Addendum Information

for the Scheme

The JISEC (Japan Information Technology Security Evaluation and Certification Scheme) aims to contribute to the supply of secure information technology (IT) products primarily for procurement by government agencies, and to conduct IT product evaluation and certification based on the Common Criteria (CC), which is an international security evaluation standard. This addendum information describes the decisions of the Scheme, for items not prescribed in the CC, in relation to operating the Scheme.

This addendum information must be confirmed when making an application for certification. When an application is submitted, it is assumed that relative parties have an understanding of this addendum information. If there are any matters herein that require clarification, please contact JISEC before submitting an application.

Information Security Certification Office,
IT Security Center, Technology Headquarters,
Information-technology Promotion Agency, Japan (IPA)
Issued on May 23, 2014

◆The Handling of Ciphers Under the Scheme (JISEC)

An evaluation is made of the usage of ciphers, appropriateness of key management and vulnerabilities upon implementation under the CC. However, cryptographic specifications, including hash functions, and assessment of the mathematical properties of cryptographic algorithms fall into the categories handled by each Scheme.

Cryptographic specification under JISEC is basically the cryptographic algorithm designated by the requirements for government procurement in regards to PPs, etc.

Furthermore, those ciphers that are included in the "e-Government Recommended Ciphers List" of “The list of ciphers that should be referred to in the procurement for the e-Government system (CRYPTREC Ciphers List)" established by the Japanese Ministry of Internal Affairs and Communications (MIC) as well as the Ministry of Economy, Trade and Industry (METI), are accepted by the Scheme.

When using a cryptographic algorithm other than the aforementioned (i.e., if an ST assuming original requirements other than the requirements for government procurement is prepared, and a cipher not in the e-Government Recommended Ciphers List is being used), the applicant must reach an agreement in advance with the assumed procurement entity[1] in regards to the cipher being used. At the same time, objective documentation regarding security must be submitted to the Evaluation Facility for an evaluation of the appropriateness of the requirements.

In particular, when the functional requirements of an original cipher are used as a measure against threats, the possession of specialized techniques with credentials are generally required for making objective evaluations of the cipher security. The applicant needs to select and designate in advance an Evaluation Facility that has sufficient expertise in this field.

The Scheme will not become involved in the verification of such cipher security that is not included in the e-Government Recommended Ciphers List, and the STs which fail to mention the procurement entity with the cipher as requirement will not be accepted under the Scheme.

[1] The name of the agency, etc., listed under "Purpose of acquiring certification" in the Application for Certifications (Form 1).

◆Organizational Security Policies (OSPs)

OSPs are sometimes defined in the PP. OSPs are security rules, procedures, or guidelines imposed in the TOE operational environment and are generally based on statutory regulations related to the TOE field, security policies of government agencies and the security policies unique to the procurement division.

When creating a PP (or when a developer is creating an original ST) and specifying OSPs as requirements, sufficient consideration of the background of the rules and policies used as the rationale should be made in writing. For example, if the requirement "the communication channel must be encrypted" is designated as an OSP, it is an implicit policy to use the “e-Government Recommended Ciphers List.” If key size during cipher use and other matters are defined as separate security policies of the same organization, then it is not possible to fulfill the regulations and procedures that are the rationales with just OSP information.

The evaluations will determine whether or not the OSP statement reflects the policies to be imposed on the TOE operational environment. For this reason, even in the case that the applicant uniquely establishes the OSP on the applicant's own, there is a need to specify specific security rules, procedures, or guidelines imposed in the TOE operational environment of the assumed procurement entity[2].

If specific security rules, procedures, or guidelines that are the rationales for the OSPs are not specified, they are inappropriate as OSPs. Such contents will most likely be described as threats in the ST. Contents for which regulations, procedures or even threats that serve as rationales do not exist must not be described as OSPs.

[2] The name of the agency, etc., listed under "Purpose of acquiring certification" in the Application for Certifications (Form 1).

◆Preparation of Evaluation Documentation

The applicant (TOE developer or sponsor) that is responsible for the relevant application for evaluation has the obligation to provide the technical documentation (e.g., design document and tools used in development and/or testing) and assurance procedures (e.g., entry and exit management log, and acceptance of site visits of the development environment) required for evaluations in accordance with the scope of the evaluation assurance. In the CC Part 3[3], those actions that the developer must carry out in the process of developing the target of evaluation are listed under "Developer action elements," and those materials that the developer should prepare and present are listed under "Content and presentation of evidence elements."

Prior to the evaluation, the applicant must recognize and prepare for the necessary response that must be made within the scope of the evaluation assurance as required by the PP. If the applicant completes development in advance without recognizing the need to consider those matters that require response, or if an evaluation is commenced without the preparation of necessary documentation and a delay in the evaluation schedule arises, it becomes impossible to continue the evaluation depending on circumstances, and such risks and responsibility will be borne by the applicant.

There has been a case in the past when an applicant created an ST on the applicant's own without referring to the PP. The applicant was unable to provide sufficient documentation despite having declared the scope of the evaluation assurance.

For example, the following cases have actually occurred. A part of the target of evaluation was developed by a company that was affiliated with the division making the application, and it later became evident that the affiliated company could not provide materials of the required level because the company did not utilize development methods that were of the same level as the division making the application. In another case, a part of the development was completely outsourced to an external entity. However, the agreement between the developer and the outsourced entity does not include matters concerning evaluation. For this reason, evaluators and certifiers were not granted permission to enter some sites.

It should be noted that it is a waste of expenses and time for relevant parties if the applicant declares a scope of evaluation assurance, which includes the scope that the applicant cannot be responsible for, such as inability to provide documentation.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components

◆Certification Applications with the Same Document

As a rule, a certification application shall be submitted for each single TOE. A single TOE means that identification for the purpose of procurement is unique, and the evaluated configuration and evaluation assurance level are fixed. The reason for doing this is to avoid generating any misunderstanding on the part of the procurement entity through a cumbersome and complicated ST and Certification Report, which might be caused by conducting an evaluation with multiple configurations or different security problem definitions. Furthermore, because a CC evaluation covers a broad area, such as describing detailed differences related to multiple products in an Evaluation Technical Report, it can easily trigger the occurrence of mistakes in certification tasks. The rule is also prescribed under the Scheme from the viewpoint of the appropriate bearing of certification expenses.

However, applications may be submitted using the same application documents in cases where the TOE is the same from the aforementioned viewpoint but there are different product model numbers that are given due to sales circumstances. For example, even if it has the same TOE, product model numbers are sometimes differentiated for sales convenience in order to make it possible to distinguish differences in the number of licenses used or the supported platform. In such cases, if there is no difference in regards to the TOE evaluation results for any product model number to the procurement entity, then the same document for the TOE certification application will be accepted.

It should be noted, however, that because there is a danger that the procurement entity may misunderstand what the certification target is, as a general rule, it will be limited to cases in which the TOE name and version found in the TOE identification are completely the same.

Furthermore, there will be one certificate for each application, and all TOEs described in the application will become the target of the evaluation. Consequently, the evaluation results and maintenance conditions of some licenses and platform model numbers in the application will have an impact on all TOEs at the time of the same application. Even if the certification of a part of the certified TOEs is revoked, all of the TOEs described in the certificate will become the target of the certification revocation. Therefore, careful thought should be given before submitting an application for multiple TOEs under a single application.

Note that this reference made here only mentions the format of the certification application. The treatment of matters such as expenses and man-hours during the evaluation of multiple similar TOEs will be left to the discretion of each Evaluation Facility. As such, the Evaluation Facility should be consulted in advance.

◆Obligation to Maintain the Reliability of the Certified Products

In the case that an event related to the reliability or vulnerability of a TOE evaluation becomes evident after certification is obtained, the applicant bearing the responsibility for the evaluation has the obligation to report such incident or take corrective actions.

In the case that concerns arise regarding the evaluation result of a certified product, the applicant must, on the basis of instructions from the Scheme, carry out a review on the concern related to the evaluation result, report its findings, and take corrective actions. In the meantime, the product cannot be sold as a certified product. Furthermore, the applicant must publish the incident on a website that provides a description of the problem outline, its impact, and procedures for corrective actions, to the procurement entities. For specific procedures, the section on surveillance in the JISEC Documentation should be referenced.

Concerns regarding evaluation results may be pointed out by a third party or persons involved in the Scheme, or reported by the applicant. Contributing factors for such concerns include the adequacy of documentation or the validity of the evaluation verdict during the evaluation process. However, the Scheme will not isolate these factors. It is recommended that the applicant should discuss with the Evaluation Facility in advance regarding the service level agreement (SLA) on such matters as the response to be made in case concerns arise in relation to evaluation results.

Vulnerabilities may also become evident after obtaining the certification through changes in technological conditions or the development of new attack methods. The applicant has the obligation to inform the Scheme of the outline, its impact, and the countermeasure method of the vulnerability so that a warning will be notified to the procurement entities. Such information related to vulnerability will be published in the Certified Product List on the Scheme website. This will prevent procurement entities from operating or procuring a certified product without knowing the risk of exploiting critical vulnerabilities.

Furthermore, in the case that the vulnerability is determined to attribute to the validity of an evaluation, the Scheme may make the relevant certified product a target of surveillance.

Regaining trust would be difficult in the case that a vulnerability-related incident arose for the certified product while being used in the context of procurement by the government, etc. To avoid such situations, the Scheme will disclose information related to vulnerabilities to procurement entities. Your proactive cooperation with surveillance and provision of information on vulnerabilities are highly appreciated.