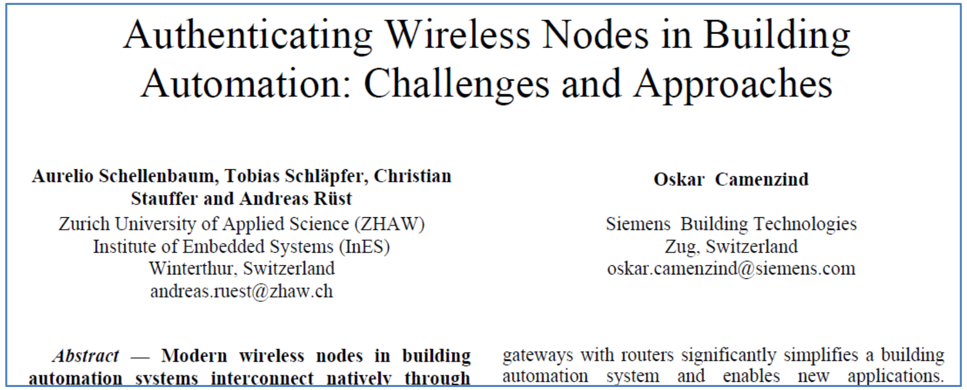
Authenticating Wireless Nodes in Building Automation: Challenges and Approaches

Funded by Innosuisse - Swiss Innovation Agency under project number 19328.1 PFES-ES

Prof. Andreas Rüst
Zurich University of Applied Sciences – Institute of Embedded Systems
Winterthur, Switzerland
andreas.ruest@zhaw.ch

https://doi.org/10.21256/zhaw-2750



Authenticating Wireless Nodes in Building Automation: Challenges and Approaches

Aurelio Schellenbaum, Tobias Schläpfer, Christian Stauffer and Andreas Rüst
Zurich University of Applied Science (ZHAW)
Institute of Embedded Systems (InES)
Winterthur, Switzerland
andreas.ruest@zhaw.ch

Oskar Camenzind
Siemens Building Technologies
Zug, Switzerland
oskar.camenzind@siemens.com

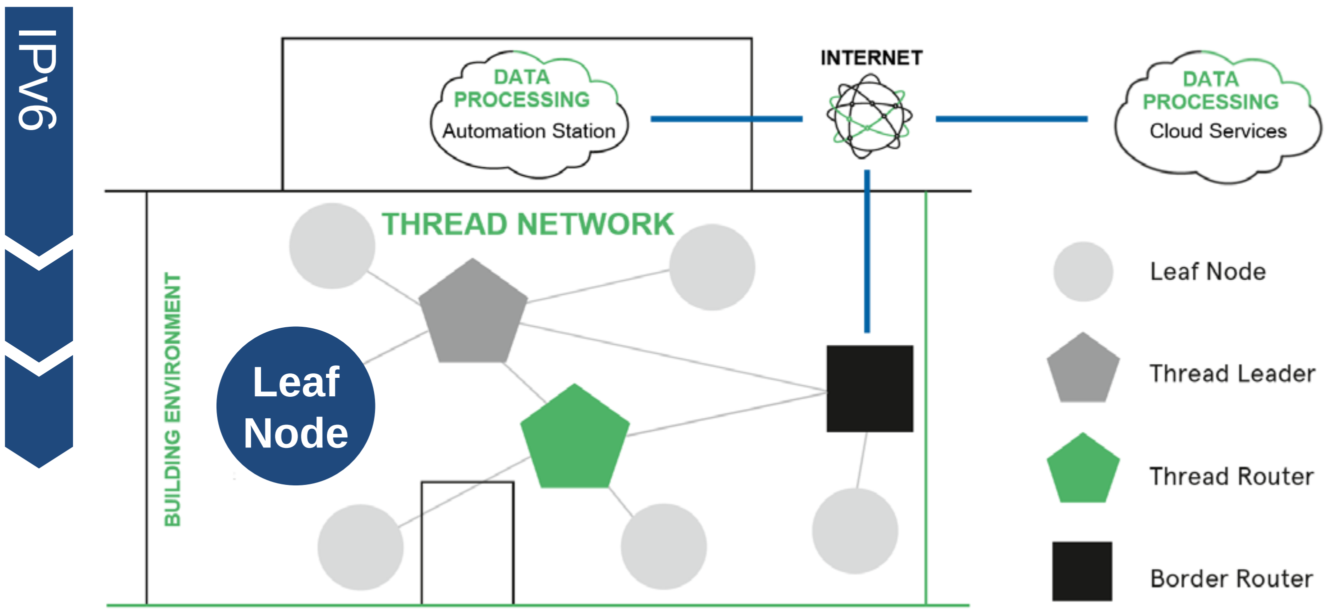
***Abstract* — Modern wireless nodes in building automation systems interconnect natively through**

gateways with routers significantly simplifies a building automation system and enables new applications.

Building Automation System

- **Extending IPv6 down to the field level**
  - Sensor networks coalesce with existing IT networks
  - Authentication requires simple but secure provisioning

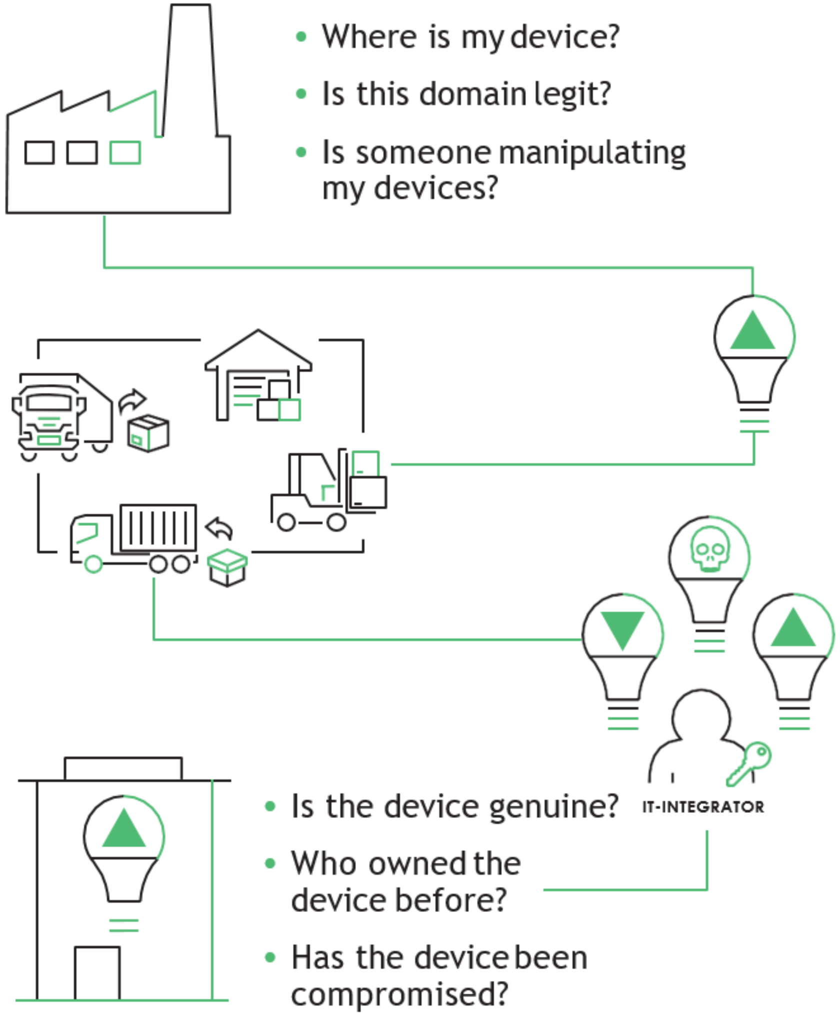
→ **Autonomic Secure Bootstrapping**



KNX	BACnet	zigbee → dotdot	others
CoAPs			
DTLS		DHCPv6	MLE
UDP			
IPv6 & routing protocols			
6LoWPAN			
IEEE 802.15.4 MAC			
IEEE 802.15.4 PHY 2.4 GHz			

Establishing Trust: From Supply Chain to System Integration

- **Goal of manufacturer**
  - Ship a single device type, with a uniform firmware load directly to all customers
- **Device travels through long supply chain**
  - Exposed to potential manipulations
  - E.g. unauthorized replication, compromised firmware updates and deceiving reuse of device identities
- **Enrolling installed device into specific IT-environment**
  - Manually by IT-integrator
  - Does he trust the device?
  - Trustworthy previous owners?

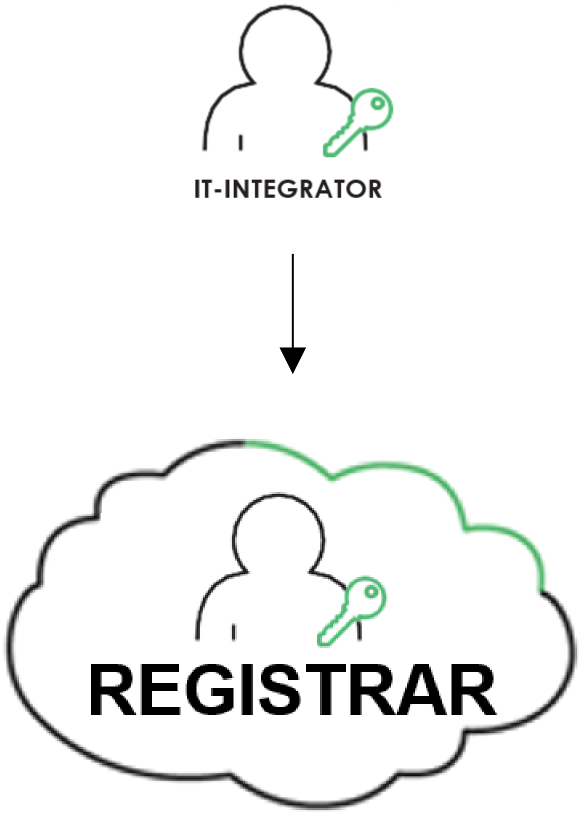


- Where is my device?
- Is this domain legit?
- Is someone manipulating my devices?
IT-INTEGRATOR
- Is the device genuine?
- Who owned the device before?
- Has the device been compromised?

Autonomic Secure Bootstrapping

The role of the Registrar

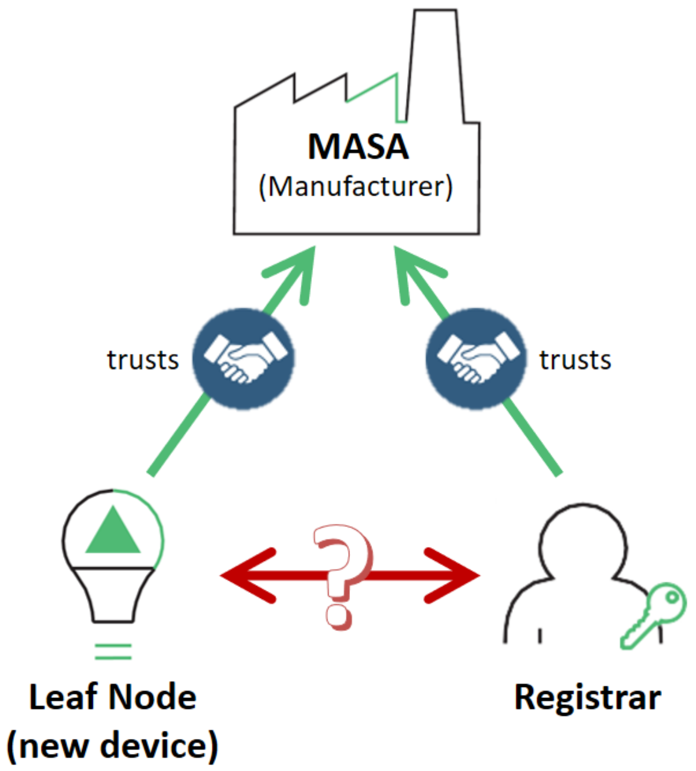
- Growing number of nodes in building automation
  - Need to automate enrollment process
  - Replace IT-Integrator (person) with fully automated service entity
- Registrar represents the individual domain of a building
  - Acts as registration authority
  - Takes decision whether a Leaf Node is allowed to join the domain



→ Makes fully automated enrollment possible

Initial Trust Relationships

Manufacturer Authorized Signing Authority (MASA)



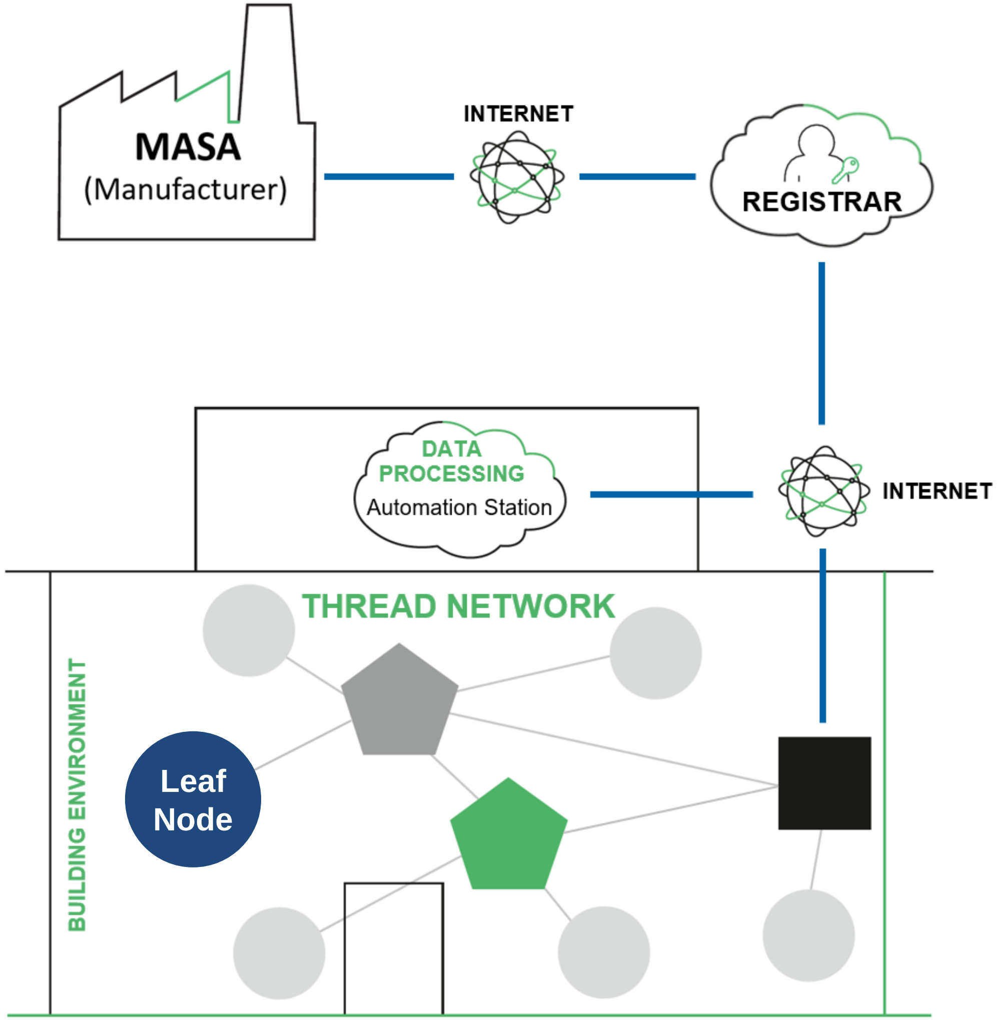
Both, Leaf node and Registrar trust in MASA
But there is no trust between them

- **Trust of Leaf Node in MASA**
  - Imprinted during manufacturing process

IDevID – Initial Device Identifier	
Manufacturer Device Certificate with individual device serial number	**X.509 public-key certificate signed by manufacturer. Certifies Identity of Leaf Node.**
Manufacturer CA's public-key certificate Identifies manufacturer CA as root of trust	**X.509 public-key certificate chain. Self-signed by manufacturer. Cannot be changed.**

- **Trust of Registrar in MASA**
  - Many options, e.g. manual configuration by IT-Admin

Autonomic Secure Bootstrapping



Autonomic Secure Bootstrapping

Fully automated enrollment of Leaf Node

1. Establishing mutual trust between Leaf Node and Registrar	Anima BRSKI
2. Enrollment over secure transport	EST-coaps
3. Operational network enrollment	

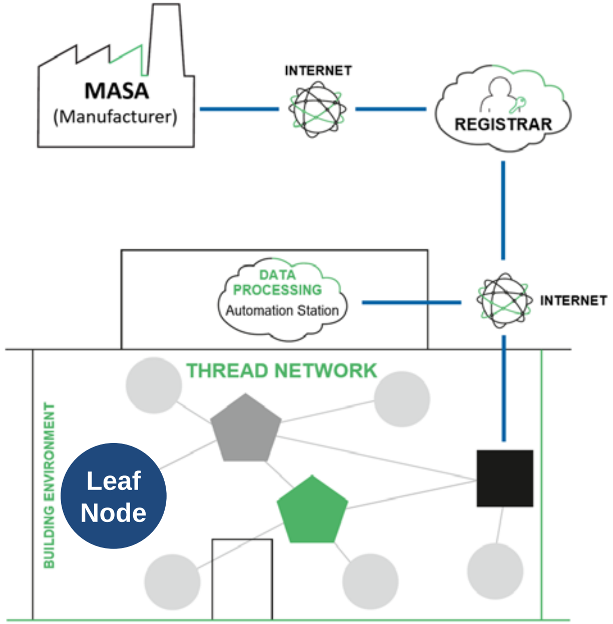
Fairhair Alliance

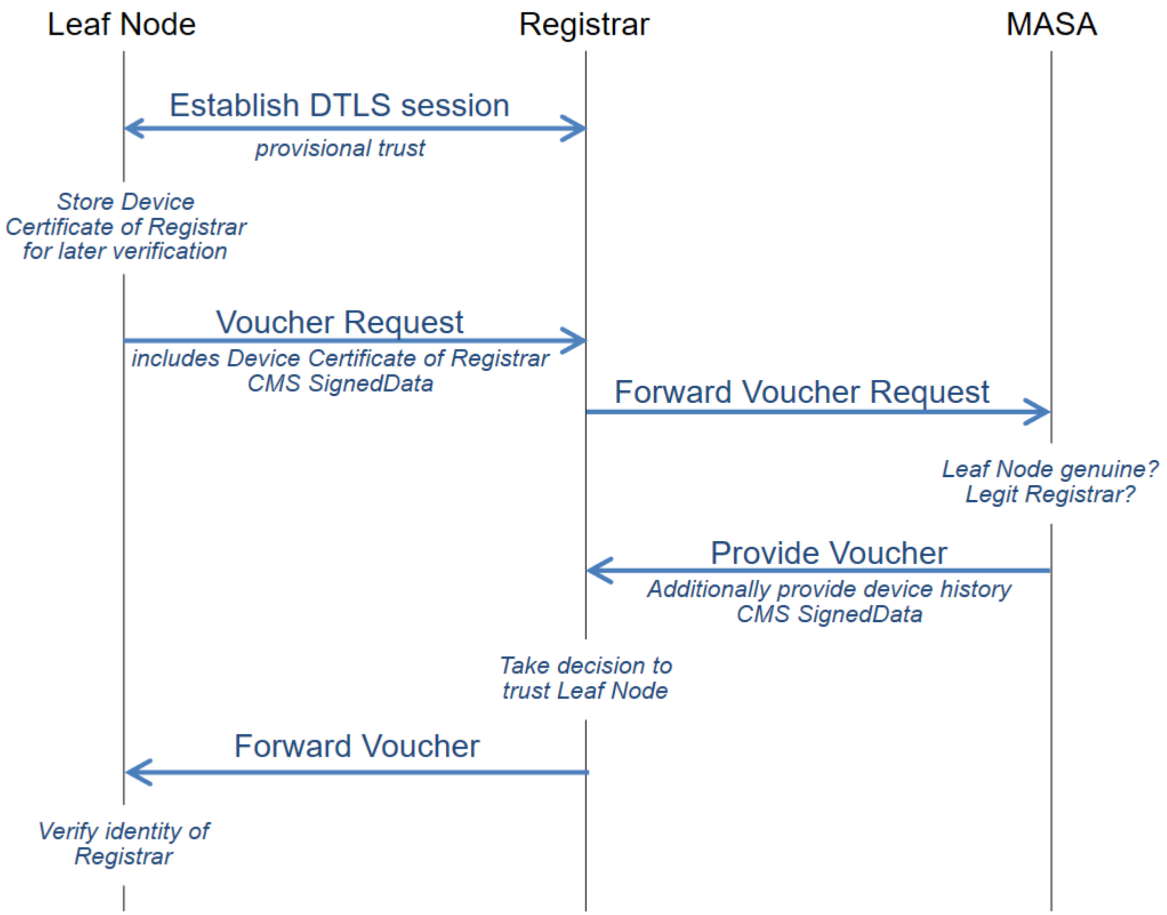
Establishing Mutual Trust between Leaf Node and Registrar (A)

- **MASA introduces Leaf Node and Registrar to each other**

Voucher based system using

X.509 Certificates + Digital Signatures




Leaf Node | Registrar | MASA

Establish DTLS session
provisional trust

Store Device Certificate of Registrar for later verification

Voucher Request
includes Device Certificate of Registrar CMS SignedData

Forward Voucher Request

Leaf Node genuine? Legit Registrar?

Provide Voucher
Additionally provide device history CMS SignedData

Take decision to trust Leaf Node

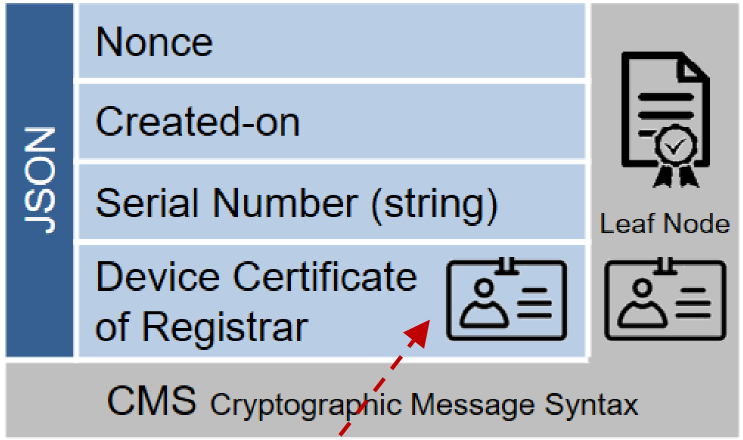
Forward Voucher

Verify identity of Registrar

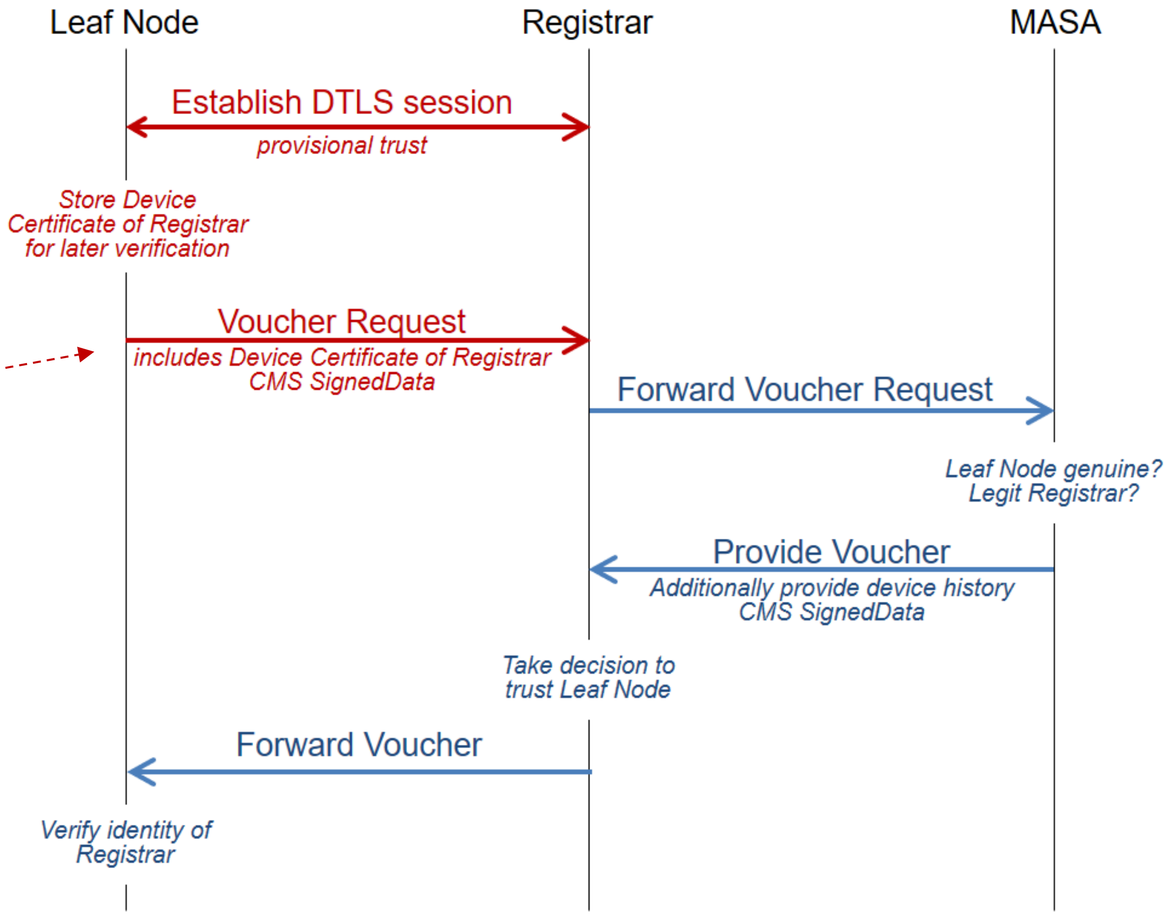
Establishing Mutual Trust between Leaf Node and Registrar (B)

■ Leaf Node issues Voucher Request

Through DTLS session with provisional trust

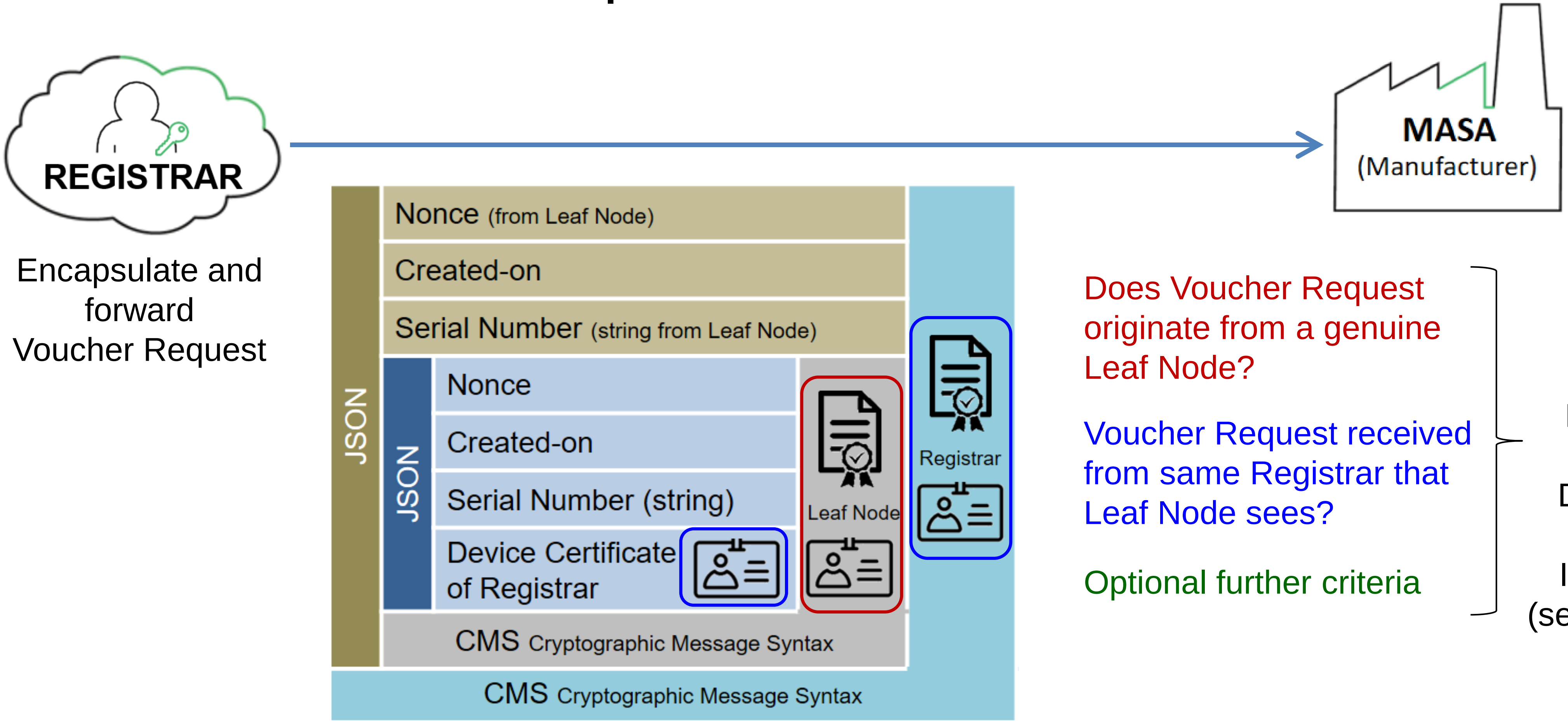

JSON
Nonce
Created-on
Serial Number (string)
Device Certificate of Registrar
Leaf Node
CMS Cryptographic Message Syntax

As presented by Registrar during DTLS handshake


Leaf Node
Registrar
MASA
Establish DTLS session
provisional trust
Store Device Certificate of Registrar for later verification
Voucher Request
includes Device Certificate of Registrar
CMS SignedData
Forward Voucher Request
Leaf Node genuine?
Legit Registrar?
Provide Voucher
Additionally provide device history
CMS SignedData
Take decision to trust Leaf Node
Forward Voucher
Verify identity of Registrar

Establishing Mutual Trust between Leaf Node and Registrar (C)

- **MASA verifies Voucher Request**


REGISTRAR
MASA
(Manufacturer)
JSON
Nonce (from Leaf Node)
Created-on
Serial Number (string from Leaf Node)
JSON
Nonce
Created-on
Serial Number (string)
Device Certificate of Registrar
Leaf Node
Registrar
CMS Cryptographic Message Syntax
CMS Cryptographic Message Syntax

Encapsulate and forward Voucher Request

Does Voucher Request originate from a genuine Leaf Node?

Voucher Request received from same Registrar that Leaf Node sees?

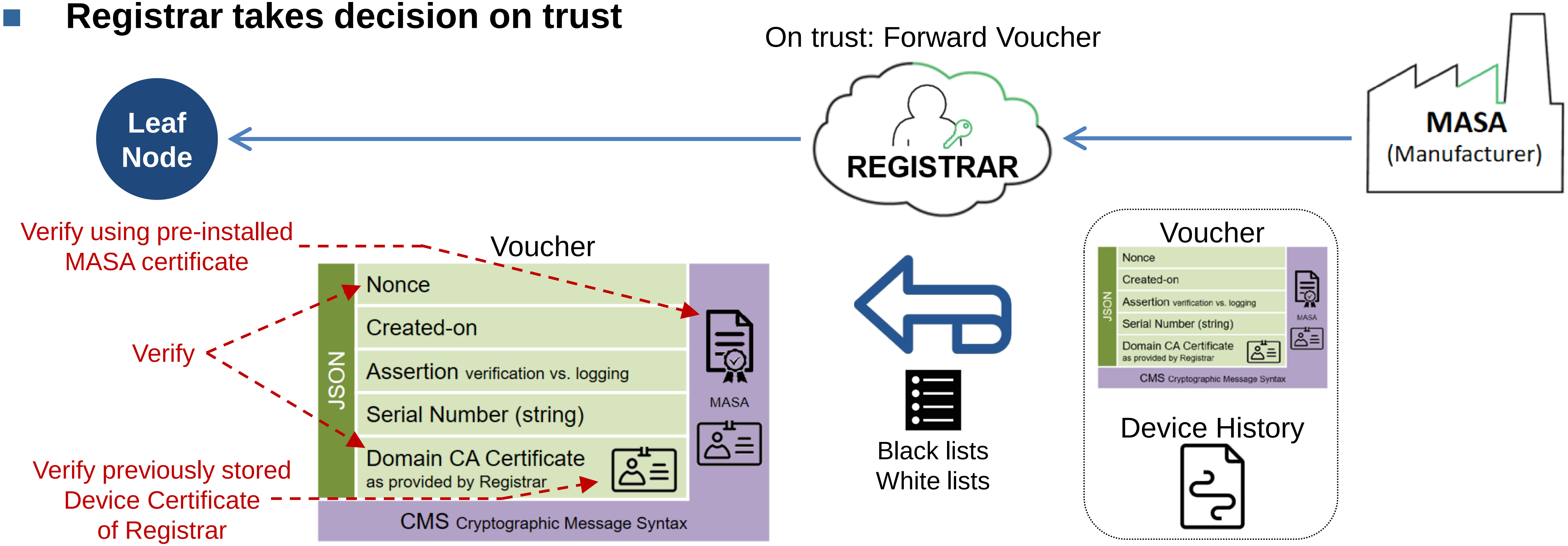
Optional further criteria

Log Registrar as owner in Device History

Issue Voucher (send to Registrar)

Establishing Mutual Trust between Leaf Node and Registrar (D)

- **Registrar takes decision on trust**

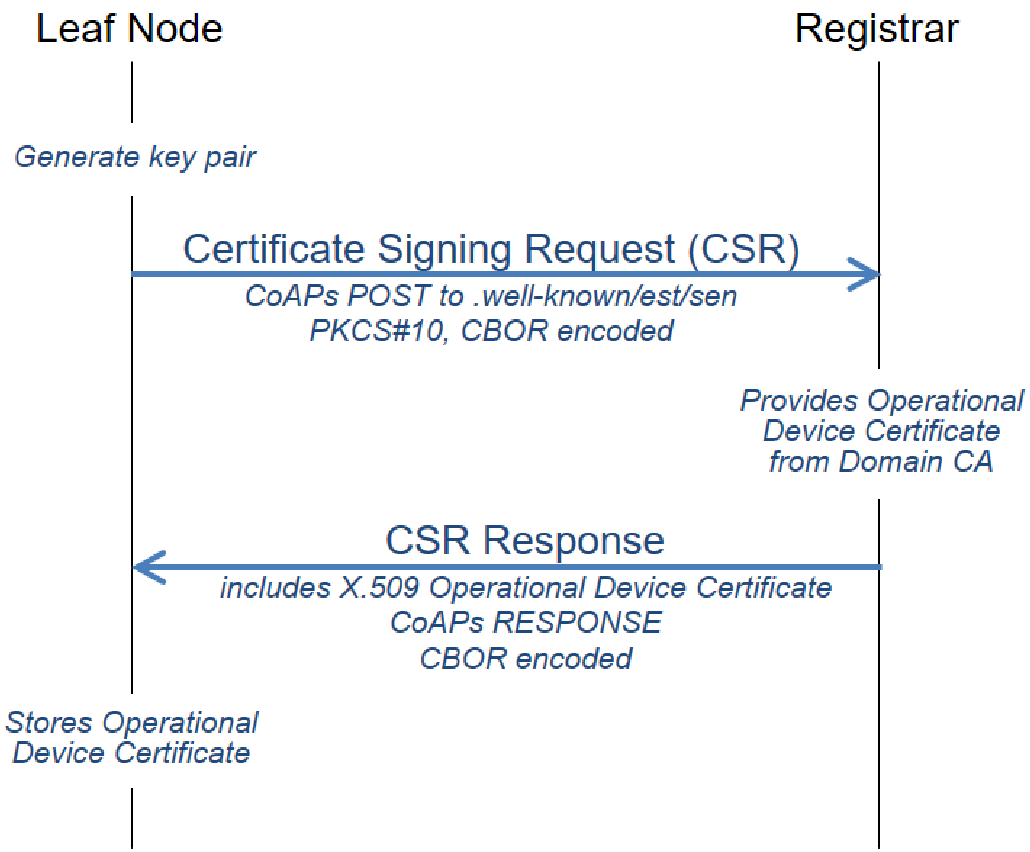

On trust: Forward Voucher
Leaf Node
REGISTRAR
MASA
(Manufacturer)
Verify using pre-installed MASA certificate
Verify
Verify previously stored Device Certificate of Registrar
Voucher
JSON
Nonce
Created-on
Assertion verification vs. logging
Serial Number (string)
Domain CA Certificate as provided by Registrar
MASA
CMS Cryptographic Message Syntax
Black lists
White lists
Voucher
JSON
Nonce
Created-on
Assertion verification vs. logging
Serial Number (string)
Domain CA Certificate as provided by Registrar
MASA
CMS Cryptographic Message Syntax
Device History

→ Leaf Node and Registrar now mutually trust each other

Step 2: Enrollment over Secure Transport (EST-coaps)

- **Provisioning of operational identity**
  - Uses mutual trust: Leaf Node ←→ Registrar
  - Leaf Node
    - Generates new private-public key pair
    - Requests certification of public key
  - Registrar
    - Provides Operational Device Certificate
    - LDevID: Locally significant secure device identifier

→ **Leaf Node holds certified operational identity to authenticate itself in domain.**



Leaf Node

Registrar

Generate key pair

Certificate Signing Request (CSR)

CoAPs POST to .well-known/est/sen
PKCS#10, CBOR encoded

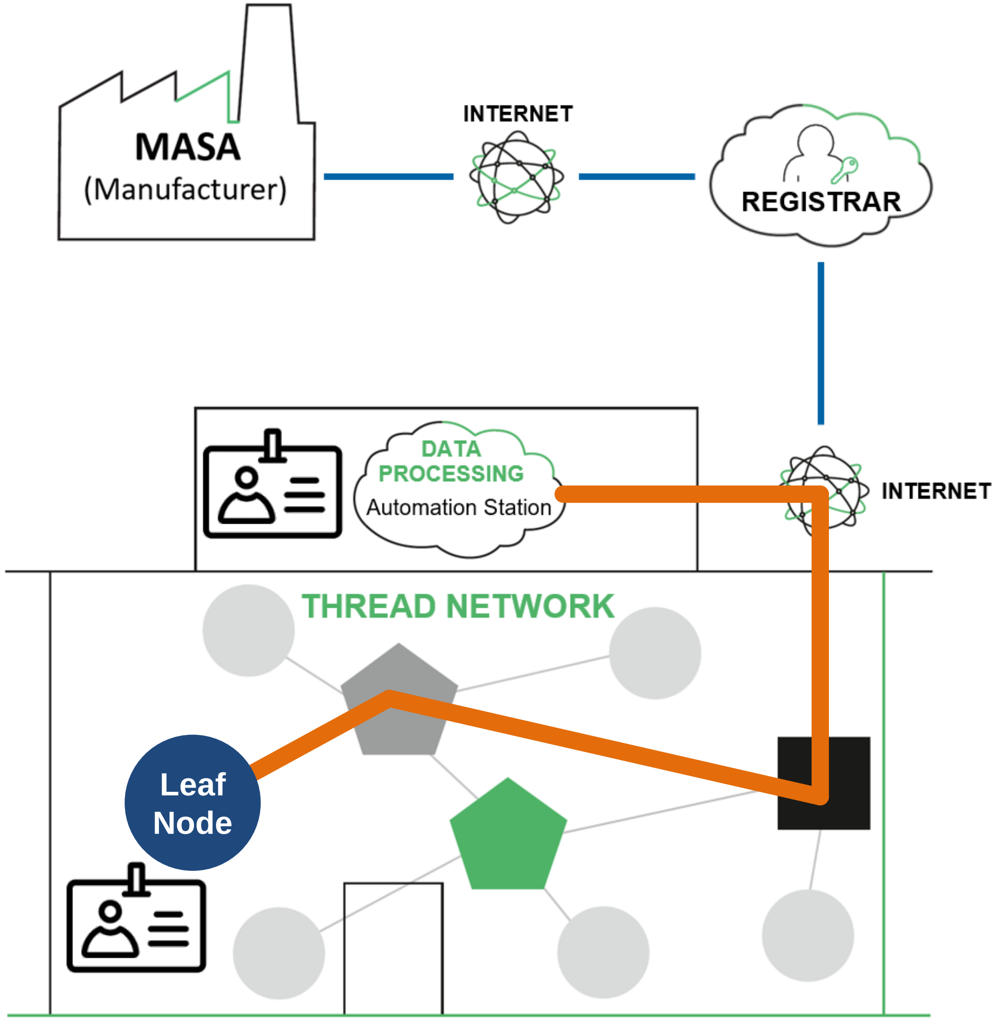
Provides Operational Device Certificate from Domain CA

CSR Response

includes X.509 Operational Device Certificate
CoAPs RESPONSE
CBOR encoded

Stores Operational Device Certificate

Step 3: Operational Network Enrollment



- **Leaf Node authenticates itself in domain**
  - E.g. post data to Automation Station
  - Leaf Node and Automation Station can both verify the identity of each other
  - Authorization based on presented identity
  - End-to-end security → DTLS, CoAPS

Implementation of Leaf Node

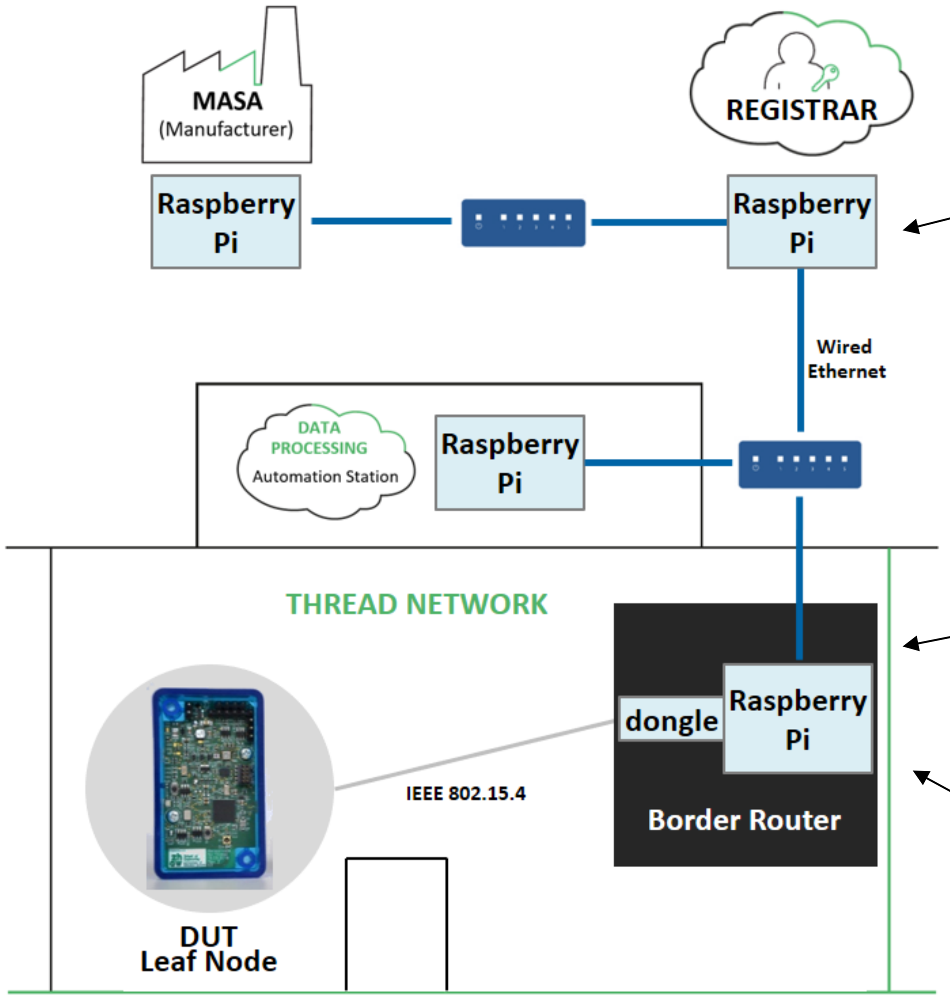
Secure Elements physically isolate secret cryptographic material from application.

However, individual integration effort for each secure element has been high.
→ Need for harmonization

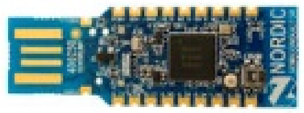
- **Nordic nRF52840 System-on-Chip**
  - 2.4GHz PCB antenna
- **Sensors**
  - InvenSense ICS 41350 microphone
  - Bosch BME680 temperature, humidity, pressure and gas sensor
  - Texas Instruments OPT3001 light sensor
  - STMicroelectronics LSM6DSL accelerometer and gyroscope
- **Secure Elements**
  - Microchip ATECC608A
  - NXP A71CH
  - Infineon Optiga TrustX
  - Trusted Objects TO136

Verification

- **Test Set-up**



CoAP framework

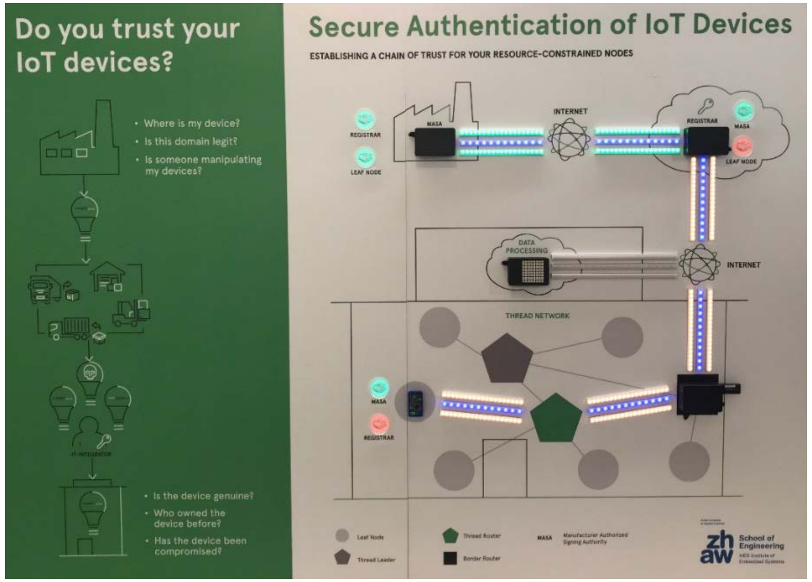


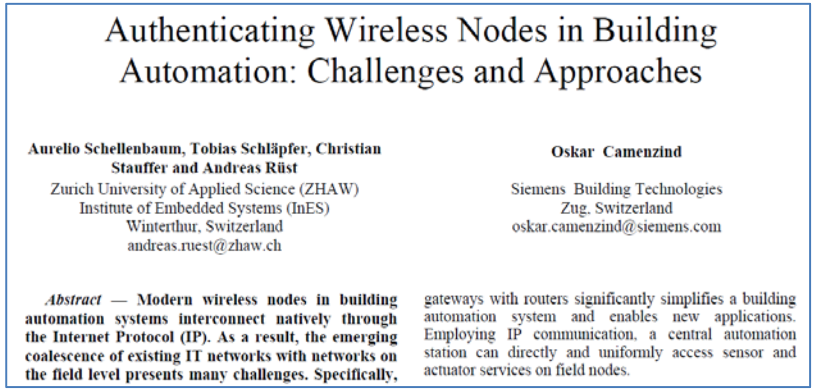
nRF5280 dongle
Runs OpenThread in Network Coprocessor Mode

OpenThread Border Router Software

Conclusions

- **Autonomic Secure Bootstrapping**
  - Fully automated enrollment process for IoT devices
  - Provisions operational identity (LDevID)
  - Starting from Initial Device Identifier (IDevID) imprinted by manufacturer
  - Based on public-key cryptography
  - Fairhair Alliance / IETF Anima
- **Fully functional implementation**
  - Cryptographic operations possible in software as well as in secure elements of four different vendors
  - Secure elements show need for harmonization
- **Read the details https://doi.org/10.21256/zhaw-2750**


Do you trust your IoT devices?
• Where is my device?
• Is this domain legit?
• Is someone manipulating my devices?
IT-INTEGRATOR
• Is the device genuine?
• Who owned the device before?
• Has the device been compromised?
Secure Authentication of IoT Devices
ESTABLISHING A CHAIN OF TRUST FOR YOUR RESOURCE-CONSTRAINED NODES
REGISTRAR
LEAF NODE
MASA
INTERNET
REGISTRAR
MASA
LEAF NODE
DATA PROCESSING
INTERNET
THREAD NETWORK
MASA
REGISTRAR
Leaf Node
Thread Leader
Thread Router
Border Router
MASA Manufacturer Authorized Signing Authority
zh aw School of Engineering
InES Institute of Embedded Systems



Authenticating Wireless Nodes in Building Automation: Challenges and Approaches

Aurelio Schellenbaum, Tobias Schläpfer, Christian Stauffer and Andreas Rüst
Zurich University of Applied Science (ZHAW)
Institute of Embedded Systems (InES)
Winterthur, Switzerland
andreas.ruest@zhaw.ch

Oskar Camenzind
Siemens Building Technologies
Zug, Switzerland
oskar.camenzind@siemens.com

***Abstract* — Modern wireless nodes in building automation systems interconnect natively through the Internet Protocol (IP). As a result, the emerging coalescence of existing IT networks with networks on the field level presents many challenges. Specifically,**

gateways with routers significantly simplifies a building automation system and enables new applications. Employing IP communication, a central automation station can directly and uniformly access sensor and actuator services on field nodes.