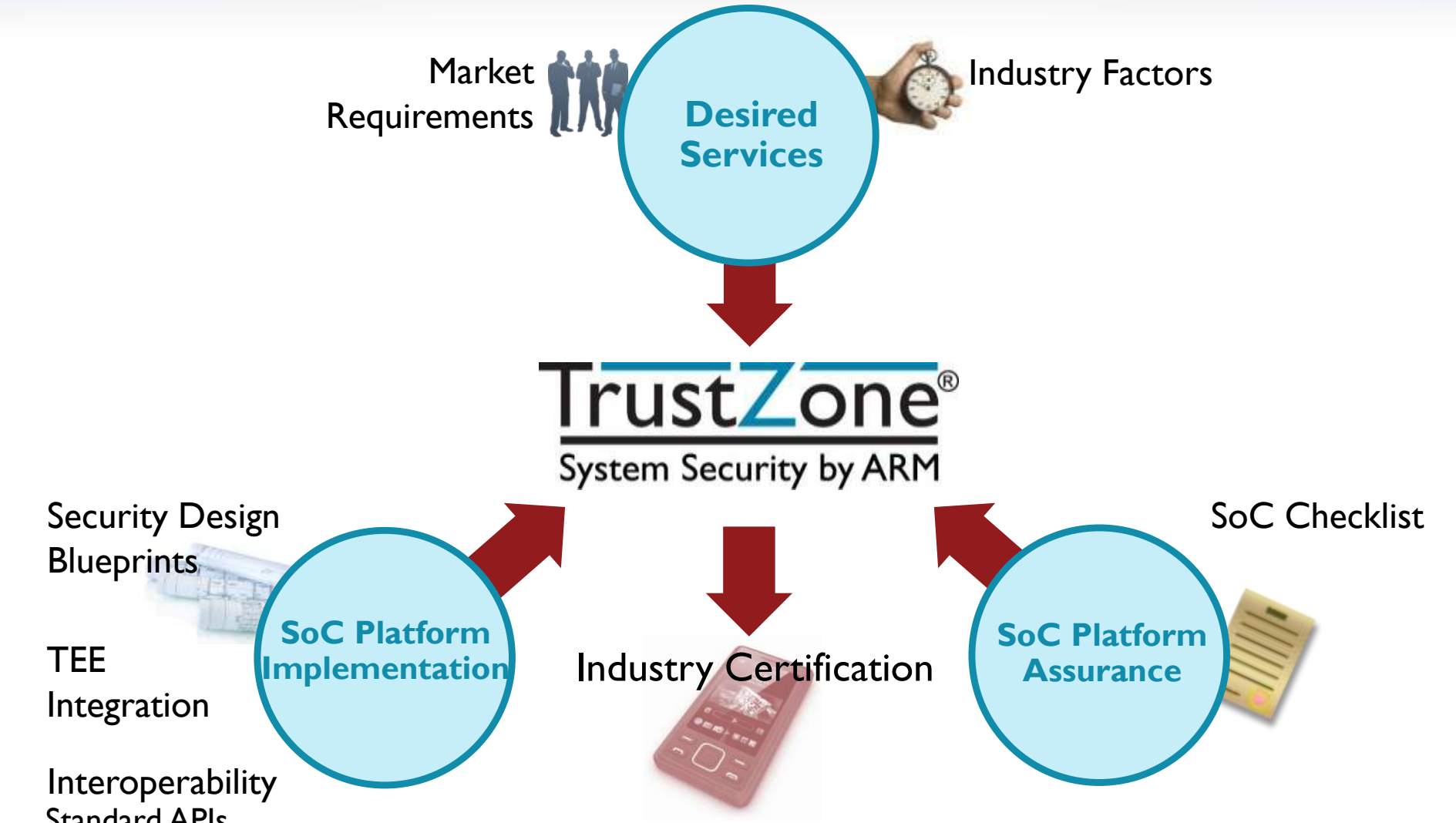
TrustZone Ready Program

Mapping security use cases to SoC requirements

TrustZone® Ready Program

- Partner Enablement
  - A cohesive set of design documents and checklists providing best practice SoC security requirements, checklists and market requirements – primarily for silicon partners, OEMs and those with security requirements
- Aligned with industry certification schemes
  - Focus on helping silicon and secure OS partners build correct system
  - Engage existing certification bodies to align TrustZone Ready with their program(s)
- The focus of the program is
  - Mapping high level security requirements from multiple industry stakeholders to silicon requirements
  - Providing the right security foundations for easy Trusted OS integration
  - Means for TrustZone Ready partners to move through certifications quicker

Introducing: TrustZone Ready Program



Requirements Flow

Security Use Cases

SoC Requirements

TrustZone Ready Enablement Program

Service Provider

Requirements

- Security Capabilities
- Application functions
- System and infrastructure
- Performan
- ...

Generic Secure Service

Requirements

- Device Security Functions
- Robustness rules
- Provisioning and Infrastructure rules

Generic Device Security

Requirements

- Platform Security Guidelines
- Application level security
- Provisioning and key infrastructur

Security PDDs

Requirements

- Trusted board boot
- Trusted Base System Architecture

ARM IP

Requirements

- ARM IP Licences

TrustZone® System Security by ARM

Industry Security Certification Alignment

PAYMENTS COUNCIL
DRIVING CHANGE IN UK PAYMENTS
EMVCo
HDMI HDCP
Microsoft PlayReady®

GLOBALPLATFORM
THE COMMON CRITERIA
EVALUATION AND VALIDATION SCHEME
NIST
TRUSTED COMPUTING GROUP

sepia

OMTP OPEN MOBILE TERMINAL PLATFORM

ARM IP enables partner to reach certification

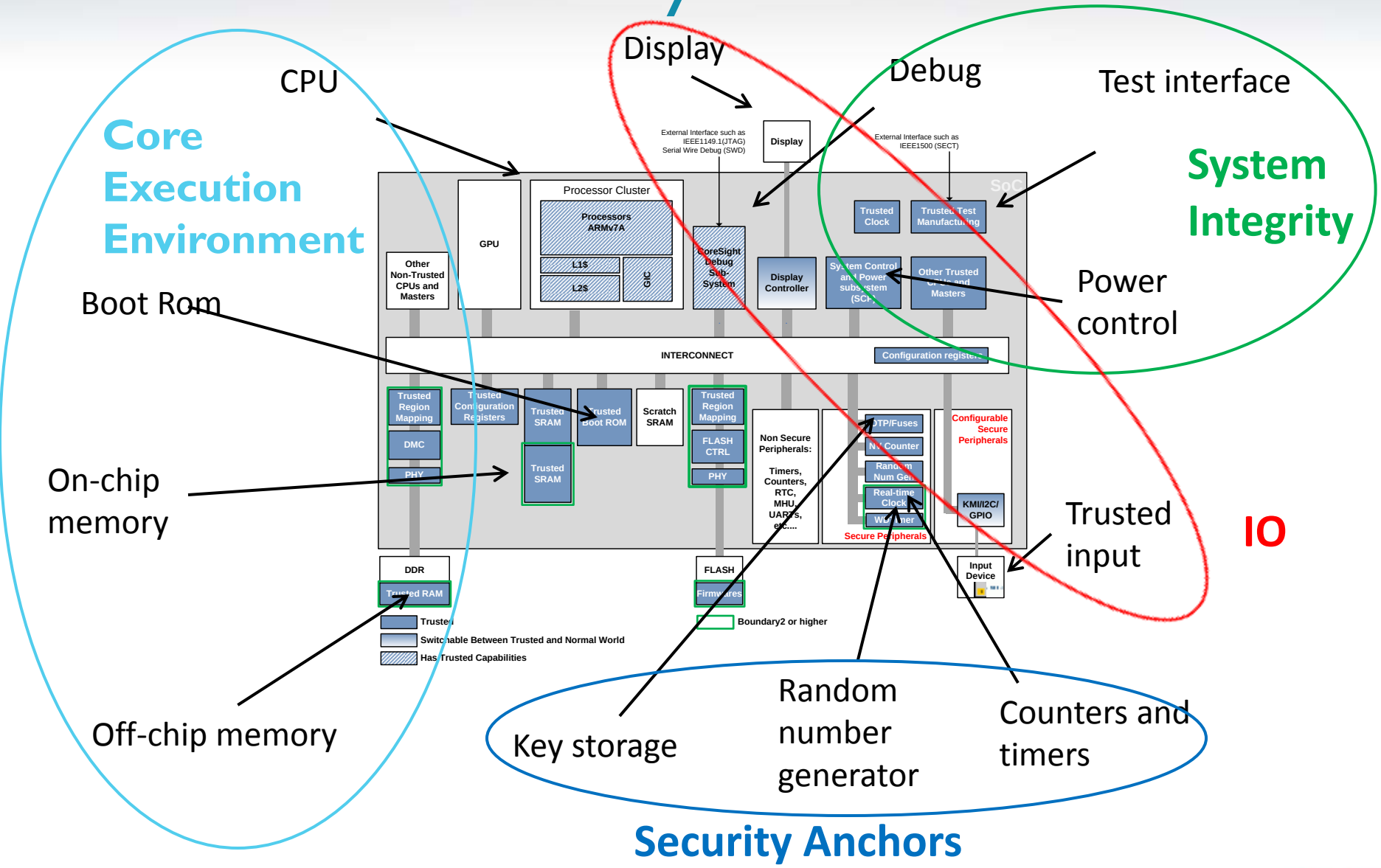
Roadmap

- Regular updates
  - Delivered by dropzone
- Released documents:
  - TBSA-Client1 (DEN0007)
  - TBBR-Client (DEN0006)
- Draft proposals
  - Client-2
  - Server

Designing the Right Chip: We Can Help

- ARM is making it quicker and easier to develop a SoC with the right security features:
  - Market requirements mapped to Security design blueprints
  - Checklists
  - Discussions with ARM security team
  - Training

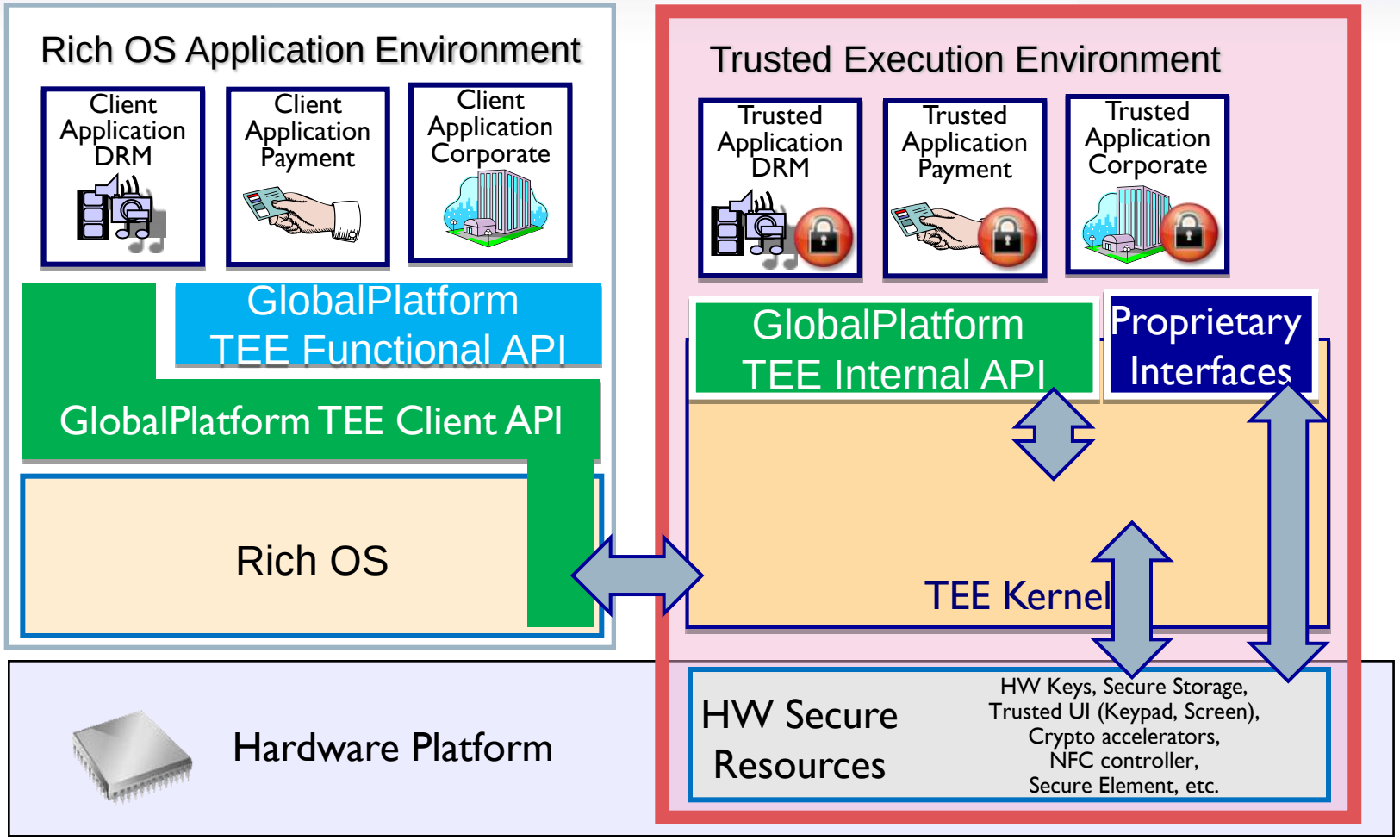
ARM Trusted Base System Architecture



TrustZone is System Wide Security

- Complete TrustZone solution consists of:
  - TrustZone-Enabled CPU Core (eg Cortex®-A5 core)
  - TrustZone secure firmware running on the CPU core
  - TrustZone-Aware L2 cache controller (if L2 cache is used)
  - TrustZone-Aware AXI Interconnect Fabric
  - Secure-World Memory (in addition to Normal World memory)
  - TrustZone-Aware Interrupt Controller
  - On-SoC ROM protection for Trusted Boot Code
  - Off-SoC Memory Address Space Control
  - Secure Debug Control – Disable debug of Secure World

GlobalPlatform Defining API Standards



Global Platform Standards Status :

Done

Future Development

Evolved Enablement Story

- TrustZone Ready aims to provide the hardware foundations for a TEE, payment services, Content Protection, Enterprise use cases
- GlobalPlatform are working on Compliance and Certification and ARM intends that TrustZone Ready can help accelerate partners route to certification
- TrustZone Ready will make it faster and easier to port a Trusted OS and achieve certifications

Summary

Security & Trusted Services is a new opportunity

- Leading OEMs and MNOs are already implementing and deploying
- We are working with lead partners who are interested in enabling TrustZone/TEE enabled devices
- Lots of use cases and opportunity for differentiation
- Enterprise
- MNO
- Payment
- Content
- TrustZone Ready Program is a key enablement program helping ARM's partners achieve best practice platform security and unlocking new business opportunities