SIEMENS
Ingenuity for life

Security for IEC/IEEE 60802

Overview of Approach

K. Fischer, A. Furch, L. Lindemann, O. Pfaff, T. Pössler, G. Steindl

Siemens AG 2021

The Challenge for IEC/IEEE 60802 Security

SIEMENS
Ingenuity for life

The input for security in IEC/IEEE 60802:

Building blocks for security

The expected outcome:

Tailor-made security for industrial automation

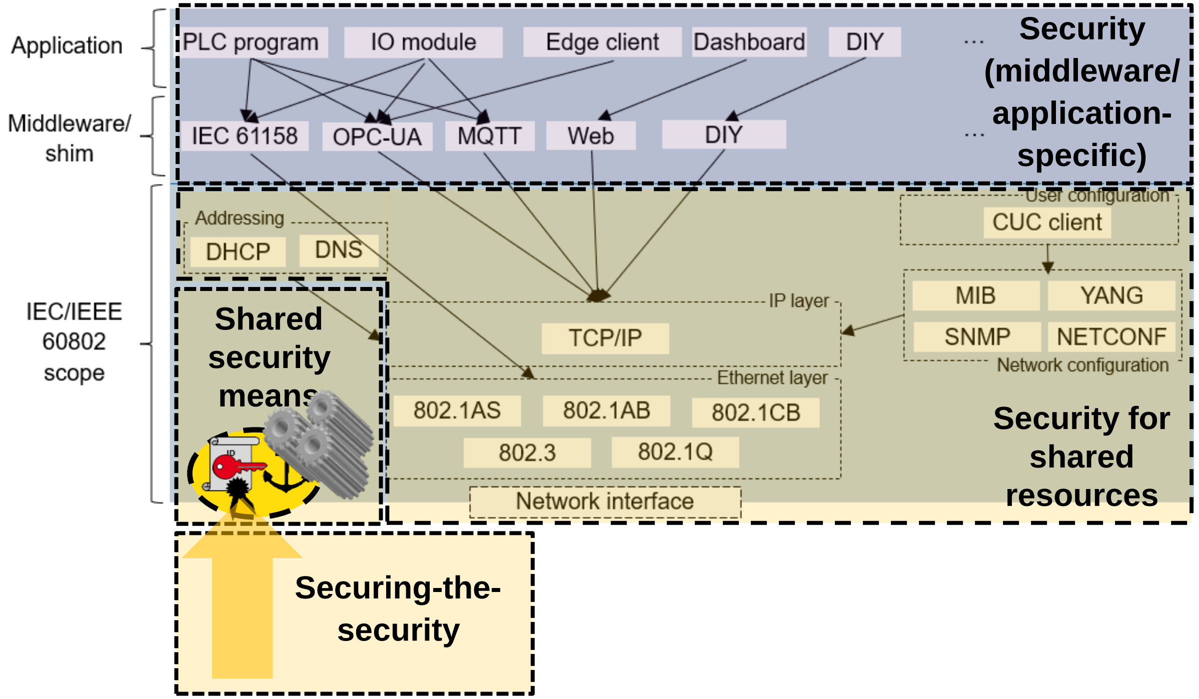
Proposed Approach for the Security Contribution

SIEMENS
Ingenuity for life

1. Kicking-off:
   - Working group presentation, 2021-02-21 (done)
   - Plenary workshop, 2021-03-10 (today incl. a deep-dive preview, using NETCONF as example)
2. Establish goals and constraints, agree on use cases (automation and security-specific)
3. Perform deep-dives for the security technology candidates
   - Shortlist: 802.1AE/X/AR, 802.1AS security, DNS security, NETCONF/SNMP security
   - Longlist (inclusion of items is tbd): BRSKI, COSE, IPsec/IKE, JOSE, LwM2M security, OAuth, OneM2M security, OSCORE…
4. Identify cross-relation/common interests with middleware/application-specific security
   - Shortlist: security for IEC 61158 technologies, OPC-UA security, Web security…
5. Create the blueprint of an overarching security architecture
   - More details are tbd

→ Participation is welcome ←

Proposed Topics for the Security Contribution

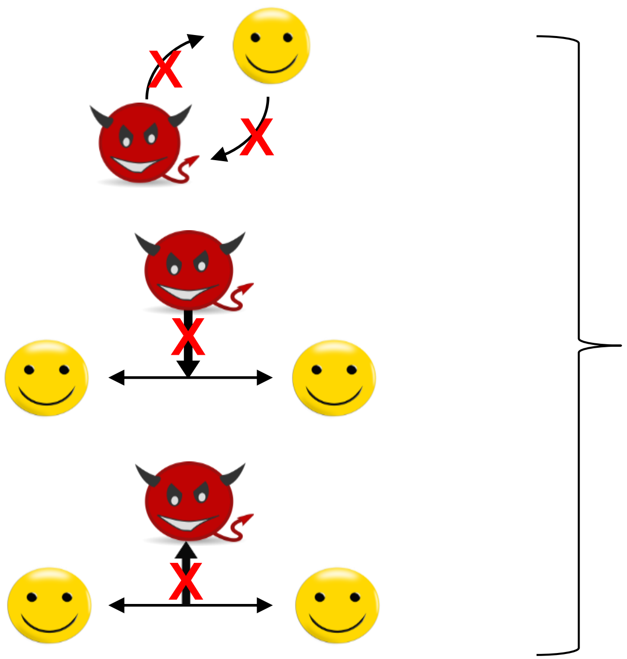


i. **Security for shared resources:** *how to protect resources upon IA devices/controllers that are shared among multiple middleware/applications?* E.g.:
   - Stream establishment
   - Network management

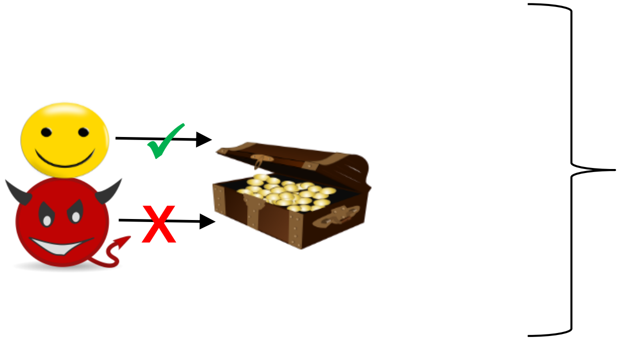
ii. **Shared security means**: *how to facilitate the joint use of singleton means for security upon the IA device/controller?* E.g.:
   - Secure elements providing secure storage and execution environment for keys/credentials

iii. **Securing-the-security**: *how to protect the management of IA device/controller resources underpinning the security?* E.g.:
   - Equipment originality checking
   - Entity/key bindings esp. proving the correctness of identifier(s)/entity association
   - Component-global security configuration

Considered Security Objectives

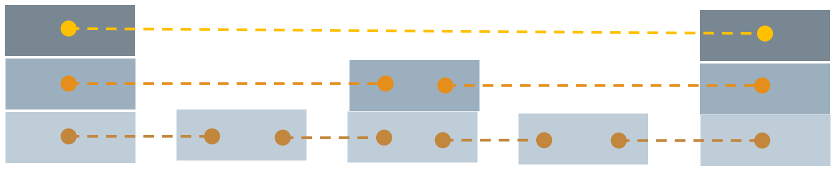


- **Message exchange protection**:
  - *Protect communications against **forgery**, **tampering**, and **eavesdropping***
  - Distinguished properties: (peer) entity authentication, (data) integrity and confidentiality, replay protection, non-repudiation

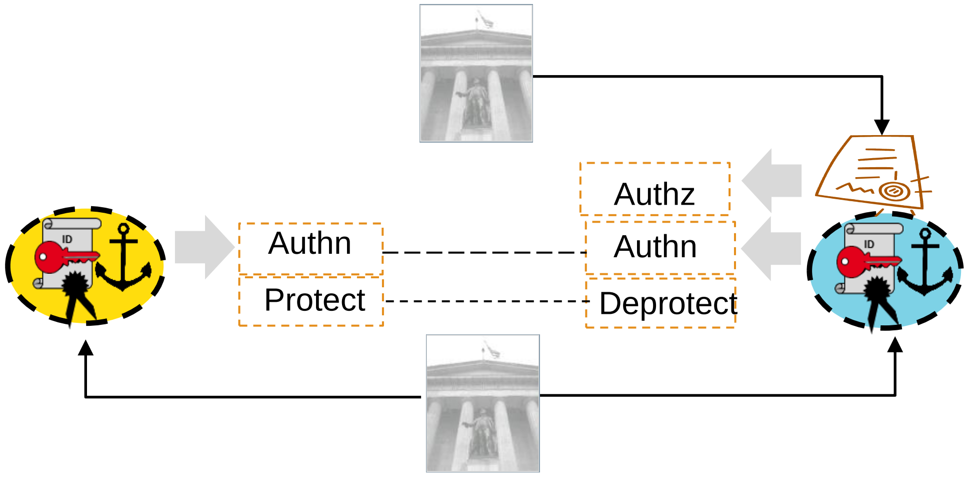


- **Resource access authorization**:
  - *Protect system resources against **unauthorized access***
  - Distinguished aspects: decision enforcement, decision making, policy making, authorization strategy

Properties for these Security Objectives



- **E2E span**:
  - *Message exchange protection*: (expected/actual) span between the spots of protection/deprotection
  - *Resource access authorization*: (expected/actual) peer entity which is authenticated



- **Keying/authorization control ownership**:
  - *Message exchange protection*: (designated/actual) authority exercising control over keys and their bindings to entities
  - *Resource access authorization*: (designated/actual) authority exercising control over authorization rules

Industrial Automation Expectations On Security

- Ability to deal with:
  - Industrial automation use cases, e.g. ‘device replacement without engineering’
  - Physical world impacts, esp. security co-existence with safety
  - Double perspective of a single component - physical entity and computing entity
  - Embedded and constrained components (IO means, memory, computing power…)
  - Unattended operations
  - Undisturbed operations, e.g. bumpless key updates
  - Autonomy of production cells (with external cell control)
  - Deterministic cyclic communications
  - …

➢ These expectations show: there are fundamental differences between *IA and IT*

➔ ***Assume IA and IT security to be unequal***

Next Steps During Plenary Session

1. First shortlist topic: NETCONF security deep-dive
2. Review again proposed approach and proposed topics

Abbreviations (1)

APDU	Application Protocol Data Unit
ASN	Abstract Syntax Notation
Authn	Authentication
Authz	Authorization
BRSKI	Bootstrapping Remote Security Key Infrastructure
CA	Certification Authority
CBOR	Constrained Binary Object Representation
CMS	Cryptographic Message Syntax (ASN.1)
CORE	Constrained RESTful Environments
COSE	CBOR Object Signing and Encryption
CRUD	Create, Read, Update, Delete
CUC	Centralized User Configuration
DAC	Discretionary Access Control
DHCP	Dynamic Host Configuration Protocol
DIY	Do It Yourself
DNS	Domain Name Service
DNSSEC	DNS SECurity
E2E	End-to-End
EE	End Entity
HW	HardWare

IA	Industrial Automation
ID	Identifier
IDevID	Initial Device IDentifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IO	Input Output
IP	Internet Protocol IPsec IP security
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
LDevID	Locally significant Device IDentifier
LwM2M	Lightweight M2M
M2M	Machine-to-Machine
MAC	Media Access Control (networking) or Message Authentication Code (security)
MACsec	MAC security
MIB	Management Information Base
MQTT	Message Queuing Telemetry Transport
NETCONF	NETwork CONFiguration

Abbreviations (2)

OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization
OEM	Original Equipment Manufacturer
OPC	Open Platform Communications
OSCORE	Object Security for CORE
OT	Operational Technology
PHY	PHYsical
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
RADIUS	Remote Authentication Dial In User Service
REST	REpresentational State Transfer
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
SSH	Secure SHell
SW	SoftWare
T2T	Thing-to-Thing
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
UA	Unified Architecture
UDP	User Datagram Protocol
URL	Uniform Resource Locator
URN	Uniform Resource Name
URI	Uniform Resource Identifier
XML	eXtensible Markup Language
YANG	Yet Another Next Generation

Glossary (1)

Access control (RFC 4949): Protection of system resources against unauthorized access

Access control matrix (NIST CRSC): A table in which each row represents a subject, each column represents an object, and each entry is the set of access rights for that subject to that object

Authorization (RFC 4949): An approval that is granted to a system entity to access a system resource

Certificate (RFC 4949): A document that attests to the truth of something or the ownership of something

Certification authority (RFC 5280): A system entity that generates public-key certificates

Credential (IEEE 802.1AR): Information that an entity (a person or device) possesses that allow it to make a verifiable claim of identity, i.e., to be authenticated

(Data) confidentiality (RFC 4949): The property that data is not disclosed to system entities unless they have been authorized to know the data

(Data) integrity (RFC 4949): The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Discretionary access control (RFC 4949): A means of restricting access to objects based on the identity of subjects and/or groups to which they belong

End entity (RFC 5280): A user of public key certificates and/or end user system that is the subject of a certificate

Integrity (RFC 8446): Data sent over the channel after establishment cannot be modified by attackers without detection

Glossary (2)

Key (RFC 4949): An input parameter used to vary a transformation function performed by a cryptographic algorithm

Non-repudiation (**service**, RFC 4949): A security service that provide protection against false denial of involvement in an association

(Peer) entity authentication (RFC 4949): The process of verifying a claim that a system entity or system resource has a certain attribute value. An authentication process consists of two basic steps:

> Identification step: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem.
>
> Verification step: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed.

Private key (RFC 4949): The secret component of a pair of cryptographic keys used for asymmetric cryptography

Public key (RFC 4949): The publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography

Public-key certificate (RFC 4949): A digital certificate that binds a system entity's identifier to a public key value

Replay (**attack**, RFC 4949): An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it, possibly as part of a masquerade attack

Trust anchor (RFC 5280): A CA certificate that serves as a trust anchor for the certification path validation

Voucher (inspired by RFC 8366): An artifact to securely assign a (network) device to an owner and to securely convey local trust anchors

References, Chronologically Ordered (1)

SIEMENS
Ingenuity for life

1. IETF RFC 2246: The Transport Layer Security (TLS) Protocol Version 1.0, 1999
2. IETF RFC 2459: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 1999
3. Stajano, F.; Anderson, R: The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, 1999
4. IETF RFC 2828: Internet Security Glossary, 2000
5. IETF RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2002
6. IETF RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 2003
7. IEEE 802.1AE-2006: IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security, 2006
8. IETF RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1, 2006
9. IETF RFC 4949: Internet Security Glossary, Version 2, 2007
10. IETF RFC 5116: An Interface and Algorithms for Authenticated Encryption, 2008
11. IETF RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2, 2008
12. IETF RFC 5216: The EAP-TLS Authentication Protocol, 2008
13. IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008
14. IEEE 802.1AR-2009: IEEE Standard for Local and Metropolitan Area Networks–Secure Device Identity, 2009

References, Chronologically Ordered (2)

15. IEEE 802.1X-2010: IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control, 2010
16. IETF RFC 6125: Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS), 2011
17. Seaman, M.: MACsec hops, Revision 2.0, 2013
18. IETF RFC 7525: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), 2015
19. NIST SP 800-63: Digital Identity Guidelines, 2017
20. IEEE 802.1AE-2018: IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security – Revision D 1.3, 2018
21. IEEE 802.1AR-2018: IEEE Standard for Local and Metropolitan Area Networks–Secure Device Identity, 2018
22. IETF RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3, 2018
23. IEC/IEEE 60802: Use Cases, Version 1.3, 2018
24. IETF RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges, 2019
25. IEC/IEEE 60802: Time-Sensitive Networking Profile for Industrial Automation, Draft 1.2, 2020

Authors

SIEMENS
Ingenuity for life

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

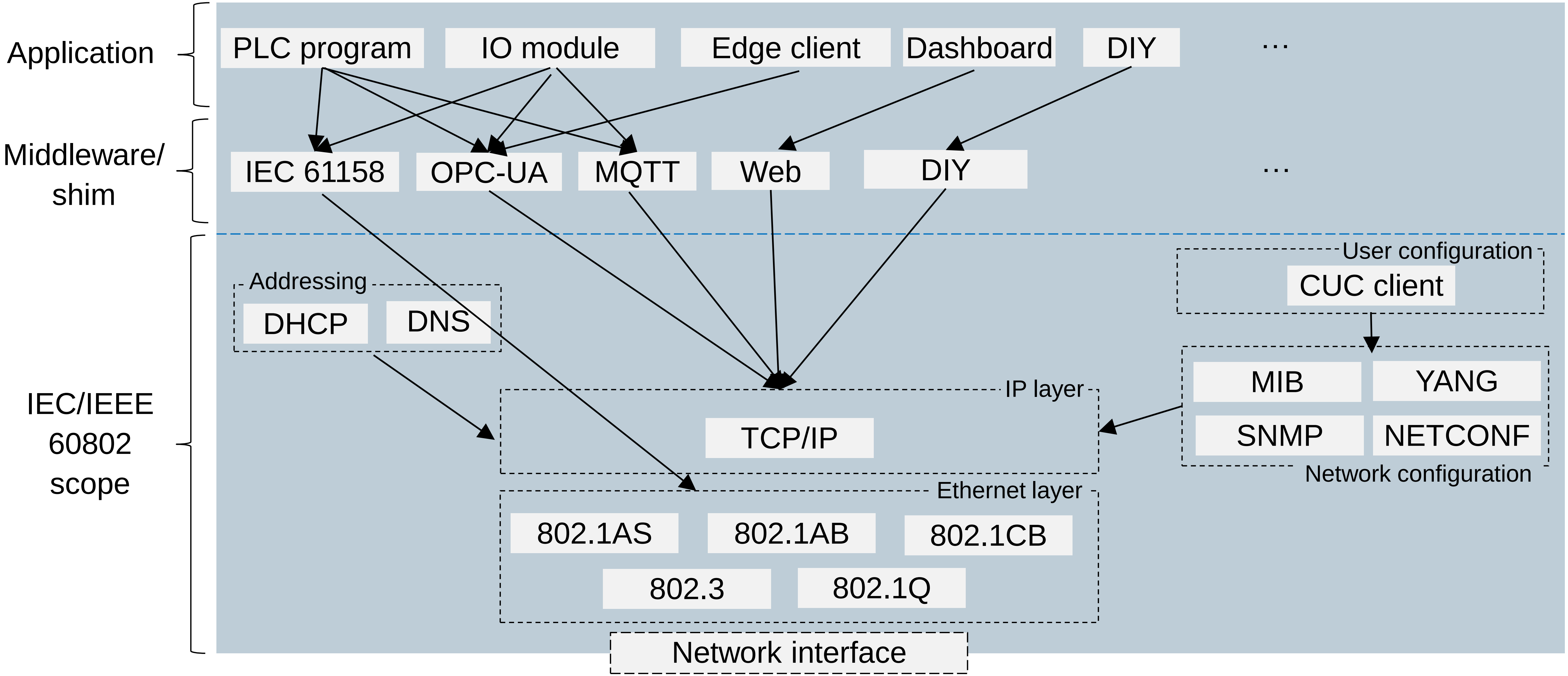
Lars Lindemann, Siemens AG, DI FA CTR ICO ARC,
lars.Lindemann@siemens.com

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

Thomas Pössler, Siemens AG, RC-AT DI FA DH-GRAZ SAS,
thomas.poessler@siemens.com

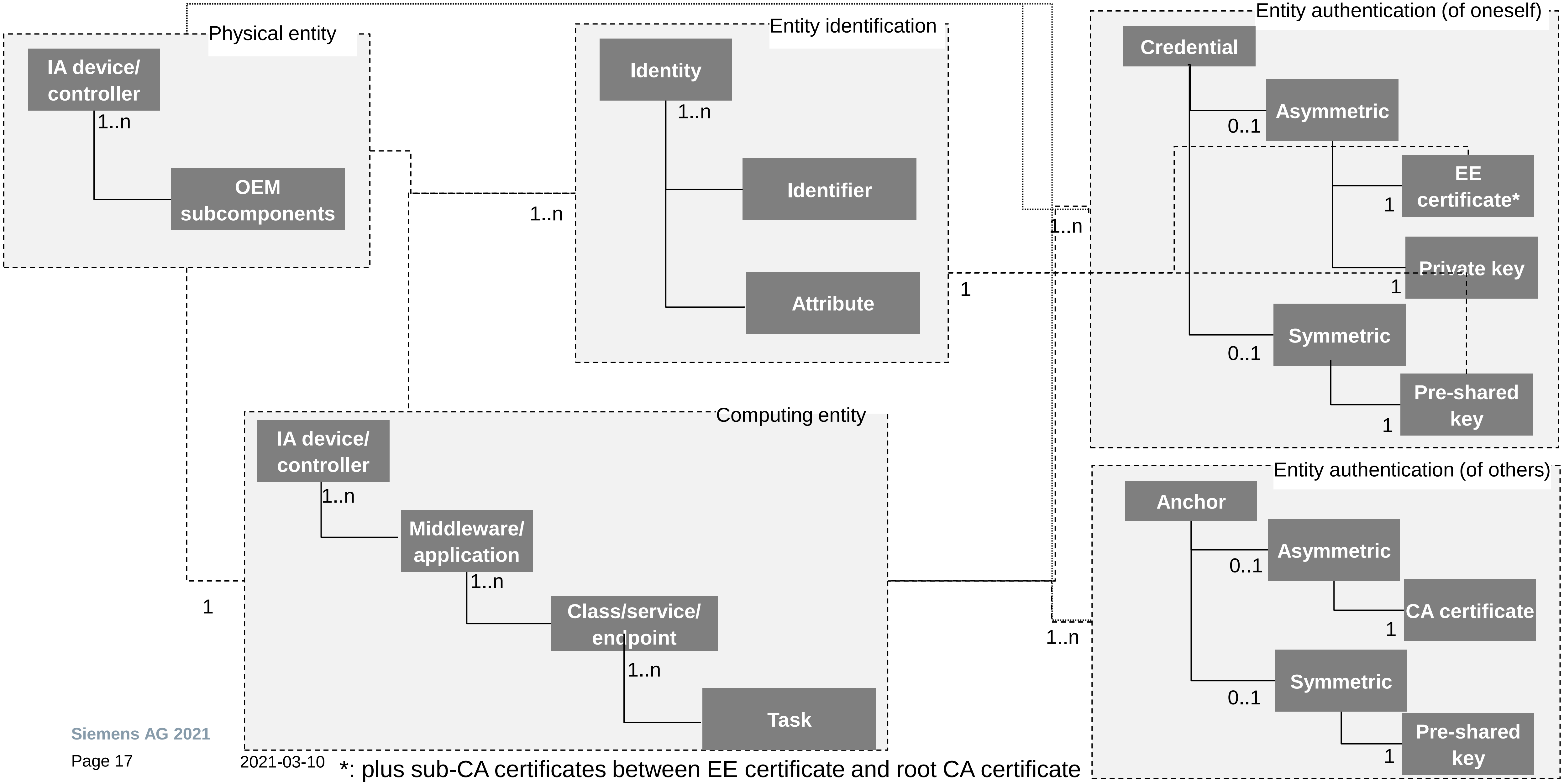
Günter Steindl, Siemens AG, DI FA TI ART EA,
guenter.steindl@siemens.com

Illustrating IA Devices/Controllers



Modelling IA Devices/Controllers

SIEMENS



*: plus sub-CA certificates between EE certificate and root CA certificate