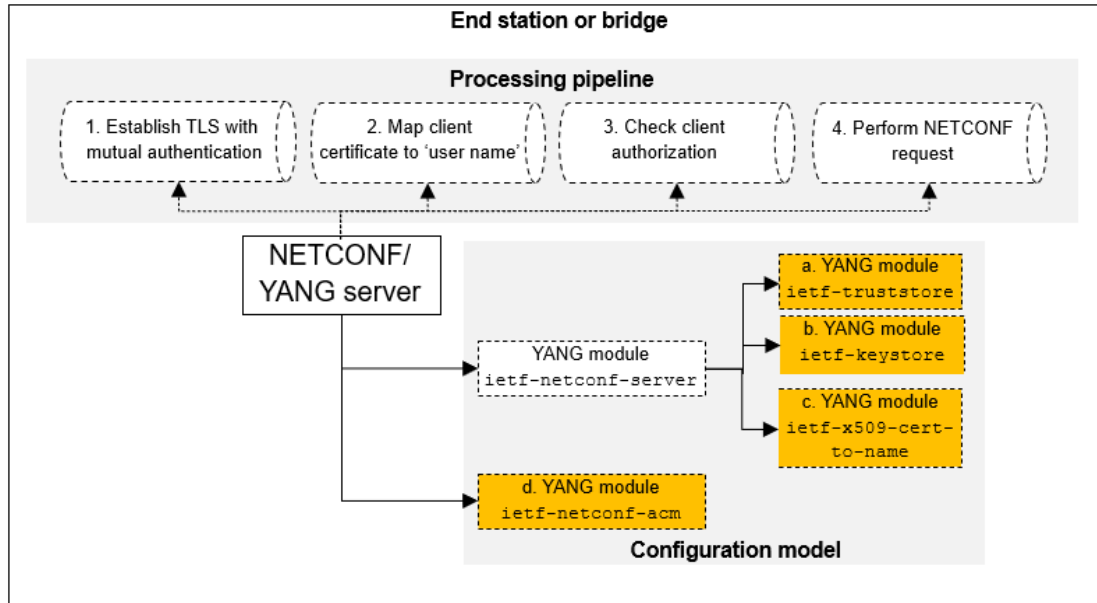


- Not affected:
  - Processing pipeline **steps 2, 3 and 4**
  - YANG modules **a, b, c and d**
  - Suite of **individual cryptographic algorithms** - the cryptographic primitives identified in D1.3 resp 1.4 can be used with TLSv1.2 and TLSv1.3
  - LDevID-NETCONF and IDevID **credential and trust anchor objects** - the objects described in D1.3 resp 1.4 can be used with TLSv1.2 and TLSv1.3
  - YANG modules for **NETCONF client/server configuration**: [ietf-tls-common](#), [ietf-tls-client](#), [ietf-tls-server](#), [ietf-netconf-client](#), [ietf-netconf-server](#) - can be used with TLSv1.2 and TLSv1.3
- Affected:
  - Processing pipeline **step 1** (its internal mechanics, not its features and the main input to/outcome of it)

# Moving Forward

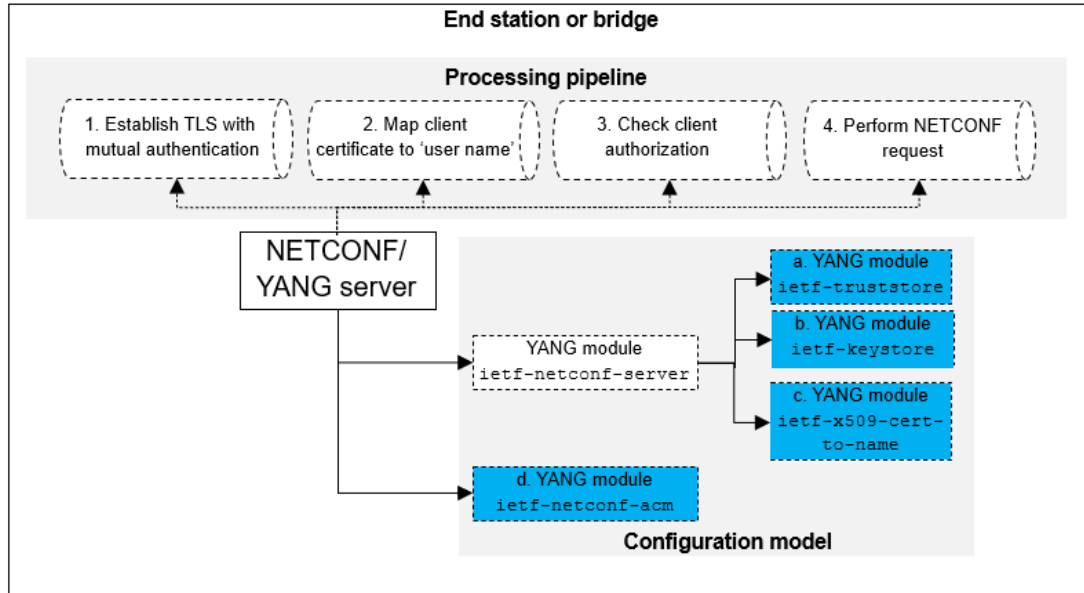
- The planning should envision subsequent points-in-time X, Y and Z ( $\text{now} < X < Y < Z$ ) and following intervals:
  - **[now, X]:** IETF standards cover NETCONF-over-TLS with TLSv1.2 → IEC/IEEE 60802 uses TLSv1.2
  - **[X, Y]:** IETF standards cover NETCONF-over-TLS with TLSv1.2 or v1.3 → IEC/IEEE 60802 may use TLSv1.2 and/or v1.3
  - **[Y, Z]:** IETF standards cover NETCONF-over-TLS with TLSv1.3 → IEC/IEEE 60802 will use TLSv1.3
- **Time-wise**, predicting values for X, Y and Z is difficult - the answer to the '*when?*' question is open:
  - X is likely >2022
  - Y and Z can not be predicted by today
- **Content-wise**, the impact on IEC/IEEE 60802 specification text is quite clear - the answer to the '*what?*' question is pretty obvious (see last slide for a summary)
- There is essentially a **single decision** that will have to be made:
  - Support TLSv1.2 and v1.3 as secure transports for NETCONF/YANG in parallel during the period [X, Y]? Which TLS version as common requirement resp. option?
  - As of today, there is no need to decide about this question

# NETCONF/YANG Server in Operational State



- To meet the security model set forth by the IETF for NETCONF/YANG, the following configuration state must be established at the NETCONF/YANG server of any IEC/IEEE 60802 end station or bridge:
  - must* have a trust anchor which allows to **verify LDevID-NETCONF credentials** that are presented by NETCONF/YANG clients (incl. CNCs)
  - must* have an **own LDevID-NETCONF credential** containing the address info (DNS name or IP address) of this end station or bridge in a SAN certificate extension
  - must* have instructions for the **mapping of LDevID-NETCONF credentials** which are presented by NETCONF/YANG clients (incl. CNCs) to NETCONF 'username' values
  - may* have **locally significant** NACM rules; must have NACM rules

# Factory Default ≠ Operational State



- Modulo YANG module d, this operational state is not existing in factory default. According IEC/IEEE 60802 D1.3/1.4 the factory default comprises:
  - has a trust anchor which allows to **verify IDevID credentials** but NETCONF/YANG clients (incl. CNCs) usually will not have objects from this domain*
  - has an **own IDevID credential** but they can not be assumed to contain the required address info*
  - has an instruction for the **mapping of IDevID credentials** but NETCONF/YANG clients (incl. CNCs) usually will not have objects from this domain*
  - has **initial NACM rules** (IEC/IEEE 60802-specified)*
- The operational state needs to be established from factory default state by a process called **security setup\***

\*: to avoid confusion, it is intentional not to use an already occupied term such as bootstrapping, commissioning, provisioning

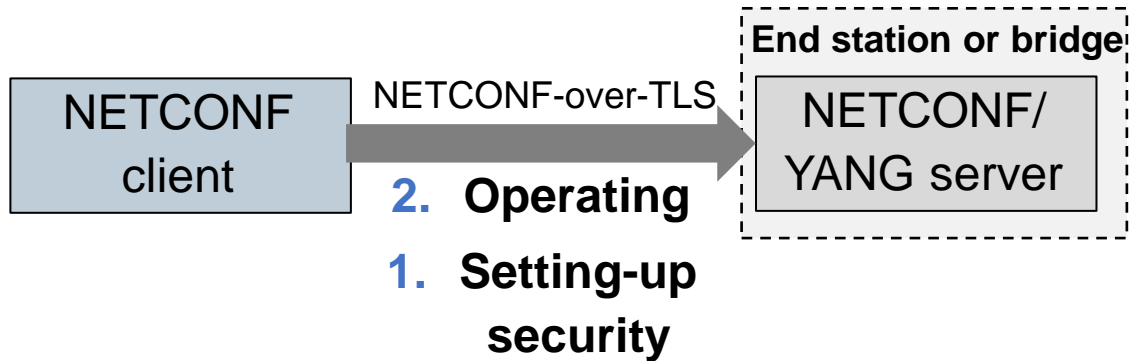


## Alternatives

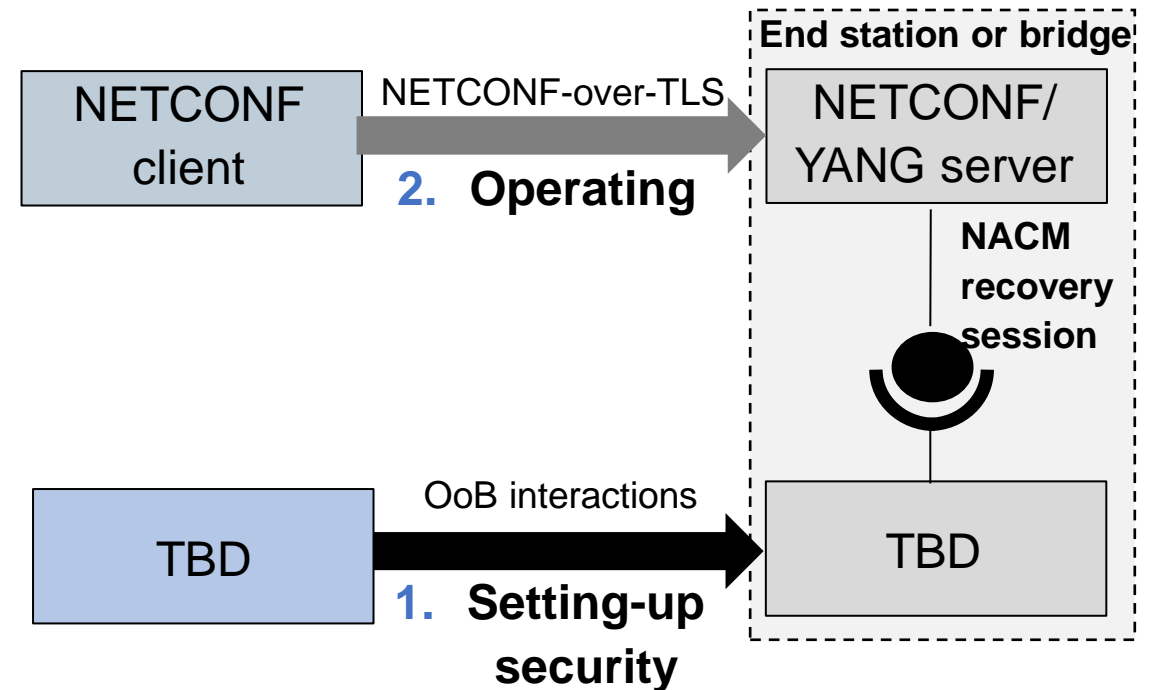
# Goals and Design Options for the Security Setup

- Goal: **interoperable security setup** i.e. a tool by manufacturer A, B or C can be used to perform the security setup for an end station or bridge supplied by manufacturer B
- Design options:




**In-band security setup:**  
use NETCONF/YANG exchanges  
for NETCONF/YANG security setup



**Out-of-band security setup:**  
use other means for  
NETCONF/YANG security setup



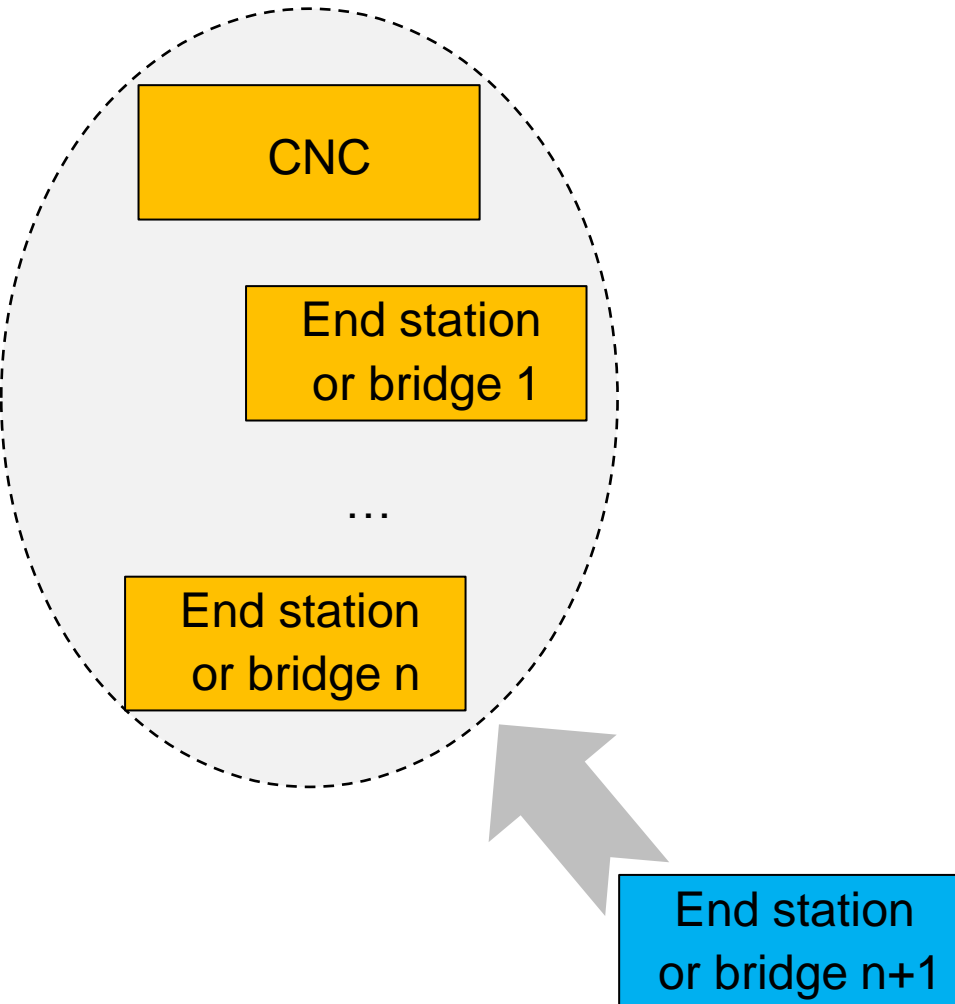
Color code:

-  Manufacturer A
-  Manufacturer B
-  Manufacturer C (might equal A or B)

# Out-of-Band Security Setup

- Feasibility: the concept of the **NACM recovery session** (IETF RFC 8341) allows to do that
- Prerequisites:
  - i. Secondary **means for OoB interaction or supply** e.g. as a network protocol (other than NETCONF) or as removable media
  - ii. The **security model** for the secondary means of interaction covering its message exchange protection and resource access authorization
  - iii. The **processing steps** for the utilization of this secondary means
    - Small-print: i-iii includes (but is not limited) to an incarnation of a NACM recovery session and a model to protect it. Note: the IETF refrains from specifying any incarnation of this
- Assessment: there is no **common requirement** (candidate) in IEC/IEEE 60802 which covers the prerequisites for an interoperable out-of-band security setup
- Conclusion: IEC/IEEE 60802 describes an **in-band mechanism** for facilitating the feature of an **interoperable security setup**

# The Problem Behind an Interoperable Security Setup



- Actual problem:
  - **Introduce** an end station or bridge to the local security domain i.e. equip it with a locally significant credential (LDevID-NETCONF) and corresponding trust anchor – in an interoperable fashion
  - Respect its **native properties**: the introduction process must work based on the ‘common requirements’ for IEC/IEEE 60802 (→ considered in section ‘Alternatives’)
  - Assure its **security**: the introduction process must be sufficiently secure (→ considered in section ‘Risk’)
- Surrounding noise\*:
  - Name of the security protocol family e.g. TLS, SSH
  - Number of the security protocol version e.g. TLSv1.2, v1.3
  - The maths resp. procedural details of the cryptographic algorithm e.g. ECC, RSA/DSA, DH, DHE...

\*: changing items may result in a rephrasing of details of a solution to the introduction problem (security set-up) but does not provide a new solution

# Synopsis of this Introduction Problem

	Client	Server
Trust anchor	Domain-A	Domain-B
Credential	Domain-B	Domain-A with matching SAN

	Client	Server
Trust anchor	Domain-A	None or Domain-X
Credential	Domain-B	None or Domain-Y with no or no matching SAN

	Client	Server
Trust anchor	None or Domain-X	Domain-B
Credential	None or Domain-Y	Domain-A with matching SAN

- **Plain vanilla** case for mutual TLS authentication; HTTP-over-TLS (@IT) or NETCONF-over-TLS (@TSN-IA)
- **Server introduction** problem:
  - IT synopsis: concerns servers in installation state; solved by administrative configuration done OoB and a-priori (rescue option: end-user overrides happening a-posteriori)
  - TSN-IA synopsis: concerns end stations/bridges in factory default; solution is TBD - the IT pattern does not do it
- **Client introduction** problem:
  - IT synopsis: n.a. - client authentication on TLS level is an exception
  - TSN-IA synopsis: concerns end stations in factory default; solution is a corollary of the server introduction → can focus on solving the server introduction problem

# Digesting the IEC/IEEE 60802 Security Set-Up

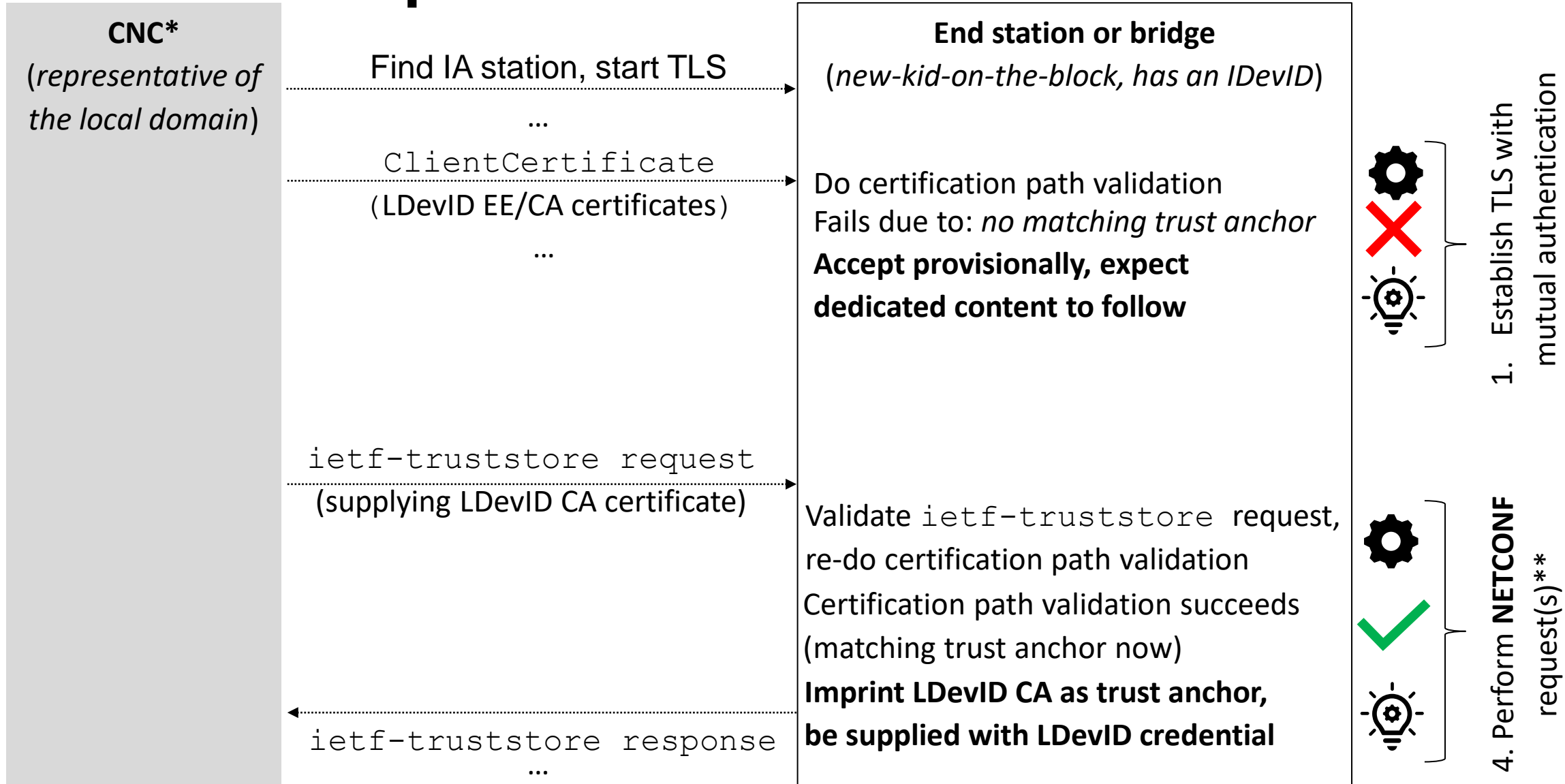
- Synopsis:

	IEC/IEEE 60802
Problem class	Server introduction
Solution class	In-band security setup happening in NETCONF
Security model	<ul style="list-style-type: none"> <li>Local domain: can check a to-be-introduced end station or bridge</li> <li>New component: not meant to check its new home; aims at TOFU</li> </ul>
Application protocol	NETCONF
Component state management	NMDA

- Procedure:

1. Establish secure transport (TLSv1.2 for the time being) according a '**provisional accept**' model
2. Perform NETCONF exchanges over provisionally accepted TLS to supply locally significant information for following YANG modules: ietf-truststore, ietf-keystore, ietf-x509-cert-to-name
3. Terminate secure transport according provisionally accepted TLS
4. Proceed with operational state (plain vanilla)

# 'Provisional Accept' in IEC/IEEE 60802



\*: encounters naming info from a non-local domain (IDevID) during the 'provisional accept' exchange

\*\* : intentional numbering for an alignment with the NETCONF/YANG processing pipeline

# Digesting the IETF RFC 8995 (BRSKI) Security Set-Up

- Synopsis:

	IETF RFC 8995 (BRSKI)
Problem class	Client introduction
Solution class	In-band security setup happening in HTTP*
Security model	<ul style="list-style-type: none"> <li>Local domain: can check a to-be-introduced component</li> <li>New component: can check its new home; aims beyond TOFU. Note: this creates added complexity esp. voucher request/response objects, MASA components</li> </ul>
Application protocol	Misc. including HTTP
Component state management	None

- Procedure:

1. Establish secure transport (TLSv1.3) according a '**provisional accept**' model
2. Perform HTTP exchanges over provisionally accepted TLS to supply locally significant information (trust anchor and credential)
3. Terminate secure transport according provisionally accepted TLS
4. Proceed with operational state (plain vanilla)

# 'Provisional Accept' in IETF RFC 8995 (BRSKI)

1. Establish TLS with mutual authentication



**IoT component**  
*(new-kid-on-the-block, has an IDevID)*

Do certification path validation  
Fails due to: *no matching trust anchor*  
**Accept provisionally, expect dedicated content to follow**

Discover registrar, start TLS

**Registrar\***  
*(representative of the local domain)*

ServerCertificate  
(LDevID EE/CA certificates)

4. Perform HTTP request(s)\*\*



Validate Voucher response, re-do certification path validation  
Certification path validation succeeds (matching trust anchor now)  
**Imprint LDevID CA as trust anchor, acquire LDevID credential**

VoucherRequest

Acquire voucher (sync/async)



VoucherResponse (supplying LDevID CA certificate)

\*: encounters naming info from a non-local domain (IDevID) during the 'provisional accept' exchange

\*\* : intentional numbering for an alignment with the NETCONF/YANG processing pipeline



# Summary

- *Impact of **TLSv1.3** as a secure transport for NETCONF*
  - The impact is **minor** for IEC/IEEE 60802 security
  - The **timeline** requires more attention than the actual content
- *Alternatives to setting-up security for NETCONF/YANG with an **in-band** mechanism*
  - In-band security set-up: allows to be **manufacturer-agnostic**; works with generic CNCs in online engineering scenarios (plug&produce); is elaborated by IEC/IEEE 60802
  - Out-of-band security set-up: is limited to being **manufacturer-specific**; works with manufacturer-specific tools in offline engineering; regarded a manufacturer-specific option that is not elaborated by IEC/IEEE 60802
- *Risk of screwing something by setting-up security for NETCONF/YANG with an **in-band** mechanism*
  - Risk is **equivalent** to the provisional accept mechanism in IETF RFC 8995 (BRSKI) being screwed
  - The **same** basic ingredients are utilized by IEC/IEEE 60802 security – just in **another composition** (for a reason)

# Abbreviations

AEAD	Authenticated Encryption with Added Data	OoB	Out-of-Band
ASN.1	Abstract Syntax Notation Nb. 1	OS	Operating System
BRSKI	Bootstrapping Remote Security Key Infrastructure	OT	Operational Technology
CA	Certification Authority	RSA	Rivest Shamir Adleman
CNC	Centralized Network Configuration	RTT	zero Round Trip Time
DevID	Device ID	SAN	Subject Alternative Name
DH	Diffie-Hellman	SZTP	Secure Zero Touch Provisioning
DHE	Diffie-Hellman Ephemeral	TOFU	Trust On First Use
DSA	Digital Signature Algorithm	TLS	Transport Layer Security
ECC	Elliptic Curve Cryptography	TSN	Time-Sensitive Networking
EE	End Entity	YANG	Yet Another Next Generation
HMAC	Hash-based Message Authentication Code		
HKDF	HMAC-based Key Derivation Function		
IA	Industrial Automation		
ID	IDentifier		
IDevID	Initial Device ID		
IT	Information Technology		
LDevID	Locally significant Device ID		
MASA	Manufacturer Authorized Signing Authority		
NACM	NETCONF Access Control Model		
NETCONF	NETwork CONFiguration		
NMDA	Network Management Datastore Architecture		

# | Contacts

Kai Fischer, Siemens AG, T CST SES-DE, [kai.fischer@siemens.com](mailto:kai.fischer@siemens.com)

Andreas Furch, Siemens AG, T CST SES-DE, [andreas.furch@siemens.com](mailto:andreas.furch@siemens.com)

Oliver Pfaff, Siemens AG, DI FA CTR ICO PO, [oliver.pfaff@siemens.com](mailto:oliver.pfaff@siemens.com)

# Benchmarking of Security Setup Mechanisms\*

	IEC/IEEE 60802	IETF RFC 8995 (BRSKI)	IETF RFC 8572 (SZTP)
Problem class	Server introduction	Client introduction	
Solution class	In-band security setup**		Out-of-band security setup (uses HTTP)
Security model	Local domain: can check the to-be-introduced component		
	New component: not meant to check its new home; aims at TOFU	New component: can check its new home; aims beyond TOFU	
Application protocol	NETCONF	Misc. especially HTTP	NETCONF
Component state management	NMDA	None	NMDA
Added complexity (checking the new home)	None	Voucher request/response objects, MASA components etc.	

\*: selected security set-up mechanisms

\*\* : assumes utilization of HTTP as an application protocol in case of IETF RFC 8995 (BRSKI)

# Out-of-Band Security Setup by NACM Recovery Session

2. Operating

NETCONF client

NETCONF exchanges over the network

(subject to the processing pipeline and configuration model given for NETCONF/YANG servers)

NETCONF/  
YANG server

**NACM recovery session:**  
conceptual element (IETF RFC 8341)  
allowing NETCONF/YANG servers to  
escape from the pipeline and configuration  
model – on an individual basis

OS user privileges: <least>

1. Setting-up security

TBD

OoB interactions (remote/local)

(non-NETCONF, possibly using another  
networking mechanisms e.g. nearfield)



OoB exchanges via local  
inter-process communications

TBD

OS user privileges: <root>

System component

Color code:



Manufacturer A



Manufacturer B



Manufacturer C (might equal A or B)