Java Card™ Secure Elements for the Matter enabled Smarthome

Java Card Forum Webinar 2022-11-25
Daniel Hübner - System Architect IoT Security

The sad state of IoT security

>70%

of customers would purchase more IoT devices if security was addressed

(Source: Bain and Co: “Cybersecurity Is the Key to Unlocking)

45%

of respondents agree that security concerns have held back IoT adoption

(Source: 2020 IoT Business Index Survey: Economist Intelligence Unit)

Security is a

leading barrier

for IoT adoption

(Source: Bain and Co: “Cybersecurity Is the Key to Unlocking Demand in the Internet of Things)

Less than

4%

of new IoT devices include sufficient security

(Source: ABI Research)

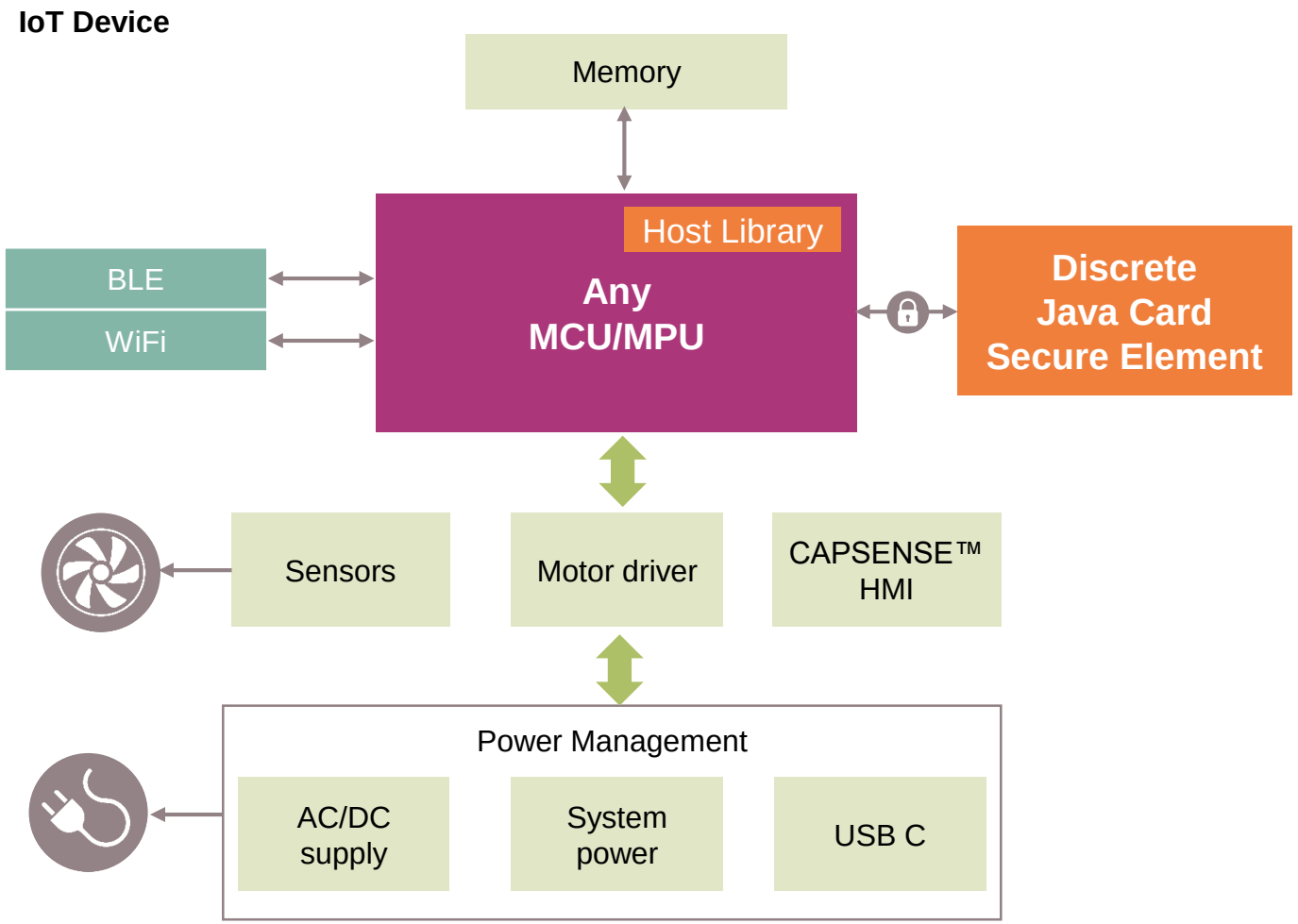
Massive lack of skills:

3.5 million

cybersecurity jobs unfilled

(Source: The New York Times (Nov. 7th 2018))

Discrete Java Card Secure Element
Typical system diagram and focus applications



Typical Applications		
Smart Home	Enterprise / Smart Building	Industrial Automation
Smart speaker	Smart door lock	PLC
Residential HVAC	Commercial HVAC	Drives
Ceiling fan	Surveillance camera	Service robots
Refrigerator Washing machines	Street lighting	
Other home appliances		

Why discrete Security

Secured Pre-provisioned Trust

- Trust credentials are provisioned by the Semi during silicon manufacturing
- Sophisticated, flexible custom configuration possible (not only keys)
- PKI (worth 500k$) provided

Modularity

- Works with any Microcontroller to big SystemOnChip Processors

Discrete Security

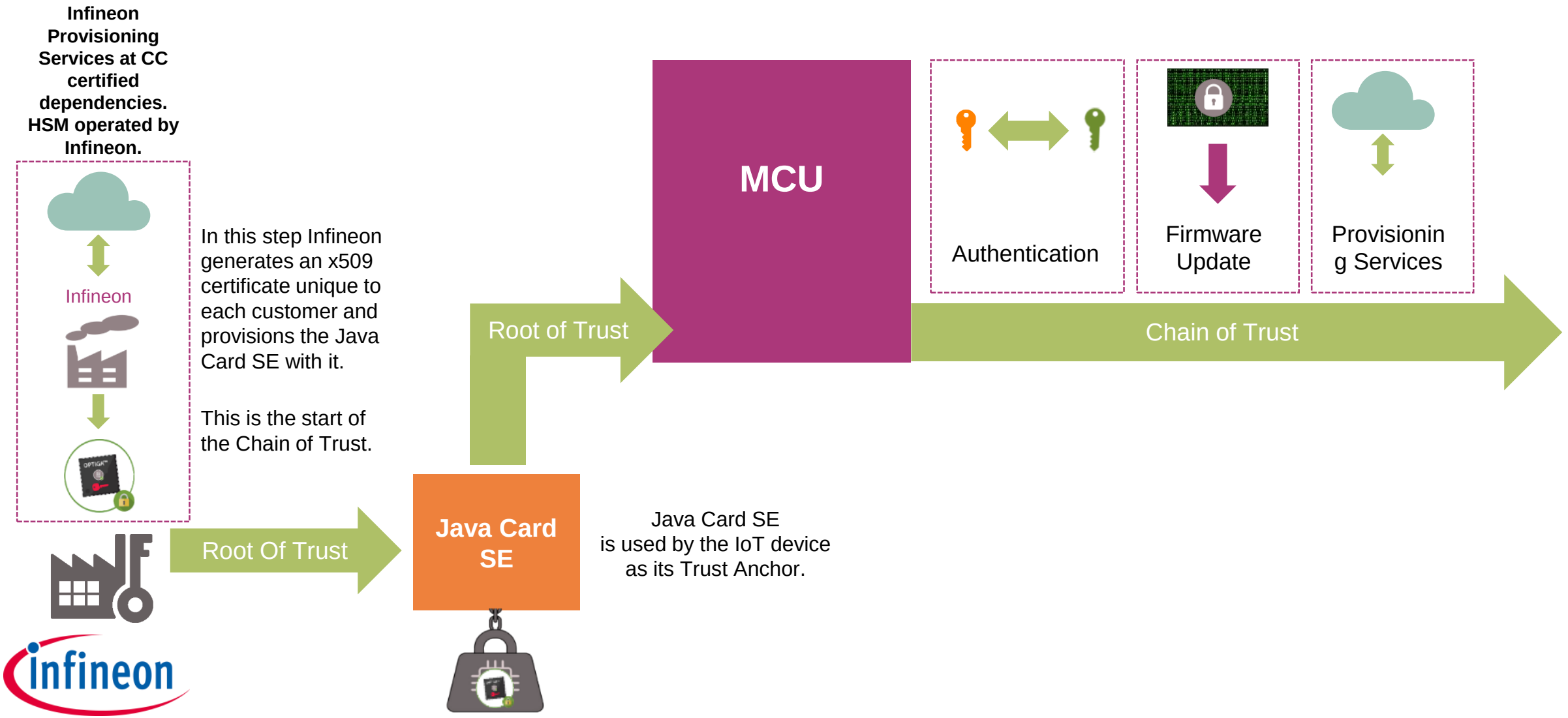
Key Isolation

- Keys are completely isolated by OS Software stack in an separate chip
- Secrete Key never leaves
- Extremely reduced attack surface by simple and formally verifiable OS and less- complex interfaces

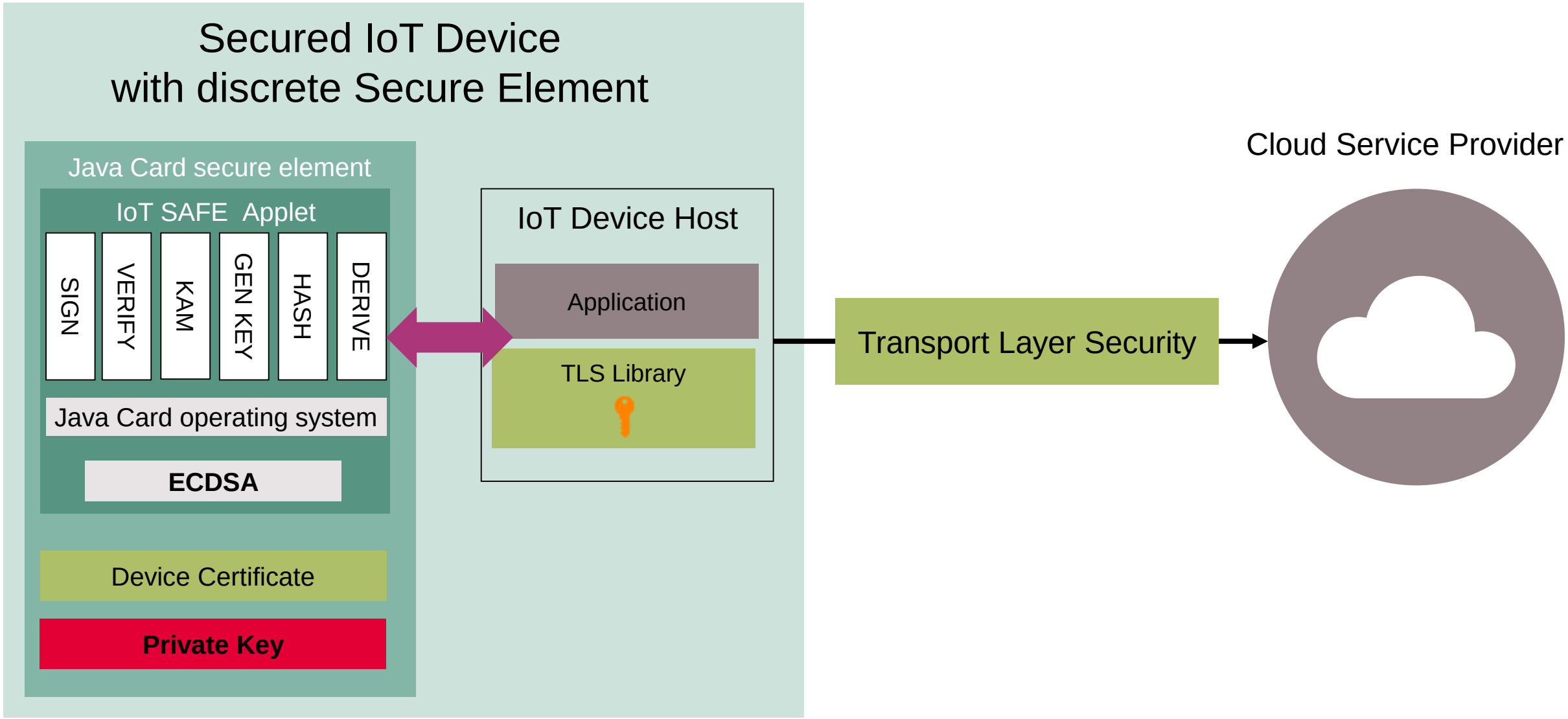
Crypto Offloading

- Dedicates on-chip crypto accelerators boosts any crypto operations especially on constrained MCUs
- BSI and NIST approved Random Number Generators

Secure pre-provisioning trust is the foundation for a chain of trust



Key Isolation on the example of the TLS handshake



GSMA IoT SAFE
Supporting Documents

Download from here

Download from here

- Standardized approach for a TLS Root of Trust in form of an Java Card Applet
- Eases the integration efforts with middleware ecosystems eg. openSSL
- Compliance Program in place
- Interface designed for Crypto Agility

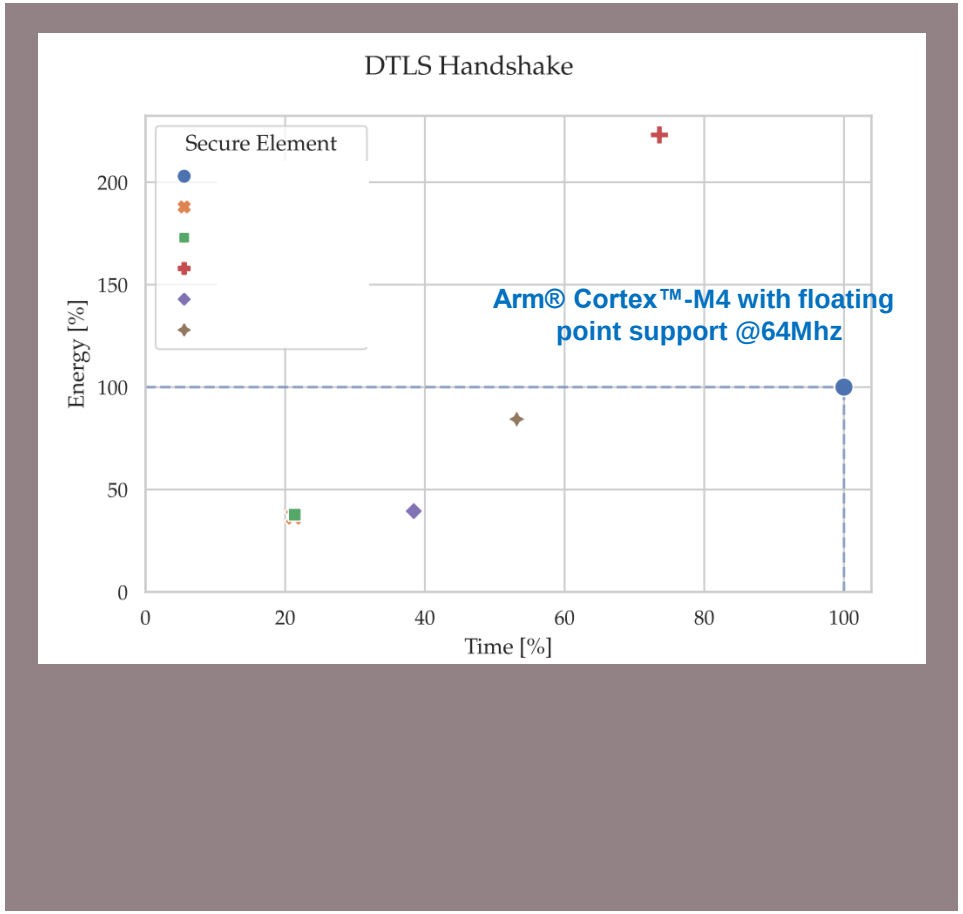
Crypto Offloading: Discrete Secure Element shortens cryptographic execution and saves energy

5 times faster

- ✓ For better User Experience
- ✓ Easier to meet performance requirements

60% less energy

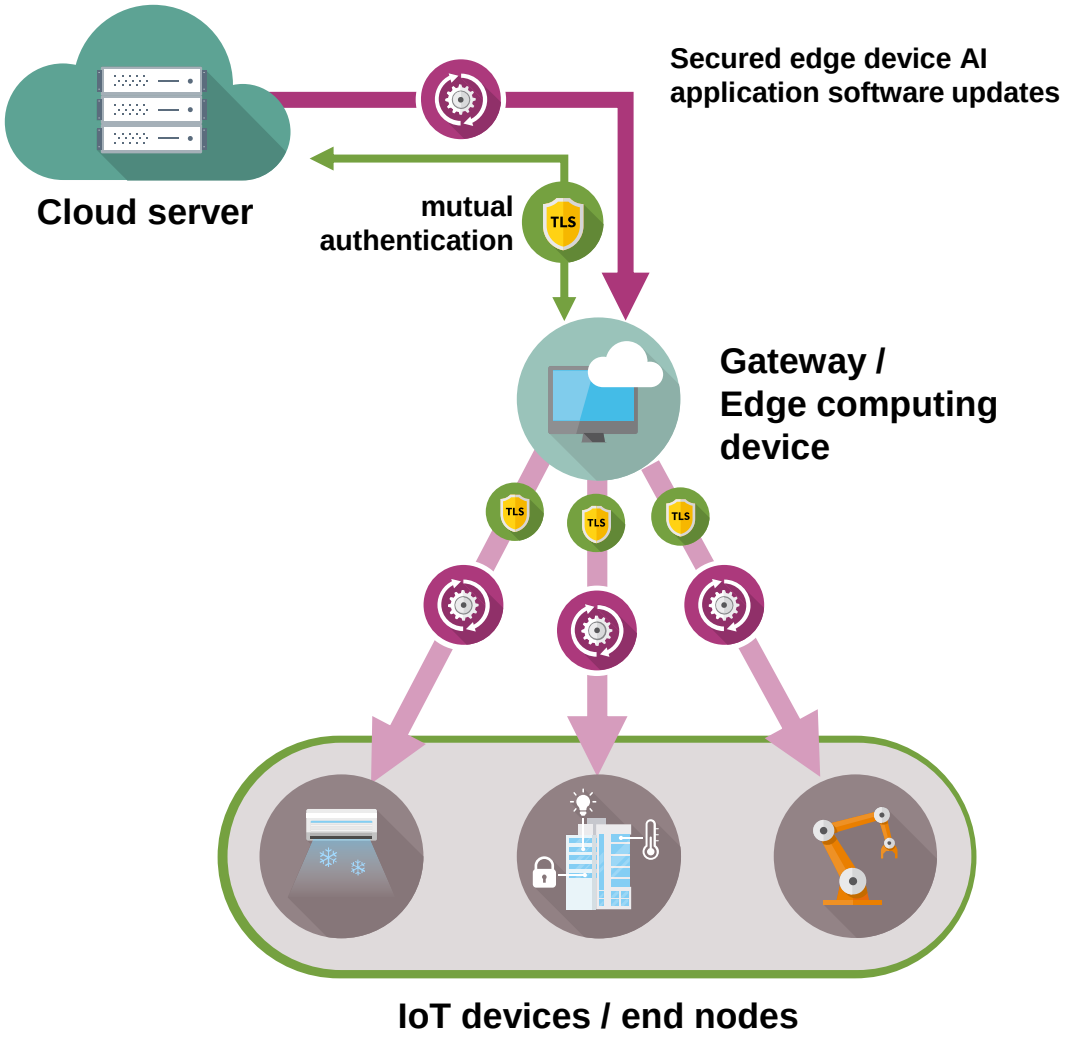
- ✓ Stay in the power budget for battery driven applications
- ✓ Less heat dissipation measurement required



Source: [Article "Performance Analysis of Secure Elements for IoT"]

Discrete Secure Element: Classical Usecases

Protecting the IoT from cloud to end nodes



TLS

Secured connectivity

Secured cloud authentication

Secured software update over-the-air

Matter Background and Motivation: Smart Home IoT Protocols are Fragmented

THREAD

Wi Fi™

ZigBee®

Bluetooth®

"Closed" Ecosystems in Smart Home

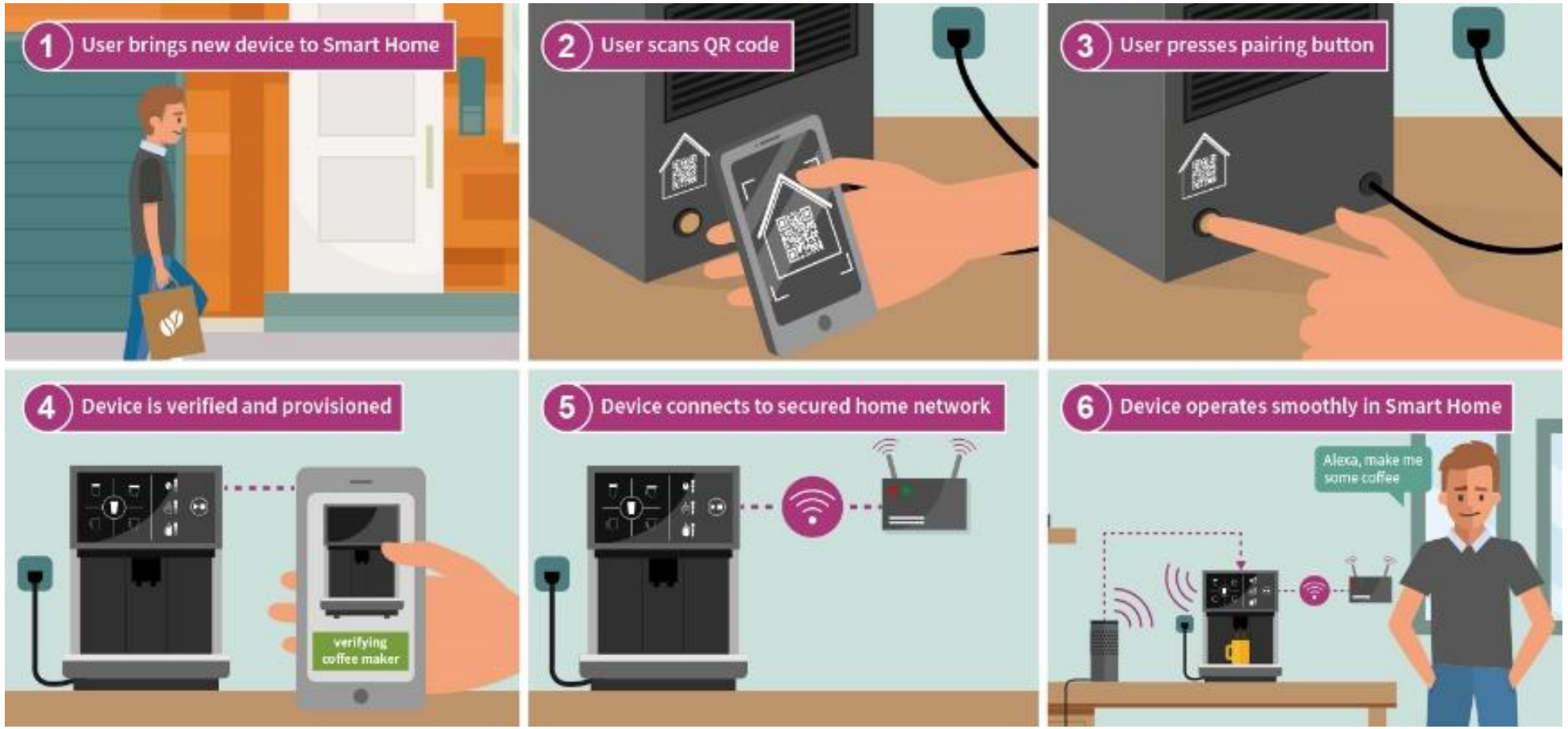
- Apple, Amazon, Google have been using their own "closed" ecosystems for their IoT products: Apple Homekit, Amazon Alexa, Google Assistant
- Consumers don't see interoperability, e.g. can't control Nest Thermostat using Alexa

Multiple Wireless Technologies in Smart Home

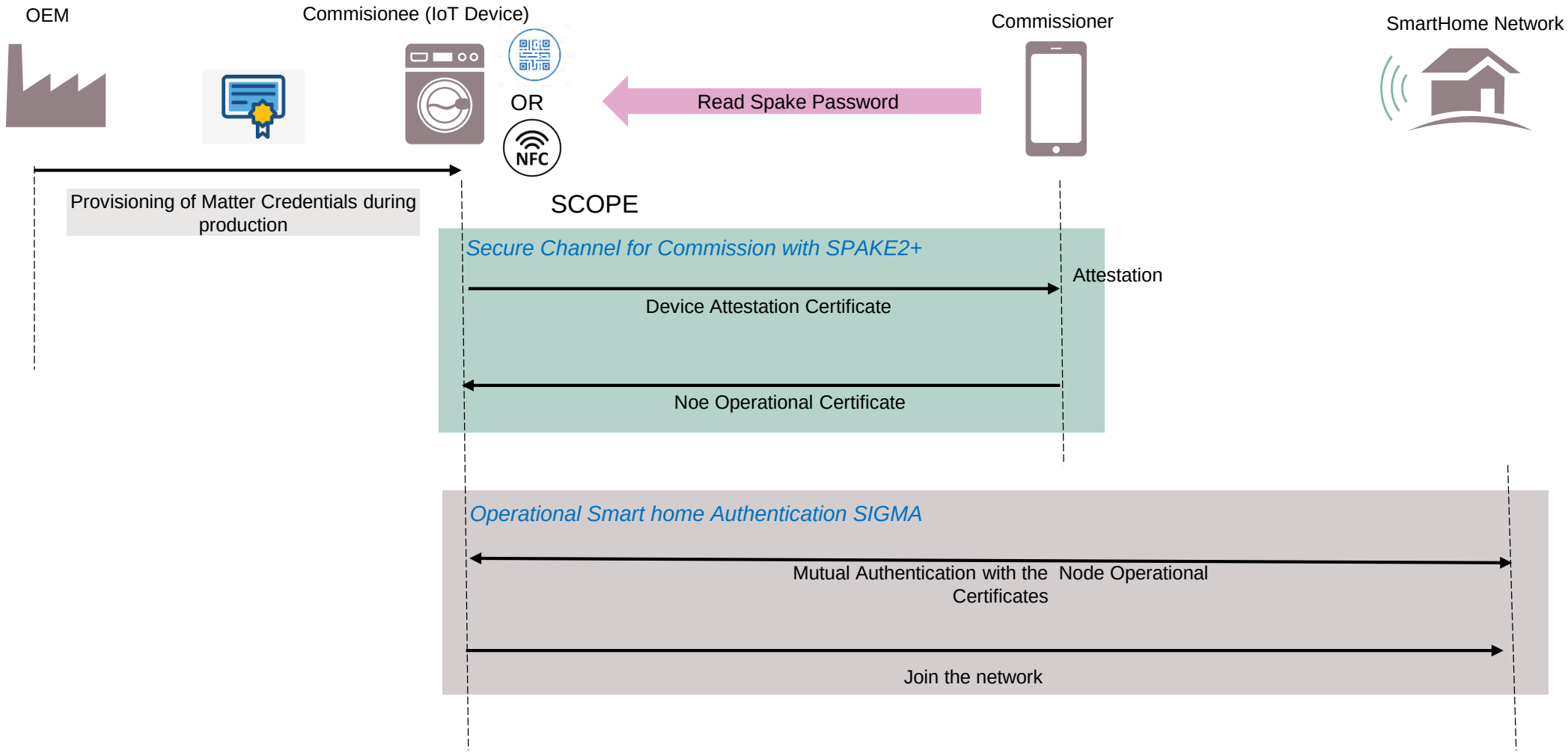
- Different IoT devices use different underlying wireless technologies to best match their application (e.g. IP cam can use Wi-Fi, a smart light build can use 802.15.4 and a voice remote can use BLE)
- Wi-Fi, BLE, 802.15.4 are fundamentally different wireless technologies and can't directly communicate with each other
- Protocol stacks on 15.4 don't interoperate (Thread vs ZigBee)

These barriers increase complexity and slow down the roll-out of new Smart Home devices

The Matter Experience



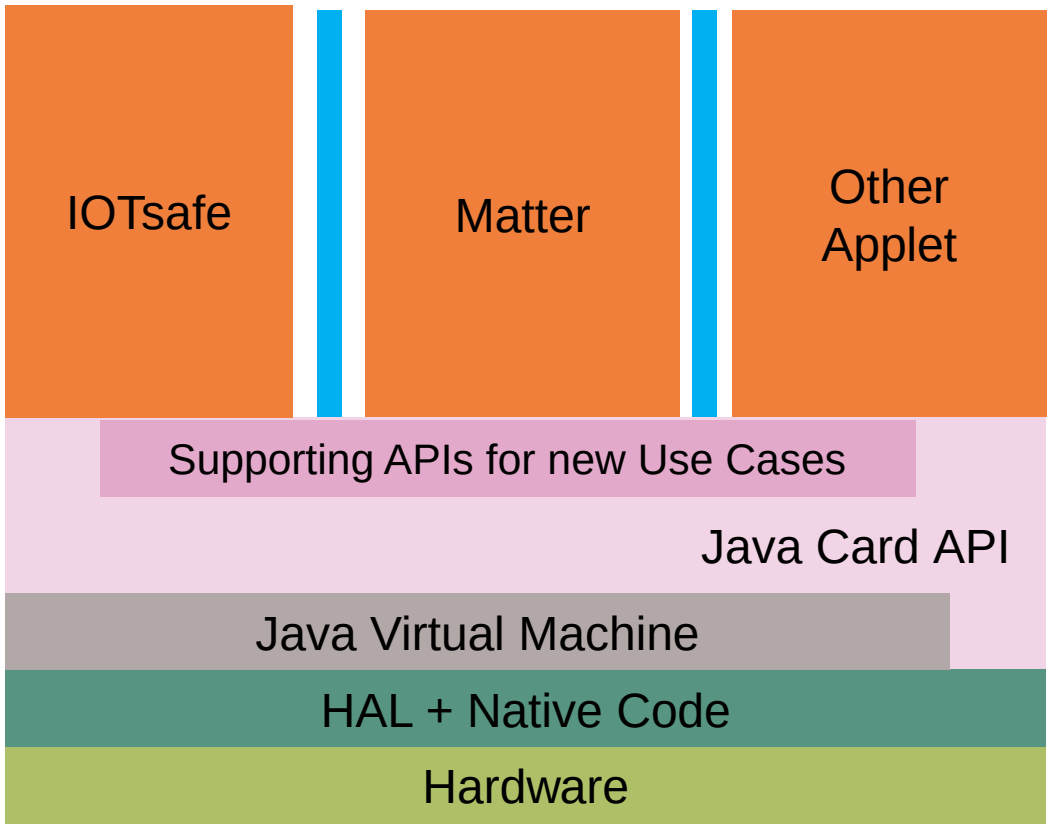
Matter onboarding Flow



This certificates, keys and data needs to be provisioned

Digital Certificates	› Device Attestation Certificate (DAC) › Product Attestation Intermediate Certificate (PAI) › Firmware Update Verification Trust Anchor Certificate
Secret Keys	› DAC Private Key › Firmware Update Encryption Key
Matter Data	› Certification Declaration › Setup Code (VID,PID, PassCode,…) › SPAKE Values (w0,L, PBKDF(Salt, Iterations))
Arbitrary Data	› Any customer data

Conclusion: Discrete Java Card SE for IoT



- Discrete Java Card Secure Elements provide many advantages in terms of security, provision and flexible integration
- Emerging Usecases like Matter secure onboarding can be supported by Java Card products as well
- The Java Card Forum is defining new APIs supporting the ermerging usecases in IoT