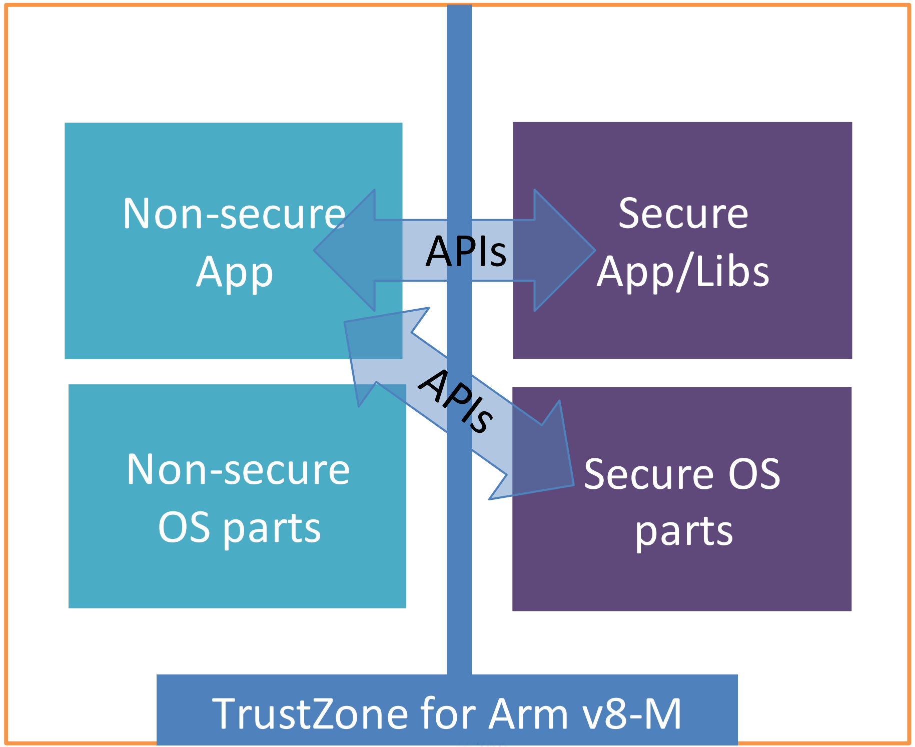
Attestation Roadmap

Mathias Brossard
mathias.brossard@arm.com

W3C Workshop on Strong
Authentication & Identity
December 10th and 11th, 2018

Platform Security Architecture (PSA)

- IoT security desperately needed.
- PSA aims to offer guidance + designs + software
- Open Source project: Arm Trusted Firmware-M
- Arm v8-M with TrustZone support
- APIs currently being defined
  - Crypto API published
  - Attestation API planned for 1Q 2019



Non-secure App

APIs

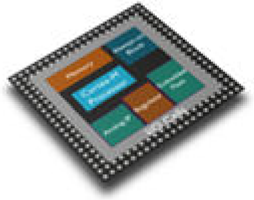
Secure App/Libs

Non-secure OS parts

APIs

Secure OS parts

TrustZone for Arm v8-M



Attestation

- Many existing attestation efforts:
  - Trusted Computing Group (TCG): Trusted Platform Module (TPM)
  - Android
  - FIDO
  - Global Platform
  - …
- Expressed interest for some convergence towards IETF EAT
  - CWT / JWT based container
  - CWT preferred in constrained environments (token size, RAM/Code requirements)

Roadmap

- EAT is the starting point
- Interoperability Model
- Trust Model(s)
- Protocols
  - Remote Attestation
  - Integration with Enrollment / Credentialing / On-boarding
  - Integration with Authentication
  - Integration with Authorization

Parting thoughts

- Increasingly disaggregated systems (Cloud, IoT, Web) with many components.
- Attestation is a building block for trust in connected systems.