[l06] solutions

[l06_t02] certification

wim mees

introduction

remember risk management

security controls

management, operational, physical and technical safeguards or countermeasures implemented in order to protect the confidentiality, integrity, and availability of the system and its information

questions

- which security controls are needed to adequately address the identified risks ?
- is there a realistic plan to implement these controls ?
- is there a sufficient level of **assurance** (grounds for confidence) that the selected controls as implemented will be effective ?

types of controls

yet another classification of controls

- **directive controls:** define expected employee behavior when interacting with the information systems
- **preventive controls:** preclude actions violating policy or increasing risk to the information systems
- **detective controls:** practices, processes, and tools that identify and possibly react to security violations
- **corrective controls:** reduce or eliminate the opportunity for an unwanted event to recur after an incident occurred
- **recovery controls:** restore the system or operation to a normal operating state after an incident occurred

why certification and accreditation ?

certification

disciplined approach to evaluate the level of conformance of the security controls to the prescribed security requirements, and possibly the correctness of their implementation

accreditation

official management decision to operate the certified system

note: C & A do no guarantee that there are no risks, therefore periodic security assessments are needed

why the Common Criteria (CC) ?

- provide a comparable standard
  - evaluations should be **repeatable**
  - evaluations should be **consistent**
- make it possible for an individual organisation to
  - enumerate security needs
  - match them with existing products
- make it possible for a group of organisations to
  - enumerate common security needs (e.g. US government for operating systems or intrusion detection systems)
- open foreign markets for vendors
  - up to EAL 3

what is the CC ?

Common Criteria for Information Technology Security Evaluation

- is an international standard (ISO/IEC 15408)
- focuses on flexibility
- not a *requirements document* (~~product shall meet the CC~~)
- provides a catalogue of building blocks to build criteria

the CC evaluation approach

- **Protection Profile**: this is what I want you to build
- **Security Target**: this is what I have built (typically referring to a given protection profile)

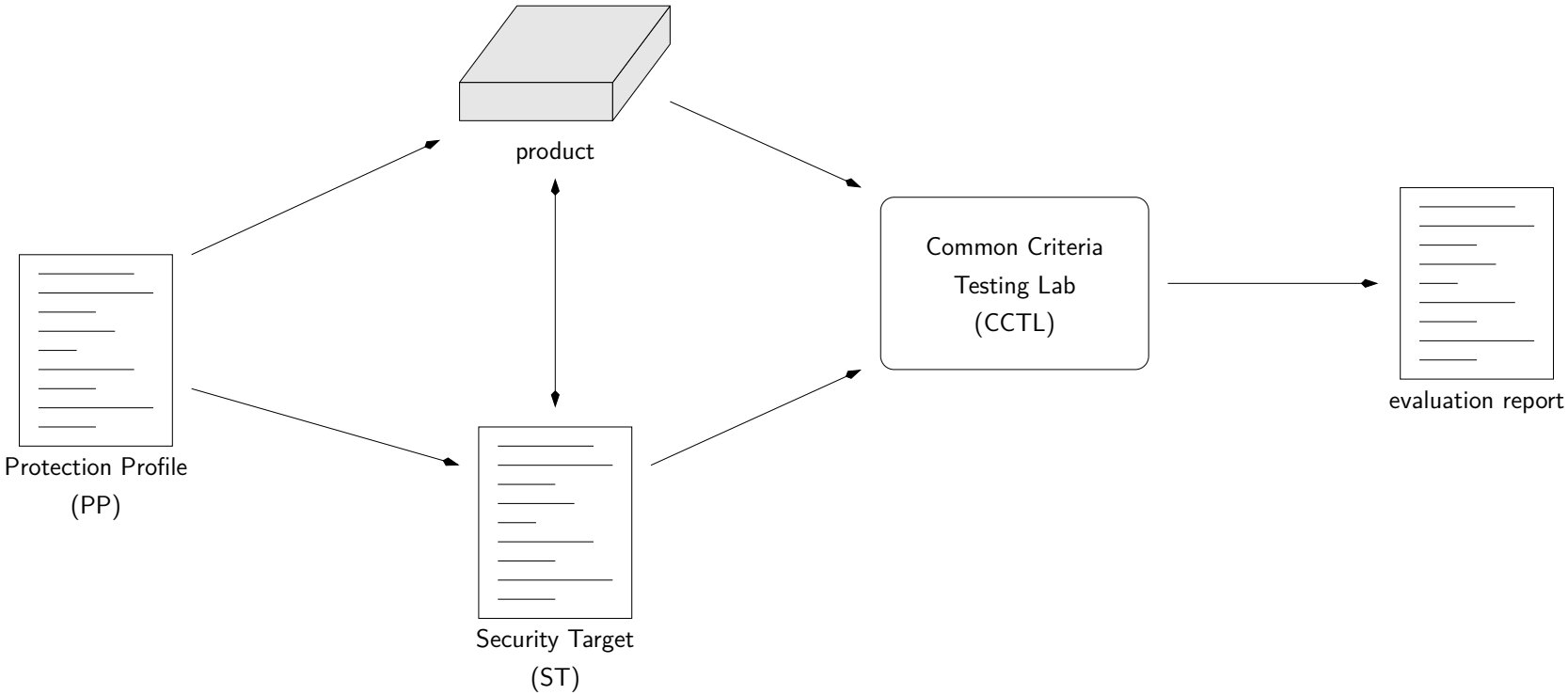

Figure 1: CC approach

the CC documentation

- part 1: model of how to express security requirements
  - generic requirement sets: Protection Profiles (PP)
  - specific requirement sets: Security Targets (ST)
- parts 2 & 3: catalogue of security requirements
  - functional requirements (part 2)
  - assurance requirements (part 3)
- evaluation methodology
  - ensure that different CCTL produce consistent results

the CC model

- requirements are selected to meet specific security objectives
- security objectives are based on:
  - threats
  - organizational policies (e.g. printouts must be labelled at the top and at the bottom with the classification)
  - assumptions
- requirements are expressed in PPs/STs
- products (the *"Target Of Evaluation"* or TOE) are evaluated against STs (those STs may claim compliance with a given PP)

Protection Profile (PP)

what is a PP ?

- generic set of requirements for a class of systems or products (e.g. intrusion detection system, firewall, public key infrastructure, . . .)
- provides specification of the environment of use:
  - threats ("this attacker will try this attack to get this result")
  - policies
  - assumptions about the environment (e.g. "all the users are trained", "to be used in a non-hostile environment")
- note: the environment specification addresses. . .
  - IT and non-IT environment (examples of non-IT: appropriate physical protection is in place, users receive appropriate training, users follow written guidance)
  - TOE and non-TOE IT environment (example for non-TOE: the software gets reliable timestamps from the operating system)

generic requirements

- CC requirements can be open-ended
  - example from the PP: "The TSF shall provide *[assignment: authorized users]* with the capability to read *[assignment: list of audit information]* from the audit records."
  - this could become in the ST: "The TSF shall provide *the auditor* with the capability to read *all records in the audit trail*."
- CC defines specific operations than can be performed on requirements:
  - *assignment:* fill in the blanks
  - *selection:* pick one from a list
  - *refinement:* add implementation detail
  - *iteration:* include a requirement multiple times
- goal is to address a common consumer need

structure of a PP

1. descriptive front-matter (TOE, conformance claims, . . .)
2. intended (generic) security environment
   - threats
   - policies
   - assumptions
3. security objectives (e.g. threat: users may take an action for which they are not accountable and as a result I cannot prosecute them, therefore we add an objective that users must be accountable for their actions, and then select the appropriate functional requirements from part 2 of the CC that satisfy that objective)
4. requirements to meet objectives
5. rationale of how requirements meet objectives

Security Target (ST)

what is an ST ?

- similar structure as a PP
- key differences:
  - all operations must be completed
  - include a TOE summary specification (TSS), an enumeration of what security functions in the TOE meet each security requirement
- difference in intent:
  - ST is specific to a product/system
  - ST specifies the claimed features and assurance of a product/system

structure of an ST

- additional material in an ST:
  - TOE summary specification (TSS)
    - boundaries of the TOE (what is inside and what is outside of the scope of the evaluation)
    - example: developed application and its configuration files are inside the TOE; the database manager and any hardware security modules it uses, as well as applications calling the API of the developed application are outside the TOE
  - PP claims
  - rationale
    - how requirements meet objectives
    - how security features meet requirements

quick how-to

developing a PP or ST

- specify threats, policies and assumptions based on:
  - physical environment
  - assets requiring protection
  - purpose of the TOE
- from these determine your objectives
- develop requirements to satisfy objectives
  - functional
  - assurance (EAL 1-2-3-4-. . . possibly with a "+")
  - environmental
- PP/ST include mappings that show that
  - each threat is countered by one or more objectives
  - policy requirements are satisfied by objectives
  - each objective is achieved by one or more requirements

functional requirements

- express requirements on the TOE
- typically demonstrable through the interface
- organization:
  - classes: general functional groupings
  - families: specific areas of functions
  - components: specific groups of requirements (smallest chunk of requirements that can be included in PP/ST)
  - elements: single requirements

functional requirements

functional classes

- FAU: security audit
- FCO: communication
- FCS: cryptographic support
- FDP: user data protection
- FIA: identification and authentication
- FMT: security management
- FPR: privacy
- FPT: protection of the TSF security function
- FRU: resource utilization
- FTA: TOE access
- FTP: trusted path

functional classes: some examples

FAU: security audit

- FAU_ARP: audit automatic response
- FAU_GEN: audit data generation
- FAU_SAA: audit analysis
- FAU_SAR: audit review
- FAU_SEL: audit event selection
- FAU_STG: audit event storage

functional classes: some examples (cont'd)

FCO: communication

- FCO_NRO: non-repudiation of origin
- FCO_NRR: non-repudiation of receipt

FCS: cryptographic support

- FCS_CKM: cryptographic key management
- FCS_COP: cryptographic operation

functional classes: some examples (cont'd)

FDP: user data protection

- FDP_ACC: access control policy (DAC)
- FDP_ACF: access control functions (DAC)
- FDP_DAU: data authentication
- FDP_ETC: export to outside TSF control
- FDP_IFC: information flow control policy (MAC)
- FDP_IFF: information flow control functions (MAC)
- FDP_ITC: import from outside TSF control
- FDP_ITT: internal TOE transfer
- FDP_RIP: residual information protection (object reuse)

with:

- DAC: discretionary access control
- MAC: mandatory access control

some examples more in-depth

FAU_GEN Security audit data generation

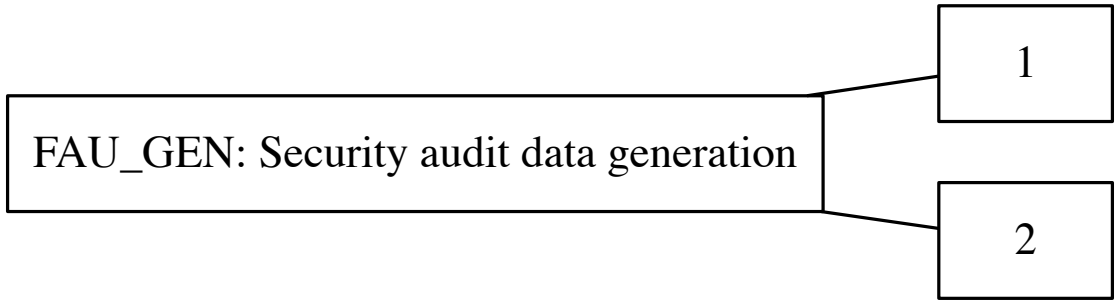

Figure 2: FAU_GEN

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

FAU_GEN.1 Audit data generation

- 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 [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
  c) [assignment: other specifically defined auditable events].
- 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, [assignment: other audit relevant information].

FAU_GEN.2 User identity association

- 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.

FAU_SAR Security audit review

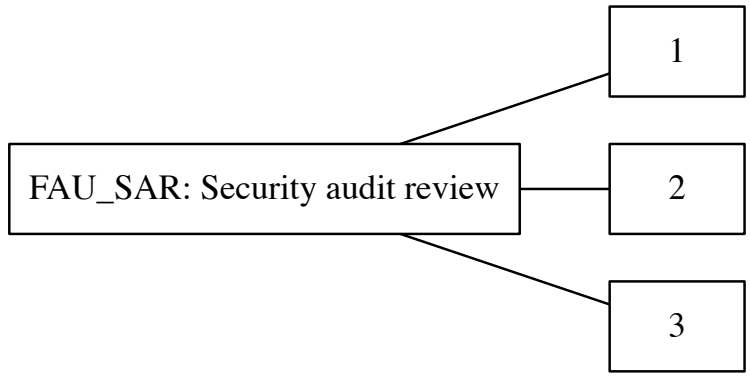

Figure 3: FAU_SAR

This family defines the requirements for audit tools that should be available to authorised users to assist in the review of audit data.

FAU_SAR.1 Audit review

- FAU_SAR.1.1 The TSF shall provide [assignment: authorised users] with the capability to read [assignment: list of audit information] from the audit records.
- FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

- FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

- FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: methods of selection and/or ordering] of audit data based on [assignment: criteria with logical relations].

FAU_SEL Security audit event selection

Figure 4: FAU_SEL

This family defines requirements to select the set of events to be audited during TOE operation from the set of all auditable events.

FAU_SEL.1 Selective audit

- FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:
  a) [selection: object identity, user identity, subject identity, host identity, event type]
  b) [assignment: list of additional attributes that audit selectivity is based upon]

FAU_STG Security audit event storage

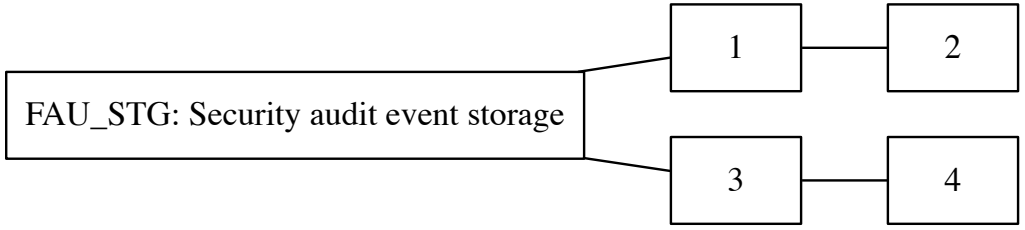

Figure 5: FAU_STG

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit records refers to those records within the audit trail, and not the audit records that have been retrieved (to temporary storage) through selection.

FAU_STG.1 Protected audit trail storage

- FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
- FAU_STG.1.2 The TSF shall be able to [selection, choose one of: prevent, detect] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2 Guarantees of audit data availability

- FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
- FAU_STG.2.2 The TSF shall be able to [selection, choose one of: prevent, detect] unauthorised modifications to the stored audit records in the audit trail.
- FAU_STG.2.3 The TSF shall ensure that [assignment: metric for saving audit records] stored audit records will be maintained when the following conditions occur: [selection: audit storage exhaustion, failure, attack]

FAU_STG.3 Action in case of possible audit data loss

- FAU_STG.3.1 The TSF shall [assignment: actions to be taken in case of possible audit storage failure] if the audit trail exceeds [assignment: pre-defined limit].

FAU_STG.4 Prevention of audit data loss

- FAU_STG.4.1 The TSF shall [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorised user with special rights”, “overwrite the oldest stored audit records”] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

FDP_ACC Access control policy

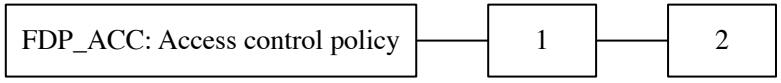

Figure 6: FDP_ACC

This family identifies the access control SFPs (by name) and defines the scope of control of the policies that form the identified access control portion of the SFRs related to the SFP. This scope of control is characterised by three sets: the subjects under control of the policy, the objects under control of the policy, and the operations among controlled subjects and controlled objects that are covered by the policy. The criteria allows multiple policies to exist, each having a unique name. This is accomplished by iterating components from this family once for each named access control policy.

(cont'd on next slide)

FDP_ACC Access control policy (cont'd)

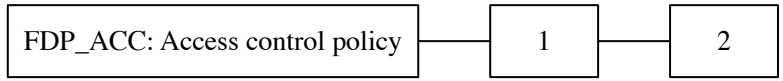

Figure 7: FDP_ACC

The rules that define the functionality of an access control SFP will be defined by other families such as Access control functions (FDP_ACF) and Export from the TOE (FDP_ETC). The names of the access control SFPs identified here in Access control policy (FDP_ACC) are meant to be used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an "access control SFP."

FDP_ACC.1 Subset access control

- FDP_ACC.1.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

FDP_ACC.2 Complete access control

- FDP_ACC.2.1 The TSF shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.
- FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF Access control functions

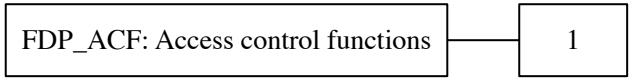

Figure 8: FDP_ACF

This family describes the rules for the specific functions that can implement an access control policy named in Access control policy (FDP_ACC). Access control policy (FDP_ACC) specifies the scope of control of the policy.

This family addresses security attribute usage and characteristics of policies. The component within this family is meant to be used to describe the rules for the function that implements the SFP as identified in Access control policy (FDP_ACC). The PP/ST author may also iterate this component to address multiple policies in the TOE.

FDP_ACF.1 Security attribute based access control

- FDP_ACF.1.1 The TSF shall enforce the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].
- FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

(cont'd on next slide)

FDP_ACF.1 Security attribute based access control (cont'd)

- FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
- FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FDP_IFC Information flow control policy

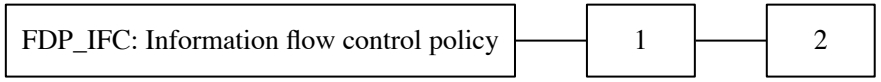

Figure 9: FDP_IFC

This family identifies the information flow control SFPs (by name) and defines the scope of control for each named information flow control SFP. This scope of control is characterised by three sets: the subjects under control of the policy, the information under control of the policy, and operations which cause controlled information to flow to and from controlled subjects covered by the policy. The criteria allows multiple policies to exist, each having a unique name. This is accomplished by iterating components from this family once for each named information flow control policy.

(cont'd on next slide)

FDP_IFC Information flow control policy (cont'd)

The rules that define the functionality of an information flow control SFP will be defined by other families such as Information flow control functions (FDP_IFF) and Export from the TOE (FDP_ETC). The names of the information flow control SFPs identified here in Information flow control policy (FDP_IFC) are meant to be used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an "information flow control SFP."

The TSF mechanism controls the flow of information in accordance with the information flow control SFP. Operations that would change the security attributes of information are not generally permitted as this would be in violation of an information flow control SFP. However, such operations may be permitted as exceptions to the information flow control SFP if explicitly specified.

FDP_IFC.1 Subset information flow control

- FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

FDP_IFC.2 Complete information flow control

- FDP_IFC.2.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment: list of subjects and information] and all operations that cause that information to flow to and from subjects covered by the SFP.
- FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF Information flow control functions

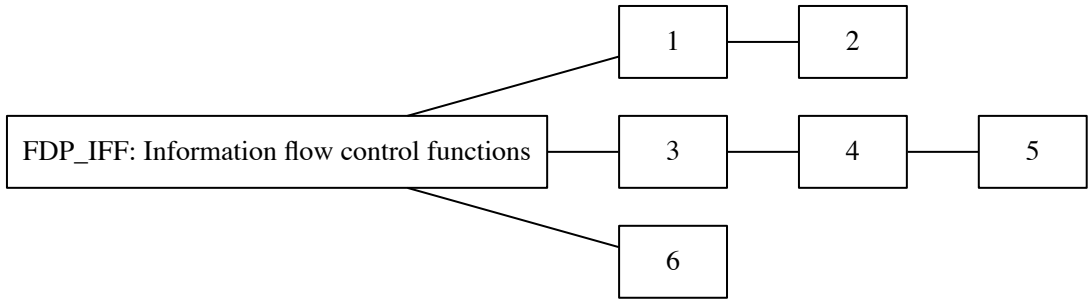

Figure 10: FDP_IFF

This family describes the rules for the specific functions that can implement the information flow control SFPs named in Information flow control policy (FDP_IFC), which also specifies the scope of control of the policy. It consists of two kinds of requirements: one addressing the common information flow function issues, and a second addressing illicit information flows (i.e. covert channels).

(cont'd on next slide)

FDP_IFF Information flow control functions (cont'd)

This division arises because the issues concerning illicit information flows are, in some sense, orthogonal to the rest of an information flow control SFP. By their nature they circumvent the information flow control SFP resulting in a violation of the policy. As such, they require special functions to either limit or prevent their occurrence.

FDP_IFF.1 Simple security attributes

- FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].
- FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].
- FDP_IFF.1.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].
- FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].
- FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_IFF.2 Hierarchical security attributes

- FDP_IFF.2.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes].
- FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].
- FDP_IFF.2.3 The TSF shall enforce the [assignment: additional information flow control SFP rules].
- FDP_IFF.2.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

(cont'd on next slide)

FDP_IFF.2 Hierarchical security attributes (cont'd)

- FDP_IFF.2.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].
- FDP_IFF.2.6 The TSF shall enforce the following relationships for any two valid information flow control security attributes:
  a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and
  b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
  c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

FDP_IFF.3 Limited illicit information flows

- FDP_IFF.3.1 The TSF shall enforce the [assignment: information flow control SFP] to limit the capacity of [assignment: types of illicit information flows] to a [assignment: maximum capacity].

FDP_IFF.4 Partial elimination of illicit information flows

- FDP_IFF.4.1 The TSF shall enforce the [assignment: information flow control SFP] to limit the capacity of [assignment: types of illicit information flows] to a [assignment: maximum capacity].

FDP_IFF.5 No illicit information flows

- FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [assignment: name of information flow control SFP].

FDP_IFF.6 Illicit information flow monitoring

- FDP_IFF.6.1 The TSF shall enforce the [assignment: information flow control SFP] to monitor [assignment: types of illicit information flows] when it exceeds the [assignment: maximum capacity].

FDP_ITC Import from outside of the TOE

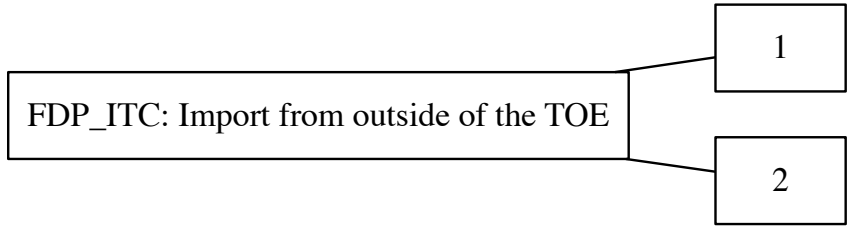

Figure 11: FDP_ITC

This family defines the mechanisms for TSF-mediated importing of user data into the TOE such that it has appropriate security attributes and is appropriately protected. It is concerned with limitations on importation, determination of desired security attributes, and interpretation of security attributes associated with the user data.

FDP_ITC.1 Import of user data without security attributes

- FDP_ITC.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when importing user data, controlled under the SFP, from outside of the TOE.
- FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
- FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: additional importation control rules].

FDP_ITC.2 Import of user data with security attributes

- FDP_ITC.2.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] when importing user data, controlled under the SFP, from outside of the TOE.
- FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.
- FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the 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: [assignment: additional importation control rules].

FDP_RIP Residual information protection

Figure 12: FDP_RIP

This family addresses the need to ensure that any data contained in a resource is not available when the resource is de-allocated from one object and reallocated to a different object. This family requires protection for any data contained in a resource that has been logically deleted or released, but may still be present within the TSF-controlled resource which in turn may be re-allocated to another object.

FDP_RIP.1 Subset residual information protection

- FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] the following objects: [assignment: list of objects].

FDP_RIP.2 Full residual information protection

- FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] all objects.

FIA_AFL Authentication failures

Figure 13: FIA_AFL

This family contains requirements for defining values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. Parameters include, but are not limited to, the number of failed authentication attempts and time thresholds.

FIA_AFL.1 Authentication failure handling

- 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].

FIA_ATD User attribute definition

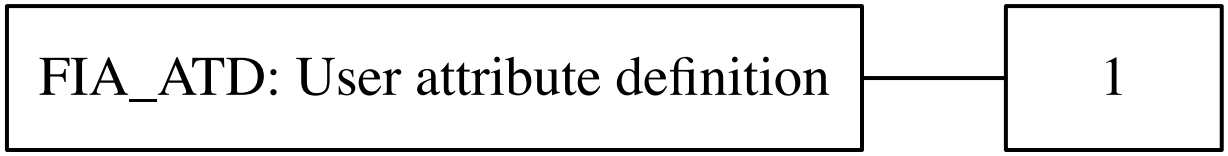

Figure 14: FIA_ATD

All authorised users may have a set of security attributes, other than the user's identity, that is used to enforce the SFRs. This family defines the requirements for associating user security attributes with users as needed to support the TSF in making security decisions.

FIA_ATD.1 User attribute definition

- FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: list of security attributes].

FIA_SOS Specification of secrets

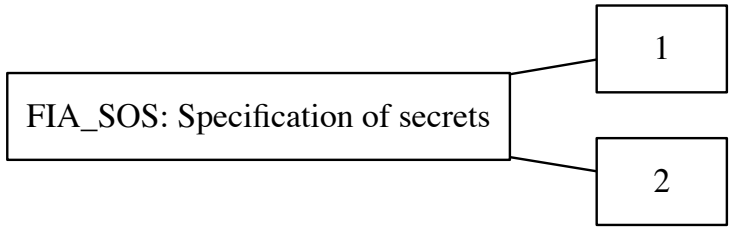

Figure 15: FIA_SOS

This family defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.

FIA_SOS.1

- FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: a defined quality metric].

FIA_SOS.2 TSF Generation of secrets

- FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [assignment: a defined quality metric].
- FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [assignment: list of TSF functions].

FIA_UAU User authentication

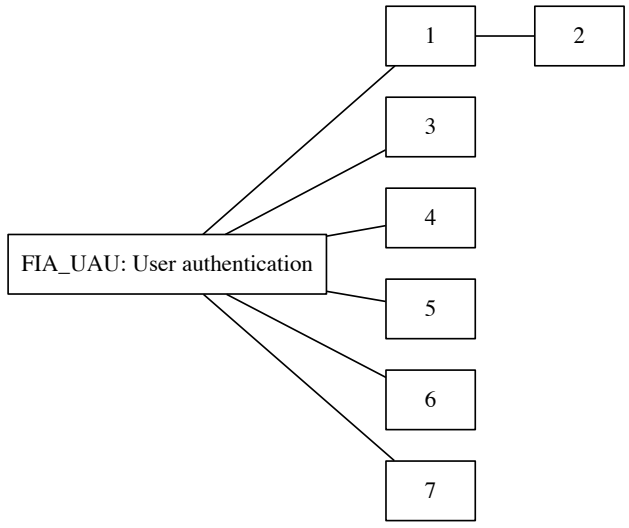

Figure 16: FIA_UAU

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

FIA_UAU.1 Timing of authentication

- FIA_UAU.1.1 The TSF shall allow [assignment: list of TSF mediated actions] 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_UAU.2 User authentication before any action

- 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.

FIA_UAU.3 Unforgeable authentication

- FIA_UAU.3.1 The TSF shall [selection: detect, prevent] use of authentication data that has been forged by any user of the TSF.
- FIA_UAU.3.2 The TSF shall [selection: detect, prevent] use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.4 Single-use authentication mechanisms

- FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: identified authentication mechanism(s)].

FIA_UAU.5 Multiple authentication mechanisms

- FIA_UAU.5.1 The TSF shall provide [assignment: list of multiple authentication mechanisms] to support user authentication.
- FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].

FIA_UAU.6 Re-authenticating

- FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: list of conditions under which re-authentication is required].

FIA_UAU.7 Protected authentication feedback

- FIA_UAU.7.1 The TSF shall provide only [assignment: list of feedback] to the user while the authentication is in progress.

FIA_UID User identification

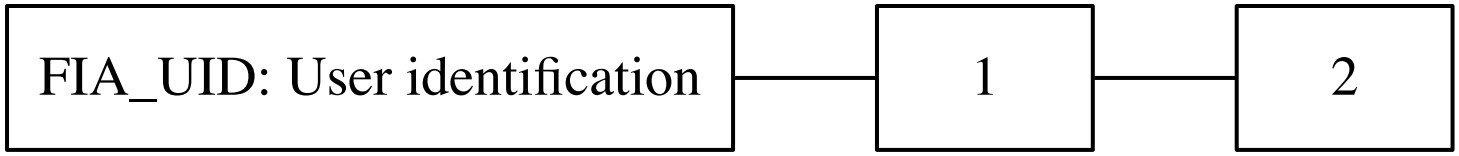

Figure 17: FIA_UID

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

FIA_UID.1 Timing of identification

- FIA_UID.1.1 The TSF shall allow [assignment: list of TSF-mediated actions] 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_UID.2 User identification before any action

- FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB User-subject binding

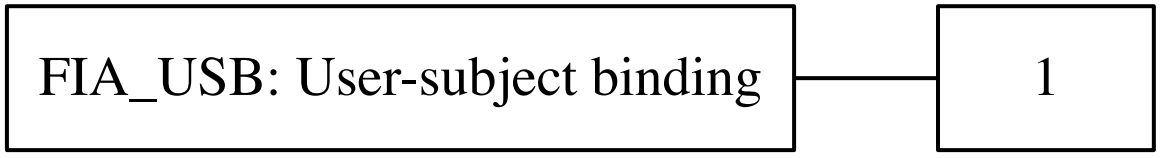

Figure 18: FIA_USB

An authenticated user, in order to use the TOE, typically activates a subject. The user's security attributes are associated (totally or partially) with this subject. This family defines requirements to create and maintain the association of the user's security attributes to a subject acting on the user's behalf.

FIA_USB.1 User-subject binding

FIA_USB.1 User-subject binding

- FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].
- 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: [assignment: rules for the initial association of attributes].
- 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: [assignment: rules for the changing of attributes].

FMT_MSA Management of security attributes

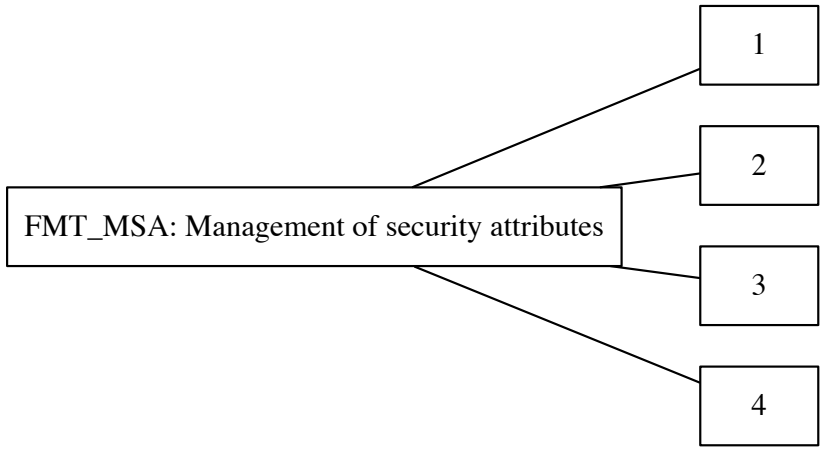

Figure 19: FMT_MSA

This family allows authorised users control over the management of security attributes. This management might include capabilities for viewing and modifying of security attributes.

FMT_MSA.1 Management of security attributes

- FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP(s), information flow control SFP(s)] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

FMT_MSA.2 Secure security attributes

- FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [assignment: list of security attributes].

FMT_MSA.3 Static attribute initialisation

- FMT_MSA.3.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.
- FMT_MSA.3.2 The TSF shall allow the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4 Security attribute value inheritance

- FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes: [assignment: rules for setting the values of security attributes]

FMT_MTD Management of TSF data

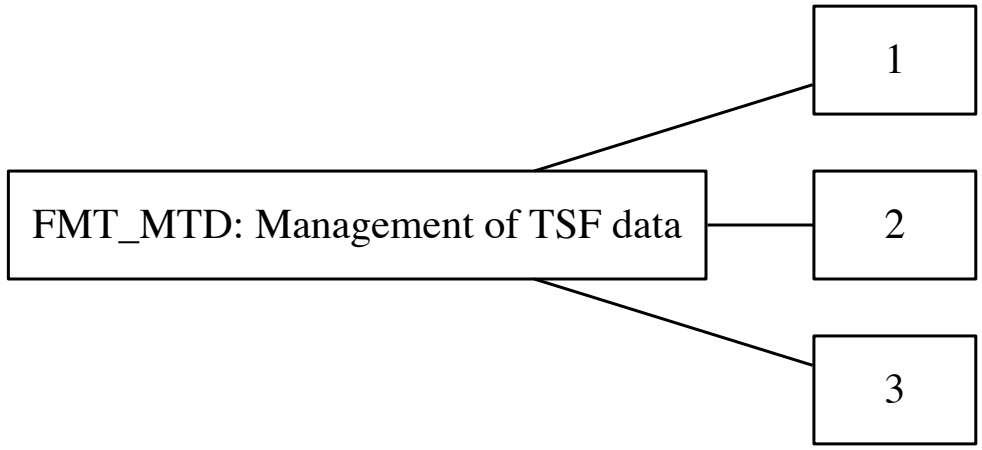

Figure 20: FMT_MTD

This family allows authorised users (roles) control over the management of TSF data. Examples of TSF data include audit information, clock and other TSF configuration parameters.

FMT_MTD.1 Management of TSF data

- FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, [assignment: other operations]] the [assignment: list of TSF data] to [assignment: the authorised identified roles].

FMT_MTD.2 Management of limits on TSF data

- FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [assignment: list of TSF data] to [assignment: the authorised identified roles].
- FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: actions to be taken].

FMT_MTD.3 Secure TSF data

- FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [assignment: list of TSF data].

FMT_REV Revocation

Figure 21: FMT_REV

This family addresses revocation of security attributes for a variety of entities within a TOE.

FMT_REV.1 Revocation

- FMT_REV.1.1 The TSF shall restrict the ability to revoke [assignment: list of security attributes] associated with the [selection: users, subjects, objects, [assignment: other additional resources]] under the control of the TSF to [assignment: the authorised identified roles].
- FMT_REV.1.2 The TSF shall enforce the rules [assignment: specification of revocation rules].

FMT_SMF Specification of Management Functions

Figure 22: FMT_SMF

This family allows the specification of the management functions to be provided by the TOE. Management functions provide TSFI that allow administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes.

(cont'd on next page)

FMT_SMF Specification of Management Functions (cont'd)

Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery. This family works in conjunction with the other components in the FMT: Security management class: the component in this family calls out the management functions, and other families in FMT: Security management restrict the ability to use these management functions.

FMT_SMF.1 Specification of Management Functions

- FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

FMT_SMR Security management roles

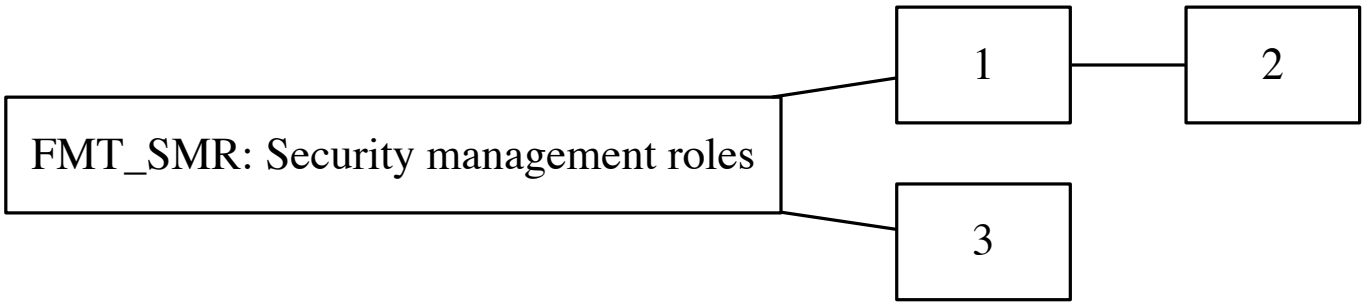

Figure 23: FMT_SMR

This family is intended to control the assignment of different roles to users. The capabilities of these roles with respect to security management are described in the other families in this class.

FMT_SMR.1 Security roles

- FMT_SMR.1.1 The TSF shall maintain the roles [assignment: the authorised identified roles].
- FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FMT_SMR.2 Restrictions on security roles

- FMT_SMR.2.1 The TSF shall maintain the roles: [assignment: authorised identified roles].
- FMT_SMR.2.2 The TSF shall be able to associate users with roles.
- FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: conditions for the different roles] are satisfied.

FMT_SMR.3 Assuming roles

- FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: [assignment: the roles].

FPT_STM Time stamps

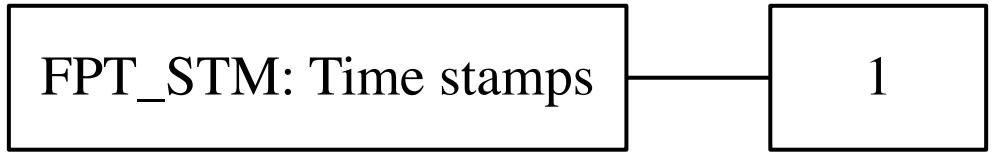

Figure 24: FPT_STM

This family addresses requirements for a reliable time stamp function within a TOE.

FPT_STM.1 Reliable time stamps

- FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TDC Inter-TSF TSF data consistency

Figure 25: FPT_TDC

In a distributed environment, a TOE may need to exchange TSF data (e.g. the SFP-attributes associated with data, audit information, identification information) with another trusted IT product, This family defines the requirements for sharing and consistent interpretation of these attributes between the TSF of the TOE and a different trusted IT product.

FPT_TDC.1 Inter-TSFbasicTSFdataconsistency

- FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: list of TSF data types] when shared between the TSF and another trusted IT product.
- FPT_TDC.1.2 The TSF shall use [assignment: list of interpretation rules to be applied by the TSF] when interpreting the TSF data from another trusted IT product.

FTA_SSL Session locking and termination

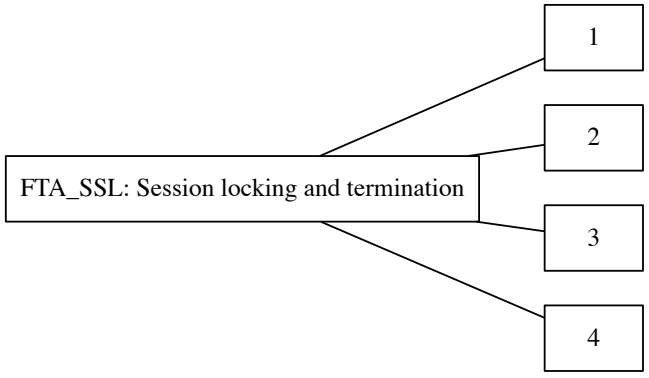

Figure 26: FTA_SSL

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

FTA_SSL.1 TSF-initiated session locking

- FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: time interval of user inactivity] by:
  a) clearing or overwriting display devices, making the current contents unreadable;
  b) disabling any activity of the user's data access/display devices other than unlocking the session.
- FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: events to occur].

FTA_SSL.2 User-initiated locking

- FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session, by:
  a) clearing or overwriting display devices, making the current contents unreadable;
  b) disabling any activity of the user's data access/display devices other than unlocking the session.
- FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: events to occur].

FTA_SSL.3 TSF-initiated termination

- FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: time interval of user inactivity].

FTA_SSL.4 User-initiated termination

- FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

FTP_ITC Inter-TSF trusted channel

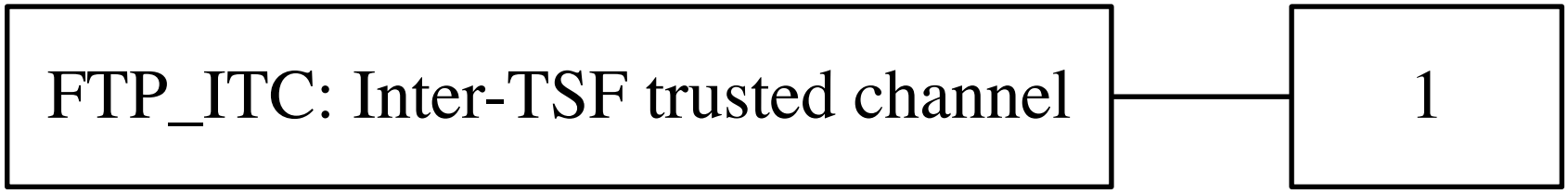

Figure 27: FTP_ITC

This family defines requirements for the creation of a trusted channel between the TSF and other trusted IT products for the performance of security critical operations. This family should be included whenever there are requirements for the secure communication of user or TSF data between the TOE and other trusted IT products.

FTP_ITC.1 Inter-TSF trusted channel

- FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
- FTP_ITC.1.2 The TSF shall permit [selection: the TSF, another trusted IT product] to initiate communication via the trusted channel.
- FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: list of functions for which a trusted channel is required].

evaluation

evaluation

what is tested ?

- documentation
  - Is the documentation of the security functions complete?
- implementation
  - Do the security functions actually do what they claim to do?
- development environment
  - Is the development environment secure?
- development process
  - Is the development performed in a secure way?

Evaluation Assurance Level (EAL)

- TOE is evaluated against one of seven predefined EALs
- EAL informs consumers how confident they can be on the result of the evaluation, based on how much information was available to the evaluation lab and how carefully the system was examined
- EAL levels:
  - EAL 1: functionally tested (product conforms with manual)
  - EAL 2: structurally tested (black box)
  - EAL 3: methodically tested and checked (gray box)
  - EAL 4: methodically designed, tested and reviewed (white box)
  - EAL 5: semi-formally designed and tested
  - EAL 6: semi-formally verified, designed and tested
  - EAL 7: formally verified, designed and tested

conclusions

conclusions

Figure 28: questions or comments ?