TECHNICAL SPECIFICATION

ISO/IEC TS 19608

First edition
2018-10

Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

Lignes directrices pour l'élaboration des exigences fonctionnelles de sécurité et de confidentialité fondées sur l'ISO/IEC 15408

Reference number
ISO/IEC TS 19608:2018(E)

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

Published in Switzerland

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 document 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 and IEC 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 of 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 www.iso.org/iso/foreword.html.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

ISO/IEC 29100 defines a framework of privacy principles that should be considered when developing systems or applications that deal with personally identifiable information (PII). This document analyses those principles and maps them, where possible, to the security functional requirements defined in ISO/IEC 15408-2. Where such a mapping is not possible, this document derives new security functional requirements collected in one new class that contains several families of privacy related security functional components following the guidance for developing new classes, families and components provided in ISO/IEC 15408-1 and ISO/IEC 15408-2.

This document can also be used as guidance for developing further privacy functional requirements using the framework of ISO/IEC 15408. The class, families, and components defined in this document can be extended for cases where the components defined here are not sufficient to express specific privacy functional requirements.

Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

1 Scope

This document provides guidance for:

— selecting and specifying security functional requirements (SFRs) from ISO/IEC 15408-2 to protect Personally Identifiable Information (PII);

— the procedure to define both privacy and security functional requirements in a coordinated manner; and

— developing privacy functional requirements as extended components based on the privacy principles defined in ISO/IEC 29100 through the paradigm described in ISO/IEC 15408-2.

The intended audience for this document are:

— developers who implement products or systems that deal with PII and want to undergo a security evaluation of those products using ISO/IEC 15408. They will get guidance how to select security functional requirements for the Security Target of their product or system that map to the privacy principles defined in ISO/IEC 29100;

— authors of Protection Profiles that address the protection of PII; and

— evaluators that use ISO/IEC 15408 and ISO/IEC 18045 for a security evaluation.

This document is intended to be fully consistent with ISO/IEC 15408; however, in the event of any inconsistency between this document and ISO/IEC 15408, the latter, as a normative standard, takes precedence.

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, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408 -1, ISO/IEC 18045, ISO/IEC 29100 and the following apply.

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

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

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

3.1
privacy functional component
extended component that serves as a standard template on which to base *privacy functional requirements* (3.3) for TOEs

3.2
privacy requirement
requirement, stated in a standardized language, which is meant to contribute to achieving the technical privacy controls for a TOE based on *privacy functional requirements* (3.3)

3.3
privacy functional requirement
PFR
translation of the technical privacy controls for the TOE into a standardised language based on *privacy functional components* (3.1)

4 Symbols and abbreviated terms

The following abbreviated terms are used in this document.

MRTD	Machine Readable Travel Document
OSP	Organizational Security Policy
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PP	Protection Profile
SPD	Security problem definition
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TRA	Threat Risk Assessment
TSF	TOE Security Functionality

5 Purpose and structure of this document

Research shows that security and privacy should be considered from the beginning of the development life cycle for IT products, systems and applications in order to avoid expensive rework and reduce potential problems.

Security and privacy should also complement and mutually reinforce each other. The degree of protection should depend on the sensitivity of data and the linkability of data to personal identifiers. Therefore, successful implementation of security and privacy depends on defining accurate and complete requirements for both in a coordinated manner from the start of the development.

ISO/IEC 15408-2 defines a catalogue of security functional requirements (SFRs). ISO/IEC TR 15446 also provides detailed guidance on how to specify SFRs for a Target Of Evaluation (TOE). Developers can refer to these documents to specify SFRs to protect PII and other assets.

There are currently no ISO/IEC documents that specifically support privacy friendly design of IT products, systems and applications. Guidance on deriving privacy functional requirements from the privacy principles described in ISO/IEC 29100, as well as a procedure for defining both SFRs and privacy functional requirements in a collaborative manner is, therefore, missing.

This document aims to fill this gap and provide guidance for developers on how to:

a) select and specify SFRs from ISO/IEC 15408-2 to protect personally identifiable information (PII) (this guidance refers to ISO/IEC 15408 and ISO/IEC TR 15446);

b) develop new privacy functional requirements, as extended components, based on the privacy principles defined in ISO/IEC 29100 using the paradigm described in ISO/IEC 15408-2. (This guidance is the main focus of this document); and

c) conduct both of the above steps in a coordinated manner.

Clause 6 provides an introduction to SFRs — what they are, when and how they can be used to specify accurate and complete security requirements.

Clause 7 explains the privacy principles defined in ISO/IEC 29100 and what privacy requirements can be derived from these principles. These privacy requirements are formulated as privacy functional components in Clause 8.

Clause 8 lists the privacy functional components developed in this document.

Annex A lists the security functional components in ISO/IEC 15408-2 that address privacy threats.

Annex B provides examples of PPs that define extended components to specify privacy requirements.

Annex C defines the extended privacy functional components in the format required by ISO/IEC 15408-1.

6 Requirement definition

6.1 General

Requirement definition is the first step in developing IT products, applications and systems. Security requirements are derived to address security threats that shall be countered or to address specific regulations or policies for the protection of PII. How far those regulations and policies are addressed by the target of evaluation (TOE) and which requirements are assumed to be addressed by the environment in which the TOE operates, are expressed by specifying security objectives for the TOE and assumptions for the TOE environment. The security objectives, which are often very general, are addressed by security requirements, which can be implemented and tested.

In ISO/IEC 15408, security requirements are expressed in the form of SFRs in the protection profile (PP) or security target (ST). The author of a ST or PP explains how the SFRs address the security objectives defined for the TOE. These SFRs are the core of TOE evaluations because evaluators examine these specifications and the TOE design documents in order to determine that they are a complete and accurate instantiation of SFRs of the TOE. Evaluators also test whether the TOE operates according to these specifications and the design or not. TOE evaluations also include a vulnerability analysis, based on the SFRs, in order to help the identification of vulnerabilities in the TOE. Therefore, SFRs shall be accurate, testable and traceable so that the TOE evaluations can be conducted objectively.

While there can be occasions where privacy and security objectives are the same, they are not always aligned. As explained in ISO/IEC 15408-1, security objectives can be derived from a threat analysis or from organizational security policies. Whereas these policies can also define privacy requirements which are typically derived from an analysis of relevant legislation, regulation and any organizational privacy policies that can be in place.

ISO/IEC 15408 defines a vulnerability as a weakness in the TOE that can be used to violate the security objectives or SFRs in some environment that satisfies the assumptions defined for the TOE environment.

A vulnerability analysis therefore focuses on the detection of scenarios where the security objectives are not met although all SFRs are correctly implemented and all assumptions made for the TOE environment are satisfied.

EXAMPLE Examples of such vulnerabilities are implementation side effects like incomplete parameter validation or design side effects like covert communication channels that can be used to obtain information in violation of a defined information flow policy.

The following subclauses provide readers with minimum knowledge of the concept of SFRs so that readers can understand the content of this document, minimizing the need to refer to other documents. Most of descriptions in the following subclauses are extracted as a summary from ISO/IEC 15408 and ISO/IEC TR 15446.

6.2 Security functional requirements (SFRs)

6.2.1 General

The TOE implements security functions to protect its assets from unauthorized disclosure, modification, or loss of use. SFRs are the requirements for those security functions that the TOE security functionality (TSF) shall provide.

NOTE The TSF is the part of the TOE that implements the SFRs.

ISO/IEC 15408-1 provides a framework to define SFRs, in a standardized language in order to ensure exactness and facilitate the comparability of security requirements. ISO/IEC 15408-2 then provides a catalogue of security functional components which are the basis for the SFRs. PP/ST authors select an appropriate set of security functional components from this catalogue for their TOE and tailor these security functional components through operations (see 6.2.3) in order to meet their needs and to ensure that the specification of security requirements in the form of SFRs is complete.

TOE evaluations determine if the TOE actually meets the all of these SFRs through the evaluation activities defined in ISO/IEC 18045.

NOTE Evaluation activities include the review of the PP/ST, specification, functional testing and vulnerability analysis.

The catalogue of SFRs defined in ISO/IEC 15408-2 covers many aspects of security functionality but also allows for the specification of additional SFRs that are not in this catalogue. The framework provided in ISO/IEC 15408-1 shall be used to define additional SFRs for a security functionality that is not covered by the SFRs defined in ISO/IEC 15408-2.

6.2.2 Example of security functional requirements

Figure 1 gives an example of a security functional component provided in ISO/IEC 15408-2.

EXAMPLE 1

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[*assignment: *positive integer number]*], an administrator configurable positive integer within [assignment: *range of acceptable values*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

Figure 1 — Security functional component for authentication failure handling

FIA_AFL.1 is a component for authentication failure handling. This component requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry from which the attempts were made until an administrator-defined condition occurs.

EXAMPLE 2 An example of a point of entry is a work station.

6.2.3 The selection, assignment, refinement and iteration operations

ISO/IEC 15408 permits a degree of flexibility in the way the SFRs are specified by allowing PP/ST authors to tailor the security requirement appropriately. In FIA_AFL.1, PP/ST authors can specify appropriate variables and actions after the word "assignment:" and select appropriate elements from several items specified after the word "selection:" to complete the security requirement.

EXAMPLE 1 If the TOE needs to lockout telnet administrator's login after 3 unsuccessful login attempts, PP/ST authors assign and select appropriate values or items as follows:

FIA_AFL.1.1 The TSF shall detect when **[3]** unsuccessful authentication attempts occur related to [**authentication of the telnet administrator**].
FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**met**], the TSF shall [**lockout the telnet administrator's login**].

Figure 2 — A completed SFR for authentication failure handling

PP/ST authors can also tailor the requirement using the refinement operation under the following restrictions:

a) a TOE meeting the refined requirement also meets the unrefined requirement in the context of the PP/ST (i.e. a refined requirement must be "stricter" than the original requirement); and

b) refinement shall be related to the original component.

EXAMPLE 2 An example of a valid refinement is shown in Figure 3.

In ISO/IEC 15408-2;
FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user."
being refined to:
FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated **by username/password** before allowing any other TSF-mediated actions on behalf of that user.

Figure 3 — Example of the refined SFR for timing of authentication

The PP/ST authors can use the same functional component to express two or more distinct requirements for the TOE. Each iteration of a component shall be different from all other iterations of that component, which is realized by completing assignments and selections in a different way, or by applying refinements to it in a different way.

ISO/IEC 15408 does not provide any other methods to tailor the SFRs other than selection, assignment, and refinement operations. However, there can be security requirements for the TOE that existing components in ISO/IEC 15408-2 cannot cover. In this case, new components (extended components) shall be defined in the PP/ST.

6.2.4 Dependencies between components

Dependencies can exist between security functional components. Dependencies arise when a component is not self-sufficient and relies on the presence of another component to provide security functionality.

EXAMPLE 1 As shown in Figure 1, FIA_AFL.1 has a dependency to "FIA_UAU.1 Timing of authentication" that is a component for user authentication because the TOE must authenticate users before detecting unsuccessful authentication attempts.

EXAMPLE 2 In FAU_GEN.1 (Audit data generation) and FPT_STM.1 (Reliable time stamps). FAU_GEN.1 requires that for audit record generation and has a dependency to FPT_STM.1 because FAU_GEN.1 requires the inclusion of the date and time of the event in each audit record. Such time stamps must be reliable in order to provide the correct date and time of the event.

If FIA_AFL.1 is selected in the PP/ST, then the PP/ST authors shall either include FIA_UAU.1 in the PP/ST or provide a justification as to why the PP/ST does not contain FIA_UAU.1. The same is true for FAU_GEN.1 and FPT_STM.1.

6.2.5 Structure of security functional components

In ISO/IEC 15408-2 the security functional components are organized into hierarchical structures:

— classes; consisting of

— families; consisting of

— components; consisting of

— elements.

ISO/IEC 15408-2 contains classes of families and components, which are rough groupings on the basis of related function or purpose.

EXAMPLE

Two elements, FIA_AFL.1.1 and FIA_AFL.1.2, belong to the security functional component FIA_AFL.1. FIA_AFL.1 belongs to the FIA_AFL family that contains requirements for defining values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. This FIA_AFL family also belongs to the FIA (Identification and authentication) class that addresses the requirements for functions to establish and verify a claimed user identity. This FIA class includes other relevant families such as FIA_UAU (User authentication), FIA_UID (User identification) and FIA_SOS (Specification of secrets).

This organization into a hierarchy of class-family-component-element is provided to assist PP/ST authors in locating specific components. ISO/IEC 15408-2 presents all of the security functional components in the same general hierarchical style and uses the same organization and terminology for each.

6.2.6 List of classes

ISO/IEC 15408-2 defines the following classes which cover a broad spectrum of security requirements.

Table 1 — List of classes

Class name	Security requirements
FAU: Security audit	Requirements for security auditing involving recognizing, recording, storing, and analysing information related to security-relevant activities to determine which security-relevant activities took place and who is responsible for them.
FCO: Communication	Requirements concerned with assuring the identity of a party participating in a data exchange which are the originator of transmitted information and identity of the recipient of transmitted information.
FCS: Cryptographic support	Requirements for cryptographic functionality to help satisfy other security components belong to other classes. Components in this class are used when the TOE implements cryptographic functions, the implementation of which can be in hardware, firmware and/or software.
FDP: User data protection	Requirements related to protecting user data and split into four groups of families that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.
FIA: Identification and authentication	Requirements for functions to establish and verify a claimed user identity. Identification and Authentication is required to ensure that users are associated with the proper security attributes. EXAMPLE Security attributes include identity, groups, roles, security, and integrity levels.
FMT: Security management	Requirements to specify the management of several aspects of the TSF: security attributes, TSF data and functions. The different management roles and their interaction, such as separation of capability, can be specified
FPR: Privacy	This class contains privacy requirements. These requirements provide a user protection against discovery and misuse of identity by other users.
FPT: Protection of the TSF	Requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. In some sense, families in this class can appear to duplicate components in the FDP.
FRU: Resource utilization	Requirements that support the availability of required resources such as processing capability and/or storage capacity.
FTA: TOE access	Requirements for controlling the establishment of a user's session such as limiting number of concurrent sessions that belong to the same user.
FTP: Trusted path/channels	Requirements for a trusted communication path between users and the TSF and for a trusted communication channel between the TSF and other trusted IT products.

6.3 Procedure to specify security functional requirements

It is expected that PPs and STs are developed in a logical “top-down” manner such that:

a) the security problem is first defined;

b) the security objectives are then identified to address the security problem; and

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

In the security problem definition (SPD), the PP/ST authors define the threats to the assets that the TOE shall protect and the organizational security policies (OSP) that the TOE shall comply with. This is done by:

a) identifying the security objectives that address the threats and security policies; and

b) translating these security objectives into SFRs in the PP/ST.

Therefore, PP/ST authors shall include an appropriate set of threats and security organizational policies in the security problem definition in order to enable the specification SFRs for the TOE.

However, ISO/IEC 15408 does not assume or mandate any particular process or methodology for preparing the security problem definition and so PP/ST authors can use any method they like. ISO/IEC TR 15446 includes a detailed description of a simple methodology to define the security problem that has been tried and tested in practice and found to work in a variety of organizations and environments.

6.4 Procedure to develop functional components

6.4.1 Procedure

During specification of the SFRs, it is possible that PP/ST authors are not able to correctly specify a requirement even when using the freedom given in refining existing components from ISO/IEC 15408-2.

In this case, ISO/IEC 15408-1 allows for the definition of extended components. However, PP/ST authors cannot define extended components freely. As part of an evaluation, extended components defined in a PP/ST shall be evaluated in order to determine if the extended components are necessary (i.e. that they cannot be clearly expressed using existing ISO/IEC 15408-2 components), and if such extended components are necessary, that they have been clearly and unambiguously defined.

Before defining extended components, PP/ST authors should:

a) first attempt to use existing components from ISO/IEC 15408-2, potentially with refinements. Extended components can be used only in cases where this is either not possible or becomes too complicated. Annex A shows examples of existing components that have been used to address privacy threats.

b) investigate extended components in evaluated and published PPs/STs to check if an extended component has already been defined that the PP/ST authors can use. Taking an already defined extended component from an evaluated PP/ST has the advantage that the component itself has already been checked for consistency and conformance against the requirements of the ISO/IEC 15408 series as part of the evaluation of the PP/ST that contained it. Annex B shows examples of extended components defined in PPs/STs that have been used to address privacy threats.

When defining new extended components, PP/ST authors should:

a) define components in a similar way to existing components in ISO/IEC 15408-2. This applies to the naming of the extended component, the way they are expressed and the level of detail provided. It is therefore recommended to describe an extended component using the same structure that is given in ISO/IEC 15408-2.

b) define components in such a way that they are testable and traceable through the appropriate TSF representations (i.e., the specification and design documentation of TOE).

c) identify the functional components that are needed along with any newly defined components that satisfy the security requirements associated with the extended component and specify them in the dependency list.

All terms in the extended components should be well defined in order to avoid any misunderstanding due to the introduction of vague terms. This is because vague terms are neither testable nor traceable.

6.4.2 Existing components for privacy requirements in ISO/IEC 15408-2

The class FPR (Privacy) is directly related to privacy requirements. This class includes the families shown in Table 2 that provide privacy requirements for a user protection against discovery and misuse of identity by other users.

Table 2 — FPR Families

FPR family name	Related requirements
Anonymity (FPR_ANO)	This family ensures that a user can use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity.
Pseudonymity (FPR_PSE)	This family ensures that a user can use a resource or service without disclosing its user identity but can still be accountable for that use.
Unlinkability (FPR_UNL)	This family ensures that a user can make multiple uses of resources or services without others being able to link these uses together.
Unobservability (FPR_UNO)	This family ensures that a user can use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

The other classes listed in Table 1, such as FIA, can also be used to address privacy objectives. As described in 6.3, PP/ST authors define the "security" problem that describes threats to confidentiality, integrity, and availability of informational assets. However, ISO/IEC 15408-1 and ISO/IEC 15408-2 are flexible enough to also cover privacy threats and hence for the PP/ST authors to identify corresponding functional components that address such privacy threats. Annex A gives examples of the use of existing functional components in addressing privacy threats such as location tracking of users.

6.4.3 Extended components for privacy requirements in published PP/STs and research papers

As explained in 6.4.1 b), extended components in evaluated PPs/STs should be used when possible. There are many PPs/STs published in various catalogues. However, very few PPs/STs define extended components for privacy threats. Two such PPs and their extended components are listed in Annex B.

EXAMPLE A commonly used catalogue is the Common Criteria portal[1].

7 Privacy principles

7.1 General

Security functional components defined in ISO/IEC 15408-2 serve as a "common language" among consumers, developers, and evaluators for expressing security requirements for the TOE. However, as described in 6.4.2, ISO/IEC 15408-2 only defines a limited set of security functional components to address privacy threats.

This document provides extended components that can serve as the "common language" for privacy requirements. PP/ST authors can specify both security and privacy requirements at the same time and still achieve the same level of quality expressed in ISO/IEC 15408-2, by using the extended components defined in this document.

7.2 Input for extended components

ISO/IEC 29100 describes privacy principles derived from existing principles that have been developed by a number of states, countries, and international organizations. These privacy principles should be used to guide the design, development, and implementation of privacy controls. This document considered all of the privacy principles given in ISO/IEC 29100 in order to identify the privacy requirements given in this document. However, only those requirements that can be objectively tested in TOE evaluations are included in this document.

This document assumes that PP/ST authors determine the following items based on the purpose of the TOE. In this document, extended components have been developed with the assumption that the following were well defined in advance:

a) the purpose(s) of processing PII: PP/ST authors define the legitimate purposes for processing of PII;