

Trustonic & Automotive

June 27th, 2017



Agenda

- < Introduction to Trustonic
- < Technology trends in Connected Car market
 - < Major systems in Connected Car;
 - < Threat areas
- < Trustonic offering in Automotive and IoT
 - < How Trustonic solutions forms a core component in connected car security;
 - < Security principles for overall car platform security;
 - < Joint offering with Mediatek Automotive
- < Q&A



Introduction to Trustonic

Who are we and what we do

About Trustonic

Governance

- › Founded in 2012. Strategic Investors



Twin Mission

- › To embed the best SECURITY into the world's smart devices
- › To empower app developers to deliver simpler, richer, SAFER services

Credentials

- › Protecting more than one Billion smart devices
- › Recognized leader in application security
 - › GSMA 2016 Award Winner – Best mobile security solution
- › Underpins security in services including



We Essentially do 3 Things

We secure devices

Provide **hardware security** by integrating our **Trusted Execution Environment (TEE)** into connected devices



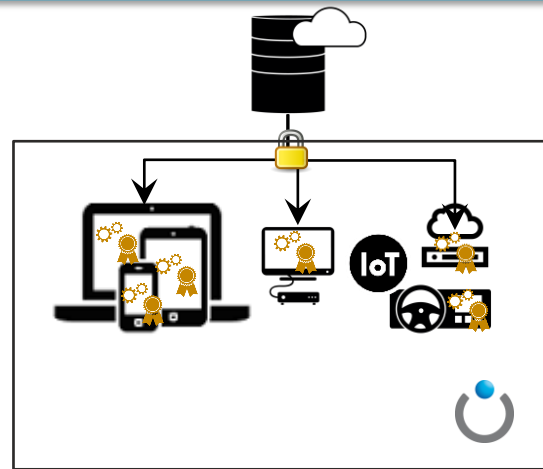
We enable trusted device identity

Inject a **root of trust** to **individually identify** and classify devices enabling **remote verification**



We enable application/data protection

Protect assets inside devices with **hardware isolation** and enable **remote provisioning/management**



IOT from Trustonic

Secure Device Lifecycle

*Discovery/Enrolment/Association
Attestation and Audit
Secure Patching / App Install*

Secure Platform

*Hardware Isolation
Secure storage and communication
Simple/GP APIs*

Secure Device Manufacture

*Root of Trust Provisioning
Tracking all manufacturing stages
Cloud-based component audit*

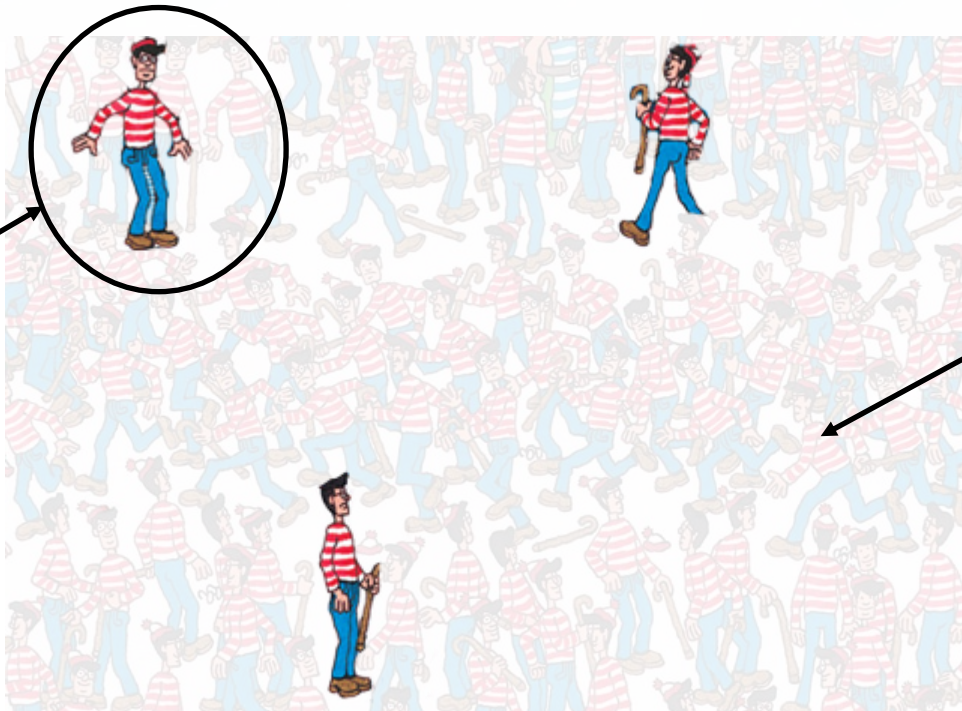
Trust and Certification

*Certificate per Device
Enable 3rd party attestation
Build on certification experience*



“We believe that securely identifying individual devices enables a new way of thinking about internet security”

Identify
&
Enable



Ignore

What makes a 'thing' secure?

- ◀ To protect IOT manufacturers and users, IoT devices must be:

Legitimate – to avoid fraudulent clients and fake components and devices

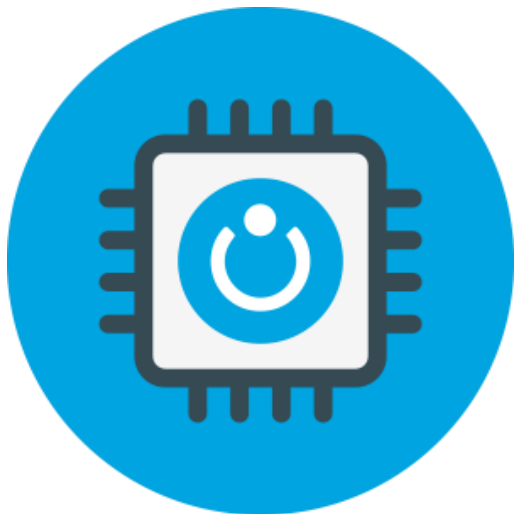
Identifiable – linked to an account or purpose during operational lifetime.

Protected – Combating new threats and exploits require secure in-field automatic update



What does a secure 'thing' need?

- ◀ To enable IoT devices to operate securely they need:



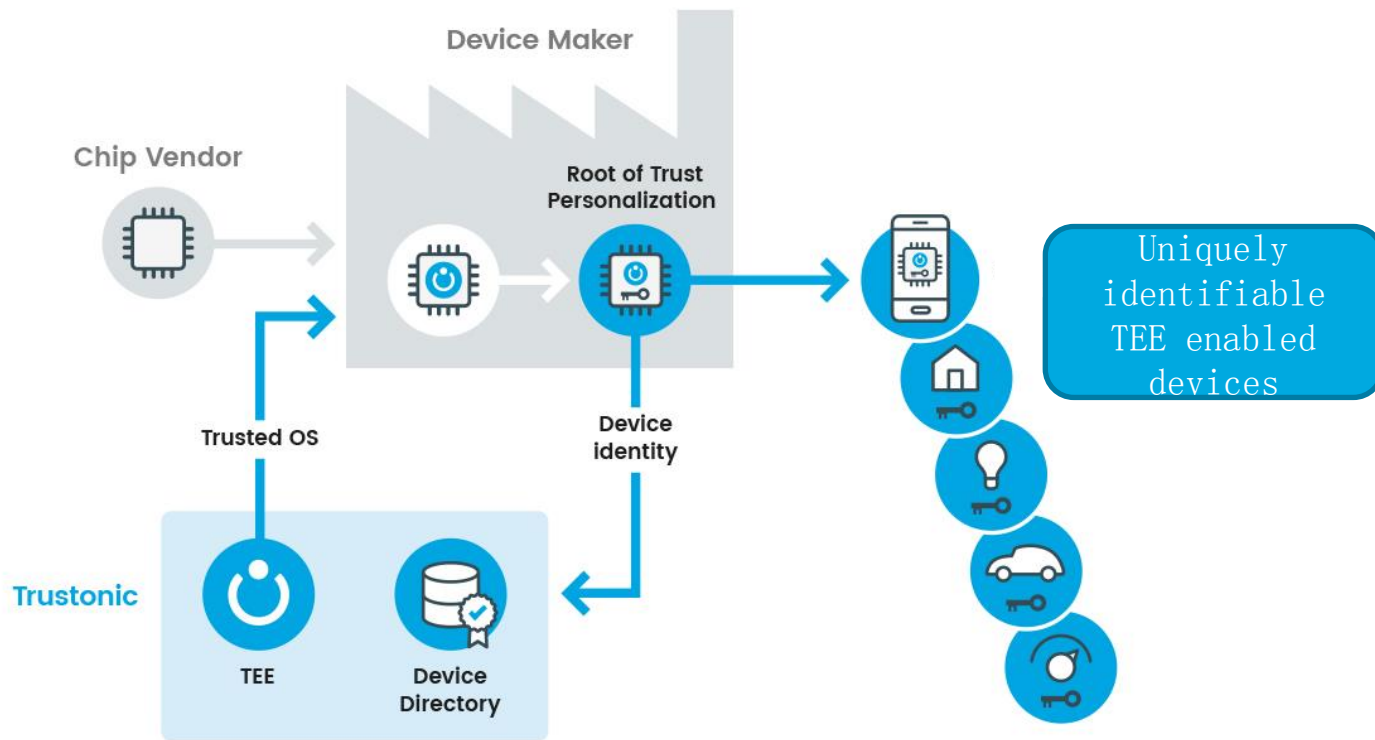
Simple Security – Device programmers need access to strong security without having to become security experts

Strong Separation – Security/Safety critical code must be isolated for protection

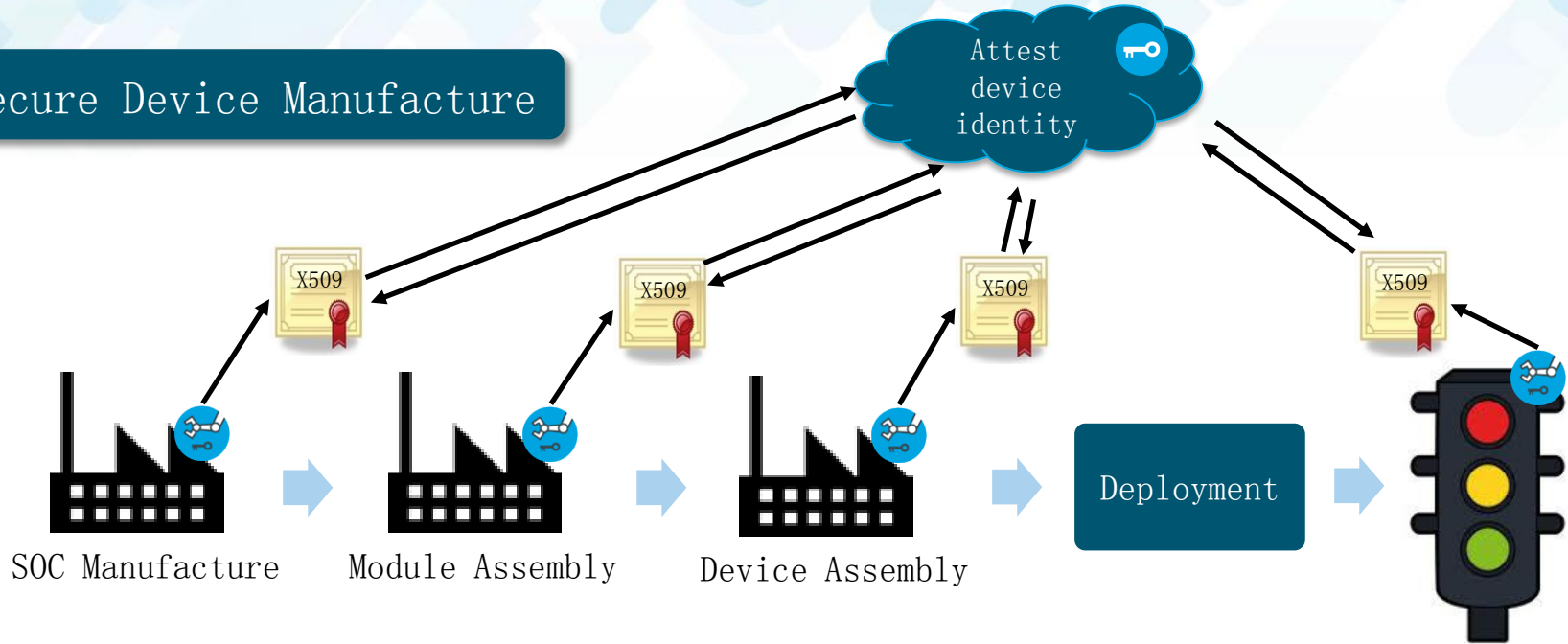
Certifiable Security – IoT devices will inevitably require certification in many key verticals

Trustonic Secured Platforms

Embedding TEE and Root of Trust during manufacture



Secure Device Manufacture



- Device manufacture includes outsourcing to 'untrusted' factories
- Need to attest to manufacturing chain when 'thing' comes on line

“Root of Trust”

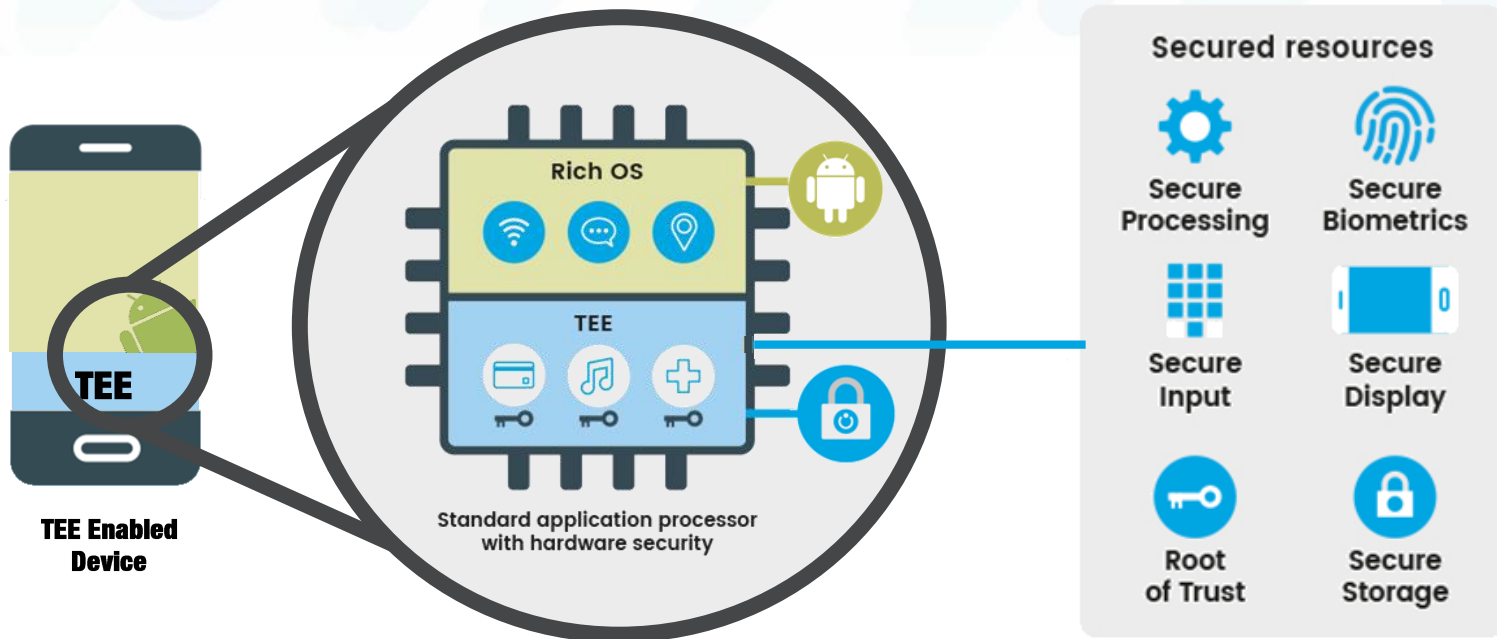
Enables you to security identify devices, and deliver content to them



- < Attest that device was securely manufactured
- < Determine the device type / properties
- < Securely deliver apps and secrets
- < Identify rogue / counterfeit clients

Trustonic TEE

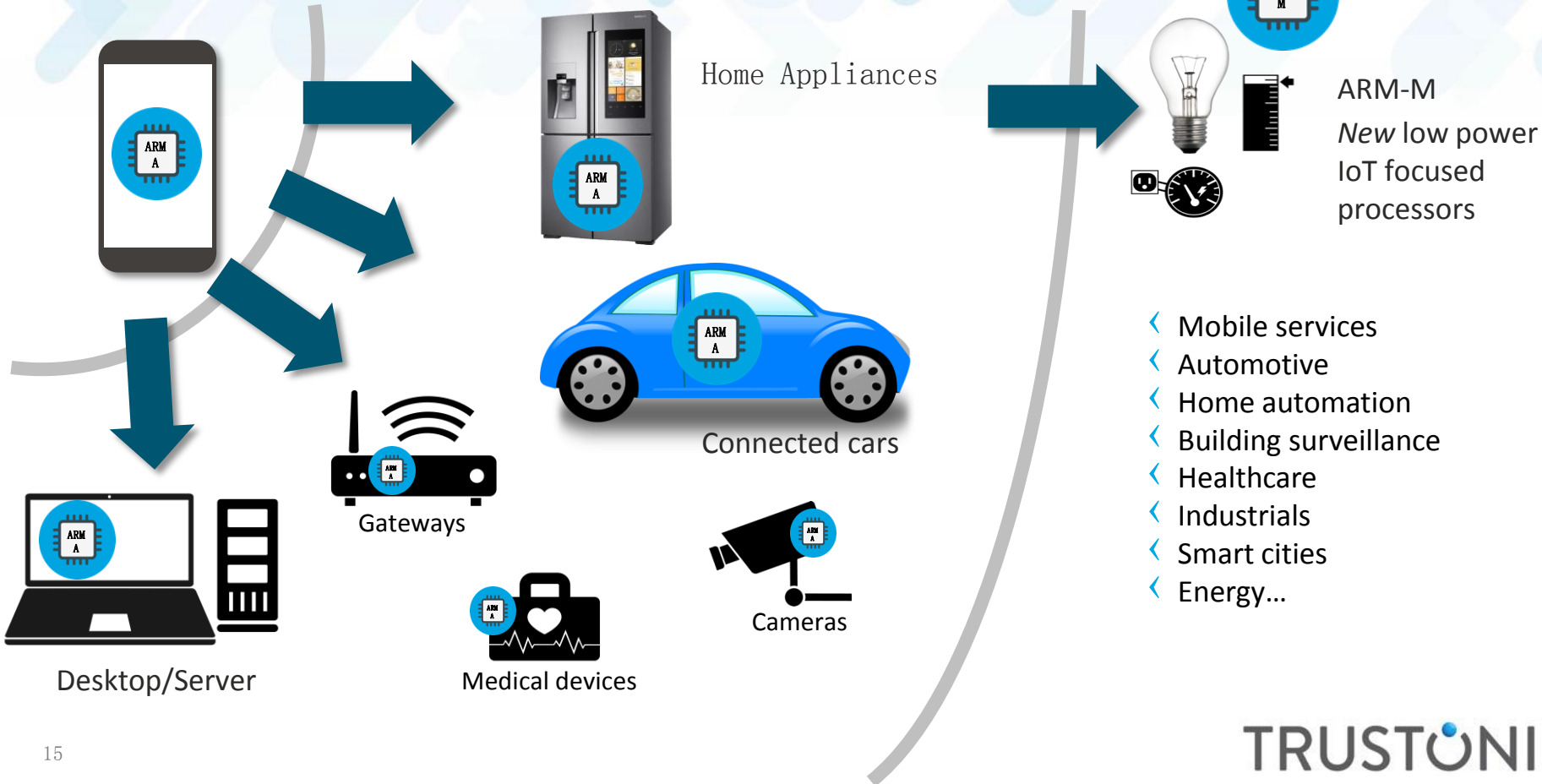
Hardware security for critical applications, on 1 billion devices





Technology Trends in Automotive

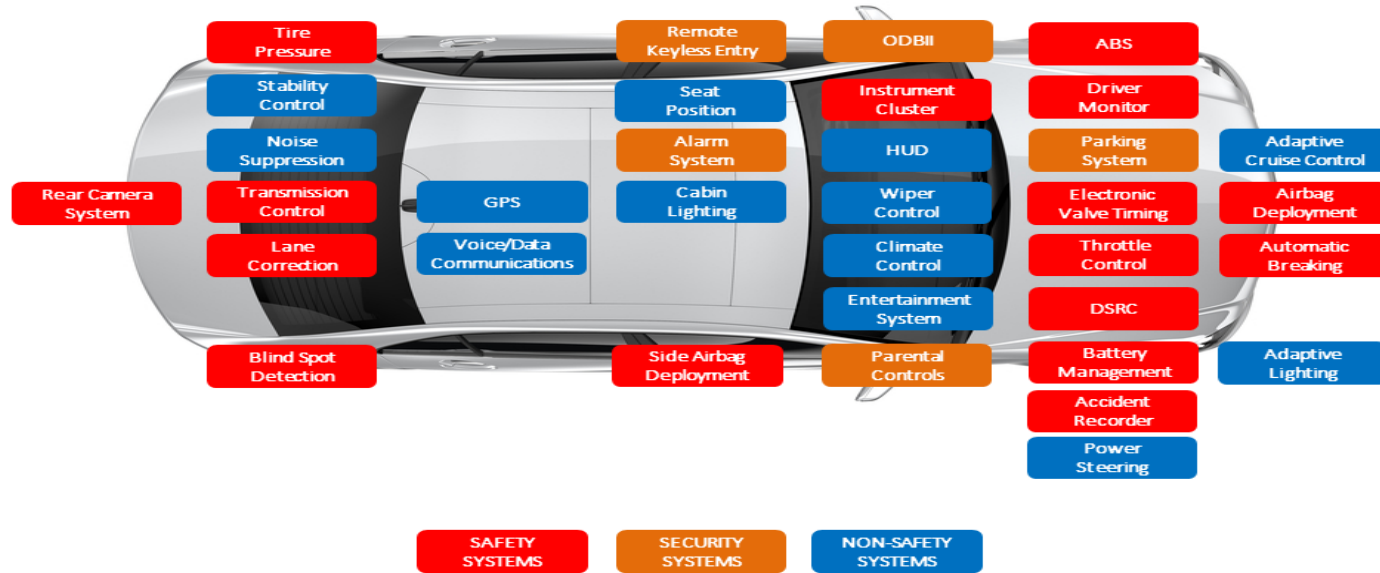
Technology Landscape...



Increasing capability in Car



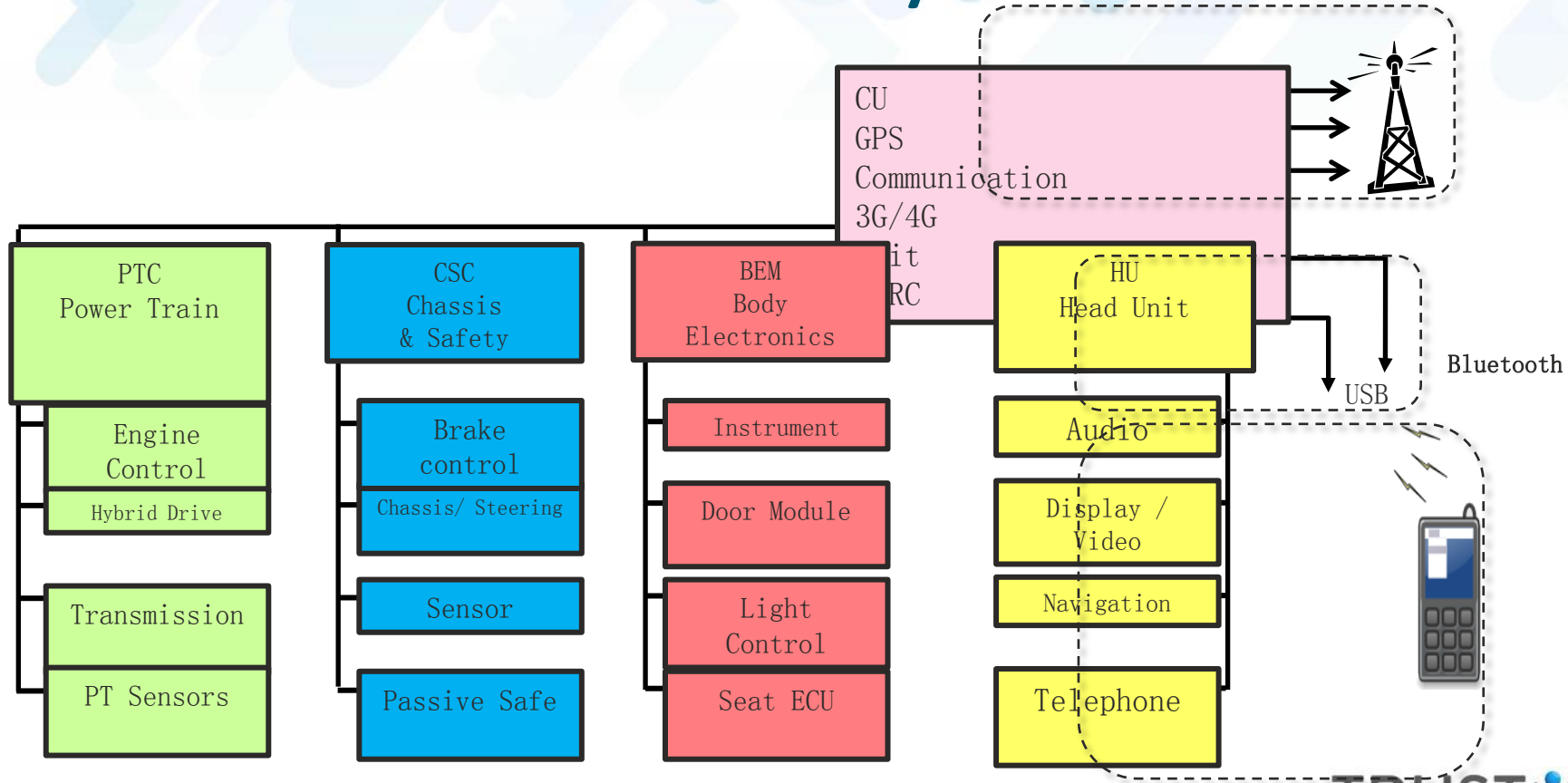
Increasingly connected systems



Increasingly controlled by devices



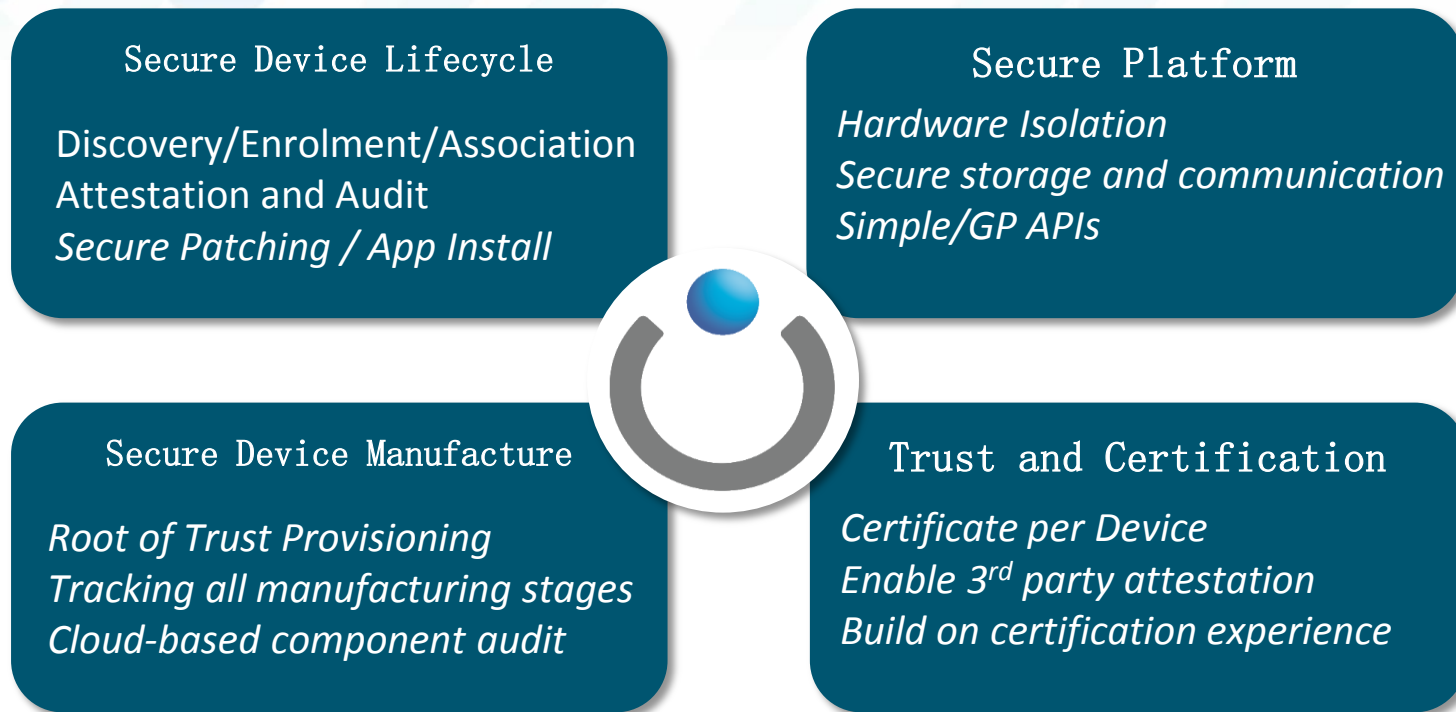
Automotive Security Areas



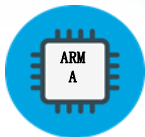


Trustonic Offering for Automotive

Trustonic Security offering for IoT and Automotive

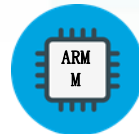


Trustonic Solutions



Kinibi: TEE for ARM Cortex-A

- Common Criteria Security Certified
- GlobalPlatform compliant
- Upcoming FIPS 140-2
- Support our Root of Trust
- Support OTA provisioning
- e.g. Enabled in Samsung's ARTIK IoT platform



Kinibi-M: modular security system for ARM Cortex-M{23, 33}

(under development)

- TrustZone-M
- Our offering is a modular system
- Chipsets are not yet available

Trustonic Solutions



Root of Trust

- In factory provisioning of
 - Unique device identity
 - Unique Symmetric and/or Asymmetric keys
- Factory reporting of device characteristics
 - Identity, secret, IMEI, other characteristics
 - + refurbishment and other workflows



Attestation Services

- X509 Certificate per device
- Online attestation of device properties
- Generation of device specific messages using secret keys
- Binary (app) and/or data push to trusted world

Increasing capability requires certification

Secure Platform

Trust and
Certification

- < Provable, isolated, security enables certification
- < Identity Management
- < Car personalization
- < Insurance
- < Connection to roadside services
- < Traffic information
- < Entertainment



TRUSTONIC

Lifecycle management required for connectivity

- < Leverage secure phone/installer identity to attest to traffic light's location
- < Traffic light/Cloud service become tightly bound
- < Cannot 'fake' traffic light nor steal for use elsewhere

Secure Device
Lifecycle

Trusted
Phone



Trusted
User



App-Thing
Pairing



Cloud-Sign
Trust



Use Case – Using the Smartphone as a Key

- < Customer downloads Car App to phone
 - < “Pairs” phone with Car
 - < Setup security options (e.g. fingerprint)
- < Phone now acts as key
 - < Can register more keys
 - < Can associate with site to enable account
- < Managed lifecycle
 - < Create temporary keys (valet, hire car...)
 - < Owner can deregister account/keys. (etc)





Mediatek/Trustonic Partnership

Joint Offerings in H2 2017

◀ Superior In-Vehicle Infotainment:

- ◀ MediaTek has developed powerful 2D and 3D processing technologies to ensure its application processors perform at the highest levels of efficiency and speed. MediaTek in car entertainment solutions offer a high level of integration of navigational and multimedia features and connectivity options.

◀ Enhanced Telematics:

- ◀ MediaTek Telematics is a robust solution to handle a variety of high-bandwidth information transfers and is able to support a wide variety of connectivity standards (Cellular 4G/3G/2G, Wi-Fi, BT/BLE etc.) and map-based applications. MediaTek Telematics offerings align with the company's core strengths: power-efficiency, highly integrated system-in-packages, broad networking and connectivity support.



Thank you

Michael.lu@trustonic.com

Why Trustonic?

Cost

- ZERO additional hardware BOM cost

Scalability

- Trustonic solutions deployed through more than 1 billion smart connected devices and produced through more than 50 manufacturing sites

Fragmentation Abstraction

- Trustonic solution is supported in more of 50 chipsets references across more than 8 chipset vendors and across various device types
- Trustonic SDK allows to secure services across a diversity of devices with different capabilities

Security

- Trustonic DNA is security
- Trustonic products are regularly evaluated by 3rd party security labs and are as well certified