Infocom Security Technical Inspection Guidelines of Embedded Software on Smartphone Systems

2017/3/3

Table of Contents

Infocom Security Technical Inspection Guidelines of Embedded Software on Smartphone Systems

1. Overview

The communications network and smartphone devices are now more a part of our lives than ever before; due to their ubiquity and utility, our productivity and efficiency can be greatly enhanced. However, once connected to the internet, these devices may also bring about security threats to users. In view of this and after referring to practices in the EU and US, the National Communications Commission (NCC) has proposed "the Infocom Security Technical Inspection Guidelines of Embedded Software on Smartphone Systems" (hereinafter referred to as "the Technical Inspection Guidelines") as a basis for the testing to be undertaken by smartphone manufacturers, distributors, telecom operators and Infocom Security testing laboratories.

2. Scope of Application

The Technical Inspection Guidelines are applicable to the smartphone system and its embedded software to ensure that it meets current information security requirements, but does not include additional services or content that users may have downloaded themselves onto the device.

The essence of information security is risk control. Following confirmation of the embedded software of the smartphone (hereinafter as embedded software) conforming to the Technical Inspection Guidelines upon testing, there is still no guarantee that the tested smartphone will not be maliciously attacked or hacked.

In order to minimize potential risks and impact of the security problems, users should still be alert to information security while using their devices.

2.1 Properties of the Embedded Software

Embedded software has been categorized into three types: factory pre-loaded software, distributor loaded software, and iconless software, wherein test applicants may arbitrarily wish to test unbranded software:

- Factory Pre-loaded Software: application software that has been installed onto the smartphone at the factory, and can be activated by the user through the icon.
- Distributor Loaded Software: application software that has been installed onto the smartphone when it is sold or will be automatically installed onto the smartphone when it is connected to the network for the first time, and can be activated by the user through the icon.
- Iconless Software: application software that is installed in the above two cases, and cannot be activated by the user through an icon. The Iconless Software begins the communication function.

2.2 Layers for Testing

Adhering to the globally accepted concept of layered security in smartphones, the Technical Inspection Guidelines divides the security layers of the smartphone into five layers: data layer, application layer, communication protocol layer, operating system layer and hardware layer, and evaluates potential information security risks each layer may confront The security testing of each layer can be outlined as follows:

- Data Layer: The security concerns of the data layer mainly involve data transmission, storage or use; the aim of the testing is to ensure that users' data can be protected from unauthorized gathering, sharing, use, deletion, tampering and storage by the system embedded software.

- Application Layer: The security concerns of the application layer mainly involve the program source, execution and authorization, etc; the aim of testing this layer is to shall ensure that the embedded software is not subject to unauthorized access to system resources.

- Protocol Layer: The security concerns of a communication protocol mainly involve the security of the wireless transmission technologies and communication protocols; the aim of testing is to ensure that users can maintain control over data transmission and connection of peripheral devices.

- Operating System Layer: The security concerns of the operating system layer mainly involve operating system related services and identification; the aim of testing is to ensure that the operating system protects the system resources and reminds users to update the system.

- Hardware Layer: The security concerns of the hardware mainly involve the key cryptographic modules; the aim of the testing of this layer is to ensure that key management, storage and protection, as well as the security and strength of algorithms, are in line with international norms, and allow users to be informed when updates are conducted.

3. Security Levels

In line with various security requirements, the Technical Inspection Guidelines divides the information security levels of the embedded software into three types: basic, medium and advanced security levels, each of which is outlined in Table 1.

Table 1 Requirements and descriptions of Information Security Levels

Information Security Level	Requirements	Description
Basic (B)	The device provides data security features for protection of personal privacy and sensitive data. For example, the collection of sensitive data must be clearly communicated.	The minimum requirements of privacy protection for smartphone users.

Medium (M)	The device provides a complete data protection mechanism that can secure all data in use, storage and transmission.	In addition to all the necessary and basic testing items, testing items for advanced data protection have also been added.
Advanced (H)	The device ensures that the core underlying layer is not tampered with or subjected to improper data acquisition.	In order to ensure that the core underlying layer of the smartphone will not be tampered with or subjected to improper data acquisition, in addition to the testing items of basic and medium levels, testing items for security review of the smartphone design have also been added.

4. Reference Standards

ISO / IEC 15408 Common Criteria (Common Criteria for Information Technology Security Evaluation CC).

5. Terms and Definitions

5.1 Encryption

Refers to the use of mathematical algorithms to process electronic data, so that the data is not be presented in its original form; the original content of the encrypted data can be obtained by decryption.

5.2 Communication Port

Refers to the communication port that embedded software has enabled for service needs.

5.3 Session Identification, Session ID

Refers to the unique work phase ID assigned to each user when connection is established. When the connection ends, the ID is released and the server reassigns the ID to a new user in connection.

5.4 Near Field Communication, NFC

Refers to close-range (usually less than 10 cm) wireless communication technology with a primary operating frequency of 13.56 megahertz (MHz) and a data transmission speed of up to 424 Kbps per second. NFC includes three modes: peer-to-peer, read/write, and card emulation, in which multiple physical card functions, such as credit cards, EasyCard, etc can be simulated. When near field communication technology uses the card simulation mode, it can be used without a power supply.

5.5 Non-Operating System Protection Area

Refers to the space that the user can access via connection to the smartphone through an external device (such as a computer) under non-administrator authority, including

the storage space of the smartphone itself and the external memory card provided at the factory.

5.6 SQL Attack

Refers to attacks that use data entry fields or database vulnerabilities to run unintended external programs or instructions to obtain unauthorized data.

5.7 XML Attack

Refers to a network attack method. XML format files are commonly used as an input and output of applications. When an application uses the XML format as the input for executing a job, an attacker may change the structure or data of the XML format and tamper with the contents of important files or materials to achieve intrusion.

5.8 Personal Data

Refers to a natural person's name, date of birth, national identity card number, passport number, characteristics, fingerprints, marriage, family, education, occupation, medical history, medical, genetic, gender, health checks, criminal records, contact information, financial statements, social activities, and other information that directly or indirectly identifies the individual.

5.9 Sensitive Information, Sensitive Data

Refers to personal data or smartphone related information that may result in damage to the rights of individuals or data owners if disclosed.

5.10Data Type

Technical Inspection Guidelines classifies the data into Type 1, 2, 3 and 4 according to the sensitivity of the data and whether it is user input (see Table 2). Type 1 and Type 2 are sensitive data.

Table 2 Data Type Classification

Type	Criteria		Example
	Data sensitive (Y/N)	Is it user input?	
Type 1	Yes	Yes	1. The personal data specified by the Technical Inspection Guidelines. 2. Smartphone related information: SMS content, call recording, device password, account password, and photos.
Type 2	Yes	No	IMEI, IMSI [Note], positioning information.
Type 3	No	No	APP list, music playback information, smartphone operating system, smartphone model, smartphone firmware version, MCC, MNC, mobile carrier, network transmission method, and configuration

			file.
Type 4	Unable to determine	Unable to determine	Data encryption, protocol encryption, or no encryption, but the content is unknown.
[Note] The IMEI code and the IMSI code must be linked to the sales guarantee of the mobile communication company or the smartphone manufacturer to be uniquely identifiable, but the user and the registrant may be different, so they are classified as type 2.			

5.11 Robustness Testing

Refers to the verification of the program stability through manufacturing errors or unpredictable inputs, and the ability of the error handler or algorithm to continue operations normally when an operating system, mobile application, or network service encounters an input, operation, or other exception during execution.

5.12 International Mobile Subscriber Identity, IMSI

Refers to the unique ID that binds the mobile device user over all GSM and UMTS networks. The IMSI consists of a series of decimal numbers with a maximum length of 15 digits. The first 3 digits on the SIM card in the mobile phone represent the Mobile Country Code (MCC), followed by the Mobile Network Code (MNC), which contains 3 digits (North American Standard) or 2 digits (European Standard). The remaining digits represent the Mobile Subscription Identification Number (MSIN), which is determined by the operator. Thus, the IMSI is comprised of the 3 representative codes – MCC, MNC and MSIN.

5.13 International Mobile Equipment Identity, IMEI

Refers to the identification of each individual mobile communication device in the mobile network, which is equivalent to the identity card of the device. The SEQ ID contains a total of 15 digits, where the first 6 digits (Type Approval Code, TAC) are the type approval number, representing the smartphone type. Then, 2 digits (Final Assembly Code, FAC) are the final assembly number, representing the place of origin. Then, the 6 digits (Serial Number, SNR is the serial number, representing the production sequence number). The last digit (SP) is the check digit, which is generally 0. The international mobile device ID is usually attached to the back and outer packaging of the body; it can also be present in the smartphone memory.

5.14 Password

Refers to a set of strings used to protect a particular piece of data for a particular application. It is typically used for identification and data encryption.

5.15 User Consent

User consent refers to a message prompt that the system provides for the user to be able to agree or disagree. User consent refers to the behavior of the user's active operation and the user's consent obtained through the user consent mechanism.

5.16 Wireless Transmission Technology

Refers to the connection built upon the wireless communication standard, allowing the smartphone to transmit data through the network or peer-to-peer connection. Wireless

transmission technologies used by smartphones include Bluetooth, WLAN, NFC, mobile communication networks, GPS (positioning services), infrared and wireless charging.

5.17 Wireless Local Network, WLAN

Refers to internet connection via radio waves, laser light or infrared rays. Its function is the same as that of the wired area network.

5.18 Embedded Software of Smartphone

Refers to the software unconditionally installed by the software manufacturer, mobile communications service provider, or application software developer when the user uses the smartphone or enables network services for the first time.

5.19 Internet Protocol Address, IP Address

Refers to the address that uniquely identifies the host on the internet. It is commonly referred to as the IP address, which can be divided into either IPv4 or IPv6.

5.20 Domain Name

Refers to a combination of words or numbers used to map the internet address to the internet user's address (IP address).

5.21 Digital Signature

Refers to the electronic file calculated by mathematical algorithm or other means into a certain length of digital data, and then encrypted by the signatory's private key to form an electronic signature, which can be verified by the public key.

5.22 Buffer Overflow Attack

Refers to an attack method in which a malicious attacker uses a programming vulnerability to input a string or data that exceeds a predetermined length, causing an unexpected situation in the program to generate a buffer overflow problem. A malicious attacker may use program syntax with malicious purposes or insert data into the original code to cause the program to stop abnormally, run arbitrary codes, or gain system authorization.

5.23 Certificate

Refers to an electronic certificate containing signature verification information to confirm the identity and qualifications of the signatory.

5.24 Certification Authority, CA

Refers to the authority or legal person that issues the certificate and is an impartial organization trusted by the user. Its business is to issue and manage the public key certificate in X.509 format and maintain a list of institutions that cancel and abolish the certificates.

5.25 Address Space Layout Randomization, ASLR

Refers to the disruption of the key element locations in the memory during the execution of the program, so that an attacker can position the base address, library, memory stack and heap and other key addresses, making it difficult to correctly run malicious programs.

5.26 Common Criteria, CC

Refers to the International Information Security Product Evaluation and Verification Standard (ISO/IEC 15408). The Evaluation Assurance Level (EAL) defines the Security Levels of the products. The EAL has 7 levels, the lowest being EAL 1, while the highest level set at EAL 7, allowing applicants / sponsors, testing laboratories and certification authorities (institutions) to evaluate and verify the security and functionality of the security products. (Link for reference: http://www.commoncriteriaportal.org)

5.27 Target of Evaluation, TOE

Refers to the products and related manuals for information security evaluation and verification.

5.28 Protection Profile, PP

Refers to the basic requirements for the information security product as the Target of Evaluation (TOE).

5.29 Security Target, ST

Refers to the specification document for the information security product to meet the protection profile (PP) or specific security requirements.

5.30 Security Functional Requirement, SFR

Refers to the security-related requirement defined in the Common Criteria (Part 2), which describe the requirements for the TOE Security Functions (TSF) of an Information Security product. This requirement is referenced in the protection profile and the security label to specify the security requirements of the product.

5.31 TOE Security Functions, TSF

Refers to the related functions that meet the Security Functional Requirement (SFR) for the information security product to implement the Security Target (ST).

5.32 TOE Security Function Interface, TSFI

Refers to the External Communication Interface (TOE) used to implement the Security Function Requirement (SFR).

5.33 Security Domain

Refers to a collection of resources that a proactive individual (person or machine) is authorized to access as one of the attributes of the security architecture.

5.34 Self-Protection

Refers to the security function that can automatically identify itself and protect it from being destroyed by irrelevant code or facilities and is one of the attributes of the security architecture.

5.35 Non-Bypassibility

Refers to the technique of preventing security inspection, such as not being possible to enter the audit function interface without identification.

6. Technical Requirements

The testing laboratory shall conduct document review and actual testing of the relevant materials and smartphone samples submitted by the applicant according to the Scope of Application and Testing Items described in the Technical Inspection Guidelines.

6.1 Materials Required for Testing Applications

The applicant shall complete the Testing Application (Annex 1), the Manufacturer Self-Declaration Form (Annex 2), and the Embedded Software Summary Form (Annex 3), and provide smartphone samples to be tested in the testing laboratory. If the applicant applies for advanced information security, the Security Function Specification Sheet (Annex 4), Design Security Table (Annex 5) and Security Structure Table (Annex 6) shall be additionally submitted.

6.1.1 Testing Applications

Content includes related information of the applicant, the manufacturer and specifications of the smartphone (including brand, model, name, operating system version, positioning function, wireless transmission technology, biometric identification, external memory, etc.).

6.1.2 Manufacturer Self-Declaration Form

Content includes name of system embedded software, publisher, version, package name, attributes, feature description, authority description, access data type, communication port and more.

6.1.3 Embedded Software Summary Table

Content includes name of system embedded software, publisher, version, attributes, feature description, and authority description. This summary form should be available for reference and disclosure by the NCC.

6.1.4 Security Function Specification Sheet

Content includes the name of the TOE Security Function Interface (TSFI), its purpose, the achievable security function requirements, mode of operation, parameters, actions performed, and error messages. The applicant shall complete and explain this sheet; the testing laboratory shall determine whether the security function interface can achieve the TOE Security Function (TSF) requirements.

6.1.5 Security Designation Sheet

Content includes how to use the subsystem to form the security function interface of the security function specification, as well as the name and purpose of the security function subsystem, the security function interface of the subsystem, and description of the subsystem behavior.

6.1.6 Security Architecture Sheet

Content shall be based on the security function specification table, indicating how the security architecture of the tested equipment meets the security function requirements

(SFR), and proposes the security concept design concept and operation security recommendations for the security function interface and subsystem. The security architecture shall describe the security domain of the tested equipment due to the execution of the security function, the security initial procedure of the security function, the self-protection mechanism of the security function, and how the security function implementation avoids being bypassed.

6.2 Testing Items

The Technical Inspection Guidelines stipulates the testing items according to the layers for testing, and then stipulates testing items according to the security requirements of each item. The testing items and security requirements are outlined in Table 3. The corresponding relations between the testing items, testing details and Information Security Levels are shown in Table 4. The testing coding principles for each of the testing items are as follows:

- Testing code:

  Layer code, Testing Item code, Testing Detail code. Information Security Level code (+)

- Description:

  (1) The layer codes are as follows:

Layer	Code
Data Layer	D
Application Layer	A
Communication Protocol Layer	P
Operating System Layer	O
Hardware Layer	H

  (2) The codes of the Information Security Levels are as follows:

Information	Code
Basic	B
Medium	M
Advanced	H

  (3) If the testing code is marked with the (+) symbol, the applicant is provided with the option test the item arbitrarily.

- Example:

  (1) For the data layer, the first testing sub-item of the first testing item is Basic, which is a required testing item, its testing code thus D.1.1.B.

  (2) The second testing detail of the second testing item is Medium, which is an optional testing item, so its testing code is D.2.2.M(+).

Table 3 Testing Items and Security Requirements

Layer	Testing Items	Security requirements
Data Layer (D)	1. Data authorization	The embedded software shall obtains user consent prior to accessing sensitive data.
	2. Data storage protection	The embedded software shall store sensitive data in the operating system protected with encryption so as to prevent sensitive data from being accessed improperly.
	3. Data loss protection	The smartphone system shall provide data protection and backup functions to avoid data leakage and prevent data loss.
Application Layer (A)	1. Program identification	When the embedded software initially accesses the account on the user's bound device, it shall attempt to verify user identification and authorization to avoid misuse or abuse of the user account.
	2. Program trust source	The embedded software shall confirm the payment function mechanism and the security of the data source.
	3. Program execution authorization	The actions performed by the embedded software are subject to the consent of the user and shall be consistent with the content of the declaration.
	4. Program execution security	The embedded software shall be able to process malicious string input.
Communication protocol layer (P)	1. Protocol for use of license agreement	When the smartphone is connected to an external device, the user shall be given corresponding prompts to turn on or off the wireless transmission technology.
	2. Protocol for transmission protection	Encryption data transmission between the embedded software and the server shall adopt a secure encryption algorithm and avoid possible transmission attacks.
	3. Protocol for implementation security	The smartphone system shall be able to handle errors in the content of the protocol.
Operating system layer (O)	1. System operation authorization	The behavior performed by the smartphone system shall be subject to user consent and, if necessary, a risk alert shall be issued.
	2. System identification	The smartphone system shall provide a secure identification and protection mechanism.
	3. System execution security	The smartphone system shall have a memory protection mechanism for program execution and provide a channel to report security concerns.
Hardware layer (H)	1. Key management protection	The key management of the smartphone shall comply with key usage and management standards.
	2. Algorithm strength requirements	The encryption, decryption and signature algorithms of the smartphone implementation shall conform to the key algorithm standards and the initialization vector requirements.

Table 4 Testing Items, Testing Subitems and Information Security Levels

Layer	Test items	Testing subitems	Information Security Level	Testing code
Data layer (D)	1. Data use license	1. The embedded software shall obtain the user's consent prior to accessing sensitive data.	B	D.1.1.B
		2. After the user forbids the embedded software to access sensitive data through user settings, the software shall not be able to access relevant data.	M	D.1.2.M (+)
	2. Data storage protection	1. The embedded software shall store the password of the account in the Operating System Protection Area or in encrypted form.	B	D.2.1.B
		2. The embedded software shall provide data encryption when storing sensitive data to avoid improper access to sensitive data.	M	D.2.2.M (+)
		3. The account and password communicated between the embedded software and the remote server shall not exist in plaintext in the executable file to avoid improper access.	M	D.2.3.M (+)
	3.Data loss protection	1. The smartphone system shall provide the user with the remote locking function and related security settings to ensure the user can remotely lock the smartphone system if the smartphone is lost or stolen.	B	D.3.1.B
		2. The smartphone system shall provide the user with remote data deletion function and related security settings to ensure the user can delete the data remotely if the smartphone is lost or stolen.	B	D.3.2.B
		3. The smartphone system shall provide a data backup function.	B	D.3.3.B
Application layer (A)	1.Program identification	1. When the embedded software first accesses the account that is bound to the device, it shall first authenticate user identity and authority to ensure that the embedded software has the authority to use the account.	B	A.1.1.B
	2. Program trust source	1. When the embedded software has payment function, the server credentials within the valid period shall be used to ensure the security of the payment transaction.	B	A.2.1.B
		2. The embedded software shall be able to identify its release information to ensure that the user understands its source.	B	A.2.2.B

	3. Program execution authorization	1. The embedded software shall obtain the user's consent to prior to each payment before any adjustment to the payment function being made.	B	A.3.1.B
		2. The authorization required for the Embedded Software must match the "Function Description" and " Authorization Description" declared in the "Manufacturer Self-Declaration Form".	B	A.3.2.B
		3. The network connection port opened by the Embedded Software must match the "Communication Port Status" declared in the "Manufacturer Self-Declaration Form".	M	A.3.3.M
		4. The embedded software shall not make calls or send text messages in the background without the user's consent.	M	A.3.4.M (+)
		5. The embedded software shall stop all related programs of the embedded software when turned off by the user.	M	A.3.5.M (+)
	4. Program execution security	1. The embedded software shall provide a channel for reporting security issues.	B	A.4.1.B
		2. The embedded software shall be able to process malicious SQL injection.	M	A.4.2.M
		3. The embedded software shall be able to process the extensible markup language (XML) attack string.	M	A.4.3.M
Communication protocol layer (P)	1. Protocol authorization	1. The smartphone shall provide an interface for users to enable and disable the wireless transmission technology.	B	P.1.1.B
		2. When the wireless transmission technology function of the smartphone is confirmed as being on, the corresponding prompt state shall be given to the user.	B	P.1.2.B
		3. When the smartphone is connected to other devices through the wireless transmission technology for the first time, the connection shall be established only after the user agrees.	B	P.1.3.B
		4. The smartphone shall provide an interface for users to enable and disable the Near Field Communication (NFC) technology.	B	P.1.4.B
	2. Protocol transmission protection	1. When the embedded software transmits sensitive data through wireless transmission technology, encrypted transmission shall be used to ensure security of sensitive data.	B	P.2.1.B
		2. The embedded software shall avoid the attack of resending the Session ID.	M	P.2.2.M
		3. Encrypted data transmission between the	M	P.2.3.M

		embedded software and the payment function server shall adopt a secure encryption algorithm.		
	3. Protocol implementation security	1. The smartphone system shall be able to handle errors in the content of the protocol.	M	P.3.1.M
Operating system layer (O)	1. System operation authorization	1. The update source of the smartphone system shall match the "IP/DN/ Company Name and Server Type of the data link server" declared in the "Manufacturer Self-Declaration Form".	B	O.1.1.B
		2. The smartphone system shall provide update information when downloading or installing the updates of the operating system and informs the user of the content of update.	B	O.1.2.B
	2. System identification	1. The smartphone system shall support the screen unlock protection mechanism to protect personal information from unauthorized use.	B	O.2.1.B
		2. The smartphone system shall support the screen forced lock protection mechanism when attempting to unlock incorrectly to protect personal information from unauthorized use.	B	O.2.2.B
		3. The smartphone system shall provide at least 72 types of password input values, including English uppercase, lowercase, numbers and special symbols, and the password shall be able to be long as 14 characters.	B	O.2.3.B
		4. The screen lock/unlock information of the smartphone system shall not be stored on the smartphone in plaintext to avoid unauthorized use.	M	O.2.4.M
	3. System execution security	1. The smartphone system shall provide a channel for reporting security issues.	B	O.3.1.B
		2. The smartphone system shall have a memory configuration protection mechanism to prevent improper application of the program and reference functions in the memory.	M	O.3.2.M
		3. The smartphone system shall establish a trusted transmission channel with the communication target during transmission for data protection purpose.	H	O.3.3.H
		4. The smartphone boot process shall include a password function test and a system software integrity self-test mechanism.	H	O.3.4.H

		5. The smartphone system shall include a verification error counting mechanism. When the attempted error exceeds the threshold set by the smartphone, the protected information shall be erased.	H	O.3.5.H
Hardware layer (H)	1. Key management protection	1. The key management of smartphone, including the generation, merging and destruction of encryption and communication keys, shall comply with the key usage and management standards issued by NIST, ANSI or IEEE.	H	H.1.1.H
		2. The smartphone's key stored in the mobile device shall include additional protection of its confidentiality and integrity.	H	H.1.2.H
		3. Keys shall not stored in plaintext in non-volatile memory and shall not be exported in any way or directly transmitted.	H	H.1.3.H
	2. Algorithm strength requirements	1. The encryption, decryption and signature algorithms of the smartphone implementation shall comply with the key algorithm standard issued by NIST, ANSI or IEEE.	H	H.2.1.H
		2. The algorithm for the smartphone implementation shall generate an initialization vector according to the requirements of each mode and meet the initialization vector requirements issued by NIST.	H	H.2.2.H
		3. The random number used by the key shall comply with the requirements of the random bit generation specification issued by NIST or ANSI.	H	H.2.3.H

6.3 Basic Testing Items

As part of the testing method and criteria of the Technical Inspection Guidelines, the smartphone system is referred to as the system under test (or the tested system), and the built-in software of the smartphone system is referred to as the software under test (or the tested software). The testing laboratory shall test the smartphone samples in accordance with the following testing details to ensure compliance with the Testing Items of the Technical Inspection Guidelines.

6.3.1 Required items

The embedded software is divided into three types: Factory Pre-loaded, Distributor Loaded and Iconless. This section describes pre-loaded and distributor loaded software and explains the testing conditions, testing methods and judgment criteria for the basic required items.

D.1 Data Authorization	
D.1.1.B The The embedded software shall obtain the user's consent prior to accessing sensitive data.	
Testing conditions: ■ The tested software is able to access sensitive data ■ Data type: Type 1 data and Type 2 data ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Determine whether the tested system's privacy policy or use statement provides a corresponding description and a user consent mechanism for the tested software to access sensitive data. (3) If step (2) is not met, the software under test is executed and the user sensitive data is accessed. (4) Determine whether the software under test provides a corresponding user consent mechanism.	Step (2), the privacy policy or the usage statement includes a corresponding description and a user consent mechanism for the tested software to access sensitive data. Or Step (4), the tested software has a corresponding user consent mechanism. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

D.2 Data Storage Protection	
D.2.1.B The embedded software shall store the password of the account in the Operating System Protection Area or in encrypted form.	
Testing conditions: ■ The tested software has an account password login function ■ Data type: Password of the Account ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Run the tested software, enter the account password; agree to save the account password and log in successfully. (4) Read the data of the files stored in the protection area of the non-operating system. (5) Determine whether the software under test stores the password of the account in plaintext in the Protection	Step (5), the software under test does not store the password of the account in plaintext in the non-operating system protection area. If the criteria have been met, the testing detail shall be deemed as passed; if the criteria have not been met, the testing detail shall be deemed as not passed.

Area of the non-operating system.	

D.3 Data Loss Protection	
D.3.1.B The smartphone system shall provide the user with the remote locking function and related security settings to ensure the user can remotely lock the smartphone system if the smartphone is lost or stolen.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Set and run the remote lock function for the system under test. (3) Determine whether the system under test is locked remotely.	Step (3), the system under test has been locked remotely. If the criteria have been met, the testing detail shall be deemed as passed; if the criteria have not been met, the testing detail shall be deemed as not passed.
D.3.2.B The smartphone system shall provide the user with remote data deletion function and related security settings to ensure the user can delete the data remotely if the smartphone is lost or stolen.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Enter the test data and save it. (3) Perform the remote deletion function of the system under test and delete the test data entered in step (2) remotely. (4) Determine whether the test data entered in step (2) is deleted.	Step (4), the test data has been deleted remotely. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
D.3.3.B The smartphone system shall provide a data backup function.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Determine whether the system under test has the data backup	Step (2), the system under test has a data backup function. If the criteria have been met, the

function.	testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

A.1 Program Identification	
A.1.1.B When the embedded software first accesses the account that is bound to the device, it shall first authenticate user identity and authority to ensure that the embedded software has the authority to use the account.	
Testing conditions: ■ The tested software has the ability to connect to the user's account ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Perform the user account authentication function of the tested software. (4) Determine whether the software under test provides a mechanism for user login confirmation and authorization.	Step (4), when the software under test accesses the user account, the user is prompted to authenticate and authorize. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

A.2 Program trust source	
A.2.1.B When the embedded software has payment function, the server credentials within the valid period shall be used to ensure the security of the payment transaction.	
Testing conditions: ■ The tested software has a payment function ■ Server Type: Payment Function Server ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) The software under test transmits data to the remote server through the network. (4) Determine whether the certificate data provided by the server to the	Step (4), the certificate data provided by the server to the tested software has not expired. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the

tested software has expired.	testing detail shall be deemed as not passed.

A.2.2.B The embedded software shall be able to identify its release information to ensure that the user understands its source.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Determine whether the software under test or the manufacturer's self-declaration form provides information about the publisher and version of the software under test.	Step (3), the software under test or the manufacturer's self-declaration table provides information about the publisher and version of the software under test. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

A.3 Program execution authorization	
A.3.1.B The embedded software shall obtain the user's consent to prior to each payment before any adjustment to the payment function being made.	
Testing conditions: ■ The tested software has a payment function ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Run the tested software and enable the payment function. (4) Determine whether the system under test or the software under test requires user consent prior to payment being made.	Step (4), the system under test or the software under test performs payment with the consent of the user. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
A.3.2.B The authorization required for the Embedded Software must match the "Function Description" and " Authorization Description" declared in the "Manufacturer Self-Declaration Form".	
Testing conditions: ■ The applicant shall complete the fields of "Function Description" and "Authority Description" in the "Manufacturer Self-Declaration Form" ■ Data type: N/A	

■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software

Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Run and operate the software under test, and enumerate the functions and access authority used by the software under test. (4) Determine whether the content listed in step (3) is consistent with the content of the manufacturer's self-declaration form.	Step (4), the content listed in step (3) is consistent with the content of the "Manufacturer Self-Declaration Form". If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

A.4 Program execution security	
A.4.1.B The embedded software shall provide a channel for reporting security issues.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Determine whether the software under test, the official website or the instruction manual provides a problem reporting channel.	Step (3), the problem found by the software under test can be reported through the problem reporting channel. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

P.1 Protocol for use license	
P.1.1.B The smartphone shall provide an interface for users to enable and disable the wireless transmission technology.	
Testing conditions: ■ Tested wireless transmission technologies: Bluetooth, WLAN, Mobile Communication Network and GPS (positioning service) ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Determine whether the	Step (3), the smartphone has an interface for turning on and off wireless transmission technology functions, and the state of the

smartphone provides an interface for turning on and off wireless transmission technology functions, and confirms whether the smartphone status matches the display status.	smartphone matches the display state. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
P.1.2.B When the wireless transmission technology function of the smartphone is confirmed as being on, the corresponding prompt state shall be given to the user.	
Testing conditions: ■ Tested wireless transmission technologies: Bluetooth, WLAN, NFC (Peer-to-Peer mode and Read/Write mode), mobile communications network and GPS (positioning service) ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Turn on the wireless transmission technology function of the smartphone. (4) Determine whether the smartphone provides the corresponding prompt.	Step (4), the smartphone provides a corresponding prompt for the user. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
P.1.3.B When the smartphone is connected to other devices through the wireless transmission technology for the first time, the connection shall be established only after the user agrees.	
Testing conditions: ■ Wireless transmission technology under test: Bluetooth and WLAN ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Turn on the wireless transmission technology function of the smartphone. (4) Turn on another device that can be connected through the wireless transmission technology and connect it to the mobile phone. (5) Select to reject or not accept the connection for the system under test.	Step (6), the system under test cannot establish a connection with the device in step (4). If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

(6) Determine whether the system under test can establish a connection with the equipment in step (4).	
P.1.4.B The smartphone shall provide an interface for users to enable and disable the Near Field Communication (NFC) technology.	
Testing conditions: ■ Tested wireless transmission technology: Near Field Communication technology (Near Field Communication, referred to as NFC) ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Determine whether the smartphone displays an interface for turning on and off the Near Field Communication technology function, and confirm whether the smartphone status matches the display status.	Step (3), the smartphone has an interface for turning on and off the Near Field Communication technology function (including the software binding mode), and the state of the smartphone matches the display state. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

P.2 Protocol transmission protection	
P.2.1.B When the embedded software transmits sensitive data through wireless transmission technology, encrypted transmission shall be used to ensure security of sensitive data.	
Testing conditions: ■ Software-enabled wireless transmission technology: Bluetooth, WLAN and mobile communication networks ■ Data type: Type 1 data (excluding photos) and positioning information ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Run the software under test and transmit sensitive data with the wireless transmission technology function.	Step (4), the tested software does not transmit sensitive data in plain text. If the criteria have been met, the testing detail shall be deemed as passed;

(4) Determine whether the software under test transmits sensitive data in plaintext.	If the criteria have not been met, the testing detail shall be deemed as not passed.

O.1 System operation authorization	
O.1.1.B The update source of the smartphone system shall match the "IP/DN/ Company Name and Server Type of the data link server" declared in the "Manufacturer Self-Declaration Form".	
Testing conditions: ■ The tested system has an operating system update function ■ The applicant is required to complete the "IP/DN/ Company Name and Server Type of the data link server" field in the "Manufacturer Self-Declaration Form" ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Perform the operating system update through the built-in operating system update function of the system under test. (4) Obtain the destination address of the operating system update. (5) Determine whether the destination address in step (4) matches the content of the manufacturer's self-declaration form.	Step (5), the destination address matches the content of the "Manufacturer Self-Declaration Form". If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
O.1.2.B The smartphone system shall provide update information when downloading or installing the updates of the operating system and informs the user of the content of update.	
Testing conditions: ■ The tested system has an operating system update function ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Determine whether the system under test or the official website provides information on the operating system updates and informs the user	Step (3), the system under test or the official website shall provide information about the operating system updates and inform the user to update the content. If the criteria have been met, the testing detail shall be deemed as

of the content of the update.	passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

O.2 System identification	
O.2.1.B The smartphone system shall support the screen unlock protection mechanism to protect personal information from unauthorized use.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Open the screen lock setting function interface of the system under test, and set the screen lock mode and unlock data. (3) Lock the system under test (including closing the screen and turning off the system under test). (4) Wake up the system under test (including opening the screen and turning on the system under test) and conduct the unlock operations. (5) Determine whether the unlocked data set in step (3) can be used to wake up the system under test.	Step (5), the tested system can be awaken by the password set in step (2). If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

O.2.2.B The smartphone system shall support the screen forced lock protection mechanism when attempting to unlock incorrectly to protect personal information from unauthorized use.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Open the screen lock setting function interface, and set the screen lock mode and unlock data. (3) Lock the system under test. (4) Wake up the system under test and repeatedly input the wrong	Step (5), the system under test displays a message indicating forced lock. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not

unlocking data several times. (5) Determine whether the system under test displays a message of forced lock.	passed.
O.2.3.B The smartphone system shall provide at least 72 types of password input values, including English uppercase, lowercase, numbers and special symbols, and the password shall be able to be long as 14 characters.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Open the password input setting interface. (3) Determine whether the password input value provided by the system under test includes English uppercase, lowercase, numbers and special symbols in more than 72 types. (4) Determine whether the password length can reach 14 characters or more.	Step (3), the password input value provided by the system under test includes English uppercases, lowercases, numbers and special symbols in more than 72 types. And Step (4), the password length can contain up to 14 characters or more. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

O.3. System execution security	
O.3.1.B The smartphone system shall provide a channel for reporting security issues.	
Testing conditions: ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Determine whether the system under test, the official website or the instruction manual provides a channel to report issues.	Step (2), the problem found by the system under test can be reported through the problem reporting channel. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not

	passed.

6.3.2 Optional testing items

If the applicant wishes to determine the security of Iconless Software, basic testing items for the Iconless Software as shown in Table 5 can also be selected for testing. For details of relevant tests, please refer to 6.3.1.

Table 5 Basic Testing Items and Testing subitems of Iconless Software

Layer	Testing Items	Testing subitems	Information Security Level	Testing code
Application layer (A)	2. Program trust source	1. When the embedded software has payment function, the server credentials within the valid period shall be used to ensure the security of the payment transaction.	B	A.2.1.B (+)
Communication protocol layer (P)	2. Protocol for transmission protection	1. When the embedded software transmits sensitive data through wireless transmission technology, encrypted transmission shall be used to ensure security of sensitive data.	B	P.2.1.B (+)

6.4 Medium Testing Items

6.4.1 Required items

This section describes the testing conditions, testing methods and criteria for the required Medium testing items for Factory Pre-loaded Software and Distributor Loaded Software.

A.3 Program execution authorization	
A.3.3.M The network connection port opened by the Embedded Software must match the "Communication Port Status" declared in the "Manufacturer Self-Declaration Form".	
Testing conditions: ■ The tested software has an open network connection port for network connection ■ The applicant must complete the " Communication Port Status " field in the " Manufacturer Self-Declaration Form " ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing	Step (4), the obtained network port number is consistent with the

conditions have been met. (3) Run the software under test and start communication, and obtain the network port number turned on by the tested software. (4) Determine whether the obtained network port number is consistent with the "Communication Port Status" declared by the "Manufacturer's Self-Declaration Form".	"Communication Port Status" declared by the "Manufacturer's Self-Declaration Form". If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

A.4 Program execution security	
A.4.2.M The embedded software shall be able to process malicious SQL injection.	
Testing conditions: ■ The tested software displays fields for users to input data ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Run the tested software and enter at least 50 common but different SQL Injection Attack strings. (4) Determine whether the tested software in step (3) performs the SQL Injection Attack string.	Step (4), the tested software does not perform the SQL Injection Attack string. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
A.4.3.M The embedded software shall be able to process the extensible markup language (XML) attack string.	
Testing conditions: ■ The tested software can receive the extensible markup language (XML) ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Perform the network transmission function of the software under test. (4) Intercept the communication packet transmitted by the remote host to the tested software. (5) Inject at least 10 sets of different	Step (6), the tested software does not perform the Injection Attack string. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not

extensible markup language attack strings into the communication packets intercepted by step (4) one by one, and then transmit them to the tested software. (6) Determine whether the tested software performs the injection attack string.	passed.

P.2 Protocol transmission protection	
P.2.2.M The embedded software shall avoid the attack of resending the Session ID.	
Testing conditions: ■The tested software has a Session ID when transmitting data over the network ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Perform the network transmission function of the software under test. (4) Record the communication packet between the tested software and the remote host, and retrieve the session ID. (5) Perform the resend attack using the Session ID in step (4) through the host computer.	Step (5), there is no effect when the host computer performs the resend attack using the Session ID. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
P.2.3.M Encrypted data transmission between the embedded software and the payment function server shall adopt a secure encryption algorithm.	
Testing conditions: ■ Server Type: Payment Function Server ■ The applicant can provide written information as the basis for review ■ If necessary, the testing laboratory may require the applicant to demonstrate the function ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Perform the network transmission function of the software under test. (4) Determine whether the server	Step (4), the encryption algorithm for communication between the tested software and the server is a FIPS 140 approved encryption and compilation algorithm or with the supporting evidence provided by the applicant to prove it has equivalent security.

accessed by the software under test uses the encryption algorithm approved by FIPS 140 or has the supporting evidence provided by the applicant to prove it has equivalent security.	If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

P.3 Protocol for implementation security	
P.3.1.M The smartphone system shall be able to handle errors in the content of the protocol.	
Testing conditions: ■ Tested wireless transmission technology: Bluetooth and WLAN ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Perform the network transmission function of the software under test. (4) In the wireless transmission environment under test, the fuzzy test method is used to transmit different error packets one by one for the communication protocol used, starting from the negotiation of the communication connection for up to 10000 times. (5) Determine whether the wireless transmission technology interface or the system under test is still operating normally.	Step (4), the system under test can perform communication connection and data transmission and operate normally. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

O.2 System identification	
O.2.4.M The screen lock/unlock information of the smartphone system shall not be stored on the smartphone in plaintext to avoid unauthorized use.	
Testing conditions: ■ The applicant must provide the smartphone with administrator authority ■ Screen lock function: graphics, passwords and biometrics ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Open the screen lock setting	Step (4), the screen lock unlock data is not stored in the plaintext on the smartphone.

function interface, and set the screen lock mode and unlock data. (4) Determine whether the unlocked data is stored on the smartphone in plaintext via the administrator authority. If the administrator authority is not provided, supporting information shall be provided or screenshot to be the proof in details. The testing laboratory may require the applicant to perform a functional demonstration if necessary.	If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

O.3. System execution security	
O.3.2.M The smartphone system shall have a memory configuration protection mechanism to prevent improper application of the program and reference functions in the memory.	
Testing conditions: ■ The applicant can provide written information as the basis for review ■ The applicant shall demonstrate the function if deemed necessary ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Determine whether this function is available according to review of the written materials. (2) When there is no sufficient data to display this function, the applicant will be required to demonstrate the function.	Step (1) or (2), the system under test has a memory configuration protection mechanism. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

6.4.2 Optional testing items

6.4.2.1 Optional testing items for Factory Pre-loaded Software and Distributor Loaded Software

This section describes the testing conditions, testing methods and criteria for the optional Medium testing items for Factory Pre-loaded Software and Distributor Loaded Software.

D.1 Data Use Authorization
D.1.2.M(+)After the user forbids the embedded software to access sensitive data through user settings, the software shall not be able to access relevant data.
Testing conditions:

■ The tested software has the function to refuse access to sensitive data
■ The applicant can provide written information as the basis for review
■ The applicant shall demonstrate the function if deemed necessary
■ Data type: Type 1 data and Type 2 data
■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software

Testing methods	Criteria
(1) Turn on the system under test. (2) Determine whether the tested system's privacy policy or statement of use provides a corresponding description and a user consent mechanism for the tested software to access sensitive data. (3) If there is a corresponding description and user consent mechanism for the tested software to access sensitive data in step (2), then choose to reject the privacy policy or statement of use and determine whether the system under test can continue to operate. (4) If there is no corresponding description of the software's access to sensitive data and the user consent mechanism in step (2), the software under test shall be ran, and the tested software's access sensitive data shall be rejected. (5) Determine whether the tested software still has access to sensitive data. (6) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.	Step (3), the system under test cannot continue to operate. Or in steps (5) and (6), the software under test cannot continue to operate or access the user's sensitive data. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

D.2 Data storage protection
D.2.2.M (+)The embedded software shall provide data encryption when storing sensitive data to avoid improper access to sensitive data.
Testing conditions: ■ The applicant must provide the smartphone administrator authority ■ The tested software has the ability to store sensitive data ■ Data type: Type 1 data (without photos) ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software

Testing methods	Criteria
(1) Turn on the system under test.	Step (4), the software under test does

(2) Confirm that the testing conditions have been met. (3) Run the software under test and store sensitive data. (4) Determine whether the tested software in step (3) stores the sensitive data in plaintext using the administrator authority.	not store sensitive data in plaintext. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
D.2.3.M (+) The account and password communicated between the embedded software and the remote server shall not exist in plaintext in the executable file to avoid improper access.	
Testing conditions: ■ The applicant must provide the smartphone administrator authority ■ The tested software has the account password login function ■ Data type: Account Number and Password ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Use the data reading tool to read the data of the tested software's executable file. (4) Determine whether the account and password communicated with the remote server are stored in plaintext in the tested software's executable file as shown in step (3).	Step (4), the account and password communicated with the remote server are not stored in plaintext in the tested software's executable file. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

A.3 Program execution authorization	
A.3.4.M (+) The embedded software shall not make calls or send text messages in the background without the user's consent.	
Testing conditions: ■ The applicant must provide the smartphone administrator authority ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Run the software under test and operate its functions. (4) Determine whether there call or a short message in the background has	Step (4), no record of calls and short messages in the background is found. If the criteria have been met, the testing detail shall be deemed as

occurred by comparing the call record and the time stamp of the short messages.	passed;; If the criteria have not been met, the testing detail shall be deemed as not passed.
A.3.5.M (+) The embedded software shall stop all related programs of the embedded software when turned off by the user.	
Testing conditions: ■ The applicant must provide the smartphone administrator authority ■ The tested software is a non-permanent program ■ Data type: N/A ■ Tested software properties: Factory Pre-loaded, Distributor Loaded Software	
Testing methods	Criteria
(1) Turn on the system under test. (2) Confirm that the testing conditions have been met. (3) Obtain a list of all applications in execution with the administrator authority. (4) Run and operate the software under test. (5) Close the tested software in step (4) and attain the list of all applications in execution with the administrator authority once more. (6) Determine whether the list of step (5) is the same as the list of step (3).	Step (6), the list of step (5) is the same as the list of step (3). If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

6.4.2.2 Optional Testing Items for Iconless Software

If the applicant wishes to determine the security of Iconless Software, Medium testing items for the Iconless Software as shown in Table 6 can be selected for testing. For details of relevant tests, please refer to 6.4.1.

Table 6 Medium Testing Items and Testing subitems of Iconless Software

Layer	Testing Items	Testing subitems	Information Security Level	Testing code
Application layer (A)	3. Program execution authorization	3. The network connection port opened by the Embedded Software must match the "Communication Port Status" declared in the "Manufacturer Self-Declaration Form".	M	A.3.3.M(+)
Communication protocol layer (P)	2. Protocol for	3. Encrypted data transmission between the embedded software and the payment	M	P.2.3.M(+)

	transmissi on protection	function server shall adopt a secure encryption algorithm.		

6.5 Advanced Testing Items

6.5.1 Required items

This section describes the testing conditions, testing methods and criteria for the required advanced testing items for Factory Pre-loaded Software and Distributor Loaded Software.

O.3. System execution security	
O.3.3.H The smartphone system shall establish a trusted transmission channel with the communication target during transmission for data protection purpose.	
Testing conditions: ■ The applicant shall provide written information as the basis for review ■ The applicant shall demonstrate the function if necessary ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Determine whether this function is available according to the written material. (2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.	Step (1) or (2), the transmission process of the system under test has a security channel. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
O.3.4.H The smartphone boot process shall include a password function test and a system software integrity self-test mechanism.	
Testing conditions: ■ The applicant shall provide written information as the basis for review ■ The applicant shall demonstrate the function if necessary ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Determine whether this function is available according to the written material. (2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.	Step (1) or (2), the booting process of the system under test has its own security function test. If the criteria have been met, the testing detail shall be deemed as passed;

	If the criteria have not been met, the testing detail shall be deemed as not passed.
O.3.5.H The smartphone system shall include a verification error counting mechanism. When the attempted error exceeds the threshold set by the smartphone, the protected information shall be erased.	
Testing conditions: ■ The applicant can provide written information as the basis for review ■ The applicant shall demonstrate the function if necessary ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Determine whether this function is available according to the written material. (2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.	Step (1) or (2), if the authentication fails, the system under test can initiate the data coverage mode, so that the protected data can be erased securely. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

<table>
<tr><td colspan="2">Key management protection</td></tr>
<tr><td colspan="2">H.1.1.H The key management of smartphone, including the generation, merging and destruction of encryption and communication keys, shall comply with the key usage and management standards issued by NIST, ANSI or IEEE.</td></tr>
<tr><td colspan="2">Testing conditions:
■ The applicant can provide written information as the basis for review
■ The applicant shall demonstrate the function if necessary
■ Data type: N/A
■ Tested software properties: N/A</td></tr>
<tr><td>Testing methods</td><td>Criteria</td></tr>
<tr><td>(1) Determine whether this function is available according to the written material.

(2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.</td><td>Step (1) or (2), the key of the hardware under test is managed in conformance to the confidentiality and integrity requirements.
If the criteria have been met, the testing detail shall be deemed as passed;
If the criteria have not been met, the testing detail shall be deemed as not passed.</td></tr>
<tr><td colspan="2">H.1.2.H The smartphone's key stored in the mobile device shall include additional protection of its confidentiality and integrity.</td></tr>
<tr><td colspan="2">Testing conditions:
■ The applicant can provide written information as the basis for review
■ If necessary, the manufacturer shall demonstrate the function
■ Data type: N/A
■ Tested software properties: N/A</td></tr>
<tr><td>Testing methods</td><td>Criteria</td></tr>
<tr><td>(1) Determine whether this function is available according to the written material.
(2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.</td><td>Step (1) or (2), the key of the hardware under test is stored and protected in conformance to the confidentiality and integrity requirements.

If the criteria have been met, the testing detail shall be deemed as passed;
If the criteria have not been met, the testing detail shall be deemed as not passed.</td></tr>
<tr><td colspan="2">H.1.3.H Keys shall not stored in plaintext in non-volatile memory and shall not be exported in any way or directly transmitted.</td></tr>
<tr><td colspan="2">Testing conditions:
■ The applicant can provide written information as the basis for review
■ The applicant shall demonstrate the function if necessary
■ Data type: N/A</td></tr>
</table>

■ Tested software properties: N/A

Testing methods	Criteria
(1) Decide whether this function is available according to the written material. (2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.	Step (1) or (2), the key transmission protection of the tested hardware conforms to the requirement of no export or transmission. If the key needs to be exported or transmitted by encryption, the strength of the encryption must be greater than or equal to the key strength based on the original algorithm. For the encryption strength, please refer to data published by NIST, ANSI or IEEE. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.

H.2 Algorithm strength requirements	
H.2.1.H The encryption, decryption and signature algorithms of the smartphone implementation shall comply with the key algorithm standard issued by NIST, ANSI or IEEE. The relevant standards are listed below: IEEE 802.11ac-2013, IEEE 802.1X. NIST SP 800-38A, 38C~F, 56A~B, 57, 90B	
Testing conditions: ■ The applicant can provide written information as the basis for review ■ The applicant shall demonstrate the function if necessary ■ Data type: N/A ■ Tested software properties: N/A	
Testing methods	Criteria
(1) Decide whether this function is available according to the written material. (2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.	Step (1) or (2), the algorithm of the tested hardware conforms to the Technical Requirements. If the criteria have been met, the testing detail shall be deemed as passed; If the criteria have not been met, the testing detail shall be deemed as not passed.
H.2.2.H The algorithm for the smartphone implementation shall generate an initialization vector according to the requirements of each mode and meet the initialization vector requirements issued by NIST. The relevant standards are: NIST SP 800-38A, 38C~F, 56A~B, 57, 90B	

<table>
<tr><td colspan="2">Testing conditions:
■ The applicant can provide written information as the basis for review
■ The applicant shall demonstrate the function if necessary
■ Data type: N/A
■ Tested software properties: N/A</td></tr>
<tr><td>Testing methods</td><td>Criteria</td></tr>
<tr><td>(1) Decide whether this function is available according to the written material.
(2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.</td><td>Step (1) or (2), the initial vector of the hardware under test conforms to the Technical Requirements.
If the criteria have been met, the testing detail shall be deemed as passed;
If the criteria have not been met, the testing detail shall be deemed as not passed.</td></tr>
<tr><td colspan="2">H.2.3.H The random number used by the key shall comply with the requirements of the random bit generation specification issued by NIST or ANSI. The relevant standards are listed below:
NIST SP 800-90A, ANSI X9.31-1998</td></tr>
<tr><td colspan="2">Testing conditions:
■ The applicant can provide written information as the basis for review
■ The applicant shall demonstrate the function if necessary
■ Data type: N/A
■ Tested software properties: N/A</td></tr>
<tr><td>Testing methods</td><td>Criteria</td></tr>
<tr><td>(1) Determine whether this function is available according to the written material.
(2) When there is no sufficient data to display this function, the applicant shall be required to demonstrate the function.</td><td>Step (1) or (2), the random number of the hardware under test conforms to the Technical Requirements.
If the criteria have been met, the testing detail shall be deemed as passed;
If the criteria have not been met, the testing detail shall be deemed as not passed.</td></tr>
</table>

Annex 1 Application for Testing the Infocom Security of the Embedded Software

Application Date: YYYY/MM/DD

<table>
<tr><td colspan="2">Applicant (Company, Trade Name)</td><td>☐ Manufacturer
☐ Telecom Operator
☐Agency in Taiwan</td><td colspan="2">○○○ Limited Company</td><td rowspan="4">Seal of the Applicant (Big/Small Seals)</td></tr>
<tr><td colspan="2">Unified Business Code</td><td colspan="3"></td></tr>
<tr><td colspan="2">Business Address</td><td colspan="3">☐☐☐-☐☐</td></tr>
<tr><td colspan="2">Representative Name</td><td colspan="3"></td></tr>
<tr><td rowspan="2">Contact Person</td><td>Name and Title</td><td></td><td>Email</td><td></td><td rowspan="2">Seal of the Applicant (Big/Small Seals)</td></tr>
<tr><td>Contact Phone</td><td></td><td>Fax Machine</td><td></td></tr>
<tr><td colspan="2">Manufacturer and Address</td><td colspan="4">○○○ Limited Company
☐☐☐-☐☐</td></tr>
<tr><td colspan="3">Smartphone brand / model / name</td><td colspan="3">ex. APPLE / a16xx / iPhone 6s</td></tr>
<tr><td colspan="3">Version of the Smartphone Operating System for Testing</td><td colspan="3">○○○-○○○-○○○</td></tr>
<tr><td colspan="2">Application for Testing the Security Level</td><td colspan="4">☐Basic ☐Medium ☐Medium (including selected testing items) ☐ High ☐ High (including selected testing items)</td></tr>
<tr><td colspan="2" rowspan="4">Smartphone Functions</td><td>Positioning Function</td><td colspan="3">☐U.S. GPS ☐Europe Galileo
☐ Russia GLONASS ☐ Other,_
☐ China Beidou Navigation Satellite (☐ Two-Way Transmission)</td></tr>
<tr><td>Wireless transmission technology</td><td colspan="3">☐ Bluetooth ☐ Mobile Communication Network (☐ 3G ☐ 4G)
☐ WLAN ☐ Other,_
☐ NFC (☐ Peer-to-Peer Mode ☐ Read/Write Mode)</td></tr>
<tr><td>Biometric identification</td><td colspan="3">☐ No ☐ Yes, Fingerprint identification,...</td></tr>
<tr><td>External memory</td><td colspan="3">☐ ☐ No ☐ Yes, microSD card,...</td></tr>
<tr><td colspan="2" rowspan="3">Smartphone samples / Quantity</td><td>Basic</td><td colspan="3">☐ Number of Tested Samples: 2</td></tr>
<tr><td>Medium</td><td colspan="3">☐ Number of Tested Samples: 2. Grant the administrator authority according to the testing items and specific needs.</td></tr>
<tr><td>Advanced</td><td colspan="3">☐ Number of Tested Samples: 2. Grant the administrator authority according to the testing items and specific needs.</td></tr>
<tr><td colspan="2">Attached Documents (Original or photocopy)</td><td colspan="4">☐ 1. Chinese or English Manual or Instructions
☐ 2. Chinese or English Specifications
☐ 3. Company registration certificate or business registration certificate; if the applicant is a foreign manufacturer, the relevant certification documents of the manufacturer should be attached.
☐ 4. Manufacturer Self-Declaration Form, Embedded Software summary form
☐ 5. Security function specification sheet, design security sheet and security structure sheet (Must be attached for advanced testing items)
☐ 6. CD in 1 copy (including the Testing Application and the contents specified in Item 1 through Item 5)</td></tr>
</table>

<table>
<tr><td colspan="6">[Note] Asides from retaining the originals and CD-ROM of the application, the testing laboratory shall return the photocopy of the testing application, the smartphone samples and the rest of the documents to the applicant upon the issuance of the test report.</td></tr>
<tr><td rowspan="4">Testing Laboratory (to be completed by the Laboratory)</td><td colspan="4">Testing Laboratory Name:</td><td rowspan="4">Testing Laboratory</td></tr>
<tr><td colspan="4">Issue a test report: 1.
Test Report No:
2.Security Level: ☐ Basic ☐ Medium ☐ Advanced</td></tr>
<tr><td>Date of Acceptance</td><td></td><td>Completion Date</td><td></td></tr>
<tr><td>Contact Person</td><td></td><td>Contact Number</td><td></td></tr>
</table>

Annex 2 Manufacturer Self-Declaration Form -1 (Example)

Basic Information of the Tested Software					Data layer		Communication protocol
Item	**Tested software name**	**Publisher and version**	**Tested Package Name**	**Tested software name**	**Does the device access sensitive data?**	**Does the device support wireless transmission technology?**	**Does the device allow login with an account Password?**
1	Phone	Company 1.2.2	Com. android. Phone	☐Factory pre-loaded software ☐Distributor Loaded Software ☐ Iconless software	☐ No ☐ Type 1 ☐ Type 2	☐ No ☐ Wifi ☐ GPS (Positioning Service) ☐ Bluetooth ☐ Mobile network ☐ NFC (Peer-to-Peer mode) ☐ NFC (Read/Write mode) ☐ Infrared ☐ Other____	☐ No ☐ Yes

Annex 2 Manufacturer Self-Declaration Form -2 (Example)

Basic Information of the Tested Software			Application layer			
Item	**Tested software name**	**Publisher and version**	**Function Description**	**Authorization description**	**IP/DN/ Company Name and Server Type of the data link server**	**Communication Port Status**
1	Phone	Company 1.2.2	☐ Resident software ☐ Non-permanent software - Description: Can make a call from contacts.	READ_CONTACTS: For message sharing	apPchat. example.net： Surfer 111.112. 113.114: Payment Function Host	☐ Opened ☐ Closed **Port No.:** ____
				ACCOUNT_MANAGER: Used to add accounts to the community		
				CAMERA: for picture recording		
				INTERNET: Used to connect hosts and obtain notifications		

[Note] The server types include the surfer and the payment function host.

Annex 3 Embedded Software Summary Table

Embedded Software Summary Table

1. Smartphone brand/model/marketing name: APPLE / a16xx / iPhone 6s

2. Operating system version: ○○○-○○○-○○○

3. Embedded software information:

No.	Name	Publisher and version	Attributes	Function Description	Authority description
APP01	Phone	Company 1.2.2	■Factory Pre-loaded □Distributor Loaded Software □Iconless	(1) Make a call from the directory	(1) READ_CONTACTS: for message sharing (2) ACCOUNT_MANAGER: for adding account to the community (3) CAMERA: for picture recording (4) INTERNET: for connecting the host and getting the latest information
APP02	…		□Factory Pre-loaded □Distributor Loaded Software □Iconless		
…	…		□Factory Pre-loaded □Distributor Loaded Software □Iconless		

Annex 4 Security Function Specification Sheet

TOE Security function interface name TSFI	Purpose	Security function requirements that can be implemented by the security function interface SFR	Method of Use	Parameters	Actions	Error Message
List all Security function interfaces.	Describe the purpose/the security function of each security function interface.	Describe how each security function interface implements the security function requirements listed in O.7~O.11 and H.1~H.5.	Describe how to use the various security features.	Describe all the parameters of the security function interfaces and their meanings.	Describe how each security function interface works and its execution details.	Describe the error message generated by each security function interface, including its meaning and generation conditions.
Example: *TSFI_CLI*	Example: Provides the command line mode operation interface.	Example: SFR_ Security Management: Provides security management capabilities.	Example: Connect the object to be tested with ssh. That is, provide the command line mode operation interface.	Example: *ID & password*	Example: Can issue management commands to operate the object under test.	Example: Connection failed Authentication failed

Annex 5 Design Security Sheet

Subsystem	**Purpose**	**Subsystem security function interface** **TSFI**	**Description of Behavior**
List the subsystem of each security function of the interface.	Explain the purpose/security function of each subsystem.	Explain that each subsystem belongs to the security function interface listed in Annex 3.	Describe the actions of each subsystem as follows: (1) How the subsystem implements the function of the security function interface. (2) Information about interaction with other subsystems, including the communication between different subsystems and the characteristics of the transmitted data.
Example: *Subsystem_ssh*	Example: Provide the *ssh* service.	Example: *TSFI_CLI*	Example: *(1)* Provide the *TSFI_CLI* command line mode operation interface. *(2)* Interaction with other subsystems: *(A) Subsystem_auth:* Pass the authentication information to *Subsystem_auth* and confirm the success of the authentication by replying to the message. *(B) Subsystem_terminal: …*

Annex 6 Security Architecture Sheet

Item	Description	
	Security Domain Name	**Security Domain Description**
1. Security Domain	List the security areas corresponding to each security function interface Example: *TSFI_GUI:* *Domain_SecureLogAudit* *Domain_SecureConnection*	Describe how data to be protected under the operating environment of security function and internal execution restrictions is separated. Example: When the *TSFI_GUI is* used to execute the management function, the *TSFI* can only have a single remote connection at a time, and can only perform a single request for data auditing.

Item	Description	
	Related components	**Initial program description**
2. Initial program Secure Initialization	Operate the relevant components / environment of the object to be tested. Example: Network connection program for the object to be tested.	Provide the secure initialization steps and installation procedures for relevant components of the object to be tested. Example: *1.* The port labeled from *0/0 (ethernet0/0 interface)* is connected to the security zone of the switch or router via a cable *RJ- 45*. 2. The port labeled from 0/1 (ethernet 0/1 interface) is connected to the DMZ zone of the switch or router via a cable RJ- 45.

Item	Description		
	Self-protection function	**Relationship with external devices**	**Self-protection mechanism description**
3. Self- Protection	List the self-protection mechanisms corresponding to each of the security function interfaces. Example: *TSFI_WEB:* Self-protection *1:* Identity verification Self-protection *2:* Remote connection encryption	Describe the data exchange actions between the security functions and its interface and, external devices. Example: When the tested object is remotely connected via the browser using the management function, the *TSFI_WEB GUI* interface shall be used for authentication.	Describe how the security function interface provides a physical or logical self-protection mechanism. Example: *1.* Key in the password to enter the interface. *2.* Data transmission mechanism: *TLS/SSL*. *3.* Special execution mode: Fingerprint identification. *4.* Special equipment requirements: Fingerprint reader.

Item	Description	
4. Non-Bypassibility	**Non-Bypassibility function**	**Non-Bypassibility mechanism description**
	List the Non-Bypassibility mechanisms for each security function. Example: *TSF_Authentication* Identity verification function	1. List possible ways of bypassing. 2. Describe the precautionary approach, including how to enter the security function interface under protection, how to protect the data processing during the implementation phase, and whether there are other external channels and related mechanisms to prevent illegal entry. Example: It is possible to directly manipulate the object to be tested with the maintenance interface without identity authentication. Precautionary approach: Use the physical blockade to prevent the use of the maintenance interface to bypass the identity authentication process.