System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications

V4.2

Mobile Application Security Alliance

January 2022

Version History of «System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications»

Date	Version
August 2015	V1.0
February 2016	V2.0
March 2017	V3.0
August 2018	V4.0
September 2019	V4.1
January 2022	V4.2

Table of Contents

Part I:

Regulations of the System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications

Background

With the popularity of mobile devices, various types of mobile applications have become inseparable from people's lives. Yet, due to the fact that some developers lack information security awareness, users may need to face data leakage or property damages. As a result, in 2014, in accordance with the resolution of the 26th Committee Meeting of the National Information & Communication Security Taskforce of the Executive Yuan, the Industrial Development Bureau of the Ministry of Economic Affairs (hereinafter referred to as "IDB") had planned the formulation of information security testing standard and had encouraged vendors to engage in voluntary inspection. In 2015, «Basic Information Security Standard for Mobile Applications» was formulated and published as the basis for the promotion of inspection mechanism of information security for mobile applications. In order to implement Basic Information Security Standard for Mobile Applications and let non-official organizations to independently promote the inspection system, the IDB had appointed the Mobile Application Security Alliance as the body for the promotion and the certification of the system, which will be responsible for the implementation of information security accreditation/certification mechanism and promotional activities.

1. Purpose of the System

    1.1. To implement «Basic Information Security Standard for Mobile Applications», and to formulate basic information security testing standards for mobile applications, and encourage developers and platform operators to follow them.

    1.2. To establish the "Mobile Application Basic Security Seal" (abbreviated as "MAS Seal"), so that consumers can easily identify the mobile applications which have passed the inspection of the «System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications» (hereinafter "the

given System").

1.3. To promote the «System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications» so as to establish mobile application security.

2. Scope of Application

2.1. The given information security accreditation/certification System is applicable to the certification of mobile applications based on the various mobile application information security standards and testing standards released by the mobile application regulating departments (and the agencies entrusted by them).

2.2. The given Regulations are applicable to system promoting/certifying bodies of mobile application security accreditation/certification system(s), accreditation bodies, mobile application testing laboratories, mobile application developers.

3. Glossary

3.1. Mobile Application Basic Security Seal: A certificate in recognition of that the test results of a mobile application is compliant with the requirements the «Basic Information Security Testing Standard for Mobile Applications»; it is also abbreviated as "MAS Seal".

3.2. System Promoting/Certifying Body: The abbreviation of "system promoting/certifying body of mobile application security accreditation/certification system(s)." The body shall be selected and appointed by the mobile application regulating departments. The body is responsible for the management, maintenance, and implementation of the given System, and it is also responsible for the authorization, review of the MAS Seal and the maintenance of the Management Website.

3.3. Mobile Application Security Alliance: An organization

established independently by the private sector. It is selected and appointed by the mobile application regulating departments to be the "system promoting/certifying body of mobile application security accreditation/certification system(s)." The missions of the organization are: to facilitate the development of mobile-application-related industries in Taiwan; to make the voluntary information security inspection system more complete; to cultivate talents in the mobile application information industry; to improve the information security of mobile applications in Taiwan; to expand domestic and foreign business opportunities so as to facilitate the improvement of the voluntary information security inspection system; to improve the information security of mobile applications in Taiwan. Its work tasks are as follow:

A. Promotion of «Basic Information Security Standard for Mobile Applications» and its certification system.

B. Assisting the government to promote the industrial policies regarding mobile applications; handling the maintenance of the System and the revision(s) of the Standard; management of accredited testing laboratories and reviewing test reports; authorization and management of certificate of conformity and the MAS Seal; handling training programs, international cooperation, promotional activities; etc.

3.4. Accreditation Registration Management Website: Abbreviated as the "Management Website", a public website established by the "system promoting/certifying body", which registers accreditation bodies, the list of accredited testing laboratories, the mobile applications which passed the inspection and were granted the MAS Seal.

3.5. Accreditation: The procedure of granting formal recognition to a specific person or organization/institution by an accreditation

body as a proof that the person/organization/institution is competent to perform specific task(s).

3.6. Certification: The procedure in which a written certification is issued by an accredited testing laboratory proving that a specific product or service complies with the requirements of certain regulations.

3.7. Accreditation Body: A body responsible for accreditation on whether a testing laboratory has sufficient capability in the inspection of basic information security for mobile applications. In the given System, the accreditation body is Taiwan Accreditation Foundation (abbreviated as TAF).

3.8. Testing Laboratory: An agency that accepts applications from mobile application developers and provides information security inspection services for mobile application developers based on the «Basic Information Security Testing Standard for Mobile Applications». A testing laboratory must submit an application for accreditation in accordance with the «Regulations governing the Accreditation and Management of Testing Laboratory for Basic Information Security for Mobile Applications». For details regarding the accreditation procedure, please refer to Appendix I; for relevant registration application form and the regulations regarding its rights & obligations, please consult Appendix II and Appendix III.

3.9. Accredited Laboratory: A testing laboratory can submit application based on «Regulations governing the Accreditation and Management of Testing Laboratory for Basic Information Security for Mobile Applications». Should the testing laboratory be accredited by TAF, it will be referred as an “accredited laboratory”, of which the validity period of the accreditation is 3 years.

3.10. Mobile Application: A type of program which is designed for smartphones, tablet computers, and other mobile devices to use. In the given System, it is also abbreviated as “mobile app”.

3.11. Mobile Application Developer: An individual who develops, designs, and maintains mobile applications. When the development is commissioned, the commissioner may be regarded as the developer.

3.12. Application Store: Browsing, downloading, and/or purchasing applications, music, magazines, books, movies, and TV programs done by mobile devices users through the application store(s) built-in in the device or through website(s).

4. Mobile Application Basic Security Seal (MAS Seal)

4.1. For a mobile application that has passed the inspection of a testing laboratory, the testing laboratory shall apply the “Certificate of Conformity of Basic Information Security Testing for Mobile Applications” and the MAS Seal based on the inspection report, in which the mobile application passed all the necessary test items of its mobile application category defined by the «Basic Information Security Testing Standard for Mobile Applications». For the procedure regarding the application for inspection and certificate of conformity (including the MAS Seal), please consult Appendix IV; For the relevant application form(s) for the use of the MAS Seal and the regulations regarding the rights and obligations on the use of the MAS Seal, please consult Appendix V and Appendix VI.

4.2. The MAS Seal categorizes mobile applications into three categories based on their security levels: L1, L2, and L3; if the application has higher security demand, then there are also additional optional test items – the F-type test items. The description of the three major categories and the F-type test items

is as follow:

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

B. L2: A mobile application that requires user authentication.

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

D. F: A mobile application that has higher security requirements, which is an additional category of test items. For the applications belonging the above-mentioned three major security levels, additional tests with the F-type test items can be performed based on the security requirements of the mobile application (in which, the security level will be respectively abbreviated as: “L1+1”, “L2+F”, and “L3+F”).

4.3. Announcement: The mobile applications that has passed the inspection and obtained the MAS Seal shall be registered and announced on the Management Website.

4.4. Validity Period: The validity period of MAS Seal is 1 year. Also, in one of the following situations, the Mobile Application Security Alliance can suspend or terminate its validity:

A. Where there is a violation of the «Regulations governing the Use and the Management of Mobile Application Basic Security Seal»

B. Where there is a violation of the regulations regarding the rights and obligations on the use of the Seal.

4.5. Miscellaneous Matters regarding MAS Seal Management: For a mobile application which has passed the inspection done by a testing laboratory accordingly to the «Basic Information Security Testing Standard for Mobile Applications», application

for certificate of conformity and the MAS Seal shall be submitted accordingly to the aforementioned Section 4.1. If the above-mentioned application is not submitted, then the testing laboratory to which the inspection was entrusted shall ask the application developer to provide an affidavit, with which the testing laboratory will report to the Mobile Application Security Alliance. Relevant operation regulations will be separately stipulated and announced by the Mobile Application Security Alliance.

5. Information Control

When there is any changes in the name, ownership and/or other information of the mobile application, the developer(s) of the mobile application shall notify the Mobile Application Security Alliance immediately.

6. Tracking Management

The Mobile Application Security Alliance may regularly or irregularly perform inspection with methods such as census or random sampling to see whether the version of the mobile application which passed the test(s) matches the version on the application store(s).

7. Fees

7.1. The fees of the given System include miscellaneous administrative expenses, e. g. accreditation fee, inspection fee, application fee for certificate of conformity, etc.

7.2. Accreditation fee of testing laboratories will be announced and collected by the accreditation body.

7.3. Inspection fee will be collected by testing laboratories.

7.4. Application fee for certificate of conformity and other types of fees will be announced and collected by the Mobile Application

Security Alliance.

Part II:

Regulations governing the Accreditation and Management of Testing Laboratory for Basic Information Security for Mobile Applications

1. General Provisions

1.1. According to Article 7 of the «Regulations of the System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications», affairs regarding the qualification and management of testing laboratories shall be implemented in accordance with the Regulations; where there are special provisions by the accreditation body, such provisions shall prevail.

1.2. For all of the testing laboratories subordinate to a legally registered domestic legal person or an academic research institution, which has certain professional capability, performs tasks relevant to mobile application testing/inspection accordingly to its management system, and issues reports, their representative(s) [or responsible person(s)] can submit an application to the accreditation body so as to let the accreditation body conduct the accreditation procedure.

2. Procedural Review of Testing Laboratory Accreditation

In the Testing Laboratory Accreditation Procedure, the following items shall be examined:

2.1. Accreditation application form to the accreditation body by the testing laboratory.

2.2. Photocopies of supporting documents of legally established domestic legal person/entity.

2.3. Supporting documents regarding the capability of the testing laboratory.

2.3.1. Qualification of Testing Laboratory: Accredited with a laboratory certificate of accreditation of CNS 17025 or ISO/IEC 17025 issued by a domestic or international accreditation body.

2.3.2. Personnel Qualification: The basic members of a testing laboratory shall be established based on the principle of decentralization of responsibility, in which at least 3 formal employees shall be included: laboratory director, quality director, and report signatory. The qualifications of the aforementioned employees shall meet the requirements listed below:

2.3.2.1. Laboratory Director: College degree or above, with more than 2 years of management experience relevant to information security, and possesses the ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories (or CNS 17025) training certificate.

2.3.2.2. Quality Director: College degree or above, with more than 2 years of relevant work experience in quality management or auditing, and possesses a certificate of training related to quality management or auditing.

2.3.2.3. Report Signatory: College degree or above, with more than 3 years of work experience relevant to information security, and qualified with the professional licenses relevant to information security within the validity period accordingly to the following conditions:

A. Possesses a Certified Ethical Hacker (CEH) Certificate or a GIAC Security Essentials (GSEC) Certificate.

B. Possesses one of the following certificates: Certified Information Systems Security Professional (CISSP), Certified Secure Software Lifecycle Professional (CSSLP), EC-Council Certified Security Analyst (ECSA), EC-Council Computer Hacking Forensic

Investigator (CHFI), GIAC Penetration Tester (GPEN), GIAC Mobile Device Security Analyst (GMOB), or Certificate of Application Vetting Professional (CAVP).

2.3.3. Executive Performance: The testing laboratory has the practical experience of 2 cases (or more) in mobile application information security testing within 3 years. Supporting documents regarding the aforementioned experience (e.g. contracts/orders from clients, test reports, etc.) shall be provided for review.

3. Supplementation Period

If the documents specified in Article 2 are insufficient or incomplete, the accreditation body shall notify the testing laboratory to make necessary supplements and/or rectifications within a specified period. If the testing laboratory failed to make the supplements and/or rectifications within the specified period or that the supplements and/or rectifications are incomplete, the application will not be accepted. The length of the specified period for supplements and/or rectifications will be subject to the notification(s) from the accreditation body.

4. Certificate of Accreditation of Testing Laboratory

If a testing laboratory is found meeting the qualification after an inspection conducted by an accreditation body, the accreditation body will issue the “Certificate of Accreditation of Testing Laboratory” (Hereinafter referred to as Certificate of Accreditation).

5. Principle of Confidentiality for the Personnel of Testing Laboratory

The testing laboratory or its service personnel shall keep all the testing-related and submitter-related information strictly confidential; and the same Principle shall also apply to retired personnel.

6. Principles regarding the Pricing Policy of Testing Laboratory

The testing fee quoted by a testing laboratory shall comply with the principles of transparency and fairness.

6.1. The testing fee shall be based on the category of the mobile application submitted by the application developer(s).

6.2. When the testing laboratory informs the mobile application developer(s) that the mobile application does not meet the requirements, it shall list the items of non-conformity and notify the developer(s) to improve accordingly. The method(s) of the aforementioned notification and the charging mechanism will be determined by the testing laboratory.

6.3. The testing laboratory shall collect the miscellaneous administrative fees (e. g. certification fee) announced by the Mobile Application Security Alliance on the Alliance's behalf.

7. Rights and Obligations of Testing Laboratory

After the testing laboratory is accredited, it shall abide by the following obligations:

7.1. The testing laboratory shall maintain the testing quality and technical capabilities to meet the requirements listed in Article 2.

7.2. The information security testing reports issued by the testing laboratory shall not be false or untrue, or be found non-conforming by the Mobile Application Security Alliance when the Alliance performs random sampling inspection.

7.3. The testing laboratory shall adhere to a fair, impartial and independent standpoint when accepting submission(s) for inspection, and shall not refuse to accept submission without justifiable reasons, or give discriminatory treatment, or conduct acts which cause breach of fairness and/or impartiality.

7.4. There shall be no relationship which impairs the impartiality of

the inspection system between the testing laboratory and the developer(s) whose mobile application is accepted for inspection by the testing laboratory.

7.5. Should there be any breach of Section 7.1, 7.2, 7.3, 7.4, the Mobile Application Security Alliance may make announcement on the Management Website and notify the accreditation body to revoke the Certificate of Accreditation of the testing laboratory.

7.6. The testing laboratory shall accept and cooperate with the regular or irregular supervision, evaluation, inspection, interview, re-evaluation and other operations arranged by the accreditation body, and shall also provide necessary assistance for the sake of the successful completion of the operation(s). For the aforementioned operations, the Mobile Application Security Alliance may perform inspections and/or reviews on a regular or irregular basis.

7.7. The testing laboratory shall notify the accreditation body of any changes in the following information, and shall also notify the Mobile Application Security Alliance within 15 days from the date of the change(s).

A. Change(s) of ownership, name or address of the entity.

B. Change(s) of the head(s) of the entity.

C. Change(s) in the items recorded in the Certificate of Accreditation.

D. Termination or closure of business.

7.8. For the changes regarding the items listed in Section 7.7, if the testing laboratory fails to notify the Mobile Application Security Alliance within the specified period, the Mobile Application Security Alliance may notify the accreditation body to revoke the Certificate of Accreditation of the testing laboratory if necessary.

7.9. The testing laboratory shall archive the mobile application file(s) submitted for inspection, and keep the file(s) for at least one year to ensure that the version of the mobile application submitted for inspection is correct and is free from tampering and corruption. When a random sampling inspection is necessary, the Mobile Application Security Alliance may ask the testing laboratory to provide the data of the application's original file(s) archived by the testing laboratory.

7.10. If there is any change in personnel in laboratory director(s), quality director(s), and/or report signatory(s), the testing laboratory shall actively inform the Mobile Application Security Alliance.

8. Principles regarding Inspection Visit to Testing Laboratory

8.1. After that a newly established testing laboratory has the experiences of 20 cases (or more) of application submission (including its subsequent MAS Seal acquisition), an inspection visit will be conducted within 3 months.

8.2. If the testing laboratory has not accepted any cases of application submission within 6 months, the Mobile Application Security Alliance shall conduct an inspection visit within 3 months in order to learn the state of the laboratory.

8.3. In other relevant scenarios, according to the regulations by TAF, an inspection visit shall be conducted in collaboration with the Mobile Application Security Alliance.

9. Regulations regarding Performance Evaluation of Testing Laboratory

To ensure the consistency of quality in application testing by testing laboratories, and to encourage testing laboratories to actively participate in the activities of the Mobile Application Security Alliance, the Alliance had especially stipulated the regulations regarding performance evaluation of testing laboratories, in which the Alliance

will select Testing Laboratories of Excellence via scoring methods in “performance evaluation” every year and make subsequent announcements on the Management Website.

Part III:

Regulations governing the Use and the Management of Mobile Application Basic Security Seal

1. General Provisions

1.1. According to “Article 9. Mobile Application Basic Security Seal” of the «Regulations of the System for the Promotion of Voluntary Inspection of Mobile Applications», management regarding the Seal shall be in accordance with the given Regulations.

1.2. The purpose of enactment of the given Regulations is to clarify the application, issuance, and management of the “Mobile Application Basic Security Seal”.

2. Terms and Definitions

2.1. Where the given Regulations do not provide, the Provisions of «Regulations of the System for the Promotion of Voluntary Inspection of Mobile Applications» and «Basic Information Security Standard for Mobile Applications» shall apply.

2.2. “Mobile Application Basic Security Seal” (Abbreviated as “MAS Seal”) is a certificate which recognizes that the inspection performed on a mobile application conforms to the «Basic Information Security Testing Standard for Mobile Applications».

3. Issuance and Use of the MAS Seal

3.1. Issuance of the MAS Seal

3.1.1. An accredited testing laboratory is responsible for the certification of basic information security for mobile applications; the aforementioned laboratory will also issue a conformance testing report and a certificate of conformity, and notify the Mobile Application Security Alliance. After passing the verification, the application developer(s) may fill the “Application Form for Certificate of Conformity of Basic Information Security Testing for Mobile Applications and the MAS Seal” and the “Regulations governing the Rights

and Obligations on the Use of Mobile Application Basic Security Seal" so as to apply for the use of the MAS Seal.

3.1.2. The Mobile Application Security Alliance shall review the application mentioned in 3.1.1. If the application does not pass the review or that relevant supplementation/correction is needed, the applicant shall be notified.

3.2. Use of the MAS Seal

3.2.1. The developer(s) shall use the MAS Seal on the webpage of the application store in accordance with the style specified by the Mobile Application Security Alliance, and shall not change the shape, color or put on any additional text. If there is any need to use the MAS Seal in a different fashion, an application shall be submitted to the Mobile Application Security Alliance with the Application Form attached in the "Appendix VII. Application Form for Exceptional Use of the Mobile Application Basic Security Seal".

3.2.2. The MAS Seal shall not be used for purposes other than a certification seal.

3.2.3. The Mobile Application Security Alliance shall announce the mobile application awarded with the MAS Seal on the Management Website for inquiry.

4. Renewal and Information Notification of the MAS Seal

4.1. Period of Use: The period of use of the MAS Seal is 1 year; However, in the following situations, the Mobile Application Security Alliance may suspend or terminate its validity:

a. Where there exists a violation of the given Regulations regarding the use, renewal and tracking management of the MAS Seal.

b. Where there exists a violation of the regulations regarding the

rights and obligations on the use of the Seal.

4.2. When there is a change in the name or the version of the mobile application, if the mobile application of which name or version is changed would like to use the MAS Seal, re-application shall be submitted accordingly to the given Regulations.

4.3. When there is a change in the name, ownership and other information of the mobile application, the Mobile Application Security Alliance shall be notified immediately.

5. Tracking Management of the MAS Seal

5.1. The Mobile Application Security Alliance may, by itself or by entrusting a testing laboratory, conduct regular or irregular inspection with census or random sampling method, to confirm whether the version of the mobile application which has passed the testing is consistent with the version on which the MAS Seal is used; if not, the Alliance shall suspend its right to use the MAS Seal.

5.2. If the developer(s) of the mobile application finds that the mobile application, which had obtained the MAS Seal, may cause improper access to the mobile device, or the risks of personal data leakage, tampering, damage, or loss, the developer(s) shall notify the Mobile Application Security Alliance immediately.

5.3. When the Mobile Application Security Alliance is aware of the situation described in Section 5.2, the Alliance shall conduct a re-inspection to the mobile application in question. If the mobile application may indeed cause improper access to the mobile device, or the risks of personal data leakage, tampering, damage, or loss, the Alliance shall suspend the mobile application's right to use the MAS Seal. Also, the Alliance shall demand the developer(s) of the mobile application to conduct

improvements/corrections within a specified period; if such improvements/corrections are not made within the specified period, the right to use the MAS Seal shall be terminated.

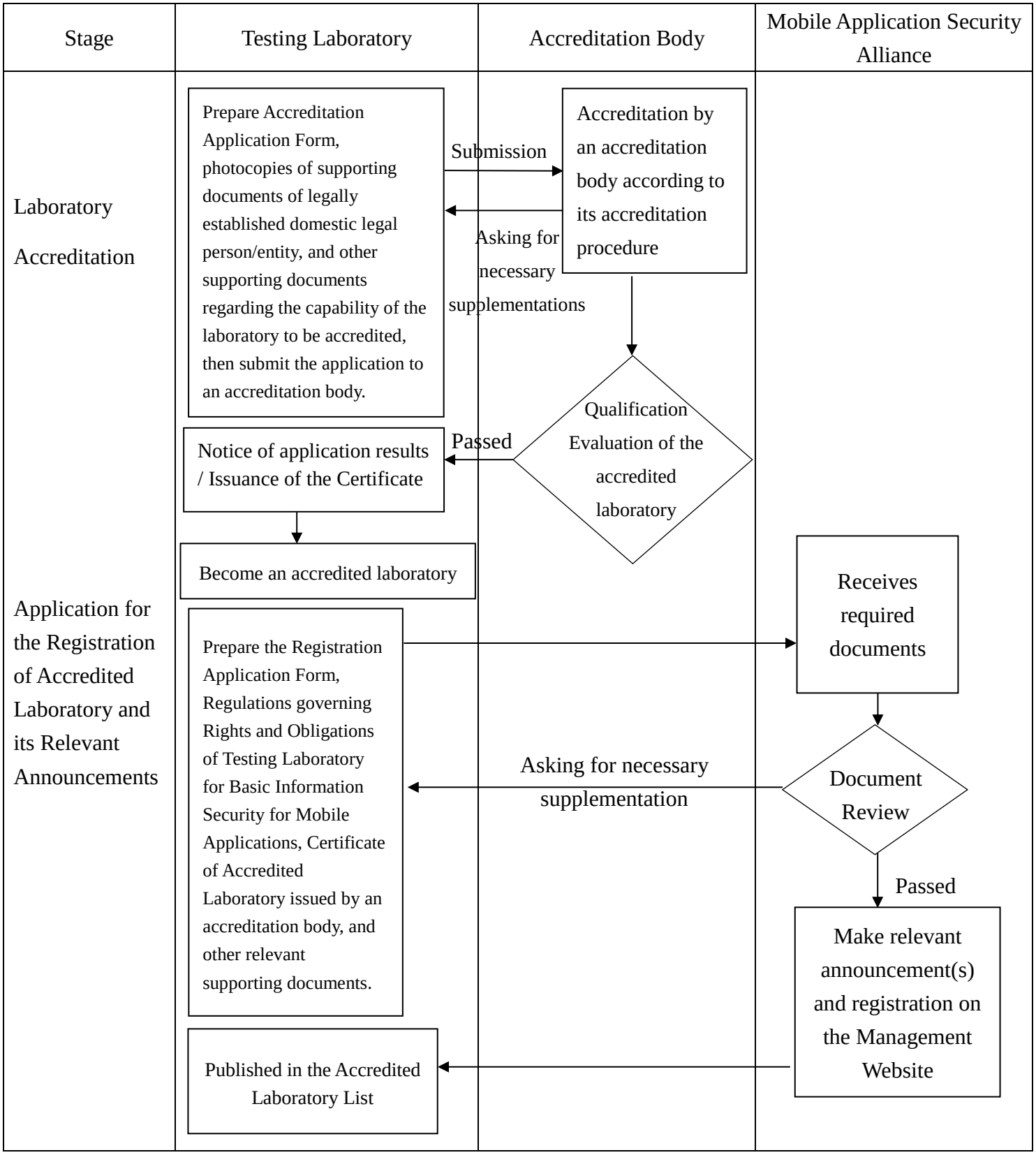
6. Fees

6.1. Inspection fee will be announced and collected by each testing laboratory. The collection of the fee shall be based on “Section 6. Principles regarding the Pricing Policy of Testing Laboratory” of the «Regulations governing the Accreditation and Management of Testing Laboratory for Basic Information Security for Mobile Applications».

6.2. Miscellaneous administrative fees will be announced and collected by the Mobile Application Security Alliance.

Appendix

Appendix I. Application Procedure of Accreditation for Testing Laboratory



Appendix II. Application Form for Registration of Testing Laboratory for Basic Information Security for Mobile Applications

The Company (hereinafter referred as the Entity Applicant) hereby submits the application to the "Mobile Application Security Alliance" for the registration of "Testing Laboratory for Basic Information Security for Mobile Applications". The Entity Applicant hereby agrees to the following terms:

I. Basic Information of the Entity Applicant

Full Name of the Entity Applicant	
Head of the Entity Applicant	
Address of the Entity Applicant	
Name of the Laboratory	
Laboratory Director	
Address of the Laboratory	
TAF Accreditation No.	
Contact Person	Name: Tel: ext. Fax: e-mail:

II. The Entity Applicant fully understands and agrees that the «Regulations governing Rights and Obligations of Testing Laboratory for Basic Information Security for Mobile Applications» (Please consult the attachment for the full text) constitutes the stipulation governing rights and obligations of both Parties.

III. The Entity Applicant authorizes the Laboratory Director of the Testing Laboratory listed in Article I to be the representative of the Entity Applicant and the Testing Laboratory, who will also be responsible for supervising the Testing Laboratory in following the Regulations enacted by the Committee.

IV. The Entity Applicant agrees that the information listed in Article I of the given Application Form can be used by the Committee in the following purposes: various types of external announcements, notification service, sending relevant messages, etc. Also, the Entity Applicant had make sure that the above-mentioned Laboratory Director and Contact Person are aware of and understand all the aforementioned matters and agree to the

reasonable collection, processing, and utilization of the aforementioned information within the scope of the purposes of collection listed above. Should there be change(s) in the information listed in Article I of the given Application Form, the Committee shall be notified within 15 days from the date of the change(s).

To:

Mobile Application Security Alliance

Seal of the Entity Applicant	Signature (or Seal) of the Head of the Entity Applicant

Date of Application: (YYYY) (MM) (DD)

As the «Regulations governing Rights and Obligations of Testing Laboratory for Basic Information Security for Mobile Applications» being a part of the given Application Form, please kindly attach them to the given Application Form and affix the official seal(s).

Appendix III. Regulations governing Rights and Obligations of Testing Laboratory for Basic Information Security for Mobile Applications

The Testing Laboratory hereby submits the Application to the "Mobile Application Security Alliance" (hereinafter referred to as the Alliance) for the registration of "Testing Laboratory for Basic Information Security for Mobile Applications" (hereinafter referred to as Testing Laboratory) of the «System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications» (hereinafter referred to as the given System). The Testing Laboratory hereby agrees to abide by the following terms:

1. The Definition of Testing Laboratory

   The testing laboratory referred in the given Regulations is the testing laboratory which had submitted application to the "Accreditation Service Program for Testing Laboratories for Basic Information Security of Mobile Applications" of the "Taiwan Accreditation Foundation" (hereinafter referred to as TAF) and had been accredited by TAF as a "Testing Laboratory for Basic Information Security of Mobile Applications".

2. The Rights and Obligations of the Mobile Application Security Alliance

   2.1. The Alliance may change the given Regulations at any time under the regulations or requirements announced by competent authorities or the Alliance; for the parts or segments directly involved with the aforementioned changes, the Alliance shall notify the Testing Laboratory within a reasonable time. After receiving the notification, if an objection is not expressed immediately by the Testing Laboratory, it will be deemed that the aforementioned changes are agreed by the Testing Laboratory.

   2.2. The Alliance shall announce the information listed on the Certificate of Accreditation on the website of the Alliance or publicize the information with other means.

3. The Rights and Obligations of the Testing Laboratory

   3.1. The Testing Laboratory shall provide the required documents relevant to accreditation (or other similar operations) accordingly to the facts, and provide relevant information in cooperation with the Alliance's regular or irregular supervision, inspection, interview, random sampling inspection and/or requirements of other operations. If the information provided by the Entity Applicant is found false or insufficient, the Alliance may notify the accreditation body to revoke the Certificate of Accreditation of the Testing Laboratory; and, the Entity Applicant shall be liable for damages (if any) caused by the misrepresentation or relevant negligence.

   3.2. When the Alliance is claimed for compensation by any third party

due to the provision of registration to the Testing Laboratory, the Testing Laboratory shall be liable for such claims.

3.3. The Testing Laboratory shall notify the Alliance of the change(s) in the following relevant information within 15 days from the date of the change(s):

a. Change(s) of the entity's name or address;

b. Change(s) of the head(s) of the entity;

c. Change(s) of the laboratory's name or address;

d. Change(s) of the laboratory director(s);

e. Change(s) in the items listed in the Certificate of Accreditation;

f. Termination or Closure of Business.

3.4. For the change(s) in the previous Paragraph, if the Testing Laboratory fails to notify the Alliance within the specified period, the Alliance may, if necessary, notify the accreditation body to revoke the Certificate of Accreditation of the Testing Laboratory.

4. The Rights and Obligations of the Testing Laboratory

4.1. The Testing Laboratory shall maintain quality systems and technical capabilities to comply with the standards and requirements set by the Alliance.

4.2. The Testing Laboratory shall accept regular or irregular supervision, inspection, interview, random sampling inspection and other operations conducted by the Alliance, and cooperate with the requirements of the Alliance in providing the required relevant information, venues, personnel, and necessary assistance to complete the operation(s).

4.3. The information security testing reports issued by the Testing Laboratory shall not be false or untrue, or be found non-conforming by the Alliance when performing random sampling inspection.

4.4. The Testing Laboratory shall adhere to a fair, impartial and independent standpoint when accepting submission(s) for inspection, and shall not refuse to accept submission(s) without justifiable reasons, or give discriminatory treatment, or conduct acts which cause breach of fairness and/or impartiality.

4.5. There shall be no relationship which impairs the impartiality of the inspection system between the Testing Laboratory and the developer(s) whose mobile application is accepted for inspection by the Testing Laboratory.

4.6. The Testing Laboratory or its service personnel shall keep all the testing-related and submitter-related information strictly confidential; and the same shall also apply to retired personnel.

4.7. Should there be any breach of the Paragraph 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, the Alliance may announce and notify the accreditation body to revoke the Certificate of Accreditation of the Testing Laboratory.

4.8. The Testing Laboratory shall archive the mobile application file(s) submitted for inspection, and keep the file(s) for at least one year to ensure that the version of the mobile application submitted for inspection is correct and is free from tampering and corruption. When a random sampling inspection is necessary, the Alliance may ask the Testing Laboratory to provide the data of the application's original file(s) archived by the Testing Laboratory.

5. Principles regarding the Pricing Policy of the Testing Laboratory

5.1. The testing fee quoted by the Testing Laboratory shall comply with the principles of transparency and fairness.

5.2. The testing fee shall be announced and collected by each testing laboratory and shall be based on the three categories of mobile applications and their respective test items defined by the latest published version of the «Basic Information Security Testing Standard for Mobile Applications».

5.3. When the Testing Laboratory informs the mobile application developer(s) that the mobile application does not meet the requirements, it shall list the items of non-conformity and notify the developer(s) to improve accordingly. The method(s) of notification and the charging mechanism will be determined by the Testing Laboratory.

5.4. The Alliance shall collect the miscellaneous administrative fees announced by the Alliance; if the Testing Laboratory is authorized by the Alliance, the aforementioned fees may be collected by the Testing Laboratory from the application submitter(s) on the Alliance's behalf.

6. Certificate of Conformity and the MAS Seal

6.1. The Testing Laboratory must handle affairs regarding the Certificate of Conformity and the MAS Seal accordingly to the given System or the «Regulations governing “Certificate of Conformity of Basic Information Security Testing for Mobile Applications” and the MAS Seal» announced by the Alliance.

6.2. The Testing Laboratory shall issue the “Certificate of Conformity of Basic Information Security Testing for Mobile Applications” based on the inspection report, in which the mobile application passed all the necessary test items of its mobile application category defined by the «Basic Information Security Testing Standard for Mobile Applications».

6.3. The format of the Certificate of Conformity will be designed and printed by the Alliance. The items to be listed on the Certificate of

Conformity are as follows:

a. Certificate serial № [which will be printed accordingly to the serial № assigning principles stipulated by the Alliance, the information includes: the Testing Laboratory's TAF accreditation number, year of issuance (in the format of Republic of China calendar), serial №];

b. Name of the applicant;

c. Name of the application; Version of the application;

d. Version of the «Basic Information Security Testing Standard for Mobile Applications»; the category of the application;

e. Validity Period of the Certificate (1 year from the date of issuance);

f. Name of the Testing Laboratory;

g. Date of Testing (i. e. the date on which the Testing Laboratory issued the test report).

6.4. For the Certificate of Conformity issued by the Alliance (which contains one original copy), the relevant examination fee will be collected.

7. Ownership of Intellectual Property

7.1. For the needs of certification, random sampling inspection or other similar operations, the Testing Laboratory authorizes the Alliance to use the documents or articles submitted by the Entity Applicant without compensation.

7.2. Unless otherwise agreed in writing between the two Parties, any intellectual property which existed before the application by the Entity Applicant is not affected by the given Instrument.

8. Breach of Contract

8.1. Unless otherwise specially provided in the given Regulations, should there be any minor breach of contract by the Testing Laboratory, the Alliance may notify the Testing Laboratory in writing in order to ask the Testing Laboratory to complete improvements within the period of one month; if there exist special reasons, the aforementioned period may be extended by one month.

8.2. If the circumstances of breach of contract, as described in Paragraph 8.1, is not improved by the specified period, and that the breach of contract is in nature a material breach, then the Alliance may notify the accreditation body to revoke the Certificate of Accreditation of the Testing Laboratory.

8.3. If the Testing Laboratory has one of the following circumstances, the Alliance may notify the accreditation body to revoke the

Certificate of Accreditation of the Testing Laboratory:

a. The Testing Laboratory provides false or untrue information when submitting the application;

b. The operation of the Testing Laboratory violates relevant laws and/or regulations;

c. The Testing Laboratory issues false certificates (or documents which serve the same purpose);

d. The Testing Laboratory makes inappropriate statements or use, causing the Alliance to be mired in controversy;

e. The Testing Laboratory exceeds the content of its Certificate of Accreditation; or the Testing Laboratory commits serious violation to the regulations of the Alliance.

9. Duty of Confidentiality

9.1. The Testing Laboratory shall provide reasonable confidentiality measures to the information provided by the application developer(s) and its relevant information. Except for the executive personnel, who have the necessity to know due to the fact that they provide or conduct application information security testing services, the Testing Laboratory shall not use, disclose, or copy any confidential information, and shall not use confidential information for other purposes.

9.2. The confidential information referred to in the previous Paragraph does not include any information in the following circumstances:

a. The information was already disclosed at the time of provision by the application developer(s); or that it was disclosed afterwards without any negligence of the Testing Laboratory.

b. The Testing Laboratory acquired the information legally from a third-party who has no duty of confidentiality to the application developer(s).

c. The information had already been held by the Testing Laboratory before the provision by the application developer(s), and the Testing Laboratory has a written record to prove it.

d. The information was independently developed by the employee(s) of the Testing Laboratory without referring to the confidential information in any way, and the Testing Laboratory has a written record to prove it.

e. The information was provided due to the request of law/regulations and/or by a governmental agency.

9.3. Either Party to the given Instrument is free to decide whether to inform the other Party of the following information:

a. Confidential information of the other Party obtained from a third party.

b. Laws, regulations, technical rules, or technical standards which are applicable to accreditation.

c. Information which shall be disclosed by the accreditation body as required by laws/regulations.

10. Liability

10.1. If the Testing Laboratory abuses the accreditation issued by the accreditation body, and subsequently causes damages to the Alliance, the Testing Laboratory shall be liable for the damages to the Alliance.

10.2. Each Party shall be solely responsible for the damages to any third party resulted from the causes attributable to themselves.

10.3. Either Party to the given Instrument shall immediately notify the other Party upon knowing any event that may cause the above-mentioned claims for compensation, and shall take any possible measures to prevent the occurrence and/or expansion of the damages.

11. Miscellaneous Matters

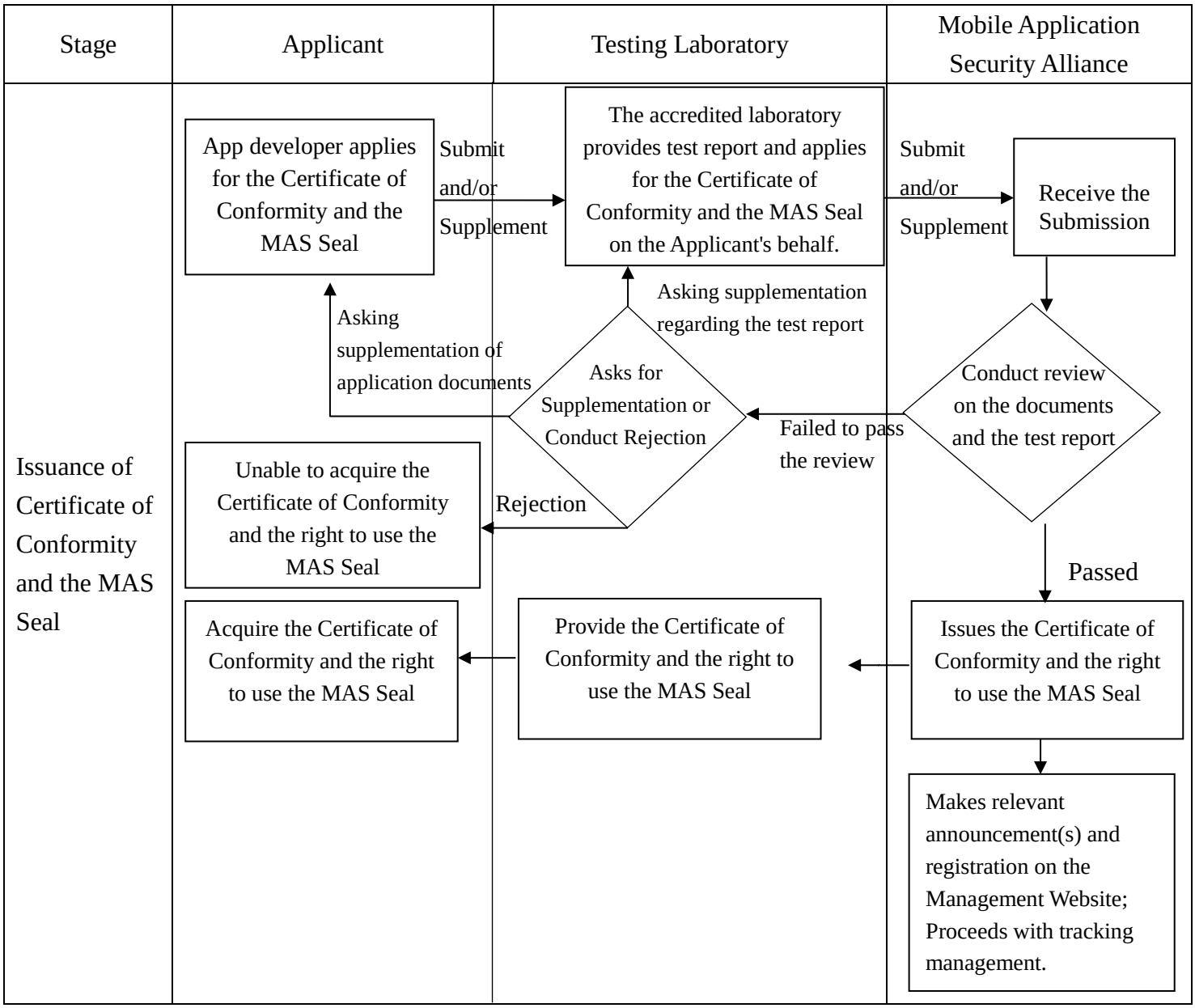
11.1. Upon any controversy, dispute, disagreement or breach regarding the given Regulations, an application for arbitration shall be filed in accordance with the Arbitration Law of the Republic of China, with Taipei City as the seat of arbitration.

11.2. Any matters not covered in the given Instrument may be stipulated through another supplementary agreement signed by both Parties.

(The remainder of this page is intentionally left blank.)

Appendix IV. Application Procedure for Certificate of Conformity of Basic Information Security Testing for Mobile Applications and the MAS Seal

For a mobile application that has passed the inspection of a testing laboratory, the testing laboratory shall issue "Certificate of Conformity of Basic Information Security Testing for Mobile Applications" and the MAS Seal based on the inspection report, in which the mobile application passed all the necessary test items of its mobile application category defined by the «Basic Information Security Testing Standard for Mobile Applications».



Appendix V. Application Form for Certificate of Conformity of Basic Information Security Testing for Mobile Applications and the MAS Seal

The Company (hereinafter referred as the Entity Applicant) hereby submits the application to the "Mobile Application Security Alliance" (hereinafter referred to as the Alliance) for the use of the Mobile Application Basic Security Seal (hereinafter abbreviated as the MAS Seal). The Entity Applicant hereby agrees to abide by the following terms:

I. Basic Information of the Entity Applicant

<table>
<tr><td colspan="4">Basic Information of the Mobile Application</td></tr>
<tr><td>Date of Application</td><td colspan="3">(YYYY) (MM) (DD)</td></tr>
<tr><td>Name of the Mobile Application</td><td colspan="3"></td></tr>
<tr><td>Operating System</td><td colspan="3">□ Android □ iOS</td></tr>
<tr><td>Application Version</td><td></td><td>Version of the «Basic Information Security Testing Standard for Mobile Applications»</td><td></td></tr>
<tr><td>Security Category</td><td>□L1 □L2 □L3</td><td>Additional Testing Items</td><td>□F</td></tr>
<tr><td rowspan="2">Category of the App [Main function(s); single selection]</td><td>□ Governmental</td><td colspan="2" rowspan="2">□ Finance □ Mobile Payment
□ Shopping □ Business
□ Communication (Telephone, messaging, meeting software) □ Medical Care (Medicine) □ Health (Sports, fitness, pregnancy) □ Education □ Weather
□ Social Life □ Video/Audio
□ Camera □ Map/Navigation □ Travel (local information) □ Image (Art, design)
□ Entertainment (Game, comic)
□ Tools/Application (Developer tools, productivity tools, program library and trial of programs, watch application)
□ Other: _____</td></tr>
<tr><td>□ Non-Governmental</td></tr>
<tr><td>Competent Authority (Multiple answers are</td><td>□ Central Governmental Agency</td><td colspan="2">□ Executive Yuan □ Legislative Yuan
□ Judicial Yuan □ Examination Yuan</td></tr>
</table>

<table>
<tr><td rowspan="2">accepted.)</td><td></td><td>□ Control Yuan
Name of the Agency: _____</td></tr>
<tr><td>□ Local Governmental Agency</td><td>□ New Taipei City □ Taipei City
□ Keelung City □ Taoyuan City
□ Hsinchu County □ Hsinchu City
□ Miaoli County □ Taichung City
□ Changhua County □ Nantou County
□ Yunlin County □ Chiayi County
□ Chiayi City □ Tainan City
□ Kaohsiung City □ Pingtung County
□ Yilan County □ Hualien County
□ Taitung County □ Penghu County
□ Kinmen County □ Lienchiang County
Name of the Agency: _____</td></tr>
<tr><td>Willingness in Submitting the Application for Inspection</td><td colspan="2">□ Voluntary
□ Policy Requirement (required by the competent authority)</td></tr>
<tr><td colspan="3">Testing Entity</td></tr>
<tr><td>Name of the Testing Entity</td><td colspan="2"></td></tr>
<tr><td>Name of the Testing Laboratory</td><td colspan="2"></td></tr>
<tr><td>Date of the Submission for Testing</td><td colspan="2">(YYYY) (MM) (DD)</td></tr>
<tr><td>Date of the Completion of Testing</td><td colspan="2">(YYYY) (MM) (DD)</td></tr>
<tr><td>Test Report №</td><td colspan="2"></td></tr>
<tr><td colspan="3">Information of the Mobile Application Vendor</td></tr>
<tr><td>Name of the Entity applying the Certificate</td><td colspan="2">□ Entity Submitting the App for Testing (App Owner)
□ Entity Developer (App Developer)</td></tr>
</table>

Name of the Entity	(Required)
VAT Id. №	(Required)
Address of the Entity	(Required)
Name of the Entity Developer	(Required)
VAT Id. №	(Required)
Address of the Entity Developer	(Required)
Name of the Contact Person(s)	(Required)
Telephone № of the Contact Person(s)	(Required)
E-mail of the Contact Person(s)	(Required)
Announcements	
Make relevant announcement(s) on the MAS Website?	□ Yes. □ No.
Release Status	□ Released. □ Unreleased; expected release date: _____ (YYYY/MM/DD) □ For internal use only, will not be publicly released.
URL of App on the Application Store	
Application for Certificate in English	
Applying for Certificate in English?	□Yes. (Please complete the rest of the form) □ No.
Name of the App (EN)	
Name of the Entity (EN)	[* Please fill the "Name of the Entity applying the Certificate" in English]

Name of the Testing Entity (EN)	
Name of the Testing Laboratory (EN)	

II. The Entity Applicant fully understands and agrees that «Regulations governing the Rights and Obligations on the Use of Mobile Application Basic Security Seal» constitutes the stipulation governing rights and obligations of both Parties.

III. If the Applicant causes damages due to the provision of misinformation, the Applicant will be willing to bear responsibility accordingly to the relevant laws, and the Applicant shall also ensure that it has the right to put the mobile application on the application store.

To:

Mobile Application Security Alliance

Signature or Seal of the Laboratory Director of the Testing Laboratory
(Required)
Signature or Seal of the Case Officer of the Entity Submitting the App for Testing (App Owner)
(Required)
Signature or Seal of the Case Officer of the Entity Developer (App Developer)
(Required if the App was submitted for testing by the Entity Developer)

As the «Regulations governing the Rights and Obligations on the Use of "Mobile Application Basic Security Seal"» being a part of the given Application Form, please kindly attach them to the given Application Form and affix the official seal(s).

Appendix VI. Regulations governing the Rights and Obligations on the Use of Mobile Application Basic Security Seal

The Entity Applicant hereby submits the application to the "Mobile Application Security Alliance" (hereinafter referred to as the Alliance) for the use of the Mobile Application Basic Security Seal (hereinafter abbreviated as the MAS Seal). The Entity Applicant hereby agrees to abide by the following terms:

1. Period of Use of the MAS Seal

   The validity period of MAS Seal is 1 year. The Alliance agrees that the Entity Applicant can use the MAS Seal with the name of the mobile application provided on the Application Form.

2. Methods of Use of the MAS Seal

   2.1 The Entity Applicant shall use the MAS Seal on the webpage of the application store in accordance with the style specified by the Alliance, and shall not change the shape, color or put on any additional text. If there is any need to use the MAS Seal in a different fashion, an application shall be submitted to the Alliance with the Application Form for Exceptional Use of the Mobile Application Basic Security Seal.

   2.2 The MAS Seal shall not be used by the Entity Applicant for purposes other than a certification seal.

3. Legal Basis for the Use of the MAS Seal

   The Entity Applicant, when using the MAS Seal, shall strictly abide by the relevant regulations, such as the «Regulations of the System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications» and the «Regulations governing the Use and the Management of Mobile Application Basic Security Seal».

4. The Rights and Obligations of the Mobile Application Security Alliance

   4.1 The Alliance may change the given Regulations at any time under the regulations or requirements announced by competent authorities or the Alliance; for the parts or segments of the aforementioned changes which are directly involved with the Entity Applicant, the Alliance shall notify the Entity Applicant within a reasonable time. After receiving the notification, if an objection is not expressed immediately by the Entity Applicant, it will be deemed that the aforementioned changes are agreed by the Entity Applicant.

   4.2 The Alliance shall announce the serial № of the MAS Seal listed on the Certificate of Conformity on the website of the Alliance or publicize the information with other means.

5. The Rights and Obligations of the Mobile Application Developer(s)

5.1 The Entity Applicant agrees to accept random inspections by the Alliance at an irregular basis at any time, and shall not refuse with any reason. If the Alliance finds that the Entity Applicant does not meet the requirements of the given Regulations or the requirements of the «Basic Information Security Testing Standard for Mobile Applications», the Alliance may immediately notify the Entity Applicant to stop using the MAS Seal and may make relevant announcements.

5.2 After the Alliance issues a notification or an announcement, the Entity Applicant shall immediately stop using the MAS Seal and recall the relevant advertising materials. After the Alliance gives a written notice to ask the Entity Applicant to make relevant improvements within a specified period. And the Alliance will conduct a review after the lapse of the specific period; if the review indicates that the requirements are still not met, the Alliance may terminate the use of the MAS Seal.

5.3 During the validity period of the MAS Seal, if the Alliance finds that the Entity Applicant had obtained the permission to use the MAS Seal by fraud, coercion, counterfeiting, alteration, or other improper means, the Alliance may terminate the use of the MAS Seal. The Entity Applicant shall be responsible for recalling advertising materials and compensating the Alliance for any damages incurred by the incident.

5.4 The Entity Applicant agrees that when there is any change(s) in the name, ownership and any other information of the mobile application, the Entity Applicant shall report to the Alliance with relevant supporting documents.

5.5 During the validity period of the MAS Seal, if the Entity Applicant has one of the following circumstances, the Alliance shall terminate the Entity Applicant's right to use the MAS Seal, and the Entity Applicant shall not raise any objection:

a. The Entity Applicant submits application for the termination of the use.

b. The Entity Applicant is dissolved or closed.

c. The business registration certificate of the Entity Applicant has been revoked by the competent authority in accordance with the laws.

d. The Entity Applicant violates Article 2 of the given Regulations.

e. The Entity Applicant violates Article 6 of the given Regulations.

f. The Entity Applicant violates Paragraph 7.1 and 7.2 of the given Regulations, in which the Entity Applicant did not notify the Alliance or did not complete the improvements within the specified period.

g. The Entity Applicant evades, hinders or refuses the irregular

random sampling inspection conducted by the Alliance.

h. The certified mobile application of the Entity Applicant is found not meeting the requirements of the «Basic Information Security Testing Standard for Mobile Applications» via re-examination by conducting random sampling inspection.

i. The MAS Seal of the certified mobile application of the Entity Applicant had lost its validity in accordance with the Paragraph 8.4 of the «Regulations of the System for the Promotion of Voluntary Inspection on Basic Information Security for Mobile Applications». If the Alliance terminates the Entity Applicant's right to use the MAS Seal, the Alliance shall notify the Entity Applicant in writing to stop using the MAS Seal and remove the MAS Seal (and its relevant symbols) from the application store within a specified period. If the Entity Applicant fails to remove the MAS Seal within the specified period, the Entity Applicant shall compensate the Industrial Development Bureau of the Ministry of Economic Affairs (hereinafter referred to as the IDB) and/or the Alliance for all the damages incurred thereby.

6. Breach of Contract

6.1 The Entity Applicant guarantees that the MAS Seal will only be used on the mobile application listed in Article 1 of the given Regulations; consequently, on other mobile applications, the MAS Seal shall not be used.

6.2 The right to use the MAS Seal obtained by the Entity Applicant in accordance with the given Regulations shall not be assigned, traded or transferred to any third party. If the Entity Applicant breaches this Paragraph, it shall compensate the IDB and/or the Alliance for all the damages caused thereby.

7. Liability

7.1 If the Entity Applicant finds that their mobile application, which had obtained the MAS Seal, may cause improper access to the mobile device, or the risks of personal data leakage, tampering, damage, or loss, the Entity Applicant shall notify the Alliance.

7.2 When the Alliance is aware of the situation described in the previous Paragraph, the Alliance shall conduct a re-inspection to the mobile application in question. If the mobile application may indeed cause improper access to the mobile device, or the risks of personal data leakage, tampering, damage, or loss, the Alliance shall suspend the validity of the MAS Seal of the mobile application and demand the Entity Applicant to conduct improvements/corrections within a specified period.

7.3 The Entity Applicant agrees that if the breach of the given Instrument damages the rights and interests of the IDB and/or the Alliance, the Entity Applicant is willing to take full responsibility for the compensation.

7.4 After the Entity Applicant had passed the inspection on the use of MAS Seal and had signed the given Regulations, the Entity Applicant shall actively cooperate in various technical seminars, training seminars, and promotional activities carried out with the aim of promoting the MAS Seal by the IDB and/or the Alliance.

8. Miscellaneous Matters

8.1 For disputes arising from the application, testing, use, suspension, or termination of the MAS Seal, within 1 month from the date of receipt of the relevant notice, an appeal shall be filed to the Alliance, in which the reasons and demands shall be clearly stated in writing. The Alliance shall inform the complainant of the results of the appeal in writing within one month from the date of receipt of the appeal.

8.2 Disputes arising from the application, testing, use, suspension, or termination of the MAS Seal may be filed for mediation or be handled in accordance with civil procedures with the Taipei District Court be the court of first instance jurisdiction.

8.3 The exchange of notes of the given Instrument, which are supplemented/amended afterwards, shall all be deemed to be a part of the given Instrument and shall have the same effect as the given Instrument.

(The remainder of this page is intentionally left blank.)

Appendix VII. Application Form for Exceptional Use of the Mobile Application Basic Security Seal

Date of Application: (YYYY) (MM) (DD)

Name of the Applicant	
Name of the Mobile Application	(Chinese) (English)
Description of the Exceptional Use(s)	(Please list the method(s) and the location(s) needed for the exceptional use and/or posting of the MAS Seal.)