Cyber Security White Paper of HiSilicon (Shanghai)

Issue 01

Date 2020-09-27

Notice

The purchased products, services and features are stipulated by the contract made between HiSilicon (Shanghai) and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change because of product version upgrades or any other reasons without notice. Unless otherwise specified, this document is for reference only. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

HiSilicon (Shanghai) Technologies Co., Ltd.

Address:	Room 101, No. 318, Shuixiu Road, Jinze Town (Xicen), Qingpu District, Shanghai (201799), China
Website:	http://www.hisilicon.com
Email:	support@hisilicon.com

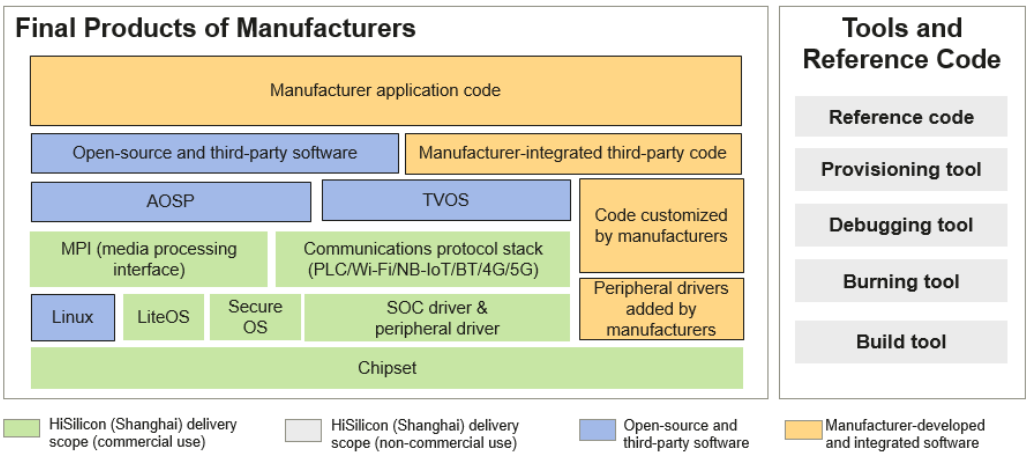
Contents

1 Overview

HiSilicon (Shanghai) Technology Co., Ltd, hereinafter referred to as HiSilicon (Shanghai), is a world-leading fabless semiconductor design company, providing leading chipset solutions and services for general smart devices in smart homes, smart cities, smart mobility, and more. Our portfolio covers a wide range of fields, including smart vision, smart IoT, smart media, smart transportation, automotive electronics, and display.

HiSilicon (Shanghai) provides developer-oriented services, delivering chipsets and SDKs to manufacturers. SDKs include LiteOS, secure OS, SOC drivers & peripheral drivers, UNF/MPI (media processing interface), and communication protocol stacks (PLC/Wi-Fi/NB-IoT/BT/4G/5G), tools, reference code, open-source and third-party software, and documents. Manufacturers can define, design, develop, test, release, produce, and maintain their own products based on the deliverables of HiSilicon (Shanghai). Figure 1-1 shows the business scope of HiSilicon (Shanghai).

Figure 1-1 Business scope



Business Scope

1. Commercial components delivered by HiSilicon (Shanghai): chipsets and SDKs. Here, SDKs refer to LiteOS, secure OS, SOC drivers & peripheral drivers, UNF/MPI (media processing interface), communications protocol stack (PLC/Wi-Fi/NB-IoT/BT/4G/5G), open-source and third-party software, as well as documents.
2. Non-commercial components delivered by HiSilicon (Shanghai): tools and reference code contained in SDKs
3. Deliverables by manufacturers: In addition to developing the application layer code, manufacturers will add, modify, and delete the code delivered by HiSilicon (Shanghai) based on their product requirements.

Cyber Security Responsibility Model

HiSilicon (Shanghai) does not directly sell chip products to end users but sells chipsets, SDKs, and documents to manufacturers who can add, modify, and delete the code we provide based on their requirements. That means we cannot provide technical support for end users on devices. End users who encounter any problems when using a product containing chipsets from HiSilicon (Shanghai) should contact the manufacturer for direct technical support.

The following describes the cyber security responsibility model that is based on the business scope shown in Figure 1-1.

1. HiSilicon (Shanghai) provides basic cyber security technologies for commercial chipsets and SDKs, including LiteOS, secure OS, SOC drivers & peripheral drivers, UNF/MPI (media processing interface), communications protocol stack (PLC/Wi-Fi/NB-IoT/BT/4G/5G), and documents. It also provides vulnerability remediation solutions for open-source and third-party software used in the SDKs. HiSilicon (Shanghai) offers cyber security support according to contracts.
2. The tools in the SDKs delivered by HiSilicon (Shanghai) are used only for development and debugging by manufacturers, and the reference code provided is used only to demonstrate chip functions – it is not commercially available. HiSilicon (Shanghai) makes no representations or warranties of any kind to the tools and reference code.
3. Manufacturers are responsible for the security of the code that they add, modify, and delete in addition to their application code.

HiSilicon (Shanghai) is dedicated to closely collaborating, innovating, and establishing standards with stakeholders to ensure that the integrity and security of the chipsets and solutions we provide meet or exceed the needs of our manufacturers and provide the assurance confidence required by their own customers.

2 Basic Security Technologies

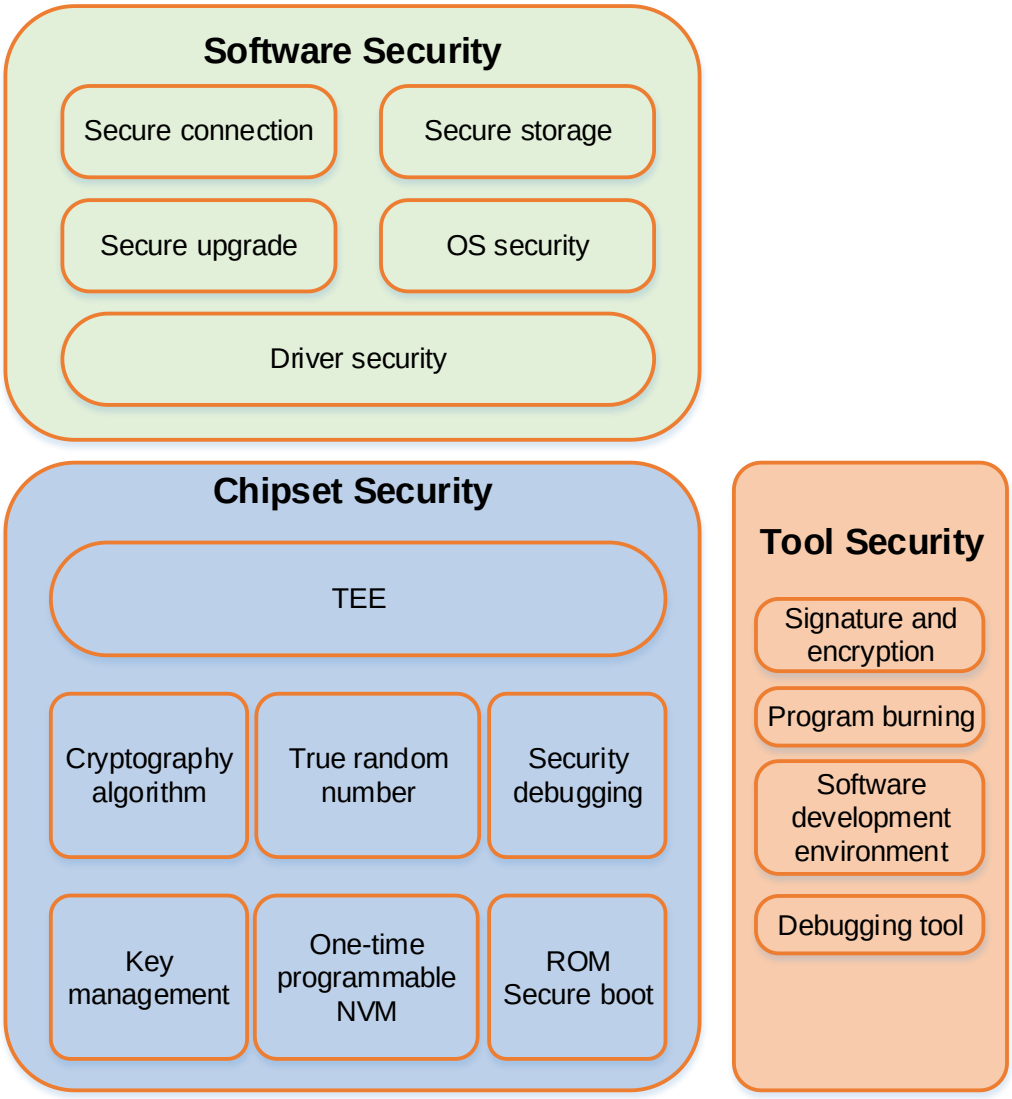
The security system, which is usually built on hardware security, provides a security platform for the operation of vital services and applications. HiSilicon (Shanghai) provides a wide range of basic hardware security technologies in chipsets for manufacturers, helping them build secure, trusted devices. This chapter describes the basic security technologies that HiSilicon (Shanghai) uses in hardware chipsets.

2.1 Basic Security Technology Architecture

HiSilicon (Shanghai) provides a broad array of security technologies for chipsets, software, and tools to help manufacturers quickly build secure, trusted products and solutions.

- Hardware security: Chip secure boot, secure debugging, and one-time programmable (OTP) nonvolatile memory (NVM) are used for key/ID storage, key management, and cryptographic algorithms. These security features contribute to a hardware-level security foundation. Furthermore, a Trusted Execution Environment (TEE) provides assurance for security software running and secure solution building.
- Software security: Operating systems (OSs), drivers, and critical services (such as secure storage, connectivity, and upgrade) provide basic security protection and can significantly help manufacturers develop security products.
- Tool security: Facilities such as signing and encryption, program burning, software development environment, and debugging tools enable manufacturers to efficiently develop competitive security products and solutions based on the chip platform provided by HiSilicon (Shanghai).

Figure 2-1 Architecture of security technologies



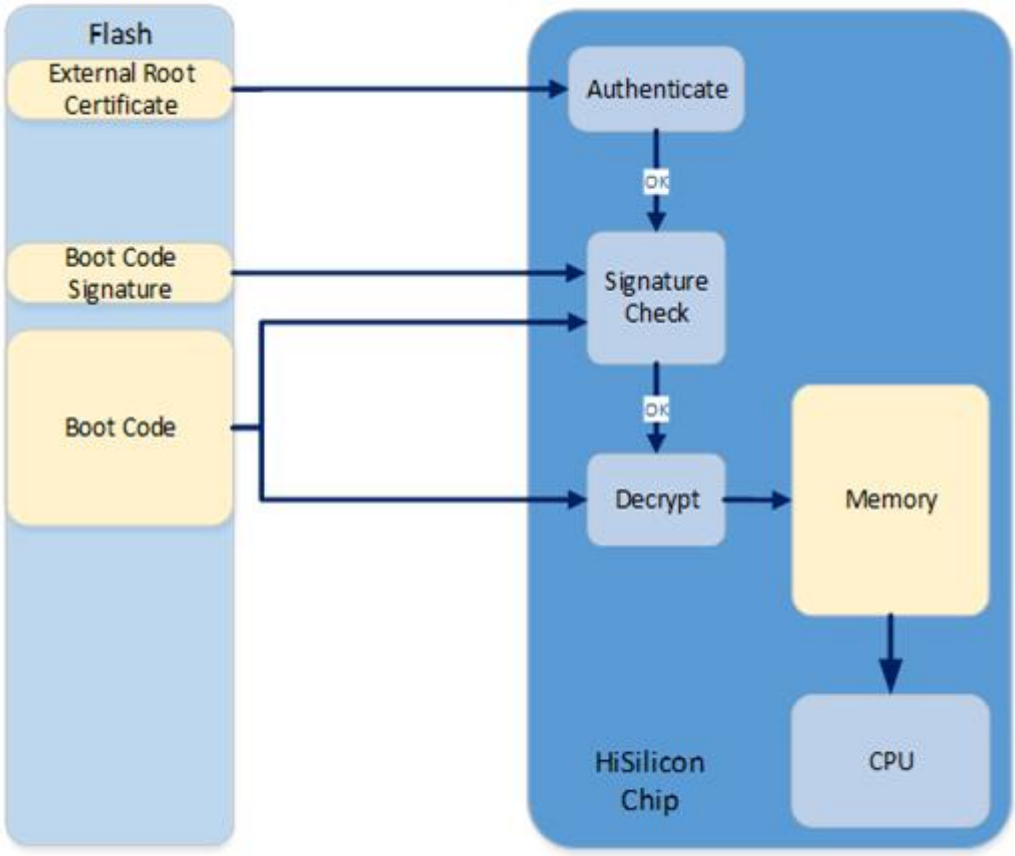
2.2 Secure Boot

To provide the root of trust (RoT) for the system, the main CPU will boot from an on-chip BootROM. The immutable code embedded in the on-chip BootROM is natively trusted, and is the starting point in the software chain of trust. The first task performed by this code is to read and authenticate the external root public key. After this, the CPU will read and decrypt the system boot code, and the external root public key is used to authenticate a digital signature of this code. The CPU will execute the code that is proven authentic. System boot code can be encrypted using a key, which is derived from the root key stored in the OTP memory within the chip. The certified system boot code can be used to verify other software code using a similar mechanism, to form a chain of trust.

Chips can also boot from other media (such as serial port, SDIO, and USB devices) as well as flash memory. BootROM obtains the root public key and boot code from

the boot media and uses the same method to verify the boot. Internationally-recognized algorithms and protocols are used throughout the boot process.

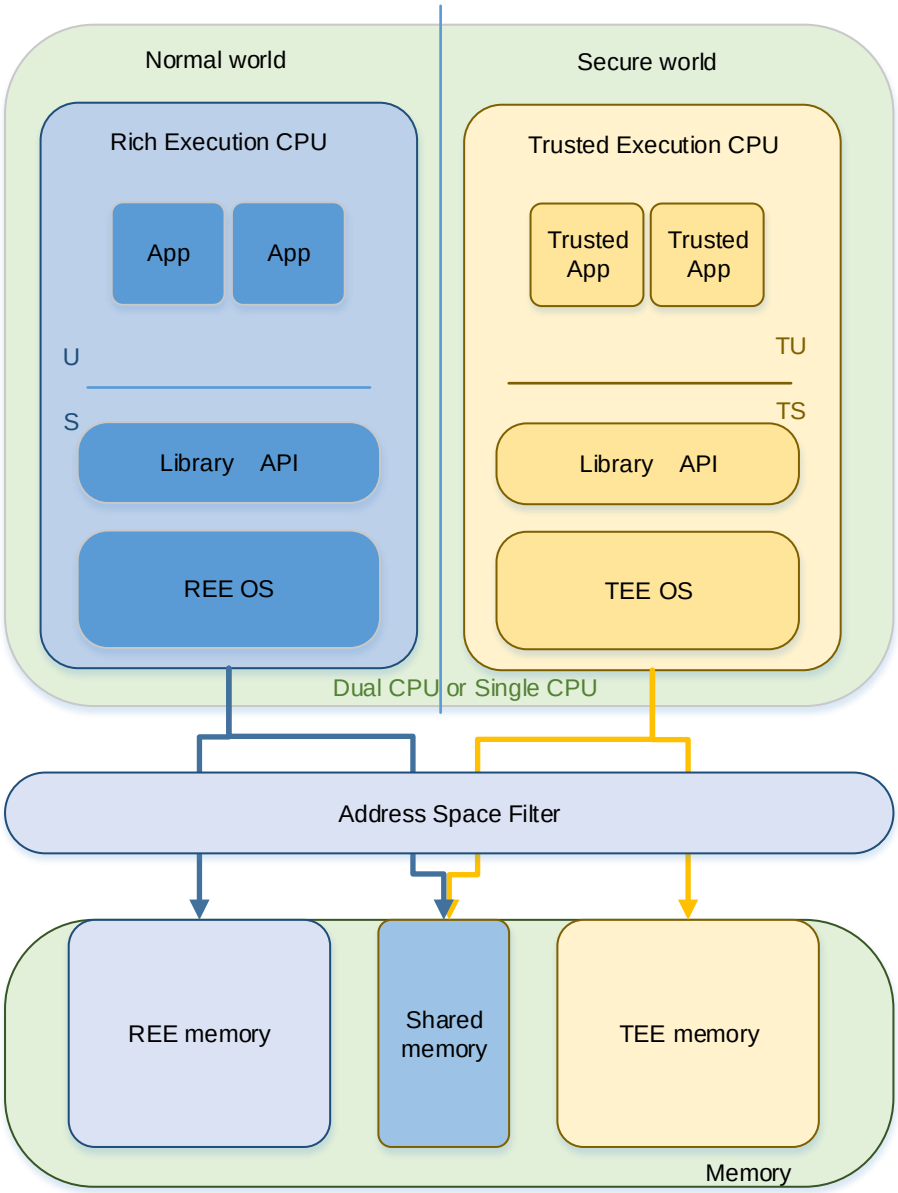
Figure 2-2 Secure boot



2.3 Trusted Execution Environment

To allow for implementation of critical services with access to sensitive data in a more trusted way, the chip supports partitioning of the system into the Trusted Execution Environment (TEE) (which is known as the secure world) and the Rich Execution Environment (REE) (the normal word). This may be achieved by designating one entire CPU as the secure world, and another CPU as the normal world, or by utilizing a virtual processor (ARM TrustZone, for example). Access to memory is partitioned so that each world only has access to its own authorized memory. Additionally, each world has its own encryption/decryption hardware resources and peripheral resources. iTrustee is a TEE OS that is designed to provide a TEE for mission-critical computing and secure access to sensitive data.

Figure 2-3 TEE



iTrustee Introduction

iTrustee is a TEE OS that HiSilicon (Shanghai) has developed based on ARM TrustZone. The TEE protects and isolates hardware resources, such as memory and peripherals, and provides execution process protection, key confidentiality, data integrity, and access control to implement end-to-end security and prevent malware attacks from the REE. Essential services such as secure storage, encryption/decryption, and secure time are embedded in iTrustee.

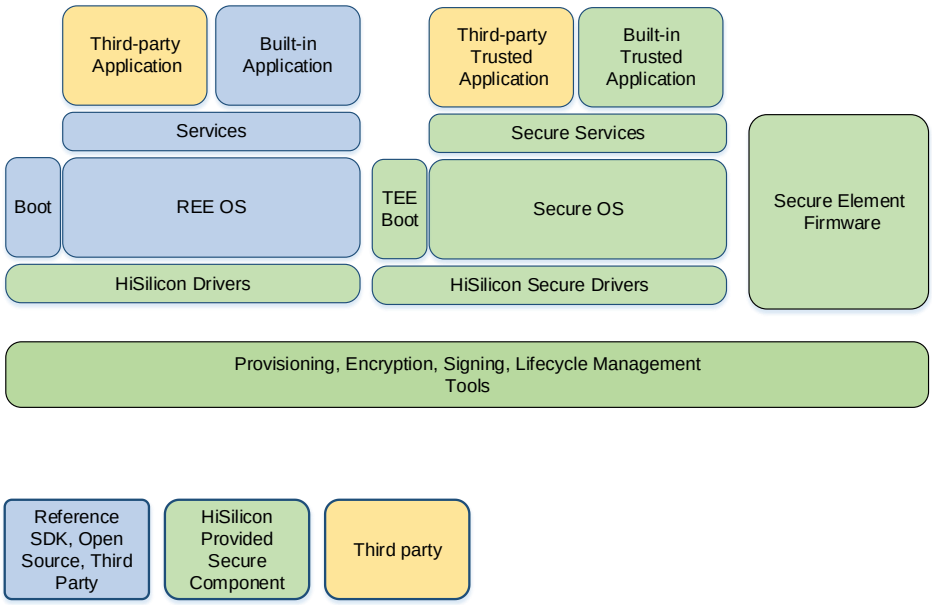
2.4 Secure Software Components

In order for a system to benefit from a TEE, the software running in the TEE must be hardened to protect it from logical and physical attacks, in turn providing higher security for device keys and data. HiSilicon (Shanghai) provides critical secure software components that are pre-integrated into the chip and TEE to facilitate fast, simple development of secure, robust devices.

Secure OSs are provided along with the required secure services (such as encryption and secure storage). These secure OSs can run trusted applications (TAs) from manufacturers or third parties, or simply use the built-in TAs for general security functions. Secure OSs, TAs, low-level hardware drivers, and secure boot programs are carefully reviewed by internal and external experts to ensure robustness against attacks. The firmware required for the chip containing embedded secure elements is certified by external security bodies as required.

Such components must be encrypted and digitally signed before the secure system allows them to execute code. For this reason, HiSilicon (Shanghai) provides tools to simplify this process and ensure that only the authenticated code can be executed.

Figure 2-4 Secure software components



2.5 One Time Programmable

Unique per-device identity is a critical requirement of IoT standards to enable secure authentication and authorization of IoT devices. Unique symmetric keys provide the basis for a more general secure storage, while asymmetric keys that are used for software authentication must be permanently bound to devices. All vital information is stored in the OTP memory that is embedded into the chip.

2.6 Hardware Key Management

Symmetric keys can only be used by key derivation hardware to cryptographically (AES or PBKDF2) create further keys, and the resulting secrets can then only be used by on-chip cryptographic hardware to encrypt or decrypt data. The root keys and derived keys in the chip remain inaccessible to software.

2.7 Cryptographic Algorithms

The chipsets provided by HiSilicon (Shanghai) support multiple international standard cryptographic algorithms (including common symmetric algorithms AES and TDES and public key algorithms RSA and ECC) and key modes, and can defend against side-channel attacks. Some chipsets support Chinese national cryptographic algorithms.

2.8 True Random Number Generator

Cryptographic protocols commonly use random numbers to prevent replay attacks and man-in-the-middle attacks. To ensure the quality of random numbers that are necessary for security, the chip provides a hardware-based True Random Number Generator (TRNG). CPUs can read and use these random numbers to set up secure communication channels or derive keys.

2.9 Debugging Protection

JTAG debugging and testing ports can be hardware locked using unique, per device passwords to prevent unauthorized data and code extraction and hijacking of running systems. On each chip, unique passwords are used to lock the JTAG debugging and testing ports. HiSilicon (Shanghai) provides a tool to read device identities and provides the password necessary to unlock the debugging ports. The chip also supports permanent disabling of debugging ports by OTP.

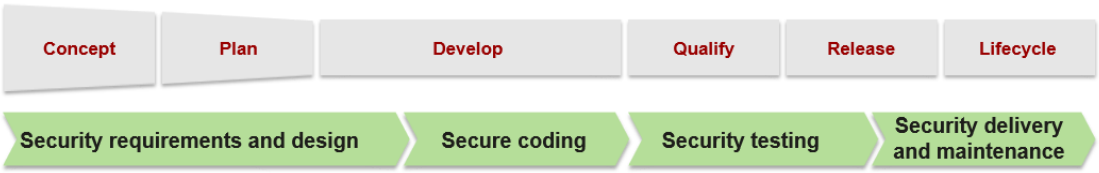
3 Engineering Security

HiSilicon (Shanghai) has adapted and released a cyber security development process that is applicable to chip development. This chapter describes the process as well as security practices in security requirements and design, secure coding, security testing, and security delivery and maintenance.

3.1 Cyber Security Development Process

HiSilicon (Shanghai) integrates cyber security into product R&D, as shown in Figure 3-1.

Figure 3-1 Cyber security development process



3.2 Security Requirements and Design

In compliance with laws, regulations, and industry standards, HiSilicon (Shanghai) uses industry-standard security design principles and our own security specifications when analyzing security threats in business scenarios. Furthermore, we use the general STRIDE threat modeling method in the industry (which is short for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). After a threat is identified, our design engineers develop suitable mitigations based on the mitigation and security design solution libraries to offer a suitable security solution design. All threat mitigations will be converted into security requirements and incorporated into the development process. Engineers will then test these mitigations by designing test cases based on the specific security requirements to ensure high cyber security for our products.

3.3 Secure Coding

HiSilicon (Shanghai) strictly complies with its secure coding standards, and all security R&D and test engineers are all certified. HiSilicon (Shanghai) also introduces the industry-leading static code scanning tool. The scan results are imported into the tool chains for continuous integration and deployment, and the gated check-in mechanism is used to secure product code.

3.4 Security Testing

All HiSilicon (Shanghai) projects will undergo multiple security tests before being released, and these tests include but are not limited to white-box testing on high-risk interfaces in the development phase, gray-box fuzzing on external interfaces and protocols in the testing phase, along with internal security testing by security experts. Tests cover the security requirements identified in the security design phase and penetration test cases from the perspective of attackers. Moreover, HiSilicon (Shanghai) verifies the compliance with customer security requirements and industry standards, and also develops security testing tools.

3.5 Security Delivery and Maintenance

As manufacturers can develop more code based on the SDKs provided by HiSilicon (Shanghai), we provide the cyber security precautions (for example, how to disable the debugging port after productization) together with the SDKs.

The Product Security Incident Response Team (PSIRT) of HiSilicon (Shanghai) receives, investigates, and discloses security vulnerabilities of HiSilicon (Shanghai) products and solutions. It is an important vulnerability disclosure window. We encourage security researchers, industry organizations, government agencies, and vendors to report the security vulnerabilities to our PSIRT. For details about how to report a vulnerability, visit http://www.hisilicon.com/en/PSIRT.

4 Security Certifications

This chapter describes the security standards that HiSilicon (Shanghai) complies with and the security certifications that its hardware, chips, and SDK platform software have obtained.

Compliance with Security Standards

- GM/T 0002-2012 SM4 block cipher algorithm
- GM/T 0003-2012 Public key cryptographic algorithm SM2 based on elliptic curves
- GM/T 0004-2012 SM3 cryptographic hash algorithm
- GM/T 0008-2013 Cryptography test criteria for security IC
- GB/T 18336-2015 Information technology – Security techniques – Evaluation criteria for IT security
- ISO/IEC 15408:2009 Information technology – Security techniques – Evaluation criteria for IT security

Security Certifications

- Conditional access system (CAS) for content protection: security certifications by Irdeto, Nagra, Viaccess, DCAS, Novel, and Suma
- Digital rights management (DRM) for content protection: security certifications by Riscure, ChinaDRMLab, Netflix, etc.
- Riscure RAPC gold certification
- TÜViT nuSIM security certification
- iTrustee 5.0 CC EAL2+
- Microkernel CC EAL 5+
- EAL 3 of China Information Technology Security Evaluation Center
- Security chip certification by China's State Cryptography Administration

5 Conclusion

HiSilicon (Shanghai) values the security of user devices and provides basic security technologies such as underlying chips, drivers, and secure OSs to help manufacturers develop secure, reliable products. Furthermore, we strive to develop strong security technologies and processes to implement security management throughout the product lifecycle. HiSilicon (Shanghai) has set up the PSIRT to improve product security, welcoming any organization or individual to report any of our product's security vulnerabilities at http://www.hisilicon.com/en/PSIRT. PSIRT will promptly and rigorously follow up any reports, organize vulnerability remediation, publish security advisories, and deliver patches. Together we can make devices more secure.