分级文档编写指南

EAL1

版本：3.0

2017 年 12 月

目　　录

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 安全目的

陈述运行环境的安全目的。

1.4 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。

1.5 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 1.4 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）安全要求的陈述应是内在一致的。

1.6 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

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。

2.2 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 本身和安全保障要求的评估证据；

2）配置项列表应唯一标识配置项。

3 开发类文档（ADV）

3.1 功能规范

文档应描述功能规范到安全功能要求的追溯。

功能规范应描述每个 SFR-执行和 SFR-支撑的 TSFI 的目的和使用方法；应识别每个 SFR-执行和 SFR-支撑的 TSFI 相关的所有参数；应提供暗含的 SFR-无关的接口分类的基本原理；应证实安全功能要求到 TSFI 的追溯。

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。