Basic Information Security Standard for Mobile Applications

V1.4

Mobile Application Security Alliance

January 2022

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

Date	Version
April 2015	V1.0
October 2016	V1.1
August 2018	V1.2
September 2019	V1.3
January 2022	V1.4

Table of Contents

1. Foreword

The convenience brought by mobile devices has made them an indispensable equipment in our everyday life; in the given background, various types of mobile applications (abbr. apps) have emerged. Yet, as some of mobile application developers do not have the awareness of information security, the mobile applications developed by them may cause the risks of user data leakage or financial loss. Therefore, based on the resolution of the 26th Committee Meeting of the National Information & Communication Security Taskforce of the Executive Yuan on June 24, 2014, the Industrial Development Bureau of the Ministry of Economic Affairs (hereinafter referred to as "IDB") had been actively discussing the formulation of «Basic Information Security Standard for Mobile Applications» (hereinafter referred to as "the Standard").

As a result, the IDB appointed the Institute for Information Industry (hereinafter referred to as "III") to establish a working group by inviting information security experts in Taiwan; the III then started to codify the Standard by taking reference from relevant international information security standards and criteria. In each stage of the codification of the Standard, via holding meetings such as expert symposiums and public seminars, advices from industry, governmental agencies, academia, researchers and opinions from practioners of different fields are solicited. These solicited advices and opinions then serve as the major directions for codification; the Standard was thus formulated for vendors to voluntarily follow and take reference from when developing mobile applications. The Standard was revised to version 1.2 in August 2018, and was updated to «Basic Information Security Standard for Mobile Applications V1.3» in September 2019. Afterwards, in order to regulate the security of mobile applications, Taipei Computer Association was appointed as the executive agency in January 2022 in order to revise and update the Standard to «Basic Information Security Standard for Mobile Applications V1.4» (hereinafter referred to as "the Standard")

The Standard is a non-mandatory regulation. The main purpose of the Standard is to improve the basic security protection capabilities of mobile application in Taiwan. From the initial stage of design, basic information security concepts shall be introduced. With the key points of the Standard, Application developers are thus prompted to strengthen their awareness of information security and gradually improve the security protection capabilities of the app(s) developed by them.

The Standard has proposed information security technical requirements for six different aspects respectively, including “Security regarding Mobile Application Release”, “Sensitive Data Protection”, “Security regarding Transaction Resource Management”, “Security regarding User Authentication, Authorization, and Connection Management in Mobile Applications”, “Code Security of Mobile Applications”, and “Server-side Security Inspection”. As a result, app developers can take reference from the Standard to independently improve the security quality of the mobile apps developed by them, so as to enhance users’ trust and the willingness to use the app, thus create a win-win situation for both app developers and users.

2. Scope of application

The Standard primarily proposes basic information security requirements for the security of mobile applications on the mobile-device side. Information security requirements on the server side are also included in the Standard.

The Standard is applicable to mobile applications of non-specific fields[1] and the common functions of mobile applications[2]. For the mobile applications of specific fields, on the other hand, the information security standards required for the fuctions in their fields are recommended to be formulated by respective regulating departments.

The Standard is a basic information security guideline for the relevant vendors who provide mobile applications, which is a voluntary code for vendors to follow or take reference from.

---

[1] Specific field: A field that is categorized under a certain professional field, which is regulated and controlled by specific competent authorities and laws, e.g. finance, medical care, taxation, etc.

[2] Common functions: Basic functions which have commonality, similarity and are required by the operation of mobile applications, e.g. data storage, transmission protection mechanisms, or user authentication mechanisms, etc.

3. Glossary

The Chinese translation of technical terms in this chapter primarily adopts those of the Bilingual Vocabulary, Academic Terms and Dictionary Information Network of the National Academy for Educational Research of the Bureau of Standards, Metrology and Inspection, M.O.E.A.

3.1. Mobile Application

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

3.2. Application Store

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

3.3. Personal Data

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

3.4. Sensitive Data

The information created, stored or transmitted on the mobile device and its storage media due to the user's behavior or the operation of mobile applications, in which the access to personal private information is classified as collection, storing data in the local device is classified as storage, and of which the leakage may cause harm to users. The information, in addition to the personal information defined in 3.3, also includes, but not limited to, passwords, keys, videos, photos,

phone calls, audio files, instant messaging messages, call logs, SMS, memo, contacts, notes, geographic location, calendar, device identifier, and any other information related to personal privacy.

3.5. Password

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

3.6. Transaction Resource

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

3.7. Session Identification, Session ID

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

connection.

3.8. Server Certificate

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

3.9. Certification Authority

An agency or legal person that issues certificate.

3.10. Malicious Code

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

3.11. Vulnerability

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

3.12. Library

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

3.13. Code Injection

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

3.14. Mobile Operating System

An operating system which operates on mobile devices.

3.15. Mobile Resource

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

3.16. In-Application Update

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

3.17. Common Vulnerabilities and Exposures

Abbreviated as “CVE”, a vulnerability management program sponsored by the U.S. Department of Homeland Security, in which a globally recognized unique universal number will be assigned to each vulnerability item.

3.18. Known Vulnerabilities

The vulnerabilities with CVE numbers.

3.19. Authentication

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

3.20. Advanced Encryption Standard

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

3.21. Triple Data Encryption Standard

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

3.22. Elliptic Curve Cryptography

A type of algorithm for establishing public key encryption, which is based on

additive groups or mathematical structures generated by elliptic curves. The use of elliptic curves in cryptography was independently proposed by Neal Koblitz and Victor Miller respectively in 1985.

3.23. Certificate Pinning

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

3.24. Hash

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

3.25. Obfuscation

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

3.26. Using Sensitive Data

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

3.27. Log File

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

3.28. Device Identifier

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

3.29. Cache Files or Temporary Files

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

3.30. Configuration File

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

3.31. Encode

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

3.32. Decode

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

3.33. Payload

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

3.34. Collecting Sensitive Data

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

3.35. Storing Sensitive Data

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

3.36. Common Vulnerability Scoring System

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

3.37. Secure Random Number Generator

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

3.38. Secure Domain

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

3.39. Secure Encryption Function

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

3.40. System Credentials Storage Facilities

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

4. Technical Requirements

4.1. Technical Requirements regarding Information Security for Mobile Applications

In the given section, Technical Requirements are formulated regarding mobile application security of different aspects, which include five major aspects: “Security regarding Mobile Application Release”, “Sensitive Data Protection”, “Security regarding Transaction Resource Management”, “Security regarding User Authentication, Authorization, and Connection Management in Mobile Applications” and “Code Security of Mobile Applications”.

4.1.1. Security regarding Mobile Application Release

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

4.1.1.1. Mobile Application Release

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

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

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

4.1.1.2. Mobile Application Updates

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

The mobile application shall provide an update mechanism.

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

4.1.1.3. Mobile Application Security Issue Reporting

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

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

4.1.2. Sensitive Data Protection

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

4.1.2.1. Sensitive Data Collection

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

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

4.1.2.2. Sensitive Data Utilization

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

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

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

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

4.1.2.3. Sensitive Data Storage

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.1.2.4. Sensitive Data Transmission

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

4.1.2.5. Sensitive Data Sharing

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

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

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

4.1.2.6. Deletion of Sensitive Data

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

4.1.3. Security regarding Transaction Resource Management

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

4.1.3.1. Using Transaction Resource

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

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

4.1.3.2. Transaction Resource Management

The mobile application shall perform user authentication when using

transaction resources.

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

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

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

4.1.4.1. User Authentication and Authorization

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

The mobile application shall authorize based on user identity.

4.1.4.2. Mechanism regarding Connection Management

The mobile application shall avoid using session IDs with regularity.

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

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

4.1.5. Code Security of Mobile Applications

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

4.1.5.1. Prevention from Malicious Code and Avoidance of Information Security

Vulnerabilities

The mobile application shall avoid containing malicious code.

The mobile application shall avoid information security vulnerabilities.

4.1.5.2. Mobile Application Integrity

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

4.1.5.3. Security Regarding the Reference of Library

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

4.1.5.4. User Input Verification

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

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

4.1.5.5. Prevention from Dynamic Analysis and Tampering

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

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

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

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

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

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

4.2. Technical Requirements regarding Information Security for the Server-side

The Standard aims to provide basic information security requirements regarding the security of mobile applications; therefore, if the server-side information security requirements are involved with the mobile application, it is recommended that the vendor shall provide self-declaration or an affidavit regarding its server-side information security protection and management measures, or that the vendor shall provide a certificate of compliance from a third-party inspection on the information security protection and management of its server-side service(s).

4.2.1. Server-side Security Management

It is recommended that server-side security shall take the applications and services provided as the starting point in order to perform threat modeling analysis to applications and services as a whole; and, with the analysis above, identify the security risks to the services to implement necessary and effective subsequent control measures.

4.2.2. Server-side Security Inspection

The protection measures for the server-side security are easily overlooked by developers due to the fact that the access interface provided by the server side of the mobile application platform for the mobile application is the mobile application itself, rather than the interface directly accessed by the user. The

server side of the mobile application platform is essentially a website and a web service server; therefore, should there be no proper security design and development, there will be vulnerabilities of traditional web applications as well. As a result, for the security inspection on the server side, it is recommended that the developers can consider using penetration testing methods for inspection.

4.2.2.1. WebView Security Inspection

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

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

5. Categorization of Mobile Applications

Mobile applications of different application categories have different security requirements. In the given chapter, mobile applications are categorized based on the information security requirements of different types of mobile applications. There are three major categories and one category requiring additional testing, which are listed as below:

L1: A mobile application that does not require user authentication.

L2: A mobile application that requires user authentication.

L3: A mobile application in which transaction behavior is involved.

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

For each mobile application category, its definition shall meet the minimum set of items of information security technical requirements; that is, the mobile application shall meet all the information security technical requirements of the category to which it belongs. If there are special situations which do not belong to the above-mentioned categories, they will be otherwise stated in the testing standard. In addition to the categorization based on the functionality of mobile applications, there are also the F-type test items, which are advanced additional test items for apps demanding high security. The main content of inspection of F-type test items is reverse engineering analysis, tampering attacks, etc.

6. References

Open Web Application Security Project (OWASP)

[1] OWASP Mobile App Security Checklist v1.2

https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main

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

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

Cloud Security Alliance (CSA)

[4] Mobile Application Security Testing Initiative,
https://www.csaapac.org/mast.html, 2016

U.S.A.

[5] Vetting the Security of Mobile ApplicationsApp, NIST Special Publication 800-163, http://dx.doi.org/10.6028/NIST.SP.800-163, 2015

[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] Government Mobile and Wireless Security Baseline, Federal CIO Council,
https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf, 2013

Europe

[9] Smartphone Secure Development Guidelines, https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016, ENISA, 2017

China

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

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

Japan

[12] Security Guideline for using Smartphones and Tablets - Advantages for work style innovation - [Version 1], https://www.jssec.org/dl/guidelines2012Enew_v1.0.pdf, JSSEC, 2011

International Standards

[13] ISO/IEC 27001:2013 (Information security management)

[14] ISO/IEC 20000:2011 (Information technology - Service management)

[15] ISO/IEC 19790:2012 (Information technology - Security techniques - Security requirements for cryptographic modules)

[16] ISO/IEC 15408:2009 (Information technology - Security techniques - Evaluation criteria for IT security)

[17] ISO/IEC 14598:2001 (Information technology - Software product evaluation)

[18] ISO/IEC TR 9126-4:2004 (Software engineering - Product quality)

Municipal Law of Taiwan

[19] Personal Data Protection Act (30th December 2015)

[20] Enforcement Rules of the Personal Data Protection Act (2nd March 2016)

Appendix I. Comparison Table of the Technical Requirements and Regulations of Other Countries

TECHNICAL REQUIREMENTS	CORRESPONDING ITEMS IN OWASP	NIST (U.S.A.) [SEE NOTE 1]	ENISA (EUROPE) [SEE NOTE 2]	YD/T 2407-2013 (CHINA) [SEE NOTE 3]
4.1.1.1. Mobile Application Release	V1: Architecture, design and threat modelling	Executive Summary	9. Secure software distribution	5.5.2 Requirements regarding Authentication Mechanisms to Applicaiton Security
4.1.1.2. Mobile Application Updates	V1: Architecture, design and threat modelling	Executive Summary	9. Secure software distribution	5.5.4. Security Requirements for Pre-installed Applications
4.1.1.3. Mobile Application Security Issue Reporting	N/A	Executive Summary	9. Secure software distribution	5.5.4. Security Requirements for Pre-installed Applications
4.1.2.1. Sensitive Data Collection	V1: Architecture, design and threat modelling	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	1. Identify and protect sensitive data	5.5.4. Security Requirements for Pre-installed Applications
4.1.2.2. Sensitive Data Utilization	V2: Data Storage and Privacy	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	1. Identify and protect sensitive data	5.5.4. Security Requirements for Pre-installed Applications 5.6.2. Authorized Access to User Data

TECHNICAL REQUIREMENTS	CORRESPONDING ITEMS IN OWASP	NIST (U.S.A.) [SEE NOTE 1]	ENISA (EUROPE) [SEE NOTE 2]	YD/T 2407-2013 (CHINA) [SEE NOTE 3]
				Files
4.1.2.3. Sensitive Data Storage	V2: Data Storage and Privacy	4. Mobile App Evaluation - Protect Sensitive Data	1. Identify and protect sensitive data on the mobile device	5.6.3. Encrypted Storage of User Data
4.1.2.4. Sensitive Data Transmission	V5: Network Communication	4. Mobile App Evaluation - Protect Sensitive Data	4. Ensure sensitive data protection in transit	5.5.4. Security Requirements for Pre-installed Applications 5.6.2. Authorized Access to User Data Files
4.1.2.5. Sensitive Data Sharing	V2: Data Storage and Privacy	4. Mobile App Evaluation - Preserve Privacy	1. Identify and protect sensitive data on the mobile device	5.6.2. Authorized Access to User Data Files
4.1.2.6. Deletion of Sensitive Data	V2: Data Storage and Privacy	N/A	1. Identify and protect sensitive data on the mobile device	5.6.4. Complete Deletion of User data
4.1.3.1. Using Transaction Resource	V4: Authentication and Session Management	N/A	8. Protect paid resources	5.5.4. Security Requirements for Pre-installed Applications
4.1.3.2. Transaction Resource Management	V4: Authentication and Session Management	N/A	8. Protect paid resources	5.5.4. Security Requirements for Pre-installed Applications

TECHNICAL REQUIREMENTS	CORRESPONDING ITEMS IN OWASP	NIST (U.S.A.) [SEE NOTE 1]	ENISA (EUROPE) [SEE NOTE 2]	YD/T 2407-2013 (CHINA) [SEE NOTE 3]
4.1.4.1. User Authentication and Authorization	V4: Authentication and Session Management	4. Mobile App Evaluation - Privacy and Personally Identifiable Information	3. Handle authentication and authorization factors securely on the device correctly	5.6.2. Authorized Access to User Data Files
4.1.4.2. Mechanism regarding Connection Management	V5: Network Communication	4. Mobile App Evaluation – Network Events	2. User authentication, authorization and session management	5.5.4. Security Requirements for Pre-installed Applications
4.1.5.1. Prevention from Malicious Code and Avoidance of Information Security Vulnerabilities	V7: Code Quality and Build Settings	4. Mobile App Evaluation: Malicious Functionality Malware Detection Communication with Known Disreputable Sites Libraries Loaded	6. Secure data integration with third party code 10. Handle runtime code interpretation	5.5.4. Security Requirements for Pre-installed Applications
4.1.5.2. Mobile Application Integrity	V7: Code Quality and Build Settings	4. Mobile App Evaluation – Classes Loaded	N/A	5.5.4. Security Requirements for Pre-installed Applications
4.1.5.3. Security Regarding the Reference of Library	V7: Code Quality and Build Settings	4. Mobile App Evaluation: Native Methods Libraries Loaded	6. Secure data integration with third party code	5.5.4. Security Requirements for Pre-installed Applications

TECHNICAL REQUIREMENTS	CORRESPONDING ITEMS IN OWASP	NIST (U.S.A.) [SEE NOTE 1]	ENISA (EUROPE) [SEE NOTE 2]	YD/T 2407-2013 (CHINA) [SEE NOTE 3]
4.1.5.4. User Input Verification	V7: Code Quality and Build Settings	4. Mobile App Evaluation – Input Validation	10. Handle runtime code interpretation	5.5.4. Security Requirements for Pre-installed Applications
4.1.5.5. Prevention from Dynamic Analysis and Tampering	V8: Resiliency Against Reverse Engineering Requirements	N/A	11. Check device and application integrity	N/A
4.2.2.1. WebView Security Inspection	N/A	N/A	N/A	N/A

[NOTE 1] Vetting the Security of Mobile Applications App, NIST Special Publication 800-163, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163r1.pdf, 2019

[NOTE 2] Smartphone Secure Development Guidelines, https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016, ENISA, 2017

[NOTE 3] TECHNICAL REQUIREMENTS FOR SECURITY CAPABILITY OF SMART MOBILE TERMINAL, 2018

Appendix II. Quick Reference Table for Technical Requirements

SUBSUBSECTION NO.	SERIAL NO.	TECHNICAL REQUIREMENTS
4.1.1.1. Mobile Application Release	1	The mobile application shall be released in an application store of a trusted source.
	2	When releasing, the mobile application shall elucidate the sensitive data and the mobile device resources to be accessed, and the purposes of the declared permissions.
	3	The mobile application shall prompt the user to install protection software on the mobile device in a prominent location (e. g. the official website, the application download page, etc.).
4.1.1.2. Mobile Application Updates	4	The updates of the mobile application shall be released in an application store of a trusted source.
	5	The mobile application shall provide an update mechanism.
	6	The mobile application shall make announcements actively when there are security updates.
4.1.1.3. Mobile Application Security Issue Reporting	7	Mobile application developers shall provide a channel for reporting security issues.
	8	Mobile application developers shall respond to questions and make relevant improvements within an appropriate period.
4.1.2.1. Sensitive Data Collection	9	The mobile application shall obtain user consent before collecting sensitive data.
	10	The mobile application shall provide users with the right to refuse the collection of sensitive data.
4.1.2.2. Sensitive Data Utilization	11	The mobile application shall obtain user consent before using sensitive data.
	12	The mobile application shall provide users with the right to refuse the use of

SUBSUBSECTION NO.	SERIAL NO.	TECHNICAL REQUIREMENTS
		sensitive data.
	13	If the mobile application uses password authentication, it shall actively prompt the user to set a more complex password.
	14	The mobile application shall remind users to change their passwords regularly.
4.1.2.3. Sensitive Data Storage	15	The mobile application shall obtain user consent before storing sensitive data.
	16	The mobile application shall provide users with the right to refuse the storage of sensitive data.
	17	The sensitive data stored by the mobile application shall only be used for the purpose(s) stated in its declaration of use.
	18	The mobile application shall avoid storing sensitive data in redundant files or log files after closure and/or log-out.
	19	The mobile application shall avoid storing sensitive data in redundant files or log files.
	20	Sensitive data shall be encrypted with appropriate and effective key length and encryption algorithm(s) before being stored.
	21	In order to prevent unauthorized access by other applications, sensitive data shall be stored in the areas protected by the OS.
	22	Sensitive data shall be avoided in the code of the mobile application.
	23	The mobile application shall actively alert the user when non-user-initiated screenshots are taken.
	24	The mobile application shall store sensitive data, e. g. personally identifiable information, user credentials, encryption keys, etc., in system credential storage

SUBSUBSECTION NO.	SERIAL NO.	TECHNICAL REQUIREMENTS
		facilities.
	25	The mobile application shall disable the keyboard cache mechanism when the user is entering sensitive data.
	26	The mobile application shall avoid the leakage of sensitive data in the IPC mechanism.
	27	The user interface in the mobile application shall avoid the leakage of sensitive data.
	28	The sensitive data of the mobile application shall not be stored in the backup data of the mobile device operating system.
4.1.2.4. Sensitive Data Transmission	29	The mobile application shall apply appropriate and effective key length and encryption algorithm(s) for secure encryption when transmitting sensitive data via network.
4.1.2.5. Sensitive Data Sharing	30	User consent shall be obtained before the sensitive data are shared among different mobile applications in the mobile device.
	31	The mobile application shall provide users with the right to refuse sensitive data sharing.
	32	Accesses from unauthorized mobile applications shall be avoided when the mobile application is sharing sensitive data.
4.1.2.6. Deletion of Sensitive Data	33	The mobile application shall provide users with the function of deletion if the mobile application involves the storage of users' sensitive data.
4.1.3.1. Using	34	The mobile application shall actively notify users when using transaction

SUBSUBSECTION NO.	SERIAL NO.	TECHNICAL REQUIREMENTS
Transaction Resource		resources.
	35	The mobile application shall provide users with the right to refuse the use of transaction resources.
4.1.3.2. Transaction Resource Management	36	The mobile application shall perform user authentication when using transaction resources.
	37	The mobile application shall record the used transaction resource(s) and the time of use.
4.1.4.1. User Authentication and Authorization	38	The mobile application shall have an appropriate authentication mechanism in order to confirm the user's identity.
	39	Mechanism regarding Connection ManagementThe mobile application shall authorize based on user identity.
4.1.4.2. Mechanism regarding Connection Management	40	The mobile application shall avoid using session IDs with regularity.
	41	The mobile application shall verify the validity of the server certificate.
	42	The mobile application shall confirm that the server certificate is issued by a trusted certificate authority.
4.1.5.1. Prevention from Malicious Code and Avoidance of Information Security Vulnerabilities	43	The mobile application shall avoid containing malicious code.
	44	The mobile application shall avoid information security vulnerabilities.
4.1.5.2. Mobile Application Integrity	45	The mobile application shall use appropriate and effective integrity verification mechanisms to ensure its integrity.
4.1.5.3. Security Regarding the Reference of Library	46	When the library referred by the mobile application is updated, the corresponding updated version shall be prepared. Regarding the update method, please consult subsection: 4.1.1. Security regarding Mobile Application Release.

SUBSUBSECTION NO.	SERIAL NO.	TECHNICAL REQUIREMENTS
4.1.5.4. User Input Verification	47	The mobile application shall perform security checks to the strings entered by the user at the input phase.
	48	The mobile application shall provide protection mechanism(s) relevant to injection attacks.
4.1.5.5. Prevention from Dynamic Analysis and Tampering	49	The mobile application must detect whether the protection layer of the mobile operating system is cracked (e.g. rooted, jailbroken) or is not properly protected; if so, the mobile application shall actively notify the user or terminate itself.
	50	The mobile application shall be able to actively detect whether all the files and data in the sandbox are tampered with.
	51	The mobile application shall detect whether there is any use of dynamic analysis tools or frameworks in the mobile device.
	52	The mobile application shall detect whether the code and data in the memory are tampered with.
	53	Either that the executable files and the libraries belonging to the mobile application shall all be encrypted on the file level or that the important code and data segments inside the executable files shall be encrypted or packed, making it

SUBSUBSECTION NO.	SERIAL NO.	TECHNICAL REQUIREMENTS
		difficult to acquire important code or data via trivial static analysis.
	54	The mobile application shall have code obfuscation mechanism(s).
4.2.2.1. WebView Security Inspection	55	The mobile application shall use WebView to exchange web resources with remote servers.
	56	When the mobile application renders functions in the Webview, the connected domain shall be a secure domain.