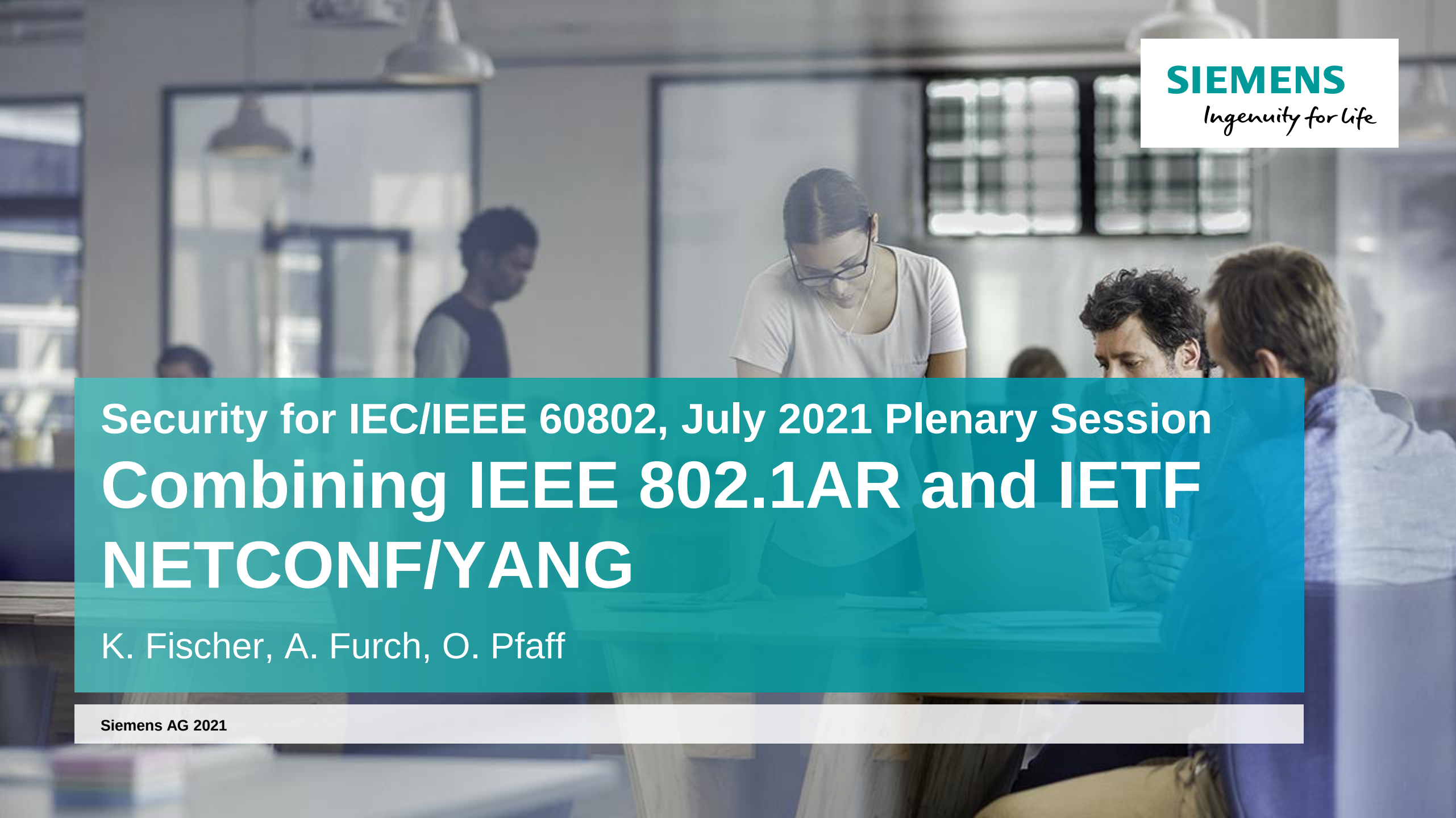


SIEMENS
Ingenuity for life

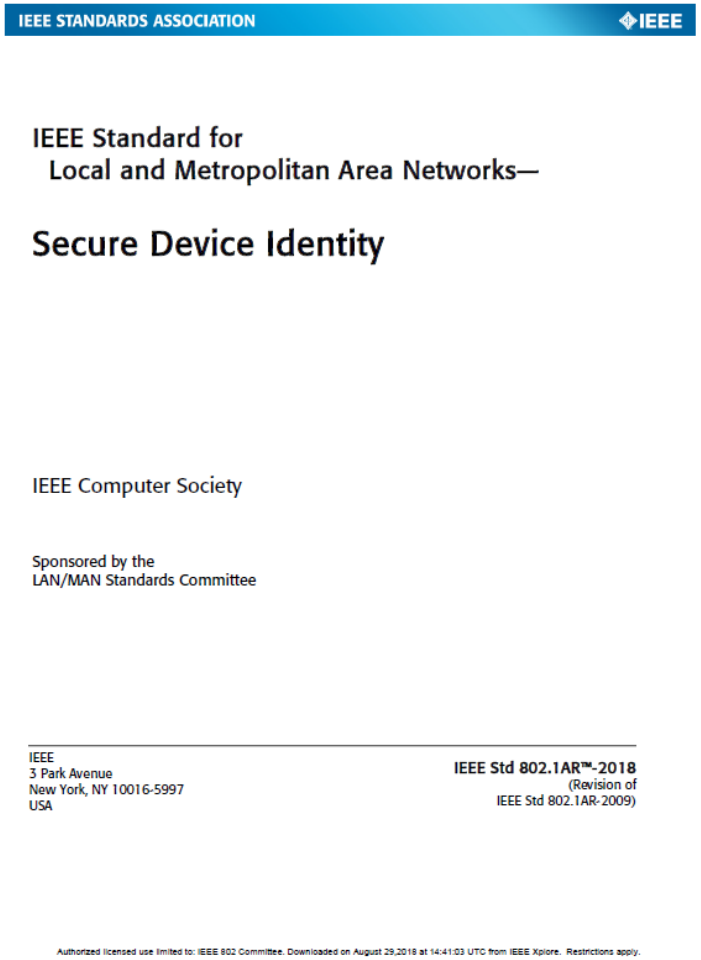
Security for IEC/IEEE 60802, July 2021 Plenary Session

Combining IEEE 802.1AR and IETF NETCONF/YANG

K. Fischer, A. Furch, O. Pfaff

Why IEEE 802.1AR?

SIEMENS
Ingenuity for life


IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for
Local and Metropolitan Area Networks—

Secure Device Identity

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

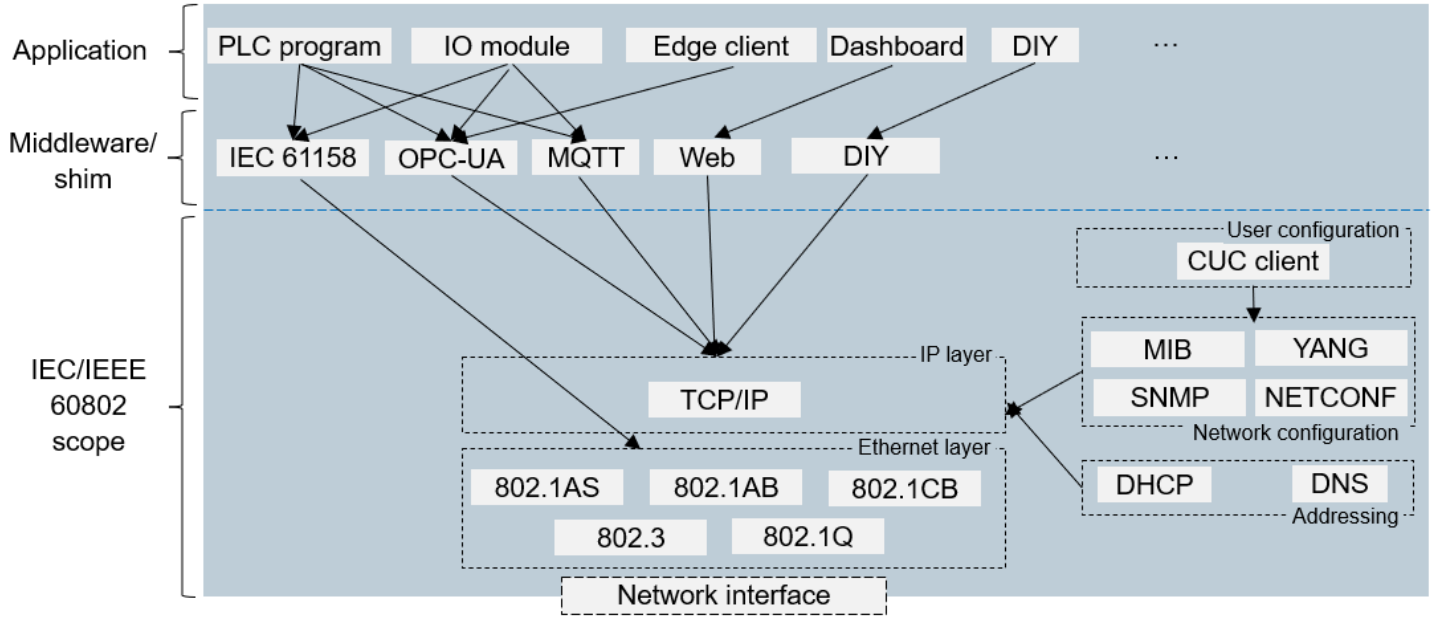
IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.1AR™-2018
(Revision of
IEEE Std 802.1AR-2009)

- **Asymmetric cryptography** is superior to symmetric with respect to entity authentication
  - Symmetric cryptographic based on authenticated key establishment is used for message protection
- **X.509 public key certificates** are the best current practice for utilizing public keys in distributed systems
  - If this will remain true on the long run has to be seen
- **HW-based products** allow to built-in sensitive information by the ‘time of birth’ and can make its cloning difficult
  - Difficult with human users (built-in sensitive information)
  - Difficult with pure SW (prevent cloning)
- 802.1AR has the **foundational concept** to equip HW-based products with objects for asymmetric cryptography using a “*birth certificate* ➔ *ID card* ➔ *driving license*” metaphor

Why NETCONF/YANG?

SIEMENS
Ingenuity for life

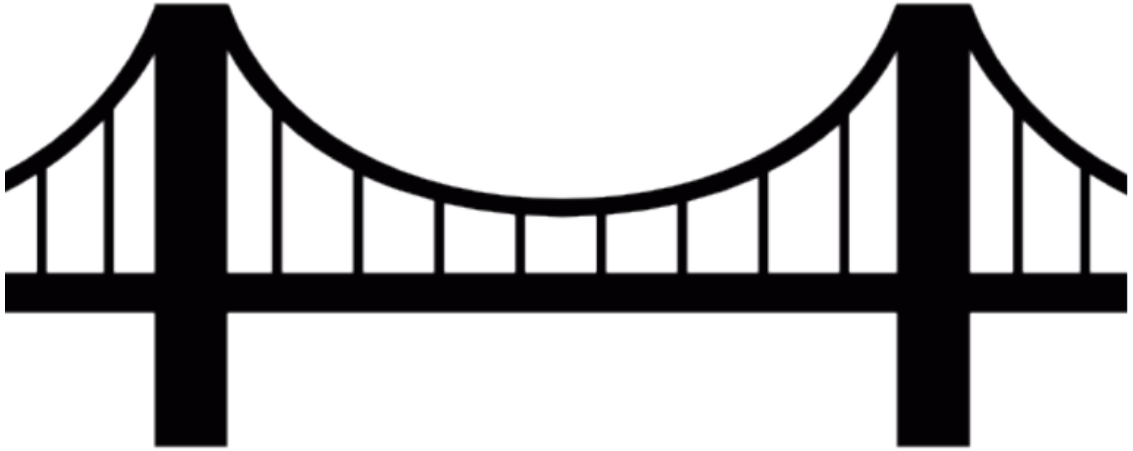


- Means of interaction that are **always available** on an IA component are needed to perform the supplies according 802.1AR in a way that is interoperable and manufacturer-neutral:
  - This is true for **NETCONF/YANG** (modulo the "*and/or SNMP/MIB*" discussion not addressed herein)
  - This is not true for any of the identified middleware/application components

Hint: *the dashed blue line matters with respect to that*

Why Combining 802.1AR and NETCONF/YANG?

SIEMENS
Ingenuity for life



IEEE 802.1AR

- *Provides*: foundational concept and terminology
- *Not covers*: architectural building blocks for its implementation

IETF NETCONF/YANG

- *Provides*: architectural building blocks for configuring network components
- *Not covers*: details for a push-supply according 802.1AR

Which NETCONF/YANG Building Blocks to Consider?

SIEMENS
Ingenuity for life

- Internet standards:
  - RFC 6241 Network Configuration Protocol (NETCONF) ← *protocol for configuring a network component*
  - RFC 7589 Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication ← *message exchange protection for network configuration*
  - RFC 7950 The YANG 1.1 Data Modeling Language ← *basic info model for network configuration*
  - **RFC 8341 Network Configuration Access Control Model** ← *resource access authorization for network configuration*
  - **RFC 8526 NETCONF Extensions to Support the Network Management Datastore Architecture** ← *management model for handling of network configuration*
  - **RFC 8808 A YANG Data Model for Factory Default Settings** ← *info model for factory reset*
- NETCONF WG draft documents (work-in-progress):
  - **draft-ietf-netconf-trust-anchors-15 A YANG Data Model for a Truststore** ← ***info model for trust anchors***
  - **draft-ietf-netconf-keystore-22.html A YANG Data Model for a Keystore** ← ***info model for credentials***
  - draft-ietf-netconf-crypto-types-20.html YANG Data Types and Groupings for Cryptography ← *underpinnings*

Bold: HTTP/CoAP camp does not have equivalents

What Shall Be Achieved?

SIEMENS
Ingenuity for life

- **Imprinting** of production cell/site-specific **trust anchors** and **credentials** to system components that boot with factory default – in an interoperable, manufacturer-neutral way
  - For protecting IEC/IEEE 60802-defined resources and exchanges
  - For protecting other resources and exchanges – *at the discretion of the specification owners or manufacturers of middleware/application components*
- **Subsequent management** incl. adding/renewing/terminating of production cell/site-specific **trust anchors** and **credentials** to system components (that have been initially imprinted) – in an interoperable, manufacturer-neutral way
  - For protecting IEC/IEEE 60802-defined resources and exchanges
  - For protecting other resources and exchanges – *at the discretion of the specification owners or manufacturers of middleware/application components*

Will this Re-Invent the Wheel?

SIEMENS
Ingenuity for life

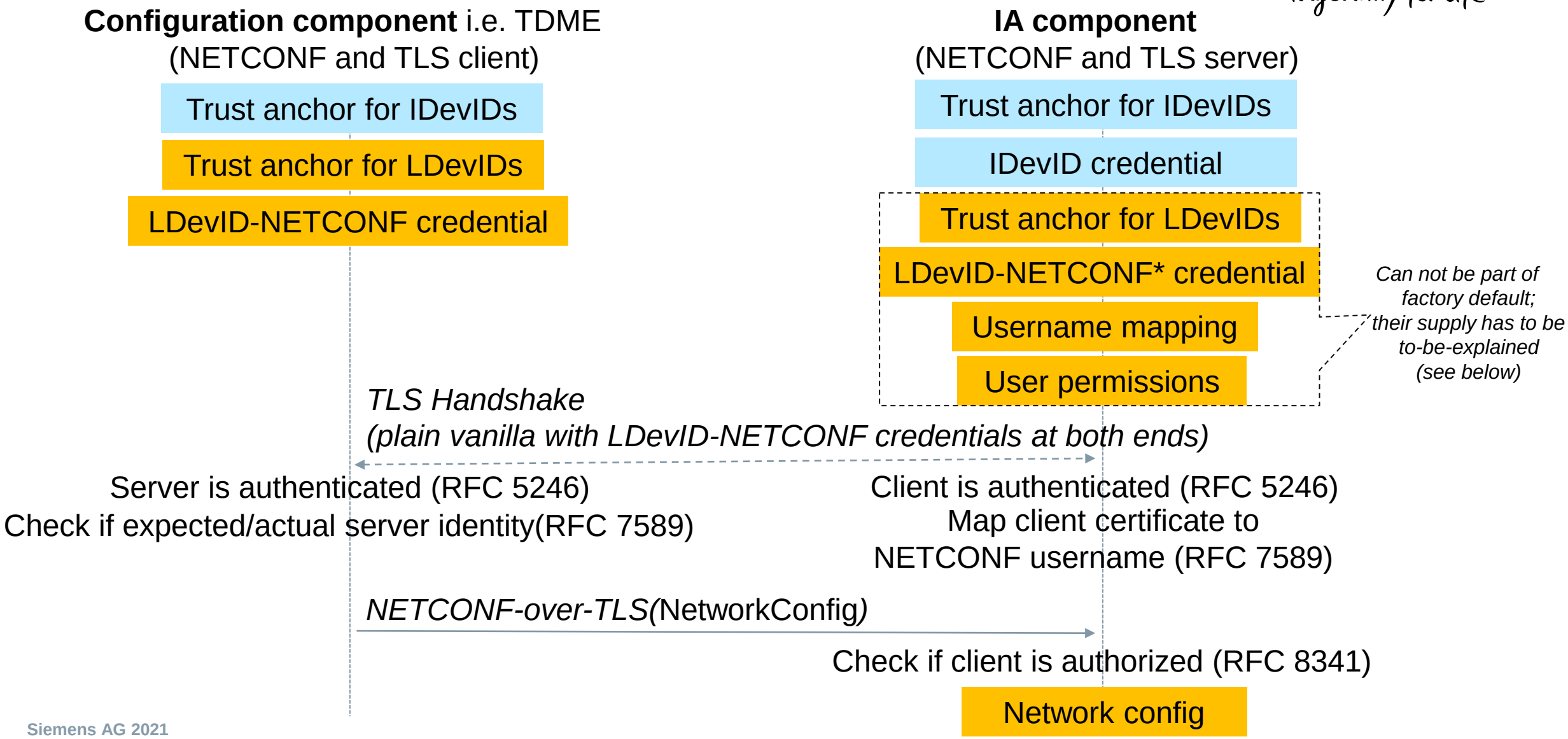
- *Upfront statement*: the level of elaboration that is required by IEC/IEEE 60802 for an interoperable, manufacturer-neutral imprinting of production cell/site-specific trust anchors and credentials and their subsequent management is not provided by current NETCONF/YANG documents
  - Also see slide “Why Combining 802.1AR and NETCONF/YANG?” above
- *Otherwise*: this question will be raised again later; need to look at the 802.1AR and NETCONF/YANG combination first

Will this Boil the Ocean?

SIEMENS
Ingenuity for life

- *Upfront statement*: certainly there is no intent to do that. However we'll encounter some complexity that appears unavoidable
- *Otherwise*: this question will be raised again later; need to look at the 802.1AR and NETCONF/YANG combination first

Which IA Component State Is the Target?



*: short-hand term for an 802.1AR LDevID that fulfills the prerequisites of RFC 7589 (NETCONF-over-TLS)

Expressed In Terms of the Applicable Data Model and Its Stores

SIEMENS
Ingenuity for life

- YANG module `ietf-truststore`:
  - **Owner/operator configured trust anchor for LDevID(-NETCONF) credentials**
  - *Manufacturer built-in trust anchor for verifying IDevID credentials (read-only)*
- YANG module `ietf-keystore`:
  - **Owner/operator configured LDevID(-NETCONF) credential**
  - *Manufacturer built-in IDevID credential (read-only)*
- YANG module `ietf-x509-cert-to-name`:
  - **Owner/operator created configuration instance of the IEC/IEEE 60802-defined cert-to-name mapping**
- YANG module `ietf-netconf-acm`:
  - **Owner/operator configured NACM rules (optional)**
  - *IEC/IEEE 60802-defined and manufacturer built-in NACM rules (read-only)*
- Other YANG modules: not considered

Italics: available when a system component boots with factory defaults
Bold: to be imprinted when a system component boots with factory defaults

What Is the Processing Pipeline?

SIEMENS
Ingenuity for life

1. Establish TLS session with mutual authentication (RFC 7589, RFC 5246)
2. Map client certificate to NETCONF username (RFC 7589, section 7)
3. Enforce client authorization (RFC 8526)
4. Perform configuration operation esp. imprinting (RFC 6241, RFC 7950, RFC 8526, RFC 8808)

Quote from RFC 7589:
*The NETCONF protocol [RFC6241] requires that the transport protocol's authentication process results in an **authenticated NETCONF client identity** whose **permissions** are known to the server. The authenticated identity of a client is commonly referred to as the NETCONF username.*

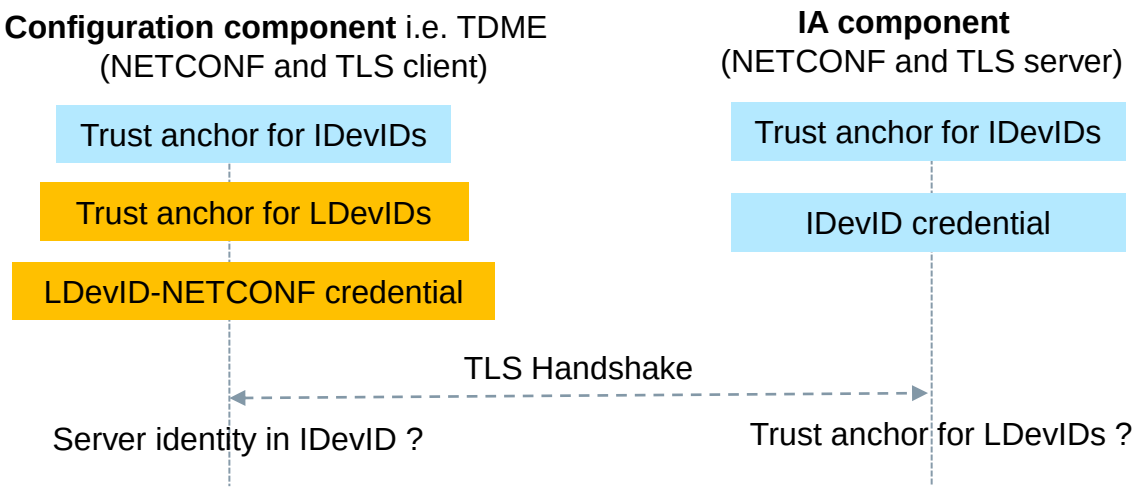
Which Challenges Are Encountered In this Pipeline?

SIEMENS
Ingenuity for life

1. Establish TLS session with mutual authentication (RFC 7589, RFC 5246)
   - Describe add-ons to cover the initial case: server has IDevID credential and trust anchor, client has LDevID-NETCONF credential and trust anchor
2. Map client certificate to NETCONF username (RFC 7589, section 7)
   - Profile this mapping for IEC/IEEE 60802 (role-based)
   - Describe the employment of this mapping (can not be directly done when booting with factory default)
3. Enforce client authorization (RFC 8526)
   - Profile the rules for IEC/IEEE 60802 (role-based)
   - Describe the employment of their enforcement (can not be directly done when booting with factory default)
4. Perform configuration operation (RFC 6241, RFC 7950, RFC 8526, RFC 8808)
   - Profile the configuration requests for writing to the YANG modules `ietf-truststore`, `ietf-x509-cert-to-name`, `ietf-keystore`, `ietf-netconf-acm`
   - Handle the resulting repercussion: imprinting changes the information state for subsequent exchanges

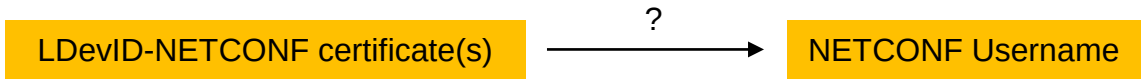
Establishing TLS Session with Mutual Authentication

SIEMENS
Ingenuity for life



- Client identity verification challenge:
  - Use "*PROVISIONAL accept of client cert*" scheme (either trust on first use or protected model)
  - This is mirroring the "*PROVISIONAL accept of server cert*" in RFC 8995 Bootstrapping Remote Secure Key Infrastructure (BRSKI)
  - For details see chapter 4.1.2 herein
- Server identity verification challenge:
  - Use product master data from EE certificate in IDevID e.g. product serial number, MAC address(es), manufacturer/type (see backup slide)
    - Note: the contribution for IEC/IEEE 60802 security evolves according to an incremental, step-by-step approach. For the current increment the system components are assumed to be equipped with IDevID
  - For details see chapter 4.1.1 herein

Mapping Client Certificate to NETCONF Username



- Profiling challenge:
  - Number of mapping entries: 1
    - Certificate `fingerprint`: fingerprint of production cell/site-specific CA certificate
    - Map type: `common-name`
      - Allows usage with role-based authorization model (the other RFC 7589-defined map types e.g. `san-rfc822-name` do not fit roles well)
      - But confines the solution to the X.500 naming scheme (explicitly deprecated by RFC 7589) ➔ an alternative ext-60802-role (new additional map type) would be preferred (in discussion)
  - For details see chapter 5.1.4 herein
- Employment challenge:
  - The mapping entry can not be part of factory default since the `fingerprint` value is not known at manufacturing time
  - Can be addressed by using a specifically privileged session (NACM recovery session), for details see chapter 5.1.5 herein

Enforce Client Authorization Esp. Imprinting

SIEMENS
Ingenuity for life

- Profiling challenge:
  - For illustrations in form of HelloWorld examples (not yet: a fully-fledged suite) of NACM rules for IEC/IEEE 60802 see chapter 5.1.3 herein
  - The mindset behind the current approach is:
    - IEC/IEEE 60802 profiles a fully-fledged suite of NACM rules for protecting IEC/IEEE 60802 resources (including security resources) on a system component.
    - These rules can be supplied by the manufacturer as part of the factory default (read-only). Other actors e.g. owners/operators can employ custom NACM rules for further resources at an own discretion.
- Employment challenge:
  - The IEC/IEEE 60802 profiled NACM permissions can and shall be part of factory default but can not be employed when booting with factory default (a corollary to the employment challenge for the client certificate to NETCONF username mapping)
  - Can be addressed by using a specifically privileged session (NACM recovery session), for details see chapter 5.1.5 herein

Perform Configuration Operation

SIEMENS
Ingenuity for life

- Profiling challenge:
  - For prototypes of NETCONF/YANG exchanges for imprinting production-cell/site-specific trust anchors and credentials see chapter 4.2.2.5.3 herein
    - Trust anchor imprinting in plain form: provided in section 4.2.2.5.3.1.1
    - Trust anchor imprinting in protected form: provided in section 4.2.2.5.3.1.2
    - Credential imprinting with external key generation: provided in section 4.2.2.5.3.2.1
    - Credential imprinting with Internal key generation: provided in section 4.2.2.5.3.2.2
- Repercussion challenge:
  - This imprinting changes the state that is used by itself (the NETCONF/YANG service) with subsequent exchanges
  - Can be addressed by employing a carefully designed sequence of processing steps, for details see chapter 5.1.5 herein

To-Be-Discussed with Security TG

SIEMENS
Ingenuity for life

- Right or wrong direction?
- Support of DevID signature suites with >200 bit security strength e.g. secp521?
- Support of DevID signature suites for Bernstein curve25519 and Goldilocks/Edwards curve448?
- Ability to avoid X.500 naming in EE certificates? Support of product serial number in subject alternative name extension instead subject DN?
- …

Authors

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

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

Oliver Pfaff, Siemens AG, T RDA CST,
oliver.pfaff@siemens.com

Info Items Along the IA Component Lifecycle

SIEMENS
Ingenuity for life

- **Manufacturing phase**
  - *Manufactured*
- **Bootstrapping phase**
  - *Installed*
  - *Commissioned*
- **Operational phase**
  - *(Devices) started*
  - *Application running*
- **Maintenance phase**
  - *Updated*
  - *Application reconfigured*
- **Off-boarding phase**
  - *Decommissioned*
  - *Removed and replaced*
  - *Re-owned*

Info items	Can live in LDevID	Can live in IDevID
Product master data: product serial number, MAC address(es), manufacturer/type/ order ID, HW/SW version…	**Yes**	**Yes**
Deployment master data: application name(s), IP address(es), physical location…	**Yes**	**No** (not known at manufacturing time

Source: Figure 1 in RFC 8576 (modified to fit PROFINET)

Corollaries:

- Deployment master data e.g. application name(s), IP address(es), physical location can not live in IDevID objects; LDevID objects are needed to have a home for this data
- Deployment master data is needed for sound security. As example: RFC 7589 mandates this for NETCONF-over-TLS (similar for other stacks in the IA domain e.g. OPC-UA)