SIEMENS
Ingenuity for life

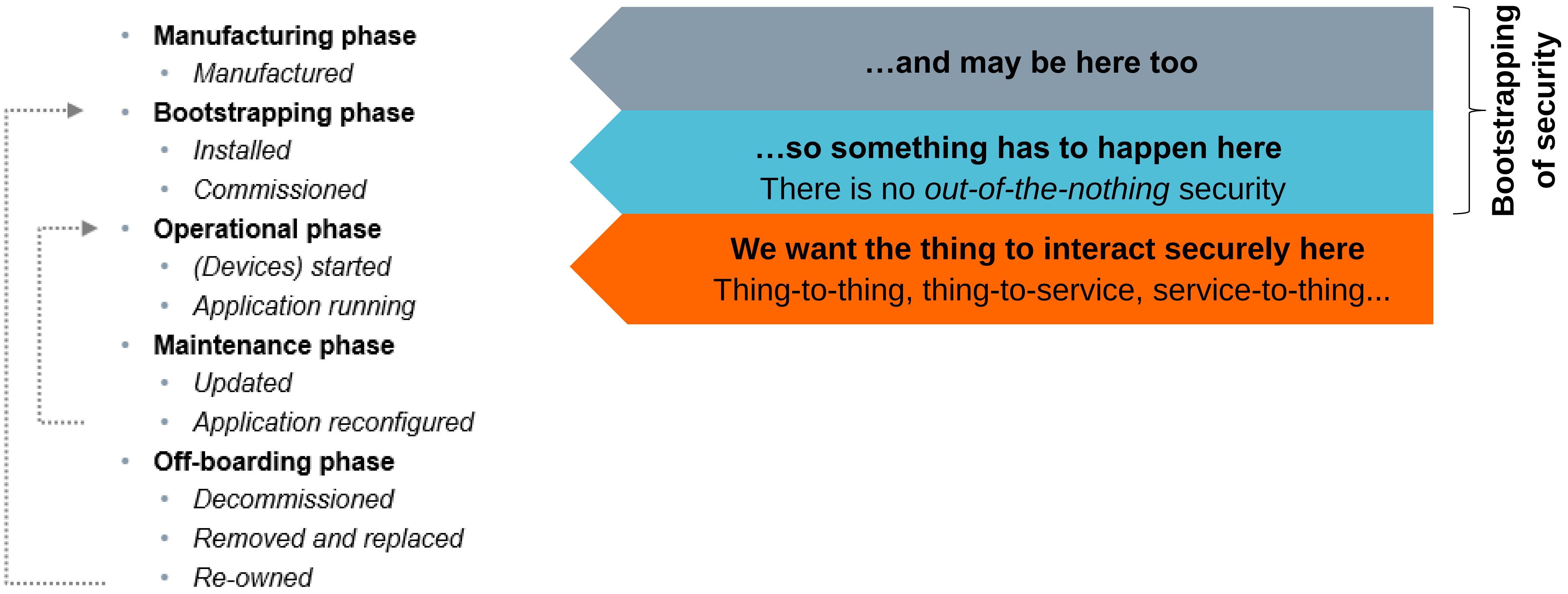
Second W3C Workshop on the Web of Things – Munich, June 3-5, 2019

About the Bootstrapping of Security in IoT

Oliver Pfaff

The Challenge

- Lifecycle of a thing (WoT/IoT/OT):



- **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 may be here too

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

We want the thing to interact securely here
Thing-to-thing, thing-to-service, service-to-thing...

Bootstrapping of security

Common Practices

- *What solution properties do we find today - with respect to the bootstrapping of security?*
  - **Easy-to-use but not (really) secure**: naïve security (e.g. shared credentials) or no security at all

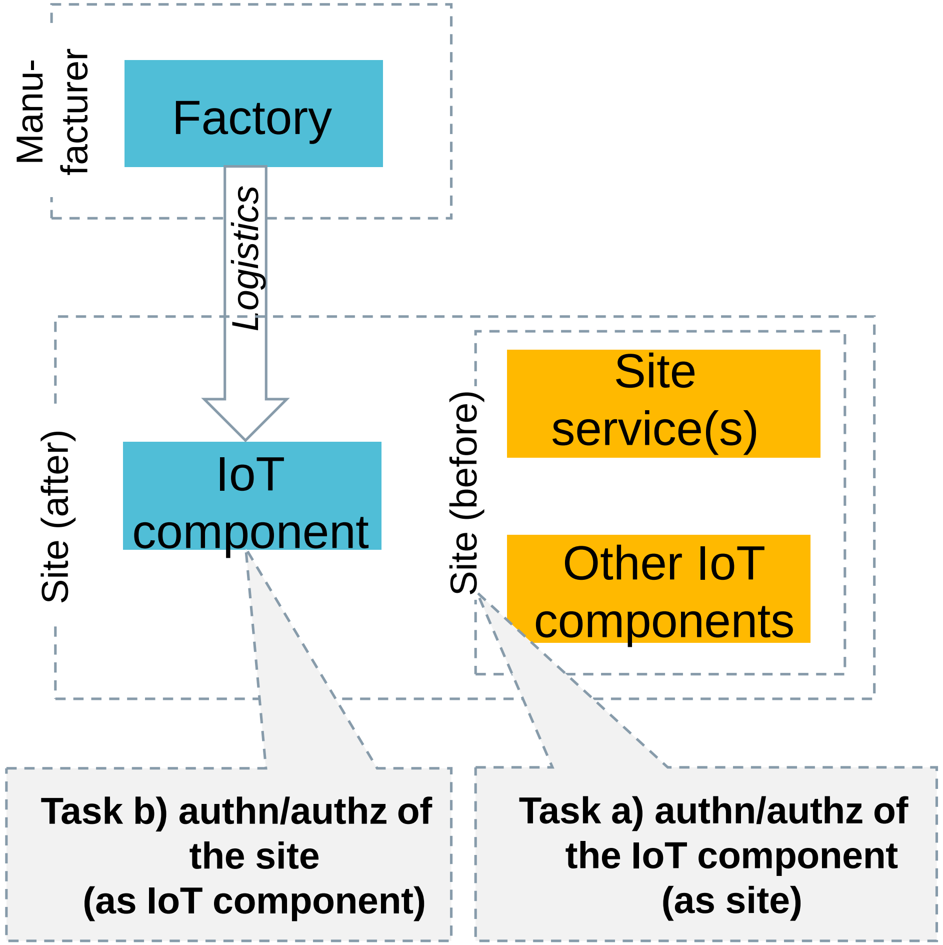
  OR
  - **Secure but not easy-to-use**: tedious handling, manual processing steps…

- *What do we not yet find?*
  - **Easy-to-use *AND* secure**

Not Yet Championed Task

SIEMENS

Ingenuity for life



Manu-facturer

Factory

Logistics

Site (after)

IoT component

Site (before)

Site service(s)

Other IoT components

Task b) authn/authz of the site (as IoT component)

Task a) authn/authz of the IoT component (as site)

- The overall **security challenge**: IoT component and site shall establish mutual trust
- Is comprised of following tasks:

  a) Site authenticates and authorizes the IoT component: *What is this component? Do I want it?*

  b) IoT component authenticates and authorizes the site: *What is this site? Should I join it?*

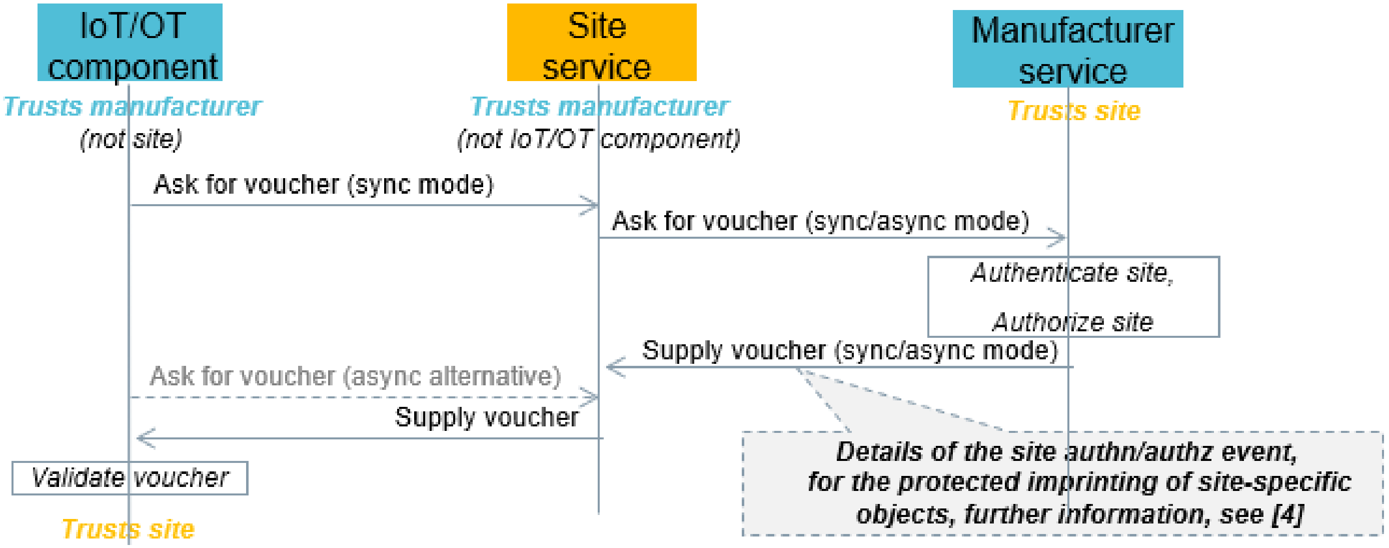
- Their hardness differs:

  a) is moderate; can be solved by using known recipes

  b) is hard and is **not yet solved** esp. when this task shall be done without manual intervention at the thing

Relevant Initiatives

- Anima (IETF WG, BSRKI/EST)
- 6tisch Zero Touch (IETF WG Draft)
- 6tisch Minimal Security (IETF WG Draft)
- Netconf SZTP (IETF WG Draft)
- …(*not meant to be an exhaustive list*)



IoT/OT component

Trusts manufacturer

(not site)

Site service

Trusts manufacturer

(not IoT/OT component)

Manufacturer service

Trusts site

Ask for voucher (sync mode)

Ask for voucher (sync/async mode)

Authenticate site,

Authorize site

Supply voucher (sync/async mode)

Ask for voucher (async alternative)

Supply voucher

Validate voucher

Trusts site

Details of the site authn/authz event, for the protected imprinting of site-specific objects, further information, see [4]

Their trick: ***let somebody else*** *(manufacturer service)* ***do the hard task***

Takeaways

SIEMENS
Ingenuity for life

- Bootstrapping security is a **key concern** in WoT/IoT/OT. It is not yet championed to a full extent
- Important **innovations** and **adoptions** are happening right **now,** on international level e.g. the IETF Anima working group, the Fairhair Alliance or the Thread Group
- The emerging IETF Anima solution is in a leading position. It allows to **do more** than just security bootstrapping

Abbreviations

Anima	Autonomic Networking Integrated Model and Approach
Authn	Authentication
Authz	Authorization
BRSKI	Bootstrapping Remote Secure Key Infrastructures
CA	Certification Authority
CoAP	Constrained Application Protocol
coaps	Access scheme for CoAP-over-DTLS
(D)TLS	TLS or DTLS
DTLS	Datagram Transport Layer Security
EE	End Entity
EST	Enrollment over Secure Transport
HTTP	Hypertext Transfer Protocol
https	Access scheme for HTTP-over-TLS
IDevID	Initial Device IDentifier
IoT	Internet of Things
LDevID	Locally significant Device Identifier
MASA	Manufacturer Authorized Signing Authority
OT	Operational Technology
SZTB	Secure and Zero-Touch Bootstrapping
SZTP	Secure and Zero-Touch Provisioning
TLS	Transport Layer Security

References

[1] IEEE 802.1AR-2009, *IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity*, 2009

[2] IETF BRSKI: *Bootstrapping Remote Secure Key Infrastructures (BRSKI)*, Draft (work-in-progress), 2019

[3] IETF 6tisch Minimal Security: *Minimal Security Framework for 6TiSCH, Draft (work-in-progress), 2019*

[4] IETF 6tisch Zero-Touch: *6tisch Zero-Touch Secure Join protocol, Draft (work-in-progress), 2018 (expired)*

[5] IETF Constrained Voucher: *Constrained Voucher Artifacts for Bootstrapping Protocols,* Draft (work-in-progress), 2019

[6] IETF EST-coaps: *EST over secure CoAP (EST-coaps),* Draft (work-in-progress), 2019

[7] IETF Netconf SZTP: *Secure Zero Touch Provisioning (SZTP),* Draft (work-in-progress), 2019

[8] IETF RFC 7030: *Enrollment over Secure Transport*, RFC 7030, 2013

[9] IETF RFC 8366: *A Voucher Artifact for Bootstrapping Protocols*, RFC 8366, 2018

[10] Stajano, F.; Anderson, R.: *The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks.* In: Securi Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999

[11] Wikipedia: *Mirai (malware)*. Retrieved May 25, 2019

Author

SIEMENS
Ingenuity for life

Oliver Pfaff

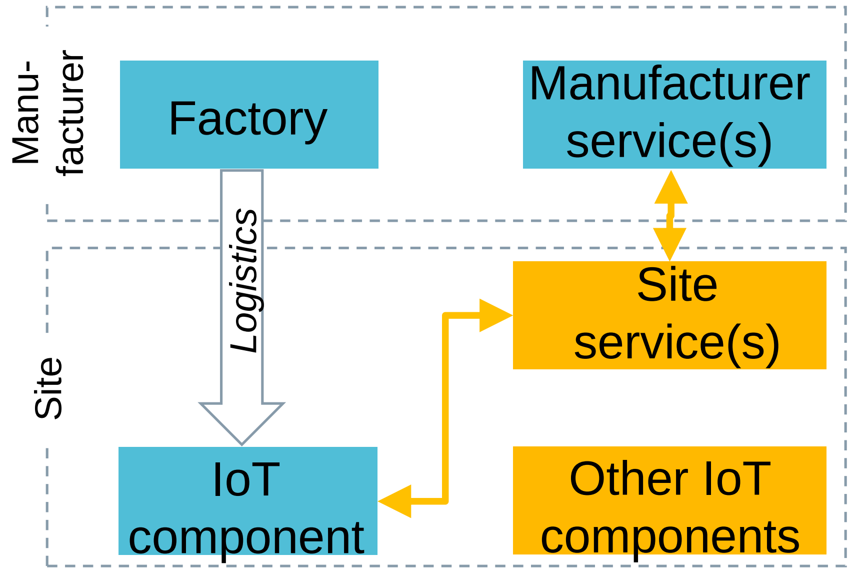
Siemens AG

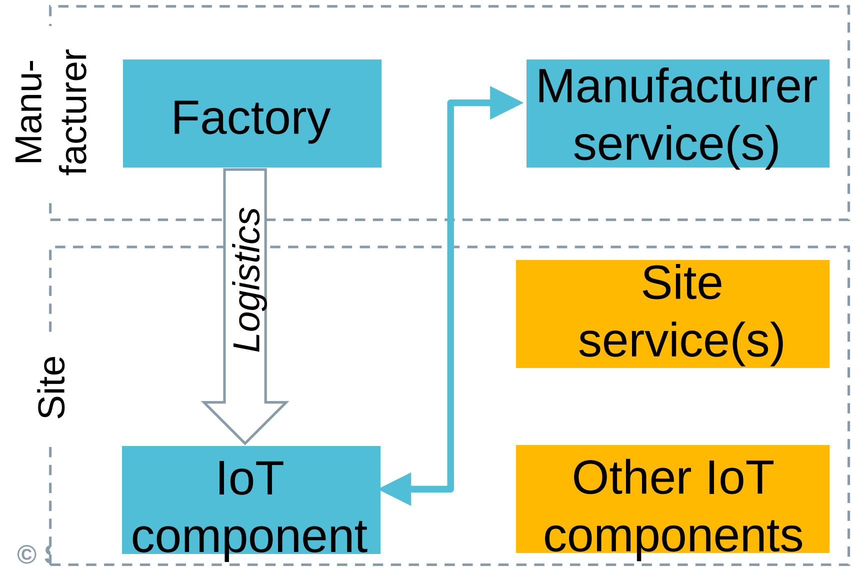
CT RDA ITS

oliver.pfaff@siemens.com

siemens.com

Architectural Patterns



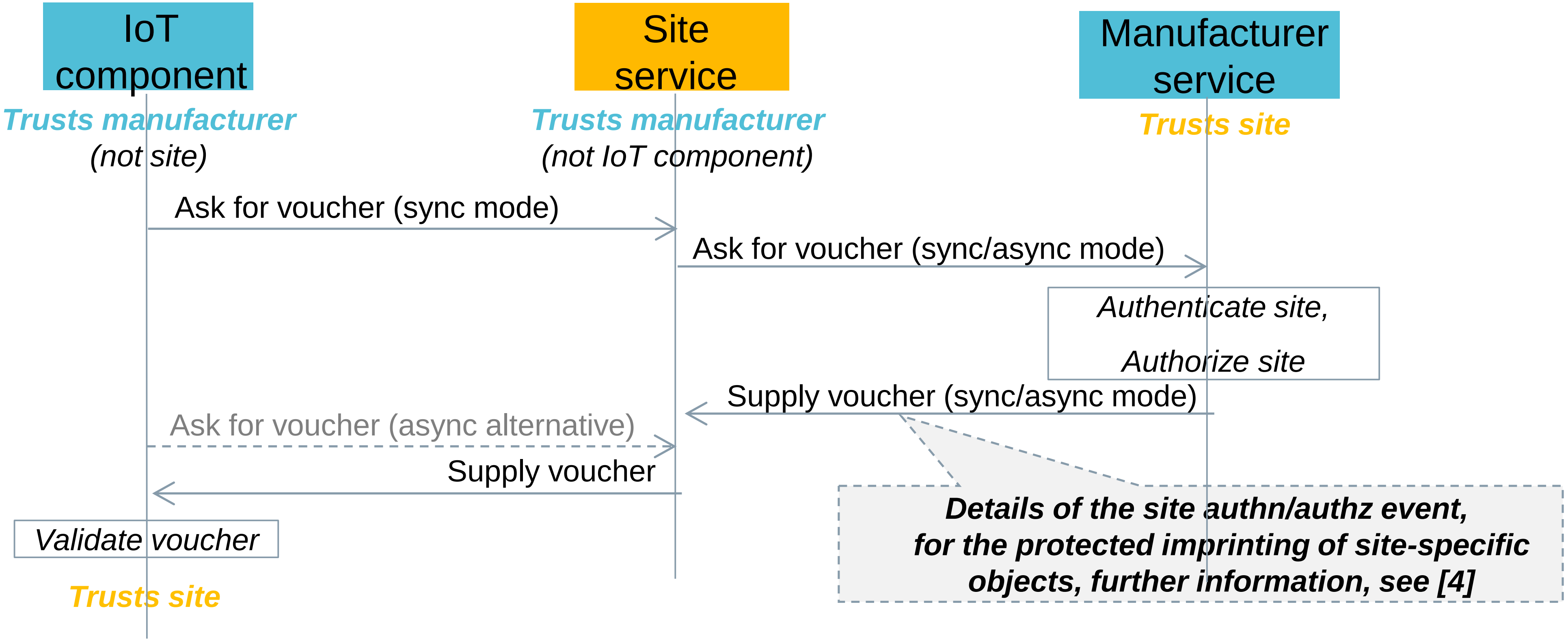


- **Site-facing** manufacturer services:
  - The manufacturer does authenticate and authorize (3rd party) sites i.e. the users of its IoT components through this service
  - This requires interoperability, local-area network connectivity is sufficient for IoT components
  - It allows to support site/user-aware use cases e.g. SZTB and CRM
- **IoT component-facing** manufacturer services:
  - The manufacturer does authenticate (own) IoT components through this service
  - This requires wide-area connectivity, DIY services sufficient
  - It allows to support site/user-unaware use cases e.g. component maintenance

Doing the SZTB Trick with IETF Anima

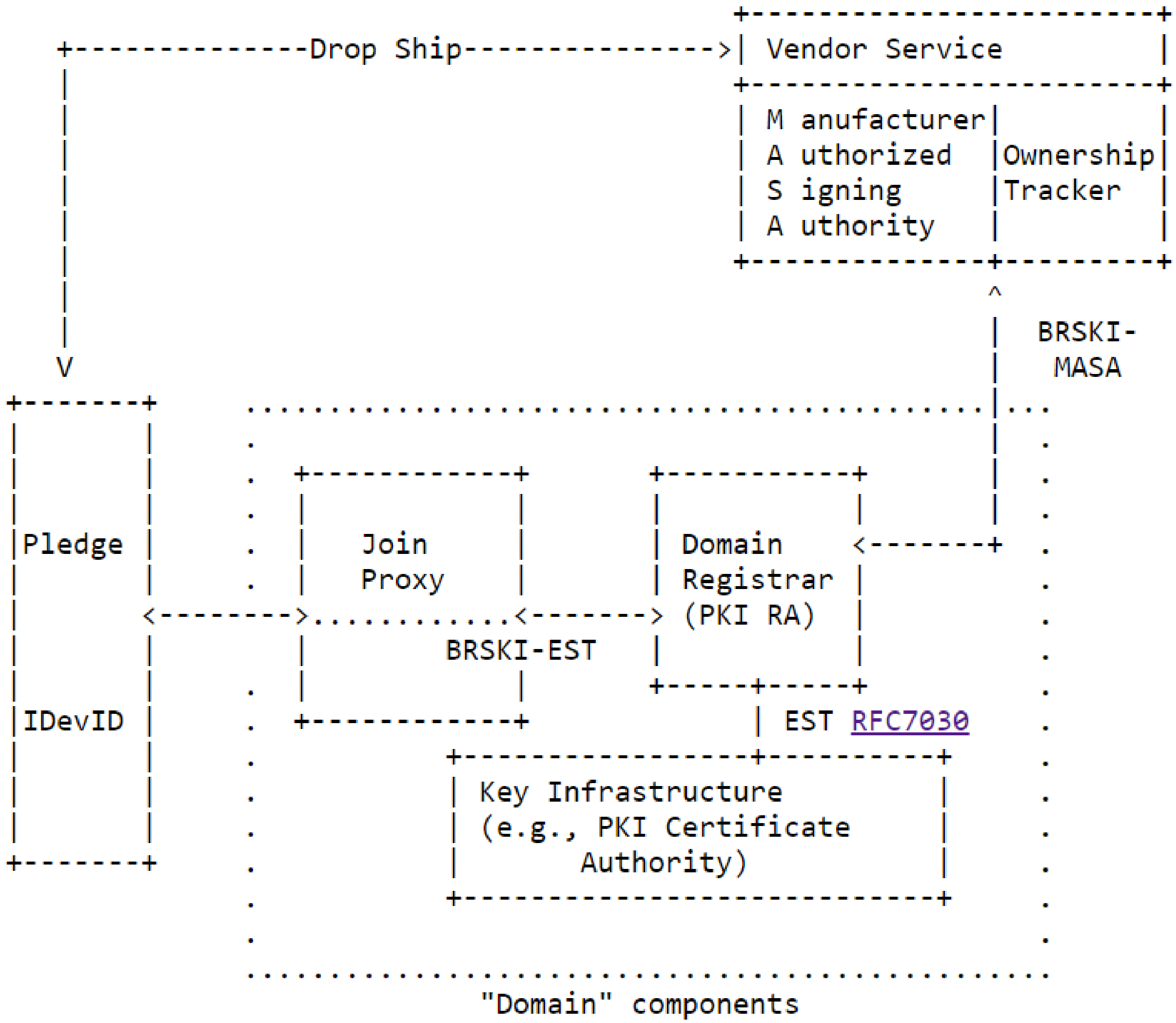
SIEMENS
Ingenuity for life

- *Moderate task a)* is addressed by a **site service**. It authenticates and authorizes the IoT component using (D)TLS with manufacturer credentials (called IDevID) plus information about acceptance
- *Hard task b)* is solved by an indirection: a **manufacturer service** is introduced that authenticates and authorizes the site and reports about this to the IoT component, see [5]



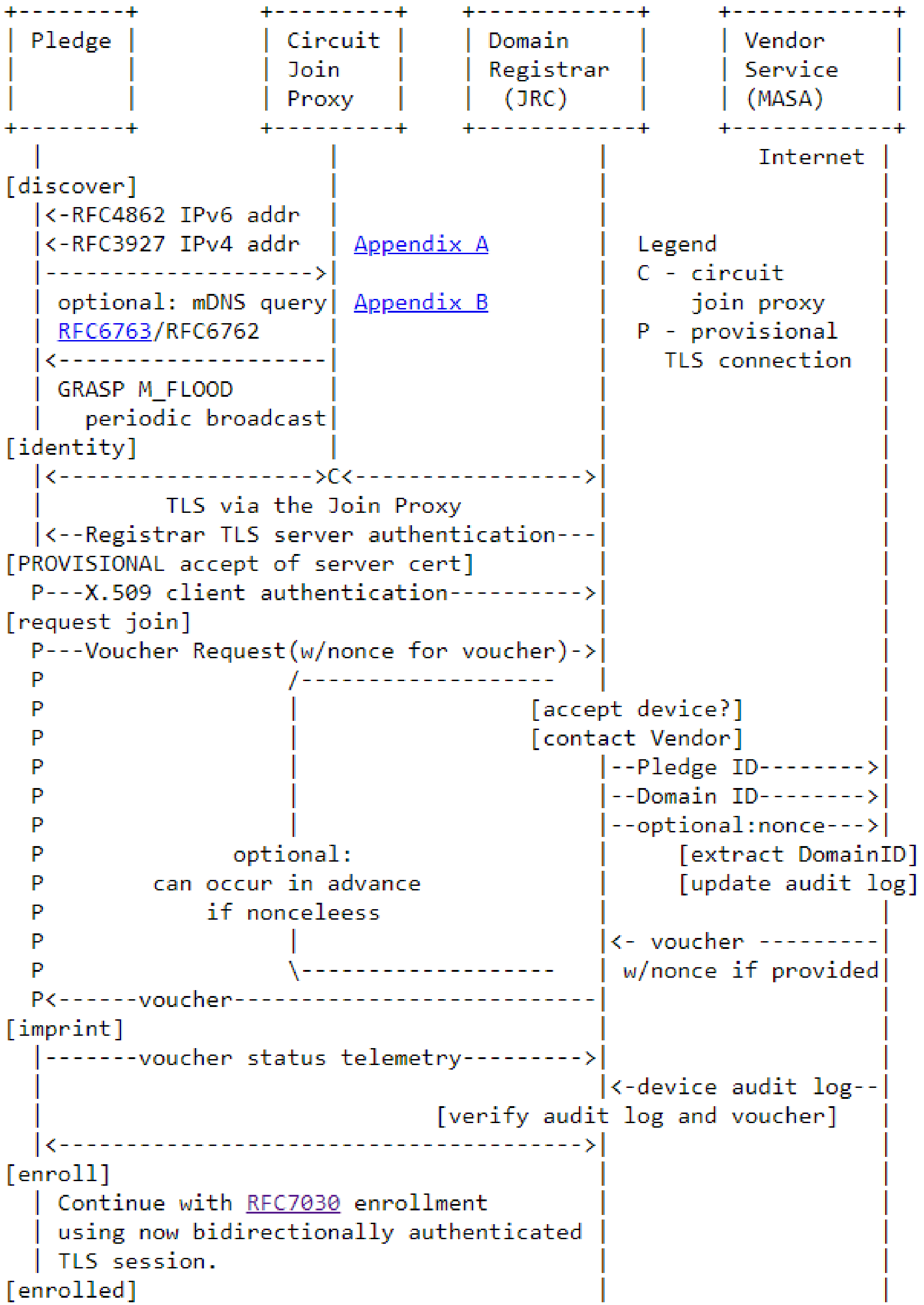
IoT component
Trusts manufacturer
(not site)
Site service
Trusts manufacturer
(not IoT component)
Manufacturer service
Trusts site
Ask for voucher (sync mode)
Ask for voucher (sync/async mode)
Authenticate site,
Authorize site
Supply voucher (sync/async mode)
Ask for voucher (async alternative)
Supply voucher
Validate voucher
Trusts site
Details of the site authn/authz event, for the protected imprinting of site-specific objects, further information, see [4]

Anima System Architecture



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

Anima 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]                                   |                    |
```

Current Blind Spots of Anima

SIEMENS
Ingenuity for life

- Blueprints for site-facing manufacturer services emerge right now ➔ do expect to get a core; not yet expect fully-blown specifications covering all possible aspects
- The current IETF Anima specifications come with white-spots and limitations including:
  - **Site-facing services**: assuming manufacturers to provide site-facing services
  - **Brown-field friendliness**: the current addressing scheme is not adequate for manufacturers with many, small pools of unique product serial numbers
  - **Sustainability**: service API versioning is not yet covered, message objects are self-contained but do not embody information about their structure
  - **Scalability**: bulk operation modes are not yet supported
  - **Unified credentialing**: supplying multiple, site-specific credentials that are bound to dedicated application domains to one IoT component can be accommodated but this is not yet profiled or detailed