TRUSTONIC

A handbook for approaching IoT security and why it is Important

> “Without trusted and secured end-points, reliability and sustainability in IoT services and infrastructures are merely a dream”
>
> Ben Cade, Trustonic CEO

enquiries@trustonic.com

Contents

Target Audience & Scope of this Whitepaper 2

Introduction – Beliefs and Why the Industry Should Care 3

Overview of your IoT System 4

- What is a Connected Device 4
- Why Security within Devices Matters 5

Trustonic Security and Positioning in IoT 7

- Device Security with Trustonic Secured Platforms 7
- Hardware-backed Security Embedded at the Heart of Devices 7
- Device Identity and Root of Trust 8
- Application Security with Trustonic Application Protection 9
- Who Can Use Trustonic Security and for What Type of Solutions? 9
- Trustonic Positioning within the IoT Ecosystem 11
- Proactivity – Design Defensively 11
- Establish Trust 11
- Differentiation 11
- Scalability & Flexibility 11
- Cost-Effectiveness 11

Conclusion: There is Light at the End of the Tunnel 12

Resources 13

- Example of IoT Initiatives and Opportunities 13
- Example of Breaches and Hacks 13
- Example of Thought Leadership and Market Initiatives for Security in IoT: 13
- About Trustonic and Technical Documentation 14

Target Audience & Scope of this Whitepaper

This positioning whitepaper is targeted at the key stakeholders of the IoT ecosystem, including:

1. Decision makers and buyers of IoT devices/infrastructures and services
2. System integrators
3. IoT solution/service providers
4. Hardware manufacturers

The purpose is not to provide a deep dive into IoT and end-point security, but rather to educate and create awareness around the need to bring security to the forefront of project definition and solution design when building an IoT environment. It is focused primarily on end-point security, but it is clear that IoT security includes additional multiple layers that need to be considered.

Resources and contact details are located at the end of the document.

Introduction –
Beliefs and Why the Industry Should Care

Operating in the cybersecurity space, Trustonic has to date deployed its secure platform into well **over 1 billion connected devices** and currently protects more than **500 million applications**. This document is based on Trustonic's market feedback from various sectors of the IoT industry, including government, financial, healthcare and automotive.

This section provides a few facts that will set the basis for this paper.

TRUE – Internet of Things will keep growing

The Internet of Things value proposition is very desirable - cost savings, new/faster/better services, increased revenue, improved operational efficiency, enhanced users' digital lives - and it's possible that some of the best benefits haven't even been imagined yet.

TRUE – There will be more large scale attacks

Large enterprises and consumers have already been targeted and hit by cyber attacks*. Each attack is potentially very damaging to an organization's brand or reputation.

Massive scale attacks are also finding their way into the business and consumer markets. A popular example is ransomware that take a workstation or mobile device hostage and then demand money to unlock them.

TRUE – There is a lack of knowledge in the industry about the possible threats in the IoT space

Many businesses don't know about the potential threats and how to mitigate them. There is a strong need for security experts to educate and guide businesses especially during project definition and design.

FALSE - It only happens to others

Well, those to whom it **has** happened probably thought the same thing and they are now making the news headlines. Complacency is not an option.

In a perfect world, everything would go smoothly, but the reality is that, if there are weaknesses, then someone will try to exploit them. There have already been many security attacks, including data breaches, user impersonation, compromised devices, safety issues, data corruption and Distributed Denial of Service attacks.

FALSE – Security is not yet part of some major IoT plans

Leaders in the IoT industry have already recognized the need to deliver security and, in particular, on end-points.*

FALSE - Security is too complicated, too expensive and not scalable.

Whilst deploying secure solutions does indeed require expertise and investment, it does not have to be onerous. Security is not a one-size-fits-all approach, and trade-offs can be made, based upon the particular use case.

*See references in resources and contact details page

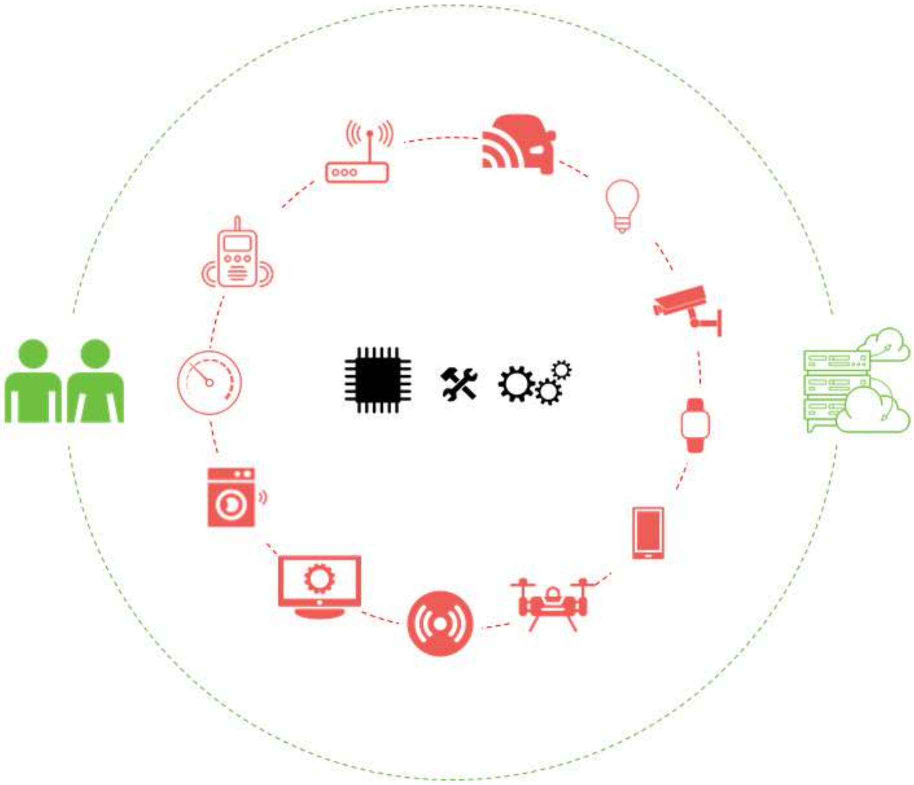
Overview of your IoT System

To state the obvious, there is, by definition, no Internet of Things without end-point devices. But this means that all the infrastructures and associated services will rely on end-points to manage and deliver what are, in many cases, safety-critical or business-critical services.

Gartner predicts that there will be around 20 billion connected devices by 2020*. This represents 20 billion potential threats.

What is a Connected Device

An end-point, whether it is a small sensor, or a large appliance, will consist of a combination of both hardware and software components. This end-point will then potentially be able to host services and data and to communicate with other end-points, a cloud environment or a user.



An end-point device will be designed for a specific given purpose, with a combination of hardware, software, connectivity and application support capabilities.

It is clear that a smart heart-rate monitor or a pacemaker will not have the same capabilities as a smart car. Nevertheless, they both embed critical software and handle highly sensitive data that it is crucial to protect at any time.

*http://www.gartner.com/newsroom/id/3598917

Why Security within Devices Matters

It should be obvious that a connected device is at the heart of an IoT system. Below are some examples of potential risks:

Scenario 1: A sensor tells a driver-less car that it is slowing down, when, in reality, it is not.

Scenario 2: A hacker remotely alters a pacemaker's settings

Scenario 3: A hacker sends false alert signals to public safety authorities or takes control of CCTV cameras

These situations may sound extreme and may have not yet happened, but they are actually feasible, as all these IoT use cases either exist or soon to be deployed.

From a more generic perspective, where could something go wrong with a device?

During hardware and software design

- Introduction of hardware and software design weaknesses that could be exploited
- Lack of design review and validation
- Lack of security expertise
- Absence of hardware-backed security

During hardware and software integration

- Improper integration of hardware and software components, thereby introducing exploitable bugs
- Integration of uncertified software
- Lack of secure app/data management
- Lack of integration validation

During manufacturing

- Counterfeit devices entering the supply chain
- Lack of device identity/root of trust
- Lack of manufacturing-stage tracking

During device usage & user interaction

- Stolen devices
- User impersonation
- Malware installation
- Data corruption
- DDOS Attacks
- Software debugging and code analysis
- Side channel attacks

During device lifecycle

- Installation of illegitimate patches and firmware
- Loss of device identity and trustworthiness
- Device cloning

There is a need to be aware of both known and unknown threats, as they will affect all the major IoT segments, such as smart cities, smart homes, industrial, automotive and healthcare. Too often, security in IoT is an afterthought or, even worse, perceived as being irrelevant or less important than the device's primary function.

While you may not need strong security in your coffee machine, you probably want to have adequate security in your car, in your house or in your city. Even then, do you really want your coffee machine to become a weapon, helping perform denial of service attacks? Some nascent markets can indeed function with limited security. However, the majority of solutions will require strong, adequate security built in from the ground up.

Mistakes are not acceptable when you build a smart car, a smart home, a smart warehouse or, on an even bigger scale, a smart city. This is simply because one failure to protect data or to ensure that services are not corrupted can result in loss of life and/or failure of a business.

Trustonic Security and Positioning in IoT

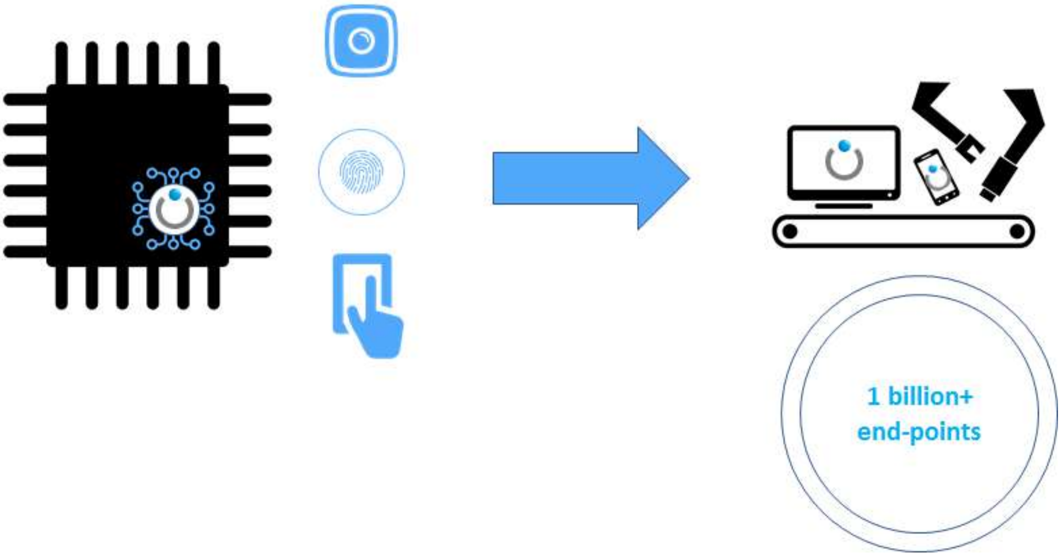
Trustonic helps to deliver security at various stages in IoT ecosystems.

Device Security with Trustonic Secured Platforms

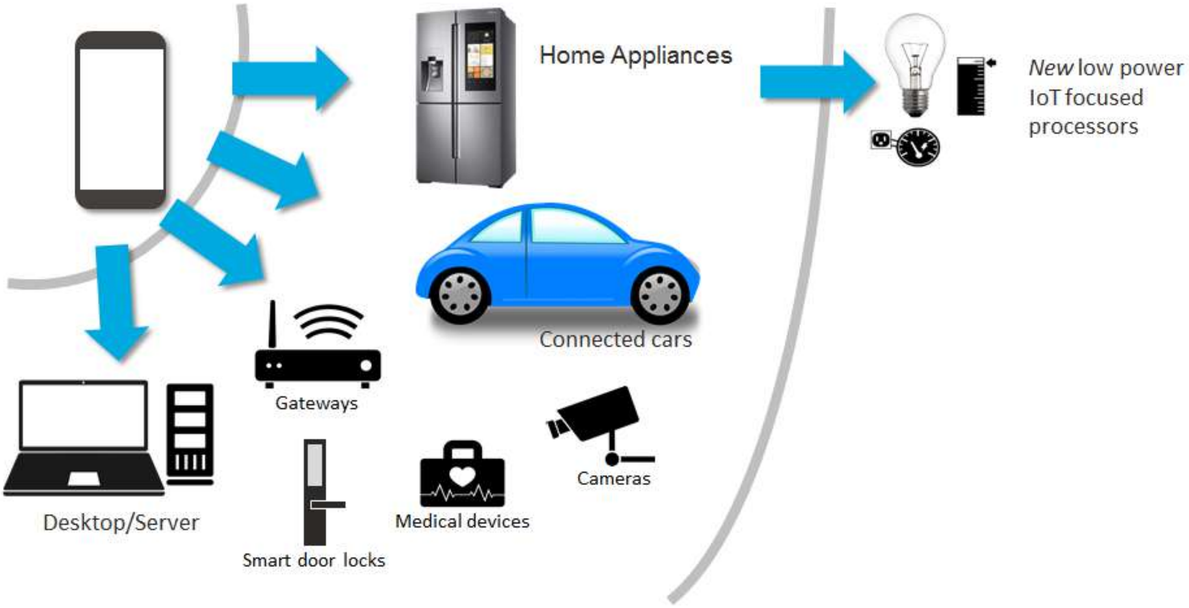
Hardware-backed Security Embedded at the Heart of Devices

The **Trustonic Secured Platforms** product suite includes a security-certified operating system – **Kinibi** – that is integrated with chipset and device manufacturers to provide a hardware-based isolated operating environment in end-point devices.

Kinibi relies on a secure hardware design, widely available in the market, to create a Trusted Execution Environment (TEE) whose integrity can be verified, that can host multiple applications, perform secure data processing and storage and obtain privileged access to peripherals (e.g. camera, fingerprint sensor or touchscreen).



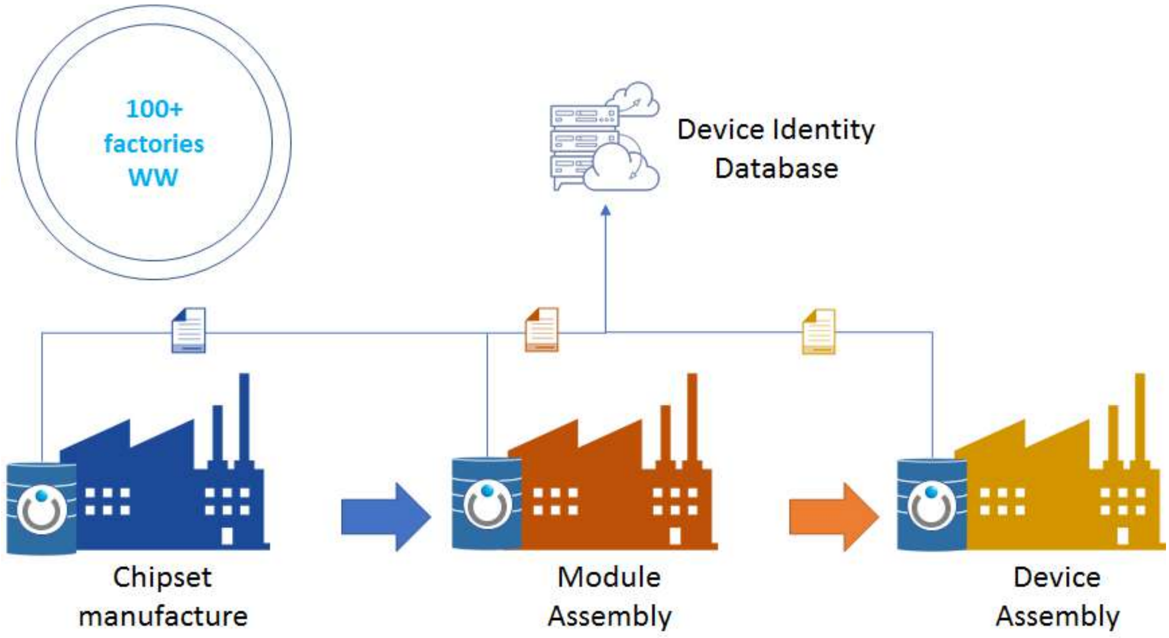
The concept of a Trusted Execution Environment applies to the majority of IoT devices.



Device Identity and Root of Trust

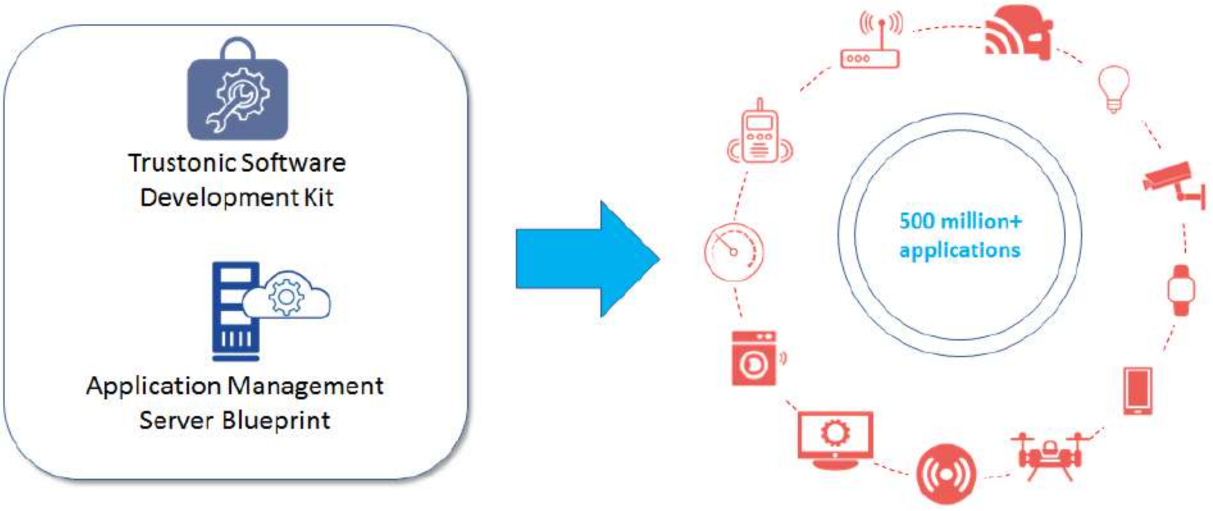
Device manufacture may include outsourcing to “untrusted” manufacturing locations and there is a need to attest the manufacturing chain when an end-point becomes live. In addition, many services are based on the trustworthiness of data received from one or several end-point(s) and it is essential to make sure that end-points themselves are trustworthy.

Trustonic’s **Key Provisioning Host** is also part of the Trustonic Secured Platforms product suite. Easily integrated within manufacturing plants, it allows the creation of a unique device identity by injecting a Root of Trust at manufacturing time, which can then be remotely verified when the device is in the field.



Application Security with Trustonic Application Protection

Once devices are equipped with Trustonic's security, solution developers can leverage the **Trustonic Application Protection** software development kit to develop and deploy their secure services.


Trustonic Software Development Kit
Application Management Server Blueprint
500 million+ applications

Trustonic also provides resources to support users during the development and deployment phases.

Who Can Use Trustonic Security and for What Type of Solutions?

Whether one builds a whole IoT infrastructure/system or a specific IoT component, there is considerable value to be derived from providing and leveraging the maximum level of security.

Trustonic Secured Platforms	• Chipset manufacturers • IoT module manufacturers • Device manufacturers • System Integrators
Trustonic Application Protection	• Hardware manufacturers • System Integrators • Application/Solution developers

If we look at the major IoT verticals, we can see that device security applies to the vast majority of services. Here some examples :

Smart cities

- Public safety, energy, transport

Smart homes

- Surveillance, energy management

Industrial

- Production streamlining, inventory management

Automotive

- Driverless car, telematics, infotainment, in-car payment

Healthcare

- Telehealth, remote drug prescription and administration

If we look at the solutions themselves that are used in these verticals, here are some key use cases:

- Secure software/firmware management
- User and device enrolment
- Data analytics
- Data transmission
- Device to device communication
- Device to cloud communication
- Device authentication
- Device counterfeit protection
- Device tracking
- Payment

Trustonic Positioning within the IoT Ecosystem

It would be foolish to think that securing the end-point itself could solve every problem. This is, of course, not what Trustonic believes. End-point security is not the only element to take into consideration, but it is a great start and security should be built into devices, not added after devices are deployed. With its services and partnerships, Trustonic foundations of security rely on the following principles:

Proactivity – Design Defensively

Security needs to be pre-embedded into devices in order to be effective. The larger the software, the more bugs it is likely to have that could be exploited by an attacker. It is essential to leverage environments that are designed for security and to minimize risks by separating sensitive code/data and controlling how they are accessed.

Establish Trust

If you cannot ensure the origin of the information, then you should not trust it. If you do not trust it, then the whole system relying on this information becomes irrelevant. There is a need to identify the appropriate devices and services and to validate that they are legitimate. Trust should apply across all IoT infrastructure layers, not only to the end-points.

Differentiation

Additional security is key to create differentiation within the hardware, software/applications and services. It both allows safe innovation and prevents irreparable damage.

Scalability & Flexibility

Security should not be a closed environment. It is important to have a comprehensive ecosystem of service providers that can access it, if we want the whole market to benefit from it. It is also essential for a service provider to have as much control as possible over its own services. This will enable not only faster response-time to incidents, but also a better service to their customers.

Cost-Effectiveness

If a security system is well designed, the associated costs can be reduced and optimized. Scalability is also a factor that will minimize the effort involved in bringing solutions in the market and then managing them.

Conclusion: There is Light at the End of the Tunnel

Many businesses believe that security hampers a fast go-to-market model and a positive ROI, as it is often perceived as too complicated or expensive.

Security itself is not a simple task. If it was, it would also be easy to circumvent.

- However, the IoT industry is full of security experts that can provide advice, assist during projects and provide the necessary proven building blocks for a sustainable IoT environment.

Security has a cost, but it does not have to be prohibitive.

- It is essential for industries to understand that the potential incremental costs involved in bringing security to the appropriate level for their needs will deliver value within the overall ROI.
- Trade-offs can be made

Security in IoT is a multi-layered approach where end-point security is critical.

- IoT devices are the link between services and users. Therefore, protecting such devices cannot be an afterthought

Security must be seen as adding value and not as detrimental to the overall offering.

Industries are now catching up and increasing numbers of initiatives around security in IoT are being initiated. Trustonic's recommendation is for businesses to be more proactive in assessing their risks and properly protecting their IoT systems, rather than waiting to react and suffering irreparable damage.

Trustonic's mission has not changed since its inception. This is to provide hardware-based security in devices and to enable users of these devices to easily develop innovative services while protecting their assets. Being part of the AT&T Cybersecurity Alliance, alongside key security providers IBM, Nokia, Palo Alto Network, Qualcomm and Symantec opens up exciting and fresh opportunities for the IoT ecosystem.

Resources

Example of IoT Initiatives and Opportunities

Smart cities

- http://about.att.com/sites/internet-of-things/smart_cities
- http://www.techrepublic.com/article/smart-cities/

Connected cars

- https://www.bloomberg.com/news/features/2016-08-18/uber-s-first-self-driving-fleet-arrives-in-pittsburgh-this-month-is06r7on
- http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car

Healthcare and IoT

- https://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#7bf9b4dc69d9

Smart agriculture

- https://www.thingworx.com/ecosystem/markets/smart-connected-systems/smart-agriculture/

Example of Breaches and Hacks

Target data breach – Target Profit Falls 46% On Credit Card Breach

- https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#3bdca2987326

DDOS Attack – Mirai botnet

- https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

Baby monitor hack

- http://www.cnn.com/videos/us/2014/04/28/dnt-baby-monitor-hacked.wxix

Network router backdoors

- http://thehackernews.com/2014/04/router-manufacturers-secretly-added-tcp.html

Network transport vulnerability - Heartbleed bug

- http://heartbleed.com/

Remote device access control

- https://blog.qualys.com/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability

Example of Thought Leadership and Market Initiatives for Security in IoT:

US Government - Senators Introduce Bipartisan Legislation to Improve Cybersecurity of IoT Devices

- https://www.warner.senate.gov/public/index.cfm/pressreleases?id=06A5E941-FBC3-4A63-B9B4-523E18DADB36

AT&T – The CEO’s guide to securing the Internet of Things

- https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf

GSMA – IoT Security Guidelines for Endpoint Ecosystems

- http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.13-v1.0.pdf

Mediatek and Trustonic – Trustonic, Mediatek Partner to Secure Smart Car Software

- https://mobileidworld.com/trustonic-mediatek-smart-car-software-006263/

Samsung and Trustonic – Samsung Advances Open IoT Ecosystem

- http://www.samsung.com/us/ssic/pdf/pr-artik-commercial-release-final.pdf

About Trustonic and Technical Documentation

- https://www.trustonic.com/
- https://www.trustonic.com/about-us/downloads/

Trustonic

At Trustonic, we see both the exciting opportunities and inherent new challenges that come from having to protect and secure individual users and service providers in an increasingly connected world. Our proven foundation of hardware-backed security and Root of Trust forms the basis upon which a secure and trusted IoT infrastructure should be built and provides IoT devices with the robust protection that they will need, long into the future.

As a founding member of the IoT Cybersecurity Alliance, we bring industry-leading expertise in embedding security into the world's smart devices, collaborating with customers and partners to protect critical IoT applications and assets. Ultimately, Trustonic empowers developers to deliver simpler, safer services that customers expect and demand.

Learn more at https://www.trustonic.com/markets/iot/

Florent Joubert
Sr. Manager, Secure Services & Business Development
florent.joubert@trustonic.com

TRUSTONIC

Securing Mobile Apps, Vehicles And More

Trustonic Security for Mobile Vehicle Applications on Android

WHITE PAPER

PREFACE

This document aims to provide information to clearly explain the security concepts related to the Trusted Execution Environment (TEE) and Trustonic's value in developing and deploying trusted applications and services. The document will help readers to quickly grasp these principles and explain how they could apply them to automotive mobile applications.

Table of Contents

1 Introduction And Definitions........3

2 TEE Overview........4

2.1 How to Leverage the TEE........5

2.2 Fundamental TEE Features........7

2.2.1 Secure Storage........7

2.2.2 Secure Peripheral Access........7

2.2.3 Device Authentication........7

2.2.4 Secure Communication with Remote Entities........8

3 TEE Security for Automotive Mobile Applications........8

3.1 Internal Data Leakage........8

3.1.1 TEE Protection Against Internal Data Leakage........9

3.2 Overlapping of the Application........9

3.2.1 TEE Protection Against Application Overlapping........9

3.3 Re-packaging of the Application........9

3.3.1 TEE Protection Against Application Re-packaging........10

4 Virtual Vehicle Key with Trustonic........10

5 Applications of the TEE Beyond Vehicle Mobile Apps........11

5.1 Premium Content........11

5.2 Secure Messaging........11

5.3 Mobile Financial Services........11

5.4 User Authentication........12

5.5 Securing the Internet of Things (IoT)........12

5.6 Non-Android and Additional information........12

6 About the Author........13

1 Introduction And Definitions

The “Trusted Execution Environment”, or “TEE”, is the combination of a secure and isolated operating system that can execute both secure/protected applications and the underlying hardware security capabilities of the application processor in a device. The TEE runs alongside the standard operating system.

ARM developed a technology called “TrustZone” which is implemented by hardware manufacturers (chipset makers) utilizing ARM chip designs. TrustZone enables a high degree of hardware separation between “trusted” and “untrusted” code and is an implementation of a TEE. Today, ARM’s TrustZone technology is present in over 95% of smartphone/tablet devices. Intel also has a technology named Intel® SGX, which delivers a TEE with the same philosophy of separation between trusted and untrusted code.

Kinibi, Trustonic’s TEE operating system, has been integrated with many chipsets and devices. It has already been deployed in over one billion devices, including smartphone/tablets, wearables, laptops and other IoT devices.

- Kinibi supports GlobaPlatform standards.
- Kinibi enables traditional applications executed on a connected device (e.g. an Android application) to have an associated secured application which runs within the TEE. This application is referred in the industry to as a “Trusted Application” or “TA”.
- Kinibi has been validated by payment schemes (e.g. Visa, Mastercard…) to secure mobile payment applications
- Kinibi has fully passed the Common Criteria security certification
    - Security target can be found here https://www.ssi.gouv.fr/uploads/2017/02/anssi_cc-2017_03-cible-publique.pdf
- Finally, Kinibi supports the ability to securely deliver/manage TAs on devices which are already deployed in the field, by using a network service called a Trusted Application Manager (TAM).

This document refers to a concept called a Rich Execution Environment (REE). This is the normal unsecured operating system running in a device, such as Android, for example.

2 TEE Overview

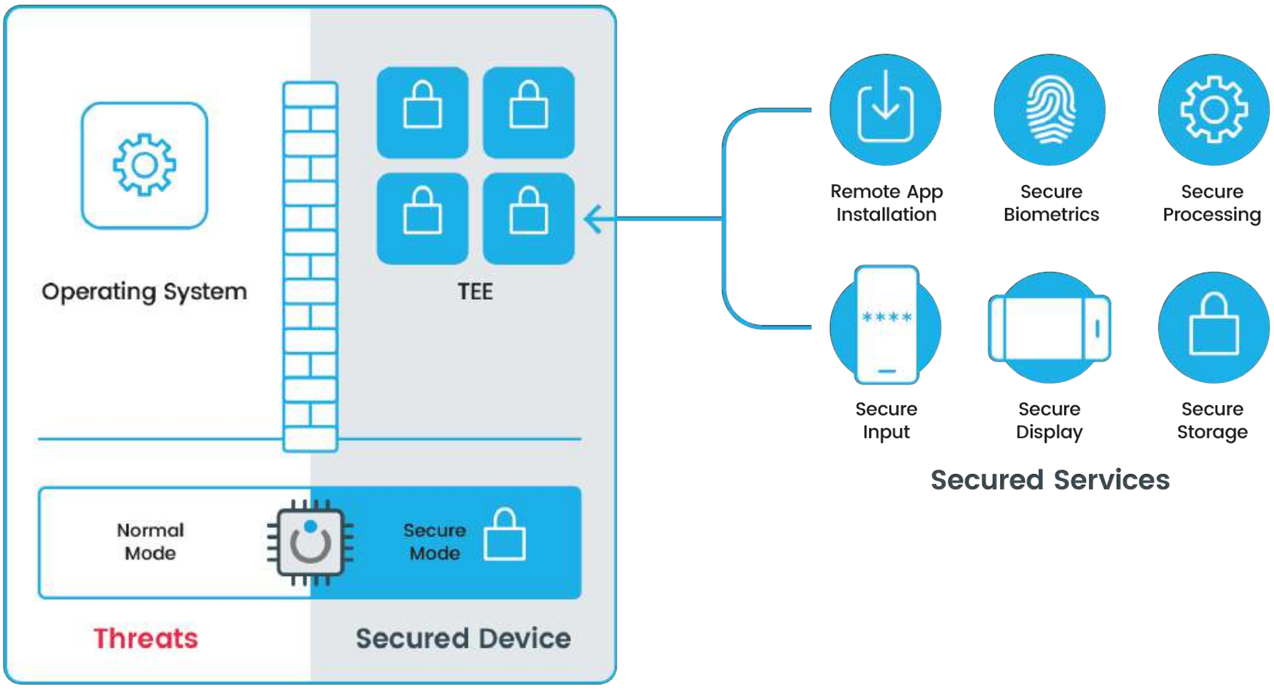


Figure 1 Trusted Execution Environment Overview

The TEE relies on the principle of providing hardware security and isolation on the main application processor of the device itself. This means that the TEE does not require any extra hardware components to be implemented and deployed.

As can be seen from the figure above, the TEE is a separate operating environment in the “Secure Mode” running alongside the main operating system running in the “Normal Mode” or “REE”, but completely isolated.

In particular, Trustonic’s TEE operating system, Kinibi, has the following properties:

1. Based on hardware Roots of Trust for
    a. Data encryption/decryption
    b. Device authentication
    c. Integrity of the TEE operating system
2. Privileged and secure access to peripherals (e.g. the touchscreen or fingerprint). Access is provided from inside the TEE, so malware on the REE operating system cannot spy on, or tamper with, the user interaction
3. Isolation of sensitive code execution
4. Secure data storage
5. Support of secure remote installation of applications

a. Device authentication to ensure the authenticity of the environment
b. Application encryption (only decrypted when executed inside the TEE)
c. Application personalization

Kinibi is included in the secure boot chain of the device and its integrity is verified at each device boot.

2.1 How to Leverage the TEE

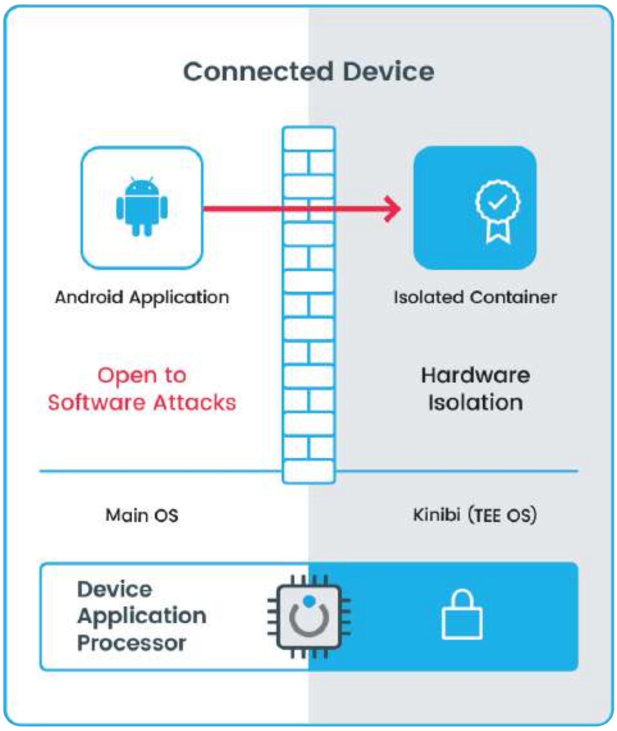


Figure 2 Principle of Application Leveraging the TEE

The goal of the TEE is to protect and isolate sensitive assets. When an application is developed using the TEE (in our example, an Android application), the application developer extracts the sensitive parts of their Android application and executes it in a separate application (the TA).

- Typically, the TA will process the sensitive data (crypto key, payment tokens…) as well as any sensitive user interaction (such as PIN entry, biometric authentication…).
- All the business logic or non-sensitive processing is handled in the REE Android application.

Protected from Android, the Trusted Application is executed in an isolated container. It is also completely isolated from other TAs which may be present in the TEE.

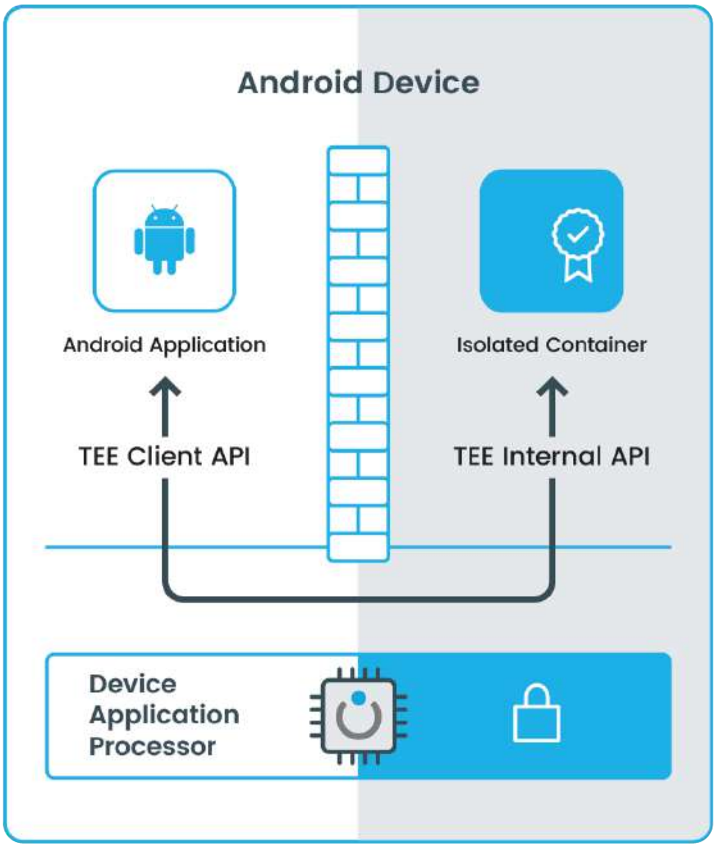


Figure 3 The TEE APIs

The TEE client API defines the transport layer enabling the communication between the Android application and its associated TA in the TEE.

The TEE Internal API defines the functions, such as cryptographic algorithms, secure storage and secure interaction with the device that can be used to develop a Trusted Application.

2.2 Fundamental TEE Features

2.2.1 Secure Storage

The TEE secure storage relies on a “Hardware Unique Key” (HUK) randomly generated and e-fused into chipsets at the time of manufacture. This HUK is only accessible by the TEE operating system (e.g. Kinibi). Trusted Applications inside the TEE have access to a key derived from this HUK. Applications in the REE operating system (e.g. Android applications), or even the REE itself, cannot access this HUK or the derived keys.

The sensitive data can only be encrypted and decrypted inside the TEE, remaining protected at all times from malicious applications running in the REE.

This also ensures that data can be bound to a specific device and therefore cannot be copied and re-used on another device. This becomes very relevant in a scenario where someone wants to ensure the uniqueness of a device.

2.2.2 Secure Peripheral Access

The TEE has the unique capability of being able to directly access peripherals, independently of the REE. For example, some devices today support the Trusted User Interface (secure access to the touchscreen and display) or secure fingerprint authentication (secure access to the fingerprint sensor). It is also possible to secure other peripherals, such as the camera, the speakers, the NFC interface or the microphone on the device. As long as the hardware supports it, even device sensors can be secured by the TEE.

What it delivers:

- Secure user interaction/authentication with the device (what the user sees, what the user enters, what the user does…)
- A physical authentication with the device can be ensured:
  - It is not a malware that is mimicking the user’s behaviour
  - Many of the software scalable attacks, such as replay or relay attacks, can be prevented by requiring the user’s approval using the TEE
- Service providers have the assurance of the identity of the person that has initiated the functionality (e.g. a transaction validation)
- Secure end-to-end communication can be performed

This secure access is performed through the implementation of secure drivers. However, it is not something that an application developer has to deal with. Trustonic collaborates with chipset makers and device makers to make these features available. Application developers can then access the TEE-internal API to leverage the secure peripheral access, whenever present inside the device.

2.2.3 Device Authentication

During the download/installation of a Trusted Application on Kinibi, the device legitimacy is verified. This ensures that a service provider knows if its application(s) and sensitive data are being installed on a trusted device.

In addition, each device has an embedded hardware unique identifier that enables a service provider to verify the identity of the device itself.

2.2.4 Secure Communication with Remote Entities

As we have seen, the TEE can securely store data. This implies that any secret usually used to authenticate an application can also be protected inside the TEE.

Thus, a Trusted Application can securely share secrets with a remote entity, such as a server or a secure element, in order to establish a secure communication channel. The remote entity has the assurance that the application it is talking to in the device can be trusted, since the secrets involved are strongly protected within the TEE.

By combining the secure user interaction with a strong device with application identity, Service Providers can have a high degree of trust in the service that they are deploying and can, therefore, enable more features.

3 TEE Security for Automotive Mobile Applications

A TEE-secured smartphone has the potential to become a virtual vehicle key, but offers many more possibilities too. It is now possible to control vehicle settings from a mobile phone, start the engine, drive the vehicle and manage user profiles. Many Android vehicle mobile applications are available on the Google platform today – and, if not properly secured, provide a high value target for hackers.

Android's notoriety for malware and security vulnerabilities is well known in the mobile industry. A presentation from Kaspersky[1] during the RSA 2017 Conference showed the latest issues found on Android devices running vehicle mobile applications. In particular, three attack techniques were listed (and none of the nine Android applications tested were protected):

1. Internal data leakage
2. Overlapping of the application
3. Re-packaging of the application

The TEE can help to prevent all such attacks.

3.1 Internal Data Leakage

Connected vehicle applications often store valuable and sensitive data on the mobile device (user login/password, authentication token, vehicle/driver data, profiles/settings and more.)

Two major concerns arise:

[1] https://www.rsaconference.com/writable/presentations/file_upload/hta-r10-hey-android-where-is-my-car.pdf

1. The cryptographic keys used to protect this data are usually protected by software protection only and are usually unencrypted at some point during the processing to handle the data. This means that an attacker can access it and decrypt the data.
2. Users often intentionally root their devices, or unintentionally install malware that makes sensitive files and data more easily available.

3.1.1 TEE Protection Against Internal Data Leakage

As shown in section 2.2, the TEE is a hardware-isolated environment, which is separated from Android and relies on hardware security to protect cryptographic keys and data.

This implies the following:

- The cryptographic keys used to encrypt data are never exposed to Android applications
- Malware cannot read the data associated with a Trusted Application
- Data can be bound to a single device, ensuring that it cannot be re-used on other devices
- Even on rooted devices, the TEE, its applications and data remain protected

Finally, part of the security design of an application is to make sure that, if sensitive data goes outside the TEE, for example to the vehicle or a remote server, it should be done via a secure end to end communication between the TEE and the remote entity. For example, it should be established via a secure channel between the mobile vehicle, the Trusted Application and the remote entity.

3.2 Overlapping of the Application

Application overlapping is a well-known technique for interception of user entries on a device, such as a login/password. This attack technique has proven successful in mobile banking/payments and can easily be replicated for mobile vehicle applications.

3.2.1 TEE Protection Against Application Overlapping

As we saw in section 2.2.2, the TEE can ensure secure and privileged access to peripherals on the device. This means that the touchscreen can be protected for a certain period of time in the execution of the vehicle mobile application and that a user can securely enter their login password. This is called the Trusted User Interface.

Even if an Android device is rooted or infected with a keylogger or a screenlogger, the user entry on the device leveraging the Trusted User Interface will be protected against such attacks.

3.3 Re-packaging of the Application

The concept of application re-packaging relies on modifying an application to inject some malicious code in order to steal sensitive information, recompile it and then send it to the victim. The victim then thinks that they are using a genuine app, without knowing that they have been attacked.

3.3.1 TEE Protection Against Application Re-packaging

When leveraging the TEE, the application developer isolates the sensitive code and data in a Trusted Application separate from the Android application. Additionally, the Trusted Application can be signed and encrypted by the Service Provider / app developer, which means that, whilst the Android application can be modified and re-packaged, the Trusted Application will not be affected and will remain secure at all times.

Finally, the service provider/app developer has control of their Trusted Application(s) (encryption, signature), which ensures that a change to the Trusted Application is under their control and could not be carried out by a rogue developer.

4 Virtual Vehicle Key with Trustonic

Trustonic has worked with a leading vehicle manufacturer to develop a virtual vehicle key solution. A demo was presented at the Mobile World Congress conference in 2017. Other demonstrations include Hyundai Mobis (at 2017 Consumer Electronics Show) and during the 2016 GlobalPlatform TEE conference, where there were demos of mobile virtual vehicle solutions utilizing the Trustonic TEE.

These solutions rely on the following TEE security principles[2]:

- Hardware isolation of the sensitive code execution
- Use of the TUI to authenticate the user and to control the vehicle (e.g. lock/unlock)
- Hardware protection of sensitive data

The TEE becomes the trusted environment of choice to enable new use cases, enrich the user experience and create differentiation in the automotive market with future-proof solutions.

[2] Public information

5 Applications of the TEE Beyond Vehicle Mobile Apps

The TEE meets the needs of various industries and Trustonic's website details many of the market verticals in which we are currently operating, see www.trustonic.com.

5.1 Premium Content

In the premium content sector (e.g. video streaming), Digital Rights Management is essential to protect the content published by studios.

The TEE is mandated by many Hollywood studios to protect high definition video. There are several features that the TEE delivers to achieve this:

- Hardware isolation from the Rich Execution Environment (e.g. Android), to encrypt/decrypt the streaming on the fly
- Secure storage of credentials used to decrypt the content.
- Secure display of the decrypted content, directly performed inside the TEE without going back into the REE, thus preventing the content from being captured. This feature is called "Secure Video Path"

Trustonic's TEE is used today to protect premium content from various providers across many devices.

5.2 Secure Messaging

Government/enterprise and even consumer messaging applications require high levels of security. Businesses need to better protect themselves against competitors spying on them, while consumers are facing privacy issues. Secure Voice over IP (VoIP) is a typical example of a messaging solution that can be made more secure by using the TEE.

Koolspan is an example of a Trustonic partner which provides such a solution. By protecting the encryption keys and enabling a secure communication with a relay server, the TEE provides the ability to harden phone calls and messaging.

5.3 Mobile Financial Services

Various assets/procedures can be protected by the TEE, whether these are payment tokens, credit card information, cardholder verification, transaction validation or device authentication. The assurance of higher-grade security enables financial institutions to deploy additional, new and innovative services.

Samsung, major card schemes, several banks and service providers already use Kinibi to secure their banking and payment solutions. Use cases span mobile banking, proximity and online payment, mobile PoS, cash withdrawal and peer to peer money transfer.

5.4 User Authentication

No matter what service is used (automotive keys, mobile banking, secure messaging, healthcare, physical/logical access…), there always is a need to strongly authenticate the user. These authentication services include One-time Password, standalone fingerprint-based authentication or other standards- based schemes, such as FIDO.

Symantec and HYPR are examples of providers of secure authentication solutions using Trustonic's TEE.

The TEE's ability to harden devices and protect applications has enabled organizations to leverage traditional consumer devices for both business and governments where they require a very high level of security, especially in Bring Your Own Device (BYOD) initiatives.

5.5 Securing the Internet of Things (IoT)

The number of use cases that the TEE covers seems limited only by the application developers' imagination. For example, automotive, financial services, home/building automation & surveillance, industrial, healthcare, smart cities etc.

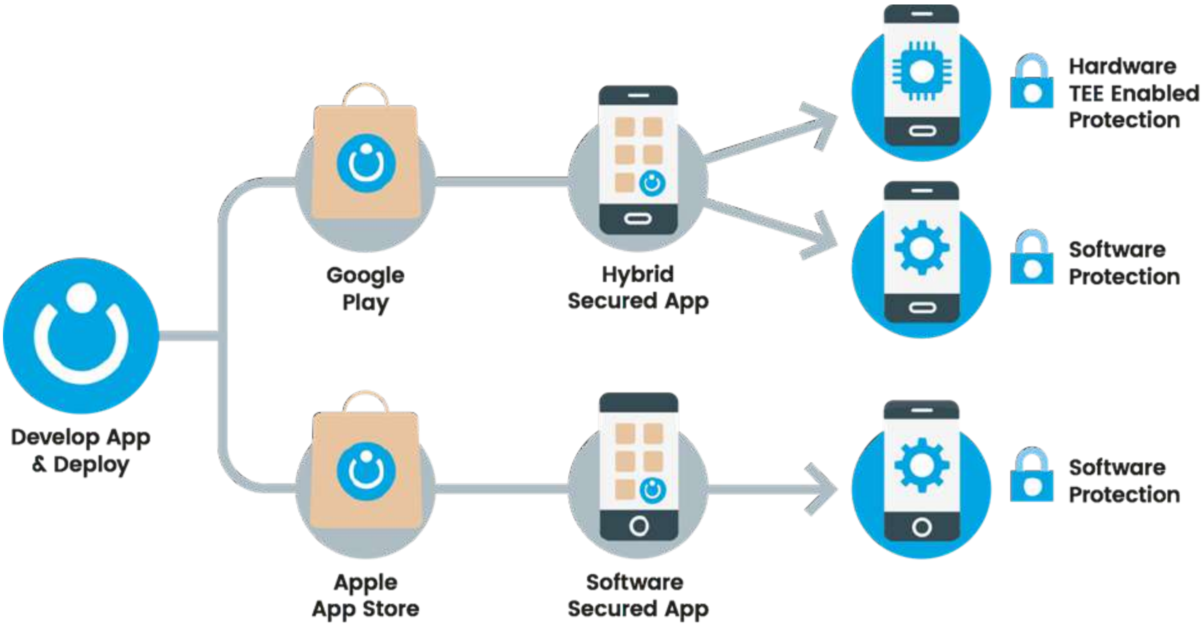
As security and privacy concerns keep pace with innovation, there is a strong need to build more secure and future-proof services. The TEE has a key role in enabling solution/service providers to innovate, distribute and manage trusted solutions in multiple marketplaces, leading to faster adoption, higher security and greater scale across numerous connected devices.

Trustonic is a founding member of the IoT Cybersecurity Alliance, along with AT&T, IBM, Nokia, Palo Alto Networks and Symantec. The group aims to research and raise awareness of ways to better secure the IoT ecosystem.

5.6 Non-Android and Additional information

For devices where hardware-security does not exist, or is not accessible to third-party developers, leading industry practice is to use whitebox cryptography software protection. Trustonic offers a unique value proposition for solution developers to use a single SDK, compliant with GlobalPlatform API standards, to build Trusted Applications that make use of best available security. That is, using the Trustonic TEE where present (currently available in over one billion devices) and reverting to a FIPS 140-2 certified whitebox cryptography where it is not. This provides coverage on all potential mobile handsets, including Android, iOS and others.

Any app developer simply takes a single set of APIs from Trustonic and the Trustonic code will utilize the optimum level of security deployed on each end device – TEE where available and software protection elsewhere:



6 About the Author

Florent Joubert, Senior Manager, Secure Services & Business Development

florent.joubert@trustonic.com

+1 425 892 3385

Florent has been involved in mobility, cybersecurity and standardization for all of his career, starting at Trusted Logic Mobility, a subsidiary of Gemalto. There, Florent gained experience as a product marketing manager for the Trusted Execution Environment (TEE). During his time at Gemalto, be became more involved in the Global Platform standard definition, bringing his knowledge to a wider industrial level.

Florent has been part of Trustonic since its creation in 2012 and has held a range of roles, focusing on building the security business across US and Europe with key partners, encompassing hardware manufacturers, financial institutions, carriers, government entities and global solution providers. Enabling the expansion of the use of TEEs and services across a wider range of device types, Florent is currently supporting the development of Trustonic's business in the Americas and program-managing major projects across the globe.

For more information on partnering with Trustonic for securing platforms and application protection contact your local sales team or visit https://www.trustonic.com/

TRUSTONIC

WHITE PAPER

The need for hardware-based security in mobile devices

VERSION HISTORY

Version	Date	Status	Modification
1.0	15 Mar 2017	Release	First release
1.1	24 Mar 2017	Update	Minor updates

TABLE OF CONTENTS

Why mobile security is important 2
Trustonic's beliefs 2
What is hardware-based security? 3
More detail on the alternatives to a TEE? 4
Where TEEs are in use today? 6
How do I use a TEE in my application? 7
About the author 10

WHY MOBILE SECURITY IS IMPORTANT

Securing mobile phones and other connected devices is becoming increasingly important, as these are now the primary means by which people access the web and other applications. Many people now rely on their mobile devices for a huge array of services, including banking, payments, work and personal communications (including voice, messaging and email), watching premium content, healthcare monitoring and much more.

There are many initiatives which require the use of a mobile device for user authentication. For example, in the European banking sector, the forthcoming PSD2[1] initiative will propose the use of biometric authentication through a mobile device to be used for approval of most payment transactions, irrespective of whether that transaction was initiated on the mobile device. For this and other new services to become mainstream, they need to be trusted and secure and, in turn, appropriately secured devices must be utilized.

Like PCs before them, mobile devices are susceptible to numerous threats. Spyware can monitor user activity to gather passwords and sensitive data, malware can infect applications and users may deliberately or accidentally install root kits that undermine any security the operating system provides. Given the increasing use of mobile devices for sensitive financial and personal information, the need for strong security has never been greater.

TRUSTONIC'S BELIEFS

It is a well-known fact that modern mobile operating systems such as Android are so complex that they inherently have many bugs, weaknesses and security holes. They are, therefore, open to malware and device rooting, which compromise the security of normal applications. Therefore, best practice is to isolate and protect the most sensitive code and data and to keep it as small as possible, in order to remove the possibility that weaknesses could be exploited.

[1] PSD2 is the second Payment Services Directive, designed by the countries of the European Union. This new EU directive will allow companies to give their customers the option of using third-party providers to manage their finances. It could revolutionise the payments industry, affecting everything from the way payments are made online, to what information is seen when making a payment.

Trustonic’s fundamental belief is that, when developing applications, security-related code and sensitive data should be isolated and protected away from the main application. That sensitive code should then be executed in an environment that is known to be trustworthy.

Currently, most applications running on mobile devices are secured by pure software technologies running on the main device OS. Whilst software security can certainly provide a level of protection and reduce the risk of attack, it requires regular application updates to keep ahead of the hackers and other malware that may be resident on any given device. Most software-based security solutions using software obfuscation or white-box cryptographic techniques also produce a noticeable impact on the performance of an application, as these techniques add significant code overhead. Furthermore, most of the software security solutions are not sufficiently diversified per unique device and are, therefore, subject to very scalable attacks.

Trustonic believes that security by design, built from the hardware level up, is the best mechanism for properly securing applications. Software security does, however, have its place. It provides a certain level of security generically and offers security on mobile devices where hardware security features might not be accessible in a scalable and economical manner.

What is hardware-based security?

Hardware-based security is enabled via a hardware-isolated execution environment for security sensitive code. This may be a separate physical processor, such as a smartcard (or secure element), a separate CPU, such as in Apple’s secure enclave, or a hardware mode of the main processor, called a Trusted Execution Environment (TEE) such as that delivered by ARM’s TrustZone technology. A TEE running on TrustZone is an example of the technology used by Trustonic for its smartphone-class products.

Hardware-based security utilizes physical hardware technology to protect against attacks. There are several different types of hardware-based security that offer differing levels of effectiveness, but they all protect fully against Trojans and other software-based threats. These are the threats that most organisations are worried about, as they are both scalable and replicable. Software-based security can be thought of like a vaccination, it will protect to a certain level for a while, but will need updating on a regular basis. On the other hand, hardware-based protection can be thought of as a cure.

Traditionally, the most common hardware mechanism was a SIM-based solution, preferred by the mobile network operators. In this model, the SIM is the device that holds the keys and performs cryptographic operations, but, as well as requiring a complex and costly TSM[2] infrastructure, the SIMs themselves are limited in power and capacity. An alternative model is an embedded secure element, preferred by some handset OEMs. The embedded secure element is technically very like a SIM, but differs in that it is physically embedded into the handset. It also requires a similar TSM infrastructure if post-deployment updates are needed. Neither model is open or scalable and deployments are dwindling worldwide.

The Trusted Execution Environment (TEE) is a hardware protection mechanism, requiring no additional hardware to be installed into the device and, therefore, results in no additional bill of materials cost to the OEM. The TEE makes use of the device's main processor which, in the clear majority of cases, can operate in a special operating mode, enabling the device to run two operating systems: the 'real-world' operating system (e.g. Android) and a 'secure-world' operating system (e.g. Trustonic's Kinibi). These two operating systems are physically isolated from each other.

More detail on the alternatives to a TEE?

Secure Element - In the banking and payments world, a secure element (SE) has typically been used to provide security. The secure element takes many forms, either on a smart card, a SIM or physically embedded into a mobile phone. As described previously, the secure element can provide secure key storage and a limited amount of secure processing, but access for an application provider to the secure element, whether embedded or as part of the SIM, is complex from both a technical and business model standpoint. Secure elements have very limited processing power, have access to limited amounts of memory and are restricted in their capabilities, as they are not directly connected to the different peripherals of the device.

The TEE has many benefits over secure elements. One of the major benefits to handset OEMs is the fact that there is no additional discrete hardware required, as the TEE is built-in on the main device processor. It therefore saves space and cost in the device, providing effective, affordable on-device hardware-based security.

Software - Software-based protection is another alternative and, whilst not as strong as a hardware-based security solution, offers a reasonable level of security and features. It does

[2] A TSM, or Trusted Service Manager, is a solution designed to deploy secure credentials to SIMs or embedded secure elements. The TSM enables service providers to distribute and manage their applications remotely, by allowing access to the secure element in handsets.

however suffer from several drawbacks; software protecting software is always prone to attack and, therefore, software-protected applications need to be regularly updated to keep ahead of the hackers. Software protection mechanisms, such as white-box and code obfuscation, can also have a level of performance impact on the application, as a large amount of additional code is required to deliver cryptographic and anti-tamper detection functions. In contrast, TEE-based applications run directly on the processor and have access to large amounts of memory. Trustonic delivers software-based protection as an integral part of its solution, thereby enabling protection across all available devices, not just devices with the embedded Trustonic TEE.

Android Key Store - Android provides applications with access to a TEE-backed key store, which provides effective protection against lost and stolen devices. However, it does not protect against software threats. Access to the key store also needs to be protected to stop rogue applications requesting the use of a protected key, thereby bypassing its effectiveness.

WHERE TEEs ARE IN USE TODAY?

Both Apple and Android rely on TEEs to secure their platforms, in fact Google now mandates the use of a TEE in Android to secure features such as biometric sensors, key storage and content protection. Many phone OEMs deliver system level trusted applications to provide capabilities around payment, secure content storage, DRM and other services. Samsung itself uses the Trustonic TEE to underpin its Knox security platform, to perform biometric matching as well as to deliver Samsung Pay services.

Trustonic believe that third-party applications should be able to gain access to the same level of protection as the OEMs and has worked hard to create the ecosystem that exists today, offering service providers with the ability to properly secure their applications on an ever-growing number of devices.

Samsung Pay is underpinned by Trustonic's TEE. Both key storage and cryptogram generation are performed inside the TEE, delivering a card scheme-certified solution.

Samsung ARTIK is an integrated IoT platform designed to simplify the process of delivering and launching IoT products. It has the Trustonic TEE at its core, delivering strong security for any solution.

Symantec VIP is a one-time code generator that uses the TEE to securely store the keys and code generation functions. It offers users with a Trustonic TEE-equipped device a lower cost, faster and more convenient method of accessing corporate services.

Samsung SDS FIDO is a solution where a biometric face recognition function is performed inside the TEE and a FIDO authentication credential is released if the faces match.

Alipay & WeChat Pay utilize the Trustonic TEE to secure a fingerprint sensor, enabling trusted and convenient user authentication and transaction validation.

Koolspan uses the Trustonic TEE to add an additional layer of security, safeguarding the TrustCall application on end-user devices against malicious attacks, thereby adding hardware-based protection to secure voice and text communications.

Shinhan Card & Hana Bank use the Trustonic TEE to enable trusted and convenient one-time password on mobile to deliver premium banking services.

HOW DO I USE A TEE IN MY APPLICATION?

Whilst TEEs are used in almost all Android devices today, unless they are open, they are of no use to a third-party application vendor. Trustonic believes that an open ecosystem is vital to ensuring that application developers have access to hardware-based device security. Trustonic is the only vendor delivering third-party developers access to the TEE and delivers its TEE (called Kinibi) to silicon and device vendors, who embed it into the heart of their devices. Trustonic's TEE has so far been embedded into over one billion[3] devices and every one of these devices is capable of hosting third party-secured applications.

Applications can be developed that consist of both a real-world component (running on the main OS of the device like Android) and a secure-world component, a trusted application, running inside the TEE.

The functions to manage features like the general user interface, high-level communications and business logic would typically remain in the real-world Android application, whilst functions dealing with sensitive operations such as user authentication, communications encryption, cryptography and secure storage would be executed and protected inside the trusted application running inside the TEE.

Any Android application including malware is physically unable to "see" and modify what is happening in the trusted applications running inside the TEE. The security is delivered at the processor level and cannot be bypassed by software, even if the device is rooted. This level of hardware-based separation ensures that rogue applications like Trojans are unable to gather sensitive information from resident applications and, therefore, cannot interfere with them.

Multiple trusted applications, usually coming from different sources (OEM, different service providers) running in the TEE, are also completely isolated from each other. As well as embedding the TEE into the device, each device is loaded with a unique device key - a unique hardware-based root of trust. This unique identity is injected when the device is on the production line and guarantees the authenticity and security of each Trustonic TEE-enabled device.

Trustonic also delivers a Trusted Application Manager (TAM), which enables secure application deployment and lifecycle management. The TAM can be hosted by the service provider or by a trusted third party, delivering them control of deployment of applications

[3] Trustonic announced at Mobile World Congress in 2017 that its TEE has been embedded into over one billion devices. http://bit.ly/2mF8NIy

and credentials. The TAM, utilising the multiple application capability of the Kinibi TEE, is what delivers the capability to load secured applications into the device post-deployment.

Trustonic's TEE delivers several unique functions that cannot be delivered through software or secure elements. One key feature is a Trusted User Interface (TUI). The TUI enables applications to use the touchscreen and display without the ability for other applications to eavesdrop. It delivers the ability to perform features such as a secure PIN or passcode entry screen, or a truly secure messaging application. Many messaging apps claim to be secure, but most are just securing the communications and therefore any Trojan running on the device could intercept the display or touchscreen and could gather data that way. With a TUI that is not possible.

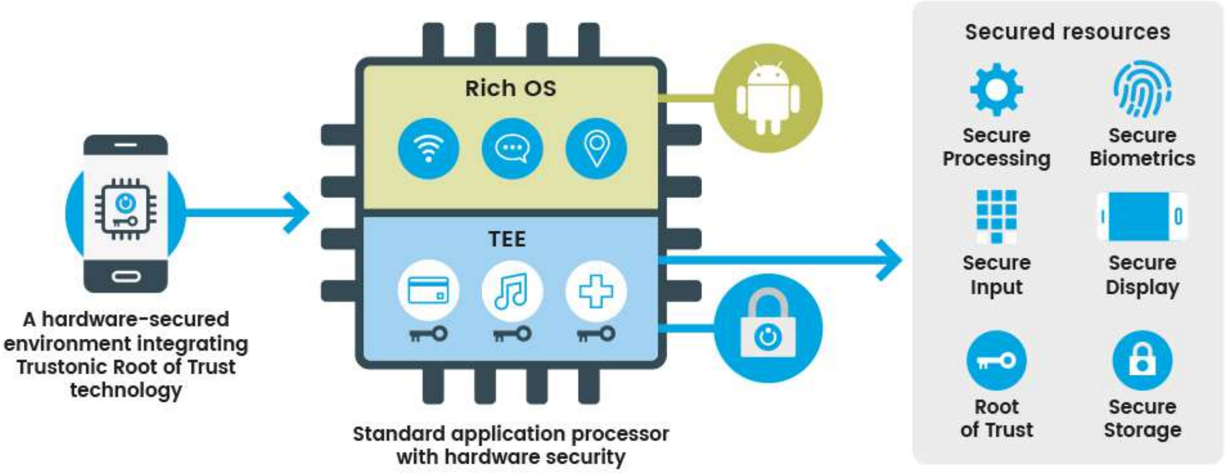

A hardware-secured environment integrating Trustonic Root of Trust technology
Rich OS
TEE
Standard application processor with hardware security
Secured resources
Secure Processing
Secure Biometrics
Secure Input
Secure Display
Root of Trust
Secure Storage

Figure 1 - TEE secured peripherals

Trustonic ensures that its products are secure by submitting them to security evaluations performed by independent certification laboratories. The Trustonic TEE is the first to have successfully achieved Common Criteria security certification for a TEE, based on GlobalPlatform's[4] TEE Protection Profile. The Trustonic TEE is also compliant with the GlobalPlatform TEE configuration version 1.1. The Trustonic TEE will be undergoing FIPS certification during 2017.

[4] GlobalPlatform (www.globalplatform.org) is an international body that defines standards around hardware security. Trustonic has been an active member in the working groups and has helped define many of these standards. Trustonic meets these standards and certifies its products against them. GlobalPlatform has more than 110 members including MasterCard, Visa, ARM, Apple, Gemalto and Samsung.

Trustonic delivers a secure ecosystem enabling handset manufacturers, mobile application developers and service providers to deliver secure applications onto mobile devices. Trustonic has been working for over four years with chip manufacturers, mobile phone OEMs and IoT industry vendors to embed security into the heart of their connected devices. Once in-situ, this secure platform can be used by the device manufacturer to secure system-level services, as well as by service providers to secure their applications that will run on the devices.

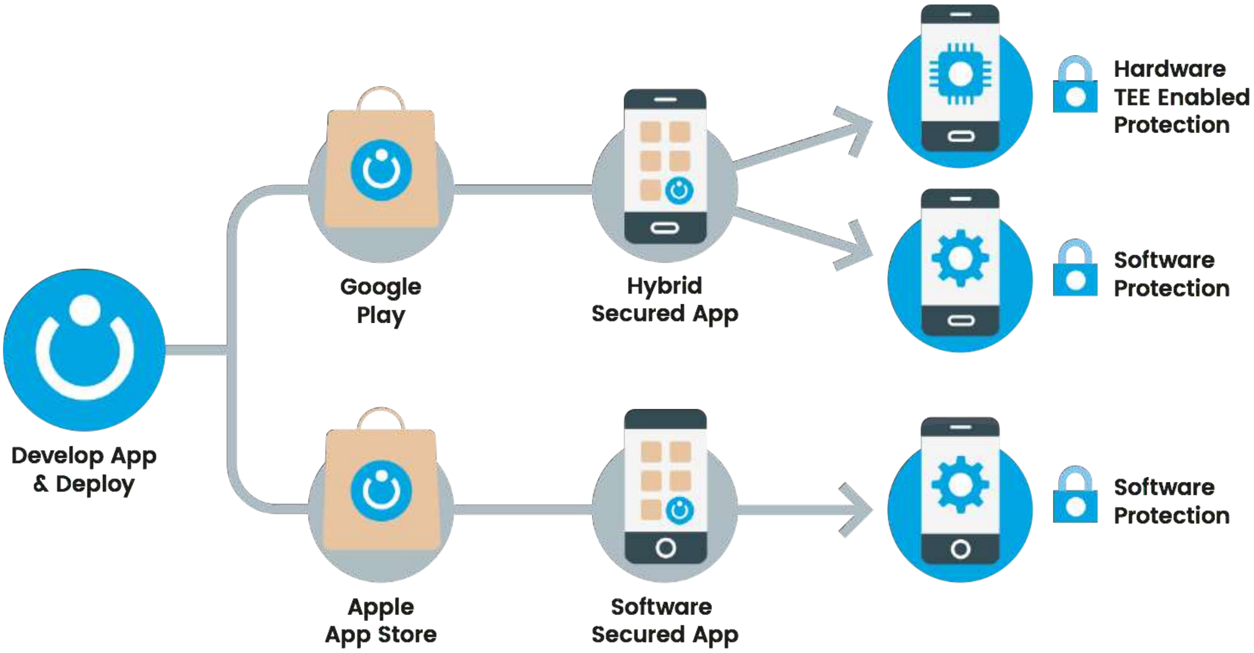


Figure 2 - Hybrid application deployment

If you have a need to deliver secure mobile applications to your employees or customers, then Trustonic can help. We provide a toolkit and training to get you started. When you develop your applications, you need to identify the security-critical parts and migrate those to a trusted application, using the Trustonic GlobalPlatform compliant API. A secured application, including a combination of hardware and software-based security, will be created. The application can then be published into the appropriate app store as usual and, at runtime on the end device, the highest level of security available will be deployed. Over time, as your customers upgrade their devices, more of them will be able to take advantage of hardware-based security.

To find out more about how Trustonic can deliver the best on-device security to your mobile applications, please email enquiries@trustonic.com or go to www.trustonic.com/contact to request a meeting.

ABOUT THE AUTHOR

Paul Butterworth, the Strategic Marketing Director at Trustonic, has 25 years of experience in the IT security and card payments industry. Currently, he is helping Trustonic to deliver ground-breaking products to the mobile security market. Prior to joining Trustonic, he spent four years at Proxama, a leading mobile wallet and proximity marketing organisation, helping to drive technology strategy and leading the R&D team. In previous roles, Paul worked for ViVOtech as the lead technical resource in Europe, helping to deploy TSMs into the market, for nCipher as the product lead for the payShield HSM and for Verifone in a pre-sales role for the eCommerce division. He has a wealth of experience in understanding the challenges organisations face around security and deployment of large-scale mobile solutions.

Trustonic is a technology company whose mission is twofold:

- To establish a common security platform embedded in smart connected devices
- To enable app developers to utilize these advanced security capabilities