ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18336.2—2015/ISO/IEC 15408-2:2008
代替 GB/T 18336.2—2008

信息技术　安全技术
信息技术安全评估准则
第2部分:安全功能组件

**Information technology—Security techniques—
Evaluation criteria for IT security—
Part 2: Security functional components**

(ISO/IEC 15408-2:2008,IDT)

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 18336《信息技术　安全技术　信息技术安全评估准则》分为以下三部分：

——第1部分：简介和一般模型；

——第2部分：安全功能组件；

——第3部分：安全保障组件。

本部分是GB/T 18336的第2部分。

本部分按照GB/T 1.1—2009给出的规则编写。

本部分代替GB/T 18336.2—2008《信息技术　安全技术　信息技术安全评估准则　第2部分：安全功能要求》。

本部分与GB/T 18336.2—2008的主要差异如下：

——将“保证”(assurance)改为“保障”；

——将“10.4 输出到TSF控制之外(FDP_ETC)”改为“10.4 从TOE输出(FDP_ETC)”；

——将“10.7 从TSF控制之外输入(FDP_ITC)”改为“10.7 从TOE之外输入(FDP_ITC)”；

——删除了“14FPT类：TSF保护”中的“14.1 底层抽象机测试(FPT_AMT)”、“14.10 引用仲裁(FPT_RVM)”、“14.11 域分离(FPT_SEP)”；

——在“14FPT类：TSF保护”中增加了“14.12 外部实体测试(FPT_TEE)”；

——将“16.3 会话锁定(FTA_SSL)”改为“16.3 会话锁定和终止(FTA_SSL)”；

——将“门限值”改为“临界值”；

——将“介导”改为“促成”。

本部分使用翻译法等同采用国际标准ISO/IEC 15408-2:2008《信息技术　安全技术　信息技术安全评估准则　第2部分：安全功能组件》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 18336.1　信息技术　安全技术　信息技术安全评估准则　第1部分：简介和一般模型(GB/T 18336.1—2015，ISO/IEC 15408-1:2009，IDT)

本部分做了下列编辑性修改：

——第4.1条标准原文有编辑性错误，现已更正为“对于有关结构、规则和指南，编写PP或ST的人员应参见ISO/IEC 15408-1第3章和相关附录”。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出和归口。

本部分起草单位：中国信息安全测评中心、信息产业信息安全测评中心、公安部第三研究所、吉林信息安全测评中心。

本部分主要起草人：张翀斌、郭颖、石竑松、毕海英、张宝峰、高金萍、王峰、杨永生、李国俊、董晶晶、谢蒂、王鸿娴、张怡、顾健、邱梓华、宋好好、陈妍、杨元原、李凤娟、庞博、张骁、刘昱函、王书毅、周博扬、唐喜庆、蒋显岚、张双双。

本部分所代替标准的历次版本发布情况为：

——GB/T 18336.2—2001；

——GB/T 18336.2—2008。

引　言

本部分定义的安全功能组件为在保护轮廓(PP)或安全目标(ST)中表述的安全功能要求提供了基础。这些要求描述了评估对象(TOE)所期望的安全行为，并旨在满足在 PP 或 ST 中所提出的安全目的。这些要求描述那些用户能直接通过 IT 交互(即输入、输出)或 IT 激励响应过程探测到的安全特性。

安全功能组件表达了安全要求，这些要求试图对抗针对假定的 TOE 运行环境中的威胁，并/或涵盖了所有已标识的组织安全策略和假设。

本部分的目标读者主要包括安全的 IT 产品的消费者、开发者、评估者。ISO/IEC 15408-1 第 5 章提供了关于 ISO/IEC 15408 的目标读者和目标读者群体如何使用 ISO/IEC 15408 的附加信息。这些群体可以按如下方式使用本部分：

a) 消费者，为满足 PP 或 ST 中提出的安全目的，通过选取本部分的组件来表述功能要求。ISO/IEC 15408-1 提供了更多关于安全目的和安全要求之间的关系的详细信息；

b) 开发者，在构造 TOE 时响应实际的或预测的消费者安全要求，可以在本部分中找到一种标准的方法去理解这些要求。也可以以本部分的内容为基础，进一步定义 TOE 的安全功能和机制来满足那些要求；

c) 评估者，使用本部分所定义的功能要求检验在 PP 或 ST 中表述的 TOE 功能要求是否满足 IT 安全目的，以及所有的依赖关系是否都已解释清楚并得到满足。评估者也宜使用本部分去帮助确定指定的 TOE 是否满足规定的要求。

信息技术　安全技术
信息技术安全评估准则
第2部分:安全功能组件

1　范围

为了安全评估的意图,GB/T 18336的本部分定义了安全功能组件所需要的结构和内容。本部分包含一个安全组件的分类目录,将满足许多IT产品的通用安全功能要求。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修订版)适用于本文件。

ISO/IEC 15408-1　信息技术 安全技术　信息技术安全评估准则　第1部分:简介和一般模型(Information technology—Security techniques—Evaluation criteria for IT security —Part 1:Introduction and general model)

3　术语、定义和缩略语

ISO/IEC 15408-1中给出的术语、定义、符号和缩略语适用于本文件。

4　概述

ISO/IEC 15408和本部分在此描述的相关安全功能要求,并不意味着是对所有IT安全问题的最终回答。相反,本标准提供一组广为认同的安全功能要求,以用于制造反映市场需求的可信产品。这些安全功能要求的给出,体现了当前对产品的要求规范和评估的技术发展水平。

本部分并不计划包括所有可能的安全功能要求,而是尽量包含那些在本部分发布时作者已知的并认为是有价值的那些要求。

由于消费者的认知和需求可能会发生变化,因此本部分中的功能要求需要维护。可预见的是,某些PP/ST作者可能还有一些安全要求未包含在本部分提出的功能要求组件中。此时,PP/ST的作者可考虑使用ISO/IEC 15408之外的功能要求(称之为可扩展性),有关内容参见ISO/IEC 15408-1的附录A和附录B。

4.1　本部分的结构

第5章是本部分安全功能要求使用的范型。

第6章介绍本部分功能组件的分类,第7章～第17章描述这些功能类。

附录A为功能组件的潜在用户提供了解释性信息,其中包括功能组件间依赖关系的一个完整的交叉引用表。

附录B～附录M提供了功能类的解释性信息。在如何运用相关操作和选择恰当的审计或文档信

息时，这些材料必须被看作是规范性说明。使用助动词“应”表示该说明是首要推荐的，但是其他的只是可选的。这里只给出了不同的选项，具体的选择留给了 PP/ST 作者。

对于有关结构、规则和指南，编写 PP 或 ST 的人员应参见 ISO/IEC 15408-1 第 3 章和相关附录：

a) ISO/IEC 15408-1 第 3 章定义了 ISO/IEC 15408 中使用的术语。

b) ISO/IEC 15408-1 附录 A 定义了 ST 的结构。

c) ISO/IEC 15408-1 附录 B 定义了 PP 的结构。

5 功能要求范型

本章描述了本部分安全功能要求中所使用的范型。讨论中所涉及的关键概念均以粗体/斜体突出表示。本章并不打算替换或取代 ISO/IEC 15408-1 第 3 章中所给出的任何术语。

本部分是一个有关安全功能组件的目录，可用于规约一个**评估对象**(**TOE**)的安全功能要求。TOE 可以是软件、固件和/或硬件的集合，并可能配有用户和管理员的指导性文档。TOE 可包含用于处理和存储信息的资源，诸如电子存储媒介(如主存、磁盘空间)、外设(如打印机)以及计算能力(如 CPU 时间)等，并且是评估的对象。

TOE 评估主要关注的是，确保对 TOE 资源执行了所定义的**安全功能要求**(**SFR**)集。这些 SFR 定义了一些规则，TOE 通过这些规则来管制对其资源的访问和使用，从而实现对信息和服务的管控。

这些 SFR 可定义多个**安全功能策略**(**SFP**)，以表达 TOE 必须执行的规则。每一个这样的 SFP 必须通过定义主体、客体、资源或信息及其适用的操作，来明确说明该安全功能策略的**控制范围**。所有 SFP 均由 TSF(见下文)实现，其机制执行 SFR 中定义的规则并提供必要的能力。

TOE 中为正确执行 SFR 而必须依赖的部分统称为 **TOE 安全功能**(**TSF**)。TSF 由 TOE 中为了安全执行而直接或间接依赖的所有软件、硬件和固件组成。

TOE 可以是一个包含硬件、固件和软件的整体合一式的产品。

TOE 也可以是一个分布式产品，内部由多个不同的部分组成，每一部分都为 TOE 提供特定的服务，并且通过**内部通信信道**与 TOE 其他部分相连接。该信道可以小到为一个处理器总线，也可以是 TOE 之内的一个网络。

当 TOE 由多个部分组成时，TOE 的每一部分可拥有自己的那部分 TSF，该部分通过内部通信信道与 TSF 的其他部分交换用户数据和 TSF 数据，这种交互称为 **TOE 内部传送**。在这种情况下，这些 TSF 的不同部分抽象地形成了执行 SFR 的组合型 TSF。

TOE 接口可能只局限在特定的 TOE 内部使用，或者也可允许通过**外部通信信道**与其他 IT 产品交互。与其他 IT 产品的外部交互可以采取以下两种形式：

a) 其他“可信 IT 产品”的安全功能要求和 TOE 的安全功能要求已进行了管理方面的协调，并假设这些其他可信 IT 产品已正确执行了其安全功能要求(例如：通过独立的评估)。在这种情况下，信息交换被称为 **TSF 间传送**，因为它们存在于不同可信产品的 TSF 之间。

b) 其他 IT 产品可能是不可信的，被称为“不可信 IT 产品”。因此，它的 SFR 或是未知的，或这些 SFR 的实现被视为是不可信赖的。在这种情况下，TSF 促成的信息交换被称为 **TOE 的外部传送**，因为在其他 IT 产品上没有 TSF(或它的策略特征是未知的)。

一个接口集合，不管是交互式的(人机接口)，还是可编程的(应用编程接口)，通过这些接口，由 TSF 协调对资源的访问，或者从 TSF 中获取信息，这一接口集合被称为 **TSF 接口**(**TSFI**)。TSFI 定义了为执行 SFR 而提供的 TOE 功能边界。

用户在 TOE 的外部。但为了请求由 TOE 执行且由 SFR 中定义的规则所控制的服务，用户要通过 TSFI 和 TOE 交互。本部分关注两种类型用户：**人类用户**和**外部 IT 实体**。人类用户可进一步分为**本地用户**和**远程用户**，本地用户通过 TOE 设备(如工作站)直接与 TOE 交互，远程用户通过其他 IT 产

品间接与 TOE 交互。

用户和 TSF 之间的一段交互期称为用户**会话**。可以根据各种因素来控制用户会话的建立，例如：用户鉴别、时段、访问 TOE 的方法以及允许的(每个用户的或总的)并发会话数。

本部分使用术语**"授权的"**来表示一个用户持有执行某项操作的权力或特权。因此术语**"授权用户"**表明用户允许执行由 SFR 定义的特定操作或一组操作。

为了表达分离管理责任的要求，相关的安全功能组件(来自 FMT_SMR 族)明确指出了所要求的管理性**角色**。角色是预定义的一组规则，用于建立用户按此角色操作时所允许的与 TOE 之间的交互。一个 TOE 可以支持任意多个角色的定义。例如，与 TOE 安全运行相关的角色可以包括"审计管理员"和"用户账号管理员"。

TOE 包含可用于处理和存储信息的**资源**。TSF 的主要目标是对 TOE 所控制的资源和信息完整而正确地执行 SFR。

TOE 资源能以多种方式组织并加以利用。但是，本部分作出了一个明确的区分，以便允许规范所期望的安全特性。所有可通过资源来创建的实体，可用以下两种方式中的一种来刻画：实体可以是主动的，意指它们是促使在 TOE 内部出现动作并导致信息操作的原因；或者，实体也可以是被动的，意指它们或是产生信息的载体，或是存储信息的载体。

TOE 中对客体执行操作的主动实体，被称为**主体**。TOE 内可存在以下类型的主体：

a) 代表一个授权用户的那些实体(如 UNIX 进程)；

b) 作为一个特殊功能进程，可依次代表多个用户的那些实体(如在客户/服务器结构中可能找到的某些功能)；

c) 作为 TOE 自身一部分的那些实体(如不代表某个用户的进程)。

本部分用于解决在上述各类主体上实施 SFR 的问题。

TOE 中包含和接收信息，且主体得以在这些信息上执行操作的被动实体，称作**客体**。在一个主体(主动实体)是某个操作的对象(例如进程间通信)的情况下，该主体也可以作为一个客体。

客体可以包含**信息**。引入这一概念是为了详细说明在 FDP 类中描述的信息流控制策略。

由 SFR 中各规则所控制的用户、主体、信息、客体、会话和资源，可具有某种**属性**。属性包含 TOE 为了正确运行而使用的信息。某些属性，如文件名，可能只是提示性的，或者可用来标识单个资源，而另一些属性，如访问控制信息，可能是专为执行 SFR 而存在的。后面这些属性通常称为**"安全属性"**。在本部分的某些地方中，"属性"一词将用作"安全属性"的简称。另一方面，无论属性信息的预期目的如何，均有必要按 SFR 的规定对属性施加控制。

TOE 中的数据可分为用户数据和 TSF 数据，图 1 示意了它们之间的关系。**用户数据**是存储在 TOE 资源中的信息，用户可以根据 SFR 对其进行操作，而 TSF 对用户数据并不赋予任何特殊的含义。例如，电子邮件消息的内容是用户数据。**TSF 数据**是 TSF 在按 SFR 的要求做决策时使用的信息。如果 SFR 允许，TSF 数据可以受用户的影响。安全属性、鉴别数据、由 SFR 中定义的规则，或为了保护 TSF 及访问控制列表条目所使用的 TSF 内部状态变量都是 TSF 数据的例子。

有几个用于数据保护的 SFP，诸如**访问控制 SFP** 和**信息流控制 SFP**。实现访问控制 SFP 的机制依据受控范围内的用户、资源、主体、客体、会话、TSF 状态数据以及操作等的属性来建立策略决策。这些属性用于管控主体操作客体的规则集中。

实现信息流控制 SFP 的机制依据受控范围内的主体和信息的属性以及管控主体操作信息的规则来建立策略决策。信息的属性与信息一起由 TSF 予以处理，这些属性可能与载体属性相关联，或可能是来源于载体中的数据。

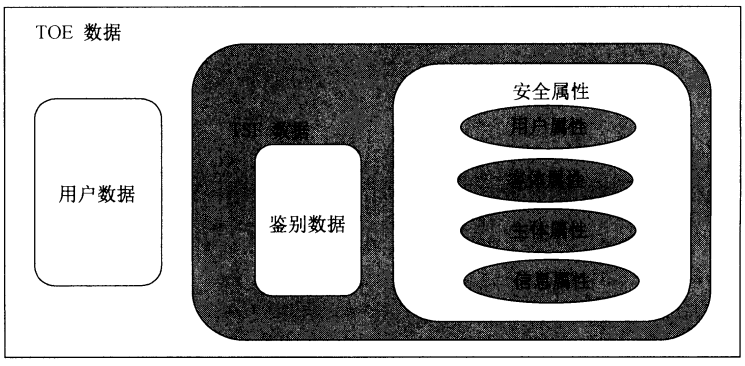

图 1 用户数据和 TSF 数据的关系

在本部分中处理的两种特殊类型的 TSF 数据-**鉴别数据**和**秘密**可以相同，也可以不同。

鉴别数据用于验证用户请求 TOE 服务时所声称的身份。最常用的鉴别数据形式是口令，为了使安全机制有效，这一形式的鉴别数据需要保密。但是，并非所有形式的鉴别数据都需要保密，生物特征鉴别设备（例如，指纹识别器、视网膜扫描仪）就不依赖于数据保密，而依赖于这些数据只能被一个用户拥有，且不能被伪造。

本部分中使用的术语“秘密”，尽管可用于鉴别数据，也同样适用于其他为了执行某特定 SFP 而必须保密的数据。例如，在强度方面，依靠密码技术保护信道信息机密性的可信信道机制，仅与防止密钥未授权泄露机制是一样的。

因此，不是所有的鉴别数据都需要保密，也不是所有的秘密都可用做鉴别数据。图 2 给出了秘密和鉴别数据间的关系。在该图中，指出了常见的鉴别数据和秘密的数据类型。

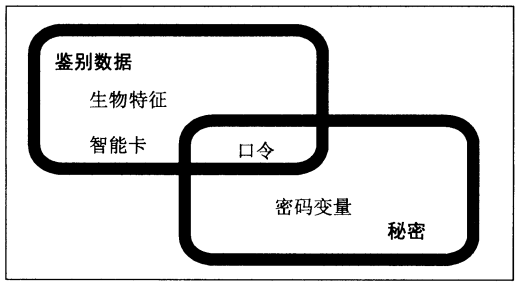

图 2 “鉴别数据”和“秘密”的关系

6 安全功能组件

6.1 概述

本章定义了 ISO/IEC 15408 功能要求的内容和形式，并提供了一个组织方法，以便对 ST 中添加的新组件的安全功能要求进行描述。功能要求用类、族和组件来表达。

6.1.1 类结构

图 3 以框图形式示意了功能类的结构。每个功能类包括类名、类介绍和一个或多个功能族。

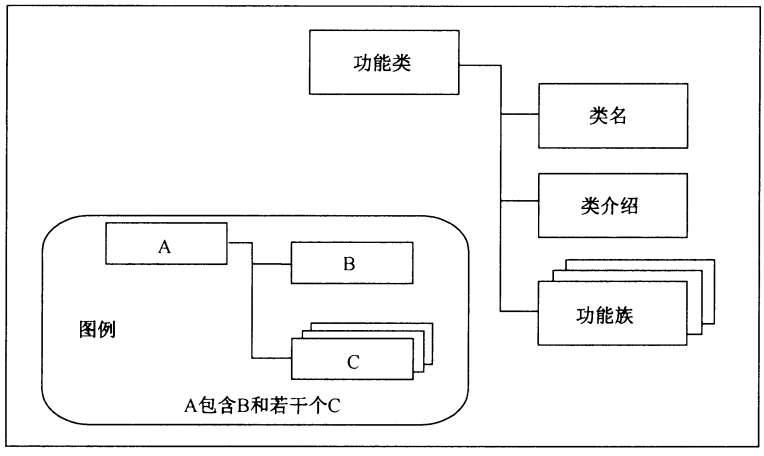

图 3 功能类结构

6.1.1.1 类名

类名提供标识和划分功能类所必需的信息。每个功能类都有一个唯一的名称，分类信息由三个字符的简名组成。类的简名也用于该类中族的简名规范中。

6.1.1.2 类介绍

类介绍描述了这些族满足安全目的的通用意图或方法。功能类的定义不反映要求规范中的任何正式分类法。

类介绍用图的形式来描述类中的族以及每个族中组件的层次结构，见 6.2 的解释。

6.1.2 族结构

图 4 以框图形式示意了功能族的结构。

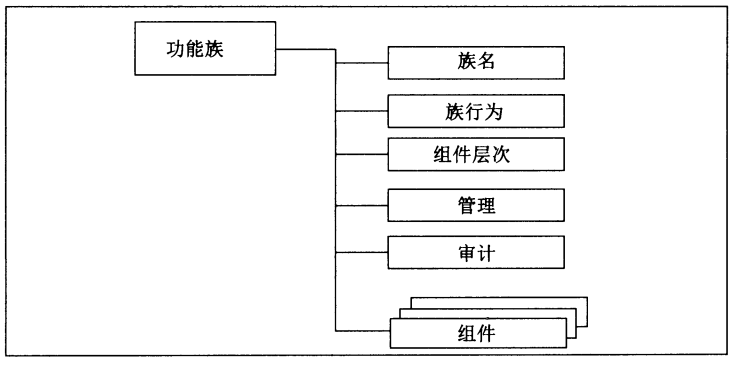

图 4 功能族结构

6.1.2.1 族名

族名部分提供了标识和划分功能族所必需的分类和描述信息。每个功能族有一个唯一的名称。族的分类信息由 7 个字符的简名组成，前三个字符与类名相同，后跟一个下划线和族名，形如 XXX_YYY。唯一的简短族名为组件提供了主要的引用名称。

6.1.2.2 族行为

族行为是对功能族的叙述性描述，陈述其安全目的，并且是功能要求的概括描述。以下是更详细的描述：

a) 族的*安全目的*描述了一个安全问题，该问题可通过 TOE 利用该族中的一个组件予以解决；

b) *功能要求*的描述概述了组件中包含的所有要求。该描述是面向 PP、ST 和功能包的作者的，他们希望评价该族是否与他们的特定要求相关。

6.1.2.3 组件层次

功能族包含一个或多个组件，任何一个组件都可被选出来包含到 PP、ST 和功能包中。本条的目的是，当族一旦被确定为是表达用户安全要求的一个必须的或有用的部分时，为用户选取合适的功能组件提供信息。

功能族描述部分的本条内容描述了可使用的组件以及它们的基本原理。组件的详细细节包含在每个组件中。

功能族内组件间的关系可能是分级的。如果一个组件相对另一个组件提供更多的安全性，那么该组件对另一个组件来说是更高级的。

如 6.2 所述，族的描述提供了族中组件间层次结构的一个图示。

6.1.2.4 管理

*管理*包含 PP/ST 作者认为是给定组件管理活动的一些信息。此条款参考管理类(FMT)的组件，并提供关于通过操作这些组件可能应用的潜在管理活动的指导。

PP/ST 作者可以选择已明示的管理要求，也可以选择其他没有列出的管理要求以细化管理活动。因而这些信息是提示性的。

6.1.2.5 审计

如果 PP/ST 中包含来自 FAU 类“安全审计”中的要求，*审计*要求要包含可供 PP/ST 作者选择的可审计事件。这些由 FAU_GEN“安全审计数据产生”族的组件支持的要求包括各种按不同详细级别描述的安全相关事件。例如，一个审计记录可能包括下述动作：最小级——安全机制的成功使用；基本级——对安全机制的使用以及涉及安全属性的信息；详细级——任何机制的配置变化，包括改变前后的实际配置值。

显然可审计事件的分类是分级的。例如，当期望的审计数据产生级别满足基本级时，除非高级事件仅仅比低级事件提供更多的细节，所有已标识为最小级和基本级的可审计事件都应通过适当的赋值操作包括在 PP/ST 内。当期望的审计数据产生级别满足详细级时，所有标识为最小级、基本级和详细级的可审计事件都应包括在 PP/ST 内。

在 FAU 类“安全审计”中，更详尽地解释了一些控制审计的规则。

6.1.3 组件结构

图 5 示意了功能组件的结构。

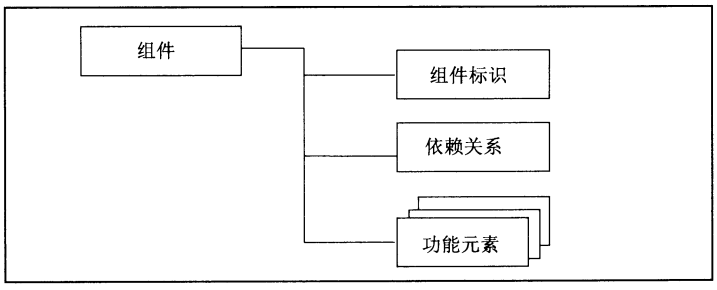

图 5 功能组件结构

6.1.3.1 组件标识

组件标识部分提供识别、分类、注册和交叉引用组件所必需的描述性信息。下列各项作为每个功能组件的部分：

——一个*唯一的名称*，该名字反映了组件的目的。

——一个*简名*，即功能组件名的唯一简写形式。简名作为组件分类、注册和交叉引用的主要引用名。简名反映出组件所属的类和族以及在族中组件的编号。

——一个*从属于列表*。这个组件所从属于的其他组件列表，以及该组件能用于满足与所列组件间的依赖关系。

6.1.3.2 功能元素

为每一组件提供了一组元素。每个元素都分别定义并且是自包含的。

功能元素是一个安全功能要求，该要求如果再进一步划分将不会产生有意义的评估结果。它是ISO/IEC 15408 中标识和认可的最小安全功能要求。

当构建包、PP 或 ST 时，不允许从一个组件中只选择一个或几个元素，必须将组件的整套元素包含在 PP、ST 或包中。

每个功能元素名都有一个唯一的简化形式。例如，要求名 FDP_IFF.4.2 意义如下：F——功能要求，DP——“用户数据保护”类，_IFF——“信息流控制功能”族，.4——第四个组件，名为“部分消除非法信息流”，.2——该组件的第 2 个元素。

6.1.3.3 依赖关系

当一个组件不是自我充分的而需要依赖于其他组件的功能，或与其他组件交互才能正确发挥其功能时，就产生了功能组件间的依赖关系。

每个功能组件都提供了一个对其他功能和保障组件依赖关系的完整列表。有些组件可能列出“无依赖关系”。所依赖的组件又可能依赖其他组件。组件中提供的列表是直接的依赖关系。这只是为该功能要求能正确实现其功能提供参考。间接依赖关系，也就是由所依赖组件产生的依赖关系，见本部分附录 A。值得注意的是，在某些情况下，依赖关系所提供的多个功能要求是可自由选择的，这些功能要求中的任一个都足以满足依赖关系（例如 FDP_UIT.1“数据交换完整性”）。

依赖关系列表标识出了为满足一个既定组件相关的安全要求，所必需的最少功能或保障组件。从属于既定组件的那些组件也可用来满足依赖关系。

本部分指明的依赖关系是规范性的，在 PP/ST 中它们必须得到满足。在特定的情况下，这种依赖关系可能不适用。只要在基本原理中说清不适用的理由，PP/ST 作者就可以在包、PP 或 ST 中舍弃该依赖组件。

6.2 组件分类

本部分中组件的分组不代表任何正式的分类法。

本部分包含了族和组件的分类，它们是基于相关功能和目的进行的粗略分组，并且按字母顺序给出。每个类的开始部分都有一个提示性框图，指出该类的分类法、类中的族和族中的组件。这个图对于指明可能会存在于组件间的层次关系是有用的。

在功能组件的描述中，有一段文字指出了该组件和任何其他组件之间的依赖关系。

在每个类中，都有一个与图 6 类似的描述族层次关系的图。在图 6 中，第 1 个族(族 1)包括了三个有从属关系的组件，其中组件 2 和组件 3 都可以用来满足对组件 1 的依赖关系。组件 3 从属于组件 2，并且可以用来满足对组件 2 的依赖关系。

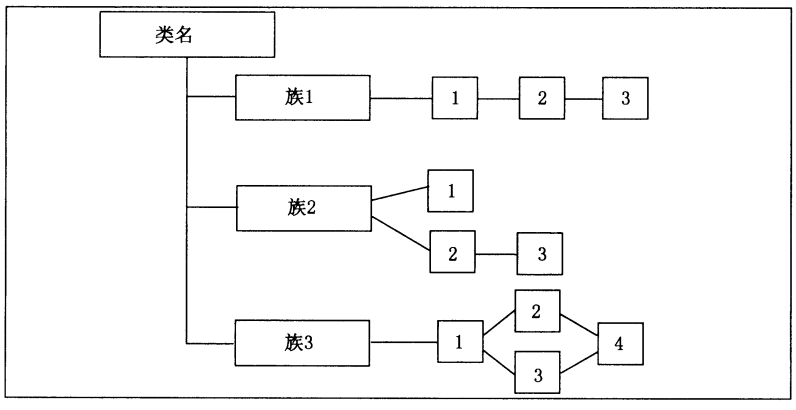

图 6 示范类分解图

在族 2 中有三个组件，这三个组件不全都有从属关系。组件 1 和组件 2 不从属于其他组件。组件 3 从属于组件 2，可以用来满足对组件 2 的依赖关系，但不能满足对组件 1 的依赖关系。

在族 3 中，组件 2、3、4 都从属于组件 1。组件 2 和组件 3 也都从属于组件 1，但无可比性。组件 4 从属于组件 2 和组件 3。

这些图的目的是补充族中的文字说明，使关系的识别更容易。它们并不能取代每个组件中的“从属于:”的注释，这些注释是对每个组件从属关系的强制性声明。

6.2.1 突出表示组件变化

族中组件的关系约定以**粗体字**突出表示。在此约定所有新的要求用粗体表示。对于有从属关系的组件，当要求被增强或修改而超出前一组件的要求时，要用**粗体字**表示。另外，超出前一组件的任何新的或增强的允许操作，也使用**粗体字**突出表示。

7 FAU 类:安全审计

安全审计包括识别、记录、存储和分析那些与安全相关活动(即由 TSP 控制的活动)有关的信息。可通过检查审计记录结果确定发生了哪些安全相关活动以及哪个用户要对这些活动负责。本类的组件构成分解如图 7 所示。

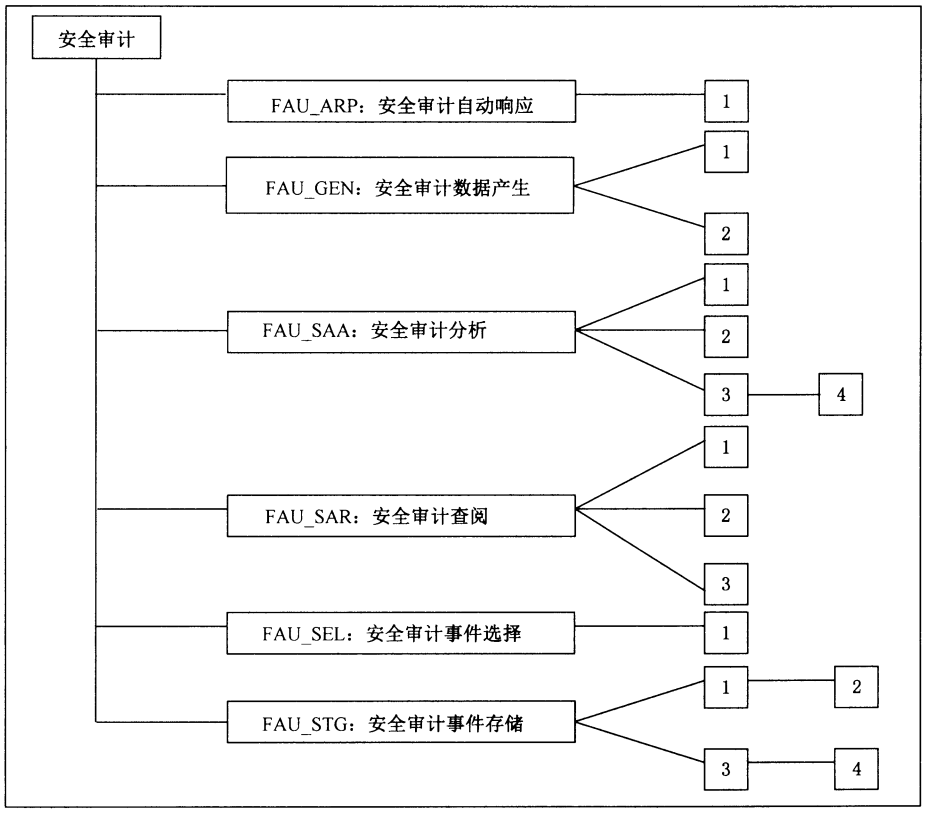

图 7　FAU：安全审计类分解

7.1　安全审计自动响应(FAU_ARP)

7.1.1　族行为

本族定义了在检测到潜在安全侵害事件时所作出的响应。

7.1.2　组件层次

FAU_ARP.1“安全告警”，当检测到潜在的安全侵害时 TSF 应采取动作。

7.1.3　FAU_ARP.1 管理

FMT 中的管理功能可考虑下列行为：

a)　对行为的管理(添加、删除或修改)。

7.1.4　FAU_ARP.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a)　最小级：由于潜在的安全侵害而采取的动作。

7.1.5　FAU_ARP.1 安全告警

从属于：无其他组件。

依赖关系：FAU_SAA.1 潜在侵害分析。

7.1.5.1 FAU_ARP.1.1

当检测到潜在的安全侵害时，TSF 应采取的[赋值：*动作列表*]。

7.2 安全审计数据产生(FAU_GEN)

7.2.1 族行为

本族定义了一些在 TSF 控制下对安全相关事件的发生情况进行记录的要求。本族识别审计的级别，列举 TSF 可审计的事件类型，以及标识在各种审计记录内应提供的审计相关信息的最小集合。

7.2.2 组件层次

FAU_GEN.1“审计数据产生”定义可审计事件的级别，并规定在每个记录中应记录的数据列表。

FAU_GEN.2“用户身份关联”，TSF 应把可审计事件与单个用户身份相关联。

7.2.3 FAU_GEN.1、FAU_GEN.2 管理

尚无预见的管理活动。

7.2.4 FAU_GEN.1、FAU_GEN.2 审计

尚无预见的可审计事件。

7.2.5 FAU_GEN.1 审计数据产生

从属于：无其他组件。

依赖关系：FPT_STM.1 可信时间戳。

7.2.5.1 FAU_GEN.1.1

TSF 应能为下述可审计事件产生审计记录：

a) **审计功能的开启和关闭；**

b) **有关[选择，选取一个：*最小级*、*基本级*、*详细级*、*未规定*]审计级别的所有可审计事件；**

c) **[赋值：*其他专门定义的可审计事件*]。**

7.2.5.2 FAU_GEN.1.2

TSF 应在每个审计记录中至少记录下列信息：

a) **事件的日期和时间、事件类型、主体身份(如果适用)、事件的结果(成功或失效)；**

b) **对每种审计事件类型，基于 PP/ST 中功能组件的可审计事件的定义，[赋值：*其他审计相关信息*]。**

7.2.6 FAU_GEN.2 用户身份关联

从属于：无其他组件。

依赖关系：FAU_GEN.1 审计数据产生；

FIA_UID.1 标识的时机。

7.2.6.1 FAU_GEN.2.1

对于已标识身份的用户的行为所产生的审计事件，TSF 应能将每个可审计事件与引起该事件的用

户身份相关联。

7.3 安全审计分析(FAU_SAA)

7.3.1 族行为

本族定义了一些采用自动化手段分析系统活动和审计数据以寻找可能的或真正的安全侵害的要求。这种分析通过入侵检测来实现,或对潜在的安全侵害作出自动响应。

基于检测而采取的动作,可用 FAU_ARP"安全审计自动响应"族来规范。

7.3.2 组件层次

在 FAU_SAA.1"潜在侵害分析"中,要求在固定规则集的基础上进行基本的阈值检测。

在 FAU_SAA.2"基于轮廓的异常检测"中,TSF 维护系统使用的单个轮廓。这里的"轮廓"表示由轮廓目标组成员所完成的历史模式的使用。轮廓目标组是指与 TSF 交互的一个或多个个体(如单个用户、共享一个组 ID 或账号的用户、分配了指定角色的用户、整个系统或网络节点的用户)。轮廓目标组的每个成员都被分配了一个单独的置疑等级,表明成员当前的行为与轮廓中已建立的使用模式的一致程度如何。此分析可实时进行,也可在信息采集后的批量分析阶段进行。

FAU_SAA.3"简单攻击探测",TSF 应能检测到那些对 SFR 实施将产生重大威胁的特征事件的发生。对特征事件的搜索可以实时进行,也可以在信息采集后的批量分析阶段进行。

FAU_SAA.4"复杂攻击探测",TSF 应能表示并检测到多步骤入侵情景。TSF 应能对照已知事件序列来比较(可能是由多个用户执行的)系统事件以表示完整入侵情景。TSF 应能在发现特征事件或事件序列时进行提示,该事件预示一个对 SFR 实施的潜在违反。

7.3.3 FAU_SAA.1 管理

FMT 中的管理功能可考虑采取下列行为:

a) 通过(添加、修改、删除)规则集中的规则来维护规则。

7.3.4 FAU_SAA.2 管理

FMT 中的管理功能可考虑下列行为:

a) 对轮廓目标组中的用户组进行维护(删除、修改、添加)。

7.3.5 FAU_SAA.3 管理

FMT 中的管理功能可考虑下列行为:

a) 对系统事件的子集进行维护(删除、修改、添加)。

7.3.6 FAU_SAA.4 管理

FMT 中的管理功能可考虑下列行为:

a) 对系统事件的子集进行维护(删除、修改、添加);

b) 对系统事件的序列集进行维护(删除、修改、添加)。

7.3.7 FAU_SAA.1、FAU_SAA.2、FAU_SAA.3、FAU_SAA.4 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:开启和关闭任何分析机制;

b) 最小级:通过工具软件实现自动响应。

7.3.8 FAU_SAA.1 潜在侵害分析

从属于:无其他组件。

依赖关系:FAU_GEN.1 审计数据产生。

7.3.8.1 FAU_SAA.1.1

TSF 应能使用一组规则去监测审计事件,并根据这些规则指示出对实施 SFR 的潜在侵害。

7.3.8.2 FAU_SAA.1.2

TSF 应执行下列规则监测审计事件:

a) **已知的用来指示潜在安全侵害的[赋值:*已定义的可审计事件的子集*]的累积或组合;**

b) **[赋值:*任何其他规则*]。**

7.3.9 FAU_SAA.2 基于轮廓的异常检测

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

7.3.9.1 FAU_SAA.2.1

TSF 应能维护系统使用轮廓。在这里单个轮廓代表由[赋值:*轮廓目标组*]成员完成的历史使用模式。

7.3.9.2 FAU_SAA.2.2

TSF 应维护一个与每个用户相对应的置疑等级,这些用户的活动已记录在轮廓中。在这里,置疑等级代表用户当前活动与轮廓中已建立的使用模式不一致的程度。

7.3.9.3 FAU_SAA.2.3

当用户的置疑等级超过门限条件[赋值:*TSF 报告异常活动的条件*]时,TSF 应能指出对 SFR 实施的可能侵害即将发生。

7.3.10 FAU_SAA.3 简单攻击探测

从属于:无其他组件。

依赖关系:无依赖关系。

7.3.10.1 FAU_SAA.3.1

对预示可能违反 SFR 实施的下列特征事件[赋值:*系统事件的一个子集*],TSF 应能维护一个内部表示。

7.3.10.2 FAU_SAA.3.2

TSF 应能对照特征事件比对系统活动记录,系统活动可以通过检查[赋值:*用来确定系统活动的信息*]而辨明。

7.3.10.3 FAU_SAA.3.3

当发现一个系统事件与一个预示可能潜在违反 SFR 实施的特征事件匹配时,TSF 应能指出潜在违

反 SFR 实施的事件即将发生。

7.3.11 FAU_SAA.4 复杂攻击探测

从属于:FAU_SAA.3 简单攻击探测。

依赖关系:无依赖关系。

7.3.11.1 FAU_SAA.4.1

对**已知入侵情景的事件序列**[**赋值**:***已知攻击出现的系统事件序列列表***]**和**预示可能**潜在**违反 SFR 实施的下列特征事件[赋值:*系统事件的一个子集*],TSF 应能维护一个内部表示。

7.3.11.2 FAU_SAA.4.2

TSF 应能对照特征事件**和事件序列比对**系统活动记录,这里系统活动可以通过检查[赋值:*用来确定系统活动的信息*]而辨明。

7.3.11.3 FAU_SAA.4.3

当发现一个系统**活动**与一个预示可能潜在违反 SFR 实施的特征事件**或事件序列**匹配时,TSF 应能指出潜在违反 SFR 实施的事件即将发生。

7.4 安全审计查阅(FAU_SAR)

7.4.1 族行为

本族定义了一些有关审计工具的要求,授权用户可使用这些审计工具查阅审计数据。

7.4.2 组件层次

FAU_SAR.1“审计查阅”,提供从审计记录中读取信息的能力。

FAU_SAR.2“限制审计查阅”,要求除在 FAU_SAR.1“审计查阅”中确定的用户外,其他用户不能读取信息。

FAU_SAR.3“可选审计查阅”,要求审计查阅工具根据标准来选择要查阅的审计数据。

7.4.3 FAU_SAR.1 管理

FMT 中的管理功能可考虑下列行为:

a) 维护(删除、修改、添加)对审计记录有读访问权的用户组。

7.4.4 FAU_SAR.2、FAU_SAR.3 管理

尚无预见的管理活动。

7.4.5 FAU_SAR.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 基本级:从审计记录中读取信息。

7.4.6 FAU_SAR.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 基本级:从审计记录中读取信息的未成功尝试。

7.4.7 FAU_SAR.3 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 详细级：用于查阅的参数。

7.4.8 FAU_SAR.1 审计查阅

从属于：无其他组件。

依赖关系：FAU_GEN.1 审计数据产生。

7.4.8.1 FAU_SAR.1.1

TSF 应为[赋值：*授权用户*]提供从审计记录中读取[赋值：*审计信息列表*]的能力。

7.4.8.2 FAU_SAR.1.2

TSF 应以便于用户理解的方式提供审计记录。

7.4.9 FAU_SAR.2 限制审计查阅

从属于：无其他组件。

依赖关系：FAU_SAR.1 审计查阅。

7.4.9.1 FAU_SAR.2.1

除明确准许读访问的用户外，TSF 应禁止所有用户对审计记录的读访问。

7.4.10 FAU_SAR.3 可选审计查阅

从属于：无其他组件。

依赖关系：FAU_SAR.1 审计查阅。

7.4.10.1 FAU_SAR.3.1

TSF 应根据[赋值：*具有逻辑关系的标准*]提供对审计数据进行[赋值：选择和/或排序的方法]的能力。

7.5 安全审计事件选择(FAU_SEL)

7.5.1 族行为

本族定义在 TOE 运行期间从所有审计事件集合中选取被审计事件的要求。

7.5.2 组件层次

FAU_SEL.1“选择性审计”，要求能够由 PP/ST 作者根据规定的属性从所有在“FAU_GEN.1 审计事件产生”组件中标识的审计事件集合中选取被审计事件。

7.5.3 FAU_SEL.1 管理

FMT 中的管理功能可考虑下列行为：

a) 维护查阅/修改审计事件的权限。

7.5.4 FAU_SEL.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：审计收集功能运行时，所有因审计配置修改而产生的事件。

7.5.5 FAU_SEL.1 选择性审计

从属于：无其他组件。

依赖关系：FAU_GEN.1 审计数据产生。

FMT_MTD.1 TSF 数据管理。

7.5.5.1 FAU_SEL.1.1

TSF 应能根据以下属性从所有审计事件集合中选择可审计事件：

a) [**选择：*客体身份*、*用户身份*、*主体身份*、*主机身份*、*事件类型***]；

b) [**赋值：*审计选择所依据的附加属性表***]。

7.6 安全审计事件存储(FAU_STG)

7.6.1 族行为

本族定义一些 TSF 能够创建并维护一个安全审计迹的要求。存储的审计记录是指在审计迹中的那些记录，而不是指经过选择操作后得到的临时存储的审计记录。

7.6.2 组件层次

FAU_STG.1“受保护的审计迹存储”，要求保护审计迹避免未授权的删除或修改。

FAU_STG.2“审计数据可用性保证”，规定保证假定意外情况出现时 TSF 还能维护审计数据。

FAU_STG.3“审计数据可能丢失时的行为”，规定当审计迹超出门限值时所采取的动作。

FAU_STG.4“防止审计数据丢失”，规定当审计迹满时所采取的动作。

7.6.3 FAU_STG.1 管理

尚无预见的管理活动。

7.6.4 FAU_STG.2 管理

FMT 中的管理功能可考虑下列行为：

a) 维护控制审计存储能力的参数。

7.6.5 FAU_STG.3 管理

FMT 中的管理功能可考虑下列行为：

a) 维护门限值；

b) 当审计存储即将失效时所应采取的维护(删除、修改、添加)的动作。

7.6.6 FAU_STG.4 管理

FMT 中的管理功能可考虑下列行为：

a) 维护(删除、修改、添加)审计存储失效时所采取的行动。

7.6.7 FAU_STG.1、FAU_STG.2 审计

尚无预见的可审计事件。

7.6.8 FAU_STG.3 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 基本级：因超过门限而采取的动作。

7.6.9 FAU_STG.4 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 基本级：因审计存储失效而采取的动作。

7.6.10 FAU_STG.1 受保护的审计迹存储

从属于：无其他组件。

依赖关系：FAU_GEN.1 审计数据产生。

7.6.10.1 FAU_STG.1.1

TSF 应保护审计迹中存储的审计记录，以避免未授权的删除。

7.6.10.2 FAU_STG.1.2

TSF 应能[选择，选取一个：*防止*、*检测*]对审计迹中所存审计记录的未授权修改。

7.6.11 FAU_STG.2 审计数据可用性保证

从属于：FAU_STG.1 受保护的审计迹存储。

依赖关系：FAU_GEN.1 审计数据产生。

7.6.11.1 FAU_STG.2.1

TSF 应保护审计迹中所存储的审计记录，以避免未授权的删除。

7.6.11.2 FAU_STG.2.2

TSF 应能[选择，选取一个：*防止*、*检测*]对审计迹中所存审计记录的未授权修改。

7.6.11.3 FAU_STG.2.3

当下列情况发生时：[选择：*审计存储耗尽*、*失效*、*受攻击*]，TSF 应确保[赋值：*保存审计记录的度量*]审计记录将维持有效。

7.6.12 FAU_STG.3 审计数据可能丢失时的行为

从属于：无其他组件。

依赖关系：FAU_STG.1 受保护的审计迹存储。

7.6.12.1 FAU_STG.3.1

如果审计迹超过[赋值：*预定的限度*]，TSF 应采取[赋值：*审计存储可能失效时所采取的行动*]。

7.6.13 FAU_STG.4 防止审计数据丢失

从属于:FAU_STG.3 审计数据可能丢失时的行为。

依赖关系:FAU_STG.1 受保护的审计迹存储。

7.6.13.1 FAU_STG.4.1

如果审计迹**已满**,**TSF** 应[**选择**,**选取一个**:***"忽略可审计事件"***、***"阻止可审计事件,具有特权的授权用户产生的事件除外"***,***"覆盖所存储的最早的审计记录"***]和[**赋值**:*审计存储失效时所采取的**其他动作***]。

8 FCO 类:通信

本类提供了两个族,特别关注如何确认在数据交换中参与方的身份。这些族与确认信息传送的原发者身份(原发证明)和确认信息传送的接收者身份(接收证明)相关。这些族确保原发者不能否认发送过信息,接收者也不能否认收到过信息。本类的组件构成分解如图 8 所示。

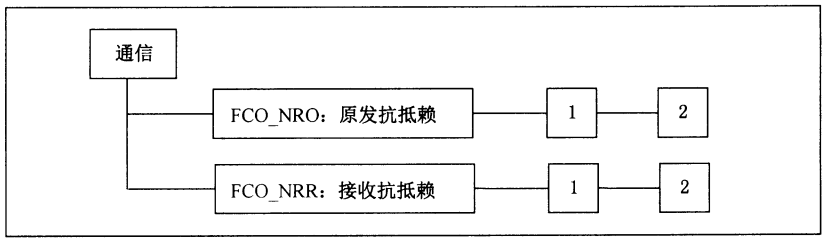

图 8 FCO:通信类分解

8.1 原发抗抵赖(FCO_NRO)

8.1.1 族行为

原发抗抵赖确保信息的发起者不能成功地否认曾经发送过信息。本族要求 TSF 提供一种方法来确保接收信息的主体在数据交换期间获得了证明信息原发的证据,此证据可由该主体或其他主体验证。

8.1.2 组件层次

FCO_NRO.1"选择性原发证明",要求 TSF 为主体提供请求信息原发证据的能力。

FCO_NRO.2"强制性原发证明",要求 TSF 总是为所传送的信息产生原发证据。

8.1.3 FCO_NRO.1、FCO_NRO.2 管理

FMT 中的管理功能可考虑下列行为:

a) 对改变信息类型、域、原发者属性和证据接收者的管理。

8.1.4 FCO_NRO.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:请求产生原发证据的用户的身份;

b) 最小级:抗抵赖服务的调用;

c) 基本级:信息的标识、目的地和所提供的证据副本;

d) 详细级:请求验证证据的用户的身份。

8.1.5 FCO_NRO.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:抗抵赖服务的调用;

b) 基本级:信息的标识、目的地和所提供的证据副本;

c) 详细级:请求验证证据的用户的身份。

8.1.6 FCO_NRO.1 选择性原发证明

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

8.1.6.1 FCO_NRO.1.1

在[选择:*原发者*、*接收者*或[*赋值:第三方列表*]]请求时,TSF 应能对所传送的[赋值:*信息类型列表*]产生原发证据。

8.1.6.2 FCO_NRO.1.2

TSF 应能将信息原发者的[赋值:*属性列表*]和信息的[赋值:*信息域列表*]与证据相关联。

8.1.6.3 FCO_NRO.1.3

给定[赋值:*原发证据的限制条件*],TSF 应能为[选择:*原发者*、*接收者*或[*赋值:第三方列表*]]提供验证信息原发证据的能力。

8.1.7 FCO_NRO.2 强制性原发证明

从属于:FCO_NRO.1 选择性原发证明。

依赖关系:FIA_UID.1 标识的时机。

8.1.7.1 FCO_NRO.2.1

TSF 在**任何时候**都应对所传送的[赋值:*信息类型列表*]**强制产生**原发证据。

8.1.7.2 FCO_NRO.2.2

TSF 应能将信息原发者的[赋值:*属性列表*]和信息的[赋值:*信息域列表*]与证据相关联。

8.1.7.3 FCO_NRO.2.3

给定[赋值:*原发证据的限制条件*],TSF 应能为[选择:*原发者*、*接收者*,[*赋值:第三方列表*]]提供验证信息原发证据的能力。

8.2 接收抗抵赖(FCO_NRR)

8.2.1 族行为

接收抗抵赖确保信息的接收者不能成功地否认对信息的接收。本族要求 TSF 提供一种方法来确保发送信息的主体在数据交换期间获得了证明信息接收的证据,此证据可由该主体或其他主体验证。

8.2.2 组件层次

FCO_NRR.1“选择性接收证明”,要求 TSF 为主体提供请求信息接收证据的能力。

FCO_NRR.2“强制性接收证明”,要求 TSF 总是为接收到的信息产生接收证据。

8.2.3 FCO_NRR.1、FCO_NRR.2 管理

FMT 中的管理功能可考虑下列行为:

a) 对改变信息类型、域、原发者属性和证据的第三方接收者的管理。

8.2.4 FCO_NRR.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:请求产生提供接收证据的用户的身份;

b) 最小级:抗抵赖服务的调用;

c) 基本级:信息的标识、目的地和所提供的证据副本;

d) 详细级:请求验证证据的用户的身份。

8.2.5 FCO_NRR.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:抗抵赖服务的调用;

b) 基本级:信息的标识、目的地和所提供的证据副本;

c) 详细级:请求验证证据的用户的身份。

8.2.6 FCO_NRR.1 选择性接收证明

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

8.2.6.1 FCO_NRR.1.1

在[选择:*原发者*、*接收者*或[*赋值:第三方列表*]]请求时,TSF 应能对接收到的[赋值:*信息类型表*]产生接收证据。

8.2.6.2 FCO_NRR.1.2

TSF 应能将信息接收者的[赋值:*属性列表*]和信息的[赋值:*信息域列表*]与证据相关联。

8.2.6.3 FCO_NRR.1.3

给定[赋值:*接收证据的限制条件*],TSF 应能为[选择:*原发者*、*接收者*或[*赋值:第三方列表*]]提供验证信息接收证据的能力。

8.2.7 FCO_NRR.2 强制性接收证明

从属于:FCO_NRR.1 选择性接收证明。

依赖关系:FIA_UID.1 标识的时机。

8.2.7.1 FCO_NRR.2.1

TSF 在**任何时候**都应对接收到的[赋值:*信息类型表*]**强制产生**接收证据。

8.2.7.2 FCO_NRR.2.2

TSF 应能将信息接收者的[赋值:*属性列表*]和信息的[赋值:*信息域列表*]与证据相关联。

8.2.7.3 FCO_NRR.2.3

给定[赋值:*接收证据的限制条件*],TSF 应能为[选择:*原发者、接收者或*[赋值:*第三方列表*]]提供验证信息接收证据的能力。

9 FCS 类:密码支持

TSF 可以利用密码功能来满足几个高级别安全目的。这些安全目的包括(但不限于):标识和鉴别、抗抵赖、可信路径、可信信道和数据分离。在 TOE 实现密码功能时使用本类,这种密码功能的实现形式可以是硬件、固件和/或软件。

FCS"密码支持类"由两个族组成:FCS_CKM"密钥管理"和 FCS_COP"密码运算"。密钥管理(FCS_CKM)族解决密钥管理方面的问题,而密码运算(FCS_COP)族关注这些密钥的运算使用情况。本类的组件构成分解如图 9 所示。

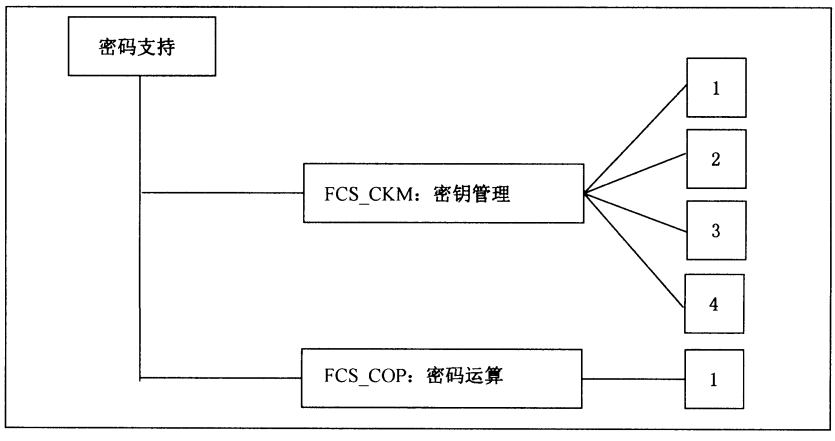

图 9 FCS:密码支持类分解

9.1 密钥管理(FCS_CKM)

9.1.1 族行为

密钥在其整个生命期内都必须进行管理。本族试图支持此生命期,并为此定义了对以下几种操作的要求:密钥生成、密钥分发、密钥存取和密钥销毁。只要存在密钥管理的功能要求,都必须包含本族。

9.1.2 组件层次

FCS_CKM.1"密钥生成",要求根据某个指定标准规定的算法和密钥长度来生成密钥。
FCS_CKM.2"密钥分发",要求根据某个指定标准规定的分发方法来分发密钥。
FCS_CKM.3"密钥存取",要求根据某个指定标准规定的存取方法来存取密钥。
FCS_CKM.4"密钥销毁",要求根据某个指定标准规定的销毁方法来销毁密钥。

9.1.3 FCS_CKM.1、FCS_CKM.2、FCS_CKM.3、FCS_CKM.4 管理

无可预见的管理行为。

9.1.4 FCS_CKM.1、FCS_CKM.2、FCS_CKM.3、FCS_CKM.4 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：操作的成功和失败；

b) 基本级：除任何敏感信息（如秘密密钥或私有密钥）以外的客体属性和客体值。

9.1.5 FCS_CKM.1 密钥生成

从属于：无其他组件。

依赖关系：[FCS_CKM.2 密钥分发，或
FCS_COP.1 密码运算]；
FCS_CKM.4 密钥销毁。

9.1.5.1 FCS_CKM.1.1

TSF 应根据符合下列标准[赋值：*标准列表*]的一个特定的密钥生成算法[赋值：*密钥生成算法*]和规定的密钥长度[赋值：*密钥长度*]来生成密钥。

9.1.6 FCS_CKM.2 密钥分发

从属于：无其他组件。

依赖关系：[FDP_ITC.1 不带安全属性的用户数据输入，或
FDP_ITC.2 带有安全属性的用户数据输入，或
FCS_CKM.1 密钥生成]；
FCS_CKM.4 密钥销毁。

9.1.6.1 FCS_CKM.2.1

TSF 应根据符合下列标准[赋值：*标准列表*]的一个特定的密钥分发方法[赋值：*密钥分发方法*]来分发密钥。

9.1.7 FCS_CKM.3 密钥存取

从属于：无其他组件。

依赖关系：[FDP_ITC.1 不带安全属性的用户数据输入，或
FDP_ITC.2 带有安全属性的用户数据输入，或
FCS_CKM.1 密钥生成]；
FCS_CKM.4 密钥销毁。

9.1.7.1 FCS_CKM.3.1

TSF 应根据符合下列标准[赋值：*标准列表*]的一个特定的密钥存取方法[赋值：*密钥存取方法*]来执行[赋值：*密钥存取类型*]。

9.1.8 FCS_CKM.4 密钥销毁

从属于：无其他组件。

依赖关系：[FDP_ITC.1 不带安全属性的用户数据输入，或
FDP_ITC.2 带有安全属性的用户数据输入，或
FCS_CKM.1 密钥生成]。

9.1.8.1 FCS_CKM.4.1

TSF 应根据符合下列标准[赋值:*标准列表*]的一个特定的密钥销毁方法[赋值:*密钥销毁方法*]来销毁密钥。

9.2 密码运算(FCS_COP)

9.2.1 族行为

为了确保密码运算功能的正确执行,必须按照特定的算法和规定长度的密钥来进行运算。凡有执行密码运算要求的地方,都必须包含本族。

密码运算通常包括:数据加密或解密、数字签名产生或验证、密码校验和(用于完整性或校验和验证)产生、安全散列(消息摘要)、密钥加密或解密,以及密钥协商。

9.2.2 组件层次

FCS_COP.1"密码运算",要求根据特定的算法和规定长度的密钥来进行密码运算。可以基于某个指定标准规定算法和密钥长度。

9.2.3 FCS_COP.1 管理

尚无预见的管理活动。

9.2.4 FCS_COP.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:成功和失败,以及密码运算的类型;

b) 基本级:所有有效的密码运算模式、主体属性和客体属性。

9.2.5 FCS_COP.1 密码运算

从属于:无其他组件。

依赖关系:[FDP_ITC.1 不带安全属性的用户数据输入,或
FDP_ITC.2 带有安全属性的用户数据输入,或
FCS_CKM.1 密钥生成];
FCS_CKM.4 密钥销毁。

9.2.5.1 FCS_COP.1.1

TSF 应根据符合下列标准[赋值:*标准列表*]的特定的密码算法[赋值:*密码算法*]和密钥长度[赋值:*密钥长度*]来执行[赋值:*密码运算列表*]。

10 FDP 类:用户数据保护

本类包含的族详细说明了与用户数据保护相关的要求。FDP"用户数据保护"分为四组族(如下所示)来描述在输入、输出和存储过程中的 TOE 内部的用户数据,以及与用户数据直接相关的安全属性。本类的组件构成分解如图 10 所示。

本类中的族可分成如下4组：

a) 用户数据保护安全功能策略：
   - FDP_ACC 访问控制策略；
   - FDP_IFC 信息流控制策略。

   这些族中的组件允许PP/ST作者命名用户数据保护安全功能策略，并定义该安全策略的控制范围，这对于说明安全目的是必要的。这些安全策略的名称将在其他有要求对“访问控制SFP”、“信息流控制SFP”赋值或选择操作的功能组件中广泛使用。定义已命名访问控制和信息流控制SFP功能性的规则将分别在FDP_ACF“访问控制功能”和FDP_IFF“信息流控制功能”族中定义。

b) 用户数据保护形式：
   - FDP_ACF 访问控制功能；
   - FDP_IFF 信息流控制功能；
   - FDP_ITT TOE内部传送；
   - FDP_RIP 残余信息保护；
   - FDP_ROL 回退；
   - FDP_SDI 存储数据的完整性。

c) 离线存储、输入和输出：
   - FDP_DAU 数据鉴别；
   - FDP_ETC 从TOE输出；
   - FDP_ITC 从TOE之外输入。

   这些族内的组件负责处理进出TOE的可信传送。

d) TSF间的通信：
   - FDP_UCT TSF间用户数据机密性传送保护；
   - FDP_UIT TSF间用户数据完整性传送保护。

   这些族内的组件负责处理TOE的TSF与其他可信IT产品间的通信。

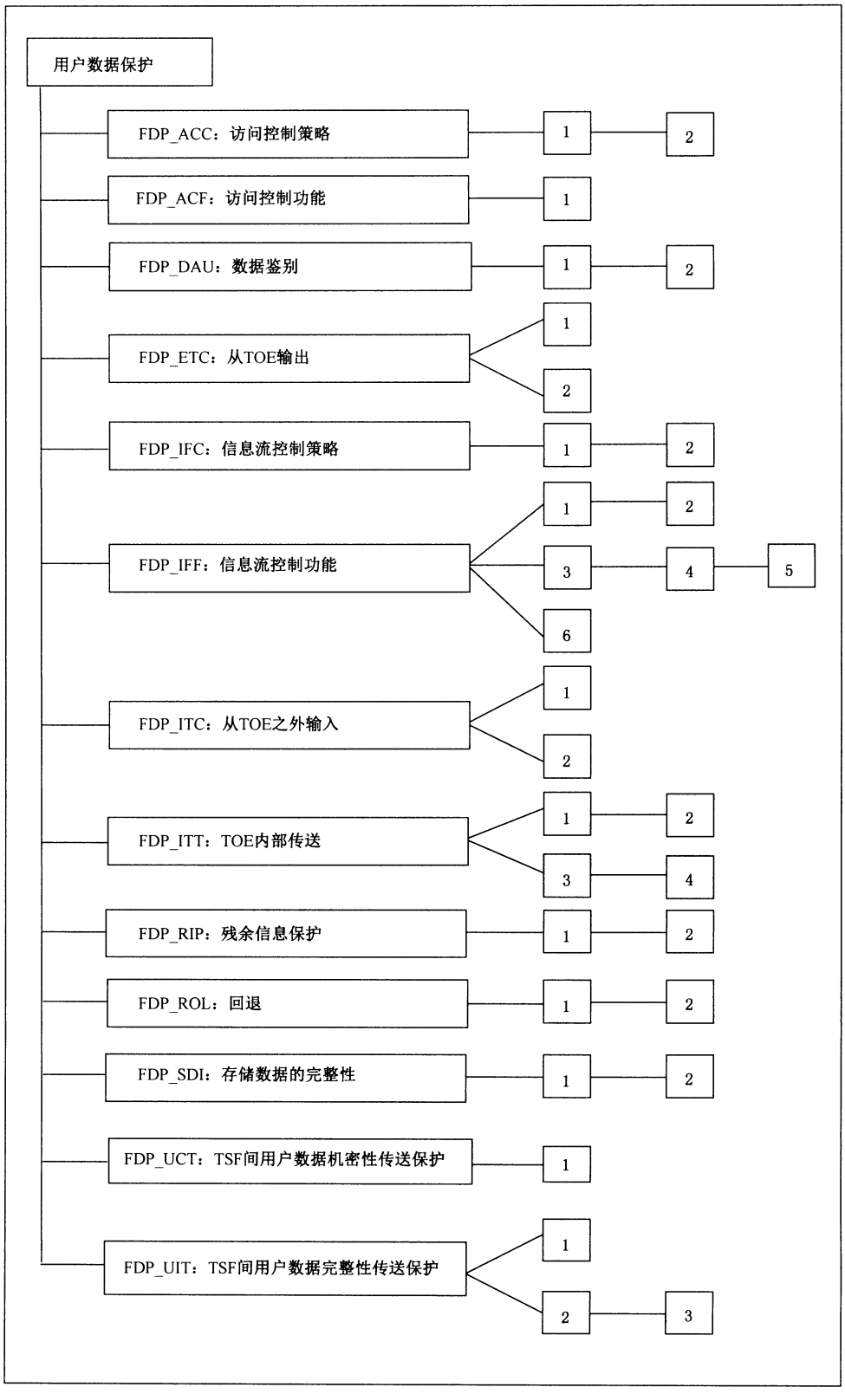

图 10　FDP：用户数据保护类分解

10.1 访问控制策略(FDP_ACC)

10.1.1 族行为

本族(通过命名)标识访问控制 SFP 并定义策略的控制范围,这些策略组成了既定 SFR 的访问控制部分。控制范围由以下三个集合刻画:策略控制下的主体、策略控制下的客体以及策略所涵盖受控主体和受控客体间的操作。本准则允许存在多个策略,只是每个策略需要有唯一的名称,这可以通过对每个已命名的访问控制策略反复使用本族中的组件来实现。定义访问控制 SFP 功能的规则将在其他族中定义,如 FDP_ACF"访问控制功能"和 FDP_ETC"从 TOE 输出"。在 FDP_ACC"访问控制策略"中所确定的访问控制 SFP 的名称,将用在其余所有需要对"访问控制 SFP"赋值或选择操作的功能组件中。

10.1.2 组件层次

FDP_ACC.1"子集访问控制",要求每个确定的访问控制 SFP 适用于对某个 TOE 客体子集可能执行的操作子集。

FDP_ACC.2"完全访问控制",要求每个确定的访问控制 SFP 涵盖被该 SFP 涵盖的主体和客体之间的所有操作,进而要求由 TSF 保护的所有客体和操作都至少被一个确定的访问控制 SFP 涵盖。

10.1.3 FDP_ACC.1、FDP_ACC.2 管理

尚无预见的管理活动。

10.1.4 FDP_ACC.1、FDP_ACC.2 审计

尚无预见的可审计事件。

10.1.5 FDP_ACC.1 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1 基于安全属性的访问控制。

10.1.5.1 FDP_ACC.1.1

TSF 应对[赋值:*主体、客体及 SFP 所涵盖主体和客体之间的操作列表*]执行[赋值:*访问控制 SFP*]。

10.1.6 FDP_ACC.2 完全访问控制

从属于:FDP_ACC.1 子集访问控制。

依赖关系:FDP_ACF.1 基于安全属性的访问控制。

10.1.6.1 FDP_ACC.2.1

TSF 应对[赋值:主体和客体列表]及 **SFP** 所涵盖主体和客体之间的**所有**操作执行[赋值:访问控制 SFP]。

10.1.6.2 FDP_ACC.2.2

TSF 应确保 TSF 控制内的任何主体和客体之间的所有操作都被一个访问控制 SFP 涵盖。

10.2 访问控制功能(FDP_ACF)

10.2.1 族行为

本族描述了与特定功能相关的规则,这些特定功能可实现在 FDP_ACC"访问控制策略"中所命名的访问控制策略。FDP_ACC"访问控制策略"规定了策略控制的范围。

10.2.2 组件层次

本族说明安全属性的用法和策略的特征。本族中的组件将用来描述实施 SFP 的功能的一些规则,该 SFP 由 FDP_ACC"访问控制策略"确定。PP/ST 作者可以反复使用本组件以说明 TOE 中的多个策略。

FDP_ACF.1"基于安全属性的访问控制",允许 TSF 基于安全属性和已命名属性组的执行访问。此外,TSF 有能力根据安全属性明确地授权或拒绝对某个客体的访问。

10.2.3 FDP_ACF.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理用于作出明确访问或拒绝决定的属性。

10.2.4 FDP_ACF.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:对 SFP 涵盖的客体执行某个操作的成功请求;

b) 基本级:对 SFP 涵盖的客体执行某个操作的所有请求;

c) 详细级:用于进行访问检查的特定安全属性。

10.2.5 FDP_ACF.1 基于安全属性的访问控制

从属于:无其他组件。

依赖关系:FDP_ACC.1 子集访问控制;

FMT_MSA.3 静态属性初始化。

10.2.5.1 FDP_ACF.1.1

TSF 应基于[赋值:*指定 SFP 控制下的主体和客体列表,以及每个与 SFP 的相关安全属性或与 SFP 相关的已命名安全属性组*]对客体执行[赋值:*访问控制 SFP*]。

10.2.5.2 FDP_ACF.1.2

TSF 应执行以下规则,以确定在受控主体与受控客体间的一个操作是否被允许:[赋值:*在受控主体和受控客体间,通过对受控客体采取受控操作来管理访问的一些规则*]。

10.2.5.3 FDP_ACF.1.3

TSF 应基于以下附加规则:[赋值:*基于安全属性的,明确授权主体访问客体的规则*],明确授权主体访问客体。

10.2.5.4 FDP_ACF.1.4

TSF 应基于[赋值:*基于安全属性的,明确拒绝主体访问客体的规则*]明确拒绝主体访问客体。

10.3 数据鉴别(FDP_DAU)

10.3.1 族行为

数据鉴别允许实体为信息的真实性承担责任(如对它进行数字签名)。本族提供一种方法,以保证特定数据单元的有效性,进而可用于验证信息内容没有被伪造或篡改。与FAU“安全审计”类不同,本族适用于“静态”数据而不是正在传送的数据。

10.3.2 组件层次

FDP_DAU.1“基本数据鉴别”,要求TSF具有为客体(如文档)信息内容的真实性提供保证的能力。

FDP_DAU.2“带担保者身份的数据鉴别”,还另外要求TSF具有建立为提供真实性担保的主体身份的能力。

10.3.3 FDP_DAU.1、FDP_DAU.2 管理

FMT中的管理功能可考虑下列行为:

a) 适用于数据鉴别的客体的赋值或修改应是可配置的。

10.3.4 FDP_DAU.1 审计

如果PP/ST中包含FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:有效性证据的成功生成;

b) 基本级:有效性证据的未成功生成;

c) 详细级:请求证据的主体身份。

10.3.5 FDP_DAU.2 审计

如果PP/ST中包含FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:有效性证据的成功生成;

b) 基本级:有效性证据的未成功生成;

c) 详细级:请求证据的主体身份;

d) 详细级:产生证据的主体身份。

10.3.6 FDP_DAU.1 基本数据鉴别

从属于:无其他组件。

依赖关系:无依赖关系。

10.3.6.1 FDP_DAU.1.1

TSF应提供一种能力,以生成能用来作为[赋值:*客体或信息类型列表*]有效性担保的证据。

10.3.6.2 FDP_DAU.1.2

TSF应为[赋值:*主体列表*]提供能力,以验证指定信息有效的证据。

10.3.7 FDP_DAU.2 带担保者身份的数据鉴别

从属于:FDP_DAU.1 基本数据鉴别。

依赖关系:FIA_UID.1 标识的时机。

10.3.7.1 **FDP_DAU.2.1**

TSF 应提供一种能力，以生成能用来作为[赋值：*客体或信息类型列表*]有效性担保的证据。

10.3.7.2 **FDP_DAU.2.2**

TSF 应为[赋值：*主体列表*]提供一种能力，以验证所指定信息的有效性证据**和产生证据的用户身份**。

10.4 从 TOE 输出(FDP_ETC)

10.4.1 族行为

本族定义了由 TSF 促成的从 TOE 输出用户数据的功能，一旦数据被输出，其安全属性和保护机制不是被明确保留，就是被忽略。这涉及对输出的限制，以及安全属性与所输出用户数据之间的关联关系。

10.4.2 组件层次

FDP_ETC.1 “不带安全属性的用户数据输出”，要求 TSF 在把用户数据输出到 TSF 之外时执行合适的 SFP。经由本功能输出的用户数据输出时没有输出相关的安全属性。

FDP_ETC.2 “带有安全属性的用户数据输出”，要求 TSF 利用一个功能执行合适的 SFP，该功能准确无误地将安全属性与所输出的用户数据相关联。

10.4.3 FDP_ETC.1 管理

尚无预见的管理活动。

10.4.4 FDP_ETC.2 管理

FMT 中的管理功能可考虑下列行为：

a) 已定义角色中的一个用户能够配置的附加输出控制规则。

10.4.5 审计：FDP_ETC.1，FDP_ETC.2

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：信息的成功输出；

b) 基本级：输出信息的所有尝试。

10.4.6 FDP_ETC.1 不带安全属性的用户数据输出

从属于：无其他组件。

依赖关系：[FDP_ACC.1 子集访问控制，或
FDP_IFC.1 子集信息流控制]。

10.4.6.1 **FDP_ETC.1.1**

在 SFP 控制下将用户数据输出到 TOE 之外时，TSF 应执行[**赋值：*访问控制 SFP 和/或信息流控制 SFP***]。

10.4.6.2 **FDP_ETC.1.2**

TSF 应输出用户数据但不带用户数据关联的安全属性。

10.4.7 FDP_ETC.2 带有安全属性的用户数据输出

从属于:无其他组件。

依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制]。

10.4.7.1 FDP_ETC.2.1

在 SFP 控制下将用户数据输出到 TOE 之外时,TSF 应执行[赋值:*访问控制 SFP 和/或信息流控制 SFP*]。

10.4.7.2 FDP_ETC.2.2

TSF 应输出用户数据且带有用户数据关联的安全属性。

10.4.7.3 FDP_ETC.2.3

TSF 应确保输出安全属性到 TOE 之外时,与所输出的用户数据确切关联。

10.4.7.4 FDP_ETC.2.4

当从 TOE 输出用户数据时,TSF 应执行下列规则[赋值:*附加的输出控制规则*]。

10.5 信息流控制策略(FDP_IFC)

10.5.1 族行为

本族标识信息流控制 SFP(通过命名),并为每个已命名的策略定义了控制范围,这些策略组成了既定 TSP 的信息流控制部分。控制范围由以下 3 个集合刻画:策略控制下的主体、策略控制下的信息以及策略所涵盖的引起受控信息流入、流出受控主体的操作。本准则允许存在多个策略,只是每个策略需要有一个唯一的名称,这可以通过对每个已命名的信息流控制策略反复使用本族中的组件来实现。定义信息流控制 SFP 功能的规则将在其他族中定义,如 FDP_IFF“信息流控制功能”和 FDP_ETC“从 TOE 输出”。在 FDP_IFC“信息流控制策略”中所确定的信息流控制 SFP 名称,将用在所有其余需要对“信息流控制 SFP”赋值或选择可操作的组件中。

TSF 机制根据信息流控制 SFP 控制信息的流向。一般不允许执行改变信息的安全属性的操作,因为这将违背信息流控制 SFP。不过,如果明确指明,这种操作也可以作为信息流控制 SFP 的例外,得到允许。

10.5.2 组件层次

FDP_IFC.1“子集信息流控制”,要求对 TOE 内的信息流子集可能执行的操作子集,有确定的信息流控制 SFP。

FDP_IFC.2“完全信息流控制”,要求每个确定的信息流控制 SFP 覆盖该 SFP 所涵盖主体和信息之间的所有操作,并进一步要求由 TSF 控制的所有信息流和操作都至少被一个确定的信息流控制 SFP 覆盖。

10.5.3 FDP_IFC.1、FDP_IFC.2 管理

尚无预见的管理活动。

10.5.4 FDP_IFC.1、FDP_IFC.2 审计

尚无预见的可审计事件。

10.5.5 FDP_IFC.1 子集信息流控制

从属于:无其他组件。

依赖关系:FDP_IFF.1 简单安全属性。

10.5.5.1 FDP_IFC.1.1

TSF 应对[赋值:*主体、信息及 SFP 所覆盖的导致受控信息流入、流出受控主体的操作列表*]执行[赋值:*信息流控制 SFP*]。

10.5.6 FDP_IFC.2 完全信息流控制

从属于:FDP_IFC.1 子集信息流控制。

依赖关系:FDP_IFF.1 简单安全属性。

10.5.6.1 FDP_IFC.2.1

TSF 应对[赋值:*主体列表和信息列表*]及 SFP 所覆盖的导致信息流入、流出主体的**所有操作**执行[赋值:*信息流控制 SFP*]。

10.5.6.2 FDP_IFC.2.2

TSF 应确保导致 TOE 中的任何信息从 TOE 中的任何主体流入、流出的所有操作都被一个信息流控制 SFP 覆盖。

10.6 信息流控制功能(FDP_IFF)

10.6.1 族行为

本族描述了 FDP_IFC“信息流控制策略”中实现已命名的信息流控制 SFP 的特定功能的一些规则,并规定策略控制的范围。本族中包含两种要求:一种是针对通用的信息流功能问题,另一种是针对非法的信息流(如隐蔽信道)。之所以这样划分是因为非法信息流涉及的问题,在某种意义上与其他的信息流控制 SFP 是完全不相干的。非法信息流的本质就是为了规避信息流控制 SFP,导致策略失效,因而需要特定的功能限制或防止非法信息流的出现。

10.6.2 组件层次

FDP_IFF.1“简单安全属性”,对信息的安全属性、导致信息流动的主体的安全属性以及作为信息接收者的主体的安全属性提出了要求。它规定了功能必须执行的一些规则,并描述该功能如何得到安全属性。

FDP_IFF.2“分级安全属性”,扩展了 FDP_IFF.1“简单安全属性”的要求,要求 SFRs 中所有信息流控制 SFP 使用格结构的(遵从数学上的定义)分级安全属性。FDP_IFF.2.6 来自格的数学属性。格是由一个元素集合及在该集合上定义的有序关系组成的数学结构,该关系由 FDP_IFF.2.6 的第一点要求定义;格中存在一个唯一的最大下界元素,(按有序关系来说)它大于或等于格中其他下界元素;并存在一个唯一的最小上界元素,它小于或等于格中其他上界元素。

FDP_IFF.3“受限的非法信息流”,要求 SFP 覆盖非法信息流,但不必消除它们。

FDP_IFF.4“部分消除非法信息流”,要求 SFP 覆盖部分(不必是全部)非法信息流的消除。

FDP_IFF.5“无非法信息流”,要求 SFP 覆盖所有非法信息流的消除。

FDP_IFF.6“非法信息流监视”,要求 SFP 针对指定的最大流量监视非法信息流。

10.6.3 FDP_IFF.1、FDP_IFF.2 管理

FMT 中的管理功能可考虑下列行为:

a) 管理用于作出明确访问决定的属性。

10.6.4 FDP_IFF.3、FDP_IFF.4、FDP_IFF.5 管理

尚无预见的管理活动。

10.6.5 FDP_IFF.6 管理

FMT 中的管理功能可考虑下列行为:

a) 监视功能的启动或关闭;

b) 监视时最大流量的修改。

10.6.6 FDP_IFF.1、FDP_IFF.2、FDP_IFF.5 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:允许请求的信息流动的决定;

b) 基本级:请求信息流动的所有决定;

c) 详细级:用于做出信息流动执行决定的特定安全属性;

d) 详细级:根据策略目标(如降级材料的审计)而流动的信息的某些特定子集。

10.6.7 FDP_IFF.3、FDP_IFF.4、FDP_IFF.6 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:允许请求的信息流动的决定;

b) 基本级:请求信息流动的所有决定;

c) 基本级:确定的非法信息流信道的使用;

d) 详细级:用于做出信息流动执行决定的特定安全属性;

e) 详细级:根据策略目标(如降级材料的审计)而流动的信息的某些特定子集;

f) 详细级:估算的最大容量超过一个特定值的已标识非法信息流信道的使用。

10.6.8 FDP_IFF.1 简单安全属性

从属于:无其他组件。

依赖关系:FDP_IFC.1 子集信息流控制;

FMT_MSA.3 静态属性初始化。

10.6.8.1 FDP_IFF.1.1

TSF 应基于下列类型主体和信息的安全属性:[赋值:*指定 SFP 控制下的主体和信息列表,以及每个对应的安全属性*]执行[赋值:*信息流控制 SFP*]。

10.6.8.2 FDP_IFF.1.2

**如果支持下列规则:[赋值:*对每一个操作,必须在主体和信息的安全属性之间成立的基于安全属*

性的关系],TSF 应允许信息在受控主体和受控信息之间经由受控操作流动。

10.6.8.3 **FDP_IFF.1.3**

TSF 应执行[**赋值**:***附加的信息流控制 SFP 规则***]。

10.6.8.4 **FDP_IFF.1.4**

TSF 应根据下列规则:[**赋值**:***基于安全属性,明确批准信息流的规则***]**明确批准一个信息流。**

10.6.8.5 **FDP_IFF.1.5**

TSF 应根据下列规则:[**赋值**:***基于安全属性,明确拒绝信息流的规则***]**明确拒绝一个信息流。**

10.6.9 **FDP_IFF.2 分级安全属性**

从属于:FDP_IFF.1 简单安全属性。

依赖关系:FDP_IFC.1 子集信息流控制;

FMT_MSA.3 静态属性初始化。

10.6.9.1 **FDP_IFF.2.1**

TSF 应基于下列类型主体和信息的安全属性:[赋值:*指定* ***SFP*** *控制下的主体和信息列表,以及每个对应的安全属性*]执行[赋值:*信息流控制 SFP*]。

10.6.9.2 **FDP_IFF.2.2**

如果**基于安全属性间的有序关系**支持下列的规则[赋值:*对每一个操作,****必须在主体和信息的安全属性之间成立的基于安全属性的关系***],TSF 应允许信息在受控主体和受控信息之间经由受控操作流动。

10.6.9.3 **FDP_IFF.2.3**

TSF 应执行[赋值:*附加的信息流控制 SFP 规则*]。

10.6.9.4 **FDP_IFF.2.4**

TSF 应根据下列规则:[赋值:*基于安全属性,明确批准信息流的规则*]明确批准一个信息流。

10.6.9.5 **FDP_IFF.2.5**

TSF 应根据下列规则:[赋值:*基于安全属性,明确拒绝信息流的规则*]明确拒绝一个信息流。

10.6.9.6 **FDP_IFF.2.6**

TSF 应对任意两个有效的信息流控制安全属性执行下列关系:

a) **存在一个排序函数,即给定两个有效的安全属性,确定它们是否相等,是否其中一个大于另一个,或两者不可比较;**

b) **在安全属性集合中存在一个"最小上界",也就是说,给定任意两个有效的安全属性,存在一个有效的安全属性大于或等于这两个安全属性;**

c) **在安全属性集合中存在一个"最大下界",也就是说,给定任意两个有效的安全属性,存在一个有效的安全属性不大于这两个安全属性。**

10.6.10 FDP_IFF.3 受限的非法信息流

从属于:无其他组件。

依赖关系:FDP_IFC.1 子集信息流控制。

10.6.10.1 FDP_IFF.3.1

TSF 应执行[赋值:*信息流控制 SFP*],以限制[赋值:*非法信息流的类型*]的容量,不超过[赋值:*最大容量*]。

10.6.11 FDP_IFF.4 部分消除非法信息流

从属于:FDP_IFF.3 受限的非法信息流。

依赖关系:FDP_IFC.1 子集信息流控制。

10.6.11.1 FDP_IFF.4.1

TSF 应执行[赋值:*信息流控制 SFP*],以限制[赋值:*非法信息流的类型*]的容量,不超过[赋值:*最大容量*]。

10.6.11.2 FDP_IFF.4.2

TSF 应阻止[赋值:*非法信息流的类型*]。

10.6.12 FDP_IFF.5 无非法信息流

从属于:FDP_IFF.4 部分消除非法信息流。

依赖关系:FDP_IFC.1 子集信息流控制。

10.6.12.1 FDP_IFF.5.1

TSF 应确保不存在规避[赋值:*信息流控制 SFP 名称*]的非法信息流。

10.6.13 FDP_IFF.6 非法信息流监视

从属于:无其他组件。

依赖关系:FDP_IFC.1 子集信息流控制。

10.6.13.1 FDP_IFF.6.1

TSF 应执行[赋值:*信息流控制 SFP*],以监视[赋值:*非法信息流的类型*]何时超过了[赋值:*最大容量*]。

10.7 从 TOE 之外输入(FDP_ITC)

10.7.1 族行为

本族定义通过 TSF 将用户数据输入到 TOE 内的机制,如此这样数据才具有合适的安全属性并得到适当的保护。这和数据输入限制、期望安全属性的确定,以及用户数据相关安全属性的解释有关。

10.7.2 组件层次

FDP_ITC.1“不带安全属性的用户数据输入”,要求安全属性正确表示用户数据,且与客体分离。

FDP_ITC.2“带有安全属性的用户数据输入”，要求安全属性正确表示用户数据，并且准确无误地与从 TOE 外输入的用户数据相关联。

10.7.3 FDP_ITC.1、FDP_ITC.2 管理

FMT 中的管理功能可考虑下列行为：

a) 对用于输入的附加控制规则的修改。

10.7.4 FDP_ITC.1、FDP_ITC.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：用户数据的成功输入，包括任何安全属性；

b) 基本级：用户数据的所有输入尝试，包括任何安全属性；

c) 详细级：授权用户提供的用于输入的用户数据的安全属性规范。

10.7.5 FDP_ITC.1 不带安全属性的用户数据输入

从属于：无其他组件。

依赖关系：[FDP_ACC.1 子集访问控制，或
FDP_IFC.1 子集信息流控制]；
FMT_MSA.3 静态属性初始化。

10.7.5.1 FDP_ITC.1.1

在 SFP 控制下从 TOE 之外输入用户数据时，TSF 应执行[赋值：*访问控制 SFP 和/或信息流控制 SFP*]。

10.7.5.2 FDP_ITC.1.2

从 TOE 外部输入用户数据时，TSF 应忽略任何与用户数据相关的安全属性。

10.7.5.3 FDP_ITC.1.3

在 SPF 控制下从 TOE 之外输入用户数据时，TSF 应执行下面的规则：[赋值：*附加的输入控制规则*]。

10.7.6 FDP_ITC.2 带有安全属性的用户数据输入

从属于：无其他组件。

依赖关系：[FDP_ACC.1 子集访问控制，或
FDP_IFC.1 子集信息流控制]；
[FDP_ITC.1 TSF 间的可信信道，或
FTP_TRP.1 可信路径]；
FPT_TDC.1 TSF 间基本的 TSF 数据一致性。

10.7.6.1 FDP_ITC.2.1

在 SFP 控制下从 TOE 之外输入用户数据时，TSF 应执行[赋值：*访问控制 SFP 和/或信息流控制 SFP*]。

10.7.6.2 FDP_ITC.2.2

TSF 应使用与所输入数据相关的安全属性。

10.7.6.3 FDP_ITC.2.3

TSF 应确保所使用的协议在安全属性和接收到的用户数据之间进行了明确的关联。

10.7.6.4 FDP_ITC.2.4

TSF 应确保对所输入用户数据的安全属性的解释与用户源数据所预期的安全属性是一样的。

10.7.6.5 FDP_ITC.2.5

当在 SFP 控制下从 TOE 之外输入用户数据时，TSF 应执行[赋值：*附加的输入控制规则*]。

10.8 TOE 内部传送(FDP_ITT)

10.8.1 族行为

本族提供当用户数据通过内部信道在 TOE 各部分之间传送时，对数据进行保护的要求。本族与族 FDP_UCT“TSF 间用户数据机密性传送保护”和 FDP_UIT“TSF 间用户数据完整性传送保护”的不同之处在于，后两者为用户数据经外部信道在不同的 TSF 间传送时提供保护；而与族 FDP_ETC“从 TOE 输出”和 FDP_ITC“从 TOE 之外输入”的不同之处则在于，它们处理由 TSF 仲裁的传送到 TOE 之外，或从 TOE 之外传入的数据保护问题。

10.8.2 组件层次

FDP_ITT.1“基本内部传送保护”，要求用户数据在 TOE 的各部分间传输时受保护。

FDP_ITT.2“按属性分隔传送”，除第一个组件的要求外，还要求基于 SFP 相关属性把数据分隔开。

FDP_ITT.3 “完整性监视”，要求 TSF 针对已标识的完整性错误，监视在 TOE 各部分间传递的用户数据。

FDP_ITT.4“基于属性的完整性监视”，允许完整性监视可根据 SFP 的相关属性进行设置，以此来扩展第 3 个组件的要求。

10.8.3 FDP_ITT.1、FDP_ITT.2 管理

FMT 中的管理功能可考虑下列行为：

a) 如果 TSF 提供了多种方法保护在 TOE 物理上分隔的部分间传递的用户数据，则 TSF 能提供一个预定义的角色，使其有能力选择将使用哪种方法。

10.8.4 FDP_ITT.3、FDP_ITT.4 管理

FMT 中的管理功能可考虑下列行为：

a) 对于检测到一个完整性错误而采取的行为规范应是可配置的。

10.8.5 FDP_ITT.1、FDP_ITT.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：用户数据的成功传送，包括所用保护方法的标识；

b) 基本级：用户数据传送的所有尝试，包括所用的保护方法和出现的任何错误。

10.8.6 FDP_ITT.3、FDP_ITT.4 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级:用户数据的成功传送,包括所用的完整性保护方法的标识;
b) 基本级:用户数据传送的所有尝试,包括所用的完整性保护方法和出现的任何错误;
c) 基本级:改变完整性保护方法的未授权尝试;
d) 详细级:检测到一个完整性错误而采取的行为。

10.8.7 FDP_ITT.1 基本内部传送保护

从属于:无其他组件。
依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制]。

10.8.7.1 FDP_ITT.1.1

在 TOE 物理上分隔的部分间传递用户数据时,TSF 应执行[赋值:*访问控制 SFP 和/或信息流控制 SFP*],以防止用户数据的[选择:*泄露、篡改、丧失可用性*]。

10.8.8 FDP_ITT.2 按属性分隔传送

从属于:FDP_ITT.1 基本内部传送保护。
依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制]。

10.8.8.1 FDP_ITT.2.1

在 TOE 物理上分隔的部分间传递用户数据时,TSF 应执行[赋值:*访问控制 SFP 和/或信息流控制 SFP*],以防止用户数据的[选择:*泄露、篡改、丧失可用性*]。

10.8.8.2 FDP_ITT.2.2

在 TOE 物理上分隔的部分间传递用户数据时,TSF 应基于下列值:[赋值:*需要分隔的安全属性*],将 SFP 控制的数据分隔开。

10.8.9 FDP_ITT.3 完整性监视

从属于:无其他组件。
依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制];
FDP_ITT.1 基本内部传送保护。

10.8.9.1 FDP_ITT.3.1

TSF 应执行[赋值:*访问控制 SFP 和/或信息流控制 SFP*],以监视用户数据在 TOE 物理上分隔的部分间传递时存在的下列错误:[赋值:*完整性错误*]。

10.8.9.2 FDP_ITT.3.2

检测到数据完整性错误时,TSF 应[赋值:*详细说明对完整性错误应采取的动作*]。

10.8.10 FDP_ITT.4 基于属性的完整性监视

从属于:FDP_ITT.3 完整性监视。
依赖关系:[FDP_ACC.1 子集访问控制,或

FDP_IFC.1 子集信息流控制]；
FDP_ITT.2 按属性分隔传送。

10.8.10.1 FDP_ITT.4.1

TSF 应**基于下列属性**：[**赋值**：**需要分隔传送信道的安全属性**]，执行[赋值：*访问控制 SFP 和/或信息流控制 SFP*]，以监视用户数据在 TOE 物理上分隔的部分间传递时存在的下列错误：[*赋值：完整性错误*]。

10.8.10.2 FDP_ITT.4.2

检测到数据完整性错误时，TSF 应[赋值：*详细说明对完整性错误应采取的动作*]。

10.9 残余信息保护(FDP_RIP)

10.9.1 族行为

本族需要确保当资源从一个客体释放并重新分配给另一个客体时，其中的任何数据都不可用。本族要求保护那些已逻辑上删除或释放但仍可能残存在 TSF 控制的资源中的数据，这些资源仍可能被重新分配给另一个客体。

10.9.2 组件层次

FDP_RIP.1“子集残余信息保护”，要求 TSF 确保任何资源的任何残余信息，在资源分配或释放时，对由 TSF 控制的已定义的客体子集而言都是不可用的。

FDP_RIP.2“完全残余信息保护”，要求 TSF 确保任何资源的任何残余信息，在资源分配或释放时，对于所有客体都是不可用的。

10.9.3 FDP_RIP.1、FDP_RIP.2 管理

FMT 中的管理功能可考虑下列行为：

a) 执行残余信息保护(即分配或释放)的时机选择在 TOE 内是可以配置的。

10.9.4 FDP_RIP.1、FDP_RIP.2 审计

尚无预见的可审计事件。

10.9.5 FDP_RIP.1 子集残余信息保护

从属于：无其他组件。

依赖关系：无依赖关系。

10.9.5.1 FDP_RIP.1.1

TSF 应确保一个资源的任何先前信息内容，在[**选择**：***分配资源到、释放资源自***]**下列客体**：[**赋值**：***客体列表***]**时不再可用**。

10.9.6 FDP_RIP.2 完全残余信息保护

从属于：FDP_RIP.1 子集残余信息保护。

依赖关系：无依赖性。

10.9.6.1 FDP_RIP.2.1

TSF 应确保一个资源的任何先前信息内容，在[选择：*分配资源到*、*释放资源自*]**所有客体**时不再可用。

10.10 回退(FDP_ROL)

10.10.1 族行为

回退操作指在某个条件(如一段时间)限制下，撤消最后一次操作或一系列操作，并返回到一个先前已知的状态。回退提供了撤销最后一次或一系列操作结果的能力，以保持用户数据的完整性。

10.10.2 组件层次

FDP_ROL.1“基本回退”，要求在既定的限制条件下回退或撤消有限个操作。

FDP_ROL.2“高级回退”，要求在既定的限制条件下回退或撤消所有操作。

10.10.3 FDP_ROL.1、FDP_ROL.2 管理

FMT 中的管理功能可考虑下列行为：

a) 执行回退操作的边界限制条件可能是 TOE 中的一个可配置项；

b) 执行回退操作的权限可以被限制到一个明确定义的角色。

10.10.4 FDP_ROL.1、FDP_ROL.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：所有成功的回退操作；

b) 基本级：执行回退操作的所有尝试；

c) 详细级：执行回退操作的所有尝试，包括回退操作类型的标识。

10.10.5 FDP_ROL.1 基本回退

从属于：无其他组件。

依赖关系：[FDP_ACC.1 子集访问控制，或
FMT_IFC.1 子集信息流控制]。

10.10.5.1 FDP_ROL.1.1

TSF 应执行[赋值：*访问控制 SFP 和/或信息流控制 SFP*]，以允许对[赋值：*信息和/或客体列表*]的[赋值：*操作列表*]进行回退。

10.10.5.2 FDP_ROL.1.2

TSF 应允许在[赋值：*执行回退操作的边界限制条件*]下进行回退操作。

10.10.6 FDP_ROL.2 高级回退

从属于：FDP_ROL.1 基本回退。

依赖关系：[FDP_ACC.1 子集访问控制，或
FMT_IFC.1 子集信息流控制]。

10.10.6.1 FDP_ROL.2.1

TSF 应执行[赋值:*访问控制 SFP 和/或信息流控制 SFP*],以允许对[赋值:*客体列表*]的**所有操作**进行回退。

10.10.6.2 FDP_ROL.2.2

TSF 应允许在[赋值:*执行回退操作的边界限制条件*]下进行回退操作。

10.11 存储数据的完整性(FDP_SDI)

10.11.1 族行为

本族提供了对存储在由 TSF 控制的载体内的用户数据进行保护的要求。完整性错误可能会影响存放在内存或存储设备中的用户数据。本族与 FDP_ITT“TOE 内部传送”的不同之处在于,后者保护的是用户数据在 TOE 内部传送时的完整性。

10.11.2 组件层次

FDP_SDI.1“存储数据的完整性监视”,要求 TSF 监视存储在由 TSF 控制的载体内的用户数据是否存在已被识别的完整性错误。

FDP_SDI.2“存储数据完整性监视和行动”,在检测到某个错误时,相比第一个组件增加了允许采取相应动作的能力。

10.11.3 FDP_SDI.1 管理

尚无预见的管理活动。

10.11.4 FDP_SDI.2 管理

FMT 中的管理功能可考虑下列行为:

a) 检测到完整性错误时所要采取的动作是可配置的。

10.11.5 FDP_SDI.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:检查用户数据完整性的成功尝试,包括检查的结果;

b) 基本级:检查用户数据完整性的所有尝试,如果成功的话,还包括检查的结果;

c) 详细级:出现的完整性错误的类型。

10.11.6 FDP_SDI.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:检查用户数据完整性的成功尝试,包括检查的结果;

b) 基本级:检查用户数据完整性的所有尝试,如果成功的话,还包括检查的结果;

c) 详细级:出现的完整性错误的类型;

d) 详细级:检测到完整性错误时所采取的动作。

10.11.7 FDP_SDI.1 存储数据完整性监视

从属于:无其他组件。

依赖关系:无依赖关系。

10.11.7.1 FDP_SDI.1.1

TSF 应基于下列属性:[赋值:*用户数据属性*],对所有客体,监视存储在由 TSF 控制的载体内的用户数据的[赋值:*完整性错误*]。

10.11.8 FDP_SDI.2 存储数据完整性监视和行动

从属于:FDP_SDI.1 存储数据完整性监视。

依赖关系:无依赖关系。

10.11.8.1 FDP_SDI.2.1

TSF 应基于下列属性:[赋值:*用户数据属性*],对所有客体,监视存储在由 TSF 控制的载体内的用户数据是否存在[赋值:*完整性错误*]。

10.11.8.2 FDP_SDI.2.1

检测到数据完整性错误时,TSF 应[赋值:*采取的动作*]。

10.12 TSF 间用户数据机密性传送保护(FDP_UCT)

10.12.1 族行为

本族定义当用户数据通过外部信道在 TOE 和其他可信 IT 产品间传送时,确保用户数据机密性的要求。

10.12.2 组件层次

FDP_UCT.1"基本的数据交换机密性",目的是为用户数据提供保护,防止其在传送过程中被泄露。

10.12.3 FDP_UCT.1 管理

尚无预见的管理活动。

10.12.4 FDP_UCT.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:使用数据交换机制的任何用户或主体的身份;
b) 基本级:企图使用用户数据交换机制的任何未授权用户或主体的身份;
c) 基本级:可用于识别传送或接收用户数据的名称或其他索引信息的参照表,该表可能包括与信息有关的安全属性。

10.12.5 FDP_UCT.1 基本的数据交换机密性

从属于:无其他组件。

依赖关系:[FTP_ITC.1 TSF 间的可信信道,或
FTP_TRP.1 可信路径];
[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制]。

10.12.5.1 FDP_UCT.1.1

TSF 应执行[赋值:*访问控制 SFP 和/或信息流控制 SFP*],以便能[选择:*传送、接收*]用户数据,并保护其免遭未授权泄露。

10.13 TSF 间用户数据完整性传送保护(FDP_UIT)

10.13.1 族行为

本族定义一些关于用户数据在 TOE 和其他可信 IT 产品间传送时提供完整性保护,以及从可检测的错误中恢复的要求。本族至少要监视对用户数据完整性的篡改,此外还支持采取不同方法纠正检测到的完整性错误。

10.13.2 组件层次

FDP_UIT.1"数据交换的完整性",处理对所传送用户数据的篡改、删除、插入和重放等错误的检测问题。

FDP_UIT.2"原发端数据交换恢复",处理由接收端 TSF 借助原发端可信 IT 产品对原始用户数据的恢复问题。

FDP_UIT.3"接受端数据交换恢复",处理在无需原发端可信 IT 产品的任何帮助的情况下,由接收端 TSF 自己对原始用户数据的恢复问题。

10.13.3 FDP_UIT.1、FDP_UIT.2、FDP_UIT.3 管理

尚无预见的管理活动。

10.13.4 FDP_UIT.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:使用数据交换机制的任何用户或主体的身份;
b) 基本级:企图使用用户数据交换机制的任何未授权用户或主体的身份;
c) 基本级:可用于识别传送或接收用户数据的名称或其他索引信息的参照表,该表可能包括与信息有关的安全属性;
d) 基本级:阻止用户数据传送的任何已标识的尝试;
e) 详细级:任何检测到的对所传送用户数据的篡改类型和/或结果。

10.13.5 FDP_UIT.2、FDP_UIT.3 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:使用数据交换机制的任何用户或主体的身份;
b) 最小级:从错误中成功的恢复,包括检测到的错误类型;
c) 基本级:企图使用用户数据交换机制的任何未授权用户或主体的身份;
d) 基本级:可用于识别传送或接收用户数据的名称或其他索引信息的参照表,该表可能包括与信息有关的安全属性;
e) 基本级:妨碍用户数据传送的任何确定的尝试;
f) 详细级:任何检测到的对所传送用户数据的篡改类型和/或结果。

10.13.6 FDP_UIT.1 数据交换完整性

从属于:无其他组件。

依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制];
[FTP_ITC.1 TSF 间的可信信道,或
FTP_TRP.1 可信路径]。

10.13.6.1 **FDP_UIT.1.1**

TSF 应执行[**赋值**:***访问控制 SFP 和/或信息流控制 SFP***],**以便能**[**选择**:***传送***、***接收***]**用户数据,并保护数据免遭**[**选择**:***篡改***、***删除***、***插入***、***重放***]**错误**。

10.13.6.2 **FDP_UIT.1.2**

TSF 应能确定在用户数据的接收过程中是否发生了[**选择**:***篡改***、***删除***、***插入***、***重放***]**。

10.13.7 **FDP_UIT.2 原发端数据交换恢复**

从属于:无其他组件。
依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制];
[FDP_UIT.1 数据交换完整性,或
FTP_ITC.1 TSF 间的可信信道]。

10.13.7.1 **FDP_UIT.2.1**

TSF 应执行[**赋值**:***访问控制 SFP 和/或信息流控制 SFP***],**以便能在原发端可信 IT 产品的帮助下,从**[**赋值**:***可恢复的错误列表***]**中恢复用户数据**。

10.13.8 **FDP_UIT.3 接受端数据交换恢复**

从属于:FDP_UIT.2 原发端数据交换恢复。
依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制];
[FDP_UIT.1 数据交换完整性,或
FTP_ITC.1 TSF 间的可信信道]。

10.13.8.1 **FDP_UIT.3.1**

TSF 应执行[赋值:*访问控制 SFP 和/或信息流控制 SFP*],以便能在**没有任何**原发端可信 IT 产品的帮助下,从[赋值:*可恢复的错误列表*]中恢复用户数据。

11 FIA 类:标识和鉴别

本类中的族描述了关于建立和验证所声称的用户身份的功能要求。

需要通过标识和鉴别确保用户与正确的安全属性(如身份、组、角色、安全性或完整性等级)相关联。

授权用户的明确标识以及安全属性与用户和主体的正确关联是实施预定安全策略的关键。本类中的族负责确认和验证用户身份、确认他们与 TOE 交互的权限以及每个授权用户安全属性的正确关联。其他要求类(如 FDP“用户数据保护”、FAU“安全审计”)的有效性都是建立在对用户的正确标识和鉴别基础上的。本类的组件构成分解如图 11 所示。

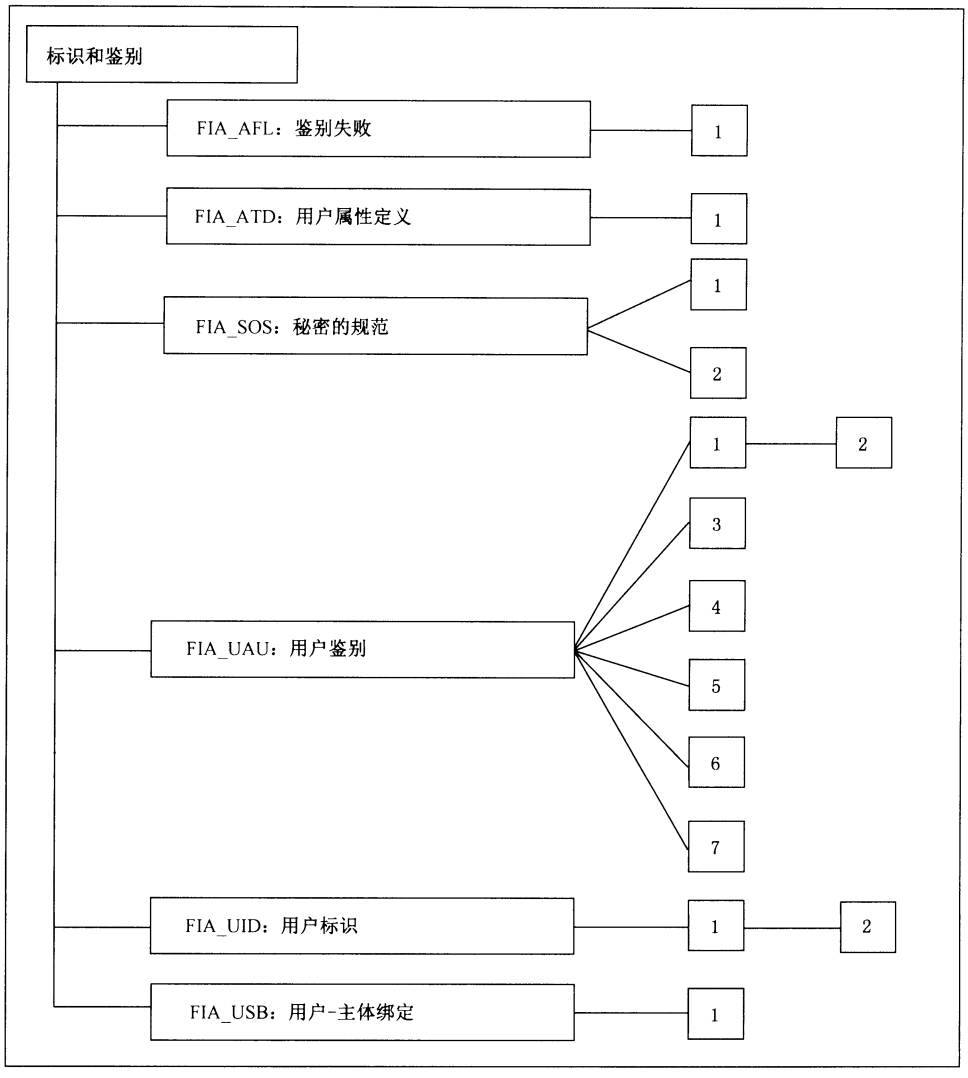

图 11　FIA：标识和鉴别类分解

11.1　鉴别失败(FIA_AFL)

11.1.1　族行为

本族包含为不成功的鉴别尝试次数定义数值和鉴别尝试失败时 TSF 应采取的动作等方面的要求。参数包括但不限于，失败的鉴别尝试次数和次数临界值。

11.1.2　组件层次

FIA_AFL.1“鉴别失败处理”，要求 TSF 能够在用户鉴别尝试失败达到指定的次数后，终止会话建立进程。此外，它还要求会话建立进程终止后，TSF 能够使进行尝试的用户账号或登录点(如工作站)无效，直到满足管理员定义的条件才再次激活。

11.1.3　FIA_AFL.1 管理

FMT 中的管理功能可考虑下列行为：

a)　未成功鉴别尝试的阈值的管理；

b) 鉴别失败事件中要采取的动作的管理。

11.1.4 FIA_AFL.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:未成功鉴别尝试达到阈值、达到阈值后所采取的动作(如,使终端无效),及后来(适当时)还原到正常状态(如,重新使终端有效)。

11.1.5 FIA_AFL.1 鉴别失败处理

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

11.1.5.1 FIA_AFL.1.1

TSF 应检测当[选择:*[赋值:正整数]*,*管理员可设置的[赋值:可接受数值范围]*内的一个*正整数*]时,与[赋值:*鉴别事件列表*]相关的未成功鉴别尝试。

11.1.5.2 FIA_AFL.1.2

当[选择:*达到*,*超过*]所定义的未成功鉴别尝试次数时,TSF 应采取的[赋值:*动作列表*]。

11.2 用户属性定义(FIA_ATD)

11.2.1 族行为

所有授权用户可能都有一组除用户身份外的安全属性用来执行 SFR。本族定义了关联用户属性和用户的要求,以为 TSF 做安全决策时提供支持。

11.2.2 组件层次

FIA_ATD.1“用户属性定义”,允许对每个用户的用户安全属性分别加以维护。

11.2.3 FIA_ATD.1 管理

FMT 中的管理功能可考虑下列行为:

a) 如果赋值中提及的话,授权管理员应该能够为用户定义附加的安全属性。

11.2.4 FIA_ATD.1 审计

尚无预见的可审计事件。

11.2.5 FIA_ATD.1 用户属性定义

从属于:无其他组件。

依赖关系:无依赖关系。

11.2.5.1 FIA_ATD.1.1

TSF 应维护属于单个用户的下列安全属性列表:[赋值:*安全属性列表*]。

11.3 秘密的规范(FIA_SOS)

11.3.1 族行为

本族定义秘密应满足规定的质量度量,并生成秘密以满足所定义的度量机制的要求。

11.3.2 组件层次

FIA_SOS.1“秘密的验证”,要求 TSF 验证秘密满足规定的质量度量要求。

FIA_SOS.2“TSF 生成秘密”,要求 TSF 能够产生满足规定质量度量要求的秘密。

11.3.3 FIA_SOS.1 管理

FMT 中的管理功能可考虑下列行为:

a) 用于验证秘密的度量方法的管理。

11.3.4 FIA_SOS.2 管理

FMT 中的管理功能可考虑下列行为:

a) 用于产生秘密的度量方法的管理。

11.3.5 FIA_SOS.1、FIA_SOS.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:TSF 对任何已测试秘密的拒绝;

b) 基本级:TSF 对任何已测试秘密的拒绝或接受;

c) 详细级:对既定的质量度量要求的任何改动的标识。

11.3.6 FIA_SOS.1 秘密的验证

从属于:无其他组件。

依赖关系:无依赖关系。

11.3.6.1 FIA_SOS.1.1

TSF 应提供一种机制以验证秘密满足[赋值:*一个既定的质量度量要求*]。

11.3.7 FIA_SOS.2 TSF 生成秘密

从属于:无其他组件。

依赖关系:无依赖关系。

11.3.7.1 FIA_SOS.2.1

TSF 应提供一种机制以产生满足[赋值:*一个既定的质量度量要求*]的秘密。

11.3.7.2 FIA_SOS.2.2

TSF 应能够为[赋值:*TSF 功能列表*]使用 TSF 产生的秘密。

11.4 用户鉴别(FIA_UAU)

11.4.1 族行为

本族定义 TSF 所支持的用户鉴别机制的类型,也定义了用户鉴别机制所依赖的必要属性。

11.4.2 组件层次

FIA_UAU.1“鉴别的时机”,允许用户在其身份被鉴别前执行某些动作。

FIA_UAU.2“任何动作前的用户鉴别”,要求在 TSF 允许采取任何动作之前,先鉴别用户。

FIA_UAU.3“不可伪造的鉴别”,要求鉴别机制能够检测并防止伪造或复制的鉴别数据的使用。

FIA_UAU.4“一次性鉴别机制”,要求鉴别机制使用一次性的鉴别数据。

FIA_UAU.5 “多重鉴别机制”,要求提供和使用不同的鉴别机制,为特定的事件鉴别用户的身份。

FIA_UAU.6“重鉴别”,要求有能力指定对于哪些特定事件,用户需要被重新鉴别。

FIA_UAU.7“受保护的鉴别反馈”,要求在鉴别期间,只提供给用户有限的反馈信息。

11.4.3 FIA_UAU.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理员对鉴别数据的管理;

b) 相关用户对鉴别数据的管理;

c) 用户被鉴别前可执行的动作列表的管理。

11.4.4 FIA_UAU.2 管理

FMT 中的管理功能可考虑下列行为:

a) 管理员对鉴别数据的管理;

b) 与鉴别数据相关的用户对鉴别数据的管理。

11.4.5 FIA_UAU.3、FIA_UAU.4、FIA_UAU.7 管理

尚无预见的管理活动。

11.4.6 FIA_UAU.5 管理

FMT 中的管理功能可考虑下列行为:

a) 鉴别机制的管理;

b) 鉴别规则的管理。

11.4.7 FIA_UAU.6 管理

FMT 中的管理功能可考虑下列行为:

a) 如果一个授权管理员能请求重鉴别,则管理将包含一个重鉴别请求。

11.4.8 FIA_UAU.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:鉴别机制的未成功使用;

b) 基本级:鉴别机制的所有使用;

c) 详细级:用户鉴别前执行的所有由 TSF 促成的动作。

11.4.9 FIA_UAU.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:鉴别机制的未成功使用;

b) 基本级:鉴别机制的所有使用。

11.4.10 FIA_UAU.3 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:对欺骗性鉴别数据的检测;

d) 基本级:当前采用的所有措施,以及对欺骗性数据检查的结果。

11.4.11 FIA_UAU.4 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:重用鉴别数据的企图。

11.4.12 FIA_UAU.5 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:对鉴别的最终裁决;

b) 基本级:每个已激活机制的结果以及最终裁决。

11.4.13 FIA_UAU.6 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:重鉴别失败;

b) 基本级:所有重鉴别尝试。

11.4.14 FIA_UAU.7 审计

尚无预见的可审计事件。

11.4.15 FIA_UAU.1 鉴别的时机

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

11.4.15.1 FIA_UAU.1.1

在用户被鉴别前,TSF 应允许执行代表用户的[赋值:由 TSF 促成的动作列表]。

11.4.15.2 FIA_UAU.1.2

在允许执行代表该用户的任何其他由 TSF 促成的动作前,TSF 应要求每个用户都已被成功鉴别。

11.4.16 FIA_UAU.2 任何动作前的用户鉴别

从属于:FIA_UAU.1 鉴别的时机。

依赖关系:FIA_UID.1 标识的时机。

11.4.16.1 FIA_UAU.2.1

在允许执行代表该用户的任何其他由 TSF 促成的动作前,TSF 应要求每个用户都已被成功鉴别。

11.4.17 FIA_UAU.3 不可伪造的鉴别

从属于:无其他组件。

依赖关系:无依赖关系。

11.4.17.1 FIA_UAU.3.1

TSF 应[选择:*检测*、*防止*]由任何 TSF 用户伪造的鉴别数据的使用。

11.4.17.2 FIA_UAU.3.2

TSF 应[选择:*检测*、*防止*]从任何其他的 TSF 用户处拷贝的鉴别数据的使用。

11.4.18 FIA_UAU.4 一次性鉴别机制

从属于:无其他组件。
依赖关系:无依赖关系。

11.4.18.1 FIA_UAU.4.1

TSF 应防止与[赋值:*确定的鉴别机制*]有关的鉴别数据的重用。

11.4.19 FIA_UAU.5 多重鉴别机制

从属于:无其他组件。
依赖关系:无依赖关系。

11.4.19.1 FIA_UAU.5.1

TSF 应提供[赋值:*多重鉴别机制列表*]以支持用户鉴别。

11.4.19.2 FIA_UAU.5.2

TSF 应根据[赋值:*描述多重鉴别机制如何提供鉴别的规则*]鉴别任何用户所声称的身份。

11.4.20 FIA_UAU.6 重鉴别

从属于:无其他组件。
依赖关系:无依赖关系。

11.4.20.1 FIA_UAU.6.1

TSF 应在[赋值:*需要重鉴别的条件列表*]条件下重新鉴别用户。

11.4.21 FIA_UAU.7 受保护的鉴别反馈

从属于:无其他组件。
依赖关系:FIA_UAU.1 鉴别的时机。

11.4.21.1 FIA_UAU.7.1

鉴别进行时,TSF 应仅向用户提供[赋值:*反馈列表*]。

11.5 用户标识(FIA_UID)

11.5.1 族行为

本族定义了在执行任何其他由 TSF 促成的、且需要用户标识的动作前,要求用户标识其身份的条件。

11.5.2 组件层次

FIA_UID.1“标识的时机”,允许用户在被 TSF 识别前,执行某些动作。

FIA_UID.2“任何动作前的用户标识”,在 TSF 允许其执行任何动作之前,要求用户进行身份识别。

11.5.3 FIA_UID.1 管理

FMT 中的管理功能可考虑下列行为:

a) 用户身份的管理;

b) 如果一个授权管理员能够改变在标识前所允许的动作,则可考虑对动作列表的管理。

11.5.4 FIA_UID.2 管理

FMT 中的管理功能可考虑下列行为:

a) 用户身份的管理。

11.5.5 FIA_UID.1、FIA_UID.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:未成功用户标识机制的使用,包括所提供的用户身份;

b) 基本级:所有用户标识机制的使用,包括所提供的用户身份。

11.5.6 FIA_UID.1 标识的时机

从属于:无其他组件。

依赖关系:无依赖关系。

11.5.6.1 FIA_UID.1.1

在用户被识别之前,TSF 应允许执行代表用户的[赋值:*TSF 促成的动作列表*]。

11.5.6.2 FIA_UID.1.2

在允许执行代表该用户的任何其他 TSF 仲裁动作之前,TSF 应要求每个用户身份都已被成功识别。

11.5.7 FIA_UID.2 任何动作前的用户标识

从属于:FIA_UID.1 标识的时机。

依赖关系:无依赖关系。

11.5.7.1 FIA_UID.2.1

在允许执行代表该用户的任何其他 TSF 促成动作之前,TSF 应要求每个用户身份都已被成功识别。

11.6 用户-主体绑定(FIA_USB)

11.6.1 族行为

已成功鉴别的用户,为了使用 TOE,一般会先激活一个主体。用户的安全属性(全部或部分地)与该主体相关联。本族定义了建立和维护用户安全属性与代表该用户的主体间关联关系的要求。

11.6.2 组件层次

FIA_USB.1“用户-主体绑定”,要求对用户属性及其映入的主体属性之间的关联关系的管理规则进

行规范。

11.6.3 FIA_USB.1 管理

FMT 中的管理功能可考虑下列行为：

a) 授权管理员可以定义默认的主体安全属性；

b) 授权管理员可以改变主体的安全属性。

11.6.4 FIA_USB.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：用户安全属性与一个主体的未成功绑定（如，创建一个主体）；

b) 基本级：用户安全属性与一个主体的成功绑定和失败绑定（如，创建一个主体的成功和失败）。

11.6.5 FIA_USB.1 用户-主体绑定

从属于：无其他组件。

依赖关系：FIA_ATD.1 用户属性定义。

11.6.5.1 FIA_USB.1.1

TSF 应将下列用户安全属性：[赋值：*用户安全属性列表*]与代表用户活动的主体相关联。

11.6.5.2 FIA_USB.1.2

TSF 应对用户安全属性与代表用户活动的主体初始关联关系执行下列规则：[赋值：*属性初始关联规则*]。

11.6.5.3 FIA_USB.1.3

TSF 应执行下列规则管理用户安全属性与代表用户活动的主体间的关联关系的变化：[赋值：*属性更改规则*]。

12 FMT 类：安全管理

本类目的是详细说明安全属性、TSF 数据和功能等几个方面的管理，也规范了不同的管理角色及其相互作用，如能力的分离。

本类有几个目的：

a) 管理 TSF 数据，例如旗标；

b) 管理安全属性，例如访问控制列表和能力列表；

c) 管理 TSF 功能，例如功能的选择，影响 TSF 行为的规则或条件；

d) 定义安全角色。

本类的组件构成分解如图 12 所示。

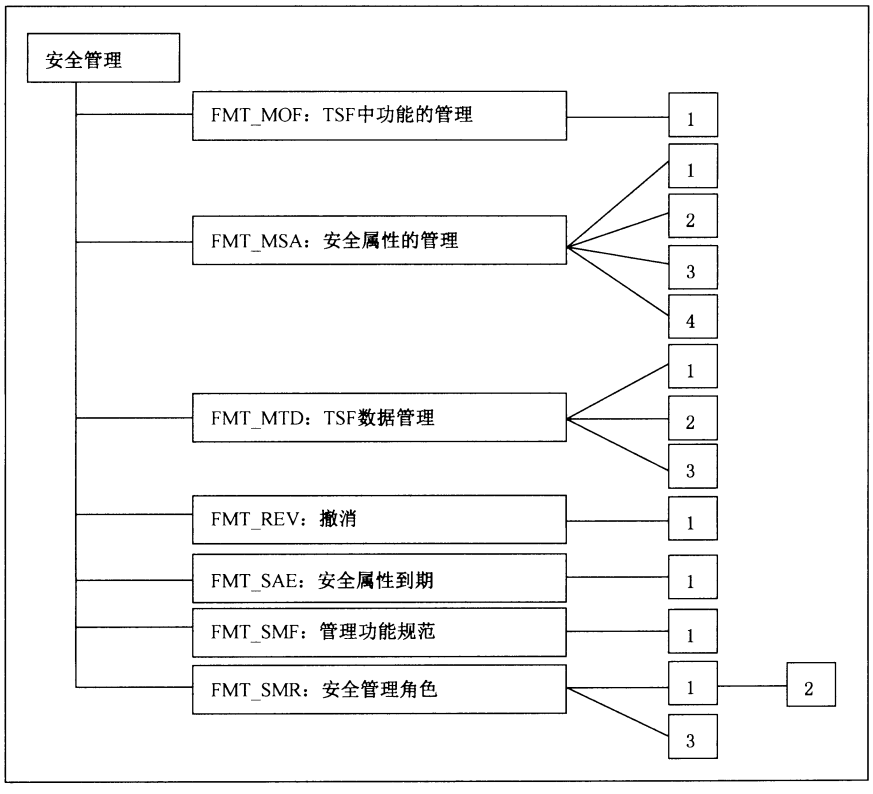

图 12 FMT:安全管理类分解

12.1 TSF 中功能的管理(FMT_MOF)

12.1.1 族行为

本族允许授权用户控制对 TSF 中功能的管理。例如,审计功能和多重鉴别功能都是 TSF 中的功能实例。

12.1.2 组件层次

FMT_MOF.1“安全功能行为的管理”,允许授权用户(角色)管理 TSF 中的功能行为,这些功能使用了可以管理的规则或具有可管理的特定条件。

12.1.3 FMT_MOF.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理可以与 TSF 中功能交互的角色组。

12.1.4 12.1.4 FMT_MOF.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 基本级:TSF 中功能行为的所有改动。

12.1.5 FMT_MOF.1 安全功能行为的管理

从属于:无其他组件。

依赖关系:FMT_SMR.1 安全角色;

FMT_SMF.1 管理功能规范。

12.1.5.1 FMT_MOF.1.1

TSF 应仅限于[赋值:*已标识的授权角色*]对功能[赋值:功能列表]具有[选择:*确定其行为*、*终止*、*激活*、*修改其行为*]的能力。

12.2 安全属性的管理(FMT_MSA)

12.2.1 族行为

本族允许授权用户控制安全属性的管理。这种管理可能包括查看和修改安全属性的能力。

12.2.2 组件层次

FMT_MSA.1“安全属性的管理”,允许授权用户(角色)管理指定的安全属性。

FMT_MSA.2“安全的安全属性”,确保赋给安全属性的值对安全状态而言是有效的。

FMT_MSA.3“静态属性初始化”,确保安全属性的默认值是恰当的,即或者是容许的,或者事实上是受限的。

FMT_MSA.4 “安全属性值的继承”,允许规则/策略来指定由安全属性继承的值。

12.2.3 FMT_MSA.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理可以和安全属性交互的角色组;

b) 管理安全属性继承指定值的规则。

12.2.4 FMT_MSA.2 管理

FMT 中的管理功能可考虑下列行为:

a) 管理为安全属性继承指定值的规则。

12.2.5 FMT_MSA.3 管理

FMT 中的管理功能可考虑下列行为:

a) 管理能指定初始值的角色组;

b) 对于某个给定的访问控制 SFP,对允许或限制的默认值的设置进行管理;

c) 管理安全属性继承指定值的规则。

12.2.6 FMT_MSA.4 管理

FMT 中的管理功能可考虑下列行为:

a) 指定允许建立或修改安全属性的角色。

12.2.7 FMT_MSA.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 基本级:所有对安全属性值的改动。

12.2.8 FMT_MSA.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:所有已提供的和被拒绝的安全属性的值;
b) 详细级:所有已提供的和被接受的安全属性的值。

12.2.9 FMT_MSA.3 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:
a) 基本级:对允许或限制规则默认设置的修改;
b) 基本级:所有对安全属性初始值的修改。

12.2.10 FMT_MSA.4 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:
a) 基本级:对旧的安全属性值的修改和/或修改后的安全属性值。

12.2.11 FMT_MSA.1 安全属性的管理

从属于:无其他组件。
依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制];
FMT_SMR.1 安全角色;
FMT_SMF.1 管理功能规范。

12.2.11.1 FMT_MSA.1.1

TSF 应执行[赋值:*访问控制 SFP、信息流控制 SFP*],以仅限于[赋值:*已标识的授权角色*]能够对安全属性[赋值:*安全属性列表*]进行[选择:*改变默认值、查询、修改、删除、[赋值:其他操作]*]。

12.2.12 FMT_MSA.2 安全的安全属性

从属于:无其他组件。
依赖关系:ADV_SPM.1 非形式化的 TOE 安全策略模型;
[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制];
FMT_MSA.1 安全属性的管理;
FMT_SMR.1 安全角色。

12.2.12.1 FMT_MSA.2.1

TSF 应确保安全属性[赋值:*安全属性列表*]只接受安全的值。

12.2.13 FMT_MSA.3 静态属性初始化

从属于:无其他组件。
依赖关系:FMT_MSA.1 安全属性的管理;
FMT_SMR.1 安全角色。

12.2.13.1 FMT_MSA.3.1

TSF 应执行[赋值:*访问控制 SFP、信息流控制 SFP*],以便为用于执行 SFP 的安全属性提供[选择,从中选取一个:*受限的、许可的、[赋值:其他特性]*]默认值。

12.2.13.2 FMT_MSA.3.2

TSF 应允许[赋值:*已标识的授权角色*]在创建客体或信息时指定替换性的初始值以代替原来的默认值。

12.2.14 FMT_MSA.4 安全属性值的继承

从属于:无其他组件。

依赖关系:[FDP_ACC.1 子集访问控制,或
FDP_IFC.1 子集信息流控制]。

12.2.14.1 FMT_MSA.4.1

TSF 应使用下列规则[赋值:*用于设置安全属性值的规则*]来设置安全属性的值。

12.3 TSF 数据的管理(FMT_MTD)

12.3.1 族行为

本族允许授权用户(角色)控制 TSF 数据的管理。这里的 TSF 数据包括审计信息、时钟和其他 TSF 配置参数。

12.3.2 组件层次

FMT_MTD.1"TSF 数据的管理",允许授权用户管理 TSF 数据。

FMT_MTD.2"TSF 数据限值的管理",指定如果达到或超过了 TSF 数据的限值所应采取的动作。

FMT_MTD.3"安全的 TSF 数据",确保赋给 TSF 数据的值针对安全状态而言是有效的。

12.3.3 FMT_MTD.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理可以和 TSF 数据交互的角色组。

12.3.4 FMT_MTD.2 管理

FMT 中的管理功能可考虑下列行为:

a) 管理可以和 TSF 数据限值交互的角色组。

12.3.5 FMT_MTD.3 管理

尚无预见的管理活动。

12.3.6 FMT_MTD.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 基本级:所有对 TSF 数据值的改动。

12.3.7 FMT_MTD.2 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 基本级:所有对 TSF 数据限值的改动;

b) 基本级:在超出限值时,所要采取动作的所有改动。

12.3.8 FMT_MTD.3 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：所有被拒绝的 TSF 数据值。

12.3.9 FMT_MTD.1 TSF 数据的管理

从属于：无其他组件。

依赖关系：FMT_SMR.1 安全角色；

FMT_SMF.1 管理功能规范。

12.3.9.1 FMT_MTD.1.1

TSF 应仅限于[赋值：*已标识的授权角色*]能够对[赋值：*TSF 数据列表*][选择：*改变默认值、查询、修改、删除、清除、[赋值：其他操作]*]。

12.3.10 FMT_MTD.2 TSF 数据限值的管理

从属于：无其他组件。

依赖关系：FMT_MTD.1 TSF 数据的管理；

FMT_SMR.1 安全角色。

12.3.10.1 FMT_MSA.2.1

TSF 应仅限于[赋值：*已标识的授权角色*]规定[赋值：*TSF 数据列表*]的限值。

12.3.10.2 FMT_MSA.2.2

如果 TSF 数据达到或超过了设定的限值，TSF 应采取下面的动作：[赋值：*要采取的动作*]。

12.3.11 FMT_MTD.3 安全的 TSF 数据

从属于：无其他组件。

依赖关系：FMT_MTD.1 TSF 数据的管理。

12.3.11.1 FMT_MSA.3.1

TSF 应确保 TSF 数据[赋值：*TSF 数据列表*]只接受安全的值。

12.4 撤消(FMT_REV)

12.4.1 族行为

本族负责处理 TOE 内各种实体安全属性的撤消问题。

12.4.2 组件层次

FMT_REV.1“撤消”，规定了撤消在某一时刻将实施的安全属性的要求。

12.4.3 FMT_REV.1 管理

FMT 中的管理功能可考虑下列行为：

a) 管理能够调用安全属性撤消这一功能的角色组；

b) 管理可能发生撤消的用户、主体、客体和其他资源列表；

c) 管理撤消规则。

12.4.4 FMT_REV.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：安全属性的未成功撤消；

b) 基本级：所有撤消安全属性的尝试。

12.4.5 FMT_REV.1 撤消

从属于：无其他组件。

依赖关系：FMT_SMR.1 安全角色。

12.4.5.1 FMT_REV.1.1

TSF 应仅限于[赋值：*已标识的授权角色*]能够撤消在 TSF 控制下的与[选择：*用户*、*主体*、*客体*、[*赋值：其他额外资源*]]相关联的安全属性[赋值：*安全属性列表*]。

12.4.5.2 FMT_REV.1.2

TSF 应执行规则[赋值：*撤消规则的详细说明*]。

12.5 安全属性到期(FMT_SAE)

12.5.1 族行为

本族处理对安全属性的有效性实施时间限制能力的问题。

12.5.2 组件层次

FMT_SAE.1“时限授权”，为授权用户提供对指定的安全属性规定有效期的能力。

12.5.3 FMT_SAE.1 管理

FMT 中的管理功能可考虑下列行为：

a) 管理支持有效期的安全属性表；

b) 如果到期，将要采取的动作。

12.5.4 FMT_SAE.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 基本级：属性有效期的规定；

b) 基本级：因属性到期而采取的动作。

12.5.5 FMT_SAE.1 时限授权

从属于：无其他组件。

依赖关系：FMT_SMR.1 安全角色；

FPT_STM.1 可靠时间戳。

12.5.5.1 FMT_SAE.1.1

TSF 应仅限于[赋值：*已标识的授权角色*]能够为[赋值：*支持有效期的安全属性列表*]指定有效期。

12.5.5.2 FMT_SAE.1.2

对每个这样的安全属性，在超过指定的安全属性的有效期后，TSF 应能够[赋值：*对每一个安全属性将要采取的动作列表*]。

12.6 管理功能规范(FMT_SMF)

12.6.1 族行为

本族规范 TOE 的管理功能。管理功能提供 TSFI 以便于管理员定义控制 TOE 安全相关操作的参数，如数据保护属性、TOE 保护属性、审计属性、标识和鉴别属性等。管理功能也包含由操作员执行的用以确保 TOE 连续运行的功能，如备份和恢复。本族同 FMT“安全管理”类中的其他组件合在一起使用：本族的组件负责提出管理功能，FMT“安全功能”类中其他族对使用这些管理功能的能力进行了限制。

12.6.2 组件层次

FMT_SMF.1“管理功能规范”，要求 TSF 提供特定的管理功能。

12.6.3 FMT_SMF.1 管理

尚无预见的管理活动。

12.6.4 FMT_SMF.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：管理功能的使用。

12.6.5 FMT_SMF.1 管理功能规范

从属于：无其他组件。

依赖关系：无依赖关系。

12.6.5.1 FMT_SMF.1.1

TSF 应能够执行如下管理功能：[赋值：*TSF 提供的安全管理功能列表*]。

12.7 安全管理角色(FMT_SMR)

12.7.1 族行为

本族目的是控制对用户分配不同的角色。这些角色在安全管理方面的能力在本类的其他族中描述。

12.7.2 组件层次

FMT_SMR.1“安全角色”，规定 TSF 认可的与安全相关的一些角色。

FMT_SMR.2“安全角色限制”，除了规定角色外，还规定了控制角色之间关系的规则。

FMT_SMR.3“承担角色”，要求向 TSF 明确请求承担某个角色。

12.7.3 FMT_SMR.1 管理

FMT 中的管理功能可考虑下列行为：

a) 管理用户组(某个角色的一部分)。

12.7.4 FMT_SMR.2 管理

FMT 中的管理功能可考虑下列行为:

a) 管理充当某个角色的用户组;

b) 管理角色必须满足的条件。

12.7.5 FMT_SMR.3 管理

尚无预见的管理活动。

12.7.6 FMT_SMR.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:对充当某个角色的用户组的修改;

b) 详细级:对角色权限的每一次使用。

12.7.7 FMT_SMR.2 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:对充当某个角色的用户组的修改;

b) 最小级:由于对角色的限制条件,而导致使用某个角色时的未成功尝试;

c) 详细级:对角色权限的每一次使用。

12.7.8 FMT_SMR.3 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:承担一个角色的明确请求。

12.7.9 FMT_SMR.1 安全角色

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

12.7.9.1 FMT_SMR.1.1

TSF 应维护角色[赋值:*已标识的授权角色*]。

12.7.9.2 FMT_SMR.1.2

TSF 应能够把用户和角色关联起来。

12.7.10 FMT_SMR.2 安全角色限制

从属于:FMT_SMR.1 安全角色。

依赖关系:FIA_UID.1 标识的时机。

12.7.10.1 FMT_SMR.2.1

TSF 应维护角色[赋值:*已标识的授权角色*]。

12.7.10.2 FMT_SMR.2.2

TSF 应能够把用户和角色关联起来。

12.7.10.3 FMT_SMR.2.3

TSF 应确保条件[赋值:*不同角色的条件*]得到满足。

12.7.11 FMT_SMR.3 承担角色

从属于:无其他组件。

依赖关系:FMT_SMR.1 安全角色。

12.7.11.1 FMT_SMR.3.1

TSF 应要求提供一个明确请求以承担下列角色:[赋值:*角色*]。

13 FPR 类:隐私

本类包含与隐私有关的要求。这些要求为用户提供保护,以防止其身份被其他用户发现并滥用。

本类的组件构成分解如图 13 所示。

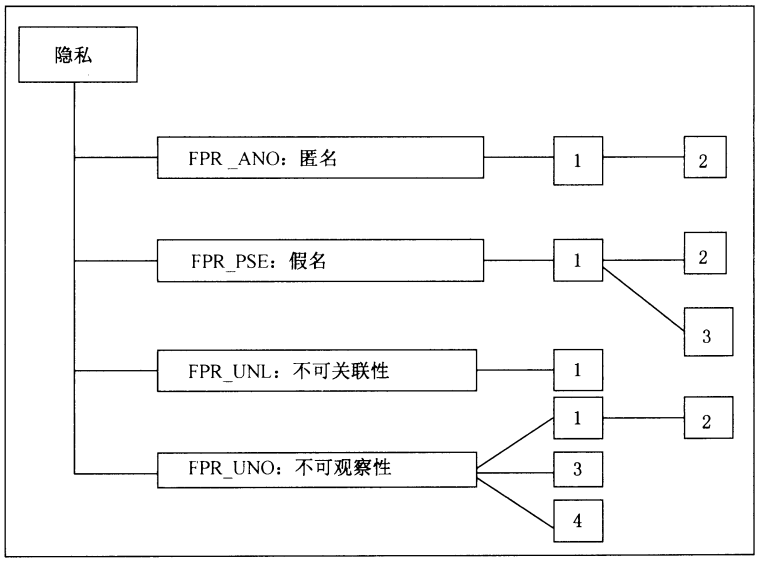

图 13 FPR:隐私类分解

13.1 匿名(FPR_ANO)

13.1.1 族行为

本族确保用户在不暴露其身份的情况下使用资源或服务。本族的要求提供了对用户身份的保护,但并不提供主体身份的保护。

13.1.2 组件层次

FPR_ANO.1"匿名",要求其他用户或主体不能确定与某个主体或操作绑定的用户身份。

FPR_ANO.2"无索求信息的匿名",通过确保 TSF 不询问用户身份来增强 FPR_ANO.1"匿名"的要求。

13.1.3 FPR_ANO.1、FPR_ANO.2 管理

尚无预见的管理活动。

13.1.4 FPR_ANO.1 、FPR_ANO.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:匿名机制的调用。

13.1.5 FPR_ANO.1 匿名

从属于:无其他组件。

依赖关系:无依赖关系。

13.1.5.1 FPR_ANO.1.1

TSF 应确保 [赋值:*用户和/或主体集*]不能确定与 [赋值:*主体、操作和/或客体列表*]绑定的真实用户名。

13.1.6 FPR_ANO.2 无索求信息的匿名

从属于:FPR_ANO.1 匿名。

依赖关系:无依赖关系。

13.1.6.1 FPR_ANO.2.1

TSF 应确保 [赋值:*用户和/或主体集*]不能确定与[赋值:*主体、操作和/或客体列表*]绑定的真实用户名。

13.1.6.2 FPR_ANO.2.2

TSF 应提供 [赋值:*服务列表*]给[赋值:*主体列表*],而不需索求任何有关其真实用户名的信息。

13.2 假名(FPR_PSE)

13.2.1 族行为

本族确保用户在不暴露其身份的情况下使用资源或服务,但仍能对该次使用负责。

13.2.2 组件层次

FPR_PSE.1“假名”,要求一组用户或主体不能确定与主体或操作相绑定的用户身份,但是该用户仍能对其行为负责。

FPR_PSE.2“可逆假名”,要求 TSF 提供一种可根据用户所提供的别名确定原始用户身份的能力。

FPR_PSE.3“别名假名”,要求 TSF 采用某种构造规则对用户身份和别名进行关联。

13.2.3 FPR_PSE.1、FPR_PSE.2、FPR_PSE.3 管理

尚无预见的管理活动。

13.2.4 FPR_PSE.1、FPR_PSE.2、FPR_PSE.3 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:审计主体/用户请求辨别用户身份的行为。

13.2.5 FPR_PSE.1 假名

从属于:无其他组件。

依赖关系:无依赖关系。

13.2.5.1 FPR_PSE.1.1

TSF 应确保[赋值:*用户和/或主体集*]不能确定与[赋值:*主体和/或操作和/或客体列表*]绑定的真实用户名。

13.2.5.2 FPR_PSE.1.2

TSF 应能提供真实用户名的[赋值:*别名的数目*]个别名给[赋值:*主体列表*]。

13.2.5.3 FPR_PSE.1.3

TSF 应[选择,选取一个:*确定一个用户的别名,接受该用户的别名*]并验证它是否符合[赋值:*别名的度量要求*]。

13.2.6 FPR_PSE.2 可逆假名

从属于:FPR_PSE.1 假名。

依赖关系:FIA_UID.1 标识的时机。

13.2.6.1 FPR_PSE.2.1

TSF 应确保[赋值:*用户和/或主体集*]不能确定与[赋值:*主体和/或操作和/或客体列表*]相绑定的真实用户名。

13.2.6.2 FPR_PSE.2.2

TSF 应能提供真实用户名的[赋值:*别名的数目*]个别名给[赋值:*主体列表*]。

13.2.6.3 FPR_PSE.2.3

TSF 应能[选择:*确定一个用户的别名、接受该用户的别名*]并验证它是否符合[赋值:*别名的度量要求*]。

13.2.6.4 FPR_PSE.2.4

TSF 应为[选择:*授权用户、[赋值:可信主体列表]*]提供一种能力,以便只有在[赋值:*条件列表*]下能基于所提供的别名确定用户的身份。

13.2.7 FPR_PSE.3 别名假名

从属于:FPR_PSE.1 假名。

依赖关系:无依赖关系。

13.2.7.1 FPR_PSE.3.1

TSF 应确保[赋值:*用户和/或主体集*]不能确定与[赋值:*主体和/或操作和/或客体列表*]相绑定的真实用户名。

13.2.7.2 FPR_PSE.3.2

TSF 应能提供真实用户名的[赋值:*别名的数目*]个别名给[赋值:*主体列表*]。

13.2.7.3 FPR_PSE.3.3

TSF 应能[选择:*确定一个用户的别名*、*接受该用户的别名*]并验证它是否符合[赋值:*别名的度量要求*]。

13.2.7.4 FPR_PSE.3.4

TSF 应能为真实用户名提供一个别名,在[赋值:*条件列表*]下,该别名应当与先前所提供的别名相同,而其他情况下,所提供的别名应与先前所提供的别名无关。

13.3 不可关联性(FPR_UNL)

13.3.1 族行为

本族确保一个用户可多次使用资源或服务,而其他人不能将这些使用关联在一起。

13.3.2 组件层次

FPR_UNL.1“不可关联性”,要求用户和/或主体不能确定是否同一个用户在系统中进行了某种特定的操作。

13.3.3 FPR_UNL.1 管理

FMT 中的管理功能可考虑下列行为:

a) 不可关联性功能的管理。

13.3.4 FPR_UNL.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:不可关联性机制的调用。

13.3.5 FPR_UNL.1 不可关联性

从属于:无其他组件。

依赖关系:无依赖关系。

13.3.5.1 FPR_UNL.1.1

TSF 应确保[赋值:*用户和/或主体集*]不能确定[赋值:*操作列表*]是否[选择:*由同一个用户引起*、*与如下[赋值:关系列表]有关*]。

13.4 不可观察性(FPR_UNO)

13.4.1 族行为

本族确保一个用户在使用某个资源和服务时,其他人尤其是第三方不能观察到该资源和服务正被使用。

13.4.2 组件层次

FPR_UNO.1“不可观察性”,要求用户和/或主体不能确定一个操作是否正在被执行。

FPR_UNO.2“影响不可观察性的信息的分配”,要求 TSF 提供专门的机制以避免 TOE 内有关隐私信息的汇集。当出现安全性损害时,这种汇集可能会影响到不可观察性。

FPR_UNO.3“无索求信息的不可观察性”,要求 TSF 不要试图获得隐私有关的信息,因为可能会损害不可观察性。

FPR_UNO.4“授权用户可观察性”,要求 TSF 能够给一个或多个授权用户提供具有观察资源和/或服务使用情况的能力。

13.4.3 FPR_UNO.1、FPR_UNO.2 管理

FMT 中的管理功能可考虑下列行为:

a) 不可观察性功能的行为的管理。

13.4.4 FPR_UNO.3 管理

尚无预见的管理活动。

13.4.5 FPR_UNO.4 管理

FMT 中的管理功能可考虑下列行为:

a) 有能力确定操作发生的授权用户列表。

13.4.6 FPR_UNO.1、FPR_UNO.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:不可观察性机制的调用。

13.4.7 FPR_UNO.3 审计

尚无预见的可审计事件。

13.4.8 FPR_UNO.4 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:用户或主体对一个资源或服务使用情况的观察结果。

13.4.9 FPR_UNO.1 不可观察性

从属于:无其他组件。

依赖关系:无依赖关系。

13.4.9.1 FPR_UNO.1.1

TSF 应确保[赋值:*用户和/或主体列表*]不能观察到由[赋值:*受保护的用户和/或主体列表*]对[赋值:*客体列表*]进行的操作[赋值:*操作列表*]。

13.4.10 FPR_UNO.2 影响不可观察性的信息的分配

从属于:FPR_UNO.1 不可观察性。

依赖关系:无依赖关系。

13.4.10.1 FPR_UNO.2.1

TSF 应确保[赋值:*用户和/或主体列表*]不能观察到由[赋值:*受保护的用户和/或主体列表*]对[赋值:*客体列表*]进行的操作[赋值:*操作列表*]。

13.4.10.2 FPR_UNO.2.2

TSF 应在 TOE 的不同部分中分配[赋值:*不可观察性相关信息*],使得下列条件在信息的生存期内成立:[赋值:*条件列表*]。

13.4.11 FPR_UNO.3 无索求信息的不可观察性

从属于:无其他组件。

依赖关系:FPR_UNO.1 不可观察性。

13.4.11.1 FPR_UNO.3.1

TSF 应当在没有索求任何有关[赋值:*隐私相关信息*]的情况下为[赋值:*主体列表*]提供[赋值:*服务列表*]。

13.4.12 FPR_UNO.4 授权用户可观察性

从属于:无其他组件。

依赖关系:无依赖关系。

13.4.12.1 FPR_UNO.4.1

TSF 应给[赋值:*授权用户集*]提供观察[赋值:*资源和/或服务列表*]使用情况的能力。

14 FPT 类:TSF 保护

本类包含了多个功能要求族,这些要求与组成 TSF 的安全机制的完整性和管理有关,也与 TSF 数据的完整性有关。本类的组件构成分解如图 14 所示。

在某种意义下,FPT 类的族可能出现与 FDP“用户数据保护”类中完全相同的组件,它们甚至利用相同的机制来实现。但是,FDP“用户数据保护”主要侧重于用户数据的保护,而 FPT“TSF 保护”则侧重于 TSF 数据的保护。实际上,FPT“TSF 保护”类的组件针对 TOE 中的 SFP 不被篡改或旁路方面的要求是很有必要的。

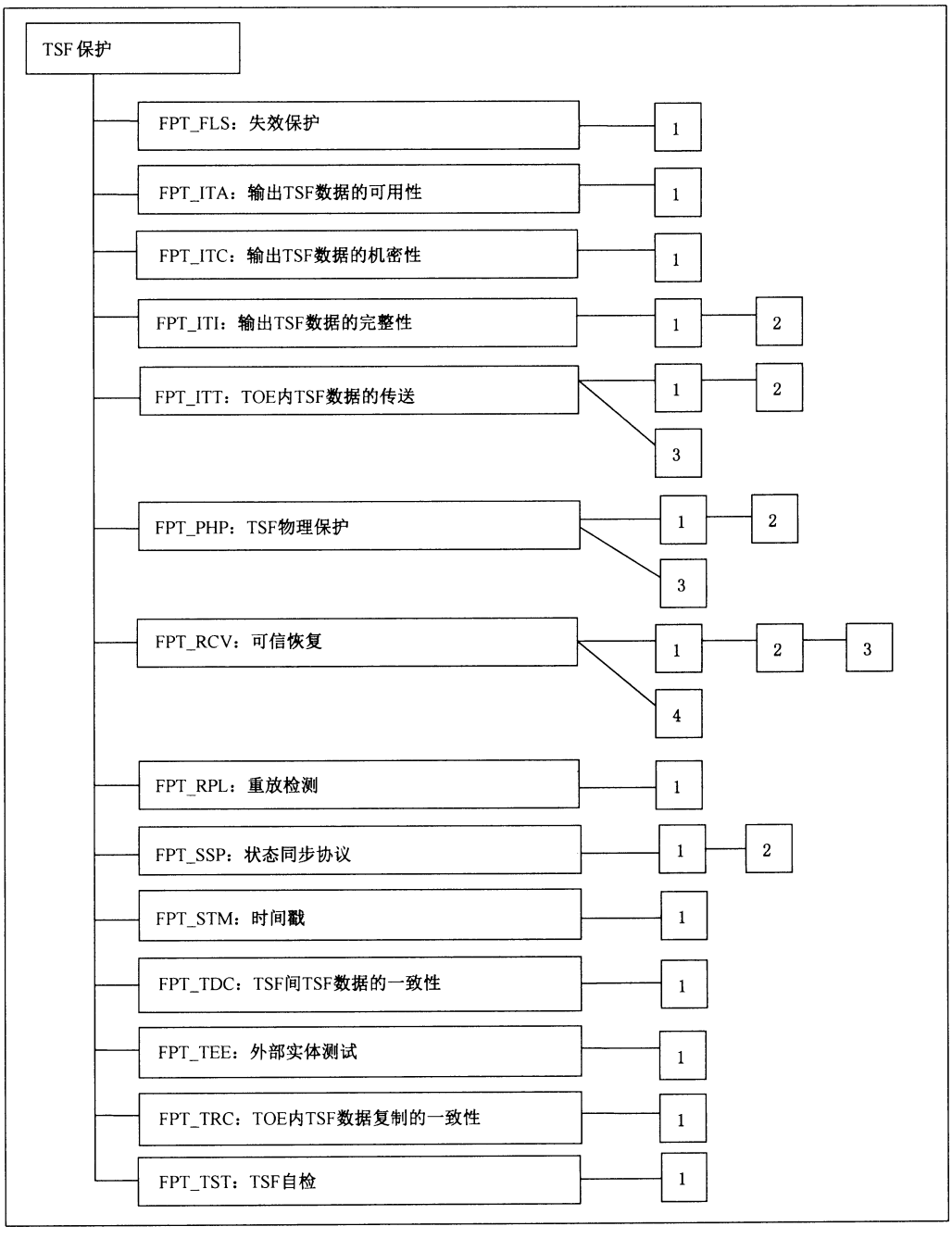

图 14　FPT:TSF 保护类分解

从 FPT 类的观点看，与 TSF 相关的有 3 个重要元素：

a）　TSF 实现，执行和实现那些实施 SFR 的机制。

b）　TSF 数据，指导 SFR 实施的管理性数据库。

c）　TSF 与 SFR 所要实施两者间可能相互作用的外部实体。

14.1 失效保护(FPT_FLS)

14.1.1 族行为

本族要求确保当 TSF 中已确定的失效类型出现时,该 TOE 总是执行它的 SFR。

14.1.2 组件层次

本族只有一个组件,FPT_FLS.1"失效即保持安全状态",要求 TSF 当确定的失效出现时保持一种安全状态。

14.1.3 FPT_FLS.1 管理

尚无预见的管理活动。

14.1.4 FPT_FLS.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 基本级:TSF 失效。

14.1.5 FPT_FLS.1 失效即保持安全状态

从属于:无其他组件。

依赖关系:无依赖关系。

14.1.5.1 FPT_FLS.1.1

TSF 在下列失效发生时应保持一种安全状态:[赋值:*TSF 的失效类型列表*]。

14.2 输出 TSF 数据的可用性(FPT_ITA)

14.2.1 族行为

本族定义了一些规则,用于防止 TSF 数据在 TSF 与另一个可信 IT 产品之间转移时失去其可用性。该数据可能是 TSF 的关键数据,如口令、密钥、审计数据或 TSF 可执行代码。

14.2.2 组件层次

本族只有一个组件,FPT_ITA.1"TSF 间可用性不超过既定可用性度量",要求 TSF 确保向另一个可信 IT 产品提供的 TSF 数据的可用性,达到一个确定可能性的程度。

14.2.3 FPT_ITA.1 管理

FMT 中的管理功能可考虑下列行为:

a) 另一个可信 IT 产品必须可用的 TSF 数据类型列表的管理。

14.2.4 FPT_ITA.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:当 TOE 需要 TSF 数据时,TSF 数据不存在。

14.2.5 FPT_ITA.1 TSF 间可用性不超过既定可用性度量

从属于:无其他组件。

依赖关系:无依赖关系。

14.2.5.1 FPT_ITA.1.1

在[赋值:*确保可用性的条件*]条件下,TSF 应确保提供给另一个可信 IT 产品的[赋值:*TSF 数据类型列表*]的可用性不会超过[赋值:*一个既定可用性度量*]。

14.3 输出 TSF 数据的机密性(FPT_ITC)

14.3.1 族行为

本族定义了一些规则,用于保护 TSF 数据在 TSF 与另一个可信 IT 产品之间传送时不被未授权泄露。该数据可能是 TSF 的关键数据,如口令、密钥、审计数据或 TSF 可执行代码。

14.3.2 组件层次

本族只有一个组件,FPT_ITC.1"传送过程中 TSF 间的机密性",要求 TSF 确保数据在 TSF 与另一个可信 IT 产品间传送时不被泄露。

14.3.3 FPT_ITC.1 管理

尚无预见的管理活动。

14.3.4 FPT_ITC.1 审计

尚无预见的可审计事件。

14.3.5 FPT_ITC.1 传送过程中 TSF 间的机密性

从属于:无其他组件。

依赖关系:无依赖关系。

14.3.5.1 FPT_ITC.1.1

TSF 应保护所有从 TSF 传送到另一个可信 IT 产品的 TSF 数据在传送过程中不会被未授权泄漏。

14.4 输出 TSF 数据的完整性(FPT_ITI)

14.4.1 族行为

本族定义了一些规则,用于保护 TSF 数据在 TSF 与另一个可信 IT 产品之间传送时被未授权修改。该数据可能是 TSF 的关键数据,如口令、密钥、审计数据或 TSF 可执行代码。

14.4.2 组件层次

FPT_ITI.1"TSF 间修改的检测",提供检测 TSF 数据在 TSF 与另一个可信 IT 产品之间传送时是否被修改的能力,假设另一个可信 IT 产品所使用的安全机制是已知的。

FPT_ITI.2"TSF 间修改的检测与纠正",提供让另一个可信 IT 产品不仅可以检测到 TSF 数据的修改,还可以更正被修改数据的能力,假设另一个可信 IT 产品所使用的安全机制是已知的。

14.4.3 FPT_ITI.1 管理

尚无预见的管理活动。

14.4.4 FPT_ITI.2 管理

FMT 中的管理功能可考虑下列行为：

a) TSF 数据在传送中若被修改，TSF 将试图纠正的那些 TSF 数据类型的管理；

b) TSF 数据在传送过程中被修改，TSF 能采取的动作类型的管理。

14.4.5 FPT_ITI.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：所传送 TSF 数据的修改检测；

b) 基本级：为检测所传送 TSF 数据的修改而采取的动作。

14.4.6 FPT_ITI.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：所传送 TSF 数据的修改检测；

b) 基本级：为检测所传送 TSF 数据的修改而采取的动作；

c) 基本级：纠正机制的使用。

14.4.7 FPT_ITI.1 TSF 间篡改的检测

从属于：无其他组件。

依赖关系：无依赖关系。

14.4.7.1 FPT_ITI.1.1

TSF 应提供能力，以检测在下列度量下：[赋值：*一个既定的修改度量*]TSF 与另一个可信 IT 产品间所传送的所有 TSF 数据是否被修改。

14.4.7.2 FPT_ITI.1.2

TSF 应提供能力，以验证 TSF 与另一个可信 IT 产品间所传送的所有 TSF 数据的完整性，以及如果检测到修改将执行[赋值：*采取的动作*]。

14.4.8 FPT_ITI.2 TSF 间篡改的检测与纠正

从属于：FPT_ITI.1 TSF 间篡改的检测。

依赖关系：无依赖关系。

14.4.8.1 FPT_ITI.2.1

TSF 应提供能力，以检测在下列度量下：[赋值：*一个既定的修改度量*]TSF 与另一个可信 IT 产品间所传送的所有 TSF 数据被修改。

14.4.8.2 FPT_ITI.2.2

TSF 应提供能力，以验证 TSF 与另一个可信 IT 产品间所传送的所有 TSF 数据的完整性，以及如果检测到修改将执行[赋值：*采取的动作*]。

14.4.8.3 FPT_ITI.2.3

TSF 应提供能力，以纠正 TSF 与另一个可信 IT 产品间所传送的所有 TSF 数据的[赋值：*修改类*

型]。

14.5 TOE 内 TSF 数据的传送(FPT_ITT)

14.5.1 族行为

本族提供的要求,旨在解决 TSF 数据通过一个内部信道在 TOE 的不同部件间传送时的保护问题。

14.5.2 组件层次

FPT_ITT.1"内部 TSF 数据传送的基本保护",要求对在 TOE 的不同部件间传送的 TSF 数据进行保护。

FPT_ITT.2"TSF 数据传送的分离",要求 TSF 在传送过程中把用户数据从 TSF 数据中分离出来。

FPT_ITT.3"TSF 数据完整性监视",要求监视在 TOE 不同部件间传送的 TSF 数据是否存在已确定的完整性错误。

14.5.3 FPT_ITT.1 管理

FMT 中的管理功能可考虑下列行为:

a) TSF 要保护的修改类型的管理;

b) 用来保护在 TSF 不同部分间传送数据的机制的管理。

14.5.4 FPT_ITT.2 管理

FMT 中的管理功能可考虑下列行为:

a) TSF 要保护的修改类型的管理;

b) 用来保护在 TSF 不同部分间传送数据的机制的管理;

c) 分离机制的管理。

14.5.5 FPT_ITT.3 管理

FMT 中的管理功能可考虑下列行为:

a) TSF 要保护的修改类型的管理;

b) 用来保护在 TSF 不同部分间传送数据的机制的管理;

c) TSF 试图要检测的 TSF 数据修改类型的管理;

d) 将采取的动作的管理。

14.5.6 FPT_ITT.1、FPT_ITT.2 审计

尚无预见的可审计事件。

14.5.7 FPT_ITT.3 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:TSF 数据的修改检测;

b) 基本级:检测到完整性错误后采取的动作。

14.5.8 FPT_ITT.1 内部 TSF 数据传送的基本保护

从属于:无其他组件。

依赖关系:无依赖关系。

14.5.8.1 FPT_ITT.1.1

TSF 应保护 TSF 数据在 TOE 不同部分间传送时不被[选择:*泄漏*、*修改*]。

14.5.9 FPT_ITT.2 TSF 数据传送的分离

从属于:FPT_ITT.1 内部 TSF 数据传送的基本保护。

依赖关系:无依赖关系。

14.5.9.1 FPT_ITT.2.1

TSF 应保护 TSF 数据在 TOE 不同部分间传送时不被[选择:*泄漏*、*修改*]。

14.5.9.2 FPT_ITT.2.2

当数据在 TOE 不同部分间传送时,TSF 应将用户数据从 TSF 数据中分离出来。

14.5.10 FPT_ITT.3 TSF 数据完整性监视

从属于:无其他组件。

依赖关系:FPT_ITT.1 内部 TSF 数据传送的基本保护。

14.5.10.1 FPT_ITT.3.1

TSF 应能检测在 TOE 不同部分间传送的 TSF 数据的[选择:数据的修改、数据的替换、数据的重排、数据的删除、[赋值:其他类型完整性错误]]。

14.5.10.2 FPT_ITT.3.2

检测到数据的完整性错误后,TSF 应采取下列动作:[赋值:*指定将采取的动作*]。

14.6 TSF 物理保护(FPT_PHP)

14.6.1 族行为

TSF 物理保护组件涉及限制对 TSF 进行未授权的物理访问,以及阻止和抵抗对 TSF 进行未授权的物理修改或替换。

本族中组件的要求确保了 TSF 不被物理侵害和干扰。若满足了这些组件要求,TSF 就可以被封装起来使用,并可检测出物理侵害或抵抗物理侵害。如果没有这些组件,在物理性损害无法避免的环境中,TSF 的保护功能就会失效。关于 TSF 如何对物理侵害尝试作出反应,本族也提供了要求。

14.6.2 组件层次

FPT_PHP.1"物理攻击的被动检测",规定了指示 TSF 设备或 TSF 元件遭到侵害所应具备的特征。然而侵害告知不是自动的,授权用户必须利用一个安全管理功能或进行手工检查才能判断侵害是否发生。

FPT_PHP.2"物理攻击报告",规定了对一个指定的物理渗透子集进行自动侵害通告的要求。

FPT_PHP.3"物理攻击抵抗",规定了防止或抵抗对 TSF 设备和 TSF 元件进行物理侵害所应具备的特征。

14.6.3 FPT_PHP.1 管理

FMT 中的管理功能可考虑下列行为：

a) 确定物理侵害是否发生的用户或角色的管理。

14.6.4 FPT_PHP.2 管理

FMT 中的管理功能可考虑下列行为：

a) 获取入侵报告的用户或角色的管理；

b) 向指定用户或角色报告入侵的设备列表的管理。

14.6.5 FPT_PHP.3 管理

FMT 中的管理功能可考虑下列行为：

a) 对物理侵害的自动应答管理。

14.6.6 FPT_PHP.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：如果使用 IT 手段检测，入侵检测应可审计。

14.6.7 FPT_PHP.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：入侵的检测。

14.6.8 FPT_PHP.3 审计

尚无预见的可审计事件。

14.6.9 FPT_PHP.1 物理攻击的被动检测

从属于：无其他组件。

依赖关系：无依赖关系。

14.6.9.1 FPT_PHP.1.1

TSF 应提供对可能危及 TSF 的物理侵害的明确检测。

14.6.9.2 FPT_PHP.1.2

TSF 应提供确定 TSF 设备或 TSF 元件是否已被物理侵害的能力。

14.6.10 FPT_PHP.2 物理攻击报告

从属于：FPT_PHP.1 物理攻击的被动检测。

依赖关系：FMT_MOF.1 安全功能行为管理。

14.6.10.1 FPT_PHP.2.1

TSF 应提供对可能危及 TSF 的物理侵害的明确检测。

14.6.10.2 FPT_PHP.2.2

TSF 应提供确定 TSF 设备或 TSF 元件是否已被物理侵害的能力。

14.6.10.3 FPT_PHP.2.3

对于[赋值:*需主动检测的 TSF 设备/元件列表*],TSF 应监视这些设备和元件,并当其发生物理侵害时通报给[赋值:*指定的用户或角色*]。

14.6.11 FPT_PHP.3 物理攻击抵抗

从属于:无其他组件。

依赖关系:无依赖关系。

14.6.11.1 FPT_PHP.3.1

TSF 应通过自动响应以抵抗对[赋值:*TSF 设备/元件列表*]的[赋值:*各种物理侵害*],这样才能满足 SFR 要求。

14.7 可信恢复(FPT_RCV)

14.7.1 族行为

本族的要求,确保 TSF 能确定 TOE 是在没有削弱保护能力的情况下启动的,并在运行中断后能在不削弱保护能力的情况下恢复。因为 TSF 的启动状态确定了后续状态的保护情况,故本族是很重要的。

14.7.2 组件层次

FPT_RCV.1“手工恢复”,允许 TOE 只提供人工干预以返回安全状态的机制。

FPT_RCV.2“自动恢复”,规定了对至少一种类型的服务中断,需在无人工干预的情况下恢复到安全状态;对其他类型的服务中断可要求手动恢复。

FPT_RCV.3“无过度损失的自动恢复”,也规定了自动恢复,但通过不允许过度损失被保护的客体来加强要求。

FPT_RCV.4“功能恢复”,规定了在特定的功能层次上进行恢复,确保成功完成恢复或将 TSF 数据回退到一个安全状态。

14.7.3 FPT_RCV.1 管理

FMT 中的管理功能可考虑下列行为:

a) 在维护模式下谁能够获得恢复能力的管理。

14.7.4 FPT_RCV.2 、FPT_RCV.3 管理

FMT 中的管理功能可考虑下列行为:

a) 在维护模式下谁能够获得恢复能力的管理;

b) 对通过自动化程序处理的失效/服务中断列表的管理。

14.7.5 FPT_RCV.4 管理

尚无预见的管理活动。

14.7.6 FPT_RCV.1、FPT_RCV.2、FPT_RCV.3 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：失效或服务中断的发生；

b) 最小级：正常运行的恢复；

c) 基本级：失效或服务中断类型。

14.7.7 FPT_PCV.4 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：如有可能，TOE 安全功能失效后，不能返回到安全状态的可能性；

b) 基本级：如有可能，某个功能失效的检测。

14.7.8 FPT_RCV.1 手工恢复

从属于：无其他组件。

依赖关系：AGD_OPE.1 用户操作指南。

14.7.8.1 FPT_RCV.1.1

当发生[赋值：*失效/服务中断列表*]后，TSF 应进入一种维护模式，该模式提供将 TOE 返回到一个安全状态的能力。

14.7.9 FPT_RCV.2 自动恢复

从属于：FPT_RCV.1 手工恢复。

依赖关系：AGD_OPE.1 用户操作指南。

14.7.9.1 FPT_RCV.2.1

当**不能**从[赋值：*失效/服务中断列表*]**自动恢复**时，TSF 应进入一种维护模式，该模式提供将 TOE 返回到一个安全状态的能力。

14.7.9.2 FPT_RCV.2.2

对[赋值：*失效/服务中断列表*]，TSF 应确保通过自动化过程使 TOE 返回到一个安全状态。

14.7.10 FPT_RCV.3 无过度损失的自动恢复

从属于：FPT_RCV.2 自动恢复。

依赖关系：AGD_OPE.1 用户操作指南。

14.7.10.1 FPT_RCV.3.1

当不能从[赋值：*失效或服务中断列表*]自动恢复时，TSF 应进入一种维护模式，该模式提供将 TOE 返回到一个安全状态的能力。

14.7.10.2 FPT_RCV.3.2

对[赋值：*失效/服务中断列表*]，TSF 应确保通过自动化过程使 TOE 返回到一个安全状态。

14.7.10.3 FPT_RCV.3.3

TSF 提供的从失效或服务中断状态恢复的功能，应确保在 TSF 的控制内 TSF 数据或客体不超出[赋值：*数量*]的情况下，恢复到安全初始状态。

14.7.10.4 FPT_RCV.3.4

TSF 应提供确定客体能否被恢复的能力。

14.7.11 FPT_RCV.4 功能恢复

从属于：无其他组件。

依赖关系：无依赖关系。

14.7.11.1 FPT_RCV.4.1

TSF 应确保[赋值：*功能和失效情景列表*]有如下特性，即功能或者成功完成，或者针对指明的失效情景恢复到一个前后一致的且安全的状态。

14.8 重放检测(FPT_RPL)

14.8.1 族行为

本族负责对各种类型实体(如消息、服务请求、服务应答)的重放检测及随后的纠正动作。只要检测出重放，就可以有效地避免重放。

14.8.2 组件层次

本族只有一个组件，FPT_RPL.1“重放检测”，要求 TSF 应能够检测出既定实体的重放。

14.8.3 FPT_RPL.1 管理

FMT 中的管理功能可考虑下列行为：

a) 应该检测出其重放的既定实体列表的管理；

b) 发生重放时需采取的动作列表的管理。

14.8.4 FPT_RPL.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 基本级：检测到的重放攻击；

b) 详细级：基于具体操作而采取的动作。

14.8.5 FPT_RPL.1 重放检测

从属于：无其他组件。

依赖关系：无依赖关系。

14.8.5.1 FPT_RPL.1.1

TSF 应检测对以下实体的重放：[赋值：*既定实体列表*]。

14.8.5.2 FPT_RPL.1.2

检测到重放时，TSF 应执行[赋值：*具体操作列表*]。

14.9 状态同步协议(FPT_SSP)

14.9.1 族行为

分布式 TOE 由于存在 TOE 各部分间潜在的状态差别及通信延迟等问题，因而比单一 TOE 复杂得多。大多数情况下，分布式功能间的状态同步涉及一个交换协议，而不是一个简单的动作。当在这些协议的分布式环境中存在蓄意的危害时，就需要更为复杂的防御协议。

FPT_SSP“状态同步协议”规定了关于 TSF 某些关键安全功能如何使用该可信协议的要求。FPT_SSP“状态同步协议”确保 TOE 的两个分布式部分(如主机)在完成一个安全有关的动作后，状态保持同步。

14.9.2 组件层次

FPT_SSP.1“简单可信回执”，只要求数据接收者给出简单回执。

FPT_SSP.2“相互可信回执”，要求数据交换相互回执。

14.9.3 FPT_SSP.1、FPT_SSP.2 管理

尚无预见的管理活动。

14.9.4 FPT_SSP.1、FPT_SSP.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：期待接收一个回执时，发生的失效。

14.9.5 FPT_SSP.1 简单可信回执

从属于：无其他组件。

依赖关系：FPT_ITT.1 内部 TSF 数据传送的基本保护。

14.9.5.1 FPT_SSP.1.1

当 TSF 的另一部分发出请求时，TSF 应承认接收到一个未经修改的 TSF 数据传送。

14.9.6 FPT_SSP.2 相互可信回执

从属于：FPT_SSP.1 简单可信回执。

依赖关系：FPT_ITT.1 内部 TSF 数据传送的基本保护。

14.9.6.1 FPT_SSP.2.1

当 TSF 的另一部分发出请求时，TSF 应承认接收到一个未经修改的 TSF 数据传送。

14.9.6.2 FPT_SSP.2.2

TSF 应通过使用回执，确保 TSF 的有关部分知道在不同部分间所传送数据处于正确状态。

14.10 时间戳(FPT_STM)

14.10.1 族行为

本族对一个 TOE 内可靠的时间戳功能提出要求。

14.10.2 组件层次

本族只有一个组件,FPT_STM.1“可靠的时间戳”,要求 TSF 为 TSF 功能提供可靠的时间戳。

14.10.3 FPT_STM.1 管理

FMT 中的管理功能可考虑下列行为:

a) 时间的管理。

14.10.4 FPT_STM.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:时间的改变;

b) 详细级:提供一个时间戳。

14.10.5 FPT_STM.1 可靠的时间戳

从属于:无其他组件。

依赖关系:无依赖关系。

14.10.5.1 FPT_STM.1.1

TSF 应有能力提供可靠的时间戳。

14.11 TSF 间 TSF 数据的一致性(FPT_TDC)

14.11.1 族行为

在分布式环境下,TOE 或许需要与其他可信 IT 产品交换 TSF 数据(如与数据有关的 SFP 属性、审计信息、标识信息等)。本族定义了一些关于在 TOE 的 TSF 和不同可信 IT 产品的 TSF 间共享这些属性并对其作出一致性解释的要求。

14.11.2 组件层次

FPT_TDC.1“TSF 间基本的 TSF 数据一致性”,要求 TSF 提供确保 TSF 间属性一致性的能力。

14.11.3 FPT_TDC.1 管理

尚无预见的管理活动。

14.11.4 FPT_TDC.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:TSF 数据一致性机制的成功使用;

b) 基本级:TSF 数据一致性机制的使用;

c) 基本级:已被解释的 TSF 数据的标识;

d) 基本级:TSF 数据修改的检测。

14.11.5 FPT_TDC.1 TSF 间基本的 TSF 数据一致性

从属于:无其他组件。

依赖关系:无依赖关系。

14.11.5.1 FPT_TDC.1.1

当 TSF 与其他可信 IT 产品共享 TSF 数据时,TSF 应提供对[赋值:*TSF 数据类型列表*]进行一致性解释的能力。

14.11.5.2 FPT_TDC.1.2

当解释来自其他可信 IT 产品的 TSF 数据时,TSF 应使用[赋值:*TSF 使用的解释规则列表*]。

14.12 外部实体测试(FPT_TEE)

14.12.1 族行为

本族定义了实施一个或多个外部实体测试时的 TSF 要求。

这个组件不适用于人类用户。

外部实体可以包括运行在 TOE 上的应用程序,硬件或 TOE 下运行的软件(平台、操作系统等)或与 TOE 连接的应用程序/装置(入侵检测系统、防火墙、登录服务器、时间服务器等)。

14.12.2 组件层次

FPT_TEE.1“外部实体测试”,规定了由 TSF 测试外部实体的要求。

14.12.3 FPT_TEE.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理的外部实体测试发生时的条件管理,例如在最初的启动、有规律的间隔,或规定的条件下;

b) 时间间隔的管理,如适用。

14.12.4 FPT_TEE.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 基本级:外部实体测试的执行和测试结果。

14.12.5 FPT_TEE.1 外部实体的测试

从属于:无其他组件。

依赖关系:无依赖关系。

14.12.5.1 FPT_TEE.1.1

TSF 应运行一套测试[选择:*在最初的启动、定期地正常运行期间、授权用户要求下*,[赋值:*其他条件*]]来检查[赋值:*外部实体特性列表*]的实施。

14.12.5.2 FPT_TEE.1.2

如果测试失败，TSF 将[*赋值：行动*]。

14.13 TOE 内 TSF 数据复制的一致性(FPT_TRC)

14.13.1 族行为

在 TOE 内部复制 TSF 数据时，需要满足本族的要求以确保 TSF 数据的一致性。如果 TOE 不同组成部分间的内部信道不能正常工作，这些复制的 TSF 数据就可能不一致。如果 TOE 内部被构造一个网络并且部分 TOE 网络连接中断时，这种不一致的情况就会在部分 TOE 网络失效时发生。

14.13.2 组件层次

本族只有一个组件，FPT_TRC.1“内部 TSF 的一致性”，要求 TSF 确保 TSF 数据在多处复制时的一致性。

14.13.3 FPT_TRC.1 管理

尚无预见的管理活动。

14.13.4 FPT_TRC.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：重新连接时恢复一致性；

b) 基本级：检测 TSF 数据间的不一致情形。

14.13.5 FPT_TRC.1 内部 TSF 的一致性

从属于：无其他组件。

依赖关系：FPT_ITT.1 内部 TSF 数据传送的基本保护。

14.13.5.1 FPT_TRC.1.1

TSF 应确保 TSF 数据在 TOE 各部分间复制时是前后一致的。

14.13.5.2 FPT_TRC.1.2

当含有所复制 TSF 数据的 TOE 部分断开连接时，TSF 在处理任何对[赋值：*依赖于 TSF 数据复制一致性的功能列表*]的请求前，应确保重建连接后所复制 TSF 数据的一致性。

14.14 TSF 自检(FPT_TST)

14.14.1 族行为

本族定义了一些关于 TSF 自检的要求，这些检测与某些期望的正确操作有关，比如执行功能的接口和 TOE 关键部分的抽样算术运算。这些检测可在启动时进行，或周期性地进行，或应授权用户的请求进行，或满足其他条件时进行。TOE 根据自检结果所采取的动作在其他族中定义。

本族的要求也用于检测由多种失效造成的 TSF 可执行代码(例如：TSF 软件)和 TSF 数据损坏，这种检测并不需要 TOE 停止工作(这将由别的族处理)。因为这些失效不可避免，故必须执行这些检测。这些失效可能是由不可预见的失效方式，或硬件、固件和软件设计上的某些疏忽所造成的，也可能是由

于逻辑和/或物理层面上的保护不当而导致 TSF 被恶意损坏所造成的。

14.14.2 组件层次

FPT_TST.1“TSF 检测”，提供检测 TSF 是否正确运转的能力。这些检测可在启动时进行，或周期性地进行，或当授权用户要求时进行，或满足别的条件时进行。本组件也提供验证 TSF 数据及可执行代码完整性的能力。

14.14.3 FPT_TST.1 管理

FMT 中的管理功能可考虑下列行为：

a) TSF 自检触发条件的管理，如初始化启动期间、固定时间间隔或特定条件；

b) 时间间隔的管理，如果适用。

14.14.4 FPT_TST.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 基本级：TSF 自检的执行及检测结果。

14.14.5 FPT_TST.1 TSF 测试

从属于：无其他组件。

依赖关系：无依赖关系。

14.14.5.1 FPT_TST.1.1

TSF 应在[选择：*初始化启动期间*、*正常工作期间周期性地*、*授权用户要求时*、*在[赋值：产生自检的条件]条件时*]运行一套自检程序以证实[选择：*[赋值：TSF 的组成部分]*、*TSF*]能正确运行。

14.14.5.2 FPT_TST.1.2

TSF 应为授权用户提供验证[选择：*[赋值：TSF 的组成部分]*、*TSF 数据*]完整性的能力。

14.14.5.3 FPT_TST.1.3

TSF 应为授权用户提供验证所存储的 TSF 可执行代码完整性的能力。

15 FRU 类：资源利用

本类提供 3 个族以支持所需资源的可用性，诸如处理能力或存储容量。“容错”族提供保护以防止由 TOE 失效引起的能力不可用。“服务优先级”族确保资源将被分配到更重要的或时间要求更苛刻的任务中，而且不能被优先级低的任务所独占。“资源分配”族提供对可用资源的使用限制，从而防止用户独占资源。本类的组件构成分解如图 15 所示。

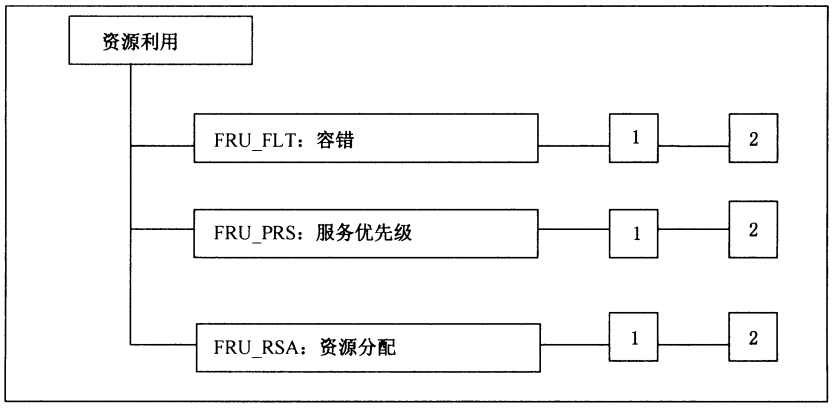

图 15　FRU：资源利用类分解

15.1　容错(FRU_FLT)

15.1.1　族行为

本族的要求确保即便发生了失效，TOE 也将维持正常运转。

15.1.2　组件层次

FRU_FLT.1“降级容错”，要求如果发生了确定的失效，TOE 能继续正确发挥既定能力。

FRU_FLT.2“受限容错”，要求如果发生了确定的失效，TOE 能继续正确发挥所有能力。

15.1.3　FRU_FLT.1、FRU_FLT.2 管理

尚无预见的管理活动。

15.1.4　FRU_FLT.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a)　最小级：TSF 检测出的任何失效；

b)　基本级：由于一个失效而中断的所有 TOE 能力。

15.1.5　FRU_FLT.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a)　最小级：TSF 检测出的任何失效。

15.1.6　FRU_FLT.1 降级容错

从属于：无其他组件。

依赖关系：FPT_FLS.1 带保存安全状态的失效。

15.1.6.1　FRU_FLT.1.1

TSF 应确保当以下失效：[赋值：*失效类型列表*]发生时，[赋值：*TOE 能力列表*]能正常发挥。

15.1.7　FRU_FLT.2 受限容错

从属于：FRU_FLT.1 降级容错。

依赖关系：FPT_FLS.1 带保存安全状态的失效。

15.1.7.1 FRU_FLT.2.1

TSF 应确保当以下失效：[赋值：*失效类型列表*]发生时，**所有 TOE 能力均**能正常发挥。

15.2 服务优先级(FRU_PRS)

15.2.1 族行为

本族的要求允许 TSF 控制用户和主体对 TSF 控制下的资源的使用，以确保 TSF 控制下高优先级活动均能完成，而不受低优先级活动造成的不当干扰或延迟影响。

15.2.2 组件层次

FRU_PRS.1“有限服务优先级”，提供一个主体使用 TSF 控制下某个资源子集的优先级。

FRU_PRS.2“全部服务优先级”，提供一个主体使用 TSF 控制下全部资源的优先级。

15.2.3 FRU_PRS.1、FRU_PRS.2 管理

FMT 中的管理功能可考虑下列行为：

a) TSF 中每个主体优先级的分配。

15.2.4 FRU_PRS.1、FRU_PRS.2 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：基于分配中优先级的使用，对操作的拒绝；

b) 基本级：对涉及服务功能优先级的分配功能的所有使用尝试。

15.2.5 FRU_PRS.1 有限服务优先级

从属于：无其他组件。

依赖关系：无依赖关系。

15.2.5.1 FRU_PRS.1.1

TSF 应给 TSF 中的每个主体分配一个优先级。

15.2.5.2 FRU_PRS.1.2

TSF 应确保对[赋值：*受控资源*]的每次访问都应该基于主体所配得的优先级进行协调。

15.2.6 FRU_PRS.2 全部服务优先级

从属于：FRU_PRS.1 有限服务优先级。

依赖关系：无依赖关系。

15.2.6.1 FRU_PRS.2.1

TSF 应给 TSF 中的每个主体分配一个优先级。

15.2.6.2 FRU_PRS.2.2

TSF 应确保对**所有可共享资源**的每次访问都应该基于主体所配得的优先级进行协调。

15.3 资源分配(FRU_RSA)

15.3.1 族行为

本族的要求允许 TSF 通过控制用户和主体对资源的使用,使得不因未授权地独占资源而出现拒绝服务。

15.3.2 组件层次

FRU_RSA.1"最高配额",提供配额机制的要求,确保用户和主体不会独占某种受控资源。

FRU_RSA.2"最低和最高配额",提供配额机制的要求,确保用户和主体总能至少拥有最少的规定资源且不会独占某种受控资源。

15.3.3 FRU_RSA.1 管理

FMT 中的管理功能可考虑下列行为:

a) 由管理员为用户组、单个用户或主体指定某种资源的最大使用限度。

15.3.4 FRU_RSA.2 管理

FMT 中的管理功能可考虑下列行为:

a) 由管理员为用户组、单个用户或主体指定某种资源的最小和最大使用限度。

15.3.5 FRU_RSA.1、FRU_RSA.2 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:由于资源的限制导致分配操作的拒绝;

b) 基本级:在 TSF 控制下对资源分配功能的所有尝试的使用。

15.3.6 FRU_RSA.1 最高配额

从属于:无其他组件。

依赖关系:无依赖关系。

15.3.6.1 FRU_RSA.1.1

TSF 应对以下资源:[赋值:*受控资源*]分配最高配额,以便[选择:*单个用户、预定义用户组、主体*]能[选择:*同时、在规定的时间间隔内*]使用。

15.3.7 FRU_RSA.2 最低和最高配额

从属于:FRU_RSA.1 最高配额。

依赖关系:无依赖关系。

15.3.7.1 FRU_RSA.2.1

TSF 应对以下资源:[赋值:*受控资源*]分配最高配额,以便[选择:*单个用户、预定义的用户组、主体*]能[选择:*同时、规定的时间间隔内*]使用。

15.3.7.2 FRU_RSA.2.2

TSF 应确保每个[赋值:*受控资源*]的最低供应量,以便[选择:*单个用户、预定义的用户组、主体*]能

[选择:*同时、规定的时间间隔内*]使用。

16 FTA 类:TOE 访问

本类规定用以控制建立用户会话的功能要求。本类的组件构成分解如图 16 所示。

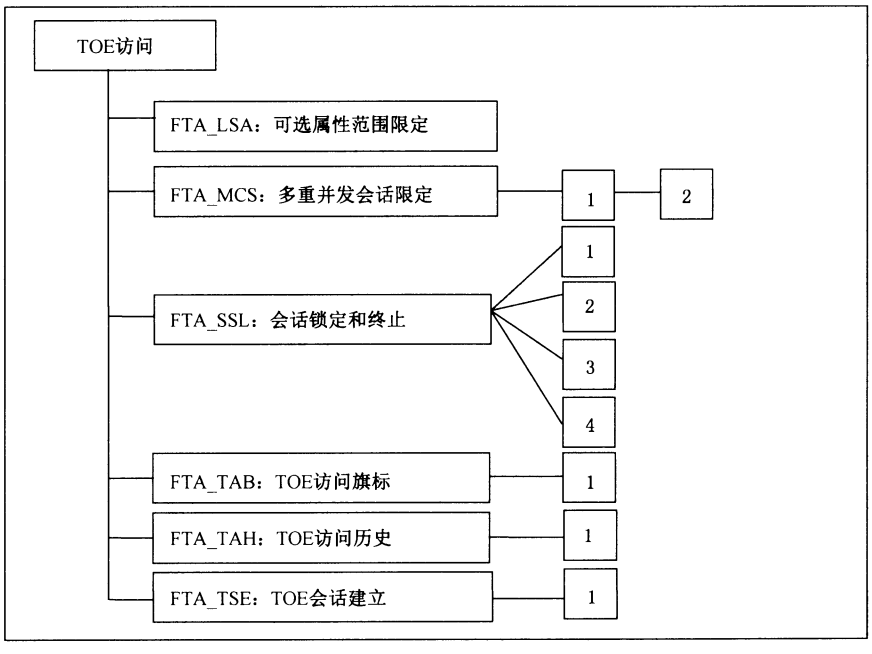

图 16 FTA:TOE 访问类分解

16.1 可选属性范围限定(FTA_LSA)

16.1.1 族行为

本族定义了限制一个用户可以为某个会话选择的会话安全属性范围的要求。

16.1.2 组件层次

FTA_LSA.1“可选属性范围限定”,提供关于 TOE 在建立会话时限制会话安全属性范围的要求。

16.1.3 FTA_LSA.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理员对会话安全属性范围的管理。

16.1.4 FTA_LSA.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:选择某种会话安全属性时的所有失败尝试;

b) 基本级:选择某种会话安全属性时的所有尝试;

c) 详细级:每种会话安全属性的值的获取。

16.1.5 FTA_LSA.1 可选属性范围限定

从属于:无其他组件。

依赖关系:无依赖关系。

16.1.5.1 **FTA_LSA.1.1**

TSF 应基于[赋值:*属性*],限制下列会话安全属性的范围:[赋值:*会话安全属性*]。

16.2 多重并发会话限定(FTA_MCS)

16.2.1 族行为

本族定义了限制属于同一个用户的并发会话数的要求。

16.2.2 组件层次

FTA_MCS.1"多重并发会话的基本限定",提供了适用于 TSF 内所有用户的限定。

FTA_MCS.2"基于属性的单用户多重并发会话限定"要求基于有关安全属性来限制并发会话数的能力,并以此实现对 FTA_MCS.1"多重并发会话的基本限定"的扩展。

16.2.3 FTA_MCS.1 管理

FMT 中的管理功能可考虑下列行为:

a) 管理员所允许的用户并发会话数最大值的管理。

16.2.4 FTA_MCS.2 管理

FMT 中的管理功能可考虑下列行为:

a) 控制管理员所允许的用户并发会话数最大值的规则的管理。

16.2.5 FTA_MCS.1、FTA_MCS.2 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:基于多重并发会话限制对新会话的拒绝;

b) 详细级:当前的用户并发会话数和用户安全属性的捕获。

16.2.6 FTA_MCS.1 多重并发会话的基本限定

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

16.2.6.1 **FTA_MCS.1.1**

TSF 应限制属于同一用户的并发会话的最大数目。

16.2.6.2 **FTA_MCS.1.2**

TSF 应缺省地限制每个用户[赋值:*缺省数*]次会话。

16.2.7 FTA_MCS.2 基于属性的单用户多重并发会话限制

从属于:FTA_MCS.1 多重并发会话的基本限制。

依赖关系:FIA_UID.1 标识的时机。

16.2.7.1 **FTA_MCS.2.1**

TSF 应**依据规则[赋值:*并发会话最大数的规则*]**限制属于同一用户的并发会话的最大数目。

16.2.7.2 FTA_MCS.2.2

TSF 应缺省地限定每个用户[赋值:*缺省数*]次会话。

16.3 会话锁定和终止(FTA_SSL)

16.3.1 族行为

本族为 TSF 定义了一些要求,以提供 TSF 原发和用户原发的交互式会话的锁定和解锁和终止能力。

16.3.2 组件层次

FTA_SSL.1"TSF 原发会话锁定",要求用户在规定的时间内一直不活动,系统就发起对一个交互式会话的锁定。

FTA_SSL.2"用户原发会话锁定",提供用户锁定和解锁其拥有的交互式会话的能力。

FTA_SSL.3"TSF 原发会话终止",为 TSF 提供在用户在一段指定时间不活动后终止该会话的要求。

FTA_SSL.4"用户原发会话终止",为用户提供自己终止交互会话的能力。

16.3.3 FTA_SSL.1 管理

FMT 中的管理功能可考虑下列行为:

a) 对于单个用户不活动时间的规定,达到该时限会话将被锁定;

b) 用户不活动的默认时间的规定,达到该时限会话将被锁定;

c) 会话解锁前发生事件的管理。

16.3.4 FTA_SSL.2 管理

FMT 中的管理功能可考虑下列行为:

a) 会话解锁前发生事件的管理。

16.3.5 FTA_SSL.3 管理

FMT 中的管理功能可考虑下列行为:

a) 对于单个用户不活动时间的规定,达到该时限交互式会话将被终止;

b) 用户不活动的默认时间的规定,达到该时限交互式会话将被终止。

16.3.6 FTA_SSL.4 管理

无预见管理活动。

16.3.7 FTA_SSL.1、FTA_SSL.2 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:利用会话锁定机制对交互式会话的锁定;

b) 最小级:交互式会话的成功解锁;

c) 基本级:对交互式会话解锁的各种尝试。

16.3.8 FTA_SSL.3 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:利用会话锁定机制对交互式会话的终止。

16.3.9 FTA_SSL.4 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”,下列行为应是可审计的:

a) 最小级:用户对交互式会话的终止。

16.3.10 FTA_SSL.1 TSF 原发会话锁定

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

16.3.10.1 FTA_SSL.1.1

TSF 应在达到[赋值:*用户不活动的时间间隔*]后,通过以下方法锁定一个交互式会话:

a) **清除或覆写显示设备,使当前的内容不可读;**

b) **除了会话解锁活动之外,终止用户数据存取/显示设备的任何活动。**

16.3.10.2 FTA _SSL.1.2

TSF 应要求在解锁会话之前发生以下事件:[赋值:*发生的事件*]。

16.3.11 FTA_SSL.2 用户原发会话锁定

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

16.3.11.1 FTA_SSL.2.1

TSF 应允许通过以下方法实现对其拥有的交互会话进行用户原发锁定:

a) **清除或覆写显示设备,使当前的内容不可读;**

b) **除了会话解锁活动之外,终止用户数据存取/显示设备的任何活动。**

16.3.11.2 FTA_SSL2.2

TSF 应要求在解锁会话之前发生以下事件:[赋值:*发生的事件*]。

16.3.12 FTA_SSL.3 TSF 原发会话终止

从属于:无其他组件。

依赖关系:无依赖关系。

16.3.12.1 FTA_SSL.3.1

TSF 应在达到[赋值:*用户不活动的时间间隔*]之后终止一个交互式会话。

16.3.13 FTA_SSL.4 用户原发终止

从属于:无其他组件。

依赖关系:无依赖关系。

16.3.13.1 FTA_SSL.4.1

TSF 应允许用户终止自己的交互式会话。

16.4 TOE 访问旗标(FTA_TAB)

16.4.1 族行为

本族定义了向用户显示有关适当使用 TOE 的一个可配置劝告性警示信息的要求。

16.4.2 组件层次

FTA_TAB.1“缺省的 TOE 访问旗标”,提供了一个 TOE 访问旗标相关的要求。该旗标应在会话的对话建立之前予以显示。

16.4.3 FTA_TAB.1 管理

FMT 中的管理功能可考虑下列行为:

a) 授权管理员对旗标的维护。

16.4.4 FTA_TAB.1 审计

尚无预见的可审计事件。

16.4.5 FTA_TAB.1 缺省的 TOE 访问旗标

从属于:无其他组件。

依赖关系:无依赖关系。

16.4.5.1 FTA_TAB.1.1

在建立一个用户会话之前,TSF 应显示有关未授权使用 TOE 的一个劝告性警示信息。

16.5 TOE 访问历史(FTA_TAH)

16.5.1 族行为

本族定义了 TSF 在成功地建立了会话的基础上,为一个用户显示访问该用户账号的成功和不成功尝试历史的一些要求。

16.5.2 组件层次

FTA_TAH.1“TOE 访问历史”,提供了 TOE 显示与先前尝试建立一个会话相关的信息的要求。

16.5.3 FTA_TAH.1 管理

尚无预见的管理活动。

16.5.4 FTA_TAH.1 审计

尚无预见的可审计事件。

16.5.5 FTA_TAH.1 TOE 访问历史

从属于:无其他组件。

依赖关系:无依赖关系。

16.5.5.1 FTA_TAH.1.1

在会话成功建立的基础上,TSF 应向用户显示上一次成功建立的会话的[赋值:*日期、时间、方法、*

位置]。

16.5.5.2 **FTA_TAH.1.2**

在会话成功建立的基础上,TSF 应显示上一次会话建立的未成功尝试的[赋值:*日期、时间、方法、位置*]和从上一次成功的会话建立以来的不成功尝试次数。

16.5.5.3 **FTA_TAH.1.3**

如果没有向用户提供审阅访问历史信息的机会,TSF 就不能从用户接口擦除该信息。

16.6 TOE 会话建立(FTA_TSE)

16.6.1 族行为

本族定义了拒绝用户与 TOE 建立会话的要求。

16.6.2 组件层次

FTA_TSE.1"TOE 会话建立",提供了拒绝用户基于属性对 TOE 进行访问的要求。

16.6.3 FTA_TSE.1 管理

FMT 中的管理功能可考虑下列行为:

a) 授权管理员对会话建立条件的管理。

16.6.4 FTA_TSE.1 审计

如果 PP/ST 中包含 FAU_GEN"安全审计数据产生",下列行为应是可审计的:

a) 最小级:依据会话建立机制对一个会话建立的拒绝;

b) 基本级:用户会话建立时的所有尝试;

c) 详细级:所选的访问参数值(例如访问位置、访问时间)的获得。

16.6.5 FTA_TSE.1 TOE 会话建立

从属于:无其他组件。

依赖关系:无依赖关系。

16.6.5.1 **FTA_TSE.1.1**

TSF 应能基于[赋值:*属性*]拒绝会话的建立。

17 FTP 类:可信路径/信道

本类中的族提供关于用户和 TSF 之间可信通信路径的要求,以及关于 TSF 和其他可信 IT 产品之间可信通信信道的要求。可信路径和信道具备以下特点:

- 通信路径由内部和外部通信信道构成(对组件适当的话),它将 TSF 数据和命令的确定子集与余下的 TSF 和用户数据分离。
- 通信路径的启用可由用户或 TSF 来发起(对组件适当的话)。
- 通信路径有能力保证用户正在同正确的 TSF 通信,并且 TSF 也正在同正确的用户通信(对组件适当的话)。

在本范型中，可信信道是可以由该信道的任何一端发起的一条通信信道，并且提供该信道两端身份的抗抵赖特性。

可信路径通过与 TSF 进行有保证地直接交互，为用户提供一种手段以完成功能。可信路径通常用于初始标识或鉴别等用户活动，但也可用于用户会话过程中的其他时刻。可信路径的交换可以由用户或 TSF 发起。应确保经由可信路径的用户应答受到保护，不会被不可信应用修改或泄露给不可信应用。

本类的组件构成分解如图 17 所示。

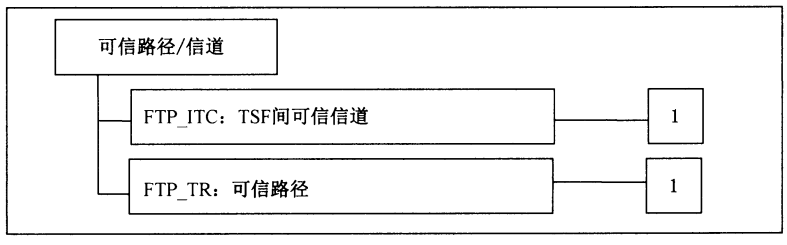

图 17　FTP：可信路径/信道类分解

17.1　TSF 间可信信道(FTP_ITC)

17.1.1　族行为

本族定义为执行关键的安全操作，在 TSF 和其他可信 IT 产品之间建立一个可信信道的要求。只要在 TOE 和其他可信 IT 产品之间进行用户或 TSF 数据的保密通信，就应包括本族的要求。

17.1.2　组件层次

FTP_ITC.1“TSF 间可信信道”，要求 TSF 在它自己和另一个可信 IT 产品之间提供一条可信信道。

17.1.3　FTP_ITC.1 管理

FMT 中的管理功能可考虑下列行为：

a)　需要可信信道的动作的配置，如果支持的话。

17.1.4　FTP_ITC.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a)　最小级：可信信道功能的失效；

b)　最小级：失效的可信信道功能的发起者和目标端的标识；

c)　基本级：可信信道功能的所有使用尝试；

d)　基本级：所有可信信道功能的发起者和目标端的标识。

17.1.5　FTP_ITC.1 TSF 间可信信道

从属于：无其他组件。

依赖关系：无依赖关系。

17.1.5.1　FTP_ITC.1.1

TSF 应在它自己和另一个可信 IT 产品之间提供一条通信信道，此信道在逻辑上与其他通信信道截

然不同，并对其端点进行了有保障的标识，且能保护信道中数据免遭修改或泄露。

17.1.5.2 **FTP_ITC.1.2**

TSF 应允许[选择：*TSF*、*另一个可信 IT 产品*]经由可信信道发起通信。

17.1.5.3 **FTP_ITC.1.3**

对于[赋值：*需要可信信道的功能列表*]，TSF 应经由可信信道发起通信。

17.2 可信路径(FTP_TRP)

17.2.1 族行为

本族定义了建立并维护用户和 TSF 间可信通信的要求。对任何与安全有关的交互活动而言，一条可信路径可能是必需的。可信路径的交换可以由用户在与 TSF 交互期间发起，或者 TSF 可能经由一条可信路径与用户建立通信。

17.2.2 组件层次

FTP_TRP.1“可信路径”，要求为 PP/ST 作者定义的一组事件，在 TSF 和用户之间提供一条可信路径。用户或 TSF 均有能力发起该可信路径。

17.2.3 FTP_TRP.1 管理

FMT 中的管理功能可考虑下列行为：

a) 需要可信路径的动作的配置，如果支持的话。

17.2.4 FTP_TRP.1 审计

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 最小级：可信路径功能的失效；

b) 最小级：如果有的话，与所有可信路径失效相关的用户标识；

c) 基本级：可信路径功能的所有使用尝试；

d) 基本级：如果有的话，与所有可信路径调用相关的用户标识。

17.2.5 FTP_TRP.1 可信路径

从属于：无其他组件。

依赖关系：无依赖关系。

17.2.5.1 **FTP_TRP.1.1**

TSF 应在它自己和[选择：*远程*、*本地*]用户之间提供一条通信路径，此路径在逻辑上与其他通信路径截然不同，并对其端点进行了有保障的标识，并能保护通信数据免遭[选择：*修改*、泄露[*赋值：其他类型的完整性或机密性违背*]]。

17.2.5.2 **FTP_TRP.1.2**

TSF 应允许[选择：*TSF*、*本地用户*、*远程用户*]经由可信路径发起通信。

17.2.5.3 **FTP_TRP.1.3**

对于[选择：*启动用户鉴别*、[*赋值：其他需要可信路径的服务*]]，TSF 应要求使用可信路径。

附 录 A
（规范性附录）
安全功能要求应用注释

本附录包含关于本部分中所定义族和组件的附加指南，用户、开发者和评估者在使用组件时可能需要参考这些指南。为了便于查找，本附录中类、族和组件的表示与标准中的表示相似。

A.1 注释的结构

本条定义与本标准功能要求相关的注释的内容和形式。

A.1.1 类结构

下面的图 A.1 说明本附录中功能类的结构。

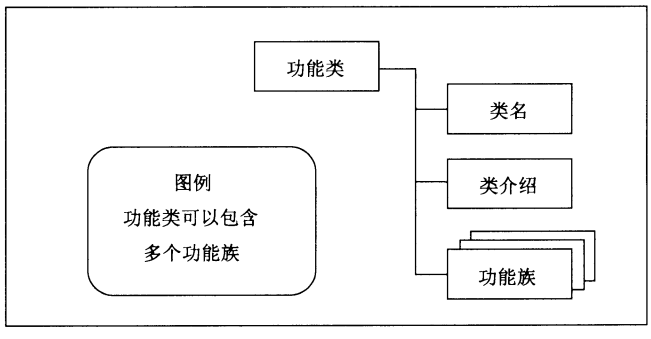

图 A.1 功能类结构

A.1.1.1 类名

这是本部分中所定义类的唯一名称。

A.1.1.2 类介绍

本附录中的类介绍提供使用该类中族和组件的有关信息。这些信息连同相关的图表描述了每个类的组织形式和每个类中的族，以及每个族中组件间的层次关系。

A.1.2 族结构

图 A.2 用图解形式说明应用注释部分功能族的结构。

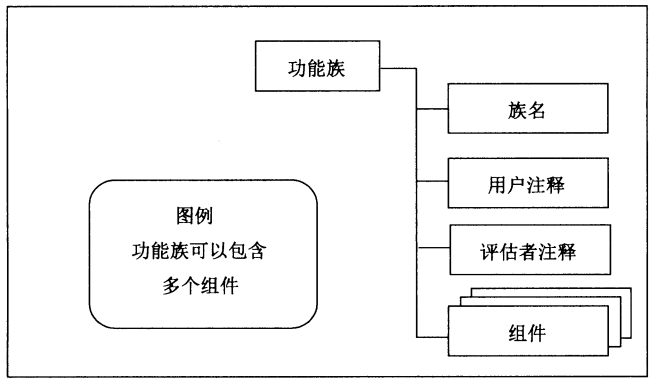

图 A.2 功能族结构及应用注释

A.1.2.1 族名

这是本部分中所定义族的唯一名称。

A.1.2.2 用户注释

用户注释包含功能族的潜在用户所关心的一些附加信息。潜在用户包括 PP、ST 和功能包的作者，以及具体化功能组件的 TOE 开发者。本部分陈述是提示性的，可包括与使用的局限性有关的一些警示信息以及使用组件时应当特别注意的地方。

A.1.2.3 评估者注释

评估者注释包含 TOE 开发者和评估者所关心的所有信息。该 TOE 声称符合族中某一组件。本部分陈述是提示性的，可涵盖评估 TOE 时需特别注意的各个方面，其中可包括澄清含义，详细说明解释这些要求的方式，以及评估者特别关心的一些警告和警示信息。

“用户注释”和“评估者注释”这两条不是必需的，仅在适当时出现。

A.1.3 组件结构

图 A.3 说明了应用注释部分功能组件的结构。

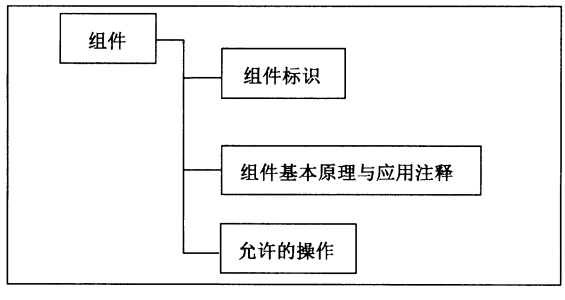

图 A.3 功能组件结构

A.1.3.1 组件标识

这是本部分中所定义组件的唯一名称。

A.1.3.2 组件基本原理与应用注释

任何与组件有关的特定信息都可在本条中找到。

- *基本原理*包含基本原理的详细解释，在特定级别下细化关于基本原理的一般性陈述，且应仅在需要特定级别详述的情况下使用。
- *应用注释*包含对于一个特定组件在叙述的详细程度方面的进一步的细化。这种细化可相对于 A.1.2 条所描述的用户注释或评估者注释。这种细化可用于解释依赖关系的性质(例如，共享信息或共享操作)。

本条内容不是必需的，仅在适当时出现。

A.1.3.3 允许的操作

每个组件的这部分内容包含与该组件所允许的操作有关的一些建议。

本条内容不是必需的，仅在适当时出现。

A.2 依赖关系表

以下的功能组件依赖关系表列出了功能组件之间直接、间接和可选的依赖关系。作为功能组件依赖方的每个组件在表中占据一列，每个功能组件在表中占据一行。表格单元中的值表示行中标的组件是直接要求列中标的组件(用“×”表示)，间接要求列中标的组件(用“—”表示)，还是可选要求列中标的组件(用“○”表示)。例如 FDP_ETC.1“不带安全属性的用户数据输出”就是一个具有可选依赖关系的组件，它要求依赖 FDP_ACC.1“子集访问控制”，或依赖 FDP_IFC.1“子集信息流控制”，所以如果满足了 FDP_ACC.1，就不必满足 FDP_IFC.1，反之亦然。如果表格单元为空，则该组件不依赖于另一个组件。表 A.1～表 A.10 分别给出了各类组件的依赖关系。

表 A.1 FAU：安全审计类依赖关系表

	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_ARP.1	—	×							—
FAU_GEN.1									×
FAU_GEN.2	×				×				—
FAU_SAA.1	×								—
FAU_SAA.2					×				
FAU_SAA.3									
FAU_SAA.4									
FAU_SAR.1	×								—
FAU_SAR.2	—		×						—
FAU_SAR.3	—		×						—
FAU_SEL.1	×				—	×	—	—	—
FAU_STG.1	×								—
FAU_STG.2	×								—

表 A.1（续）

	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_STG.3	—			×					—
FAU_STG.4	—			×					—

表 A.2 FCO：通信类依赖关系表

	FIA_UID.1
FCO_NRO.1	×
FCO_NRO.2	×
FCO_NRR.1	×
FCO_NRR.2	×

表 A.3 FCS：密码支持类依赖关系表

	FCS-CKM.1	FCS-CKM.2	FCS-CKM.4	FCS-COP.1	FDP-ACC.1	FDP-ACF.1	FDP-IFC.1	FDP-IFF.1	FDP-ITC.1	FDP-ITC.2	FIA-UID.1	FMT-MSA.1	FMT-MSA.3	FMT-SMF.1	FMT-SMR.1	FPT-TDC.1	FTP-ITC.1	FTP-TRP.1
FCS_CKM.1	—	○	×	○	—	—	—	—	—	—	—	—	—	—	—	—	—	—
FCS_CKM.2	○	—	×	—	—	—	—	—	○	○	—	—	—	—	—	—	—	—
FCS_CKM.3	○	—	×	—	—	—	—	—	○	○	—	—	—	—	—	—	—	—
FCS_CKM.4	○	—	—	—	—	—	—	—	○	○	—	—	—	—	—	—	—	—
FCS_COP.1	○	—	×	—	—	—	—	—	○	○	—	—	—	—	—	—	—	—

表 A.4 FDP：用户数据保护类依赖关系表

	FDP-ACC.1	FDP-ACF.1	FDP-IFC.1	FDP-IFF.1	FDP-ITT.1	FDP-ITT.2	FDP-UIT.1	FIA-UID.1	FMT-MSA.1	FMT-MSA.3	FMT-SMF.1	FMT-SMR.1	FPT-TDC.1	FTP-ITC.1	FTP-TRP.1
FDP_ACC.1	—	×	—	—				—	—	—	—	—			
FDP_ACC.2	—	×	—	—				—	—	—	—	—			
FDP_ACF.1	×	—	—	—				—	—	×	—	—			
FDP_DAU.1															
FDP_DAU.2								×							
FDP_ETC.1	○	—	○	—				—	—	—	—	—			

表 A.4（续）

	FDP-ACC.1	FDP-ACF.1	FDP-IFC.1	FDP-IFF.1	FDP-ITT.1	FDP-ITT.2	FDP-UIT.1	FIA-UID.1	FMT-MSA.1	FMT-MSA.3	FMT-SMF.1	FMT-SMR.1	FPT-TDC.1	FTP-ITC.1	FTP-TRP.1
FDP_ETC.2	○	—	○	—				—	—	—	—	—			
FDP_IFC.1	—	—	—	×				—	—	—	—	—			
FDP_IFC.2	—	—	—	×				—	—	—	—	—			
FDP_IFF.1	—	—	×	—				—	—	×	—	—			
FDP_IFF.2	—	—	×	—				—	—	×	—	—			
FDP_IFF.3	—	—	×	—				—	—	—	—	—			
FDP_IFF.4	—	—	×	—				—	—	—	—	—			
FDP_IFF.5	—	—	×	—				—	—	—	—	—			
FDP_IFF.6	—	—	×	—				—	—	—	—	—			
FDP_ITC.1	○	—	○	—				—	—	×	—	—			
FDP_ITC.2	○	—	○	—				—	—	—	—	—	×	○	○
FDP_ITT.1	○	—	○	—				—	—	—	—	—			
FDP_ITT.2	○	—	○	—				—	—	—	—	—			
FDP_ITT.3	○	—	○	—	×			—	—	—	—	—			
FDP_ITT.4	○	—	○	—		×		—	—	—	—	—			
FDP_RIP.1															
FDP_RIP.2															
FDP_ROL.1	○	—	○	—				—	—	—	—	—			
FDP_ROL.2	○	—	○	—				—	—	—	—	—			
FDP_SDI.1															
FDP_SDI.2															
FDP_UCT.1	○	—	○	—				—	—	—	—	—		○	○
FDP_UIT.1	○	—	○	—				—	—	—	—	—		○	○
FDP_UIT.2	○	—	○	—			○	—	—	—	—	—		○	—
FDP_UIT.3	○	—	○	—			○	—	—	—	—	—		○	—

表 A.5 FIA：标识和鉴别类依赖关系表

	FIA_ATD.1	FIA_UAU.1	FIA_UID.1
FIA_AFL.1		×	—
FIA_ATD.1			

表 A.5（续）

	FIA_ATD.1	FIA_UAU.1	FIA_UID.1
FIA_SOS.1			
FIA_SOS.2			
FIA_UAU.1			×
FIA_UAU.2			×
FIA_UAU.3			
FIA_UAU.4			
FIA_UAU.5			
FIA_UAU.6			
FIA_UAU.7		×	—
FIA_UID.1			
FIA_UID.2			
FIA_USB.1	×		

表 A.6 FMT：安全管理类依赖关系表

	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FMT_MOF.1					—				×	×	
FMT_MSA.1	○	—	○	—	—	—	—		×	×	
FMT_MSA.2	○	—	○	—	—	×	—		—	×	
FMT_MSA.3	—	—	—	—	—	×	—		—	×	
FMT_MSA.4	○	—	○	—	—	—	—		—	—	
FMT_MTD.1					—				×	×	
FMT_MTD.2					—			×	—	×	
FMT_MTD.3					—			×	—	—	
FMT_REV.1					—					×	
FMT_SAE.1					—					×	×
FMT_SMF.1											
FMT_SMR.1					×						
FMT_SMR.2					×						
FMT_SMR.3					—					×	

表 A.7 FPR:隐私类依赖关系表

	FIA_UID.1	FPR_UNO.1
FPR_ANO.1		
FPR_ANO.2		
FPR_PSE.1		
FPR_PSE.2	×	
FPR_PSE.3		
FPR_UNL.1		
FPR_UNO.1		
FPR_UNO.2		
FPR_UNO.3		×
FPR_UNO.4		

表 A.8 FPT:TSF 保护类依赖关系表

	AGD_OPE.1.1	FIA_UID.1	FMT_MOF.1	FMT_SMF.1	FMT_SMR.1	FPT_ITT.1
FPT_FLS.1						
FPT_ITA.1						
FPT_ITC.1						
FPT_ITI.1						
FPT_ITI.2						
FPT_ITT.1						
FPT_ITT.2						
FPT_ITT.3						×
FPT_PHP.1						
FPT_PHP.2		—	×	—	—	
FPT_PHP.3						
FPT_RCV.1	×					
FPT_RCV.2	×					
FPT_RCV.3	×					
FPT_RCV.4						
FPT_RPL.1						
FPT_SSP.1						×
FPT_SSP.2						×
FPT_STM.1						
FPT_TDC.1						

表 A.8（续）

	AGD_OPE.1.1	FIA_UID.1	FMT_MOF.1	FMT_SMF.1	FMT_SMR.1	FPT_ITT.1
FPT_TEE.1						
FPT_TRC.1						×
FPT_TST.1						

表 A.9 FRU：资源利用类依赖关系表

	FPT_FLS.1
FRU_FLT.1	×
FRU_FLT.2	×
FRU_PRS.1	
FRU_PRS.2	
FRU_RSA.1	
FRU_RSA.2	

表 A.10 FTA：TOE 访问类依赖关系表

	FIA_UAU.1	FIA_UID.1
FTA_LSA.1		
FTA_MCS.1		×
FTA_MCS.2		×
FTA_SSL.1	×	—
FTA_SSL.2	×	—
FTA_SSL.3		
FTA_SSL.4		
FTA_TAB.1		
FTA_TAH.1		
FTA_TSE.1		

附 录 B
（规范性附录）
功能类、族和组件

下面的附录C～附录M提供本部分正文中定义的功能类的应用注释。

附 录 C
（规范性附录）
FAU 类：安全审计

本标准的审计族允许 PP/ST 作者能够定义监测用户活动以及在某些情况下检测对 TSP 真实的、可能的或即将发生的侵害等方面的要求。定义 TOE 的安全审计功能有助于监测与安全有关的事件，并能对安全侵害起到威慑作用。审计族的要求涉及审计数据保护、记录格式和事件选择，以及分析工具、侵害报警和实时分析等功能。审计迹应以易读的格式直接（如存储）或间接（如使用审计归纳工具）呈现。

在开发安全审计要求时，PP/ST 作者必须注意审计族及其组件之间的相互关系。存在这样的可能：规定了一组遵从族/组件依赖表的审计要求，但同时导致了一个有缺陷的审计功能（例如，某个审计功能要求对所有与安全有关的事件加以审计，但是缺乏基于任何合理的基础，诸如按单个用户或客体来选择性控制它们）。

C.1 在分布式环境中的审计要求

对网络和其他大型系统的审计要求，在实现上可能明显地有别于那些独立系统。对于更大、更复杂和更活跃的系统而言，由于解释（甚至存储）所收集审计数据的可行性较低，所以必须更多地考虑收集哪些审计数据以及如何对其进行管理。在一个随时可能发生许多事件的多时区全球性网络中，按时间排序罗列或“跟踪”被审计事件的传统方法可能就不适用。

此外，在分布式 TOE 中的不同主机和服务器可能具有不同的命名策略和名称。对于审计查阅而言，符号名称的表示法可能就需要在整个网络范围内加以约定，以避免重复和“命名冲突”。

如果在分布式系统中审计仓库服务于一个实用的功能，则可能需要一个多对象审计仓库，其中该仓库的某一部分可以接受潜在的各种各样的授权用户的访问。

最后，授权用户的权限滥用问题，应通过彻底避免在本地存储与管理员活动有关的审计数据来解决。

本类的组件构成分解如图 C.1 所示。

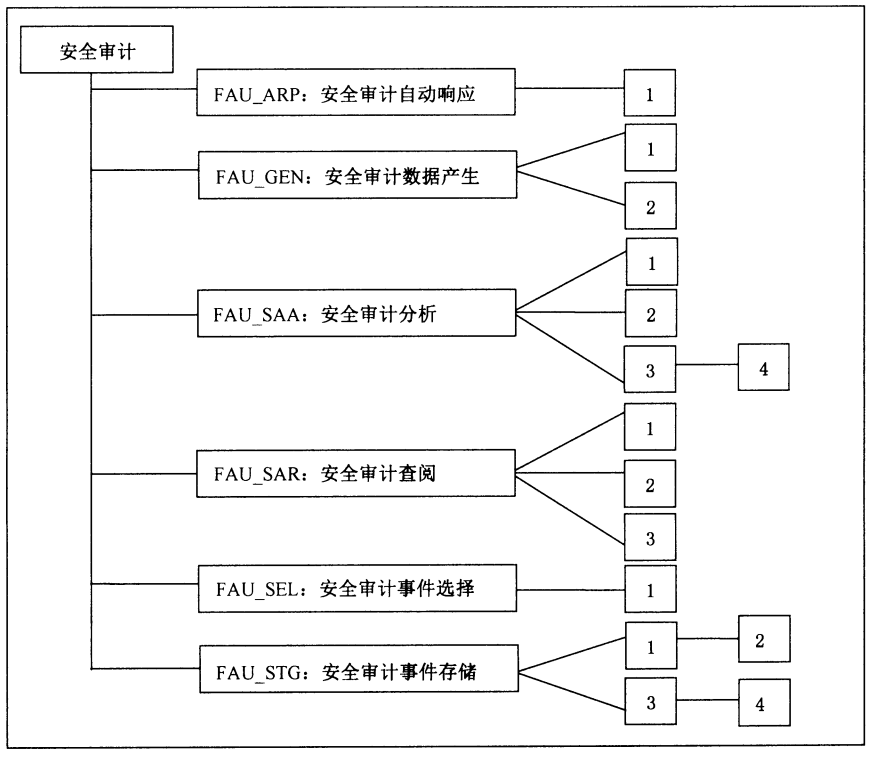

图 C.1　FAU 安全审计类分解

C.2　安全审计自动响应(FAU_ARP)

C.2.1　用户注释

安全审计自动响应族描述了处理审计事件的要求。这些要求包括告警或 TSF 采取动作(自动应答)。例如,TSF 可能采取的动作包括产生实时报警、终止违例进程、中断服务、断开连接或者使用户账号失效等。

如果 FAU_SAA“安全审计分析”中的组件指出一个审计事件是对 TSP 的一个潜在侵害,那么定义该审计事件为一个“潜在的安全侵害”。

C.2.2　FAU_ARP.1 安全告警

C.2.2.1　用户应用注释

应在出现一个告警事件之后随即采取动作。这种动作可以是通知授权用户,可以是提供给授权用户一组可能的遏制动作,或是采取纠正动作,PP/ST 作者应认真考虑采取这些动作的时机。

C.2.2.2　操作

C.2.2.2.1　赋值

在 FAU_ARP.1.1 中,PP/ST 作者应详细说明一旦出现潜在的安全侵害时要采取的动作。“通知授权用户,使产生潜在安全侵害的主体失效”就是动作列表的一个例子。也可以详细说明由授权用户来确定要采取的动作。

C.3 安全审计数据产生(FAU_GEN)

C.3.1 用户注释

安全审计数据产生族包括了详细说明应由 TSF 生成、与安全有关的审计事件的要求。

引入本族在某种意义上避免了一种关于所有需要审计支持的组件的依赖关系。在本部分中每个组件都有一个审计条,在该条中列出了该功能区中要审计的事件。当 PP/ST 作者编写 PP/ST 时,相关组件审计部分中的条款可用来填补本组件中的变量。这样,对于一个功能区中能够被审计的详细规范就局限在该功能区中。

可审计事件的列表完全依赖于 PP/ST 内其他功能族,所以每个族的定义应包括该族所规定的可审计事件列表。在功能族中所规定可审计事件列表中的每个可审计事件必须对应于本族所规定的某个审计事件产生级别(例如最小级、基本级和详细级)。这就向 PP/ST 作者提供了必要的信息,以确保所有适当的可审计事件都将在 PP/ST 中加以规范。下面的例子说明了可审计事件如何在适当的功能族中加以规定:

"如果 PP/ST 中包含 FAU_GEN'安全审计数据产生',下列行为应是可审计的:

a) 最小级:用户安全属性管理功能的成功使用;

b) 基本级:用户安全属性管理功能的所有尝试使用;

c) 基本级:用户安全属性已被修改的标识;

d) 详细级:除特定敏感属性数据项(如口令、密钥)以外,应俘获新的属性值。"

对于所选定的每一个功能组件,该组件所指出的可审计事件,只要属 FAU_GEN"安全审计数据产生"指定的级别和低于该级别都应被审计。例如,在上面的例子中,如果 FAU_GEN"安全审计数据产生"中选择了"基本级",则 a)、b)和 c)中提到的可审计事件必须被审计。

很明显,可审计事件的分类是层次化的。例如,当期望"基本级审计产生"时,通过使用适当的赋值操作,所有被标识为最小级或基本级的可审计事件都应包括在 PP/ST 之内,除非高级别的事件只是比低级别事件提供的信息更详细。当期望"详细级产生审计"时,所有已标识的可审计事件(最小级、基本级和详细级)都应该包括在 PP/ST 之内。

PP/ST 的作者可以决定增加一些超出给定审计级别要求之外的可审计事件。例如,某个 PP/ST 尽管包含了大部分基本级能力,由于少数几个基本级能力因与 PP/ST 中其他的约束要求相冲突(例如它们需要收集不可用的数据)而没有被包括进来,因此仅可声称具备最小级审计能力。

创建可审计事件的功能应在 PP 或 ST 中作为一项功能要求加以规定。

下面列出了一些应该在每个 PP/ST 功能要求中定义为可审计事件的事件类型例子:

a) 把 TSF 控制之内的客体引入到一个主体的地址空间;

b) 客体的删除;

c) 访问权限或能力的分配和撤消;

d) 改变主体或客体的安全属性;

e) 由 TSF 执行的策略检查,作为一个主体的请求结果;

f) 访问权限的使用以回避策略检查;

g) 标识和鉴别功能的使用;

h) 操作员或授权用户所采取的动作(如禁止可读标签这样的一个 TSF 保护机制);

i) 从可移动介质输出数据或将数据输入到可移动介质(如打印输出、磁带和磁盘等)。

C.3.2 FAU_GEN.1 审计数据产生

C.3.2.1 用户应用注释

本组件定义了标识可审计事件的一些要求，包括应产生审计记录以及审计记录中所应提供的信息。

当 SFR 不要求单个用户身份与审计事件相关联时，可单独使用 FAU_GEN.1“审计数据产生”，当 PP/ST 包含隐私要求时这种情况就可能存在。如果必须在审计中考虑用户身份，就应增加使用 FAU_GEN.2“用户身份关联”。

如果主体是一个用户，用户身份可能作为主体身份被记录。如果用户鉴别(FIA_UAU)没有被应用，用户的身份可能还没有被验证。因此在一个无效登录的实例中所声称的用户身份应该被记录。应考虑指明已记录的身份没有被鉴别的情况。

C.3.2.2 评估者注释

存在与 FPT_STM“时间戳”的依赖关系，如果时间的正确性对 TOE 而言不是问题，可删去这一依赖关系。

C.3.2.3 操作

C.3.2.3.1 选择

在 FAU_GEN.1.1 中，PP/ST 作者应选择 PP/ST 中其他功能组件的审计条中所提出的可审计事件级别。这些级别可以是“最小级”、“基本级”、“详细级”或“未规定”。

C.3.2.3.2 赋值

在 FAU_GEN.1.1 中，PP/ST 作者应指定一个其他专门定义的可审计事件列表，一并归入可审计事件列表中。这种赋值可以是“无”，也可以是一个功能要求的可审计事件，其审计级别比 b)中所要求的审计级别更高，也可以是由特定应用程序接口(API)的使用而产生的一些事件。

在 FAU_GEN.1.2 中，PP/ST 作者应对 PP/ST 中每个可审计事件指定一个其他审计相关信息列表，并将其纳入审计事件记录中，或者指定为“无”。

C.3.3 FAU_GEN.2 用户身份关联

C.3.3.1 用户应用注释

本组件负责处理在单个用户身份级别上可审计事件的责任追溯性方面要求。本组件应该用作 FAU_GEN.1“审计数据产生”的补充。

审计要求和隐私要求之间存在着潜在的冲突，为了审计，希望能了解谁完成了一个动作，而该用户则可能希望只有自己知道自己的动作，而不被他人(如同事)识别出，或者可能在组织安全策略要求必须保护用户身份。在这些情况下，审计与隐私的目标是互相矛盾的。所以，如果选定这一审计要求，并且隐私也很重要，应考虑增加用户假名组件。隐私类中规定了基于假名确定真实用户名的要求。

如果用户的身份还没有通过鉴别被验证，在一个无效登录的实例中所声称的用户身份应该被记录。应考虑指明已记录的身份没有被鉴别的情况。

C.4 安全审计分析(FAU_SAA)

C.4.1 用户注释

本族定义关于自动方式分析系统活动和审计数据，以寻找可能的或真实的安全侵害等方面的要求。

这种分析可以由入侵检测来支持，或通过对潜在的安全侵害作出自动响应来支持。

FAU_ARP“安全审计自动响应”中的组件定义了在检测到潜在的安全侵害后，TSF 应采取的动作。

为了实时分析，审计数据可能被转换成一种便于自动处理的格式，在交付给授权用户查阅时再转换成另一种可读格式。

C.4.2 FAU_SAA.1 潜在的侵害分析

C.4.2.1 用户应用注释

本组件用于详细说明一个可审计事件集，这些事件的出现或累计出现预示着一个对 SFR 的执行的潜在侵害，也用来规定用于执行侵害分析的所有规则。

C.4.2.2 操作

C.4.2.2.1 赋值

在 FAU_SAA.1.2 中，PP/ST 作者应识别已定义的可审计事件的子集，需要检测这些事件的出现或累计出现，作为对 SFR 的执行的潜在侵害的一个预示。

在 FAU_SAA.1.2 中，PP/ST 作者应详细说明 TSF 用于分析审计迹的所有其他规则，这些规则可以包括需要事件在某个确定的时间周期内（如天数、持续时间）出现的特殊要求。如果没有额外的规则供 TSF 用于分析审计迹，则此赋值可以为“无”。

C.4.3 FAU_SAA.2 基于轮廓的异常检测

C.4.3.1 用户应用注释

*轮廓*是一种表征用户或主体行为的结构，它描绘了用户/主体怎样以各种方法与 TSF 交互。使用模式的建立对应于用户/主体所从事的各种类型活动，例如异常情况出现模式、资源利用模式（何时、哪个、怎样）、动作执行模式等。轮廓中记录各种类型活动的方式（如资源测量、事件计数器、定时器），称作轮廓度量。

每个轮廓代表由*轮廓目标组*成员执行的预期使用模式。此模式可以基于过去的使用（历史模式）或相似目标组用户的正常使用（预期模式）。轮廓目标组指与 TSF 交互的一个或多个用户。轮廓组每个成员的活动被分析工具用来建立轮廓中描绘的使用模式。以下是几个轮廓目标组的例子：

a) **单用户账号**：每个用户一个轮廓。

b) **组 ID 或组账号**：所有拥有同一个组 ID 或使用同一个组账号的用户为一个轮廓。

c) **操作角色**：共享一个给定操作角色的所有用户为一个轮廓。

d) **系统**：某系统的所有用户为一个轮廓。

对一个轮廓目标组的每个成员分配了一个单独的*置疑等级*，它表示成员的新活动对应于在组轮廓中已建立使用模式的相近程度。

异常检测工具的复杂程度将主要由 PP/ST 所要求目标轮廓组的数量和所要求轮廓度量的复杂性来确定。

PP/ST 作者应该明确列举出由 TSF 监测或分析的活动。PP/ST 作者也应该明确识别构造使用轮廓所需的相关活动信息。

FAU_SAA.2“基于轮廓的异常检测”要求 TSF 维护系统的使用轮廓。“维护”这个词暗示异常检测工具基于轮廓目标组成员进行的新活动来主动更新使用轮廓。重点的是表示用户活动性的度量都由 PP/ST 作者来定义。例如，一个个体可能执行一千个不同的动作，而异常检测工具可以仅选择监测这些活动的一个子集。异常活动可以像正常活动一样被集成到轮廓中（假设工具正在监测那些活动）。在

四个月以前可能已出现异常的事件经过一段时间，随着用户职责的改变可能已变成正常（反之亦然）。如果 TSF 利用轮廓更新算法过滤掉异常活动，它就不能够捕获这种情况。

应提供管理性通告，以便于授权用户理解置疑等级的重要性。

PP/ST 作者应定义如何解释置疑等级和向 FAU_ARP“安全审计自动响应”机制指示异常活动的条件。

C.4.3.2 操作

C.4.3.2.1 赋值

在 FAU_SAA.2.1 中，PP/ST 作者应详细说明轮廓目标组。单个 PP/ST 可包括多个轮廓目标组。

在 FAU_SAA.2.3 中，PP/ST 作者应详细说明由 TSF 报告的异常活动的条件。条件可以包括达到某一确定值的置疑等级，或基于观察到的异常活动的类型。

C.4.4 FAU_SAA.3 简单攻击探测

C.4.4.1 用户应用注释

实际上，很少有分析工具能确切检测到安全侵害即将在何时发生，但确实有一些系统事件非常重要，值得进行单独查阅。这种事件的例子有，删除一个关键 TSF 安全数据文件（如口令文件）或远程用户试图获得管理员级特权的行为。这些事件都称作*特征事件*，如果它们的出现独立于系统的其他活动就预示着入侵活动。

给定工具的复杂程度将在很大程度上依赖于 PP/ST 作者在确定特征事件基本集时所定义的赋值。

为执行分析，PP/ST 作者应逐一列举出哪些事件应该由 TSF 监测。PP/ST 作者应识别那些与事件有关的必要信息，以确定该事件是否映射为特征事件。

应提供管理性通告，以便授权用户能够理解事件的意义以及如何做出适当的响应。

为了避免把审计数据作为监测系统活动唯一的输入，在这些功能要求的详细说明中要求利用以前开发的入侵检测工具，而该工具不只使用审计数据进行系统活动分析（其他的输入数据包括如网络数据报文、资源/计账数据或者各类系统数据的组合等）。

FAU_SAA.3“简单攻击探测”的元素不要求实现直接攻击探测的 TSF 与其活动受监测的 TSF 为同一个。因此，可以开发一个入侵检测组件，其运行能够独立于那些系统活动正在被分析的系统。

C.4.4.2 操作

C.4.4.2.1 赋值

在 FAU_SAA.3.1 中，PP/ST 作者应确定系统事件的一个基本子集，其出现独立于所有其他系统活动，可预示着一个对 SFR 的执行的侵害。这包括那些本身就清晰地指明对 SFR 的执行侵害的事件，或其出现对证明活动正常十分重要的那些事件。

在 FAU_SAA.3.2 中，PP/ST 作者应详细说明用于确定系统活动的信息。该信息是分析工具所使用的输入数据，用来确定发生在 TOE 上的系统活动。这些数据可包括审计数据、审计数据与其他系统数据的组合、或者也可由其他非审计数据组成。PP/ST 作者应准确定义在所输入的数据中哪些系统事件及其属性正在被监测。

C.4.5 FAU_SAA.4 复杂攻击探测

C.4.5.1 用户应用注释

实际上，很少有分析工具能确切检测到安全侵害即将在何时发生，但确实有一些系统事件非常重

要，值得进行单独查阅。这种事件的例子有，删除一个关键 TSF 安全数据文件（如：口令文件）或远程用户试图获得管理员级特权的行为。这些事件都称作特征事件，如果它们的出现独立于系统的其他活动就预示着入侵活动。事件的序列是可预示入侵活动的特征事件有序集合。

给定工具的复杂程度将在很大程度上依赖于 PP/ST 作者在确定特征事件基本集和事件序列时所定义的赋值。

为执行分析，PP/ST 作者必须逐一列举出哪些事件应该由 TSF 所监测。PP/ST 作者应识别那些与事件有关的必要信息，以确定该事件是否映射为特征事件。

应提供管理性通告，以便授权用户能够理解事件的意义以及如何做出适当的响应。

为了避免把审计数据作为监测系统活动唯一的输入，在这些功能要求的详细说明中要求利用以前开发的入侵检测工具，而该工具不只使用审计数据进行系统活动分析（其他的输入数据包括如网络数据报、资源/计账数据或者各类系统数据的组合等），因此需要 PP/ST 作者详细说明用于监测系统活动的输入数据的类型。

FAU_SAA.4“复杂攻击探测”的元素不要求实现复杂攻击探测的 TSF 与其活动受监测的 TSF 为同一个。因此，可以开发一个入侵检测组件，其运行能够独立于那些系统活动正在被分析的系统。

C.4.5.2 操作

C.4.5.2.1 赋值

在 FAU_SAA.4.1 中，PP/ST 作者应确定系统事件序列列表的一个基本集，其出现表示已经有入侵的情况发生。这些事件序列表示已知的入侵情形，序列中所描绘的每一个事件应映射到一个受监测的系统事件，从而使得随着这些系统事件被执行，它们就映射到已知的入侵事件序列。

在 FAU_SAA.4.1 中，PP/ST 作者应确定系统事件的一个基本子集，其出现独立于所有其他系统活动，可预示着一个对 SFR 的执行的侵害。这包括那些本身就清晰地指明对 SFR 侵害的事件，或其出现对证明活动正常十分重要的那些事件。

在 FAU_SAA.4.2 中，PP/ST 作者应详细说明用于确定系统活动的信息。该信息是分析工具所使用的输入数据，用来确定发生在 TOE 上的系统活动。这些数据可包括审计数据、审计数据与其他系统数据的组合、或者也可由其他非审计数据组成。PP/ST 的作者应准确定义在所输入的数据中哪些系统事件及其属性正在被监测。

C.5 安全审计查阅（FAU_SAR）

C.5.1 用户注释

安全审计查阅族定义了与审计信息查阅有关的一些要求。

这些功能应该允许对存储前或存储后的审计数据进行选择性查阅，如下列几个方面内容：

- 一个或者多个用户的动作（如识别、鉴别、TOE 登录以及访问控制活动）；
- 对某个特定客体或 TOE 资源采取的动作；
- 规定的审计例外情况集的全部内容；
- 与某个特定的 SFR 属性有关的动作。

以下几种审计查阅之间的区别在于功能性。“审计查阅”只包含查阅审计数据的能力。而“可选审计查阅”更加复杂，要求能够基于某个标准或带逻辑关系（即“与”/“或”）的多个标准选择审计数据的子集，并能够在查阅审计数据之前对它们进行排序。

C.5.2 FAU_SAR.1 审计查阅

C.5.2.1 用户应用注释

本组件用于规定用户或授权用户能够读取审计记录。审计记录将以适合于用户的方式加以提供，因为不同类型的用户(人员用户、机器用户)可能有不同的需求。

可以规定能被查阅的审计记录内容。

C.5.2.2 操作

C.5.2.2.1 赋值

在 FAU_SAR.1.1 中，PP/ST 作者应详细说明能够使用这种能力的授权用户。PP/ST 作者也可以适当地指定一些安全角色(参见 FMT_SMR.1 安全角色)。

在 FAU_SAR.1.1 中，PP/ST 作者应详细说明准许指定的用户从审计记录中获得信息的类型，如可以是“全部”、“主体身份”或“涉及该用户的所有审计记录信息”。当使用 SFR 时，FAU_SAR.1 不必重复，详细的审计信息列表首先在 FAU_GEN.1 中规定。使用像“所有”或者“所有审计信息”之类的术语有助于消除歧义并且进一步需要比较分析两个安全要求。

C.5.3 FAU_SAR.2 限制审计查阅

C.5.3.1 用户应用注释

本组件规定，未在 FAU_SAR.1“审计查阅”中标识的用户不能读取审计记录。

C.5.4 FAU_SAR.3 可选审计查阅

C.5.4.1 用户应用注释

本组件详细说明应能对要查阅的审计数据进行选择。如果基于多个标准，这些标准之间必须具有某种逻辑关系(即“与”/“或”)，审计工具也应该提供处理审计数据的能力(如分类、筛选等)。

C.5.4.2 操作

C.5.4.2.1 赋值

在 FAU_SAR.3.1 中，PP/ST 作者应详细说明选择和/或排序审计数据的能力是否在 TSF 中要求。

在 FAU_SAR.3.1 中，PP/ST 作者应指定用于选择需要查阅的审计数据的标准(可能连同逻辑关系一起)。逻辑关系预期用于详细说明是否对单个属性或还是对属性的集合进行操作。这种赋值可能形如“应用、用户账号或位置”。在这种情况下，操作可用应用、用户账号和位置这三种属性的任意组合来规定。

C.6 安全审计事件选择(FAU_SEL)

C.6.1 用户注释

安全审计事件选择族提供一些关于识别能力方面的要求，这种能力指从可能发生的可审计事件中识别出哪些需要被审计。FAU_GEN“安全审计数据产生”族中定义了可审计事件，但这些事件在本组件中应定义为是可选的事件。

本族通过定义所选择安全审计事件的适当粒度，确保所保留的审计迹不至过于庞大而无法使用。

C.6.2 FAU_SEL.1 选择性审计

C.6.2.1 用户应用注释

本组件定义了用于根据用户属性、主体属性、客体属性或事件类型从所有可审计事件集中选择作为结果被审计的子集的标准。

本组件假设不存在单个用户身份，如路由器等设备就是不支持用户概念的 TOE。

对于分布式环境，主机身份可以用作被审计事件的选择条件。

管理功能 FMT_MTD.1“TSF 数据的管理”将处理授权用户对选择进行查询或修改的权限。

C.6.2.2 操作

C.6.2.2.1 选择

在 FAU_SEL.1.1 中，PP/ST 作者应该选择审计选择性所依据的安全属性是否与客体身份、用户身份、主体身份、主机身份或事件类型相关。

C.6.2.2.2 赋值

在 FAU_SEL.1.1 中，PP/ST 作者应详细说明审计选择性所依据的所有附加属性。如果没有附加规则供审计选择性依据，则赋值为“无”。

C.7 安全审计事件存储(FAU_STG)

C.7.1 用户注释

安全审计事件存储族描述了存储审计数据以备今后使用的要求，包括对由于 TOE 失效、发生攻击或存储空间满等原因所引起审计数据丢失进行控制的要求。

C.7.2 FAU_STG.1 受保护的审计迹存储

C.7.2.1 用户应用注释

在分布式环境中，由于审计迹位于 TSF 中，不一定要与生成审计数据的功能模块在一起，PP/ST 作者可能要求对审计记录的原发者进行鉴别，或在将此记录存入审计迹之前要求记录的源不可否认。

TSF 将保护在审计迹中存储的审计记录免遭未授权地删除或修改。值得注意的是，在某些 TOE 中审计员(角色)可能不具备删除特定时间段内审计记录的授权。

C.7.2.2 操作

C.7.2.2.1 选择

在 FAU_STG.1.2 中，PP/ST 作者应该详细说明 TSF 是应防止，还是只能检测对在审计迹中存储的审计记录的修改。这二者中只能选择一个。

C.7.3 FAU_STG.2 审计数据可用性保证

C.7.3.1 用户应用注释

本组件允许 PP/ST 作者详细说明审计迹应该符合某个度量标准。

在分布式环境中，由于审计迹位于 TSF 中，不一定要与生成审计数据的功能模块在一起，PP/ST 作者可能请求对审计记录的原发者进行鉴别，或在将此记录存入审迹之前要求记录的源不可否认。

C.7.3.2 操作

C.7.3.2.1 选择

在 FAU_STG.2.2 中，PP/ST 作者应该详细说明 TSF 是应防止，还是只能检测对在审计迹中存储的审计记录的修改。这二者中只能选择一个。

C.7.3.2.2 赋值

在 FAU_STG.2.3 中，PP/ST 作者应对于存储的审计记录详细说明 TSF 必须确保的度量。该度量通过列举必须保持的记录数或保证记录维护的时间来限制数据的丢失。例如，度量值“100000”就意味着能够存储 100000 条审计记录。

C.7.3.2.3 选择

在 FAU_STG.2.3 中，PP/ST 作者应该详细说明 TSF 仍能维护确定数量的审计数据的条件。这些条件可能是：审计存储耗尽、失效和受攻击。

C.7.4 FAU_STG.3 审计数据可能丢失时的动作

C.7.4.1 用户应用注释

本组件要求当审计迹超过预先定义限度时应采取相应的动作。

C.7.4.2 操作

C.7.4.2.1 赋值

在 FAU_STG.3.1 中，PP/ST 作者应指明预定的限度。如果管理功能指出这个数值可被授权用户改变，该值便为默认值。PP/ST 作者可选择让授权用户来定义该值，在这种情况下，该赋值可以是“授权用户设定的限度”。

在 FAU_STG.3.1 中，PP/ST 作者应详细说明即将发生由超过临界值所指示的审计存储失效时所应采取的动作。这些动作可包括通知授权用户。

C.7.5 FAU_STG.4 防止审计数据丢失

C.7.5.1 用户应用注释

本组件规定了审计迹已满时 TOE 的行为：或者忽略审计记录，或者冻结 TOE 使得任何被审计的事件都不能发生。本要求还规定无论怎样规定这类要求，对此具有特殊权限的授权用户总可以继续产生被审计的事件(采取动作)，这是因为要不这样，授权用户甚至将无法重启 TOE。因此，一旦审计存储空间满，应考虑选择 TSF 要采取的动作，如忽略事件，这样能提供更好的 TOE 可用性，也将准许不带记录且不追查用户责任地执行动作。

C.7.5.2 操作

C.7.5.2.1 选择

在 FAU_STG.4.1 中，PP/ST 作者应选定 TSF 是否忽略被审计的动作，或者是否应该防止被审计

动作的发生，或当 TSF 不能再存储审计记录时将最早的审计记录覆盖。只选择其中一项。

C.7.5.2.2 赋值

在 FAU_STG.4.1 中，PP/ST 作者应详细说明一旦发生审计存储失效，所应采取的其他动作，如通知授权用户。如审计存储失效时不需采取任何其他动作，则赋值为“无”。

附 录 D
（规范性附录）
FCO 类：通信

本类所描述的要求对用于传送信息的 TOE 有特殊意义。本类中各族都涉及抗抵赖。

本类中使用了“信息”这一概念。在这里信息应该解释为进行通信的客体，可能包括电子邮件消息、文件或一组预定义属性的类型。

在文献资料中，术语“接收证明”和“原发证明”是常用的术语。然而，通常认为术语“证明”应该以一种合法的方式进行解释，以蕴含某种形式的数学原理。本类中的组件解释了术语“证明”在谈及“证据”时的实际用途，这些证据用于 TSF 证实各种信息传输的不可否认性。

本类的组件构成分解如图 D.1 所示。

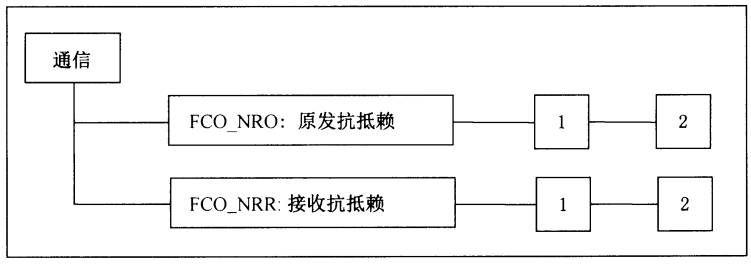

图 D.1 FCO 通信类分解

D.1 原发抗抵赖（FCO_NRO）

D.1.1 用户注释

原发抗抵赖定义了向用户/主体提供信息原发者身份证据的要求。由于原发证据（如数字签名）在原发者和所发送的信息之间提供了绑定的证据，原发者不能成功地否认已发送该信息，接收者或第三方可验证原发证据。原发证据应是不可伪造的。

如果以任何方式改变了信息或相关属性，对原发证据的验证就可能失败。因此，PP/ST 作者应考虑在 PP/ST 中加入完整性方面要求，如 FDT_UIT.1“数据交换完整性”。

抗抵赖涉及几个不同的角色，每个角色都可能结合一个或多个主体。第一个角色是请求原发证据的主体（仅在 FCO_NRO.1“选择性原发证明”中）；第二个角色是接收者或将证据提供给的其他主体（如公证人）；第三个角色是请求验证原发证据的主体，如接收者或像仲裁者这样的第三方。

PP/ST 作者必须详细说明为了能验证证据的有效性而必须满足的条件。例如，可能规定的一个条件是对证据的验证必须在 24 h 内进行。因此，这些条件允许按法律要求对抗抵赖进行裁剪，例如能够提供几年内的证据。

在多数情况下，接收者的身份是接收传送数据的用户。在一些情况下，PP/ST 作者不希望用户身份被输出，此时 PP/ST 作者应该考虑包括此类是否合适，或者是否应使用传送服务提供者的身份或主机的身份。

除了（或代替）用户身份，PP/ST 作者可能更关注信息发送的时间。例如，请求建议必须在某个确定日期之前发送才能被接纳，在这种情形下，这些要求应能被定制以提供时间戳作为标记（原发时间）。

D.1.2 FCO_NRO.1 选择性原发证明

D.1.2.1 操作

D.1.2.1.1 赋值

在 FCO_NRO.1.1 中，PP/ST 作者应将信息主体的类型填充到原发功能的证据中，如电子邮件消息。

D.1.2.1.2 选择

在 FCO_NRO.1.1 中，PP/ST 作者应详细说明可以请求原发证据的用户/主体。

D.1.2.1.3 赋值

在 FCO_NRO.1.1 中，PP/ST 作者应根据选择结果详细说明能请求原发证据的第三方。第三方可以是仲裁者、法官和法定机构。

在 FCO_NRO.1.2 中，PP/ST 作者应填写可关联到信息的属性列表，如原发者身份、发送时间和发送位置。

在 FCO_NRO.1.2 中，PP/ST 作者应在信息域列表中填写能够提供原发证据属性的信息，如消息体。

D.1.2.1.4 选择

在 FCO_NRO.1.3 中，PP/ST 作者应详细说明能验证原发证据的用户/主体。

D.1.2.1.5 赋值

在 FCO_NRO.1.3 中，PP/ST 作者应填充可验证证据的限制条件列表。例如，证据只能在 24 h 之内被验证。赋值为“立即的”或“不确定的”也是可接受的。

在 FCO_NRO.1.3 中，PP/ST 作者应根据选择结果详细说明能验证原发证据的第三方。

D.1.3 FCO_NRO.2 强制性原发证明

D.1.3.1 操作

D.1.3.1.1 赋值

在 FCO_NRO.2.1 中，PP/ST 作者应将信息主体的类型填充到原发功能的证据中，如电子邮件消息。

在 FCO_NRO.2.2 中，PP/ST 作者应填写可关联到信息的属性列表，如原发者身份、发送时间和发送位置。

在 FCO_NRO.2.2 中，PP/ST 作者应在信息域列表中填写能够提供原发证据属性的信息，如消息体。

D.1.3.1.2 选择

在 FCO_NRO.2.3 中，PP/ST 作者应详细说明能验证原发证据的用户/主体。

D.1.3.1.3 赋值

在 FCO_NRO.2.3 中，PP/ST 作者应填写可验证证据的限制条件列表。例如，证据只能在 24 h 之

内被验证。赋值为“立即的”或“无期限的”也是可接受的。

在 FCO_NRO.2.3 中，PP/ST 作者应根据选择结果详细说明能验证原发证据的第三方。第三方可以是仲裁者、法官或法律机构。

D.2 接收抗抵赖(FCO_NRR)

D.2.1 用户注释

接收抗抵赖定义了向其他用户/主体提供信息已被接收者接收到的证据的要求。由于接收证据(例如数字签名)在接收者和所接收信息之间提供了证据绑定，接收者必须承认已接收该信息，原发者或第三方可验证接收证据。此证据应是不可伪造的。

应该注意的是，提供收到信息的证据不一定意味着信息主体被读取或被理解，而只是已传递了信息。

如果以任何方式改变了信息或相关属性，验证与原始信息相关的接收证据就可能失败。因此，PP/ST 作者应考虑在 PP/ST 中加入完整性方面要求，如 FDT_UIT.1“数据交换完整性”。

抗抵赖涉及几个不同的角色，每个角色都可能结合在一个或多个主体。第一个角色是请求接收证据的主体(仅在 FCO_NRO.1“选择性接收证明”中)；第二个角色是接收者或其他向其提供证据的主体(如公证人)；第三个角色是请求验证接收证据的主体，如接收者或像仲裁者这样的第三方。

PP/ST 作者必须详细说明为了能验证证据的有效性而必须满足的条件。例如，可能规定的一个条件是对证据的验证必须在 24 h 内进行。因此，这些条件允许按法律要求对抗抵赖进行裁剪，例如能够提供在几年内的证据。

在多数情况下，接收者的身份是接收传送数据的用户。在一些情况下，PP/ST 作者不希望用户身份被输出。此时 PP/ST 作者必须考虑包括此类是否合适，或者是否应使用传送服务提供者的身份或主机的身份。

除了(或代替)用户身份，一个 PP/ST 作者可能更关注接收信息的时间。例如，报价将在某个日期终止，定单必须在某个确定日期前接收到才能被接纳，在这些情况下，这些要求应能被定制以提供时间戳指示(接收时间)。

D.2.2 FCO_NRR.1 选择性接收证明

D.2.2.1 操作

D.2.2.1.1 赋值

在 FCO_NRR.1.1 中，PP/ST 作者应将信息主体的类型填充到接收功能的证据中，如电子邮件消息。

D.2.2.1.2 选择

在 FCO_NRR.1.1 中，PP/ST 作者应详细说明可以请求接收证据的用户/主体。

D.2.2.1.3 赋值

在 FCO_NRR.1.1 中，PP/ST 作者应根据选择结果详细说明能请求接收证据的第三方。第三方可以是仲裁者、法官和法律机构。

在 FCO_NRR.1.2 中，PP/ST 作者应填写可关联到信息的属性列表，如接收者身份、接收时间和接收位置。

在 FCO_NRR.1.2 中，PP/ST 作者应在信息域列表中填写能够提供接收证据属性的信息，如消

息体。

D.2.2.1.4 选择

在 FCO_NRR.1.3 中，PP/ST 作者应指定能验证接收证据的用户/主体。

D.2.2.1.5 赋值

在 FCO_NRR.1.3 中，PP/ST 作者应填写可验证证据的限制条件列表。例如，证据只能在 24 h 之内被验证。赋值为“立即的”或“无限期的”也是可接受的。

在 FCO_NRR.1.3 中，PP/ST 作者应根据选择结果指定能验证接收证据的第三方。

D.2.3 FCO_NRR.2 强制接收证明

D.2.3.1 操作

D.2.3.1.1 赋值

在 FCO_NRR.2.1 中，PP/ST 作者应将信息主体的类型填写到接收功能的证据中，如电子邮件消息。

在 FCO_NRR.2.2 中，PP/ST 作者应填写可关联到信息的属性列表，如接收者身份、接收时间和接收位置。

在 FCO_NRR.2.2 中，PP/ST 作者应在信息域列表中填写能够提供接收证据属性的信息，如消息体。

D.2.3.1.2 选择

在 FCO_NRR.2.3 中，PP/ST 作者应详细说明能验证接收证据的用户/主体。

D.2.3.1.3 赋值

在 FCO_NRR.2.3 中，PP/ST 作者应填写可验证证据的限制条件列表。例如，证据只能在 24 h 之内被验证。赋值为“立即的”或“无期限的”也是可接受的。

在 FCO_NRR.2.3 中，PP/ST 作者应根据选择结果指定能验证接收证据的第三方。第三方可以是仲裁者、法官和法律机构。

附 录 E
（规范性附录）
FCS 类：密码支持

TSF 可以利用密码功能来帮助满足几种高级安全目的。这些安全目的包括（但不限于）：标识和鉴别、抗抵赖、可信路经、可信信道和数据分离。在 TOE 实现密码功能时使用本类，其实现形式可为硬件、固件或软件。

FCS“密码支持”类是由两个族构成：FCS_CKM“密钥管理”和 FCS_COP“密码运算”。FCS_CKM 族解决密钥管理方面的问题，而 FCS_COP 族则关注这些密钥的运算使用情况。

若由 TOE 实现每个密钥的生成方法，PP/ST 作者应选择 FCS_CKM.1“密钥生成”组件。

若由 TOE 实现每个密钥的分发方法，PP/ST 作者应选择 FCS_CKM.2“密钥分发”组件。

若由 TOE 实现每个密钥的存取方法，PP/ST 作者应选择 FCS_CKM.3“密钥存取”组件。

若由 TOE 实现每个密钥的销毁方法，PP/ST 作者应选择 FCS_CKM.4“密钥销毁”组件。

若由 TOE 执行每个密钥的运算（如数字签名、数据加密、密钥协商、安全散列等），PP/ST 作者应该选择 FCS_COP.1“密码运算”组件。

密码功能可以用来满足 FCO“通信”类中规定的安全目的，还可以满足 FDP_DAU“数据鉴别”、FDP_SDI“存储数据的完整性”、FDP_UCT“TSF 间用户数据机密性传送保护”、FDP_UIT“TSF 间用户数据完整性传送保护”、FIA_SOS“秘密的规范”、FIA_UAU“用户鉴别”族中规定的各种目的。当密码功能用于满足其他功能类的目的时，应有单独的功能组件详细说明密码功能必须满足的目的。当消费者特地需要 TOE 的密码功能时，应使用 FCS“密码支持”类中的目的。

本类的组件构成分解如图 E.1 所示。

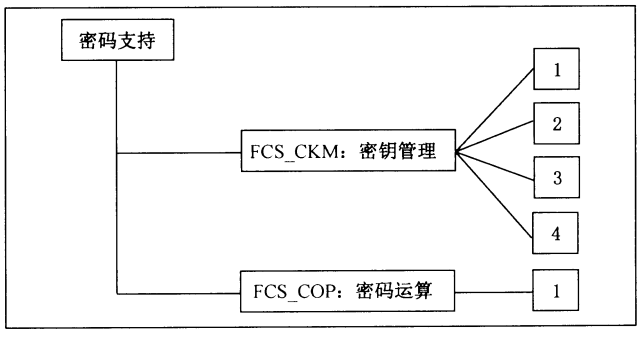

图 E.1 FCS 密码支持类分解

E.1 密钥管理（FCS_CKM）

E.1.1 用户注释

密钥的管理必须在其整个生命期内进行，密钥生命期中的典型事件包括（但不限于）：生成、分发、导入、存储、存取（如备份、托管、归档、恢复）和销毁。

密钥至少要经历以下阶段：生成、存储和销毁，是否包括其他阶段取决于所实施的密钥管理策略，因为 TOE 不一定涉及整个密钥生命期（例如 TOE 可以只生成并分发密钥）。

本族预期要支持密钥生命期，因此定义了对以下活动的要求：密钥生成、密钥分发、密钥存取和密钥销毁。只要存在密钥管理方面的功能要求，就应选择本族。

如果 PP/ST 中包含 FAU_GEN“安全审计数据产生”，下列行为应是可审计的：

a) 客体属性可包括密钥的指定用户、用户角色、将使用该密钥的密码运算、密钥标识和密钥有效期。

b) 客体值可包括密钥值和任何敏感信息外的参数(例如密钥或私钥)。

一般来讲，随机数用于生成密钥，在这种情况下，应使用 FCS_CKM.1“密钥生成”代替 FIA_SOS.2“TSF 生成秘密”。当不是为生成密钥而要求生成随机数时，应使用组件 FIA_SOS.2“TSF 生成秘密”。

E.1.2 FCS_CKM.1 密钥生成

E.1.2.1 用户应用注释

本组件要求规定密钥的长度和用于生成密钥的方法，密钥长度和生成方法要符合一个指定标准。该标准能被用于详细说明密钥的长度和规定用于生成密钥的方法(例如算法)。对于同一种方法和多种密钥长度的情况，本组件只需使用一次。密钥长度对于不同的实体可能是相同的或不同的，可以作为方法的输入，也可作为方法的输出。

E.1.2.2 操作

E.1.2.2.1 赋值

在 FCS_CKM.1.1 中，PP/ST 作者应详细说明所使用的密钥生成算法。

在 FCS_CKM.1.1 中，PP/ST 作者应详细说明所使用的密钥长度。所规定的密钥长度应适合于算法及其预期使用。

在 FCS_CKM.1.1 中，PP/ST 作者应详细说明指定的标准，该标准描述生成密钥所使用的方法。指定的标准可不包含任何现行公开标准，也可包含一个或多个现行标准，如国际、国家、行业或组织标准。

E.1.3 密钥分发

E.1.3.1 用户应用注释

本组件要求规定用于分发密钥的方法，该方法应符合赋值的标准。

E.1.3.2 操作

E.1.3.2.1 赋值

在 FCS_CKM.2.1 中，PP/ST 作者应详细说明所使用的密钥分发方法。

在 FCS_CKM.2.1 中，PP/ST 作者应详细说明赋值的标准，该标准描述分发密钥的方法。赋值的标准可不包含任何现行公开标准，也可包含一个或多个现行标准，如国际、国家、行业或组织标准。

E.1.4 FCS_CKM.3 密钥存取

E.1.4.1 用户应用注释

本组件要求规定用于密钥存取的方法，该方法应符合赋值的标准。

E.1.4.2 操作

E.1.4.2.1 赋值

在 FCS_CKM.3.1 中，PP/ST 作者应详细说明所使用的密钥存取类型，密钥存取的类型包括(但不限于)：密钥备份、密钥归档、密钥托管和密钥恢复。

在 FCS_CKM.3.1 中，PP/ST 作者应详细说明所使用的密钥存取方法。

在 FCS_CKM.3.1 中，PP/ST 作者应详细说明赋值的标准，该标准描述存取密钥的方法。赋值的标准可不包含任何现行公开标准，也可包含一个或多个现行标准，如国际、国家、行业或组织标准。

E.1.5 FCS_CKM.4 密钥销毁

E.1.5.1 用户应用注释

本组件要求规定用于密钥销毁的方法，该方法应符合赋值的标准。

E.1.5.2 操作

E.1.5.2.1 赋值

在 FCS_CKM.4.1 中，PP/ST 作者应指定用来销毁密钥的方法。

在 FCS_CKM.4.1 中，PP/ST 作者应规定指定的标准，该标准描述了密钥销毁的方法。指定的标准可不包含任何现行公开标准，也可包含一个或多个现行标准，如国际、国家、行业或组织标准。

E.2 密码运算(FCS_COP)

E.2.1 用户注释

密码运算可能具有与之相关联的密码模式，因此必须规定密码模式。常见的密码模式有密码块链接模式(CBC)、输出反馈模式(OFB)、电子密本模式(ECB)和密码反馈模式(CFB)等。

密码运算可用于支持一个或多个 TOE 安全服务。FCS_COP“密码运算”中的组件可以根据需要重复多次，这取决于：

a) 使用安全服务的用户应用；
b) 不同密码算法或密钥长度的使用；
c) 所运算数据的类型或敏感度。

如果 PP/ST 中包含 FAU_GEN “安全审计数据产生”，则以下密码运算事件应被审计：

a) 密码运算的类型可以包括数字签名的产生和/或验证、用于完整性和/或校验和验证的密码校验和的产生、安全散列(消息摘要)的计算、数据加密和/或解密、密钥加密和/或解密、密钥协商和随机数生成；
b) 主体属性可包括同主体有关的主体角色和用户；
c) 客体属性可包括密钥的指定用户、用户角色、使用密钥的密码运算、密钥标识和密钥有效期。

E.2.2 FCS_COP.1 密码运算

E.2.2.1 用户应用注释

本组件要求基于赋值的标准，明确用于执行指定密码操作的密码算法和密钥大小。

E.2.2.2 操作

E.2.2.2.1 赋值

在 FCS_COP.1.1 中，PP/ST 作者应规定所执行的密码运算。密码运算通常包括：数字签名的产生和/或验证、用于完整性和/或校验和验证的密码校验和的产生、安全散列(消息摘要)的计算、数据加密和/或解密、密钥加密和/或解密、密钥协商和随机数生成。密码运算可针对用户数据或 TSF 数据执行。

在 FCS_COP.1.1 中，PP/ST 作者应规定所使用的密码算法。通常的密码算法包括(但不限于)

DES、RSA 和 IDEA 等。

在 FCS_COP.1.1 中，PP/ST 作者应规定所使用的密钥长度。规定的密钥长度应适合于算法及其预期使用。

在 FCS_COP.1.1 中，PP/ST 作者应规定所赋值的标准，该标准文本应描述如何执行已确定的密码运算。赋值的标准可不包含任何现行公开标准，也可以包含一个或多个现行的公开标准，例如国际、国家、行业或组织标准。

附 录 F
（规范性附录）
FDP 类：用户数据保护

本类所包含的族详细说明了与用户数据保护相关的要求。本类中的组件不同于 FIA 和 FPT 中的组件：FDP 规定了一些保护用户数据的组件，FIA 规定了一些保护与用户相关属性的组件，FPT 规定了一些保护 TSF 信息的组件。

本类没有对常用的强制访问控制（MAC）和自主访问控制（DAC）做明确的要求，然而，这些要求可由本类中的一些组件构建。

FDP“用户数据保护”并不明确地处理机密性、完整性或可用性，因为上述三种属性经常与策略和机制紧密相关。但在 PP/ST 中，TOE 安全策略必须完全涵盖这三个方面。

本类的最后一个方面就是用术语“操作”来规定访问控制。操作就是对特定客体的一种特定类型访问。它依赖于 PP/ST 作者的抽象水平，是否将这些操作描述成“读”或“写”操作，还是更复杂的操作，比如“更新数据库”。

访问控制策略是控制对信息载体访问的策略。其属性代表该载体的属性。一旦信息在载体之外，访问者就可以自由地修改，包括将信息写入具有不同属性的载体中。相对应的，信息流策略控制对信息的访问，而与载体无关。信息的属性，可能与载体的属性相关（也可能无关，如多级数据库），将与信息一起移动。没有明确的授权，访问者无法改变信息的属性。

本类并不像人们想像的那样，是一个 IT 访问策略的完备分类。这里所包括的策略仅仅是当前实际系统中一些具有的经验，这些经验为规范要求提供了一个基础。也可能还存在其他形式的目的不被这里的定义所关注。

比如，你可以设想一个目的，由用户施行（和用户定义）对信息流的控制（例如，一个非外部自动告警工具），这种概念就可以通过细化或扩展 FDP“用户数据保护”的组件来处理。

最后要强调一点，在阅读 FDP“用户数据保护”中组件时要记住，这些组件都是关于某机制可实现功能方面的要求，同样也服务于或能够服务于另外的目的。比如，可以建立一种访问控制策略（FDP_ACC“访问控制策略”），此策略使用标签（FDP_IFF.1“简单安全属性”）作为访问控制机制的基础。

SFR 集可以包含多个安全功能策略（SFP），每一个 SFP 都可标识为 FDP_ACC“访问控制策略”和 FDP_IFC“信息流控制策略”中组件所确定的策略。这些策略主要考虑机密性、完整性和可用性三个方面以满足 TOE 要求。值得注意的是，要确保所有客体都至少被一个 SFP 涵盖，并且在实现多个 SFP 时不会出现冲突。

在编制 PP/ST 时，以下信息有助于查找和选择 FDP“用户数据保护”类中的组件。

FDP“用户数据保护”类中的要求都是针对将要执行一个 SFP 的 SFR 集而定义的。由于 TOE 可以同时执行多个 SFP，PP/ST 作者必须为每一个 SFP 命名，以便能在其他族中引用。这个名字将用在每一个所选组件，表明其用作该功能要求定义的部分。这便于作者指定操作的范围，如涵盖的客体、涵盖的操作和授权用户等。

组件的每一个实例化只能用于一个 SFP。因此，如果一个组件指定了某个 SFP，则该 SFP 将适用于此组件中的所有元素。在 PP/ST 中，可以对组件多次实例化，以说明预期的各种策略。

从本族中选取组件的关键，是有一个明确定义的 TOE 安全目的集，以便能够从两个策略族（FDP_ACC“访问控制策略”和 FDP_IFC“信息流控制策略”）中选择合适的组件。分别在 FDP_ACC 和 FDP_IFC 相关组件中，为所有的访问控制策略和信息流控制策略命名，而且这些组件在主体、客体和操作方

面的控制范围都被该安全功能涵盖。这些策略名将广泛用于其他要求对“访问控制 SFP”或“信息流控制 SFP”进行赋值或选择操作的功能组件中。定义所命名访问控制 SFP 和信息流控制 SFP 的功能性规则将分别在 FDP_ACF“访问控制功能”和 FDP_IFF“信息流控制功能”族中定义。

下列步骤将指导我们在编制 PP/ST 时如何使用本类：

a) 从 FDP_ACC“访问控制策路”和 FDP_IFC“信息流控制策略”族中识别出将要执行的策略。这两个族定义了策略的控制范围、控制粒度，并可以确定一些与策略相对应的规则。

b) 识别组件并执行策略组件中所有合适的操作。赋值操作可以一般性地执行（如表述为“所有文件”），也可以特定地执行（如指定文件“A”、“B”等），这取决于掌握的详细程度。

c) 从 FDP_ACF“访问控制功能”和 FDP_IFF“信息流控制功能”中识别出所有合适的功能组件，以处理 FDP_ACC 和 FDP_IFC 中所命名的策略。执行这个操作，使组件定义出已命名策略所执行的规则。应当使组件满足预期的或已建立的所选功能要求。

d) 识别该功能中谁有能力控制和改变安全属性，比如只有安全管理员、只有客体的所有者等。从 FMT 安全管理类中选择合适的组件并执行操作。这里可能需要细化操作，以确定某些缺少的特征，比如部分或所有的修改都必须通过可信路径来完成。

e) 对于新客体和主体的初始值，在 FMT“安全管理”类中识别所有合适的组件。

f) 在 FDP_ROL“回退”族中识别出所有适用的回退组件。

g) 在 FDP_RIP“残余信息保护”族中识别出所有适用的残余信息保护要求。

h) 在 FDP_ITC“从 TOE 之外输入”和 FDP_ETC“从 TOE 输出”族中，识别出所有适用的输入、输出组件，以及在输入、输出中应如何处理安全属性。

i) 在 FDP_ITT“TOE 内部传送”族中识别出所有适用的 TOE 内部通信组件。

j) 在 FDP_SDI“存储数据的完整性”中识别出所存储信息完整性保护的所有要求。

k) 在 FDP_UCT“TSF 间用户数据机密性传送保护”或 FDP_UIT“TSF 间用户数据完整性传送保护”族中识别出所有适用的 TSF 间通信组件。

本类的组件构成分解如图 F.1 所示。

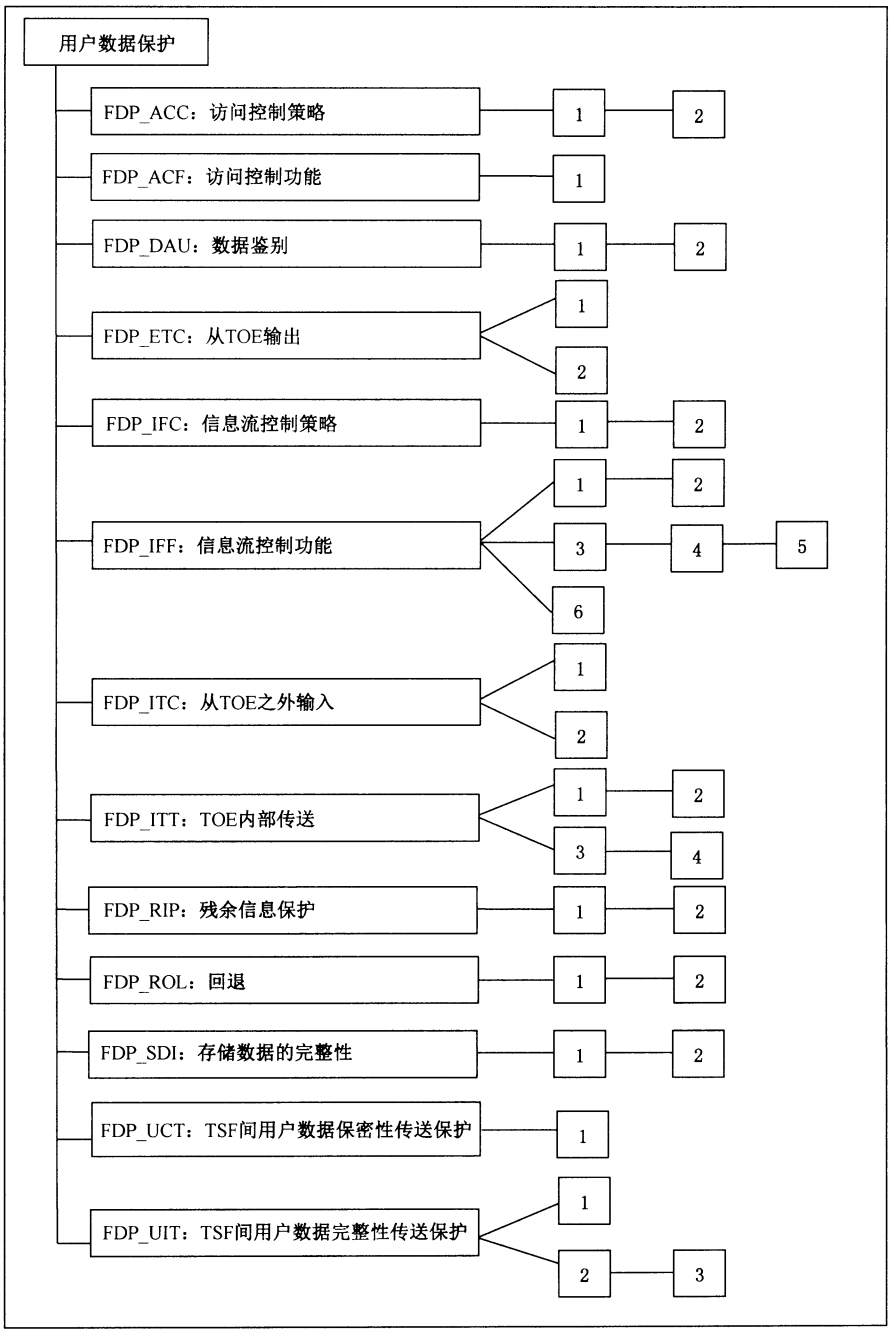

图 F.1 FDP 用户数据保护类分解

F.1 访问控制策略(FDP_ACC)

F.1.1 用户注释

本族是基于独立的概念，控制主体和客体间的相互作用。控制的范围和目的是基于访问者(主体)的属性、被访问载体(客体)的属性、行为(操作)和任何相关的访问控制规则。

本族中的组件能(通过命名)识别出由传统自主访问控制机制(DAC)执行的访问控制 SFP，进一步定义所识别访问控制 SFP 涵盖的主体、客体和操作。定义访问控制 SFP 功能性的规则将在其他族中定

义，如 FDP_ACF“访问控制功能”和 FDP_ETC“从 TOE 输出”。FDP_ACC“访问控制策略”中定义的访问控制 SFP 名将广泛用于其他要求对“访问控制 SFP”进行赋值或选择操作的功能组件中。

访问控制 SFP 涵盖一个三元组：主体、客体和操作。因此一个主体可由多个访问控制 SFP 所涵盖，但只涉及单个操作或单个客体。对于多个客体和多个操作也同样如此。

实施访问控制 SFP 的访问控制功能的关键点是用户能够修改访问控制决定中涉及的属性，而 FDP_ACC“访问控制策略”族没有涉及这些方面。有些要求没有定义，但可以在细化操作中增加，而余下的要求可包含在其他族和类中，比如 FMT“安全管理”类。

FDP_ACC“访问控制策略”中没有审计要求，因为本族只规定访问控制 SFP 要求。审计要求将在规定功能以满足本族中确定的访问控制 SFP 的相关族中出现。

本族为 PP/ST 作者提供了规定多种策略的能力，比如，在一个控制范围内实施固定的访问控制 SFP，在另外的控制范围中实施灵活的访问控制 SFP。为规定多个访问控制策略，本族中的组件可以在 PP/ST 中针对不同的操作和客体子集多次反复，这将适应于具有多重策略的 TOE，每一个策略处理一组特定的操作和客体。也就是说，PP/ST 作者应对 TSF 执行的每一个访问控制 SFP 指定 ACC 组件中所要求的信息。比如，一个 TOE 实施了三个访问控制 SFP，每个 SFP 只涵盖 TOE 中客体、主体和操作的一个子集，对于各个访问控制 SFP，都将包含一个 FDP_ACC.1“子集访问控制”组件，从而总共需要三个 FDP_ACC.1 组件。

F.1.2 FDP_ACC.1 子集访问控制

F.1.2.1 用户应用注释

术语客体和主体都是指 TOE 中的一般元素。对于一个可执行的策略，必须清晰地定义相关的实体。对于一个 PP，客体和操作可以表示为命名的客体、数据仓库、观察访问等类型。对于一个特定的 TOE，这些一般的术语（主体、客体）必须细化，比如：文件、寄存器、端口、守护进程、开放调用接口等。

本组件规定策略应涵盖定义好的对某个客体子集的操作集合，而不对集合外的任何操作做任何限制，包括对其他操作受控的客体进行的操作。

F.1.2.2 操作

F.1.2.2.1 赋值

在 FDP_ACC.1.1 中，PP/ST 作者应规定一个唯一命名的访问控制 SFP 以执行 TSF。

在 FDP_ACC.1.1 中，PP/ST 作者应规定一个主体、客体以及主体和客体间操作列表。

F.1.3 FDP_ACC.2 完全访问控制

F.1.3.1 用户应用注释

本组件要求所有对客体的可能操作，都包含在访问控制 SFP 中，都被一个访问控制 SFP 涵盖。

PP/ST 的作者必须证实每一组客体和主体都被一个访问控制 SFP 涵盖。

F.1.3.2 操作

F.1.3.2.1 赋值

在 FDP_ACC.2.1 中，PP/ST 作者应规定唯一命名的访问控制 SFP 以执行 TSF。

在 FDP_ACC.2.1 中，PP/ST 作者应规定 SFP 所涵盖的主体和客体列表。所有这些主体和客体间操作都将被 SFP 涵盖。

F.2 访问控制功能(FDP_ACF)

F.2.1 用户注释

本族描述了关于能实现 FDP_ACC 中所命名访问控制策略的特定功能的一些规则,并规定策略控制的范围。

本族为 PP/ST 作者提供了描述访问控制规则的能力。这导致 TOE 中对客体的访问不会发生改变。作为这种客体的一个例子就是,"今日消息",它可以被所有人阅读,但只能被授权管理员修改。本族也为 PP/ST 作者提供了描述普通访问控制规则之外的规则。这些例外规则可以明确允许或者拒绝授权对一个客体的访问。

没有明确的组件规定其他可能的功能,比如双人控制、操作顺序规则或互斥控制。然而,这些机制同传统 DAC 机制一样,能够通过仔细制定访问控制规则,用现有的组件来表示。

在本族中可描述各种可接受的访问控制功能性,如:

——访问控制表(ACL);

——基于时间的访问控制规范;

——基于原发端的访问控制规范;

——属主控制的访问控制属性。

F.2.2 FDP_ACF.1 基于安全属性的访问控制

F.2.2.1 用户应用注释

本组件对基于与主体和客体有关的安全属性仲裁访问控制的机制提出要求。每一个客体和主体都有一组相关的属性,比如位置、创建时间、访问权限[如访问控制表(ACL)]。本组件允许 PP/ST 作者指定用于访问控制仲裁的属性,并允许使用这些属性来指定访问控制规则。

下面的段落中给出 PP/ST 作者对属性进行赋值的例子。

身份属性可与用于仲裁的用户、主体或客体有关。这种属性的例子可能是用于创建主体的程序镜象名,或者是授予程序镜象的一个安全属性。

时间属性能用来指定在一天中的哪些时间,或者在一星期中的哪几天,或在哪一年授予访问权限。

位置属性能规定该地址是不是操作请求的地址,或是不是操作执行的地址,或两者都是。它能基于内部表格,将 TSF 逻辑接口转换成位置,比如通过终端位置、CPU 位置等。

为了达到访问控制的目的,组属性允许将单个用户组与某个操作相关联。如果需要,应使用细化操作来指定可定义的最大组数、一个组的最大成员数以及用户可以同时关联的最大组数。

本组件也要求访问控制安全功能能基于安全属性,明确授权或拒绝对一个客体的访问,可用来在 TOE 中设置特权、访问权限或访问授权。这些特权、权限或授权可适用于用户、主体(代表用户或应用)和客体。

F.2.2.2 操作

F.2.2.2.1 赋值

在 FDP_ACF.1.1 中,PP/ST 作者应指定 TSF 要执行的访问控制 SFP 名称。访问控制 SFP 名称和该策略的控制范围在 FDP_ACC 的组件中定义。

在 FDP_ACF.1.1 中,PP/ST 作者应针对每一个受控主体和客体,指定安全属性或命名安全属性组,其功能将用于规则的规范。例如,这些属性可以是用户身份、主体身份、角色、时间、位置、ACL 或者 PP/ST 作者指定的其他属性。可规定已命名的安全属性组以提供一种便捷的方式引用多个安全属性。

命名组能提供一种有效的方法，将 FMT_SMR“安全管理角色”中定义的角色和所有相关角色与主体相关联。换句话说，每个角色都能与一个命名属性组相关联。

在 FDP_ACF.1.2 中，PP/ST 作者应规定在受控主体和受控客体间，通过对受控客体执行受控操作来管理访问的 SFP 规则。这些规则规定何时访问被允许或被拒绝。可以指定普通访问控制功能（如典型的许可位）或粒状访问控制功能（如 ACL）。

在 FDP_ACF.1.3 中，PP/ST 作者应基于安全属性规定主体对客体的明确授权访问规则，用于明确授权访问。这些规则是 FDP_ACF.1.1 中规定规则的补充，之所以被包含在 FDP_ACF.1.3 中，是因为含有FDP_ACF.1.1中规定规则的例外情况。明确授权访问规则的例子有，基于一个与主体相关的特权向量，总是准许访问已指定访问控制 SFP 所涵盖的客体。如果不需要这种能力，PP/ST 作者应给定赋值为“无”。

在 FDP_ACF.1.4 中，PP/ST 作者应基于安全属性规定主体对客体的明确拒绝访问规则。这些规则是对 FDP_ACF.1.1 中规定规则的补充，之所以被包含在 FDP_ACF.1.4 中，是因为含有FDP_ACF.1.1中规定规则的例外情况。明确拒绝访问规则的例子有，基于一个与主体相关的特权向量，总是拒绝访问已指定访问控制 SFP 所涵盖的对象。如果不需要这种能力，PP/ST 作者应给定赋值为“无”。

F.3 数据鉴别（FDP_DAU）

F.3.1 用户注释

本族描述能用于鉴别“静态”数据的特定功能。

当需要“静态”数据鉴别时，即数据被标记但不传送时，使用本族中的组件。（注意，FCO_NRO“原发抗抵赖”族规定了数据交换时所接收信息的源的不可否认要求）。

F.3.2 FDP_DAU.1 基本数据鉴别

F.3.2.1 用户应用注释

本组件可由单向散列函数（密码校验和、指纹、信息摘要）来满足，可通过对一个确定的文档产生散列值验证文档信息内容的有效性或真实性。

F.3.2.2 操作

F.3.2.2.1 赋值

在 FDP_DAU.1.1 中，PP/ST 作者应指定客体或信息类型列表，对此 TSF 应能够生成数据鉴别证据。

在 FDP_DAU.1.2 中，PP/ST 作者应指定一个主体列表，这些主体能验证在先前的元素中所确定客体的数据鉴别证据。如果主体已知，或者能更一般化并归诸于一“类”主体，比如某确定的角色，主体列表就可以非常具体。

F.3.3 FDP_DAU.2 带担保者身份的数据鉴别

F.3.3.1 用户应用注释

本组件还额外要求能够验证提供鉴别保证的用户（如可信第三方）的身份。

F.3.3.2 操作

F.3.3.2.1 赋值

在 FDP_DAU.2.1 中，PP/ST 作者应指定客体或信息类型列表，对此 TSF 应能够生成数据鉴别证据。

在 FDP_DAU.2.2 中，PP/ST 作者应指定一个主体列表，这些主体应能验证在先前的元素中所确定客体的数据鉴别证据和产生数据鉴别证据的用户身份。

F.4 从 TOE 输出(FDP_ETC)

F.4.1 用户注释

本族定义从 TOE 中用户数据的 TSF 促成输出功能，既可以在输出时明确保留安全属性，也可以不保留安全属性。这些安全属性的一致性将由 FPT_TDC“TSF 间 TSF 数据的一致性”负责处理。

FDP_ETC“从 TOE 输出”主要关注对数据输出的限制和所输出用户数据与安全属性的关联性。

本族以及相应的输入族 FDP_ITC“从 TOE 之外输入”，负责说明 TOE 如何将用户数据输入到其控制范围内和从其控制范围输出。原则上，本族只涉及用户数据及其相关安全属性的 TSF 促成输出。

这里可包含下列两种活动：

a) 不带任何安全属性的用户数据输出；

b) 带有安全属性的用户数据输出，这两者彼此相互关联，并且安全属性明确无误地表征了所输出的用户数据。

如果存在多个(访问控制或信息流控制)SFP，那么对每一个已命名的 SFP 就可以反复使用本族中的这些组件。

F.4.2 FDP_ETC.1 不带安全属性的用户数据输出

F.4.2.1 用户应用注释

本组件用来指定在用户数据的 TSF 促成输出时，并不输出其安全属性。

F.4.2.2 操作

F.4.2.2.1 赋值

在 FDP_ETC.1.1 中，PP/ST 作者应指定输出用户数据时将执行的访问控制 SFP 或信息流控制 SFP。这些 SFP 赋值限定了此功能所输出用户数据的范围。

F.4.3 FDP_ETC.2 带有安全属性的用户数据输出

F.4.3.1 用户应用注释

用户数据与它的安全属性一起被输出，安全属性明确地与用户数据相关联。有多种方法实现这种关联，一种方法是物理上将用户数据和安全属性结合在一起(如，同一张软盘)，或使用如安全签名的密码技术将属性和用户数据相关联。FTP_ITC“TSF 间可信信道”可以用来保证属性被另一个可信 IT 产品正确接收，同时，FPT_TDC“TSF 间 TSF 数据的一致性”可以用来保证那些属性得到正确的解释。此外，FTP_TRP“可信路径”可用来保证输出是由正确的用户发起的。

F.4.3.2 操作

F.4.3.2.1 赋值

在 FDP_ETC.2.1 中，PP/ST 作者应指定在输出用户数据时要执行的访问控制 SFP 或信息流控制 SFP。这些 SFP 赋值限定了此功能所输出用户数据的范围。

在 FDP_ETC.2.4 中，PP/ST 作者应指定所有附加的输出控制规则，如果没有额外的输出控制规则则赋值为“无”。除在 FDP_ETC.2.1 中选择的访问控制 SFP 或信息流控制 SFP 之外，TSF 还应执行这些规则。

F.5 信息流控制策略(FDP_IFC)

F.5.1 用户注释

本族包含信息流控制 SFP 的识别，以及针对每个 SFP，分别确定其控制范围。

本族中的组件能够识别 TOE 中传统的强制访问控制机制执行的信息流控制 SFP。虽然，它们已经超出了传统 MAC 机制，但可用来识别和描述无干扰策略和状态转变，并进一步为 TOE 中每个信息流控制 SFP 定义策略控制下的主体、策略控制下的信息以及引发受控信息流入、流出受控主体的操作。信息流控制 SFP 将由其他诸如 FDP_IFF“信息流控制功能”和 FDP_ETC“从 TOE 输出”等族定义。在 FDP_IFC“信息流控制策略”中命名的访问控制 SFP，应在其他所有选择“信息流控制 SFP”的功能组件或为其进行赋值操作的功能组件中使用。

这些组件非常灵活，它们允许指定信息流控制的域，而对基于标签的机制则没有这方面的要求。可允许信息流控制组件的不同元素对策略有不同程度的偏离。

每个 SFP 都包含一个三元组：主体、信息和导致信息流入流出主体的操作。一些信息流控制策略可能处于一个非常低的详细程度，但仍可根据操作系统中的进程明确描述主体。另一些可能处于较高的详细程度，用通常意义上的用户或输入/输出信道来描述主体。如果信息流控制策略所处的详细程度太高，就有可能不能清晰地定义所需要的 IT 安全功能。在这种情况下，将信息流控制策略描述作为目的会更合适。这样就能规定所期望的 IT 安全功能，作为对那些目的的支持。

在第二个组件(FDP_IFC.2“完全信息流控制”)中，每一个信息流控制 SFP 将涵盖所有可能引发 SFP 所涵盖信息流入、流出 SFP 所涵盖主体的操作。进而，所有信息流都应被 SFP 所涵盖。因此，对于引起信息流动的每一个动作，都有一组规则来决定该动作是否被允许。如果有多个 SFP 适用于一个给定的信息流，在准许其发生之前，应得到所有相关 SFP 的许可。

一个信息流控制 SFP 涵盖一组明确定义的操作。对于一些信息流而言，SFP 涵盖范围可能是“完备”的，或仅处理部分影响信息流的操作。

访问控制 SFP 控制对包含信息的客体的访问，信息流控制 SFP 控制对信息的访问，而独立于它的载体。信息流动时，其属性可能与承载信息的载体属性相关(也可能无关，如多级数据库)。在没有明确授权的情况下，访问者不能改变信息的属性。

信息流和操作可以从多个层面来表述。对于 ST，信息流和操作可以在一个特定系统级别上进行规范：如 TCP/IP 包基于已知的 IP 地址穿越防火墙。对于 PP，信息流和操作可表示为不同类型，如：电子邮件、数据仓库、观测访问等。

本族中的组件，在一个 PP/ST 中可以针对不同的操作和客体子集多次使用。这将满足包含多种策略的 TOE，其中每个策略对应一个特定的客体、主体和操作子集。

F.5.2 FDP_IFC.1 子集信息流控制

F.5.2.1 用户应用注释

本组件要求一个信息流控制策略适用于 TOE 中所有可能操作的一个子集。

F.5.2.2 操作

F.5.2.2.1 赋值

在 FDP_IFC.1.1 中，PP/ST 作者应指定由 TSF 执行的唯一命名的信息流控制 SFP。

在 FDP_IFC.1.1 中，PP/ST 作者应指定 SFP 所涵盖的主体列表、信息列表和引发受控信息流入流出受控主体的操作列表。如上所述，根据 PP/ST 作者的需要，主体列表可有不同的详细程度，比如可以指定为用户、机器或进程。信息可以引用数据，如电子邮件、网络协议或类似访问控制策略中指定的更特殊的客体。如果指定的信息包含在某个遵从访问控制策略的客体中，则在所指定的信息流入、流出客体之前，访问控制策略和信息流控制策略都必须执行。

F.5.3 FDP_IFC.2 完全信息流控制

F.5.3.1 用户应用注释

本组件要求一个信息流控制 SFP 涵盖所有可能引发信息流入、流出 SFP 中主体的操作。

PP/ST 作者必须证实信息流控制 SFP 涵盖了每一个信息流和主体的组合。

F.5.3.2 操作

F.5.3.2.1 赋值

在 FDP_IFC.2.1 中，PP/ST 作者应指定由 TSF 执行的唯一命名的信息流控制 SFP。

在 FDP_IFC.2.1 中，PP/ST 作者应指定 SFP 所涵盖的主体和信息列表。所有引发信息流入流出主体的操作也应被 SFP 涵盖。与上面所述，根据 PP/ST 作者的需要，主体列表可有不同的详细程度，比如可以指定为用户、机器或者进程。信息可以引用数据，如电子邮件、网络协议或类似访问控制策略中指定的更特殊的客体。如果指定的信息包含在某个遵从访问控制策略的客体中，则在所指定的信息流入、流出客体之前，访问控制策略和信息流控制策略都必须执行。

F.6 信息流控制功能(FDP_IFF)

F.6.1 用户注释

本族描述关于能实现在 FDP_IFC 中命名的信息流控制 SFP 的一些特定功能的规则，这些规则同样也指定了策略的控制范围。它由两方面组成：一个负责处理一般的信息流控制功能，另一个负责处理关于一个或多个信息流控制 SFP 的非法信息流问题。这样划分是因为与非法信息流有关的问题，在某种程度上与 SFP 的其余部分毫不相关，非法信息流是指信息流违背了策略，因而不是一个策略问题。

为了实现对不可信任软件的强有力的保护，防止泄露和修改，对信息流的控制是必需的。仅仅只有访问控制是不够的，因为它只控制对信息载体的访问，却允许其中的信息能不加控制地在一个系统中流动。

本族使用了短语“非法信息流类型”，这个短语可以用于指如“存储信道”或“时间信道”一样的信息流分类方法，或者用于指体现 PP/ST 作者需求的改进分类方法。

由于这些组件的灵活性，因而允许在 FDP_IFF.1 和 FDP_IFF.2 中定义特权策略，以允许对全部或

部分特定 SFP 的实现受控旁路。如果需要一个旁路 SFP 的预定义方法，PP/ST 作者应考虑包括一个特权策略。

F.6.2 FDP_IFF.1 简单安全属性

F.6.2.1 用户应用注释

本组件对信息的安全属性、引发信息流动的主体的安全属性以及作为信息接收者的主体的安全属性提出了要求。如果期望信息载体的属性能在信息流控制决策中起一定的作用，或者被一个访问控制策略涵盖，则信息载体的属性也应被考虑。本组件规定应执行的重要规则，并描述如何导出安全属性。

本组件没有规定如何确定安全属性的细节(即，用户相对进程)。策略的灵活性可以通过赋值，以按需指定附加策略和功能要求来实现。

本组件也提供了对信息流控制功能的要求，以便能基于安全属性明确地授权或拒绝信息流。这可用来实现包含本组件所定义的基本策略之外的特权策略。

F.6.2.2 操作

F.6.2.2.1 赋值

在 FDP_IFF.1.1 中，PP/ST 作者应规定 TSF 执行的信息流控制 SFP。信息流控制 SFP 的名字及其控制范围由 FDP_IFC“信息流控制策路”中的组件负责定义。

在 FDP_IFF.1.1 中，PP/ST 作者应针对每一类受控主体和信息，规定与 SFP 规则规范有关的安全属性。比如，这些属性可以是主体标识符、主体敏感性标签、主体通行标签、信息敏感性标签等。安全属性的类型应足以满足环境的需求。

在 FDP_IFF.1.2 中，PP/ST 作者应针对每一个 TSF 将执行的操作，规定主体和信息安全属性之间必须支持基于安全属性的关系。

在 FDP_IFF.1.3 中，PP/ST 作者应详细说明 TSF 将执行的任何其他信息流控制 SFP 规则。这包括那些不是基于信息和主体的安全属性的 SFP 规则，或者那些由于访问操作而引起信息或主体安全属性自动更新的 SFP 规则。第一种情况的例子是一个控制特定信息类型阈值的 SFP 规则。例如，一个包含了统计数据访问规则的信息流 SFP，限制了一个主体只允许在限定的次数下访问这些信息。第二种情况的例子是一个论述在何种条件下，以及主体或客体的安全属性如何随访问操作而变化的 SFP 规则。例如某些信息流策略可对带有特定安全属性的信息的可访问次数进行限制。如果没有附加规则，PP/ST 作者应指明为“无”。

在 FDP_IFF.1.4 中，PP/ST 作者应基于安全属性，规定明确授权信息流的规则。这些规则是前面元素中规定规则的补充，之所以包含在 FDP_IFF.1.4 中，是因为它们含有前面元素中规定规则的例外情况。明确授权信息流的规则的例子是，基于一个与主体相关的特权向量，对于已规定 SFP 所涵盖的信息，总是批准主体具有引发一个信息流的能力。如果不需要这种能力，PP/ST 作者应指明为“无”。

在 FDP_IFF.1.5 中，PP/ST 作者应基于安全属性，规定明确拒绝信息流的规则。这些规则是前面元素中规定规则的补充，之所以包含在 FDP_IFF.1.5 中，是因为它们含有前面元素中规定规则的例外情况。明确拒绝信息流动的规则的例子是，基于一个与主体相关的特权向量，对于已规定 SFP 所涵盖的信息，总是拒绝主体具有引发一个信息流的能力。如果不需要这种能力，PP/ST 作者应指明为“无”。

F.6.3 FDP_IFF.2 分级安全属性

F.6.3.1 用户应用注释

本组件要求已命名的信息流控制 SFP 使用格结构的分级安全属性。

值得注意的是，FDP_IFF.2.4 中确定的分级关系要求，仅需应用于在 FDP_IFF.2.1 中所确定的信息流控制 SFP 的信息流控制安全属性。本组件不打算用于其他的 SFP，比如访问控制 SFP。

FDP_IFF.2.6 描述了构成一个格结构的安全属性集的要求。许多在文献中定义的和在 IT 产品中实现的信息流策略都依赖于格结构的安全属性集。FDP_IFF.2.6 专门处理这种类型的信息流策略。

如果规定了多个信息流控制 SFP，各个 SFP 都有自己的安全属性，并且这些 SFP 互不相关时，PP/ST 作者应为每个 SFP 反复使用本组件。否则，会因为所需的关系不存在，而导致 FDP_IFF.2.4 的各子项之间互相冲突。

F.6.3.2 操作

F.6.3.2.1 赋值

在 FDP_IFF.2.1 中，PP/ST 作者应规定 TSF 执行的信息流控制 SFP。信息流控制 SFP 的名字及其控制范围由 FDP_IFC“信息流控制策略”中的组件负责定义。

在 FDP_IFF.2.1 中，PP/ST 作者应针对每一类受控主体和信息，规定与 SFP 规则规范有关的安全属性。比如，这些属性可以是主体标识符、主体敏感性标签、主体通行标签、信息敏感性标签等。安全属性的类型应足以满足环境的需求。

在 FDP_IFF.2.2 中，PP/ST 作者应针对每一个 TSF 将执行的操作，规定主体和信息安全属性之间必须支持基于安全属性的关系。这些关系应基于安全属性间的有序关系。

在 FDP_IFF.2.3 中，PP/ST 作者应规定 TSF 将执行的任何其他信息流控制 SFP 规则。这包括那些不是基于信息和主体的安全属性的 SFP 规则，或者那些由于访问操作而引起信息或主体安全属性自动更新的 SFP 规则。第一种情况的例子是一个控制特定信息类型阈值的 SFP 规则。例如，一个包含了统计数据访问规则的信息流 SFP，限制了一个主体只允许在限定的次数下访问这些信息。第二种情况的例子是一个论述在何种条件下，以及主体或客体的安全属性如何随访问操作而变化的 SFP 规则。例如某些信息流策略可对带有特定安全属性的信息的可访问次数进行限制。如果没有附加规则，PP/ST 作者应指明为“无”。

在 FDP_IFF.2.4 中，PP/ST 作者应基于安全属性，规定明确授权信息流的规则。这些规则是前面元素中规定的规则的补充，之所以包含在 FDP_IFF.2.4 中，是因为它们含有前面元素中规定规则的例外情况。明确授权信息流的规则的例子是，基于一个与主体相关的特权向量，对于已规定 SFP 所涵盖的信息，总是批准主体具有引发一个信息流的能力。如果不需要这种能力，PP/ST 作者应指明为“无”。

在 FDP_IFF.2.5 中，PP/ST 作者应基于安全属性，规定明确拒绝信息流的规则。这些规则是前面元素中规定的规则的补充，之所以包含于 FDP_IFF.2.5 中，是因为它们含有前面元素中规定规则的例外情况。明确拒绝信息流动的规则的例子是，基于一个与主体相关的特权向量，对于已规定 SFP 所涵盖的信息，总是拒绝主体具有引发一个信息流动的能力。如果不需要这种能力，PP/ST 作者应指明为“无”。

F.6.4 FDP_IFF.3 受限的非法信息流

F.6.4.1 用户应用注释

当要求控制非法信息流的 SFP 中至少有一个不要求消除非法信息流时，应使用本组件。

对于指定的非法信息流，应规定某个最大容量。此外，PP/ST 作者能够指定是否必须审计非法信息流。

F.6.4.2 操作

F.6.4.2.1 赋值

在 FDP_IFF.3.1 中，PP/ST 作者应规定 TSF 执行的信息流控制 SFP。信息流控制 SFP 的名字及其控制范围在 FDP_IFC“信息流控制策略”的组件中定义。

在 FDP_IFF.3.1 中，PP/ST 作者应指定非法信息流的类型，并服从最大流量限制。

在 FDP_IFF.3.1 中，PP/ST 作者应对所有确定的非法信息流规定最大容量。

F.6.5 FDP_IFF.4 部分消除非法信息流

F.6.5.1 用户应用注释

当所有要求控制非法信息流的 SFP 都要求部分(而不必全部)消除非法信息流时，应使用本组件。

F.6.5.2 操作

F.6.5.2.1 赋值

在 FDP_IFF.4.1 中，PP/ST 作者应规定 TSF 执行的信息流控制 SFP。信息流控制 SFP 的名字及其控制范围在 FDP_IFC“信息流控制策略”的组件中定义。

在 FDP_IFF.4.1 中，PP/ST 作者应指定非法信息流类型，并服从最大流量限制。

在 FDP_IFF.4.1 中，PP/ST 作者应对所有确定的非法信息流规定最大容量。

在 FDP_IFF.4.2 中，PP/ST 作者应指定要消除的非法信息流类型。该列表不能为空，因为本组件要求一些非法信息流必需被消除。

F.6.6 FDP_IFF.5 无非法信息流

F.6.6.1 用户应用注释

当要求控制非法信息流的 SFP 要求消除所有非法信息流时，应使用本组件。然而，PP/ST 作者应仔细考虑消除所有非法信息流对 TOE 正常的功能操作可能造成的影响。许多实际应用表明，TOE 中的功能与非法信息流之间存在着某种间接的联系，消除所有非法信息流将减少预期的 TOE 功能。

F.6.6.2 操作

F.6.6.2.1 赋值

在 FDP_IFF.5.1 中，PP/ST 作者应规定需要消除非法信息流的信息流控制 SFP。信息流控制 SFP 的名字及其控制范围在 FDP_IFC“信息流控制策略”的组件中定义。

F.6.7 FDP_IFF.6 非法信息流监视

F.6.7.1 用户应用注释

当期望 TSF 监视非法信息流的使用是否超出一个规定容量时，应使用本组件。如果期望审计这种流，那么本组件可作为 FAU_GEN“安全审计数据产生”族中组件所使用的审计事件源。

F.6.7.2 操作

F.6.7.2.1 赋值

在 FDP_IFF.6.1 中，PP/ST 作者应规定 TSF 执行的信息流控制 SFP。信息流控制 SFP 的名字及

其控制范围在 FDP_IFC“信息流控制策略”的组件中定义。

在 FDP_IFF.6.1 中,PP/ST 作者应规定非法信息流类型,并监视此类信息流是否超出最大容量。

在 FDP_IFF.6.1 中,PP/ST 作者应规定 TSF 监视非法信息流是否超出最大容量。

F.7 从 TOE 之外输入(FDP_ITC)

F.7.1 用户注释

本族定义从 TOE 之外向 TOE 进行 TSF 促成输入用户数据的机制,以使用户数据的安全属性得到保护。安全属性的一致性由 FPT_TDC“TSF 间 TSF 数据的一致性”负责。

FDP_ITC 涉及对输入的限制、安全属性的用户规范以及安全属性与用户数据的关联。

本族以及相应的输出族 FDP_ETC“从 TOE 输出”,说明了 TOE 如何处理其控制之外的用户数据。本族涉及用户数据安全属性的赋值和抽象。

可能涉及下列活动:

a) 从未格式化的媒体(如软盘、磁带、扫描仪、视频或音频信号)输入用户数据,其未包含任何安全属性,通过对媒体进行物理标记来指示其内容;

b) 从媒体输入用户数据,其包括安全属性,并校验客体安全属性是否适当;

c) 从媒体输入用户数据,其包括安全属性,并使用密码封装技术保护用户数据及其安全属性的关联性。

本族并不关注判断用户数据是否可以输入,而只关注与所输入用户数据相关联的安全属性值。

用户数据的输入有两种可能性:用户数据明确无误地与可靠的客体安全属性相关联(安全属性的值和含义都没有被修改),或者从输入源没有获得可靠的安全属性(甚至没有安全属性)。本族负责处理了以上两种情况。

如果有可靠的安全属性,它们可通过物理方式(安全属性在同一媒体上)或逻辑方式(安全属性分布各不相同,但包含唯一的客体标识,比如密码校验和)与用户数据相关联。

本族关注用户数据的 TSF 促成输入,以及维持 SFP 所需安全属性的关联关系。其他族关注输入的其他方面,比如一致性、可信信道和完整性,这些都超出本族的范围。此外,FDP_ITC“从 TOE 之外输入”只关注与输入媒体的接口。FDP_ETC“从 TOE 输出”负责媒体的另一端(原发端)。

下面是一些常见的输入要求:

a) 不带任何安全属性的用户数据输入;

b) 带有安全属性的用户数据输入,两者相互关联,并且安全属性明确无误地表征了所输入的信息。

有没有人为干预,TSF 都可以处理这些输入要求,这取决于 IT 限制和组织安全策略。比如,如果通过“机密”信道接收用户数据,客体安全属性将置为“机密”。

如果存在多个(访问控制或信息流控制)SFP,那么对每个已命名的 SFP 就可以反复使用本族中的这些组件。

F.7.2 FDP_ITC.1 不带安全属性的用户数据输入

F.7.2.1 用户应用注释

本组件用于规定没有可靠的(或者任何)安全属性与之关联的用户数据的输入。此功能要求关于所输入用户数据的安全属性要在 TSF 中初始化。也可以是 PP/ST 作者规定输入规则。在某些环境中,要求通过可信路径或可信信道机制来提供这些属性也是合适的。

F.7.2.2 操作

F.7.2.2.1 赋值

在 FDP_ITC.1.1 中，PP/ST 作者应规定，当从 TOE 外部输入用户数据时，将执行的访问控制 SFP 或信息流控制 SFP。对这些 SFP 的赋值确定了该功能输入的用户数据的范围。

在 FDP_ITC.1.3 中，PP/ST 作者应规定所有附加的输入控制规则，如果没有额外的输入控制规则则赋值为“无”。这些规则将与 FDP_ITC.1.1 中所选访问控制 SFP 或信息流控制 SFP 一起被 TSF 执行。

F.7.3 FDP_ITC.2 带有安全属性的用户数据输入

F.7.3.1 用户应用注释

本组件用于规定具有可靠的安全属性与之关联的用户数据的输入。此功能依赖于安全属性准确无误地与输入媒体上的客体相关联。一旦输入后，那些客体将具有相同的属性。这需要 FPT_TDC“TSF 间 TSF 数据一致性”保证数据的一致性。也可以是 PP/ST 作者规定输入规则。

F.7.3.2 操作

F.7.3.2.1 赋值

在 FDP_ITC.2.1 中，PP/ST 作者应规定，当从 TOE 外部输入用户数据时，将执行的访问控制 SFP 或信息流控制 SFP。对这些 SFP 的赋值确定了该功能输入的用户数据的范围。

在 FDP_ITC.2.5 中，PP/ST 作者应规定所有附加的输入控制规则，如果没有额外的输入控制规则则赋值为“无”。这些规则将与 FDP_ITC.2.1 中所选访问控制 SFP 或信息流控制 SFP 一起被 TSF 执行。

F.8 TOE 内部传送(FDP_ITT)

F.8.1 用户注释

当用户数据通过内部信道在 TOE 各部分间传送时，本族提供对用户数据进行保护的要求。本族与 FDP_UCT“TSF 间用户数据机密性传送保护”和 FDP_UIT“TSF 间用户数据完整性传送保护”族的不同之处在于，后两者为用户数据经外部信道在不同的 TSF 间传送时提供保护；而与族 FDP_ETC“从 TOE 输出”和 FDP_ITC“从 TOE 之外输入”的不同之处则在于，它们处理的是由 TSF 促成的与 TOE 之外的数据交互。

当用户数据在 TOE 内部传送时，本族中的要求允许 PP/ST 作者规定对其所期望的安全性，这种安全性可保护数据以避免其被泄露、被篡改或丧失可用性。

决定本族应采用的物理隔离程度取决于预期的使用环境。在恶劣环境中，只用一条系统总线在分散的 TOE 部分间传送数据，可能会产生风险。在比较可靠的环境中，传送就可通过更多的传统网络媒介进行。

如果存在多个(访问控制或信息流控制)SFP，对每个已命名的 SFP，可反复使用本族中的这些组件。

F.8.2 FDP_ITT.1 基本内部传送保护

F.8.2.1 操作

F.8.2.1.1 赋值

在 FDP_ITT.1.1 中，PP/ST 作者应规定涵盖所传送信息的访问控制 SFP 或信息流控制 SFP。

F.8.2.1.2 选择

在 FDP_ITT.1.1 中，PP/ST 作者应规定用户数据在传送时，TSF 应防止发生的传送错误类型。选项为：泄露、篡改、丧失可用性。

F.8.3 FDP_ITT.2 按属性分隔传送

F.8.3.1 用户应用注释

本组件可用于对具有不同通行级别的信息提供不同形式的保护。

在数据传送时实现相互隔离的方法之一是使用不同的逻辑或物理信道。

F.8.3.2 操作

F.8.3.2.1 赋值

在 FDP_ITT.2.1 中，PP/ST 作者应规定涵盖所传送的信息的访问控制 SFP 或信息流控制 SFP。

F.8.3.2.2 选择

在 FDP_ITT.2.1 中，PP/ST 作者应规定用户数据在传送时，TSF 应防止发生的传送错误类型。选项为：泄露、篡改、丧失可用性。

F.8.3.2.3 赋值

在 FDP_ITT.2.2 中，PP/ST 作者应规定安全属性，TSF 将使用这些属性值，确定何时分离在 TOE 物理上分隔的部分之间传送的数据。比如，与一个属主身份相关联的用户数据将与关联另一个属主身份的用户数据分别传送。在这种情况下，数据属主的身份值，就用来确定何时分隔传送的数据。

F.8.4 FDP_ITT.3 完整性监视

F.8.4.1 用户应用注释

本组件与 FDP_ITT.1 或 FDP_ITT.2 结合起来使用，确保 TSF 检查所接收到的用户数据（及其属性）的完整性。FDP_ITT.1 或 FDP_ITT.2 将以一种保护数据不被篡改的方式提供数据（所以 FDP_ITT.3 能检测出对数据的任何篡改）。

PP/ST 作者应规定必须检测的错误类型。PP/ST 作者应考虑：数据篡改、数据替换、数据不可恢复的排序改变、数据重放、不完全的数据以及其他完整性错误。

PP/ST 作者必须规定在检测到一个失败后 TSF 应采取的动作。比如：忽略用户数据、重新请求数据、告知授权管理员、从其他线路重新路由。

F.8.4.2 操作

F.8.4.2.1 赋值

在 FDP_ITT.3.1 中，PP/ST 作者应规定涵盖所传送信息的信息访问控制 SFP 或信息流控制 SFP，并监视完整性错误。

在 FDP_ITT.3.1 中，PP/ST 作者应规定在用户数据传送时，应监视的可能的完整性错误类型。

在 FDP_ITT.3.2 中，PP/ST 作者应规定当出现一个完整性错误时，TSF 应采取的动作。比如：TSF 应请求重新发送用户数据。在 FDP_ITT.3.1 中规定的 SFP 将作为 TSF 采取的动作被执行。

F.8.5 FDP_ITT.4 基于属性的完整性监视

F.8.5.1 用户应用注释

本组件与 FDP_ITT.2 结合使用，确保 TSF 检查所接收的通过不同信道（基于指定的安全属性值）传送的用户数据的完整性。允许 PP/ST 作者规定检测到完整性错误后应采取的动作。

例如，本组件可用来规定不同的完整性错误检测和对不同完整性级别信息应采取的动作。

PP/ST 作者应指定必须检测的错误类型。PP/ST 作者应考虑：数据篡改、数据替换、数据不可恢复的排序改变、数据重放、不完全的数据以及其他完整性错误。

PP/ST 作者应指定使得需要完整性错误监视的属性（以及相关的传送信道）。

PP/ST 作者必须规定在检测到一个失败后 TSF 应采取的动作。比如：忽略用户数据、重新请求数据、告知授权管理员、从其他线路重新路由。

F.8.5.2 操作

F.8.5.2.1 赋值

在 FDP_ITT.4.1 中，PP/ST 作者应规定涵盖所传送信息的信息访问控制 SFP 或信息流控制 SFP 并监视完整性错误。

在 FDP_ITT.4.1 中，PP/ST 作者应规定在用户数据传送时，应监视的可能的完整性错误类型。

FDP_ITT.4.1 中，PP/ST 作者应规定需要分隔传送信道的安全属性列表。该列表用于确定哪些用户数据需要基于其安全属性和传送信道进行完整性错误监视。本元素与 FDP_ITT.2“按属性分隔传送”直接相关。

在 FDP_ITT.4.2 中，PP/ST 作者应规定当出现一个完整性错误时，TSF 应采取的动作。比如：TSF 应请求重新发送用户数据。在 FDP_ITT.4.1 中规定的 SFP 将作为 TSF 采取的动作被执行。

F.9 残余信息保护（FDP_RIP）

F.9.1 用户注释

残余信息保护保证 TSF 控制的资源当从一个客体被解除分配时并且在它们被再分配给其他客体之前由 TSF 处理，在某种程序上在它被解除分配以前不可能重建所有或部分包含在资源中的数据。

TOE 通常有许多功能，这些功能潜在地从客体解除分配资源并且潜在地再分配这些资源给客体。所有资源中的一些资源可能被用来存储以前使用的资源的关键数据，并且那些资源因 FDP_RIP 要求准备重新使用。客体重用适用于主体或用户对释放资源的明确需要，也适用于 TSF 导致资源的解除分配和后来再分配给不同的客体的明确活动。明确需要的例子是删除或截断文件，或者主存储器区域的释放。TSF 的明确活动的例子是缓存区域的解除分配和再分配。

客体重用的要求与属于客体的资源的内容有关，不是所有有关资源或客体的信息都可以被存储在TSF中的其他地方。例如以满足对文件作为客体的FDP_RIP要求，组成文件的所有扇区需要准备被重新使用。

它也适用于被系统中不同主体连续重复使用的资源。比如，大多数操作系统通常依赖硬件寄存器(资源)来支持系统中的进程。当进程从“运行”状态转换为“休眠”状态(反之亦然)，这些寄存器被不同的主体连续地重复使用。“转换”动作并没有考虑一个资源的分配或释放，FDP_RIP“残余信息保护”适用于这种事件和资源。

FDP_RIP“残余信息保护”通常控制对信息的访问，此信息不是任何当前所定义的或可访问的客体的一部分，但在某些情况下可能并不如此。比如，客体A是一个文件，客体B是驻留该文件的一个磁盘，如果客体A被删除，尽管它仍是客体B的一部分，但来自客体“A”的信息将受FDP_RIP的控制。

值得注意的是，FDP_RIP仅适用于在线客体，不适用于那些诸如备份在磁带上的离线客体。比如，如果一个TOE内的文件被删除，就可以实例化FDP_RIP，要求在释放资源时不能有残余信息存在；然而，TSF不能将该要求扩展到离线备份中的同一文件，因此该文件仍然可用。如果要关注离线客体，PP/ST作者应确保具有适当的环境目的，以支持操作用户指南负责处理离线客体。

当FDP_RIP实例化要求，在应用程序释放客体到TSF(即重新分配)的同时立即清除残余信息时，FDP_RIP“残余信息保护”和FDP_ROL“回退”会产生冲突。因而，FDP_RIP选择“释放资源”时，不应与FDP_ROL同时使用，因为没有信息可以回退。另一个选择，“无效分配”可与FDP_ROL同时使用，但存在一个风险，就是带有信息的资源在回退发生前分配给了新客体，如果是这样，回退就不可能实现。

在FDP_RIP中没有审计要求，因为这不是一个由用户使用的功能。分配或释放资源的审计将作为访问控制SFP或信息流控制SFP操作的一部分来进行。

本族适用于由访问控制SFP或信息流控制SFP所指定的客体，如PP/ST作者所规定的那样。

F.9.2 FDP_RIP.1 子集残余信息保护

F.9.2.1 用户注释

对于TOE中的一个客体子集，本组件要求TSF确保在分配给这些客体的资源或从这些客体释放的资源中都没有可用的残余信息。

F.9.2.2 操作

F.9.2.2.1 选择

在FDP_RIP.1.1中，PP/ST作者应规定调用残余信息保护功能分配或释放资源的事件。

F.9.2.2.2 赋值

在FDP_RIP.1.1中，PP/ST作者应规定受残余信息保护的客体列表。

F.9.3 FDP_RIP.2 完全残余信息保护

F.9.3.1 用户应用注释

对于TOE中的所有客体，本组件要求TSF确保在分配给这些客体的资源或从这些客体释放的资源中都没有可用的残余信息。

F.9.3.2 操作

F.9.3.2.1 选择

在FDP_RIP.2.1中，PP/ST作者应规定调用残余信息保护功能分配或释放资源的事件。

F.10 回退(FDP_ROL)

F.10.1 用户注释

本族负责处理返回到一个明确定义的有效状态的这类需求,如用户需要撤销对一个文件的修改操作或撤销对数据库的一连串未完成的处理操作。

本族的目的在于帮助用户,在撤销最后一组操作后,返回到一个明确定义的有效状态,或对于分布式数据库,将数据库的所有分布式拷贝返回到操作失效发生之前的状态。

当 FDP_RIP"残余信息保护"使得在释放客体资源的同时其内容不再可利用时, FDP_RIP"残余信息保护"与 FDP_ROL"回退"会相互冲突。因此,FDP_RIP 不能与 FDP_ROL 结合使用,因为已没有信息可以回退。当仅要求在给客体分配资源时使其内容不可用,FDP_RIP 可与 FDP_ROL 一起使用,这是因为 FDP_ROL 机制将有机会访问仍然存于 TOE 中的那些早先信息,以成功实现回退操作。

回退要求受某些约束条件限制。比如,文本编辑器常常只允许回退一定数量的命令。另一个例子是备份,在备份磁带重复使用后,它以前的信息将不能恢复,这同样就需要对回退要求提出限制。

F.10.2 FDP_ROL.1 基本回退

F.10.2.1 用户应用注释

本组件允许用户或主体对预先定义的一组客体撤销一组操作。撤销只能在某种限制条件下进行,如一定数量的字符或一定的时间段。

F.10.2.2 操作

F.10.2.2.1 赋值

在 FDP_ROL.1.1 中,PP/ST 作者应指定进行回退操作时需执行的访问控制 SFP 或信息流控制 SFP。有必要确保回退不是用来绕开 SFP 的。

在 FDP_ROL.1.1 中,PP/ST 作者应指定能被回退的操作列表。

在 FDP_ROL.1.1 中,PP/ST 作者应指定服从于回退策略的信息或客体列表。

在 FDP_ROL.1.2 中,PP/ST 作者应指定回退操作可以进行的边界条件。该边界条件可以是预定义的时间段,比如可以撤销在过去的两分钟内所执行的操作。其他可能的边界可定义为允许的最大操作数量或缓冲器大小。

F.10.3 FDP_ROL.2 高级回退

F.10.3.1 用户应用注释

本组件要求 TSF 提供回退全部操作的能力,但用户只能选择仅回退其中一部分操作。

F.10.3.2 操作

F.10.3.2.1 赋值

在 FDP_ROL.2.1 中,PP/ST 作者应指定进行回退操作时要执行的访问控制 SFP 或信息流控制 SFP。有必要确保回退不是用来绕开 SFP 的。

在 FDP_ROL.2.1 中,PP/ST 作者应指定服从于回退策略的客体列表。

在 FDP_ROL.2.2 中,PP/ST 作者应指定回退操作可以进行的边界条件。该边界条件可以是预定义的时间段,比如可以撤销在过去的两分钟内所执行的操作。其他可能的边界可定义为允许的最大操

作数量或缓冲器大小。

F.11 存储数据的完整性(FDP_SDI)

F.11.1 用户注释

本族提供了对由 TSF 控制的载体内所存用户数据进行保护的要求。

硬件失灵或错误都可能影响存储在内存中的数据。本族提出检测这些无意的错误的要求。保存在 TSF 控制的存储设备中的用户数据的完整性也由本族负责。

要想避免主体修改数据,应选择 FDP_IFF"信息流控制功能"或 FDP_ACF"访问控制功能"族(而不是本族)。

本族不同于 FDP_ITT"TOE 内部传送",FDP_ITT 是保护用户数据在 TOE 内部传送时不出现完整性错误。

F.11.2 FDP_SDI.1 存储数据的完整性监视

F.11.2.1 用户应用注释

本组件监视在媒体中所存储数据的完整性错误。PP/ST 作者可指定各种用户数据属性作为监视的基础。

F.11.2.2 操作

F.11.2.2.1 赋值

在 FDP_SDI.1.1 中,PP/ST 作者应指定 TSF 应检测的完整性错误。

在 FDP_SDF.1.1 中,PP/ST 作者应指定作为监视基础的用户数据属性。

F.11.3 FDP_SDI.2 存储数据完整性监视和反应

F.11.3.1 用户应用注释

本组件监视在媒体中所存储数据的完整性错误。PP/ST 作者应指定监视到完整性错误时应采取的动作。

F.11.3.2 操作

F.11.3.2.1 赋值

在 FDP_SDI.2.1 中,PP/ST 作者应指定 TSF 应检测的完整性错误。

在 FDP_SDI.2.1 中,PP/ST 作者应指定作为监视基础的用户数据属性。

在 FDP_SDI.2.2 中,PP/ST 作者应指定检测到完整性错误时应采取的动作。

F.12 TSF 间用户数据机密性传送保护(FDP_UCT)

F.12.1 用户注释

当用户数据通过外部信道,在 TOE 和其他可信 IT 产品间传递时,本族定义确保其机密性的要求。用户数据在两点间传送时,通过防止未授权的泄露来实现机密性。端点可以是一个 TSF 或用户。

本族对传送中的用户数据保护提出了要求,大不相同的是,FTP_ITC"输出 TSF 数据的机密性"处

理的是 TSF 数据。

F.12.2 FDP_UCT.1 基本的数据交换机密性

F.12.2.1 用户应用注释

TSF 应有能力对交换的用户数据实施保护，以防止其被泄露。

F.12.2.2 操作

F.12.2.2.1 赋值

在 FDP_UCT.1.1 中，PP/ST 作者应指定交换用户数据时所执行的访问控制 SFP 或信息流控制 SFP。指定的策略将用于决定谁可以交换数据以及哪些数据可以交换。

F.12.2.2.2 选择

在 FDP_UCT.1.1 中，PP/ST 作者应指定本元素是用在传送用户数据的机制中，还是用在接收用户数据的机制中。

F.13 TSF 间用户数据完整性传送保护(FDP_UIT)

F.13.1 用户注释

当用户数据在 TSF 和其他可信 IT 产品间传送时，本族定义提供完整性保护以及从可检测到的错误中恢复的要求。至少，本族要针对篡改行为监视用户数据的完整性。此外，本族还支持采用不同方法纠正检测到的完整性错误。

本族对传送中的用户数据提出了完整性要求，而 FPT_ITI“输出 TSF 数据的完整性”处理的是 TSF 数据。

FDP_UIT“TSF 间数据完整性传送保护”和 FDP_UCT“TSF 间数据机密性传送保护”彼此都是成双成对的，由于 FDP_UCT 负责处理用户数据的机密性，因此实现 FDP_UIT 的机制同样可用于实现 FDP_UCT 和 FDP_ITC 族。

F.13.2 FDP_UIT.1 数据交换的完整性

F.13.2.1 用户应用注释

TSF 应具有以某种方式发送和接收用户数据，以便检测对用户数据的篡改的能力。本组件没有对试图从篡改中恢复数据的 TSF 机制提出要求。

F.13.2.2 操作

F.13.2.2.1 赋值

在 FDP_UIT.1.1 中，PP/ST 作者应指定在发送或接收数据时所执行的访问控制 SFP 或信息流控制 SFP。指定的策略将用于确定谁可以发送或接收数据以及哪些数据可以发送或接收。

F.13.2.2.2 选择

在 FDP_UIT.1.1 中，PP/ST 作者应指定本元素用在发送客体的 TSF 中，还是用在接收客体的 TSF 中。

在 FDP_UIT.1.1 中，PP/ST 作者应指定是否需要保护数据，以避免被篡改、删除、插入或重放。

在 FDP_UIT.1.2 中，PP/ST 作者应指定是否应检测以下错误类型：篡改、删除、插入或重放。

F.13.3 FDP_UIT.2 原发端数据交换恢复

F.13.3.1 用户应用注释

本组件提供从一组确定的传送错误中恢复数据的能力，必要时需要其他可信 IT 产品提供帮助。由于其他可信 IT 产品处于 TOE 之外，TSF 不能控制其行为。但，本组件可提供能与其他可信 IT 产品合作共通实现恢复目的的功能。例如，TSF 可包含这种功能：在检测到错误时，依靠原发端可信 IT 产品来重新发送数据。本组件涉及 TSF 恢复这种错误的能力。

F.13.3.2 操作

F.13.3.2.1 赋值

在 FDP_UIT.2.1 中，PP/ST 作者应指定在恢复用户数据时所执行的访问控制 SFP 或信息流控制 SFP。指定的策略用于确定哪些数据能被恢复以及如何恢复。

在 FDP_UIT.2.1 中，PP/ST 作者应指定完整性错误列表，这样 TSF 在原发端可信 IT 产品的帮助下，能够从其中恢复原来的用户数据。

F.13.4 FDP_UIT.3 接受端数据交换恢复

F.13.4.1 用户应用注释

本组件提供从一组确定的传送错误中恢复数据的能力。它能在没有原发端可信 IT 产品的帮助下完成该任务。例如，如果检测到某些错误，传送协议必须足够健壮，使 TSF 能基于校验和协议中其他可用信息，从错误中恢复数据。

F.13.4.2 操作

F.13.4.2.1 赋值

在 FDP_UIT.3.1 中，PP/ST 作者应指定在恢复用户数据时所执行的访问控制 SFP 或信息流控制 SFP。指定的策略用于确定哪些数据能够恢复以及如何恢复。

在 FDP_UIT.3.1 中，PP/ST 作者应指定完整性错误的列表，这样，接收端 TSF 就能独自恢复原始用户数据。

附 录 G
（规范性附录）
FIA 类：标识和鉴别

一个常见的安全要求是无歧义地标识执行 TOE 中功能的人和/或实体。这不仅包括设置每一个用户所声称的身份，而且包括验证每一个用户确实是他或她所声称的人，这可通过要求用户向 TSF 提供一些已为 TSF 所知的与该用户有关的信息来实现。

此类中的族负责处理关于设置和验证所声称的用户身份方面的功能要求。需要“标识和鉴别”，是为了确保用户与正确的安全属性（比如身份、组、角色、安全性或完整性级别）相关联。

授权用户的明确标识和安全属性与用户和主体的正确关联是安全策略实施的关键。

FIA_UID“用户标识”族负责确定用户的身份。

FIA_UAU“用户鉴别”族负责验证用户的身份。

FIA_AFL“鉴别失败”族负责对重复的未成功鉴别尝试定义限制条件。

FIA_ATD“用户属性定义”族负责定义用于执行 SFR 的用户属性。

FIA_USB“用户-主体绑定”族负责正确关联每一授权用户安全属性。

FIA_SOS“秘密的规范”族负责生成和验证满足一个指定度量的秘密。

本类的组件构成分解如图 G.1 所示。

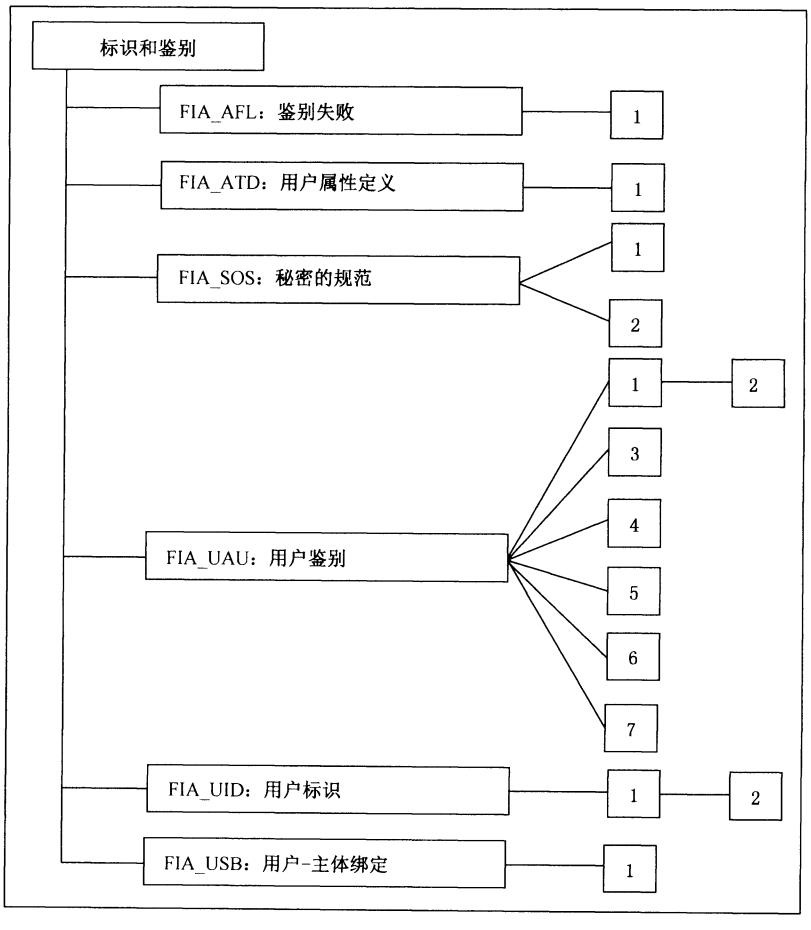

图 G.1 标识和鉴别类分解

G.1 鉴别失败(FIA_AFL)

G.1.1 用户注释

本族要求定义鉴别尝试的值和鉴别尝试失败时 TSF 的动作。参数包括但不限于尝试的次数和时间门限值。

会话建立过程是与用户进行交互,执行会话建立的过程,独立于实际实现。如果不成功的鉴别尝试次数超过指定的门限值,那么用户账号或终端(或者两者都)将被锁定。如果用户账号被禁止,用户就不能登录到系统上。如果终端被禁止,终端(或终端所拥有的地址)就不能再使用。这两种状态都将保持,直到满足重建条件为止。

G.1.2 FIA_AFL.1 鉴别失败处理

G.1.2.1 用户应用注释

PP/ST 作者可以定义不成功鉴别尝试的次数,也可选择让 TOE 开发者或授权用户来定义该数值。不成功的鉴别尝试不必是连续的,但应与鉴别事件相关。如鉴别事件可以是,在指定的终端上从上一次成功建立会话以来的尝试计数。

PP/ST 作者可以规定在鉴别失败的情况下,TSF 将采取的动作列表。如果 PP/ST 作者认为合适的话,也可让授权的管理员来管理这些事件。这些动作可以是:终端失效、用户账号失效或向管理员报警等。对这些动作必须说明,在什么条件下,情况可恢复正常。

为了防止拒绝服务,TOE 通常保证至少有一个用户账号不能失效。

PP/ST 作者可以说明 TSF 可采取的进一步动作,包括重新允许用户会话建立过程或向管理员报警等。例如这些动作有:直到过了指定的时间、直到授权管理员重新激活终端/账号、与上次失败尝试相关的一个时间(每次尝试失败,失效时间就加倍)。

G.1.2.2 操作

G.1.2.2.1 选择

在 FIA_AFL.1.1 中,PP/ST 作者应选择一个正整数赋值,或选择"管理员可设置的正整数"来规定可接受的数值范围。

G.1.2.2.2 赋值

在 FIA_AFL.1.1 中,PP/ST 作者应指定鉴别事件。例如,这些鉴别事件可以是:对指定的用户身份,自从上次鉴别成功以来的不成功鉴别尝试;当前终端自从上次成功鉴别以来的不成功鉴别尝试;最后 10 min 内不成功鉴别尝试的次数,等等。至少应规定一个鉴别事件。

在 FIA_AFL.1.1 中,如果选择了一个正整数赋值,PP/ST 作者应规定不成功鉴别尝试的缺省次数(正整数),一旦达到或超过该次数,将触发这些事件。

在 FIA_AFL.1.1 中,如果选择了管理员可设置的正整数,PP/ST 作者应规定可接受的数值范围,TOE 管理员可从中配置不成功鉴别尝试的次数。鉴别尝试的次数不应小于或等于上限值,和大于或等于下限值。

G.1.2.2.3 选择

在 FIA_AFL.1.2 中,PP/ST 作者应选择当达到或超过已定义的未成功鉴别尝试次数时由 TSF 触

发动作。

G.1.2.2.4 赋值

在 FIA_AFL.1.2 中，PP/ST 作者应规定当达到或超过（与选择的一样）临界值时，将采取的动作。这些动作可以是：使一个账户失效 5 min、使终端失效一段随次数增加的时间（2 的不成攻鉴别次数次幂，单位是秒）、或使账号失效到直到管理员解除并且同时通知管理员。这些动作应规定措施，措施的持续时间（若适用的话），或措施终止的条件。

G.2 用户属性定义（FIA_ATD）

G.2.1 用户注释

除了用户身份之外，所有授权用户还可以拥有一组安全属性，用以执行 SFR。本族定义了将用户安全属性与用户相关联的要求，并为 TSF 做安全决策时提供支持。

存在着对单个安全策略（SFP）定义的依赖关系。这些单独的定义应列出策略执行所需的属性。

G.2.2 FIA_ATD.1 用户属性定义

G.2.2.1 用户应用注释

本组件规定安全属性应在用户层面上加以维护。这意味着所列出的安全属性可以在用户层面上分配和改变。也就是说，改变这个列表中与一个用户有关的某个安全属性，对其他任何用户的安全属性不会产生影响。

在安全属性属于一组用户的情况下（如组的能力列表），用户将需要有一个对有关组的引用（作为安全属性）。

G.2.2.2 操作

G.2.2.2.1 赋值

在 FIA_ATD.1.1 中，PP/ST 作者应规定与单个用户相关联的安全属性。例如，{“许可”、“组的标识符”、“权限”}就是此类列表的一个实例。

G.3 秘密的规范（FIA_SOS）

G.3.1 用户注释

本族定义关于对所提供的秘密进行既定质量度量，以及生成满足既定度量的秘密的机制的要求。例如，用户所提供口令的自动校验，或自动生成口令就是一种机制。

秘密可以在 TOE 之外生成（比如，由用户选择并导入 TOE 中）。在这种情况下，FIA_SOS.1 “秘密的验证”组件可用来确保外部生成的秘密遵从某些标准，比如最小长度、非字典用字或以前未用过。

秘密也可由 TOE 生成。在这种情况下，FIA_SOS.2“TSF 生成秘密”组件可用来要求 TOE 确保秘密将遵从某些指定的度量。

用户为鉴别机制提供的包含鉴别数据的秘密是基于用户所拥有的知识的。当采用密钥时，应使用 FCS“密码支持”类来代替本族。

G.3.2 FIA_SOS.1 秘密的验证

G.3.2.1 用户应用注释

秘密可以由用户生成。这个组件确保,可以验证那些由用户生成的秘密满足某个质量度量。

G.3.2.2 操作

G.3.2.2.1 赋值

在 FIA_SOS.1.1 中,PP/ST 作者应提供一个既定的质量度量。该质量度量的规范可以简单到只是对一个要执行的质量检查进行描述,也可像引用政府出版的标准一样正式定义秘密必须满足的质量度量。例如,质量度量可包括对可接受的秘密的字母数字形式的描述或可接受的秘密必须满足的空间大小的描述。

G.3.3 FIA_SOS.2 TSF 生成秘密

G.3.3.1 用户应用注释

本组件允许 TSF 为特定的功能,如利用口令方式的鉴别功能生成秘密。

当秘密的生成算法中使用了伪随机数生成器时,应允许输入的随机数将提供具有高不可预见性的输出。该随机数(种子)可从许多可用的参数中导出,如系统时钟、系统寄存器、日期、时间等。参数的选择应保证可以从这些输入中生成的唯一性种子数至少应等于必须生成的最少秘密数。

G.3.3.2 操作

G.3.3.2.1 赋值

在 FIA_SOS.2.1 中,PP/ST 作者应提供一个既定的质量度量。该质量度量的规范可以简单到只是对一个要执行的质量检查进行描述,也可像引用政府出版的标准一样正式定义秘密必须满足的质量度量。例如,质量度量可包括对可接受的秘密的字母数字形式的描述或可接受的秘密必须满足的空间大小的描述。

在 FIA_SOS.2.2 中,PP/ST 作者应提供一个必须使用 TSF 所生成秘密的 TSF 功能列表。例如,基于口令的鉴别机制即属于此类功能。

G.4 用户鉴别(FIA_UAU)

G.4.1 用户注释

本族定义 TSF 所支持的用户鉴别机制类型,也定义用户鉴别机制必须依赖的属性。

G.4.2 FIA_UAU.1 鉴别的时机

G.4.2.1 用户应用注释

本组件要求 PP/ST 作者定义 TSF 促成的动作,在用户声称的身份得到鉴别前,TSF 可代表用户执行这些动作。这些 TSF 促成的动作应该与在得到鉴别之前错误标识自己的用户无任何安全关系。对于其他一切不在该列表中的 TSF 促成的动作,在动作能够被 TSF 代表用户执行前,用户必须得到鉴别。

本组件不能控制这些动作在标识发生前是否也能被执行。这需要使用 FIA_UID.1“标识的时机”或 FIA_UID.2“任何动作前的用户标识”,且适当的赋值。

G.4.2.2 操作

G.4.2.2.1 赋值

在 FIA_UAU.1.1 中,PP/ST 作者应规定在用户声称的身份得到鉴别前,TSF 代表用户可执行的 TSF 促成的动作列表。这个列表不能为空,如果没有合适的动作,应使用组件 FIA_UAU.2“任何动作前的用户标识”来代替。此类动作的一个实例是:在登录过程中请求帮助。

G.4.3 FIA_UAU.2 任何动作前的用户鉴别

G.4.3.1 用户应用注释

本组件要求在代表用户的任何其他 TSF 促成的动作发生前,用户已被成功鉴别。

G.4.4 FIA_UAU.3 不可伪造的鉴别

G.4.4.1 用户应用注释

本组件对提供鉴别数据保护的机制提出了要求。应检测出或拒绝掉从另一个用户处拷贝来的,或用其他方法构建的鉴别数据。这些机制提供一种信任,即 TSF 鉴别过的用户确实是他们所声称的那个。

本组件可能只对基于不可共享的鉴别数据(比如生物测定学)的鉴别机制有用。对 TSF 来说,检测或防止 TSF 控制之外的口令共享是不可能的。

G.4.4.2 操作

G.4.4.2.1 选择

在 FIA_UAU.3.1 中,PP/ST 作者应规定 TSF 是检测、防止还是检测并防止对鉴别数据的伪造。

在 FIA_UAU.3.2 中,PP/ST 作者应规定 TSF 是检测、防止还是检测并防止对鉴别数据的拷贝。

G.4.5 FIA_UAU.4 一次性鉴别机制

G.4.5.1 用户应用注释

本组件对基于一次性鉴别数据的鉴别机制提出了要求。一次性鉴别数据可以是用户拥有或知道的某些事情,而非用户是什么。例如,一次性口令、加密的时间戳或秘密查找表中的随机数都是一次性鉴别数据。

PP/ST 作者可规定本要求适用于哪一种鉴别机制。

G.4.5.2 操作

G.4.5.2.1 赋值

在 FIA_UAU.4.1 中,PP/ST 作者应规定本要求适用的鉴别机制列表。该赋值可以是“所有鉴别机制”。例如,该赋值可以是“用于鉴别外部网络上人员的鉴别机制”。

G.4.6 FIA_UAU.5 多重鉴别机制

G.4.6.1 用户应用注释

本组件提出在 TOE 内使用一个以上鉴别机制的要求。对每个不同的机制，必须从 FIA“标识和鉴别”类中选择合适的要求以应用于该机制。为了反映鉴别机制的不同用途需要满足不同的要求，同一组件可能被多次选中。

FMT 类中的管理功能可以为这组鉴别机制提供维护能力，也为确定鉴别是否成功的规则提供维护能力。

为了让匿名用户使用 TOE，“无”鉴别机制这样的赋值也是可接受的，此类访问的使用应在 FIA_UAU.5.2 的规则中清晰地加以解释。

G.4.6.2 操作

G.4.6.2.1 赋值

在 FIA_UAU.5.1 中，PP/ST 作者应定义可利用的鉴别机制。例如，此类列表可以是：“无、口令机制、生物测定(视网膜扫描)、S/Key 机制”。

在 FIA_UAU.5.2 中，PP/ST 作者应规定描述鉴别机制如何提供鉴别以及每一机制将在何时使用的规则。这意味着，对每一种情况必须描述可用于鉴别用户的那组机制。例如，“如果用户有特殊权限，口令机制和生物测定机制两者都将使用，只有两者都鉴别成功后，这个鉴别才成功；对所有其他用户将使用口令机制。”。

PP/ST 作者可以给出一个范围，在这个范围内，授权管理员可以规定具体规则。规则的例子如：“应总是使用令牌(token)的方式对用户来进行鉴别；管理员也可规定必须使用的附加鉴别机制”。PP/ST 作者也可以选择不指定任何范围，把鉴别机制和它们的规则全部留给授权管理员。

G.4.7 FIA_UAU.6 重鉴别

G.4.7.1 用户应用注释

本组件负责处理在既定的时刻对用户重新鉴别的潜在需求。可能包括用户要求 TSF 执行安全相关的动作，以及非 TSF 实体要求重新鉴别(例如，服务器应用程序要求 TSF 对客户端进行重鉴别)。

G.4.7.2 操作

G.4.7.2.1 赋值

在 FIA_UAU.6.1 中，PP/ST 作者应规定需要重鉴别的条件列表。该列表可包括：所指定的用户不活动期已过，用户要求改变正在活动的安全属性，或用户请求 TSF 执行某关键的安全功能。

PP/ST 作者可以给出重鉴别发生的边界条件，而把详细规则留给授权管理员。这样一条规则的实例如：“用户在一天之内至少被重鉴别一次；管理员可以指定经常进行重鉴别，但不能比每 10 分钟一次更频繁”。

G.4.8 FIA_UAU.7 受保护的鉴别反馈

G.4.8.1 用户应用注释

本组件负责处理在鉴别过程中提供给用户的反馈。在一些系统中，反馈显示出了用户所输入的字符数，但不显示字符本身；在另一些系统中，甚至这些信息可能也是不合适的。

本组件要求不能把鉴别数据原样返回给用户。在工作站环境中,对每一个输入的口令字符不显示原始字符,可以如星号等字符代替。

G.4.8.2 操作

G.4.8.2.1 赋值

在 FIA_UAU.7.1 中,PP/ST 作者应规定提供给用户的与鉴别过程相关的反馈。例如,可指定反馈为:"所输入字符数",另一种类型的反馈是"鉴别失败的鉴别机制"。

G.5 用户标识(FIA_UID)

G.5.1 用户注释

本族定义用户在执行任何其他由 TSF 促成的并需要用户标识的动作之前,要求用户识别他自己的条件。

G.5.2 FIA_UID.1 标识的时机

G.5.2.1 用户应用注释

本组件对被识别的用户提出要求。PP/ST 作者可以指出在标识发生前可执行的具体动作。

如果使用了 FIA_UID.1"标识的时机",在 FIA_UID.1 中提到的 TSF 促成的动作也应在 FIA_UAU.1"鉴别的时机"中出现。

G.5.2.2 操作

G.5.2.2.1 赋值

在 FIA_UID.1.1 中,PP/ST 作者应规定在用户必须识别他自己之前,TSF 代表用户可执行的 TSF 促成动作列表。如果没有合适的动作,应使用组件 FIA_UID.2"任何动作前的用户标识"来替代。此动作的实例可能有:在登录过程中请求帮助。

G.5.3 FIA_UID.2 在任何动作之前的用户标识

G.5.3.1 用户应用注释

在本组件中用户将被识别。在用户被识别之前,TSF 不允许用户执行任何动作。

G.6 用户－主体绑定(FIA_USB)

G.6.1 用户注释

一个已鉴别了的用户,为了使用 TOE,一般要先激活一个主体。用户的安全属性(全部或部分地)与这个主体相关联。本族定义建立和维护用户安全属性与代表用户活动的主体间关联的要求。

G.6.2 FIA_USB.1 用户－主体绑定

G.6.2.1 用户应用注释

主体代表的是导致主体产生或被激活以执行某个任务的用户。

因此,当一个主体被创建时,该主体就代表了发起该创建的用户。在使用匿名的情况下,主体仍代

表着用户,但用户的身份是未知的。一类特殊的主体是它们服务于多个用户(例如,一个服务器进程),在这种情况下,创建这个主体的用户就被假定为这个主体的“所有者”。

G.6.2.2 操作

G.6.2.2.1 赋值

在 FIA_USB.1.1 中,PP/ST 作者应规定与主体绑定的用户属性列表。

在 FIA_USB.1.2 中,PP/ST 作者应规定任何适用于属性与主体初始关联的规则,或“无”。

在 FIA_USB.1.3 中,PP/ST 作者应规定任何适用于改变与代表用户活动的主体相关联的用户安全属性的规则,或“无”。

附 录 H
（规范性附录）
FMT 类:安全管理

本类规定 TSF 几个方面的管理:安全属性、TSF 数据和 TSF 中的功能。不同的管理角色和它们之间的相互作用(如能力的分离)也可在本类中规定。

在 TOE 由多个物理上分离的部件组成的环境中,与安全属性传播、TSF 数据和功能修改的时机问题变得非常复杂,尤其是当这些信息需要在 TOE 的各部分间复制时更是如此。当选取诸如 FMT_REV.1“撤消”或 FMT_SAE.1“时限授权”这样的组件时,由于行为有可能被削弱,更需要考虑上面的问题。在这种情况下,建议使用 FPT_TRC“TOE 内 TSF 数据复制的一致性”中的组件。

本类的组件构成分解如图 H.1 所示。

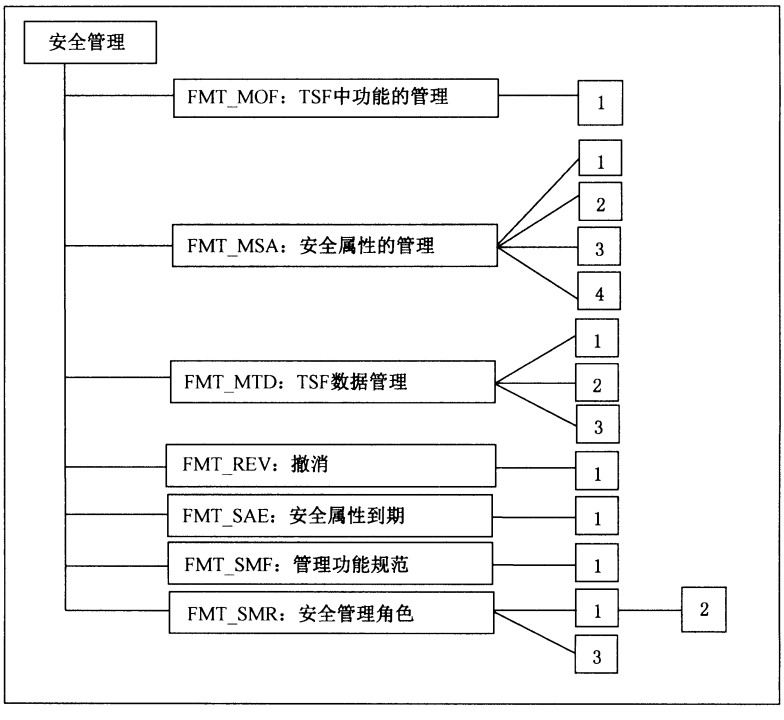

图 H.1 安全管理类分解

H.1 TSF 中功能的管理(FMT_MOF)

H.1.1 用户注释

TSF 管理功能使授权用户能够建立和控制 TOE 的安全操作。这些管理功能通常分为以下几种不同的类别:

a) 涉及 TOE 执行的访问控制、责任可追查性和鉴别控制的管理功能。例如,用户安全特征(如与用户名、用户账号、系统入口参数相关的唯一标识符)的定义和更新;审计性系统控制(如审计事件的选取、审计迹的管理、审计迹的分析和审计报告的生成)的定义与更新;每个用户策略属性(如用户许可)的定义和更新;已知系统访问控制标签的定义,用户组的控制与管理。

b) 涉及可用性控制的管理功能。例如,可用性参数或资源配额的定义和更新。

c) 涉及普通安装和配置的管理功能。例如,TOE 的配置、手工恢复、TOE 安全补丁的安装(如果有的话)、硬件的修复和重装。

d) 涉及 TOE 资源常规控制和维护的管理功能。例如,激活或终止外围设备、移动存储设备的加载、备份与恢复。

注意,这些功能需根据 PP 或 ST 中包含的族,呈现在一个 TOE 中。PP/ST 作者有责任确保提供了足够的功能,以便以安全的方式管理系统。

TSF 可能包含一些能够被管理员控制的功能。例如,关闭审计功能,切换时间同步方式,更改鉴别机制。

H.1.2 FMT_MOF.1 安全功能行为的管理

H.1.2.1 用户应用注释

本组件允许已标识的角色管理 TSF 的安全功能。这可能需要获取安全功能的当前状态、终止或激活安全功能、修改安全功能的行为。例如,改变鉴别机制就是一个修改安全功能行为的例子。

H.1.2.2 操作

H.1.2.2.1 选择

在 FMT_MOF.1.1 中,PP/ST 作者应该选择角色是否能确定终止、激活和/或修改安全功能的行为。

H.1.2.2.2 赋值

在 FMT_MOF.1.1 中,PP/ST 作者应规定能够被已标识的角色修改的功能,例如审计和确定时间等。

在 FMT_MOF.1.1 中,PP/ST 作者应规定允许修改 TSF 中功能的角色。可能的角色在 FMT_SMR.1"安全角色"中规定。

H.2 安全属性的管理(FMT_MSA)

H.2.1 用户注释

本族定义关于安全属性管理的一些要求。

安全属性可影响 TSF 的行为。此类安全属性的例子如:用户所属的组、用户可能承担的角色、进程(主体)的优先级以及属于一个角色或用户的权限。这些安全属性可能需要由用户、主体或特定的授权用户(即对于此管理具有明确给定权限的用户)来管理,或通过指定的策略或规则集来继承值。

必须注意,给用户分配权限的权限本身就是一个安全属性,或者潜在地受 FMT _MSA.1"安全属性的管理"的管理。

FMT_MSA.2 "安全的安全属性"可用来确保任何可以接受的安全属性组合都处于一个安全状态。"安全的"定义留待 TOE 指南中给出。

在某些情况下,主体、客体或用户账号都已建立,如果没有对相关的安全属性给出明确的值,那么就需使用默认值,FMT_MSA.1"安全属性的管理"可以用来规定这些默认值是可管理的。

H.2.2 FMT_MSA.1 安全属性的管理

H.2.2.1 用户应用注释

本组件允许担当特定角色的用户管理指定的安全属性。在组件 FMT_SMR.1"安全角色"内,这些

用户都被赋予一个角色。

参数的默认值是指在参数实例化没有专门指定某个值时，该参数所取的值。初始值是指在参数实例化(创建)过程中提供的值，将取代默认值。

H.2.2.2 操作

H.2.2.2.1 赋值

在 FMT_MSA.1.1 中，PP/ST 作者应列出安全属性所适用的访问控制 SFP 或信息流控制 SFP。

H.2.2.2.2 选择

在 FMT_MSA.1.1 中，PP/ST 作者应规定可应用于指定的安全属性的操作。PP/ST 作者可规定：某角色可以修改安全属性的默认值(改变默认值)、查询安全属性、修改安全属性、删除整个安全属性或定义他们自己的操作。

H.2.2.2.3 赋值

在 FMT_MSA.1.1 中，PP/ST 作者应规定那些能够由已标识角色操作的安全属性。PP/ST 作者可规定默认值，如可被管理的默认访问权限。这些安全属性的例子有：用户许可、服务优先级、访问控制列表、默认访问权限。

在 FMT_MSA.1.1 中，PP/ST 作者应规定允许对安全属性进行操作的角色。可能的角色在 FMT_SMR.1“安全角色”中规定。

在 FMT_MSA.1.1 中，如果选择了“其他操作”，PP/ST 作者应规定该角色能够执行哪些其他操作。“创建”便可能是这种操作的一个例子。

H.2.3 FMT_MSA.2 安全的安全属性

H.2.3.1 用户应用注释

本组件包含对安全属性能被赋予的值的一些要求。所赋值应使得 TOE 保持一种安全状态。

“安全”含义的定义在本组件中没有给出，而留给了 TOE 的开发和指南给出的信息。例如：如果建立了一个用户账号，则应拥有一个复杂口令。

H.2.3.2 操作

H.2.3.2.1 赋值

在 FMT_MSA.2.1 中，PP/ST 作者应列出仅需要提供安全值的安全属性列表。

H.2.4 FMT_MSA.3 静态属性初始化

H.2.4.1 用户应用注释

本组件要求 TSF 为相关客体的安全属性提供默认值，该默认值能够被初始值所取代。如果存在一种机制在创建时规定许可权，一个新客体在创建时仍可能有不同的安全属性。

H.2.4.2 操作

H.2.4.2.1 赋值

在 FMT_MSA.3.1 中，PP/ST 作者应列出安全属性所适用的访问控制 SFP 或信息流控制 SFP。

H.2.4.2.2 选择

在 FMT_MSA.3.1 中，PP/ST 作者应选择访问控制属性的默认特性是受限的，是许可的，还是其他特性。这些选项只能选择一个。

H.2.4.2.3 赋值

在 FMT_MSA.3.1 中，如果 PP/ST 作者选择了“其他特性”，PP/ST 作者应规定默认值的预期特征。

在 FMT_MSA.3.2 中，PP/ST 作者应规定允许修改安全属性值的角色。这些可能的角色在 FMT_SMR.1“安全角色”中规定。

H.2.5 FMT_MSA.4 安全属性值继承

H.2.5.1 用户应用注释

本组件要求 TSF 描述一套安全功能属性继承值的规则，和这些规则被应用时需符合的条件。

H.2.5.2 操作

H.2.5.2.1 赋值

在 FMT_MSA.4.1 中，PP/ST 作者应列出管理被指定安全属性继承的值的规则，包括规则应用需符合的条件。例如，如果一个新文件或目录被建立（在多级文件系统），它的标签是用户登录时建立的标签。

H.3 TSF 数据的管理（FMT_MTD）

H.3.1 用户注释

本组件对 TSF 数据管理提出要求。TSF 数据的例子有：当前时间、审计迹等。因此，本族允许规定谁能读、删除或创建审计迹。

H.3.2 FMT_MTD.1 TSF 数据的管理

H.3.2.1 用户应用注释

本组件允许具有某个角色的用户管理 TSF 数据的值。在组件 FMT_SMR.1“安全角色”中为用户分配了角色。

参数的默认值是指在参数实例化过程中没有专门指定某个值时，该参数所取的值。初始值是指在参数实例化（创建）过程中提供的值，将取代默认值。

H.3.2.2 操作

H.3.2.2.1 选择

在 FMT_MTD.1.1 中，PP/ST 作者应规定可用于指定 TSF 数据的操作。PP/ST 作者规定修改 TSF 数据的默认值（改变默认值）、清除 TSF 数据、查询 TSF 数据、修改 TSF 数据或完全删除 TSF 数据的角色。如此，PP/ST 作者可以规定任何类型的操作。需要澄清的是“清除 TSF 数据”意味着 TSF 数据的内容被移除，但是存储 TSF 数据的实体还保留在 TOE 内。

H.3.2.2.2 赋值

在 FMT_MTD.1.1 中，PP/ST 作者应规定能够被已标识角色操作的 TSF 数据。PP/ST 作者可能规定可被管理的默认值。

在 FMT_MTD.1.1 中，PP/ST 作者应规定允许对 TSF 数据进行操作的角色。可能的角色在 FMT_SMR.1“安全角色”中规定。

在 FMT_MTD.1.1 中，如果选择了“其他操作”，PP/ST 作者应规定角色能够执行哪些其他操作。“创建”就是这种操作的一个例子。

H.3.3 FMT_MTD.2 TSF 数据限值的管理

H.3.3.1 用户应用注释

本组件规定关于 TSF 数据的限制，以及当超过这些限制时将要采取的动作。例如，本组件将允许定义对审计记录大小的限值，以及规定超过这些限值时将要采取动作。

H.3.3.2 操作

H.3.3.2.1 赋值

在 FMT_MTD.2.1 中，PP/ST 作者应规定可能有限值的 TSF 数据及其限值。这种 TSF 数据的一个例子是：登录用户数。

在 FMT_MTD.2.1 中，PP/ST 作者应规定允许修改 TSF 数据限值的角色以及将采取的动作。可能的角色在 FMT_SMR.1“安全角色”中规定。

在 FMT_MTD.2.2 中，PP/ST 作者应规定如果超过对指定 TSF 数据的指定限值，所要采取的动作。此类 TSF 动作的一个例子是：通知授权用户且生成审计记录。

H.3.4 FMT_MTD.3 安全的 TSF 数据

H.3.4.1 用户应用注释

本组件包含了一些关于 TSF 数据能赋予的值的要求。所赋值应使得 TOE 保持在一个安全状态。“安全”含义的定义在本组件中没有给出，而留给了 TOE 的开发者和指南给出的信息。

H.3.4.2 操作

H.3.4.2.1 赋值

在 FMT_MTD.3.1 中，PP/ST 作者应规定哪些 TSF 数据只接受安全的值。

H.4 撤消(FMT_REV)

H.4.1 用户注释

本族负责处理一个 TOE 内各种实体安全属性的撤消。

H.4.2 FMT_REV.1 撤消

H.4.2.1 用户应用注释

本组件规定关于权限撤消的要求。它需要规定撤消规则，例如：

a) 撤消将发生在用户下次登录时；
b) 撤消将发生在下次试图打开该文件时；
c) 撤消将发生在某一固定时间段内。这可能意味着所有打开的连接每隔 X 分钟后就要重新评价。

H.4.2.2 操作

H.4.2.2.1 赋值

在 FMT_REV.1.1 中，PP/ST 作者应规定当相关的客体、主体、用户和其他资源发生改变时，哪些安全属性应被撤销。

H.4.2.2.2 选择

在 FMT_REV.1.1 中，PP/ST 作者应规定 TSF 是否应提供撤消来自用户、主体、客体或任何额外资源的安全属性的能力。

H.4.2.2.3 赋值

在 FMT_REV.1.1 中，PP/ST 作者应规定允许修改 TSF 中功能的角色。这些可能的角色在 FMT_SMR.1“安全角色”中规定。

在 FMT_REV.1.1 中，如果选择了“其他额外资源”，PP/ST 作者应规定 TSF 是否应提供撤销这些资源的安全属性的能力。

在 FMT_REV.1.2 中，PP/ST 作者应规定撤消规则。例如，撤消发生在“对相关资源的下一次操作之前”或“所有新主体创建时”。

H.5 安全属性到期(FMT_SAE)

H.5.1 用户注释

本族提出对安全属性的有效性实施时间限制的能力。本族可用来为访问控制属性、标识和鉴别属性、证书(密钥证书，如 ANSI X.509)和审计属性等规定到期要求。

H.5.2 FMT_SAE.1 时限授权

H.5.2.1 操作

H.5.2.1.1 赋值

在 FMT_SAE.1.1 中，PP/ST 作者应提供支持有效期的安全属性列表。此类属性的一个例子是：用户的安全许可。

在 FMT_SAE.1.1 中，PP/ST 作者应规定允许修改 TSF 中安全属性的角色。可能的角色在 FMT_SMR.1“安全角色”中规定。

在 FMT_SAE.1.2 中，PP/ST 作者应对每一个安全属性提供一个到期时将采取的动作列表。例如：用户的安全许可，当它到期时，将被设置为 TOE 上允许的最低级别的许可。如果 PP/ST 希望立即撤消，则应指定为“立即撤消”这一动作。

H.6 管理功能规范(FMT_SMF)

H.6.1 用户注释

本族允许管理功能的规范由 TOE 提供。每个被列出以完成赋值的安全管理功能不是安全属性管理,就是 TSF 数据管理或安全功能管理。

H.6.2 FMT_SMF.1 管理功能规范

H.6.2.1 用户应用注释

本组件规定 TSF 提供的管理功能。

PP/ST 作者应参考其 PP/ST 中“管理”条中的组件,该章节为本组件列出管理功能提供了一个基础。

H.6.2.2 操作

H.6.2.2.1 赋值

在 FMT_SMF.1.1 中,PP/ST 作者应规定 TSF 提供的管理功能,不是安全属性管理,就是 TSF 数据管理或安全功能管理。

H.7 安全管理角色(FMT_SMR)

H.7.1 用户注释

本族用于减少因用户采取超越已赋予的功能职责范围的动作,滥用其授权而遭受损失的可能性,也负责处理当采用不适当的机制对 TSF 进行安全管理时产生的威胁。

本族要求维护信息,以识别一个用户是否有权使用一个特定的安全相关管理功能。

某些管理动作可由用户完成,另外一些仅能由组织内的指定人员完成。本族允许定义不同的角色,如拥有者、审计员、管理员、日常管理者。

本族中所用的角色都是与安全有关的角色。每个角色可拥有一组广泛的能力(如 Unix 中的 root),也可以只拥有一个单一的权限(如读取像帮助文件这样的单个客体的权限)。本族定义这些角色,而角色的能力则在 FMT_MOF“TSF 中功能的管理”、FMT_MSA“安全属性的管理”和 FMT_MTD “TSF 数据的管理”中定义。

某些类型的角色可能是互斥的。例如日常管理者可能能够定义和激活用户,但可能不能删除用户[这留给管理员(角色)]。本族允许规定两人控制这样的策略。

H.7.2 FMT_SMR.1 安全角色

H.7.2.1 用户应用注释

本组件规定 TSF 应认可的不同角色。通常系统区分实体的拥有者、管理员和其他用户。

H.7.2.2 操作

H.7.2.2.1 赋值

在 FMT_SMR.1.1 中,PP/ST 作者应规定系统所认同的角色,这些角色都是用户可以拥有的,与安

全有关的角色。例如:拥有者、审计员和管理员。

H.7.3 FMT_SMR.2 安全角色限制

H.7.3.1 用户应用注释

本组件规定 TSF 应该认同的不同角色,以及如何管理这些角色的条件。通常系统区分实体的拥有者、管理员和其他用户。

这些角色的条件规定了不同角色之间的相互关系,以及限制用户何时能承担这些角色。

H.7.3.2 操作

H.7.3.2.1 赋值

在 FMT_SMR.2.1 中,PP/ST 作者应规定系统所认同的角色。这些角色都是用户可以拥有的,与安全有关的角色。例如:拥有者、审计员、管理员。

在 FMT_SMR.2.3 中,PP/ST 作者应规定管理角色分配的条件。这些条件的例子有:“一个账号不能同时具有审计员和管理员两种角色”或“具有助理角色的用户也必须具有拥有者角色。”

H.7.4 FMT_SMR.3 承担角色

H.7.4.1 用户应用注释

本组件规定必须给出明确的请求以承担特定的角色。

H.7.4.2 操作

H.7.4.2.1 赋值

在 FMT_SMR.3.1 中,PP/ST 作者应规定需要作出明确请求才能承担的角色。例如:审计员和管理员。

附 录 I
（规范性附录）
FPR 类：隐私

本类描述了这样的要求，它能被用来满足用户的隐私需求，同时允许系统具有尽可能强的灵活性，以保持对系统操作的充分控制。

在本类的组件中，所要求的安全功能是否覆盖授权用户是具有灵活性的。例如，PP/ST 作者可认为，不要求针对适当的授权用户保护用户的隐私是合理的。

本类同其他的类（如有关审计、访问控制、可信路径和抗抵赖等的类）一起，提供了灵活性以规定期望的隐私行为。另一方面，本类中的要求可能会影响其他类（如 FIA“标识和鉴别”或 FAU“安全审计”）中组件的使用限制。例如，如果不允许授权用户看到用户的身份（如，匿名或假名），则显然由于隐私的要求，使得不可能让单个用户对他们所执行的任何安全相关行为负责。然而，仍然有可能在 PP/ST 中包括审计要求，因为发生特定安全相关事件的这个事实比知道谁对它负责更加重要。

在 FAU“安全审计”类的应用注释中，提供了附加的信息，其中解释了关于审计的“身份”定义，也可能是一个别名或其他能标识用户身份的信息。

本类描述了 4 个族：匿名、假名、不可关联性、不可观察性。匿名、假名和不可关联性有复杂的相互关系。对族的选择应依赖所标识的威胁。对某些类型的隐私威胁，假名会比匿名更合适（如有审计要求时）。此外，某些类型的隐私威胁，要通过几个族的组件组合，才可以很好地予以抵抗。

所有的族都假定用户不会明显地执行暴露用户自己身份的动作。例如，TSF 不应在电子消息或数据库中筛查用户名。

本类中的所有族都有通过指定操作来确定私密保护范围的组件。在这些操作中，PP/ST 作者可以指明 TSF 应防止哪些协作用户/主体察觉私密信息。一个具体的匿名实例如：“TSF 应确保不能通过用户或主体来确定与电话咨询应用绑定的用户身份。”

要注意 TSF 不仅应该防止单个用户获取信息，而且应防止用户协作获取信息。

本类的组件构成分解如图 I.1 所示。

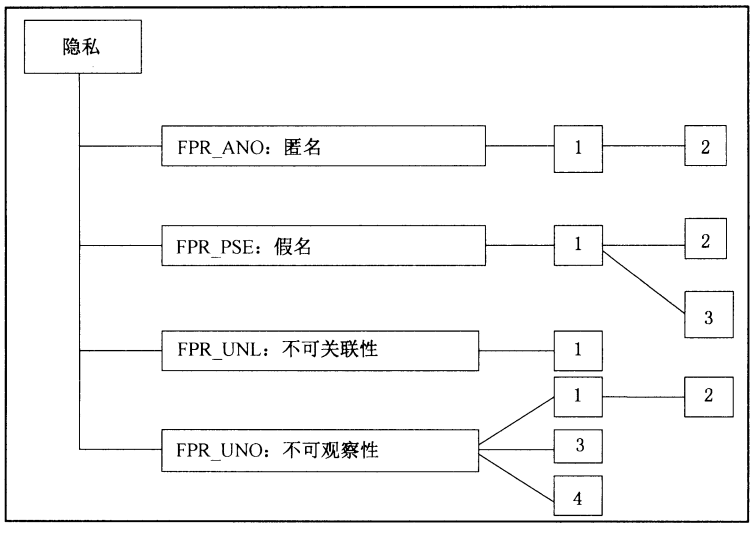

图 I.1 隐私类分解

I.1 匿名(FPR_ANO)

I.1.1 用户注释

匿名确保主体可使用资源和服务而不暴露它的用户身份。

本族的意图是规定一个用户或主体可以采取动作而不把用户的身份暴露给其他的用户、主体或客体。本族为 PP/ST 作者提供了一个方法去标识一组用户,这些用户不能看到那些执行某些动作的用户的身份。

因此,如果使用匿名的主体执行一个动作,另一个主体将不能确定其身份,甚至不能确定利用主体的用户身份的引用名。匿名的焦点是保护用户的身份,而不是保护主体的身份,所以主体的身份不受防止泄露的保护。

虽然主体的身份没有发布给其他主体和用户,但并不明确禁止 TSF 获得用户的身份。如果不允许 TSF 知道用户的身份,可以调用 FPR_ANO.2"无索求信息的匿名"。此时,TSF 不应要求用户的信息。

对"确定"一词的解释应在最广的字面意义上来理解。

本组件分级区分了用户和授权用户。授权用户经常被排除在本组件之外,因此允许找回一个用户的身份。然而,并没有特别要求一个授权用户必须有能力确定用户的身份。在极端的隐私情况下,本组件将意味着没有用户或授权用户能看到执行任何动作的任何人的身份。

虽然一些系统将为所提供的所有服务提供匿名,仍然存在其他的一些系统只为某些确定的主体/操作提供匿名。为了提供这一灵活性,一个操作应包括在已定义的要求范围内。如果 PP/ST 作者想处理所有的主体/操作,则应规定为"所有的主体和所有的操作"。

可能的应用包括查询公用数据库的机密性质、响应电子民意调查、匿名支付或捐赠。

潜在的敌意用户或主体包括把恶意部件(如特洛伊木马)偷偷引入系统中的那些提供者、系统操作员、通信伙伴和用户。所有这些用户能研究使用模式(如哪些用户使用哪些服务)并滥用这些信息。

I.1.2 FPR_ANO.1 匿名

I.1.2.1 用户应用注释

本组件保证用户的身份受到保护而不被泄露。然而,可能有这样的实例,即一个授权用户能确定谁执行某些动作。本组件提供了遵守有限还是全部隐私策略的灵活性。

I.1.2.2 操作

I.1.2.2.1 赋值

在 FPR_ANO.1.1 中,PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如,即使 PP/ST 作者只规定了单个用户或主体角色,但 TSF 不仅必须防范每一单个用户或主体,而且也必须防范用户或主体的协作。例如,用户集可以是一组用户,他们能在相同的角色下操作或都能用相同的进程。

在 FPR_ANO.1.1 中,PP/ST 作者应确定主体、操作或客体的一个列表,其中主体的真实用户名应受到保护。例如"投票表决应用"。

I.1.3 FPR_ANO.2 无索求信息的匿名

I.1.3.1 用户应用注释

本组件用来确保不允许 TSF 知道用户的身份。

I.1.3.2 操作

I.1.3.2.1 赋值

在 FPR_ANO.2.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范用户或主体的协作。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR_ANO.2.1 中，PP/ST 作者应标识主体、操作或客体的一个列表，其中主体的真实用户名应受到保护。例如“投票表决应用”。

在 FPR_ANO.2.2 中，PP/ST 作者应标识满足匿名要求的服务列表。例如，“工作描述的访问”。

在 FPR_ANO.2.2 中，PP/ST 应标识出主体的列表，当提供规定的服务时，这些主体的真实用户名应受到保护。

I.2 假名(FPR_PSE)

I.2.1 用户注释

假名确保一个用户能够使用资源或服务而不泄露自己的身份，但仍能对该使用负责。通过直接将用户与 TSF 持有的一个参照(别名)关联起来，或是通过提供用于处理目的的别名(如一个账号)，用户可以被追溯。

在许多方面，假名类似于匿名。假名和匿名都保护用户的身份，但在假名中，维护对用户身份的一个参照，是为追查相关责任或其他目的。

组件 FPR_PSE.1“假名”没规定引用用户身份的要求。为了规定关于这种引用的要求，提供了两组要求：FPR_PSE.2“可逆假名”和 FPR_PSE.3“别名假名”。

一种是以满足可获得原始用户身份能力的方式来使用参照。例如，在一个电子现金环境中，当一张支票已经被多次签发时(即欺骗)，若能追踪用户的身份将更有意义。一般来说，用户身份须在特定的条件下才被检索。PP/ST 作者可能要结合 FPR_PSE.2“可逆假名”来描述这些服务。

另一种是以用户别名的形式来使用参照。例如，一个用户不希望被标识，可向他提供一个账户，使用资源就向该账户收费。在这种情形下，用户身份的参照是该用户的一个别名，其他用户或主体无需获得该用户的身份就可以利用此别名执行它们的功能(例如，对其使用系统的次数进行统计操作)。在此情形下，PP/ST 作者可能希望结合 FPR_PSE.3“别名假名”来规定参照须遵守的规则。

通过使用上面的这些结构，用 FPR_PSE.2“可逆假名”可建立电子货币，它规定用户身份将得到保护，而且如果在条件中就是这么规定的话，则当电子货币被使用两次时，就有一个追踪用户身份的要求。若用户是诚实的，用户身份受到保护；当用户试图欺骗时，用户身份能被追踪。

一种不同的系统可能是电子信用卡，其中用户提供一个假名，指示一个可从中提取现金的账户。在这种情形下，可以使用 FPR_PSE.3“别名假名”。该组件将规定用户身份将得到保护，此外同一个用户仅能获得与他/她已提供钱款相符的数目(如果在条件中已这样规定的话)。

应当认识到，更严格的组件可能不能同其他要求组合使用，诸如标识和鉴别、审计。“确定身份”的解释应在更广的字面意义上理解。在操作过程中，TSF 不提供这些信息，实体也不能确定调用操作的主体或主体的拥有者，TSF 也不会记录用户或主体可用的、在将来会暴露用户身份的一些信息。

目的是 TSF 不揭示任何有损用户身份的信息，如代表用户活动的主体的身份。信息被认为是敏感的，依赖于攻击者所付出的努力。

可能的应用包括：向声讯服务拨打者的收费而不揭示其身份，或对电子支付系统的匿名使用收费。

潜在的敌意用户或主体包括把恶意部件(如特洛伊木马)偷偷引入系统中的那些提供者、系统操作员、通信伙伴和用户。所有这些攻击者会研究哪些用户使用哪些服务,并滥用这些信息。作为对匿名服务的补充,假名服务包含了不需标识的授权方法,特别是对匿名支付("电子现金")。这将帮助提供者以安全的方式获得他们的费用,同时还维持了顾客的匿名。

I.2.2 FPR_PSE.1 假名

I.2.2.1 用户应用注释

本组件提供用户保护,防止将其身份泄露给其他用户。但用户仍能对其行为负责。

I.2.2.2 操作

I.2.2.2.1 赋值

在 FPR_PSE.1.1 中,PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如,即使 PP/ST 作者只规定了单个用户或主体角色,但 TSF 不仅必须防范单个用户或主体,而且也必须防范用户或主体的协作。例如,用户集可以是一组用户,他们能在相同的角色下操作或都能用相同的进程。

在 FPR_PSE.1.1 中,PP/ST 作者应确定主体、操作或客体的一个列表,其中主体的真实用户名应受到保护。例如"对招聘信息的访问"。注意,"客体"包括能使其他用户或主体导出真实用户身份的任何其他属性。

在 FPR_PSE.1.2 中,PP/ST 作者应确定 TSF 能提供的别名的数目(一个或多个)。

在 FPR_PSE.1.2 中,PP/ST 作者应确定 TSF 能向其提供别名的主体列表。

I.2.2.2.2 选择

在 FPR_PSE.1.3 中,PP/ST 作者应规定用户别名是由 TSF 生成,还是由用户提供。这些选项中只能选择其一。

I.2.2.2.3 赋值

在 FPR_PSE.1.3 中,PP/ST 作者应确定 TSF 生成的或用户生成的别名应遵守的度量方式。

I.2.3 FPR_PSE.2 可逆假名

I.2.3.1 用户应用注释

在本组件中,TSF 应确保在特定的条件下,可以确定与所提供引用相关的用户身份。

在 FPR_PSE.1"假名"中,TSF 应提供别名代替用户身份。当满足规定的条件时,别名所属的用户身份是可以确定的。例如,在电子现金环境下,这样条件的一个例子如下:"仅在支票已经签发两次的条件下,TSF 应向公证人提供通过别名确定用户身份的能力。"

I.2.3.2 操作

I.2.3.2.1 赋值

在 FPR_PSE.2.1 中,PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如,即使 PP/ST 作者只规定了单个用户或主体角色,但 TSF 不仅必须防范单个用户或主体,而且也必须防范用户或主体的协作。例如,用户集可以是一组用户,他们能在相同的角色下操作或都能使用相同的进程。

在 FPR_PSE.2.1 中,PP/ST 作者应确定主体、操作或客体的一个列表,其中主体的真实用户名应受到保护。例如"工作提供者的访问"。注意,"客体"包括能使其他用户或主体导出真实的用户身份的

任何其他属性。

在 FPR_PSE.2.2 中，PP/ST 作者应确定 TSF 能提供的别名的数目(一个或多个)。

在 FPR_PSE.2.2 中，PP/ST 作者应确定 TSF 能向其提供别名的主体列表。

I.2.3.2.2 选择

在 FPR_PSE.2.3 中，PP/ST 作者应规定用户别名是由 TSF 生成，还是由用户提供。这些选项中只能选择其一。

I.2.3.2.3 赋值

在 FPR_PSE.2.3 中，PP/ST 作者应确定 TSF 生成的或用户生成的别名应遵守的度量方式。

I.2.3.2.4 选择

在 FPR_PSE.2.4 中，PP/ST 作者应选择是授权用户，还是可信主体或者二者都可确定真实的用户名。

I.2.3.2.5 赋值

在 FPR_PSE.2.4 中，PP/ST 作者应确定条件列表，在这些条件下可信主体和授权用户能基于所提供的参照确定真实的用户名。这些条件可以是一天中的某个时段，或是就像法院指令一样可被管理。

在 FPR_PSE.2.4 中，PP/ST 作者应确定在规定条件下能获取真实用户名的可信主体列表。例如，公证人或特定的授权用户。

I.2.4 FPR_PSE.3 别名假名

I.2.4.1 用户应用注释

在本组件中，TSF 应确保所提供的引证满足特定的构造规则，因此可被潜在的不安全主体以安全的方式使用。

如果一个用户想使用磁盘资源但不泄露自己的身份，此时可使用假名。然而，每次用户访问这个系统时，必须使用相同的别名。这样的条件可在本组件中规定。

I.2.4.2 操作

I.2.4.2.1 赋值

在 FPR_PSE.3.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体角色，但 TSF 不仅必须防范单个用户或主体，而且也必须防范用户或主体的协作。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR_PSE.3.1 中，PP/ST 作者应确定主体、操作或客体的一个列表，其中主体的真实用户名应受到保护。例如“对招聘信息的访问”。注意，“客体”包括能使其他用户或主体导出真实的用户身份的任何其他属性。

在 FPR_PSE.3.2 中，PP/ST 作者应确定 TSF 能提供的别名的数目(一个或多个)。

在 FPR_PSE.3.2 中，PP/ST 作者应确定 TSF 能向其提供别名的主体列表。

I.2.4.2.2 选择

在 FPR_PSE.3.3 中，PP/ST 作者应规定用户别名是由 TSF 生成，还是由用户提供。这些选项中只能选择其一。

I.2.4.2.3 赋值

在 FPR_PSE.3.3 中，PP/ST 作者应确定 TSF 生成的或用户生成的别名应遵守的度量方式。

在 FPR_PSE.3.4 中，PP/ST 作者应确定条件列表，这些条件指出对真实用户名所使用的参照何时是相同的，何时是不同的。例如，“当用户登录到相同的主机上”时，将使用唯一的别名。

I.3 不可关联性(FPR_UNL)

I.3.1 用户注释

不可关联性确保一个用户可以多次使用资源和服务，而其他人不能将这些使用关联在一起。不可关联性与假名的不同在于，虽然在假名中用户也是未知的，但可提供不同动作之间的关系。

不可关联性要求试图保护用户身份，以防止对用户操作进行跟踪分析。例如，当一个电话智能卡绑定了一个唯一号码时，电话公司可确定该电话卡用户的行为。如果知道了用户的电话使用情况，就能将此卡与一个特定的用户相关联。隐藏一个服务的不同调用之间的关系，或隐藏一个资源的不同访问之间的关系，将防止对这类信息的收集。

由此，对不可关联性的一个要求可能隐含如下要求：必须保护操作的主体及其用户身份。否则，该信息可用来将不同操作关联起来。

不可关联性要求不同的操作是不能被关联的。这种关联关系有几种形式。例如，用户与操作相关，或与发起动作的终端相关，或与该动作执行的时间相关。PP/ST 作者可以规定必须阻止的关系种类。

可能的应用包括：多次使用假名，而不会建立可能泄露用户身份的使用模式。

潜在的敌意用户或主体包括把恶意部件(如特洛伊木马)偷偷引入系统中的那些提供者、系统操作员、通信伙伴和用户，他们不做操作而只想获取有关信息。所有这些攻击者都能研究哪些用户使用哪些服务并滥用这些信息。不可关联性保护用户，以防其被关联，这种关联可以从一个客户的几次动作中得出。一个例子是，匿名客户打给不同合伙人的一系列电话，这些合伙人身份的组合可以揭示该客户的身份。

I.3.2 FPR_UNL.1 不可关联性

I.3.2.1 用户应用注释

本组件确保用户不能关联系统中不同的操作并以此获取信息。

I.3.2.2 操作

I.3.2.2.1 赋值

在 FPR_UNL.1.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体角色，但 TSF 不仅必须防范单个用户或主体，而且也必须防范用户或主体的协作。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR_UNL.1.1 中，PP/ST 作者应确定应满足不可关联性要求的操作(例如，“发送电子邮件”)列表。

I.3.2.2.2 选择

在 FPR_UNL.1.1 中，PP/ST 应选取应被掩盖的关系。该选择允许规定用户身份或者对关系进行赋值。

I.3.2.2.3 赋值

在 FPR_UNL.1.1 中，PP/ST 作者应确定受到保护的关系列表。例如，“源自相同的终端”。

I.4 不可观察性(FPR_UNO)

I.4.1 用户注释

不可观察性确保一个用户可以使用一个资源或服务，而其他人，特别是第三方，不能观察到该资源或服务正被使用。

与先前的“匿名”、“假名”和“不可关联性”族不同，不可观察性从另一不同的方向处理用户的身份。在此情形下，目的是隐藏资源和服务的使用，而不是隐藏用户的身份。

一些技术可用来实现不可观察性。提供不可观察性的技术例子有：

a) 影响不可观察性的信息分配：不可观察性相关的信息(如描述一个操作发生的信息)可分配在 TOE 内的几个地方。一种方法是信息可被分配到 TOE 的一个随机选择的、单独的部分，这样攻击者不知道应攻击 TOE 的哪个部分。另一种方法是将信息分散在 TOE 的不同部分中，使得没有哪一个单独的 TOE 部分有足够的信息，从而避免用户的隐私遭到破坏。这一技术在 FPR_UNO.2“影响不可观察性的信息的分配”中明确提出。

b) 广播：在广播信息时(如以太网、无线电)，用户不能确定谁真正接收和使用了这些信息。当信息应送达对此信息(如敏感的医学信息)感兴趣但又害怕受到耻笑的接受者，这一技术特别有用。

c) 密码保护和消息填充：观察消息流的人可从消息被传送这一事实以及从该消息的属性中获得信息。通过通信量填充、消息填充以及加密消息流，可以保护消息的传送和它的属性。

有时，用户不应了解一个资源的使用情况，但是为了履行其职责，一个授权用户必须被许可知道资源的使用情况。在此情形，FRO_UNO.4“授权用户可观察性”可用来提供使一个或几个授权用户知道使用情况的能力。

本族使用了概念“TOE 的部分”，它可以是物理上或是逻辑上与 TOE 的其他部分分离的 TOE 的任何部分。

通信的不可观察性在许多领域中是重要的要素。例如固有权限的执行、组织策略或与防御相关的应用。

I.4.2 FPR_UNO.1 不可观察性

I.4.2.1 用户应用注释

本组件要求功能或资源的使用不能被未授权用户观察到。

I.4.2.2 操作

I.4.2.2.1 赋值

在 FPR_UNO.1.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体角色，但 TSF 不仅必须防范每一单个用户或主体，而且也必须防范用户或主体的协作。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR_UNO.1.1 中，PP/ST 作者应确定操作列表，这些操作遵从不可观察性要求。其他的用户/主体因而不能够观察到对指定列表中某个隐蔽客体的操作(如对该客体的读写)。

在 FPR_UNO.1.1 中，PP/ST 作者应确定被不可观察性要求覆盖的客体的列表。例如，特定的邮件服务器或 ftp 站点。

在 FPR_UNO.1.1 中，PP/ST 作者应规定一组受保护的用户或主体，他们的不可观察性信息是受保护的。这样的例子可以是："通过 Internet 访问该系统的用户。"

I.4.3 FPR_UN0.2 影响不可观察性的信息的分配

I.4.3.1 用户应用注释

本组件要求功能或资源的使用不能被规定的用户或主体观察到。进一步讲，本组件规定与用户隐私有关的信息在 TOE 内是分布式的，这样攻击者可能就不知道将 TOE 的哪一部分作为攻击目标，或是他们需要攻击 TOE 的多个部分。

使用此组件的一个例子是：使用一个随机分配的节点去提供某个功能。在这种情况下，本组件可要求与隐私相关的信息不仅只会被一个确定的 TOE 部分利用，而且不会传播到该 TOE 部分之外。

在某些"投票算法"中可以找到更复杂的例子。在该服务中将牵涉到 TOE 的几个部分，但没有一个 TOE 的独立部分能违反策略。所以一个人可以投票(或不投票)，而 TOE 不能确定某个选票是否已投，以及该选票的投票结果是怎样的(除非投票一致通过)。

I.4.3.2 操作

I.4.3.2.1 赋值

在 FPR_UNO.2.1 中，PP/ST 作者应规定 TSF 必须提供保护以防范的用户或主体集。例如，即使 PP/ST 作者只规定了单个用户或主体角色，但 TSF 不仅必须防范单个用户或主体，而且也必须防范用户或主体的协作。例如，用户集可以是一组用户，他们能在相同的角色下操作或都能用相同的进程。

在 FPR_UNO.2.1 中，PP/ST 作者应确定操作列表，这些操作遵从不可观察性要求。这样，其他用户/主体就不能够观察到对指定列表中一个隐蔽客体的操作(如对该客体的读写)。

在 FPR_UNO.2.1 中，PP/ST 作者应确定被不可观察性要求覆盖的客体的列表。例如，一个特定的邮件服务器或 ftp 站点。

在 FPR_UNO.2.1 中，PP/ST 作者应规定一组受保护的用户或主体，他们的不可观察性信息是受保护的。这样的例子可以是："通过 Internet 访问该系统的用户。"

在 FPR_UNO.2.2 中，PP/ST 作者应确定哪些与隐私相关的信息应以受控制的方式分布到系统中。这些信息的例子可以是：主体的 IP 地址、客体的 IP 地址、时间、所使用的密钥。

在 FPR_UNO.2.2 中，PP/ST 作者应规定信息分发应遵循的条件。这些条件应在每个实例的隐私相关信息的整个生命期内得到维护。这些条件的例子可以是："该信息只能出现在 TOE 的一个单独部分，且不能传送到 TOE 这部分之外"，"该信息仅驻留在 TOE 的一个单独部分，但可定期地移动到 TOE 的另一个部分"，"该信息应分布在 TOE 的不同部分中，使得即使破坏任意五个不同的 TOE 部分，也不会危及安全策略。"

I.4.4 FPR_UNO.3 无索求信息的不可观察性

I.4.4.1 用户应用注释

本组件用来要求当提供特定的服务时，TSF 不试图获取会破坏不可观察性的信息。因此 TSF 不索求(即试图从其他实体获得)能用来破坏不可观察性的任何信息。

I.4.4.2 操作

I.4.4.2.1 赋值

在 FPR_UNO.3.1 中，PP/ST 作者应确定遵从不可观察性要求的服务列表。例如，“对工作描述的访问”。

在 FPR_UNO.3.1 中，PP/ST 作者应确定主体列表，在提供特定服务时，应保护其与隐私相关的信息。

在 FPR_UNO.3.1 中，PP/ST 作者应规定特定主体受保护的隐私相关信息。例如，使用一个服务的主体身份，以及已被使用的服务程度如内存资源的使用情况。

I.4.5 FPR_UNO.4 授权用户可观察性

I.4.5.1 用户应用注释

本组件用来要求将有一个或多个授权用户有权查看资源的使用情况。如果没有本组件，则该查阅是允许的，但不是强制的。

I.4.5.2 操作

I.4.5.2.1 赋值

在 FPR_UNO.4.1 中，PP/ST 作者应规定授权用户集，TSF 须为他们提供观察资源使用情况的能力。例如，授权用户集可以是一组授权用户，他们能在相同的角色下操作或都能使用相同的进程。

在 FPR_UNO.4.1 中，PP/ST 作者应规定授权用户一定能观察的资源或服务集。

附 录 J
（规范性附录）
FPT 类：TSF 保护

本类包含了多个功能要求族，这些要求与组成 TSF 的机制的完整性和管理有关，并与 TSF 数据的完整性有关。在某种意义下，本类中的族可能出现与 FDP“用户数据保护”类中相重复的组件，甚至可以用同一个机制来实现。但是，FDP“用户数据保护”主要侧重于用户数据的保护，而 FPT“TSF 保护”主要侧重于 TSF 数据的保护。事实上，FPT“TSF 保护”类的组件对于规范 TOE 中的 SFP 不被篡改或旁路等方面的要求时是必需的。

从 FPT 类的观点看，关于 TSF 有以下 3 个重要元素：

a) TSF 实现，执行并实现那些实施 SFR 的机制。

b) TSF 数据，指导 SFR 实施的管理性数据库。

c) 为执行 SFR，TSF 可能与其相互作用的外部实体。

所有 FPT 类中的族都与这几个部分相关，并分属下面几个组：

a) FPT_PHP“TSF 物理保护”，向授权用户提供检测能力，以检测针对组成 TSF 的 TOE 各部分的外部攻击。

b) FPT_TEE“外部实体测试”和 FPT_TST“TSF 自检”，向授权用户提供这样的能力，其可验证那些与执行 SFR 的 TSF 相互作用的外部实体的正确操作，以及验证 TSF 数据和可执行代码的完整性。

c) FPT_RCV“可信恢复”、FPT_FLS“失效保护”和 FPT_TRC“TOE 内 TSF 数据复制的一致性”，负责处理失效发生时和紧接失效之后的 TSF 的行为。

d) FPT_ITA“输出 TSF 数据的可用性”、FPT_ITC“输出 TSF 数据的机密性”和 FPT_ITI“输出 TSF 数据的完整性”，负责处理 TSF 和另一个可信 IT 产品之间的 TSF 数据的保护和可用性。

e) FPT_ITT“TOE 内 TSF 数据的传送”，当 TSF 数据在物理上分离的 TOE 部分间传送时，负责处理 TSF 数据的保护。

f) FPT_RPL“重放检测”，负责处理不同类型的信息或操作的重放。

g) FPT_SSP“状态同步协议”，基于 TSF 数据，负责处理在一个分布式 TSF 的不同部分之间的状态同步。

h) FPT_STM“时间戳”，负责提供可靠的时间。

i) FPT_TDC“TSF 间 TSF 数据的一致性”，负责处理在 TSF 和另一个可信 IT 产品之间共享的 TSF 数据的一致性。

本类的组件构成分解如图 J.1 所示。

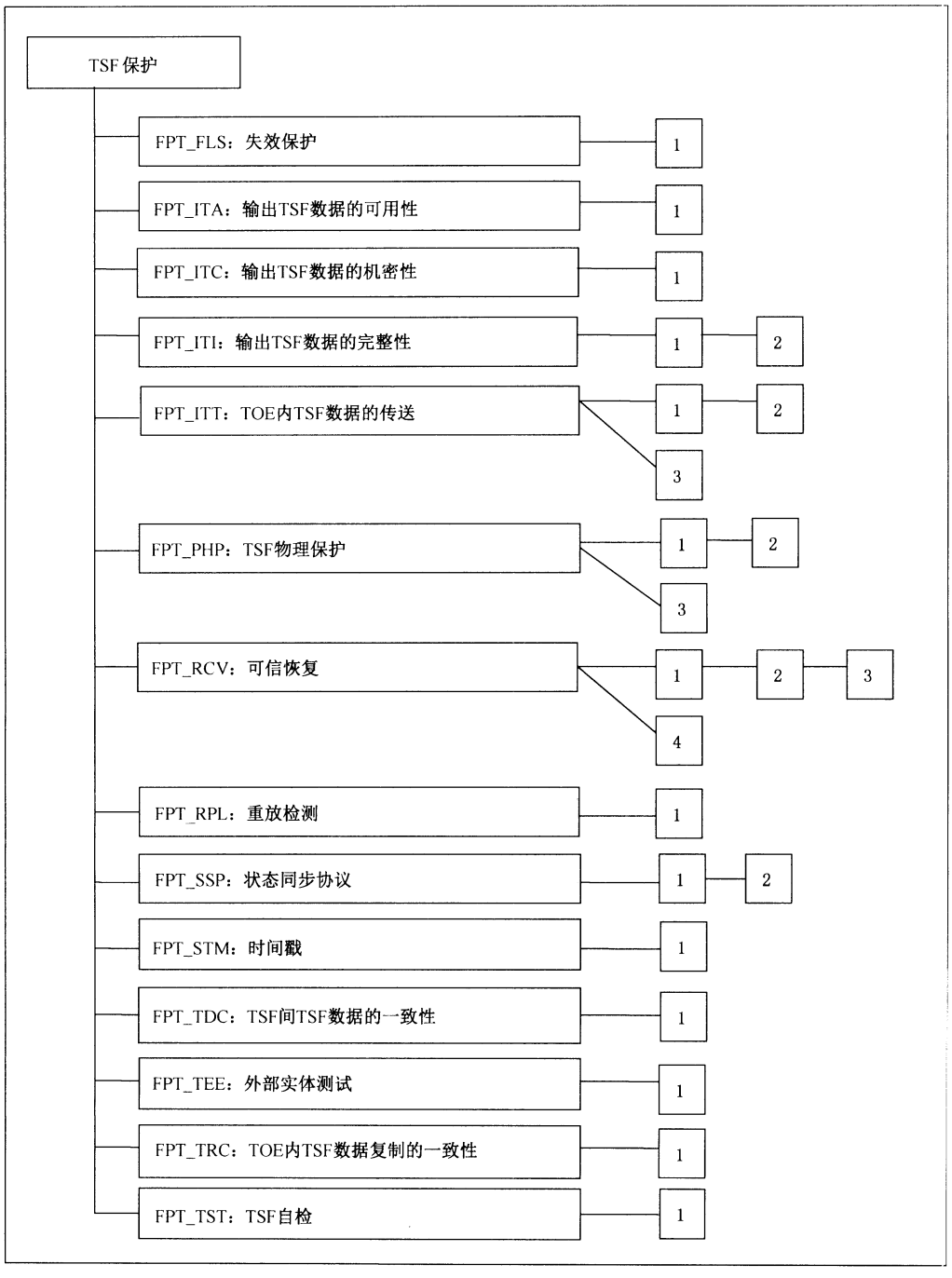

图 J.1 TSF 保护类分解

J.1 失效保护(FPT_FLS)

J.1.1 用户注释

本族的要求确保在 TSF 中发生某些类型的失效时，TOE 总能执行其 SFR。

J.1.2 FPT_FLS.1 失效即保持安全状态

J.1.2.1 用户应用注释

术语“安全状态”指示一个状态，在此状态中 TSF 数据是一致的，而且 TSF 继续正确执行 SFR。

虽然希望审计失效即保持安全状态的情况，但是不可能在所有的情况下都能审计。PP/ST 作者应规定希望审计并可执行审计的那些情形。

在 TSF 中的失效可能包括“硬”失效，它指示一个设备发生故障且需要维护、维修或修理 TSF。TSF 中的失效也可能包括可恢复的“软”失效，它仅要求初始化或重新设置 TSF。

J.1.2.2 操作

J.1.2.2.1 赋值

在 FPT_FLS.1.1 中，PP/ST 作者应列出 TSF 中失效的类型，对此失效 TSF 应“失效保护”，也就是说，应保持一个安全的状态，且继续正确执行 SFR。

J.2 输出 TSF 数据的可用性(FPT_ITA)

J.2.1 用户应用注释

本族定义了防止在 TSF 和另一个可信任 IT 产品之间移动的 TSF 数据丧失可用性的有关规则。该数据可能是 TSF 关键的数据，如口令、密钥、审计数据或 TSF 可执行代码。

本族常用于分布式的系统环境中，其中 TSF 向另一个可信 IT 产品提供 TSF 数据。该 TSF 只能在本端上采取措施，而不能对其他可信 IT 产品的 TSF 负责。

如果对不同类型的 TSF 数据，存在不同的可用性度量的话，那么对于每个唯一的度量和 TSF 数据类型配对都应重述本组件。

J.2.2 FPT_ITA.1 TSF 间可用性不超过既定可用性度量

J.2.2.1 操作

J.2.2.1.1 赋值

在 FPT_ITA.1.1 中，PP/ST 作者应规定服从可用性度量的 TSF 数据类型。

在 FPT_ITA.1.1 中，PP/ST 应针对可用的 TSF 数据，规定可用性度量。

在 FPT_ITA.1.1 中，PP/ST 作者应规定必须确保可用性的那些条件。例如：在 TOE 和另一个可信任 IT 产品之间必须有一个连接。

J.3 输出 TSF 数据的机密性(FPT_ITC)

J.3.1 用户注释

本族定义了防止在 TSF 和另一个可信任 IT 产品之间移动的 TSF 数据被未授权泄露的规则。该数据可能是 TSF 关键的数据，如口令、密钥、审计数据或 TSF 可执行代码。

本族常用于分布式的系统环境中，其中 TSF 向另一个可信 IT 产品提供 TSF 数据。该 TSF 只能在本端上采取措施，而不能对其他可信 IT 产品的行为负责。

J.3.2 FPT_ITC.1 传送过程中 TSF 间的机密性

J.3.2.1 评估者注释

传送过程中 TSF 数据的机密性是必须受保护的，以防止这些信息被泄露。某些可能的实现可提供机密性包括使用加密算法和扩频技术。

J.4 输出 TSF 数据的完整性(FPT_ITI)

J.4.1 用户注释

本族定义了一些规则，用于保护在 TSF 和另一个可信 IT 产品之间传送的 TSF 数据，防止其被未授权修改。该数据可能是 TSF 关键数据如口令、密钥、审计数据或是 TSF 可执行代码。

本族常用于分布式的系统环境中，其中 TSF 同另一个可信 IT 产品交换 TSF 数据。注意，不能规定在另一个可信 IT 产品上处理修改、检测和恢复这样的要求，因为不能事先确定另一个可信 IT 产品将用什么样的机制来保护它的数据。由于这一原因，这些要求被表述为“TSF 提供一种能力”，这种能力是另一个可信 IT 产品也能使用的。

J.4.2 FPT_ITI.1 TSF 间修改的检测

J.4.2.1 用户应用注释

本组件应用在那些足以检测到数据何时被修改的场合。例如以下场合：当检测到修改时，另一个可信 IT 产品可以要求 TOE 的 TSF 重新传送数据，或对这种类型的请求进行响应。

所期望的修改检测强度是基于一个指定的修改度量，它是所用算法的一个函数，可以涵盖从无法检测多个比特更改的一个弱校验和和奇偶校验机制，到更复杂的密码校检和方法。

J.4.2.2 操作

J.4.2.2.1 赋值

在 FPT_ITI.1.1 中，PP/ST 应规定检测机制必须满足修改度量。这一修改度量应规定所期望的修改检测强度。

在 FPT_ITI.1.2 中，PP/ST 应规定检测到对 TSF 数据的修改时应采取的动作。这种动作的一个例子就是“忽略 TSF 数据，并要求原发可信产品再次发送这些 TSF 数据。”

J.4.3 FPT_ITI.2 TSF 间修改的检测与纠正

J.4.3.1 用户应用注释

本组件应用在有必要检测或纠正 TSF 关键数据修改的场合。

所期望的修改检测强度是基于一个指定的修改度量，它是所用算法的一个函数，可以涵盖从无法检测多个比特更改的一个弱校验和和奇偶校验机制，到更复杂的密码校检和方法。需定义的度量既可参考将要抵御的攻击(如，仅有千分之一的随机消息会被接受)，也可以参考公开文献中众所周知的一些机制(如，这一强度必须与由安全散列算法提供的强度一致)。

纠正修改采用的方法可以通过某种差错纠正校验和的形式来完成。

J.4.3.2 评估者注释

满足这一要求的某些方法可能涉及密码功能的使用或校验和的某种形式。

J.4.3.3 操作

J.4.3.3.1 赋值

在 FPT_ITI.2.1 中，PP/ST 应规定检测机制必须满足的修改度量。这一修改度量应规定所期望的修改检测的强度。

在 FPT_ITI.2.2 中，PP/ST 应规定检测到对 TSF 数据的修改时应采取的动作。这种动作的一个例子就是“忽略 TSF 数据，并要求原发可信产品再次发送这些 TSF 数据。”

在 FPT_ITI.2.3 中，PP/ST 作者应定义修改的类型，TSF 应能从这些修改中恢复。

J.5 TOE 内 TSF 数据的传送(FPT_ITT)

J.5.1 用户注释

本族提供了这样的要求，即通过内部信道在 TOE 的各分离部分间传送 TSF 数据时，要对这些数据进行保护。

分离(如，物理或逻辑分离)使得本族的应用更有意义，而分离程度的确定取决于所要使用的环境。在恶意环境中，如果仅通过一条系统总线或进程间通信信道，在分离的各个 TOE 部分间传送数据，可能会产生一些风险。在比较良好的环境里，这一传送可通过更传统的网络媒体来完成。

J.5.2 评估者注释

一个适用于 TSF 以提供这种保护的实用机制是建立在密码基础上的。

J.5.3 FPT_ITT.1 内部 TSF 数据传送的基本保护

J.5.3.1 操作

J.5.3.1.1 选择

在 FPT_ITT.1.1 中，PP/ST 作者应规定希望提供的保护类型：是防止泄露，还是防止修改。

J.5.4 FPT_ITT.2 TSF 数据传送的分离

J.5.4.1 用户应用注释

基于 SFP 相关属性，实现 TSF 数据分离的方法之一，是通过使用不同的逻辑或物理信道。

J.5.4.2 操作

J.5.4.2.1 选择

在 FPT_ITT.2.1 中，PP/ST 作者应规定希望提供的保护类型：是防止泄露，还是防止修改。

J.5.5 FPT_ITT.3 TSF 数据完整性监视

J.5.5.1 操作

J.5.5.1.1 选择

在 FPT_ITT.3.1 中，PP/ST 作者应规定 TSF 所能检测到的修改类型。PP/ST 作者应从以下类型中进行选择：数据的修改、数据的替换、数据的重排、数据的删除或任何其他类型完整性错误。

J.5.5.1.2 赋值

在 FPT_ITT.3.1 中，如果 PP/ST 作者选择了上面段落中的最后一种选项，那么该作者也应该规定哪些其他类型完整性差错是 TSF 有能力检测到的。

在 FPT_ITT.3.2 中，PP/ST 作者应规定在识别到一个完整性错误时应采取的动作。

J.6 TSF 物理保护(FPT_PHP)

J.6.1 用户注释

TSF 物理保护组件涉及限制对 TSF 进行未授权的物理访问，以及阻止和抵制对 TSF 进行未授权的物理修改或替换。

本族中的要求确保了 TSF 是被保护的，以防物理上的侵害和干扰。若满足这些组件要求，将会使 TSF 被封装后以如下方式使用：物理侵害是可检测的，或基于既定工作因素对物理侵害的防御是可测量的。如果没有这些组件，在物理破坏无法避免的环境下，TSF 的保护功能就会失效。这一组件同时也提供了一些有关 TSF 必须如何响应物理侵害尝试的要求。

有关物理侵害情景的例子包括机械攻击、辐射、温度改变。

对授权用户来讲，仅在离线状态或维护模式下才能检测到物理侵害的这种功能是可接受的。在这些状态下，对授权用户应加以控制以限制访问。由于在这些状态下 TSF 可能是不可操作的，它也许不能正常执行授权用户访问。TOE 的物理实现可能由几个结构组成：例如外部屏蔽罩、卡和芯片。这一组“元件”作为一个整体必须保护(保护、报告和抵御)TSF 免受物理侵害。这并不意味着所有的设备都必须提供这些特征，不过作为一个完整的物理构造，总体上应具备上述特征。

尽管只有最小级审计与这些组件有关，这完全是因为在与审计子系统交互的层面下，存在完全以硬件实现检测和预警机制的可能性[(例如，当授权用户按下一个按钮断开电路时，一个基于电路断开就亮灯这种策略的硬件检测系统就点亮发光二极管(LED)]。不过，PP/ST 作者也可确定对一个特定的可预料的威胁环境，是否需要审计物理侵害。如果需要，PP/ST 作者应在审计事件列表中包括合适的要求。注意加入这些要求可能会对硬件设计和它的软件接口产生影响。

J.6.2 FPT_PHP.1 物理攻击的被动检测

J.6.2.1 用户应用注释

FPT_PHP.1“物理攻击的被动检测”应在当程序化方法不能对抗对 TOE 部件的未授权物理侵害时使用，负责处理对 TSF 进行未被发现的物理侵害。通常应赋予授权用户验证侵害是否发生的职责。如上所述，这一组件仅提供 TSF 检测篡改的能力。应考虑在 FMT_MOF.1“安全功能行为的管理”的管理功能规范中指定谁能使用这些能力，他们如何使用这些能力。如果这一功能由非 IT 机制(如物理检查)来实现，那么就不需要管理功能。

J.6.3 FPT_PHP.2 物理攻击报告

J.6.3.1 用户应用注释

PT_PHP.2“物理攻击报告”应在程序化方法不能对抗对 TOE 部件进行未授权物理侵害威胁时使用，要求指定人员能得到有关物理侵害的通知。本组件负责处理那种尽管检测到了对 TSF 元件的物理篡改却可能不会报告的威胁。应考虑在 FMT_MOF.1“安全功能行为的管理”的管理功能规范中指定谁能使用这些能力，他们如何使用这些能力。

J.6.3.2 操作

J.6.3.2.1 赋值

在 FPT_PHP.2.3 中，PP/ST 作者应提供需主动检测物理侵害的 TSF 设备/元件列表。

在 FPT_PHP.2.3 中，PP/ST 作者应指定在检测到侵害时应通知的用户或角色。用户或角色的类型可以根据 PP/ST 中包含的特定安全管理组件（来自 FMT_MOF.1“安全功能行为的管理”族）而改变。

J.6.4 FPT_PHP.3 物理攻击抵抗

J.6.4.1 用户应用注释

对某些形式的侵害，TSF 不仅有必要监测该侵害，更要真正地抵抗侵害或延迟攻击者的攻击。

当希望 TSF 设备或 TSF 元件运行在 TSF 设备或 TSF 元件内部，而物理侵害（如观察、分析或修改）也是可能造成威胁时，应使用本组件。

J.6.4.2 操作

J.6.4.2.1 赋值

在 FPT_PHP.3.1 中，对 TSF 应为其抵抗物理侵害的 TSF 设备/元件，PP/ST 应为其规定侵害情景。基于技术限制和相关设备的物理暴露等考虑，这一列表可用于一个既定的 TSF 物理设备或元件的子集。应明确定义和证明这些子集。另外，TSF 应能自动响应物理侵害。此自动响应应是使设备受到保护的策略。例如，根据机密性策略，物理上“禁用”该设备，这样被保护信息就不能被检索是可接受的。

在 FPT_PHP.3.1 中，PP/ST 作者应规定 TSF 设备/元件列表，TSF 应在既定的情景中为其抵抗物理侵害。

J.7 可信恢复（FPT_RCV）

J.7.1 用户注释

本族的要求确保 TSF 能确定 TOE 是在没有削弱保护能力的情况下启动的，以及在运行中断后能在没有削弱保护能力的情况下即可恢复。本族很重要，因为 TSF 的启动状态确定了后续状态的保护情况。

作为对预期失效的发生、运行中断或启动的直接响应，恢复组件重建 TSF 安全状态，或是阻止向不安全状态迁移。通常，必须预期的失效包括：

a) 总是导致系统崩溃的可揭露动作失效（如关键的系统表总是不一致、由瞬间的硬件或固件故障引起的 TSF 编码内非受控的传送、电力失效、处理器失效、通信失效）；

b) 导致代表 TSF 客体的部分或全部存储介质变得不可访问，或崩溃的存储介质失效（如奇偶错误、磁盘头损坏、由磁盘头偏离引起的持续读写失灵、磁涂层损坏、磁盘表面的灰尘）；

c) 由错误的管理行为或缺乏及时的管理行为造成的运行中断（如不可预知的关掉电闸、没有注意到关键的资源已被用尽、安装配置不适当）。

注意，恢复可以是完全失效或部分失效情况的恢复。完全失效可能发生在单一操作系统，不太可能发生在分布式的环境中。在分布式环境中，子系统可能失效，但其他部分仍能工作。另外，关键的组件可以冗余（磁盘镜像、可选路由），并且可能有检查点。因此，恢复是指恢复到一个安全状态。

在选择 FPT_RCV“可信恢复”时，应考虑 FPT_RCV“可信恢复”和 FPT_TST“TSF 自检”之间存在

不同相互影响：

a) 可信恢复需求可以通过 TSF 自检结果来指示，其中自检结果指示 TSF 处于一个非安全状态并需要回到一个安全状态或进入维护模式；

b) 如上所述，可以由管理员识别出一个失效。管理员可以执行操作将 TOE 返回到一个安全状态，然后调用 TSF 自检功能确认安全状态已经达到。或者，可以调用 TSF 自检功能完成恢复过程；

c) 上述 a)和 b)的组合，TSF 自检结果指示需要可信恢复，管理员执行操作将 TOE 返回到一个安全状态，然后调用 TSF 自检功能确认安全状态已经达到；

d) 自检检测一个失效/服务中断，然后自动恢复或进入维护模式。

本族确定了一个维护模式。在这个维护模式中，不能进行正常的操作，或正常操作受严格限制，否则另外的不安全情况可能发生。通常，应只允许授权的用户访问这一模式，但究竟谁能访问这一模式的细节规定由 FMT“安全管理”类中的一个功能负责。如果 FMT“安全管理”对谁能访问这一模式没进行控制，那么若 TOE 进入这种状态，则允许任何用户恢复系统是可接受的。但实际上，由于恢复系统的用户有机会以违反 TSP 的方式配置 TOE，因此可能并不希望这样。

用于检测运行中异常情况的机制归到 FPT_TST“TST 自检”、FPT_TLS“失效保护”和负责处理“软件安全”概念的其他领域。类似地，将要求使用这些族其中一个，以支持 FPT_RCV“可信恢复”的采用，这是为了确保 TOE 能检测到何时需要恢复。

在本族中使用了“安全状态”一词。它指的是 TOE 具有一致的 TSF 数据以及 TSF 能正确地实施策略的某个状态。该状态可能是一个干净系统的初始“引导”，或者是某个检查点状态。

对于恢复，通过 TSF 的自检确认安全状态已经达到是必需的。但是，如果以某种方式执行恢复时，要求仅当达到安全状态，否则恢复失败，则此时对 FPT_TST.1“TST 检测”组件的依赖关系可忽略。

J.7.2 FPT_RCV.1 手工恢复

J.7.2.1 用户应用注释

在可信恢复族的分层体系中，只需要手工干涉的恢复是最低要求，因为它避免在无人干涉的方式下使用系统。

本组件试图在 TOE 不要求自动恢复到安全状态时使用。本组件的要求降低了由人工介入的 TOE 从一个失效或其他中断恢复后又返回到不安全状态时所带来的削弱保护能力的威胁。

J.7.2.2 评估者应用注释

授权用户仅在维护模式下可用本组件功能进行可信恢复是可接受的。应采取控制措施限制授权用户在维护模式下的访问。

J.7.2.3 操作

J.7.2.3.1 赋值

在 FPT_RCV.1.1 中，PP/ST 作者应规定失效或服务中断列表(如电力故障、审计存储耗尽、任何失效或中断)。在该失效或服务中断发生后，TSF 将进入一种维护模式。

J.7.3 FPT_RCV.2 自动恢复

J.7.3.1 用户应用注释

由于自动恢复允许机器以无人干涉的方式进行操作，所以被认为比手工恢复更有用。

通过要求在失效或服务中断后至少有一种自动恢复方法，组件 FPT_RCV.2“自动恢复”扩展了 FPT_RCB.1“手工恢复”的作用范围。它负责处理由无人干涉的 TOE 从一个失效或其他中断恢复后又返回到不安全状态时所带来的削弱保护能力的威胁。

J.7.3.2 评估者应用注释

授权用户仅在维护模式下可用本组件功能进行可信恢复是可接受的。应采取控制措施限制授权用户在维护模式下的访问。

对 FPT_RCV.2.1，TSF 开发者有责任确定可恢复的失效和服务中断集合。

假定自动恢复机制的健壮性得到了验证。

J.7.3.3 操作

J.7.3.3.1 赋值

在 FPT_RCV.1.1 中，PP/ST 作者应规定失效或服务中断列表（如电力故障、审计存储耗尽、任何失效或中断）。在该失效或服务中断发生后，TSF 将进入一种维护模式。

在 FPT_RCV.2.2 中，PP/ST 作者应规定必须可以自动恢复的失效或其他中断列表。

J.7.4 FPT_RCV.3 无过度损失的自动恢复

J.7.4.1 用户应用注释

自动恢复被认为比手工恢复更为有用，但它存在可能损失相当数量客体的风险。防止客体的过度损失对恢复工作提出了额外的要求。

通过要求在 TSF 控制下不能出现 TSF 数据或客体的过度损失，组件 FPT_RCV.3“无过度损失的自动恢复”扩展了 FPT_RCV.2“自动恢复”的作用范围。在 FPT_RCV.2“自动恢复”中，自动恢复机制可通过删除所有客体并将 TSF 返回到一个已知的安全状态来进行恢复。这种极端的自动恢复形式被排除在 FPT_RCV.3 “无过度损失的自动恢复”之外。

本组件负责处理由无人干涉的 TOE 从一个失效或其他中断恢复后又返回到一个不安全状态，并伴随着 TSF 数据或客体大量损失时所带来的削弱保护能力的威胁。

J.7.4.2 评估者应用注释

授权用户仅在维护模式下可用本组件功能进行可信恢复是可接受的。应采取控制措施限制授权用户在维护模式下的访问。

假定评估者将验证自动恢复机制的健壮性。

J.7.4.3 操作

J.7.4.3.1 赋值

在 FPT_RCV.3.1 中，PP/ST 作者应规定失效或服务中断列表（如电力故障、审计存储空间耗尽）。在该失效或服务中断发生后，TSF 将进入一种维护模式。

在 FPT_RCV.3.2 中，PP/ST 作者应规定必须能够自动恢复的失效或其他中断列表。

在 FPT_RCV.3.3 中，PP/ST 作者规定一个可接受的 TSF 数据或客体的损失量。

J.7.5 FPT_RCV.4 功能恢复

J.7.5.1 用户应用注释

功能恢复要求如果 TSF 发生了某个失效，则 TSF 中的某些功能要么能成功地完成，要么恢复到一个安全的状态。

J.7.5.2 操作

J.7.5.2.1 赋值

在 FPT_RCV.4.1 中，PP/ST 作者应规定功能和失效情景的列表。任何一种已被标识的失效情景发生时，已规定的功能必须要么成功地完成，要么恢复到一个稳定、安全的状态。

J.8 重放检测(FPT_RPL)

J.8.1 用户注释

本族负责处理对不同类型实体的重放检测以及随后的纠正行为。

J.8.2 FPT_RPL.1 重放检测

J.8.2.1 用户应用注释

例如，实体包括：消息、服务请求、服务响应或会话。

J.8.2.2 操作

J.8.2.2.1 赋值

在 FPT_RPL.1.1 中，PP/ST 作者应提供能进行重放检测的确定实体列表。这些实体的例子可能包括：消息、服务请求、服务响应和用户会话。

在 FPT_RPL.1.2 中，PP/ST 作者应规定当检测到重放时 TSF 应采取的动作列表。可能采取的动作包括：忽略被重放的实体、请求确认来自确定来源的实体、终止重放实体的原发主体。

J.9 状态同步协议(FPT_SSP)

J.9.1 用户注释

分布式 TOE 由于不同部分之间潜在的状态差别和通信延迟，可能会比单一 TOE 更复杂。在大多数情况下，分布式功能间的状态同步涉及一个交换协议，而不是一个简单的动作。当这些协议所处的分布式环境中存在蓄意的危害时，就需要更为复杂的防御协议。

FPT_SSP“状态同步协议”规定了关于 TSF 某些关键安全功能如何使用可信协议的要求。FPT_SSP“状态同步协议”确保 TOE 的两个分布式部分(如主机)在完成一个安全有关的活动之后，已将他们的状态同步。

有些状态可能永远无法完成同步，或实际使用中同步代价太高：以加密密钥销毁为例，在销毁动作发起后的密钥状态是不可知的，要么采取了动作但回执不能发出，要么是敌意的通信方不理会这一信息且永远不执行销毁。不确定性是分布式 TOE 所特有的，不确定性和状态同步是相关的，可使用相同的解决方案。设计成不确定的状态是无意义的，PP/ST 作者应针对此情况指出其他要求(如发出警报、审

计事件)。

J.9.2 FPT_SSP.1 简单可信回执

J.9.2.1 用户应用注释

本组件要求 TSF 在收到请求时必须为 TSF 的其他部分提供回执。该回执应表明分布式 TOE 的一部分成功地接收到了来自此 TOE 其他不同部分的未被篡改的数据传输。

J.9.3 FPT_SSP.2 相互可信回执

J.9.3.1 用户应用注释

本组件要求 TSF 除了能对数据接收提供回执外,还必须应答其他 TSF 部分对该回执给出一个回执的请求。

例如,本地 TSF 发送一些数据到 TSF 远程部分。TSF 远程部分给出成功地收到了该数据的回执,并请求 TSF 发送方确认它已收到这一回执。这一机制为进行数据传送的 TSF 双方提供了额外的信心,使双方确信数据传输已成功完成。

J.10 时间戳(FPT_STM)

J.10.1 用户注释

本族负责处理一个 TOE 中的可靠时间戳功能要求。

PP/ST 作者有责任明确解释"可靠的时间戳"的含义,并指出如何才能确定其可信。

J.10.2 FPT_STM.1 可靠的时间戳

J.10.2.1 用户应用注释

可能用到这一组件的情况包括为审计目的和安全属性到期提供可靠的时间戳。

J.11 TSF 间 TSF 数据的一致性(FPT_TDC)

J.11.1 用户注释

在分布式或组合系统环境下,TOE 或许需要与其他可信 IT 产品交换 TSF 数据(如与数据有关的 SFP 属性、审计信息、标识信息等)。本族就关于在 TOE 的 TSF 和不同可信 IT 产品的 TSF 间的属性共享、属性一致性解释方面定义了一些要求。

本族中的组件意在提出这样的要求,即要求在 TOE 的 TSF 和另一个可信 IT 产品的 TSF 之间传送 TSF 数据时,自动支持 TSF 数据一致性。也有可采用完全程序化的方法来实现安全属性的一致性,但这里不做要求。

本族不同于 FDP_ETC 和 FDP_ITC,因为那两个族只涉及解决 TSF 和它的输入/输出媒体之间的安全属性。

如果关注 TSF 数据的完整性,应从 FPT_ITI"输出 TSF 数据的完整性"族中选择要求,这些组件规定了 TSF 能检测或检测并纠正传送中的 TSF 数据改动的要求。

J.11.2 FPT_TDC.1 TSF 间基本的 TSF 数据一致性

J.11.2.1 用户应用注释

TSF 负责维护被指定功能所使用或相关联的 TSF 数据的一致性，这通常存在于两个或多个可信系统之间。例如，两个不同系统的 TSF 数据可能有不同的内部约定。为了使可信 IT 产品能正确使用 TSF 数据(例如，对用户数据提供就像在 TOE 内部一样的保护)，TOE 和其他可信 IT 产品必须使用一个预先建立的协议来交换 TSF 数据。

J.11.2.2 操作

J.11.2.2.1 赋值

在 FPT_TDC.1.1 中，PP/ST 作者应定义一个 TSF 数据类型列表，从而当 TSF 数据在 TSF 和其他可信 IT 产品间共享时，TSF 应提供一致性解释的能力。

在 FPT_TDC.1.2 中，PP/ST 应规定 TSF 使用的解释规则列表。

J.12 外部实体测试(FPT_TEE)

J.12.1 用户注释

本族定义了 TSF 测试一个或多个外部实体时的要求，这些外部实体并非指人类用户，可以包括与 TOE 交互的软件和/或硬件的组合。

可能运行的测试类型包括：

a) 防火墙的存在性测试，可能包括其配置正确性测试；

b) 支撑应用类 TOE 运行的操作系统属性测试；

c) 支撑智能卡 OS 类 TOE 运行的 IC 属性测试(例如随机数生成器)。

注意外部实体可能“谎报”测试结果，其原因要么是故意的，要么是运行不正确造成的。

这些测试可以在维护状态下执行、也可在启动阶段、运行阶段、或以连续的方式执行。作为测试结果的 TOE 动作也在这个族中定义。

J.12.2 评估者注释

外部实体测试应充分的测试 TSF 依赖的所有特性。

J.12.3 FPT_TEE.1 外部实体测试

J.12.3.1 用户应用注释

这个组件不建议应用到人类用户。

通过要求周期性地调用测试的功能，这个组件提供了 TSF 操作依赖的外部实体特性的定期测试支持。

PP/ST 作者可通过提炼要求声明功能在离线、在线或维护模式下是否可用。

J.12.3.2 评估者注释

周期性测试功能只在离线或维护模式下可用是可接受的。维护模式应当限制授权用户的访问。

J.12.3.3 操作

J.12.3.3.1 选择

在 FPT_TEE.1.1 中，PP/ST 作者应详细说明 TSF 应何时执行外部实体测试，是在初始启动阶段执行，还是在正常操作期间周期性地执行，或作为授权用户请求响应方式执行。此外，还可能存在其他执行条件。如果测试执行频繁，则相比于测试频率较低的情况，最终用户将有更多的信心相信 TOE 工作正常。不过，应对提升 TOE 正常工作的信心和降低对 TOE 可用性的潜在影响这两方面进行折中考虑，因为经常性的测试可能延缓 TOE 的正常运转。

J.12.3.3.2 赋值

在 FPT_TEE.1.1 中，PP/ST 作者应规定外部实体的属性要靠测试来检查。这些属性的例子可以包括配置或支持 TSF 的访问控制部分的目录服务器的可用性。

在 FPT_TEE.1.1 中，一旦其他条件被选择，PP/ST 作者应该指定自测的频率。其他频率或条件的例子可能是每次用户需要发起与 TOE 的会话时运行这些测试。举例来说，这可能在用户鉴别过程中，在与 TSF 的交互前需测试目录服务器。

在 FPT_TEE.1.2 中，PP/ST 作者应规定，当测试失败时 TSF 应执行哪些动作。这些动作的例子，以目录服务器为例，如：连接到替代可用服务器或查找备份服务器。

J.13 TOE 内 TSF 数据复制的一致性(FPT_TRC)

J.13.1 用户注释

在 TOE 内部复制 TSF 数据时，需要满足本族的要求以确保 TSF 数据的一致性。如果 TOE 不同组成部分间的内部信道不能正常工作，这些复制的 TSF 数据就可能不一致。如果 TOE 内部被构造成像 TOE 组成部分的网络一样，则 TOE 组成部分失效时，网络连接中断时，等等，都会发生这种不一致的情况。

确保一致性的方法未在这一组件中规定。此方法可通过某种事务处理日志得到(适当的事务处理被“回退”到某一点重新连接)；通过同步协议可更新被复制的数据。如果 PP/ST 需要特定的协议，可以通过细化来指定。

某些状态的同步几乎不可能，或同步的开销太大。例如通信信道和加密密钥的撤销。不确定状态也可能发生；如果期望某个特定的行为，应通过细化来规定。

J.13.2 FPT_TRC.1，内部 TSF 的一致性

J.13.2.1 操作

J.13.2.1.1 赋值

在 FPT_TRC.1.2 中，PP/ST 作者应规定依赖于 TSF 数据复制一致性的 SF 列表。

J.14 TSF 自检(FPT_TST)

J.14.1 用户注释

本族定义了一些关于 TSF 自检的要求，这些检测与某些期待的正确操作有关。如执行功能的接口

和 TOE 关键部分的抽样算术运算。这些检测可在启动时进行，或周期性地进行，或应授权用户的请求进行，或满足其他条件时进行。TOE 根据自检结果所采取的动作在其他族中定义。

本族的要求也用于检测由多种失效造成的 TSF 可执行代码（如 TSF 软件）和 TSF 数据损坏，这种检测并不需要 TOE 停止工作（这将由别的族处理）。因为这些失效不可避免，故必须执行这些检查。这些失效可能是由不可预见的失效方式或硬件、固件、软件设计的某些疏忽所造成，也可能由于逻辑的或物理的保护不充分导致 TSF 恶意损坏所造成。

另外，在合适的条件下，作为维护活动的结果，使用这一组件可帮助防止不合适的或有害的 TSF 更改被应用到一个运行中的 TOE 上。

“TSF 正确操作”主要是指 TSF 软件操作和 TSF 数据的完整性。

J.14.2 FPT_TST.1 TSF 检测

J.14.2.1 用户应用注释

这一组件通过要求能够调用检测功能、检查 TSF 数据和可执行代码的完整性，对 TSF 操作的关键功能的检测提供支持。

J.14.2.2 评估者应用注释

授权用户可用于周期性检测的功能仅在离线或维护模式下有用是可接受的。在这些模式下，应采用控制措施限制授权用户的访问。

J.14.2.3 操作

J.14.2.3.1 选择

在 FPT_TST.1.1 中，PP/ST 作者应详细说明何时 TSF 将执行 TSF 检测：在初始化启动期间，在正常工作期间周期性地，授权用户要求时或在其他条件下。如果选择了最后一项，PP/ST 作者还应通过以下的赋值具体规定这些条件。

在 FPT_TST.1.1 中，PP/ST 作者应详细说明通过执行自检是为了证实整个 TSF 能正确运行，还是为了证实 TSF 的某些指定组成部分能正确运行。

J.14.2.3.2 赋值

在 FPT_TST.1.1 中，如果选择了“满足产生自检的条件时”，PP/ST 作者应规定应进行自检的条件。

在 FPT_TST.1.1 中，如果选择了“TSF 的某些组成部分”，PP/ST 作者应规定应该被 TSF 自检的 TSF 组成部分列表。

J.14.2.3.3 选择

在 FPT_TST.1.2 中，PP/ST 作者应规定是验证所有 TSF 数据的完整性，还是仅验证所选 TSF 数据的完整性。

J.14.2.3.4 赋值

在 FPT_TST.1.2 中，如果选择了“TSF 的部分数据”，PP/ST 作者应规定将要被验证完整性的 TSF 数据列表。

附 录 K
（规范性附录）
FRU 类：资源利用

本类提供三个族以支持所需资源的可用性，诸如处理能力或存储容量。“容错”族提供保护以防止由 TOE 失效引起的能力不可用。“服务优先级”族确保资源将被分配到更重要的或时间要求更苛刻的任务中，而且不能被优先级低的任务所独占。“资源分配”族提供可用资源的使用限制，从而防止用户独占资源。

本类的组件构成分解如图 K.1 所示。

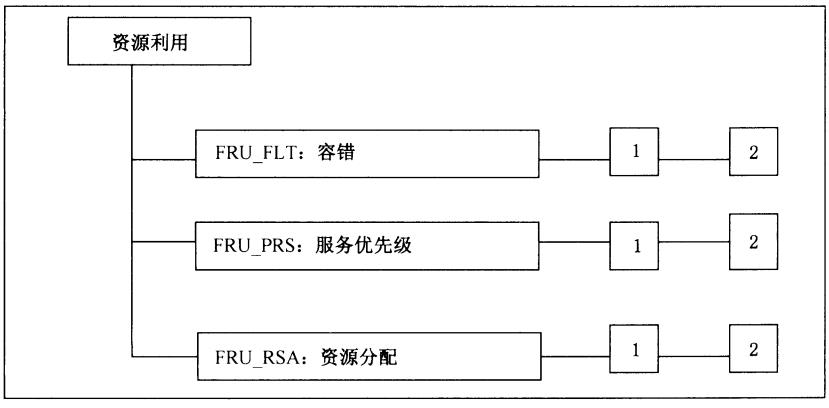

图 K.1 资源利用类分解

K.1 容错（FRU_FLT）

K.1.1 用户注释

本族提出了即便失效情况发生时也要保证能力可用性的这些要求。失效的例子有电力中断、硬件故障、软件错误。一旦发生这些错误，按本族要求，TOE 将维持指定的能力。例如，PP/ST 作者可能规定，在供电或通信失效时，用于一个核工厂的 TOE 将继续执行关机程序。

因为如果 SFR 是强制执行的，TOE 只能继续它的正确操作，这样就要求系统必须在失效发生后保持一个安全状态。这种能力由 FPT_FLS.1“失效即保持安全状态”提供。

容错机制可以是主动的，也可以是被动的。如果是主动机制，特定的功能在错误发生时将被激活。例如，火警就是一种主动机制：TSF 将监测火情并能采取措施，如切换至备份操作。在被动方案中，TOE 的架构使其能够处理错误。例如，一个带多个处理器的多数表决方案就是一个被动的解决办法：一个处理器的失效并不会扰乱整个 TOE 的运行（尽管也需要检测这种情况以便纠错）。

对于本族，失效的发生是偶然的（如洪灾或错拨设备）还是有意的（如独占）并不重要。

K.1.2 FRU_FLT.1 降级容错

K.1.2.1 用户应用注释

本组件详细说明了在系统失效后 TOE 仍将提供的能力。由于难以描述所有的特定失效情况，所以可按失效类别进行描述。例如，一般的失效情况有：计算机房进水、电力短暂中断、CPU 或主机的崩溃、软件错误或缓冲区溢出等。

K.1.2.2 操作

K.1.2.2.1 赋值

在 FRU_FLT.1.1 中，PP/ST 作者应规定在某个特定的失效发生期间或发生之后，TOE 将保持的能力列表。

在 FRU_FLT.1.1 中，PP/ST 作者应规定一个失效类型列表，对 TOE 必须加以明确保护以防止这些失效。如果列表中的一种失效发生，TOE 仍能继续运行。

K.1.3 FRU_FLT.2 受限容错

K.1.3.1 用户应用注释

本组件规定 TOE 必须抵抗的失效类型。由于难以描述所有的特定失效情况，所以可按失效类别进行描述。例如，一般的失效情况有：计算机房进水、电力短暂中断、CPU 或主机的崩溃、软件错误或缓冲区溢出等。

K.1.3.2 操作

K.1.3.2.1 赋值

在 FRU_FLT.2.1 中，PP/ST 作者应规定一个失效类型列表，对 TOE 必须加以明确保护以防止这些失效。如果列表中的一种失效发生，TOE 仍能继续运行。

K.2 服务优先级(FRU_PRS)

K.2.1 用户注释

本族的要求允许 TSF 控制用户和主体使用 TSF 所支配的资源，以便 TSF 控制下的高优先级活动总能成功完成而不会受到低优先级活动的干扰和延迟。换句话说，时间紧要程度高的任务不会被时间紧要程度低的任务耽搁。

本族可应用于几种不同类型的资源，如处理能力、通信信道容量。

“服务优先级”机制可以是被动的，也可以是主动的。在一个被动的服务优先级系统中，对两个等待中的应用作选择时，系统会选择具有最高优先级的任务。使用被动服务优先级机制时，一个正在运行的低优先级的任务不会被另一个高优先级的任务打断。而当使用主动服务优先机制时，低优先级的任务则有可能被新的高优先级的任务打断。

审计要求规定所有拒绝的原因都应被审计。有关一个操作不被拒绝而只是延缓执行的问题留给开发者去考虑。

K.2.2 FRU_PRS.1 有限服务优先级

K.2.2.1 用户应用注释

本组件定义了一个主体的优先级，以及使用这一优先级的资源。如果一个主体打算对由服务优先级要求控制的一个资源采取动作，那么其访问或访问时间将取决于该主体的优先级、当前活动的主体的优先级和仍在队列中的主体的优先级。

K.2.2.2 操作

K.2.2.2.1 赋值

在 FRU_PRS.1.2 中，PP/ST 作者应规定 TSF 为之实施服务优先级的受控资源列表（诸如进程、磁盘空间、内存、带宽等资源）。

K.2.3 FRU_PRS.2 全部服务优先级

K.2.3.1 用户应用注释

本组件定义一个主体的优先级。TSF 中所有可共享资源都服从服务优先级机制。如果一个主体打算对一个可共享的 TSF 资源采取动作，那么其访问或访问时间将取决于该主体的优先级、当前活动的主体的优先级和仍在队列中的主体的优先级。

K.3 资源分配(FPR_RSA)

K.3.1 用户注释

本族的要求允许 TSF 控制用户和主体使用 TSF 所支配的资源，使得通过其他用户或主体垄断资源而导致的未授权拒绝服务的情况不会发生。

资源分配规则允许通过建立配额或其他方式来定义为特定用户或主体分配的资源空间或时间量的限度。例如，这些规则可以：

——规定客体配额，限制某一特定用户可以分配的客体数量或大小。

——控制预先指定资源单位的分配/取消分配，这些单位受 TSF 的控制。

一般来讲，这些功能将通过使用赋给用户和资源的属性来实现。

这些组件的目的是为了在用户和主体间保证一定的公平（如单个的用户不能分配所有的可用空间）。由于资源的分配常常超出了一个主体的生命期（即文件通常比产生它们的应用存在的时间更长），并且同一用户对主体的多个实例化不应对其他用户产生太多的负面影响，这些组件允许分配限值与用户相关。有些情况下，资源是按主体来分配的（如主内存或 CPU 周期），在那些实例中，这些组件允许资源在主体层面上进行分配。

本族的重点在对资源分配提出要求，而没有对资源本身的使用提出要求。因而审计要求也适用于资源的分配，而不是资源的使用。

K.3.2 FRU_RSA.1 最高配额

K.3.2.1 用户应用注释

本组件对仅应用于 TOE 中一组特定的可共享资源的配额机制提出了要求。这些要求允许配额关联一个用户，或者如适用于 TOE 一样可以赋给用户组或主体。

K.3.2.2 操作

K.3.2.2.1 赋值

在 FRU_RSA.1.1 中，PP/ST 作者应规定需要最大资源分配限值的受控资源列表（如进程、磁盘空间、内存、带宽）。如果 TSF 中的所有资源都需包括在内的话，那么可规定为“所有 TSF 资源”。

K.3.2.2.2 选择

在 FRU_RSA.1.1 中，PP/ST 作者应选择是将最高配额应用给单个用户，预定义的用户组、主体，还是应用给他们的任何组合。

在 FRU_RSA.1.1 中，PP/ST 作者应选择最高配额是在任何给定时间（同时）都可使用，还是在某一规定的时间间隔内可使用。

K.3.3 FRU_RSA.2 最低和最高配额

K.3.3.1 用户应用注释

本组件对仅应用于 TOE 中的一组特定的可共享资源的配额机制提出了要求。这些要求允许配额关联一个用户，或者如适用于 TOE 一样可能赋给用户组。

K.3.3.2 操作

K.3.3.2.1 赋值

在 FRU_RSA.2.1 中，PP/ST 作者应规定需要最大和最小资源分配限值的受控资源列表（如进程、磁盘空间、内存、带宽）。如果 TSF 中的所有资源都需包括在内的话，那么可规定为“所有 TSF 资源”。

K.3.3.2.2 选择

在 FRU_RSA.2.1 中，PP/ST 作者应选择是将最高配额应用给单个用户，预定义的用户组、主体，还是应用给它们的任何组合。

在 FRU_RSA.2.1 中，PP/ST 作者应选择最高配额是在任何给定时间（同时）都可使用，还是在某一规定的时间间隔内可使用。

K.3.3.2.3 赋值

在 FRU_RSA.2.2 中，PP/ST 作者应规定需要对其最小分配限值进行设定的受控资源（例如进程、磁盘空间、内存、带宽）。如果 TSF 中的所有资源都需包括在内的话，则可规定为“所有 TSF 资源”。

K.3.3.2.4 选择

在 FRU_RSA.2.2 中，PP/ST 作者应选择是将最低配额应用给单个用户，预定义的用户组，主体，还是到它们的任何组合上。

在 FRU_RSA.2.2 中，PP/ST 作者应选择最低配额是在任何给定时间（同时）都可使用，还是在某一规定的时间间隔内可使用。

附 录 L
（规范性附录）
FTA 类:TOE 访问

用户会话的建立通常包括一个或多个主体的创建,这个(些)主体在 TOE 中代表用户执行操作。在会话建立过程的最后,倘若 TOE 的访问要求都已满足,所创建的主体则具有由标识和鉴别功能确定的属性。本族规定了控制一个用户会话的建立的功能要求。

一个用户会话被定义为一个周期,它开始于标识/鉴别时间,更恰当地说是开始于用户和系统之间进行交互时,止于所有与会话相关的主体(资源和属性)都已被释放的那一刻。

图 L.1 给出了本类具体组件的分解情况。

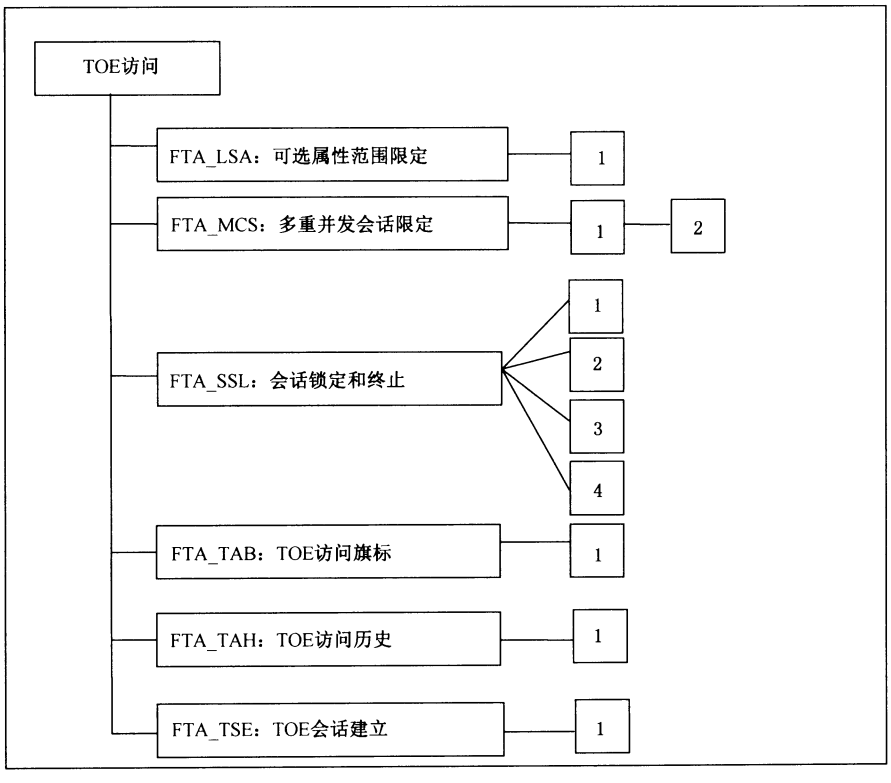

图 L.1 TOE 访问类分解

L.1 可选属性范围限定(FTA_LSA)

L.1.1 用户注释

本族定义了一些要求,这些要求将限制一个用户可能选择的会话安全属性和一个用户可能被绑定到的主体,这些限定取决于:访问方法、访问的位置或端口、时间(如一日的某时、一周的某天)。

本族使 PP/ST 作者能为 TSF 规定一些要求,以基于环境条件对授权用户的安全属性域设置限制。例如,可允许一个用户在正常的工作时间内建立一个“秘密会话”,但在除此之外的时间里该用户就可能会受到约束,只能建立“非保密会话”。可选属性域的相关约束标识可用选择操作来完成。这些限定可按逐个属性来应用。当需要规定对多个属性的限定时,这一组件就必须被复制到每一属性上。可用于

限制会话安全属性的属性例子有：

a) 访问方法可用于规定用户将在何种环境下工作(如文件传送协议、终端、vtam)；

b) 访问位置可用于限定基于用户访问位置或访问端口的用户可选属性域。这种能力主要用于使用拨号设备或网络设备的环境中；

c) 访问时间可用来限定一个用户可选属性域。例如，时间范围可基于一日的某些时间、一周的某些天或日历日期。这一限定提供了一些操作性的保护，以防止用户行为在未实施正确的监测或正确的程序性措施时就能发生。

L.1.2 FAT_LSA.1 可选属性范围限定

L.1.2.1 操作

L.1.2.1.1 赋值

在 FTA_LSA.1.1 中，PP/ST 作者应规定要受到限制的会话安全属性集。这些会话安全属性的例子有用户许可级别、完整性级别和角色。

在 FTA_LSA.1.1 中，PP/ST 作者应规定可用于确定会话安全属性范围的属性集，这些属性的例子有用户身份、原发地点、访问时间和访问方法。

L.2 多重并发会话限制(FTA_MCS)

L.2.1 用户注释

本族定义了一个用户在同一时间可以拥有多少个会话(并发会话)。并发会话数也可为一组用户或为每一个单独用户设置。

L.2.2 FTA_MCS.1 多重并发会话的基本限制

L.2.2.1 用户应用注释

本组件允许系统限制会话数以便有效地使用 TOE 的资源。

L.2.2.2 操作

L.2.2.2.1 赋值

在 FTA_MCS.1.2 中，PP/ST 作者应规定可使用的最大并发会话数的默认值。

L.2.3 FTA_MCS.2 基于每个用户属性的多重并发会话限制

L.2.3.1 用户应用注释

本组件通过允许对用户可调用的并发会话数进行更进一步的限定，提供了超出 FTA_MCS.1“多重并发会话的基本限制”的额外能力。这些限定与用户安全属性相关，如用户的身份或某个角色的成员资格。

L.2.3.2 操作

L.2.3.2.1 赋值

在 FTA_MCS.2.1 中，PP/ST 作者应规定确定最大并发会话数的规则。一个规则的例子是“如果用户的分类级别为‘秘密的’，则最大并发会话数为 1，否则为 5”。

在 FTA_MCS.2.2 中，PP/ST 作者应规定可使用的最大并发会话数的默认值。

L.3 会话锁定和终止(FTA_SSL)

L.3.1 用户注释

本族为 TSF 定义了一些要求，以为交互式会话提供锁定、解锁、终止能力。

当一个用户直接与 TOE 中的主体进行交互(交互会话)时，用户的终端在无人照管的情况下很容易受到攻击。本族为 TSF 提供了一些要求，在规定时间内不活动时，锁定终端或终止会话，并要求用户可以发起终端的锁定行为。为了重新激活终端，必须发生由 PP/ST 作者规定的一个事件，如用户再次鉴别。

如果一个用户在一段时间内没有向 TOE 提供任何刺激，则认为该用户是非活动的。

PP/ST 作者应考虑是否应该把 FTP_TRP.1“可信路径”包括进去。那样的话，“会话锁定”功能应包括在 FTP_TRP.1“可信路径”的操作中。

L.3.2 FTA_SSL.1 TSF 原发会话锁定

L.3.2.1 用户应用注释

FTA_SSL.1“TSF 原发会话锁定”为 TSF 提供了在规定的一段时间后锁定一个活动的用户会话的能力。锁定一个终端可防止通过使用被锁定终端与现有活动会话进行任何进一步的交互。

如果覆写显示设备，则替代内容不必是静态的(即允许“屏幕保护”)。

本组件允许 PP/ST 作者规定何种事件将解锁会话。这些事件可能与终端(如用固定的一组按键来解锁会话)、用户(如重鉴别)或时间有关。

L.3.2.2 操作

L.3.2.2.1 赋值

在 FTA_SSL.1.1 中，PP/ST 作者应规定将触发交互式会话锁定的用户不活动时间间隔。如果期望这样，PP/ST 作者可通过赋值规定这一时间间隔的设置是留给授权管理者还是用户。FMT 类中的管理功能可规定修改这一时间间隔或将其设为默认值的能力。

在 FTA_SSL.1.2 中，PP/ST 作者应规定解锁会话之前应发生的事件。例如这一事件可能是“用户重鉴别”或“用户输入解锁按键序列”。

L.3.3 FTA_SSL.2 用户原发锁定

L.3.3.1 用户应用注释

FTA_SSL.2“用户原发锁定”为授权用户提供了锁定和解锁自身交互会话的能力。这使得授权用户具备无需终止活动的会话就能有效地阻止活动会话继续保持的能力。

如果设备被改写，则替代内容不必是静态的(即允许“屏幕保护”)。

L.3.3.2 操作

L.3.3.2.1 赋值

在 FTA_SSL.2.2 中，PP/ST 作者应规定解锁会话之前应发生的事件。例如这一事件可能是“用户重鉴别”或“用户输入解锁按键序列”。

L.3.4 FTA_SSL.3 TSF 原发终止

L.3.4.1 用户应用注释

FTA_SSL.3 “TSF 原发终止”要求 TSF 在用户一段时间不活动后终止一个交互式用户会话。

PP/ST 作者应意识到，在用户终止其活动后，会话可能仍在继续，如后台处理。在用户一段时间不活动后，不管主体处于何种状态，本要求将终止该后台主体。

L.3.4.2 操作

L.3.4.2.1 赋值

在 FTA_SSL.3.1 中，PP/ST 作者应规定将触发交互式会话锁定用户不活动的时间间隔。如果期望这样，PP/ST 作者可通过赋值规定这一时间间隔的设置是留给授权管理者还是用户。FMT 类中的管理功能可规定修改这一时间间隔或将其设为默认值的能力。

L.3.5 FTA_SSL.4 用户原发终止

L.3.5.1 用户应用注释

FTA_SSL.4 “用户原发终止”为授权用户提供了终止自身交互会话的能力。

PP/ST 作者应注意到在用户终止自身行动后，其交互会话可能还在继续，例如：后台进程。本组件允许用户终止这个后台主体，而无需考虑这个主体的状态。

L.4 TOE 访问旗标（FTA_TAB）

L.4.1 用户注释

在标识和鉴别之前，TOE 访问要求为 TOE 提供了向潜在用户显示有关慎用 TOE 的一个劝告性警示信息的能力。

L.4.2 FTA_TAB.1 缺省的 TOE 访问旗标

L.4.2.1 用户应用注释

本组件要求对 TOE 的未经授权使用存在一个劝告性警示。PP/ST 作者可细化这一要求以包含一个缺省旗标。

L.5 TOE 访问历史（FTA_TAH）

L.5.1 用户注释

本族为 TSF 定义了一些要求，要求在与 TOE 成功地建立了会话后，向用户显示那些对该账户的不成功访问尝试的历史记录。这些历史记录包括日期、时间、访问方法、最后一次成功访问 TOE 的端口，以及已标识用户自上次成功访问以来企图访问这个 TOE 的未成功尝试次数。

L.5.2 FTA_TAH.1 TOE 访问历史

L.5.2.1 用户应用注释

本族可向授权用户提供可表明其用户账号可能被滥用的信息。

本组件要求向用户呈现这些信息。用户应能够审阅这些信息，但并不强制这么做。例如，如果一个用户不想审阅这些信息的话，他可以创建脚本以忽视这些信息并启动其他进程。

L.5.2.2 操作

L.5.2.2.1 选择

在FTA_TAH.1.1中，PP/ST作者应选择将在用户界面上显示的最近一次成功会话建立相关的安全属性，包括：日期、时间、访问方法（如FTP）或位置（如终端50）。

在FTA_TAH.1.2中，PP/ST作者应选择将在用户界面上显示的最近一次不成功会话建立相关的安全属性，包括：时间、日期、访问方法（如FTP）或位置（如终端50）。

L.6 TOE会话建立（FTA_TSE）

L.6.1 用户注释

本族定义了基于安全属性拒绝一个用户与TOE建立会话的要求，这些属性如：如访问位置或端口、用户安全属性（如用户身份、许可级别、完整性级别、一个角色中的成员）、时间范围（如一日的某时、一周的某天、日历日期）或这些参数的组合。

本族为PP/ST作者提供如下能力：可规定一些要求，要求TOE能限制一个授权用户与TOE建立会话的能力。相关限制的标识可用选择操作来完成。可用来规定会话建立限制的属性如：

a) 基于用户的访问位置，访问位置可用来限制一个用户与TOE建立一个活动会话的能力。这一能力尤其可用在使用拨号设备或网络设备的环境中。

b) 用户的安全属性可用来限制一个用户与TOE建立一个活动会话的能力。例如，这些属性将提供基于下述各项拒绝会话建立的能力：

- 用户身份；
- 用户许可级别；
- 用户完整性级别；
- 在一个角色中用户的成员资格。

这一能力尤其与授权或登录可发生在不同地点、TOE访问核查都要被执行的情形相关。

a) 基于时间范围，访问时间可用来限制一个用户与TOE建立活动会话的能力。例如，时间范围可基于一日的某些时间、一周的某些天或日历日期。这一限制提供了一些操作性的保护，防止一些动作在未实施正确的监测或正确的程序性措施时就能发生。

L.6.2 FTA_TSE.1 TOE会话建立

L.6.2.1 操作

L.6.2.2.1 赋值

在FTA_TSE.1.1中，PP/ST作者应规定可用于限制会话建立的属性。例如可能的属性有用户身份、原发地点（如非远程终端）、访问时间（如外部时间）或访问方法（如X-windows）。

附 录 M
（规范性附录）
FTP 类：可信路径/信道

用户经常需要直接与 TSF 进行交互来执行一些功能。一条可信路径提供了一种信任，即用户无论何时都可调用 TSF 直接与之通信。通过可信路径的用户响应确保那些不可信应用不能截取或修改用户的响应。同样，可信信道是在 TSF 和远程 IT 产品之间安全通信的一种方式。

缺少一条可信路径可能引起使用不可信应用的环境中的责任可追查性或访问控制的缺失。这些应用可截取用户私有的信息，如口令，并用它来冒名顶替其他用户。因而，对所有系统行为的职责都不能可靠地赋予一个可追查责任的实体。同样，这些应用可在可信用户的显示上输出错误信息，导致用户后来的动作是错误的，进而导致安全缺失。

图 M.1 给出了本类的组件的分解图。

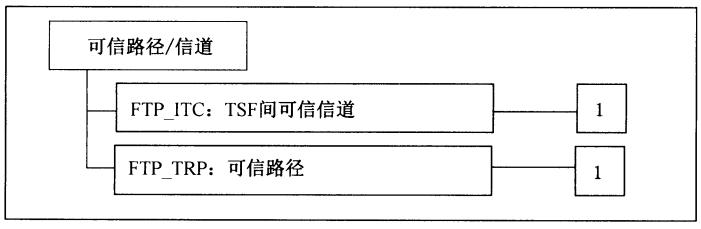

图 M.1 可信路径/信道类分解

M.1 TSF 间可信信道（FTP_ITC）

M.1.1 用户注释

本族定义了在 TSF 和其他可信 IT 产品之间为执行关键安全操作而创建可信信道连接的规则。关键安全操作的一个例子是，通过其功能是收集审计数据的可信产品传送数据，更新 TSF 鉴别数据库。

M.1.2 FTP_ITC.1 TSF 间可信信道

M.1.2.1 用户应用注释

在 TSF 和其他可信 IT 产品之间要求有可信通信信道的时候应使用这一组件。

M.1.2.2 操作

M.1.2.2.1 选择

在 FTP_ITC.1.2 中，PP/ST 作者必须规定是本地 TSF、另一个可信 IT 产品还是两者都具有初始化可信信道的能力。

M.1.2.2.2 赋值

在 FTP_ITC.1.3 中，PP/ST 作者应规定要求可信信道的功能。这些功能的例子可包括用户、主体或客体安全属性的传送，以及保持 TSF 数据的一致性。

M.2 可信路径(FTP_TRP)

M.2.1 用户注释

本族定义了建立和维护用户和 TSF 间的可信通信的要求。任何与安全相关的交互都可能要求有可信路径。可信路径交换可由用户在与 TSF 进行交互的时候初始化,TSF 也可通过可信路径与用户建立通信。

M.2.2 FTP_TRP.1 可信路径

M.2.2.1 用户应用注释

当需要在用户和 TSF 之间可信通信时,不管是为了原发鉴别,还是为了额外的特定用户操作,应使用本组件。

M.2.2.2 操作

M.2.2.2.1 选择

在 FTP_TRP.1.1 中,PP/ST 作者应规定可信路径是否必须扩展到远程或本地的用户。

在 FTP_TRP.1.1 中,PP/ST 作者应规定可信路径是否保护数据防止被修改、泄露和/或其他违反完整性或机密性事件。

M.2.2.2.2 赋值

在 FTP_TRP.1.1 中,PP/ST 作者应规定附加类型的违反可信信道保护的数据去完整性或机密性的事件。

M.2.2.2.3 选择

在 FTP_TRP.1.2 中,PP/ST 作者应规定 TSF、本地用户或远程用户是否能初始化可信路径。

在 FTP_TRP.1.3 中,PP/ST 作者应规定可信路径是否应被应用于原发用户鉴别或其他特定的服务。

M.2.2.2.4 赋值

在 FTP_TRP.1.3 中,如果选择了的话,PP/ST 作者应标识需要可信路径的其他服务(如果有的话)。

中华人民共和国
国家标准
信息技术 安全技术
信息技术安全评估准则
第2部分:安全功能组件
GB/T 18336.2—2015/ISO/IEC 15408-2:2008
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 12.5 字数 365 千字
2015年5月第一版 2015年5月第一次印刷
*
书号:155066·1-51489 定价 116.00 元

GB/T 18336.2-2015