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;

b) the minimum set of PII that the TOE needs to process: PP/ST authors identify the minimum set of PII that the TOE needs to process for the specified purposes.

7.3 Procedure to develop privacy requirements from privacy principles

This document applied the following procedure to develop privacy functional components based on the guidance described in 6.4.1:

a) derivation of privacy requirements from each privacy principle. Such requirements are described using defined terms in ISO/IEC 15408 and ISO/IEC 29100 in italic font as source text;

b) identification of existing functional components in ISO/IEC 15408-2 or of extended components found in published PPs/STs that can be used to express these requirements;

c) formulation of the privacy requirements as new extended components if existing components are not applicable.

7.4 Extended components for privacy

7.4.1 "Consent and choice" principle

7.4.1.1 General

The methods, timing of choice and conditions of consent should be determined by PP/ST authors considering any applicable law, the sensitivity of the PII and other factors.

7.4.1.2 Presenting choice and obtaining consent

The TOE can implement functionality to present one or more choices to PII principals regarding the processing of their PII and to obtain their consent for such processing.

There can be legal requirements in some jurisdictions. These legal requirements shall be considered in the development of any mechanisms intended to facilitate the obtaining of consent.

EXAMPLE Some legal requirements express that consent must be informed, freely given and specific.

There are a number of different methods used to implement the choice and consent principle. However, choice and consent should be presented at a time and in a context that is relevant to the PII principals' decision about whether to permit PII collection. Choice and consent should be also presented to PII principals in a prominent and easily accessible place. Consent and choice assumes that the PII principal is aware of the organization's privacy practices, which shall be described in the notice that is made available to the PII principal. For more information about the purpose and content of the notice, see ISO/IEC 29100:2011 4.6. If conditions of consent described in the notice are related to other functional components, PP/ST authors shall include such components in the PP/ST.

EXAMPLE 1 An example of a method to implement choice and consent is opt-in and opt-out.

EXAMPLE 2 An example where conditions of consent are related to other functional components is the means offered for accessing PII (7.4.5.1) and retention period of PII [7.4.4.1 f)].

The access control policy defined for PII is applicable.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall provide choice and obtain consent for the processing of PII through methods, timing and conditions specified by PP/ST authors.

PP/ST authors may iterate the above component, using the iteration operation, if the TOE implements different types of choice and consent for different types of PII.

Applicable security functional components

ISO/IEC 15408-2 does not define any functional components for this requirement because the ISO/IEC 15408 functional requirements paradigm does not cover the concept of "choice and consent".

New extended components, FFPW_COL.1 and FFPW_CON.1 are defined in 8.2.1.

Dependencies

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.1.3 Reaffirming the choice selected

The TOE may implement functionality in order to reaffirm the choices made, and the consent granted, by PII principals before the TOE processes their sensitive PII.

PII principals may not remember the choice they selected for their PII in the past. Past choices (explicit or implied) may not have been provided by the current user of the TOE. If a choice is provided only at the time of consent, PII principals can inadvertently distribute PII over a long period of time if they do not know the current choice. The TOE can proactively notify PII principals of their choice through various methods when the TOE collects or transfers sensitive PII. The TOE can also provide an interface that allows the PII principals to review the choice they selected for their PII.

EXAMPLE Methods of notification include displaying an icon or light when collecting location information.

The method used and applicable PII should be determined by PP/ST authors.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall be able to notify the PII principal, or a duly authorized individual acting on their behalf, about choices previously made and consents previously granted before processing the specific PII. The PP/ST author may also specify the type of PII for which the SFR applies and the method used to notify the PII principal.

Applicable security functional components

ISO/IEC 15408-2 does not define any functional components for this requirement because the existing paradigm does not cover the concept of "choice and consent".

New extended components, FPFW_MOC.1 and FPFW_NOC.1, are defined in 8.2.2.

Dependencies

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.1.4 Preserving a record of choices

The TOE can preserve records of the PII principals' choices.

The PII principals can access the TOE through different types of external IT entities. The PII principals can also delete configuration files that save the PII principals' choices. In some jurisdictions, there can be limitations on the extent to which a TOE can preserve a principal's choices. The TOE can, where permitted to do so, implement mechanisms to preserve PII principals' choices, even if such choices have been deleted by the principal. The TOE can, where permitted to do so, also preserve the principals' choices across multiple devices used to access the TOE.

Conditions under which the TOE can preserve records of the choices of PII principals can be determined by PP/ST authors.

EXAMPLE 1 Mobile devices and personal computers are types of external IT entities.

EXAMPLE 2 Cookies are examples of configuration files that save a PII principal's choices.

EXAMPLE 3 Login by unique ID is a condition under which the TOE can preserve the choices made by a PII principal.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall preserve users' choice given the conditions specified by PP/ST authors.

Applicable security functional components

In some cases, but not all, preserving the choice previously selected by the user is similar to preserving the definition of an access control list or preserving configurations made. In these circumstances, no explicit SFR is required for this.

New extended components, FFPW_COL.1 and FFPW_CON.1 that are related to this principle are defined in 8.2.1.

Dependencies

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.1.5 Exempting PII from processing upon modification or withdrawal of consent

The TOE shall exempt PII from processing upon modification or withdrawal of consent.

Subclause 7.4.1.2 describes the requirement to implement functionality to present to PII principals the choice whether or not to allow processing of their PII. The TOE shall also implement functionality to allow PII principals to modify or withdraw their consent on their own. With limited exceptions, the TOE shall exempt their PII from further processing in accordance with such modification or withdrawal and the TOE can exempt their PII with limited exceptions according to such modification or withdrawal.

EXAMPLE 1 An example of exempting PII is delete or archive.

EXAMPLE 2 An example of a limited exception is the requirement to retain PII according to applicable laws.

After modification or withdrawal of the consent the TOE shall delete the PII collected under the consent. If such PII deletion is not possible or can only be partially performed, the TOE shall inform the PII principal about the limits on the modification or deletion of their PII.

EXAMPLE 3 An example of where PII deletion is not possible is where the PII must be retained to satisfy a legal obligation.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall stop processing the PII upon modification or withdrawal of consent, through methods specified by the PP/ST authors and delete PII previously collected with exceptions specified by PP/ST authors unless otherwise specified in the applicable legislation or regulation. If the previously collected PII cannot be deleted completely, the TSF shall notify the user about the limitations in deleting PII.

Applicable security functional components

ISO/IEC 15408-2 does not define any functional components for this requirement because the existing paradigm does not cover the concept of "choice and consent".

A new extended component, FPFW_MOC.1, is defined in 8.2.2.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.2 "Purpose legitimacy and specification" principle

This document assumes that PP/ST authors define the legitimate purposes for PII processing. ISO/IEC 15408-2 does not define and components related to this principle and no extended components are defined for this principle.

7.4.3 "Collection limitation" principle: Collecting PII

The TOE shall collect only that PII strictly necessary for the specified purposes.

This document assumes that PP/ST authors define in detail which PII the TOE collects and the purposes of processing the PII. This document also assumes that PP/ST authors ensure that the PII to be collected is strictly necessary for its purposes. Therefore, the TOE shall collect only PII specified by PP/ST authors and shall not require the user to provide any other PII.

Elements of PII to be collected should be determined by PP/ST authors.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall collect only PII specified by the PP/ST authors and shall not require the user to provide other PII.

Applicable security functional components

ISO/IEC 15408-2 defines functional components for importing and protecting data under the defined access control or information flow control policy given in the FDP class. These components, with refinements, may be used to specify this requirement.

See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

Dependencies

This requirement depends on the import of user data and the protection of user data.

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

7.4.4 "Data minimization" and "Use, retention and disclosure limitation" principles

7.4.4.1 Minimizing PII

7.4.4.1.1 General

The TOE shall minimize PII for processing.

Subclause 7.4.3.1 defines a requirement to collect PII strictly necessary for the specified purposes. However, the TOE can further minimize PII through one or more of the methods described below.

7.4.4.1.2 Minimize PII by filtering and removal

When the TOE imports PII from PII principals, different types of metadata can be unintentionally transmitted to the TOE. Such metadata can be identified and removed by the TOE if it is not necessary for the specified purposes.

EXAMPLE An example of metadata is EXIF data attached with image file.

PP/ST authors shall specify which PII the TOE is to remove as well as the methods of removal.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall be capable of determining when imported data contains more PII than required and shall be capable of identifying that data as PII that it should not process. The TSF shall remove those parts of the PII so identified.

Applicable security functional components

A new extended component, FPFW_RMV, that can be used to minimize PII by filtering and removal and to minimize PII retention are defined in 8.2.3.

Dependencies

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.4.1.3 Minimize sensitivity of PII by conversion

After the TOE receives PII, part of this PII, especially sensitive PII that has been received can be converted to a less sensitive or pseudonymized form.

EXAMPLE An example of sensitive PII is that received because it is part of general information received or received for statistical purposes only.

EXAMPLE Examples of conversion include:

— If the TOE uses IP address to determine the location of PII principals for statistical analysis, the TOE can discard the IP address after mapping it to a city or town.

— If the TOE receives video data from surveillance cameras, the TOE can recognize persons standing or moving within the scene and obfuscates them in specific region.

— If the TOE is a smart metering system, the TOE can aggregate the energy use over a certain period, rather than recoding it in real time.

PII that the TOE shall convert and the conversion method can be specified in the PP/ST.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall, after identifying PII for conversion, convert that PII to a less sensitive form as defined by the PP/ST authors using methods specified by the PP/ST authors.

Applicable security functional components

ISO/IEC 15408-2 defines the classes that can be used to address those requirements.

See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

7.4.4.1.4 Minimize identifiability of PII by use of anonymity, pseudonymity, unlinkability and unobservability

The TOE can ensure that:

a) PII principals can use a resource or service without disclosing its identity to others (Anonymity);

b) PII principals can use a resource or service without disclosing its identity, but can still be accountable for that use (Pseudonymity);

c) PII principals can make multiple uses of resources or services without others being able to link these uses together (Unlinkability); and

d) PII principals can use a resource or service without others, especially third parties, being able to observe that the resource or service is being used (Unobservability).

The goal selected from the list above depends on the identified requirements and associated risks. In some instances, pseudonymity is more appropriate than anonymity. In addition, some types of privacy threats are best countered by a combination of components from several methods.

EXAMPLE An example of when pseudonymity rather than anonymity is appropriate is when there is a requirement for auditing.

Applicable security functional components

ISO/IEC 15408-2 defines the components in the FPR class for these requirements.

See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

7.4.4.1.5 Minimize accumulation of PII by division

Depending on the circumstances, the TOE can be structured into independent parts, each subject to distinct access control functions. The PII can also be split among the independent parts and controlled by each part using different access control mechanisms. If one part of the TOE is compromised, the damage to the whole PII can be reduced.

Expression of the requirement

The requirement can be expressed as follows:

The TSF shall be structured in separate, independent parts governed by distinct access control mechanisms to minimize the damage to the PII.

Applicable security functional components

ISO/IEC 15408-2 defines components in the FDP classes that can be used to address this requirement.

See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

7.4.4.1.6 Minimize access to PII

The TOE can limit access to PII based on the “need-to-know” principle. Sensitive PII can be segregated and be subject to additional access controls. The TOE can also encrypt sensitive PII in transit and in storage. Access to temporary shadow files created during the processing of PII can also be restricted to those with a “need-to-know”.

Applicable security functional components

ISO/IEC 15408-2 defines the FDP and FCS classes that can be used to address those requirements.

See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

7.4.4.1.7 Minimize PII retention

The longer data is retained, the higher the likelihood of compromise and data becoming inaccurate. The TOE shall retain PII only as long as necessary to fulfil the stated purposes, and securely dispose of it afterwards. The TOE can also allow the administrators to set the retention period and delete PII automatically when the period is expired.

PP/ST authors should set PII retention periods in accordance with relevant legislation and legislation. Where no specific requirements are provided by legislation or regulation, PP/ST authors should specify minimal retention periods.

Expression of the requirement

The requirement can be expressed as follows:

When PII is no longer required, the TOE shall securely dispose of PII in accordance with relevant legislation or regulation, or in the absence of such legislation or regulation, by using methods specified by the PP/ST authors.

Applicable security functional components

ISO/IEC 15408-2 defines security functional components for requirements defined for access control and encryption. See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

A new extended component, FPFW_DEL, that can be used to minimize PII by filtering and removal and to minimize PII retention are defined in 8.2.3.

NOTE 1 The requirement defined for "Minimize accumulation of PII by division" is a requirement for the architecture. Such architectural requirements cannot be expressed using the framework defined in ISO/IEC 15408-2.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.5 "Openness, transparency and notice" principle

This principle given in ISO/IEC 29100 is about:

a) providing PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the processing of PII;

b) providing notice of what PII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PII may be disclosed, and the identity of the PII controller including information on how to contact the PII controller;

c) where permitted by legislation or regulation, disclosing the choices and means offered by the PII controller to PII principals for the purposes of limiting the processing of, and for accessing, correcting and removing their information; and

d) giving notice to the PII principals when major changes in PII processing procedures occur.

In summary, this principle defines the obligations of the PII controller to provide information about their PII processing policy in general, any changes to the PII processing policy, or to the handling procedures, in regard to the choices offered to the PII principal. In addition, the PII controller shall inform the PII principal about any issues related to the processing of the principal's PII.

Depending on how the PII principal can access the information, there can also be a requirement to establish a trusted channel between the TOE and the PII principal before transferring information about issues related to PII.

Typically, the PII principal connects to the system to get information about the current policy or the choices they have made with respect to processing of their PII.

For changes in the policy and for getting information about specifics of the processing of the PII principal's PII, the PII principal should be sent notice of these events, requesting that they access the system to obtain the details.

Expression of the requirements

The requirements can be expressed as follows:

The TOE shall ensure that the PII principal is able to access information about the PII handling policy in general.

The TOE shall ensure that the PII principal is informed about changes to the policy.

The TOE shall ensure that the PII principal is informed about defined issues related to the processing of the PII.

Applicable security functional components

ISO/IEC 15408-2 does not define security functional components specific to the case where the TOE actively contacts a user to pass information to the user. Also, no security functional components are defined where the TOE creates information for a specific user that only that user has access to. Therefore, extended components are required to specify the requirements.

ISO/IEC 15408-2 defines security functional components in the FDP class that can be used to express authentication requirements. See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

New extended components, FPFW_IPO.1, FPFW_IPO.2 and FPFW_IPO.3 that can be used to express this principle are defined in 8.2.4.

Dependencies

A dependency on the successful authentication of the PII principal exists because the PII principal shall be able to obtain information about issues related to the principal's own PII.

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.6 "Individual participation and access" principle

7.4.6.1 Accessing and reviewing the PII principal's own PII

Many regulations ask that the TOE give PII principals the ability to access and review their PII upon authentication.

Where required, the TOE shall identify and authenticate PII principals and then apply an access control policy to ensure that PII principals can access only their own PII and not that of other PII principals. PP/ST authors can also specify additional requirements such as authentication failure handling and auditing such failure to prevent unauthorized access to PII.

Expression of the requirements

The requirements can be expressed as follows:

The TOE shall ensure that PII principals are able to access and review their PII but only after successful authentication.

PII principals shall not be able to either access or review the PII of other PII principals.

Applicable security functional components

ISO/IEC 15408-2 defines functional components for expressing user authentication and access control in the FDP class. See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors should follow.

7.4.7 "Accuracy and quality" principle

7.4.7.1 Changing PII properly

The TOE shall provide PII principals with the ability to verify the accuracy of their PII. The TOE shall also permit PII principals to request changes to their PII, but only after proper authorization and only to the extent permitted by relevant legislation and regulation.

Applicable security functional components

ISO/IEC 15408-2 defines functional components for expressing user authentication and access control requirements in the FDP class. An appropriate access control policy can distinguish between users authorized to view the PII and users authorized to modify the PII. See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

If the policy requires that users are held accountable for the modifications they make then ISO/IEC 15408-2 defines functional components for auditing a user's activity in the FAU class.

New extended functional components, FPFW_RAC.1, FPFW_RAC.2 and FPFW_RAC.3, are required for access to and review of PII, see 8.2.5.

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each of its functional components, which the PP/ST authors shall follow.

7.4.7.2 Updating PII periodically

The TOE shall provide a control mechanism to periodically check the accuracy and quality of collected and stored PII.

The TOE shall provide a mechanism to inform PII principals about PII that shall be checked for accuracy and quality.

Expression of the requirements

The requirements can be expressed as follows:

The TOE shall maintain a security attribute for PII that indicates when the next periodic review and update is required.

The TOE shall ensure that PII principals can obtain information about PII they are allowed to review and modify that require periodic checking and update.

Applicable security functional components

ISO/IEC 15408-2 does not define a functional component for periodic review and update.

New extended functional components, FPFW_PUD.1 and FPFW_PUD.2, are required for access to and review of PII, see 8.2.6.

Dependencies

Dependencies to the SFRs for user authentication and access control in ISO/IEC 15408-2 exist because periodic review and update shall be restricted to users authorized to view and modify the PII.

When using the extended SFRs given in Annex C, the dependencies identified in Annex C shall be followed by PP/ST authors.

7.4.8 "Accountability" and "Privacy compliance" principles

Technical and testable requirements cannot be derived from these principles. No extended components are defined for these principles.

7.4.9 "Information Security" principle

7.4.9.1 Protecting PII

The TOE shall protect PII through appropriate controls, including but not limited to technical controls. Organizations should conduct risk assessments to identify required controls.

EXAMPLE Threat risk assessments (TRA) and privacy impact assessments (PIA) are examples of such risk assessments.

Applicable security functional components

ISO/IEC 15408-2 defines several relevant security functional components. PP/ST authors shall identify threats and select an appropriate set of security functional components. See Annex A for guidance on using existing components from ISO/IEC 15408-2 for privacy requirements.

Dependencies

ISO/IEC 15408-2 defines the dependencies for each functional component, which the PP/ST authors shall follow. The PP/ST authors shall also include additional functional components where necessary.

8 Summary of extended components and related privacy principles

8.1 General

The following subclauses define the extended components identified in Clause 7, following guidance described in ISO/IEC 15408-1. PP/ST authors can copy relevant extended components into their PP/ST. However, PP/ST authors should keep in mind that these components have not been formally evaluated by evaluation authorities.

The extended components listed here are mapped to the general requirements identified in Clause 7. ISO/IEC 15408-1 requires extended components to be defined using the structure defined in ISO/IEC 15408-2. The extended components are not fully defined here using this structure. The full definition of the extended components can be found in Annex C.

8.2 Extended components - general definition

8.2.1 General

This subclause lists the requirements identified in Clause 7 as those that require the definition of an extended SFR. For each of those requirements, the components for such an extended SFR are listed. Annex C puts those into the framework defined by ISO/IEC 15408-2 and also defines additional extended SFRs that can be useful for specifying privacy functional requirements.

The nomenclature for the extended components follows that described in ISO/IEC 15408-1. In this case, the class name, FFPW, represents that the families, components and elements are privacy requirements from the ISO/IEC 29100 Privacy Framework and the abbreviated family name representing the subject addressed.

8.2.2 "Consent and choice" principle

8.2.2.1 Presenting choice and obtaining consent

The TSF shall provide choice and obtain consent for the processing of PII through methods, timing and conditions specified by PP/ST authors.

The TSF shall preserve users' choice given the conditions specified by PP/ST authors.

FPFW_COI.1.1 The TSF shall present a choice of [assignment: *List of PII types or items*] to [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]].

FPFW_COI.1.2 The TSF shall record and maintain the choice selected.

FPFW_CON.1.1 The TSF shall obtain consent from [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] to allow collection and processing of [assignment: *list of PII types*].

FPFW_CON.1.2 Before obtaining consent, the TSF shall inform the [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] about the purpose(s) of collecting the PII, their rights and the access principles enforced by the TSF and also inform about the implications of granting or withholding consent.

FPFW_CON.1.3 The TSF shall record the consent of the [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] in [selection: *the audit trail, [assignment: other repository*]] with the time and date, the identifier of the PII principal, [assignment: *additional information*].

FPFW_CON.1.4 The TSF shall [selection: not collect additional PII, allow [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] to specify the following optional PII: [assignment: *list of optional PII items*] that the TSF is allowed to collect].

FPFW_CON.1.5 The TSF shall protect any PII obtained in accordance with the consent statement using the [assignment: *access control policy*].

8.2.2.2 Reaffirming the choice selected

The TSF shall be able to notify the PII principal, or a duly authorized individual acting on their behalf, about choices previously made and consents previously granted before processing the specific PII. The PP/ST author may also specify the type of PII for which the SFR applies and the method used to notify the PII principal.

EXAMPLE An example of when to notify about the choice(s) is by request of the PII principals, after a specific time period, when the policy has changed.

FPFW_NOC.1.1 The TSF shall provide a method to notify [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] about the choice(s) previously made for [selection: *all PII covered by the choice*, [assignment: *list of PII items*]] under the following conditions: [selection: *when explicitly requested, after a defined time period, upon changes to the policy*, [assignment: *other conditions*]].

8.2.2.3 Exempting PII from processing upon modification or withdrawal of consent

The TSF shall stop collecting the PII upon modification or withdrawal of consent through methods specified by the PP/ST authors and delete PII previously collected with exceptions specified by PP/ST authors. If the previously collected PII cannot be deleted completely, the TSF shall notify the user about the limitations in deleting PII.

FPFW_MOC.1.1 The TSF shall provide an interface that allows the [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] to modify or revoke the choice to collect PII.

FPFW_MOC.1.2 After changes are made to the choice or consent, the TSF shall record and maintain the modification or revocation of consent.

FPFW_MOC.1.3 The TSF shall not collect PII from the PII principal in violation of the modification or the revocation of consent.

8.2.3 "Data minimization" and "Use, retention and disclosure limitation" principles

8.2.3.1 Minimizing PII

8.2.3.1.1 Minimization by filtering and removal

The TSF shall be capable of determining when imported data contains more PII than required and shall be capable of identifying that data as PII that it should not process. The TSF shall remove those parts of the PII so identified.

The TSF shall collect PII specified by the PP/ST authors and not require the user to provide other PII.

FPFW_RMV.1.1 The TSF shall analyze imported data for PII and use the following rules [assignment: *rules used to analyze imported data for PII that should not be collected*].

FPFW_RMV.1.2 The TSF shall remove PII identified in imported data and not covered by the consent of the PII principal when it detects such PII during data import.

FPFW_RMV.1.3 Prior to such removal the TSF shall not process such imported data.

8.2.3.1.2 Minimization sensitivity by conversion

The TSF shall convert those parts of PII specified by the PP/ST authors to a less sensitive form after receipt and initial processing of the PII.

The TSF shall convert part of PII specified by the PP/ST authors through methods specified by PP/ST authors after processing the PII.

FPFW_CNV.1.1 The TSF shall convert [assignment: *list of PII*] when obtained using [assignment: conversion methods] to achieve [selection: *anonymity, pseudonymity, unlinkability, unobservability* [assignment: *other goal to be achieved by the conversion*]].

8.2.3.1.3 Minimize retention

The TOE shall eliminate or archive PII under conditions specified by the PP/ST authors.

FPFW_DEL.1.1 The TSF shall delete [assignment: *list of PII*] when the following conditions are satisfied: [selection: *after* [assignment: *period of time*], [assignment: *other conditions that cause the TSF to delete the PII*]].

8.2.4 "Openness, transparency and notice" principle

The TOE shall ensure that the PII principal is able to access information about the PII handling policy in general.

NOTE 1 The information about the PII handling policies and procedures is often public. Therefore, there is no need for users that want to obtain this information to be identified or authenticated.

FPFW_IPO.1.1 The TSF shall provide users with the ability to access information about the PII handling policy and procedures.

The TOE shall ensure that the PII principal is informed about changes to the policy.

NOTE 2 Changes in the policy are often public. Therefore, a system can allow users to register to obtain such information without the need that those users are authenticated.

FPFW_IPO.2.1 The TSF shall use [selection: *E-mail, assignment: other methods*]] to notify registered users about changes in its PII handling policies and procedures.

The TOE shall ensure that the PII principal is informed about defined issues related to the processing of the PII.

FPFW_IPO.3.1 The TSF shall use [selection: *E-mail, assignment: other methods*]] to notify [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] to connect to the TOE to obtain information about [assignment: *list of specific issues related to the PII of that user*].

FPFW_IPO.3.2 The TSF shall provide those users with the ability to access the information after they have been successfully authenticated.

8.2.5 "Individual participation and access" principle: Challenging the accuracy and completeness of PII

The TOE shall ensure that PII principals after they have been successfully authenticated are able to review their PII and challenge their correctness.

NOTE The requirements class FPFW_RAC is subject to requirements, conditions and limitations specified in relevant legislation and regulation.

FPFW_RAC.1.1 The TSF shall provide an interface that allows the [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] to challenge the accuracy and completeness of the PII reviewed.

FPFW_RAC.1.2 The TSF shall allow the [selection: *the PII principal, a user representing the PII principal*, [assignment: *other entity*]] to [selection: *amend, correct, remove*] their PII.

FPFW_RAC.1.3 The TSF shall perform the following actions to ensure the correctness and consistency of the revised PII: [selection: *none*, [assignment: *list of actions performed to ensure correctness and consistency*]].

FPFW_RAC.1.4 The TSF shall inform any parties it has distributed the PII to about any changes to the PII.

FPFW_RAC.2.1 The TSF shall process the PII obtained using [assignment: *rules for processing the PII*] and afterwards convert the PII using the following rules: [assignment: *rules for converting the PII*].

The TOE shall ensure that PII specified by PP/ST authors shall be eliminated or archived from the TOE at the timing specified by PP/ST authors.

FPFW_RAC.3.1 The TSF shall review the PII stored [selection: *periodically every [assignment: time interval*], when [assignment: *event*] happens, [assignment: *other action or event that triggers the PII review*]] for PII that is to be eliminated or archived.

FPFW_RAC.3.2 PII detected to be eliminated shall be [assignment: *process for elimination or archiving*].

FPFW_RAC.3.3 PII detected to be archived shall be [assignment: *process for archiving*]. After successful archiving the original PII shall be [selection: *kept, deleted*, [assignment: *other way of processing the original PII*].

8.2.6 "Accuracy and quality" principle: Updating PII periodically

The TOE shall maintain a security attribute for PII that indicates when the next periodic review and update is required.

The TOE shall provide an interface that allows the definition of intervals for periodic review and update of PII.

FPFW_PUD.1.1 The TSF shall maintain a security attribute for PII that defines the time interval for periodic review and update.

FPFW_PUD.1.2 The TSF shall allow the [selection: the PII principal, a user representing the PII principal, [assignment: *other entity*]] to set the value for the time interval [selection: *applicable for all PII, for the PII they own,* [assignment: *other criteria that define the PII for which the time interval applies*]].

The TOE shall ensure that PII principals can obtain information about PII they are allowed to review and modify that require periodical checking and update.

FPFW_PUD.2.1 The TSF shall provide an interface that [selection: t*he PII principal, a user representing the PII principal,* [assignment: *other entity*]] can use to obtain information about PII that must be reviewed because their periodic update interval has expired.

Annex A
(informative)

Existing components used for privacy requirements

A.1 Overview

A.1.1 General

Security functional components given in ISO/IEC 15408-2 can be used to address privacy threats. The following subclauses provide a discussion about how existing SFRs from ISO/IEC 15408-2 can be used.

A.1.2 Class FAU: Security Audit

A.1.2.1 General

In a TOE that implements privacy requirements, an audit log can serve three different purposes:

a) auditing of attempts to breach the privacy requirements or of successful breaches detected by the TOE after the fact;

b) auditing of access to PII either by the PII principal or in cases where the PII principal has agreed to some type of access under specific conditions. In those cases, the user that performs the access shall be held accountable for this; and

EXAMPLE An example of specific conditions is by the PII controller.

c) auditing for support of the principles defined in ISO/IEC 29100.

NOTE List item c) can be used to audit the consent and choice made by the PII principal or any occasion where PII was transferred (as allowed by applicable legislation, regulation or organizational policy) to a third party.

In all those cases, the requirement is that PII themselves do not show up in the audit record (see Figure A.1).

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [**not specified**] level of audit; and c) **[Attempts to breach the privacy requirements,** d) **Access to PII as defined by the PII access control policy,** e) **Consent decisions made by a PII principal,** f) **Choice decisions made by a PII principal].**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**no PII shall be included in any audit record**].
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Figure A.1 — Use of the FAU_GEN family

A.1.2.2 Rationale for the operations made:

Selecting the "not specified" level of audit allows the PP/ST authors to effectively ignore the audit considerations defined for SFRs in ISO/IEC 15408-2. The assignments made for FAU_GEN.1.1 define the events that support the PII policy. This does not prevent other events not claimed from being included in the audit trail.

The assignment "no PII shall be included in any audit record" defines the requirement that PII should not show up in the audit trail, regardless if the audit record is related to an event defined in FAU_GEN.1.1 or if the audit record is related to an event not defined in FAU_GEN.1.1.

In some cases where users are allowed to access PII in anonymized form, rules can exist that monitor a user's activity to ensure that the user is not attempting to circumvent the anonymization allowing them to relate anonymized PII to a PII principal. To prevent this, a TOE shall have a set of rules implemented that indicate such attempts and report such activities, allowing administrators to take the appropriate action. Such a requirement can be expressed using the SFR FAU_SAA.2 (see Figure A.2).

EXAMPLE 1 An example of circumvention is the statistical evaluation of a database that contains PII.

FAU_SAA.2.1	The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [**the group of users that can have access to functions providing statistical data extracted from a database that contains PII**].
FAU_SAA.2.2	The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.
FAU_SAA.2.3	The TSF shall be able to indicate a possible violation of the enforcement of the SFRs when a user's suspicion rating exceeds the following threshold conditions [**sufficient access attempt have been made to potentially relate PII to the PII principal**].

Figure A.2 — Using the FAU_SAA family to model anonymization circumvention

This could be supporting the 'Information security' principle defined in ISO/IEC 29100.

Other SFRs in the FAU class deal with protecting the audit trail, restricting access to audit records and selecting the actual events that shall be audited. While those SFRs are important for the protection and management of the audit functionality (and can therefore be claimed in a TOE that shall manage and protect PII), they do not directly contribute to the principles defined in ISO/IEC 29100 and are therefore not considered further in this document.

A.1.2.3 Class FCO: Communication

This class contains two families: “Non-repudiation of origin” and “Non-repudiation of receipt”. SFRs from those classes can be used in cases where the TOE wants to enforce a policy where PII principals cannot deny information they passed to the TOE and where the TOE generates a receipt for PII it has received. Both families can be useful when non-repudiation is required as supporting evidence for the consent and choice principle.

EXAMPLE SFRs in this class can be used to express a requirement to send the information to the PII principal for the consent and choice principle digitally signed and get a digitally signed response, allowing both parties to proof what has been agreed upon.

A.1.3 Class FCS: Cryptographic support

Cryptographic functions in general can be useful for protecting the confidentiality and integrity of data both in transit and when stored. Otherwise, no specific support for the principles defined in ISO/IEC 29100 is provided by the families in this class.

A.1.4 Class FDP: User data protection

Several families in this class can be used to model requirements for the enforcement of restrictions on the flow of PII within the TOE and from the TOE to third parties. Those include the general discretionary access control related families, the families related to information flow control and the families defining security requirements for importing and exporting user data. The following example shows how a combination of existing SFRs from the class FDP can be used to model specific access control related aspects of a policy for handling PII:

EXAMPLE

Assume the policy agreed upon between the PII principal and the PII controller is as follows:

It has been agreed that a PII principal will submit the PII principal’s PII to the TOE in digitally signed form and assign a class (A, B, C) to each PII. The policy for the classes of PII are:

— PII of class A is not allowed to be presented to a third party – regardless whether this third party is a user of the TOE or another system;

— PII of class B is allowed to accessed by a person with the role “supervisor” in the TOE; and

— PII of class C is allowed to be passed to a statistical database after the PII has been processed by an “anonymizer program”, but not allowed to be accessed otherwise.

The first two bullet points can be modelled using the classical discretionary access control SFRs:

FDP_ACC.1.1	The TSF shall enforce the [**PII Discretionary access control policy**] on [**users of the TOE as subjects, PII of classes A, B and C as objects and read, write, delete, modify as operations**].
FDP_ACF.1.1	The TSF shall enforce the [**PII Discretionary access control policy**] to objects based on the following: [**class of the PII**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**PII of class B can be read only by a user with the supervisor role**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**PII of class C can be passed to the anonymizer function, PII of all classes can be created or modified when they have been digitally signed by the PII principal**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**PII of class A and C cannot be read, written, modified, or deleted by any user**].
NOTE 1 Export of class C PII is only allowed to the statistical database after being processed by the anonymizer function (Separate SFRs on the anonymizer functionality are not given here).	
FDP_ETC.2.1	The TSF shall enforce the [**PII Discretionary access control policy**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [**PII can only be exported after it has been processed by the anonymizer subject**].
NOTE 2 The PII controller ensures that all PII imported has been digitally signed by the PII principal and that the PII items have classes assigned to them.	
FDP_ITC.2.1	The TSF shall enforce the [**PII Discretionary access control policy**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes assigned to classes of PII associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**before processing the data the TSF shall verify that the data was correctly digitally signed by the PII principal**].
NOTE 3 These SFRs imply that additional SFRs are defined stating the details of the digital signatures schemes and algorithms accepted.	

Figure A.3 — Using the FDP class to model requirements for the enforcement of restrictions on the flow of PII

A.1.5 Class FIA: Identification and authentication

The identification and authentication of users is required for all cases where the TOE shall make a decision that is either based on the identity of the user or where the identity of the user shall be associated with data like an audit record. On the other hand, a TOE that deals with PII can also require that the identity of the user be anonymized or replaced by a pseudonym to prevent that PII can associated with a specific person.

This can be modelled using existing SFRs from ISO/IEC 15408-2 as shown in the following example:

EXAMPLE

Assume the privacy policy allows general read access to the description of the PII policies and procedures at any time, requires successful identification to notify the user about non-confidential information that can be of interest for that user and requires successful identification and authentication of a PII principal, but then requires that the identify be replaced by a pseudonym before the PII is processed. This can be modelled as described in Figure A.4 below:

FIA_UID.1.1	The TSF shall allow [**access to general information about the PII policies and procedures**] on behalf of the user, without requiring the user to be identified beforehand.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF- mediated actions on behalf of that user.
FIA_UAU.1.1	The TSF shall allow [**access to the general information about the PII policies and procedures, notification on non-confidential issues related to the user**] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**a pseudonym representing the user**].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**the pseudonym shall be selected by the pseudonymization component in accordance with the rules specified for this component**].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**no change is allowed**].

Figure A.4 — Using the FIA class to model identification and authentication requirements related to privacy

NOTE SFRs FIA_UID.1 and FIA_UAU.1 need the user "to be successfully identified/authenticated", not that the TOE itself has performed the identification and/or authentication. This can be used in cases where the TOE obtains information from another trusted entity (via a secure channel) that the user has been successfully identified and authenticated. In those cases, the TOE obtains sufficient information about the user to be able to enforce its own policy. This would be the case where the TOE only obtains a pseudonym of the user that can be used in policy enforcement.

A.1.6 Class FMT: Security Management

The families in this class are used to define the policy the TOE uses for the enforcement of its own management policies. This shall include the management of the rules of the PII processing policies when those rules can be changed dynamically. The component FMT_MTD.1 can be used to define who is allowed to change such rules as shown in Figure A.5, below:

EXAMPLE

FMT_MTD.1.1	The TSF shall restrict the ability to [**change the rules of the PII handling policy**] the [**the PII processing policy**] to [**users in the role of a PII controller**].

Figure A.5 — Using the FMT class to define the policy the TOE uses for the enforcement of its own management policies

A.1.7 Class FPR: Privacy

SFRs in this class have been defined to address specific aspects of privacy. The components in this class have been defined to express what a TOE shall achieve, not how the TOE shall do this. For a PP, this can be acceptable but, for a ST, more information is required. Otherwise, this results in problems when attempting to map interfaces and test cases to such components. When using those components, the ST author shall include information that describes the functions used to implement those generic requirements, potentially using SFRs from other classes.

A.1.8 Class FPT: Protection of the TSF

SFRs in this class describe how the TSF protects itself and its own data. While those aspects are of high importance for a TOE that handles PII, no component in this class has specific aspects related to a privacy policy.

A.1.9 Class FRU: Resource utilization

The families in this class are not related to privacy principles. Nevertheless, a TOE that implements privacy requirements can also include requirements from this class to ensure availability and fault tolerance aspects.

A.1.10 Class FTA: TOE access

The families in this class are not related to privacy principles. Nevertheless, a TOE that implements privacy requirements can also include requirements from this class to control sessions between a user and the TOE and to inform a user about the user's access history.

A.1.11 Class FTP: Trusted path/channels

Securing the communication between the TOE and a user or between the TOE and another trusted system are important aspects also for a TOE that implements privacy policies. A PII principal that discloses the PII principal's PII to the TOE shall be assured that the information is effectively released to the TOE and not to an entity that attempts to impersonate the TOE. The component FTP_TRP.1 can be used to model this requirement.

On the other hand, the TOE can communicate with another trusted system to exchange information including PII with the other system. In this case, the integrity and confidentiality of the data exchanged is essential and the component FTP_ITC.1 can be used to define the requirements for a communication channel between the TOE and the other system that provides the required level of protection.

A.2 Protection Profile for "Machine-Readable Travel Document with “ICAO Application", Basic Access Control"[2]

A.2.1 TOE

The TOE is the contactless integrated circuit chip of machine-readable travel documents (MRTD's chip). The TOE is used by the holder for international travel and presented to terminals at inspection system to prove the holder’s identity.

A.2.2 Privacy threat

The terminal and the MRTD's chip use an identifier for the communication channel to allow the terminal to communicate with more than one MRTD's chip. If the identifier is fixed, this identifier can be used to trace movement of the holder by identifying remotely holder’s MRTD's chip through the contactless communication interface.

A.2.3 Functional components

To counter the threat, the MRTD's chip shall randomize the identifier. FIA_UID.1 and FIA_UAU.1 are used to express this requirement. SFRs below are extracted from the PP.

FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow: 1) to read the Initialization Data in Phase 2 "Manufacturing"; 2) to read the random identifier[1)] in Phase 3 "Personalization of the MRTD"; 3) to read the random identifier[1)] in Phase 4 “Operational Use" on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.1	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow: 1) to read the Initialization Data in Phase 2 "Manufacturing"; 2) to read the random identifier[1)] in Phase 3 "Personalization of the MRTD"; 3) to read the random identifier[1)] in Phase 4 "Operational Use" on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

1) In this PP, “random identifier” is defined as "Random identifier used to establish a communication to the TOE in Phase 3 and 4 preventing the unique identification of the MRTD and thus participates in the prevention of traceability".

Annex B
(informative)

Extended components for privacy in existing Protection Profiles

B.1 General

A number of Security Targets and Protection Profiles that incorporate extended components for privacy already exist. PP/ST authors should review existing PPs to determine if they include a component that will address their particular requirement. If so, then these should be used before new components are created.

B.2 Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)[3]

B.2.1 TOE

The TOE is the Smart Meter Gateway. The TOE serves as the communication unit between devices of private and commercial consumers and service providers of commodity industry. It also collects, processes, and stores the Meter Data and is responsible for the distribution of this data to external entities.

EXAMPLE Examples of commodity industries include electricity, gas and water.

B.2.2 Privacy threat

Meter Data is readings that allow calculation of the quantity of a commodity consumed over a period. Such Meter Data can reveal how many people live in a home, their daily routines, changes in those routines, what types of electronic equipment are in the home, and other details if enough Meter Data are accumulated. Therefore, Meter Data shall be encrypted by the TOE before transmission to the wide area network (WAN). However, research[4] suggests that private information can be extracted from encrypted communication by searching for patterns in that data stream.

B.2.3 Extended components

This PP defines a new extended component in FPR class because ISO/IEC 15408-2 does not currently define any components to address this threat.

Communication concealing (FPR_CON.1)

Hierarchical to: No other components.

Dependencies: No dependencies

FPR_CON.1.1 The TSF shall enforce the [assignment: *information flow policy*] in order to ensure that no personally identifiable information (PII) can be obtained by an analysis of [assignment: *characteristics of the information flow that shall be concealed*].

FPR_CON.1.2 The TSF shall connect to [assignment: *list of external entities*] in intervals as follows [selection: *weekly, daily, hourly,* [assignment: *other interval*]] to conceal the data flow.

B.3 User-Oriented Protection Profile for Unobservable Message Delivery using MIX networks [4]

B.3.1 TOE

The TOE is a software system for unobservable and anonymous message delivery on an open network such as the Internet and is implemented using a structure known as MIX network. MIX network is a network of remailer systems, though which a message transits in an encrypted form, along a path (MIX chain) chosen by user. The aim of this system is to hide the correspondence between origin and destination of a message to possible attackers and it is structured in such a way that not even the MIX nodes visited by the message know its full path.

B.3.2 Privacy threats

There are several threats to the MIX network. An attacker can compromise some MIX nodes to gain information useful to trace or reveal the content of communications. MIX node administrators can configure the nodes in an insecure manner. The MIX network shall also provide for an untraceable message delivery service. This means that, for any message transiting through the system at any time, it shall not be possible to obtain enough information to link its origin and destination users.

B.3.3 Extended components

B.3.3.1 General

This protection profile uses new extended components in the FDP and FPR classes because ISO/IEC 15408-2 does not define any components to address the respective threats. The following subclauses summarize the extended components defined in [6].

B.3.3.2 Information retention control (FDP_IRC)

FDP_IRC.1 Subset information retention control

Hierarchical to: No other components

Dependencies: No dependencies

FDP_IRC.1.1 The TSF shall ensure that [assignment: *list of user data and/or TSF data*] required for [assignment: *list of operations and/or functions*] shall be eliminated immediately from the TOE upon termination of the operations and/or functions for which they are required.

FDP_IRC.2 Full information retention control

Hierarchical to: FDP_IRC.1

Dependencies: No dependencies.

FDP_IRC.2.1 The TSF shall ensure that all data required for [assignment: *list of operations and/or functions*] shall be erased immediately from the TOE upon termination of the operations and/or functions for which they are required.

B.3.3.3 Unlinkability (FPR_UNL)

FPR_UNL.1 Unlinkability of operations

Hierarchical to: No other components

Dependencies: No dependencies.

FPR_UNL.1.1 The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine whether [assignment: *list of operations*] [selection: *were caused by the same user, are related as follows* [assignment: *list of relations*]].

FPR_UNL.2 Unlinkability of users

Hierarchical to: No other components

Dependencies: No dependencies.

FPR_UNL.2.1 The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine whether [assignment: *list of users*] [selection: *are referenced by the same operation, are referenced by the same object, are referenced by the same subject, are related as follows* [assignment: *list of relations*]].

FPR_UNL.3 Unlinkability of subjects

Hierarchical to: No other components

Dependencies: No dependencies.

FPR_UNL.3.1 The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine whether [assignment: *list of subjects*] [selection: *act on behalf of the same user, are referenced by the same object, are referenced by the same operation, are related as follows* [assignment: *list of relations*]].

FPR_UNL.4 Unlinkability of objects

Hierarchical to: No other components

Dependencies: No dependencies.

FPR_UNL.4.1 The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine whether [assignment: *list of objects*] [selection: *are associated to the same user, are associated to the same subject, are associated to the same operation, are related as follows* [assignment: *list of relations*]].

B.3.3.4 Distribution of trust (FPR_TRD)

FPR_TRD.1 Administrative domains

Hierarchical to: No other components

Dependencies: No dependencies.

FPR_TRD.1.1 The TOE shall be divided in separate, independent, intercommunicating parts (administrative domains) governed by distinct access control and authentication configurations.

FPR_TRD.1.2 The distinct administrative domains of the TOE shall explicitly request access to data stored on other parts of the TOE to be granted access to it.

FPR_TRD.2 Allocation of information assets

Hierarchical to: FPR_TRD.1

Dependencies: No dependencies.

FPR_TRD.2.1 The TOE shall be divided in separate, independent, intercommunicating parts (administrative domains) governed by distinct access control and authentication configurations.

FPR_TRD.2.2 The distinct administrative domains of the TOE shall explicitly request access to data stored on other parts of the TOE to be granted access to it.

FPR_TRD.2.3 The TSF shall ensure that [assignment: *list of data and/or objects*] shall be stored [selection: *on different administrative domains of the TOE, in a form unreadable by a single administrative domain of the TOE*] as to maintain the following conditions: [assignment: *list of conditions on data and/or objects*].

FPR_TRD.3 Allocation of processing activities

Hierarchical to: FPR_TRD.1

Dependencies: No dependencies

FPR_TRD.3.1 The TOE shall be divided in separate, independent, intercommunicating parts (administrative domains) governed by distinct access control and authentication configurations.

FPR_TRD.3.2 The distinct administrative domains of the TOE shall explicitly request access to data stored on other parts of the TOE to be granted access to it.

FPR_TRD.3.3 The TSF shall ensure that [assignment: *list of operations*] shall be performed by different administrative domains of the TOE, so that the following conditions are maintained: [assignment: *list of conditions on operations*].

Annex C
(normative)

Example of extended components for privacy

C.1 General

This annex defines extended components using the structure required by ISO/IEC 15408-2.

C.2 Class FPFW: Privacy Requirements from the ISO/IEC 29100 Privacy Framework

C.2.1 General

Security functional requirements in this class allow the specification of requirements derived from ISO/IEC 29100. Those requirements can be used when the framework defined in ISO/IEC 29100 has been used to define requirements for the collection, storage and processing of personally identifiable information (PII) (see Figure C.1).

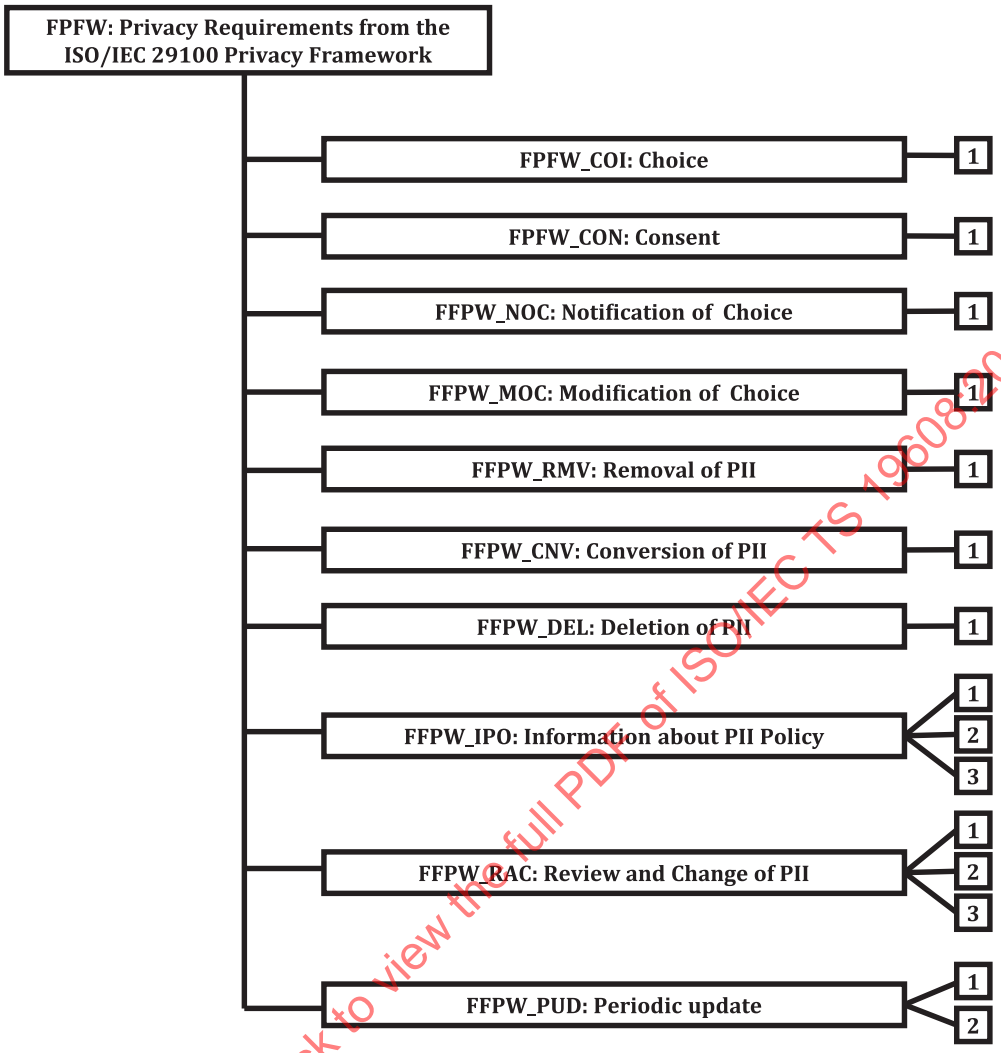

Figure C.1 — FPFW: Privacy Requirements from the ISO/IEC 29100 Privacy Framework class decomposition

C.2.2 Choice

C.2.2.1 Family behaviour

This family defines the security functions derived from the "consent and choice" principle of ISO/IEC 29100 (see Figure C.2).

Figure C.2 — FFPW_COI family component leveling

C.2.2.2 Component levelling

The TSF shall provide choice and obtain consent for the processing of PII through methods, timing and conditions specified by PP/ST authors.

Management: FPFW_COI

The following action should be considered for the management functions in FMT:

— The management of the presentation of the choice.

Audit: FPFW_COI

There are no auditable events foreseen.

C.2.2.3 FPFW_COI.1 Presentation of choice

Hierarchical to: No other components

Dependencies: No dependencies

FPFW_COI.1.1 The TSF shall present a choice of [assignment: *List of PII types or items*] to [selection: *the PII principal, a user representing the PII principal,* [assignment: *other entity*]].

FPFW_COI.1.2 The TSF shall record and maintain the choice selected.

C.2.3 Obtaining consent

C.2.3.1 Family behaviour

This family defines the security functions derived from the "consent and choice" principle of ISO/IEC 29100 (see Figure C.3).

Figure C.3 — FFPW_CON family component leveling

C.2.3.2 Component levelling

The TSF shall provide a mechanism for obtaining consent for processing PII through methods, timing and conditions specified by the PP/ST authors.

Management: FPFW_CON

The following actions should be considered for the management functions in FMT:

— The management of the presentation of the request for consent.

Audit: FPFW_CON

The following actions should be auditable if FPFW_CON.1 is included in the PP/ST:

— User entry for consent.

C.2.3.3 FPFW_CON.1 Obtaining consent

Hierarchical to: No other components

Dependencies: FPFW_COI.1 Presentation of choice

FPFW_CON.1.1 The TSF shall obtain consent from [selection: *the PII principal, a user representing the PII principal,* [assignment: *other entity*]] to allow collection and processing of [assignment: *list of PII types*].

