ISCCC-QOG-0311-B/0

EAL1-EAL5级认证评估文档编写指南

中国信息安全认证中心 制

发布日期：二〇一七年八月十四日

目 录

适用范围

本文依据 GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》概述了作为 EAL1-EAL5 级评估基础的安全保障能力文档的强制性内容，为编制相关安全保障能力文档提供指南，对于安全保障能力文档的名称、形式不做限制。

1 评估保障级 1（EAL1）—功能测试

1.1 概述

EAL1适用于对（产品的）正确运行需要一定信心，但安全威胁又并不太被看重的场合。对于需要进行独立的保障评估来支持个人信息或类似信息已经得到适当保护的情况，EAL1具有一定的价值。

EAL1仅要求一个简化的ST。该ST只需简单地陈述TOE满足的安全功能要求，而不用通过从假设、威胁和组织安全策略，进而从安全目的来推导安全功能要求。

EAL1提供了一个对客户可用的TOE的评估，包括依据独立测试和对所提供的指导性文档的检查。

在这个级别上的评估应当提供这样的证据，即TOE的功能与其文档是一致的。

1.2 保障组件

EAL1提供了一种基本的保障级别来理解安全行为，该保障级别是在利用功能和接口规范以及指导性文档的基础上，通过分析一个部分ST中的安全功能要求而建立的。

这种分析是通过从公开领域搜索潜在脆弱性并开展TSF的独立测试（功能测试和穿透性测试）来获得支持的。

EAL1还通过TOE和相关评估文档的唯一标识来提供保障。

与未经评估的IT产品相比，本EAL在保障方面提供了有意义的增强。

表1 评估保障级 1

保障类	保障组件
ADV：开发	ADV_FSP.1 基本功能规范
AGD：指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC：生命周期支持	ALC_CMC.1 TOE标识
	ALC_CMS.1 TOE CM覆盖

保障类	保障组件
ASE：ST评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义（可选）
	ASE_INT.1 ST引言
	ASE_OBJ.1 运行环境安全目的
	ASE_REQ.1 陈述性的安全要求
	ASE_TSS.1 TOE概要规范
ATE：测试	ATE_IND.1 独立测试—符合性
AVA：脆弱性评定	AVA_VAN.1 脆弱性调查

1.3 安全保障能力文档

1.3.1 ST

ST 文档编写参见《EAL1-EAL5 级 ST 文档编写指南》

1.3.2 开发类文档

1.3.2.1 功能规范

功能规范文档用于对 SFR-执行和 SFR-支撑类型的 TSFI 进行高层描述；提供从 TOE 安全功能要求到 TSFI 的映射，目的是证实 TOE 提供的安全功能能够满足 ST 的安全功能要求，可采用表格的形式来描述其对应关系，具体要求如下：

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

1.3.3 指导性文档

1.3.3.1 操作用户指南

操作用户指南文档用来描述 TSF 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，具体要求如下：

1. 操作用户指南文档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；
2. 操作用户指南文档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；
3. 操作用户指南文档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；

4. 操作用户指南文档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；
5. 操作用户指南文档应标识 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；
6. 操作用户指南文档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；
7. 操作用户指南文档应是明确和合理的。

1.3.3.2 准备程序

准备程序文档用于保证 TOE 以开发者预期的安全方式被接收和安装，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，具体要求如下：

1. 准备程序文档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；
2. 准备程序文档应描述安全安装 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必需的所有步骤。

1.3.4 生命周期支持相关文档

1.3.4.1 配置管理文档

配置管理相关文档包括配置管理能力和配置管理范围两部分内容。

- 配置管理能力

本部分描述 TOE 唯一的参照号，以确保 TOE 实例在被评估时不会产生歧义。本部分具体要求如下：

1. 配置管理相关文档应描述 TOE 的唯一参照号。

- 配置管理范围

本部分列出 TOE 本身和安全保障要求的评估证据等配置项，以便于对 CM 系统下的配置项进行管理。本部分具体要求如下：

1. 配置项列表应包括：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。

1.3.5 脆弱性分析文档（如适用）

脆弱性分析文档用于给评估者提供脆弱性分析的相关证据，具体要求如下：

1. 脆弱性分析文档应在收集和分析 TOE 公开可用信息的基础上，描述 TOE 潜在的脆弱性。

2 评估保障级 2（EAL2）—结构测试

2.1 概述

EAL2需要开发者在交付设计信息和测试结果方面提供配合，除了要求其与良好的商业习惯一致外，不应要求开发方付出更多的努力。这样，就不需要增加过多的费用或时间投入。

EAL2适用于以下情况：在缺乏现成可用的完整的开发记录时，开发者或用户需要一种低到中等级别的安全性保障。这种情况可能出现在对遗留系统进行安全保护、或者不易联系到开发者的时候。

2.2 保障组件

EAL2在利用功能和接口规范、指导性文档和TOE结构的基本描述的基础上，通过分析一个完整的ST中的安全功能要求来提供保障，以理解安全行为。

这种分析由对TSF的独立测试、开发者基于功能规范文档进行测试的证据、对开发者测试结果的选择性独立确认、证实可抵御具有基本攻击潜力攻击者攻击的脆弱性分析（基于功能规范文档、TOE设计、安全架构描述和提供的指导性证据）等证据来支持。

EAL2还通过配置管理系统的使用和安全交付程序的证据来提供保障。

与EAL1相比，本EAL通过增加开发者测试、脆弱性分析（除了公开领域的搜索外）和基于更详细的TOE规范进行独立测试等内容，在保障方面提供了有意义的增强。

表2 评估保障级 2

保障类	保障组件
ADV：开发	ADV_ARC.1 安全架构描述
	ADV_FSP.2 安全执行功能规范
	ADV_TDS.1 基础设计
AGD：指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC：生命周期支持	ALC_CMC.2 CM系统的使用
	ALC_CMS.2 部分TOE CM覆盖

保障类	保障组件
	ALC_DEL.1 交付程序
ASE：ST评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义（可选）
	ASE_INT.1 ST引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导出的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE概要规范
ATE：测试	ATE_COV.1 覆盖证据
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试—抽样
AVA：脆弱性评定	AVA_VAN.2 脆弱性分析

2.3 安全保障能力文档

2.3.1 ST

ST 文档编写参见《EAL1-EAL5 级 ST 文档编写指南》

2.3.2 开发类文档

2.3.2.1 安全架构描述

安全架构描述文档用于描述 TSF 安全架构，包括自保护、域分离、不可旁路的原理，及用于 TSF 初始化的那部分 TOE 所支持的原理，并论证 TSF 的可靠性及如何满足所有安全功能要求，具体要求如下：

1. 安全架构描述文档应与在 TOE 设计文档中对 SFR-执行的抽象描述的级别一致；
2. 安全架构描述文档应描述与安全功能要求一致的 TSF 安全域；
3. 安全架构描述文档应描述 TSF 初始化过程为何是安全的；
4. 安全架构描述文档应证实 TSF 可防止被破坏；
5. 安全架构描述文档应证实 TSF 可防止 SFR-执行的功能被旁路。

2.3.2.2 功能规范

功能规范文档用于对所有 TSFI 进行高层描述；对于每个 SFR-执行 TSFI，描述 TSFI 相关的 SFR-执行行为和行为引起的相关直接错误消息；提供从 TOE 安全功能要求到 TSFI 的映射，目的是证实 TOE 提供的安全功能能够满足 ST 的安全功能要求，可采用表格的形式来描述其对应关系，具体要求如下：

1. 功能规范文档应完整地描述 TSF；

2. 功能规范文档应描述所有的 TSFI 的目的和使用方法；
3. 功能规范文档应识别和描述每个 TSFI 相关的所有参数；
4. 对于每个 SFR-执行 TSFI，功能规范文档应描述 TSFI 相关的 SFR-执行行为；
5. 对于 SFR-执行 TSFI，功能规范文档应描述由 SFR-执行行为相关处理而引起的直接错误消息；
6. 功能规范文档应证实安全功能要求到 TSFI 的追溯。

2.3.2.3 TOE 设计

TOE 设计文档用于描述 TOE 的基础设计，将子系统分为 SFR-执行、SFR-支撑、SFR-无关三类描述其行为及相互作用，并提供从功能规范文档的 TSFI 到 TOE 设计中的所有 TSF 子系统的映射，可采用表格的形式来描述其对应关系，具体要求如下：

1. TOE 设计文档应根据子系统描述 TOE 的结构；
2. TOE 设计文档应标识 TSF 的所有子系统；
3. TOE 设计文档应对每一个 SFR-支撑或 SFR-无关的 TSF 子系统的行为进行足够详细的描述，以确定它不是 SFR-执行；
4. TOE 设计文档应概括 SFR-执行子系统的 SFR-执行行为；
5. TOE 设计文档应描述 TSF 的 SFR-执行子系统间的相互作用和 TSF 的 SFR-执行子系统与其它 TSF 子系统间的相互作用；
6. 映射关系应证实 TOE 设计中描述的所有行为能够映射到调用它的 TSFI。

2.3.3 指导性文档

2.3.3.1 操作用户指南

操作用户指南文档用来描述 TSF 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，具体要求如下：

1. 操作用户指南文档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；
2. 操作用户指南文档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；

3. 操作用户指南文档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；
4. 操作用户指南文档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；
5. 操作用户指南文档应标识 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；
6. 操作用户指南文档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；
7. 操作用户指南文档应是明确和合理的。

2.3.3.2 准备程序

准备程序文档用于保证 TOE 以开发者预期的安全方式被接收和安装，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，具体要求如下：

1. 准备程序文档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；
2. 准备程序文档应描述安全安装 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必需的所有步骤。

2.3.4 生命周期支持相关文档

2.3.4.1 配置管理文档

配置管理相关文档包括配置管理能力和配置管理范围两部分内容。

- 配置管理能力

本部分描述 TOE 和配置项的标识，以确保 TOE 实例在被评估时不会产生歧义，使我们对 TOE 的组成有更清晰的理解，从而有助于确定哪些配置项满足 TOE 评估要求。本部分具体要求如下：

1. 配置管理相关文档应描述 TOE 的唯一参照号；
2. 配置管理相关文档应描述用于唯一标识配置项的方法。

- 配置管理范围

本部分描述 TOE 本身、TOE 的组成部分和安全保障要求所需的评估证据，以确保它们的修改是在一个带正确授权的受控方式下进行，具体要求如下：

1. 配置项列表应包括：TOE 本身、安全保障要求的评估证据和 TOE 的组成部分；
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。

2.3.4.2 交付程序

交付程序文档用于描述如何将完成的 TOE 从开发环境安全传递到负责接受的用户手中。交付要求需要详细说明系统控制、分发工具和程序等必要措施，确保在向用户分发 TOE 期间 TOE 的安全性得到维护，具体要求如下：

1. 交付程序文档应描述，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。

2.3.5 测试文档

2.3.5.1 测试范围分析

测试范围分析文档用于表明在功能测试文档中的测试如何与功能规范文档中的 TSF 接口对应，从而证实已经按照功能规范文档对 TSF 的一些接口进行了测试，可采用表格的形式来描述其对应关系，具体要求如下：

1. 测试范围分析文档应表明功能测试文档中的测试与功能规范文档中的 TSF 接口之间的对应性。

2.3.5.2 功能测试

功能测试文档用于对开发者执行的测试进行记录，应包括测试计划、测试环境、测试工具、命令、测试方法、测试步骤、预期的测试结果、实际的测试结果等，具体要求如下：

1. 功能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；
2. 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；
3. 预期的测试结果应指出测试成功执行后的预期输出；
4. 实际的测试结果应和预期的测试结果一致。

2.3.6 脆弱性分析文档（如适用）

脆弱性分析文档用于给评估者提供脆弱性分析的相关证据，具体要求如下：

1. 脆弱性分析文档应在执行 TOE 脆弱性分析的基础上，描述 TOE 潜在的脆弱性，在分析过程中使用指导性文档、功能规范文档、TOE 设计文档和安全架构描述文档。

3 评估保障级 3（EAL3）－系统地测试和检查

3.1 概述

EAL3可使负责任的开发者在设计阶段不需要对现有合理的开发实践作实质性变更，就能从正确的安全工程中获得最大限度的保障。

EAL3适用于以下情况：开发者或用户需要中等级别的安全性保障，同时要求在不进行大规模重建的情况下，对TOE及其开发过程进行彻底调查。

3.2 保障组件

EAL3在利用功能和接口规范、指导性文档和TOE的设计架构描述的基础上，通过分析一个完整的ST中的安全功能要求来提供保障，以理解安全行为。

这种分析由对TSF的独立测试、开发者基于功能规范文档和TOE设计进行测试的证据、对开发者测试结果的选择性独立确认、证实可抵御具有基本攻击潜力攻击者攻击的脆弱性分析（基于功能规范文档、TOE设计、安全架构描述和提供的指导性证据）等证据来支持。

EAL3还通过使用开发环境控制措施、TOE配置管理和安全交付程序的证据来提供保障。

与EAL2相比，本EAL通过增加覆盖安全功能的完备测试，以及提供在开发过程中TOE不会被篡改的信任机制和/或程序等内容，在保障方面提供了有意义的增强。

表3 评估保障级 3

保障类	保障组件
ADV：开发	ADV_ARC.1 安全架构描述
	ADV_FSP.3 带完整摘要的功能规范
	ADV_TDS.2 结构化设计
AGD：指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC：生命周期支持	ALC_CMC.3 授权控制
	ALC_CMS.3 实现表示CM覆盖

保障类	保障组件
	ALC_DEL.1 交付程序
	ALC_DVS.1 安全措施标识
	ALC_LCD.1 开发者定义的生命周期模型
ASE：ST评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义（可选）
	ASE_INT.1 ST引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导出的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE概要规范
ATE：测试	ATE_COV.2 覆盖分析
	ATE_DPT.1 测试：基本设计
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试—抽样
AVA：脆弱性评定	AVA_VAN.2 脆弱性分析

3.3 安全保障能力文档

3.3.1 ST

ST 文档编写参见《EAL1-EAL5 级 ST 文档编写指南》

3.3.2 开发类文档

3.3.2.1 安全架构描述

安全架构描述文档用于描述 TSF 安全架构，包括自保护、域分离、不可旁路的原理，及用于 TSF 初始化的那部分 TOE 所支持的原理，并论证 TSF 的可靠性及如何满足所有安全功能要求，具体要求如下：

1. 安全架构描述文档应与在 TOE 设计文档中对 SFR-执行的抽象描述的级别一致；
2. 安全架构描述文档应描述与安全功能要求一致的 TSF 安全域；
3. 安全架构描述文档应描述 TSF 初始化过程为何是安全的；
4. 安全架构描述文档应证实 TSF 可防止被破坏；
5. 安全架构描述文档应证实 TSF 可防止 SFR-执行的功能被旁路。

3.3.2.2 功能规范

功能规范文档用于对所有 TSFI 进行高层描述；对于每个 SFR-执行 TSFI，描述 TSFI 相关的 SFR-执行行为和特定的直接错误消息；提供足够的关于 SFR-支撑和 SFR-无关行为的信息，用以表明它们不是 SFR-执行的；提供从 TOE 安全功能

要求到 TSFI 的映射，目的是证实 TOE 提供的安全功能能够满足 ST 的安全功能要求，可采用表格的形式来描述其对应关系，具体要求如下：

1. 功能规范文档应完全描述 TSF；
2. 功能规范文档应描述所有的 TSFI 的目的和使用方法；
3. 功能规范文档应识别和描述每个 TSFI 相关的所有参数；
4. 对于每个 SFR-执行 TSFI，功能规范文档应描述 TSFI 相关的 SFR-执行行为；
5. 对于每个 SFR-执行 TSFI，功能规范文档应描述与 TSFI 的调用相关的安全实施行为和异常而引起的直接错误消息；
6. 功能规范文档需总结与每个 TSFI 相关的 SFR-支撑和 SFR-无关的行为；
7. 功能规范文档应证实安全功能要求到 TSFI 的追溯。

3.3.2.3 TOE 设计

TOE 设计文档用于描述 TOE 的结构化设计，将子系统分为 SFR-执行、SFR-支撑、SFR-无关三类描述其行为及相互作用，并提供 TOE 设计中的所有 TSF 子系统到功能规范文档的 TSFI 的映射，可采用表格的形式来描述其对应关系，具体要求如下：

1. TOE 设计文档应根据子系统描述 TOE 的结构；
2. TOE 设计文档应标识 TSF 的所有子系统；
3. TOE 设计文档应对每一个 TSF 的 SFR-无关子系统的行为进行足够详细的描述，以确定它是 SFR-无关；
4. TOE 设计文档应描述 SFR-执行子系统的 SFR-执行行为；
5. TOE 设计文档应概括 SFR-执行子系统的 SFR-支撑和 SFR-无关行为；
6. TOE 设计文档应概括 SFR-支撑子系统的行为；
7. TOE 设计文档应描述 TSF 所有子系统间的相互作用；
8. 映射关系应证实 TOE 设计中描述的所有行为能够映射到调用它的 TSFI。

3.3.3 指导性文档

3.3.3.1 操作用户指南

操作用户指南文档用来描述 TSF 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，具体要求如下：

1. 操作用户指南文档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；
2. 操作用户指南文档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；
3. 操作用户指南文档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；
4. 操作用户指南文档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；
5. 操作用户指南文档应标识 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；
6. 操作用户指南文档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；
7. 操作用户指南文档应是明确和合理的。

3.3.3.2 准备程序

准备程序文档用于保证 TOE 以开发者预期的安全方式被接收和安装，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，具体要求如下：

1. 准备程序文档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；
2. 准备程序文档应描述安全安装 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必需的所有步骤。

3.3.4 生命周期支持相关文档

3.3.4.1 配置管理文档

配置管理相关文档包括配置管理能力和配置管理范围两部分内容。

- 配置管理能力

本部分用于描述 TOE 和配置项的标识，以及 CM 系统对配置项的控制措施及在 TOE 开发过程中的应用，以确保 TOE 实例在被评估时不会产生歧义，并确保 CM 系统的正确使用，增强对配置项以受控方式进行维护的保障。本部分具体要求如下：

1. 配置管理相关文档应描述 TOE 的唯一参照号；
2. 配置管理相关文档应描述用于唯一标识配置项的方法；
3. 配置管理相关文档应描述只能对配置项进行授权修改的措施；
4. 配置管理相关文档应包括一个 CM 计划；
5. CM 计划应描述 CM 系统是如何应用于 TOE 的开发过程。

- 配置管理范围

本部分用于描述 TOE 本身、TOE 的组成部分、TOE 的实现表示和安全保障要求所需的评估证据，以确保它们的修改是在一个带正确授权的受控方式下进行。本部分具体要求如下：

1. 配置项列表应包括：TOE 本身、安全保障要求的评估证据、TOE 的组成部分和实现表示；
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。

3.3.4.2 交付程序

交付程序文档用于描述如何将完成的 TOE 从开发环境安全传递到负责接受的用户手中。交付要求需要详细说明系统控制、分发工具和程序等必要措施，确保在向用户分发 TOE 期间 TOE 的安全性得到维护，具体要求如下：

1. 交付程序文档应描述，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。

3.3.4.3 开发安全文档

开发安全文档用于描述物理的、程序的、人员的以及其它的为保护 TOE 或者其部分而在开发环境中采用的安全措施，包括开发场地的物理安全和任何用于选择开发人员的程序，具体要求如下：

1. 开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的保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。

3.3.4.4 生命周期定义

生命周期定义文档用于描述 TOE 开发和维护模型。尽早在 TOE 生命周期内建

立 TOE 开发和维护模型能够为 TOE 的开发和维护提供必要的控制，有助于 TOE 满足它的所有安全要求，应包括用于开发和维护 TOE 的程序、工具和技术，还应描述出控制程序应用的总体管理框架，具体要求如下：

1. 生命周期定义文档应描述用于开发和维护 TOE 的模型；
2. 生命周期模型应为 TOE 的开发和维护提供必要的控制。

3.3.5 测试文档

3.3.5.1 测试范围分析

测试范围分析文档用于表明在功能测试文档中的测试如何与功能规范文档中的 TSF 接口对应，从而证实已经按照功能规范文档对所有的 TSF 接口都进行了测试，可采用表格的形式来描述其对应关系，具体要求如下：

1. 测试范围分析文档应证实功能测试文档中的测试与功能规范文档中 TSF 接口之间的对应性；
2. 测试范围分析文档应证实已经对功能规范文档中的所有 TSF 接口都进行了测试。

3.3.5.2 测试深度分析文档

测试深度分析文档用于描述功能测试文档中的测试如何与 TOE 设计中 TSF 子系统对应，可采用表格的形式来描述其对应关系。在 TOE 子系统级别上进行测试，能保障 TSF 子系统的行为和交互，与 TOE 设计、安全架构描述是一致的，具体要求如下：

1. 测试深度分析文档应证实功能测试文档中的测试与 TOE 设计中 TSF 子系统之间的对应性；
2. 测试深度分析文档应证实 TOE 设计中的所有 TSF 子系统都已经进行过测试。

3.3.5.3 功能测试

功能测试文档用于对开发者执行的测试进行记录，应包括测试计划、测试环境、测试工具、命令、测试方法、测试步骤、预期的测试结果、实际的测试结果等，具体要求如下：

1. 功能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；

2. 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；
3. 预期的测试结果应指出测试成功执行后的预期输出；
4. 实际的测试结果应和预期的测试结果一致。

3.3.6 脆弱性分析文档（如适用）

脆弱性分析文档用于给评估者提供脆弱性分析的相关证据，具体要求如下::

1. 脆弱性分析文档应在执行 TOE 脆弱性分析的基础上，描述 TOE 潜在的脆弱性，在分析过程中使用指导性文档、功能规范文档、TOE 设计文档和安全架构描述文档。

4 评估保障级 4（EAL4）—系统地设计、测试和复查

4.1 概述

EAL4可使开发者基于良好的商业开发惯例，从正确的安全工程中获得最大限度的保障，虽然这种实践很严格，但并不需要大量的专业知识、技巧和其它资源。

EAL4适用于以下这些情况：开发者或用户在传统的商品化TOE中需要一个中等到高等级别的安全性保障，并准备负担额外的安全专用的工程费用。

4.2 保障组件

EAL4在利用功能和全部接口规范、指导性文档、TOE基本模块设计的描述和实现的子集的基础上，通过分析一个完整的ST中的安全功能要求来提供保障，以理解安全行为。

这种分析由对TOE安全功能的独立测试、开发者基于功能规范文档和TOE设计进行测试的证据、对开发者测试结果的选择性独立确认、证实可抵御具有增强型基本攻击潜力攻击者攻击的脆弱性分析（基于功能规范文档、TOE设计、实现表示、结构性设计和提供的指导性证据）等证据来支持。

EAL4还通过使用开发环境控制措施、包括配置管理自动化在内的更多的TOE配置管理措施和安全交付程序的证据来提供保障。

与EAL3相比，本EAL通过增加更多的设计描述、所有安全功能的实现表示，以及为在开发过程中TOE不会被篡改提供一定信任的改进机制和/或程序，在保障方面提供了有意义的增强。

表4 评估保障级 4

保障类	保障组件
ADV：开发	ADV_ARC.1 安全架构描述
	ADV_FSP.4 完备的功能规范
	ADV_IMP.1 TSF实现表示
	ADV_TDS.3 基础模块设计
AGD：指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC：生命周期支持	ALC_CMC.4 生产支持和接受程序及其自动化
	ALC_CMS.4 问题跟踪CM覆盖
	ALC_DEL.1 交付程序
	ALC_DVS.1 安全措施标识
	ALC_LCD.1 开发者定义的生命周期模型
	ALC_TAT.1 明确定义的开发工具
ASE：ST评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义（可选）
	ASE_INT.1 ST引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导出的安全要求
	ASE_SPD.1安全问题定义
	ASE_TSS.1 TOE概要规范
ATE：测试	ATE_COV.2 覆盖分析
	ATE_DPT.2 安全执行模块
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试—抽样
AVA：脆弱性评定	AVA_VAN.3 关注点脆弱性分析

4.3 安全保障能力文档

4.3.1 ST

ST 文档编写参见《EAL1-EAL5 级 ST 文档编写指南》

4.3.2 开发类文档

4.3.2.1 安全架构描述

安全架构描述文档用于描述 TSF 安全架构，包括自保护、域分离、不可旁路的原理，及用于 TSF 初始化的那部分 TOE 所支持的原理，并论证 TSF 的可靠性及如何满足所有安全功能要求，具体要求如下：

1. 安全架构描述文档应与在 TOE 设计文档中对 SFR-执行的抽象描述的级别一致；
2. 安全架构描述文档应描述与安全功能要求一致的 TSF 安全域；

3. 安全架构描述文档应描述 TSF 初始化过程为何是安全的；
4. 安全架构描述文档应证实 TSF 可防止被破坏；
5. 安全架构描述文档应证实 TSF 可防止 SFR-执行的功能被旁路。

4.3.2.2 功能规范

功能规范文档用于对所有 TSFI 进行高层描述；对于每个 SFR-执行 TSFI，应描述 TSFI 相关的所有行为和与 TSFI 调用相关的所有直接错误消息；提供从 TOE 安全功能要求到 TSFI 的映射，目的是证实 TOE 提供的安全功能能够满足 ST 的安全功能要求，可采用表格的形式来描述其对应关系，具体要求如下：

1. 功能规范文档应完全描述 TSF；
2. 功能规范文档应描述所有的 TSFI 的目的和使用方法；
3. 功能规范文档应识别和描述每个 TSFI 相关的所有参数；
4. 对于每个 SFR-执行 TSFI，功能规范文档应描述 TSFI 相关的所有行为；
5. 功能规范文档应描述可能由每个 TSFI 的调用而引起的所有直接错误消息；
6. 功能规范文档应证实安全功能要求到 TSFI 的追溯。

4.3.2.3 实现表示

实现表示文档以评估者能够分析的形式为全部 TSF 提供实现表示，并在实现表示和 TOE 设计描述之间建立映射，可采用表格的形式来描述其对应关系，具体要求如下：

1. 实现表示文档应按详细级别定义 TSF，且详细程度达到无须进一步设计就能生成 TSF 的程度；
2. 实现表示文档应以开发人员使用的形式提供；
3. 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。

4.3.2.4 TOE 设计

TOE 设计文档包括子系统设计（高层设计）和模块设计（低层设计）两部分内容。

- 子系统设计

本部分描述 TOE 的子系统设计，包括每一个 TSF 子系统及 TSF 所有子系统间的相互作用，提供所有 TSF 子系统到调用它的 TSFI 的映射，可采用表格的形式

来描述其对应关系。本部分具体要求如下：

1. TOE 设计文档应根据子系统描述 TOE 的结构；
2. TOE 设计文档应标识 TSF 的所有子系统；
3. TOE 设计文档应描述每一个 TSF 子系统；
4. TOE 设计文档应描述 TSF 所有子系统间的相互作用；
5. TOE 设计文档应描述所有 TSF 子系统到调用它的 TSFI 间的映射关系。

- 模块设计

本部分描述 TOE 的模块设计，将模块分为 SFR-执行、SFR-支撑、SFR-无关三类描述其目的、相互作用及行为，并提供所有 TSF 模块到对应的 TSFI 的映射及 TSF 子系统到 TSF 模块的映射，可采用表格的形式来描述其对应关系。本部分具体要求如下：

1. TOE 设计文档应根据模块描述 TSF；
2. TOE 设计文档应提供 TSF 子系统到 TSF 模块间的映射关系；
3. TOE 设计文档应描述每一个 SFR-执行模块，包括它的目的及与其他模块间的相互作用；
4. TOE 设计文档应描述每一个 SFR-执行模块，包括它的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
5. TOE 设计文档应描述每一个 SFR-支撑或 SFR-无关模块，包括它的目的及与其他模块间的相互作用；
6. TOE 设计文档应描述所有 TSF 模块到对应的 TSFI 间的映射关系。

4.3.3 指导性文档

4.3.3.1 操作用户指南

操作用户指南用来描述 TSF 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，具体要求如下：

1. 操作用户指南文档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；
2. 操作用户指南文档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；

3. 操作用户指南文档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；
4. 操作用户指南文档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；
5. 操作用户指南文档应标识 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；
6. 操作用户指南文档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；
7. 操作用户指南文档应是明确和合理的。

4.3.3.2 准备程序

准备程序文档用于保证 TOE 以开发者预期的安全方式被接收和安装，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，具体要求如下：

1. 准备程序文档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；
2. 准备程序文档应描述安全安装 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必需的所有步骤。

4.3.4 生命周期支持相关文档

4.3.4.1 配置管理文档

配置管理相关文档包括配置管理能力和配置管理范围两部分内容。

- 配置管理能力

本部分用于描述 TOE 和配置项的标识、CM 系统对配置项的控制措施和配置项变更程序、CM 系统在 TOE 开发过程中的应用、CM 系统如何以自动化的方式支持 TOE 的生产，以确保 TOE 实例在被评估时不会产生歧义，并确保 CM 系统的正确使用，增强对配置项以受控方式进行维护的保障。本部分具体要求如下：

1. 配置管理相关文档应描述 TOE 的唯一参照号；
2. 配置管理相关文档应描述用于唯一标识配置项的方法；
3. 配置管理相关文档应描述只能对配置项进行授权变更的自动化措施；
4. 配置管理相关文档应描述 CM 系统如何以自动化的方式支持 TOE 的生产；

5. 配置管理相关文档应包括 CM 计划；
6. CM 计划应描述 CM 系统是如何应用于 TOE 的开发的；
7. CM 计划应描述用来接受修改过的或新创建的作为 TOE 的组成部分的配置项的程序。

- 配置管理范围

本部分用于描述 TOE 本身、TOE 的组成部分、TOE 的实现表示、安全缺陷报告及其解决状态、安全保障要求所需的评估证据，以确保它们的修改是在一个带正确授权的受控方式下进行。本部分具体要求如下：

1. 配置项列表应包括：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。

4.3.4.2 交付程序

交付程序文档用于描述如何将完成的 TOE 从开发环境安全传递到负责接受的用户手中。交付要求需要详细说明系统控制、分发工具和程序等必要措施，确保在向用户分发 TOE 期间 TOE 的安全性得到维护，具体要求如下：

1. 交付程序文档应描述，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。

4.3.4.3 开发安全文档

开发安全文档用于描述物理的、程序的、人员的以及其它的为保护 TOE 或者其部分而在开发环境中采用的安全措施，包括开发场地的物理安全和任何用于选择开发人员的程序，具体要求如下：

1. 开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的保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。

4.3.4.4 生命周期定义

生命周期定义文档用于描述 TOE 开发和维护模型，尽早在 TOE 生命周期内建立 TOE 开发和维护模型能够为 TOE 的开发和维护提供必要的控制，有助于 TOE 满

足它的所有安全要求，应包括用于开发和维护 TOE 的程序、工具和技术，还应描述出控制程序应用的总体管理框架，具体要求如下：

1. 生命周期定义文档应描述用于开发和维护 TOE 的模型；
2. 生命周期模型应为 TOE 的开发和维护提供必要的控制。

4.3.4.5 开发工具和技术文档

开发工具和技术相关文档用于标识开发、分析和实现 TOE 的每个工具，并描述每个开发工具所选取的实现依赖选项，以防止将定义存在问题、不稳定或者不正确的开发工具用于开发 TOE，相关开发工具及配套文档的具体要求如下：

1. 用于实现的每个开发工具都应是明确定义的；
2. 开发工具和技术相关文档应无歧义地定义每个开发工具所有语句和实现用到的所有协定与命令的含义；
3. 开发工具和技术相关文档应无歧义地定义每个开发工具所有实现依赖选项的含义。

4.3.5 测试文档

4.3.5.1 测试范围分析

测试范围分析用于表明在功能测试文档中的测试如何与功能规范文档中的 TSF 接口对应,从而证实已经按照功能规范文档对所有的 TSF 接口都进行了测试，可采用表格的形式来描述其对应关系，具体要求如下：

1. 测试范围分析文档应证实功能测试文档中的测试与功能规范文档中 TSF 接口之间的对应性；
2. 测试范围分析文档应证实已经对功能规范文档中的所有 TSF 接口都进行了测试。

4.3.5.2 测试深度分析文档

测试深度分析文档用于描述功能测试文档中的测试如何与 TOE 设计中 TSF 子系统和 SFR-执行模块对应，可采用表格的形式来描述其对应关系。在此级别上进行测试，能保障 TSF 子系统和 SFR-执行模块的行为和交互，与 TOE 设计和安全架构描述中的描述是一致的，具体要求如下：

1. 测试深度分析文档应证实功能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；

2. 测试深度分析文档应证实 TOE 设计中的所有 TSF 子系统都已经进行过测试；
3. 测试深度分析文档应证实 TOE 设计中的 SFR-执行模块都已经进行过测试。

4.3.5.3 功能测试

功能测试文档用于对开发者执行的测试进行记录，应包括测试计划、测试环境、测试工具、命令、测试方法、测试步骤、预期的测试结果、实际的测试结果等，具体要求如下：

1. 功能测试应包括测试计划、预期的测试结果和实际的测试结果；
2. 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；
3. 预期的测试结果应指出测试成功执行后的预期输出；
4. 实际的测试结果应和预期的测试结果一致。

4.3.6 脆弱性分析文档（如适用）

脆弱性分析文档用于给评估者提供脆弱性分析的相关证据，具体要求如下：

1. 脆弱性分析文档应在执行 TOE 脆弱性分析的基础上，描述 TOE 潜在的脆弱性，在分析过程中使用指导性文档、功能规范文档、TOE 设计文档、安全架构描述文档和实现表示文档。

5 评估保障级 5 （EAL5） —半形式化设计和测试

5.1 概述

EAL5可使一个开发者从基于严格的商业开发实践的安全工程中获得最大限度的保障，而这种开发实践是靠专业安全工程技术的适度应用来支持的。设计和开发能够达到EAL5保障要求的TOE。

EAL5适用于以下这些情况：开发者或用户在一个有计划的开发过程中需要高级别独立的安全性保障，以及开发者或用户在未由于专业安全工程技术而导致不合理开销的条件下，需要有严格的开发手段。

5.2 保障组件

EAL5在利用功能和全部接口规范、指导性文档、TOE的设计描述和实现的基础上，通过分析一个完整的ST中的安全功能要求来提供保障，以理解安全行为。此外还需要模块化的TSF设计。

这种分析由TOE安全功能的独立测试，开发者基于功能规范文档、TOE设计进行测试的证据，对开发者测试结果的选择性独立确认，证实可抵御具有中等攻击潜力攻击者攻击的独立的脆弱性分析等证据来支持。

EAL5还通过使用开发环境控制措施、包括配置管理自动化在内的全面的TOE配置管理措施和安全交付程序的证据来提供保障。

与EAL4相比,本EAL通过增加半形式化的设计描述、具有可经受结构化分析的架构体系以及为在开发过程中TOE不会被篡改提供一定信任的改进机制和/或程序，在保障方面提供了有意义的增强。

表5 评估保障级 5

保障类	保障组件
ADV：开发	ADV_ARC.1 安全架构描述
	ADV_FSP.5 附加错误信息的完备的半形式化功能规范
	ADV_IMP.1 TSF实现表示
	ADV_INT.2 内部结构合理
	ADV_TDS.4 半形式化模块设计
AGD：指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC：生命周期支持	ALC_CMC.4 生产支持和接受程序及其自动化
	ALC_CMS.5 开发工具CM覆盖
	ALC_DEL.1 交付程序
	ALC_DVS.1 安全措施标识
	ALC_LCD.1 开发者定义的生命周期模型
	ALC_TAT.2 遵从实现标准
ASE：ST评估	ASE_CCL.1 符合性声明
	ASE_ECD.1 扩展组件定义（可选）
	ASE_INT.1 ST引言
	ASE_OBJ.2 安全目的
	ASE_REQ.2 推导出的安全要求
	ASE_SPD.1 安全问题定义
	ASE_TSS.1 TOE概要规范
ATE：测试	ATE_COV.2 覆盖分析
	ATE_DPT.3 测试：模块设计

保障类	保障组件
	ATE_FUN.1 功能测试
	ATE_IND.2 独立测试-抽样
AVA：脆弱性评定	AVA_VAN.4 系统的脆弱性分析

5.3 安全保障能力文档

5.3.1 ST

ST 文档编写参见《EAL1-EAL5 级 ST 文档编写指南》

5.3.2 开发类文档

5.3.2.1 安全架构描述

安全架构描述文档用于描述 TSF 安全架构，包括自保护、域分离、不可旁路的原理，及用于 TSF 初始化的那部分 TOE 所支持的原理，并论证 TSF 的可靠性及如何满足所有安全功能要求，具体要求如下：

1. 安全架构描述文档应与在 TOE 设计文档中对 SFR-执行的抽象描述的级别一致；
2. 安全架构描述文档应描述与安全功能要求一致的 TSF 安全域；
3. 安全架构描述文档应描述 TSF 初始化过程为何是安全的；
4. 安全架构描述文档应证实 TSF 可防止被破坏；
5. 安全架构描述文档应证实 TSF 可防止 SFR-执行的功能被旁路。

5.3.2.2 功能规范

功能规范文档采用半形式化方式描述 TSFI；对于每个 TSFI，应描述相关的所有行为和与调用相关的所有直接错误消息；提供足够的关于 SFR-支撑和 SFR-无关行为的信息，用以表明它们不是 SFR-执行的；提供从 TOE 安全功能要求到 TSFI 的映射，目的是证实 TOE 提供的安全功能能够满足 ST 的安全功能要求，可采用表格的形式来描述其对应关系，具体要求如下：

1. 功能规范文档应完全描述 TSF；
2. 功能规范文档应用半形式化方式描述 TSFI；
3. 功能规范文档应描述所有的 TSFI 的目的和使用方法；
4. 功能规范文档应识别和描述每个 TSFI 相关的所有参数；
5. 功能规范文档应描述每个 TSFI 相关的所有行为；
6. 功能规范文档应描述可能由每个 TSFI 的调用引起的所有直接错误消息；

7. 功能规范文档应描述不是由 TSFI 调用而引起的所有错误消息；
8. 功能规范文档应为每个包含在 TSF 实现中但不是由 TSFI 调用而引起的错误消息提供基本原理；
9. 功能规范文档应证实安全功能要求到 TSFI 的追溯。

5.3.2.3 实现表示

实现表示文档以评估者能够分析的形式为全部 TSF 提供实现表示，并在实现表示和 TOE 设计描述之间建立映射，可采用表格的形式来描述其对应关系，具体要求如下：

1. 实现表示文档应按详细级别定义 TSF，且详细程度达到无须进一步设计就能生成 TSF 的程度；
2. 实现表示文档应以开发人员使用的形式提供；
3. 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。

5.3.2.4 TSF 内部结构合理性论证

TSF 内部结构合理性论证相关文档用于描述整个 TSF 的内部结构并论证其合理性，提供了一种要求 TSF 结构合理的手段，目的是使用合理的工程原理设计和实现整个 TSF，具体要求如下：

1. 论证过程应描述用于判定“结构合理”的含义的特性；
2. TSF 内部描述应证实指定的整个 TSF 结构合理。

5.3.2.5 TOE 设计

TOE 设计文档包括子系统设计（高层设计）和模块设计（低层设计）两部分内容。

- 子系统设计

本部分描述 TOE 的子系统设计，包括每一个 TSF 子系统及 TSF 所有子系统间的相互作用，提供每一个 TSF 子系统的半形式化描述，并提供所有 TSF 子系统到调用它的 TSFI 的映射，可采用表格的形式来描述其对应关系。本部分具体要求如下：

1. TOE 设计文档应根据子系统描述 TOE 的结构；
2. TOE 设计文档应标识 TSF 的所有子系统；

3. TOE 设计文档应提供每一个 TSF 子系统的半形式化描述，适当时配以非形式化的、解释性的描述；
4. TOE 设计文档应描述 TSF 所有子系统间的相互作用；
5. TOE 设计文档应描述所有 TSF 子系统到调用它的 TSFI 间的映射关系。

- 模块设计

本部分描述 TOE 的模块设计，将模块分为 SFR-执行、SFR-支撑、SFR-无关三类描述其目的、相互作用及行为，并提供 TSF 模块到对应的 TSFI 的映射及 TSF 子系统到 TSF 模块的映射，可采用表格的形式来描述其对应关系。本部分具体要求如下：

1. TOE 设计文档应根据模块描述 TSF，以 SFR-执行、SFR-支撑或 SFR-无关标出每一个模块；
2. TOE 设计文档应提供 TSF 子系统到 TSF 模块间的映射关系；
3. TOE 设计文档应描述每一个 SFR-执行和 SFR-支撑模块，包括它的目的及与其他模块间的相互作用；
4. TOE 设计文档应描述每一个 SFR-执行和 SFR-支撑模块，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；
5. TOE 设计文档应描述每一个 SFR-支撑和 SFR-无关模块，包括它的目的及与其他模块间的相互作用；
6. TOE 设计文档应描述所有 TSF 模块到调用它的 TSFI 间的映射关系。

5.3.3 指导性文档

5.3.3.1 操作用户指南

操作用户指南文档用来描述 TSF 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，具体要求如下：

1. 操作用户指南文档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；
2. 操作用户指南文档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；

3. 操作用户指南文档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；
4. 操作用户指南文档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；
5. 操作用户指南文档应标识 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；
6. 操作用户指南文档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；
7. 操作用户指南文档应是明确和合理的。

5.3.3.2 准备程序

准备程序文档用于保证 TOE 以开发者预期的安全方式被接收和安装，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，具体要求如下：

1. 准备程序文档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；
2. 准备程序文档应描述安全安装 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必需的所有步骤。

5.3.4 生命周期支持相关文档

5.3.4.1 配置管理文档

配置管理相关文档包括配置管理能力和配置管理范围两部分内容。

- 配置管理能力

本部分描述 TOE 和配置项的标识、CM 系统对配置项的控制措施和配置项变更程序、CM 系统在 TOE 开发过程中的应用、CM 系统如何以自动化的方式支持 TOE 的生产，以确保 TOE 实例在被评估时不会产生歧义，并确保 CM 系统的正确使用，增强对配置项以受控方式进行维护的保障。本部分具体要求如下：

1. 配置管理相关文档应描述 TOE 的唯一参照号；
2. 配置管理相关文档应描述用于唯一标识配置项的方法；
3. 配置管理相关文档应描述只能对配置项进行授权变更的自动化措施；
4. 配置管理相关文档应描述 CM 系统如何以自动化的方式支持 TOE 的生产；

5. 配置管理相关文档应包括 CM 计划；
6. CM 计划应描述 CM 系统是如何应用于 TOE 的开发的；
7. CM 计划应描述用来接受修改过的或新创建的作为 TOE 的组成部分的配置项的程序。

- 配置管理范围

本部分用于描述 TOE 本身、TOE 的组成部分、TOE 的实现表示、安全缺陷报告及其解决状态、安全保障要求所需的评估证据、开发工具及其相关信息，以确保它们的修改是在一个带正确授权的受控方式下进行，有助于产生高质量的 TOE。本部分具体要求如下：

1. 配置项列表应包括：TOE 本身、安全保障要求的评估证据、TOE 的组成部分、实现表示、安全缺陷报告及其解决状态、开发工具及其相关信息；
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。

5.3.4.2 交付程序

交付程序文档用于描述如何将完成的 TOE 从开发环境安全传递到负责接受的用户手中。交付要求需要详细说明系统控制、分发工具和程序等必要措施，确保在向用户分发 TOE 期间 TOE 的安全性得到维护，具体要求如下：

1. 交付程序文档应描述，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。

5.3.4.3 开发安全文档

开发安全文档用于描述物理的、程序的、人员的以及其它的为保护 TOE 或者其部分而在开发环境中采用的安全措施，包括开发场地的物理安全和任何用于选择开发人员的程序，具体要求如下：

1. 开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的保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。

5.3.4.4 生命周期定义

开发者定义的生命周期模型相关文档用于描述 TOE 开发和维护模型，尽早在

TOE 生命周期内建立 TOE 开发和维护模型能够为 TOE 的开发和维护提供必要的控制，有助于 TOE 满足它的所有安全要求，应包括用于开发和维护 TOE 的程序、工具和技术，还应描述出控制程序应用的总体管理框架，具体要求如下：

1. 开发者定义的生命周期模型相关文档应描述用于开发和维护 TOE 的模型；
2. 生命周期模型应为 TOE 的开发和维护提供必要的控制。

5.3.4.5 开发工具和技术文档

开发工具和技术相关文档用于标识开发、分析和实现 TOE 的每个工具，描述每个开发工具所选取的实现依赖选项，并描述开发者所使用的实现标准，以防止将定义存在问题、不稳定或者不正确的开发工具用于开发 TOE,、本文档的具体要求如下：

1. 用于实现的每个开发工具都应是明确定义的；
2. 开发工具和技术相关文档应无歧义地定义每个开发工具所有语句的含义，以及实现用到的所有协定与指令；
3. 开发工具和技术相关文档应无歧义地定义每个开发工具所有实现依赖选项的含义。

5.3.5 测试文档

5.3.5.1 测试范围分析

测试范围分析文档用于表明在功能测试文档中的测试如何与功能规范文档中的 TSF 接口对应，从而证实已经按照功能规范文档对所有的 TSF 接口都进行了测试，可采用表格的形式来描述其对应关系，具体要求如下：

1. 测试范围分析文档应证实功能测试文档中的测试与功能规范文档中 TSF 接口之间的对应性；
2. 测试范围分析文档应证实已经对功能规范文档中的所有 TSF 接口都进行了测试。

5.3.5.2 测试深度分析

测试深度分析文档用于描述功能测试文档中的测试如何与 TOE 设计中 TSF 子系统和模块对应，可采用表格的形式来描述其对应关系。在此级别上进行测试，能保障 TSF 子系统和模块的行为和交互，与 TOE 设计和安全架构描述中的描述是

一致的，具体要求如下：

1. 测试深度分析文档应证实功能测试文档中的测试与 TOE 设计中的 TSF 子系统、模块之间的一致性；
2. 测试深度分析文档应证实 TOE 设计中的所有 TSF 子系统都已经进行过测试；
3. 测试深度分析文档应证实TOE设计中的所有TSF模块都已经进行过测试。

5.3.5.3 功能测试

功能测试文档用于对开发者执行的测试进行记录，应包括测试计划、测试环境、测试工具、命令、测试方法、测试步骤、预期的测试结果、实际的测试结果等，具体要求如下：

1. 功能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；
2. 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；
3. 预期的测试结果应指出测试成功执行后的预期输出；
4. 实际的测试结果应和预期的测试结果一致。

5.3.6 脆弱性分析文档（如适用）

脆弱性分析文档用于给评估者提供脆弱性分析的相关证据，具体要求如下：

1. 脆弱性分析文档应在针对 TOE 执行系统的脆弱性分析的基础上，描述 TOE 潜在的脆弱性，在分析过程中使用指导性文档、功能规范文档、TOE 设计文档、安全架构描述文档和实现表示文档。

附录 1：缩略语

EAL	Evaluation Assurance Level	评估保障级
ST	Security Target	安全目标
TOE	Target of Evaluation	评估对象
TSFI	TOE Security Functions Interface	TOE 安全功能接口
SFR	Security Functions Requirement	安全功能要求
TSF	TOE Security Functions	TOE 安全功能
CM	Configuration Management	配置管理
IT	Information Technology	信息技术