JISEC-CERT-2023-C30

JISEC

Impact Analysis Report Preparation Guidance

Version 3.0

Japan Information Technology Security Evaluation and Certification Scheme
Information-technology Promotion Agency, Japan

Issued on December 15, 2023

Revision History

Version	Date of Issue	Main Changes
2.1	2022/4/1	Change of the JISEC Scheme Documentation and division name
3.0	2023/12/15	Correspondence to CCRA Requirements Ver. 3.0 (e.g., the abolition of certificate validity for maintenance)

Table of Contents

1. Introduction

This document should be used as a reference when considering application for maintenance of CC certified TOEs. It contains viewpoints in determining whether changes to a TOE or its environment are within the scope of maintenance, and cites examples of the contents of an “Impact Analysis Report” necessary for maintenance application.

An application for maintenance can be submitted within the certificate validity period of the TOE (up to three months prior to the certificate validity period). Note that the certificate validity period will not be changed even when the maintenance is approved.

Please refer to “Assurance Continuity: CCRA Requirements” [1] for the meaning and process of maintenance, and to “Requirements for IT Security Certification (CCM-02)” [2] and “Guidance on IT Security Certification (CCM-02-A)” [3] for the JISEC Scheme Documentation and procedures relating to the maintenance.

2. Glossary

The definitions of terms used in this guidance document are described below:

- Certified TOE

  The TOE version which has been evaluated and for which a “certificate” has already been issued.

- Changed TOE

  A version of TOE different from a certified TOE resulting from changes being applied to a certified TOE.

- Developer Documentation

  All necessary items describing the content of changes of a changed TOE with regard to a certified TOE. The items must be usable for verification.

- Maintenance

  The process of identifying changes made to the certified TOE and its development environment and providing assurance that those changes have not adversely affected the assurance at the time of certification.

- Re-evaluation

  An evaluation equal to the original one conducted by the Evaluation Facility if assurance is no longer able to be maintained. Note that an application for re-evaluation is treated in the same way as a new application for certification under the JISEC Scheme Documentation.

- Subset evaluation

  An evaluation of only those assurance components (e.g., ALC_DEL.1) which are affected by the change in the development environment, in a case where the maintenance is applicable and changes in the assurance measures of the development environment are changed.

3. Determination of Maintenance Application

Maintenance is the process of identifying “changes” made to the certified TOE and its development environment and providing assurance that those changes have not adversely affected the assurance at the time of certification. In a case where the changes adversely affect the assurance, maintenance cannot be applied.

The following describes an overview of the changes to be covered by maintenance, the impact of the changes, and an impact analysis.

(1) “Changes” to be covered by Maintenance

“Changes” made to a certified TOE subject to maintenance are not intended to apply to new products and functions derived from a certified TOE. Within the scope of security functional specifications that had been evaluated for the certified TOE, only those “changes” for which, without requiring a third-party evaluation, developers (applicants) on their own responsibility can verify and claim that assurance will not be adversely affected will be applicable for maintenance. Such changes would include corrections to software and guidance defects or operational environment additions which do not incur changes to TOE functions.

Basically, the conditions for maintenance regarding the changes to a certified TOE are that the contents of developer documentation used in the evaluation of the certified TOE have not been changed semantically so that those changes do not affect the evaluation of the certified TOE performed by the evaluator. In addition, the conditions for maintenance regarding the changes to the development environment of the certified TOE are that those changes are within the scope of the development environment and do not affect security behaviours of the certified TOE. Therefore, some changes to the development environment in which maintenance is applicable will include the changes that may affect the evaluation by evaluators, unlike the case of the changes of the certified TOE. In that case, it is necessary to conduct a subset evaluation by the Evaluation Facility to identify the impacts by the changes.

Note that the changes in various attacks landscape affecting the vulnerability assessment of a certified TOE, such as new vulnerabilities or attack methods discovered since the certified TOE was initially certified, are not included in the scope of “changes” in maintenance.

(2) Impact of the “Changes”

Developers analyse the impact of “changes” to a certified TOE or its environment to determine whether each of the changes has a major impact or minor impact on security assurance of the certified TOE. If the developer can demonstrate that those changes to a certified TOE or its environment have a minor impact on security, those changes can be considered within the scope of maintenance.

For example, it is considered that major impacts will arise from changes to implementation of security functions provided by the TOE, notice or usage of the TOE

described in the guidance. On the other hand, it is thought that corrections of output messages unrelated to security functions or typographical errors in the guidance will have a minor impact. In addition, it is thought that changes to structure and procedures of entrance/exit management in development environment, which do not affect security functions of the certified TOE or guidance, will have a minor impact.

However, there are no absolute indicators for judging whether "changes" to a certified TOE or its environment have a major impact or minor impact on security, including examples mentioned herein.

(3) Impact Analysis of the "Changes"

The determination of the impact that changes will have on security is based on an understanding of the assurance scope of the certified TOE and demonstration through developer analysis. If changes clearly do not affect the assurance scope of the certified TOE, the changed TOE will be applicable for maintenance. In case that changes clearly affect the assurance scope of the certified TOE, re-evaluation will be necessary if the impact is major. If impact is minor, it will be necessary to make such a demonstration and compile an Impact Analysis Report.

As a reference to determine the extent of impact of changes on the assurance scope of the certified TOE, a "Checklist for Maintenance Application" is provided as an addendum to this document. The checklist provides a general summary of the kinds of items that are evaluated and assured at each assurance level. Confirming the degree of relevance that changes have to the assurance scope before implementing a detailed impact analysis for each change will enable one to decide on a re-evaluation without compiling an Impact Analysis Report or to focus on specific areas for in-depth analysis. Of course, when a re-evaluation is decided, since an Impact Analysis Report compiled by developers will be useful for evaluators, one can choose to compile an Impact Analysis Report irrespective of the scope of impact on security or application for maintenance.

Developers will demonstrate in their impact analysis of the changed TOE that the changes will have little impact on the assurance level of the certified TOE. This demonstration should be reported by developers, along with the technical background, as a result of conducting sufficient examinations. It is necessary that sufficient examinations be conducted at a deeper level than the assurance level of the certified TOE. For example, it is not enough to claim that changes to internal specifications which are not related to TOE security functions do not incur direct changes to external interface specifications for certified TOE security functions. Impacts to some parameters and messages of the external interface of security functions are sometimes discerned by examining the implementation representation of a changed area. Even when claiming that changes in operational environment do not involve any changes to TOE external interface specifications, developers should sufficiently consider the possibility that logic which was not activated in the certified TOE may be involved due to the interface invocation procedure, invocation timing, and supplied parameters.

The Certification Body will examine the Impact Analysis Report submitted by the developer and determine whether maintenance is applicable or not. If there are any unclear

points relating to the rationale of the developer's claims during the examination process, the Certification Body will request that detailed documents relating to the impact analysis process be provided and will conduct direct consultations with the developer to confirm the contents. Refer to Chapter 4 of this document for the description contents of the Impact Analysis Report.

4. Impact Analysis Report Preparation

If the developer judges that the changes do not adversely affect the assurance scope of the certified TOE, the developer will conduct analysis of the content of changes, and will examine the impact on security. To apply for maintenance, the results of impact analysis must be compiled into a report. The minimum contents which must be included in the Impact Analysis Report are indicated in Chapter 5 of "Assurance Continuity: CCRA Requirements" [1].

The Impact Analysis Report must be described in sufficient detail to make understand that changes have no impact on the assurance scope of the certified TOE, with non-disclosure information where necessary. The Impact Analysis Report will not be published by the Certification Body. It is also possible to include non-public information. The "Maintenance Report" which is published information relating to maintenance will be prepared by the Certification Body based on this Impact Analysis Report. After reviewing the "Maintenance Report" by the developer, the report will be published with approval from both the developer and the Certification Body.

Examples and points to keep in mind when preparing the Impact Analysis Report are shown below according to the composition of the Impact Analysis Report. Note that description formats other than the composition of the chapters can be arbitrary, and do not need to follow the examples.

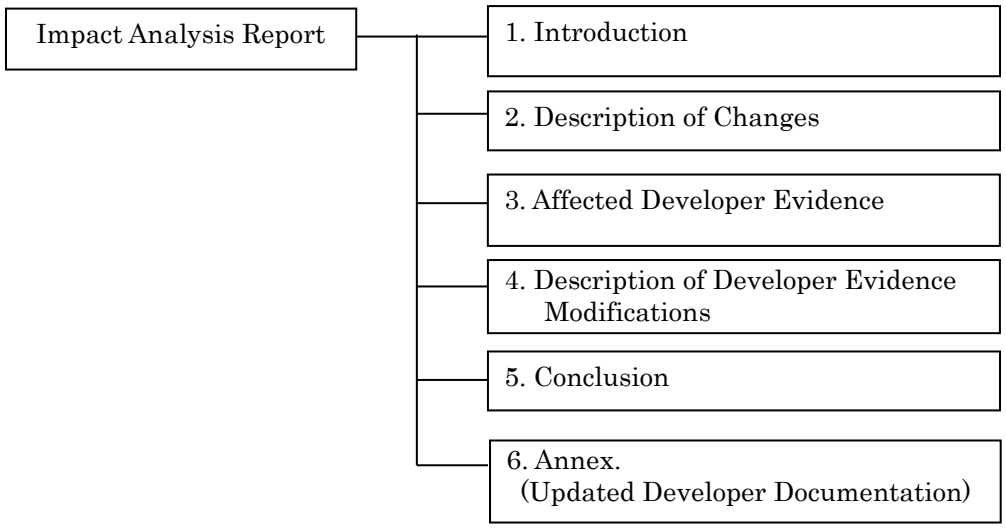

Figure 1: Composition of Impact Analysis Report

(1) Introduction

The introduction shall describe identification information for requisite materials. It may also contain information for which developers have determined as particularly requiring caution, such as the handling of the report.

1.1 Impact Analysis Report Identification

Name of Document: JISEC Ewallet SecureTrade Impact Analysis Report
Version of Document: 1.0.1
Creation Date: 2022-02-02
Author: JISEC Co., Ltd.

1.2 TOE Identification

Name of TOE: JISEC Ewallet SecureTrade
Version of TOE: Rev. 3
Developer: JISEC Co., Ltd.

1.3 Certified TOE Identification

Certification No.: C00XX
Name of TOE: JISEC Ewallet SecureTrade
Version of TOE: Rev. 2
Evaluation Assurance Level: EAL3
PP Conformance: There is no PP to be conformed.

The identifications of the ST, Evaluation Technical Report, and Certification Report of the certified TOE, should also be described.

(2) Description of Changes

The description of changes shall describe all changes made to the certified TOE and its environment. Even if maintenance has already been applied before, all changes from the time of the initial certification are subject to the description.

All changes including those judged not to affect security shall be described.

The purpose of changes, changes to products, changes to the development environment, and changes to the IT environment shall be described in the description of changes.

a. Purpose of changes

The purpose of changes shall first explain the background for why changes to the TOE became necessary. This section shall describe an overview of the changes with regard to the certified TOE. The details of each change will be described in subsequent sections.

2.1 Purpose of Changes

Additions to the guidance documentation relating to new operating hardware, functional improvements, and flaw remediation have been performed. The following is an overview of these changes:

1) Guidance modifications in response to new Type D additions to JISEC Ewallet on which the TOE operates. There are no changes to the TOE program itself due to these additions.
2) Program modifications to shorten boot time as automatic reboot was taking too long in the event of authentication failures.
3) Program modifications in response to an implementation bug in which log

information becomes empty when the audit log reaches the specified capacity during log information acquisition and file renaming is conducted.

In the event that there are numerous small bug fixes that do not involve specification changes, it is acceptable to describe the overall purpose in this section (boundary value issues in the implementation, performance improvement, etc.) and to describe the contents of each change in subsequent sections.

b. Changes to products

This section shall describe changes made to the certified TOE. Regarding the level of detail of the descriptions, the information to be included shall have sufficient precision for a third party (Certification Body) to be able to understand the developer's impact analysis claims. In some situations, the submission of additional documentation would be required for the judgement of applicability of maintenance.

It should be noted that where the changes were made (whether to the source code or to the procedure manual, etc.), why these changes were made, and specifically how they were changed should be clearly described so that the impact of the assurance scope of the certified TOE can be understood. If the assurance level of the certified TOE was EAL2, detailed information that shows the impact of changes at the level of functional specifications and subsystems is required. Therefore, there are cases where the detailed information that is not described in the specification at the level of functional specifications or subsystems is required, but even then, descriptions at the source code level will not be required.

No.	**Type of Change**	**Overview**	**Details**
S2-1	Performance improvement	Improving auto reboot time in the event of authentication failures	The boot routine program was changed, and verification of TSF parameter values, network release and network restructuring conducted during booting are skipped if authentication failure flag is set and the system error flag is not set.

c. Changes to the development environment

This section shall describe changes made to the development environment. All changes falling within the scope of assurance requirements for the certified TOE including those points judged to have a minor impact shall be listed. For example, all changes, such as changes to the development security, changes to versions of TOE configuration items in configuration management, changes to the method of identifying configuration items, and changes to configuration management procedures, among others.

D3-1	Development security	Changes to equipment for controlling entry to the development environment	Employee cards were updated, and the equipment for entry control to the development room was changed from authentication using old employee cards (magnetic) to authentication using new employee cards (contactless IC cards). There were no changes to entry procedures, etc.

d. Changes to the IT environment

This section shall describe the changes to the IT environment for the certified TOE. This environment includes hardware, firmware, and software requiring security functions which are subject to evaluation such as external services that the TOE depends on, among others. It also includes all hardware, firmware, and software constituting the TOE operational environment.

E2-1	Operating hardware	Additions to operating hardware	Additional operating assurances for "ISEC SS V.7," OEM version of the operating hardware "JISEC SecureSwitch 07."

(3) Affected Developer Evidence

This section shall identify all developer evidence that were used in evaluating the certified TOE and which will require changes or additions. The developer evidence used in evaluating the certified TOE is listed in the Evaluation Technical Report of the certified TOE.

Developers shall determine which developer evidence should be updated according to the changes made to the TOE and environment indicated in the previous description of changes. This determination shall employ a systematic method which considers the respective assurance components of certified TOE. This section shall list only the identification of developer evidences to be updated. The impact on each assurance component shall be determined with reference to Chapter 4 "Performing Impact Analysis" in the "Assurance Continuity: CCRA Requirements" [1]. For example, there are methods such as identifying the details of developer evidence associated with each developer action element as shown in the table below, and confirming their impact.

Developer Action Elements	Developer Documentation
ASE_INT.1	JISEC SmartModule Security Target Version3.1
	ST introduction
ASE_CCL.1	JISEC SmartModule Security Target Version3.1
	Conformance claims
…	…
ATE_FUN.1	JISEC SmartModule Functional testing

Of the developer evidences identified, this section calls for listing only those which need

to be updated as affected developer evidence. How these changes are associated with the assurance scope of the certified TOE and what impacts they have are described in the next section.

(4) Description of Changes to Developer Evidence

An overview of the changes to all developer evidence identified in "(3) Affected Developer Evidence" shall be described. While it is not necessary to provide a detailed description of changes to developer evidence, what was changed, why, and how it was changed to the developer evidence shall be clearly and concisely described.

This section shall describe the content of the changes in appropriate units such as for each assurance component, each change item, or each updated developer evidence, along with their references.

JISEC EasyLAN Functional Specifications			
Section Number	No	Content of Changes	Location of Change
S1-1(F)	1	In response to not supporting FDDI: ・removed FDDI from installation menu	2.1.2
	2	・removed FDDI message for error number [4]	2.5
S2-1(F)	1	Added verification logic for the code for IPA to the license key CD verification program.	3.1.1 A.3

In updating developer evidence, it is necessary to confirm that functions of the certified TOE, including those which haven't changed, operate correctly (regression test). Similarly, if an assurance component from the AVA class is included in the assurance components, it shall be confirmed that there were no impacts with regard to vulnerability. These will be confirmed by re-performing the tests, etc., which had been conducted when evaluating the certified TOE. Even if there are no major changes to security functions, there may be cases where new tests will be required. In such cases, it is necessary the developer shall include in the Impact Analysis Report what tests were additionally implemented and for what purpose.

(5) Conclusion

The judgements of whether the changes have a major impact or a minor impact on developer evidence along with the rationale for these judgements shall be described. In addition, the judgements of whether subset evaluation is required or not and the rationale for these judgements shall also be described.

a. Impact of each change

The impact of each change to developer evidence on the assurance of the certified TOE shall be described. With regard to the rationales for these claims, the developer's impact analysis results shall also be outlined in relation to "(2) Description of Changes" and "(4) Description of Developer Evidence Modifications."

Developers shall analyse the impacts of these changes across a broad range and at sufficient depth. To confirm that the certified assurance scope is not affected, analysis at a deeper level than the assurance level for the certified TOE will be necessary. For example, there are cases where changes to the source code of a given module do not involve direct changes to the external interface but may affect the error code of an indirectly called security function, or that even small changes to the start-up script may affect the start-up timing and processing time assumed for other functions. Having no such impacts should be explained technically. In addition to performing those impact analyses, it is necessary for developers to confirm with a regression test that the changes have no actual unexpected impacts.

Developers shall also be aware of consistency with developer evidence. For example, when a message displayed by the TOE is changed, it will affect not just function specifications but guidance or test specifications.

Based on the results of the analysis of the impact of changes, developers shall determine whether these changes have a major impact or a minor impact and shall report it along with their rationales. There is no general method for identifying whether impacts are major or minor. Refer to Chapter 3 “Characterisation of changes” of the “Assurance Continuity: CCRA Requirements” [1] for a general guideline.

[S3-3] Revision of the time-out period in the event of client communication disconnections			
This is a program change relating to error processing of a post-processing process for service authentication of a security function which involves impacts to specifications and administrator guidance. However, it is judged as follows that there are no direct impacts to the interface relating to security functional behaviour and secure management by the administrator, and that the impacts of these changes are minor.			
S3-3(F).1		In the specifications for “service authentication functions” in “Flow Manager Utility functions specifications,” the impacts of post-processing are as follows: 1) There are no changes to the post-processing call method or to parameters. 2) During post-processing, ・ There are no interactions with the users or other modules. ・ There are no operations interrupted (including during the shortened 7 seconds) 3) At the completion of post-processing, ・ There is no change to the error number returned. In other words, there is no change in the specification with regard to the error number [7] of error processing of the service authentication function. ・ There are no other processes which are dependent on post-processing timing.	ADV_FSP.2

		・ Although message timing displayed on the administrator interface will be 7 seconds earlier, the impact is minor as described in S3-2(G).1. The impact from changes to "Flow Manager Utility functions specifications" is judged to be minor.	
S3-2(G).1		Impacts of the change to the descriptions relating to time until error message display ("approx.10 seconds later" → "3 seconds later") in "Service authentication" of "Flow Manager Utility Guidance" are as follows: 1) There are no security management items involved during the time from service authentication start-up until error message display. 2) There are no changes to the content of the displayed error message, nor any changes to the actions to be taken by the administrator after message confirmation. Therefore, impacts from the change to "Flow Manager Utility Guidance" are judged to be minor.	AGD_OPE.1

Furthermore, the results of confirming (through a regression test) that security functions operate similarly for the changed TOE in the same way as the certified TOE shall also be described. In some cases, new tests may be required to confirm if the changes to security functions perform correctly or a regression test to confirm having no unexpected impact by the changes. The purpose and results of the newly conducted test shall also be described. It is not necessary to describe test procedures and detailed information in the Impact Analysis Report. The developer shall describe the perspective from which the test was implemented to confirm maintenance of assurance.

b. Overall impact

While changes may have little impact individually, they may have a major impact on a TOE through accumulation or interaction. Developers shall analyse each individual change as well as the overall impact on the TOE as a result of these changes. This section shall determine significance of the impact from the analysis results and describe it along with its rationale.

[Overall] Overall impact on the TOE
[S1-F] and [S2-F] are changes to processing during installation and during operation respectively. As there is no interaction between them, TOE operation is not affected due to their combination. Therefore, the overall impact through accumulation or interaction of changes can be judged as a minor.

Rationale		As indicated in the impact analysis of [S1-F] and [S2-F], each change is a closed process in a separate function of the different functionality, and there are no changes that may affect other programs such as a change to external variables. Therefore, the combination of those changes will have no new impact on the TOE.	

(6) Appendix

This section shall describe the identifications and list of items of the developer evidences updated by the changes.

a. List of updated developer evidences

The information necessary to identify developer evidence for the changed TOE as a list including developer evidence name, issue date, and version, among others shall be described.

b. List of updated items of developer evidences

The information necessary to identify changed items, that is, a list of the changed items and changed areas of each updated developer evidence shall be described. It is not necessary to include minor changes which are not related to the impact analysis (for example, the approval date for revisions).

5. Notes

Some points to which particular attention should be paid by developers for judging maintenance and preparing the Impact Analysis Report will be discussed in this chapter.

(1) Responsibility of Developers

In maintenance, developers themselves shall make a technical determination that the objective assurance which a third party evaluated can remain valid and declare the result to governmental procurement division. Developers should make a judgement about maintenance with accountability such as submitting materials that can verify what analysis was made on the impact of the change if any problem occurs with the changed TOE.

(2) Description of the Impact Analysis Report

The Certification Body will determine the impact that each change has on assurance based on the submitted Impact Analysis Report. The Impact Analysis Report needs the description of rationale based on technical analysis so that the Certification Body can objectively understand the impacts of the changes.

In the event the Impact Analysis Report contains non-technical analysis and enumeration of subjective claims such as “it is thought not to have an impact” or contains contradictory analysis results, and the Certification Body judges it necessary to confirm the content of changes and rationale of the analysis, the developer may be requested to provide development evidence or a detailed impact analysis evidence.

Bibliography

[1] Assurance Continuity: CCRA Requirements Version 3.0 March 2023

[2] Requirements for IT Security Certification (CCM-02), Information–technology Promotion Agency, Japan (IPA)

[3] Guidance on IT Security Certification (CCM-02-A), Information-technology Promotion Agency, Japan (IPA)

Addendum: Checklist for Maintenance Application

This checklist contains consideration items needed to judge whether the changed TOE is applicable for maintenance.

In procedure 1, judge whether the contents of each of the "Items to be Checked" are applicable (Yes) or not applicable (No) by proceeding with the checks in accordance with "Judgement of Maintenance" of that column. If, as a result of "Judgement of Maintenance," it is determined that investigation is necessary (cannot proceed to the next check), consider re-evaluation, etc., with reference to the supplementary explanation in procedure 2 of the following table.

This checklist assumes CC Ver3.1 or later versions.

[Procedure 1]

Determine "Yes" or "No" for all items in the following checklist. Any of those where the EAL of the certified TOE is included in the level denoted in the "EAL" column is subject to checking. If the EAL does not apply, proceed to the next check. If any one of them is determined as necessary to examine, consideration of re-evaluation, etc., with reference to "Supplementary Explanations for Re-evaluation" in procedure 2 shall be necessary.

Item Number	Items to be Checked		EAL
	Judgement	Judgement of Maintenance	
1.1	Three months prior to the certificate validity period have passed since the certificate for the certified TOE was issued.		1 or higher
	Yes	Not applicable for maintenance.	
	No	Proceed to item 1.2.	
1.2	Product procurers can identify the certified TOE and the changed TOE by way of changes made to the TOE name or version, or additions to operating environment platform, among others.		1 or higher
	Yes	Proceed to item 1.3.	
	No	Identification of the changed TOE shall be re-considered.	
1.3	If the TOE name has been changed, the name of the changed TOE shall reflect the TOE functionality and evaluation scope expected by consumers which are described in "TOE Overview" and "TOE Description" in the ST for the certified TOE.		1 or higher
	Yes	Proceed to item 1.4.	
	No	The name of the changed TOE shall be re-considered.	
1.4	The changed TOE includes the following changes: ・ A new external interface for security functions was added to the functional specifications. Or, an existing external interface was removed.		1 or higher
	・ Changes exist in the implementation representation that realise the security functions (source code, infrastructure design).		4
	・ Changes relating to security items exist in the guidance		1 or

Item Number	Items to be Checked		EAL
	Judgement	Judgement of Maintenance	
	document.		higher
	• Due to changes to the TOE, new developer tests other than the regression test and vulnerability analysis are necessary.		1 or higher
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 1.5.	
1.5	Changes/additions exist in the ST descriptions, with the exception of the following items: • ST identifiers such as ST creation date and ST version, and update information • TOE name or TOE version		1 or higher
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 2.1.	
2.1	The following changes exist in the external interface of TOE security functions: • Changes in the purpose, method of use, or parameters of the external interfaces of the TOE which had been classified as SFR-enforcing and SFR-supporting during the evaluation of the certified TOE.		1 or higher
	• Changes in the purpose, method of use, or parameters of any of the external interfaces of the TOE.		2 or higher
	• Changes in the error message of the external interfaces of the TOE which had been classified as SFR-enforcing during the evaluation of the certified TOE.		2 or higher
	• Changes in the error message of any of the external interfaces of the TOE.		4
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 2.2.	
2.2	The following changes exist in the subsystems identified in the certified TOE: • Changes in subsystem function and behaviour. • Changes in the subsystem interface corresponding to the external interface for security functions.		2 or higher
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 2.3.	
2.3	The following changes exist in the identified modules within the certified TOE: • Changes in module configuration corresponding to the subsystem • Changes in module function or behaviour. • Changes to the module interface.		4 or higher

Item Number	Items to be Checked		EAL
	Judgement	Judgement of Maintenance	
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 2.4.	
2.4	The following changes exist in the certified TOE: ・ Changes in the management method (access privileges and security properties) of resources (files and memory space) which can be accessed by each user identified by the TOE. ・ Changes in the mechanism for maintaining security during initialisation of the TOE from the shutdown state to the operational state. ・ Changes in the mechanism for protecting the security functions of the TOE. ・ Changes/additions to external interfaces of functions other than security of which impact on implementation of security functions is unclear.		2 or higher
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 2.5.	
2.5	Changes exist in the implementation representation (source code, etc.) corresponding to modules identified in the certified TOE. Or, there are changes in implementation representations for which a correspondence is unclear.		4 or higher
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 3.1.	
3.1	Changes exist in the roles (administrator, auditor, general user, etc.) identified by the TOE or to the privileges of those roles (privileges to access specific functions or resources).		1 or higher
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 3.2.	
3.2	Changes exist in the following items specified according to the roles of TOE users: ・ Items which should be implemented by users to ensure secure use. ・ TOE interface which requires secure use (parameter range, return code, responses and error messages, default values, etc.). ・ Changes to security properties and matters which users should resolve in the event of failures.		1 or higher
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 3.3.	
3.3	Changes exist in security related items like the following within the TOE operation preparation procedures and environment construction:		1 or higher

Item Number	Items to be Checked		EAL
	Judgement	Judgement of Maintenance	
	• Procedures for confirming TOE version and integrity. • TOE settings, system requirements, environmental requirements, and construction procedures required for security during TOE operation.		
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 4.1.	
4.1	The following changes exist with regard to the management of the TOE or constituent items: • Changes/removal of methods for providing means by which consumers identify the TOE (with labels or version confirmation commands, etc.).		1 or higher
	• Changes to the developer's means of identifying TOE constituent items. • Changes to the developer's means of identifying materials submitted as evaluation evidence for the certified TOE assurance requirements.		2 or higher
	• Changes to procedures and privileges for managing documents of TOE constituent items and assurance requirements, and changes to utilised management tools.		3 or higher
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 4.2.	
4.2	Changes exist in the following items with regard to procedures for maintaining TOE security during the delivery of the TOE to product procurers: • Each TOE delivery point and procedures which should be implemented after consumers receive the TOE. • Functions and means employed during procedures. • The department, facilities, or responsible persons for implementing delivery procedures for security maintenance.		1 or higher
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 4.3.	
4.3	Changes exist in the following security measures for the TOE development environment: • Control of physical access to the development environment (entry restrictions, etc.). • Control of logical access to development resources (files and tools, etc.). • Procedures in the development environment (approval of changes, rules concerning carrying items out, treatment of visitors, etc.). • Development staff selection criteria and procedures. • Responsible persons and roles of security measure implementation and monitoring.		3 or higher

Item Number	Items to be Checked		EAL
	Judgement	Judgement of Maintenance	
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 4.4.	
4.4	In the series of stages from TOE development to production, testing, delivery, installation, and operation, changes exist in either the procedures, tools, or techniques (defined by the certified TOE) used in product management.		3 or higher
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 4.5.	
4.5	Changes exist in the TOE development tools (program language, development supporting design system, etc.).		4 or higher
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 4.6.	
4.6	Changes exist in the production process (production procedures, manufacturing equipment, etc.) when the TOE is a product of hardware such as an IC card.		-
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 4.7.	
4.7	Changes exist in the processes such as the following from management to disclosure of failure information with regard to TOE security that had been evaluated for the certified TOE: ・ Acceptance procedures for problem reports relating to TOE security. ・ Problem management procedures and management items relating to TOE security. ・ Procedures for providing users with information of problematic items relating to TOE security.		ALC_FLR When applicable
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 5.1.	
5.1	Changes exist in existing test items for TOE security function, or new test items have been added.		1 or higher
	Yes	Changes may have exceeded the scope of maintenance.	
	No	Proceed to item 5.2.	
5.2	As a result of performing the regression test for the tests that had been performed on the certified TOE, items with behaviours different from the expected results exist.		1 or higher
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Proceed to item 6.1.	
6.1	Changes other than those of the assurance requirements claimed for the certified TOE are clearly affecting security items.		1 or higher
	Yes	Changes may have exceeded the scope of maintenance.	

Item Number	Items to be Checked		EAL
	Judgement	Judgement of Maintenance	
	No	Proceed to item 6.2.	
6.2	For all changes to the certified TOE since the initial certification, in the event that there are multiple changes to the TOE, it can be demonstrated that each change has little impact on the TOE but it cannot be demonstrated that a combination of those changes has little impact on the TOE.		1 or higher
	Yes	Re-evaluation is necessary as changes exceed the scope of maintenance.	
	No	Perform analysis to confirm that differences between the certified TOE and the changed TOE do not affect security, and report the results as an "Impact Analysis Report."	

[Procedure 2]

Consider re-evaluation with reference to the supplementary explanations for the relevant item numbers. If it is determined that re-evaluation is not necessary, keep in mind to describe the analysis as the rationale for this claim in the "Impact Analysis Report," and resume procedure 1 checking.

Item Number	Supplementary Explanations for Re-evaluation
1.1	The TOEs, to which certificate validity period has expired or is close, are not applicable for applying for maintenance.
1.2	If the names and versions for the certified TOE and the changed TOE are different or there are operation platform additions, it is necessary that those descriptions relating to points of changes are ones that product procurers can understand. For example, in the following cases, it is necessary to consider actions such as changing the versions of the certified TOE and the changed TOE or providing means of identification: ・Despite bug-fixing and internal specification changes to the TOE itself, those are not reflected in the TOE name or version. ・Although there are additions to the TOE operational environment, appropriate explanations for product procurers cannot be provided.
1.3	If a change to the TOE name simply reflects a change in product brand name (mechanical replacement of a string of characters), it is assumed that there will be no change in semantics of the ST. However, if the TOE name includes functions or evaluation scope, it is possible that, as a result of the change, the functionality or evaluation scope indicated by the TOE name will no longer be consistent with the

Item Number	Supplementary Explanations for Re-evaluation
	functionality and evaluation scope that ST readers will expect from the TOE type. TOE name changes assume that the changed TOE name will reflect the TOE type and scope explained in the ST.
1.4	Changes to security functional specifications are items that require evaluation, so they are not applicable to maintenance. However, source code changes have no impact on the high-level design and there are no changes to specifications, etc., so the content of changes will be judged according to the assurance level. Security item changes in guidance documents (operation manuals, etc., including installation and setup guides, etc.) significantly impact TOE users, and are items that require re-evaluation. However, if they are changes unrelated to security items such as changes to descriptions in accordance with TOE name and version changes, the analysis would be to confirm that the contents of the changes do not have an impact. Although it is necessary to present regression test results for the changed TOE, the test scope does not exceed the confirmation of the functions claimed by the certified TOE. Tests for new vulnerabilities and threats discovered after certificate acquisition for the certified TOE also do not fall within the scope of maintenance. If the impact of the changes cannot be determined here, assume that re-evaluation will be required. Furthermore, if it is determined that the changes have no impact or have almost no impact on security-related specifications or on assurance, return to Procedure 1 to resume checking and conduct a more detailed check.
1.5	Consistency with the ST is also essential to the changed TOE. Although TOE name changes and identifiers and update information in accordance with ST updates in many cases do not affect security items, if changes are made to assumptions, threats, OSP, functional requirements, and assurance requirements, re-evaluation will be necessary. If a TOE operational environment is added, unless the complete compatibility of the environment itself cannot be proven, evaluation within the newly added environment will be necessary. Proving complete compatibility means to be able to explain in the Impact Analysis Report, with accountability, that the physical design and name, etc., of self-manufactured hardware have no impact on the operation of the software TOE. When supporting third-party hardware or software with insufficient evidence of changed areas and compatibility, re-evaluation will be necessary to evaluate the impact on security functions. Sufficient attention shall be paid to the actual content of the changes for changes in the name and version of developer evidences described as assurance measures. If it is judged that the changes do not relate to the content of assurance means (various procedures and specifications, etc.), analysis should be conducted to confirm that the changes have no impact. If the changes are related to assurance means, re-evaluation within the environment that has applied the new assurance means will be necessary.

Item Number	Supplementary Explanations for Re-evaluation
2.1	Many evaluations will be implemented based on functional specifications (purpose and usage of security function interfaces). Evaluations assume that requirements of the security functions are accurately reflected in the functional specifications. As such, changes to functional specifications will necessitate re-evaluation. Interface changes include direct parameter and behavioural changes, as well as specification changes to management data, configuration files, output files, etc., that are related to the security functions. Although error message changes in many cases mean explicit changes to functional specifications and source, there are also cases where they are caused by changes in the lower layers on which security functions are dependent (errors such as those relating to resource allocation that occurred by extension of security function implementation). If such error messages could be judged to be within the scope of notational differences, analysis should be conducted to confirm that the error message does not affect security items within the changed TOE. If the change in error message is a semantic change and its impact cannot be determined, re-evaluation will be necessary. CC Ver3.1 and later versions have categorisations such as SFR-enforcing and SFR-supporting. The Evaluation Technical Report of the certified TOE should describe the categorisation of each interface.
2.2	Even if there are no changes to the external interface of TOE security functions, there may be changes at the subsystem level relating to their respective behaviours and interactions between subsystems. The validity of the implementations of security functions should be evaluated using as input, how the TOE is designed and how it functions. Therefore, subsystem changes will mean that evaluation inputs are updated, requiring re-evaluation. Even for changes to subsystems claimed as non-SFR-enforcing, re-evaluation will be necessary to determine that they are evaluated as non-SFR-enforcing.
2.3	Subsystems are important input to tests and vulnerability assessment performed individually by evaluators. At the EAL4 level, information for this purpose will be required at the module level such as source code which will be an implementation level guide. Therefore, module changes will mean that evaluation inputs are updated, requiring re-evaluation. The behaviour of modules may differ due to algorithm and implementation changes (change from local variables to global variables), even if the functions realised are the same. Even for changes to modules claimed as non-SFR-enforcing, re-evaluation will be necessary to determine that they are evaluated as non-SFR-enforcing.
2.4	As with the validity of design and implementation of TOE security functions, the mechanism for protecting these functions is also subject to evaluation. Regarding the mechanism for protecting security functions, information at the subsystem level will be used as input for evaluation in the case of EAL2 or 3, and information at the implementation level will be used as input for evaluation in the case of EAL4. If it is

Item Number	Supplementary Explanations for Re-evaluation
	not known whether these changes to the mechanism have an impact at the evaluation assurance level for the certified TOE, they will be subject to re-evaluation. Furthermore, when it is not known whether a new external interface which is not a security function has an impact on security functions, it will also be subject to re-evaluation. If it is clear that there is no impact, detailed analysis should be conducted at the evaluation assurance level to confirm that the content of changes does not have an impact.
2.5	In order for implementation representations such as source code to obtain a high assurance level such as EAL4, they are important as input to evaluator tests and vulnerability assessments, and applicable changes will require re-evaluation.
3.1	Clear explanations regarding user roles (functions) and privileges are described in guidance documents, such as how a certain user is permitted to execute a certain type of function or use a certain type of resource while other users are not granted such permission. If changes exist in user roles and privileges, re-evaluation will be necessary to confirm consistency with guidance documents as well as with other evaluation documentation (functional specifications, ST, etc.), and to confirm that users are given clear instructions of secure environments and items which should be managed.
3.2	To securely operate the TOE, if changes exist in the operations which administrators or general users must conduct, or in related security items, re-evaluation is necessary to confirm that guidance is provided to users with no misunderstanding of information required to use the TOE securely and to detect unsecure situations. In the event of changes to management command usage conditions, user procedures during resource access, policies relating to backup frequency and password quality which are required for secure TOE utilisation; changes to various messages and default values of configuration files of the security interfaces necessary for the management and the secure use of resources; and changes to the safe mode operations required when failures or security-related events occur and to account management of personnel who have left, it will be necessary to evaluate whether this content is clearly and rationally explained to users in guidance documents, etc., and that they are consistent with the operational environment described in functional specifications, design, or ST. Therefore, these changes are judged as exceeding the scope of maintenance.
3.3	If procedures of TOE operation preparation and environment construction described in guidance documents are changed, in many cases, it has potential impact on behaviours or vulnerability analysis of the TOE. However, there are cases where the behaviours or vulnerability analysis of the TOE in operating has no impact, for example, change to measures of confirming the unsealing of packages only, or change of the operation screen messages of install program only. If developers can demonstrate that changes to the operational preparation or environment construction of the TOE have no impact on the behaviours or

Item Number	Supplementary Explanations for Re-evaluation
	vulnerability analysis, the TOE can be applicable for maintenance. In this case, however, subset evaluation is required to confirm whether the changed procedures are appropriate. If the changes to the operational preparation or environment construction have potential impact on TOE operation or vulnerability analysis, re-evaluation will be necessary.
4.1	Providing TOE identification will assure product procurers that they are using an appropriate TOE (the evaluated TOE). If this means is changed, it affects not only on configuration management but on TOE guidance and tests. Therefore, re-evaluation to assure the use of appropriate TOE will be required. Identification and management (traceability) of each element constituting the TOE assures that the development and modification procedures for the TOE are appropriate and the TOE can be uniquely identified. For example, there is a case where a modified source code becomes a component of a TOE version different from the previous version, and it is traced which TOE the component constitutes at the end. When those procedures and privileges for managing configuration components are clear, and the TOE is operated accordingly, it prevents unintended design implementations from being slipped in during the development process. If developers can demonstrate that those changes to the configuration management have no impact on the TOE other than configuration management such as measures or guidance to identify the TOE, the TOE can be applicable for maintenance. In this case, however, subset evaluation is required to confirm whether the configuration items can be managed appropriately by changed procedures, etc. Based on assurance requirements employed for the certified TOE, functional specifications, source code, tools used in development, security flaw report records, etc., will be subject to configuration items of configuration management. It is not a problem to update the identifiers assigned to configuration items, such as version number associated with changes to configuration items in accordance with evaluated procedures.
4.2	Security maintenance in delivery procedures includes all processes from the transfer of the TOE from the production environment to the product procurer, to the installation environment, packaging, storage, and delivery. Procedures to maintain integrity involve the use of shrink wrap packaging and security seals to enable product procurers to confirm the presence/absence of tampering, and methods to maintain confidentiality involve encrypting data, and sending a key to product procurers through a separate route. If developers can demonstrate that those changes to the delivery procedures have no impact on the TOE other than delivery procedures such as TOE functions or guidance, the TOE can be applicable for maintenance. In this case, subset evaluation is required to confirm whether the changed delivery procedures are appropriate to maintain security.

Item Number	Supplementary Explanations for Re-evaluation
	Similarly, if developers can demonstrate that the changes to delivery procedures have an impact only on acceptance procedures and have no impact on other than acceptance procedures such as guidance or TOE functions, the TOE can be applicable for maintenance. In this case, subset evaluation for the guidance describing changed delivery procedures and acceptance procedures is required. If changes to delivery procedures may have an impact on parts other than delivery procedures or acceptance procedures, re-evaluation will be necessary.
4.3	Vulnerabilities introduced at this stage due to simplistic change, etc., to security procedures for the development environment have potential major impact on TOE security at the operation stage. In addition, if the range of disclosure or management level of confidential information of the TOE is changed such as outsourcing development work, it could potentially impact on vulnerability assessments, that is, the susceptibility to attacks against the TOE. If developers can demonstrate that changes to the security of the development environment have no impact on vulnerability assessment, the TOE can be applicable for maintenance. In this case, subset evaluation is required to confirm whether the changed procedures are appropriate for protection of design information, etc. If the changes to the security of the development environment have potential impact on the vulnerability assessment of the TOE, re-evaluation will be necessary.
4.4	If a TOE life cycle is defined and procedures, tools, or techniques employed at each stage are management methods necessary for development and maintenance, it is assumed that the potential for the occurrence of TOE flaws will be reduced. Changes to the employed coding conventions, testing methods, management system, scope of responsibilities, and others may compromise the confidence of quality. If developers can demonstrate that changes to the TOE life cycle have no impact on quality of the TOE, the TOE can be applicable for maintenance. In this case, subset evaluation for the changes is required. If the changes to the TOE life cycle have potential impact on quality of the TOE, re-evaluation will be necessary.
4.5	In the event that tools (programming language, development support, etc.) employed in TOE development are not recognised standard tools and a clear syntax cannot be completely identified, or that even the tools used by the developer are standard but those include implementation-dependent or proprietary functions, consistency between the programming language and executable objects cannot be determined. In addition, the executable objects that unintended by the developer could be a factor of vulnerability. The TOE developed in a development environment different from that of the certified TOE, this should be re-evaluated. If there are no specification changes, the result of using a compiler of a different version in same way may not have a significant impact on the TOE. On the other hand, it can be said that there is a high possibility that the result of employing different compiler options, even when using compilers of the same revisions would

Item Number	Supplementary Explanations for Re-evaluation
	affect the semantics of the executable code. If developers can demonstrate that changes to the development tools have no impact on the semantics of the executable code, the TOE can be applicable for maintenance. If there is no clear evidence regarding impact, it will be necessary to obtain assurance through re-evaluation.
4.6	In the event that the TOE is a product of hardware such as an IC card and production procedures of the TOE are changed, the resistance of the TOE to the physical attack could be altered due to the change of the physical property of the TOE. For that reason, if the changes to the production process have potential impact on physical property of the TOE, re-evaluation of physical attack to the TOE will be necessary.
4.7	The certified TOE provides assurance that, in the event that a security problem is discovered in the TOE, developers are able to share and trace details and response status, and procedures are established to provide necessary related information to users. If developers can demonstrate that changes to the flaw remediation procedures have no impact on TOE functions or guidance, the TOE can be applicable for maintenance. In this case, subset evaluation is required to confirm whether the changed procedures are appropriate. If changes to the flaw remediation procedures have potential impact on TOE functions or guidance, re-evaluation for not only the flaw remediation procedures but also including TOE functions or guidance will be necessary. For example, if user notifications relating to bug fixes are changed from direct mail to Web publication, re-evaluation will be necessary to confirm that procedures, guidance etc., to ensure that users obtain this information are appropriate. Note that this check will only be applicable if assurance class ALC_FLR is claimed as the assurance scope for the certified TOE.
5.1	Changes or additions of tests are considered to be caused by changes in TOE security functions, and re-evaluation will be necessary. However, if test environment changes are a result of performance improvement of hardware external to the TOE or the use of updated revision of the underlying software that security functions do not depend on, and there are no changes to the TOE interface, TOE test documentation might not be affected. Tests to confirm such changes shall be indicated in the report as results of analysis, apart from existing tests. Furthermore, the changed TOE is expected to possess functions equivalent to those of the certified TOE, and countermeasures to vulnerabilities which have become evident after certification was obtained for the TOE do not fall within the scope of maintenance.
5.2	If the results of changes are judged to have unexpected impacts on security functions, they will not be subject to maintenance.

Item Number	Supplementary Explanations for Re-evaluation
6.1	Basically, it is considered that changes other than those to the assurance requirements claimed for the certified TOE will not affect the security of the TOE. For example, for EAL2, if changes to the source code do not change the functional specifications or subsystems, TOE assurance will not be affected. However, it is necessary to pay attention to cases where items relating to TOE security other than the evidence evaluated for the certified TOE are inserted. If items relating to TOE security are added to documents that are not identified as procedures to maintain a secure state, they may require re-evaluation as new procedures. Developers must conduct analysis to confirm that the changes have no impact within the assurance level, regardless of whether or not the subject of the changes had been used as evidence for the certified TOE.
6.2	Even changes that have a minor impact individually could have a major impact on a TOE through accumulation or interaction. For example, in case that multiple patches for software flaw remediation are developed and applied independently, TOE security may be affected by the internal mismatching between those patches, even if each patch has individually no impact on TOE security. In addition, in the event that many changes are made to the TOE and the impacts of the combination of changes are wide-ranging, it will be hard for developers to objectively demonstrate that the overall impact of changes is small. Developers must demonstrate that not only each individual change but also the combination of all changes to the certified TOE since the initial certification has no impact on security of the TOE. If developers cannot demonstrate that, it will be necessary for them to obtain objective assurance through re-evaluation.