分级文档编写指南

EAL3

版本：2.0

二〇〇八年八月

目　录

1 安全目标（ST）

一个ST包括特定的TOE的IT安全要求以及TOE提供的规定安全功能和保证措施，以满足所述的安全要求。

对一个TOE而言，ST是开发者、评估者、用户在TOE安全特性和评估范围之间达成一致的基础。一个ST读者不限于对TOE制造和评估负有责任，但可能负有管理、营销、购买、安装、配置、操作和使用TOE的责任。

ST应是一个面向用户使用的文档，应尽可能少地引用用户不易得到的其他材料。

申请者提供的文档《安全目标》编写方法详见 GB/Z 20283《信息安全技术 保护轮廓和安全目标产生指南》，本文档只作概要性的描述。

1.1 ST 引言

1.1.1 ST 标识

1）包括ST 标识信息，如：ST 标题、版本号、申请的保证级别、编写日期和作者；

2）包括此ST文档所描述的TOE 标识信息，如：TOE 名称、TOE 版本号。

1.1.2 ST 概述

1）概括ST的文档结构及所包含的内容；

2）概括介绍TOE 的类别、形态、主要组成、功能及应用环境。

1.1.3 一致性声明

包括编写此 ST 所依据的 PP（保护轮廓）的标识信息：版本号、名称和出版日期，如果编写 ST 未依据任何 PP 则此处为：依据国家标准《GB/T18336－2001 信息技术 安全技术 信息技术安全性评估准则》。

1.2 TOE 描述

TOE描述能为读者概要的了解产品或系统预期应用提供充分的信息，从而提供评估的背景。

1.2.1 产品类型

产品或系统类型及应用领域，如：防火墙、智能卡、加密调制解调器、Web服务器和企业内部网。

1.2.2 TOE 结构

TOE描述对构成TOE的硬件、固件和软件的组件和/或模块进行说明，详细介绍TOE 的组成，如：TOE由几个模块或子系统组成，每个模块或子系统的组成及其功能和TOE各个组成部分对运行环境的要求等，达到使读者对组件和/或模块概要性了解的目的。

1.2.3 TOE 的范围和边界

应该确定TOE描述涉及了信息技术，特别是TOE提供的安全特征，且详细到能够使读者对这些特征有一个概要了解的程度。如果TOE是其它产品的一部分，应充分描述TOE与其它产品之间的关系。

对于TOE边界的描述将告诉读者哪些属于TOE，哪些不属于TOE，如：TOE的日志存储功能需要依靠第三方数据库的支持，但数据库本身不属于TOE的范围，最好以图表加入描述语言的方式进行说明，TOE的边界描述包括：

1）物理范围和边界，详细介绍构成TOE 的硬件、软件和固件，并介绍TOE的配置；

2）逻辑范围和边界，描述TOE提供的IT安全功能。

根据TOE的应用领域，一般不属于TOE范围内的内容包括但不限于：

- 所有在已定义的TSF范围外的软件；
- 所有硬件；
- 系统运行所需的操作系统环境；
- 数据库应用系统；
- 底层系统提供的安全防护功能；
- 其它。

1.2.4 应用环境

描述TOE 的使用环境及在其中发挥的作用。

1.3 TOE 安全环境

1.3.1 假设

ST中对TOE预期使用的所有假设都应进行详细解释，以保证消费者能确定其预期使用环境与这些假设相符合。如果没有清楚理解这些假设，最终可能导致消费者在非希望的环境中使用TOE。

1）包括TOE 预期使用方面的假设，如TOE 预期应用、需要TOE 保护的资产的潜在价值、以及使用TOE 可能存在的限制；

2）包括为保证TOE 安全的行使功能，对TOE使用环境的物理、人员、连接性方面的假设：

a）物理方面，对TOE 的物理位置或附加外围设施做的假设；

例如：—假设管理员控制台严格限制在管理员个人范围内；

—假设TOE所有文件的存储只能在TOE运行的工作站上进行。

b）人员方面，对安全环境内的用户和TOE 管理员，或其他人员所作的假设；

例如：—假设用户具有特殊技能或专门技术；

—假设用户具有确定的最小权限；

—假设管理员每月更新防病毒数据库。

c）连接性方面，对TOE 与TOE 之外的IT 产品或系统相连的假设；

例如:—假设存储 TOE 产生的日志文件至少需要 100MB 的外部磁盘空间；

—TOE假设是在特定工作站上运行的唯一的非操作系统应用程序；

—假设TOE的软驱是禁用的；

—假设TOE不会连接到任何不可信的网络。

3）列出上述所有的假设（对假设进行标识并作出相应的解释）。

1.3.2 威胁

列出所有与TOE 安全运行相关的威胁(对威胁进行标识并作出相应的解释)。

威胁应通过已确定的威胁主体、攻击方式和作为攻击对象的资产来描述。威胁主体应通过诸如专门技术、可用资源和动机等来描述。攻击方式应通过诸如攻击方法、可利用的脆弱性和时机等来描述。

如果安全目的仅仅源于组织安全策略和假设，那么对威胁的描述可以省略。

1.3.3 组织安全策略

组织安全策略主要包括TOE 及其应用环境必须遵守的法律、法规、规定或指南。其遵循了TOE及其环境必须遵守的规则、惯例或指南，这些规则、惯例或指南是由控制TOE使用环境的组织制定的。例如，组织安全策略可能要求口令生成和加密应符合国家政府制定的标准。

ST中对每条组织安全策略都进行详细解释，以便读者能够清晰理解。

如果TOE 及其环境的安全目的只源于假设和威胁，那么ST中就可以不包含组织安全策略陈述。

1.4 安全目的

安全目的应该是对安全问题预期响应的简明陈述，换言之，在安全环境中已经陈述了安全需求，现在必须以安全目的的陈述形式明确界定出：安全需求是由TOE还是由环境来满足或处理的。应列出所有的安全目的：TOE 安全目的（由TOE实现的技术措施来满足）和环境安全目的（非IT手段来满足，例如：使用程序性的管理或运行规定），并对确定每个安全目的的理由作出详细的解释，安全目的最好独立于实现，应重点说明预计达到的结果而不是达到结果的方法。

应详细描述安全目的能够对应到前文中所述的所有威胁、组织安全策略和假设，这部分将在“1.8.1”以表格的形式做出说明。

1.5 IT 安全要求

该部分分为安全功能要求、安全保证要求和IT环境的安全要求，如果有对应的PP，这部分可直接按照PP 的相应部分来写，只需根据TOE具体实现情况完成PP中的各种组件操作（赋值、细化、反复、选择）。

如不具备相应的PP，则安全功能要求和安全保证要求按照下面的要求来提供：

1） 安全功能要求要指的是从GB/T18336－2001 第二部分功能要求组件中抽取的那些功能要求，应参照GB/T 18336-2001第二部分的规范语言进行描述（参照GB/Z 20283 8.2节）。

2） 安全保证要求主要指的是从GB/T18336－2001 第三部分保证要求组件中抽取的那些保证要求，对于该文档，应选取EAL3保证组件包内的组

件，应参照GB/T 18336-2001第三部分的规范语言进行描述（参照GB/Z 20283 8.2节）。

3） 组件的选择应满足GB/T 18336－2001中指出的依赖关系，允许有不满足依赖关系的情况出现，但应明确说明理由（建议除明确的特殊要求，选择组件时应满足依赖关系）。

4） 当GB/T18336－2001中的功能要求组件不足以表述TOE对安全功能和保证措施的要求时，允许附加两部分之外的组件，但应使用规范语言进行描述，且应明确说明附加的理由（建议除明确的特殊要求，不对组件进行附加）。

5） 该部分应明确陈述，且证明能够对应到每一个安全目的，这部分将在“1.8.2”以表格的形式做出说明。

如不具备相应的PP，则环境安全要求按照下面的要求来提供：

1）IT 环境安全要求包含IT 环境安全功能要求和IT 环境安全保证要求。这部分描述所有TOE需要满足但又不由TOE自身提供的安全要求，例如“TOE为防火墙产品，它依赖底层操作系统，操作系统提供管理员的身份认证和审计数据的永久储存。因此，IT 环境安全要求应包含FAU 类和FIA 类（参见GB/T18336 第二部分）的功能组件。

非 IT 环境安全要求是可选的部分，与 TOE 的实现没有直接关系，如果所有的安全目的均由上述几方面来对应，则该部分不要求。

1.6 TOE 概要规范

TOE 概要规范指的是TOE 安全要求的具体实现，TOE概要规范应定义TOE安全要求的实例化，该规范描述符合TOE安全要求的TOE安全功能和保证措施。TOE概要规范的目的是确定其是否为安全功能和安全保证措施提供了清晰完整的高层定义，该定义满足指定的TOE安全要求。应详细描述符合TOE 安全要求的TOE 安全功能和保证措施。

1) TOE 安全功能包含IT 安全功能，并说明这些功能是如何满足TOE 安全功能要求的。可以通过功能和要求间双向映射的方式来表达。

2）TOE 的保证措施应列出所有符合TOE 安全要求的保证措施，并说明这些保证措施是如何满足TOE 安全保证要求的。可以通过保证措施和要求间双向映射的方式来表达。

TOE概要规范编写应满足以下要求：

1）IT安全功能应以非形式化的方式定义，其详细程度应足够理解其含义。

2）ST中引用的所有安全机制应可追溯到相关的安全功能，这样就可看到每一个功能实现时使用的安全机制。

3）当AVA_SOF.1包括在TOE保证要求里时，应指明所有利用概率和变换机制（例如口令或散列函数）实现的IT安全功能。应提供所有这些功能的TOE安全功能强度分析。每一个指定功能的强度应确定并声明为基本级功能强度、中级功能强度、高级功能强度中的一个，或另选定义明确的特定级别。所提供的功能强度证据应足够评估者作出独立的判断，确认所声称的强度是足够和正确的。

安全功能强度的确定可参照下列要求：

1） 安全功能强度的特征：

——功能可以充分对抗低等攻击潜力者偶然的攻击；

——功能可以充分对抗中等攻击潜力者直接或故意发起的攻击；

——功能可以充分对抗高等攻击潜力者有周密计划或组织的攻击。

2） 强度级别的选择基于与威胁相关的下列方面：

——持续时间；

——经验；

——对TOE的了解；

——对TOE的访问方式；

——使用的设备。

一般要求 EAL3 级达到高级功能强度。

1.7 PP 声明

如果在 ST 引言中声称符合一个或多个 PP，本节应该介绍这些 PP，还应说明为满足 ST 要求，对 PP 进行的替代和附加项。注意不能声明只部分的满足 PP。如果没有声明符合 PP，则该部分可直接写为“直接依据 GB/T 18336-2001，不满足任何 PP”。

1.8 基本原理

1.8.1 安全目的基本原理

阐明安全目的能够映射到 TOE 安全环境里的所有方面：假设、威胁和组织安全策略：

1) 这些安全目的符合了列出的所有假设和组织安全策略的要求，能够对抗列出的所有威胁；

2) 所有安全目的都是必需的；

3) 可以通过安全目的和 TOE 安全环境（假设、威胁和组织安全策略）间双向映射的方式来表达。

1.8.2 安全要求基本原理

阐明 TOE 及其环境安全要求适于满足、并能够映射到安全目的：

1) TOE 及其安全环境的功能和保证要求组件能够满足列出的所有安全目的；

2) 所有 TOE 及其环境安全要求组件都是必需的；

3）是否满足组件之间的依赖关系，及不满足的理由；

3) 可以通过 TOE 及其环境安全要求和安全目的间双向映射的方式来表达；

4）应说明安全功能强度的声明是适当的。

1.8.3 TOE 概要规范基本原理

说明 TOE 安全功能和保证措施适于满足 TOE 安全要求：

1) TOE 安全功能能协同运作，满足 TOE 安全功能要求；

2) TOE 功能强度声明是有效的；

3) TOE 保证措施与保证要求相一致的声明是合理的；

4）概要规范能够映射到所有的安全功能要求。

1.8.4 PP 声明基本原理

解释 ST 安全目的和要求与所有声明一致的 PP 之间的区别。如果没有区别或已声明不符合任何 PP，则该部分可省略。

2 配置管理

该文档用来确保配置项被唯一标识，并确保开发者用于控制和跟踪 TOE 改变的程序是充分的，这包括应跟踪那些改变、潜在的改变如何体现等方面的详细信息。包括：配置管理能力和配置管理范围。

2.1 配置管理能力

配置管理能力是为了确定开发者是否清晰定义了 TOE 和它的相关配置项，以及改变这些配置项的能力是否被适当的控制。要求包括如下内容：

1）TOE 的唯一标识，包括名称、版本号。该标识无论是从 TOE 硬件、软件、包装还是文档上都应明确，且应统一及唯一。

2）包括一份配置清单，配置清单应包括与 TOE 设计相关的所有文档（如：需求分析、概要设计、详细设计、源代码、测试文档）及与分级评估相关的文档（如：ST、功能规范等等），要唯一标识出每个配置项的版本信息（如名称、版本号等），还要作出详尽的解释。

3）包括一份配置管理计划，配置管理计划应包括如何使用配置管理系统保持 TOE 配置项完整性的描述（包括人员授权、配置项的修改、并发处理等），如过程当中有相应记录产生，应同时提供。应包括配置管理系统记录及防止对配置项非授权访问的访问控制措施。

2.2 配置管理范围

配置管理范围是为了确定开发者是否至少按照 TOE 的实现表示、设计、用户和管理员指南、CM 文档即安全缺陷执行了配置管理，要求在配置管理系统中包括如下内容：

1)完成评估所需的所有文档，如 ST、功能规范等。

2）包括在 TOE 的整个生命周期中，对 TOE 的实现表示、设计、测试、测试工具（如适用）、用户和管理员指南、配置管理相关文档及安全缺陷等方面进行配置管理。

3）还应包括 TOE 整个生命周期中标识、跟踪每个配置项的方法和程序。包括：配置项的标识、分配、替代方法、各个阶段的命名方式及阶段之间同一配置项的对应关系、配置项之间的关联性等。

3 交付和运行

该文档用来判断程序文档是否齐全，以确保以开发者期望的方式安装、生成与启动 TOE，以及 TOE 在交付中不被修改。包括：交付文档、安装生成和启动程序。

3.1 交付

交付程序适用于整个 TOE，包括可用的软件、硬件、固件和文档；交付程序也适用于从生产环境到使用环境的整个交付过程的各个阶段，如：开发环境到测试环境、公司内部到最终用户。

应描述为保证 TOE 安全地提交给用户所需的所有交付程序，如：产品包装、密封、紧压安全带、公共邮政服务和私人传递等过程。

3.2 安装、生成和启动程序

TOE 所必需的所有安装、生成和启动步骤，包括：异常处理、最小系统需求等。

如果 TOE 在已经运行的情况下交付，则该部分可不进行描述。

4 开发类文档

该文档通过 TSF 设计文档的逐步完善的描述，来解释 TSF 是如何提供 TOE 的安全功能。设计文档包括功能规范、高层设计和表述对应性。

4.1 功能规范

本文档用来确认开发者对 TOE 安全功能是否作了充分描述，TOE 提供的安全功能是否足以满足 ST 的安全功能要求。

描述 TOE 安全功能和 TSF 外部的用户可见接口，通过该接口可以激活、调用安全功能及查看安全功能的状态。

描述外部接口处的异常和出错信息及 TOE 的处理方式。

TOE 安全功能描述应比 ST 中 TOE 概要规范的安全功能描述更详尽，且应以表格的形式描述该部分中各个功能与 ST 中 TOE 概要规范的对应关系，该对应关系可在该文档中提供，也可在“开发活动对应性分析文档”中描述。

4.2 高层设计

本文档用来确认高层设计是否以子系统的方式提供了对 TSF 的描述、对这些结构单元接口的描述，并且该高层设计是功能规范的正确实现。

描述 TSF 运行要求的所有硬件、固件和软件需求，应描述哪些功能是由底层硬件、固件、软件实现的。

描述 TSF 子系统间的接口及子系统外部可见接口。

适当描述子系统接口处的异常和出错信息。

TOE 高层设计应比概要规范的安全功能描述更详尽，且应以表格的形式描述该部分中各个子系统与功能规范中的安全功能的对应关系，该对应关系可在该文档中提供，也可在“开发活动对应性分析文档”中描述。

4.3 对应性分析文档

本子文档用以确认在实现表示中开发者是否正确、完整地实施了 ST、功能规范、高层设计的要求。如果对应性分析已经在功能规范、高层设计中进行了描述，则该部分可以省略，否则，应描述如下内容：

1）ST 中的 TOE 概要规范和功能规范之间的对应性分析

该对应性分析应该阐明 TOE 概要规范中的安全功能和功能规范中的安全功能描述之间的对应关系，以确认功能规范是 TOE 概要规范的完整的陈述。

2） 功能规范和高层设计之间的对应性分析

该对应性分析应该阐明 TOE 功能规范中的安全功能和高层设计中的子系统描述之间的对应关系，以确认高层设计是功能规范的完整的陈述。

5 指导性文档

该文档用以判断描述如何使用可操作的 TOE 的文档是否详尽，这些文档针对两类用户，一类是可信的管理员用户，他们的不正确行为可以影响 TOE 安全性，另一类是那些非管理员用户，他们的不正确行为可以影响其拥有的数据的安全性。如果文档在设计初期将两部分的描述合并在了一起，则此部分可提供一份文档，不用将一份文档刻意分为两份提交，但需在文档中以明确的标识加以注明。

5.1 管理员指南

应就管理员如何以安全方式管理 TOE 进行详细而全面地说明。必要时，文档中应包括对受控功能和特权的警告。

5.2 用户指南

应详细说明 TOE 安全功能和接口及有关 TOE 安全使用方面的信息。必要时，文档中应包括对用户可访问的功能和特权的警告。

6 测试相关文档

本文档的目的是确定 TOE 的行为是否与设计文档中的一样，并且与 ST 中 TOE 的安全功能要求说明一致。该文档包括测试文档本身、测试范围分析和测试深度分析。

6.1 功能测试

该文档应包括测试计划、测试方法、测试环境、测试工具、命令、测试步骤、预期测试结果和实际测试结果。

6.2 测试范围分析

阐明测试文档中列出的测试与功能规范是一致的。可采用表格或矩阵的形式来描述其对应关系。

6.3 测试深度分析

阐明测试文档中列出的测试与高层设计是一致的。可采用表格或矩阵的形式来描述高层设计和测试计划与过程之间的对应关系。此外，还应说明高层设计中的所有子系统和内部接口都进行了相应测试。

7 生命周期支持相关文档

本文档用以是确定开发者在 TOE 开发和维护期间使用程序的能力。这一过程是为了保护 TOE 及其相关的设计信息，以防他们受到干扰或暴露。开发过程中的干扰使故意引入脆弱性成为可能。而设计信息的暴露可能导致脆弱性更容易被人利用。

7.1 开发安全

开发安全文档是指开发者对开发环境的安全控制。

应包括在 TOE 的开发环境中用于保护 TOE 设计和实现过程的机密性与完整性的物理、过程、人员等方面安全措施。应提供过程应用过程中的文档证据。

8 脆弱性分析

该文档用于确定 TOE 在特定环境下的漏洞或脆弱性的存在及可利用性。包括误用分析、安全功能强度分析和脆弱性分析。

8.1 误用分析

确认指南性文档标识了所有可能的 TOE 操作方式，包括误操作、失败的操作可能的影响的描述。描述了所有用于 TOE 的安装和配置的必要操作。提供了足够的信息确认用户能有效的管理和使用 TOE 安全功能。

8.2 安全功能强度分析

以定性或定量的形式描述 ST 中所有与安全功能强度相关的机制。

8.3 脆弱性分析

需对 TOE 所有有关领域（如所有提交评估的文档和 TOE 本身等）进行分析，说明在预期使用环境中 TOE 是否存在明显可利用的脆弱性；如果有，应列出所有存在的明显脆弱性，并需明确说明该脆弱性对于 TOE 不构成威胁或是不能利用的。应描述利用脆弱性对 TOE 造成危害所需的时间、技术、对 TOE 的了解程度、对 TOE 的访问方式及使用的设备。