Research IoT security

with the help of Arm Musca test chips

Mike Eftimakis

IoT product manager – Arm

Arm Research Summit 2018

Agenda

Arm’s vision for IoT Security

Arm developments in security

Musca test chip program

Arm’s vision for IoT Security

Arm's vision for IoT Security

Security built from the ground up

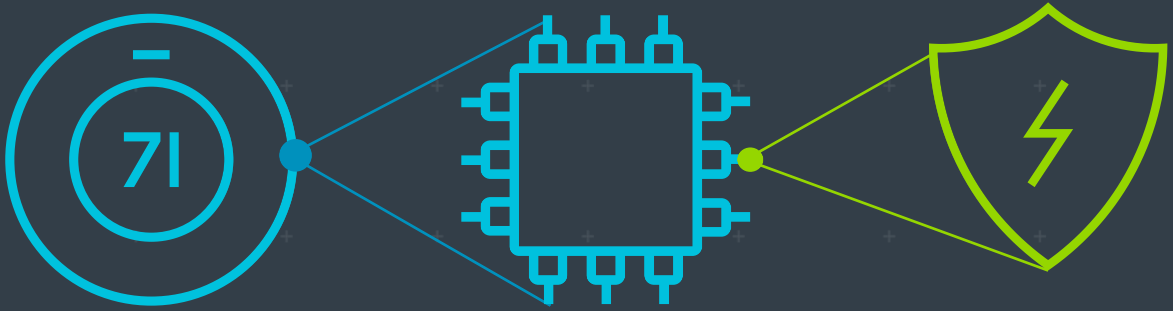
- At the core of every device

No single point of ownership

- IoT value chain share the responsibility

Simple security integration is key

- Seamless
- From foundational architecture
- To cloud service



IoT Device

Platform Security Architecture

A recipe for building a secure system & a reference implementation

Analyze
Threat models & security analysis

Architect
Hardware & firmware architecture specifications

Implement
Firmware source code

3 Parts to PSA

1 Device identity

2 Trusted boot sequence

3 Secure over-the-air software update

4 Certificate based authentication

Common principles across multiple use cases

Software architecture

Hardware requirements

Architecture & Specifications

Arm developments in security

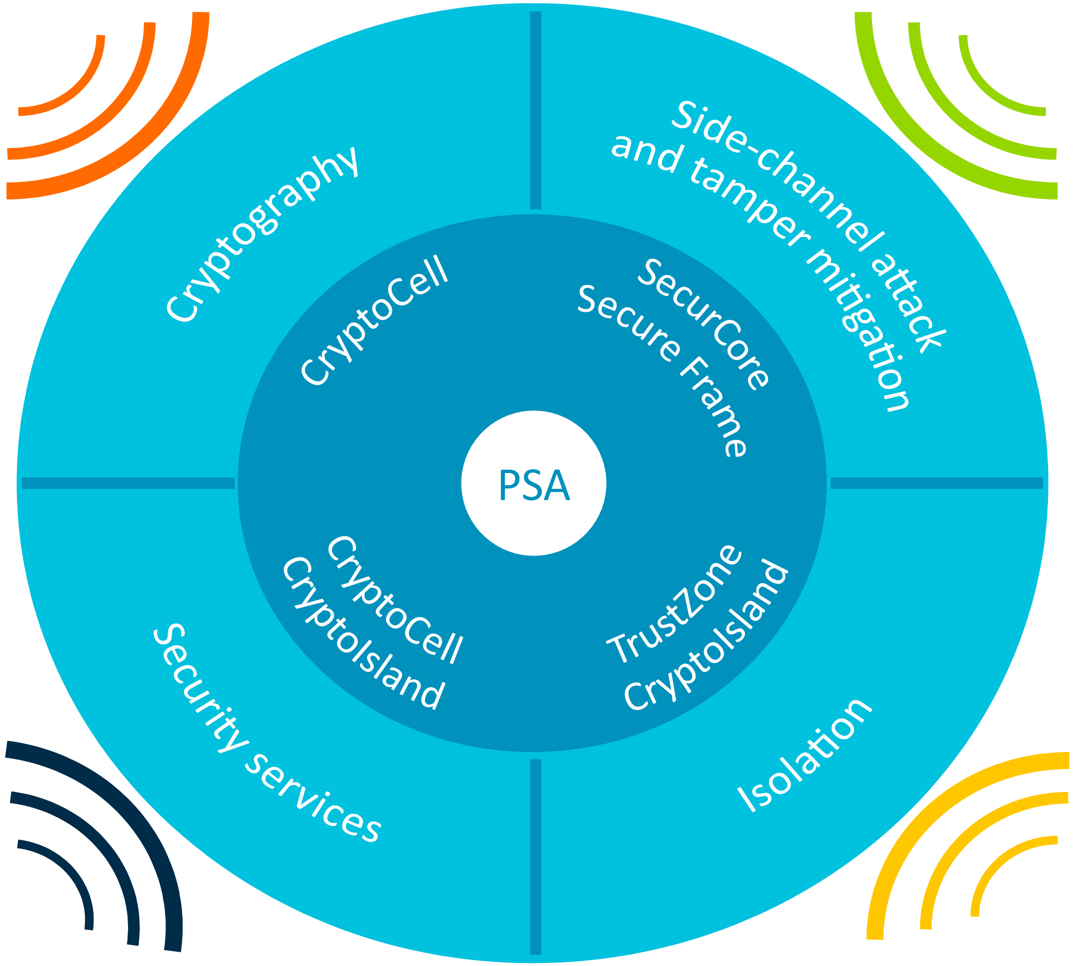
Matching the vulnerability with the right mitigation

Communications

- Man-in-the-middle
- Weak RNG
- Code vulnerabilities

Physical

- Non-invasive: e.g. clock Or power glitch or SCA
- Invasive: package removal, e.g. microprobe station FIB



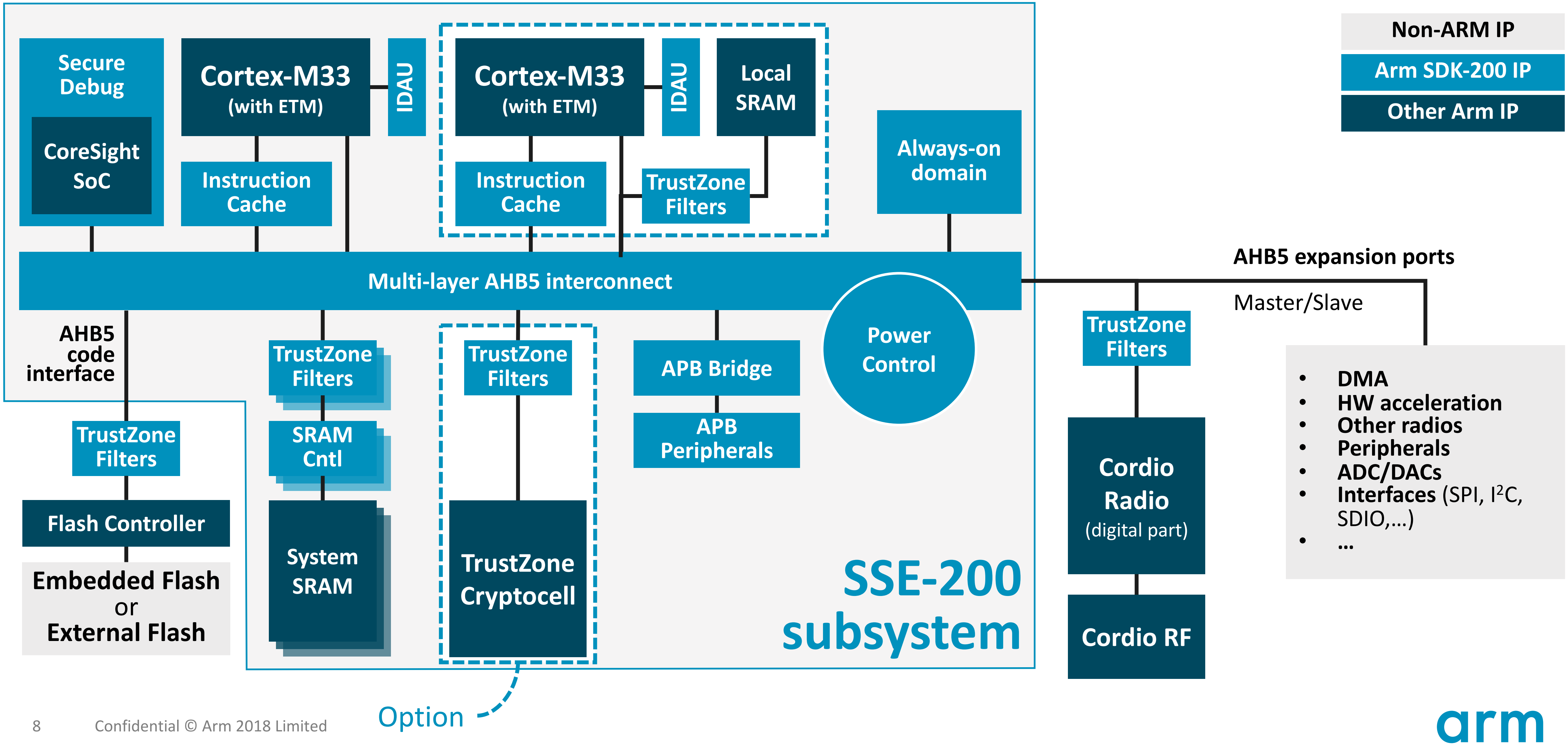
Lifecycle

- Code downgrade
- Change of ownership or environment
- Unauthorized overproduction

Software

- ROP, e.g. buffer overflows
- Interrupts
- Malware

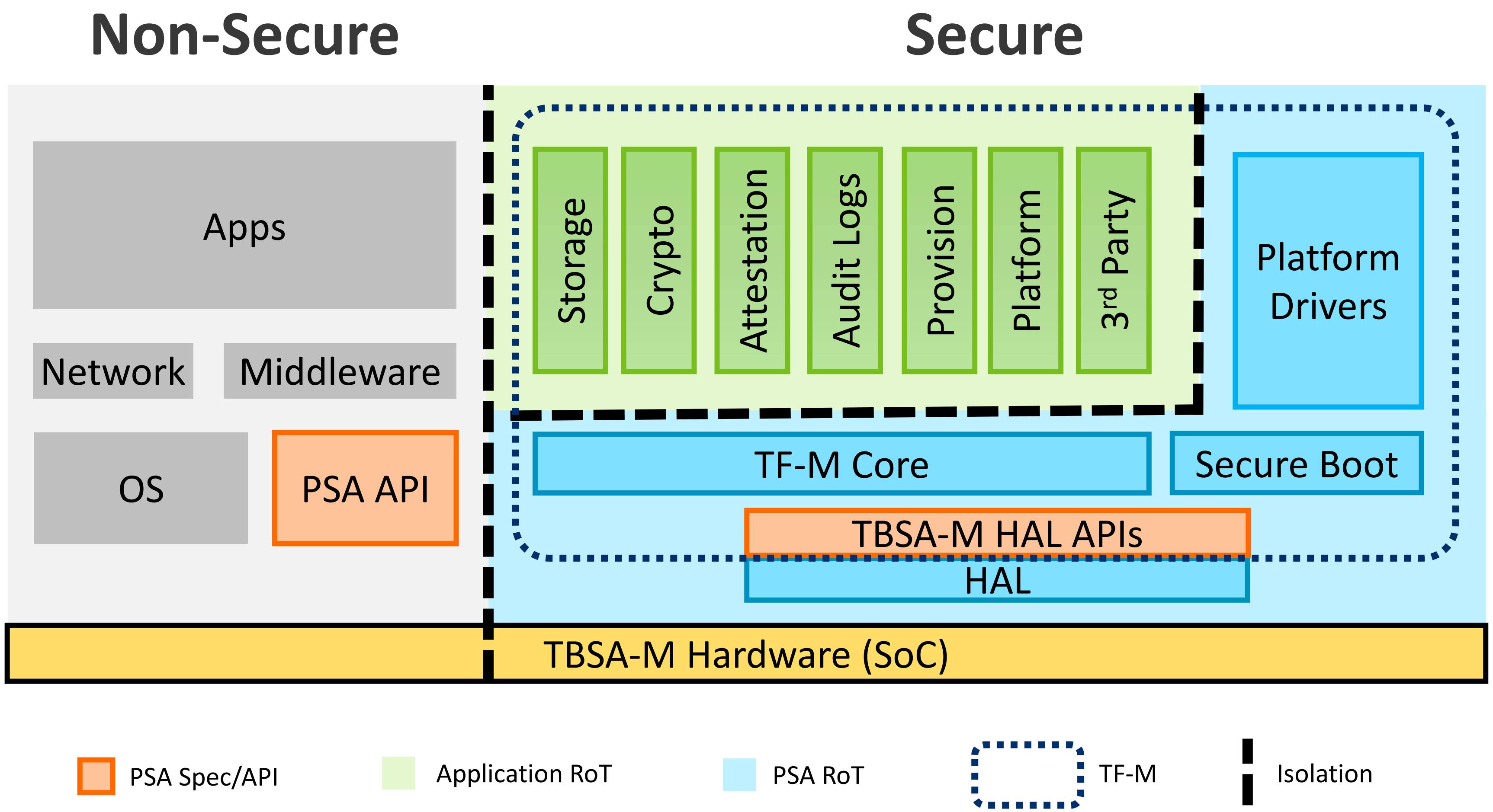
PSA-ready subsystem for IoT



- DMA
- HW acceleration
- Other radios
- Peripherals
- ADC/DACs
- Interfaces (SPI, I^{2}C, SDIO,…)
- …

Trusted Firmware-M (TF-M)

Open-source reference implementation of PSA



TRUSTED FIRMWARE
OPEN SOURCE SECURE WORLD SOFTWARE

www.trustedfirmware.org

Musca test chip program

Goals for Musca program

Marketing tool

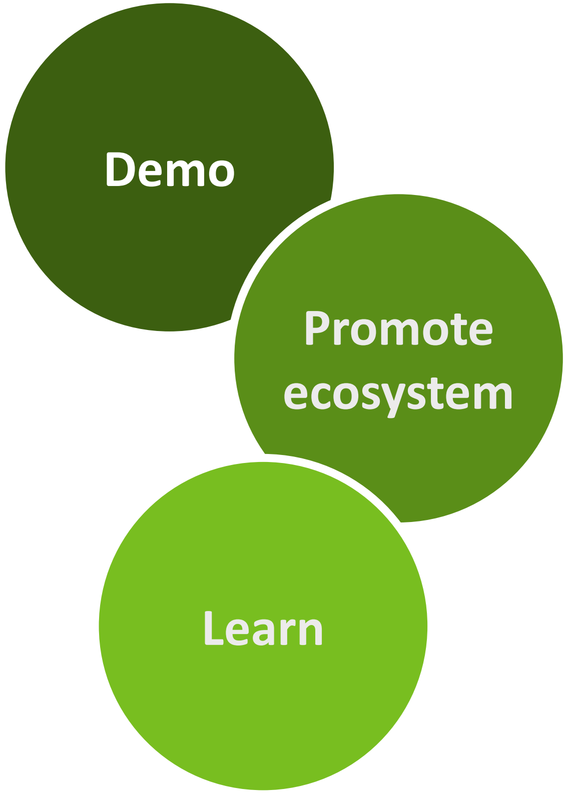
- Demonstrate ARM IoT solution based on PSA
- Use state-of-the-art IP for IoT

Promote ecosystem

- Reference architecture – enable software/device development
- Development platform for PSA

Learning vehicle

- Improve Arm IP
- Transfer to partners – enable faster design of partners' silicon



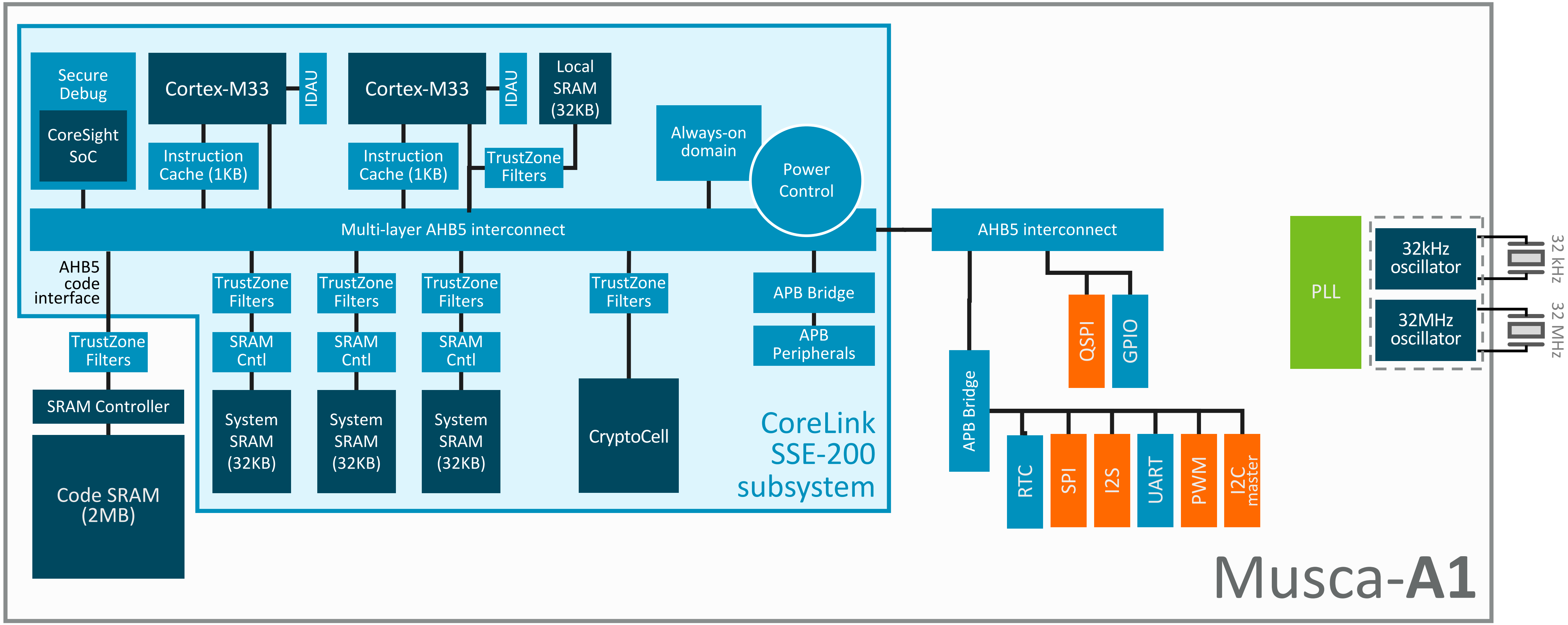
Musca-A1 – PSA development platform

🟦 Other Arm IP

🟦 Arm CoreLink SDK-200 IP

🟧 Cadence IP

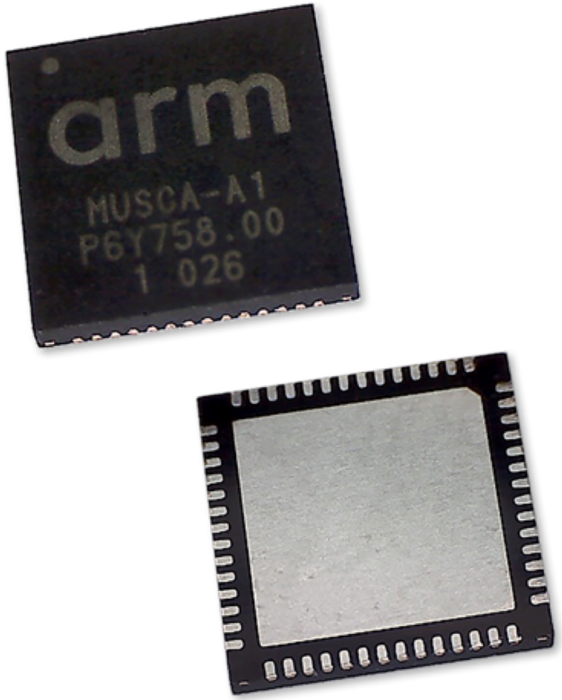
🟩 SiliconCreations IP



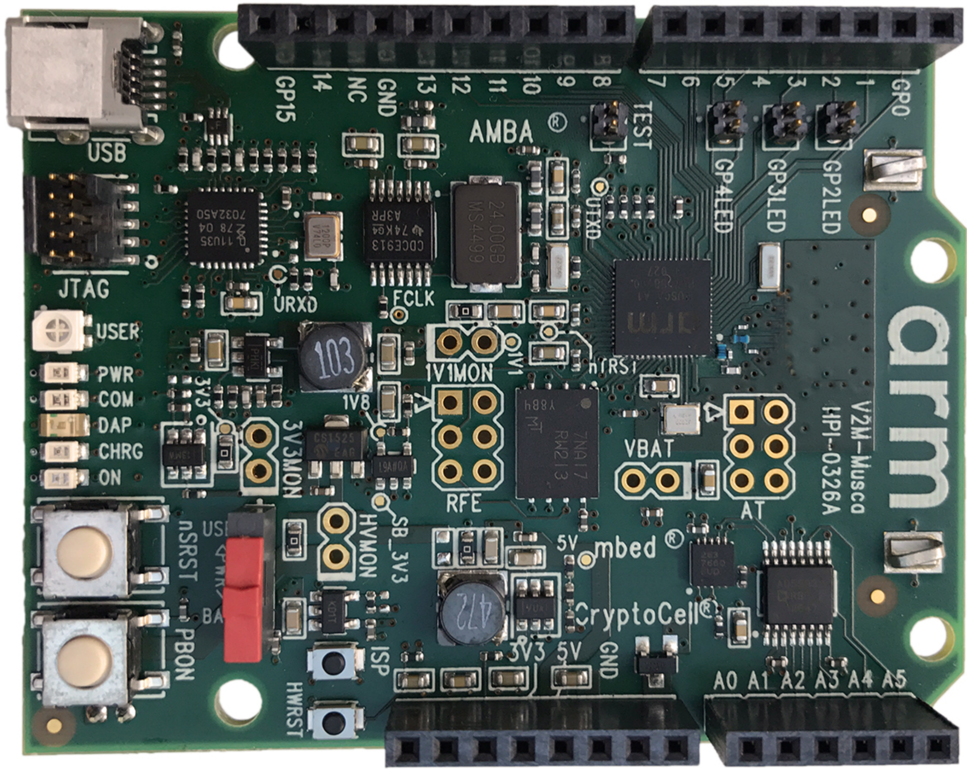
Ask for a Musca-A board!

Musca-A test chip

PSA development platform



Musca-A boards

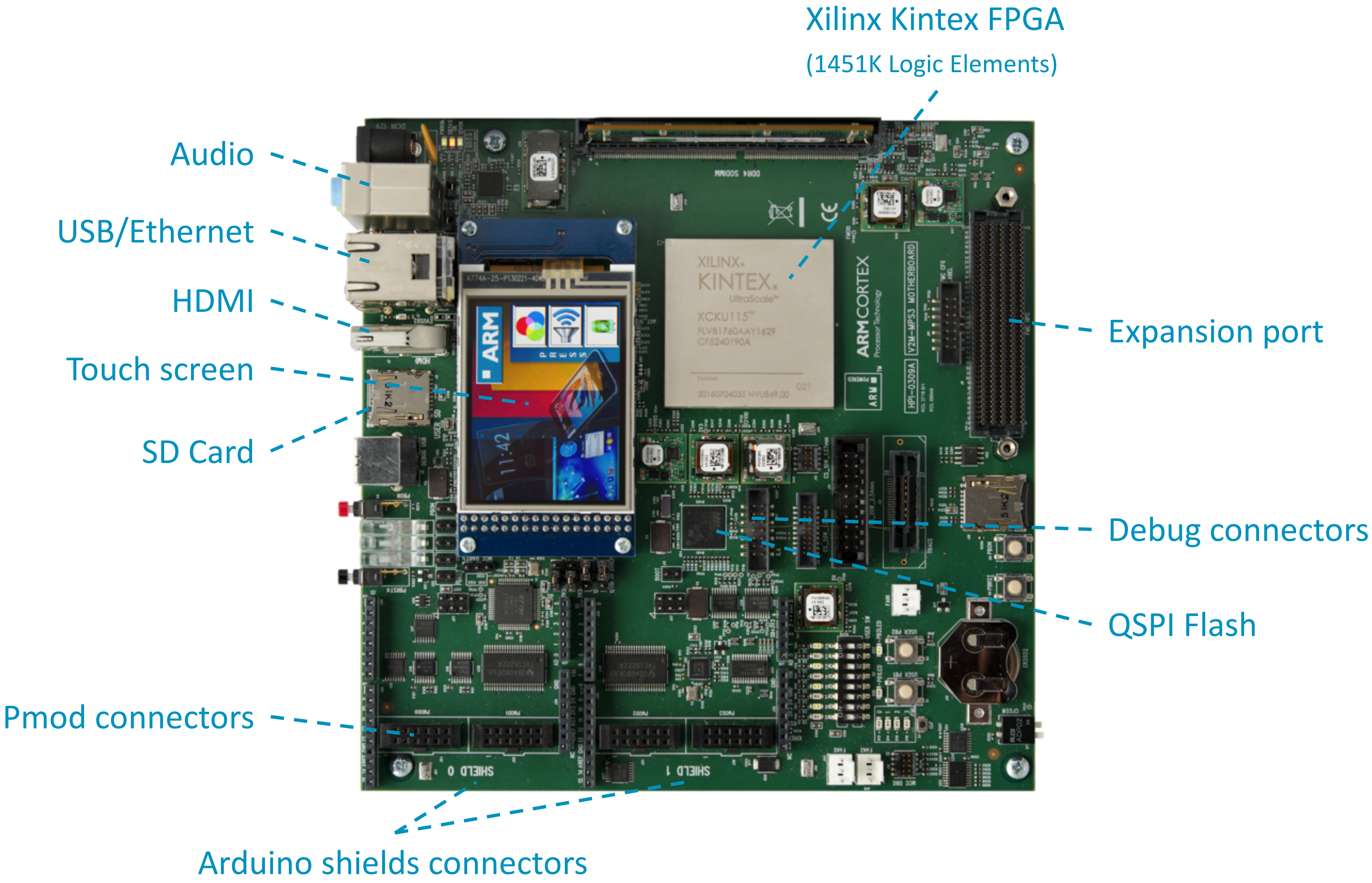


Prototype with MPS3 FPGA Board

Prototype IoT systems

- **SSE-200 subsystem** “black box”
- Add your logic on the FPGA
- Many connectors

New!



Xilinx Kintex FPGA
(1451K Logic Elements)

Audio

USB/Ethernet

HDMI

Touch screen

SD Card

Expansion port

Debug connectors

QSPI Flash

Pmod connectors

Arduino shields connectors

Conclusion

Conclusion

Loan a

Musca Board!

www.arm.com/musca

Arm invests in secure IoT solutions

- System approach – HW, SW, services, tools
- Pre-integration

Get involved!

- Participate in PSA
- Tools are available to help you develop

Thank You!

Danke!

Merci!

谢谢!

ありがとう!

Gracias!

Kiitos!

arm