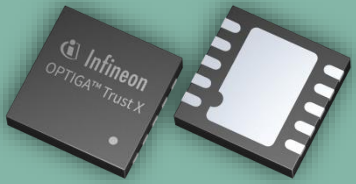
Hardware-Security
“Einfach (und) Sicher”?



Dr. **Christian Lesjak** – Infineon Technologies
Building IoT, Köln, 2018-06-04..06

Agenda

1 Motivation

2 Hardware-based security – what is it?

3 Cloud system architecture with hardware-based security

4 Getting started with hardware-security and Infineon products

5 Conclusion

Agenda

1 Motivation

2 Hardware-based security – what is it?

3 Cloud system architecture with hardware-based security

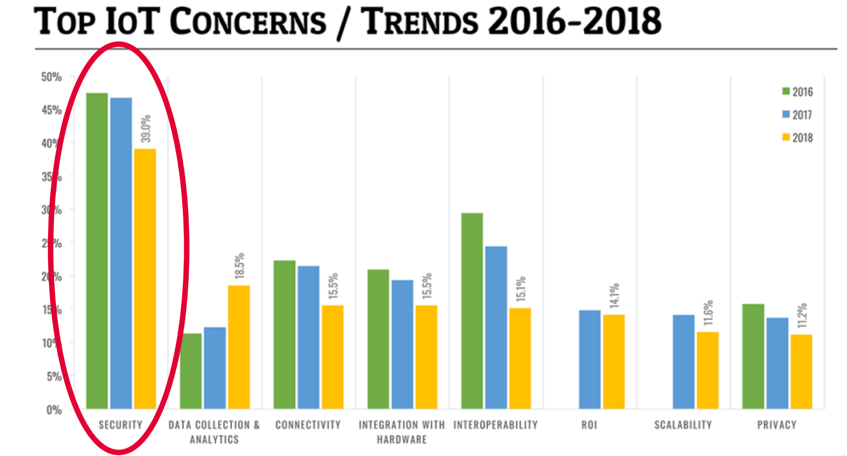
4 Getting started with hardware-security and Infineon products

5 Conclusion

Motivation /1

- **Vulnerabilities** and flaws
  - e.g., Heartbleed, Meltdown, Spectre
- **Attacks**: espionage & sabotage
  - e.g., Mirai botnet
- **Consequences** and effects
  - e.g., cost, loss of reputation

- Decreasing concern for security
  - Why?



Motivation /2

- **“13 Steps** to Developing **Secure IoT Products”** [CSA 2016]

1. Secure development methodology
2. Secure development and integration environment
3. Identity framework and platform security features
4. Establish privacy protections
5. Hardware security engineering
6. Protect data
7. Secure associated apps/services
8. Protect interfaces/APIs
9. Provide secure update capability
10. Implement secure authentication
11. Establish secure key management
12. Provide Logging mechanisms
13. Perform security reviews

[https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf]

Motivation /2

- **“13 Steps** to Developing **Secure IoT Products”** [CSA 2016]

1. Secure development methodology
2. Secure development and integration environment
3. Identity framework and platform security features
4. Establish privacy protections
5. Hardware security engineering
6. Protect data
7. Secure associated apps/services
8. Protect interfaces/APIs
9. Provide secure update capability
10. Implement secure authentication
11. Establish secure key management
12. Provide Logging mechanisms
13. Perform security reviews

[https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf]

Agenda

1 Motivation

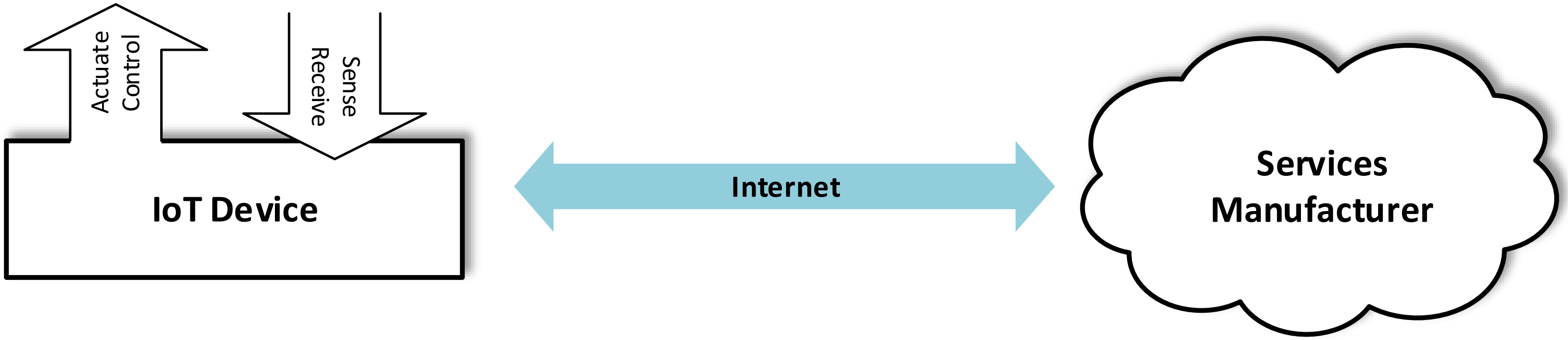
2 Hardware-based security – what is it?

3 Cloud system architecture with hardware-based security

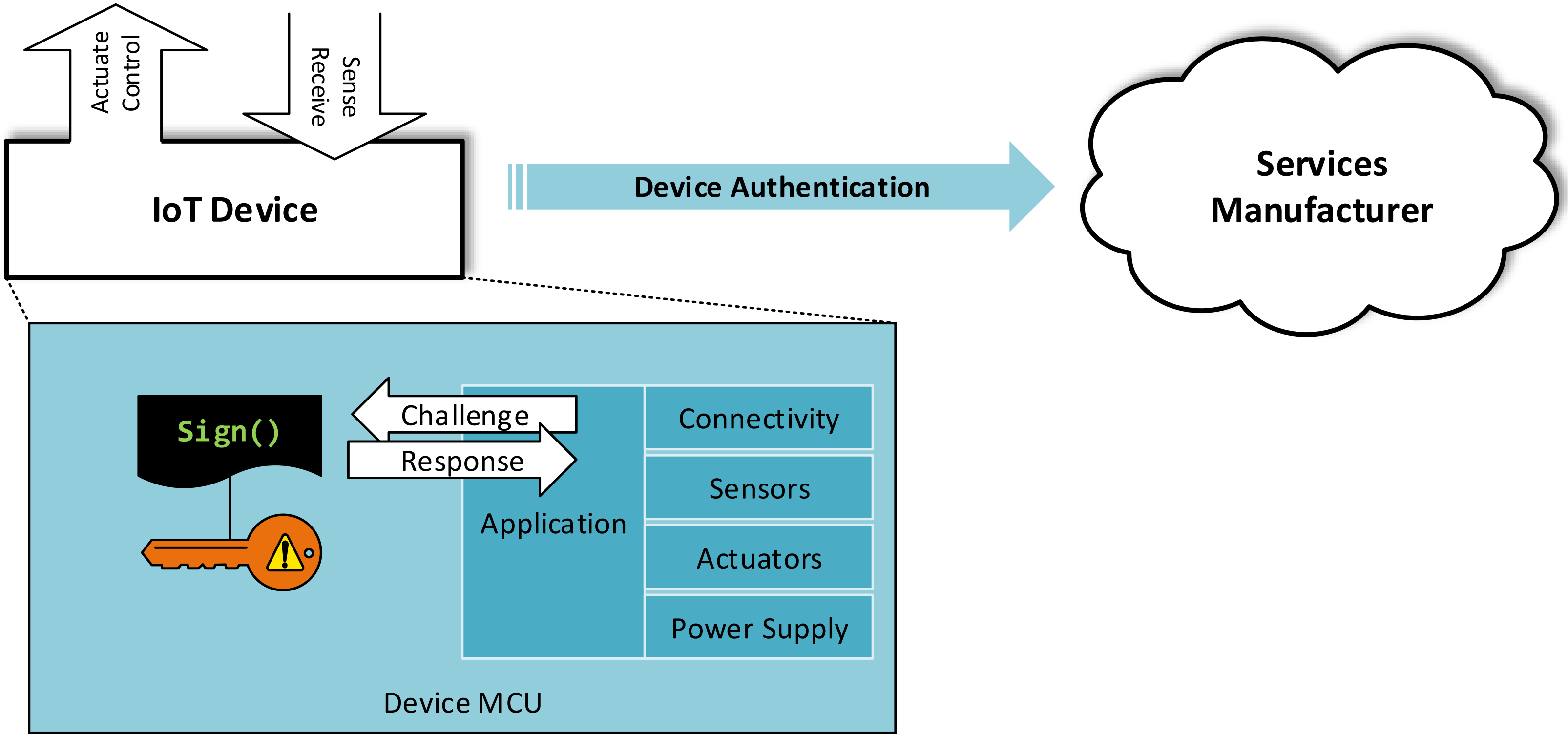
4 Getting started with hardware-security and Infineon products

5 Conclusion

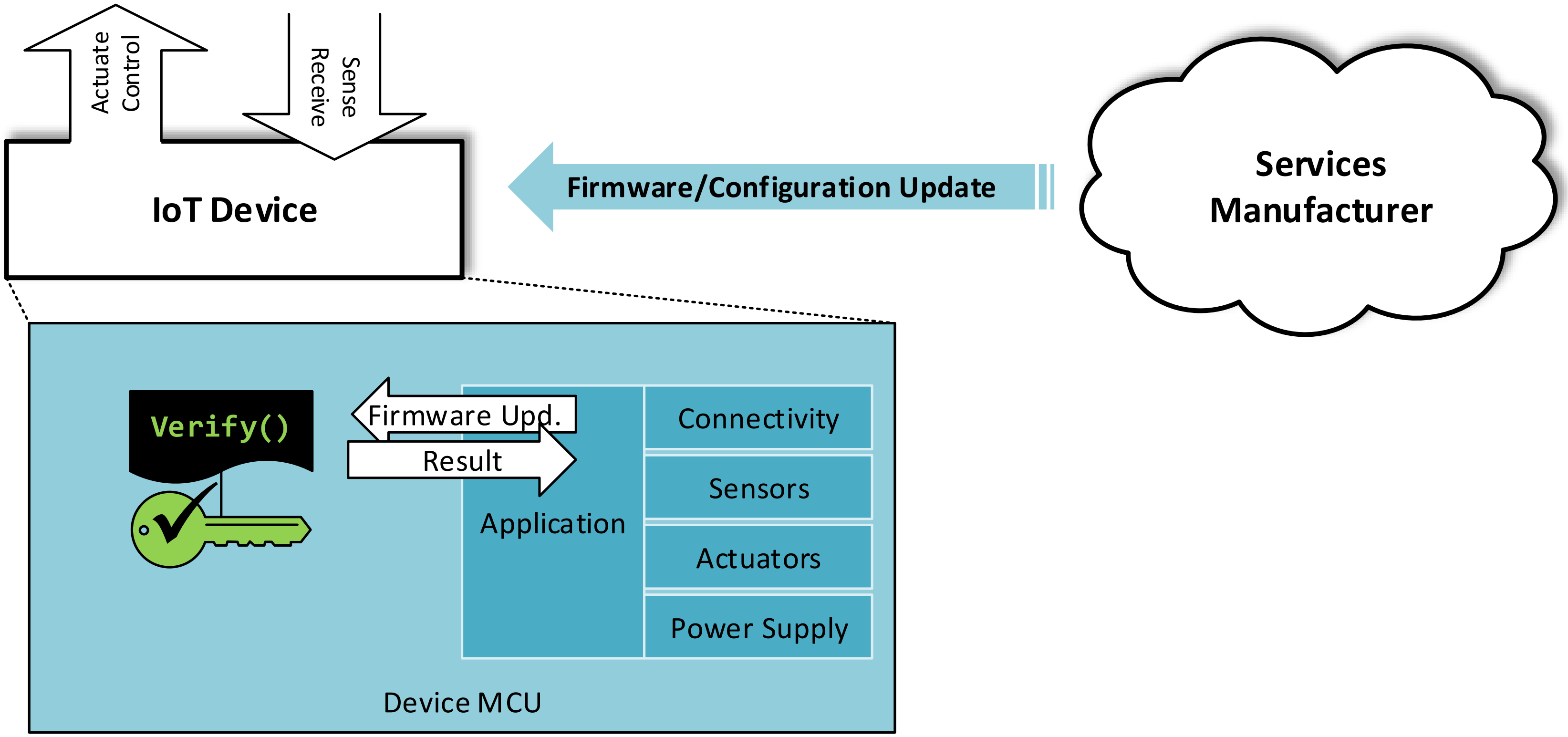
Authentication Example
“Minimum Viable IoT System”



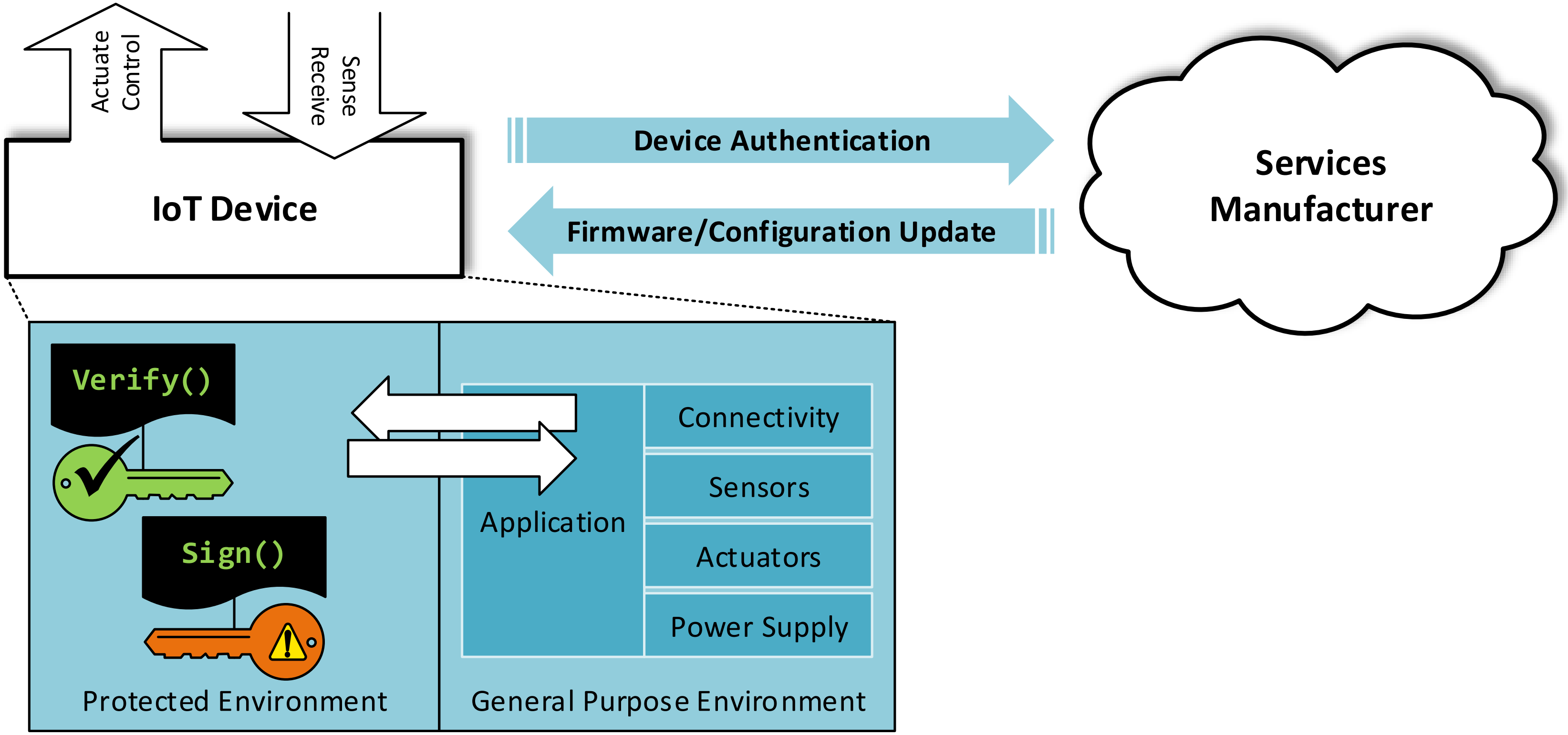
Authentication Example
Device to Cloud Authentication



Authentication Example
Device Firmware Update



Authentication Example
Device Firmware Update



Partitioning / Isolation

- “Secured world” and “normal world”

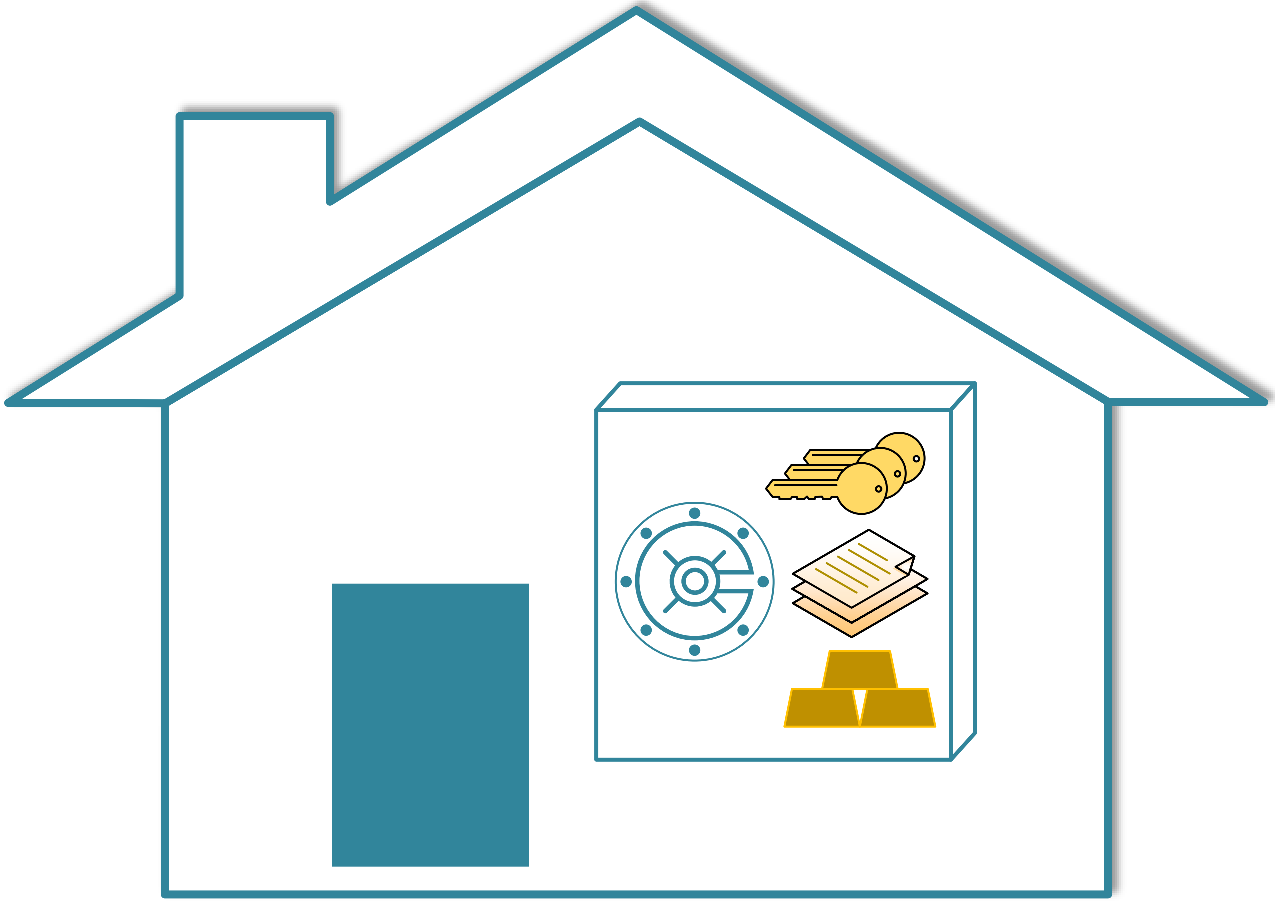
- **Software-based isolation**
  - (+)/(-)

- **Hardware-assisted isolation environments**
  - (+)/(-)

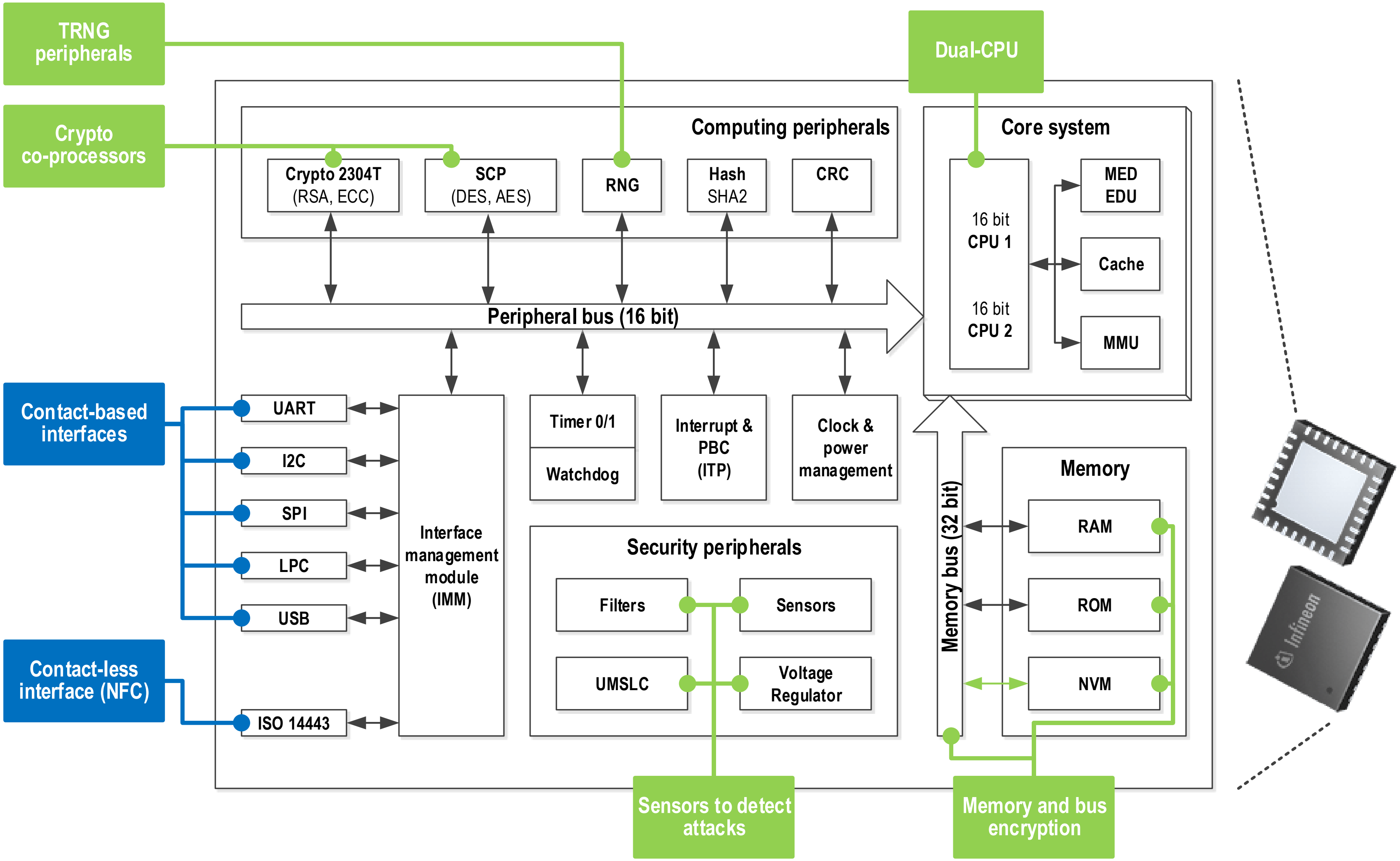
- **Discrete hardware-security / HSMs**
  - (+)/(-)

[Lesjak, C., Hein, D., & Winter, J. (2015, November). Hardware-security technologies for industrial IoT: TrustZone and security controller. In *Industrial Electronics Society, IECON 2015-41st Annual Conference of the IEEE* (pp. 002589-002595). IEEE.]

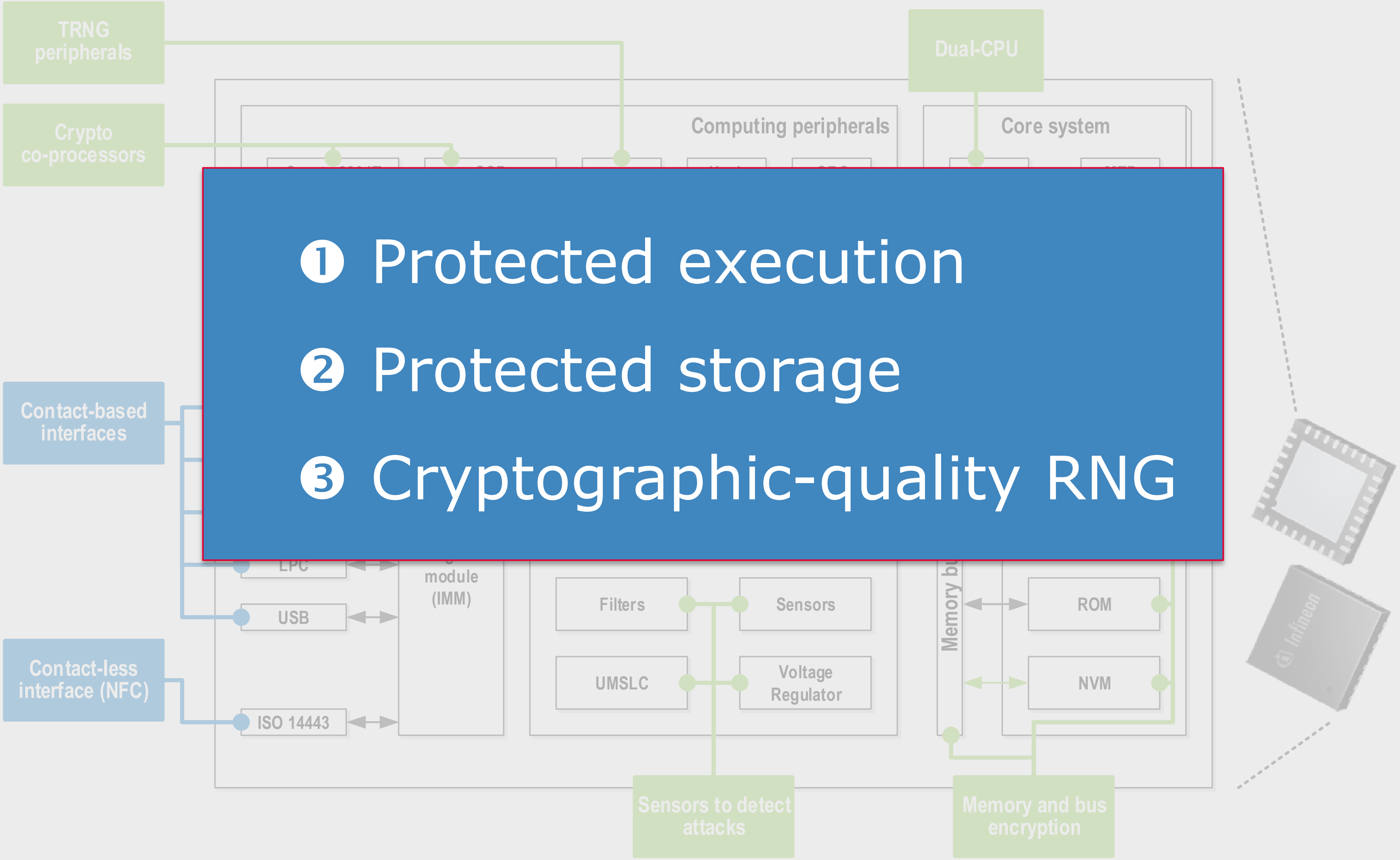
Analogy



Discrete Hardware Security: Hardware



Discrete Hardware Security: Hardware

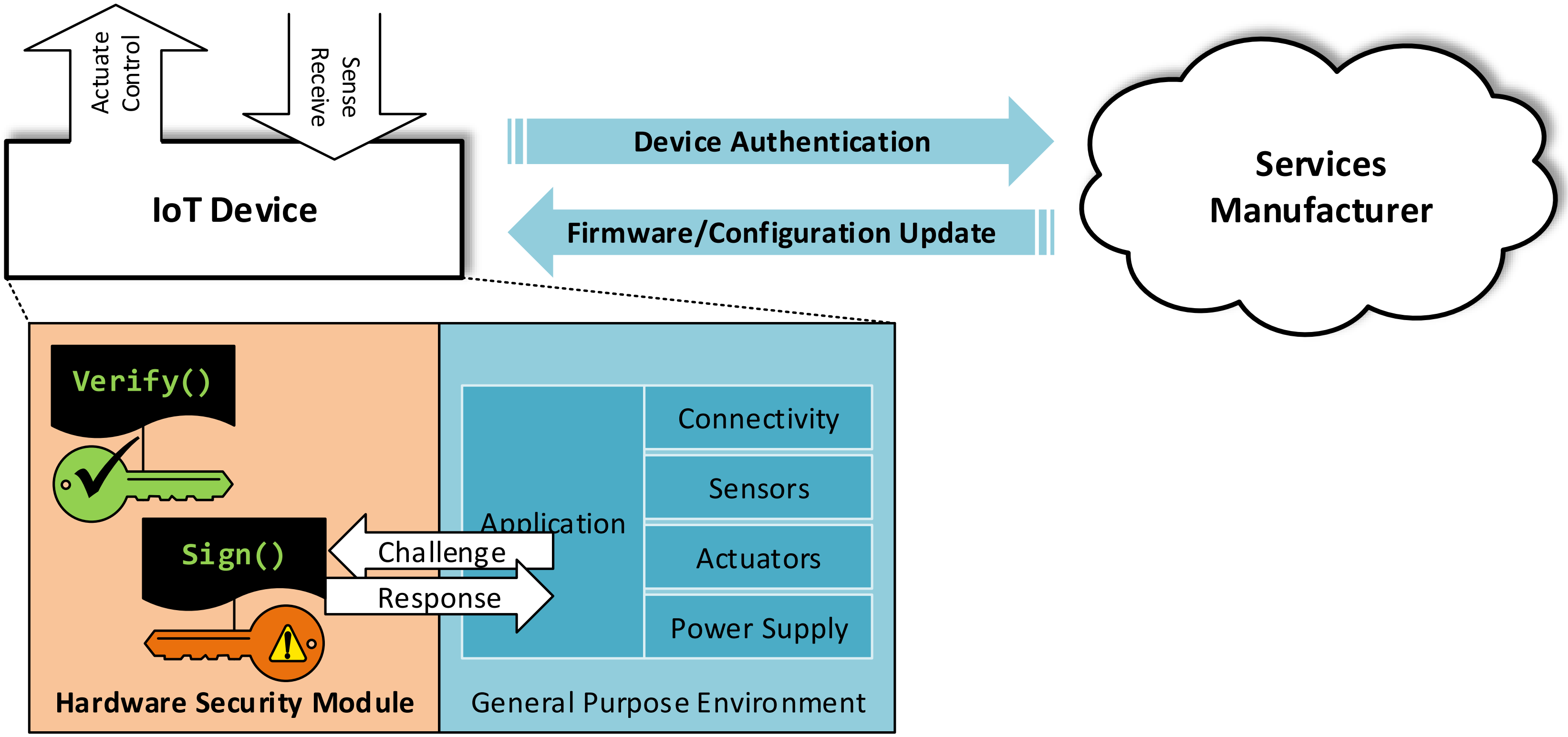


❶ Protected execution

❷ Protected storage

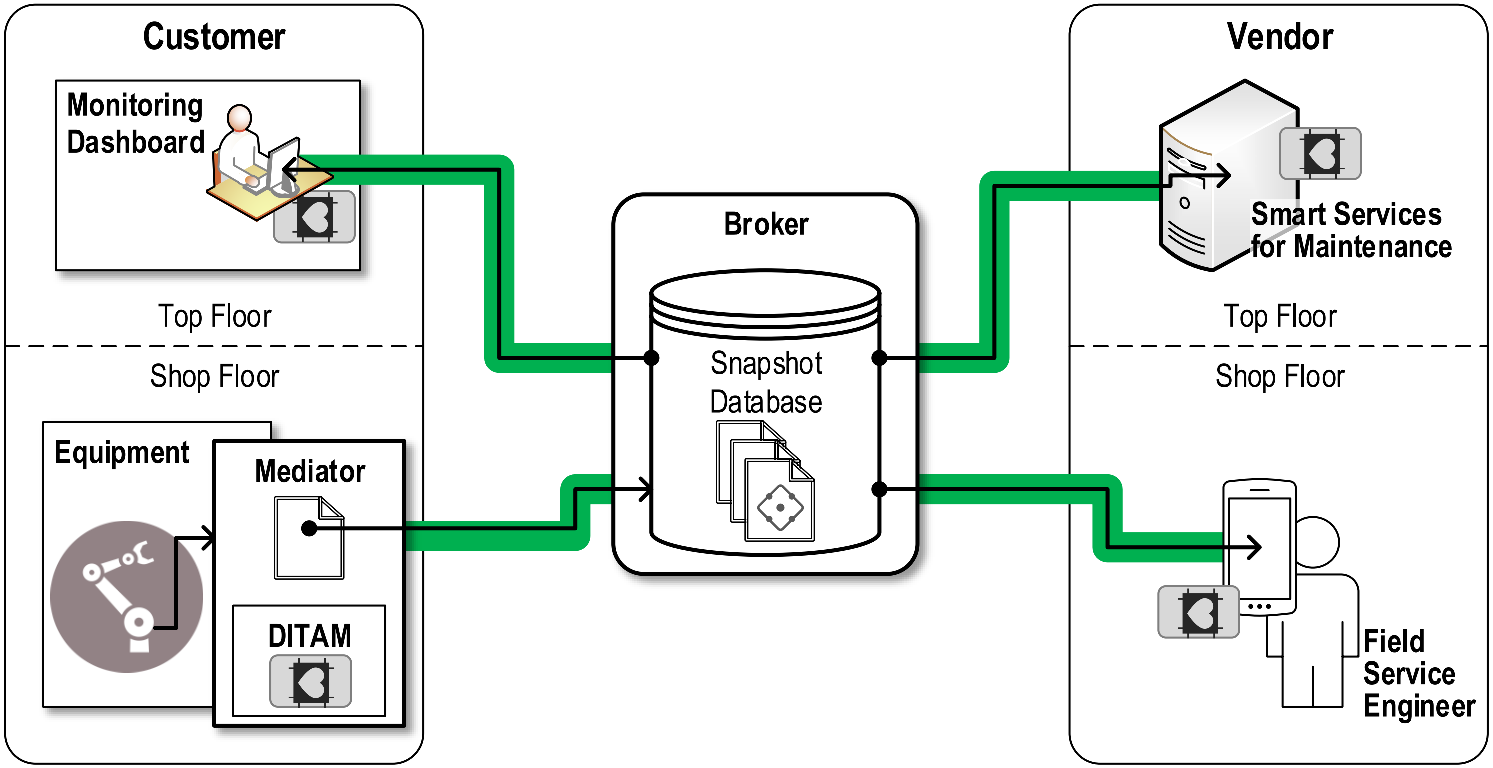
❸ Cryptographic-quality RNG

Hardware-Security Authentication Example



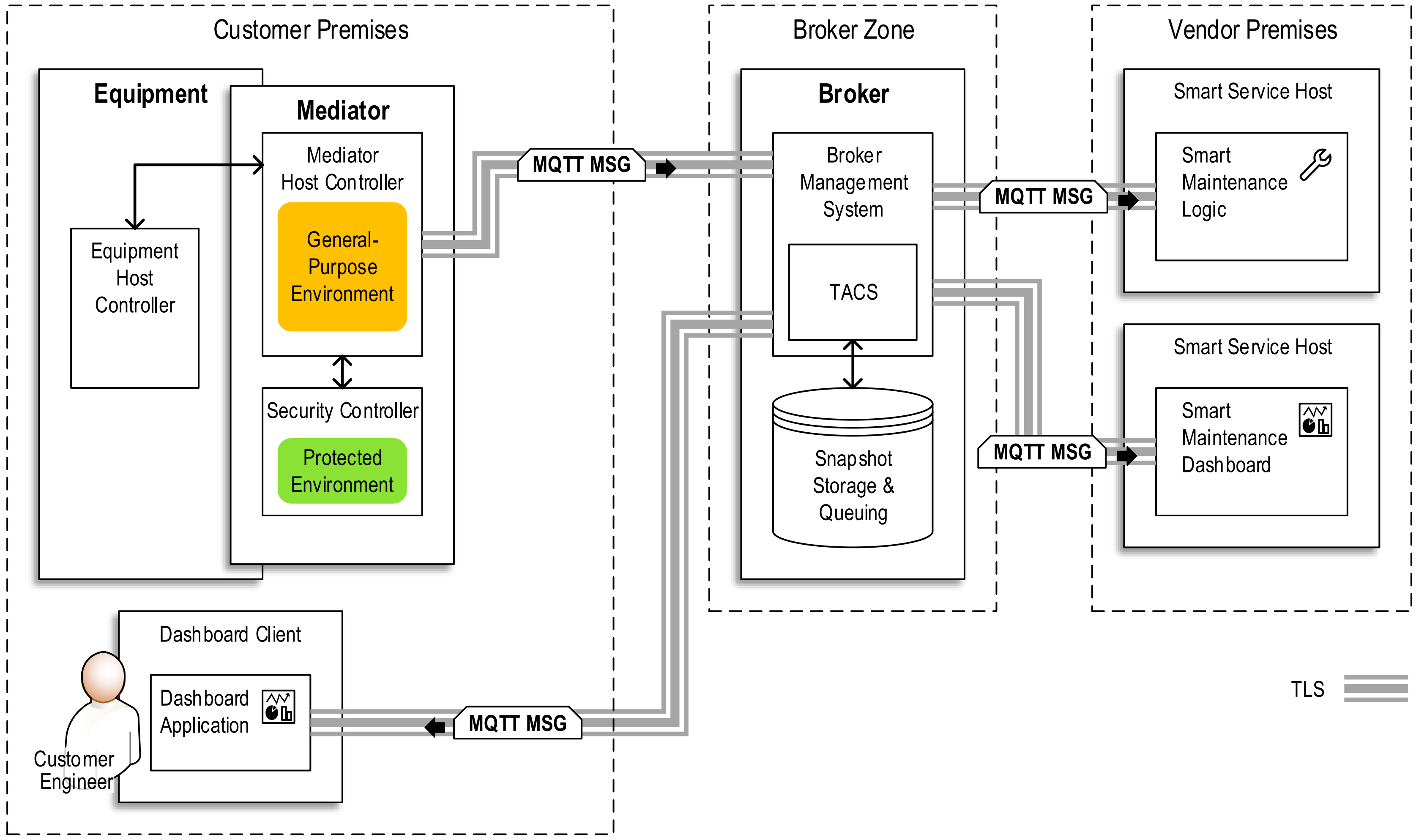
Hardware-Security
Secured Communication Example

- Smart Maintenance Services

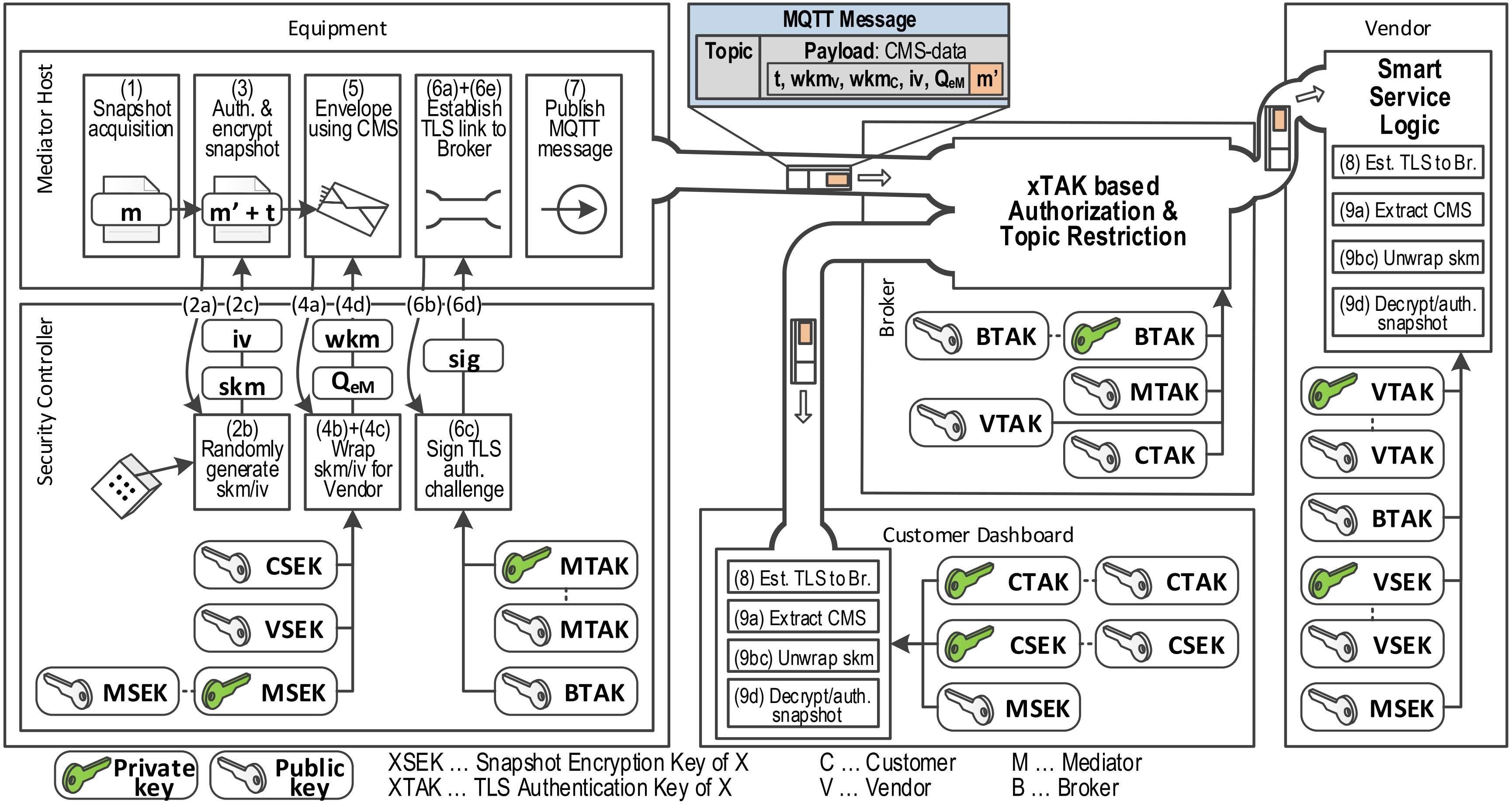


[Priller, P., Aldrian, A., & Ebner, T. (2014, September). Case study: From legacy to connectivity migrating industrial devices into the world of smart services. In *Emerging Technology and Factory Automation (ETFA), 2014 IEEE* (pp. 1-8). IEEE.]
[Lesjak, C., Druml, N., Matischek, R., Ruprechter, T., & Holweg, G. (2016). Security in industrial IoT–quo vadis?. *e & i Elektrotechnik und Informationstechnik*, *133*(7), 324-329.]

Hardware-Security
Secured Communication Example



Hardware-Security
Secured Communication Example



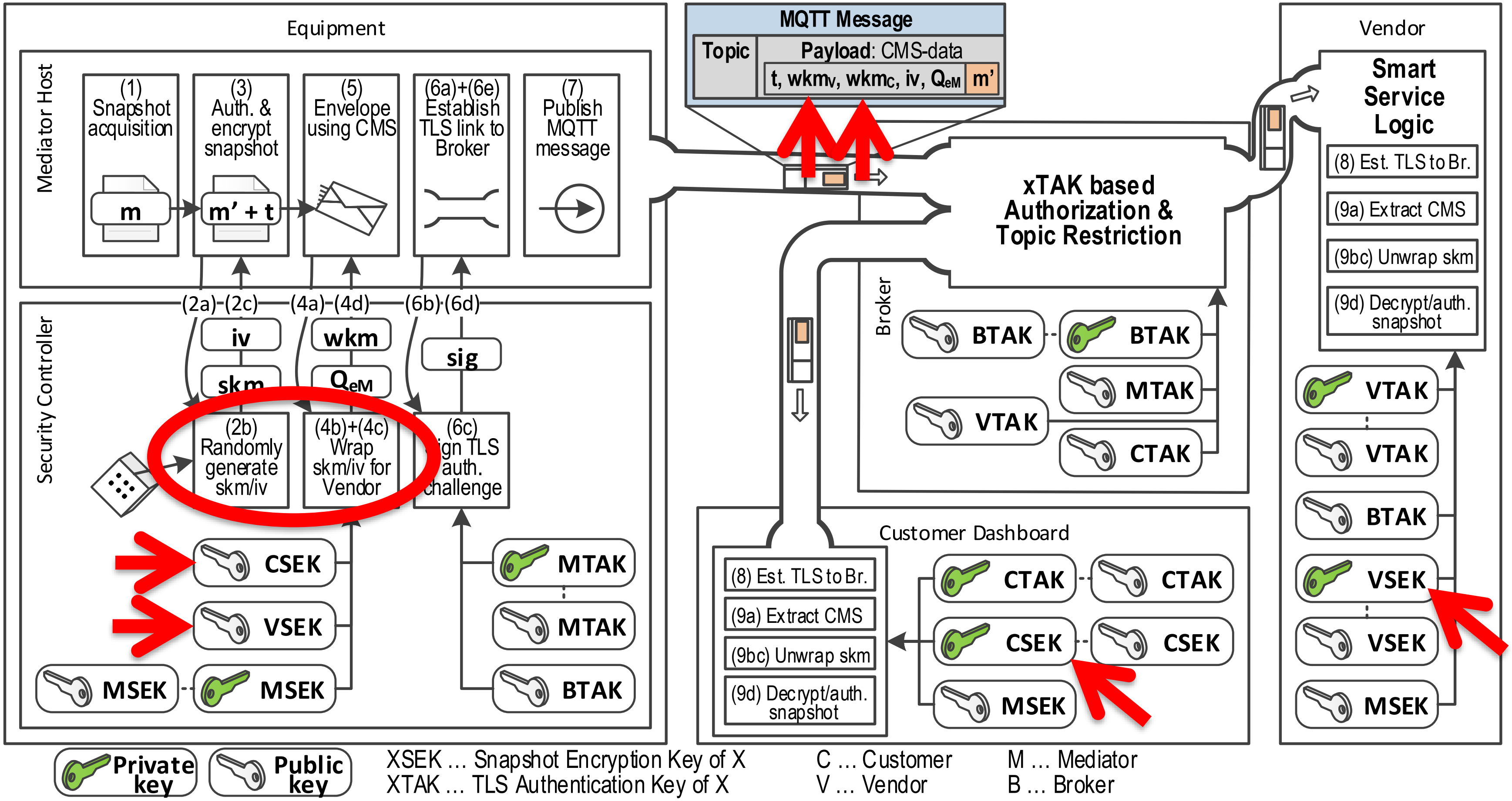
XSEK … Snapshot Encryption Key of X
XTAK … TLS Authentication Key of X

C … Customer
V … Vendor

M … Mediator
B … Broker

[Lesjak, C., Bock, H., Hein, D., & Maritsch, M. (2016, July). Hardware-secured and transparent multi-stakeholder data exchange for Industrial IoT. In *Industrial Informatics (INDIN), 2016 IEEE 14th International Conference on* (pp. 706-713). IEEE.]

Hardware-Security
Secured Communication Example

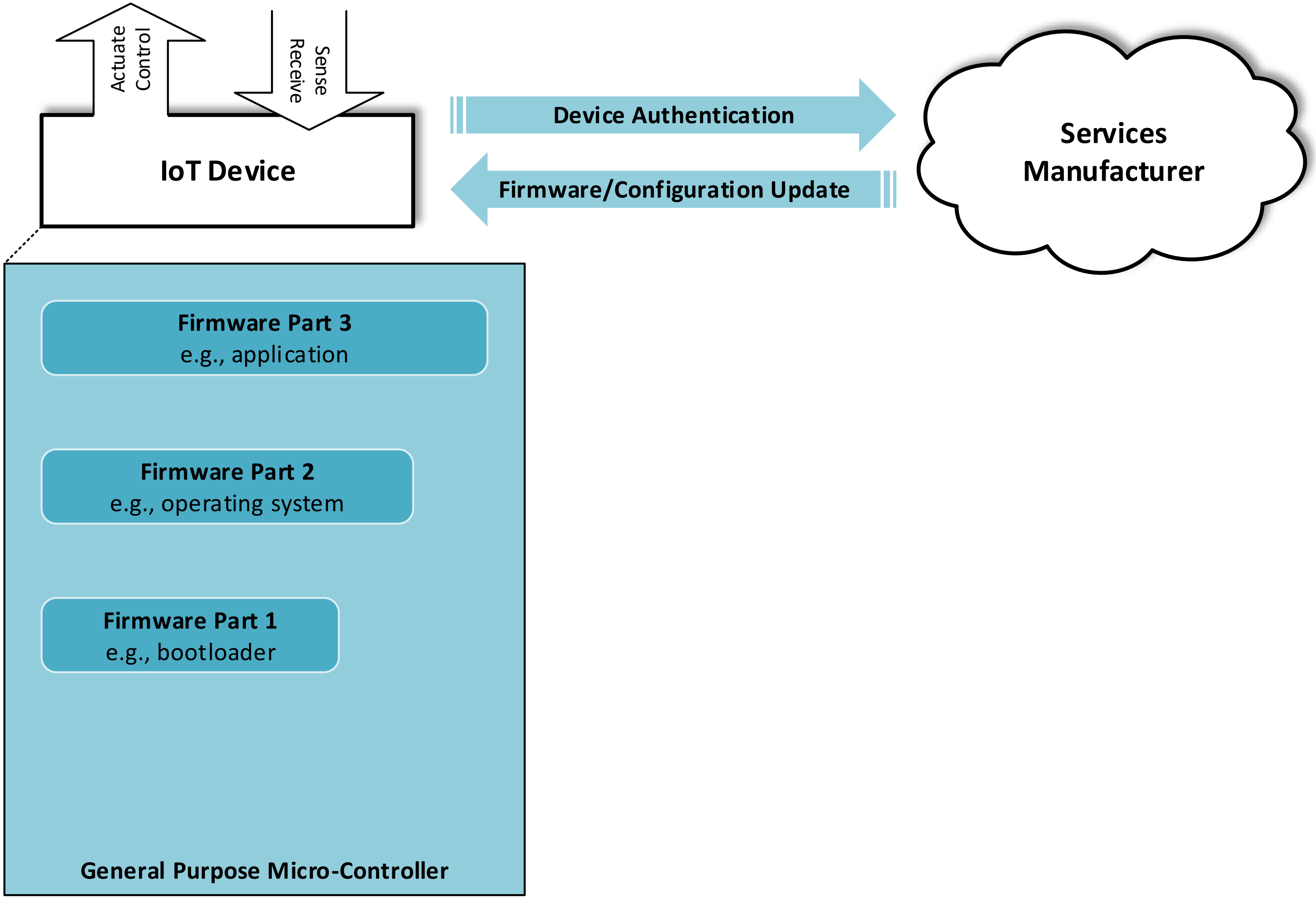


XSEK … Snapshot Encryption Key of X
XTAK … TLS Authentication Key of X

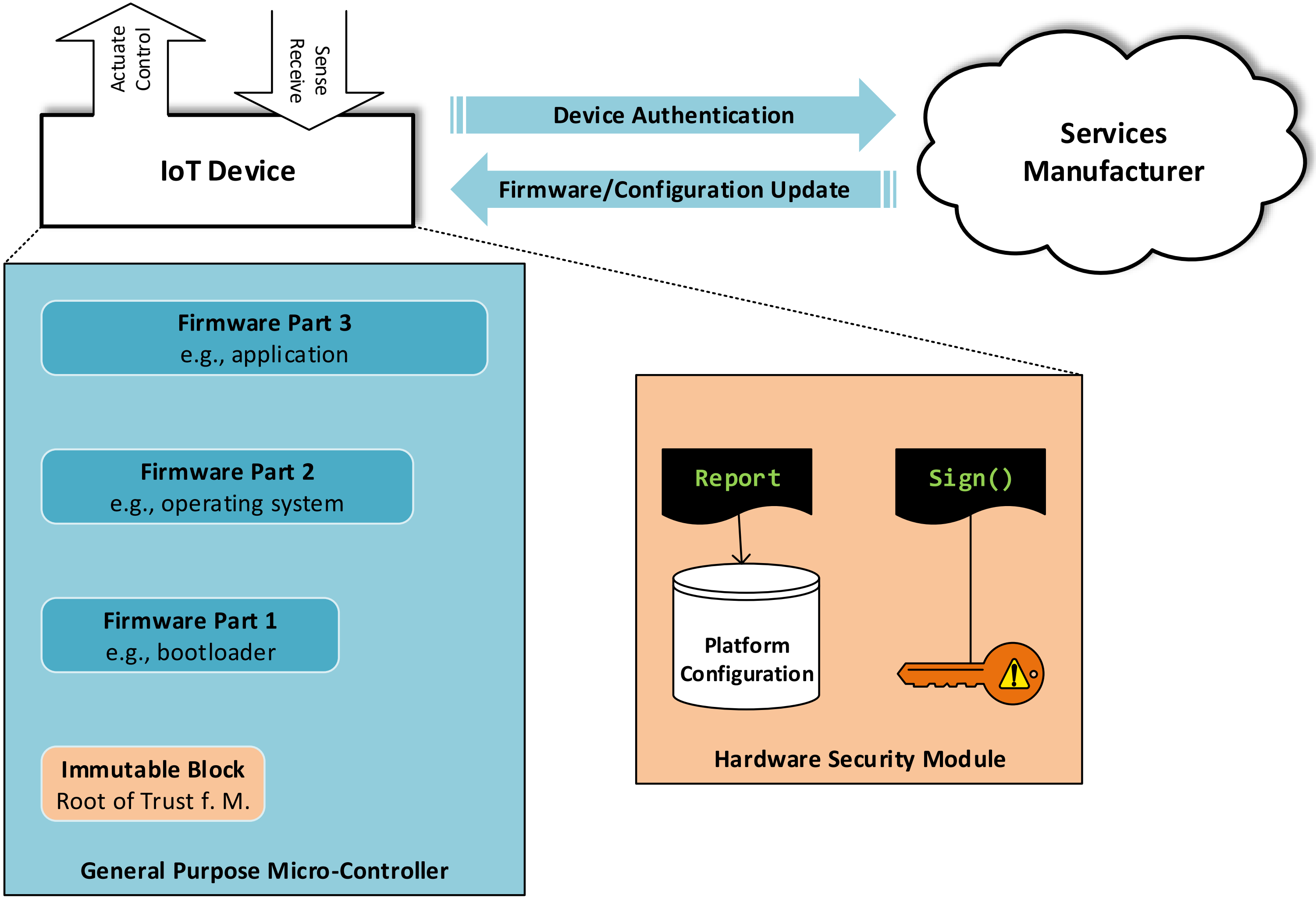
C … Customer
V … Vendor

M … Mediator
B … Broker

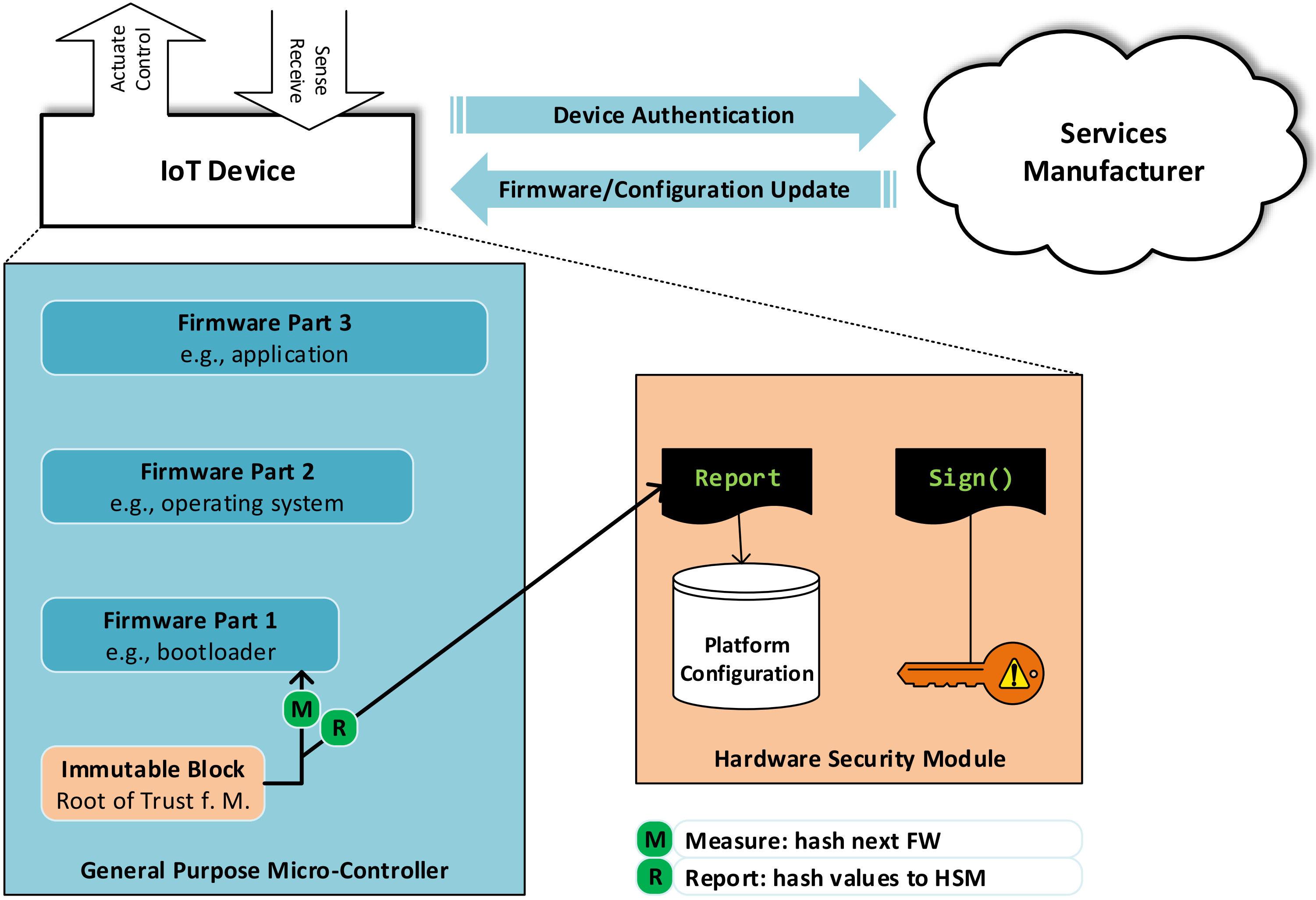
Hardware-Security
Platform Integrity Example



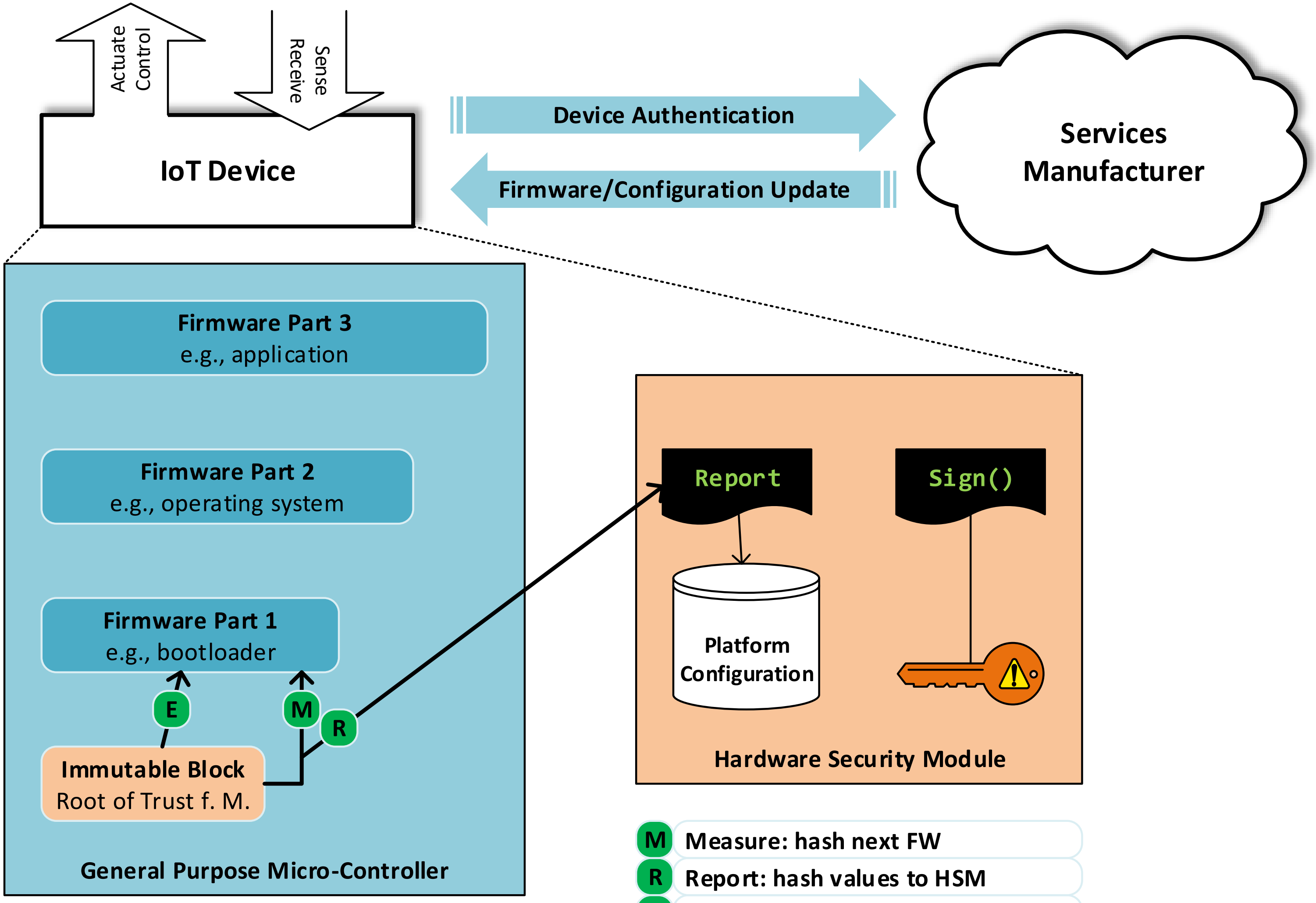
Hardware-Security
Platform Integrity Example



Hardware-Security
Platform Integrity Example



Hardware-Security
Platform Integrity Example

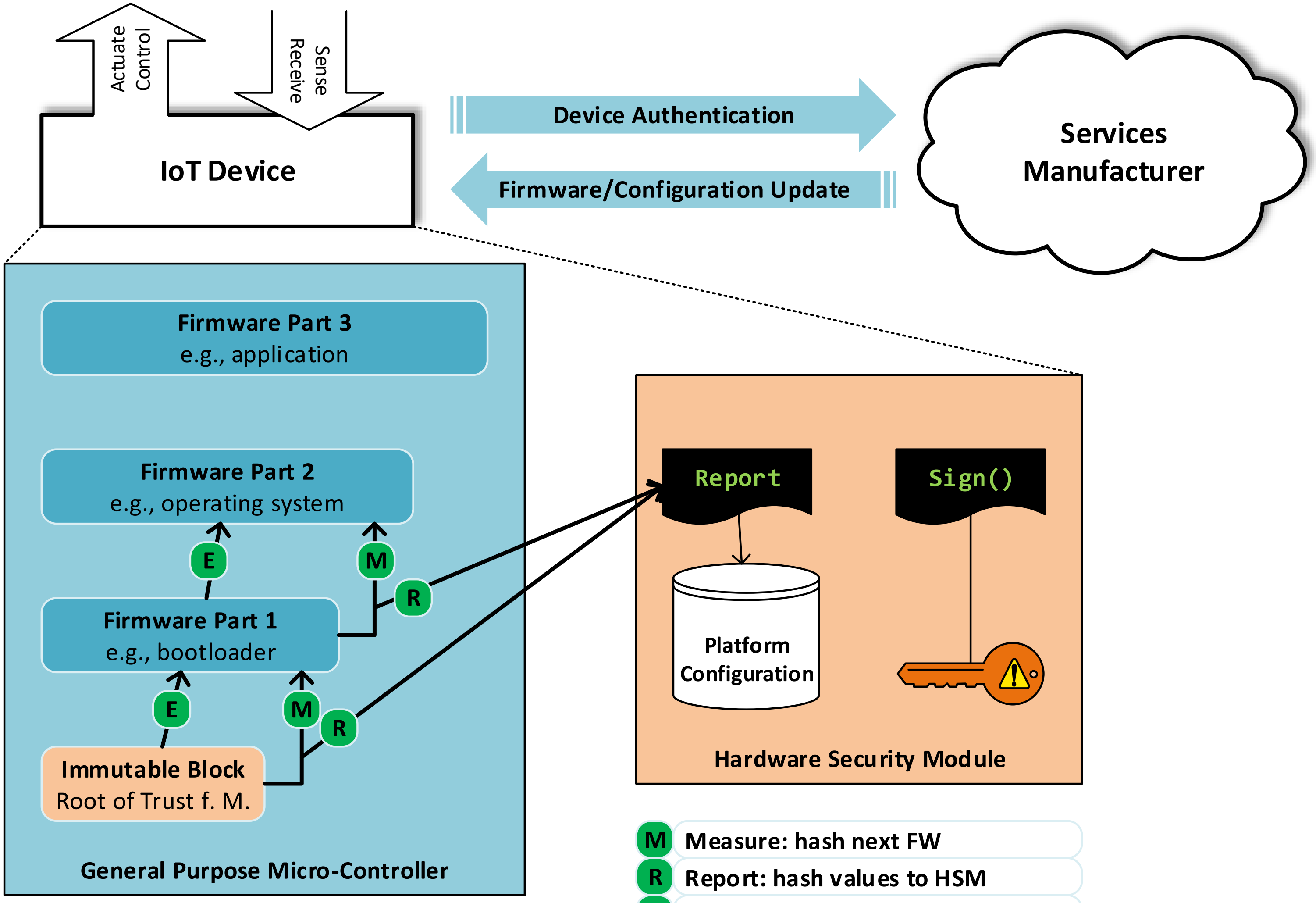


M Measure: hash next FW

R Report: hash values to HSM

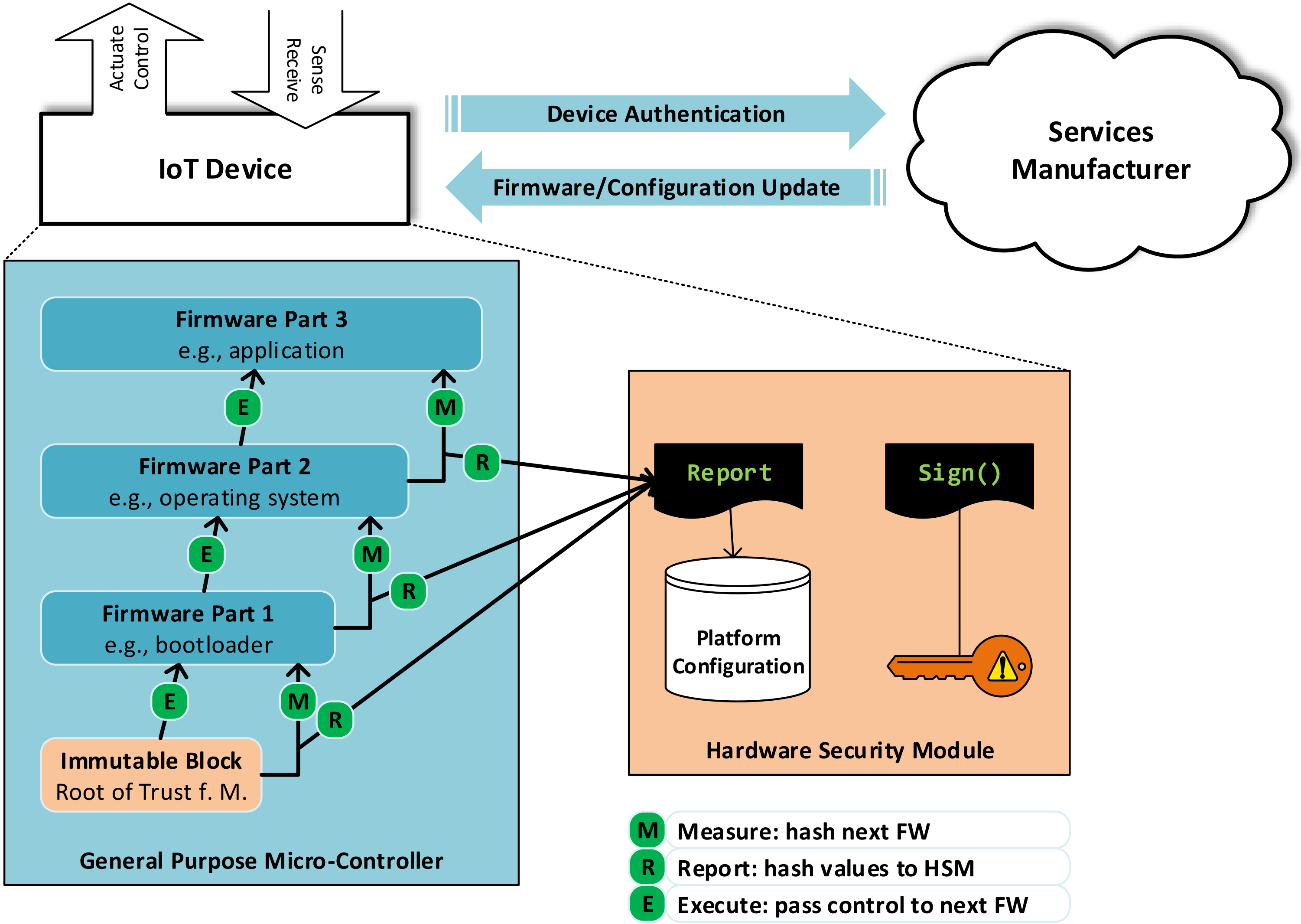
E Execute: pass control to next FW

Hardware-Security
Platform Integrity Example

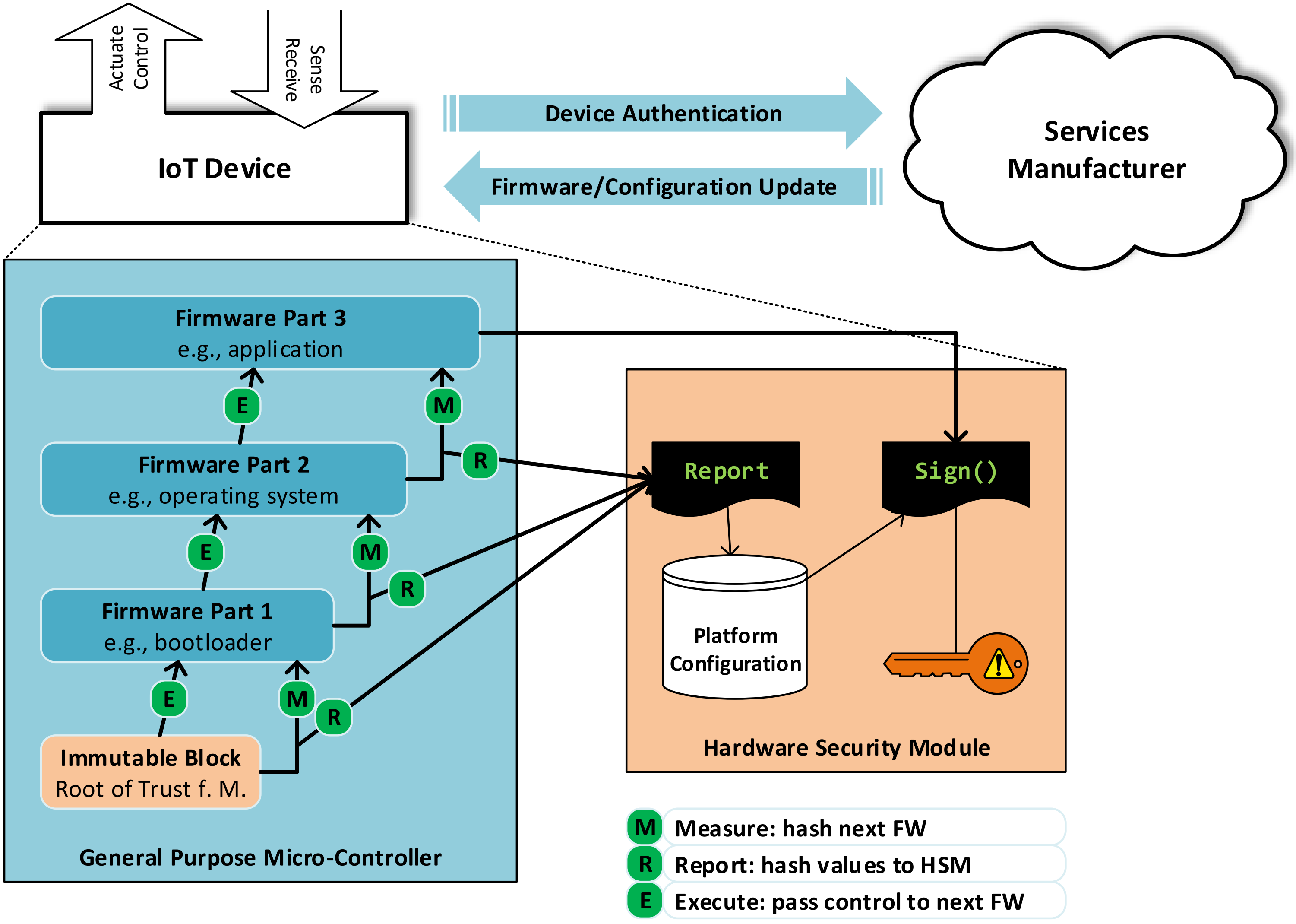


M	Measure: hash next FW
R	Report: hash values to HSM
E	Execute: pass control to next FW

Hardware-Security
Platform Integrity Example



Hardware-Security
Platform Integrity Example



- M Measure: hash next FW
- R Report: hash values to HSM
- E Execute: pass control to next FW

Agenda

1 Motivation

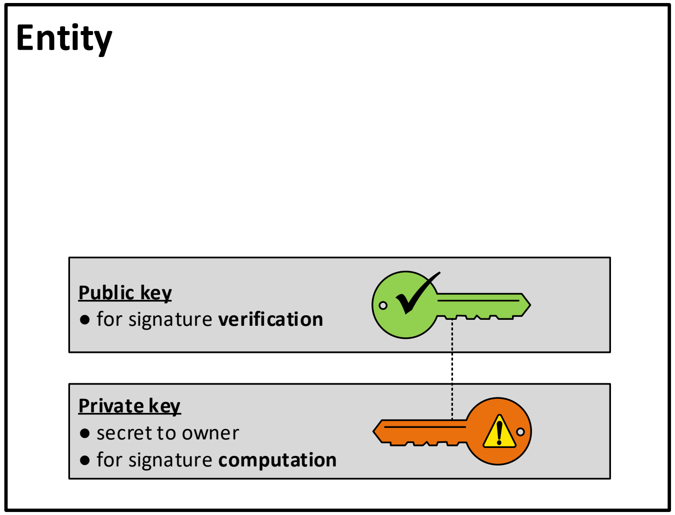
2 Hardware-based security – what is it?

3 Cloud system architecture with hardware-based security

4 Getting started with hardware-security and Infineon products

5 Conclusion

Background
Public Key Infrastructure (PKI) /1



Entity

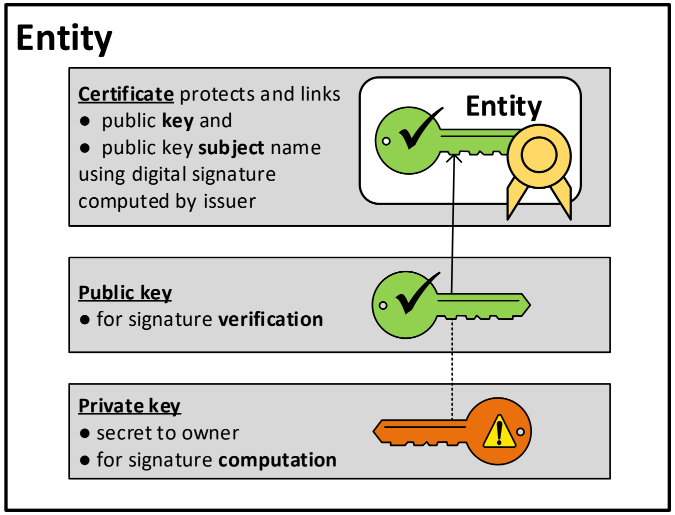
Public key

- for signature **verification**

Private key

- secret to owner
- for signature **computation**

Background
Public Key Infrastructure (PKI) /2



Entity

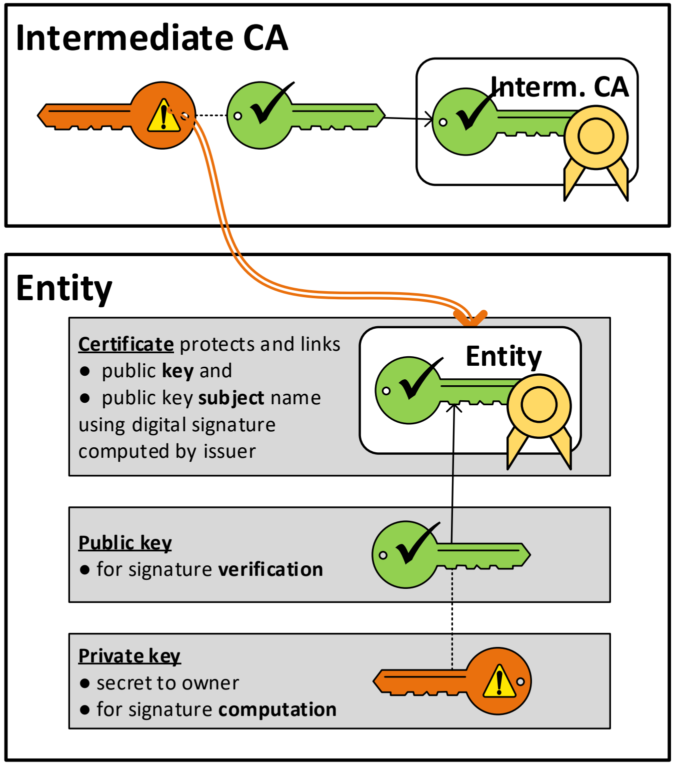
Certificate protects and links
- public **key** and
- public key **subject** name

using digital signature computed by issuer

Public key
- for signature **verification**

Private key
- secret to owner
- for signature **computation**

Background
Public Key Infrastructure (PKI) /3



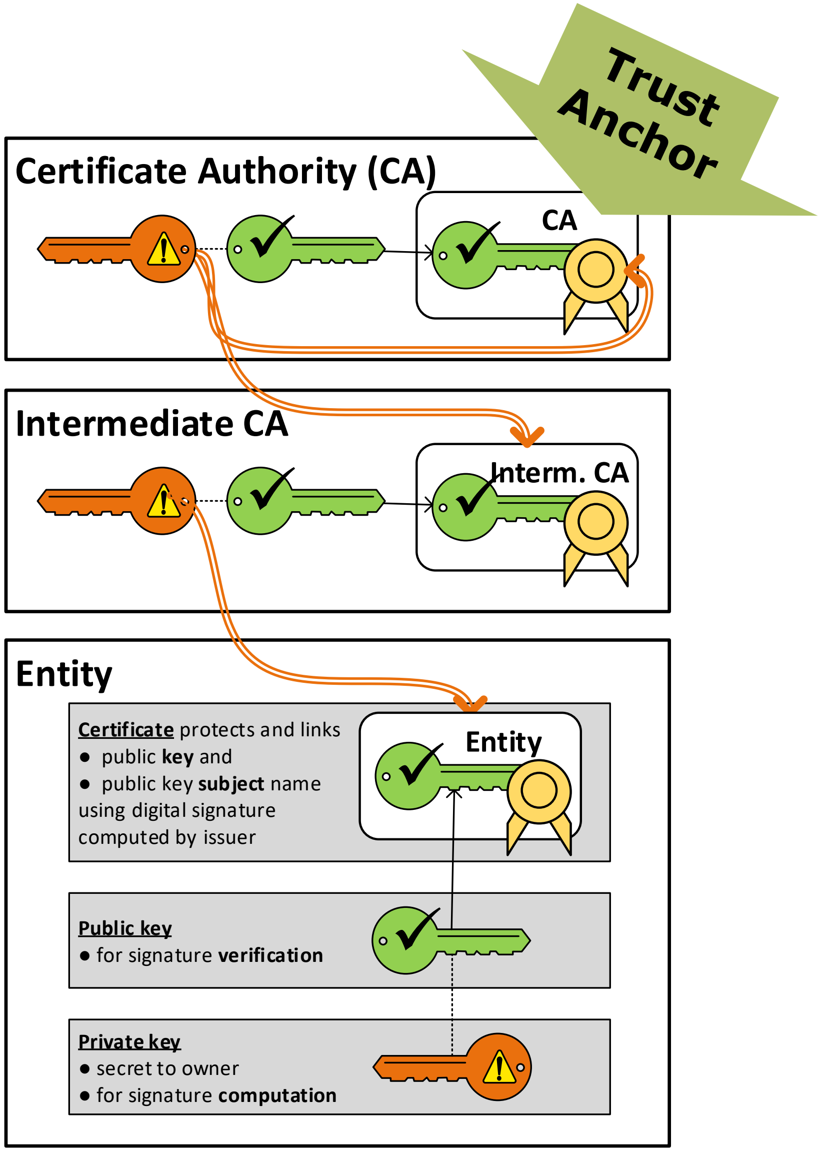
Certificate protects and links
- public **key** and
- public key **subject** name

using digital signature computed by issuer

Public key
- for signature **verification**

Private key
- secret to owner
- for signature **computation**

Background
Public Key Infrastructure (PKI) /4



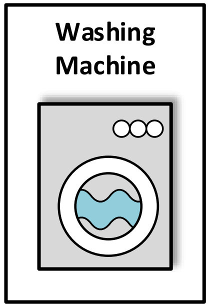
Certificate protects and links
- public **key** and
- public key **subject** name

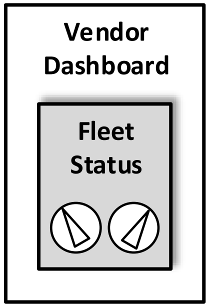
using digital signature computed by issuer

Public key
- for signature **verification**

Private key
- secret to owner
- for signature **computation**

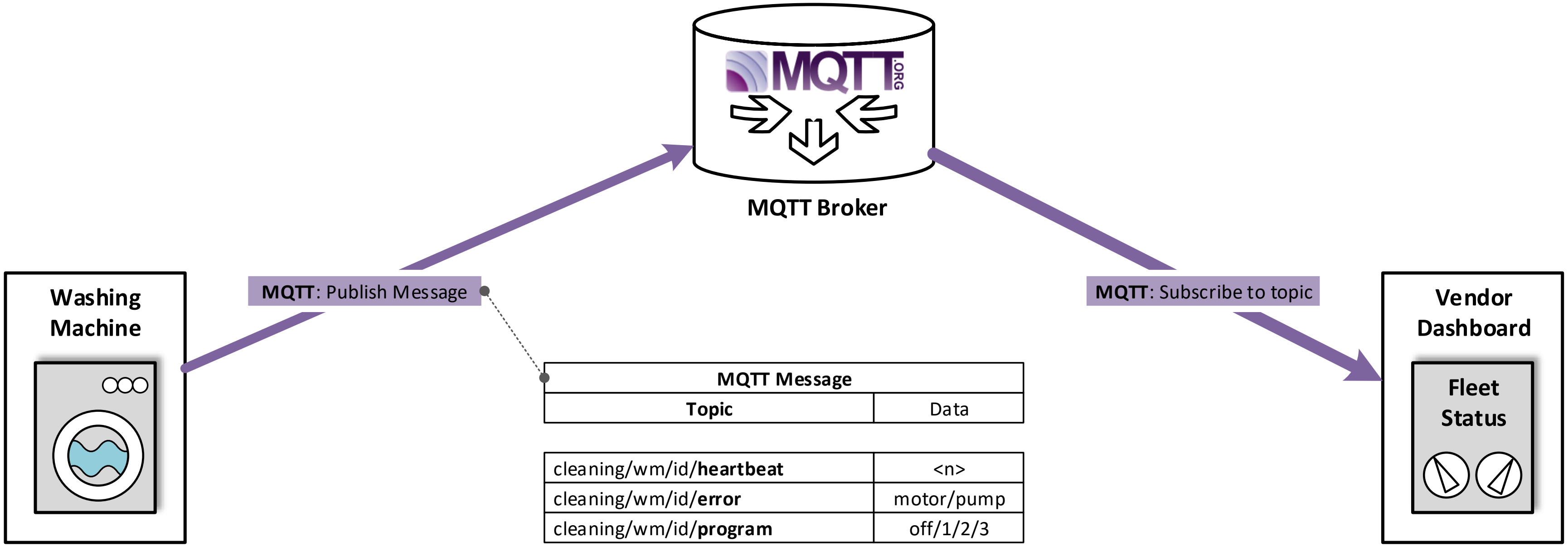
Cloud service integration – AWS IoT /1: **Business model**


Washing Machine


Vendor Dashboard

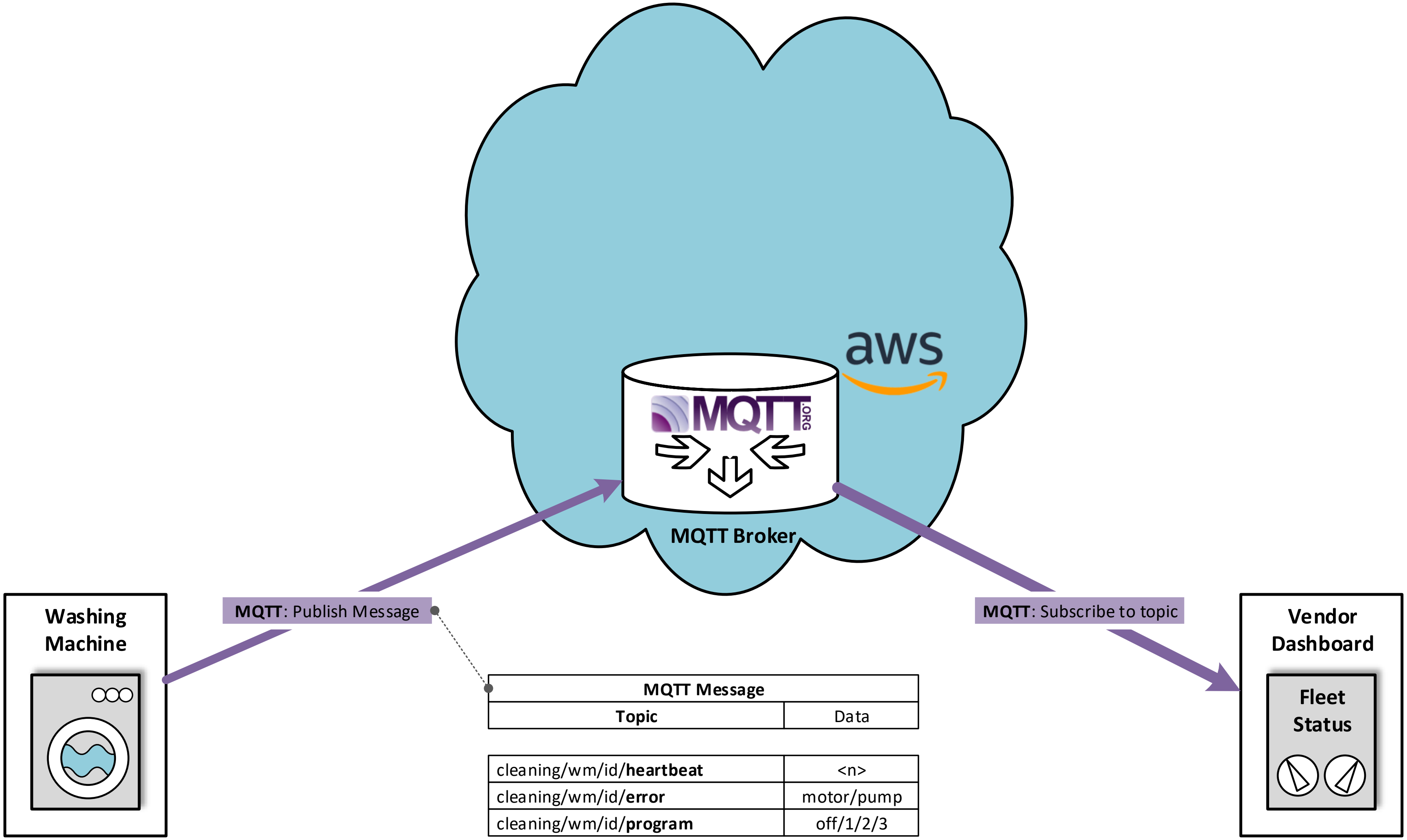
Fleet Status

Cloud service integration – AWS IoT /2: **MQTT**: Message Queue Telemetry Transport



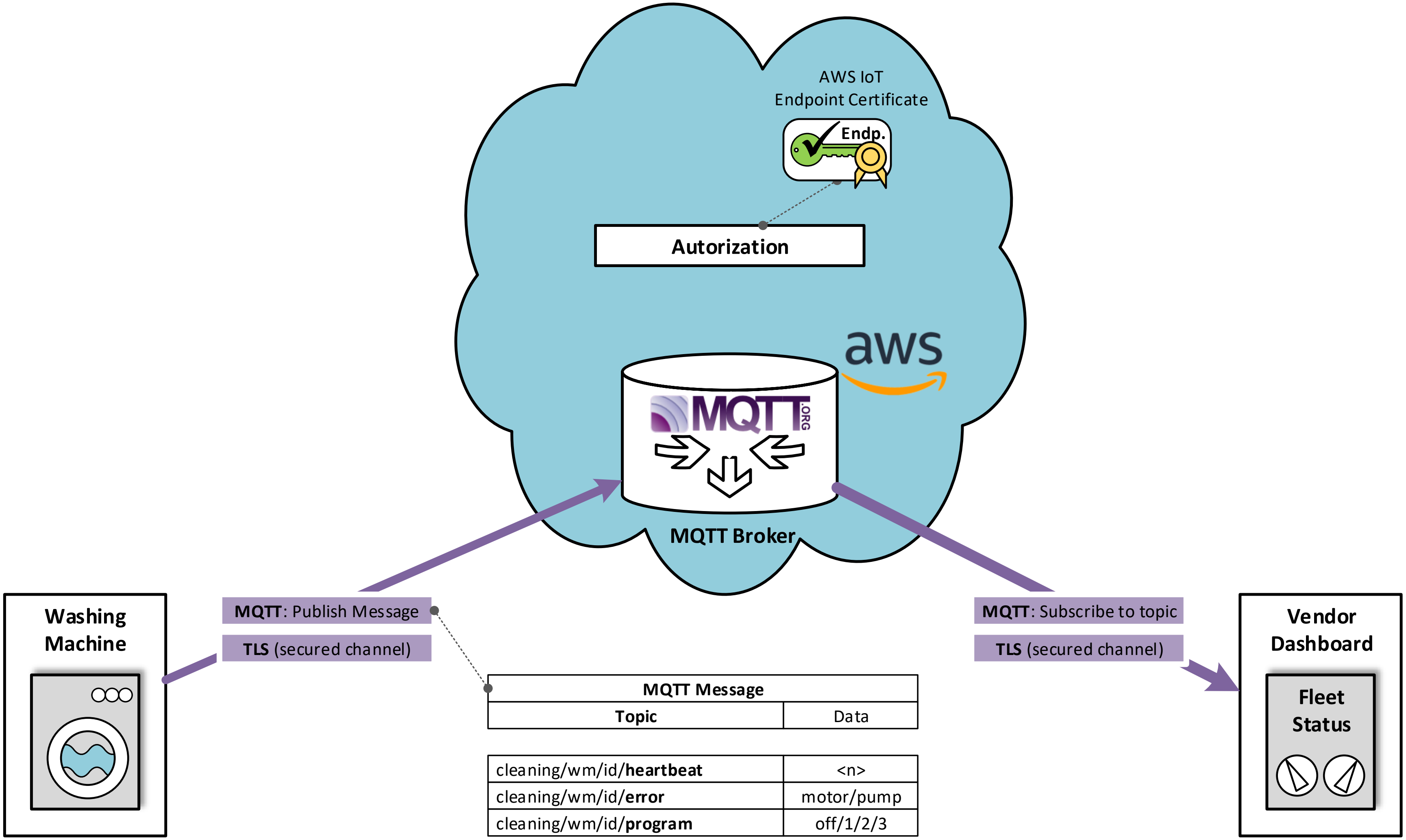
MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /3: **AWS IoT** = hosted MQTT broker in AWS cloud



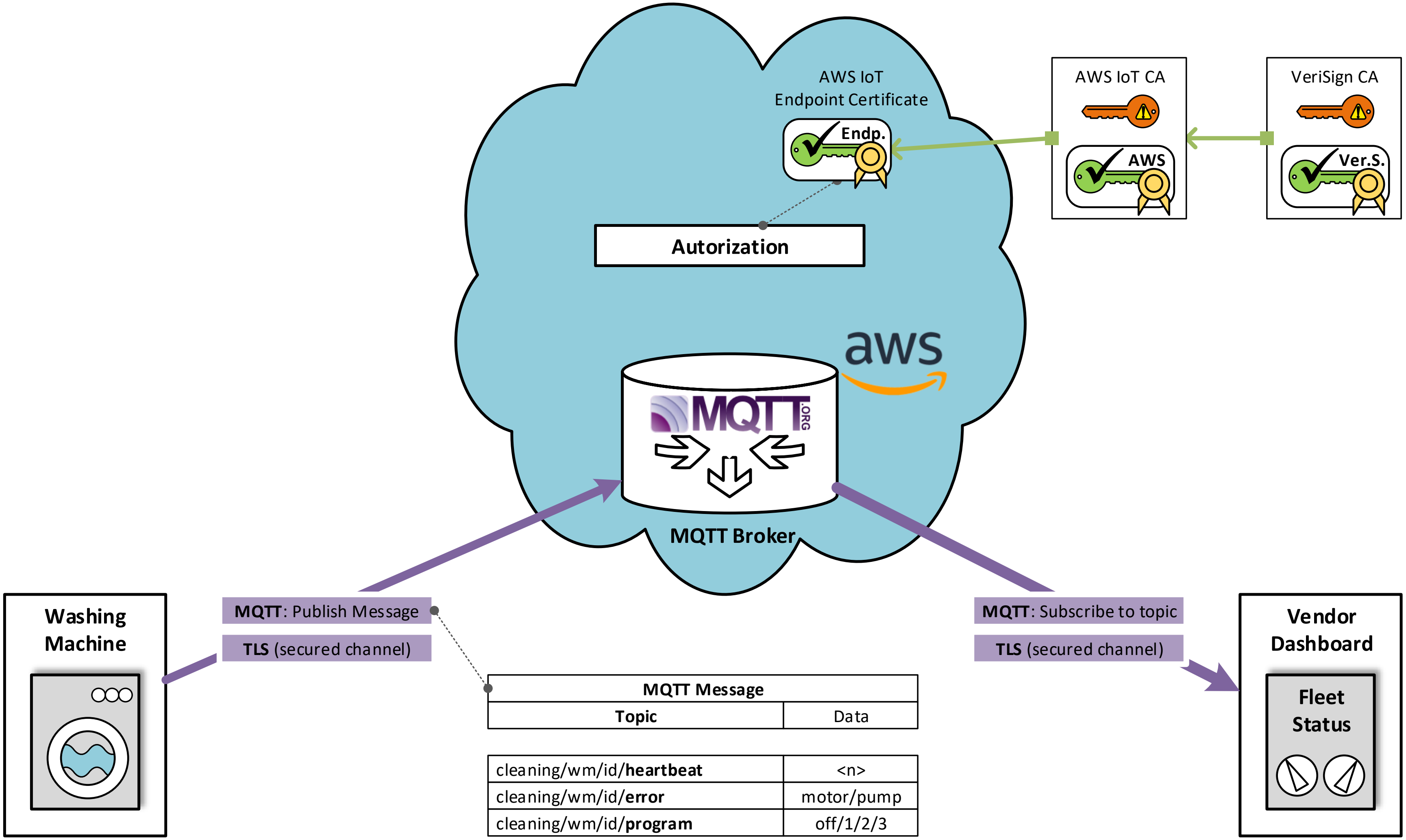
MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /4a: **Security**: TLS with server authentication



MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /4b: **Security**: TLS with server authentication



AWS IoT
Endpoint Certificate

AWS IoT CA

VeriSign CA

Autorization

MQTT Broker

Washing Machine

MQTT: Publish Message

TLS (secured channel)

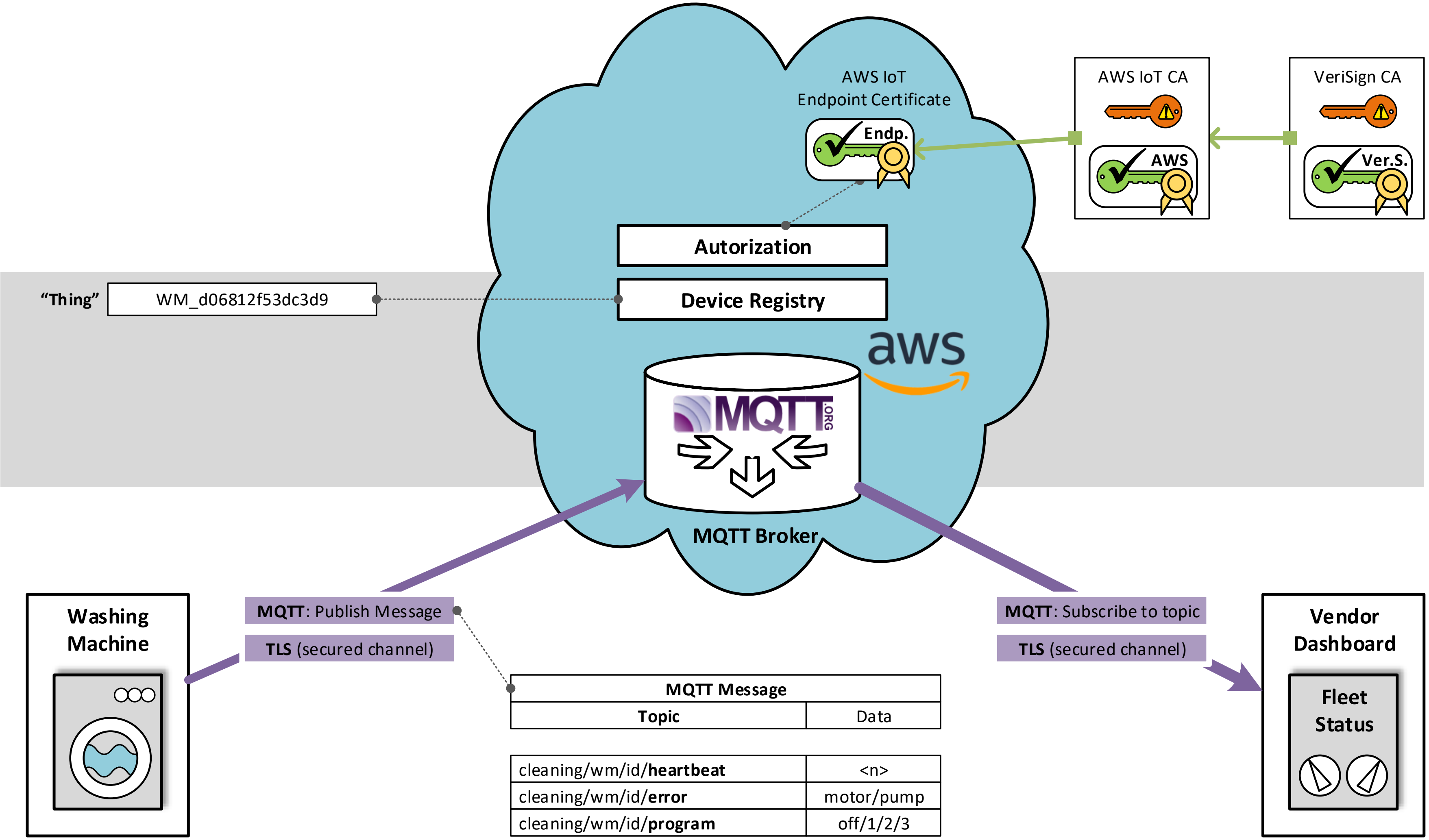
MQTT: Subscribe to topic

TLS (secured channel)

Vendor Dashboard

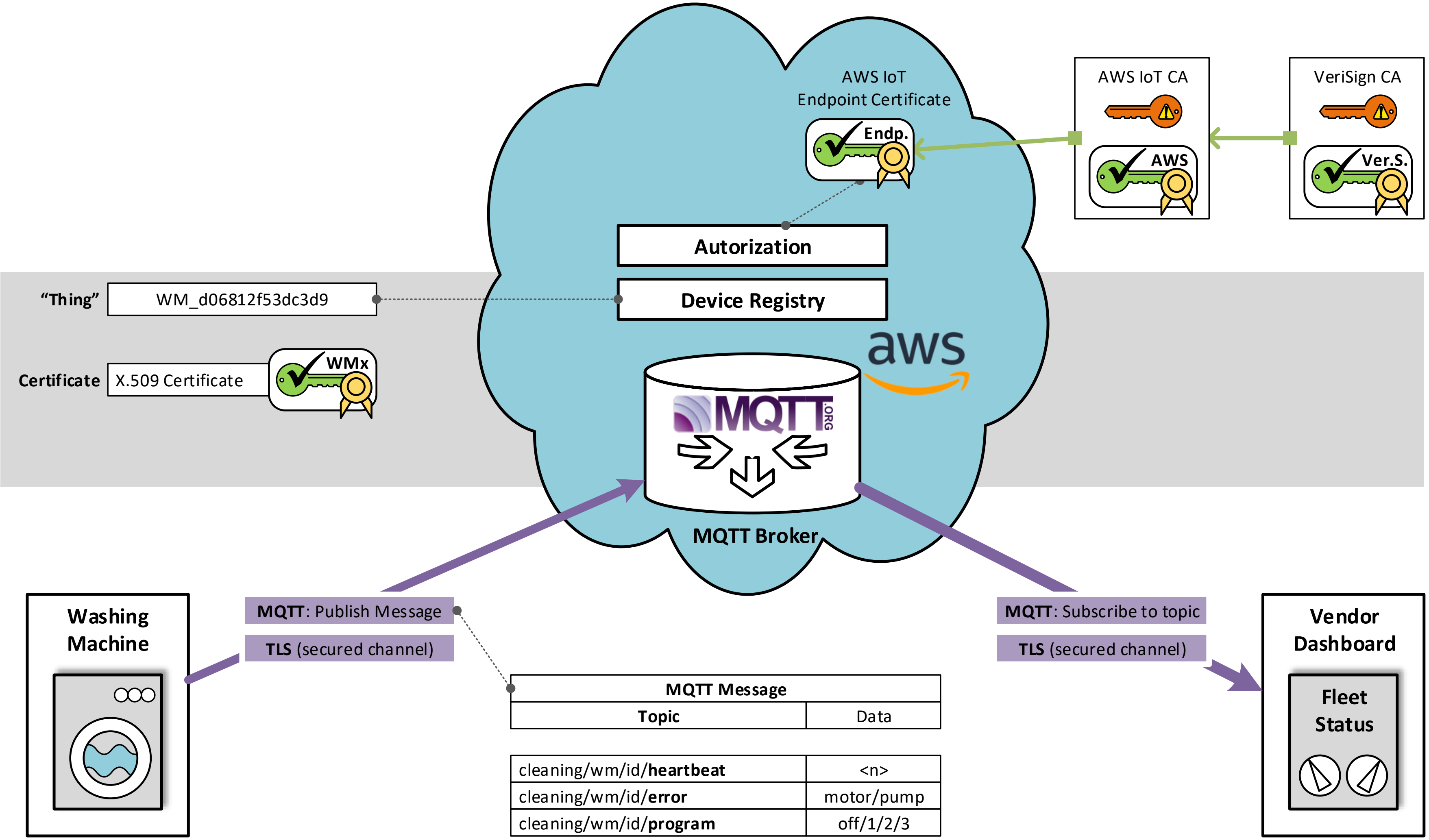
MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /5a: **Registering** Thing with private PKI



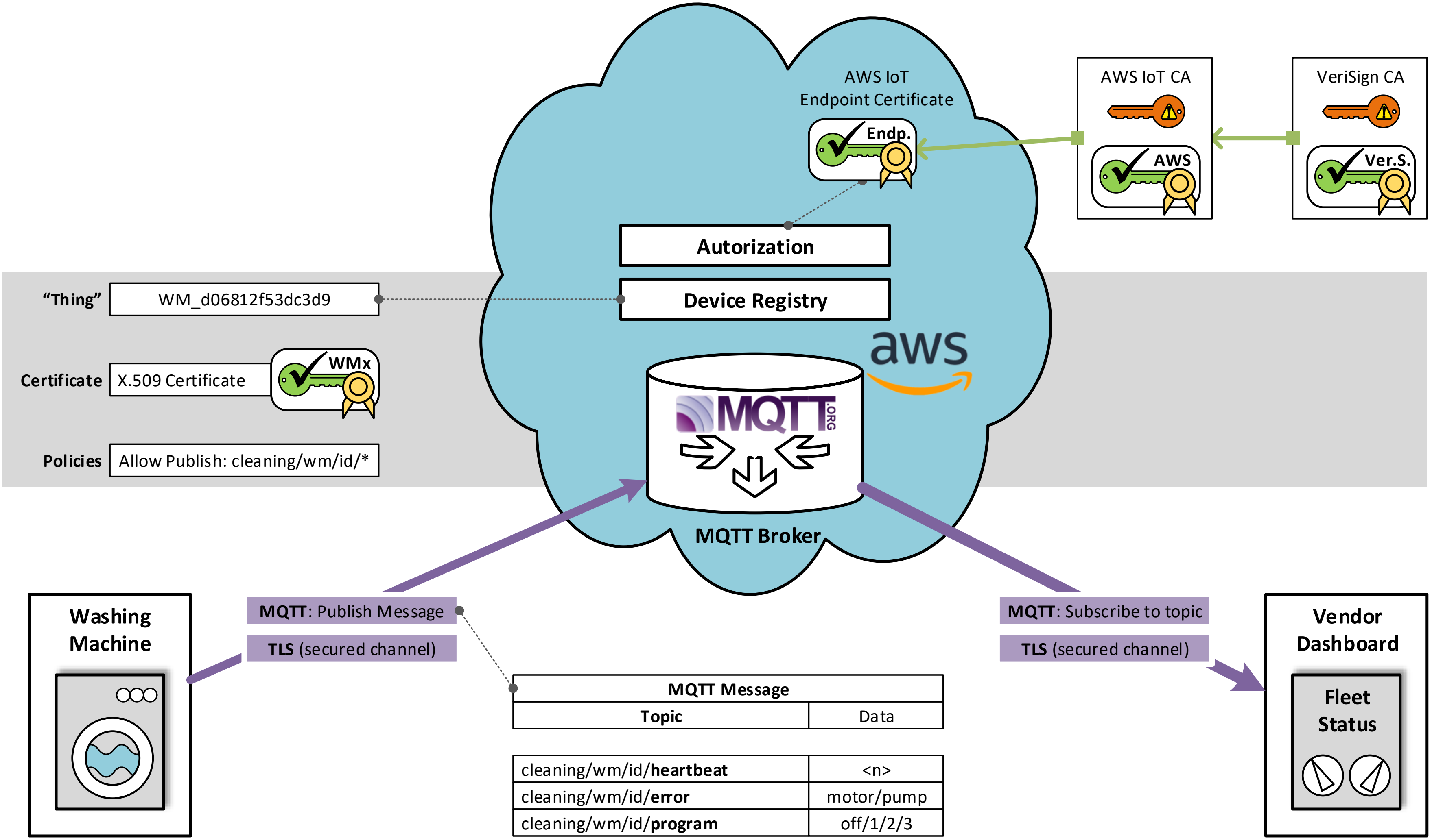
MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /5b: **Registering** Thing with private PKI



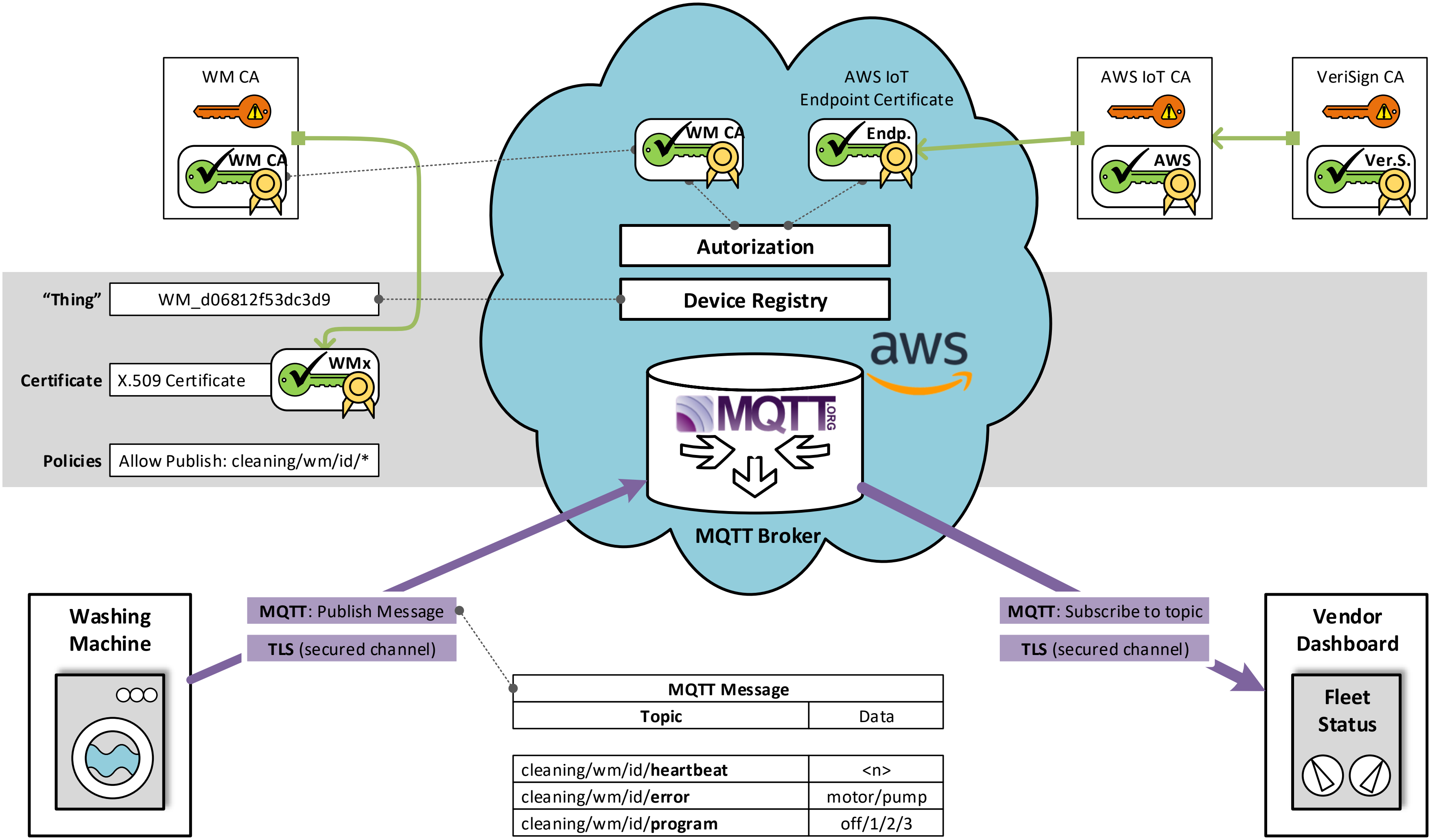
MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /5c: **Registering** Thing with private PKI



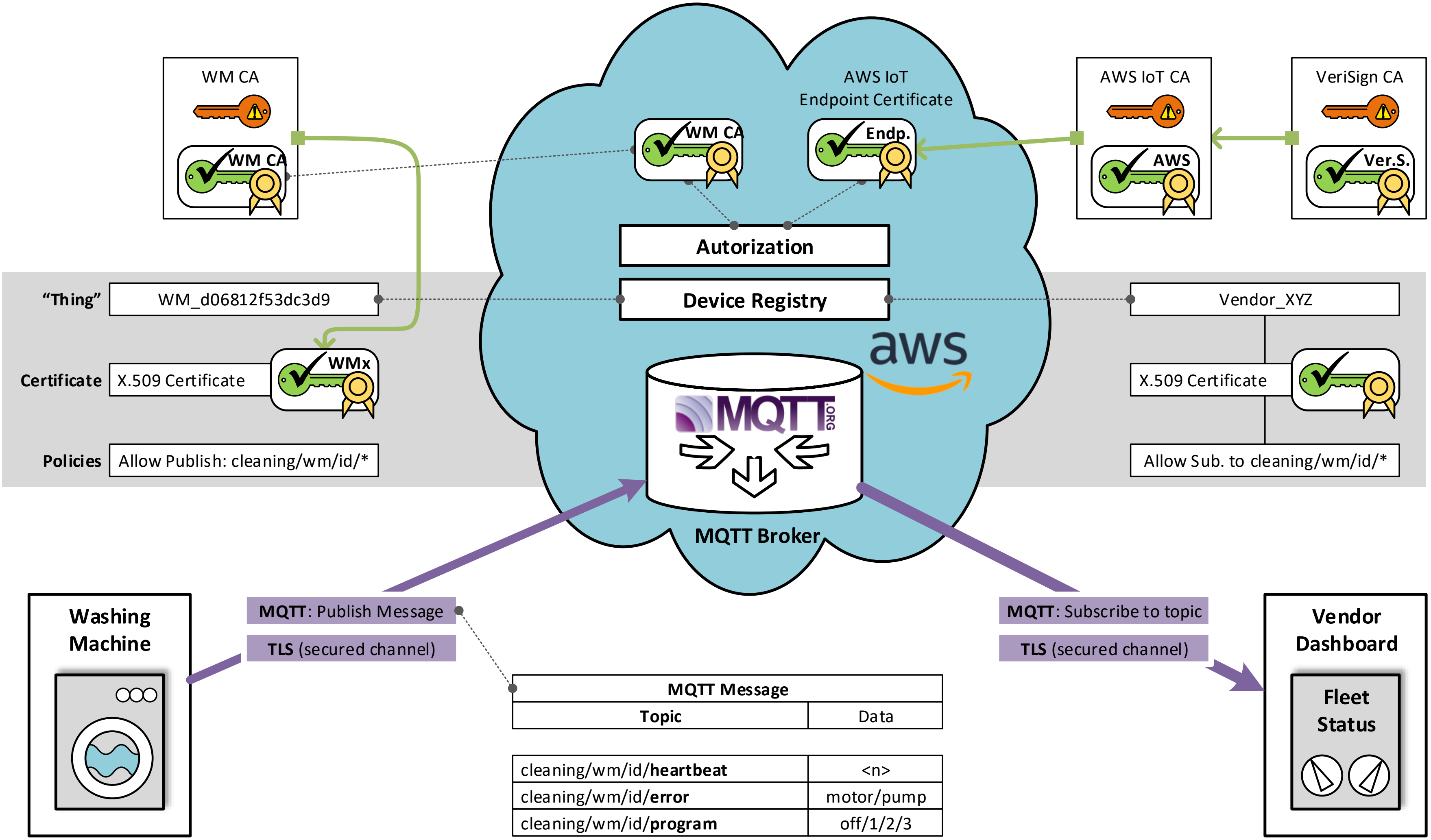
MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /5d: **Registering** Thing with private PKI



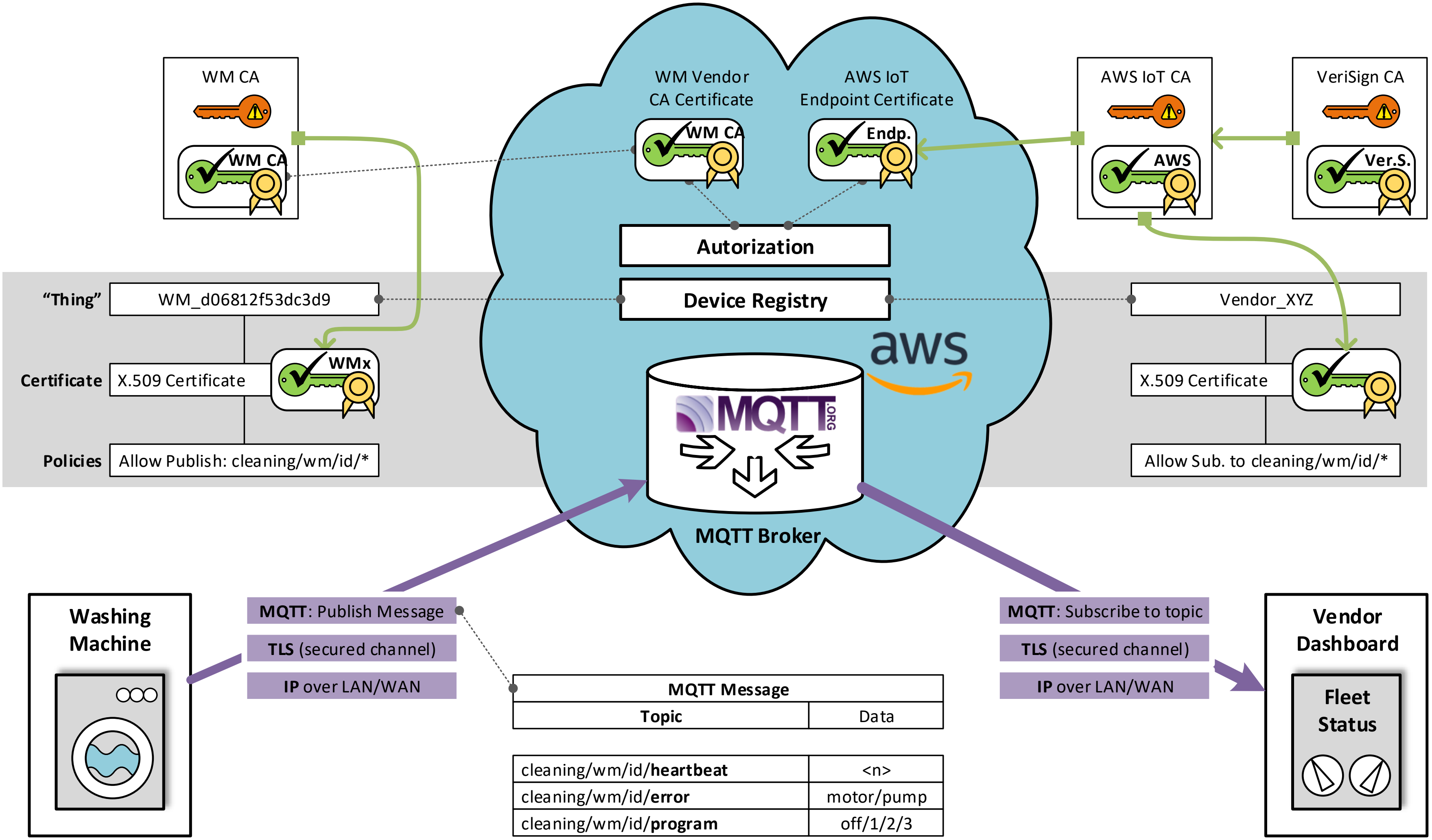
MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

Cloud service integration – AWS IoT /6: **Registering** Thing with AWS CA



MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

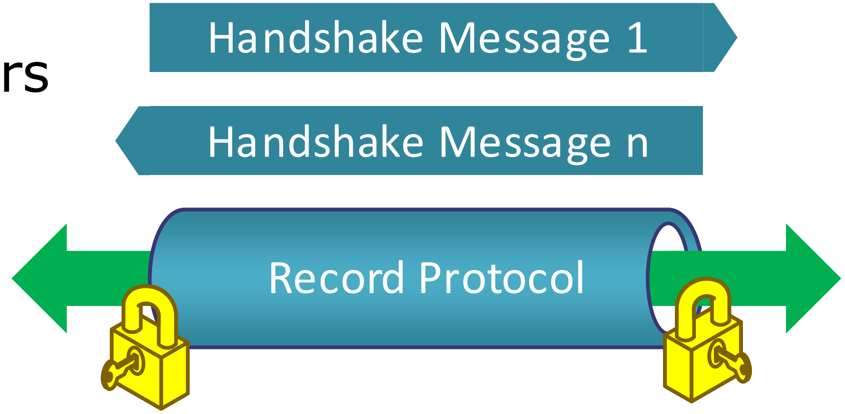
Cloud service integration – AWS IoT /7: **Complete picture** without HW-security



MQTT Message	
Topic	Data
cleaning/wm/id/**heartbeat**	<n>
cleaning/wm/id/**error**	motor/pump
cleaning/wm/id/**program**	off/1/2/3

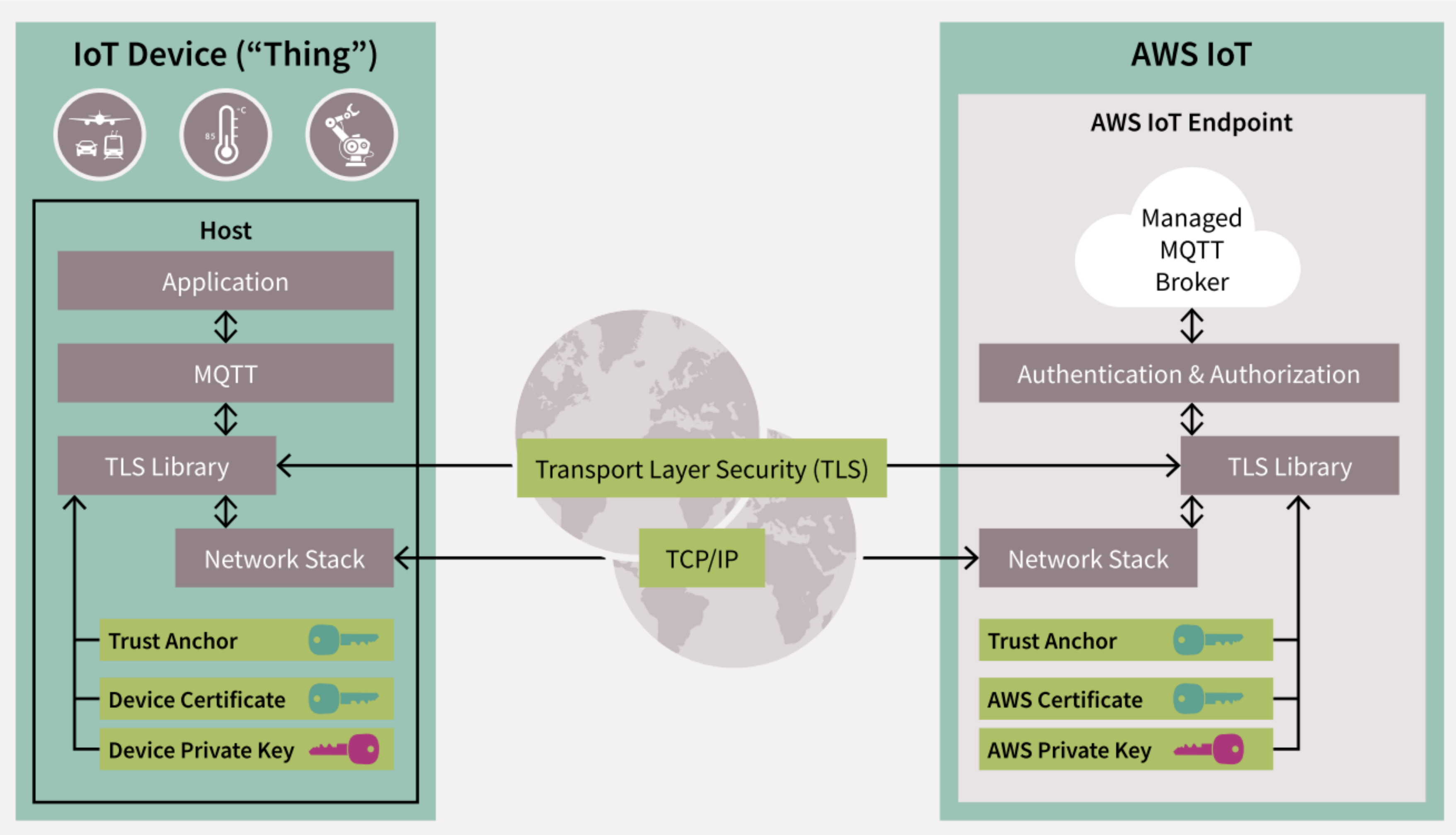
Background
Security in AWS and AWS IoT [RFC 5246], [Amazon]

- Transport Layer Security (**TLS**)
  - Secured channel between 2 peers
  - **Two phases**
    - **TLS Handshake** protocol
      - Cipher suite negotiation
      - Authentication of server (client)
      - Session key information exchange
    - **TLS Record** protocol



- **Shared Security Responsibility** Model
  - AWS protects infrastructure and services
  - Integrator secures data and protects IoT device

System Integration Perspective
Without Hardware Security



Agenda

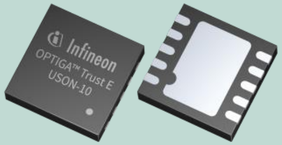
1. Motivation
2. Hardware-based security – what is it?
3. Cloud system architecture with hardware-based security
4. Getting started with hardware-security and Infineon products
5. Conclusion

Infineon offers a comprehensive **IoT security portfolio**

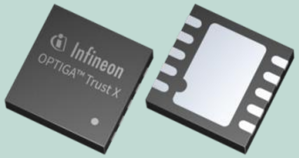
OPTIGA™ IoT security

Cellular connectivity

Trust B/Trust E authentication



Trust X connected devices



TPM

Embedded SIM

Software & tools

OPTIGA™ Trust X
Fully featured device security solution

Premium Security
- Based on CC EAL 6+ (high) certified security controller
- TLS/DTLS Support
- X.509 certificate supported
- TRNG AIS-31 certified
- USB Type C Authentication supported
- Cryptographic ToolBox for flexible customization

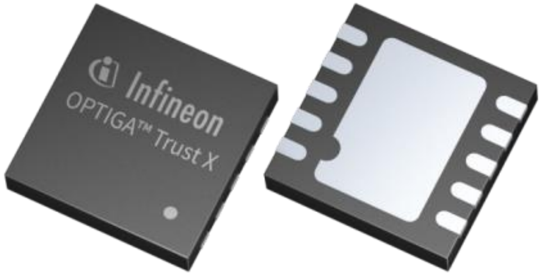
Extended Operating Temperatures
- -25 to +85°C
- -40 to +105°C

Extensive Set of Use Cases
- Mutual Authentication
- Secured Communication
- Data Store Protection
- Lifecycle Management
- Power Management
- Secure Update
- Platform Integrity Protection

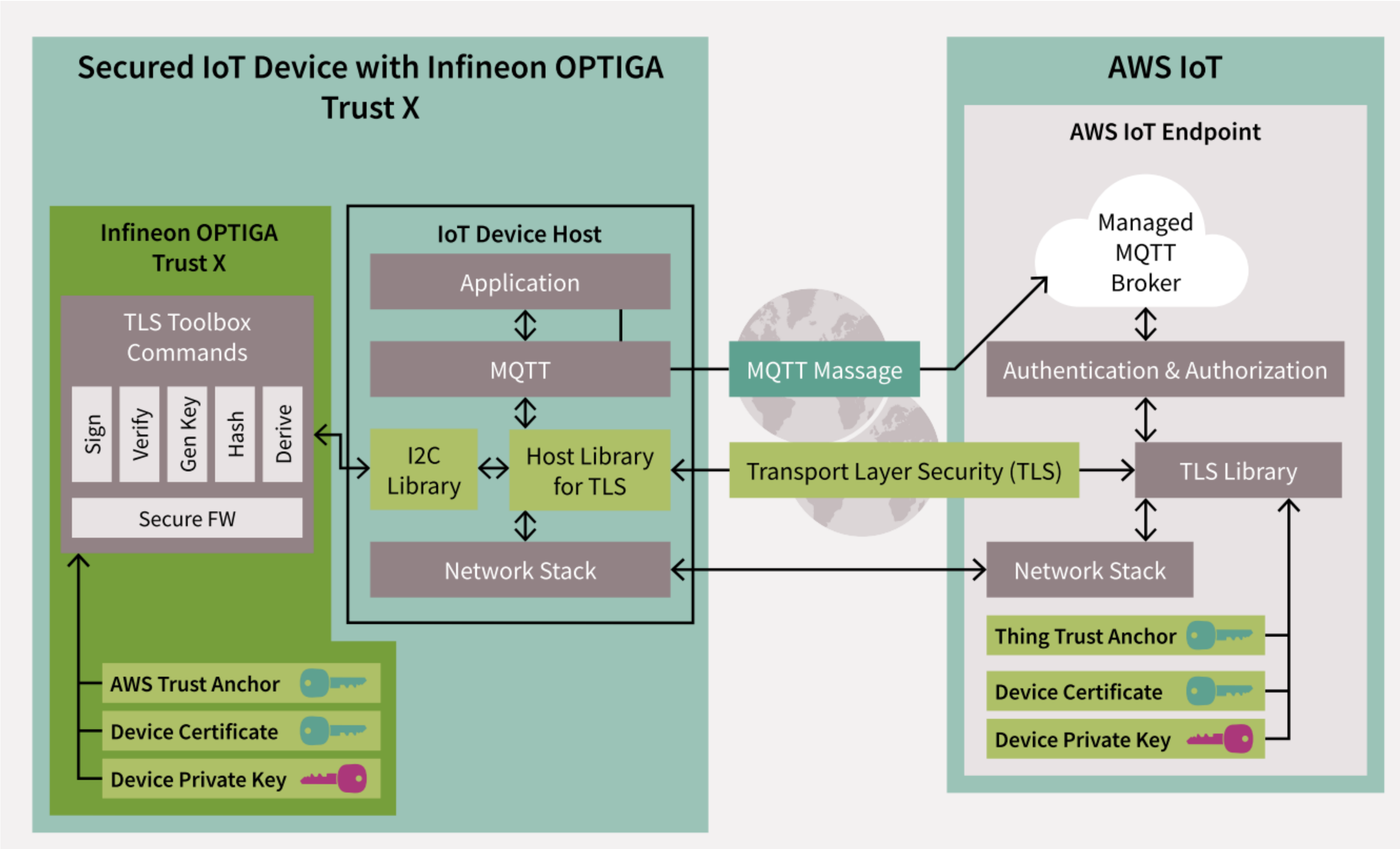
Easy to Integrate
- Full turnkey solution
- Customer specific public key system provided
- Host Code Provided
- Evaluation kit

Product Details (SLS 32AIA)

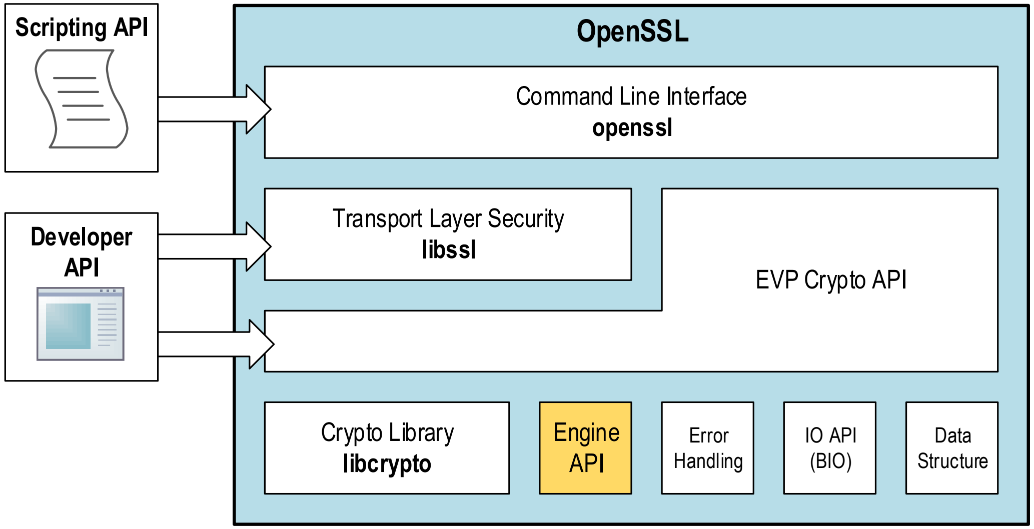
Set-up	Turnkey	Interface	I2C
Data Store	10kB	Interface Speed	1 Mbit/sec
Cryptography	ECC, AES, SHA2	Package	USON-10
Available	January 2018	Size	3 x 3 mm



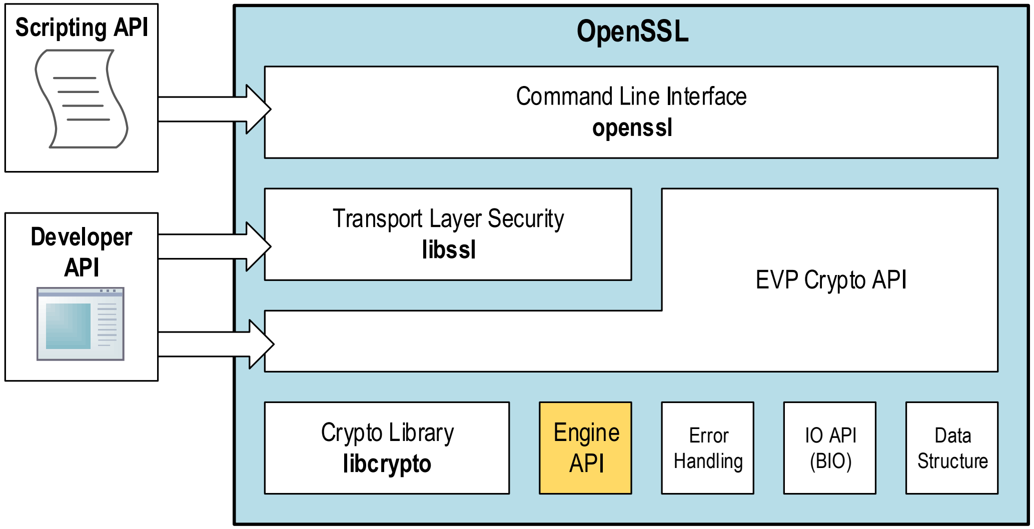
System Integration Perspective With **OPTIGA™ Trust X** Hardware Security



System Integration Perspective
TLS Library: **OpenSSL and libssl** /1



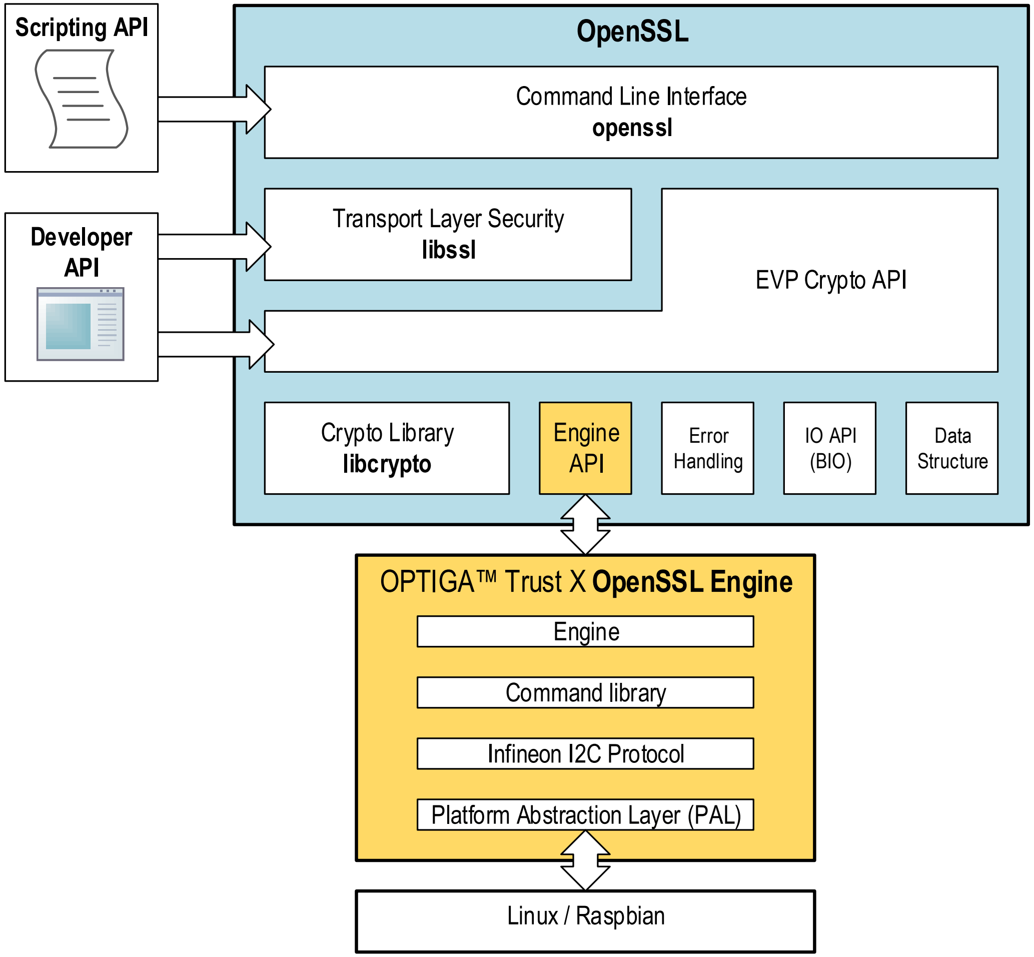
System Integration Perspective
TLS Library: **OpenSSL and libssl** /1



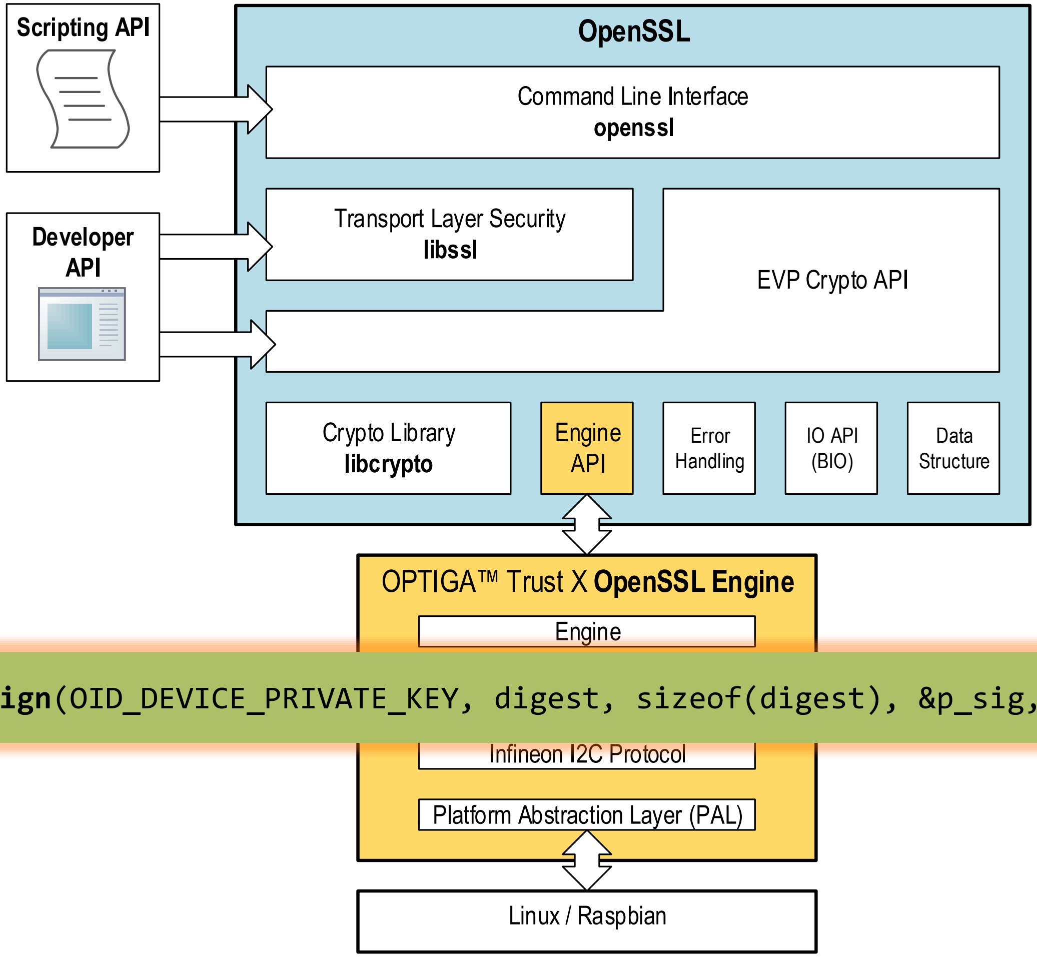
```
$ openssl dgst -sha256 -engine optiga_trust_x -keyform engine -sign “0xE0F0" $MSG
```

```
ENGINE_set_default_ECDSA(optiga_trust_x);
ECDSA_SIG *signature = ECDSA_do_sign(digest, strlen(digest), eckey);
```

System Integration Perspective
TLS Library: **OpenSSL and libssl** /2

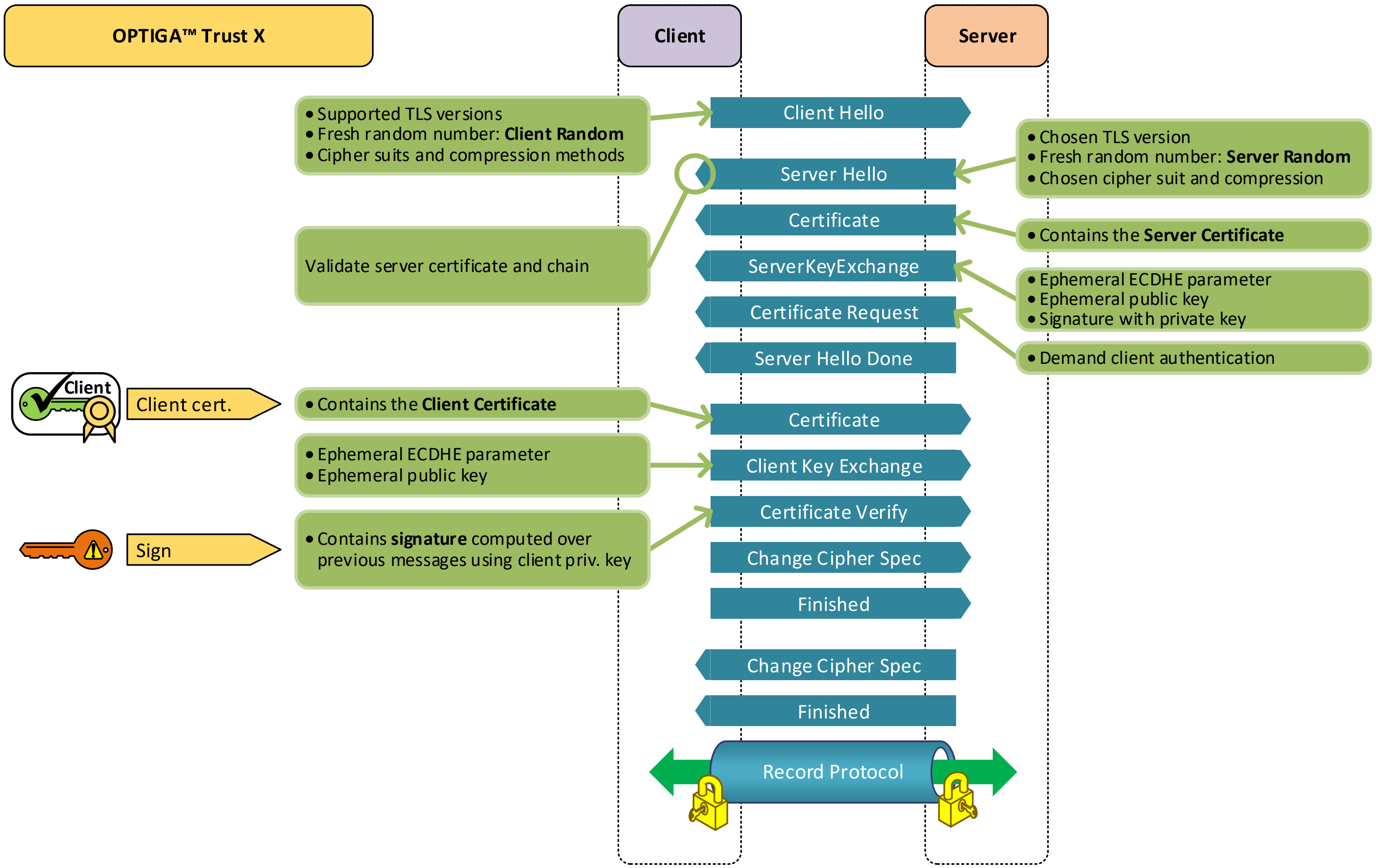


System Integration Perspective
TLS Library: **OpenSSL and libssl** /2



```
optiga_calc_sign(OID_DEVICE_PRIVATE_KEY, digest, sizeof(digest), &p_sig, &sig_len);
```

System Integration Perspective
Transport Layer Security /1



OPTIGA™ Trust X

Client

Server

- Supported TLS versions
- Fresh random number: **Client Random**
- Cipher suits and compression methods

Client Hello

- Chosen TLS version
- Fresh random number: **Server Random**
- Chosen cipher suit and compression

Server Hello

Validate server certificate and chain

Certificate

- Contains the **Server Certificate**

ServerKeyExchange

- Ephemeral ECDHE parameter
- Ephemeral public key
- Signature with private key

Certificate Request

- Demand client authentication

Server Hello Done

Client

Client cert.

- Contains the **Client Certificate**

Certificate

- Ephemeral ECDHE parameter
- Ephemeral public key

Client Key Exchange

Sign

- Contains **signature** computed over previous messages using client priv. key

Certificate Verify

Change Cipher Spec

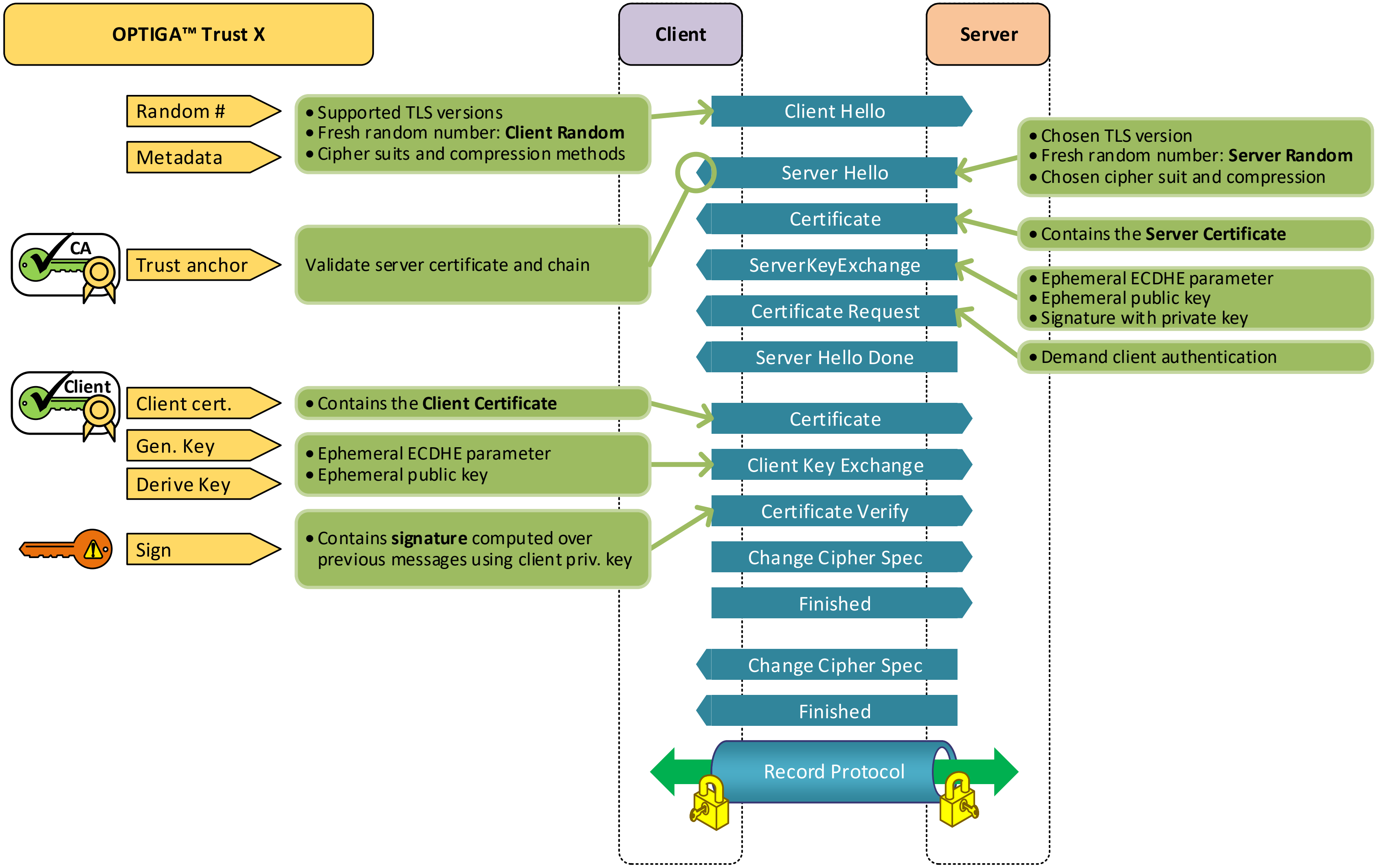
Finished

Change Cipher Spec

Finished

Record Protocol

System Integration Perspective
Transport Layer Security /2



OPTIGA™ Trust X

Client

Server

Random #

Metadata

- Supported TLS versions
- Fresh random number: **Client Random**
- Cipher suits and compression methods

Client Hello

Server Hello

- Chosen TLS version
- Fresh random number: **Server Random**
- Chosen cipher suit and compression

Trust anchor

Validate server certificate and chain

Certificate

- Contains the **Server Certificate**

ServerKeyExchange

- Ephemeral ECDHE parameter
- Ephemeral public key
- Signature with private key

Certificate Request

- Demand client authentication

Server Hello Done

Client cert.

- Contains the **Client Certificate**

Certificate

Gen. Key

Derive Key

- Ephemeral ECDHE parameter
- Ephemeral public key

Client Key Exchange

Sign

- Contains **signature** computed over previous messages using client priv. key

Certificate Verify

Change Cipher Spec

Finished

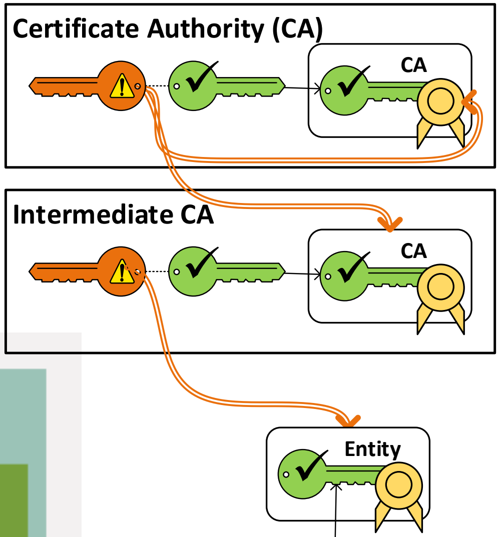
Change Cipher Spec

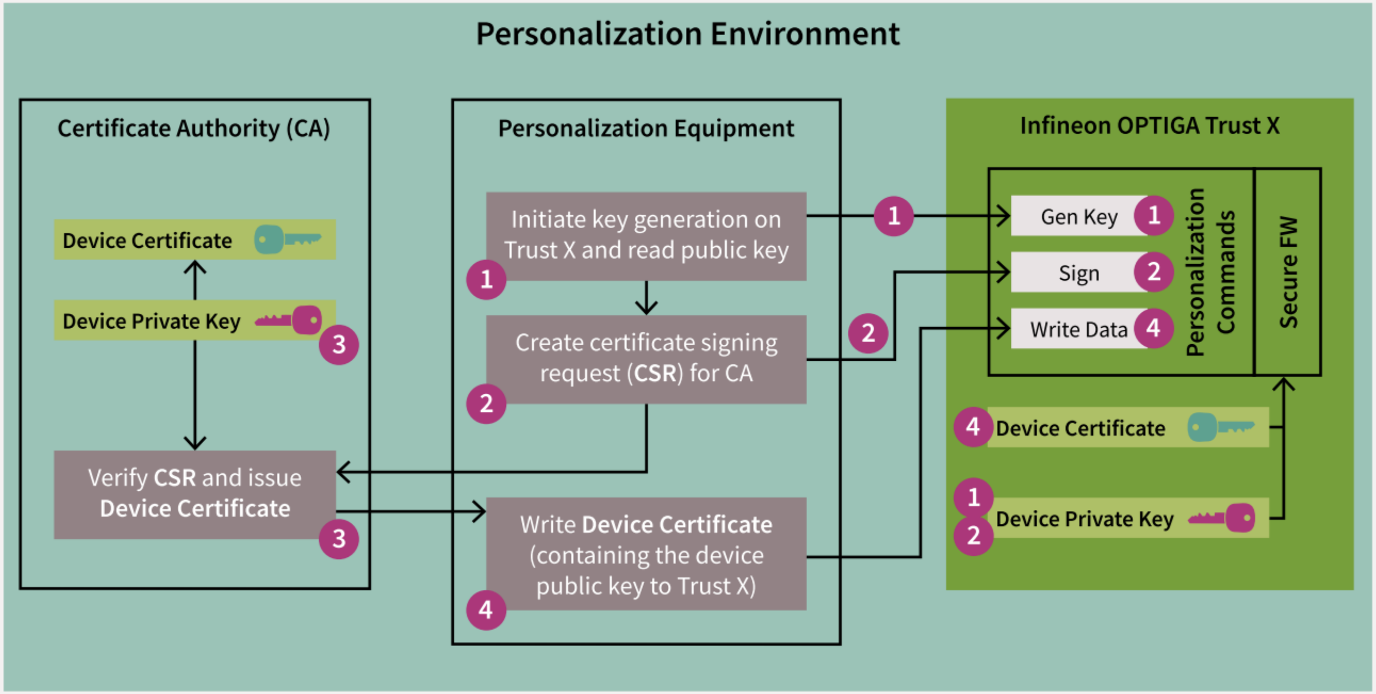
Finished

Record Protocol

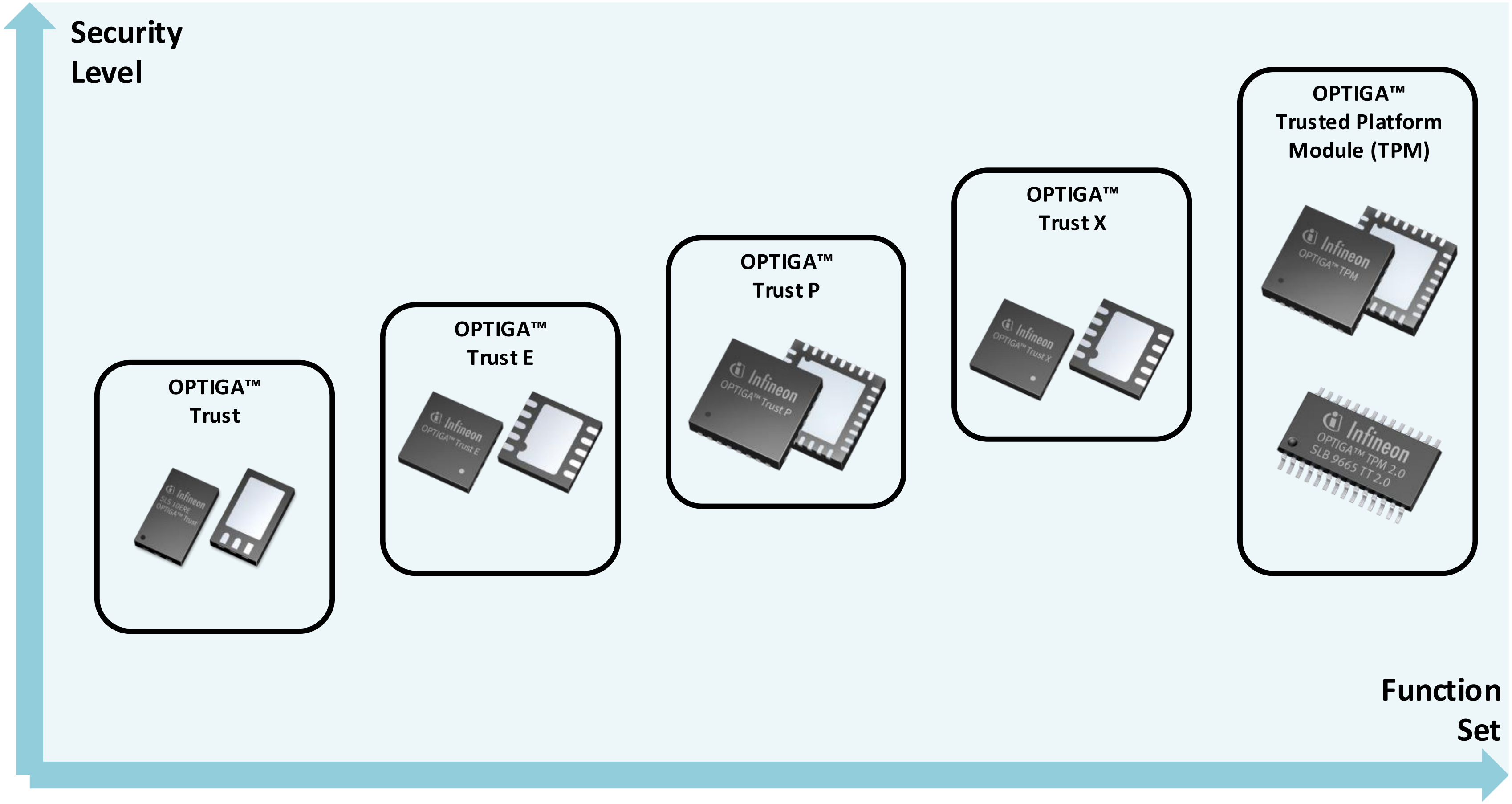
System Integration Perspective
Lifecycle Integration

- Personalization and/or PKI management by
  - Infineon, distributor or system integrator




Personalization Environment
Certificate Authority (CA)
Device Certificate
Device Private Key
3
Verify CSR and issue Device Certificate
3
Personalization Equipment
Initiate key generation on Trust X and read public key
1
Create certificate signing request (CSR) for CA
2
Write Device Certificate (containing the device public key to Trust X)
4
1
2
Infineon OPTIGA Trust X
Gen Key 1
Sign 2
Write Data 4
Personalization Commands
Secure FW
4 Device Certificate
1
2 Device Private Key

Infineon OPTIGA™ Portfolio



Security Level

OPTIGA™ Trust

OPTIGA™ Trust E

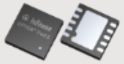
OPTIGA™ Trust P

OPTIGA™ Trust X

OPTIGA™ Trusted Platform Module (TPM)

Function Set

Infineon OPTIGA™ Family

<table>
<tr><th></th><th>OPTIGA™ Trust B</th><th>OPTIGA™ Trust E</th><th>OPTIGA™ Trust X</th><th>OPTIGA™ Trust P</th><th>OPTIGA™ TPM</th></tr>
<tr><td></td><td> </td><td></td><td> </td><td> </td><td> </td></tr>
<tr><td>Security Level</td><td>Basic</td><td>CC EAL 6+*</td><td>CC EAL 6+*</td><td>CC EAL 5+*</td><td>CC EAL 4+</td></tr>
<tr><td>Functionality</td><td>Authentication</td><td>Authentication</td><td>Connected device security</td><td>Programmable</td><td>TCG standard</td></tr>
<tr><td>NVM (Data)</td><td>64 Byte</td><td>3 kByte</td><td>10 kByte</td><td>150 kByte**</td><td>6 kByte</td></tr>
<tr><td>Cryptography
Private key stored in secured HW</td><td>ECC131</td><td>ECC256</td><td>ECC384</td><td>ECC521
RSA2K</td><td>ECC256
RSA2K</td></tr>
<tr><td rowspan="3">Type of Host System</td><td colspan="4">MCU without OS / proprietary OS / RTOS</td><td></td></tr>
<tr><td></td><td></td><td colspan="3">Embedded Linux</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Windows / Linux</td></tr>
<tr><td>Interface</td><td>SWI</td><td>I2C</td><td>I2C</td><td>UART</td><td>I2C, SPI, LPC</td></tr>
<tr><td>System integration</td><td>✓</td><td>✓</td><td>✓</td><td>✔</td><td>Platform vendor</td></tr>
</table>

✓ Done by IFX

✔ Customer Implementation, support by IFX

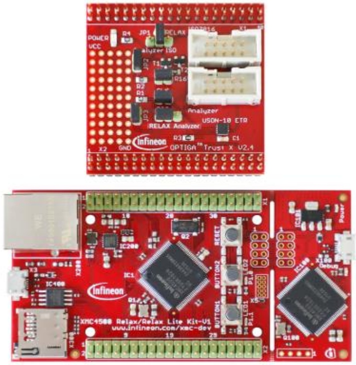
* Based on certified HW

** Code & Data

Security and Complexity

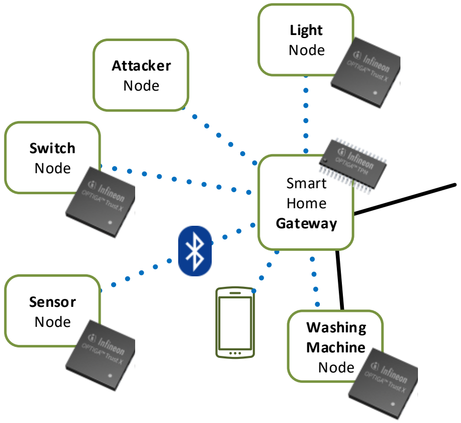
Infineon OPTIGA™ TPM and OPTIGA™ Trust **Getting Started** with Hardware Security

- **OPTIGA™ Trust X Evaluation Kit**



- **Iridium TPM board**
  - For Raspberry Pi and BeagleBone

- **Securing Bluetooth Devices and DTLS**
  - Video
  - Nordic nRF5 SDK



- **Further Material**
  - Visit infineon.com for
    - Whitepapers
    - Application notes
    - Webinars etc.
  - OPTIGA™ Trust X

Agenda

1 Motivation

2 Hardware-based security – what is it?

3 Cloud system architecture with hardware-based security

4 Getting started with hardware-security and Infineon products

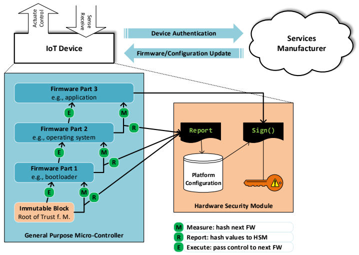
5 Conclusion

Conclusion / “Fazit”

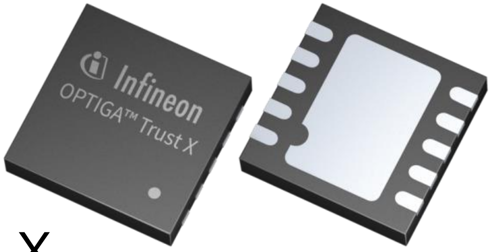
- **Discrete hardware-based security**
  - Protected and certified hardware
  - Tailored set of security functions (“API”)
  - Adds an defense-in-depth layer
    and supports protection of IoT devices

Avoid
technical debt
–
design-in
HW-security
early on!

- **HW-security protects major security use cases**
  - Provisioning, authentication & communication
  - Firmware update and platform integrity



- **Infineon** offers a range of products
  - Infineon OPTIGA™ TPM
  - Infineon OTIPGA™ Trust E and OPTIGA™ Trust X



Disclaimer

The information given in this training materials is given as a hint for the implementation of the Infineon Technologies component only and shall not be regarded as any description or warranty of a certain functionality, condition or quality of the Infineon Technologies component.

Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this training material.

Part of your life. Part of tomorrow.

infineon