JISEC

# Guideline for Determining the TOE

in Certification Applications that Do Not Use PPs

Version 2.0

This "Guideline for Determining the TOE" describes what kinds of matters to note when determining the scope of the target of evaluation (TOE) in carrying out evaluations under the Japan Information Security Evaluation and Certification Scheme (JISEC). It also deals with how to determine the appropriateness of the TOE scope in the related evaluation approaches under this Scheme.

This Guideline is intended to be used particularly in evaluations that do not utilize Protection Profiles (PPs). It is to be used as a guide for confirming the appropriateness of a scope when the applicant itself determines the TOE scope, and for confirming the appropriateness of a description related to the ST reader, who is the procurement entity of a TOE, when the ST author creates the ST.

**Information Security Certification Office,**
**IT Security Center, Technology Headquarters,**
**Information-technology Promotion Agency, Japan (IPA)**

**Issued on April 7, 2014**

# Table of Contents

Introduction....1
1. The TOE and Products....1
2. The TOE and Security Functionality....2
3. The TOE and ST Readers (Description in the ST)....4
3.1. Description of Functions and Environments Outside of Evaluation....5
3.2. TOE Description as a Product Component....6
4. TOE Name....6

## Introduction

In a security evaluation based on the Common Criteria (CC), an international standard for security evaluation, security requirements are specified through Protection Profiles (PPs) created by a procurement entity (generally a government agency), and IT products are evaluated according to those requirements. Under JISEC, on the other hand, product developers themselves determine hypothetical requirements instead of having a procurement entity provide requirement specifications. Evaluations based on a unique Security Target (ST) have also been accepted on the grounds that procurement standards are in the process of being formulated (i.e., provision of PPs by the government is delayed). Even in evaluations that do not use such PPs, the developer is expected to assume the requirements of the procurement entity, and determine the scope and security functions of a Target of Evaluation (TOE) so that they are both meaningful and clear to the TOE procurement entity.

The TOE must be clearly identified as a starting point for the security evaluation. In addition, the TOE scope must be clearly stated in the ST so that its readers (i.e., the "procurement entity" for the TOE provided by the developer, and the "consumers" who are the users of the security functions provided by the TOE) can obtain an accurate understanding of the scope. When the TOE scope is not sufficiently clear, or when it is vaguely stated in the ST, a considerable amount of man-hours can be wasted trying to clear up confusion that may be created during the evaluation process due to a gap in understanding between the developer of the TOE and the evaluator or certifier. If the consumers of the TOE find it difficult to accurately determine whether the security functions they expect are covered by the evaluation, the aim of the security evaluation that JISEC is intended to fulfill will not be achieved.

This situation often results from a discrepancy between "the product to be evaluated and the scope of evaluation," "the main security functions of the product and security functions to be evaluated," "consumers of the TOE and readers of the ST," and "the name and substance of the TOE." Based on these perspectives, matters to be noted in determining the TOE scope and describing the TOE in the ST are summarized below.

## 1. The TOE and Products

As a basic requirement, the TOE physical scope must be consistent with the product. Including only a part of a product in the TOE scope has little meaning for consumers as an evaluation assurance, unless the evaluation is being performed within the scope of self-contained, independent functions[1] that do not mutually affect each other. With a firewall product, for instance, evaluating the entire NAT function including the user interface will be useful for consumers using only NAT. On the other hand, if only a part of a filtering module is evaluated, consumers who will use the filtering function, including the unevaluated parts other than the module, will not be able to determine what was assured by the evaluation.

[1] In this Guideline, "product" indicates the minimum unit of a security service to be provided to a user through a single security function or a combination of several security functions.

In reality, operations (management and configuration) performed on individual functionality rarely have no mutual impact on security functions. For this reason, under JISEC it is a basic requirement to establish the full "product," including the entire scope of responsibility of the developer, as the TOE scope. When a part of a product is made the target of evaluation, the relevant application will not be accepted under JISEC unless it can be demonstrated in the ST what kind of evaluation assurance can be provided to the procurement entity. For the users of the external interface of the TOE, a "product" is a recognizable unit that includes the TOE, and it is usually a commercially produced product that is available for procurement.

It may also refer to a "product" that is traded between development sites as a component for a specific commercial product. The consumer in this case is the developer who uses the TOE as a component in developing the commercial product, and the reader of the ST is also the developer. The end user of the commercial product does not appear here.

One example of a special case like this is when a procurement entity procures firmware for implementing a new function on an existing application-specific IC card. In this case, a type of evaluation called a "composite evaluation" is performed, which assumes an integration with the IC card in the end.

As stated above, consumers generally are not conscious of the design and purposes of individual components and modules inside a purchased product when they use it. To put it simply, if the developer includes only certain components or modules of the product it provides in the scope of the evaluation, and if the security functionality used by consumers uses other components or modules that were not evaluated, such evaluation will provide no assurance whatsoever for the consumers. Under JISEC, it is recommended that the entire product, not just a part of it, be covered by the TOE scope, from the viewpoint of promoting security evaluations that are meaningful for consumers.

Conversely, the developer must not set a scope that exceeds the security function it provides for the TOE. To be more precise, the applicant must not set a TOE scope that assures security functionality exceeding its scope of responsibility (the scope that can be assured with the claimed evaluation assurance level) for the TOE. If a product, etc., required for the operating environment of the TOE plays a role in the security function to be evaluated, the developer must clarify the scope of the security function that will be evaluated (to put it simply, the extent of responsibility that the TOE takes, and areas that depend on the environment) before performing the evaluation. The scope of responsibility indicates the ability to provide documentation, etc., that satisfies the evaluation assurance level at the time of evaluation, and to address any concerns raised during the evaluation. It also enables the procurement entity to identify the boundary of product procurement for the TOE and the rest of the operating environment (See Chapter 3.1).

## 2. The TOE and Security Functionality

It is preferable that all security functionality included in the TOE is the target of the security evaluation. The presence of a functionality that is not included as a target of evaluation--despite

the fact that the functionality can be considered as an independent security function of the product--can cause confusion on the part of consumers as well as make the significance of evaluation assurances tenuous for consumers. This is especially the case if the security function that is naturally expected to be provided by the TOE functionality is not included as a target of evaluation. An example of this is a firewall product for which functions related to packets and protocol filtering are not included as a target of evaluation, and only management functions (e.g., filtering settings) are made the target of evaluation.

It is recommended for the TOE physical scope under this Scheme that all functionality that can be expressed as a security functional requirement to be a security function for a target of evaluation. In particular, the security functionality expected by the assumed consumer should be a target of the evaluation.

Is this a Security Function?

The "security" of the security functions that are the target of evaluation under CC evaluations generally refers to the maintenance of confidentiality, availability, and integrity. It may also include non-repudiation, accountability, and authenticity. Many of these are available as Functional Requirement Packages in the CC Part 2. Therefore, if it is consistent with these requirements, it can be considered a security function. However, if there are requirements that are not consistent with the existing requirements, a new requirement should be considered instead of forcefully changing the interpretation of the existing requirements. It should be noted that the requirements as a security function should not be confused with the logical properties[2] of the design or implementation. Furthermore, if simply invoking a security function or processing the result of a security function is included within the TOE scope, it would not have the kind of property that would be called "security" as described above. Moreover, the concept of the kind that a security function should be invoked without interference from or by being bypassed by other processes is a necessary property of all security functions that would be achieved by the TOE design. Such properties are matters that are evaluated separately from the explicit security functions set forth in the ST and are evaluated commonly on the basis of such items as development documentation.

Several supportive functions for realizing the security functionality of the TOE are sometimes present outside of the TOE logical scope. In such cases as well, for the significance of the security evaluation, at least the implemented function of the security functional requirement must be retained by the TOE. For example, if only the scope realizing the processing of the result of invoking a function (e.g., SSL library) outside of the TOE that realizes the actual security functional requirement is the TOE, then the TOE cannot be said to be implementing a security functional requirement (e.g., secure communications). This can be determined as not

[2] Specific cryptographic algorithms and protocols are sometimes specified in procurement requirements.

being a security function to be evaluated as the TOE, or as having the TOE scope that is inappropriate.

In the case that a function supporting the TOE's security function is outside of the TOE, it is generally considered an environment that is necessary for operating the TOE. As such, it is procured independently by the procurement entity. If these supportive functions exist within the product provided by the developer and are provided with the TOE, such supportive functions must also be included within the scope of evaluation. This is because evaluating only a portion of the functions that constitute the security functionality of a product provided by the developer has no meaning as an evaluation to the end user of the security functionality.

However, if the interface between the TOE's security function and the supportive function outside of the TOE is visible, and the procurement entity can procure the part that includes the supportive function (product) at the procurement entity's own responsibility, there are cases in which a separated evaluation is possible. The ability to separate the part that implements the security function directly related to realization of the security functionality from its supportive elements means that complete disclosure of the interface between them has been made, and it is possible to replace the supportive function (through procurement or by producing it on one's own.) Examples of the above include operating software (OS) that are recognized as being versatile, well-known products.

On the other hand, when evaluating an application that is dependent on the embedded OS that provides a supportive function for the security functionality, users of that security functionality cannot select or procure the embedded OS at the user's own responsibility. In such cases, the application cannot be made the only scope of evaluation. Even in the case that the developer provides the supportive functions on its own, if they are mounted in an optional product and the interface utilizing that product has been disclosed (e.g., XY standard compliant or W99API fully-compliant), the procurement entity can select something else, including that which was produced in-house by the procurement entity. Therefore, an evaluation can be made with these supportive functions as the condition. In reality, the product developer does not support the product with the supportive function provided by a third party, or there are original interfaces that have not been disclosed. Therefore, in nearly all cases, the TOE scope used is for all of the functions that are provided.

## 3. The TOE and ST Readers (Description in the ST)

When the TOE scope is determined, TOE users are specified, and ST readers are determined. In many cases, an ST reader is a TOE consumer; specifically, it becomes the procurement entity of a government agency. Here, we will use an actual example in which the ST was not written for the original TOE consumer in regards to the determined TOE scope and resulted in a huge amount of time and expense being expended not only for the ST evaluation but also the TOE evaluation that followed. Descriptions in the ST for which care should be taken will be presented.

## 3.1. Description of Functions and Environments Outside of Evaluation

Regardless of the TOE scope, the ST must not contain such descriptions that security functions outside of the target of evaluation are included in the TOE logical scope. In regards to specific descriptions in the ST, the following apply.

- It is unacceptable to describe in the "TOE overview" those security functions that are not involved in the security functionality being evaluated.
- It is unacceptable to describe in the "TOE description" those TOE security functions that are not indicated in the "TOE overview."
- It is unacceptable not to indicate in the "TOE summary specification" the security functions described in the "TOE description."
- It is unacceptable not to have security functional requirements that correspond to the description in the "TOE summary specification."

The evaluated security functionality must be consistent in the "TOE overview," "TOE description," "TOE summary specification," and security functionality requirements.

Including the explanations of unevaluated security functionality in the ST has a risk of misleading ST readers to think that the security functionality is assured. In many cases, unevaluated security functionality should be independent of the target of evaluation and composed of security functions that would not have any impact. There should not be a need to make their explanation in the ST indispensable (if the target of evaluation cannot be understood without mention of the unevaluated security functionality, there is a high possibility that there was a problem when determining the TOE scope). If unevaluated security functionality is described in the ST regardless of the above, then it cannot be helped if others understand it as intentional on the part of the developer to mislead the ST reader into thinking that those unevaluated security functions are also assured.

The same can be said in regards to product and evaluation configurations. In the case that many configurations providing support as the product are described in the ST, but the configurations and environments that were actually evaluated or were the target of evaluation are unclear, then the ST's purpose as a basic design documentation for security is not fulfilled. The ST author must avoid the inclusion of unnecessary product explanations in the ST. Clear descriptions that directly convey the evaluated target to ST readers must be made.

From the viewpoint of promoting security evaluations that have meaning for consumers, the Scheme strongly recommends that all security functions included in the functionality provided by the TOE be specified in the ST as security functionality requirements and be made a target of evaluation. However, this is not to disallow evaluations with the presence of security functionality that is not presented in the ST (as long as such functionality is completely independent of the security functionality that is the target of evaluation, and is not a security function that ST readers expect from the product type, and is understood by ST readers as being outside of the target of evaluation).

### 3.2. TOE Description as a Product Component

If a TOE is a part of the product or system (e.g., XXX module or XXX function) but the ST includes an explanation toward the end user of products and systems including the TOE, it may confuse ST readers in regards to the TOE scope.

In such cases, an explanation must be described toward the actual users of the TOE--that is to say, the developers who develop products and systems using the TOE. In the case that the TOE is a part of the product, there will naturally be a difference between the "TOE's external interface" and the "product's user interface." Regardless of this difference, it cannot be described in the ST as if the product's user interface is the TOE's external interface. Generally, how the TOE is handled by such products is outside the TOE evaluations. Therefore, ST authors should avoid including in the ST as much as possible, conceptualized explanations of the final product in which the TOE is used. Explaining the TOE in the ST from the aspect of utilization form of the product, despite the fact that the developer’s responsibility cannot cover the product, would be deceiving the ST reader into thinking that an unassured part is also assured by the security evaluation.

If a TOE is a component of a particular product and is responsible for a part of the realization of a product's security functionality, the use of the product can be handled as the use of the TOE only when it fulfills the following two cases.

1. The case that TOE's external interface and the product's user interface are the same. (Or, in the case that the correspondence between the TOE's external interface and the product's user interface is self-evident, and it is clear from the assumptions and operational environment that no manipulation or interference can be made of one by the other.)
2. The case that the product's security functions are all implemented by TOE security functional requirements.

In 1. above, cases in which the correspondence between the interfaces is self-evident may include mediation by hardware that does not require logical processing (e.g., a button). In many cases, however, the result of the logical processing of input into a product interface becomes the input made to the TOE. For this reason, it would probably not be possible to handle a product interface as being equal to the TOE.

In the past, there has been a case when the manual for the final product, which included the TOE, was submitted as documentation for the TOE evaluation. However, these were attributable to the clear lack of TOE documentation or the forced narrowing down of the TOE scope for the sake of convenience in acquiring the certification. The Scheme does not recommend such certified products for procurement by government agencies.

## 4. TOE Name

The name of the product that is related to the TOE may be used as the relevant TOE name (in the case of the ST, the TOE name is described in the section on "TOE reference"). The TOE name must be defined in a way that properly conveys to consumers the relationship between the

TOE and its product.

In particular, in cases in which the TOE scope is not consistent with the product and the TOE only targets a part of the product's security functionality (the Scheme does not recommend using only a product's partial security functionality as the TOE), there is a need to clearly indicate the relationship with the product in the TOE name. This is to avoid misleading the reader into thinking that the whole product or the security functionality other than that within the TOE scope was evaluated.

When using the product name in the TOE name used as the TOE reference, the ST author must ensure that the TOE scope, security functionality, etc., that the reader assumes from descriptions in product catalogs and manuals do not differ from the actual TOE scope, security functionality, etc.

## Checklist for Confirming the TOE Scope

When making an application with an ST that does not conform to PPs, the TOE scope should be confirmed using this checklist.

| | |
|---|---|
| ☐ | Are the TOE and product consistent? |
| ☐ | If the TOE and product are not consistent,<br>• can the procurement entity clearly differentiate between the TOE scope and the product; and<br>• is the TOE scope one that has meaning to consumers? |
| ☐ | Are there any security functions in the TOE that should not be a target of evaluation?<br>Will all security functions that are in the product catalog or manual be evaluated? |
| ☐ | In the case that there is a security function in the TOE that should not be a target of evaluation,<br>whether the security functions that would be the target of evaluation have been clearly conveyed to the procurement entity under "TOE overview" and "TOE description" in the ST? |
| ☐ | In the case that the external interface of the TOE is a product interface,<br>does the TOE developer bear responsibility up to and including the product interface? |
| ☐ | In the case that the external interface of the TOE is not a product interface,<br>whether the product consumer is not confused with the TOE consumer in the ST? |
| ☐ | Are all security functionalities within the TOE scope? |
| ☐ | In the case that all security functionalities are not within the TOE scope,<br>• can the function implemented by the TOE be defined as a security requirement; and<br>• are the TOE and security interfaces outside of TOE visible? |
| ☐ | In the case that the TOE name cites the product name,<br>• can the procurement entity understand the relationship between the TOE and the product from the TOE name; and<br>• whether it does not differ from the content found in product catalogs and manuals? |