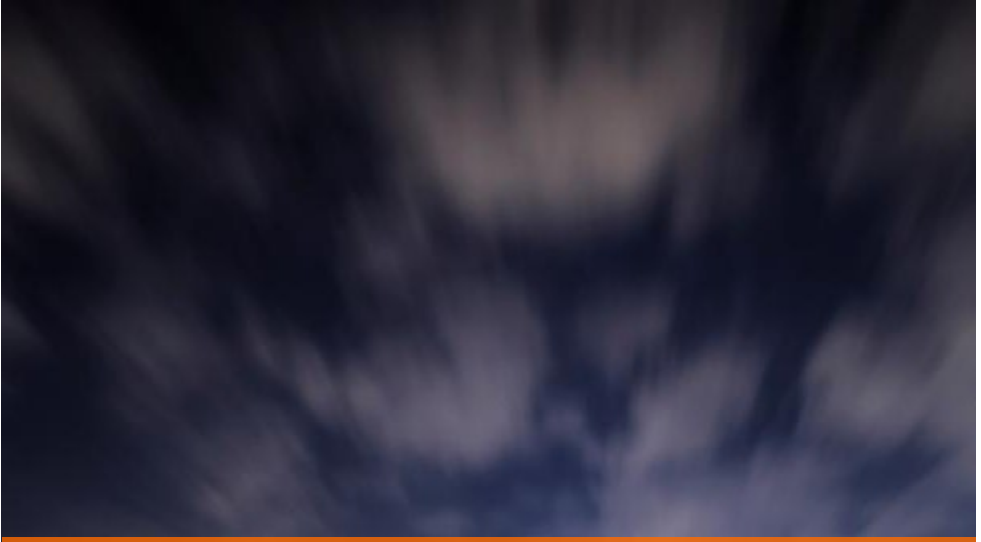
安谋中国

符合PSA的星辰处理器和山海解决方案

王骏超

安全技术市场总监

2020年9月



目　录
CONTENTS

安谋中国

01

PSA 认证介绍

安谋中国

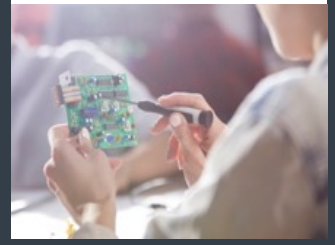
Platform Security Architecture & PSA Certified

Analyze

Threat models & security analyses

Architect

Hardware & firmware architect specifications



Implement

Firmware source code

Certify

Independently tested

psacertified™

Certification scheme with three levels

Aligned with NIST & ETSI

Choose silicon with a RoT with right level of security robustness

安谋中国

Easy to Understand Scheme

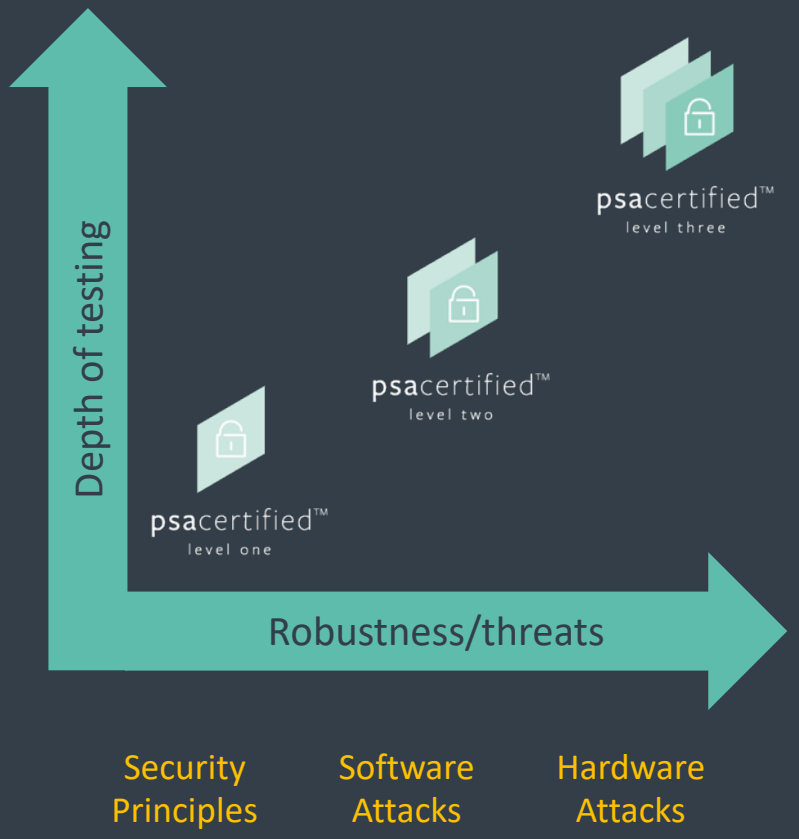
psacertified™

PSA Certified provides three progressive levels of security assurance/robustness

psacertified™
functional API

PSA Functional API Certified enables the ecosystem through a consistent high-level interface to the PSA-RoT

PSA Certified Levels



安谋中国

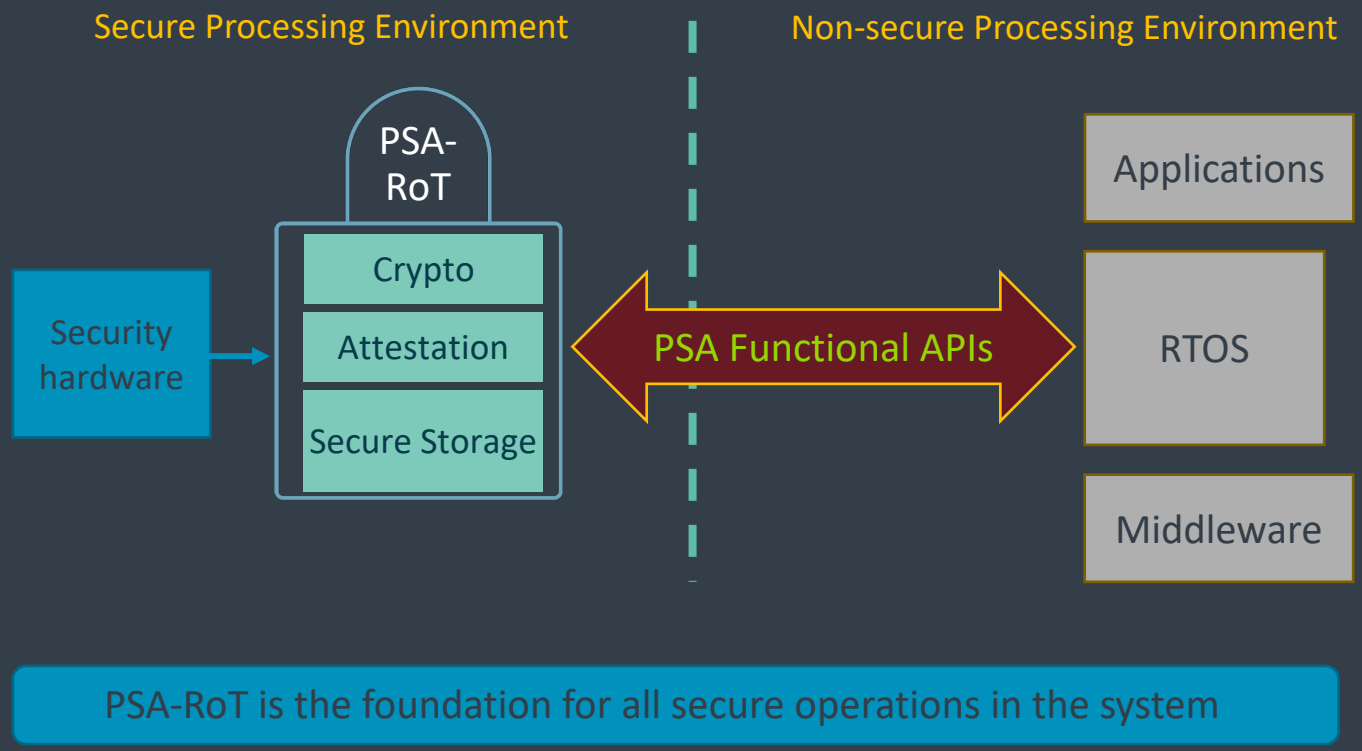
Simplifying Security Adoption

PSA Functional API Certification

Fast time-to-market by abstracting security complexities

Reduced fragmentation by using widely available security APIs

Lower total cost of ownership, maximizing ROI through re-use of APIs



安谋中国

PSA Certified Level 1

For device makers, software platforms and chip vendors

- Under 50 questions based on PSA 10 Security Goals, IoT threat models, government requirements and laws
- Can be filled in one go or as separate sections
- Quick and straight-forward – fill in and review with a PSA Certified test lab

New industry alignment mapping to:

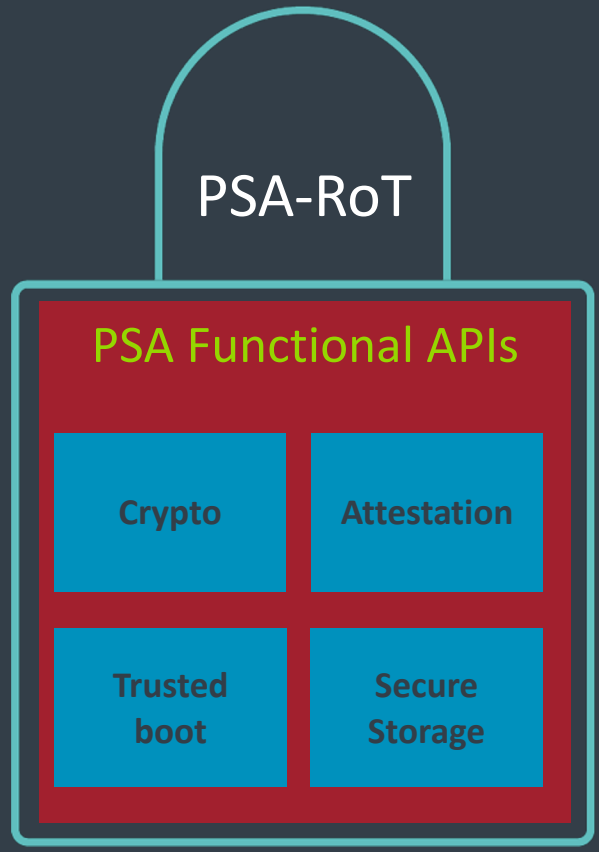
- **EN 303 645**
- **NIST 8259A**
- **SB-327**

安谋中国

PSA Certified Level 2

Lab-based evaluation of the PSA Root of Trust (PSA-RoT)

- Assurance against scalable remote software attacks
- White box evaluation against the PSA-RoT Protection Profile (nine security requirements)
- For chip vendors
- Time-limited evaluation



安谋中国

PSA Certified Level 3

- Adds physical attacker threat as well as software attacks
- Higher attack potential (21 vs. 16 for Level 2)
- 35-day evaluation to allow for physical attacks including glitching and side-channel attacks
- Two equivalent Evaluation Methodologies (EM)
  - CSPN style (existing)
  - GlobalPlatform's SESIP (new)
- Draft documents available now for lead partners

psacertified™
level three

安谋中国

PSA Certified & GlobalPlatform

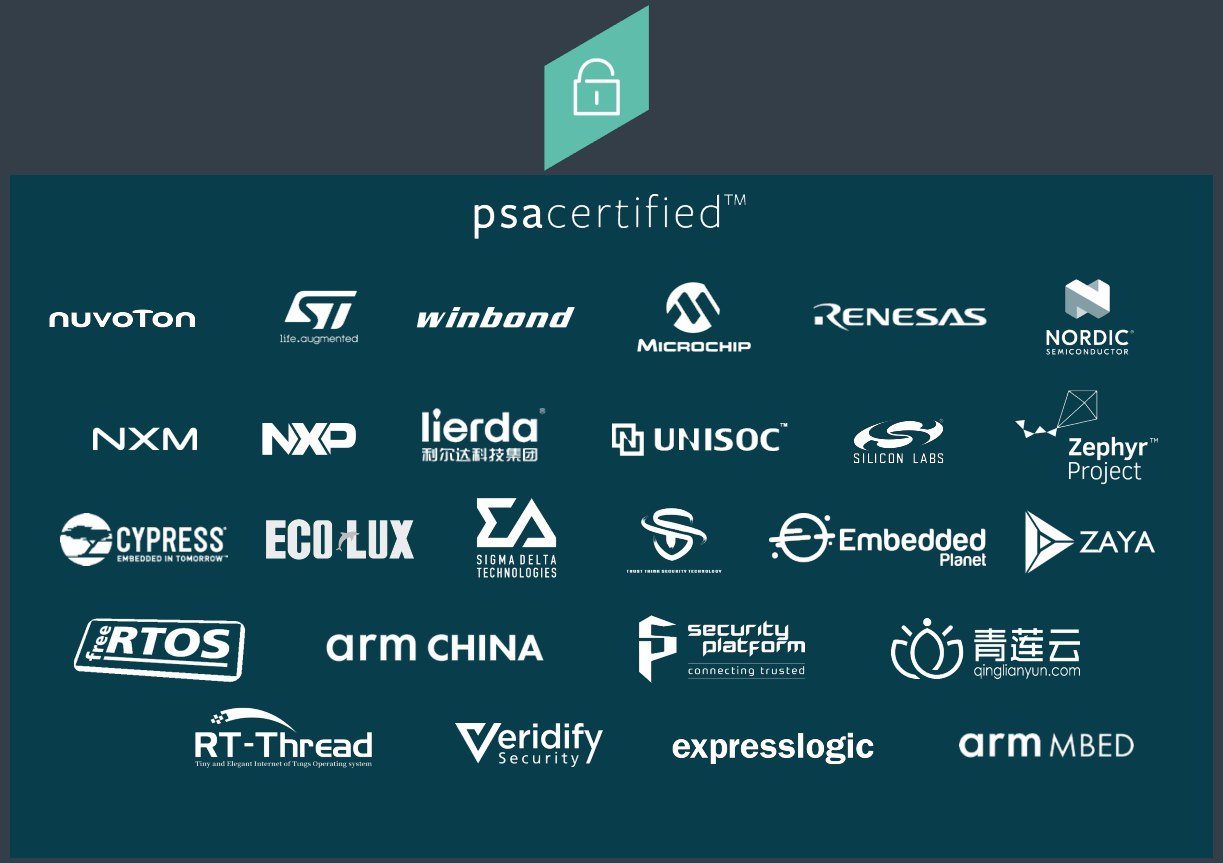
- PSA Certified Level 2 and PSA Certified Level 3 are currently based on CSPN style evaluation
- NEW - PSA Certified will provide an option to use GlobalPlatform SESIP based Evaluation Methodology from Level 3
- OEMs can opt to do a SESIP evaluation of other parts of the platform /device and make use of the already evaluated RoT security requirement
- Arm donated a Common Criteria PSA-RoT (MCU-RoT) Protection Profile to GlobalPlatform for partners wanting to use Common Criteria

安谋中国

A Growing Ecosystem of Support

PSA Certified is healing IoT security fragmentation and making life easier for IoT developers and device manufacturers

- Momentum continues to build
- Majority of the top 10 chip vendors
- Over 40 PSA Certified products



安谋中国

Join the PSA Certified Ecosystem

Access free resources and begin your certification journey today

psacertified™
level one

Download the questionnaire

Follow our step-by-step guide

psacertified™
level two

Download the PSA-RoT Protection Profile

psacertified™
level three

Contact PSA Certified

psacertified™
functional API

Download the step-by-step guide

Access the PSA Functional APIs

psacertified.org/resources

安谋中国

In Summary

Defragmentation will drive the IoT opportunity

PSA Certified can offer best practice and a level of assurance

Trust and security builds markets

Find Out More

- PSACertified.org
- Follow us on social media: @PSACertified on Twitter, LinkedIn and YouTube
- Get in touch

安谋中国

02

星辰处理器

安谋中国

星辰处理器(STAR-MC1)支持最新的Armv8-M架构

Armv6-M

Armv6-M ISA
NVIC (max 32 IRQs)
JTAG/Serial Wire
MTB
MPU
WIC

Armv7-M

Armv7-M ISA
SIMD/DSP
FPU (SP)
NVIC (max 240 IRQs)
Memory Exclusives
Divide Enhancement
'XOM' Support
ETM

Armv8-M mainline*

Armv8-M ISA
NVIC (max 480 IRQs)
Coprocessor interface
TrustZone
Enhanced MPU
Stack Limit Checking
Enhanced Debug
Customizable Instruction

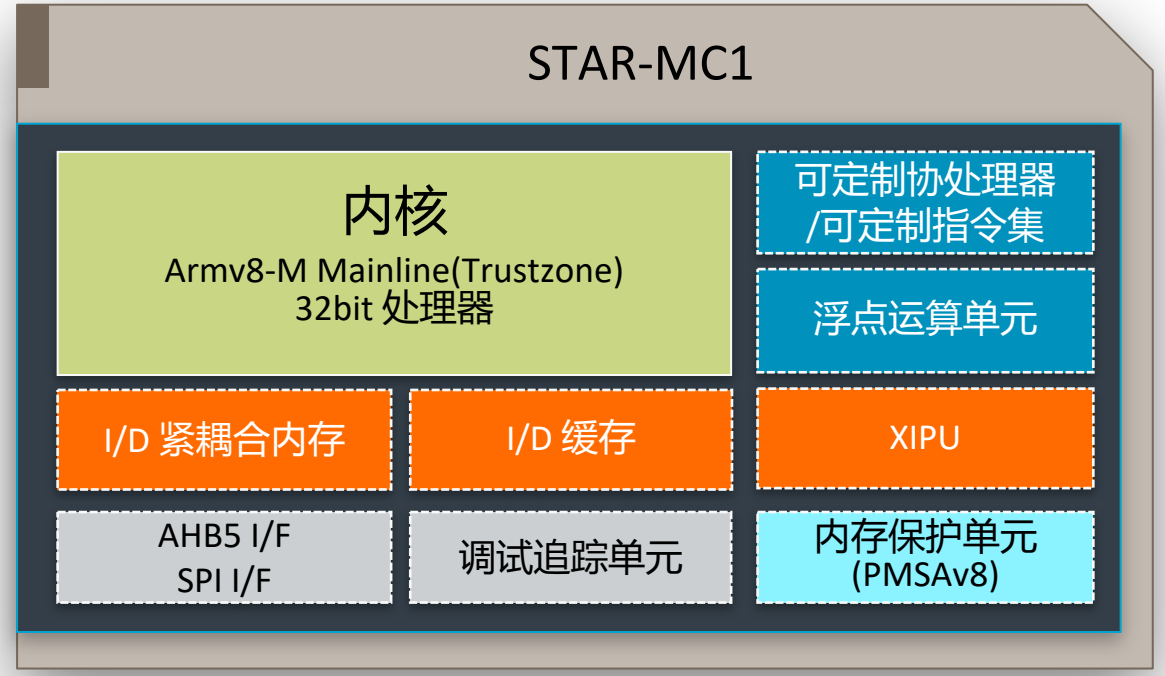
*The purple parts are additional features over Armv8-M baseline

STAR-MC1，面向智能互联安全IoT应用需求的处理器

高效计算

- 性能与功耗均衡的配置
- 1.50 DMIPS/MHz & 4.02 Coremark/MHz
- 特有的DSP指令和浮点计算单元

最新指令集带来20%同主频下性能提升



灵活扩展

- 引入TCM、Cache和Prefetcher增强存储系统效率
- 可扩展接口允许客户灵活定义与处理器耦合的协处理器或者指令集，提升系统效率

内存子系统数量级提升系统效率

全球同步首发Arm可定制指令集处理器

Trustzone 进一步提升系统安全

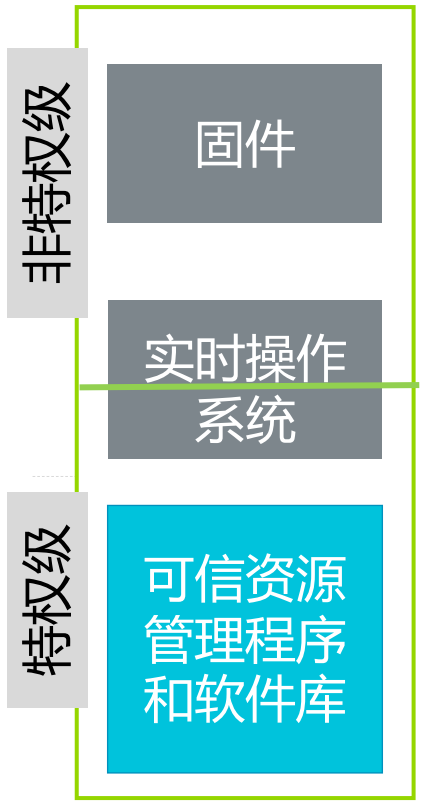
安全基石

- 基于Trustzone的系统级安全方案带来整个系统的安全能力提升
- 针对安全/非安全区，都有专门的内存保护模块进行保护

安谋中国

Trustzone: 简化软件设计，提升安全级别

传统嵌入式安全软件系统



资源隔离

代码和数据放在一个内存区域，有很宽的攻击面

切换开销

由操作系统管理，上下文切换代码和延迟都比较大

软件接口

各家自定义的软件接口，难以统一开发

基于Trustzone的嵌入式安全软件系统

资源隔离

资源物理隔离，非安全区对安全区所有资源不可见

切换开销

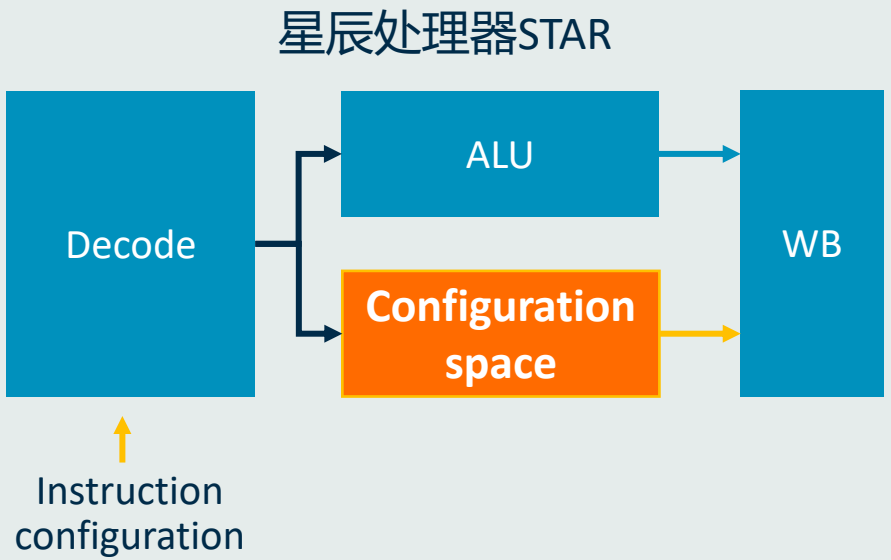
类似“函数调用”的方式切换，极小的切换开销

软件接口

标准PSA接口，业界统一的安全测试规范

安谋中国

可定制指令集： 提升性能，简化设计



基于最新的Arm Customizable Instruction技术

- ✓寄存器级直接访问
- ✓低延迟可定制指令可以显著提升系统效率
- ✓可与与现有的软件生态无缝集成
- ✓可以在不同的Arm架构处理器下灵活扩展
- ✓充分保护客户的软硬件知识产权

安谋中国

产品历程

17月

从立项到交付

30

授权客户

21

项目进行中，
其中7项目已流片

7

广泛应用于通用MCU，互联芯片，系统控制，汽车电子，存储，定位，传感器控制等领域

安谋中国

生态系统支持

工具链
- DS 2020.0
- Keil MDK Ver 5.29
- IAR EWARM 8.42.
- Lauterbach TRACE32 (R.2020.02)

and more…

编译器:
- GCC (Version 8-2018-q4-major or newer)
- Arm Compiler 6 (Version 6.0 or newer)
- IAR Compiler: (Version 8.42 or newer)

操作系统
- MbedOS
- FreeRTOS
- Zephyr

and more…

仿真器:
- ULINPRO, ULINK2 and DSTEAM:
- SEGGER: JLINK V9/V10

and more…

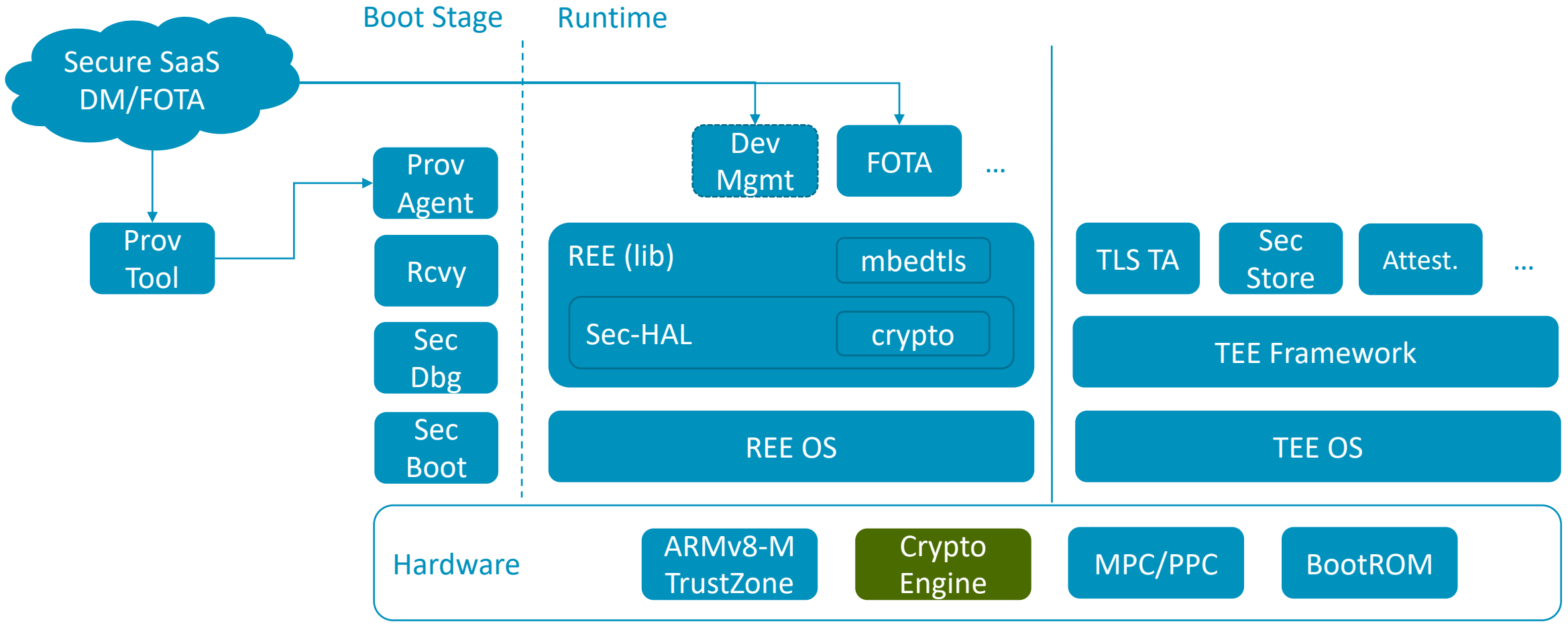
安谋中国

03

山海安全解决方案

安谋中国

山海安全解决方案



安谋中国

密码引擎

Algorithm	
Symmetric	AES128/192/256 w’ ECB/CBC/CTR/CCM, SM4.
Asymmetric	RSA (up to 4096b), ECC (up to 521b), SM2.
Digest	SHA1/224/256, SM3.
Key Management	
Key ladder	3-level AES derivation.
Lifecycle Mgmt.	
Lifecycle	4-level monotonic lifecycle: CM, DM, DD, DR.
TRNG	
Random number	20-chain ring oscillators.
OTP	
CE specific OTP	Secure and non-secure.
User-defined spec. OTP	Secure and non-secure.
PUF	3rd-party PUF integration, optional.

- Crypto engine is a key component for platform security.
  - TrustZone aware.
  - Key management: key generation, maintenance, usage, revocation.
  - Cryptographic acceleration: digest, symmetric, asymmetric, key exchange, SMx (国密).
  - TRNG (True Random Number Generator).
  - Fully configurable – secure/non-secure host number, algorithm …
  - OTP, support PUF.
- Arm China provides the API of mbedtls as the interface of crypto engine.

总结

- 星辰是安谋中国研发的，低功耗智能安全IoT应用需求的第一款CPU IP
- 同步首发Arm最新的架构和CPU设计技术，同时引入了Arm的IP设计质量标准
- 被中国客户接受并广泛用于各个嵌入式领域
- 用产品践行中国智能科技生态领航者的愿景，与本土客户共同成长

Thank You！
谢谢！

安谋中国
中国智能科技生态领航者