TECHNICAL REPORT

ISO/IEC TR 15446

Third edition
2017-10

Information technology — Security techniques — Guidance for the production of protection profiles and security targets

Technologies de l'information — Techniques de sécurité — Guide pour la production de profils de protection et de cibles de sécurité

Reference number
ISO/IEC TR 15446:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC TR 15446:2009), which has been technically revised.

Introduction

This document is an adjunct to ISO/IEC 15408 (all parts). ISO/IEC 15408 introduces the concepts of *Protection Profiles* (PPs) and *Security Targets* (STs). A Protection Profile is an implementation-independent statement of security needs for a type of IT product that can then be evaluated against ISO/IEC 15408, whereas a Security Target is a statement of security needs for a specific ISO/IEC 15408 target of evaluation (TOE).

Unlike previous editions, the third edition of ISO/IEC 15408 (all parts) provides a comprehensive explanation of *what* needs to go into a PP or ST. However, the third edition of ISO/IEC 15408 still does not provide any explanation or guidance of *how* to go about creating a PP or ST, or how to use a PP or ST in practice when specifying, designing or implementing secure systems.

This document is intended to fill that gap. It represents the collective experience over many years from leading experts in ISO/IEC 15408 evaluation and the development of secure IT products.

Information technology — Security techniques — Guidance for the production of protection profiles and security targets

1 Scope

This document provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408 (all parts). It is also applicable to PPs and STs compliant with Common Criteria Version 3.1 Revision 4[6], a technically identical standard published by the Common Criteria Management Board, a consortium of governmental organizations involved in IT security evaluation and certification.

NOTE This document is not intended as an introduction to evaluation using ISO/IEC 15408 (all parts). Readers who seek such an introduction can read ISO/IEC 15408-1.

This document does not deal with associated tasks beyond PP and ST specification such as PP registration and the handling of protected intellectual property.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 15408-1 and the following apply.

COTS	Commercial Off The Shelf
CRL	Certificate Revocation List
LDAP	Lightweight Directory Access Protocol
SPD	Security Problem Definition
SSL	Secure Sockets Layer
TLS	Transport Layer Security

5 Purpose and structure of this document

This document is intended to help people who have to prepare Protection Profiles (PPs) or Security Targets (STs) for use in evaluation against the third edition of ISO/IEC 15408 (all parts). It provides detailed guidance relating to the various parts of a PP or ST, and how they interrelate.

This document applies only to the third edition of ISO/IEC 15408 (all parts). Earlier versions of ISO/IEC 15408 have different and incompatible technical requirements. However, the strategies proposed in this document will, in the main, also be applicable to earlier versions of ISO/IEC 15408.

This document is primarily aimed at those who are involved in the development of PPs and STs. It will also be of interest to consumers and users of PPs and STs who wish to understand the contents of PPs and STs developed by others, and wish to confirm the relevance and accuracy of the information that they contain. It is also likely to be useful to evaluators of PPs and STs and to those who are responsible for monitoring PP and ST evaluation.

It is assumed that readers of this document are familiar with ISO/IEC 15408-1:2009, and in particular, Annexes A and B which describe STs and PPs, respectively. PP and ST authors will need to become familiar with the other parts of ISO/IEC 15408 as described in this document, including introductory materials such as the functional requirements paradigm described in ISO/IEC 15408-2:2008, Clause 5.

This document is intended for guidance only. It should not be cited as an International Standard on the content or structure for the evaluation of PPs and STs. It is intended to be fully consistent with ISO/IEC 15408 (all parts); however, in the event of any inconsistency between this document and ISO/IEC 15408 (all parts), the latter as a normative International Standard takes precedence.

Clauses 1 to 4 contain introductory and reference material, and are followed by this overview clause (Clause 5).

Clause 6 provides an introduction to Protection Profiles and Security Targets — what they are, when and why they may be used. Clause 6 also discusses the relationship between PPs and STs and issues relating to the PP/ST development process.

Clauses 7 to 13 provide information on how to specify the seven mandatory parts of the contents of a PP or ST, following the order outlined in ISO/IEC 15408-1:2009, A.2 and B.2.

Clause 14 examines the issues specific to PPs and STs for composed TOEs, i.e. TOEs that are composed of two or more component TOEs, each of which has its own PP or ST.

Clause 15 deals with some special cases, namely, low assurance reduced PP/ST contents, conforming to national restrictions and interpretations and some new concepts for enhancing the flexibility and usability of Protection Profiles.

Clause 16 discusses the topic of use of automated tools in PP/ST development.

6 Overview of PPs and STs

6.1 General

This clause provides an overview of the roles of PPs and STs in information security evaluation using ISO/IEC 15408 (all parts).

6.2 Audience

This document is intended for use by two distinct audiences:

a) IT professionals with security knowledge (e.g. security officers/architects with an understanding of a security requirement) but who are not experts in information security evaluation, and who have no prior knowledge of ISO/IEC 15408 (all parts);

b) experts in information security with good knowledge of ISO/IEC 15408 (all parts), who are engaged in developing PPs and STs as part of their professional activities.

If the reader falls into the former category, this clause should provide the information needed to understand the purpose and structure of PPs and STs. It should also provide the background information needed to read and understand PPs and STs, and to identify their relevance and correctness with respect to the particular circumstances. Clauses 7 to 13 explain the contents of each part of PPs and STs in detail, but are oriented towards the production of such documents and assume knowledge of ISO/IEC 15408 (all parts).

If the reader is an expert, she/he should already be familiar with the contents of this clause. Subsequent clauses will provide the methodologies, techniques and practical tips that can be used to prepare PPs and STs in an efficient yet consistent manner.

If the reader is not an expert in information security, and needs to produce a PP or ST, this document will help to do so. However, the reader will also need to find, read and understand published examples of PPs or STs similar to the requirements she/he has. The reader should also consider calling on the services of others who *do* have the necessary specialist knowledge and experience.

6.3 Use of PPs and STs

6.3.1 General

The main use of ISO/IEC 15408 (all parts) is to assess the security of IT products. The term “IT product” is never actually defined in ISO/IEC 15408; however, it can be understood to cover any type of entity built using information technology, whether a complete IT system used exclusively by one organization, or a COTS package created by a product manufacturer for sale to many different and unrelated customers. In this document, when this document talks about IT products, or just products, the advice is intended to apply to all such entities. Where the scope of our advice is limited to a particular type of product, this document talks about systems, or COTS products, or some other explicitly specific wording.

As IT products may be used in many ways, and in many types of environment, the notion of security will vary with the product. The end result of an ISO/IEC 15408 evaluation is, therefore, never “this IT product is secure”, but is always “this IT product meets this security specification”.

ISO/IEC 15408 has standardized security specifications to (among others):

— mandate-specific content needed to assess a product against the security specification;

— allow comparison of security specifications of different products.

ISO/IEC 15408 recognizes two different types of security specifications: Protection Profiles (PPs) and Security Targets (STs). The difference between these two is best explained by the roles they are intended to play in a typical product purchasing process, where a customer seeks to buy a product from a developer.

The notions of customer, developer and product are deliberately kept abstract. A customer is someone who wants to buy a product. It can be a single individual, an organization, a group of organizations, a government department, etc. A developer is someone who wants to sell a product. It can be a single programmer, a small company, a large company, a group of companies working together, etc. Finally, a product could be anything from a small software application or a smart card to a large operating system or a complete computer system containing hundreds of distinct components.

When our customer wishes to buy a product, he has essentially two possibilities.

— The customer contacts a developer, specifies his needs, and the developer creates a product that is specifically targeted towards that customer and exactly fulfils the demands of that customer. This may be expensive but the customer gets what he wants. In the remainder of this clause, this document will call this a specification-based purchasing process.

— The customer selects a product from a number of existing products. This is probably cheaper, but the resulting product may or may not exactly fulfil the customer's needs. In the remainder of this clause, this document will call this a selection-based purchasing process.

When IT security is important, these purchasing processes have an added difficulty. For the average customer, it is

— hard to define what kind of IT security he needs,

— harder to determine whether the IT security that a given product claims to have is useful or sufficient to meet his needs, and

— even harder to determine that if a product claims to have security properties, that these claims are true.

To assist a customer through a purchasing process and address the difficulties listed above, an evaluation of the product using ISO/IEC 15408 may be useful, and in this case, Protection Profiles and Security Targets play an important role. In 6.3.2 and 6.3.3, this document shows how an evaluation may assist each type of process: specification-based and selection-based.

Of course, IT products do not work in isolation. The product is used by the customer in an operational environment, which may contain security measures of its own. Sometimes, the product will make assumptions that certain types of security features exist within that operational environment. These assumptions will also form part of the PP or ST.

6.3.2 Specification-based purchasing processes

6.3.2.1 Overview

In a specification-based purchasing process, a customer writes a specification, provides this specification to a developer, and the developer then creates a product based on this specification. In more detail, the following steps should be performed.

a) The customer has to determine his security requirements informally.

b) The customer has to transform these informal security requirements into a more formal specification suitable for use by a developer.

c) The developer has to build a product based on this specification.

In the end, the customer wants to know that "this product is useful for me". Therefore, the quality of each of these steps is important.

6.3.2.2 Informal security requirements

The process of determining informal security requirements, that is determining "what is my security problem, and how should I address it?" is outside the scope of ISO/IEC 15408 and therefore outside the scope of this document. However, this does not mean that this is unimportant or easy by any means.

Nevertheless, ISO/IEC 15408 assumes that the customer is capable of defining his or her informal security requirements. If this is done incorrectly, the product that is purchased in the end may not meet the true security requirements.

Customer requirements, once written down, often have a number of problems associated with them, especially in the area of security. Customer requirements are typically

a) incomplete (not all the requirements are present). For example, important threats that the product should counter are missing;

b) not embedded. They are insufficiently tuned to the specific environment in which the product has to function, or do not describe this environment clearly enough;

c) implicit. Some product requirements have consequences, but these consequences are not included themselves. The developer may not take these implicit requirements into account;

d) not testable. The requirements are phrased ambiguously, so that it is not possible to verify whether a product meets the requirement or not;

e) too detailed. The implementation has in fact already been written down but not the reason why this was chosen. If, in a later stage, the requirements change, it is often unclear how these changes should be made;

f) filled with ambiguous terms, like "the communication shall be secure", without defining what "secure" means; and

g) inconsistent. The requirements are internally self-contradictory.

Providing these customer requirements to a developer in a raw form will generally lead to problems, as the developer may misunderstand them. Security evaluation may lead to even more problems, since evaluators may interpret requirements differently from both the customer and the developer.

For these reasons, an important step in the whole specification-based purchasing process is the formalizing of customer requirements. For security requirements based on ISO/IEC 15408, this formalization takes place using a so-called Protection Profile (PP). A PP is in essence a document that defines the customer’s security requirements in a formalized, standardized way.

6.3.2.3 Using PPs as specifications

PPs are typically written as a collaborative effort by a group consisting of large organizations, groups of organizations, government departments, as consumers and a group of developers. This collaboration should ensure that the customer needs are not only addressed, but also the technical feasibility of the requirements specified is given.

A PP contains many sections, but as a security specification, the most important is the “security functional requirements”. Using ISO/IEC 15408, it is mandatory to write these requirements in a special language, defined within that International Standard. Use of this language ensures that the Protection Profile is

a) not ambiguous. The language contains well-defined terms, so that a developer can understand the requirements and interpret them correctly;

b) testable. The language is defined to contain only testable terms. Thus, it will be possible to assess in a later stage whether the product actually fulfils the PP;

c) not too detailed. The language enforces a certain level of abstraction. This closely follows what should be the consumer requirements: the consumer wants something to be done but does not want to worry how this is accomplished; and

d) more complete. The language contains several constructions ("if this functionality is required then this other functionality is also required") to help ensure that implicit requirements are included.

A PP may also contain technology-specific refinements of the "security assurance requirements", describing in detail how the correctness and effectiveness of specific security functions need to be assessed. An example would be to demand the use of a defined test suite developed for testing the correctness of the implementation of a cryptographic algorithm or cryptographic protocol.

6.3.2.4 Building a product from a PP

The customer can now give the PP, i.e. his formalized requirements, to one or more developers. Each developer uses this PP as a starting point for the development of a product. As a first step in this process, he writes a Security Target (ST).

An ST used for this purpose is very similar to a PP, but where a PP defines the customer requirements and is in principle written by the customer, the ST is a product specification and written by the developer.

The developer can of course not deliver an arbitrary ST as a reaction to the customer's PP; his ST has to *conform* to the PP. This means that the product has to cover all the customer requirements, but

- the ST may specify more than the PP. The product will offer more security functionality than the customer requirements (note that this extra functionality is not allowed to be incompatible with the PP), because, for example, the product will be sold to several customers, each with similar but slightly different requirements, or because the product is derived from an existing, standard product; and
- the ST contains more detail than the PP. While the PP explains "what" needs to be secured, the ST also explains "how". The developer points out, in general terms, how he will implement the customer requirements.

A PP may permit the ST author flexibility to offer something that is equivalent but different in terms of security functionality provided (see 6.5.6).

The ST defines for the developer the security functionality his product should deliver, and serves as a "Specification of Security Requirements" for the rest of the development process.

The result of the development process should be a product that can be delivered to the customer, who in turn can install it and use it. Naturally, this product should perform as described in the ST.

6.3.2.5 Role of evaluation in a specification-based purchasing process

Until now, this document has only described the role of the customer and the role of the developer in this process. Based on this process, the developer could simply say to the customer (without further evidence):

a) "my ST complies with your PP";

b) "my product complies with my ST";

c) "therefore, my product complies with your PP and meets your requirements".

If the customer accepts these statements, the process ends here.

However, if a customer requires independent verification of these statements, he can enlist a third party (an evaluation facility) to check these claims of compliance by performing an ISO/IEC 15408 security evaluation. In this process, an evaluation facility uses the PP, the ST, the product and ISO/IEC 15408 to assess two statements:

a) the ST complies with the PP;

b) the product complies with the ST.

Note that two issues are still left open, despite evaluation.

a) *The translation of the customer's informal security requirements to a Protection Profile.* As said earlier, this process falls outside the scope of ISO/IEC 15408, but if this is not done correctly, the PP will not match the customer's requirements and therefore the product will likely also not match the customer's requirements.

b) *Evaluation does not "prove" compliance*. An ISO/IEC 15408 evaluation will never provide an absolute guarantee that the product meets the PP. It can only deliver a certain degree of assurance depending on the depth and scope of evaluation as specified in the PP or ST. If the PP requires compliance testing for some functions by using a specific test procedure as part of the assurance activities, the evaluation will ensure compliance for those functions as far as defined by the test procedure used.

6.3.3 Selection-based purchasing processes

6.3.3.1 Overview

6.3.2 discusses a customer delivering a specification and a developer implementing that specification. This subclause discusses a situation where a customer does not have the luxury of having a product made for him: he has to select from existing products. Therefore, the purchase is no longer based on compliance to a formalized statement of customer requirements (i.e. a PP), but on comparison of existing products by the customer.

In a selection-based purchasing process of an IT product,

a) a developer has to produce a product and a specification of this product and provide the specification to the customer, and

b) the customer has to determine from the specification (perhaps by comparing the specification to specifications from other developers) whether the specified product is the most suitable product for him to purchase.

As the customer in the end wants to know that “this product is suitable for me”, the quality of each of these steps is important.

6.3.3.2 Using a specification provided by the developer

In selection-based purchasing processes, the customer has to use a specification provided by the developer.

If this specification is informal, the same potential disadvantages hold as for the informal customer requirements discussed in 6.3.2.2. For this reason, this specification needs to be formalized as well. For this purpose, ISO/IEC 15408 uses the Security Target (ST), as already discussed in 6.3.2.4. The ST here is identical to the ST discussed in 6.3.2.4, with one obvious difference. Since it is not based on a customer’s PP, it cannot claim compliance to such a PP [it may claim compliance to other types of PP (see 6.3.4)].

Because the developer does not know a specific customer’s requirements, he will have to make an estimate of what the market wants and codify this in the ST. This, therefore, does not necessarily match with any customer’s specific requirements.

The developer builds his product according to the ST. This process is similar to that described for specification-based purchasing processes.

6.3.3.3 Comparing Security Targets by the developer

The customer can now compare the STs of a number of products and select the one that best matches his requirements (probably also considering non-security requirements such as price). This means that he will still somehow have to find out what his informal security requirements are (see 6.3.2.2) and compare these with the STs offered to him. If one or more products match his requirements, he is done. If this is not the case, he will either have to choose the “closest” product or find some other solution (i.e. change his requirements).

As already stated in 6.3.2, the process of deriving informal customer security requirements falls outside the scope of ISO/IEC 15408 and this document. Comparing requirements and an ST also falls outside the scope of ISO/IEC 15408, although guidance on this topic will be found in later clauses of this document.

6.3.3.4 The role of evaluation in a selection-based purchasing process

Similar to the specification-based purchase process, the developer could simply claim that his product meets the ST and if the customer accepts this claim, the process ends here.

However, it is customary for the developer to offer a certificate confirming that an independent third party (an evaluation facility) has validated the ST, and then performed an ISO/IEC 15408 security evaluation to confirm that the product indeed meets the ST. It is even possible for the customer to commission the evaluation if he or she believes it to be essential and the developer has not done so.

Note that using evaluated products still leaves two issues open:

a) *Proving equivalence of the customer's informal security requirements and the Security Target.* As said earlier, this process falls outside the scope of ISO/IEC 15408, but if it is not done correctly, the ST may not match the customer's requirements, and therefore, the product may not match the customer's requirements either;

b) *Evaluation does not "prove" compliance*. An ISO/IEC 15408 evaluation will never provide a perfect guarantee that the product meets the ST. It can only deliver a certain degree of assurance depending on the depth and scope of evaluation as specified in the ST.

6.3.4 Other uses of PPs

Protection Profiles have other uses. For example, standards bodies or vendor associations may specify PPs as best practice minimum security standards for specific types of applications. Governments and trade associations may mandate their use. Where these exist, both customers and developers are likely to require compliance with such PPs, as well as requiring or offering additional security functionality to meet their own specific needs.

Organizations specifying or mandating PPs for such purposes have an onerous responsibility to ensure that such PPs are minimal (they ask for no more than what is absolutely necessary) and realistic (they do not ask for functionality or assurances that are not achievable by developers).

A PP may also be developed to express the need for a certain type of security product, even though it is recognized that at the time of publication, no such products exist yet. If the reader is a product developer, treat such PPs with caution. By the time a suitable product has been developed, the requirements defined in the PP may be obsolete or the sponsors of the PP may no longer want to buy the product because they have found other ways to meet their requirements.

Finally, PPs are *security* requirement specifications. Beware of their attempted misuse to specify other types of requirements which, if made more explicitly, would be rejected.

6.4 The PP/ST development process

6.4.1 Including stakeholders in the development process

When a PP or ST is developed, it is crucial that the relevant stakeholders are represented in the development team. The development team should include experts in the product-type technology, the security functionality that will be included in the PP or ST, as well as experts familiar with the application of ISO/IEC 15408.

Although out of scope for this document, it is also important that the developer of the ST or PP has a thorough understanding of any applicable regulations and policies with regard to the proposed assurance consumer.

When developing an ST that is expected to be conformant to a PP, the team should include someone familiar with the application of that PP.

When developing a PP that several product developers may try to meet in the future, it is recommended that stakeholders from the developer community are included. This will help ensure that the requirements of the PP can be met in the future, and that the requirements given do not inadvertently preclude products provided by certain vendors. Especially for a PP intended for use in a specification-based purchasing process, those stakeholders should also include representatives from the proposed end-user community.

With such a large variety of stakeholders represented, it can be expected that developing a PP can take some time, usually in the order of months, and that the development process requires collaboration and negotiation skills.

As an example, the concept of a collaborative Protection Profile (cPP), a construct of the Common Criteria Recognition Arrangement (CCRA), seeks to ensure that all the relevant stakeholders are involved in the development of a cPP through the establishment of technical communities or an international Technical Community (iTC) recognized by the CCDB, and ensuring that the needs of the specification-based purchasing processes of the proposed assurance consumers are met.

The process for the development of a cPP by an iTC is defined by the CCDB. Details of this process can be found on the website maintained by the CCDB.

6.4.2 Method to develop a PP or ST

The order of presentation of the requirements for PPs and STs in ISO/IEC 15408-1:2009, Annexes A and B and in the earlier parts of this clause may suggest that it is expected that PPs and STs are always developed in a logical "top-down" manner, e.g. (in the case of an ST) that

a) the security problem is first defined,

b) the security objectives are then identified to address the security problem,

c) security requirements are then defined to satisfy the security objectives for the TOE, and

d) actual security functions are then selected to satisfy the security requirements.

Whilst such a possibility is not ruled out, it is more likely that an iterative process will be required. For example, definition of security requirements may highlight clarifications needed to the definition of the security objectives, or even the security problem. In general, a number of iterations may be required in which the relationships between threats, organizational security policies, security objectives and security requirements and functions are examined closely, particularly when rationales are being constructed. Only when all identified gaps in the rationales are filled may it be assumed that the PP or ST is complete.

During an iterative process of PP or ST development, new information may surface, within the scope of the current security problem, that may lead changes to the document which reflect changes in external circumstances, for example,

a) new threats may be identified,

b) organizational security policies may change,

c) cost and time constraints may impose changes in division of responsibility between what the TOE is expected to do and what is expected of the TOE environment, and

d) changes in intended attack potential may impact the TOE security problem definition.

It is also possible (particularly if the TOE is a product which has already been developed) that the PP or ST author already has a clear idea of the security functionality the TOE will provide (even if this has not yet been expressed as ISO/IEC 15408 security functional requirements). In such cases, the definition of the security concerns and security objectives will unavoidably be influenced by the knowledge of the form of the security solution the TOE provides. The PP/ST development process will in those cases be, to some extent, "bottom-up".

6.4.3 Evaluation of PPs and STs

ISO/IEC 15408 describes the evaluation of both PPs and STs. The goal of evaluating these documents is to determine whether it is complete, consistent, and technically sound. ISO/IEC 15408-3:2008 contains the evaluation criteria that an evaluator is obliged to consult in order to determine this. These criteria, and the evaluation methodology associated with Protection Profile Evaluation (APE class) and with