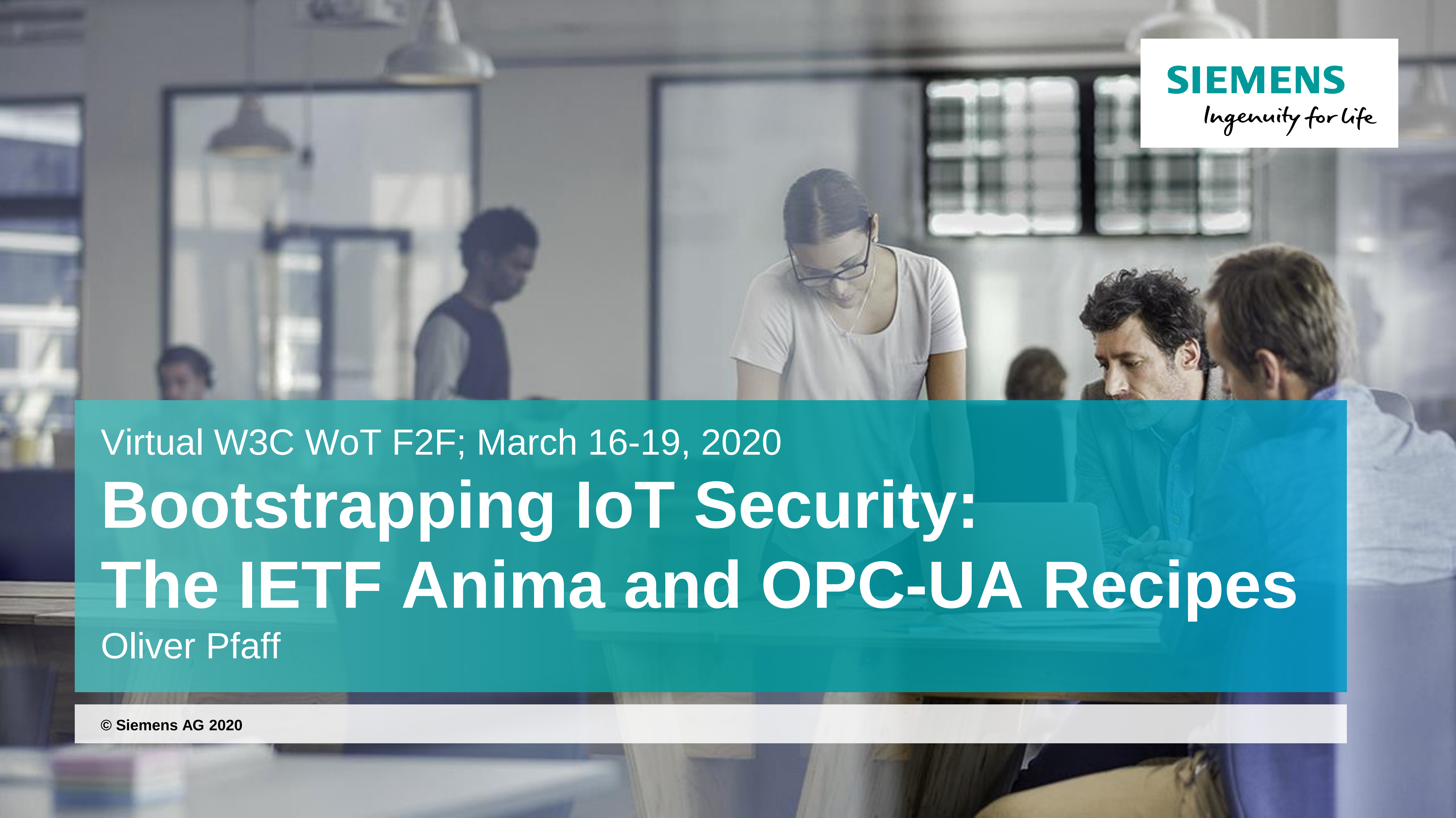


SIEMENS
Ingenuity for life

Virtual W3C WoT F2F; March 16-19, 2020

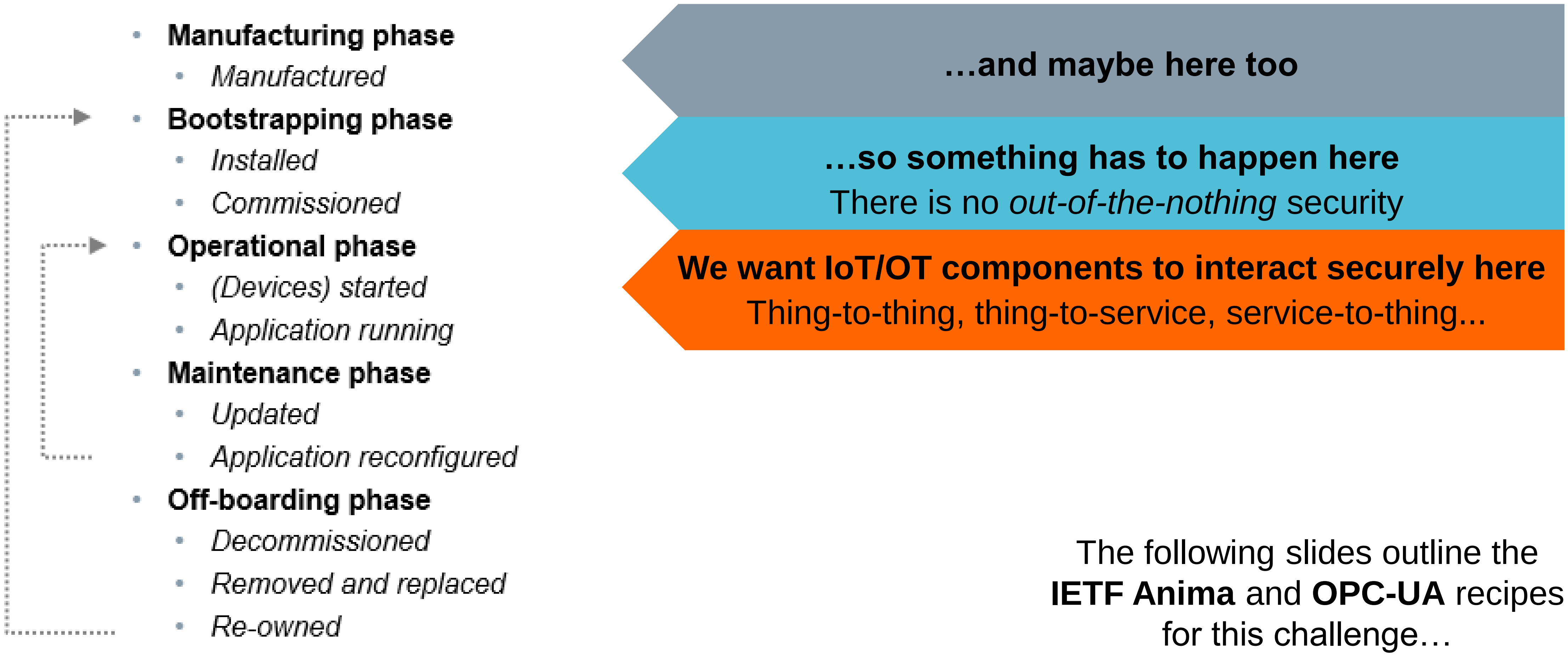
# Bootstrapping IoT Security: The IETF Anima and OPC-UA Recipes

Oliver Pfaff

# *The Challenge*: Prepare for Security

SIEMENS
Ingenuity for life

- Lifecycle of IoT/OT components - independent from their specification camp:



- **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*

**…and maybe here too**

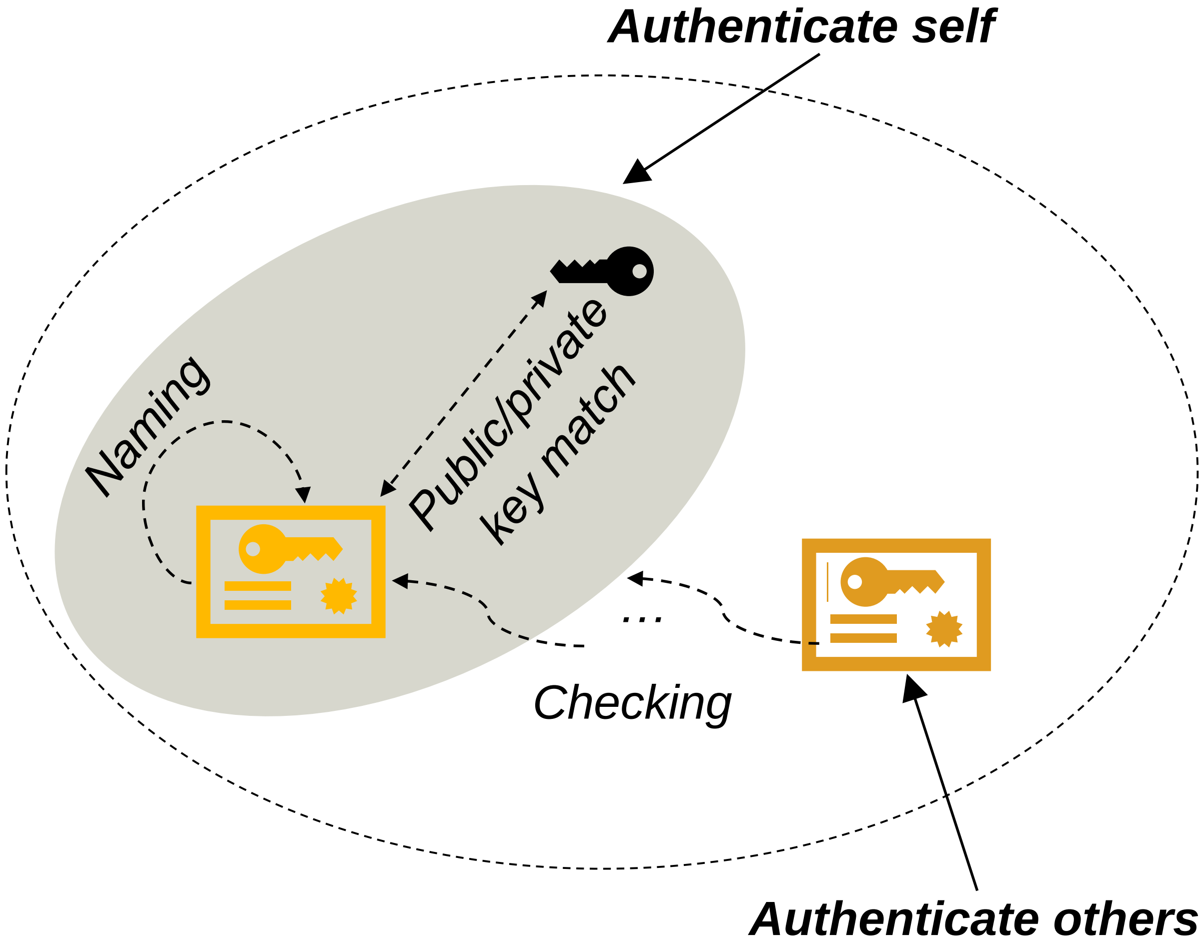
**…so something has to happen here**
There is no *out-of-the-nothing* security

**We want IoT/OT components to interact securely here**
Thing-to-thing, thing-to-service, service-to-thing...

The following slides outline the **IETF Anima** and **OPC-UA** recipes for this challenge…

# *Some Cryptonite*: LDevID/IDevID Credentials

SIEMENS
Ingenuity for life



LDevIDs/IDevIDs are **triplets** consisting of (see [1], [2]):

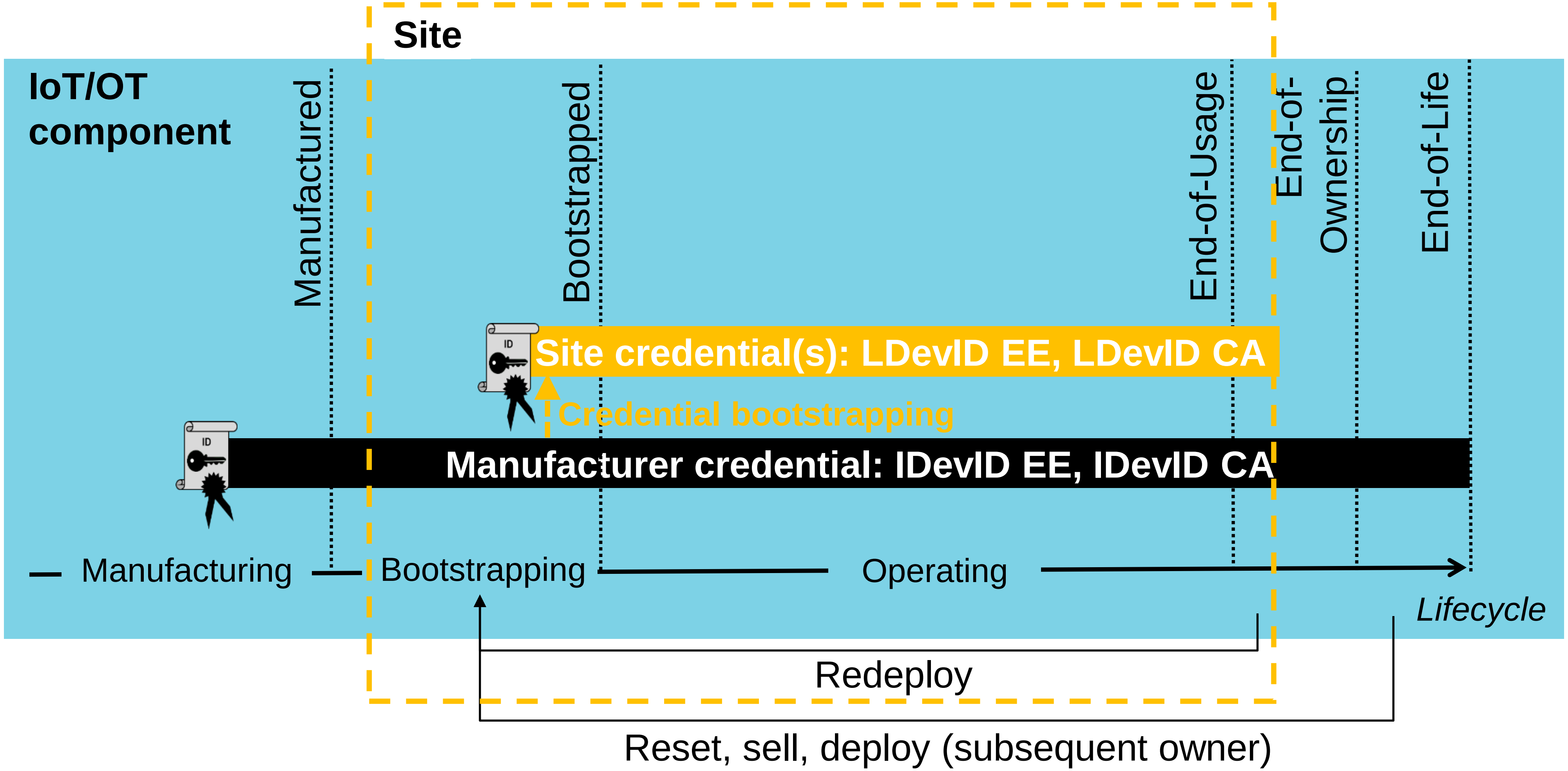
1. Private key
2. X.509 EE certificate containing a public key that matches this private key plus IoT/OT component naming information (as well as intermediate X.509 CA certificates)
3. X.509 root CA certificate

There is **no one-fits-all**: such triplets appear multiply in one IoT/OT component that uses multiple stacks:

- LDevIDs* for OPC-UA/Web/802.1 etc. security
- IDevID(s)

*: The term 'LDevID' belongs to the IEEE namespace as well as 'IDevID'. OPC-UA and Web (server) security conceptually rely on LDevIDs - without using this term

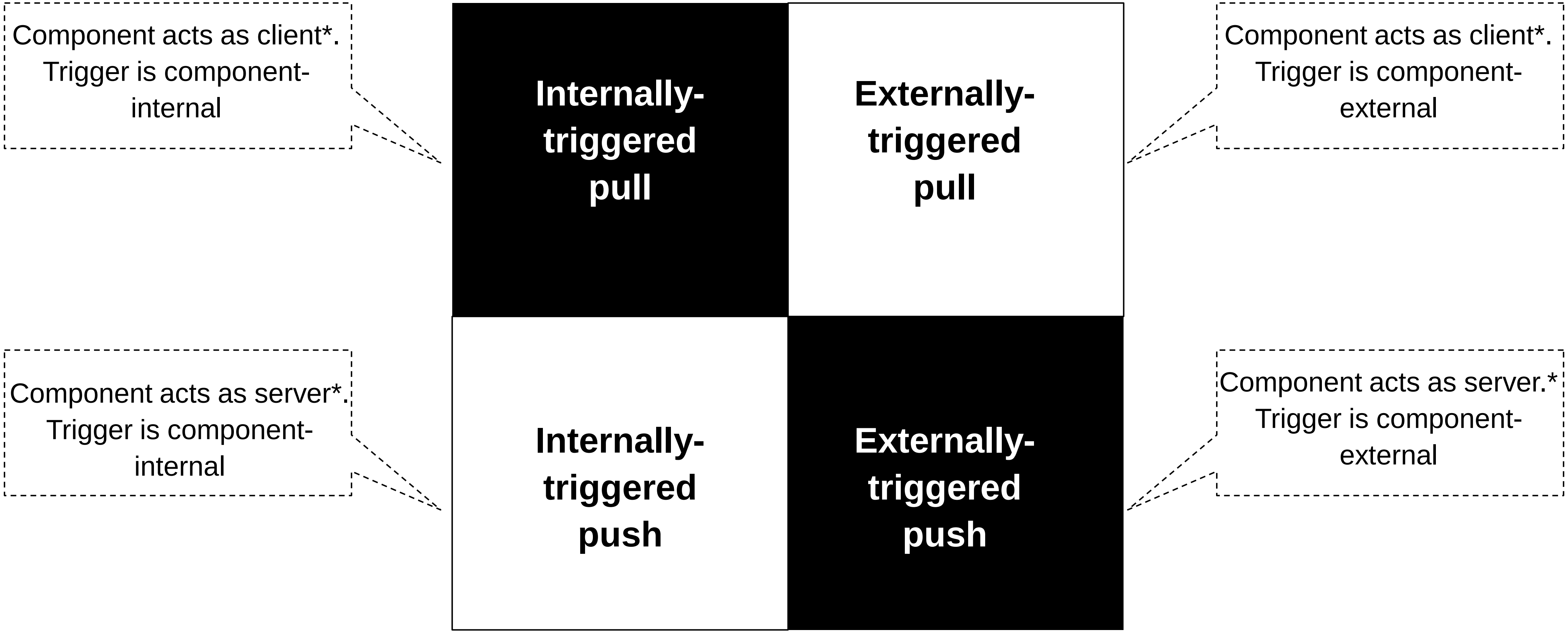
# What Does Happen Inside IoT/OT Components?



**A: acquire LDevIDs by means of credential bootstrapping from IDevIDs**

IETF Anima

# Which Patterns Are Covered?



Component acts as client*. Trigger is component-internal

Component acts as client*. Trigger is component-external

Component acts as server*. Trigger is component-internal

Component acts as server.* Trigger is component-external

| | |
|---|---|
| **Internally-triggered pull** | **Externally-triggered pull** |
| **Internally-triggered push** | **Externally-triggered push** |

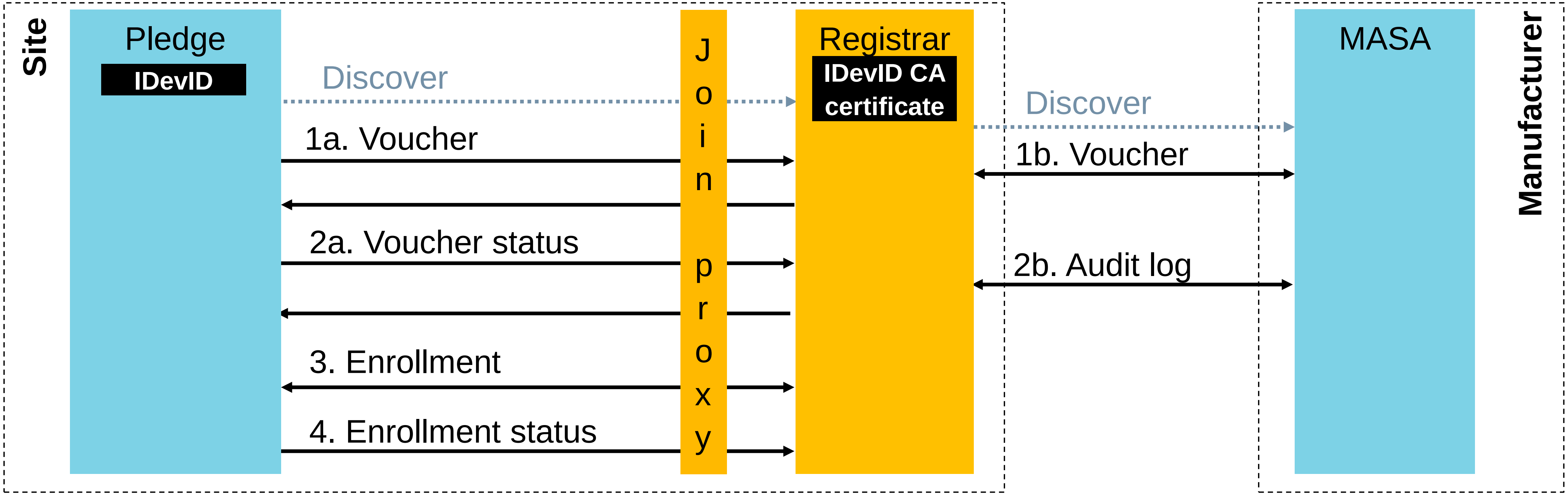
*: towards security infrastructure components (services, tools)

**A: as of now, ‘only’ internally triggered pull**

## IETF Anima

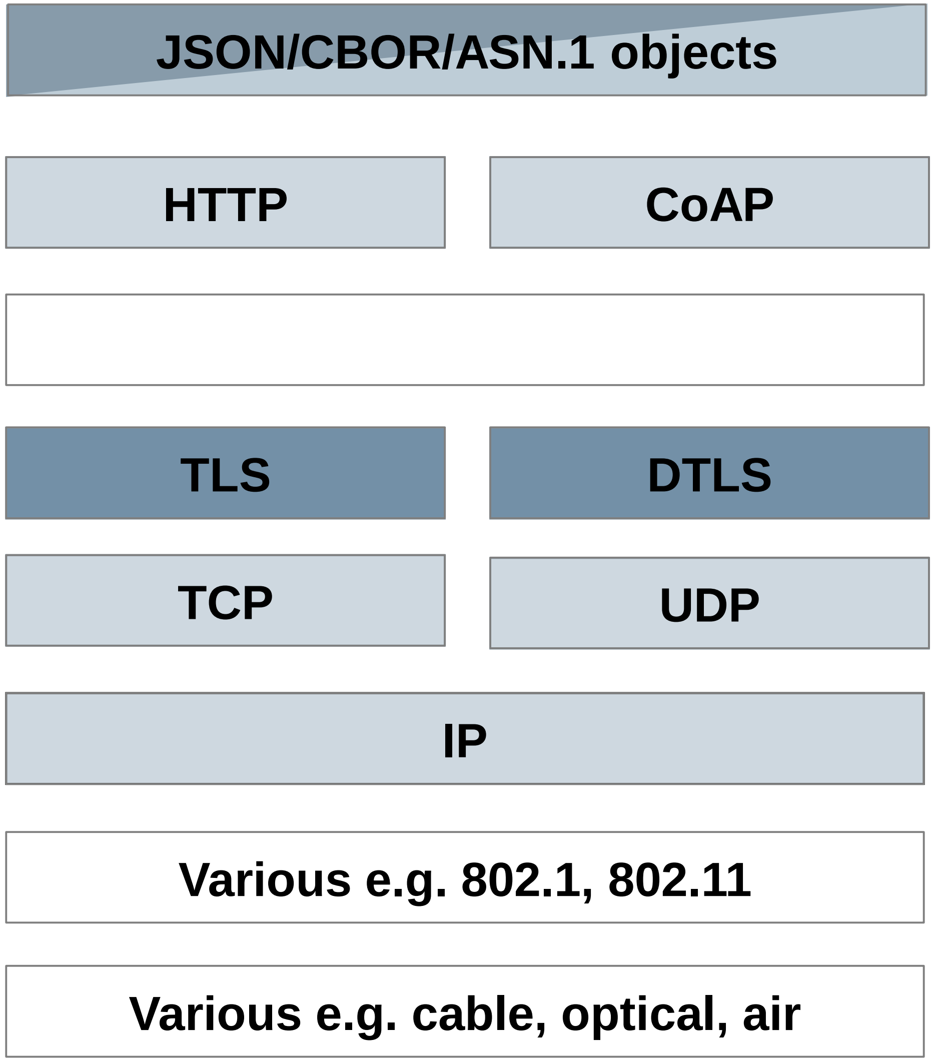
# What Are the Main Ingredients?

- **Actors**: site and manufacturer
- **Components**: pledge (aka IoT/OT component), join proxy, registrar, MASA
- **Exchanges**: 1. voucher (CA certificate portion in the LDevID), 2. voucher status (okay/not okay feedback), 3. enrollment (EE certificate portion in the LDevID), 4. enrollment status (okay/not okay feedback)



**A: 2 main actors, 4 main components, 4 main exchanges**

# How Does the Protocol Stack Look Like?



| Layer | | Protocols |
|---|---|---|
| Layer 7b | Application | JSON/CBOR/ASN.1 objects |
| Layer 7a | Application | HTTP<br>CoAP |
| Layer 6 | Presentation | |
| Layer 5 | Session | TLS<br>DTLS |
| Layer 4 | Transport | TCP<br>UDP |
| Layer 3 | Network | IP |
| Layer 2 | Data Link | Various e.g. 802.1, 802.11 |
| Layer 1 | Physical | Various e.g. cable, optical, air |

| | |
|---|---|
| ■ | Created by IETF Anima ([4], [5], [6]) |
| ▨ | Tailored by/for IETF Anima (provisional accept, [5], [6]) |
| □ | Used by IETF Anima (esp. [3] on layer 7b) |

**A: a blend of re-use, tailoring and invention**

IETF Anima

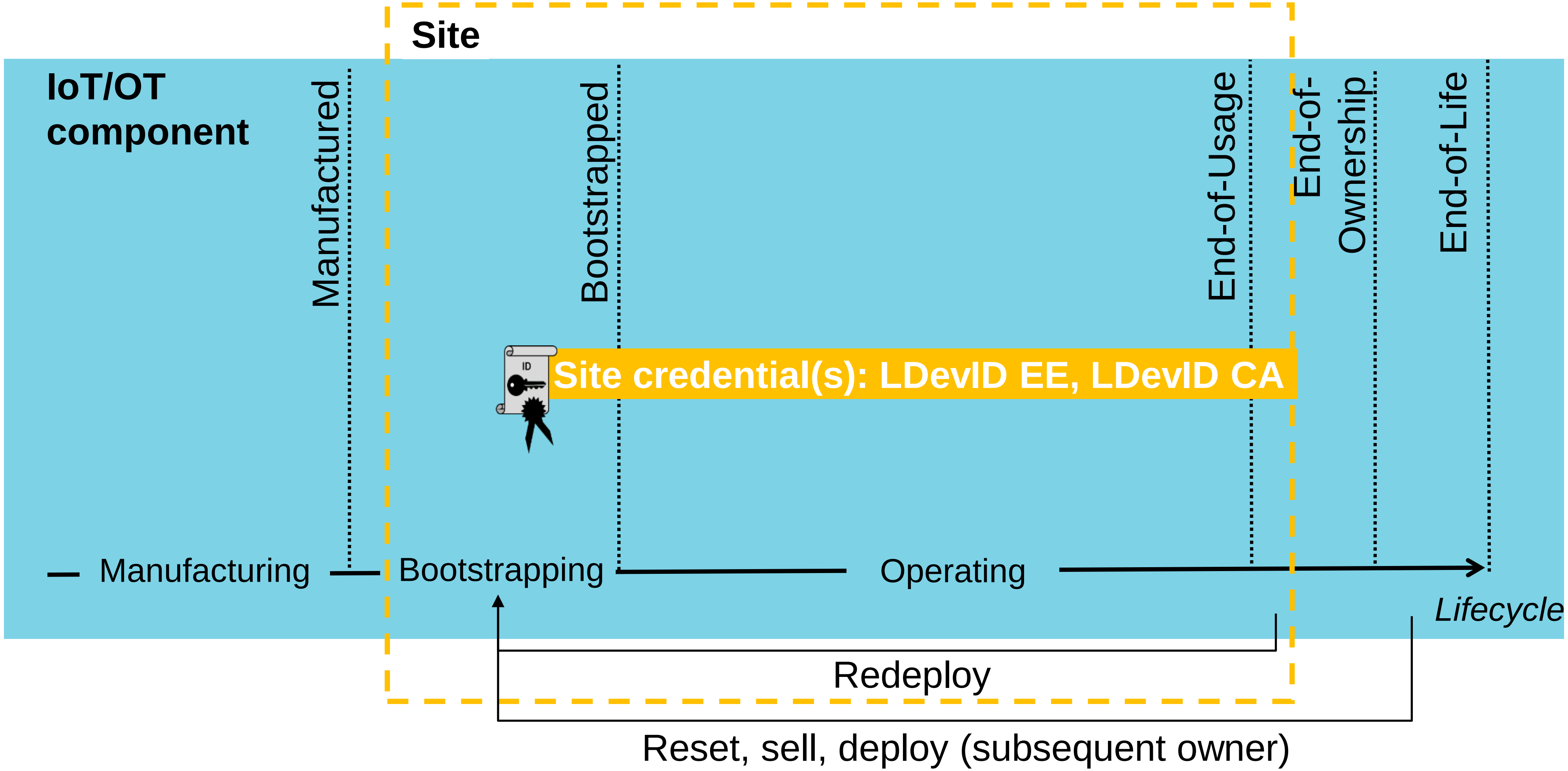
# Takeaways

- Covers the credentialing of IoT components in a way that is
  - Application-agnostic (can supply credentials for any application protocol or role)
  - Site-controlled
- Allows to supply credentials in the X.509 certificate form-factor
  - Arbitrary certificate contents
  - Arbitrary PKI hierarchies and means of revocation
- Employs services in sites (‘registrar’ and ‘join proxy’) and by component manufacturers (‘MASA’). Instances of the registrar and MASA services may be backed by traditional PKI components (RAs/CAs)
  - Enhancements for a better decoupling from manufacturer services are proposed, see [8]
- Covers the exchange pattern of internally-triggered pull
- Uses HTTP-over-TLS resp. CoAP-over-DTLS for the credentialing interactions with IoT components
- Exploits the idea of credential bootstrapping - the acquisition of new credentials, authenticated by already existing ones (from e.g. other issuers resp. for other domains)
- Aims at zero-touch

OPC-UA

# What Does Happen Inside IoT/OT Components?

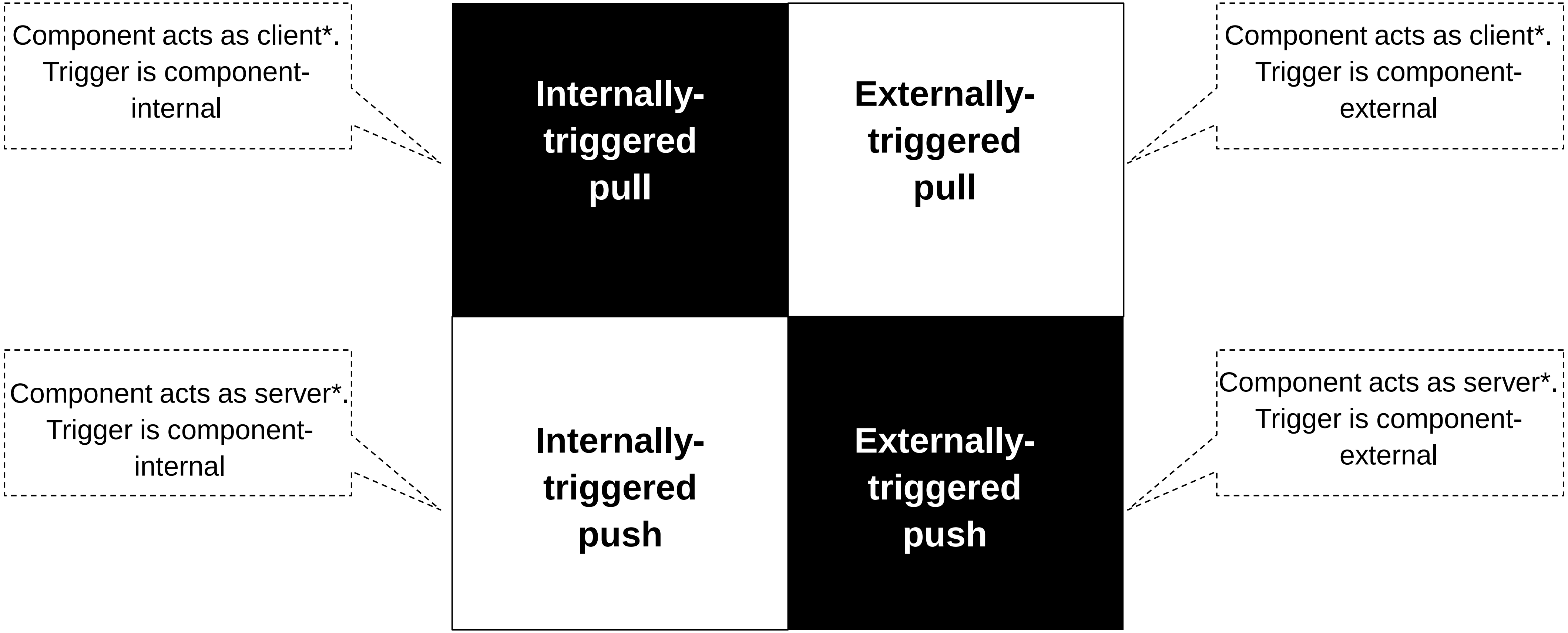
SIEMENS
Ingenuity for life



**A: acquire LDevIDs by means of administrative work (initial) or priorly established LDevIDs (subsequent)**

OPC-UA

# Which Patterns Are Covered?



Component acts as client*. Trigger is component-internal

Internally-triggered pull

Externally-triggered pull

Component acts as client*. Trigger is component-external

Component acts as server*. Trigger is component-internal

Internally-triggered push

Externally-triggered push

Component acts as server*. Trigger is component-external

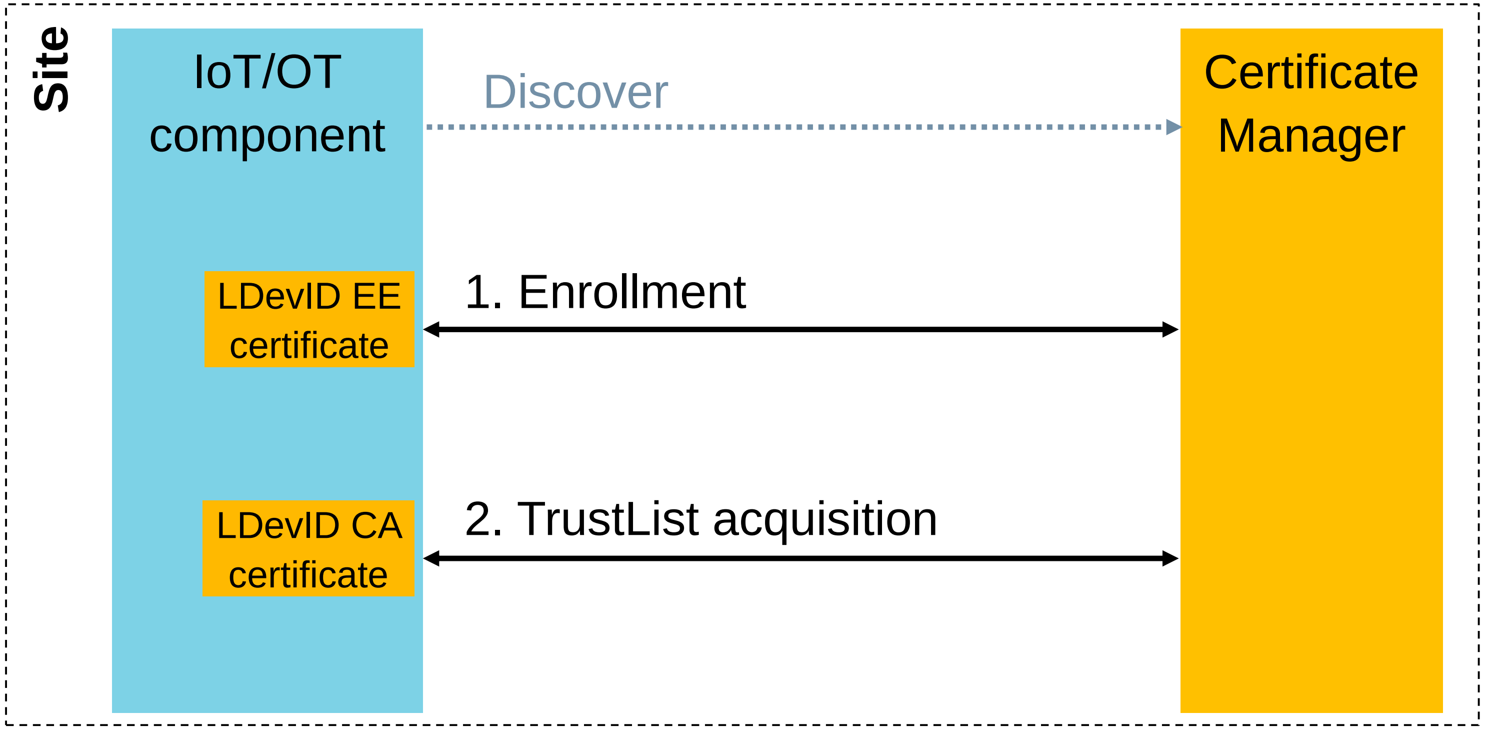
*: towards security infrastructure components (services, tools)

**A: as of now, internally triggered pull and externally trigged push**

OPC-UA

# What Are the Main Ingredients? For Pull

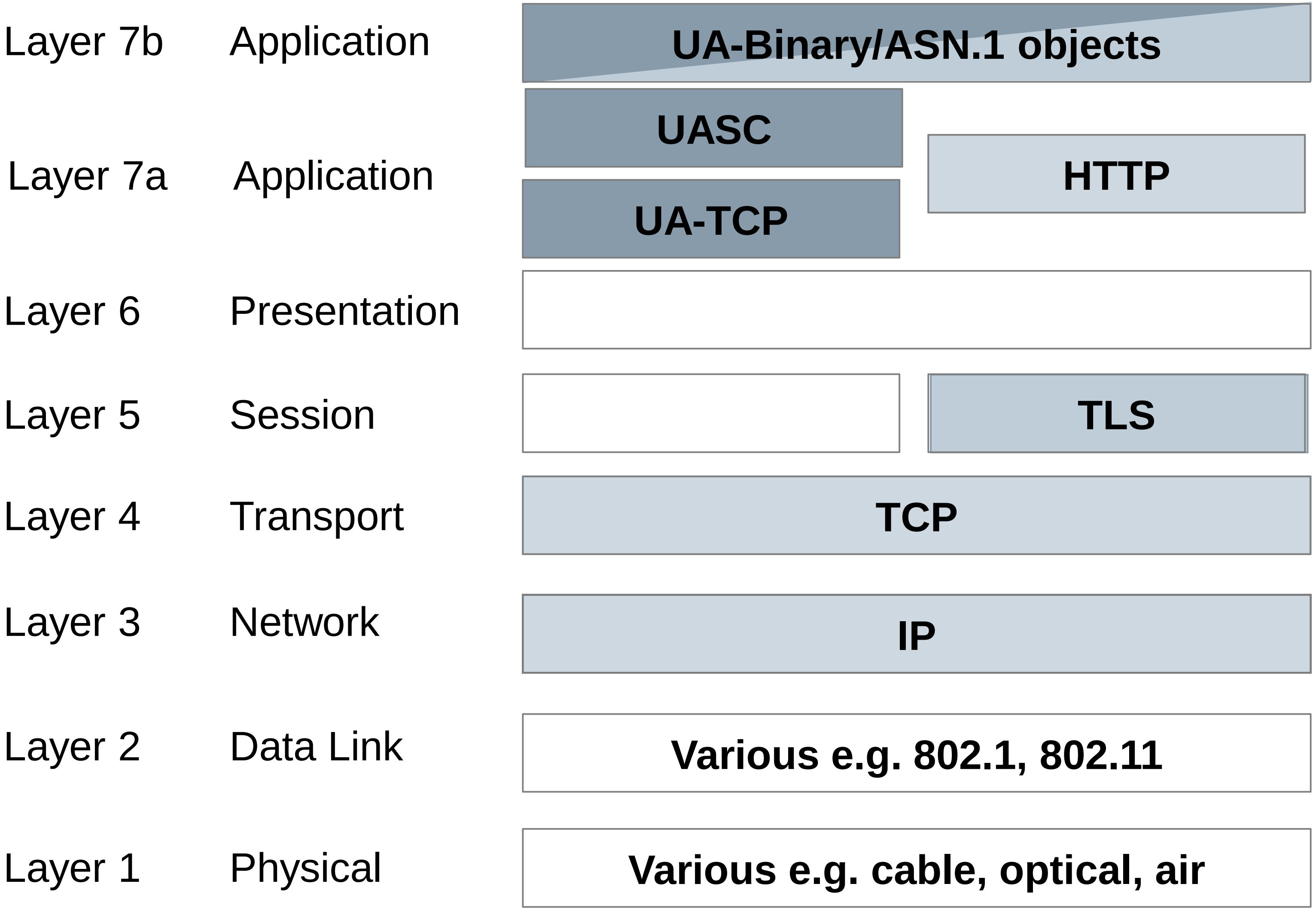
- **Actors**: site
- **Components**: IoT/OT component (OPC-UA client/server, publisher/subscriber), CertificateManager
- **Exchanges**: 1. enrollment (EE certificate portion in the LDevID), 2. TrustList acquisition (CA certificate portion in the LDevID plus revocation info)



**A (pull case): 1 main actor, 2 main components, 2 main exchanges**

# How Does the Protocol Stack Look Like?

SIEMENS
Ingenuity for life



| | | | |
|---|---|---|---|
| Layer 7b | Application | UA-Binary/ASN.1 objects | |
| Layer 7a | Application | UASC<br>UA-TCP | HTTP |
| Layer 6 | Presentation | | |
| Layer 5 | Session | | TLS |
| Layer 4 | Transport | TCP | |
| Layer 3 | Network | IP | |
| Layer 2 | Data Link | Various e.g. 802.1, 802.11 | |
| Layer 1 | Physical | Various e.g. cable, optical, air | |

■ Created by OPC-UA ([11], [12], [13])

□ Used by OPC-UA

**A: a blend of own form-factors and re-use**

## OPC-UA

# Takeaways

- Covers the credentialing of IoT components in a way that is
  - Application-specific (supplies credentials for OPC-UA clients/servers or publishers/subscribers)
  - Site-controlled
- Allows to supply credentials in the X.509 certificate form-factor
  - Dedicated certificate contents, specific to OPC-UA (aka ‘application instance certificates’)
  - Arbitrary PKI hierarchies, CRL-based revocation
- Employs services in sites (called ‘CertificateManager’). Instances of this service may be backed by traditional PKI components (RAs/CAs)
- Covers the exchange patterns of internally-triggered pull and externally-triggered push
- Uses the native OPC-UA stack for the credentialing interactions with IoT components
- Does not yet specify exchanges that employ credential bootstrapping
- Demands administrative work - does not yet address zero-touch

# Abbreviations

| | |
|---|---|
| Anima | Autonomic Networking Integrated Model and Approach |
| ASN.1 | Abstract Syntax Notation 1 |
| BRSKI | Bootstrapping Remote Secure Key Infrastructures |
| CA | Certification Authority |
| CBOR | Constrained Binary Object Representation |
| CoAP | Constrained Application Protocol |
| CRL | Certificate Revocation List |
| DTLS | Datagram Transport Layer Security |
| EE | End Entity |
| EST | Enrollment over Secure Transport |
| GDS | Global Discovery Service |
| HTTP | Hypertext Transfer Protocol |
| IDevID | Initial Device IDentifier |
| IoT | Internet of Things |
| JSON | JavaScript Object Notation |
| LDevID | Locally significant Device IDentifier |
| MASA | Manufacturer Authorized Signing Authority |
| OPC | Open Platform Communication |
| OT | Operational Technology |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| TLS | Transport Layer Security |
| UA | Unified Architecture |
| UASC | UA Secure Conversation |

# References

1. IEEE 802.1AR-2009: *IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity*, 2009
2. IEEE 802.1AR-2018: *IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity*, 2018
3. IETF RFC 7030: *Enrollment over Secure Transport*, RFC 7030, 2013
4. IETF RFC 8366: *A Voucher Artifact for Bootstrapping Protocols*, RFC 8366, 2018
5. IETF BRSKI: *Bootstrapping Remote Secure Key Infrastructures (BRSKI)*, Draft (work-in-progress), 2020
6. IETF Constrained Voucher: *Constrained Voucher Artifacts for Bootstrapping Protocols,* Draft (work-in-progress), 2020
7. IETF EST-coaps: *EST over secure CoAP (EST-coaps),* Draft (work-in-progress), 2020
8. IETF Delegated Authority: *Delegated Authority for Bootstrap Voucher Artifacts*. Draft (work-in-progress), 2020
9. OPC Foundation: The OPC-UA Security Model For Administrators, Whitepaper Version 1.00, 2010
10. OPC Foundation: Unified Architecture, Part 2 Security Model, Release 1.04, 2018
11. OPC Foundation: Unified Architecture, Part 4 Services, Release 1.04, 2017
12. OPC Foundation: Unified Architecture, Part 6 Mappings, Release 1.04, 2017
13. OPC Foundation: Unified Architecture, Part12: Discovery and Global Services, Release 1.04, 2018
14. OPC Foundation: Unified Architecture, Part 14 PubSub, Release 1.04, 2018

# Author

**Oliver Pfaff**

Principal Key Expert

Siemens AG

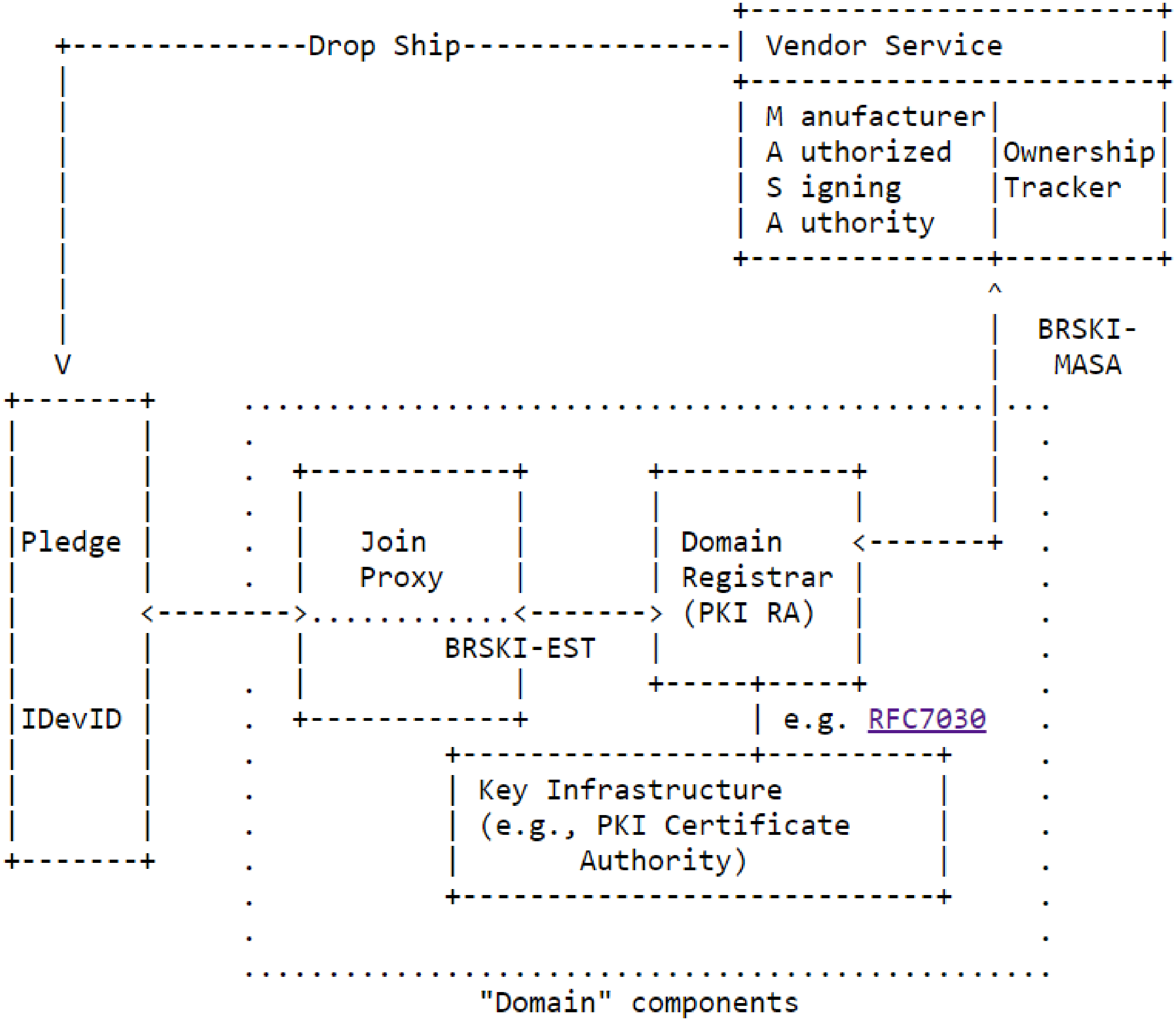
CT RDA CST

oliver.pfaff@siemens.com

**siemens.com**

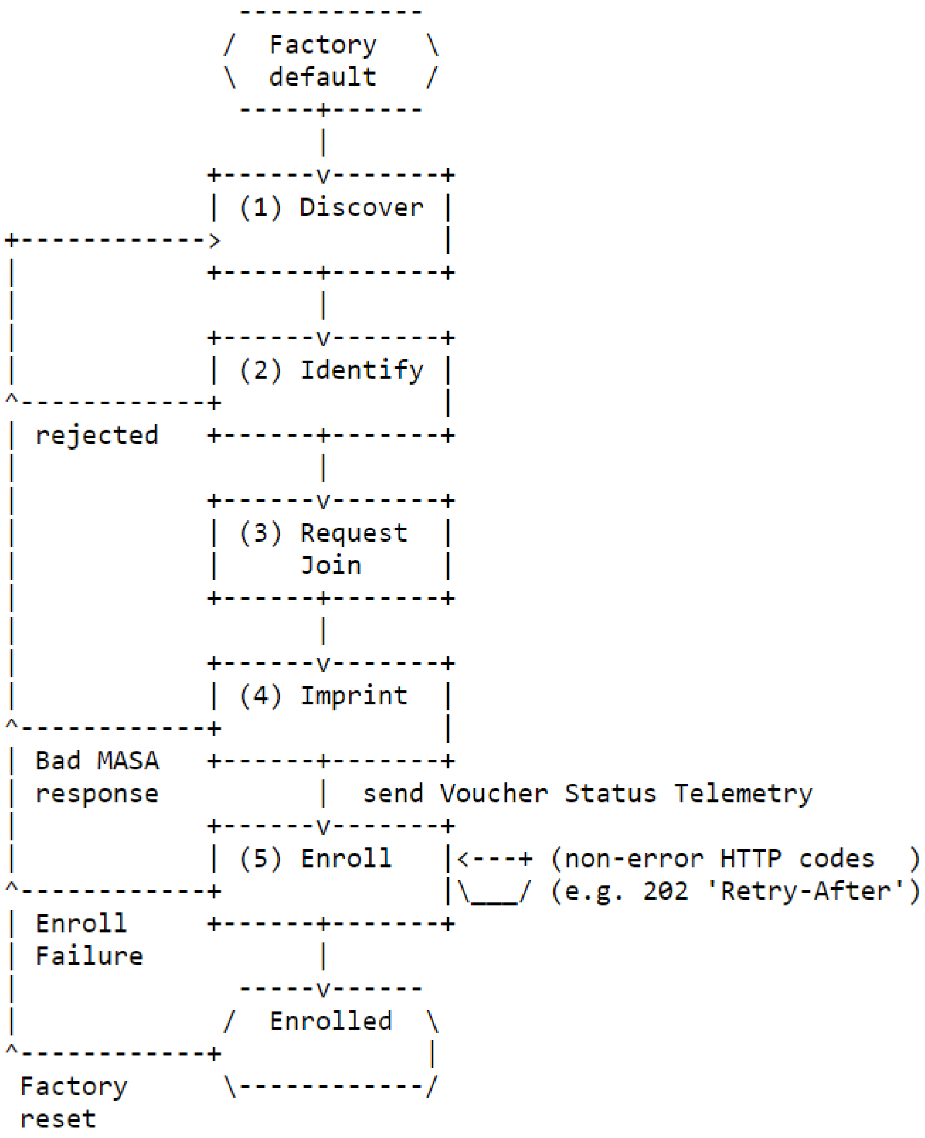
## IETF Anima

# System Architecture



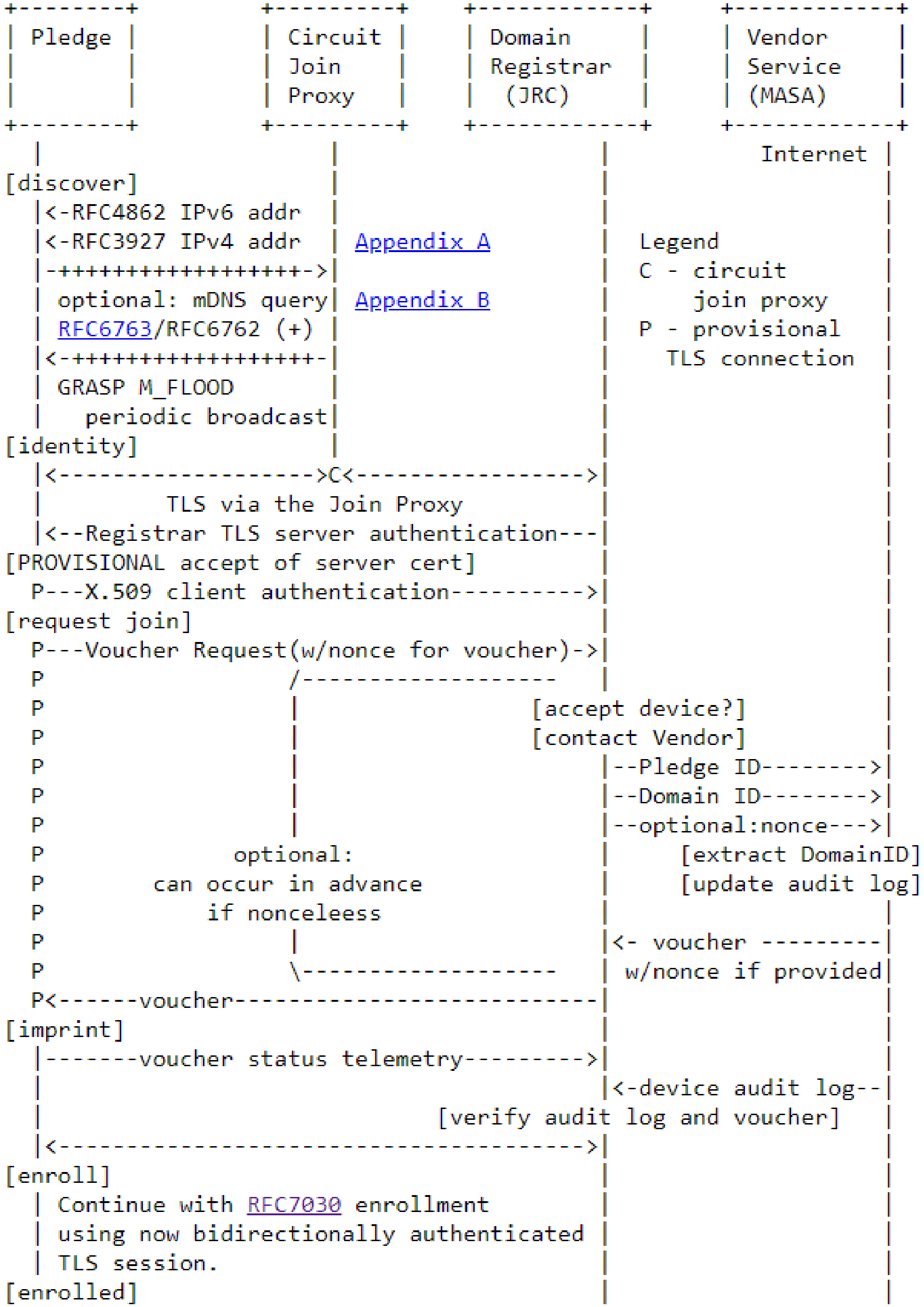
```
                                         +------------------------+
   +-------------Drop Ship---------------| Vendor Service         |
   |                                     +------------------------+
   |                                     | M anufacturer|         |
   |                                     | A uthorized  |Ownership|
   |                                     | S igning     |Tracker  |
   |                                     | A uthority   |         |
   |                                     +--------------+---------+
   |                                                    ^
   |                                                    | BRSKI-
   V                                                    |  MASA
+-------+     ..........................................|...
|       |     .                                         |  .
|       |     .  +------------+       +-----------+     |  .
|       |     .  |            |       |           |     |  .
|Pledge |     .  |   Join     |       | Domain    <-----+  .
|       |     .  |   Proxy    |       | Registrar |        .
|       <-------->............<-------> (PKI RA)  |        .
|       |        |       BRSKI-EST    |           |        .
|       |     .  |            |       +-----+-----+        .
|IDevID |     .  +------------+             | e.g. RFC7030 .
|       |     .           +-----------------+--------+     .
|       |     .           | Key Infrastructure       |     .
|       |     .           | (e.g., PKI Certificate   |     .
+-------+     .           |      Authority)          |     .
              .           +--------------------------+     .
              .                                            .
              ..............................................
                          "Domain" components
```

## IETF Anima
# Pledge States



```
               ------------
              /  Factory   \
              \  default   /
               -----+------
                    |
             +------v-------+
             | (1) Discover |
+------------>              |
|            +------+-------+
|                   |
|            +------v-------+
|            | (2) Identify |
^------------+              |
| rejected   +------+-------+
|                   |
|            +------v-------+
|            | (3) Request  |
|            |     Join     |
|            +------+-------+
|                   |
|            +------v-------+
|            | (4) Imprint  |
^------------+              |
| Bad MASA   +------+-------+
| response          |  send Voucher Status Telemetry
|            +------v-------+
|            | (5) Enroll   |<---+ (non-error HTTP codes   )
^------------+              |\___/ (e.g. 202 'Retry-After')
| Enroll     +------+-------+
| Failure           |
|              -----v------
|             /  Enrolled   \
^------------+              |
 Factory      \------------/
 reset
```

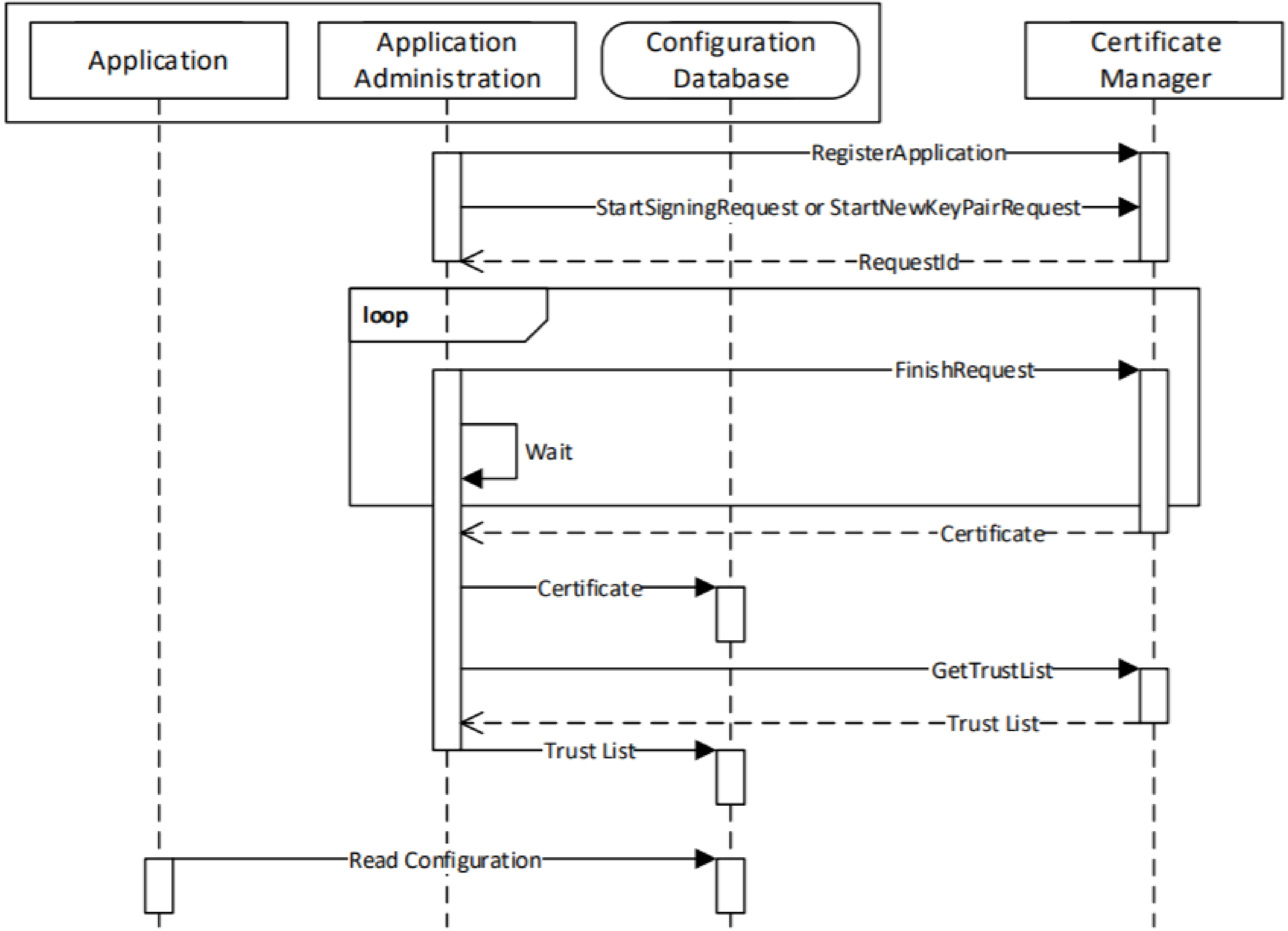
## IETF Anima
# Main Swim-Lane



```
+--------+         +---------+    +------------+     +------------+
| Pledge |         | Circuit |    | Domain     |     | Vendor     |
|        |         | Join    |    | Registrar  |     | Service    |
|        |         | Proxy   |    |  (JRC)     |     | (MASA)     |
+--------+         +---------+    +------------+     +------------+
  |                     |                   |           Internet |
[discover]              |                   |                    |
  |<-RFC4862 IPv6 addr  |                   |                    |
  |<-RFC3927 IPv4 addr  | Appendix A        |  Legend            |
  |-++++++++++++++++++->|                   |  C - circuit       |
  | optional: mDNS query| Appendix B        |      join proxy    |
  | RFC6763/RFC6762 (+) |                   |  P - provisional   |
  |<-++++++++++++++++++-|                   |    TLS connection  |
  | GRASP M_FLOOD       |                   |                    |
  |   periodic broadcast|                   |                    |
[identity]              |                   |                    |
  |<------------------->C<----------------->|                    |
  |         TLS via the Join Proxy          |                    |
  |<--Registrar TLS server authentication---|                    |
[PROVISIONAL accept of server cert]         |                    |
  P---X.509 client authentication---------->|                    |
[request join]                              |                    |
  P---Voucher Request(w/nonce for voucher)->|                    |
  P                  /-------------------   |                    |
  P                  |                 [accept device?]          |
  P                  |                 [contact Vendor]          |
  P                  |                      |--Pledge ID-------->|
  P                  |                      |--Domain ID-------->|
  P                  |                      |--optional:nonce--->|
  P              optional:                  |     [extract DomainID]
  P         can occur in advance            |     [update audit log]
  P            if nonceleess                |                    |
  P                  |                      |<- voucher ---------|
  P                  \-------------------   | w/nonce if provided|
  P<------voucher---------------------------|                    |
[imprint]                                   |                    |
  |-------voucher status telemetry--------->|                    |
  |                                         |<-device audit log--|
  |                             [verify audit log and voucher]   |
  |<--------------------------------------->|                    |
[enroll]                                    |                    |
  | Continue with RFC7030 enrollment        |                    |
  | using now bidirectionally authenticated |                    |
  | TLS session.                            |                    |
[enrolled]                                  |                    |
```

OPC-UA

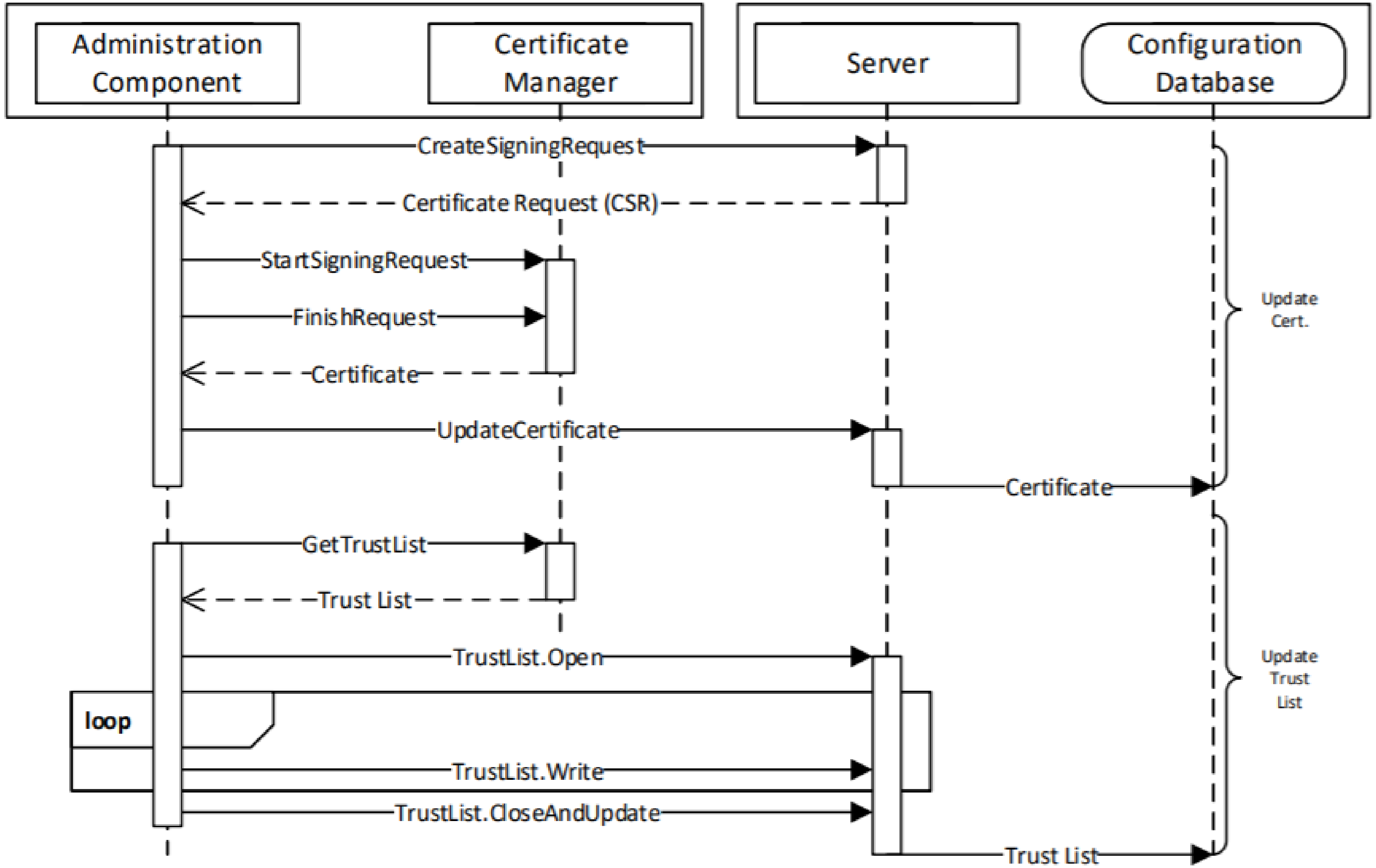
# Pull Certificate Management



OPC-UA

# Push Certificate Management

SIEMENS
Ingenuity for life



## OPC-UA

# Application Instance Certificates

SIEMENS
Ingenuity for life

- Initial credentials in form of X.509 public key certificates are assigned to instances of OPC-UA applications (clients/servers or publishers/subscribers)
- They are called **OPC-UA application instance certificates**. These objects are introduced in [10] which refers to [11] and [12] for the details. Moreover [9] provides information about them
- OPC-UA application instance certificates are X.509 certificate objects in the site resp. LDevID incarnation with following contents (see [9] and [12], table 26):
  - `subject` (X.500 distinguished name): contains `cn` and `o` attributes. The value of cn attribute is an application/product name. The value of the o attribute is name of the organization that executes the application instance (not: vendor/manufacturer)
  - `validity`: `notBefore`/`notAfter` markers with a default of 5 years
  - `subjectAltName` (X.509v3 certificate extension): contains
    - `uniformResourceIdentifier`: OPC application URI AND
    - `(dNSName`: name of the host running the OPC application OR
    - `iPAddress`: IP address of the host running the OPC application)
- Certificate revocation is done by means of CRLs