

产品安全保障能力要求 文档编写指南



中国网络安全审查技术与认证中心 制

发布日期：二〇一九年三月二十六

目 录

- 1 适用范围.....1
- 2 编写指南.....1
 - 2.1 开发类文档 1
 - 2.2 指导性文档 2
 - 2.3 测试相关文档 2
 - 2.4 脆弱性分析文档 3
 - 2.5 生命周期支持文档 3

1 适用范围

本指南旨在产品申请信息安全认证受理时,为委托人准备产品安全保障要求文档时提供编制参考。具体内容仍需根据产品的安全保障具体要求而定。

本指南主要对安全保障要求文档编制内容做出了说明,现以开发、生命周期支持、指导性文档、测试以及脆弱性分析为例。

考虑产品种类繁多,安全保障要求不尽相同,暂不对具体模板做要求,企业可以根据自己产品特点和风格准备。但是内容上一定按照产品的实际安全保障要求,并且在文档格式上要规范、清晰。

2 编写指南

2.1 开发类文档

这部分主要包括但不限于:安全架构、功能规范、产品设计等。开发类文档可以合并一个文档,也可以按照要求分别提供文档。

1、安全架构

安全架构文档应主要描述产品安全功能的安全架构,包括自保护、域分离、不可旁路的原理,具体要求如下:

- 描述与安全功能要求一致的产品安全功能的安全域。
- 描述产品安全功能初始化过程为何是安全的。
- 描述产品安全功能如何能够防止被破坏;
- 描述产安全功能能够防止安全特性被旁路;

2、功能规范

产品功能规范文档应提供完备的功能规范说明,具体要求如下:

- 应该充分描述认证产品的安全功能。
- 描述认证产品的安全功能以及安全功能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。
- 描述所有外部接口的用途与处理方法,适当时应提供所有的效果、例外情况和错误消息的全部细节。

3、产品设计

- 描述安全功能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。

- 描述安全功能子系统间的接口及子系统外部可见接口，以便于理解认证产品的预期运行。
- 描述安全功能所有子系统间的相互作用。

2.2 指导性文档

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认证产品安全性，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。

1、 管理员指南

应详细而全面地说明管理员如何以安全方式管理认证产品。必要时，文档中应包括对受控功能和特权的警告。这些操作可能影响安全策略的执行，需要管理员拥有特殊的权限。

管理员指南应标识并描述管理员安全接口与功能的用途、行为和相互关系。对每个管理员接口和功能，管理员指南应当：

- 描述调用接口的方法（如命令行、程序语言系统调用、菜单选择、命令按钮）；
- 描述由管理员设置的参数及其有效值、缺省值；
- 描述即时的安全功能响应、消息或返回代码。

2、用户指南

应详细说明安全功能和接口及有关认证产品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。

2.3 测试相关文档

本文档的目的是确定认证产品的行为是否与设计文档中的一样，并且与认证产品的安全功能要求说明一致。该文档包括但不限于测试文档本身、测试范围分析和测试深度分析。

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。

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。

2.4 脆弱性分析文档

该文档用于确定认证产品在特定环境下的漏洞或脆弱性的存在及可利用性。包括但不限于安全功能强度分析和脆弱性分析等。

1、安全功能强度分析

以定级或定量的形式描述所有与安全功能强度相关的机制。

2、脆弱性分析

应该对认证产品所有有关领域（如所有提交评估的文档和认证产品本身等）进行分析，说明在预期使用环境中认证产品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认证产品不构成威胁或是不能利用的。应描述利用脆弱性对认证产品造成危害所需的时间、技术、对认证产品的了解程度、对认证产品的访问方式及使用的设备。

2.5 生命周期支持文档

本文档用以是确定开发者在产品开发和维护期间使用程序的能力。这一过程是为了保护产品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。这部分文档主要包括但不限于开发安全、配置管理文档、交付说明文档等。

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。应包括在产品的开发环境中用于保护产品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。

2、配置管理文档

该文档是用来帮助用户识别认证产品，以确保配置项都被唯一标识。

配置管理能力是为了确定开发者是否清晰定义了认证产品和它的相关配置项。要求包括如下内容：

- 认证产品的唯一标识，包括名称、版本号。该标识无论是从认证产品硬件、软件、包装还是文档上都应明确，且应统一及唯一。
- 包括一份配置清单，配置清单应包括与认证产品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）及与认证测评相关的文档（如：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），还要做出详尽的解释。

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、生成与启动认证产品，以及认证产品在交付中不被修改。包括但不限于交付文档、安装生成和启动程序。

1) 交付

交付程序适用于整个认证产品，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。

应描述为保证认证产品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。

2) 安装、生成和启动程序

认证产品所必需的所有安装、生成和启动步骤，包括：

- 修改认证产品安全功能控制下的实体安装的特定安全特性；
- 处理异常情况和问题；
- 如果适用，列出安全安装所需的最低系统要求。

如果认证产品在已经运行的情况下交付，则该部分可不进行描述。