

TRUSTONIC RISCURE

Demystifying Secure Development for Edge Devices & Apps

Understanding security testing, evaluation and certification, and how they benefit the design, development and launch of secure products and services

April 2020

enquiries@trustonic.com

inforequest@riscure.com

Contents

1.0	Executive Overview	2
2.0	Introduction	3
3.0	Have You Heard About Secure Development Lifecycles (SDL)?	4
4.0	What is the Difference Between Security Testing, Evaluation and Certification?	5
5.0	What Gets Tested, Evaluated and/or Certified?	6
	5.1 Secure platform	6
	5.2 Application	6
6.0	Who Defines Security Requirements & Manages the Certification Processes?	8
7.0	How Might an SDL Work in Practice?	10
8.0	Why is Testing, Evaluation and Certification a Good Idea?	12
9.0	Vertical Industry Examples	13
10.0	Selecting the Right Certified Security – A Focus on TEE as a Secure Platform	15
	10.1 Tested, evaluated and certified Trusted Execution Environments (TEEs)	16
11.0	Conclusion	17
12.0	About Trustonic & Riscure	18

1.0 Executive Overview

With data breaches and security vulnerabilities creating front-page headlines, especially with the spike in attacks and fraud activity experienced during the COVID-19 crisis, security is increasingly becoming a product differentiator and business enabler in edge devices. From smartphones and mPOS terminals right through to automotive and IoT devices.

The impact of a successful breach can be catastrophic, with a significant impact on end-user confidence and loyalty. While mitigating these scenarios with risk management is fundamental, security can also be the foundation for technical and business enablement and innovation.

This paper will be valuable to:

- **Development teams** interested in implementing a secure development lifecycle to achieve security by design;
- **Executives such as CEOs and CFOs** who want to prevent reputational and revenue losses;
- **Product managers** working to unlock key geographical and vertical markets and safeguard their products and data.

This is the first in a series of papers on the role and value of security testing, evaluation and certification in the design, development and launch of secure products and services. In this paper we will focus on security for edge devices – like smartphones, in-vehicle infotainment (IVI) systems, smart TVs, smart home hubs etc. – that run applications for consumer end-users.

This paper offers an introduction to the Secure Development Lifecycle (SDL) and to the difference between testing, evaluation and certification. It also explains how they apply to the platform and application layers of devices, offers insight into the different certification bodies and requirements and discusses secure development lifecycles before highlighting the value of certification for key vertical markets and implementations. Throughout the paper, a number of misconceptions are clarified, and expert insights offered.

As standards and certification often follow innovation, this paper largely focuses on introducing some established and fast-developing industry-, stakeholder- and region-driven certification schemes and requirements. There are therefore some notable omissions from the document which Trustonic and Riscure may return to in a later paper. For example, several security standards and certification schemes for IoT devices are currently being defined.

Trustonic's mission is to embed the best security into the world's smart devices and apps; empowering mobile and IoT developers to build the trust required to deliver simple, fast and secure solutions. Riscure helps customers around the world to build robust hardware and software solutions, while speeding up the process of secure development and certification.

Trustonic and Riscure work closely together to drive more secure technology implementations. The two companies share a vision to help the ecosystem to better secure devices, apps and data.

2.0 Introduction

Edge devices and embedded systems play a hugely important role in our day to day lives. Smartphones, automotive systems, manufacturing equipment, sensors, medical equipment and many other edge devices perform increasingly critical tasks and all need to be built on secure platforms with proven reliability, trust and security.

The proliferation of connected devices is set to continue and gather increased momentum. [Industry analysis](#) projects that more than 41 billion devices will generate nearly 80 zettabytes of data in 2025.

When plotted against the [average cost of a data breach in 2019](#) – between \$1.25 million and \$8.19 million – the challenge facing product and service developers looks stark. Nearly 15 billion data records have [already been lost since 2013](#) so the rapidly expanding attack surface could compound matters further if security is not taken seriously.

Additionally, many of today's connected devices do more than simply provide information at your fingertips – they can make use of sensitive data, gather information and even impact the physical world, often in critical ways. In light of this, there is a need for ubiquitous and standardized platform, edge device and application security. This applies to all use cases as security will be necessary to prevent devices from becoming an entry point into a network or a platform for attacks.

The second largest DDoS attack of all time was directed at Dyn in October 2016.

The attack disrupted major sites including AirBnB, Netflix, PayPal, Visa, Amazon and GitHub and was achieved by creating a botnet from compromised devices including smart TVs, cameras and baby monitors.

Clearly, smart products and services need to be protected. This is only achievable with a structured approach to secure development to achieve demonstrable security and reduce risk.

3.0 Have You Heard About Secure Development Lifecycles (SDL)?

Secure solutions are not designed and developed by accident. It requires a thorough understanding of the threat scenarios and the security expectations or requirements of the product. A secure development lifecycle (SDL) is therefore an important success factor for achieving secure solutions. This brings security to the center of each development phase, from the initial design right through to the final implementation.

What is a secure development lifecycle (SDL)?

SDL is a process that standardizes security best practices across a range of products and/or applications. It usually captures industry-standard security activities, packaging them so they may be easily implemented. Without it products are more susceptible to being shipped with vulnerabilities, security mistakes get repeated, security problems get identified too late and end users have little assurance that products and services are secure.

As development needs to follow an SDL, there are two options. Development teams can build their own or they can follow pre-defined examples from companies like Microsoft and Cisco.

4.0 What is the Difference Between Security Testing, Evaluation and Certification?

As part of the SDL, it is important that product development and security teams can verify that, during each phase of a product's lifecycle from development to end-of-life, the latest design conforms to the defined risk management plan. To achieve this, products can be tested, evaluated and/or certified at various stages. Each process adds value to product development teams and the wider marketplace (which will be discussed later) but what's the difference?

Security testing – Security testing is the process of determining the possibility and feasibility of specific attacks against a certain product, or features within a product. Testing is performed either on-site or in a security laboratory and engaging security experts in the development testing phase is considered best practice.

Security evaluation – An evaluation is an expert security assessment of a product, its lifecycle and/or secure development process which is backed up by analysis and penetration testing conducted by a security laboratory. As such, it is a more formal process than security testing. It is usually carried out based on a public or private industrial standard and evaluation methodology.

Security certification – The certification process engages an accredited security laboratory to evaluate a solution against a set of formalized security requirements and standards such as a Common Criteria protection profile. Upon successful completion of the evaluation, a certification body issues a written certificate to confirm that the product, platform or app has achieved the required levels of security. For certain industries – like payments – achieving successful security certification is a prerequisite for the mass deployment of a solution.



Misconception:

Security testing happens at the final stage before launch.



Reality:

Security testing happens throughout the development lifecycle to spot design and development issues as early as possible and to mitigate delays at the final certification stage.



Misconception:

We don't need third party assessment, we perform all assessments internally.



Reality:

External and independent eyes routinely add significant value to implementations. External security laboratories can offer a wide range of technologies, market knowledge and experience. Internal teams are focused on a limited number of products.



Expert perspective:

“Security testing can demonstrate robustness but is limited in its scope. Security evaluation uses a structured, holistic approach to assess the security robustness of a solution based on its intended usage, the design, implementation and often its development cycle.”

Jasmina Omic, Riscure

5.0 What Gets Tested, Evaluated and/or Certified?

Now that the nuances of each process have been defined, it is important to understand that security evaluation and certification can be a requirement for different parts of devices. For simplicity, the below outlines the relevance of testing, evaluation and certification for two 'layers' of a device: a secure platform and an application that can run partially on the secure platform.

5.1 Secure platform

Increasingly, sensitive code which manipulates sensitive data is being executed within a specific environment that is tailored for secure operations. This environment, commonly called a secure platform, can be a combination of hardware and OS/firmware that can be evaluated and/or certified for use within a device and across various vertical use cases. Examples include secure elements and trusted execution environments (TEEs) that are used to secure code and data.

Testing, evaluation and certification assesses all facets of the secure platform and embedded sub-system. Ranging from high-level architecture review and firmware analysis to in-depth logical and hardware security testing depending on the threat model. Any code running on a tested, evaluated and certified secure platform will benefit from the assured security features offered by the secure platform.

5.2 Application

An application might be executed solely in the main device OS (e.g. Linux, Android or a RTOS for low-end IoT devices) or it can be split; with the most sensitive part of the application code running on a secure platform like a TEE. Depending on where it is located, the application can rely on the secure platform, and its security features, or it will need to embed its own security mechanisms when it can't rely on a secure platform.

Regardless of the run location, application security testing is the process of testing, analyzing and reporting on the security level and/or posture of an application while using some assumptions for the running environment, which can be a secure platform. The use of an evaluated or certified secure platform will give a reliable assurance level for the application security features provided by the secure platform.



Misconception:

Testing of the final device is always possible and is the best approach to determining security of a product.



Reality:

In practice, many devices are complex systems, potentially comprised of multiple execution environments. As such a thorough analysis of all sub-systems at the same level is often impossible. It is therefore common to focus on the secure platform(s) of a device that will protect devices' most sensitive code and data.



Misconception:

My application runs in a secure platform that protects it, so I don't need to test or evaluate my application.



Reality:

This is untrue. The design or the development of the app can integrate vulnerabilities that the secure platform will not be able to mitigate effectively. Buffer overflow vulnerabilities are one example, or an incorrectly designed API can leak sensitive information.

Overall, though, the application's security is tested independent of its running environment and is used by developers, security experts and certification laboratories to test and gauge the security strength of an app using manual and automated security testing techniques. The key objective is to identify any vulnerabilities or threats that can jeopardize the security or integrity of the application and its assets.

Security evaluation adds value as it will identify security flaws or weaknesses in protection in an efficient and cost-effective manner. Security evaluation and/or certification of an application is often a requirement.

6.0 Who Defines Security Requirements & Manages the Certification Processes?

Solution development teams need to know which certifications are relevant for their product. Depending on the use case, intended market and geographical usage of the product, global standards will likely need to be considered alongside local requirements. This will result in a range of certifications that need to be obtained and requirements to align with. We can consider the motivation behind these different certification approaches as follows:

(International) general purpose certification – E.g. Common Criteria, GlobalPlatform. These bodies deliver a common basis for certification which can, in turn, be the basis for additional combined certifications. They do not have direct market or commercial pressure to bring solutions to market. They offer a framework which risk owners (e.g. end-users, card brands, integrators and vendors) across different verticals can select based on whether they accept the certification to be sufficient for their needs as part of their risk management process.

General purpose & regionally-defined certifications – E.g. FIPS (US), various national EU schemes (BSPA/The Netherlands, CSPN/France, etc.), AISEP Australia. These national standards specify requirements for computer security and interoperability that are specifically relevant to the needs of the region.

Stakeholder-driven certification – E.g. PCI Security Standards Council (SSC) and EMVCo. These entities define requirements for payments actors to align with. Issuer and acquirers can then launch with defined levels of risk management and assurance. There is a direct balance between the required security assurance and the market pressure of bringing the solutions to market.

A non-exhaustive list of evaluations, certifications and security programs relevant to a particular technology or market can be found on the next page:



Misconception:

The security lab issues the final certificate.



Reality:

The lab performs the certification process on behalf of the certification body. The body then issues the certificate and makes the final call about the completeness of the evaluation, the sufficient assurance level and the need of any security guidelines for the product user.











Misconception:

I want to move quickly to launch my new product. I'll spend time on security in the next generation of my product or will provide a SW update to strengthen security later.



Reality:

You don't want your launch to fail because of a security vulnerability or be unable to perform security updates because you don't have the trusted foundations to do so. These issues could significantly damage your brand.

		(Secure) Platform	Application	Device
Vertical Agnostic				
	Common Criteria through National CBs	✓	✓	✓
		✓		
Regional Government Schemes e.g.	 ANSSI CSPN	✓	✓	✓
	 FIPS 140-2	✓		✓
Payment Acceptance				
	Payment Terminal	✓	✓	✓
	Mobile	✓	✓	
Payment Card				
	Secure Elements	✓	✓	✓
	Mobile Execution Environment	✓	✓	
IOT-Related¹				
		✓		✓
	PSA	✓		



Expert perspective:

“IoT is a particularly interesting area. In such a rapidly developing and fragmented ecosystem, we can see both existing certification bodies working to bring much needed trust to IoT devices and services, in addition to a number of new best practices and standards emerging. These will undoubtedly consolidate over time. However, as things stand, product and service developers should work with security experts to identify the relevant requirements for their implementations.”

Christophe Colas, Trustonic

¹ For a more detailed overview of schemes in the IoT space: https://www.eurosmart.com/wp-content/uploads/2020/02/2020-01-27-Eurosmart_IoT_Study_Report-v1.2.pdf

7.0 How Might an SDL Work in Practice?

Adding security features alone won't make a solution secure. Security by design can only be achieved when initiated from the development process onwards. This is done by implementing an SDL with threat modeling, secure design as well as testing and verification along the development path.

It is also worth noting that security testing and evaluation is a bespoke process. Automated 'push button' testing approaches can only go so far against attackers and needs to be augmented with intelligent security testing that approaches the product or solution from the perspective of an attacker. This is typically called penetration testing. The weakest points of any solution lay between the boundaries of the security functions and can only be detected by adaptive thinking. Robust security testing therefore relies on independent security experts attempting to circumvent the security features that have been implemented to protect the solution. They often need to think creatively and 'out of the box' to achieve this.

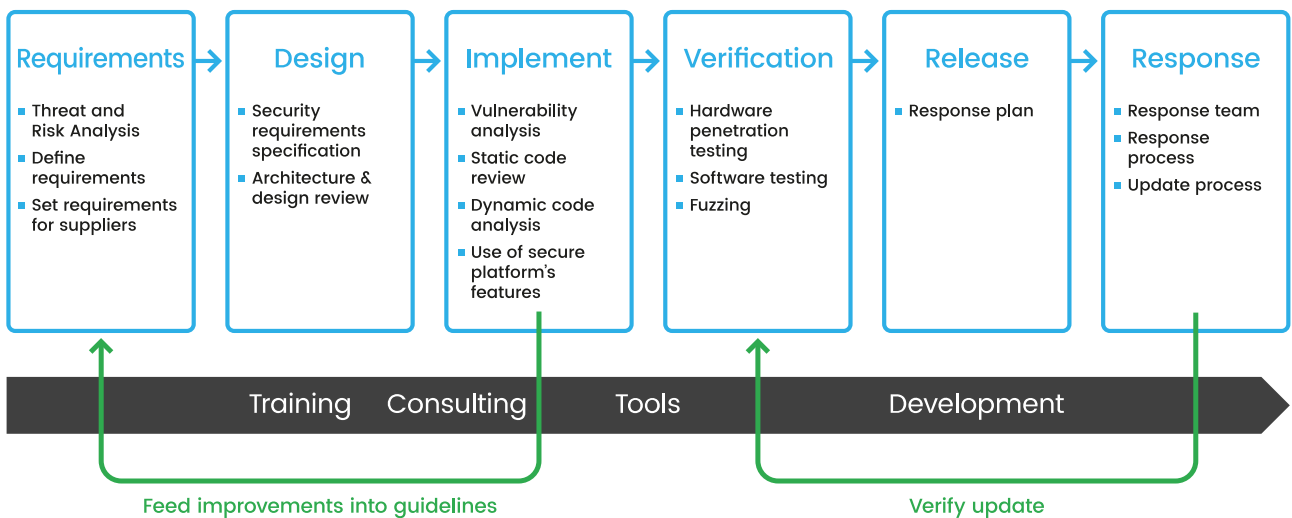
White-box (where the internal structure / design / source code / implementation of the item being tested is known to the tester) and black-box testing (where the internal structure / design / implementation of the item being tested is not known to the tester) are also common types of security evaluation that bring different perspectives to the evaluation process.

At its simplest level security experts can assist you in defining the security requirements for your product or service, ensuring secure product and code design and performing security assessments and testing on the final product.

Here is a simplified, non-exhaustive example of how as SDL might be implemented to develop, certify and launch a secure product:

Misconception: Security experts only add value for product evaluation and certification.

Reality: To achieve a secure product or service, security experts should be involved from project initiation at the design phase, right through to launch.



The security requirements phase uses threat modelling and risk analysis to define the product requirements. These are usually in line with industry standards or based on responses to problems that have occurred in the past.

The security design phase is about defining an architecture (for a single feature or the entire product) and then reviewing it for potential vulnerabilities. It is important to ensure the design follows the security requirements that were defined in the previous phase and that it is based on the risk analysis.

The implementation or coding phase sees the developers follow the design description to build the solution. This process should also be augmented with a security code review of the most sensitive software and partial testing processes.

The verification phase implements functional and security testing and evaluation processes as required. Once that is complete the product can be certified. If no certification is needed overall evaluation of the complete solution is beneficial.

The release / response phase(s) is initiated when the product or service is ready to be sent to end users. The management of security does not finish when the development is done, however. It is important that measures are in place for users and security researchers to report security problems and that a process is defined for the response team to react to identified vulnerabilities.

Ensuring security best practices are considered and implemented at every phase is the best way to achieve a successful final certification. This, in turn, delivers assurance that a secure product or service is in the hands of your end users.



Misconception:

The evaluation of code and documentation is not beneficial for us. I just need to provide the final product.



Reality:

Assessment and assurance levels are more effectively optimized by providing documentation and source code.



Expert perspective:

“Is there a place for ethical hacking and bug bounty programs? They have value at the end of the development cycle and into the device’s lifecycle in the field. Secure development lifecycles are not just about building the security, vendors need to have a clear process for the community to report vulnerabilities and then need defined procedures for how to respond and issue patches where possible. But this is a big challenge for the industry, particularly the device ecosystem, as not every product can be patched seamlessly and globally.”

Jasmina Omic, Riscure

8.0 Why is Testing, Evaluation and Certification a Good Idea?

There are many reasons to perform security testing, evaluation and certification on devices and applications. At its highest level, it is obviously essential that potential vulnerabilities are identified so systems do not stop functioning or get exploited. It also helps in detecting all possible security risks in the system and helps developers in fixing these problems through coding.

But the certification process is not only about technology, it can be both a safeguard for your business and an enabler. Here are a mix of benefits to prioritizing security by design and a robust testing and certification program for your products and services.



Misconception:

You can only evaluate a product against an industry-defined standard.



Reality:

Innovation often moves faster than standards, so security laboratories often evaluate products using bespoke test plans based on general methodologies.

Business benefits



Market access

Certifications open doors to both geographical and vertical markets. For example, FIPS is a requirement for the U.S. marketplace and EMVCo is essential for payments.



Security liability / risk management

In vertical markets, like payments and content protection, certain parties are responsible for risk management and are liable in the event of an attack or a breach.



Demonstrate robustness

Security is often a differentiator for manufacturers and developers when selling products. Even where there are no defined specifications, tailored evaluation can be a way to prove worth to potential customers.



Reputation protection

A successful cyber-attack can cause major damage to your business. It can affect your revenues, as well as your business' standing and consumer trust.



Build additional services

Service providers can use certified and trusted platforms as a foundation on which to build new value-added services because of higher trust.

9.0 Vertical Industry Examples

Many of the benefits outlined in the previous chapter can be applied to various vertical use cases. Sectors including industrial IoT, premium content protection and digital rights management (DRM), mobile payments, healthcare, automotive, smart infrastructure and government identity all rely on certified technologies to protect data and intellectual property.

Please find below some notable examples of mature and emerging vertical markets, use cases and technologies which benefit from security testing, evaluation and certification.



Mobile payment, banking & POS – device and in-app protection is fundamental across the board, making evaluation of the security sensitive parts essential.

- **Cloud-based payment (CBP) & OEM Pays** – For EMV® CBP, as the secure element is emulated in software via host card emulation (HCE), the security requirements on the software components increase. For OEM Pays, security certification evaluations are performed according to payment scheme requirements for both TEE and secure element-based solutions. Securing biometric user authentication with Consumer Device Cardholder Verification Methods (CDCVM) involves multiple parties so the major payment schemes have programs in place to verify the biometric devices and the end solution. Visa and Mastercard have mandated security evaluation for OEM Pay-integrated CDCVM since 2017.
- **mPOS** – mPOS solutions can be purely software-based apps on a smartphone, or hardware/software combined solutions based on a TEE platform. The security focus is therefore on logical attacks such as manipulation, acquisition or matching, and the requirements are scoped for the specific component the manufacturer would like to certify.
- **Mobile banking & fintechs** – Market evolution, particularly PSD2, is driving rapid change and financial institutions are particularly vulnerable to threats. Successful attacks can result in brand damage, legal and regulatory challenges, in addition to the financial impact. In-app protection and secure development processes are therefore essential to protect both banks and customers.



Content protection & DRM – This is a complex and growing ecosystem.

- **Content providers** need to protect intellectual property and revenue across an ever-growing range of devices and channels. Trusted and certified secure platforms enable this.
- **Mobile network operators** working with streaming devices need to protect content end-to-end to fulfil their obligations to content providers. Security evaluation mitigates overall risk and the potential impact of the device on backend systems and business models.
- **Chipset manufacturers** need to provide a platform, with demonstrable security, that fulfills the security requirements of the content owners, content service providers and conditional access (CAS) vendors.
- **Developers of software-based DRM solutions** need to be accredited by existing programs or demonstrate the security of the solution to content owners. They should consider evaluations in line with requirements like ChinaDRM and PlayReady.



Government ID – A wide range of secure documents – such as passports, drivers’ licenses, national ID cards, health cards, resident permits, and vehicle registrations – are now being issued, personalized and managed on digital devices like smartphones. Government services are also being made available online, abstracting identity verification beyond the ID document itself, and identity platforms are also being made available to third party app, as in India and Indonesia. To maintain trust and privacy, robust and demonstrable security is essential.



Emerging use case – Automotive – Modes of transport are increasingly connected and are evolving more and more quickly. The same is true of the related security risks.

- **Digital car key storage & sharing** on a mobile device deliver convenience and enhanced user experiences, reduce cost and enable new and innovative use-cases but require robust security to protect the asset.
- **In-vehicle infotainment & telematics** – increasingly sophisticated computing systems manage all areas of the vehicle and require a high degree of trust and reliability. In addition, they must be built on a secure foundation that can stand the test of time for many years and possibly for decades.

10.0 Selecting the Right Certified Security

– A Focus on TEE as a Secure Platform

Smart and multi-functional devices, whether IoT, mobile or automotive, are composed of multiple technologies and execution environments which can provide a spectrum of options for secure application development. Security is often best achieved by combining multiple layers of technology, but security is not the only consideration.

The right security is chosen by finding the right balance between the security level, the impact on usability, performance, scalability and reach of the solution.



Expert perspective:

“Sometimes security is at odds with the functionality and usability of the product. If users experience friction in services, adoption or use will likely be impacted along with reputation. Security needs to be appropriate and in concert with the functionality and use case of the product. For this reason, there are multiple certified security components available which can be used in isolation or together to effectively protect and enrich devices.”

Christophe Colas, Trustonic

Regarding reach and scalability, the accessibility of some security technologies is practical consideration. For example, only high-end smartphones have an embedded SE and even when they are present, some network operators or OEMs restrict access to it.

Trusted execution environments (TEEs) were designed to provide the best balance between dedicated hardware elements – offering high security, but with a significant cost, performance trade-offs and more limited functionality – and software-only security that inherently offers lower levels of security protection.

Over the last five years, TEEs have become the de-facto hardware-backed security technology for Android smartphones, protecting biometric authentication, premium content, cryptographic keys and related operations. The security platform has achieved this success because it can offer a hardware root-of-trust / security anchor within a device, while at the same time being more efficient than dedicated SEs due to the extensive resource sharing with the device systems.

Trustonic’s TEE – part of the Trustonic Secured Platform™ (TSP™) product – is deployed in over 2 billion smart devices including the leading Android smartphone brands and in automotive IVI head units. It provides a secure environment to protect critical device services and applications. It is Common Criteria, GlobalPlatform and EMVCo certified and provides security-by-design from the silicon level up, with no additional bill of materials cost, and has been designed to offer hardware protection to applications that can be downloaded by end users.

The TEE is enabled by a secure ‘mode’ of the main processor in a smart phone or other device. This enables a second, security-focused, operating system to run alongside the ‘Rich OS’ such as Android or Linux. TEEs have become almost universal and are used to protect both the device and

applications running on it. The TEE can provide access to strong device identity and is an integral part of secure boot. It also offers secure services to the Rich OS, such as cryptographic routines and key and data secure storage by providing isolated safe execution of authorized security software known as 'trusted applications'.

TEEs are an ideal choice for many secure applications, and for those developing mobile applications, Trustonic is the *only* vendor to enable full access to the TEE through its Trustonic Application Protection (TAP) SDK. TAP even enables access to other 3rd party TEEs such as Huawei. This means accessible TEEs are therefore much more widespread than accessible SEs. Unfortunately, some vendors, i.e. Apple, do not allow 3rd party TEE access; and for such devices Trustonic provides a 'software TEE' implemented using in-app protection measures like white box cryptography and code obfuscation.

10.1 Tested, evaluated and certified Trusted Execution Environments (TEEs)

The entire TEE system is a critical component for both the application using it, and for system services implemented using it.

Certified TEE's offer benefits to different players:

- **TEE vendors** can offer assurances to the market that their product meets industry-defined security levels.
- **Chipset and device manufacturers** can integrate a proven, trusted security platform that has been robustly evaluated in line with industry-agreed requirements.
- **Application and service developers** can have confidence in the device hosting their software. Apps can also be developed once and deployed across a broad range of devices, which enables universal and consistent risk management strategies and saves time and money.

11.0 Conclusion

Secure solutions are not designed and developed by accident. Trust is the result of careful planning and expertise.

This paper has outlined why a secure development lifecycle (SDL) – incorporating appropriate security testing, evaluation and certification – is essential to both achieve the levels of security and assurance defined by development teams, and meet industry, market and geographical requirements.

It is important to approach this not as a technical challenge, but as a process that is fundamental to the quality of your technology and the management of risk for both you and your end-users. All too often though, people forget that the right security can also be an enabler of both innovation and commercial value.

The challenge is to identify the right security processes, technologies and certifications that will deliver the required assurance and add value to your products, services and, by extension, revenues.

This can be a complex and nuanced process where significant expertise is required. But you are not alone and do not need to become a cybersecurity company or expert to get ahead. Partners like Riscure and Trustonic can help you to define and implement a tailored SDL to support you in your design, security solution choice, security development, testing, evaluation and certification.

This will ensure you build trust into the heart of your developments and achieve the right certifications for your current and future commercial plans.

12.0 About Trustonic & Riscure

About Trustonic

Trustonic's mission is to embed the best security into the world's smart devices and apps, empowering mobile and IoT developers to build the trust required to deliver simple, fast and secure solutions.

The Trustonic hardware-backed security platform is embedded in more than 2 billion devices, including those from Samsung, vivo, OPPO, Xiaomi, Meizu, LG and Casio. Trustonic's mobile app protection solutions secure critical apps for banks, fintechs, payment providers, cryptocurrency platforms, automotive manufacturers, mobile network operators and government bodies, including Samsung Pay, Cartes Bancaires, Alipay, WeChat Pay, Hyundai and Volkswagen Group.

To contact Trustonic email enquiries@trustonic.com or visit www.trustonic.com | [Twitter](#) | [LinkedIn](#)

About Riscure

Founded in 2001, Riscure is a leading global advisor on the security of connected and IoT devices, as well as a recognized vendor of advanced security testing tools and security training. Riscure helps customers around the world to build robust hardware and software solutions and to speed up the process of secure development and certification.

Riscure has been a frontrunner in Trusted Execution Environment evaluation methodology and has performed numerous TEE evaluations since 2014. Contributing to GlobalPlatform protection profile and working with content protection vendors on the TEE platform evaluations with over 50+ evaluations. Since 2007, Riscure has pioneered in assessing the security of mobile solutions and mobile security technology with a current extensive track record of 200+ security evaluations of Mobile Payment and Mobile POS solutions, 25+ OEM Pays with multiple smartphone vendors (OEMs), 25+ Mobile Trusted Execution Environment (TEE) and 50+ Mobile Software Security Solutions including obfuscation, white-box cryptography and biometric solutions.

Riscure's expertise is well recognized by the industry and has many accreditations, among which are Visa, MasterCard, Discover, American Express, EMVco, GlobalPlatform, Common Criteria certification body accreditation, FIDO, ARM PSA, SESIP, Nagra, Irdeto, Verimatrix and Synamedia, to perform security assessments of a wide variety of solutions.

To contact Riscure email inforequest@riscure.com or visit www.riscure.com