



ISO/IEC JTC1/SC 27 **N6855**

ISO/IEC JTC1/SC 27/WG 3 **N953**

REPLACES: N

**ISO/IEC JTC 1/SC 27**

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

**DOC. TYPE:** expert contribution

**TITLE:** **List of questions and answers concerning privacy components**

**SOURCE:** WG 3 Experts (M. Nash, K. Rannenberg)

**DATE:** 2008-07-03

**PROJECT:** 15408

**STATUS:** In accordance with resolution 5 (see SC 27 N6640) of the 36<sup>th</sup> SC 27/WG 3 meeting held in Kyoto (April 2008) this document is being circulated to the National Bodies and liaison organizations for study and comments.

Submissions should reach the SC 27 secretariat by as soon as possible but no later than **2008-09-05**

**DISTRIBUTION:** P-, O- and L-Members  
W. Fumy, SC 27 Chairman  
M. De Soete, SC 27 Vice-chair  
E. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenberg, WG-Conveners

**ACTION ID:** **COM**

**DUE DATE:** **2008-09-05**

**MEDIUM:** Livelink-server

**NO. OF PAGES:** 1 + 5

## LIST OF QUESTIONS AND ANSWERS CONCERNING PRIVACY COMPONENTS

### 1 *Introduction*

This is a list of questions and answers produced as an action arising from the ISO/IEC 15408-2 editing meeting held in Madrid between 26th and 27th February 2008. It arises from the meeting contribution paper WG 3 N923 that looked at implementing the privacy SFRs present in FDIS ISO/IEC 15408-2 (believed unchanged from ISO/IEC 15408:2:1999), and in German NB contribution SC 27 N5965.

The purpose of these questions and answers is to enable the existing privacy criteria to be reworded unambiguously and in evaluable form.

The list is organised by privacy family, starting with the existing families already present in ISO/IEC 15408. The questions identify ambiguities and undefined terms within the current specifications of these components. The answers resolve them, where this is possible.

Some questions are worded as leading questions, where a probable intended meaning can be identified. In some cases, reference is made to the 1999 Master thesis of Giovanni Iachello, which contains additional or different information relating to some components found in SC 27 N5965.

The majority of queries are resolved. There are some cases where a method of specification seems to be assumed within the ISO/IEC 15408 functional paradigm. Only if this method is the only permitted specification method is the implied answer correct.

It is believed that this paper can be used to substantially improve the precision and clarity of the privacy functional components.

### 2. *Family FPR\_ANO*

1. What is a *real user name*? Is it a security attribute required to be associated with subjects through user/subject binding using FIA\_USB? Answer: it might be, but there may be other ways of specifying the requirement for real names in SFRs. You are forcing implementation detail, when what is specified is just a requirement for a name which identifies a real person in a way such that the real person can be made responsible. But you define lots of other SFRs exclusively in terms of attributes, so perhaps it is okay to make it the only way.

2. Is a *real user name* more than one security attribute, i.e. any subject security attributes that can be used to identify the user on whose behalf the subject is currently operating? Answer: It may be a security attribute, but it could be any other item that identifies a user, regardless whether it is a security attribute or not. There is no explicit dependency on FIA\_USB.

3. What does “provide [assignment: *list of services*]” mean? Is it just a list of objects that may be accessed? Would it be better worded as “The TSF shall permit [*list of subjects*] to access [*list of objects*] without referencing [*list of subject security attributes identifying user name*]”? Answer: The term “service” was seen as more comprehensive in 1998, when this was written. It can be changed for better terminology, if this exists, e.g. depending on the meaning of “object” in the current criteria, e.g. if “objects” would cover e.g. a web service being used. But “object” is too narrow, if it just refers to the relation between users and subjects as in FIA\_USB.

### 3 Family FPR\_PSE

1. Is FPR\_PSE.1.1 intended to be identical to FPR\_ANO.1.1? If so, why is it not represented by a dependency between the FPR\_PSE components and FPR\_ANO.1? Answer: Yes, it could be. However, we were advised by CCMB (Hans? Franken) that introducing a dependency created too much overhead for relatively small components. You criteria designers can change your mind if you like...
2. In FPR\_PSE.1.2, what does the *list of subjects* represent? Is it the set of subjects that must have an *alias* security attribute where other subjects do not? Answer: The *list of subjects* represents all those subjects, that for whatever reason want an alias. Not quite the same thing.
3. In FPR\_PSE.1.2, must every subject in the *list of subjects* have the capability to handle *number of aliases* aliases? Or must the TOE as a whole be able to handle *number of aliases* aliases? Answer: The TOE must be able to provide the aliases to the subjects. The rest is at the discretion of the subjects. It may help anonymity if there are aliases that don't "lead" to a subject. In any case adding "per subject" after "*number of aliases*" would resolve this.
4. In FPR\_PSE.1.3, what is an *alias metric*? Is it an algorithm that decides if a proposed alias is acceptable or not? Answer: It can be an algorithm to decide and/or a simple rule or table that may not qualify for being called an algorithm depending on how "intellectually high" algorithms are regarded.
5. Is a dependency between FPR\_PSE.1 and FIA\_ATD.1 missing? Is the alias, generated or entered, a security attribute of the *user*? Answer: Yes to both questions.
6. The purpose of FPR\_PSE.1.2 seems to be to interfere with user/subject binding. Could its effect not be achieved through FIA\_USB if, when a user activates a subject, the *user name* attribute becomes the *alias*, and a *real user name* attribute becomes the *real user name*? If this is the case, then cannot FPR\_PSE.1.2 be deleted and replaced by a dependency on FIA\_USB.1, and an application note explaining the rules required for FIA\_USB.1.2? Answer: Yes to both questions.
7. FPR\_PSE.3.4 says "the TSF shall provide an alias ..." where FPR\_PSE.3.3 offers a choice of the TSF or the user providing the alias. Should not FPR\_PSE.3.3 have its selection eliminated? Answer: That would be one option. The other option is to add "on request of the user" after "The TSF shall provide" and before "an alias". The choice is left to the CC Project or WG 3 to decide.

### 4 Family FPR\_UNL

1. In FPR\_UNL.1.1, what is a *list of operations*? Is it the same as "set of operations" as used in the functional requirements paradigm? Is it "execution of [assignment: list of SFRs]"? Answer: It is the same as "set of operations" in the paradigm. It may well include the SFRs, but it could cover other services to which FPR\_UNL is the interface, such as web based email services. Depends on granularity of SFRs.
2. In FPR\_UNL.1.1, what is a *list of relations*? Is it the same as a *list of operations*? Is it "have the same [assignment: list of subject security attributes]"? If so, why is the selection necessary, if "caused by the same user" is identical to "have the same real user name"? Answer: A list of relations represents relationships between users that may have caused the same operations or that have caused related operations, e.g. one user has written into a blog system, another has read from there. It is not the same as a *list of operations*. Describing the fact that two user names can link to the same user can indeed theoretically be specified by a relation, but feels odd, therefore "caused by the same user" was singled out as a frequent special case.

3. Why do the user application notes for the FPR\_UNL.1.1 assignment mandate protection against collaborating users and subjects? Is a selection “[selection: working alone, working in collaboration]” missing? Answer: In general FPR\_UNL.1.1 is to protect against collaborating users and subjects, not only single ones. Selection does not seem to be needed.

4. In the German NB proposed additions to the FPR\_UNL family, what does “are referenced by” mean in terms of relationships between users, subjects and objects? Answer: Usually it means the users were initiators/creators or were past or current holders, e.g. when an audit log logs all users who opened a file or downloaded a web page, all those users are referenced by the audit log object.

5. In FPR\_UNL.2/3/4, Iachello’s thesis refers to “binding relationships” as an explanation of the selection. However, it then confuses things further by indicating that a “type of operation” or “type of subject” etc. would be substituted. What is a “type of...”? Where would this be substituted, as this is only a selection operation? Answer: It looks like parts of the applications notes may need to be removed, given the component itself makes sense.

## 5 Family FPR\_UNO

1. In FPR\_UNO.1, what does *unable to observe the operation* mean? Is it “unable to detect any changes resulting from execution of *list of services* to the attributes of *list of resources*”? Answer: Yes.

2. Should FPR\_UNO.2 be deleted as a duplicate of proposed new family FPR\_TRD? Answer: If you add FPR\_TRD, it could be deleted.

3. In FPR\_UNO.3, what is a *list of services*? Is it a “list of SFRs”? Answer: We have answered this already. It may well include the SFRs but it also includes other services to which FPR\_UNO is the interface, such as a web based email service. How would you describe this?

4. In FPR\_UNO.3, what is *privacy related information*? Is it privacy related attributes of the subjects and objects referenced in the SFRs identified by the *list of services*? If so, how do we know which attributes these are? Answer: The *privacy related information* should be defined by the PP author based on the application area of the PP. It is the privacy related attributes, but without the strict reference to SFRs. The PP author should know his environment and the privacy relation of the information used in the environment, and so be able to identify (and document) those attributes.

5. In FPR\_UNO.4, what is a *resource*? Is it an object? What is a *service*? Is it an SFR? What does *usage* mean? Answer: A resource is something static to be used, e.g. a printer or a file. Generally it is an object in CC terms. A service is something dynamic to be used, e.g. a mail service or a web service. The distinction between resource and service was introduced as it seemed necessary in 1998, when this was written. It can be changed for better terminology, if this exists. It is not necessarily a single SFR, see discussions above. Usage has no special meaning, just plain English.

## 6 Family FDP\_IRC

1. In FDP\_IRC.1.1, what does the word *immediately* mean? What criteria does the evaluator use to decide if a TOE design/implementation satisfies the requirement? What does the evaluator do if poor design means that information necessarily needs to be retained much longer than in a better design with the same functionality?

[The example that occurred to me is a TOE that is designed to generate audit records only on closedown, and therefore needs to retain all its sensitive information until that point...]

Answer: In German what we meant would be „unverzöglich“, i.e. „ohne schuldhaftes Verzögern“, i.e. “without any delay that lies in the responsibility of the TOE”. The evaluator must judge it using common sense, which is unfortunately subjective, but so far nothing comes closer. A (subjectively) poor design means that the TOE fails the criterion.

2. In FDP\_IRC.1.1 and FDP\_IRC.2.1, what is the difference between *list of operations* and *list of functions*? Are both synonyms for *list of SFRs*? [Note that the words *list of activities* are used in Iachello’s thesis]. Answer: “operations” is as in “operations of subjects/users on objects”, “functions” is as in “Functions of the TSF” (which use TSF-data).

3. In FDP\_IRC.1.1 and FDP\_IRC.2.1, why is the second occurrence of *operations and/or functions* in italics? Answer: It’s a typo, it should be in plain text.

4. The application notes in Iachello’s thesis explain that this family is intended to provide protection against misuse by trusted subjects. But is it also intended to cover cases of TOE malfunction, where objects that should be protected are exposed because of failure of other SFRs? Answer: No, it was not the intention, but it might be used so.

5. In FDP\_IRC.2.1, what does the word *all* mean? Does it apply to objects which are involved in indirect data flows from the listed operations or functions? Answer: All is as in plain English. Yes, it applies to indirect flows, perhaps this should be mentioned more explicitly.

## 7 Family FPR\_TRD

1. Is FPR\_TRD.1 an architectural requirement, thus belonging in an assurance class? Answer: No. We are talking about dividing up functionality.

2. In FPR\_TRD.1.1, what does *distinct access control and authentication configurations* mean? Is it covered by the definition of domain now found in ADV\_ARC? Answer: Distinct access control and authentication configurations means administrators of one administrative domain may not enter other administrative domains. I did not find a definition of domain in ADV\_ARC, so I cannot be sure if it is covered or not. ADV\_ARC is quite explicit on self-protection and non-bypassability, but on domain separation it is rather vague. It says “The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.”. It says that domains should be described, but it does not say what they should be. There is no definition of domains or a description of the concept in this context. There is also no requirement how independent and distinct the domains should be from each other. Further the example with the OS in Annex A on page 194<sup>1</sup> is rather limited with regard to distinction and independence of the domains.

3. In FPR\_TRD.1.2, what does “explicitly request” mean? Is this element satisfied by requiring that all inter-domain data flows are through objects defined in TSFIs? Could this element be reworded as “Information shall only pass between administrative domains through objects defined in the TSFI between them”? Answer “explicitly request” means that implicit information flows shall not happen. With regards to TSFIs, perhaps this is equivalent, but then any description of distinction of the domain is missing

4. In FPR\_TRD.1, what do “separate” and “independent” mean? Answer: what they mean in plain English.

5. Are FPR\_TRD.2.3 and FPR\_TRD.3.3 a different type of requirement to FPR\_TRD.1? Should they be expressed as components with a dependency on FPR\_TRD.1 rather than as hierarchical requirements? Answer: FPR\_TRD.2.3 and FPR\_TRD.3.3 make use of the different

---

<sup>1</sup> For example, an operating system TOE supplies a domain (address space, per-process environment variables) for each process associated with untrusted entities.

administrative domains set out in FPR\_TRD.1. With FPR\_TRD.1, one just has the domains, but one does not use them. Perhaps this should be expressed as a dependency, but what would this help?

6. In FPR\_TRD.2.3, what is the difference between *list of data* and *list of objects*? [Note that Iachello's thesis has only *list of objects*]. Answer: Usually object is used for a specific place, where data are stored (e. g. a file). So "data" was introduced as a more generic term to indicate the content, regardless of where it may be stored/processed (maybe this is the same as information).

7. In FPR\_TRD.2.3, what does *unreadable* mean? What does *by a single administrative domain* mean? Does it refer to subjects within that domain? Answer: *unreadable* means that no read access is possible. *By a single administrative domain* means that to get read access, several domains need to collaborate. It need not necessarily refer only to subjects within that domain, but this is possible.

8. In FPR\_TRD.2.3, is there an implied restriction that there are at least as many domains as there data and/or objects in the "*list of data and/or objects*"? Answer: there can be such a restriction, but this depends on the list of conditions on data and/or objects given in TRD2.3.

9. In FPR\_TRD.2.3, how do multiple conditions in the *list of conditions on data and/or objects* inter-react? Should this component be restricted to one condition, with multiple conditions handled by replication? Answer: If they inter-react, it is in a (hopefully) logical fashion. One may well be able to restrict this to just one condition, but what does it change? Complex condition systems are always complex and can be ambiguous or contradictory. It should be mentioned in the user notes that conditions should neither be ambiguous or contradictory.

10. In FPR\_TRD.3.3, is a *list of operations* a *list of SFRs*? Answer: As before, not necessarily; why should this be so restricted? Web email access would be a counter example.

11. In FPR\_TRD.3.3, what types of *conditions* can be maintained, other than the implicitly required processing of different operations by different domains? Answer: These are conditions which must hold as a result of the enforcement of the requirement of allocation of activities. They can e.g. be related to the type of privacy that the TOE is to achieve. Example from the "User-Oriented Protection Profile for Unobservable Message Delivery communication using Mix networks, Revision 2.4": "No subject in the TOE, and no attacker, may gain enough information to fully trace a message chain from sender to receiver."