分级文档编写指南

EAL4

版本：3.0

2017 年 12 月

目　　录

1　安全目标（ST）..... 1
1.1　ST 引言 1
1.2　符合性声明..... 1
1.3　安全问题定义..... 2
1.4　安全目的..... 2
1.5　扩展组件定义..... 3
1.6　安全要求..... 3
1.7　TOE 概要规范 4
2　生命周期支持（ALC）..... 5
2.1　配置管理能力..... 5
2.2　TOE 配置管理覆盖 5
2.3　交付..... 5
2.4　开发安全..... 5
2.5　生命周期定义..... 5
2.6　工具和技术..... 5
3　开发类文档（ADV）..... 7
3.1　安全架构..... 7
3.2　功能规范..... 7
3.3　实现表示..... 7
3.4　TOE 设计 7
4　指导性文档（AGD）..... 8
4.1　操作用户指南..... 8
4.2　准备程序..... 8
5　测试相关文档（ATE）..... 9
5.1　功能测试..... 9
5.2　测试覆盖分析..... 9
5.3　测试深度分析..... 9

1 安全目标（ST）

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

1.1 ST 引言

1.1.1 ST 标识

ST标识信息，包括ST标题、版本号、申请的保障级别、编写日期和作者等。

1.1.2 TOE 标识

ST 文档所描述的 TOE 标识信息，包括 TOE 名称、TOE 版本号和发布日期等。

1.1.3 TOE 概述

1）概要描述 TOE 的用途和主要安全特征，以使潜在的用户能够快速了解此 TOE 是否满足他们的安全需求；

2）概述 TOE 的类型及应用领域，如：防火墙、智能卡、加密调制解调器、Web 服务器和企业内部网；

3）标识出 TOE 额外依赖的，但又不属于 TOE 组成部分的硬件、软件和固件。

1.1.4 TOE 描述

1）TOE 的物理范围：详细介绍构成 TOE 的硬件、软件、固件和指南文档，并介绍 TOE 的配置；

2）TOE 的逻辑范围：描述 TOE 提供的逻辑安全特征。

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 符合性声明

1）GB/T 18336 符合性声明：标识出 ST 和 TOE 遵从的 GB/T 18336 的版本，此处应为：依据国家标准 GB/T18336－2015《信息技术 安全技术 信息技术安全评估准则》；还应描述对 GB/T 18336.2 和 GB/T 18336.3 及其扩展部分的符合声明；

2）PP 和包符合性声明：标识 ST 遵从的所有 PP 和安全要求包，描述对包或是扩展包的符合声明。

3）符合性声明的基本原理：证实 TOE 类型、安全问题定义的陈述、安全目的陈述、安全要求的陈述与 PP 中相关陈述是相符的。

1.3 安全问题定义

明确的对 TOE 及其运行环境负责处理的安全问题进行定义。

1.3.1 资产

明确 TOE 安全策略保护的信息或资源，如密钥、口令、TOE 提供的安全服务等;以及被 TOE 所有者赋予了价值的 TOE 自身资产,如智能卡芯片的安全算法库。

1.3.2 威胁

列出所有 TOE 及其运行环境所抵抗的威胁，按照威胁主体、资产和敌对行为进行描述。威胁主体应通过诸如专门技术、可用资源和动机等来描述。资产与 1.3.1 节中相关描述相对应。敌对行为应通过诸如攻击方法、可利用的脆弱性和时机等来描述。

注：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。

注：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。

1.3.4 假设

ST 中对 TOE 运行环境所作的所有假设都应进行详细解释，如对 TOE 使用环境的物理、人员、连接性方面的假设，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以非安全的方式使用 TOE。

1.4 安全目的

1）安全目的的描述：安全目的应该是对安全问题预期反应的简明陈述，换言之，在安全问题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 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。

2）安全目的基本原理：

- 描述每一个 TOE 安全目的均可以追溯到安全目的所对抗的威胁及安全目的实施的组织安全策略；每一个运行环境安全目的，均可以追溯到安全目的所对抗的威胁、安全目的实施的组织安全策略和安全目的支持的假设。
- 应证实安全目的能抵抗所有威胁，应证实安全目的执行所有组织安全策略，运行环境安全目的支持所有的假设。

1.5 扩展组件定义

当 ST 中的安全要求不是基于 GB/T 18336 第二部分或第三部分的组件时，必须定义扩展组件。

扩展组件定义，具有如下要求：

- 对所有扩展的安全要求进行标识；
- 应为每一个扩展的安全要求定义一个扩展的组件；
- 描述每个扩展的组件与已有组件、族和类的关联性；
- 使用已有的组件、族、类和方法学作为陈述的模型；
- 应由可测量的和客观的元素组成，以便于证实这些元素之间的符合性或不符合性。

注：如果 ST 中不包括扩展组件，那么扩展组件定义一节可以省略。

1.6 安全要求

1）该部分内容应描述安全功能要求（SFR）和安全保障要求（SAR），通过以下方式对安全要求进行标识：

- 引用 GB/T18336－2015 第二部分和第三部分的要求组件；
- 引用 1.5 节中定义的扩展组件；
- 引用遵从的 PP 中的要求组件；
- 引用遵从的安全要求包。

2）应对安全功能要求和安全保障要求中使用的所有主体、客体、操作、安全属性、外部实体及其它术语进行定义；

3）应对安全要求的所有操作进行标识；

4）所有操作应被正确地执行，关于操作的指南可参考 GB/T18336-2015 第一部分附录 C；

5）应满足安全要求间的依赖关系，或者安全要求基本原理应论证不需要满足某个依赖关系；

6）安全要求基本原理应描述每一个安全功能要求可追溯至对应的 TOE 安全目的；

7）安全要求基本原理应证实安全功能要求可满足所有的 TOE 安全目的；

8）安全要求基本原理应说明选择安全保障要求的理由；

9）安全要求的陈述应是内在一致的。

1.7 TOE 概要规范

TOE 概要规范应描述 TOE 是如何满足每一项安全功能要求的。此部分内容要求高度概括地描述针对每一项安全功能要求，TOE 是如何满足的，内容要比 TOE 概述和 TOE 描述细化，且相互一致。

2 生命周期支持（ALC）

2.1 配置管理能力

要求包括如下内容：

1）TOE 应标记唯一参照号，使得用户在购买或使用 TOE 时能够识别 TOE。参照号可通过外包装上的标识码或软件启动显示的名称和版本号等形式标识。

2）包括 CM 文档，描述以下内容：

- CM 文档应描述用于唯一标识配置项的方法；
- 应包括 CM 计划，描述 CM 系统是如何应用于 TOE 的开发；CM 系统如何提供自动化的措施使得只能对配置项进行授权变更；CM 系统如何以自动化的方式支持 TOE 的生产；用来接受修改过的或新创建的作为 TOE 组成部分的配置项的程序。

2.2 TOE 配置管理覆盖

要求包括如下内容：

1)提供 TOE 配置项列表，包括 TOE 本身、安全保障要求的评估证据、TOE 的组成部分、实现表示和安全缺陷报告及其解决状态；

2）配置项列表应唯一标识配置项；

3）对于每一个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。

2.3 交付

交付文档要求描述以下内容：

1）提供文档描述 TOE 或其部分交付给消费者的交付程序；

2）在向消费者分发 TOE 版本时，用以维护安全性所必需的所有程序。

2.4 开发安全

开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的机密性和完整性所必需的所有物理的、程序的、人员的及其它方面的安全措施。

2.5 生命周期定义

生命周期定义文档要求描述以下内容：

1）用于开发和维护 TOE 的模型；

2）生命周期模型为 TOE 的开发和维护提供必要的控制。

2.6 工具和技术

开发工具文档要求描述一下内容：

1）应标识用于开发 TOE 的每个工具；

2）应无歧义地定义所有语句和实现用到的所有协定与命令的含义；

3）描述每个开发工具所选取的实现依赖选项，应无歧义地定义所有实现依赖选项的含义。

3 开发类文档（ADV）

3.1 安全架构

安全架构文档对 TOE 的自保护、域分离和不可旁路相关的安全属性以及 TSF 初始化相关内容进行描述。

安全架构的描述应与在 TOE 设计文档中对 SFR-执行的抽象描述的级别一致；应描述与安全功能要求一致的 TSF 安全域，说明活动实体只能按照安全规则使用自身控制的安全域中的资源，不允许使用安全域之外的其他资源；应描述 TSF 初始化过程为何是安全的,如上电或复位过程；应证实 TSF 可防止被破坏；应证实 TSF 可防止 SFR-执行的功能被旁路。

3.2 功能规范

文档应描述功能规范到安全功能要求的追溯。

功能规范应完全描述 TSF；应描述所有的 TSFI 的目的和使用方法；应识别和描述每个 TSFI（TSF 接口）相关的所有参数，包括所有的通过外部实体（或者位于 TSF 之外 TOE 内部的主体）向 TSF 提供数据、接收来自于 TSF 的数据并且调用 TSF 服务的方法；对于每个 SFR-执行 TSFI，功能规范应描述 TSFI 相关的所有行为；应描述可能由每个 TSFI 的调用而引起的所有直接错误消息；应证实安全功能要求到 TSFI 的追溯。

3.3 实现表示

需提供全部 TSF 的实现表示，应按详细级别定义 TSF，且详细程度达到无须进一步设计就能生成 TSF 的程度,可以包括软件代码、固件代码、硬件图表、IC 硬件设计代码或者设计数据等；应以开发人员使用的形式提供；TOE 设计描述与实现表示示例之间的映射应能证实它们的一致性。

3.4 TOE 设计

需提供对 TSF 详尽的描述以便确定是否实现了安全功能要求。

设计文档应根据子系统描述 TOE 的结构；应根据模块描述 TSF；应标识 TSF 的所有子系统;应描述每一个 TSF 子系统;应描述 TSF 所有子系统间的相互作用；应提供 TSF 子系统到 TSF 模块间的映射关系；应描述每一个 SFR-执行模块，包括它的目的及与其它模块间的相互作用；应描述每一个 SFR-执行模块，包括它的安全功能要求相关接口、其它接口的返回值、与其它模块间的相互作用及调用的接口；应描述每一个 SFR-支撑或 SFR-无关模块，包括它的目的及与其它模块间的相互作用;映射关系应论证实 TOE 设计中描述的所有行为能够映射到调用它的 TSFI。

4 指导性文档（AGD）

4.1 操作用户指南

操作用户指南是一种书面材料，计划被 TOE 评估配置中提到的所有类型的用户使用，这包括：最终用户、保证 TOE 以正确方式和最高安全方式运行的维护和管理人员、以及其他使用 TOE 外部接口的用户（如程序员）。操作用户指南描述 TSF 所提供的安全功能，提供说明和指南（包括警告），以帮助理解 TSF 及其安全使用所必须的关键信息和动作。容易误解的或者不合理的指南不应出现在指导性文档中，而运行的所有模式的安全程序则应该包括在其中，以便于检测不安全状态。

操作用户指南应对每一种用户角色进行描述，在安全处理环境中应被控制的用户可访问的功能和特权，包含适当的警示信息；应对每一种用户角色进行描述，怎样以安全的方式使用 TOE 提供的可用接口；应对每一种用户角色进行描述，可用功能和接口，尤其是受用户控制的所有安全参数，适当时应指明安全值；应对每一种用户角色明确说明，与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变 TSF 所控制实体的安全特性；应标识 TOE 运行的所有可能状态（包括操作导致的失败或者操作性错误），它们与维持安全运行之间的因果关系和联系；应对每一种用户角色进行描述，为了充分实现 ST 中描述的运行环境安全目的所必须执行的安全策略；操作用户指南内容应是明确和合理的。

4.2 准备程序

准备程序用于保证 TOE 以开发者预期的安全方式被接收和安装。要求为实现从 TOE 交付到使它进入初始运行环境的安全过渡做准备。准备程序应描述与开发者交付程序相一致的安全接收所交付 TOE 必需的所有步骤；应描述安全安装 TOE 以及安全准备与 ST 中描述的运行环境安全目的一致的运行环境所必需的所有步骤。

5 测试相关文档（ATE）

5.1 功能测试

测试文档应包括测试计划、预期的测试结果和实际的测试结果。

测试计划应标识要执行的测试并描述执行每个测试的方案，这些方案应包括对于其它测试结果的任何顺序依赖性。

预期的测试结果应指出测试成功执行后的预期输出。

实际的测试结果应和预期的测试结果一致。

5.2 测试覆盖分析

测试覆盖分析应证实测试文档中的测试与功能规范中 TSF 接口之间的对应性，测试覆盖分析应证实已经对功能规范中的所有 TSF 接口都进行了测试。可采用表格或矩阵的形式来描述其对应关系。

5.3 测试深度分析

深度测试分析应证实测试文档中的测试与 TOE 设计中的 TSF 子系统、SFR-执行模块之间的一致性，测试深度分析应证实 TOE 设计中的 SFR-执行模块都已经进行过测试。可采用表格或矩阵的形式来描述其对应关系。