Basic Information Security Testing Standard for Mobile Applications

V3.2

Mobile Application Security Alliance

January 2022

Version History of «Basic Information Security Testing Standard for Mobile Applications»

Date	Version
August 2015	V1.0
February 2016	V2.0
March 2017	V2.1
August 2018	V3.0
September 2019	V3.1
January 2022	V3.2

Table of Contents

List of Tables

1. Foreword

As mobile devices have become an indispensable equipment in our everyday life, various types of mobile applications (abbr. apps) have emerged. Yet, as some of these mobile applications are developed without the awareness of information security, these mobile applications may cause the risks of user data leakage or financial loss. Therefore, in accordance with the resolution of the 26th Committee Meeting of the National Information & Communication Security Taskforce of the Executive Yuan on June 24, 2014, referring to relevant international information security standards and publicly solicited opinions from stakeholders of various fields, the Industrial Development Bureau of the Ministry of Economic Affairs (hereinafter referred to as "IDB") completed the formulation of the «Basic Information Security Standard for Mobile Applications», which can serve as reference and guidance for practitioners to take voluntarily when developing mobile applications.

In order to assist mobile application developers to properly follow the «Basic Information Security Standard for Mobile Applications» and to maintain secure development quality of mobile applications, the IDB appointed the Institute for Information Industry and Chinese Cryptology and Information Security Association as the executive agencies for the revision of the «Basic Information Security Testing Standard for Mobile Applications» (hereinafter referred to as "the Standard"). As a result, in August 2018, V3.0 of the Standard was published; and in September 2019, V3.1 was published. In January 2022, in order to verify and ensure the security of mobile applications, Taipei Computer Association was appointed as the executive agency for the revision of V3.2 of the Standard (hereinafter referred to as "the given Standard"). In the given Standard, the application categorization is mainly based on that of the «Basic Information Security Standard for Mobile Applications». In order to perform security risk assessment and verification to mobile applications, the given Standard took reference from the OWASP «Mobile Application Security Verification Standard v1.2» (of the OWASP «Mobile Security Testing Guide»), CSA MAST

«Cloud Security Alliance – Mobile Application Security Testing», and NIST «Special Publication 800-163 Vetting the Security of Mobile Applications», then formulated accordingly its basic information security test items, check items to be inspected in each test item, expected test results of each test item and their respective conditions for achieving the results, etc.

The given Standard is a metric for third-party institutions to perform information security testing and security level evaluation to mobile applications. Through the compliance of mobile applications with the requirements of the given Standard, a sense of security and trust can thus be established upon the use of mobile applications.

2. Scope of application

The test items of the given Standard are applicable to mobile applications of non-specific fields and the mobile applications specified as applicable in the «Basic Information Security Standard for Mobile Applications» to ensure that the tested mobile applications meet the requirements of current information security level. The essence of information security is the concept of risk control. Therefore, even if the mobile application test results passed the test categories defined by the given Standard, it cannot completely guarantee that the mobile application will not be maliciously cracked or exploited. In order to reduce risks and harm caused by intentional act or negligence, users of mobile applications shall also fulfill their responsibilities regarding the use and management of personal information, e. g. account/password management, confidentiality, etc.

3. Glossary

The following terms and definitions refer to those of the «Basic Information Security Standard for Mobile Applications V1.4». Should there be any changes, the latest version of the «Basic Information Security Standard for Mobile Applications» will prevail.

3.1. Mobile Application

A type of program which is designed for smartphones and tablet computers. In the given Standard, it is also abbreviated as “mobile app”.

3.2. Application Store

A platform or website which provides mobile device users to browse, download and/or purchase mobile applications.

3.3. Personal Data

All of the information, as primarily defined in the «Personal Data Protection Act», which can directly or indirectly identify the individual, including but not limited to the natural person's name, date of birth, ID card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, bank account balance, data concerning a person's social activities.

3.4. Sensitive Data

The information created, stored or transmitted on the mobile device and its storage media due to the user's behavior or the operation of mobile applications, in which the access to personal private information is classified as collection, storing data in the local device is classified as storage, and of which the leakage may cause harm to users. The information, in addition to the personal information defined in 3.3, also includes, but not limited to, passwords, keys, videos, photos, phone calls, audio files, instant messaging messages, call logs, SMS, memo, contacts, notes, geographic location, calendar, device identifier, and any other

information related to personal privacy.

3.5. Password

A set of character strings which allow users to use the system or the identification of users' identity, including password(s) for local files with storage encryption, users' own account(s)/password(s), account(s)/password(s) for remote web service.

3.6. Transaction Resource

The additional functions, contents or subscription items that can be obtained directly or indirectly via the purchase function provided in mobile applications; virtual or physical currency (including points or serial numbers) or any other valuable items are all regarded as transaction resources as long as any payment flow is involved. (e. g. a set of QR codes used as vouchers for tickets which is obtained through purchasing tickets in a ticketing system app; the contents of an e-book for reading which are obtained through purchasing the e-book in an online bookstore app; the provision of new functions, the removal of functions regarding use limitations, or the function of advertisement removal, etc., obtained after the transaction if transaction service items in the app are subscribed or purchased; the payment function provided by the payment apps, the transfer function provided by banking apps, or the function of purchasing physical or virtual goods provided by apps). In order to protect consumer rights, risk-taking sensitive operations, such as stock orders, shall also be recorded for the users.

3.7. Session Identification, Session ID

The identifier assigned to a connection when the connection is established, which is used as the unique identification code during the connection. When the connection ends, the identifier can be released and re-assigned to a new connection.

3.8. Server Certificate

A certificate which contains the information regarding signature verification, which is provided to mobile applications for authentication of server identity and encryption of data transmission.

3.9. Certification Authority

An agency or legal person that issues certificate.

3.10. Malicious Code

The code that infringes user rights without user consent, including but not limited to any codes with malicious features or behaviors.

3.11. Vulnerability

The flaws of mobile applications in security aspects which pose threats to the confidentiality, integrity, and availability of the system or the data of mobile applications.

3.12. Library

The binary codes for programmers to use, which are compiled from functions or objects collected by packaging some complicated or hardware-level related programs.

3.13. Code Injection

The execution of malicious commands inputted by users due to the design flaws in mobile applications, including but not limited to command injection and SQL injection.

3.14. Mobile Operating System

An operating system which operates on mobile devices.

3.15. Mobile Resource

Functions or services provided by mobile devices, including but not limited to camera, photos, microphone, wireless network, sensor and geographic location.

3.16. In-Application Update

An update of contents and functions of a mobile application via customized methods without changing the major version released on the application store.

3.17. Common Vulnerabilities and Exposures

Abbreviated as “CVE”, a vulnerability management program sponsored by the U.S. Department of Homeland Security, in which a globally recognized unique

universal number will be assigned to each vulnerability item.

3.18. Known Vulnerabilities

The vulnerabilities with CVE numbers.

3.19. Authentication

The provision of assurance of the identity claimed by an individual.

3.20. Advanced Encryption Standard

The AES (Advanced Encryption Standard) encryption algorithm published by the National Institute of Standards and Technology (NIST) in 2001 and formally implemented in 2002, of which the document number is № FIPS PUB 197. The AES can support 128-bit data blocks, and supports 128, 192, and 256-bit key sizes. In order to improve security, the AES's encryption/decryption process consists of more than 10 round numbers, and each round contains four main basic units.

3.21. Triple Data Encryption Standard

A type of product cipher, which uses the Triple Data Encryption Standard to process 64-bit data blocks.

3.22. Elliptic Curve Cryptography

A type of algorithm for establishing public key encryption, which is based on additive groups or mathematical structures generated by elliptic curves. The use of elliptic curves in cryptography was independently proposed by Neal Koblitz and Victor Miller respectively in 1985.

3.23. Certificate Pinning

The process in which the server certificate is stored in the application in advance in order to verify whether it conforms to the server certificate when establishing connection.

3.24. Hash

The data fingerprint calculated by an algorithm with a series of data. As it is often used to identify whether the files and data have been tampered with, it can ensure that the files and data are indeed provided by the original creator.

3.25. Obfuscation

The conversion of mobile application source code into a form which is hard to read without affecting the execution of functions.

3.26. Using Sensitive Data

The use of sensitive data, including the use by the application itself and the use via the provision to third parties.

3.27. Log File

The system logs, application logs, security logs, debug logs or custom log files which are only for the debugging purposes.

3.28. Device Identifier

The unique identification information of hardware or software, including International Mobile Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), International Mobile Subscriber Identity (IMSI), Integrated Circuit Card Identifier(ICCID), Media Access Control Address (MAC Address), Android Identifier (Android ID), Android Advertising ID (AID), iOS Identifier for Advertisers Identifier (IFAID), Windows Phone Device ID.

3.29. Cache Files or Temporary Files

The files generated after the installation and/or operation of a mobile application which are not related to the functionality of the application. These files are usually deleted at the termination of the application. The existence of these files, e.g. temporary files, cache files, does not affect the functionality and performance of the mobile application when it is executed again. If deleting a certain file will cause the failure of the automatic login function, then the file should be classified as a configuration file rather than a cache or temporary file.

3.30. Configuration File

The files in which a mobile application stores relevant settings; should the files be deleted, it will affect the mobile application’s performance of functionality when the mobile application is executed again.

3.31. Encode

The action of converting data into codes or characters; and, the codes or characters can also be translated (decoded) back into the original data.

3.32. Decode

The action of converting the encoded codes or characters into the original data.

3.33. Payload

The valid data or commands in the contents of a packet, message or code.

3.34. Collecting Sensitive Data

The acquisition by a mobile application of the sensitive data built-in in the mobile device or inputted by the user.

3.35. Storing Sensitive Data

The action in which a mobile application writes sensitive data in the form of a file into a mobile device or its subordinate storage media.

3.36. Common Vulnerability Scoring System

Abbreviated as “CVSS”, a system which gives scores based on the features and impacts of IT vulnerabilities. The system was originally researched by the National Infrastructure Advisory Council (NIAC); it is now handed over to the Forum of Incident Response and Security Teams (FIRST) for development, which is currently on version 3.

3.37. Secure Random Number Generator

Random number generator functions that conform to or refer to at least one of the criteria of the ANSI X9.17, FIPS 140-2, NIST SP 800-22, and SP 800-90A (CAVP Testing: Random Number Generators).

3.38. Secure Domain

The domains which include the domains where the developers and clients belong to or the commonly familiar public secure domains. The commonly familiar public secure domains include those which support the application of OAuth 2.0 protocol, e.g. Facebook, Google, Twitter, etc.

3.39. Secure Encryption Function

The encryption functions that conform to those in FIPS 140-2 Annex A.

3.40. System Credentials Storage Facilities

The services provided by the mobile operating systems for the mobile application developers and mobile device users to store user credentials or passwords, keys, e. g. Keystore (Android), Keychain (iOS), or other similar mechanisms.

4. Basic Information Security Testing Standard

The test items of the «Basic Information Security Testing Standard for Mobile Applications» (hereinafter referred to as "the Standard") are based on the content regarding information security technical requirements listed in "4. Technical Requirements" of the «Basic Information Security Standard for Mobile Applications», which mainly serve as a test basis for the information security testing companies; as the «Basic Information Security Standard for Mobile Applications» is mainly provided as a reference for mobile application developers, therefore, not all of the requirements of the «Basic Information Security Standard for Mobile Applications» need to be tested in the Standard.

The test items in the Standard are categorized into two types: test items for inspection and test items for reference. Test items for inspection are the test items that must be satisfied. Should the mobile application satisfies the test items for inspection of the given Standard, it indicates that if the user did not crack the OS layer protection of the mobile device (e.g. by rooting, jailbreaking), then the mobile application meets basic information security level (For the test items for inspection, please consult section "4.1 Basic Information Security Testing Standard for Mobile Applications"). Test items for reference, on the other hand, only serve as reference and do not require actual inspection due to the reasons listed below:

- The items are only relevant to quality and do not directly affect the security of mobile applications.
- The inspection on the items is difficult to perform or do not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present.
- The items are for developers' reference only, not the items to which actual inspection is performed.

For further information regarding items for reference, please consult "Appendix

V. Basic Information Security Test Items for Reference for Mobile Applications".

In order to formulate the scope of security requirements for each category of mobile applications, based on the functionality classification of mobile applications, the «Basic Information Security Standard for Mobile Applications» and the «Basic Information Security Testing Standard for Mobile Applications» categorize mobile applications (and their respective list of test items) into three major categories and one additional category which requires extra tests.

L1: A mobile application that does not require user authentication, which has 23 test items requiring inspection.

L2: A mobile application that requires user authentication, which has 29 test items requiring inspection.

L3: A mobile application in which transaction behavior is involved, which has 35 test items requiring inspection.

F: A mobile application that has higher security requirements, which has an additional category of test items and has 6 test items requiring inspection.

If a mobile application has the characteristics of both L2 and L3, it will be classified as an L3 mobile application.

For the test items' relationship diagram of mobile applications of each category and the relevant regulations regarding submission for inspection, please consult "Appendix I. Instructions regarding the submission categories of mobile applications". In addition to the test items categorized based on the functionality of mobile applications, there are also the F-type test items, which are the advanced additional test items for the apps demanding higher security; the main content of inspection on the F-type test items is reverse engineering analysis, tampering attacks, etc. Finally, the agencies of submission can choose whether to perform tests with the F-type test items based on their needs.

When a mobile application is submitted for inspection, the agency of submission must make a detailed declaration and filled the “Questionnaire on Basic Information Security Testing for Mobile Applications” listed in Appendix III. On the one hand, the given procedure can urge the manufacturer of submission to examine the necessary sensitive data and the reasonableness of the permissions by itself; on the other hand, it can help inspection personnel speed up their understanding of the business logic of the mobile application and its related functions, so as to facilitate the inspection.

4.1. Basic Information Security Testing Standard for Mobile Applications

In this chapter, the given Standard will stipulates criteria for basic information security testing regarding mobile application security in various aspects. There are five major aspects within this chapter, in which the test items and their criteria will be respectively elucidated in detail in these sections: “4.1.1. Security regarding Mobile Application Release”, “4.1.2. Sensitive Data Protection”, “4.1.3. Security regarding Transaction Resource Management”, “4.1.4. Security regarding User Authentication, Authorization, and Connection Management in Mobile Applications”, and “4.1.5. Code Security of the Mobile Application”.

For each test item, form fields will be formulated as follows: Test Item №, Test Description, Test Category, Test Standards, Technical Requirements, Test Criteria, Test Result and Notes; the description of the test item form fields will also be shown in Table 1.

Table 1. Description of the Test Item Form Fields

FIELD NAME	DESCRIPTION
Test Item №	The test item number consisting of 5 digits shown in the format as 4.1.x.y.z – in which the “4.1.” indicates the digits representing the chapter “Basic Information Security Testing Standard for Mobile Applications”, and the “x.y.z” stands for the affiliated item numbers which expand downwards respectively. The test item numbers are assigned accordingly to those of the Chapter “4. Technical Requirements” of the «Basic Information Security Standard for Mobile Applications».
Test Description	The summary of the test item which is formulated based on the content of the Chapter “4. Technical Requirements” of the «Basic Information Security Standard for Mobile Applications».
Test Category	L1: A mobile application that does not require user authentication. L2: A mobile application that requires user authentication. L3: A mobile application in which transaction behavior is involved. F: A mobile application that has higher security requirements. Note: If this field is marked with “L2, L3”, it indicates that the test item must be performed to both L2 and L3 mobile applications. The F-type test items are the advanced additional test items for the apps demanding higher security. As a result, whether to perform the F-type test items is selectable in testing (which will be marked as “+F”, e.g. “L1+F” indicates that L1 and F-type test items will be performed to the application)
Test Standards	The technical requirements regarding information security for mobile applications corresponding to those of the Chapter “4. Technical Requirements” of the «Basic Information Security Standard for Mobile Applications» and those of the OWASP “Mobile Security Testing Guide” (MSTG).

Technical Requirements	The “contents” of the technical requirements regarding information security for mobile applications corresponding to those of the Chapter “4. Technical Requirements” of the «Basic Information Security Standard for Mobile Applications»
Test Criteria	All the check items which require inspection according to the test items.
Test Result	The expected test results and their respective conditions for achieving the results based on the check items. The expected test results include: “Passed”, “Failed” and “Non-Applicable”. Passed – The application meets the criteria of the test item Failed – The application fails to meet the criteria of the test item. The conditions for “Non-Applicable” vary depending on the contents of each test item, e. g. there is no need to conduct the inspection on the test item due to the fact that the mobile application will not be publicly released or is not released yet, etc. Description: 1. Publicly available a、 Publicly released. b、 Not yet released: indicating that the mobile application is still in development stage, and may be publicly released in the future. 2. Not publicly available: indicating that the mobile application is internally used within the enterprise, whether to be released publicly or not.
Notes	Other additional information or remarks.

For all the test items that require “obtaining user consent”, “user consent” can be obtained via two approaches: either with the declaration which states that “download, installation, and use by the user would be deemed to be consent” in a trusted application store, or with “the active provision of elucidation and agree/disagree options” when the mobile application is executed (at least for the first time). When the mobile application submitted for inspection provides both of the above-mentioned approaches in obtaining user consent, the approach which is in the mobile application will be the basis for inspection which determines whether the mobile application meets the criteria.

4.1.1. Security regarding Mobile Application Release

This aspect is mainly applicable to relevant information security testing standards regarding mobile application release, including its releasing, updating, and problem reporting, etc.

4.1.1.1. Mobile Application Release

For the test items regarding “Mobile Application Release”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, and L3 mobile applications must pass the requirements of “4.1.1.1.2. When releasing, the mobile application shall elucidate the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions”, and the F-type mobile applications must pass the requirements of “4.1.1.1.3. The mobile application shall prompt the user to install protection software on the mobile device in a prominent location (e. g. the official website, the application download page, etc.).”

4.1.1.1.1. The mobile application shall be released in an application store of a trusted source.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.1.1.2. When releasing, the mobile application shall elucidate the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions.

TEST ITEM	4.1.1.1.2
Test Description	Elucidation regarding mobile application release.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Applications» 4.1.1.1 Mobile Application Release, MSTG-PLATFORM-1, MSTG-STORAGE-12
Technical Requirements	When releasing, the mobile application shall elucidate the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions
Test Criteria	If the mobile application has already been released, then inspect whether the mobile application elucidates the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions based on its actual needs in the application store. If the mobile application is not released yet, then inspect whether the mobile application elucidates the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions in the Questionnaire. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item.

	Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application will not be publicly released; therefore, inspection on the test item is not required.
Notes	The source of release shall be self-declared in the «Questionnaire on Basic Information of the Mobile Application» (Appendix III. Questionnaire on Basic Information Security Testing for Mobile Applications). The declaration on the application store primarily refers to that of the store interface of the mobile device.

4.1.1.1.3. The mobile application shall prompt the user to install protection software on the mobile device in a prominent location (e. g. the official website, the application download page, etc.)

TEST ITEM	4.1.1.1.3
Test Description	The prompted information of the mobile application.
Test Category	F
Test Standards	«Basic Information Security Standard for Mobile Applications» 4.1.1.1 Mobile Application Release
Technical Requirements	The mobile application shall prompt the user to install protection software on the mobile device in a prominent location (e. g. the official website, the application download page, etc.).
Test Criteria	If the mobile application has already been released, then inspect whether the mobile application shall prompt the user to install protection software on the mobile device in a prominent location (e. g. the official website, the application download page, etc.). If the mobile application is not released yet, then inspect whether "the declaration which prompts the installation of protection software and the expected location of the given declaration (Neither of them are not required if the mobile application has already been released)" are specified in the Questionnaire; in addition, the mobile application shall also specified its expected location for the prompt message and the expected contents of the prompt message. If "yes", then the application passes the given test item; if "no", the application fails to meet the criteria of the given test item.

Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application will not be publicly released; therefore, inspection on the test item is not required.
Notes	N/A

4.1.1.2. Mobile Application Updates

All the test items regarding “Mobile Application Updates” are test items for reference, which only are for reference for the developers.

4.1.1.2.1. The updates of the mobile application shall be released in an application store of a trusted source.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.1.2.2. The mobile application shall provide an update mechanism.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.1.2.3. The mobile application shall make announcements actively when there are security updates.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.1.3. Mobile Application Security Issue Reporting

For the test items regarding “Mobile Application Security Issue Reporting”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L2, L3 mobile applications must pass the requirements of “4.1.1.3.1. Mobile application developers shall provide a channel for reporting security issues”.

4.1.1.3.1. Mobile application developers shall provide a channel for reporting security issues.

TEST ITEM	4.1.1.3.1
Test Description	Mobile application problem reporting.
Test Category	L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.1.3. Mobile Application Security Issue Reporting
Technical Requirements	Mobile application developers shall provide a channel for reporting security issues.
Test Criteria	If the mobile application has already been released, then inspect whether the mobile application provides contact page, message board, email address, telephone number, or other types of contact methods in the application store or within the mobile application; also, the provided contact methods must be tested, in which the contact can actually be established successfully. If the mobile application is not released yet, then inspect whether there are expected channels and contact methods for security issue

	reporting specified in the Questionnaire; also, the provided channels/contact methods must be tested, in which the contact can actually be established successfully. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application will not be publicly released; therefore, inspection on the test item is not required.
Notes	N/A

4.1.1.3.2. Mobile application developers shall respond to questions and make relevant improvements within an appropriate period.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.2. Sensitive Data Protection

This aspect is mainly applicable to relevant information security testing standards regarding sensitive data and personal data protection, including the collection, utilization, storage, transmission, sharing, and deletion, etc., of sensitive data.

4.1.2.1. Sensitive Data Collection

For the test items regarding “Sensitive Data Collection”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, and L3 mobile applications must pass the requirements of “4.1.2.1.1. The mobile application shall obtain user consent before collecting sensitive data” and “4.1.2.1.2. The mobile application shall provide users with the right to refuse the collection of sensitive data”.

4.1.2.1.1. The mobile application shall obtain user consent before collecting sensitive data

TEST ITEM	4.1.2.1.1
Test Description	The declaration regarding the collection of sensitive data by the mobile application.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.1. Sensitive Data Collection, MSTG-STORAGE-12, MSTG-PLATFORM-1
Technical Requirements	The mobile application shall obtain user consent before collecting sensitive data.
Test Criteria	If the mobile application has already been released, then inspect whether all the sensitive data collected by the mobile application are those declared in application store or those declared within the mobile application of which user consent is obtained. If the mobile application is not released yet, then inspect whether the "needed types of sensitive data in mobile devices (resources, permissions), their description of use, whether these sensitive data are stored in the device, whether are these sensitive data shared with other applications", and whether the elucidation regarding how to obtain user consent (or regarding the declaration in the mobile application and how to obtain user consent) are specified in the Questionnaire. If "yes", then the application passes the given test item; if "no", the application fails to meet the criteria of the given test item.

Test Result	Passed – The mobile application meets the criteria of the test item; or that the mobile application does not collect sensitive data. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application will not be publicly released; therefore, inspection on the test item is not required.
Notes	The declaration on the application store primarily refers to that of the store interface of the mobile device.

4.1.2.1.2. The mobile application shall provide users with the right to refuse the collection of sensitive data

TEST ITEM	4.1.2.1.2
Test Description	The mobile application provides users with the mechanism for refusing the collection of sensitive data
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.1. Sensitive Data Collection, MSTG-STORAGE-12
Technical Requirements	The mobile application shall provide users with the right to refuse the collection of sensitive data.
Test Criteria	(1) Inspect whether the mobile application provides users with the function to refuse the collection of sensitive data. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the collection of sensitive data by the mobile application is not detected given the scenario that the user refuses the collection of sensitive data. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the collection of sensitive data by the mobile application is not detected. Failed – The mobile application fails to meet all of the criteria of the test item; or that the test result of the test item 4.1.2.1.1 shows that the mobile application fails to declare all the sensitive data it collects.

	Non-Applicable – The mobile application will not be publicly released; therefore, inspection on the test item is not required.
Notes	If the test result of the test item 4.1.2.1.1 shows that the mobile application fails to declare all the sensitive data it collects, users will be unable to exercise the right to refuse the collection of sensitive data on the sensitive data which were not declared.

4.1.2.2. Sensitive Data Utilization

For the test items regarding “Sensitive Data Utilization”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the F-type mobile applications must pass the requirements of “4.1.2.2.3. If the mobile application uses password authentication, it shall actively prompt the user to set a more complex password.”, “4.1.2.2.4. The mobile application shall remind users to change their passwords regularly”

4.1.2.2.1. The mobile application shall obtain user consent before using sensitive data

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.2.2.2. The mobile application shall provide users with the right to refuse the use of sensitive data.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.2.2.3. If the mobile application uses password authentication, it shall actively prompt the user to set a more complex password.

TEST ITEM	4.1.2.2.3
Test Description	Password authentication mechanism of the mobile application
Test Category	F
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.2. Using Sensitive Data, MSTG-STORAGE-11, MSTG-AUTH-5
Technical Requirements	If the mobile application uses password authentication, it shall actively prompt the user to set a more complex password.
Test Criteria	(1) Inspect whether the mobile application reminds the user that the password(s) shall be at least 6 characters long on the password setting page. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the mobile application reminds the user to avoid using personal data as password(s) on the password setting page. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item. Failed – The mobile application fails to meet all of the criteria of the test item. Non-Applicable – The mobile application does not apply any password mechanisms.
Notes	(1) Examples of personal data: ID card number, account name, first name, last name, email address, date of birth, etc. (2) According to NIST SP800, the suggested length for passwords

	should be 8 or more characters.

4.1.2.2.4. The mobile application shall remind users to change their passwords regularly.

TEST ITEM	4.1.2.2.4
Test Description	Password authentication mechanism of the mobile application
Test Category	F
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.2. Sensitive Data Utilization
Technical Requirements	The mobile application shall remind the users to change their passwords regularly.
Test Criteria	Inspect whether the mobile application reminds the user to change his/her passwords regularly (up to a maximum interval of 90 days). If “yes”, then the application passes the given test item; if “no”, the application fails to meet the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application does not apply any password mechanisms.
Notes	N/A

4.1.2.3. Sensitive Data Storage

For the test items regarding “Sensitive Data Storage”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the mobile applications of the respective types must pass the requirements listed below: the L1 and L2 mobile applications must pass the requirements of “4.1.2.3.4. The mobile application shall avoid storing sensitive data in redundant files or log files after closure and/or log-out.”; the L1, L2 and L3 mobile applications must pass the requirements of “4.1.2.3.1. The mobile application shall obtain user consent before storing sensitive data.”, “4.1.2.3.2. The mobile application shall provide users with the right to refuse the storage of sensitive data”, “4.1.2.3.6. Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.”, “4.1.2.3.7. In order to prevent unauthorized access by other applications, sensitive data shall be stored in the areas protected by the OS.”, “4.1.2.3.8. Sensitive data shall be avoided in the code of the mobile application.”, “4.1.2.3.10. The mobile application shall use system credential storage facilities appropriately to store sensitive data.”, “4.1.2.3.12. The mobile application shall avoid the leakage of sensitive data in the IPC mechanism”; the L2 and L3 mobile applications must pass the requirements of “4.1.2.3.11. The mobile application shall disable the keyboard cache mechanism when the user is entering sensitive data.”, “4.1.2.3.13. The user interface in the mobile application shall avoid the leakage of sensitive data.”; the L3 mobile applications must pass the requirements of “4.1.2.3.5. The mobile application shall avoid storing sensitive data in redundant files or log files”, “4.1.2.3.9. The mobile application shall actively alert the user when non-user-initiated screenshots are taken.”, and “4.1.2.3.14. The sensitive data of the mobile application shall not be stored in the backup data of the mobile device operating system.”

4.1.2.3.1. The mobile application shall obtain user consent before storing sensitive data

TEST ITEM	4.1.2.3.1
Test Description	The declaration of the mobile application regarding the storage of sensitive data.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-12, MSTG-PLATFORM-1
Technical Requirements	The mobile application shall obtain user consent before storing sensitive data
Test Criteria	If the mobile application has already been released, then inspect whether all the sensitive data stored by the mobile application are those declared in application store or those declared within the mobile application of which user consent is obtained. If the mobile application is not released yet, then inspect whether the "needed types of sensitive data in mobile devices (resources, permissions), their description of use, whether these sensitive data are stored in the device, whether are these sensitive data shared with other applications", and whether the elucidation regarding how to obtain user consent (or regarding the declaration in the mobile application and how to obtain user consent) are specified in the Questionnaire. If "yes", then the application passes the given test item; if "no", the application fails to meet the criteria of the given test item.

Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application will not be publicly released; therefore, inspection on the test item is not required.
Notes	The declaration on the application store primarily refers to that of the store interface of the mobile device.

4.1.2.3.2. The mobile application shall provide users with the right to refuse the storage of sensitive data

TEST ITEM	4.1.2.3.2
Test Description	The mobile application provides users with the mechanism to refuse the storage of sensitive data.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-12
Technical Requirements	The mobile application shall provide users with the right to refuse the storage of sensitive data.
Test Criteria	(1) Inspect whether the mobile application provides users with the function to refuse the storage of sensitive data. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the storage of sensitive data by the mobile application is not detected given the scenario that the user refuses the storage of sensitive data. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the mobile application does not store sensitive data. Failed – The mobile application fails to meet all of the criteria of the test item; or that the test result of the test item 4.1.2.3.1 shows that the mobile application fails to declare all the sensitive data it stores.

	Non-Applicable – The mobile application will not be publicly released; therefore, inspection on the test item is not required.
Notes	If the test result of the test item 4.1.2.3.1 shows that the mobile application fails to declare all the sensitive data it stores, users will be unable to exercise the right to refuse the storage of sensitive data on the sensitive data which were not declared.

4.1.2.3.3. The sensitive data stored by the mobile application shall only be used for the purpose(s) stated in its declaration of use.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.2.3.4. The mobile application shall avoid storing sensitive data in redundant files or log files after closure and/or log-out.

TEST ITEM	4.1.2.3.4
Test Description	Limitations regarding the storage of sensitive data of the mobile application
Test Category	L1, L2
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-3, MSTG-STORAGE-10, MSTG-PLATFORM-1
Technical Requirements	The mobile application shall avoid storing sensitive data in redundant files or log files after closure and/or log-out.
Test Criteria	(1) Inspect whether the storage of sensitive data in redundant files by the mobile application after closure and/or logout is not detected. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
	(2) Inspect whether the storage of sensitive data in log files by the mobile application after closure and/or logout is not detected. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the storage of sensitive data by the mobile application is not detected. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	The storage of sensitive data shall not be detected in the areas protected by the OS, either.

4.1.2.3.5. The mobile application shall avoid storing sensitive data in redundant files or log files.

TEST ITEM	4.1.2.3.5
Test Description	Limitations regarding the storage of sensitive data of the mobile application.
Test Category	L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-3, MSTG-STORAGE-13
Technical Requirements	The mobile application shall avoid storing sensitive data in redundant files or log files.
Test Criteria	(1) Inspect whether the storage of sensitive data in redundant files by the mobile application is not detected. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
	(2) Inspect whether the storage of sensitive data in log files by the mobile application is not detected. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
	(3) Inspect whether the mobile application stores sensitive data in redundant files or log files and uses encryption function(s) which are listed as secure encryption functions in FIPS 140-2 Annex A for protection. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets criterion (1) and criterion (2); or that the mobile application meets the criterion (3). Failed – The mobile application fails to meet both criterion (1) and criterion (2), and does not meet criterion (3), either.

Notes	The storage of sensitive data shall not be detected in the areas protected by the OS, either.

4.1.2.3.6. Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.

TEST ITEM	4.1.2.3.6
Test Description	Protection regarding sensitive data storage of the mobile application
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-14, MSTG-CRYPTO
Technical Requirements	Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.
Test Criteria	(1) Inspect whether the sensitive data within non-redundant files and non-log files of the mobile application are encrypted with AES or Triple DES in which the effective key length is longer than 128-bit (or above). If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the key of the encryption function(s) used by the mobile application conforms to or refers to at least one the secure random number generator functions listed in ANSI X9.17, FIPS 140-2, NIST SP 800-22, SP 800-90A (CAVP Testing: Random Number Generators). If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test

	item; or that the mobile application does not store sensitive data. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	The storage of sensitive data shall not be detected in the areas protected by the OS, either.

4.1.2.3.7. In order to prevent unauthorized access by other applications, sensitive data shall be stored in the areas protected by the OS.

TEST ITEM	4.1.2.3.7
Test Description	Management regarding sensitive data storage of the mobile application
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-2
Technical Requirements	In order to prevent unauthorized access by other applications, sensitive data shall be stored in the areas protected by the OS.
Test Criteria	Inspect whether the mobile application stores sensitive data in the area(s) which other applications cannot access by default. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the storage of sensitive data by the mobile application is not detected. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – If the storage of sensitive data by the application only failed in the test result of the test item 4.1.2.3.4, then inspection on the given item is not required.
Notes	As the condition for passing the test item 4.1.2.3.4 is that the storage of sensitive data “shall not be detected”, therefore, there will be no issues regarding the storage of sensitive data in the area(s) which

	other mobile application cannot access by default.

4.1.2.3.8. Sensitive data shall be avoided in the code of the mobile application.

TEST ITEM	4.1.2.3.8
Test Description	Hard-coded sensitive data in mobile applications
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-CRYPTO-1
Technical Requirements	Sensitive data shall be avoided in the code of the mobile application.
Test Criteria	Inspect whether password(s), identification information, or key(s) for encryption/decryption of symmetric-key algorithm(s) are not detected in the code of the mobile application and other files within the installation files of the mobile application. If “no”, then the application passes the given test item; if “yes”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	Please refer to the hard-coded vulnerability types disclosed by the CWE (e. g. CWE-259, CWE-321, CWE-798)

4.1.2.3.9. The mobile application shall actively alert the user when non-user-initiated screenshots are taken.

TEST ITEM	4.1.2.3.9
Test Description	Screenshot alert of the mobile application.
Test Category	L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-12
Technical Requirements	The mobile application shall actively alert the user when non-user-initiated screenshots are taken.
Test Criteria	Inspect whether the mobile application alerts the user when non-user-initiated screenshots are taken. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application is an application for the iOS.
Notes	N/A

4.1.2.3.10. The mobile application shall use system credential storage facilities appropriately to store sensitive data.

TEST ITEM	4.1.2.3.10
Test Description	The mobile application shall use system credential storage facilities appropriately to store sensitive data.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-1, MSTG-STORAGE-14
Technical Requirements	The mobile application shall store sensitive data (e. g. personally identifiable information, user credentials, encryption keys, etc.) in system credential storage facilities.
Test Criteria	Inspect whether the mobile application stores the sensitive data which can be stored in system credential storage facilities in those facilities. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the storage of sensitive data by the mobile application is not detected. Failed – The mobile application fails to meet the criteria of the test item.
Notes	The “system credential storage facilities” may have different limitations regarding the data they can store depending on the system. Therefore, the inspection on whether sensitive data are properly stored shall be based on the respective designs of the

	systems.

4.1.2.3.11. The mobile application shall disable the keyboard cache mechanism when the user is entering sensitive data.

TEST ITEM	4.1.2.3.11
Test Description	The mobile application shall disable the keyboard cache mechanism when the user is entering sensitive data.
Test Category	L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-5, MSTG-PLATFORM-11
Technical Requirements	The mobile application shall disable the keyboard cache mechanism when the user is entering sensitive data.
Test Criteria	Inspect whether the mobile application disables the keyboard cache mechanism on the fields in which sensitive data will be inputted. (1) Inspect whether the mobile application does not automatically correct and does not include possible strings when the user enters sensitive data. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion. (2) Inspect whether the mobile application does not store sensitive data in the keyboard cache file(s). If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the collection of sensitive data by the mobile

	application is not detected. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	N/A

4.1.2.3.12. The mobile application shall avoid the leakage of sensitive data in the IPC mechanism.

TEST ITEM	4.1.2.3.12
Test Description	The mobile application shall avoid the leakage of sensitive data in the IPC mechanism.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-6, MSTG-PLATFORM-3, MSTG-PLATFORM-4
Technical Requirements	The mobile application shall avoid the leakage of sensitive data in the IPC mechanism.
Test Criteria	Inspect whether the mobile application does not leak any sensitive data to non-specific sources in the IPC mechanism. If “no”, then the application passes the given test item; if “yes”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the collection of sensitive data by the mobile application is not detected. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application does not use IPC mechanism.
Notes	IPC is the abbreviation for “Inter-Process Communication”, which is a communication mechanism for the processes in the user space.

4.1.2.3.13. The user interface in the mobile application shall avoid the leakage of sensitive data.

TEST ITEM	4.1.2.3.13
Test Description	The user interface in the mobile application shall avoid the leakage of sensitive data.
Test Category	L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-7, MSTG-STORAGE-9
Technical Requirements	The user interface in the mobile application shall avoid the leakage of sensitive data.
Test Criteria	Inspect whether the mobile application will perform protection to sensitive data when it is running, in which the sensitive data displayed on the user interface (including at least password(s) and credit card number) shall be masked. Should there be sensitive data items which are not masked, the reason(s) shall be stated. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	N/A

4.1.2.3.14. The sensitive data of the mobile application shall not be stored in the backup data of the mobile device operating system.

TEST ITEM	4.1.2.3.14
Test Description	The sensitive data of the mobile application shall not be stored in the backup data of the mobile device operating system.
Test Category	L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage, MSTG-STORAGE-8
Technical Requirements	The sensitive data of the mobile application shall not be stored in the backup data of the mobile device operating system.
Test Criteria	Inspect whether the system backup files of the mobile device contains the sensitive data of the mobile application. If “no”, then the application passes the given test item; if “yes”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the mobile application does not collect sensitive data. Failed – The mobile application fails to meet the criteria of the test item.
Notes	System backup refers to the backup function provided by the mobile operating system in the mobile device; the backup files, inside and outside the mobile device, shall not contain the sensitive data of the mobile application.

4.1.2.4. Sensitive Data Transmission

For the test items regarding “Sensitive Data Transmission”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, and L3 mobile applications must pass the requirements of “4.1.2.4.1. The mobile application shall apply appropriate and effective key length and encryption algorithm(s) for secure encryption when transmitting sensitive data via network.”

4.1.2.4.1. The mobile application shall apply appropriate and effective key length and encryption algorithm(s) for secure encryption when transmitting sensitive data via network.

TEST ITEM	4.1.2.4.1
Test Description	Sensitive data transmission by the mobile application.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.4. Sensitive Data Transmission, MSTG-STORAGE-4, MSTG-NETWORK-1, MSTG-NETWORK-2
Technical Requirements	The mobile application shall apply appropriate and effective key length and encryption algorithm(s) for secure encryption when transmitting sensitive data via network.
Test Criteria	(1) Inspect whether the mobile application applies TLS 1.2 (or above) encryption protocol in sensitive data transmission. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the mobile application applies the RSA encryption with an effective key length of 2048 bits (or above) or the Elliptic

	Curve Cryptography with an effective key length of 224 bits (or above). If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(3) Inspect whether the mobile application applies Advanced Encryption Standard (AES) with an effective key length of 128 bits (or above) or Triple Data Encryption Algorithm (Triple DES). If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the mobile application does not transmit sensitive data. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	N/A

4.1.2.5. Sensitive Data Sharing

For the test items regarding “Sensitive Data Sharing”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, and L3 mobile applications must pass the requirements of “4.1.2.5.1. User consent shall be obtained before the sensitive data are shared among different mobile applications in the mobile device.”, “4.1.2.5.2. The mobile application shall provide users with the right to refuse sensitive data sharing.” and “4.1.2.5.3. Accesses from unauthorized mobile applications shall be avoided when the mobile application is sharing sensitive data.”

4.1.2.5.1. User consent shall be obtained before the sensitive data are shared among different mobile applications in the mobile device.

TEST ITEM	4.1.2.5.1
Test Description	The declaration of the mobile application regarding sharing sensitive data.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.5. Sensitive Data Sharing, MSTG-STORAGE-12
Technical Requirements	User consent shall be obtained before the sensitive data are shared among different mobile applications in the mobile device.
Test Criteria	If the mobile application has already been released, then inspect whether the mobile application makes declaration in the application store (or makes declaration within the mobile application and obtains user consent) before it shares sensitive data among different mobile applications in the mobile device. If the mobile application is not released yet, then inspect whether "the expected contents of the sensitive data to be shared by the mobile application, their description of use, the methods of obtaining user consent, the applications to which sensitive data would be shared (the above-mentioned information does not need to be specified if the mobile application has already been released)" and whether the elucidation regarding how to obtain user consent (or regarding the declaration in the mobile application and how to obtain user consent) are specified in the Questionnaire. If "yes", then the application passes the given test item; if "no", the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the mobile application does not share sensitive data.

	Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – The mobile application will not be publicly released and that the mobile application does not share sensitive data; therefore, inspection on the test item is not required.
Notes	N/A

4.1.2.5.2. The mobile application shall provide users with the right to refuse sensitive data sharing.

TEST ITEM	4.1.2.5.2
Test Description	The mobile application provides users with the mechanism for refusing sensitive data sharing.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.5. Sensitive Data Sharing, MSTG-STORAGE-12
Technical Requirements	The mobile application shall provide users with the right to refuse sensitive data sharing.
Test Criteria	(1) Inspect whether the mobile application provides users with the function to refuse sensitive data sharing. If “yes”, then the application passes the given test criterion; if “not”, the application fails to meet the given test criterion.
	(2) Inspect whether the mobile application does not share sensitive data given the scenario that the user refuses sensitive data sharing. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the mobile application does not share sensitive data. Failed – The mobile application fails to meet all of the criteria of the test item. Non-Applicable – The mobile application will not be publicly released and that the function in question is not provided in the mobile application; therefore, inspection on the test item is not

	required.
Notes	N/A

4.1.2.5.3. Accesses from unauthorized mobile applications shall be avoided when the mobile application is sharing sensitive data.

TEST ITEM	4.1.2.5.3
Test Description	Management regarding the permissions of sensitive data sharing of the mobile application.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.2.5. Sensitive Data Sharing, MSTG-STORAGE-4, MSTG-PLATFORM-3, MSTG-PLATFORM-4
Technical Requirements	Accesses from unauthorized mobile applications shall be avoided when the mobile application is sharing sensitive data.
Test Criteria	Inspect whether the accesses to sensitive data are limited to specific mobile applications by the mobile application sharing sensitive data. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the mobile application does not share sensitive data. Failed – The mobile application fails to meet the criteria of the test item.
Notes	N/A

4.1.2.6. Deletion of Sensitive Data

The test items regarding “Deletion of Sensitive Data” are all categorized as test items for reference, which are only for reference for developers.

4.1.2.6.1. The mobile application shall provide users with the function of deletion if the mobile application involves the storage of users’ sensitive data. This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.3. Security regarding Transaction Resource Management

This aspect is mainly applicable to relevant information security testing standards regarding transaction resource management, including the use and the management of transaction resources, etc.

4.1.3.1. Using Transaction Resource

For the test items regarding “Using Transaction Resource”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L3 mobile applications must pass the requirements of “4.1.3.1.1. The mobile application shall actively notify users when using transaction resources.” and “4.1.3.1.2. The mobile application shall provide users with the right to refuse the use of transaction resources.”

4.1.3.1.1. The mobile application shall actively notify users when using transaction resources.

TEST ITEM	4.1.3.1.1
Test Description	The declaration of the mobile application regarding the use of transaction resources.
Test Category	L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.3.1. Using Transaction Resource, MSTG-STORAGE-12
Technical Requirements	The mobile application shall actively notify users when using transaction resources.
Test Criteria	Inspect whether the mobile application actively notify the user in the mobile application when performing transaction, in which the information of notification shall at least include the name of the

	transaction resource, the amount and the transaction method. If "yes", then the application passes the given test item; if "no", the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	The mobile application shall actively notify the user "before the transaction by the mobile application" – i. e. in the given test item, whether the mobile application actively notify the user before the transaction.

4.1.3.1.2. The mobile application shall provide users with the right to refuse the use of transaction resources.

TEST ITEM	4.1.3.1.2
Test Description	The mechanism of the mobile application for refusing the use of transaction resources
Test Category	L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.3.1. Using Transaction Resource, MSTG-STORAGE-12
Technical Requirements	The mobile application shall provide users with the right to refuse the use of transaction resources.
Test Criteria	(1) Inspect whether the mobile application provides users with the function to refuse transaction in the mobile application when performing transaction. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the transaction is not performed by the mobile application given the scenario that the user refuses the transaction. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	N/A

4.1.3.2. Transaction Resource Management

For the test items regarding “Transaction Resource Management”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L3 mobile applications must pass the requirements of “4.1.3.2.1. The mobile application shall perform user authentication when using transaction resources.” and “4.1.3.2.2. The mobile application shall record the used transaction resources and the time of use.”

4.1.3.2.1. The mobile application shall perform user authentication when using transaction resources.

TEST ITEM	4.1.3.2.1
Test Description	User authentication by the mobile application regarding transaction resources
Test Category	L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.3.2. Transaction Resource Management, MSTG-AUTH-7, MSTG-AUTH-10, MSTG-NETWORK-5
Technical Requirements	The mobile application shall perform user authentication when using transaction resources.
Test Criteria	Inspect whether the mobile application provides a valid authentication mechanism before performing transaction. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test

	item.
Notes	Aside from the first transaction, which requires authentication, if it is within the same connection (session), the second and subsequent transactions do not require authentication. If the connection (session) changes, re-authentication must be performed.

4.1.3.2.2. The mobile application shall record the used transaction resource(s) and the time of use.

TEST ITEM	4.1.3.2.2
Test Description	Records of mobile application regarding transaction resources
Test Category	L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.3.2. Transaction Resource Management
Technical Requirements	The mobile application shall record the used transaction resources and the time of use.
Test Criteria	Inspect whether the mobile application provides a channel for querying the transaction records of transaction resources after the transaction, in which the transaction records of transaction resources shall at least include records of transaction resource name, transaction time and transaction amount. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	The “transaction resources and transaction time” described in the «Basic Information Security Standard for Mobile Applications» are defined as “transaction records” in the given Standard – i. e. the examiners shall inspect whether the mobile application provides transaction records and the contents of the records.

4.1.4. Security regarding User Authentication, Authorization, and Connection Management in Mobile Applications

This aspect is mainly applicable to relevant information security testing standards regarding user authentication, authorization, and connection management in mobile applications, including user authentication, authorization, and connection management mechanisms, etc.

4.1.4.1. User Authentication and Authorization

For the test items regarding “User Authentication and Authorization”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L2 and L3 mobile applications must pass the requirements of “4.1.4.1.1. The mobile application shall have an appropriate authentication mechanism in order to confirm the user's identity.” and “4.1.4.1.2. The mobile application shall authorize based on user identity.”

4.1.4.1.1. The mobile application shall have an appropriate authentication mechanism in order to confirm the user's identity.

TEST ITEM	4.1.4.1.1
Test Description	The mechanism of the mobile application for user authentication.
Test Category	L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.4.1. User Authentication and Authorization, MSTG-AUTH-1, MSTG-AUTH-8, MSTG-AUTH-9, MSTG-NETWORK-5
Technical Requirements	The mobile application shall have an appropriate authentication mechanism in order to confirm the user's identity.
Test Criteria	If the mobile application will access sensitive data related to personal data, then inspect whether the mobile application provides an authentication mechanism. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the mobile application does not access sensitive data related to personal data. Failed – The mobile application fails to meet the criteria of the test item. Non-Applicable – if it is within the scenarios exempt from authentication and authorization with the consent of the competent authority, then the inspection on the given test item is not required.
Notes	N/A

4.1.4.1.2. The mobile application shall authorize based on user identity.

TEST ITEM	4.1.4.1.2
Test Description	Authorization to the mobile application based on user identity
Test Category	L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.4.1. User Authentication and Authorization, MSTG-AUTH-1
Technical Requirements	The mobile application shall authorize based on user identity.
Test Criteria	If the mobile application will access sensitive data related to personal data, then inspect whether the mobile application provides an identity authorization mechanism. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item; or that the mobile application does not access sensitive data related to personal data. Failed – The mobile application fails to meet of the criteria of the test item. Non-Applicable – if it is within the scenarios exempt from authentication and authorization with the consent of the competent authority, then the inspection on the given test item is not required.
Notes	N/A

4.1.4.2. Mechanism regarding Connection Management

For the test items regarding “Mechanism regarding Connection Management”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, L3 mobile applications must pass the requirements of “4.1.4.2.2. The mobile application shall verify the validity of the server certificate.”, “4.1.4.2.3. The mobile application shall confirm that the server certificate is issued by a trusted certificate authority.”, and the L2, L3 mobile applications must pass the requirements of “4.1.4.2.1. The mobile application shall avoid using session IDs with regularity.”

4.1.4.2.1. The mobile application shall avoid using session IDs with regularity.

TEST ITEM	4.1.4.2.1
Test Description	Regularity of Session IDs applied by the mobile application
Test Category	L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.4.2. Mechanism regarding Connection Management, MSTG-AUTH-1, MSTG-AUTH-2, MSTG-AUTH-4, MSTG-AUTH-7
Technical Requirements	The mobile application shall avoid using session IDs with regularity.
Test Criteria	(1) Inspect whether the mobile application use Session IDs with a length of 128 bits (or above). If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the Session IDs used by the mobile application are not directly related to time, data submitted by the user, numbers/strings with regularity, or are difficult to forge. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(3) Inspect whether the Session IDs used by the mobile application have a log-out invalidation mechanism. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the mobile application does not use session IDs. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	The session IDs described in the given test item are those used after user authentication.

4.1.4.2.2. The mobile application shall verify the validity of the server certificate.

TEST ITEM	4.1.4.2.2
Test Description	Validity of server certificate applied by the mobile application
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.4.2. Mechanism regarding Connection Management, MSTG-NETWORK-3, MSTG-NETWORK-4
Technical Requirements	The mobile application shall verify the validity of the server certificate.
Test Criteria	(1) Inspect whether server certificate used by the mobile application is still within the validity period and is not revoked, and the principal name and the principal alias of the certificate includes the connected server's domain name. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(2) Inspect whether the mobile application authenticates via certificate pinning to ensure that the connected server is the one designated by the mobile application developer. If the website to which the user connects cannot be expected, then the mobile application shall notify the user that there are changes regarding the connection target and shall have a design which notifies the user that it will connect to another website. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.

Test Result	Passed – The mobile application meets all the criteria of the test item; or that the mobile application does not use secure encrypted transmission protocol(s) due to the fact that the mobile application does not transmit sensitive data. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	N/A

4.1.4.2.3. The mobile application shall confirm that the server certificate is issued by a trusted certificate authority.

TEST ITEM	4.1.4.2.3
Test Description	Issuing source(s) of the server certificate used by the mobile application.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.4.2. Mechanism regarding Connection Management, MSTG-NETWORK-3
Technical Requirements	The mobile application shall confirm that the server certificate is issued by a trusted certificate authority.
Test Criteria	Inspect whether the mobile application verifies and ensures that the server certificate is issued by a trusted certificate authority built-in in the mobile operating system. If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	A trusted certificate authority built-in in the mobile operating system is a trusted certificate issuing agency which is installed by the mobile operating system vendor. If the mobile application is only used for closed intranet connections, then the certificate issued by the enterprise itself can also be regarded as a trusted certificate.

4.1.5. Code Security of Mobile Applications

This aspect is mainly applicable to relevant information security testing standards regarding mobile application development, including prevention from malicious code, avoidance of information security vulnerabilities, mobile application integrity, security regarding the reference of library, user input verification, etc.; this aspect also takes reference from the requirements of OWASP MASVS V7.

4.1.5.1. Prevention from Malicious Code and Avoidance of Information Security Vulnerabilities

For the test items regarding “Prevention from Malicious Code and Avoidance of Information Security Vulnerabilities”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2 and L3 mobile applications must pass the requirements of “4.1.5.1.1. The mobile application shall avoid containing malicious code.”, and “4.1.5.1.2. The mobile application shall avoid information security vulnerabilities.”

4.1.5.1.1. The mobile application shall avoid containing malicious code.

TEST ITEM	4.1.5.1.1
Test Description	Malicious code of the mobile application
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.1. Prevention from Malicious Code and Avoidance of Information Security Vulnerabilities, MSTG-ARCH-10, MSTG-CODE-6, MSTG-CODE-7
Technical Requirements	The mobile application shall avoid containing malicious code.

Test Criteria	(1) Inspect whether the mobile application attempts to perform behaviors, e.g. querying, adding, modifying, deleting, accessing remote service(s), privilege escalation, etc., to files of other mobile application(s) or of the mobile operating system without authorization. If “no”, then the application passes the given test item; if “yes”, the application fails to meet the criteria of the given test item.
	(2) Inspect whether the mobile application does not contain any behaviors which will cause the mobile operating system to have unexpected errors, significant resource consumption, reboots or shutdowns, etc. If “no”, then the application passes the given test item; if “yes”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the mobile application does not store sensitive data. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	N/A

4.1.5.1.2. The mobile application shall avoid information security vulnerabilities.

TEST ITEM	4.1.5.1.2
Test Description	Information security vulnerabilities of the mobile application.
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.1. Prevention from Malicious Code and Avoidance of Information Security Vulnerabilities, MSTG-CODE-5, MSTG-PLATFORM-8
Technical Requirements	The mobile application shall avoid information security vulnerabilities.
Test Criteria	Inspect whether the mobile application does not contain any known security vulnerabilities. If “no”, then the application passes the given test item; if “yes”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	The known security vulnerabilities which cause the non-conformity to the test item are those with a CVE number and a CVSS v3.0 score greater than or equal to 7 (which have a severity level of High or Critical).

4.1.5.2. Mobile Application Integrity

The test items regarding “Mobile Application Integrity” are all categorized as test items for reference, which are only for reference for developers.

4.1.5.2.1. The mobile application shall use appropriate and effective integrity verification mechanisms to ensure its integrity.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.5.3. Security Regarding the Reference of Library

For the test items regarding “Security Regarding the Reference of Library”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, and L3 mobile applications must pass the requirements of “4.1.5.3.1. When the library referred by the mobile application is updated, the corresponding updated version shall be prepared. Regarding the update method, please consult subsection: 4.1.1. Security regarding Mobile Application Release.”

4.1.5.3.1. When the library referred by the mobile application is updated, the corresponding updated version shall be prepared. Regarding the update method, please consult subsection: 4.1.1. Security regarding Mobile Application Release.

TEST ITEM	4.1.5.3.1
Test Description	Security regarding the reference of library
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.3. Security Regarding the Reference of Library, MSTG-NETWORK-6, MSTG-CODE-5
Technical Requirements	When the library referred by the mobile application is updated, the corresponding updated version shall be prepared. Regarding the update method, please consult subsection: 4.1.1. Security regarding Mobile Application Release.

Test Criteria	Inspect whether the libraries referred by the mobile application do not have any known security vulnerabilities. If “no”, then the application passes the given test item; if “yes”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	The known security vulnerabilities which cause the non-conformity to the test item are those with a CVE number and a CVSS v3.0 score greater than or equal to 7 (which have a severity level of High or Critical). The name of the referred library and its version information must be self-declared in the Questionnaire of Appendix III. Questionnaire on Basic Information Security Testing for Mobile Applications.

4.1.5.4. User Input Verification

For the test items regarding “User Input Verification”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, and L3 mobile applications must pass the requirements of “4.1.5.4.1. The mobile application shall perform security checks to the strings entered by the user at the input phase.”, “4.1.5.4.2. The mobile application shall provide protection mechanism(s) relevant to injection attacks.”

4.1.5.4.1. The mobile application shall perform security checks to the strings entered by the user at the input phase.

TEST ITEM	4.1.5.4.1
Test Description	User input inspection of the mobile application
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.4. User Input Verification, MSTG-PLATFORM-2
Technical Requirements	The mobile application shall perform security checks to the strings entered by the user at the input phase.
Test Criteria	(1) Inspect whether the mobile application verifies the types of the expected user input strings; if the field itself needs to accept special characters, it is also an expected input string type. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.

	(2) Inspect whether the mobile application verifies the length of the user input strings. If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that the mobile application does not provide string input interface. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	N/A

4.1.5.4.2. The mobile application shall provide protection mechanism(s) relevant to injection attacks.

TEST ITEM	4.1.5.4.2
Test Description	Protection mechanism(s) of the mobile application from injection attacks
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.4. User Input Verification, MSTG-ARCH-2, MSTG-PLATFORM-2
Technical Requirements	The mobile application shall provide protection mechanism(s) relevant to injection attacks.
Test Criteria	(1) Inspect whether the mobile application has the design which prevents users from entering SQL injection strings. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(2) Inspect whether the mobile application has the design which prevents users from entering JavaScript injection strings. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(3) Inspect whether the mobile application has the design which prevents users from entering command injection strings. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(4) Inspect whether the mobile application has the design which prevents users from entering local file inclusion strings. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(5) Inspect whether the mobile application has the design which

	prevents users from entering XML injection strings. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(6) Inspect whether the mobile application has the design which prevents users from entering format string injection strings. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(7) Inspect whether the mobile application has the design which prevents users from entering IPC (inter process communication) injection strings. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that mobile application does not provide any string input interface. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	Should there be any new injection attack methods in the future, they will also be included in the given Standard. An effective injection attack protection mechanism shall process the string(s) inputted by users on the server side based on the concept of defense in depth. Also, as the scope of inspection of the given Standard is the mobile application itself, therefore, the laboratory shall at least perform inspection on whether the mobile application has a preliminary design of protection from inputting injection attack strings.

4.1.5.5. Prevention from Dynamic Analysis and Tampering

This subsubsection of the given Standard provides advices regarding defense in depth for the mobile applications with functions related to "processing" or "accessing" sensitive data. The purpose of this subsubsection is to improve the resistance of the mobile applications to reverse engineering or specific attacks from users. The test items in this subsubsection are listed as the advanced additional test items for high-security applications; therefore, whether to perform tests with all the test items listed below will be dependent on the submitter's evaluation of the risks regarding unauthorized tampering and reverse engineering to the submitted mobile application. For the test items regarding “Prevention from Dynamic Analysis and Tampering”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the F-type mobile applications must pass the requirements of “4.1.5.5.1. The mobile application must detect whether the protection layer of the mobile operating system is cracked (e.g. rooted, jailbroken) or is not properly protected; if so, the mobile application shall actively notify the user or terminate itself.”, “4.1.5.5.5. Either that the executable files and the libraries belonging to the mobile application shall all be encrypted on the file level or that the important code and data segments inside the executable files shall all be encrypted or packed, making it difficult to acquire important code or data via trivial static analysis.”, and “4.1.5.5.6. The mobile application shall have code obfuscation mechanism(s).”

4.1.5.5.1. The mobile application must detect whether the protection layer of the mobile operating system is cracked (e.g. rooted, jailbroken) or is not properly protected; if so, the mobile application shall actively notify the user or terminate itself.

TEST ITEM	4.1.5.5.1
Test Description	The mobile application must detect whether the protection layer of the mobile operating system is cracked (e.g. rooted, jailbroken) or is not properly protected; if so, the mobile application shall actively notify the user or terminate itself.
Test Category	F
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering, MSTG-RESILIENCE-1, MSTG-STORAGE-11
Technical Requirements	The mobile application must detect whether the protection layer of the mobile operating system is cracked (e.g. rooted, jailbroken) or is not properly protected; if so, the mobile application shall actively notify the user or terminate itself.
Test Criteria	Inspect whether the mobile application can actively detect and alert the user or terminate the execution of the mobile application when the protection layer of the mobile operating system in the mobile device is not properly protected or is cracked (e.g. rooted, jailbroken), and whether the mobile application notifies the user to beware of the risks and restricts the conducting of wire transfers and trade instructions/orders to non-designated accounts (if the mobile application uses transaction resources). If “yes”, then the application passes the given test item; if “no”, the application fails to meet the criteria of the given test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.

Notes	(1) In the actual testing, the submitter can provide 2 variants of the mobile application: one is the mobile application without any protection mechanisms, another is the mobile application with all the protection mechanisms; also, in order to ensure the rights of both parties, the submitter shall specify the respective hash values of the two variants and provide affidavit regarding identical functionality. (2) Test laboratories can unilaterally claim that they are capable of bypassing the detection mechanism(s) of rooting/jailbreaking. (3) If the mobile application only provides warning messages, then a screenshot shall be taken to show that there are warning messages and the program can still operate normally.

4.1.5.5.2. The mobile application shall be able to actively detect whether all the files and data in the sandbox are tampered with.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.5.5.3. The mobile application shall detect whether there is any use of dynamic analysis tools or frameworks in the mobile device.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.5.5.4. The mobile application shall detect whether the code and data in the memory are tampered with.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.1.5.5.5. Either that the executable files and the libraries belonging to the mobile application shall all be encrypted on the file level or that the important code and data segments inside the executable files shall all be encrypted or packed, making it difficult to acquire important code or data via trivial static analysis.

TEST ITEM	4.1.5.5.5
Test Description	Either that the executable files and the libraries belonging to the mobile application shall all be encrypted on the file level or that the important code and data segments inside the executable files shall all be encrypted or packed, making it difficult to acquire important code or data via trivial static analysis.
Test Category	F
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering, MSTG-RESILIENCE-11
Technical Requirements	Either that the executable files and the libraries belonging to the mobile application shall all be encrypted on the file level or that the important code and data segments inside the executable files shall all be encrypted or packed, making it difficult to acquire important code or data via trivial static analysis.
Test Criteria	Inspect whether the executable files and the libraries of the mobile application on the file level are encrypted or whether the important code and data segments inside the executable files are encrypted or packed, in which either one will make it difficult to acquire important code or data via trivial static analysis. If “yes” in either one of the two, then the application passes the given test item; if “no” in both of the two, then the application fails to meet the criteria of the given

	test item.
Test Result	Passed – The mobile application meets the criteria of the test item. Failed – The mobile application fails to meet the criteria of the test item.
Notes	(1) In the actual testing, the submitter can provide 2 variants of the mobile application: one is the mobile application without any protection mechanisms, another is the mobile application with all the protection mechanisms; also, in order to ensure the rights of both parties, the submitter shall specify the respective hash values of the two variants and provide affidavit regarding identical functionality. (2) Test laboratories can unilaterally claim that they are capable of unpacking.

4.1.5.5.6. The mobile application shall have code obfuscation mechanism(s)

TEST ITEM	4.1.5.5.6
Test Description	The mobile application shall have code obfuscation mechanism(s)
Test Category	F
Test Standards	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering, MSTG-RESILIENCE-12
Technical Requirements	The mobile application shall have code obfuscation mechanism(s)
Test Criteria	(1) Inspect whether the mobile application has obfuscation mechanism(s). If “yes”, then the application passes the given test criterion; if “no”, the application fails to meet the given test criterion.
	(2) Inspect whether the code of the mobile application can be deobfuscated into the original code via manual inspection with existing deobfuscation methods or inspection with existing automated deobfuscation tools. If “no”, then the application passes the given test criterion; if “yes”, the application fails to meet the given test criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item. Failed – The mobile application fails to meet all of the criteria of the test item.
Notes	(1) In the actual testing, the submitter can provide 2 variants of the mobile application: one is the mobile application without any protection mechanisms, another is the mobile application with all the protection mechanisms; also, in order to ensure the rights of both parties, the submitter shall specify the respective hash values of the two variants and provide affidavit regarding identical functionality. (2) Test laboratories can unilaterally claim that they are capable of deobfuscation.

4.2. Basic Information Security Testing Standard for the Server-side

According to the description in Chapter 4 Section 2 of the «Basic Information Security Standard for Mobile Application», “The Standard aims to provide basic information security requirements regarding the security of mobile applications; therefore, if the server-side information security requirements are involved with the mobile application, it is recommended that the vendor shall provide self-declaration or an affidavit regarding its server-side information security protection and management measures, or that the vendor shall provide a certificate of compliance from a third-party inspection on the information security protection and management of its server-side service(s).” As the paragraph was expressed in the form of suggestion and thus was not mandatory, the subsubsection 4.2.2.1. WebView Security Inspection is subsequently formulated as a new inspection benchmark.

In the given section, benchmarks for basic information security inspection are stipulated for mobile application security regarding server-side basic information security testing. For details, please consult 4.2.2 Server-side Security Management.

4.2.1. Server-side Security Management

It is recommended that server-side security shall take the applications and services provided as the starting point in order to perform threat modeling analysis to applications and services as a whole; and, with the analysis above, identify the security risks to the services to implement necessary and effective subsequent control measures. If the server-side adopts schemes of rental IDCs/hosts (including virtual servers) or a cloud-based service plan, then it is recommended that service providers who had passed relevant information security management standards [e.g. ISO/IEC 27001, STAR (Security, Trust & Assurance Registry) of the Cloud Security Alliance (CSA), or ECSA (EuroCloud Star Audit)] be prioritized.

4.2.2. Server-side Security Inspection

The protection measures for the server-side security are easily overlooked by developers due to the fact that the access interface provided by the server side of

the mobile application platform for the mobile application is the mobile application itself, rather than the interface directly accessed by the user. The server side of the mobile application platform is essentially a website and a web service server; therefore, should there be no proper security design and development, there will be vulnerabilities of traditional web applications as well. As a result, for the security inspection on the server side, it is recommended that the developers can consider using penetration testing methods for inspection. The following documents are the current documents regarding penetration testing with international credibility and reference value:

- The OWASP Testing Guide of the OWASP (Open Web Application Security Project); for further information, please consult the following URL: https://www.owasp.org/index.php/Category:OWASP_Testing_Project
- The Open Source Security Testing Methodology Manual (OSSTMM) of the ISECOM (the Institute for Security and Open Methodologies); for further information, please consult the following URL: https://www.isecom.org/research.html
- The documents related to penetration test of the SANS (System Administration, Networking, and Security Institute); for further information, please consult the following URL: http://pen-testing.sans.org/

4.2.2.1. WebView Security Inspection

For the test items regarding “WebView Security Inspection”, the test results must be marked as “Passed” in order to meet the information security technical requirements of this subsubsection, or the mobile application fails to meet the information security technical requirements of this subsubsection, in which, the L1, L2, and L3 mobile applications must pass the requirements of “4.2.2.1.2. When the mobile application renders functions in the Webview, the connected domain shall be a secure domain.”

4.2.2.1.1. The mobile application shall use WebView to exchange web resources with remote servers.

This item is a suggested test item for reference. For further information, please consult Appendix V. Basic Information Security Test Items for Reference for Mobile Applications.

4.2.2.1.2. When the mobile application renders functions in the Webview, the connected domain shall be a secure domain.

TEST ITEM	4.2.2.1.2
Test Description	Webview Security Inspection of the mobile application
Test Category	L1, L2, L3
Test Standards	«Basic Information Security Standard for Mobile Application» 4.2.2.1 Webview Security Inspection, MSTG-ARCH-2, MSTG-NETWORK-4, MSTG-PLATFORM-5, MSTG-PLATFORM-6, MSTG-PLATFORM-7
Technical Requirements	When the mobile application renders functions in the Webview, the connected domain shall be a secure domain.
Test Criteria	(1) Inspect whether the connected domain is a secure domain and corresponds to the actual connected domain declared by the developer in the Questionnaire when the mobile application renders functions in the WebView. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(2) Inspect whether the mobile application uses HTTPS and conducts certificate pinning during connections when the mobile application renders functions in the WebView. If the website to which the user connects cannot be expected, then the mobile application shall notify the user that there are changes regarding the connection target and shall have a design which notifies the user that it will connect to another website. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test criterion.
	(3) Inspect whether the web server vulnerability scan passes all of the check items, in which cross-site scripting and injection flaws must be verified, when the mobile application renders functions in the WebView. If "yes", then the application passes the given test criterion; if "no", the application fails to meet the given test

	criterion.
Test Result	Passed – The mobile application meets all the criteria of the test item; or that when the mobile application renders functions in the WebView, it does not conduct connection; also, if sensitive data are not transmitted in connection, then certificate pinning and HTTPS connection are not required. Failed – The mobile application fails to meet all of the criteria of the test item. Non-Applicable – The mobile application does not render functions in the WebView.
Notes	For details regarding vulnerability scan, please consult Section (1) of the Chapter 6. Supplementary Instructions.

5. Inspection Methods

The testing of the given Standard is primarily performed without obtaining the source code. In practice, inspection on mobile applications of all categories can be performed with the assistance of automation tools. Inspection on some of the test items are supplemented by manual inspection with the source code obtained by reverse engineering – i.e. conduct manual analysis after performing scan with source code scanners. As the methodology for basic information security testing for mobile applications is primarily black-box testing, the testing methods mentioned in this chapter are of a general nature. The practice regarding details of testing methods, testing environment, etc., will be left for each laboratory to develop on their own. The following sections will provide description of each inspection method.

5.1. Automatic

The types of this inspection method primarily include:

- User-interface-oriented: Performing automated testing primarily on the user interface, including conducting user operation, screenshots and other functions automatically. User-interface-oriented tools can be utilized in constructing test cases in testing.
- Data-oriented: Data-oriented method can automatically identify the data fields or labels of the test subject, transmit or fill in different data, and determine potential security issues by tracking the data flow and the response results.

5.2. Manual

In this inspection method, static analysis and dynamic analysis can be applied at the same time in the process of inspection. Based on the actual needs of inspection, reverse engineering or man-in-the-middle attack methods can also be applied to perform the inspection.

5.2.1. Static Analysis

Static analysis obtains code via performing manual or tool-assisted reverse engineering to binary code. With the sensitive data and mobile device resources to be accessed (e.g. files within mobile applications – AndroidManifest.xml, iOS

Entitlements, WMAppManifest.xml, etc.), inspection on whether the permissions requested by the mobile application correspond to those listed in the "Appendix III. Questionnaire on Basic Information Security Testing for Mobile Applications" can be performed via static analysis. Other methods such as inspection on whether the library referred by the test subject has common weaknesses and/or vulnerabilities or whether the test subject has referred improper library (e.g. when a browser mobile application that referred a version of the library with a known vulnerability visits a malicious website, the malicious website may cause the leakage of sensitive data), inspection on whether sensitive data are encrypted with appropriate and effective key length and encryption algorithm(s) before being stored, inspection on whether there are identifiable sensitive data displayed in the code after reverse engineering, inspection on whether there are sensitive data stored in redundant files or log files, etc., can all be performed via static analysis as well in order to identify the existence of security vulnerabilities or issues.

5.2.2. Dynamic Analysis

In the execution phase of the test subject, dynamic analysis will introduce dynamic user input or data/parameter input and other application behaviors in order to analyze various behaviors or states of the test target in the execution phase. Dynamic analysis can be used in inspecting different behaviors of the test subject in the simulator, physical device, remote connection, network access status, data transmission, etc. Dynamic analysis can also be utilized in inspecting whether appropriate and effective key length and encryption algorithm(s) are used in secure encryption in the transmission and storage of sensitive data, e. g. checking whether there are identifiable sensitive data during the execution of program(s) by methods such as packet sniffing, inspecting system log, etc. Dynamic analysis can also be used in checking whether sensitive data are stored in the area(s) protected by the operating system, e. g. after the execution of program(s), inspect whether there are identifiable sensitive data in the SD cards or common access areas.

5.3. Code Analysis

The analysis method performed with the code acquired by reverse engineering. This analysis method can be performed with the results of manual scanning/analysis after scanning with source code scanning tool(s).

5.4. Binary Code Analysis

In addition to the inspection methods above, other inspection or analysis methods, e. g. binary code analysis, can also be used. Binary code can be divided into byte code and machine code. Depending on the types of binary code analysis, appropriate virtual machines and physical devices shall be applied for manual inspection or inspection with automation testing tools.

6. **Supplementary Instructions**

(1) For the test item 4.2.2.1.2, each laboratory must provide information regarding the web-server-side vulnerability scan and mark the test items corresponding to the vulnerability scan in the report, in which the vulnerability scan shall be performed by the laboratory itself or by third-party vendors entrusted by the laboratory. Should there be any revision of the server-side webpage information within the effective period of the certificate of compliance and the certification mark, the developer has the obligation to actively notify the laboratory to perform vulnerability scan again. When performing vulnerability scan, the laboratory shall organize all the occurrences of this problem and note them in a specific chapter in the test report.

Notes：

i. Should there be any changes on the web server side, in addition to re-performing vulnerability scan, inspection on the test items of the given Standard shall also be re-performed.
ii. Vulnerability scan report(s) of all the first-layer links shall be attached.
iii. Vulnerability scan shall be performed with the tools specified in the list provided by Mobile Application Security Alliance.

7. Test Results and Outputs

The output of test results shall include all the records and results of the testing process, and shall describe the test results of the test subject as “Passed/Failed” based on the criteria of all the test items listed in Section 4. Information Security Technical Requirements. The test results and the output shall include but not limited to:

- Test subject
- Declaration regarding the scope of inspection
- Inspection schedule
- Inspection method(s), environment, and tools
- Executive personnel of inspection and their respective responsible items
- Verdicts of “Passed/Failed” upon the test results of test items.
- The testing procedure record and supporting information; the test items of which the results show non-conformity shall be provided in the report

8. References

[1] *Basic Information Security Standard for Mobile Applications*, Industrial Development Bureau of Ministry of Economic Affairs, 20th April 2015.

[2] «*Personal Data Protection Act*», 30th December 2015.

[3] Vetting the Security of Mobile Applications, NIST Special Publication 800-163, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf, 2015

[4] Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800-115, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, 2008

[5] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-131a.pdf, 2011

[6] Cryptographic Algorithm Validation Program (CAVP), http://csrc.nist.gov/groups/STM/cavp/, NIST

[7] Cryptographic Module Validation Program (CMVP), http://csrc.nist.gov/groups/STM/cmvp/, NIST

[8] Technical Requirements for Security Capability of Smart Mobile Terminal, YD/T 2407-2013, 2013

[9] Test Methods for Security Capability of Smart Mobile Terminal, YD/T 2408-2013, 2013

[10] Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org/

[11] Common Weakness Enumeration (CWE), https://cwe.mitre.org/

[12] Device Administration - Minimum password length, http://developer.android.com/guide/topics/admin/device-admin.html

[13] OWASP Mobile App Security Checklist v1.2, https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab

=Main

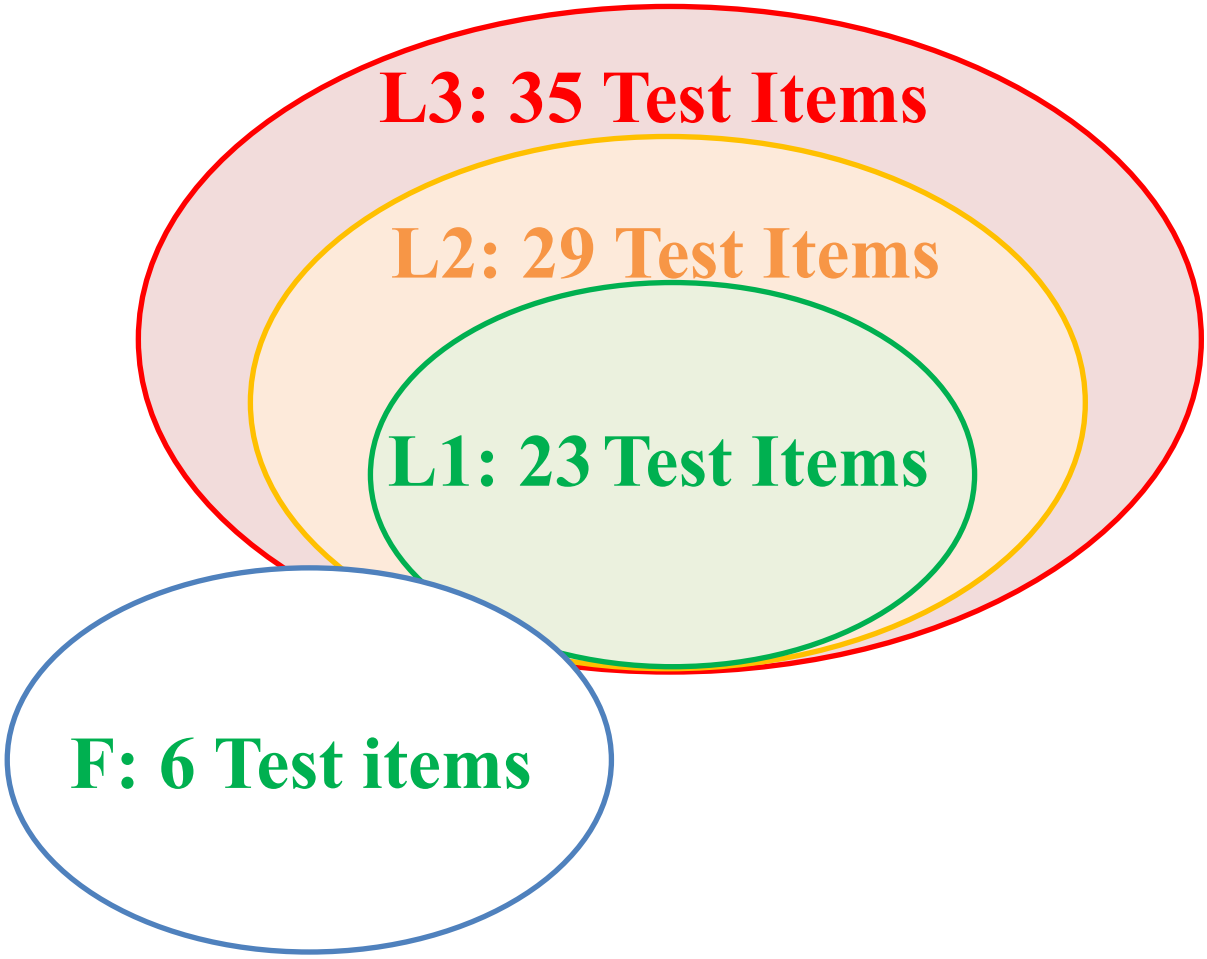
[14] OWASP Mobile Security Testing Guide (MSTG) v1.2
https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main

[15] OWASP Mobile Application Security Verification Standard (MASVS) v1.2
https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main

9. **Appendix**

Appendix I. Instructions regarding the submission categories of mobile applications

When the developer submits the mobile application for testing, the developer must declare the purpose(s), function(s) of the mobile application and the permissions which would be used by the mobile application in the Questionnaire. The testing party, on the other hand, must confirm the category of the mobile application according to the functions described in the Questionnaire. The following figure shows the number of the test items to be performed to mobile applications of respective categories.



Appendix II. Test Item List of Basic Information Security Testing for Mobile Applications

* Description regarding the symbols used in the following table: "*" – Test items for inspection; "-" – Test items for reference.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
4.1.1. Security regarding Mobile Application Release	4.1.1.1. Mobile Application Release	-	-	-	-	4.1.1.1.1. The mobile application shall be released in an application store of a trusted source
		*	*	*	-	4.1.1.1.2. When releasing, the mobile application shall elucidate the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		-	-	-	*	4.1.1.1.3 The mobile application shall prompt the user to install protection software on the mobile device in a prominent location (e. g. the official website, the application download page, etc.).
	4.1.1.2. Mobile Application Updates	-	-	-	-	4.1.1.2.1. The updates of the mobile application shall be released in an application store of a trusted source.
		-	-	-	-	4.1.1.2.2. The mobile application shall provide an update mechanism.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		-	-	-	-	4.1.1.2.3. The mobile application shall make announcements actively when there are security updates.
	4.1.1.3. Mobile Application Security Issue Reporting	-	*	*	-	4.1.1.3.1. Mobile application developers shall provide a channel for reporting security issues.
		-	-	-	-	4.1.1.3.2. Mobile application developers shall respond to questions and make relevant improvements within an appropriate period.
4.1.2. Sensitive Data Protection	4.1.2.1. Sensitive Data	*	*	*	-	4.1.2.1.1. The mobile application shall obtain user consent before collecting sensitive data.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
	Collection	*	*	*	-	4.1.2.1.2. The mobile application shall provide users with the right to refuse the collection of sensitive data.
	4.1.2.2. Sensitive Data Utilization	-	-	-	-	4.1.2.2.1. The mobile application shall obtain user consent before using sensitive data.
		-	-	-	-	4.1.2.2.2. The mobile application shall provide users with the right to refuse the use of sensitive data.
		-	-	-	*	4.1.2.2.3. If the mobile application uses password authentication, it shall actively prompt the user to set a more complex password.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		-	-	-	*	4.1.2.2.4. The mobile application shall remind users to change their passwords regularly.
	4.1.2.3. Sensitive Data Storage	*	*	*	-	4.1.2.3.1. The mobile application shall obtain user consent before storing sensitive data.
		*	*	*	-	4.1.2.3.2. The mobile application shall provide users with the right to refuse the storage of sensitive data.
		-	-	-	-	4.1.2.3.3. The sensitive data stored by the mobile application shall only be used for the purpose(s) stated in its declaration of use.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		*	*	-	-	4.1.2.3.4. The mobile application shall avoid storing sensitive data in redundant files or log files after closure and/or log-out.
		-	-	*	-	4.1.2.3.5. The mobile application shall avoid storing sensitive data in redundant files or log files.
		*	*	*	-	4.1.2.3.6. Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		*	*	*	-	4.1.2.3.7. In order to prevent unauthorized access by other applications, sensitive data shall be stored in the areas protected by the OS.
		*	*	*	-	4.1.2.3.8. Sensitive data shall be avoided in the code of the mobile application.
		-	-	*	-	4.1.2.3.9. The mobile application shall actively alert the user when non-user-initiated screenshots are taken.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		*	*	*	-	4.1.2.3.10. The mobile application shall use system credential storage facilities appropriately to store sensitive data.
		-	*	*	-	4.1.2.3.11. The mobile application shall disable the keyboard cache mechanism when the user is entering sensitive data.
		*	*	*	-	4.1.2.3.12. The mobile application shall avoid the leakage of sensitive data in the IPC mechanism.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		-	*	*	-	4.1.2.3.13. The user interface in the mobile application shall avoid the leakage of sensitive data.
		-	-	*	-	4.1.2.3.14. The sensitive data of the mobile application shall not be stored in the backup data of the mobile device operating system.
	4.1.2.4. Sensitive Data Transmission	*	*	*	-	4.1.2.4.1. The mobile application shall apply appropriate and effective key length and encryption algorithm(s) for secure encryption when transmitting sensitive data via network.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
	4.1.2.5. Sensitive Data Sharing	*	*	*	-	4.1.2.5.1. User consent shall be obtained before the sensitive data are shared among different mobile applications in the mobile device.
		*	*	*	-	4.1.2.5.2. The mobile application shall provide users with the right to refuse sensitive data sharing.
		*	*	*	-	4.1.2.5.3. Accesses from unauthorized mobile applications shall be avoided when the mobile application is sharing sensitive data.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
	4.1.2.6. Deletion of Sensitive Data	-	-	-	-	4.1.2.6.1. The mobile application shall provide users with the function of deletion if the mobile application involves the storage of users' sensitive data.
4.1.3. Security regarding Transaction Resource Management	4.1.3.1. Using Transaction Resource	-	-	*	-	4.1.3.1.1. The mobile application shall actively notify users when using transaction resources.
		-	-	*	-	4.1.3.1.2. The mobile application shall provide users with the right to refuse the use of transaction resources.
	4.1.3.2. Transaction	-	-	*	-	4.1.3.2.1. The mobile application shall perform user authentication when using transaction resources.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
	Resource Management	-	-	*	-	4.1.3.2.2. The mobile application shall record the used transaction resource(s) and the time of use.
4.1.4. Security regarding User Authentication, Authorization, and Connection Management in Mobile	4.1.4.1. User Authentication and Authorization	-	*	*	-	4.1.4.1.1. The mobile application shall have an appropriate authentication mechanism in order to confirm the user's identity.
		-	*	*	-	4.1.4.1.2. The mobile application shall authorize based on user identity.
	4.1.4.2. Mechanism	-	*	*	-	4.1.4.2.1. The mobile application shall avoid using session IDs with regularity.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
Applications	regarding Connection Management	*	*	*	-	4.1.4.2.2. The mobile application shall verify the validity of the server certificate.
		*	*	*	-	4.1.4.2.3. The mobile application shall confirm that the server certificate is issued by a trusted certificate authority.
4.1.5. Code Security of Mobile	4.1.5.1. Prevention	*	*	*	-	4.1.5.1.1. The mobile application shall avoid containing malicious code.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
Applications	from Malicious Code and Avoidance of Information Security Vulnerabilities	*	*	*	-	4.1.5.1.2. The mobile application shall avoid information security vulnerabilities.
	4.1.5.2. Mobile Application Integrity	-	-	-	-	4.1.5.2.1. The mobile application shall use appropriate and effective integrity verification mechanisms to ensure its integrity.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
	4.1.5.3. Security Regarding the Reference of Library	*	*	*	-	4.1.5.3.1. When the library referred by the mobile application is updated, the corresponding updated version shall be prepared. Regarding the update method, please consult subsection: 4.1.1. Security regarding Mobile Application Release.
	4.1.5.4. User Input Verification	*	*	*	-	4.1.5.4.1. The mobile application shall perform security checks to the strings entered by the user at the input phase.
		*	*	*	-	4.1.5.4.2. The mobile application shall provide protection mechanism(s) relevant to injection attacks.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
	4.1.5.5. Prevention from Dynamic Analysis and Tampering	-	-	-	*	4.1.5.5.1. The mobile application must detect whether the protection layer of the mobile operating system is cracked (e.g. rooted, jailbroken) or is not properly protected; if so, the mobile application shall actively notify the user or terminate itself.
		-	-	-	-	4.1.5.5.2. The mobile application shall be able to actively detect whether all the files and data in the sandbox are tampered with.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		-	-	-	-	4.1.5.5.3. The mobile application shall detect whether there is any use of dynamic analysis tools or frameworks in the mobile device.
		-	-	-	-	4.1.5.5.4. The mobile application shall detect whether the code and data in the memory are tampered with.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
		-	-	-	*	4.1.5.5.5. Either that the executable files and the libraries belonging to the mobile application shall all be encrypted on the file level or that the important code and data segments inside the executable files shall be encrypted or packed, making it difficult to acquire important code or data via trivial static analysis.
		-	-	-	*	4.1.5.5.6. The mobile application shall have code obfuscation mechanism(s).
4.2.2. Server-side Security Inspection	4.2.2.1. WebView	-	-	-	-	4.2.2.1.1. The mobile application shall use webview to exchange web resources with remote servers.

ASPECT OF INFORMATION SECURITY TECHNICAL REQUIREMENTS	INFORMATION SECURITY TECHNICAL REQUIREMENT	NECESSITY OF INSPECTION FOR MOBILE APPLICATIONS OF RESPECTIVE CATEGORIES				TEST ITEM
		L1	L2	L3	F	
	Security Inspection	*	*	*	-	4.2.2.1.2. When the mobile application renders functions in the Webview, the connected domain shall be a secure domain.

Appendix III. Questionnaire on Basic Information Security Testing for Mobile Applications

Questionnaire on Basic Information Security Testing for Mobile Applications

※Please be noted that all the information in this form must correspond with the disclosed information on the application store.

№	ITEM NAME	DESCRIPTION
1.	Company Name	
2.	Contact Information	
Basic Information of the Application		
3.	Application Name	
4.	Package Name	
5.	Hash Value of the App's APK/IPA	e.g. MD5: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX: XX:XX: SHA1: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX: SHA256: XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX
6.	Operating System	☐ Android ver.: ______________________ ☐ iOS ver.: __________________________ ☐ Windows ver.: _____________________ ☐ Other OS: _________________________
7.	Application Version	
8.	Category of the Mobile Application	Please check the security category of the App: ☐ L1: A mobile application that does NOT require user

№	ITEM NAME	DESCRIPTION
		authentication. ☐ L2: A mobile application that REQUIRES user authentication. ☐ L3: A mobile application in which transaction behavior is involved.
9.	Release Status	☐ For internal use only, not publicly released.
		(If the App is only for internal use, please skip this section.) ☐ Released. ☐ Unreleased; expected release date: _____ (DD/MM/YYYY) Released or scheduled to be released on: ☐ Application store provided by mobile OS Vendors: ☐ Apple App Store (URL): _____ ☐ Google Play (URL): _____ ☐ Microsoft Marketplace (URL): _____ ☐ Other Platform(s) (URL): _____ ☐ Application store provided by mobile device manufacturers (Please specify the name of the manufacturer and that of the application store.）_____ ☐ Application store provided by telecommunications service providers (TSPs) (Please specify the name of the TSP and that of the application store.）_____

<table>
<tr><th>№</th><th>ITEM NAME</th><th colspan="3">DESCRIPTION</th></tr>
<tr><td rowspan="5">10.</td><td colspan="4">The needed types of sensitive data in the mobile device (resources, permissions), their description of use, whether these sensitive data are stored in the device, whether are these sensitive data shared with other applications.</td></tr>
<tr><td>sensitive data (resources, permissions)</td><td>description of use & the method of obtaining user consent</td><td>Are the sensitive data stored in the device?</td><td>Are the sensitive data shared with other applications?</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>11.</td><td colspan="4">The contents of declaration regarding prompting the installation of protection software and its expected location (Please skip this section if the mobile application has already been released.)</td></tr>
<tr><td colspan="5">Expected location for the declaration:
Expected contents of the declaration:</td></tr>
<tr><td>12.</td><td colspan="4">The expected contents of the sensitive data to be shared by the mobile application, its description of use, the method(s) of obtaining user consent, the applications to which the sensitive data are shared (Please skip this section if the mobile application has already been released.)</td></tr>
<tr><td colspan="2">The expected contents to be shared</td><td>description of use & the method of obtaining user consent</td><td colspan="2">The applications to which the sensitive data are shared.</td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td></td><td colspan="2"></td></tr>
<tr><td>13.</td><td>URL of the privacy statement</td><td colspan="3"></td></tr>
<tr><td rowspan="2">14.</td><td rowspan="2">Contacts disclosed for issue reporting & improvement mechanism.</td><td colspan="3">Disclosed in: ☐ the mobile application ☐ the application store page.</td></tr>
<tr><td colspan="3">☐ Website: _____
☐ E-mail: _____
☐ Telephone №: _____</td></tr>
</table>

№	ITEM NAME	DESCRIPTION
		☐ Other means of contact:_____
15.	Library used in the App [library name, version, sources (including OS built-in libraries, third-party libraries)]	Format: < library name / library version / library source > [e.g. webkit / 534.30 / OS Bulit-in]
16.	Is the connection encrypted? (For the L1 Apps, please skip this item.)	☐ Yes; and the encryption protocol is: _____(e.g. TLS 1.2) ☐ No; and the reason for not using encryption is: _____
17.	Description of random number generator library used in encryption algorithm	e.g. The mobile application used <XX random number generating libraries> in the <OO encryption algorithm>.
18.	Is the App free of charge?	☐ Yes ☐ No
19.	Use of WebView	☐ Yes; domain name: _____ (e.g. www.moeaidb.gov.tw) ☐ No
20.	Notes	

Company Name: _____

Name of the Representative: _____

VAT Id. №: _____

Company Address:

_____

Date of Signature:_____

(DD/MM/YYYY)

Official Seal of the Company

Seal of the Represent -ative

Appendix IV. Report Template of Basic Information Security Testing for Mobile Applications

Report №:

XXXXX (Institution name) XXXXX (laboratory name)

Report of Basic Information Security Testing for Mobile Applications

(Template for front cover)

Report №	
Test Standard(s)	
Company Name	
Application Developer	
Basic Information of the Mobile Application	
Application Name	
Package Name	
Operating System	
Application Version	
Category of the Mobile Application	
Inspection Result	
Start Date of Inspection	
End Date of Inspection	
Date of Report Issuance	
Report Version	

Report Approver (Signature)	Report Signatory (Signature)	Testing Personnel (Signature)

I. Test Items and Test Results

Aspect of Information Security Technical Requirements	Test Item	Test Result (Passed / Failed / Test Item for Reference)	Notes
4.1.1. Security regarding Mobile Application Release	4.1.1.1.1. The mobile application shall be released in an application store of a trusted source		
	4.1.1.1.2. When releasing, the mobile application shall elucidate the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions		
	4.1.1.3.1. Mobile application developers shall provide a channel for reporting security issues		
...	...		

II. Number Assignment Format

(In this chapter, the test laboratory will elucidate the format(s) of number assignment it applies for the report and test items.）

III. Inspection Tools

(I) Software used in the Inspection

(The list of software/hardware tools used in the inspection)

(II) Hardware used in the Inspection

(The basic information of hardware tools used in the inspection, e. g. brand of the mobile device(s), model №, S/N of the device(s), OS version(s), etc.)

IV. Annex

(Questionnaire on Basic Information Security Testing for Mobile Applications and other supporting materials attached by the test laboratory)

Appendix V. Basic Information Security Test Items for Reference for Mobile Applications

In the given appendix, basic information security test items for reference are formulated for different aspects in mobile application security, which includes three major aspects and will be respectively elucidated in each chapter: 4.1.1. Security regarding Mobile Application Release, 4.1.2. Sensitive Data Protection, and 4.1.5. Code Security of the Mobile Application, etc.

For each test item for reference, form fields, e. g. test item №, reference basis, technical requirements, description of the test item, source of reference, notes, etc. are formulated. For the description of the above-mentioned form fields, please consult the following table:

Description of the Test Item for Reference Form Fields

FIELD NAME	DESCRIPTION
Test Item №	The test item number consisting of 4 digits, of which the categorization is based on the chapter “4. Technical Requirements” of the «Basic Information Security Standard for Mobile Applications»; the test item numbers are shown in the format as “REF-x”, in which “REF-” indicates that the digits are for the test items of “Appendix V. Basic Information Security Test Items for Reference for Mobile Applications” and the “x” stands for the affiliated item number which expands downwards respectively.
Reference Basis	The technical requirements regarding information security for mobile applications corresponding to those of the Chapter “4. Technical Requirements” of the «Basic Information Security Standard for Mobile Applications».
Technical Requirements	The “contents” of the technical requirements regarding information security for mobile applications corresponding to those of the

	Chapter “4. Technical Requirements” of the «Basic Information Security Standard for Mobile Applications»
Description of the Test Item	Reason(s) for reference: Description:
Source of Reference	The source of reference of the given test item for reference.
Notes	Other additional information or remarks.

4.1.1. Security regarding Mobile Application Release

4.1.1.1. Mobile Application Release

4.1.1.1.1. The mobile application shall be released in an application store of a trusted source.

TEST ITEM №	REF-1.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.1.1 Mobile Application Release
Technical Requirements	The mobile application shall be released in an application store of a trusted source.
Description of the Test Item	Reason(s) for reference: The test item is for the developers’ reference only, not a test item to which actual inspection is performed. Description: This test item is not an item that can be determined by inspecting the mobile application itself. It is recommended that the mobile application be released in the application stores provided by mobile operating system vendors, mobile device manufacturers

	and/or telecommunications service providers.
Source of Reference	NIST SP 800-163 3.1.6 Testing App Updates
Notes	N/A

4.1.1.2. Mobile Application Updates

4.1.1.2.1 The updates of the mobile application shall be released in an application store of a trusted source.

TEST ITEM №	REF-2.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.1.2 Mobile Application Updates
Technical Requirements	The updates of the mobile application shall be released in an application store of a trusted source.
Description of the Test Item	Reason(s) for reference: The test item is for the developers' reference only, not a test item to which actual inspection is performed. Description: This test item is not an item that can be determined by inspecting the mobile application itself. It is recommended that the updates of the mobile application be released in the application stores provided by mobile operating system vendors, mobile device manufacturers and/or telecommunications service providers.
Source of Reference	NIST SP 800-163 3.1.6 Testing App Updates
Notes	N/A

4.1.1.2.2 The mobile application shall provide an update mechanism.

TEST ITEM №	REF-3.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.1.2. Mobile Application Updates
Technical Requirements	The mobile application shall provide an update mechanism.
Description of the Test Item	Reason(s) for reference: The test item is for the developers' reference only, not a test item to which actual inspection is performed. Description: When there is a security vulnerability found in the code of the mobile application, updates shall be provided by the server-side of a trusted source.
Source of Reference	NIST SP 800-163 3.1.5 Securing App Code Dependencies
Notes	N/A

4.1.1.2.3 The mobile application shall make announcements actively when there are security updates.

TEST ITEM №	REF-4.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.1.2. Mobile Application Updates
Technical Requirements	The mobile application shall make announcements actively when there are security updates.

Description of the Test Item	Reason(s) for reference: The test item is for the developers' reference only, not a test item to which actual inspection is performed. Description: This test item is not an item that can be determined by inspecting the mobile application itself. It is recommended that the mobile application make announcements in the application stores provided by mobile operating system vendors, mobile device manufacturers and/or telecommunications service providers when there are security updates.
Source of Reference	NIST SP 800-64 3.4 SDLC Phase: Operations and Maintenance
Notes	N/A

4.1.1.3. Mobile Application Security Issue Reporting

4.1.1.3.2. Mobile application developers shall respond to questions and make relevant improvements within an appropriate period

TEST ITEM №	REF-5.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.1.3. Mobile Application Security Issue Reporting
Technical Requirements	Mobile application developers shall respond to questions and make relevant improvements within an appropriate period
Description of the Test Item	Reason(s) for reference: The test item is only relevant to quality and do not directly affect the security of the mobile application. Description: This test item is not an item that can be determined by inspecting the mobile application itself. It is recommended that mechanisms for responding questions and making improvements be provided.
Source of Reference	NIST SP 800-64 3.1.3.5 Ensure Use of Secure Information System
Notes	N/A

4.1.2. Sensitive Data Protection

4.1.2.2. Sensitive Data Utilization

4.1.2.2.1. The mobile application shall obtain user consent before collecting sensitive data.

TEST ITEM №	REF-6.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.2.2. Sensitive Data Utilization
Technical Requirements	The mobile application shall obtain user consent before collecting sensitive data.
Description of the Test Item	Reason(s) for reference: The inspection on the test item is difficult to perform or does not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present. Description: This test item is not an item that can determine whether or not the sensitive data are used by inspecting the mobile application itself. It is recommended that: (1) Before the mobile application uses sensitive data, declaration be made in the mobile application or in the application stores provided by mobile operating system vendors, mobile device manufacturers and/or telecommunications service providers. (2) Before the mobile application uses sensitive data, user consent be obtained in the mobile application or in the application stores provided by mobile operating system vendors, mobile device manufacturers and/or telecommunications service providers.

Source of Reference	NIST SP 800-163 3.1.4 Protecting Sensitive Data
Notes	N/A

4.1.2.2.2. The mobile application shall provide users with the right to refuse the use of sensitive data.

TEST ITEM №	REF-7.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.2.2. Sensitive Data Utilization
Technical Requirements	The mobile application shall provide users with the right to refuse the use of sensitive data.
Description of the Test Item	Reason(s) for reference: The inspection on the test item is difficult to perform or does not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present. Description: This test item is not an item that can determine whether or not the sensitive data are used by inspecting the mobile application itself. It is recommended that function(s) for refusing the use of sensitive data be provided to users.
Source of Reference	NIST SP 800-163 3.1.4 Protecting Sensitive Data
Notes	N/A

4.1.2.3. Sensitive Data Storage

4.1.2.3.3. The sensitive data stored by the mobile application shall only be used for the purpose(s) stated in its declaration of use.

TEST ITEM №	REF-8.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.2.3. Sensitive Data Storage
Technical Requirements	The sensitive data stored by the mobile application shall only be used for the purpose(s) stated in its declaration of use.
Description of the Test Item	Reason(s) for reference: The inspection on the test item is difficult to perform or does not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present. Description: This test item is not an item that can determine the purpose(s) of use of sensitive data by inspecting the mobile application itself. It is recommended that sensitive data be used only within the scope of the declaration of use.
Source of Reference	NIST SP 800-163 3.1.4 Protecting Sensitive Data, MSTG-ARCH-4, MSTG-ARCH-12, MSTG-STORAGE-12
Notes	N/A

4.1.2.6. Deletion of Sensitive Data

4.1.2.6.1. The mobile application shall provide users with the function of deletion if the mobile application involves the storage of users' sensitive data.

TEST ITEM №	REF-9.
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.2.6. Deletion of Sensitive Data
Technical Requirements	The mobile application shall provide users with the function of deletion if the mobile application involves the storage of users' sensitive data.
Description of the Test Item	Reason(s) for reference: The inspection on the test item is difficult to perform or does not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present. Description: This test item is not an item that can determine whether or not sensitive data are deleted by inspecting the mobile application itself. It is recommended that sensitive data shall not exist in any form in the mobile device after the function of sensitive data deletion interface of the mobile application is executed.
Source of Reference	NIST SP 800-163 3.1.4 Protecting Sensitive Data
Notes	N/A

4.1.5. Code Security of the Mobile Application

4.1.5.2. Mobile Application Integrity

4.1.5.2.1. The mobile application shall use appropriate and effective integrity verification mechanisms to ensure its integrity.

TEST ITEM №	REF-10
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.5.2. Mobile Application Integrity
Technical Requirements	The mobile application shall use appropriate and effective integrity verification mechanisms to ensure its integrity.
Description of the Test Item	Reason(s) for reference: The test item is for the developers' reference only, not a test item to which actual inspection is performed. Description: This test item is not an item that can determine whether or not the mobile application is integral by inspecting the mobile application itself. As verifying the integrity of programs needs the cooperation of platform providers, it is recommended that: (1) Mobile application developer provide the hash value of the application for the users to verify the integrity of the mobile application. (2) Obfuscation techniques be adopted in order to protect the business logic of the mobile application.
Source of Reference	OWASP Mobile App Security Checklist 0.9.3 V7.2: Verify that the app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable), MSTG-CODE-1

Notes	N/A

4.1.5.5. Prevention from Dynamic Analysis and Tampering

4.1.5.5.2. The mobile application shall be able to actively detect whether all the files and data in the sandbox are tampered with.

TEST ITEM №	REF-11
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering
Technical Requirements	The mobile application shall be able to actively detect whether all the files and critical data in the sandbox are tampered with.
Description of the Test Item	Reason(s) for reference: The inspection on the test item is difficult to perform or does not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present. Description: As it is difficult to perform inspection on whether the code and the files stored in the mobile application are tampered with, this test item is for developers' reference only.
Source of Reference	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering, OWASP MSTG-RESILIENCE-3
Notes	N/A

4.1.5.5.3. The mobile application shall detect whether there is any use of dynamic analysis tools or frameworks in the mobile device.

TEST ITEM №	REF-12
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering
Technical Requirements	The mobile application shall detect whether there is any use of dynamic analysis tools or frameworks in the mobile device.
Description of the Test Item	Reason(s) for reference: The inspection on the test item is difficult to perform or does not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present. Description: As it is difficult to detect via mobile applications whether there are dynamic analysis tools, application packages/files/background applications/libraries related to dynamic analysis framework in the mobile operating system, this test item is for developers' reference only.
Source of Reference	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering, OWASP MSTG-RESILIENCE-4
Notes	N/A

4.1.5.5.4. The mobile application shall detect whether the code and data in the memory are tampered with.

TEST ITEM №	REF-13
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering
Technical Requirements	The mobile application shall detect whether the code and data in the memory are tampered with.
Description of the Test Item	Reason(s) for reference: The inspection on the test item is difficult to perform or does not have consistent results when performed repeatedly due to the time required for inspection, the complexity, or the lack of a general inspection method at present. Description: As it is difficult to inspect whether the code and data in the memory have been modified during the execution phase of the mobile application, this test item is for developers' reference only.
Source of Reference	«Basic Information Security Standard for Mobile Application» 4.1.5.5 Prevention from Dynamic Analysis and Tampering, OWASP MSTG-RESILIENCE-6, MSTG-STORAGE-10
Notes	N/A

4.2.2. Server-side Security Inspection

4.2.2.1. WebView Security Inspection

4.2.2.1.1. The mobile application shall use WebView to exchange web resources with remote servers.

TEST ITEM №	REF-14
Reference Basis	«Basic Information Security Standard for Mobile Application» 4.2.2.1. WebView Security Inspection
Technical Requirements	The mobile application shall use WebView to exchange web resources with remote servers.
Description of the Test Item	Reason(s) for reference: The test item is for the developers' reference only, not a test item to which actual inspection is performed. Description: When the mobile application exchanges web resources with remote servers, if external apps are used (e.g. malicious browsers), then there may be concerns about data leakage or data theft. Therefore, it is recommended to use WebView to exchange web resources with servers.
Source of Reference	N/A
Notes	N/A