Thales and Trusted Computing

Adrian Waller
Thales Research, Technology & Innovation

October 19, 2018

Outline

- Who we are and what we do in Trusted Computing
- Drivers for Change
- Use Cases
- Emerging Requirements
- Conclusions

Thales and Security

AEROSPACE

SPACE

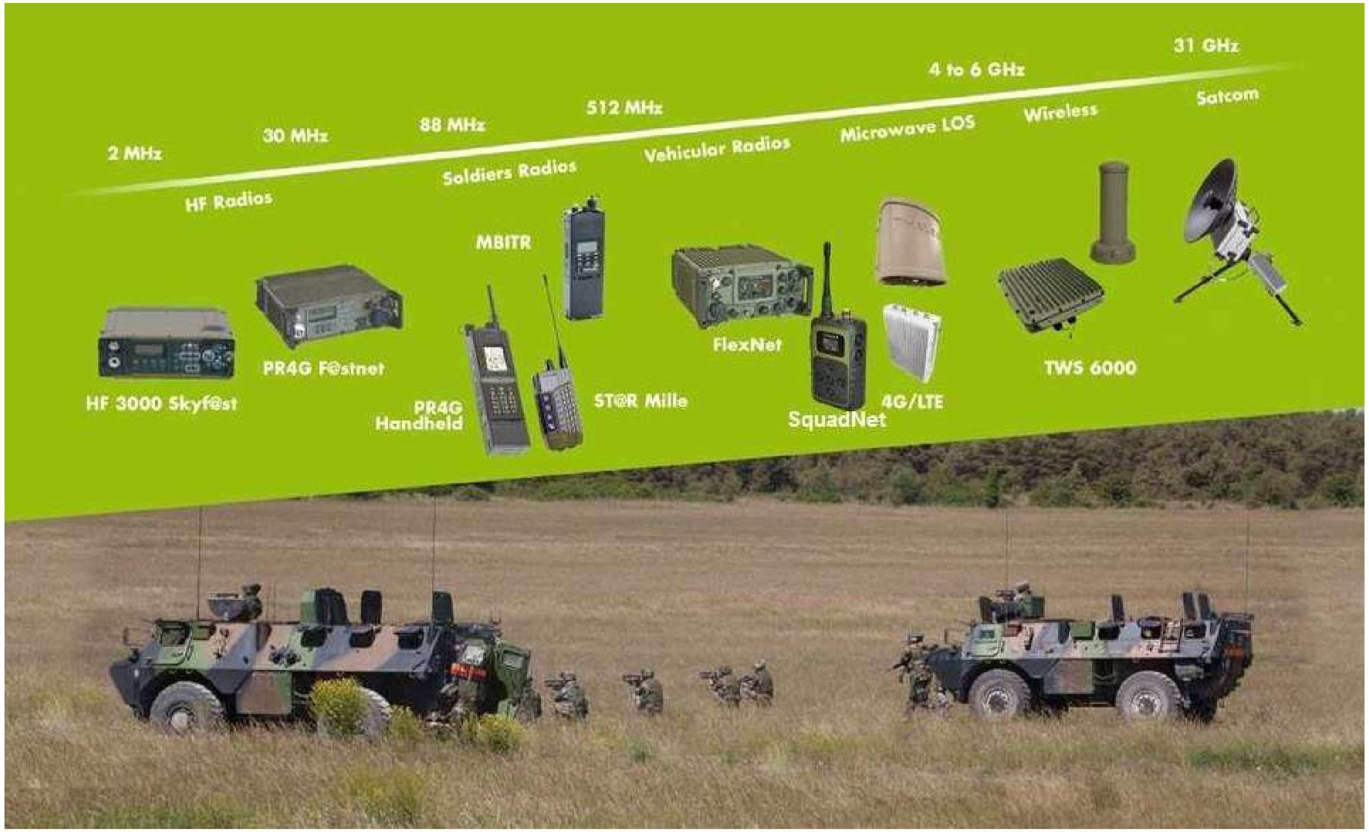
GROUND TRANSPORTATION

DEFENCE

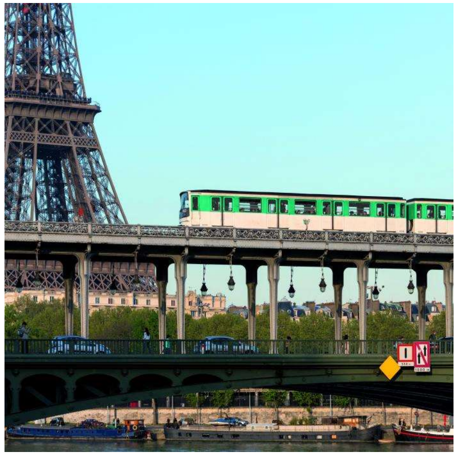
SECURITY

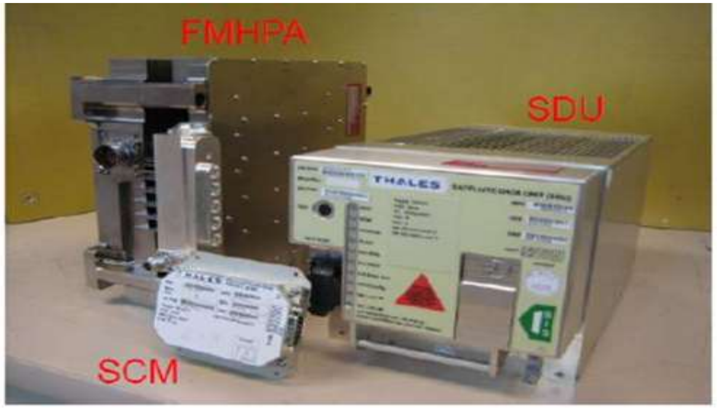
TRUSTED PARTNER FOR A SAFER WORLD

Thales Trusted Computing – Defence



Thales Trusted Computing – Commercial





How Did We Do Secure Systems

Basic Strategy

- Defend the Trusted Core
- Restrict Access
- Analyse in Depth
- Strength to Withstand a Prolonged Siege by a Determined Attacker

Cyesuta, https://www.flickr.com/photos/cyesuta/, Tunnels in Cardiff Castle, CC BY-SA 2.0

Becks, Edinburgh Castle (4945300869), CC BY 2.0

Strongpoints

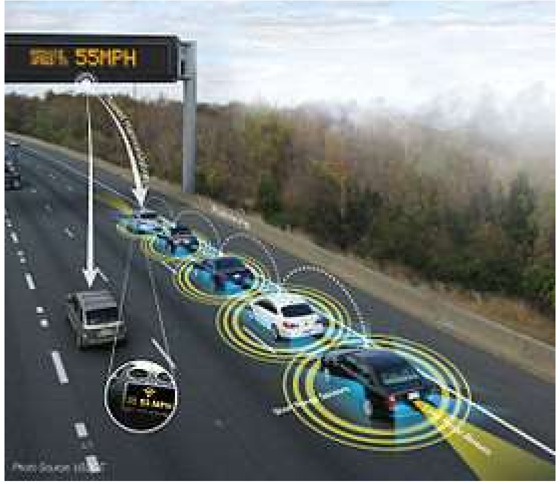
Protected Inter Strongpoint Supply Routes

Proactive Attack Against Threats

How Will We Need To Do Secure Systems

Basic Strategy

- Defend the Trusted Core
- Restrict Access
- Analyse in Depth
- Strength to Withstand a Prolonged Siege by a Determined Attacker

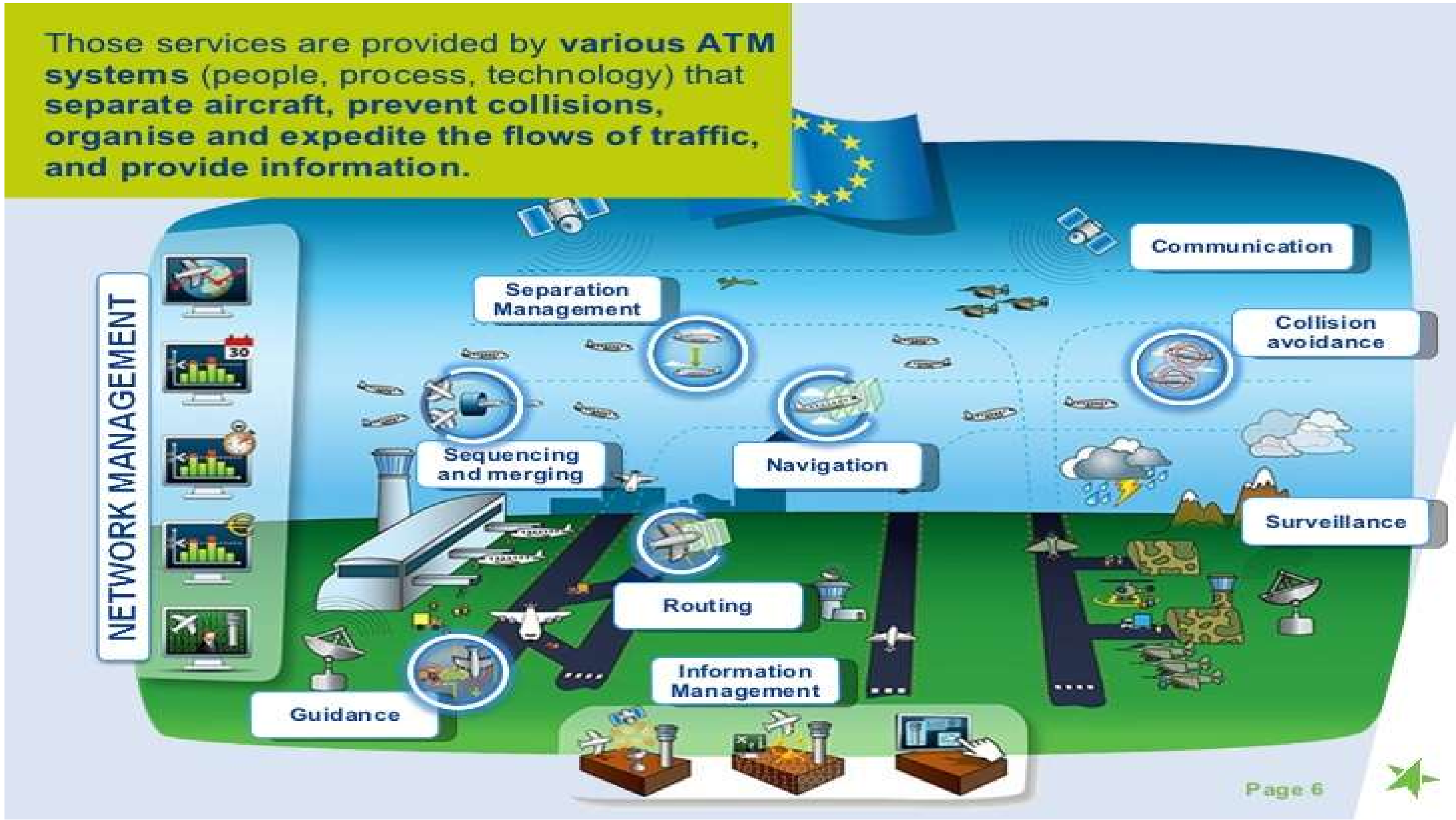


- Protected Inter Strongpoint Supply Routes
- Proactive Attack Against Threats

Let's Imagine That We've Done All That Correctly:

- **Architected.**
- **Coded.**
- **Analysed**

Another Example – Air Traffic Management



Those services are provided by **various ATM systems** (people, process, technology) that **separate aircraft, prevent collisions, organise and expedite the flows of traffic, and provide information.**

From SESAR general presentation https://www.slideshare.net/SESAREuropeanUnion/sesar-genpresfinal022011

Need for a new approach

- **Building trusted hardware from scratch is typically too expensive, and hard to change and support**
  - Difficult to respond to changes in requirements and threat landscape
- **Placing assurance in just a few, isolated, highly trusted points does not deal with problems in highly distributed systems**
  - The system that you are part of is constantly in flux. How does the baseline of a component or subsystem relate to this 'system'?
- **COTS world is significantly improving availability and assurance level of trusted hardware**
  - Low cost, well supported, easy to change (TPM, ARM TZ, Intel SGX, Smartcards,…)
- **This does not mean that trusted hardware is no longer useful, just that we need to change approach and use it in new ways**

Example of COTS – ARM TrustZone Based Trusted Execution Environment

Mobile devices with integrated HW security

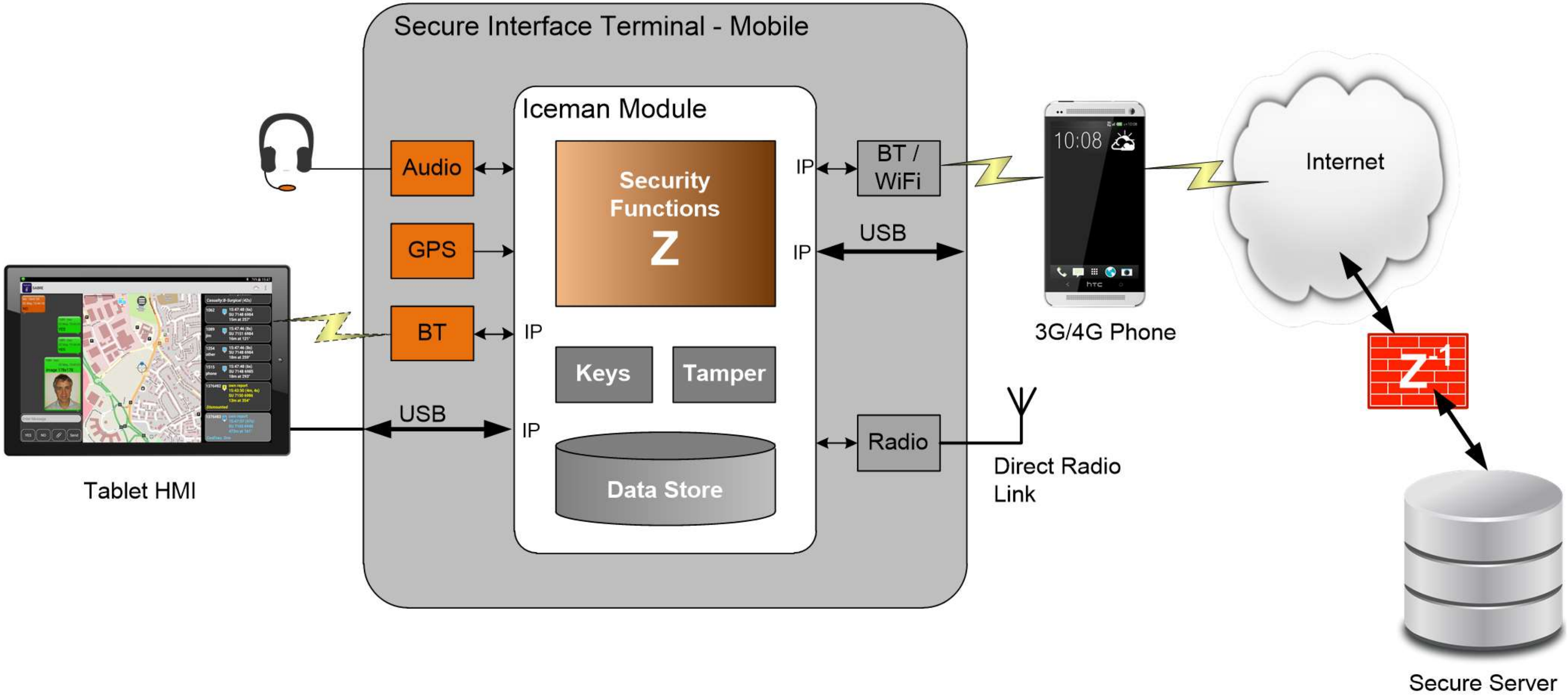
- Hardware root of trust (TrustZone)
  - Logical separation where the CPU has a secure instruction flag that puts it into the "secure world".
  - While in the secure world the "normal world" is put on pause until the execution has been complete.
- Integrity through Trusted Boot
  - A TEE can be seen as a secondary RoT, which is initialised by the primary RoT during secure boot

Use Cases

www.thalesgroup.com

THALES OPEN

Secure Communications – Iceman



Process separation – TPM for Guards

Trusted Platform Module

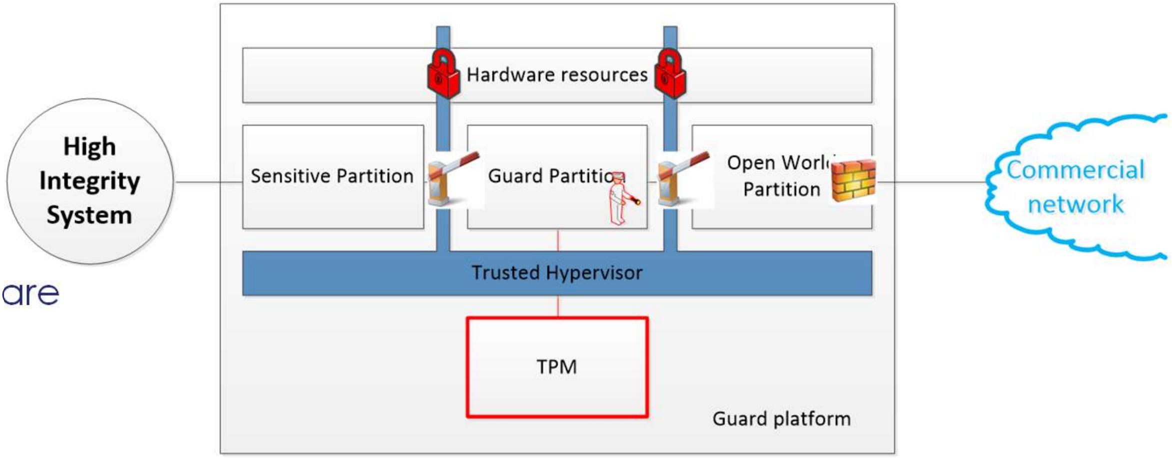
- Standard for crypto-processor
- Commonly used anchors of trust
- Available in many COTS platforms

Problem statement

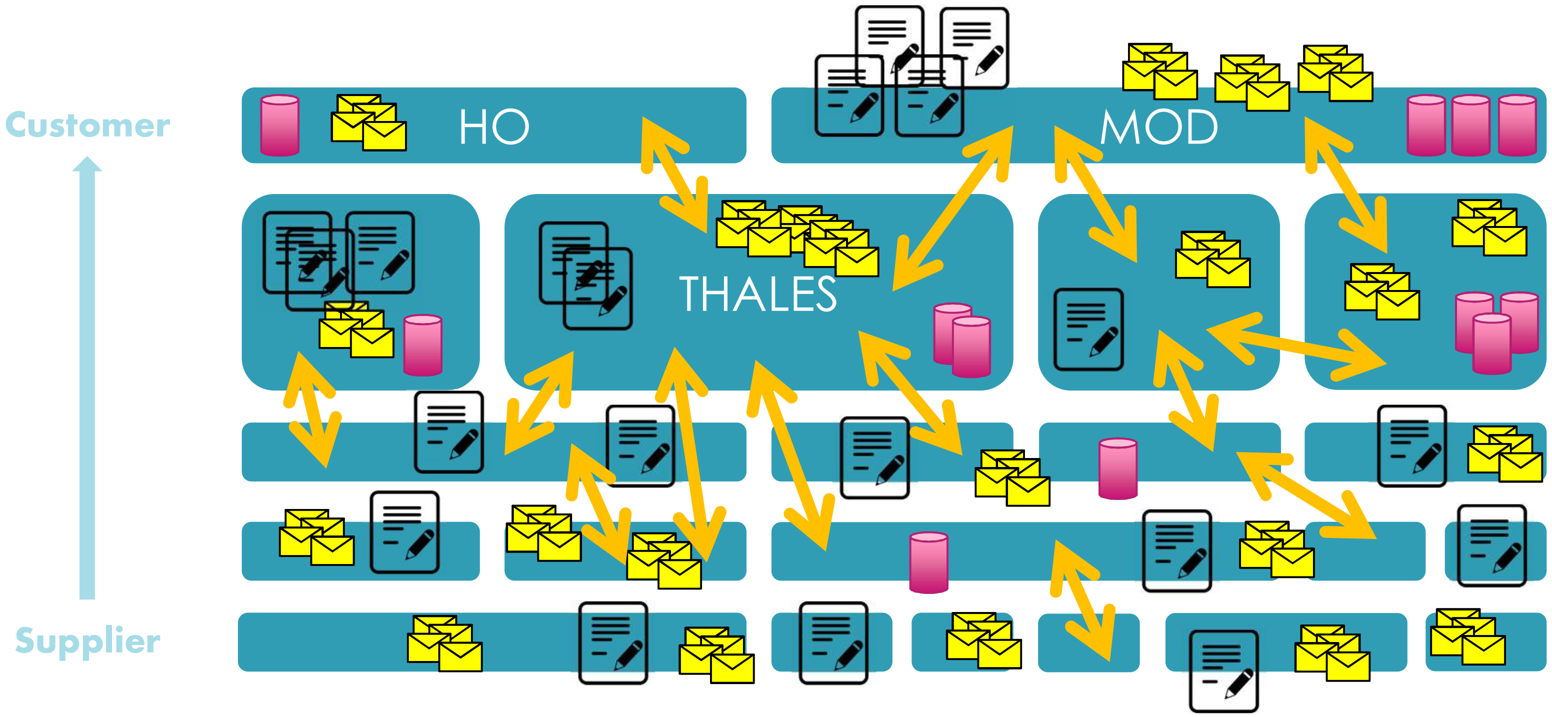
- Need Guard SW image to be integrity checked on boot
- Need root certificates to be integrity protected
- Need to check provided software images before passing to High Integrity System

Potential application

- Security Guard for critical software updates
  - Logically segregated partitions
  - Tightly controlled exchanges
  - Hardware support for security services (TPM)



Supply Chain Protection – Supply Chain Today



Supply Chain Protection – Counterfeiting

Risks of counterfeit semiconductors are often underestimated

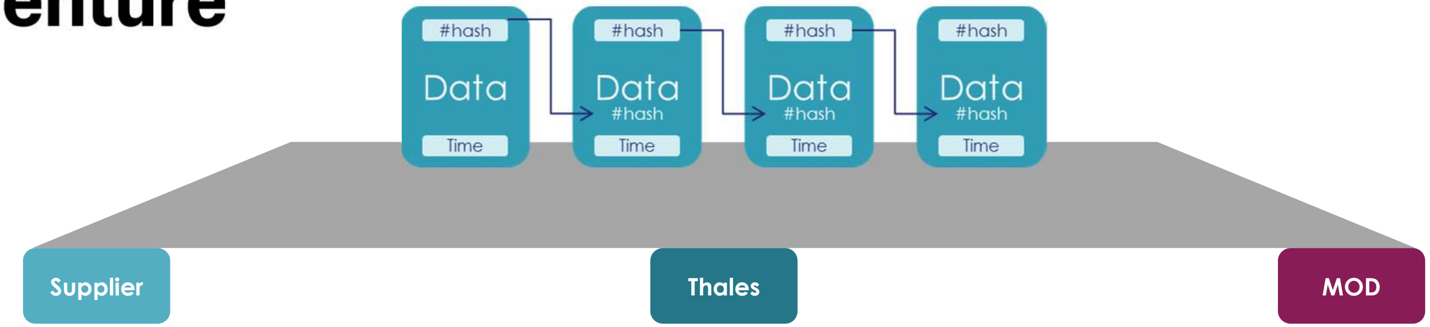
Have found their way into highly critical safety and security systems

- E.g. Train braking system
- Control System in Ballistic Missile Defence

Supply Chain Demonstrator – Trust Components

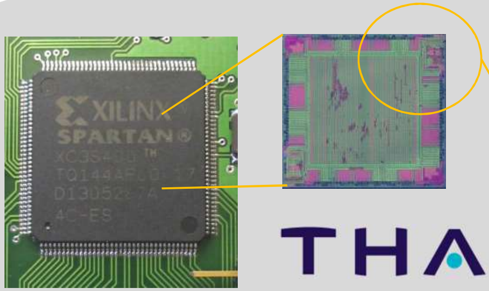
accenture

HYPERLEDGER



CHRONICLED

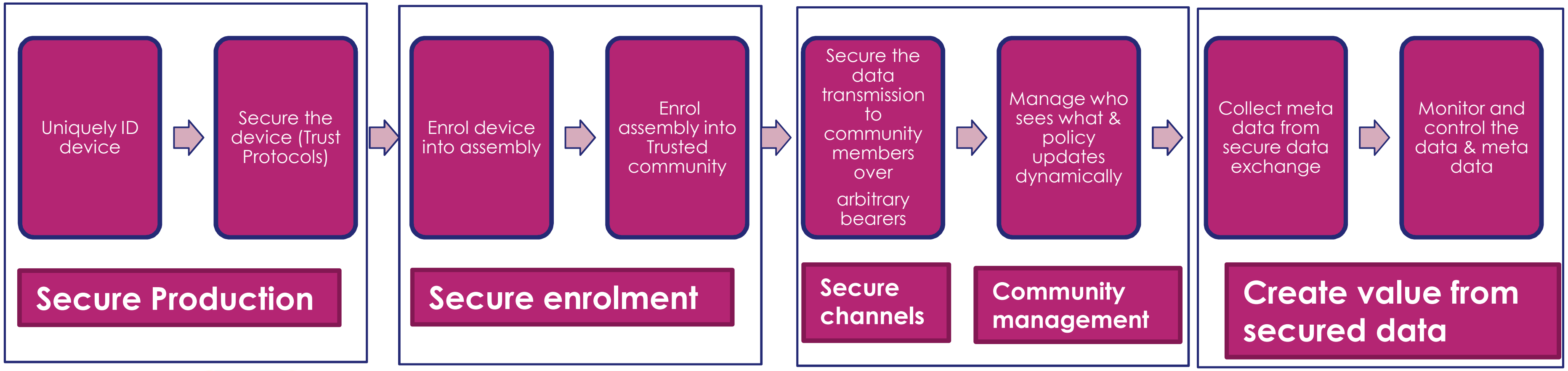
ethereum



Physically
Unclonable
Functions

THALES

Supply Chain Protection – What is T-Sure Identity?



Uniquely ID device

Secure the device (Trust Protocols)

Secure Production

Enrol device into assembly

Enrol assembly into Trusted community

Secure enrolment

Secure the data transmission to community members over arbitrary bearers

Secure channels

Manage who sees what & policy updates dynamically

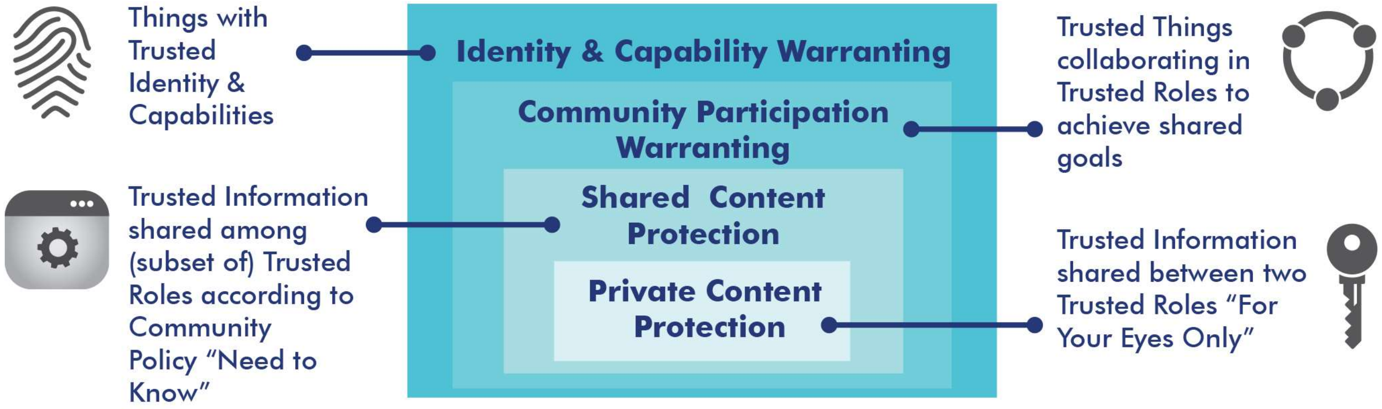
Community management

Collect meta data from secure data exchange

Monitor and control the data & meta data

Create value from secured data

Identity Warrant



Things with Trusted Identity & Capabilities

Identity & Capability Warranting

Community Participation Warranting

Trusted Things collaborating in Trusted Roles to achieve shared goals

Trusted Information shared among (subset of) Trusted Roles according to Community Policy “Need to Know”

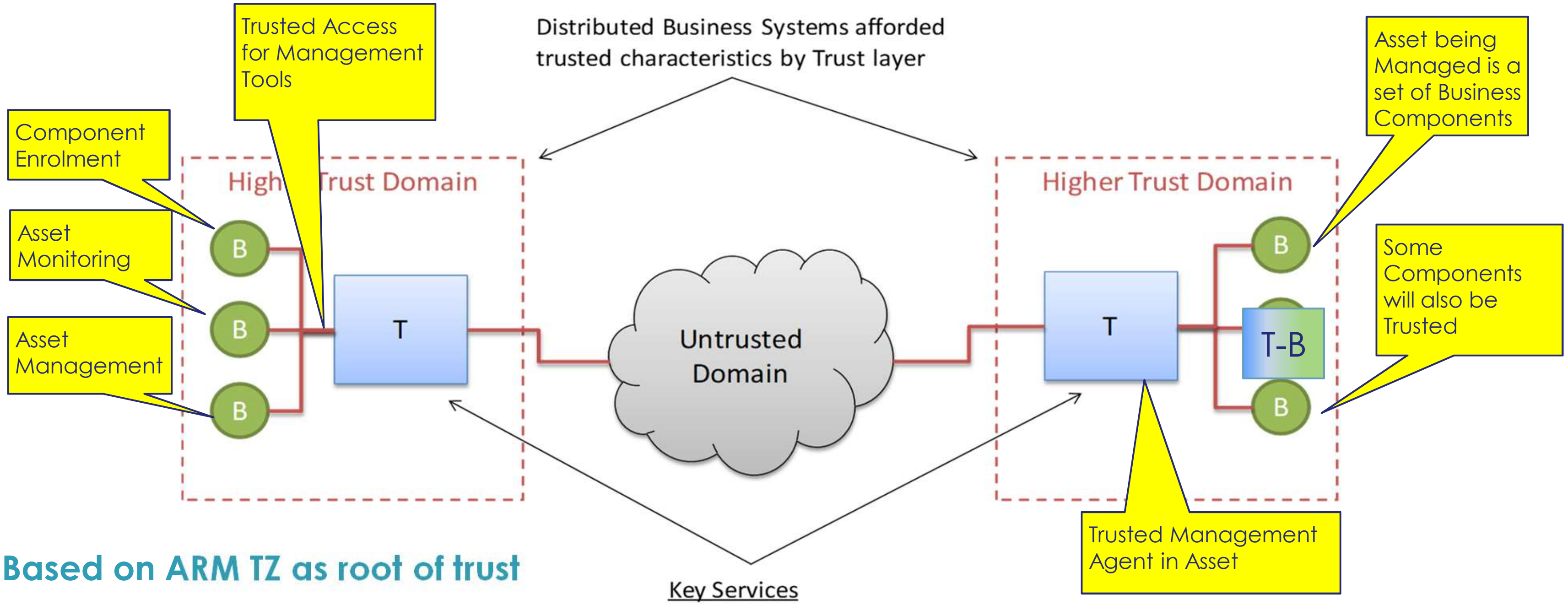
Shared Content Protection

Private Content Protection

Trusted Information shared between two Trusted Roles “For Your Eyes Only”

Remote Asset State Management

Entity Business Applications use Trust Services for dependability


Trusted Access for Management Tools
Distributed Business Systems afforded trusted characteristics by Trust layer
Asset being Managed is a set of Business Components
Component Enrolment
Asset Monitoring
Asset Management
Higher Trust Domain
B
B
B
T
Untrusted Domain
T
Higher Trust Domain
B
T-B
B
Some Components will also be Trusted
Trusted Management Agent in Asset

Based on ARM TZ as root of trust

Key Services

- Trusted Information Sharing
- Trusted Community Management
- Trusted State Management
- Trusted Audit

Emerging Requirements from Use Cases

THALES OPEN

Requirements for Trusted Hardware

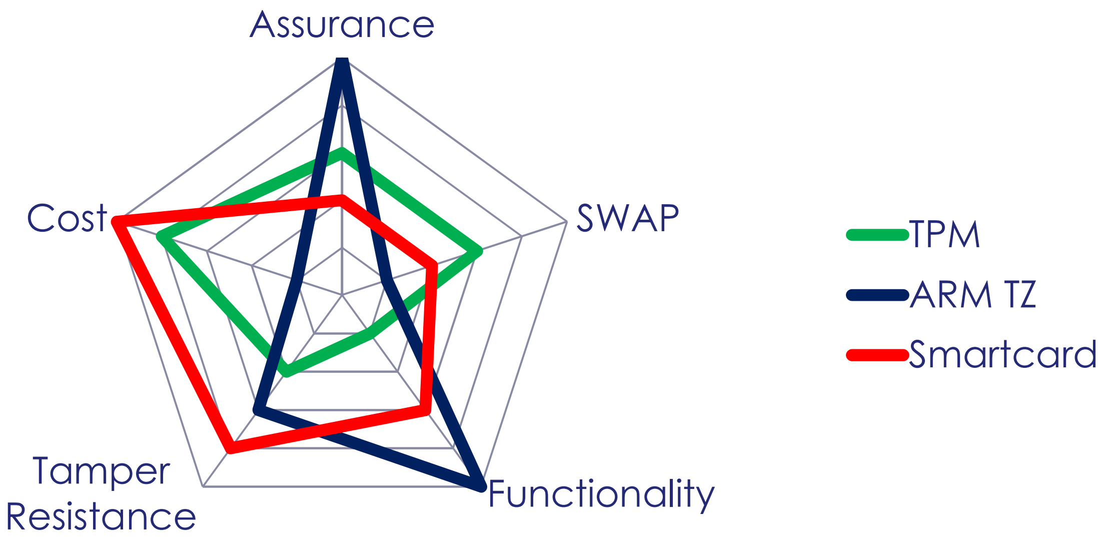
Functional Requirements

- Trusted boot and attestation
- Secure key storage (integrity and confidentiality)
- Key management
- Secure code downloading
- Communications security

Non-functional requirements

- Assurance (from moderate to high)
- Anti-tamper (sometimes not required, other times critical)
- Low SWAP (required for most use cases, but differs in how low)
- Low cost (e.g. critical for cars, not so much for aircraft)

Trusted Computing Solutions Comparison



Conclusions

No one size fits all solution

- Need to select and tailor approach to use case

Often you need to run secure applications, and not just a crypto module

COTS trusted computing building blocks are valuable even for high criticality applications

- Complex security architectures can be secured with COTS devices
- For industrial systems, future-proofing for 10+ years is a requirement (Quantum Safe algorithms are important…)