

TEE Market Trends

Prepared for SCA, Oct 28th, 2016

Michael Lu

VP Sales, Trustonic

Agenda

- › History of TEE so far
 - › Trustonic
 - › Use Cases
- › Future Trends
 - › Trends and Challenges
 - › Fragmentation
- › Trustonic Response
 - › GlobalPlatform
 - › Trustonic Hybrid Protection

Executive Summary

- › TEE now an intrinsic part of device security
 - › Trustonic's current deployment and market segments
 - › Use cases are many and varied
- › Fragmentation is exactly due to success of TEE
 - › Too many device classes, different standards for diverse ecosystems and different stakeholders, both geographical and industrial;
- › Trustonic Response
 - › Standardisation in GlobalPlatform
 - › Trustonic Hybrid Protection (THP)

About Trustonic

Who we are

- › Founded in 2012
- › A strategically owned venture by **ARM**® and **gemalto**
security to be free

Our mission

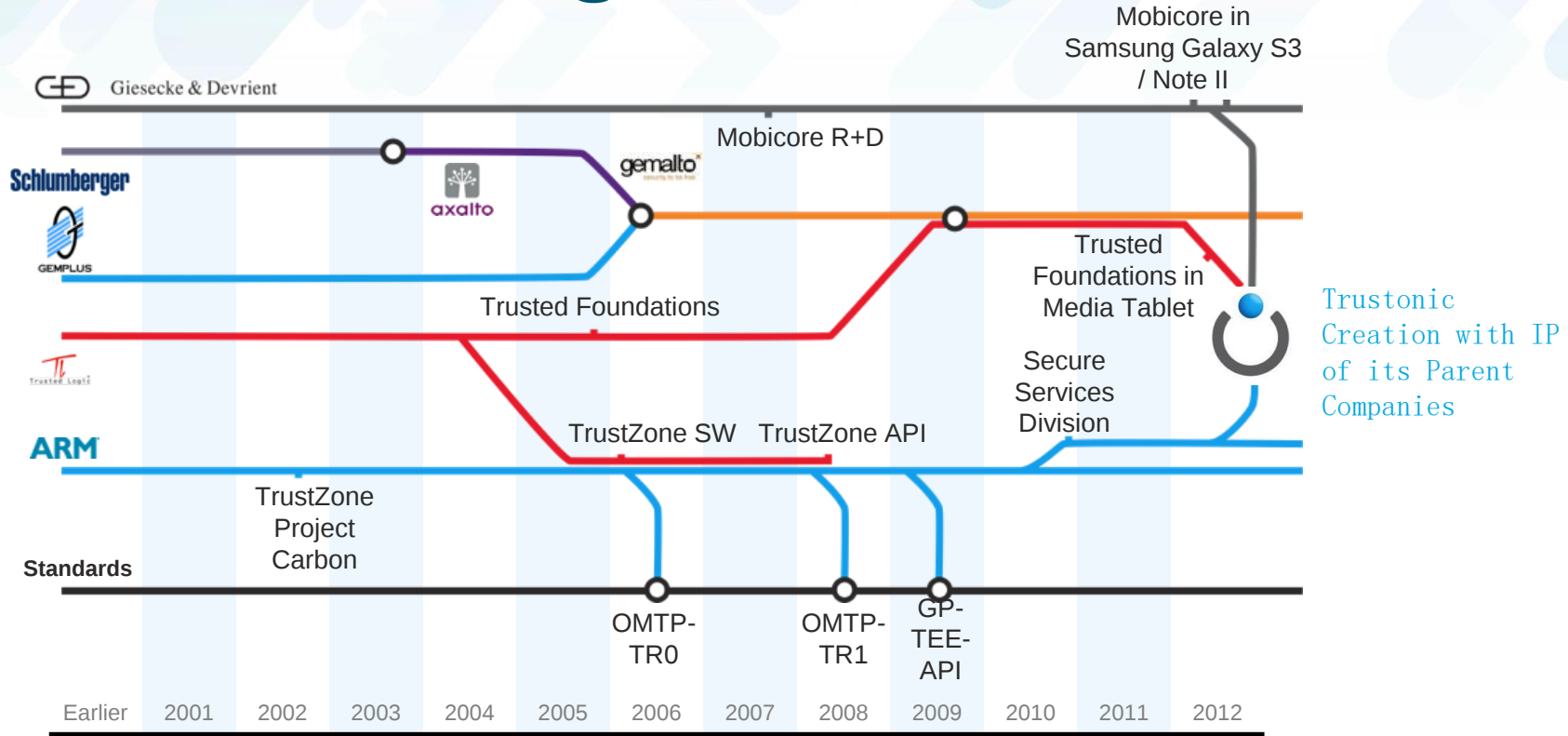
- › To protect, enrich and simplify people's digital lives by enabling optimum security on all smart connected devices, associated services & applications

Key achievements

- › Now protecting more than 700M devices globally
- › 12 of the top 15 Android smartphone makers ship devices secured by Trustonic
- › Recognized leader in app security
 - › GSMA 2016 Award Winner – Best mobile security solution
- › Provide underpinning security for Symantec VIP, Samsung Knox, Samsung Pay, Alipay, Wechat Pay, MiPay



Trustonic Background



TEE in 700M+ devices



10 top tier Android OEMs



Meizu



Gionee



vivo



OPPO



LG



HTC



Xiaomi



LeTV



ZTE



TCL

GSMA GLOMO Award Winning Security

◀ What the judges said

“No-one should be selling a connected device without a **Trusted Execution Environment** and strong hardware security. The **Trustonic secure platform allows manufacturers to do that.**”



Use Cases Driving Device Security



Identity

- Strong Auth
- Identity Protection
- Biometric storage & validation
- Private Key Storage



Content

- HD/4K content
- Multiscreen
- Pay as you go
- On demand HD services



Financial Services

- Card present PIN
- Secure display
- 1 click checkout
- Mobile POS, Mobile Banking,
- Securing HCE



Internet of Things

- Home, Healthcare
- Automotive systems
- Regulated Industries
- Government ID



Enterprise

- VPN, SSO, OTP
- Email, Messaging, Voice
- BYOD, Logical & Physical access
- Secure MDM



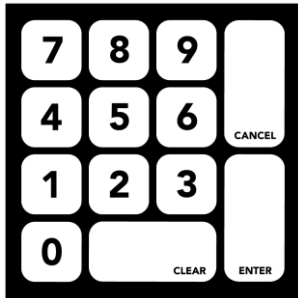
Mobile Network Operators

- Device integrity, Subsidy protect
- Network tuning
- User identity verification
- Dual numbers

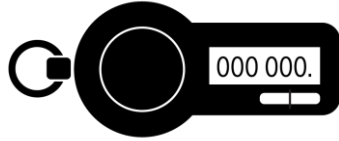
What TEEs Protect in Mobiles today



Finger Print Matching



PIN Entry



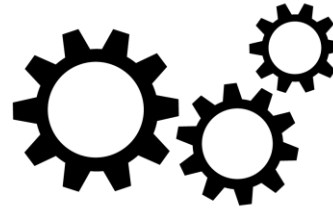
Authentication



Session Keys



Keystore
Gatekeeper



App
Policy



Secure Display
HDCP



Radio Interfaces



Challenges and Trends

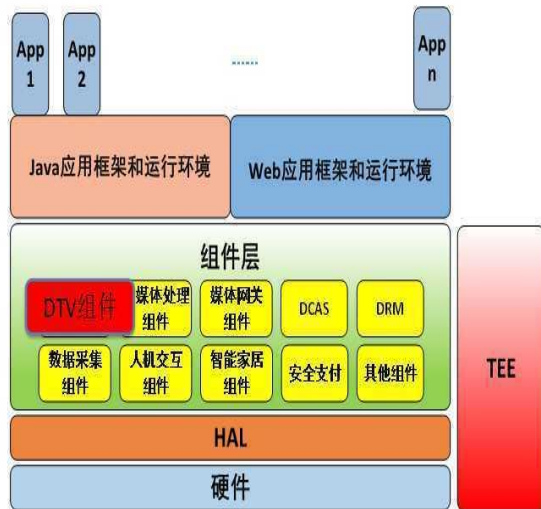
Challenges and Trends

- › Increasing Fragmentation along with increased TEE adoption
 - › Different Industries with different requirements
- › Availability of TEE SDK and Accessibility for deployment
 - › Different APIs offered by different OEMs
- › Cannot deploy to all devices and all users
 - › Developers are reluctant to develop for a small proportion of the market

Android Fragmentation - OpenSignal



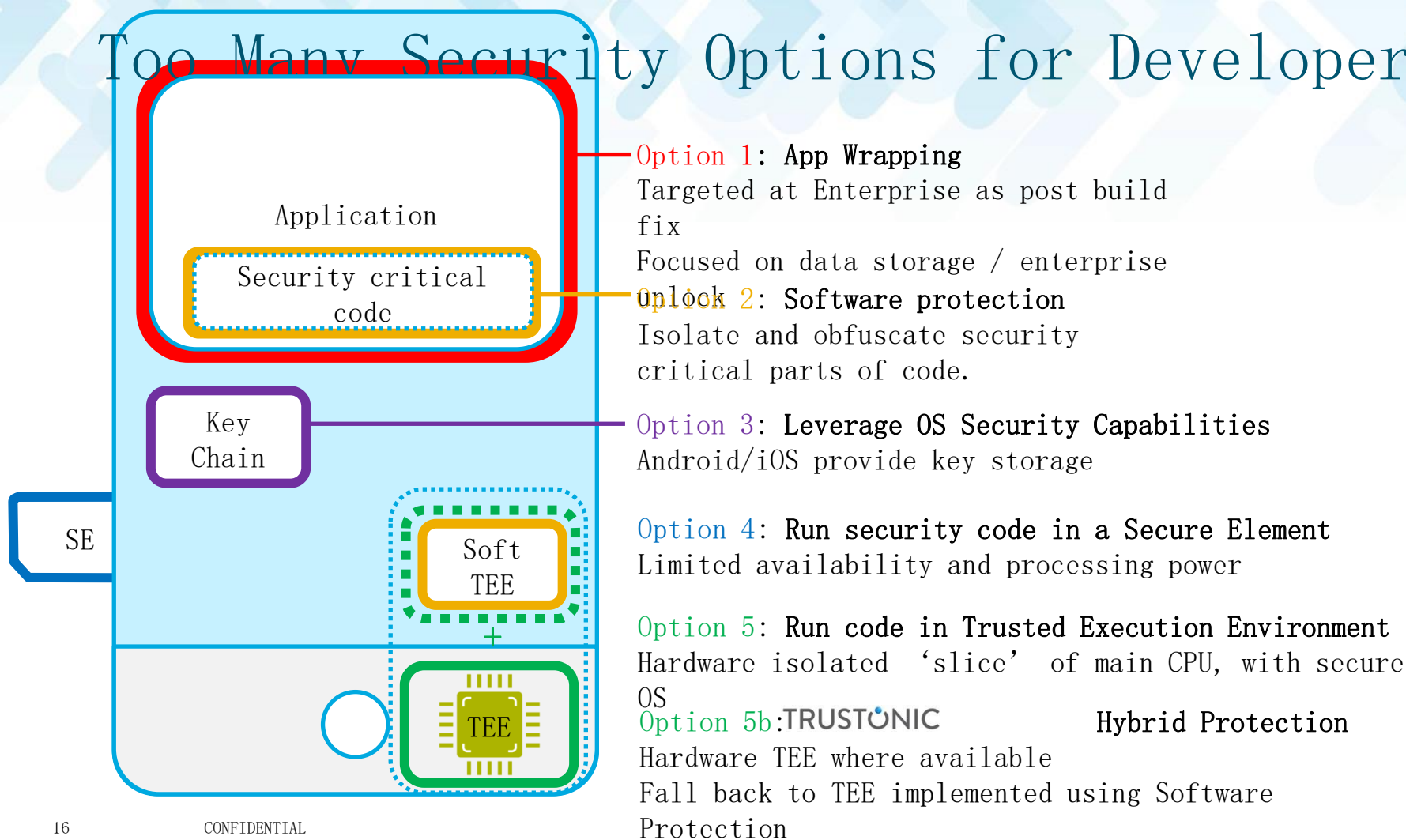
Different Requirements



IoT Stack – Top Problem

Application	• Authentication / Authorization	• Analytics, Identity Access Management
Presentation	• Access Control	
Session	• Non Repudiation	• MQTT CoAP SSH FTP Telnet HTTP
Transport	• Data Integrity	
Network	• Confidentiality	• IPv4 IPv6 6LoWPAN Thread
Data Link	• Assurance / Availability	• GSM CDMA LTE BLE Zigbee WiFi
Physical	• Notarization / Signature	• RJ45 USB Wireless

Too Many Security Options for Developers



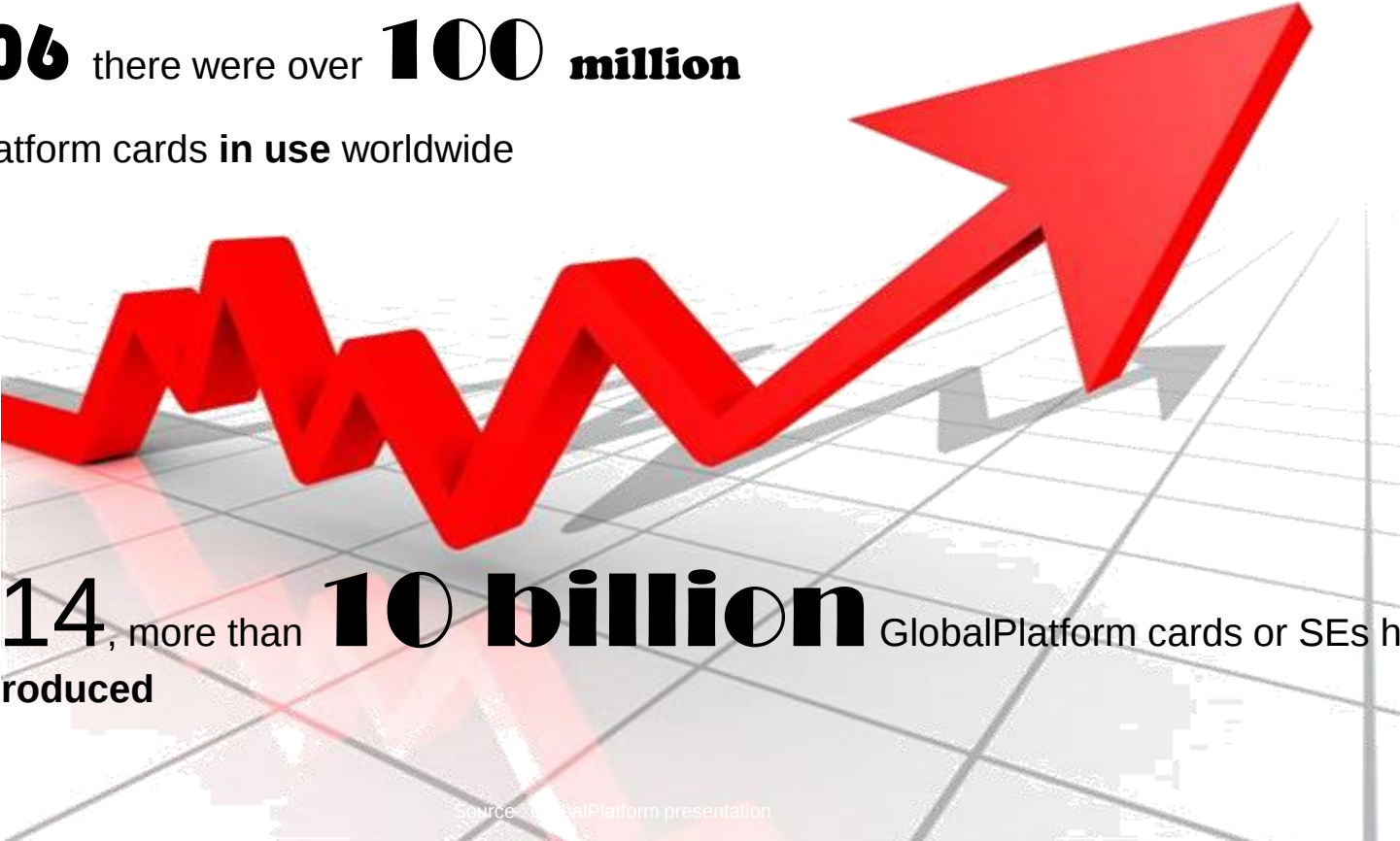


Trustonic Response

TRUSTONIC

In **2006** there were over **100 million**

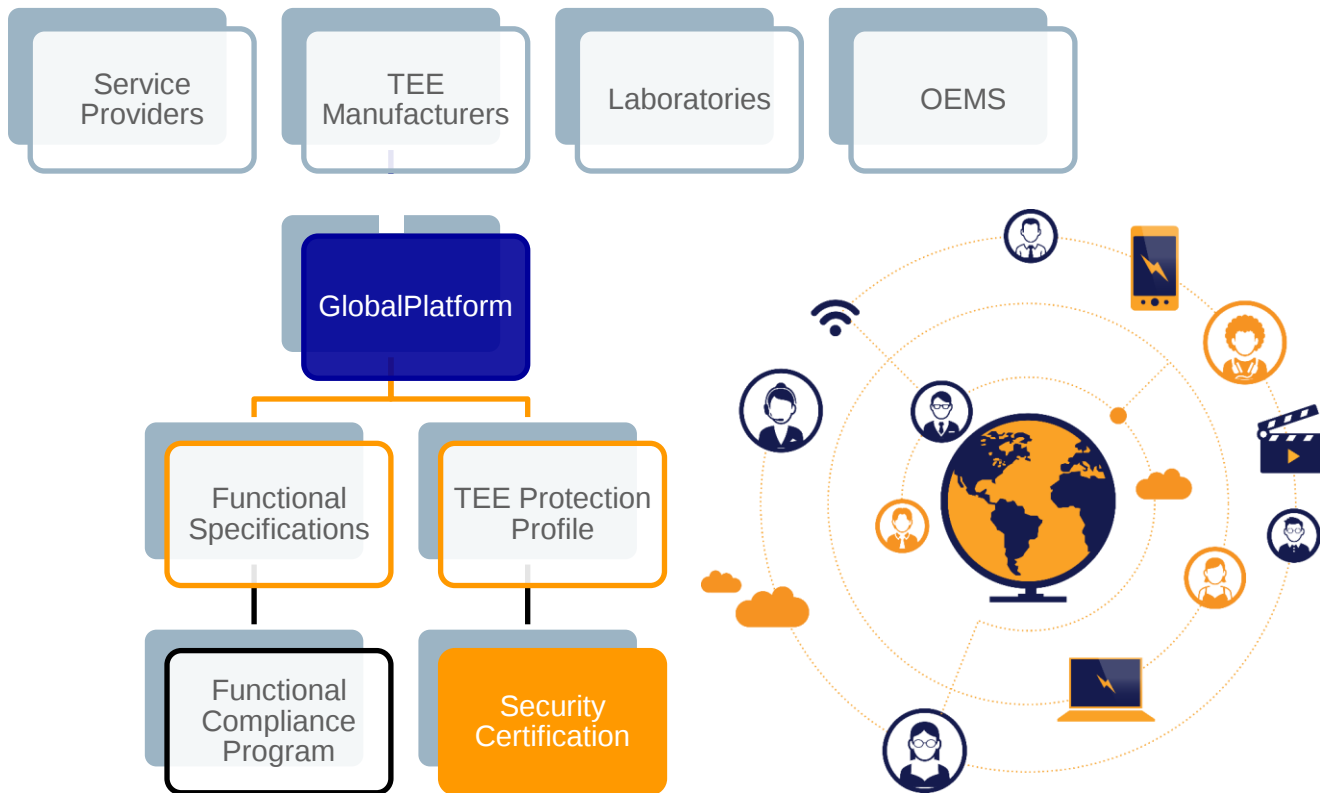
GlobalPlatform cards **in use** worldwide



In **2014**, more than **10 billion** GlobalPlatform cards or SEs have been **produced**

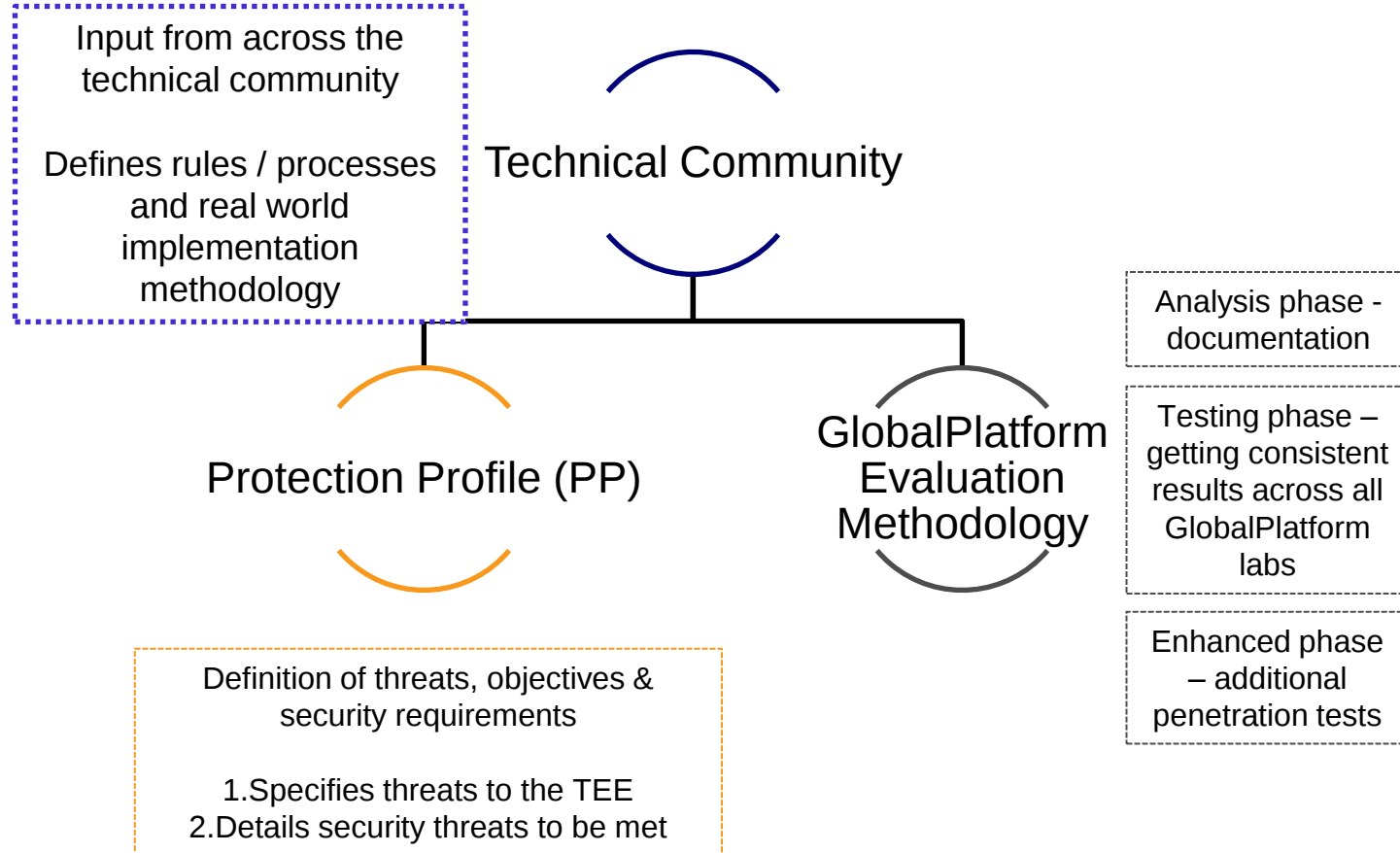
Addressing TEE Community Needs

GLOBALPLATFORM®



Creates a standardized TEE community that reflects current and future market requirements

Scope of the GlobalPlatform TEE Security Scheme





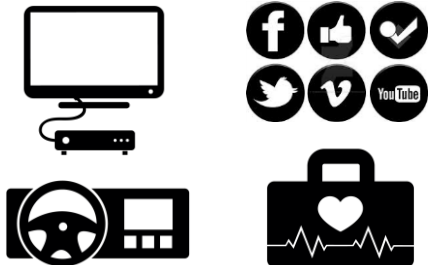
The Trustonic Solution

Trustonic Application Protection
Trustonic Secured Platform

Trustonic enables richer and safer services through a higher level of trust

› Mobile apps drive innovation

- › how we pay & bank
- › how we watch movies
- › how we connect to social media
- › how we control our homes
- › how we start our cars
- › how we unlock doors
- › how we stay healthy
- › How we access enterprise (e.g, BYOD)



› Trustonic is the ideal foundation for app protection

- › Deeply embedded Root of Trust
- › Secure storage of critical content & data
- › Secure yet simple user authentication
- › Enablement of value added services
- › Maintenance of personal privacy

Trustonic Solutions – securing applications and devices

Trustonic Application Protection

Trustonic Hybrid Protection (THP)

*Optimal hardware TEE and software protection
for mobile applications and services*

Service Providers & App
Developers



Trustonic Device Protection

Trustonic Secured Platform (TSP)

*TEE security with Root of Trust
protection for connected devices*

Device & Chipset Makers



Trustonic Secured Platform (TSP) – bringing scale to hardware security

TSP includes

- ◀ Best in-class Trusted Execution Environment
- ◀ Open, over-the-air provisioning
- ◀ Embedded Root of Trust
- ◀ Key provisioning for device and platform makers

TSP provides

- ◀ Trusted User Interface
- ◀ Protection of application data and assets
- ◀ Strong user authentication
- ◀ Device binding & attestation

TSP is available globally from 12 of the top 15 Android smartphone device makers (OEMs)

- ◀ Over 700 million TSP-enabled devices shipped to date



Trustonic Hybrid Protection

- bringing optimised security to app protection

Market Requirements

- › Address **all** users
- › **Minimise** development costs
- › **Simple**, single API integration
- › **Optimal** security

The best of both technologies

- › TEE hardware protection for all capable devices
- › White box cryptography & code protection for other devices



Trustonic Hybrid Protection - Key Market Differentiators

Unique market solution, providing **both** software protection and simple access to the largest installed base of TEE hardware protection

Proven security, including **FIPS 140-2** certification and security evaluations for international payment schemes

One simple, standards-based API integration **auto selects** optimal security on each device – hardware where available, software everywhere else

Cross platform providing security solutions **across Rich OS, including iOS and Android** via a single API

Our Customers' Use Cases



Identity

- Strong Auth
- Identity Protection
- Biometric storage & validation
- Private Key Storage



Content

- HD/4K content
- Multiscreen
- Pay as you go
- On demand HD services



Financial Services

- Card present PIN
- Secure display
- 1 click checkout
- Mobile POS, Mobile Banking,
- Securing HCE



Internet of Things

- Home, Healthcare
- Automotive systems
- Regulated Industries
- Government ID



Enterprise

- VPN, SSO, OTP
- Email, Messaging, Voice
- BYOD, Logical & Physical access
- Secure MDM



Mobile Network Operators

- Device integrity, Subsidy protect
- Network tuning
- User identity verification
- Dual numbers

Trustonic partnerships



Finance

worldpay



INTERPAY

Brightstar



Proxama



Experian
MicroAnalytics
rubean
BANKING TECHNOLOGIES



Enterprise

Symantec

KOOLSPAN

SEQUITT LABS



ExactTrak
Securing your Mobile Data and Assets



ID

Nak
LABS



Plextek

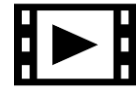
intercede™

TransData

IQUEST



SALT GROUP



Content

verimatrix

DIVX

viaccess-orca



gemalto
security to be free

ATsolutions
Advanced Thinking Solutions

Giesecke & Devrient
Creating Confidence

Vellhi

oberthur
TECHNOLOGIES
THE M COMPANY

secunet
Roke

AGREEYA
MOBILITY

DEEPSEC

SAFRAN
Morpho

alcinéo
TRUSTED PAYMENT SOLUTIONS

RAON
SECURE

smartech

ThunderSoft

rivet

SRI International



SAMSUNG

LG
Life's Good

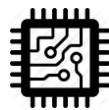
ALCATEL
onetouch
htc

KYOCERA
ZTE中兴

oppo

vivo

DOOV
coolpad



ARM
CrucialTec



FotoNation

PRECISE
BIOMETRICS

MEIZU



FINGERPRINTS



QUALCOMM

BROADCOM
Connecting everything

MEDIATEK



TEXAS
INSTRUMENTS



NVIDIA

AMD

SAMSUNG

SILVERLEAP

TRUSTONIC

Market verticals

Security

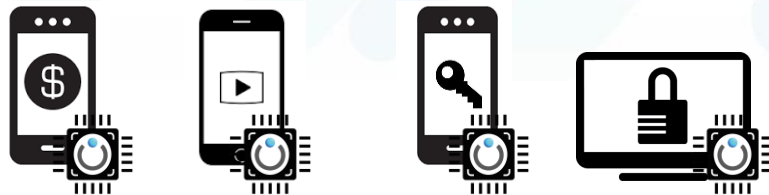
OEMs

Hardware
& Chip

Key points



> Mobile apps drive innovation



> Trustonic is the ideal foundation for app protection

Executive Summary

- ⟨ TEE now an intrinsic part of device security
- ⟨ Fragmentation is exactly due to success of TEE
- ⟨ Trustonic Response
 - ⟨ Standardisation in GlobalPlatform
- ⟨ Trustonic Hybrid Protection (THP)
 - ⟨ Develop Once One SDK, One API
 - ⟨ Best security in any device

What our customer said

- “It was important that we could offer a security solution across all platforms, with minimal integration effort. With Trustonic Hybrid Protection, all Line consumers will automatically benefit from the highest level of security available for their device; TEE hardware-based protection where available, supplemented with market leading software-based security for any non-TEE enabled devices.”
- Takeshi Nakayama, CPO/CISO, Line Messenger

Thank you for your time

Any questions?

Michael.lu@trustonic.com