Basic Security Testing Baseline for Mobile Applications

V3.0

Industrial Development Bureau, Ministry of Economic Affairs

May 2018

Revision of Basic Security Testing Baseline for Mobile Applications

Date	Revision History	Version
August 2015	V1.0	V1.0
February 2016	V2.0	V1.0
March 2017	V2.1	V1.1
May 2018	V3.0	V1.2

Table of Contents

1. Introduction 1

2. Applicability 3

3. Terms and Definitions 4

3.1. Mobile Application 4

3.2. Application Store 4

3.3. Personal Data 4

3.4. Sensitive data 4

3.5. Password 4

3.6. Transaction Resource 5

3.7. Session Identification, Session ID 5

3.8. Server Certificate 5

3.9. Certification Authority 5

3.10. Malicious Code 5

3.11. Vulnerability 5

3.12. Library 5

3.13. Code Injection 6

3.14. Mobile Operating System 6

3.15. Mobile Resource 6

3.16. In-Application Update 6

3.17. Common Vulnerabilities and Exposures 6

3.18. Weak Cryptographic Algorithm 6

3.19. Known Vulnerabilities 6

3.20. Authentication 6

3.21. Advanced Encryption Standard 6

3.22. Triple Data Encryption Standard 7

3.23. Elliptic Curve Cryptography 7

3.24. Certificate Pinning 7

3.25. Hash 7

3.26. Obfuscation 7

3.27. Using sensitive data 7

3.28. Log File 7

3.29. Device Identifier 7

3.30. Cache Files or Temporary Files 8

3.31. Configuration File 8

3.32. Encode 8

3.33. Decode 8

3.34. Payload 8

3.35. Collecting sensitive data 8

3.36. Storing sensitive data 8

3.37. Common Vulnerability Scoring System 9

3.38. Secure Random Number Generator 9

3.39. Secure domain 9

3.40. Secure Encryption Function 9

4. Basic Information Security Testing Baseline 10

4.1. Basic Security Testing Baseline for Mobile Applications 12

4.1.1. Mobile Application Release Security 14

4.1.2. Protection of Sensitive data 20

4.1.3. Transaction Resources Security Controls 43

4.1.4. User Identity Authentication, Authorization and Connection Management Security 48

4.1.5. Mobile Application Security Code 55

4.2. Server-side Basic Information Security Baseline 67

4.2.1. Server-side Security Management 67

4.2.2. Server-side Security Testing 67
5. Testing Methods 71
5.1. Automatic Testing 71
5.2. Manual Testing 71
5.2.1. Static Analysis 71
5.2.2. Dynamic Analysis 72
5.3. Code Analysis 72
5.4. Binary Code Analysis 72
6. Supplement 73
7. Test results and Outputs 74
8. Reference Materials 75
9. Appendix 76
Appendix I, Classification of the Security Testing for Mobile Applications 76
Appendix II, Inspection Item of the Mobile Application Basic Security 77
Appendix III, Questionnaire on Security Testing for Mobile Applications 88
Appendix IV, Reference Format for the Report of Security Testing for Mobile Applications 92
Appendix V. Reference for the mobile application basic security 94
4.1.1. Mobile Application Release Security 95
4.1.2. Protection of Sensitive data 99
4.1.5. Mobile Application Security Code 106
4.2.2. Server-side Security Testing 107

Table Contents

Table 1. Benchmark Table Content Description 12

1. Introduction

Mobile devices have become an integral part of everyone's life. Various types of mobile applications have also emerged due to people's demands. From applications that handles our daily schedule and task, to entertainment and gaming, and even our financials and shopping has gone mobile. However, the developers that is behind these application developments usually lacks security awareness, which could lead to security issues such as minor as insecure transactions, to information leakage, and ultimately financial loses in some cases. Industrial Development Bureau, under Ministry of Economic Affairs, in accordance to National Information and Communication Security Taskforce under Executive Yuan, has commenced during its 26th Council Meeting to refer to the relevant international regulation on such matter, and formulate with industry experts in completing "Basic Security Baseline for Mobile Applications" for the mobile application developer and its related industry to adapt voluntarily.

To help developers better understand this baseline document and maintain the level of security proficiency of its mobile applications, the Ministry of Economic Affairs commissioned Institute for Information Industry in collaboration with Chinese Cryptology and Information Security Association, to amend the "Basic Security Testing Baseline for Mobile Application" (Hereinafter as the baseline), for the latest versioning info, please refer to the versioning revision at the beginning of this document. This baseline, at this current iteration, has based primarily on its previous versions for classification, and referenced Open Web Application Security Project (OWASP) Mobile Security Testing Guideline's Mobile Application Security Checklist, Cloud Security Alliance's Mobile Application Security Testing Workgroup's Whitepaper, as well as National Institute of Standards and Technology's Special Release 800-163 titled "Vetting the Security of Mobile Applications" as its basis as well. To assist the developers in understand how to handle security risk assessment and assurance, we have formulated test items with test methodology and expected results from each test items under various conditions when executed.

This baseline provides a procedure for which the third parties can match its product against the standards listed within. With the mobile application itself aligned with the baseline, it is in our vision that users would trust the mobile application which they use on the daily basis.

2. Applicability

In order to ensure the mobile applications tested matches the current standards of information security requirements, this baseline applies to all of the non-specific domains and those specified within the "Basic Security Baseline for Mobile Applications". Information security itself is based on the concept of risk control, even if the mobile application tested has matched all the standards and requirements of the procedures listed in this document, it does not guarantee the mobile application is completely safe. Other possible hacking methods such as malicious reversal or usage of the application, could still lead to security issues. The user themselves still have the responsibility to ensure the proper usage and management of their own personal data, such as account, password and the way they kept and maintained, so to help reduce the possibility of causing any other possible security risk or threats by improper management.

3. Terms and Definitions

The following terms and definitions, refer to the "Basic Security Baseline for Mobile Applications V1.2". For any changes, refer to the latest version of "Basic Security Baseline for Mobile Applications".

3.1. Mobile Application

Refers to a designed application for smartphones, tablet and other devices, also herein as "Mobile Application".

3.2. Application Store

Refers to a platform or a website that mobile device users can browse to download and buy applications.

3.3. Personal Data

According to the "Personal Data Protection Act" on the definition of all to recognize the individual's data directly or indirectly, including but not limited to name of natural person, date of birth, identity card number, passport number, characteristics, fingerprints, marriage, family, education, occupation, medical history, medical, genetic, sex life, health check, criminal record, contact information, financial status, social activities.

3.4. Sensitive data

Refers to information that is established, stored or transmitted during user operations or application rundown in mobile device or their storage media. Leaking this kind of information endangers users, including but not limited to the defined personal information in 3.3, and addition to passcode, key, video, photos, call, audio files, chat messages, call history, text messages, memos, contacts, notes, location, calendar and device identifiers and other relevant information on personal privacy.

3.5. Password

Refers to a group of characters that allow users to use the system or to identify the users, including local storage file data encryption password, local account and password, remote web service account and password.

3.6. Transaction Resource

Refers to cash flow, no matter physical or virtual currency (points or serial number included) and other valuable items are regarded as trading resources. Those are using for mobile in-application purchase function, and may directly or indirectly acquire additional function, the content or subscriptions. Such as buying tickets in the ticketing system Application to receive a QRcode as an entry document; buying e-books in the online bookstore Application to get the contents of the e-book available for reading; subscripting or purchasing transaction services within the Application to provide new features, remove restriction functions or ads; providing payment function within a payment-site Application, providing bank transfer within a bank Application or some providing function of buying real or virtual goods.

3.7. Session Identification, Session ID

Refers to the assigned identification number when establishing a connection. Using it as a unique identifier during the connection. When the connection is released, the identification code can be reassigned to new connection.

3.8. Server Certificate

Refers to signature verification which provides mobile applications to identify the identity of the server and encrypt data during transmission.

3.9. Certification Authority

Refers to organizations or authorities that issue the certificate.

3.10. Malicious Code

Refers to source codes that violate the rights of users without their consent, including but not limited to any malicious characteristic or behavior.

3.11. Vulnerability

Refers to deficiencies of the application security making the confidentiality, integrity and availability of the system, or information of the application under threat.

3.12. Library

Refers to the compiled binary code, that provides programmers to use, formed by some complex idea or hardware-level involved function or object.

3.13. Code Injection

Refers to malicious instructions, including but not limited to command injection and SQL injection, which user inputted through vulnerabilities.

3.14. Mobile Operating System

Refers to the operating system in a mobile device.

3.15. Mobile Resource

Refers to the function or service provided by mobile devices, including but not limited to a camera, photo, microphone, wireless networks, sensors, and location.

3.16. In-Application Update

Refers to renewing contents and features of the application through a custom method updates, but not changing the major version released in the application store.

3.17. Common Vulnerabilities and Exposures

Short for "CVE". It is a vulnerability management program sponsored by the US Department of Homeland Security. It gives a globally recognized unique number to every vulnerability.

3.18. Weak Cryptographic Algorithm

Refers to cryptographic algorithms numbered in CVE.

3.19. Known Vulnerabilities

Refers to the vulnerabilities numbered in CVE.

3.20. Authentication

Refers to the authenticity of the identity of the individual claimed.

3.21. Advanced Encryption Standard

Refers to the NIST (National Institute of Standards and Technology) released in 2001 in AES (Advanced Encryption Standard) encryption algorithm, the file number is FIPS PUB 197 standard and formally implemented in 2002. AES supports 128-bit Data Block, and for 128, 192 and 256-bit of Key Size, improving the security, AES encryption and decryption contain more than ten the number of Round Number, each round consists of four main base unit.

3.22. Triple Data Encryption Standard

Refers to a product cipher method using Triple Data Encryption Standard, processes 64-bit data block.

3.23. Elliptic Curve Cryptography

Refers to a public key encryption algorithm established by elliptic curve additive group or in the mathematical structure. Using elliptic curve cryptography since the establishment by Neal Koblitz and Victor Miller independently in 1985.

3.24. Certificate Pinning

Refers to the server certificate. It is stored in advance in the application, to confirm the consistency of the server certificate during the connection.

3.25. Hash

Refers to a string of data through the algorithm that calculates fingerprint data. It is often used to identify where files or data have been tampered, in order to ensure the files and data indeed is provided by the original creator.

3.26. Obfuscation

Refers to converting the source code of the mobile application, without affecting the function, into a hard-to-read form.

3.27. Using sensitive data

Refers to providing for an application itself and third party to use.

3.28. Log File

Refers to the file that stores the system log, application log, security log, debug log or a custom log only for debugging.

3.29. Device Identifier

Refers to the unique identification information on 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 IFAID (Identifier for Advertisers Identifier, IFAID), Windows Phone Device ID.

3.30. Cache Files or Temporary Files

Refers to the files, that are independent in the application functionality, created when the mobile application is installing and running. They are usually deleted when the application exits. The files, such as temporary files or cache, do not affect the function and performance of mobile applications, no matter they exist or not, when executed again. In addition, if deleting files causes the automatic sign-in fails, these files should belong to the configuration files rather than redundant files.

3.31. Configuration File

Refers to mobile applications store files associated with settings, it will affect the performance of mobile applications when deleted.

3.32. Encode

Refers to the operation of converting data into codes or characters, and they can be decoded back to the original data.

3.33. Decode

Refers to the operation of reversing the encoded code or character back to the original data.

3.34. Payload

Refers to packets, messages or codes include effective information and instruction.

3.35. Collecting sensitive data

Refers to the collection of sensitive data embedded in the mobile device or inputted by the user.

3.36. Storing sensitive data

Refers to storing the sensitive data as a file to the mobile device or a subsidiary storage media.

3.37. Common Vulnerability Scoring System

Short for "CVSS". It provided scores on IT vulnerability characteristics and influence by National Infrastructure Advisory Council (NIAC). However, it is now the 3rd edition by Forum of Incident Response and Security Teams (FIRST).

3.38. Secure Random Number Generator

Random number generator that satisfies or refers to the standard ANSI X9.17.

3.39. Secure domain

It includes developers, customer-owned domain or generally known domains of public security, the general well-known security public domain including Facebook, Google or Twitter OAuth 2.0 Support Agreement.

3.40. Secure Encryption Function

Encryption function that satisfies FIPS 140-2 Annex A.

4. **Basic Mobile Application Security Testing Guideline**

The following items contained within this section are based on Section 4 of the "Basic Security Baseline for Mobile Applications" and serves as the technical requirement for the approval of mobile application thus forward. The primary purpose of this guideline is to provide industry standard on mobile application security testing methodology and vetting process for a secured mobile application. However, based on the purpose and usage of the mobile application being developed, the level of the security category required by this guideline differs as well.

The security category that the applications falls under are divided into the following three categories in accordance to the usage of the application itself:

- Category 1: Applications that does not require user authentications but otherwise collects basic user information
- Category 2: Applications that requires user authentications
- Category 3: Applications that contains transactions such as financial or otherwise specified types of transaction.

Based on the category listed above, each proceeding category contains the requirement specified in the previous category, and the number of test items differs as well:

- Category 1: 15 required items
- Category 2: 26 required items
- Category 3: 31 required items

The guideline has two types of test items: essential and reference items. The essential items are required for the mobile application to be satisfactory to the security standard, and only when the hosted operation system is not compromised or modified by any methods such as jailbreak or rooted system. The reference items are to be used as additional requirements for strengthened security applied under other security categories which collects additional information or transact within the mobile application itself.

The only exception that would allow mobile applications not going through test items are conditioned with one of the following:

- When application’s quality, and other relating matters, does not directly affect the security of the mobile application itself
- When there are no methodology provided to do the testing due to the complexity, duration of time or unable to conduct such the testing procedure on the mobile application itself
- The mobile application is still under development and intended as developer’s reference and not as an actual production product

All the diagrams and test vetting methodology related to the test items, please refer to "Appendix I".

When executing a mobile application testing procedure, it is necessary to complete the documents contained in "Appendix III". Developers can go through if there are sensitive data and priviledge that needs to be secured first and check it’s rationality if such testing procedure is required. In addition, it will also help if business logic of the application and it’s associated functions can be provided to test personnel or facility to better facilitate the testing which is required by the mobile application.

4.1. Basic Security Testing Baseline for Mobile Applications

In this section we provide the basic security test standards for mobile applications, includes five areas and denotes it as following:

4.1.1. Mobile application release security

4.1.2. Protection of sensitive data

4.1.3. Trading Resources Security Controls

4.1.4. User identity authentication, authorization and connection management security

4.1.5. Mobile application security code

For each test items, we provide testing ID, test items, test category, test basis, technical requirements, test standards, test results, remark as described in Table 1. .

Table 1. Test items Description

ITEMS	DESCRIPTION
Testing ID	The ID designates as the assigned Test ID for the particular test item. Each ID is in accordance with Section 4 of the "Basic Security Baseline for Mobile Applications" and expands into sub section if deemed necessary. The ID is formatted with 4.1 as primary identification number for Section 4.1, and expands to 4.1.x.y.z, where "x" indicates as area concerned which is described in Sec. 4.1. Numbers "y" and "z" are denoted as expanded items under the tested area in concern.
Test items	Abbreviated summary of this test
Test category	This section reflects to which security category this test item shall be included with. The category is defined in Section 4 of this documents.
Test basis	This section reflects to which basis of this test item shall be included with. The category is defined in Section 4 of this documents.
Technical requirements	This section denotes the pre-requisites of this test item, if available
Test standards	This section explains how the test should be executed, and the pass / failed condition for the test result

Test results	This section defines the result of the test item.　The result shall be said as “Satisfied”, “Unsatisfied”, or “Not Applicable”
Remark	Other description items

All test items that requires users’ consent can be obtained from the default agreement of the trusted application store’s “download, install and use to agree” policy.　Either that, or developer can actively provide a user agreement with the option to agree or disagree during the application initialization process and provide ability for user to review such agreement within the application after installation and usage.

4.1.1. Mobile Application Submission Security

This mainly applies to the relevant information security norm for the submission of the mobile application, including submit, updates and reporting the problem in return.

4.1.1.1. Mobile Application Submission

For test items in "Mobile Application Submission", the test result of level 2, 3 mobile applications meet criteria 4.1.1.1.2. “Mobile application should note if there are secured or sensitive data being accessed, as well as the mobile device resources and with a declaration of the permissioned purposes of use at the time of submission ". The result should return “Satisfied”, otherwise as “Failed”.

4.1.1.1.1. Mobile applications shall be submitted to trusted application stores

This list of the stores are in the reference, see "Appendix V".

4.1.1.1.2. Mobile application should note if there are secured or sensitive data being accessed, as well as the mobile device resources and with a declaration of the permissioned purposes of use at the time of submission

TESTING ID	4.1.1.1.2
Test items	Mobile Application Release Notes
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications" 4.1.1.1 Mobile application Release
Technical requirements	Mobile application should note if there are secured or sensitive data being accessed, as well as the mobile device resources and with a declaration of the permissioned purposes of use at the time of submission
Test standards	If the mobile application has been released, check whether the mobile application explains how secured and sensitive data are accessed, as well as mobile device resources and the declaration of the permission and purpose of its access and submission to a trusted application store. If the mobile application has not been released, check if there are explanations on how to provide sensitive data that is to be accessed, the mobile device resources and the declaring of the purpose and permission. “Yes” is consistent with the testing baseline; "No" is not in line with standard testing
Test results	Satisfied the requirements: meet test standards Non-Satisfied the requirements: not meet test standards NA: mobile applications are not publicly available; then this need not to be detected

Remark	The developer should self-declare the destination of the submission in "Appendix III". The announcement of application store should base mainly on the interface of mobile device stores.

4.1.1.2. Mobile Application Update

"Mobile application update" should match to the references items are in the test items, which is for developers' reference only.

4.1.1.2.1. Mobile applications shall be released the updates in trusted application stores

This item is a reference item, see "Appendix V".

4.1.1.2.2. Mobile applications should provide an update mechanism

This item is a reference item, see "Appendix V".

4.1.1.2.3. Mobile applications should notify actively when security updates

This item is a reference item, see "Appendix V".

4.1.1.3. Mobile Application Security Issues Submission

For test items in "Mobile Application Security Issues Submission", the test result of level 2 and 3 mobile applications have to be "Satisfied" in correspondand to criteria 4.1.1.3.1. “Mobile application developers should provide a channel of submission on security issues ". In order to meet the information security technical requirements; otherwise it fails.

4.1.1.3.1. Mobile application developers should provide a channel of return on security issues

TESTING ID	4.1.1.3.1
Test items	Mobile Application Security Issues In Return
Test category	Level 2, 3
Test basis	"Basic Information Security Regulation for Mobile Applications." 4.1.1.3. Mobile Application Security Issues In Return
Technical requirements	Mobile application developers should provide a channel of submission on security issues
Test standards	If the mobile application has been released, check whether the mobile application provides contact page, message boards, e-mail, telephone or other types of contact in trusted application stores and the initiation of contact through either means are successful. If the mobile application has not yet been released or publicly available, check whether it is expected to provide a submission channel and contact information on security issues in self-check list. “Yes” is consistent with this item testing baseline; "No" is not consistent with testing baseline
Test results	Satisfied the requirements: meet test standards

	Non-Satisfied the requirements: not meet test standards NA: mobile applications are not publicly available; then this need not to be detected
Remark	

4.1.1.3.2. Mobile application developers should respond and improve the problem within a reasonable period.

This item is a reference item. See "Appendix V".

4.1.2. Protection of Sensitive Data

This applies mainly to the sensitive data and personal data related to the baseline, including collection, usage, storage, transmission, sharing and deletion of sensitive data.

4.1.2.1. Sensitive Data Collection

For test items in "Sensitive Data Collection", the test result of level 2, 3 mobile applications have to be "Satisfied" in correspondant to criteria 4.1.2.1.1. " Mobile application should get users' consent before collecting sensitive data ", and criteria 4.1.2.1.2 "Mobile application should provide users the right to refuse to collect the sensitive data". In order to meet the information security technical requirements; otherwise it fails.

4.1.2.1.1. Mobile application should get users' consent before collecting sensitive data

TESTING ID	4.1.2.1.1
Test items	Mobile application sensitive data collection Statement
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications" 4.1.2.1. Sensitive Data Collection
Technical requirements	Mobile application should get users' consent before collecting sensitive data
Test standards	If the mobile application has been released, check if sensitive data is being collected, data in trusted application stores or mobile application devices if the application obtains users' consent. If the mobile application has not been released or publicly available, check if there are instructions in the check list which expectes to declare the sensitive data collection statement in application stores and obtain users' consent statement. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet test standards, or mobile applications not collect sensitive data Non-Satisfied the requirements: not meet test standards NA: mobile applications are not publicly available; then this need not to be detected
Remark	The announcement of application store should base mainly on the interface of mobile device stores.

4.1.2.1.2. Mobile application should provide users the right to refuse to collect the sensitive data

TESTING ID	4.1.2.1.2
Test items	Mechanism for the user to refuse to provide sensitive data collection within the mobile application
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.1. Sensitive Data Collection
Technical requirements	Mobile application should provide users the right to refuse the collect of sensitive data
Test standards	(1) Check whether the mobile application provides users the option to refuse the collection of sensitive data. “Yes” is consistent with this item’s test baseline; "No" is not consistent with this item’s test baseline (2) When the user declines to collect sensitive data check if mobile applications do not collect sensitive data. “Yes” is consistent with this item’s test baseline; "No" is not consistent with this item’s test baseline
Test results	Satisfied the requirements: meet all the test standards, or sensitive data detected in the mobile application Non-Satisfied the requirements: any of the tests do not meet the standard, or not satisfy due to failing to declare sensitive data based on 4.1.2.1.1 NA: mobile applications are not publicly available; then this need not to be detected
Remark	4.1.2.1.1 benchmarking results in the testing of failing to declare all sensitive data will cause the user not to be able to refuse the sensitive

	data not declared

4.1.2.2. Sensitive Data Usage

" sensitive data usage" is for developer reference purposes only.

4.1.2.2.1 Before the mobile applications use sensitive data, they must get users' consent

This item is a reference item. See Appendix V.

4.1.2.2.2 Mobile application should provide users the right to refuse the use of sensitive data

This item is a reference item. See Appendix V.

4.1.2.2.3 If mobile applications use passcode authentication, they should take the initiative to remind the user to set more complex passcode

This item is a reference item. See Appendix V.

4.1.2.2.4 Mobile applications should remind users to regularly change the passcodes

This item is a reference item. See Appendix V.

4.1.2.3. Sensitive data Storage

For test items in "Sensitive data Storage", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" corresponding to criteria 4.1.2.3.4. Mobile application should avoid sensitive data stored in a redundant file or log files after close and logout ", " 4.1.2.3.6. sensitive data should be encrypted and stored with appropriate and effective key length and encryption algorithm", " 4.1.2.3.7. sensitive data should be stored in an area protected by the operating system, in order to prevent unauthorized access by other applications", " 4.1.2.3.8. sensitive data should be avoided in the mobile application's code ". The test result of level 2, 3 mobile applications have to be “Satisfied” corresponding to criteria 4.1.2.3.1 Mobile application should get the users’ consent before storing sensitive data", " 4.1.2.3.2 Mobile application should provide users the right to refuse the storage of sensitive data"; The test result of level 3 mobile applications have to be “Satisfied” corresponding to " 4.1.2.3.5 Mobile application should avoid redundant sensitive data stored in a log file or redundant file ", " 4.1.2.3.9. Mobile application should alert user when taking screenshot ". In order to meet the information security technical requirements; otherwise it fails.

4.1.2.3.1. Mobile application should get the users' consent before storing sensitive data

TESTING ID	4.1.2.3.1
Test items	Mobile application sensitive data storage Statement
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	Mobile application should get the users' consent before storing sensitive data
Test standards	(1) Check whether the mobile application declares in the application-store or mobile applications. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) Check whether the mobile application get the users' consent in trusted application stores or mobile applications. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (3) If the mobile application has not been released, check if there are instructions in the questionnaire expecting sensitive data stores statement in the application stores and obtain the users' consent. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Testing rules: (I.) Compliance with the testing baseline (1), (2) (II.) In line with the testing baseline (3)

	(III.) Mobile application does not store sensitive data Satisfied the requirements: meet one of the testing rules Non-Satisfied the requirements: not meet all testing rules NA: mobile applications are not publicly available; then this need not to be detected
Remark	The announcement of application store should base mainly on the interface of mobile device store.

4.1.2.3.2. Mobile application should provide users the right to refuse the storage of sensitive data

TESTING ID	4.1.2.3.2
Test items	Mobile application sensitive data storage
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	Mobile application should provide users the right to refuse the storage of sensitive data
Test standards	(1) Check whether the mobile application provides users the option to refuse to store sensitive data. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) If the user decline to store sensitive data, check whether mobile applications do not store sensitive data on mobile devices. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet all test standards, or the application does not store sensitive data Non-Satisfied the requirements: any of the tests do not meet the standard, or not satisfy due to failing to declare baseline on 4.1.2.3.1 NA: mobile applications are not publicly available; then this need not to be detected
Remark	Due to failing to declare the storage of sensitive data, the test result based on 4.1.2.3.1 may cause the user not to be able to refuse the

	sensitive data not declared.

4.1.2.3.3. Sensitive data stored in mobile applications, be use for declaration only

This item is a reference item. See Appendix V.

4.1.2.3.4 Mobile application should avoid sensitive data stored in a redundant file or log files after close and logout

TESTING ID	4.1.2.3.4
Test items	Mobile application sensitive data storage limit
Test category	Level 1, level 2
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	Mobile application should avoid sensitive data stored in a redundant file or log files after close and logout
Test standards	(1) Check the mobile applications to confirm if sensitive data is stored on redundant file after close and logout. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) Check the mobile applications to confirm if the sensitive data is stored in a log file after close and logout. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet all the test standards, or mobile applications do not store sensitive data Non-Satisfied the requirements: not meet any of the tests
Remark	No sensitive data should be detected in the area protected by the operating system

4.1.2.3.5. Mobile application should avoid redundant sensitive data stored in a log file or redundant file

TESTING ID	4.1.2.3.5
Test items	Mobile application sensitive data storage limit
Test category	Level 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	Mobile application should avoid redundant sensitive data stored in a log file or redundant file
Test standards	(1) Check if the mobile application is not detected sensitive data stored on redundant file. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) Check if the mobile application is not detected sensitive data stored in a log file. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (3) Check if the mobile application will sensitive data stored on redundant file or log files encrypted and protected with the security function. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet either test standards (1) or (2) and addition to test standards (3) Non-Satisfied the requirements: not meet both test standards (1) and (2) or not meet test standards (3)
Remark	No sensitive data should be detected in the area protected by the operating system

4.1.2.3.6. Sensitive data should be encrypted and stored with appropriate and effective key length and encryption algorithm

TESTING ID	4.1.2.3.6
Test items	Mobile application sensitive data protection
Test category	Level 1, level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	sensitive data should be encrypted and stored with appropriate and effective key length and encryption algorithm
Test standards	(1) Check if the sensitive data without redundant or log files in the mobile application adopts Advanced Encryption Standard (AES) and use effective key length of 128-bit or more. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) Check if the sensitive data with non-redundant files non log files in the mobile application adopts triple data encryption algorithm (Triple DES). “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (3) Check if the mobile applications encryption uses secure random number to generate. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet either test standards (1) or (2) and addition to test standards (3) Non-Satisfied the requirements: not meet both test standards (1) and (2) or not meet test standards (3)

Remark	No sensitive data should be detected in the protected area in the operating system

4.1.2.3.7. Sensitive data should be stored in an area protected by the operating system, in order to prevent unauthorized access by other applications

TESTING ID	4.1.2.3.7
Test items	Mobile application sensitive data stored Controls
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	Sensitive data should be stored in an area protected by the operating system, in order to prevent unauthorized access by other applications
Test standards	Check whether the mobile application store sensitive data in the preset inaccessible area in the other mobile applications area. “Yes” is consistent with the testing baseline; "No" is not compliant with standard testing
Test results	Satisfied the requirements: meet test standards, or mobile applications are not detected the storage of sensitive data Non-Satisfied the requirements: not meet test standards NA: If the store sensitive data purposes only detect benchmarking 4.1.2.3.4 of the results do not meet the entry does not have to detect
Remark	The forming condition is corresponding to 4.1.2.3.4 that storage of sensitive data should be detected. There will be no issue on the storage in the preset inaccessible area in other mobile applications.

4.1.2.3.8. Sensitive data should be avoided in the mobile application's code

TESTING ID	4.1.2.3.8
Test items	Mobile application sensitive data hard code (Hard Code)
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	Sensitive data should be avoided in the mobile application's code
Test standards	Check other files in the mobile application’s code and its installing files to confirm if no password is detected, identity verification information or symmetric key encryption algorithm of. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet test standards Non-Satisfied the requirements: not meet test standards
Remark	Hard code vulnerabilities type disclosed with reference to the CWE (CWE-259, CWE-321, CWE-798 e.g.)

4.1.2.3.9. Mobile application should alert user when taking screenshot

TESTING ID	4.1.2.3.9
Test items	Mobile application screen capture warning
Test category	Level 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.3. Sensitive data Storage
Technical requirements	Mobile application should alert user when taking screenshot
Test standards	Check if the mobile applications take the initiative to alert users when taking screenshot. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet test standards Non-Satisfied the requirements: not meet test standards
Remark	

4.1.2.4. Sensitive data Transmission

For test items in "Sensitive data transmission", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" corresponding to criteria 4.1.2.4.1. Mobile application transmitting sensitive data through the internet should be securely encrypted by using appropriate and effective key length of the encryption algorithms". In order to meet the information security technical requirements; otherwise it fails.

4.1.2.4.1. Mobile application transmitting sensitive data through the internet should be securely encrypted by using appropriate and effective key length of the encryption algorithms

TESTING ID	4.1.2.4.1
Test items	Mobile application sensitive data transmission
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.4. Sensitive data Transmission
Technical requirements	Mobile application transmitting sensitive data through the internet should be securely encrypted by using appropriate and effective key length of the encryption algorithms

Test standards	(1) Check whether mobile applications with TLS 1.1 (included) or higher encryption protocol transmit sensitive data. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) Check whether the mobile application use with the effective key length of 2048 bits (or more) of the RSA encryption algorithm, or an effective length of 224 bits (or more) encryption algorithm of the Elliptic Curve Cryptography. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (3) Check whether mobile applications use with the effective key length of 128 bits (or more) of the Advanced Encryption Standard (AES), or triple data encryption algorithm (Triple DES). “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet all meaning Test standards, or mobile applications do not transmit sensitive data Non-Satisfied the requirements: not meet either of the tests
Remark	With reference to the announcement in December 2015 on lengthening the expiration date of TLS 1.0 on Payment Card Industry Security Standards Council (PCI SSC) (https://blog.pcisecuritystandards.org/migrating-from-ssl-and-early-tls), by 30th June 2018, mobile applications that do not support the operating system using TLS 1.1 (inclusive) or more, support the use of TLS 1.0, but still cannot support using SSL v3.0 (inclusive). If the Testing Laboratory detects TLS 1.0, the laboratory should add comments in the report and ask the developer stop using it after 1st July 2018. And meanwhile, mobile applications not supporting the operation system with TLS 1.1 (inclusive) or more, cannot be detected to support TLS 1.0. Developers should develop supporting policies and measures.

4.1.2.5. Sensitive data Sharing

For test items in "Sensitive data sharing", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" corresponding to " 4.1.2.5.3. Mobile application should prevent unauthorized access from other applications when sharing sensitive data"; The test result of level 2, 3 mobile applications have to be "Satisfied" corresponding to criteria 4.1.2.5.1. Different mobile devices within their mobile applications should get users' consent when sharing the sensitive data ", " 4.1.2.5.2. Mobile application should provide users with the right to refuse to share the sensitive data". In order to meet the information security technical requirements; otherwise it fails.

4.1.2.5.1. Different mobile devices within their mobile applications should get users' consent when sharing the sensitive data

TESTING ID	4.1.2.5.1
Test items	Mobile application sensitive data shared statement
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.5. Sensitive data Sharing
Technical requirements	Different mobile devices within their mobile applications should get users' consent when sharing the sensitive data
Test standards	(1) Check if the mobile applications declare in the mobile applications or trusted application stores when sharing sensitive data within the mobile device. "Yes" is consistent with this item's testing baseline; "No" is not consistent with this item's testing baseline (2) Check if the mobile applications get the users' consent before sharing sensitive data within the mobile device, if the user has agreed to allow the sensitive data sharing. "Yes" is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet all the test standards, or mobile applications do not share sensitive data Non-Satisfied the requirements: not meet either of the test standards NA: If mobile applications has not been released or publicly available, and is not provided by a mobile application; then this need not to be detected
Remark	

4.1.2.5.2. Mobile application should provide users with the right to refuse to share the sensitive data

TESTING ID	4.1.2.5.2
Test items	Mobile application users refuse to provide sensitive data-sharing mechanism
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications" 4.1.2.5. Sensitive data Sharing
Technical requirements	Mobile application should provide users with the right to refuse to share the sensitive data
Test standards	(1) Check whether the mobile application provides users the option to refuse to share the sensitive data. “Yes” is consistent with this test item; "No" is not consistent with this test item (2) Check if the user refuses to share sensitive data, and the mobile application does not share sensitive data. Accordingly, “Yes” is consistent with this test item; "No" is not consistent with this test item
Test results	Satisfy the requirements: meet all the test standards, or mobile applications do not share sensitive data Non-Satisfied the requirements: do not meet either of the test standards NA: If the mobile applications has not released or publicly available and a mobile application is not provided; then this need not to be detected
Remark	No

4.1.2.5.3. Mobile applications should prevent unauthorized access from other applications when sharing sensitive data

TESTING ID	4.1.2.5.3
Test items	Mobile application sensitive data sharing permission management
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.2.5. Sensitive data Sharing
Technical requirements	Mobile applications should prevent unauthorized access from other applications when sharing sensitive data
Test standards	Check if mobile application sharing sensitive data confine specific mobile applications to access sensitive data. “Yes” is consistent with the test item; "No" is not in line with test item.
Test results	Satisfied the requirements: meet test standards, or mobile applications are not sharing sensitive data. Non-Satisfied the requirements: do not meet test standards
Remark	No

4.1.2.6. Sensitive data Deletion

" Sensitive data Deletion" belong to the reference testing, which is for developer reference only.

4.1.2.6.1. The function of deletion should be provided if mobile application store user's sensitive data

This item is a reference item. Please see "Appendix V".

4.1.3. Transaction Resources Security Controls

This is mainly used for the related information security testing standard for Transaction Resources Controls, including the use and controls of transaction resources.

4.1.3.1. Use of Transaction Resources

For the test items in "Use of Trading Resources", the test results of level 3 mobile applications have to be "Satisfied" with reference to criteria 4.1.3.1.1. Mobile applications should inform users before using Transaction Resources". The test result should be “Satisfied” so as to meet the security information technical requirements; otherwise, it fails.

4.1.3.1.1. Mobile applications should take the initiative to inform users before using transaction resources

TESTING ID	4.1.3.1.1.
Test items	Claim of using transaction resources of mobile applications
Test category	Level 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.3.1. Use of Transaction Resources
Technical requirements	Mobile application should inform users before using transaction resources
Test standards	Check whether the mobile application actively informs the user before the transaction, and the information should at least include the name, amount and transaction method of the transaction resource. "Yes", meets the test item; if No, it is not consistent with the test item.
Test results	Satisfied the requirements: meet test standards or no transaction in this application Non-Satisfied the requirements: do not meet the test standards

Remark	Before using of the transaction resources as described in the regulation, is defined as "before the transaction", that is, whether the mobile application take the initiative to informs the user before the transaction.

4.1.3.1.2 Mobile applications should provide users with the right to refuse to use the transaction resources

TESTING ID	4.1.3.1.2
Test items	Mobile applications reject the transaction resource use mechanisms
Test category	Level 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.3.1. Use of Trading Resources
Technical requirements	Mobile application should provide users with the right to refuse to use the transaction resources
Test standards	(1) When mobile applications transact, check whether users are offered the option to reject the transaction. "Yes" is consistent with this test item; "No" is not consistent with this test item (2) Check if the mobile application is processing transaction when the user refuse to transact. "Yes" is consistent with this test item; "No" is not consistent with this test item
Test results	Satisfied the requirements: meet all the test standards or no transaction in this application. Non-Satisfied the requirements: do not meet either of the test standards.

Remark	

4.1.3.2. Transaction Resource Controls

For test items in "Transaction Resource Controls", the test results of level 3 mobile applications have to be "Satisfied" with reference to criteria 4.1.3.2.1. Mobile application should verify the user identity before using transaction resources", criteria 4.1.3.2.2.Mobile applications should record trading resources and time". The test result should be “Satisfied” so as to meet the security information technical requirements; otherwise, it fails.

4.1.3.2.1. Mobile application should verify the user identity before using trading resources

TESTING ID	4.1.3.2.1
Test items	Mobile applications transaction resources user’s identity authentication
Test category	Level 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.3.2.Trading Resources Control
Technical requirements	Mobile applications should verify the user’s identity before using trading resources
Test standards	Check if the mobile application provides identity authentication mechanism at the time of the transaction.
Test results	Satisfied the requirements: meet the test standards, or no transaction function in the mobile application Non-Satisfied the requirements: do not meet the test standards
Remark	"Regulations" "Before using transaction resources" as described in the regulations is defined as “at the time of transaction”; that is whether the mobile application verifies the user’s identity before the

	transaction. The identity authorization will be processed for the first transaction, no more identity authorization needed afterwards.

4.1.3.2.2. Mobile applications should record transaction resources and time

TESTING ID	4.1.3.2.2
Test items	Mobile application transaction resource record
Test category	Level 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.3.2. Transaction Resources Control
Technical requirements	Mobile applications should record transaction resources and time
Test standards	When the mobile application accesses the personal sensitive data, check whether the application provides the channel to search for the transaction resources records which should at least include at least transaction resource name, recording time and the transaction amount of the transaction. “Yes” is consistent with the testing baseline; "No" is not in line with test standards
Test results	Satisfied the requirements: meet the test standards, no transaction resources in the mobile application. Non-Satisfied the requirements: do not meet test standards
Remark	"Transaction time and resources," in the regulation is defined as "Transaction record", that is, to check whether the mobile application provides the content and records of transactions

4.1.4. User Identity Authentication, Authorization and Connection Management Security

This applies mainly for the testing standard related to identity authentication, authorization and connection management for mobile application, including the user identity authentication and authorization and connection management mechanism.

4.1.4.1. User Identity Authentication and Authorization

For test items in " User Identity Authentication and Authorization", the test result of level 2, 3 mobile applications have to be "Satisfied" with reference to criteria 4.1.4.1.1. Mobile applications should have an appropriate authentication mechanism to identify the user", criteria 4.1.4.1.2 Mobile applications authorize users by user’s identity". The test result should be "Satisfied" so as to meet the security information technical requirement; Otherwise it fails.

4.1.4.1.1. Mobile applications should have an appropriate authentication mechanism to identify the user

TESTING ID	4.1.4.1.1
Test items	Mobile application user identity authentication mechanism
Test category	Level 2, 3
Test basis	"Basic Information Security Regulation for Mobile Applications." 4.1.4.1. User Identity Authentication and Authorization
Technical requirements	Mobile applications should have an appropriate authentication mechanism to identify the user
Test standards	As mobile applications need to access sensitive data related to personal data, check whether the mobile applications provide authentication mechanism. “Yes” is consistent with this test item; "No" is not consistent with this test item

Test results	Satisfy the requirements: meet the test standards, or no access to users' personal sensitive data in the application Non-Satisfied the requirements: do not meet the test standards NA: If the authorities have agreed to waive identity authentication and authorization; then this need not to be detected
Remark	No

4.1.4.1.2 Mobile applications should authorize users by user’s identity

TESTING ID	4.1.4.1.2
Test items	Mobile application user identity Authorization
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.4.1. User Identity Authentication and Authorization
Technical requirements	Mobile application should be authorized by user’s identity
Test standards	As mobile applications need to access sensitive data related to personal data, check whether the mobile applications provide identity authorization mechanism. "Yes" is consistent with this test item; "No" is not consistent with this test item
Test results	Satisfied the requirements: meet the test standards, or no access to users’ personal sensitive data in the application Non-Satisfied the requirements: do not meet the test standards NA: If the authorities have agreed to waive identity authentication and authorization; then this need not to be detected
Remark	No

4.1.4.2. Connection Management Mechanism

For test items in "Connection Management Mechanism", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" with reference to criteria 4.1.4.2.2. Mobile application should confirm the validity of the server certificate", criteria 4.1.4.2.3Mobile application should ensure that the server certificate is issued by the trusted certificate authority ", criteria 4.1.4.2.4. Mobile application should avoid connecting and transmitting data with servers without valid certificate"; The test result of level 2, 3 mobile applications have to be "Satisfied" against criteria 4.1.4.2.1 Mobile application should avoid using regular conversation identifiers". The test result should be "Satisfied" so as to meet the security information technical requirements; otherwise it fails.

4.1.4.2.1 Mobile application should avoid using regular communicating identification code

TESTING ID	4.1.4.2.1
Test items	Mobile application ID rules of conversation
Test category	Level 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.4.2. Connection Management Mechanism
Technical requirements	Mobile application should avoid using unencrypted communication to transmit identification code

Test standards	(1) Check whether the mobile application is using the session identification code with length of 128 bits (or more) with secured transmission. “Yes” is consistent with this test item; "No" is not consistent with this test item (2) Check whether the session in the mobile application does not associate with time, information submitted by the user, number of string with identifiable patterns or is difficult to counterfeit. “Yes” is consistent with this test item; "No" is not consistent with this test item (3) Check if the communicating identification code of the mobile application equals with the log-out failure mechanism. “Yes” is consistent with this test item; "No" is not consistent with this test item
Test results	Satisfy the requirements: meet the test standards or no session identification code in the mobile application Non-Satisfied the requirements: do not meet either of the test standards
Remark	The session identification code in the testing standard is used after the user’s identity authorization

4.1.4.2.2 Mobile applications should confirm the validity of the server certificate

TESTING ID	4.1.4.2.2
Test items	Mobile application server certificate validity
Test category	Level 1, 2, 3
Test basis	"Basic Information Security Regulation for Mobile Applications." 4.1.4.2. Connection Management Mechanism
Technical requirements	Mobile applications should confirm the validity of the server certificate
Test standards	(1) Check whether the server certificate of the mobile application is still valid, not revoked, and the title and subtitle of the certificate contains the domain name of the connected server. “Yes” is consistent with this test item; "No" is not consistent with this test item (2) Check whether the mobile applications use certificate pinning for verification to ensure the connection of the server is specified by mobile application developers. “Yes” is consistent with this test item; "No" is not consistent with this test item
Test results	Satisfied the requirements: meet all the test standards, or no need to use secure encrypted transmission protocol in the mobile application Non-satisfy the requirements: do not meet any of the testing standard
Remark	No

4.1.4.2.3 Mobile application should ensure that the server certificate is issued by the trusted certificate authority

TESTING ID	4.1.4.2.3
Test items	Mobile application server certificate validity
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.4.2. Connection Management Mechanism
Technical requirements	Mobile application should ensure that the server certificate is issued by the trusted certificate authority
Test standards	If mobile applications use secure encrypted transmission protocol, check whether the mobile application is verified and at the same time ensure the server certificate is issued by the trusted certificate institutions built in the operation system. “Yes” is consistent with this test item; "No" is not consistent with this test item
Test results	Satisfied the requirements: meet the test standards, or the mobile application is not using secure encrypted transmission protocol Non-Satisfied the requirements: do not meet the test standards
Remark	The built-in trusted certificate institution in the operation system are installed by the operation system developer

4.1.4.2.4 Mobile applications should avoid connecting and transferring data with servers without valid certificate

TESTING ID	4.1.4.2.4
Test items	Mobile application connection security
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.4.2. Connection Management Mechanism
Technical requirements	Mobile applications should avoid connecting and transferring data with servers without valid certificate
Test standards	(1) If the mobile application does not meet the technical requirements for 4.1.4.2.2 check whether the mobile application is connected with the server to connect and transmit the sensitive data. “Yes” is consistent with the testing standard; "No" is not in line with testing standard (2) Check whether the mobile applications uses the certificate in accordance with 4.1.4.2.2 to connect and transmit the sensitive data. “Yes” is consistent with the testing standard; "No" is not in line with testing standard
Test results	Satisfied the requirements: meet either of the test standards, or the mobile application use secure encrypted transmission protocol. (no need to transmit sensitive data) Non-Satisfied the requirements: not meet all the test standards
Remark	No

4.1.5. Mobile Application Security Code

This mainly applies to the relevant security testing of standards for developing mobile application, including protection corresponding to malicious code and prevent information security vulnerabilities, mobile applications integrity, reference library security and user input validation.

4.1.5.1. Protection corresponding to Malicious Code and Prevention for Information Security Vulnerabilities

For test items in "Protection corresponding to Malicious Code and Prevention for Information Security Vulnerabilities", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" corresponding to criteria 4.1.5.1.1. Mobile application should avoid containing malicious code", " 4.1.5.1.2. Mobile application should avoid information security vulnerabilities". In order to meet the information security technical requirements; otherwise it fails.

4.1.5.1.1. Mobile application should avoid containing malicious code

TESTING ID	4.1.5.1.1
Test items	Mobile application malicious code
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.5.1. Protection corresponding to Malicious Code and Prevention for Information Security Vulnerabilities
Technical requirements	Mobile application should avoid containing malicious code

Test standards	(1) Examining whether non-mobile applications, when not authorized, try to query, add, modify, delete, access to remote servers, and privileges escalate while not to casing on other mobile applications and operation system files. “Yes” is consistent with the test standards; "No" is not in line with test standards (2) Check if mobile applications are not leading to the occurrence of unexpected errors, obvious resource depletion, restart or shut down in mobile operating system. “Yes” is consistent with the test standards; "No" is not in line with test standards
Test results	Satisfied the requirements: meet either of the test standards Non-Satisfied the requirements: not meet all the test standards
Remark	No

4.1.5.1.2. Mobile application should avoid information security vulnerabilities

TESTING ID	4.1.5.1.2
Test items	Mobile application information security vulnerabilities
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.5.1. Protection corresponding to Malicious Code and Prevention for Information Security Vulnerabilities
Technical requirements	Mobile application should avoid information security vulnerabilities
Test standards	Check the mobile applications to confirm if there are non-existing security vulnerabilities. "Yes" is consistent with the test standards; "No" is not in line with test standards
Test results	Satisfied the requirements: meet either of the test standards Non-Satisfied the requirements: not meet all the test standards
Remark	The vulnerability which does not meet the test standards is that with a CVE number and CVSS v3.0 score 7 (a severity rating of High or Critical). TLS 1.0 related vulnerabilities by 30th June, 2018 do not apply to this test item.

4.1.5.2. Mobile Application Integrity

For test items in "Mobile Application Integrity" belong to reference items, it is for developers reference only.

4.1.5.2.1. Mobile application should use appropriate and effective mechanism to verify the integrity, to ensure its integrity

This is a reference item, see Appendix V.

4.1.5.3. Reference Library Security

For test items in "Reference Library Security", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" corresponding to criteria 4.1.5.3.1. When updating the reference library of mobile applications, they should prepare for an updated version. Please refer to 4.1.1. Mobile application release security for updating methods". In order to meet the information security technical requirements; otherwise it fails.

4.1.5.3.1. When updating the reference library of mobile applications, they should prepare for an updated version. Please refer to 4.1.1. Mobile application Release Security for updating methods

TESTING ID	4.1.5.3.1
Test items	Mobile application reference library security
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.5.3. Security Reference Library
Technical requirements	When updating the reference library of mobile applications, they should prepare for an updated version. Please refer to 4.1.1. Mobile application Release Security for updating methods
Test standards	(1) Check the mobile application reference library to confirm if there are non-existing security vulnerabilities. “Yes” is consistent with the test standards; "No" is not in line with test standards (2) Before installing check if there are warnings on the mobile application store display recommending that users to install the latest version of the operating system. “Yes” is consistent with the test standards; "No" is not in line with test standards

Test results	Satisfied the requirements: meet either of the test standards Non-Satisfied the requirements: not meet all the test standards
Remark	The vulnerability which does not meet the test standards is that with a CVE number and CVSS v3.0 score 7 (a severity rating of High or Critical). TLS 1.0 related vulnerabilities by 30th June, 2018 do not apply to this test item. it is required to self-declare the name and version of the reference library in "Appendix III".

4.1.5.4. User Input Validation

For the test items in "User input validation", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" corresponding to criteria 4.1.5.4.1. Mobile applications should perform security checks on the user's input strings", criteria 4.1.5.4.2 Mobile applications should provide an injection attack protection mechanism". In order to meet the information security technical requirements; otherwise it fails.

4.1.5.4.1. Mobile applications should perform security checks on the user's input strings

TESTING ID	4.1.5.4.1
Test items	Mobile application users input validation
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.5.4. User Input Validation
Technical requirements	Mobile applications should perform security checks on the user's input strings
Test standards	(1) Check if the mobile application can verify the type for the expected input strings, for example if the column need to accept special characters, this also belongs to the expected user's input string type. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) Check if the mobile application can verify the length of the user's input string. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline
Test results	Satisfied the requirements: meet all the test standards or the mobile application does not provide the interface for string input.

	Non-Satisfied the requirements: not meet either of the test standards
Remark	No

4.1.5.4.2. Mobile application should provide an injection attack protection mechanism

TESTING ID	4.1.5.4.2
Test items	Mobile application injection attack protection mechanism
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications." 4.1.5.4. User Input Validation
Technical requirements	Mobile application should provide an injection attack protection mechanism

Test standards	(1) Check whether a mobile application is designed to protect the user inputs a string of SQL Injection. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (2) Check whether a mobile application is designed to protect the user to enter a string of JavaScript Injection. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (3) Check whether a mobile application is designed to protect the user to enter a string of Command Injection. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (4) Check whether a mobile application is designed to protect the user to enter a string of Local File Inclusion. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (5) Check whether a mobile application is designed to protect the user to enter a string of XML Injection. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (6) Check whether the mobile application is designed to protect the user to enter a string of Format String Injection. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline (7) Check whether the mobile application is designed to protect the user to enter a string of IPC (Inter process communication) Injection. “Yes” is consistent with this item testing baseline; "No" is not consistent with this item testing baseline

Test results	Satisfied the requirements: meet all the test standards or the mobile application does not provide the interface for string input. Non-Satisfied the requirements: not meet either of the test standards
Remark	New methods of attack afterwards will also be included in the testing baseline. Effective injection attack protection mechanism for the user to input the string should be processed on the server-side. Based on the concept of defense in depth, and the applicability of this testing baseline for mobile applications, the laboratory must at least detect if there is protection design for the input injection attack strings.

4.2. Server-side Basic Information Security Baseline

According to the "Basic Information Security Regulations for Mobile Application", Section 4.2 describes: "This regulation is intended to put forward the basic information security requirements for mobile applications. If mobile applications involving the need of information security on the server-side, it is suggested that the industry should self-declare or decide its server-side protection and information security management measures, or issue the third-party certificate technology requirements to prove the information security and management of this sever-side service.". Since the suggestion is not mandatory, 4.2.2.1. WebView Security Testing is enacted to be the new baseline.

This section provides mobile application basic information security test standards to process testing on the server-side. please refer to 4.2.2 server-side security management for details.

4.2.1. Server-side Security Management

Server-side security is suggested to provide applications and services to do threat analysis on the application and service, to identify security risks caused by the service, in order to implement the necessary follow-up and effective control measures. If the server-side rents an IDC room, a host (including virtual server) or cloud-type service program, it is recommended to pass the relevant information security management standards such as: ISO / IEC 27001, " Security, Trust & Assurance Registry" or "EuroCloud star Audit (ECSA)" of Cloud Security Alliance.

4.2.2. Server-side Security Testing

Server-side is a mobile application platform for mobile application. Because the access interface it provided is mobile applications rather than interface accessed directly by the user, it is easy for developers to ignore the server-side security precautions. The essence of Mobile application platform websites and Web Service server. If there is no proper security design and development, there will be vulnerabilities like traditional website applications. Therefore, to the server-side testing security, the developer may use penetration test mode for the testing. The current credible international penetration test files are:

- OWASP Testing Guide in OWASP (Open Web Application Security Project)

  https://www.owasp.org/index.php/Category:OWASP_Testing_Project

- OSSTMM (Open Source Security Testing Methodology Manual) in ISECOM (the Institute for Security and Open Methodologies)

  http://www.isecom.org/research/osstmm.html

- The penetration test related documents in SANS (System Administration, Networking, and Security Institute)

  http://pen-testing.sans.org/

4.2.2.1. WebView Security Testing

For test items in "WebView security testing", the test result of level 1, 2, 3 mobile applications have to be "Satisfied" corresponding to "The connection should be in secure domain when WebView is using on mobile applications". In order to meet the information security technical requirements; otherwise it fails.

4.2.2.1.1. WebView of mobile applications should be used to exchange the website resource with the remote server

This item is a reference item. See Appendix V.

4.2.2.1.2. The connection should be secure domain when WebView is using on mobile applications

TESTING ID	4.2.2.1.2
Test items	WebView security testing of mobile applications
Test category	Level 1, 2, 3
Test basis	"Basic Security Baseline for Mobile Applications" 4.2.2.1 WebView Security Testing
Technical requirements	The connection should be secure when WebView is using on mobile applications
Test standards	(1) Check if the connection is in secure domain and is consistent with the actual connection claimed in the questionnaire by the developer when the mobile WebView is functioning. “Yes” is consistent with the test standards; "No" is not in line with test standards (2) When the mobile applications WebView is functioning, check whether the connection is processing certificate pinning. “Yes” is consistent with the test standards; "No" is not in line with test standards (3) When the mobile applications WebView is functioning check whether the application uses HTTPS connection. “Yes” is consistent with the test standards; "No" is not in line with test standards (4) When the mobile applications WebView is functioning check if all test items of vulnerability scanning pass. “Yes” is consistent with the test standards; "No" is not in line with test standards
Test results	Satisfied the requirements: meet all the test standards, or no connection in WebView. Non-Satisfied the requirements: not meet any of defection standard reference NA: mobile applications without WebView function

Remark	For a detailed description of the vulnerability scanning, refer to "6. Supplement (a)."

5. Testing Methods

This testing test is based mainly on the case without obtaining source code. when implementing most mobile applications can be detected with automatic tools. Some may need manual testing after obtaining the source code by reverse engineering. Then, we use the source scanning tool for scanning and then do the manual analysis. Because mobile applications basic security testing is mainly a black-box detecting, the testing methods mentioned in this chapter is a introduction of concept. The details of testing methods, environment, and other implementations would be developed by each development laboratory. The testing methods are described as follows.

5.1. Automatic Testing

The main testing types include:

- User interface-oriented: Based on user interface the automatic testing is processed, including the user operation of automation, screenshots. This can be used on test stage.
- Data-oriented: It can automatically identify fields or labels of the test data, transfer or fill-in different data and track and respond to the results through data flows, to determine the possible existence of security issues.

5.2. Manual Testing

Static and dynamic analysis is used together. According to the demand of testing, it may use reverse engineering or man-in-the-middle attacks to carry out.

5.2.1. Static Analysis

Static analysis is to get the source code manually or by using tool to disassemble the Binary code so as to access sensitive data, Mobile resources, such as Androidmanifest.xml, iOS Entitlements, WMAppManifest.xml. It checks whether the required permission follows "Appendix III"; it also checks whether the reference library version exists common weaknesses and vulnerabilities, or if there are improper reference libraries. For example: when using a browser with known vulnerabilities in reference library to visit a malicious website, a malicious website may result in vulnerabilities on sensitive data. It checks whether sensitive data is using appropriate and valid encryption algorithm and key length, to encrypt and then stored. It checks whether source code can identify the sensitive data after the reverse engineering. It also checks whether sensitive data stores in Cache Files or Log Files, and confirm the existing vulnerabilities or security problems.

5.2.2. Dynamic Analysis

Dynamic analysis includes the dynamic user input, data or parameters while testing, in order to analyze the behavior or the state of the different phase of the testing. Dynamic analysis can detect in the emulator, physical devices, remote connections, network access state, data transmission and other behavior. This may be applied to checking sensitive data transmission and storage, whether appropriate and effective use of the encryption algorithm and key length for secure encryption. For example, packet sniffing, log inspection system, etc. In the execution of the program, it checks whether identifiable sensitive data exist; whether sensitive data should be stored in a protected region in the operating system. For example: after the program execution, it checks whether sensitive data exist in SD card or shared access area.

5.3. Code Analysis

Analyzing the code by reverse engineering can get the source code using a scanning tool, and then check manually.

5.4. Binary Code Analysis

Binary code can be divided into Byte-code and machine code. According to different types of binary code analysis, there should be appropriate virtual machines, physical devices to detect manually or with automatic tools.

6. Supplement

(A) For test items 4.2.2.1.2, each laboratory must provide information about scanning vulnerability on the server side, and note the corresponding scanning vulnerability test items in the report. Among them, scanning vulnerabilities can be detected by each laboratory, or by the trusted third-party commissioned by the laboratory. If there is any version change of the server web pages during the valid period of certificate and mark, the developer is obliged to do proactive notification to the laboratory for doing the vulnerability scan again. To all this, the laboratory should collect the problem and note in a specific section in the testing report.

Remarks:

i. Any server-side change required to be detected again. All the test items in this baseline as well as vulnerability scanning have to be detected again while any server-side change occurs.

7. Test results and Outputs

The test results contain all the records in the test process, and should be judged in accordance with Section 4 “the information security technical requirements”, that is the results of the testing standard should be "Satisfied" or "non-Satisfied". The test results and outputs should include, but not be limited to:

- Testing target
- Declaration of testing scope
- Testing timeline
- Testing methods, environment and tools
- Testing executive person and his responsibilities
- Test judgment of "Satisfied" or "non-Satisfied" the requirements
- The report should provide testing records, supporting evidence and the test items which do not meet the requirements

8. Reference Materials

[1] Mobile Application basic information security norm, Ministry of Economic Affairs, 20th April 2015

[2] Personal Data Protection Act, 30th December 2015

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

[4] Technical Guide to Information Security Testing and Assessment, NIST Special Release 800-115, http://csrc.nist.gov/releases/nistpubs/800-115/SP800-115.pdf, 2008

[5] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Release 800-131A, http://csrc.nist.gov/releases/nistpubs/800-131A/sp800-131A.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 mobile smart terminal security capabilities, YD/T 2407-2013, 2013

[9] Mobile smart mobile terminal security capability test method, YD / T 2408-2013, 2013

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

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

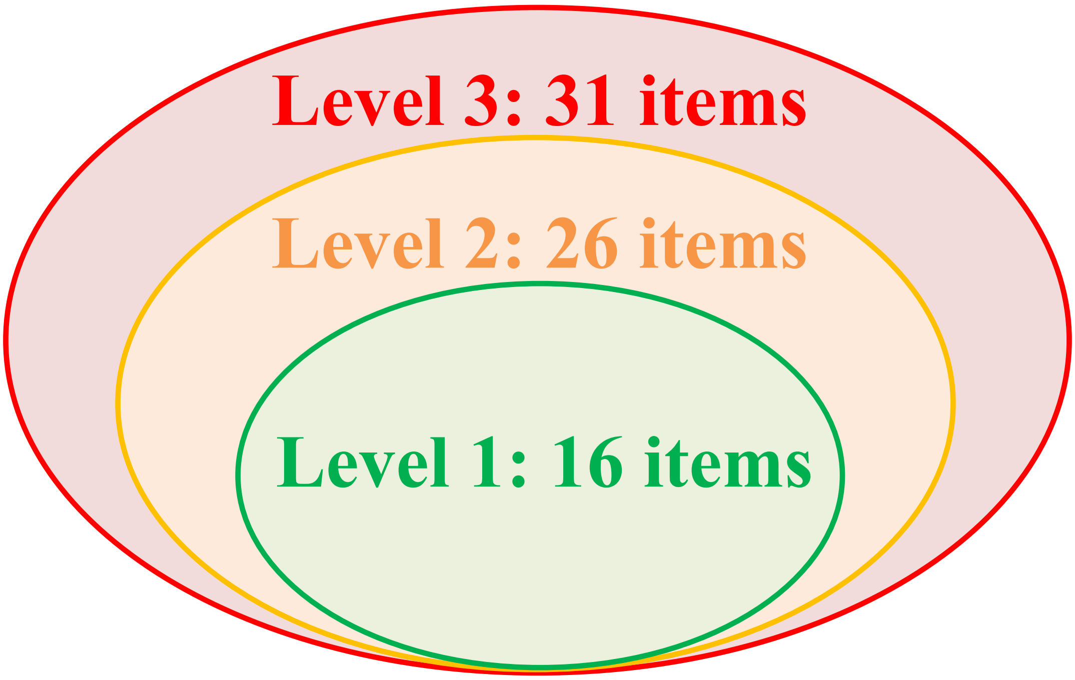
[12] Device Administration - Minimum password length, http://developer.android.com/guide/topics/admin/device-admin.html

[13] Mobile Application Security Checklist 0.9.3, https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main

9. Appendix

Appendix I, Classification of the Security Testing for Mobile Applications

The mobile application developers are required to declare the purpose, functions, and permissions of the mobile application in the check list when testing the mobile application.



Appendix II, Inspection Item of the Mobile Application Basic Security

"★" means the inspection item; "-" denotes the reference.

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
4.1.1. Mobile Application Release Security	4.1.1.1. Mobile Application Release	-	-	-	4.1.1.1.1. Mobile applications shall be released in trusted application stores
		-	★	★	4.1.1.1.2. Mobile application should be noted the sensitive data accessed, the mobile device resources and the declaration of the permissioned purposes of use at the time of release
	4.1.1.2. Mobile Application	-	-	-	4.1.1.2.1. Mobile applications shall be released the updates in trusted application stores

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
	Update	-	-	-	4.1.1.2.2. Mobile applications should provide an update mechanism
		-	-	-	4.1.1.2.3. Mobile applications should notify actively when security updates
	4.1.1.3. Mobile Application Security Issues In Return	-	★	★	4.1.1.3.1. Mobile application developers should provide a channel of return on security issues
		-	-	-	4.1.1.3.2. Mobile application developers should respond and improve the problem within a reasonable period
4.1.2. Protection of Sensitive data	4.1.2.1. Sensitive data Collection	-	★	★	4.1.2.1.1. Mobile application should get users' consent before collecting sensitive data

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
		-	★	★	4.1.2.1.2. Mobile application should provide users the right to refuse to collect the sensitive data
	4.1.2.2. Sensitive data Usage	-	-	-	4.1.2.2.1. Before the mobile applications use sensitive data, they must get users' consent
		-	-	-	4.1.2.2.2. Mobile application should provide users the right to refuse the use of sensitive data
		-	-	-	4.1.2.2.3. If mobile applications use passcode authentication, they should take the initiative to remind the user to set more complex passcode
		-	-	-	4.1.2.2.4. Mobile applications should remind users to regularly change the passcodes

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
	4.1.2.3. Sensitive data storage	-	★	★	4.1.2.3.1. Mobile application should get the users' consent before storing sensitive data
		-	★	★	4.1.2.3.2. Mobile application should provide users the right to refuse the storage of sensitive data
		-	-	-	4.1.2.3.3. Sensitive data stored in mobile applications, be use for declaration only
		★	★	-	4.1.2.3.4. Mobile application should avoid sensitive data stored in a redundant file or log files after close and logout
		-	-	★	4.1.2.3.5. Mobile application should avoid redundant sensitive data stored in a log file or redundant file

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENT S ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
		★	★	★	4.1.2.3.6. Sensitive data should be encrypted and stored with appropriate and effective key length and encryption algorithm
		★	★	★	4.1.2.3.7.Sensitive data should be stored in an area protected by the operating system, in order to prevent unauthorized access by other applications
		★	★	★	4 .1.2.3.8. Sensitive data should be avoided in the mobile application's code
		-	-	★	4.1.2.3.9. Mobile application should alert user when taking screenshot

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
	4.1.2.4. Sensitive data Transmission	★	★	★	4.1.2.4.1. Mobile application transmitting sensitive data through the internet should be securely encrypted by using appropriate and effective key length of the encryption algorithms
	4.1.2.5. Sensitive data Sharing	-	★	★	4.1.2.5.1. Different mobile devices within their mobile applications should get users' consent when sharing the sensitive data
		-	★	★	4.1.2.5.2. Mobile application should provide users with the right to refuse to share the sensitive data
		★	★	★	4.1.2.5.3. Mobile applications should prevent unauthorized access from other applications when sharing sensitive data

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
	4.1.2.6. Sensitive data Deletion	-	-	-	4.1.2.6.1. The function of deletion should be provided if mobile application store user's sensitive data
4.1.3. Transaction Resources Security Controls	4.1.3.1. Use of Transaction Resources	-	-	★	4.1.3.1.1. Mobile applications should take the initiative to inform users before using transaction resources
		-	-	★	4.1.3.1.2. Mobile applications should provide users with the right to refuse to use the transaction resources
	4.1.3.2. Transaction	-	-	★	4.1.3.2.1. Mobile application should verify the user identity before using trading resources

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENT S ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
	Resources Control	-	-	★	4.1.3.2.2. Mobile applications should record transaction resources and time
4.1.4. User Identity Authentication, Authorization and Connection Management Security	4.1.4.1. User Identity Authentication and Authorization	-	★	★	4.1.4.1.1. Mobile application should have an appropriate identity authentication mechanism to confirm user identity
		-	★	★	4.1.4.1.2. Mobile applications should authorize users by user’s identity
	4.1.4.2. Connection Management Mechanism	★	★	★	4.1.4.2.1. Mobile application should avoid using regular communicating identification code
		★	★	★	4.1.4.2.2. Mobile applications should confirm the validity of the server certificate

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
		★	★	★	4.1.4.2.3. Mobile application should ensure that the server certificate is issued by the trusted certificate authority
		★	★	★	4.1.4.2.4. Mobile applications should avoid connecting and transferring data with servers without valid certificate
4.1.5. Mobile Application	4.1.5.1. Protection corresponding to	★	★	★	4.1.5.1.1. Mobile application should avoid containing malicious code

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
Security Code	Malicious Code and Prevention for Information Security Vulnerabilities	★	★	★	4.1.5.1.2. Mobile application should avoid information security vulnerabilities
	4.1.5.2. Mobile Application Integrity	-	-	-	4.1.5.2.1. Mobile application should use appropriate and effective mechanism to verify the integrity, to ensure its integrity
	4.1.5.3. Reference Library Security	★	★	★	4.1.5.3.1. When updating the reference library of mobile applications, they should prepare for an updated version. Please refer to 4.1.1. Mobile application release security for updating methods

INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS DIRECTIONS	INFORMATION SECURITY TECHNOLOGY SATISFIED THE REQUIREMENTS ITEMS	ALL CLASS OF MOBILE APPLICATION NEED TO MEET THE TEST ITEMS			SKILLS REQUIREMENT
		LEVEL 1	LEVEL 2	LEVEL 3	
	4.1.5.4. User Input Validation	★	★	★	4.1.5.4.1. Mobile applications should perform security checks on the user's input strings
		★	★	★	4.1.5.4.2. Mobile application should provide an injection attack protection mechanism
4.2.2. Server-side Security Testing	4.2.2.1. WebView Security Testing	-	-	-	4.2.2.1.1. WebView of mobile applications should be used to exchange the website resource with the remote server
		★	★	★	4.2.2.1.2. The connection should be secure domain when WebView is using on mobile apps

Appendix III, Questionnaire on Security Testing for Mobile Applications

※ This form should be filled out in accordance with the information disclosed on the application store.

NO	ITEM		CONTENT
1.	Name of Department		
2.	Contact Information		
3.	Detected Mobile APPLICATION Information	Common Name	
4.		Unique ID	
5.		Application Signed Certificate Fingerprint	Certificate value on MD5, SHA1 or SHA256 Format: MD5: 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 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
6.		Operating System	□Android version: ________________________ □iOS version: ____________________________ □Windows version: _______________________ □other___________________________________
7.		Program Version	
8.	Application Category		Check the following categories of the APPLICATION □Level 1: the application without the need of user identification □Level 2: the application with the need of user identification

NO	ITEM	CONTENT
		☐Level 3: the applications with the transaction
9.	Post Status	☐Internal use, not publicly released
		(Internal use, not publicly released skip) ☐Released ☐Unreleased expected release date_________ Released or scheduled to be released: ☐ Application store provided by mobile operating system ☐ Apple Application Store (URL): ____________________ ☐ Google Play (URL): ____________________ ☐ Microsoft Marketplace (URL): ____________________ ☐ Other (URL): ____________________ ☐ Application store provided by mobile device manufacturers (Please fill in the name of the release of the carriers and the market) ____________________ ☐ Application store provided by mobile operators (Please fill in the name of the release of the carriers and the market) ____________________
10.	Sensitive data Types and Usages	Format: Need <XX sensitive data > Because <OO function>, <particularly Descriptions> Example: Needs National ID card number, because the sign-in function, as a user account

NO	ITEM	CONTENT
11.	Resources, Rights and Usages of Mobile Devices	Format: Need <XX permission> because <OO function>, <particularly Descriptions> Example: Need android.permission.ACCESS_FINE_LOCATION, because the navigation function, using GPS positioning
12.	Contact Information for replying on Specific Issues and Improvement	Released ☐In application ☐In application store ☐Contact website: ______________________ ☐e-mail:______________________ ☐phone:__________________________ ☐other:__________________________
13.	Reference Library Name, Version, Source (Including Built-in Operating System and Third-Party Libraries)	Format: <library name / library version / library source> Examples: webkit / 534.30 / OS built-in
14.	If Connection Adoptes Encryption (The First Category Need Not Fill)	☐ Yes, encryption protocol: _____________ (such as: TLS 1.2) ☐ No, reason: _________________
15.	Description of Random Number Generator Library in Encryption Algorithm	Format: Use <XX random number generating libraries> at <OO encryption algorithm>
16.	Free APPLICATION	☐ Yes ☐ No
17.	Use of WebView	☐ Yes, domain name: ___________________________ (Eg: www.moeaidb.gov.tw) ☐ No
18.	Remark	

Company Name:

print

Representative:

print

ID Numbers:

Address:

YY/MM/DD:

Appendix IV, Reference Format for the Report of Security Testing for Mobile Applications

Report No:

○○○○○ (agency name) ○○○○○ (lab name)

Testing Report of the Mobile Application Basic Security

Report No		
Test basis		
Censorship Name		
Developer Name		
Detected Mobile APPLICATION Information	Common Name	
	Unique ID Name	
	OS	
	Program Version	
	Test category	
Test results		
Testing Start Date		
Testing Complete Date		
Report Date		
Report Version		

Report Approved by (Signature)	Report Signed (Signature)	Testing Faculty (Signature)

I. Test item and Results

Technical Requirements for Information Security	Test items	Results (Satisfied / Non-Satisfied / References)	Remark
4.1.1. Mobile Application Release Security	4.1.1.1.1. Mobile applications shall be released in trusted application stores		
	4.1.1.1.2. Mobile application should be noted the Sensitive data accessed, the mobile device resources and the declaration of the permissioned purposes of use at the time of release		
	4.1.1.3.1. Mobile application developers should provide a channel of return on security issues		
• • •	• • •		

II. Encoding Format

(The encoding format of the Testing Laboratory report, and the encoding format of the detected item)

III. Testing Tool

a) The Testing Software Tools

(List of the testing software tools)

b) The Testing Hardware Tools

(Information of the testing hardware tools, such as mobile device brand, model number, device serial number, OS version, etc. ...)

IV. Attachments

(Testing Laboratory enclosed with Check List of the Mobile Application Basic Security and relevant information)

Appendix V. Reference for the mobile application basic security

This appendix provides a reference of security information for different mobile applications, including three major aspects, which are detailed in 4.1.1. Mobile application release security, 4.1.2. Protection of sensitive data, and 4.1.5. Mobile application security code.

For each reference item, we set the reference number, basis, technical requirements, reference description, reference source and remarks, etc., and explain the following table with reference to the item description.

Reference Item Description Table

ITEMS	DESCRIPTION
Reference Number	According to "4. Technical requirements" of the "Basic Security Baseline for Mobile Applications", the testing number consists of 4 codes, which are REF-.x respectively. "REF-." is expressed as "Appendix V", and "x" is the numbered item.
Basis	Basis is according to "4. Technical requirements” of the “Basic Security Baseline for Mobile Applications”.
Technical Requirements	Technical requirements for mobile application information security are according to "4. Technical requirements” of the “Basic Security Baseline for Mobile Applications”
Reference Description	Reference Reason: Description:
Reference Source	Reference source
Remarks	Other Description

4.1.1. Mobile Application Release Security

4.1.1.1. Mobile Application Release

4.1.1.1.1. Mobile applications shall be released in trusted application stores

REFERENCE NUMBER	REF-1.
Basis	4.1.1.1 Mobile Application Release - "Security Regulations for Mobile Application"
Technical Requirements	Mobile applications should be released in the application store of a trusted source
Reference Description	Reference Reason：For developers only, non-actually performing inspections. Description：This reference item cannot be determined by the application itself. It is recommended that the mobile application be released by mobile application store provided by mobile operators, mobile operating system operators, or mobile device manufacturers.
Reference Source	NIST SP 800-163 3.1.6 Testing Application Updates
Remarks	

4.1.1.2. Mobile application update

4.1.1.2.1. Mobile applications shall be released the updates in trusted application stores

REFERENCE NUMBER	REF-2.
Basis	4.1.1.2 Mobile Application Update – “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications’ update should be released in the application store of a trusted source
Reference Description	Reference Reason ： For developers only, non-actually performing inspections. Description：This reference item cannot be determined by the application itself. It is recommended that the mobile applications’ update be released by mobile application stores provided by mobile operators, mobile operating system operators, or mobile device manufacturers.
Reference Source	NIST SP 800-163 3.1.6 Testing Application Updates
Remarks	

4.1.1.2.2. Mobile application should provide an update mechanism

REFERENCE NUMBER	REF-3.
Basis	4.1.1.2 Mobile Application Update - “Security Regulations for Mobile Application”
Technical Requirements	Mobile application should provide an update mechanism

Reference Description	Reference Reason：For developers only, non-actually performing inspections. Description：When there exists a security weakness in the mobile application, it should be updated by the trusted source server.
Reference Source	NIST SP 800-163 3.1.5 Securing Application Code Dependencies
Remarks	

4.1.1.2.3. Mobile applications should notify actively when security updates

REFERENCE NUMBER	REF-4.
Basis	4.1.1.2 Mobile Application Update - “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications should proactively announce during security updates
Reference Description	Reference Reason：For developers only, non-actually performing inspections. Description：This reference item cannot be determined by the application itself. It is recommended that the mobile application be released by mobile application stores provided by mobile operators, mobile operating system operators, or mobile device manufacturers.
Reference source	NIST SP 800-64 3.4 SDLC Phase: Operations and Maintenance
Remarks	

4.1.1.3. Mobile Application Security Issues In Return

4.1.1.3.2. Mobile application developers should respond and improve the problem within a reasonable period

REFERENCE NUMBER	REF-5.
Basis	4.1.1.3. Mobile Application Security Issues In Return – "Security Regulations for Mobile Application"
Technical Requirements	Mobile application developers should respond to questions and improve within an appropriate period of time
Reference Description	Reference Reason：It is related to quality, not directly affecting the security of mobile applications. Description：This reference item cannot be determined by the application itself, and we suggest a reply and improvement mechanism.
Reference Source	NIST SP 800-64 3.1.3.5 Ensure Use of secure Information System
Remarks	

4.1.2. Protection of Sensitive data

4.1.2.2. Sensitive data Usage

4.1.2.2.1. Before the mobile applications use sensitive data, they must get users' consent

REFERENCE NUMBER	REF-6.
Basis	4.1.2.2. Sensitive data Usage - “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications should obtain users’ consent before collecting sensitive data
Reference Description	Reference Reason：Due to the time, the complexity, or current general testing methods, the test results may be inconsistent, or the test is difficult to perform or repeated. Description：This reference item cannot determine whether sensitive data is being used by the mobile application or not. It is recommended that： (1) Mobile application store statement provided by mobile applications, mobile device manufacturers, mobile device manufacturers, and mobile operators before the use of sensitive data. (2) The mobile application obtains users’ consent from the mobile application store provided by mobile operators, mobile operating system operators, mobile device manufacturers, or mobile carrier before using the sensitive data.
Reference	NIST SP 800-163 3.1.4 Protecting Sensitive Data

source	
Remarks	

4.1.2.2.2. Mobile application should provide users the right to refuse the use of sensitive data

REFERENCE NUMBER	REF-7.
Basis	4.1.2.2. Sensitive data Usage – “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications should provide the user with the right to refuse to use sensitive data
Reference Description	Reference Reason：Due to the time, the complexity, or current general testing methods, the test results may be inconsistent, or the test is difficult to perform or repeated. Description：This reference item cannot determine whether sensitive data is being used by the mobile application or not. It is recommended to provide users with the option to refuse to use sensitive data.
Reference source	NIST SP 800-163 3.1.4 Protecting Sensitive Data
Remarks	

4.1.2.2.3. If mobile applications use passcode authentication, they should take the initiative to remind the user to set more complex passcode

REFERENCE NUMBER	REF-8.
Basis	4.1.2.2. Sensitive data Usage – "Security Regulations for Mobile Application"
Technical Requirements	Mobile applications should actively remind users to set more complex password if password authentication is used.
Reference Description	Reference Reason：It is related to quality, not directly affecting the security of mobile applications. Description：This reference item is related to the user experience. It is recommended that： (1) The mobile application should remind the users to set the password with at least 6 characters on the password setting page. (2) The mobile application should remind the users to set the password with numbers, uppercase character, and lowercase characters on the password setting page. (3) The mobile application should remind the users to avoid using personally relevant data as a password on the password setting page.
Reference Source	OWASP Mobile Application Security Checklist 0.9.3 V2.1: Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials or cryptographic keys
Remarks	

4.1.2.2.4. Mobile applications should remind users to regularly change the passcodes

REFERENCE NUMBER	REF-9.
Basis	4.1.2.2. Sensitive data Usage – “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications should remind users to change the password periodically
Reference Description	Reference Reason：It is related to quality, not directly affecting the security of mobile applications. Description：This reference item is related to the user experience. It is recommended that the mobile application should remind the user to change the password periodically (up to 90 days) on the password setting page.
Reference Source	OWASP Mobile Application Security Checklist 0.9.3 V2.1: Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials or cryptographic keys
Remarks	

4.1.2.3. Sensitive data Storage

4.1.2.3.3. Sensitive data stored in mobile applications, be use for declaration only

REFERENCE NUMBER	REF-10.
Basis	4.1.2.3. Sensitive data Storage - “Security Regulations for Mobile Application”
Technical Requirements	The sensitive data stored by the mobile application should only be used for the purpose of its usage statement
Reference Description	Reference Reason：Due to the time, the complexity, or current general testing methods, the test results may be inconsistent, or the test is difficult to perform or repeated. Description：This reference item cannot determine the usage of sensitive data by the mobile application. It is recommended to use sensitive data only within the scope of the statement.
Reference Source	NIST SP 800-163 3.1.4 Protecting Sensitive Data
Remarks	

4.1.2.6. Sensitive data Deletion

4.1.2.6.1. The function of deletion should be provided if mobile application store user’s sensitive data

REFERENCE NUMBER	REF-11.
Basis	4.1.2.6. Sensitive data Deletion - “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications should provide the user with the ability to delete sensitive data once involving storing user-sensitive data
Reference Description	Reference Reason：Due to the time, the complexity, or current general testing methods, the test results may be inconsistent, or the test is difficult to perform or repeated. Description：This reference item cannot determine the deletion of sensitive data by the mobile application. It is recommended that the sensitive data does not exist in any form in the mobile device after the function of sensitive data deletion interface is executed.
Reference Source	NIST SP 800-163 3.1.4 Protecting Sensitive Data
Remarks	

4.1.5. Mobile Application Security Code

4.1.5.2. Mobile Application Integrity

4.1.5.2.1. Mobile applications should use appropriate and valid integrity verification mechanisms to ensure their integrity

REFERENCE NUMBER	REF-12.
Basis	4.1.5.2. Mobile Application Integrity – “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications should use appropriate and valid integrity verification mechanisms to ensure their integrity
Reference Description	Reference Reason ： For developers only, non-actually performing inspections. Description ： This reference item cannot determine mobile application integrity. The Verification the integrity of the application requires the cooperation of the platform vendor. It is recommended that ： (1) Mobile application developers provide application hashes for users to verify the integrity of mobile applications (2) Protect mobile application business logic with Obfuscation
Reference Source	OWASP Mobile Application Security Checklist 0.9.3 V7.2: Verify that the application has been built in release mode, with settings appropriate for a release build (e.g. Non-debuggable)
Remarks	

4.2.2. Server-side Security Testing

4.2.2.1. WebView Security Inspection

4.2.2.1.1. WebView of mobile applications should be used to exchange the website resource with the remote server

REFERENCE NUMBER	REF-13.
Basis	4.2.2.1. WebView Security Inspection - “Security Regulations for Mobile Application”
Technical Requirements	Mobile applications should use WebView and remote server for web resource exchange
Reference Description	Reference Reason：For developers only, non-actually performing inspections. Description：When using a mobile application to exchange web resources with a remote server, if an external application (for example, a malicious browser) may have data leakage or theft, it is recommended to use WebView and the server for web resource exchange.
Reference Source	
Remarks	