安全芯片密码检测准则

Cryptography Test Criteria for Security IC

国家密码管理局商用密码检测中心

2011 年 11 月

目　录

前言

《安全芯片密码检测准则》阐述了安全芯片的安全能力等级划分，以及适用于各安全等级安全芯片的密码检测要求。

本标准由国家密码管理局提出并归口。

本标准的主要起草单位：国家密码管理局商用密码检测中心、信息安全国家重点实验室。

本标准的主要起草人：李大为、周永彬、罗鹏、刘继业、张建人、张文婧、张翌维、陈立志、叶茵、沈海斌、李慧云、孙东昱、熊燕萍、刘宏伟、陈运、吴震。

本标准于 2012 年 1 月 1 日起实施。

本标准由国家密码管理局商用密码检测中心负责解释。

。

引言

安全芯片是一种重要的基础安全功能单元，在计算机、信息与通信系统中应用非常广泛。特别地，多数安全芯片都具有一种或多种密码功能。本标准中的安全芯片是指实现了一种或多种密码算法，直接和/或间接地使用密码技术来保护密钥和敏感信息的集成电路芯片。

安全芯片在实现的密码算法的基础上，根据设计和应用的不同须具有一种或多种安全能力。本标准将安全能力划分为密码算法、安全芯片接口、密钥管理、敏感信息保护、安全芯片固件安全、自检、审计、攻击的削弱与防护和生命周期保证九个领域，对每个领域的安全能力划分为安全性依次递增的三个安全等级，并对每个安全等级提出了安全性要求。安全芯片的安全等级定为该安全芯片所具有的各领域的安全能力的最低安全等级。

使用安全芯片所具有的密码功能时，安全芯片的安全能力对于保障整个系统的安全性举足轻重。为提供预期的安全服务，以及满足应用与环境的安全要求，应选择恰当安全等级的安全芯片，以确保使用安全芯片的计算机、信息与通信系统能够为特定应用提供一种可接受的安全等级。

本标准可以为选择满足应用与环境安全要求的适用安全等级的安全芯片提供依据，亦可为安全芯片的研制提供指导。

安全芯片密码检测准则

1 范围

本标准规定了安全能力依次递增的三个安全等级，以及适用于各安全等级安全芯片的密码检测要求。

本标准适用于安全芯片的密码检测，亦可指导安全芯片的研制。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注明日期的引用文件，其随后的所有修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 19715.1--2005/ISO/IEC TR 13335-1:1996　信息技术　信息技术安全管理指南

《随机性检测规范》　国家密码管理局

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本标准。

3.1 术语和定义

3.1.1 密钥 Key

控制密码变换操作的关键信息或参数。

3.1.2 敏感信息 Sensitive Information

安全芯片中除密钥外需要保护的数据。

3.1.3 安全芯片 Security Chip

安全芯片指实现了一种或多种密码算法，直接和/或间接地使用密码技术来保护密钥和敏感信息的集成电路芯片，包括硬件实体及依附于该硬件实体运行的固件。

3.1.4 安全能力 Security Capability

安全芯片对密钥和敏感信息能够提供的直接和/或间接的保障和防护措施。

3.1.5 分组密码算法的工作模式 Block Cipher Operation Mode

分组密码算法的工作方式，主要包括电码本模式（ECB）、密码分组链接模式（CBC）、密码反馈模式（CFB）、输出反馈模式（OFB）、计数器模式（CTR）等。

3.1.6 公钥密码算法的应用模式Public Key Cipher Application Mode

公钥密码算法的使用方式，主要包括加密/解密、签名/验证和密钥协商等。

3.1.7 密码算法的运算速率 Operation Speed of Cryptographic Algorithm

安全芯片实现的密码算法单位时间内可处理的最大数据量。

3.1.8 物理随机源 Physical Random Source

基于物理噪声所具有的不确定性而产生随机序列的源部件。

3.1.9 固件 Firmware

固化在安全芯片内的程序代码，负责控制和协调安全芯片的功能。

3.1.10 硬件 Hardware

安全芯片的物理实体。

3.1.11 生命周期 Life Cycle

安全芯片从研制到交付用户使用的全过程。

3.1.12 标识 Identification

安全芯片内部所固化的一组数据，用以识别不同的安全芯片。

3.1.13 权限 Permission

一组规则，规定用户许可的操作范围。

3.1.14 密钥管理 Key Management

密钥的生成、存储、使用、更新、导入、导出和销毁等过程的管理。

3.1.15 隐式通道 Covert Channel

可用来以违反安全要求的方式传送密钥和敏感信息的传输通道。

3.1.16 清零 Zeroization

一种擦除电子数据的方法，旨在防止数据恢复。

3.1.17 接口 Interface

安全芯片的输入或输出点，该点为信息流提供了输入或输出芯片的入口或出口，包括物理接口和逻辑接口。

3.1.18 物理接口 Physical Interface

涉及各种传输介质或传输设备的接口。

3.1.19 逻辑接口 Logic Interface

相对物理接口而言，能够实现数据交换功能但在物理上不存在，需要通过配置来建立的接口。

3.1.20 计时攻击 Timing Attack

根据密码算法在安全芯片中运行的时间差异，分析获取芯片内密钥和敏感信息的一种攻击方式。

3.1.21 能量分析攻击 Power Analysis Attack

通过采集安全芯片在密码运算时产生的能量消耗信息，利用密码学、统计学、信息论等原理分析获取芯片内密钥和敏感信息的一种攻击方式。

3.1.22 电磁分析攻击 EM Analysis Attack

通过采集安全芯片在密码运算时产生的电磁辐射信息，利用密码学、统计学、信息论等原理分析获取芯片内密钥和敏感信息的一种攻击方式。

3.1.23 故障攻击 Fault Attack

安全芯片运算过程中受到干扰时可能出现硬件故障或运算错误，利用这些故障行为或错误信息分析获取芯片内密钥和敏感信息的一种攻击方式。

3.1.24 光攻击 Light Attack

对去除封装后的安全芯片进行光照，利用光照的能量改变安全芯片的运行状态来实施的攻击。

3.1.25 源文件 Source File

安全芯片研制过程中涉及的软件源代码、版图、HDL 源代码等文件。

3.2 缩略语

ECB	分组密码算法的电码本工作模式
CBC	分组密码算法的密码分组链接工作模式
CFB	分组密码算法的密码反馈工作模式
OFB	分组密码算法的输出反馈工作模式
CTR	分组密码算法的计数器工作模式
HDL	硬件描述语言

4 安全等级的划分

4.1 安全等级 1

安全等级 1 规定了安全芯片的安全能力须满足的最低安全等级要求。安全等级 1 不要求安全芯片对密钥和敏感信息提供特定保护措施。

达到安全等级 1 的安全芯片可应用于安全芯片所部署的外部运行环境能够保障安全芯片自身物理安全和输入输出信息安全的应用场合。

4.2 安全等级 2

安全等级 2 规定了安全芯片的安全能力所能达到的中等安全等级要求。在安全等级 1 的基础上，安全等级 2 规定了安全芯片须具有的逻辑和/或物理保护措施。安全等级 2 要求安全芯片能够对密钥和敏感信息提供基本保护，具有对抗攻击的逻辑和/或物理的防御措施，并要求送检单位能够对相应防御措施的有效性进行说明，并要求安全芯片具有较全面的生命周期保障。

达到安全等级 2 的安全芯片可应用于安全芯片所部署的外部运行环境不能保障安全芯片自身物理安全和输入输出信息安全的应用场合或者其它有相应安全需求的应用场合。

4.3 安全等级 3

安全等级 3 规定了安全芯片的安全能力所能达到的高安全等级要求。在安全等级 2 的基础上，安全等级 3 规定了安全芯片须具有的逻辑和/或物理保护措施。安全等级 3 要求安全芯片能够对密钥和敏感信息提供高级保护，要求安全芯片具有的逻辑和/或物理安全机制能够对密钥和敏感信息提供完整的保护，要求安全芯片能够防御本标准指定的各种攻击，要求送检单位能够证明相关防御措施的有效性，并要求安全芯片具有完整的生命周期保障。

达到安全等级 3 的安全芯片可应用于安全芯片具有的安全能力满足应用要求的情况下，安全芯片所部署的外部运行环境不能保障安全芯片自身物理安全和输入输出信息安全，并且在该环境下安全芯片具有面临各种攻击的风险或者其它有相应安全需求的应用场合。

5 密码算法

5.1 随机数生成

1) 安全等级 1

安全芯片内必须有至少 1 个物理随机源直接生成随机数或生成随机数扩展算法的初始输入。

在安全芯片支持的电压、频率、温度、随机数生成速率等工作条件范围内，随机设定不少于 4 种工作条件的组合，安全芯片生成的随机数能够通过随机性检测。

2) 安全等级 2

安全芯片内必须有相互独立的至少 2 个物理随机源直接生成随机数或生成随机数扩展算法的初始输入。由物理随机源直接生成的随机数或生成的随机数扩展算法的初始输入必须包含全部物理随机源的所有输出信息。

在安全芯片支持的电压、频率、温度、随机数生成速率等工作条件范围内，随机设定不少于 8 种工作条件的组合，安全芯片生成的随机数能够通过随机性检测。

3) 安全等级 3

安全芯片内必须有相互独立的至少 4 个物理随机源直接生成随机数或生成随机数扩展算法的初始输入。由物理随机源直接生成的随机数或生成的随机数扩展算法的初始输入必须包含全部物理随机源的所有输出信息。

在安全芯片支持的电压、频率、温度、随机数生成速率等工作条件范围内，随机设定不少于 16 种工作条件的组合，安全芯片生成的随机数能够通过随机性检测。

如果安全芯片的首要功能是随机数生成，在安全芯片可正常运行的电压、频率和温度这 3 种工作条件的上限及下限处，安全芯片生成的随机数能够通过随机性检测。

5.2 分组密码算法

1) 安全等级 1

安全芯片支持的分组密码算法在各种工作模式下实现正确，运算结果与标准运算结果相符。

安全芯片须测定分组密码算法在各种工作模式下的运算速率；在各种工作模式的最高运算速率下，运算结果与标准运算结果相符。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片对于任何输入数据均能给出明确的结果或响应。

安全芯片支持的分组密码算法的核心运算环节须采用专用硬件模块实现。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片支持的分组密码算法须采用专用硬件模块实现。

安全芯片自身可以验证支持的分组密码算法在各种工作模式下的正确性。

5.3 公钥密码算法

1) 安全等级 1

安全芯片支持的公钥密码算法在各种应用模式下实现正确，运算结果与标准运算结果相符。

安全芯片须测定公钥密码算法在各种应用模式下的运算速率；在各种应用模式的最高运算速率下，运算结果与标准运算结果相符。

若安全芯片支持的公钥密码算法需要由安全芯片生成素数，则生成的素数须通过素性检测。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片对于任何输入数据均能给出明确的结果或响应。

安全芯片支持的公钥密码算法的核心运算环节须采用专用硬件模块实现。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片支持的公钥密码算法须采用专用硬件模块实现。安全芯片自身可以验证支持的公钥密码算法在各种应用模式下的正确性。

5.4 杂凑密码算法

1) 安全等级 1

安全芯片支持的杂凑密码算法实现正确，运算结果与标准运算结果相符。

安全芯片须测定杂凑密码算法的运算速率；在最高运算速率下，运算结果与标准运算结果相符。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片对于任何输入数据均能给出明确的结果或响应。

安全芯片支持的杂凑密码算法的核心运算环节须采用专用硬件模块实现。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片支持的杂凑密码算法须采用专用硬件模块实现。

安全芯片自身可以验证支持的杂凑密码算法的正确性。

5.5 序列密码算法

1) 安全等级 1

安全芯片支持的各种序列密码算法实现正确，运算结果与标准运算结果相符。

安全芯片须测定序列密码算法的运算速率；在最高运算速率下，运算结果与标准运算结果相符。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片能够正确处理序列密码算法的非规范的种子密钥。

安全芯片支持的序列密码算法的核心运算环节须采用专用硬件模块实现。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片支持的序列密码算法须采用专用硬件模块实现。

安全芯片自身可以验证支持的序列密码算法的正确性。

6 安全芯片接口

6.1 物理接口

1) 安全等级 1

安全芯片支持的物理接口中不得含有隐式通道。

安全芯片支持的各种不同物理接口输入输出的密码算法的运算数据须一致。

若安全芯片支持随机数生成功能，则通过安全芯片支持的物理接口输出的随机数均能够通过随机性检测。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片不得含有除声明的物理接口之外的物理接口。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须支持关闭非工作状态的物理接口。

安全芯片不得含有可能旁路安全芯片定义的安全机制的物理接口。

6.2 逻辑接口

1) 安全等级 1

安全芯片支持的逻辑接口中不得含有隐式通道。

安全芯片支持的逻辑接口输入输出的密码算法的运算数据须一致。

若安全芯片支持随机数生成功能，则通过安全芯片支持的逻辑接口得到的随机数均能够通过随机性检测。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片不得含有除声明的逻辑接口之外的逻辑接口。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片不得含有逻辑调试接口或其它可能旁路安全芯片定义的安全机制的逻辑接口。

7 密钥管理

7.1 生成

1) 安全等级 1

安全芯片能够正确、有效地生成密钥。

安全芯片生成的密钥不可预测、不可逆推。

若安全芯片在密钥生成过程中需使用非确定性数据，则须使用随机数；若安全芯片能够生成随机数，则须使用安全芯片自身生成的随机数。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片在密钥生成过程中，不得通过物理接口和逻辑接口泄露密钥的相关信息。

安全芯片在密钥生成后立即清除密钥生成过程中使用过且不再需要使用的相关数据和临时信息。

3) 安全等级 3

同安全等级 2。

7.2 存储

1) 安全等级 1

安全芯片能够正确、有效地存储密钥。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片须支持带校验的密钥存储。

安全芯片内存储的密钥及密钥相关信息须存放在可控且专用的存储区域，具有防止通过安全芯片的物理接口和逻辑接口对密钥进行非法访问的安全机制。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须支持以密文形式存储密钥。

7.3 使用

1) 安全等级 1

安全芯片能够根据密钥的类型和使用场合等情况正确、有效地使用密钥。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片在密钥使用过程中存放密钥及密钥相关信息的存储区域可控且专用。

安全芯片在密钥使用过程中，安全芯片的物理接口和逻辑接口不得泄露密钥及密钥相关信息。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片在每次使用完密钥后，除密钥的固定存储区域外，须将密钥及密钥相关信息在使用过程中涉及的存储区域立即自行清零。

7.4 更新

1) 安全等级 1

安全芯片能够正确、有效地更新密钥。

2) 安全等级 2

在安全等级 1 的基础上，

密钥更新需要相应的权限。

安全芯片完成密钥更新后须立即将原密钥安全清除。

若密钥更新过程需要与外部交换密钥的部分或全部信息，则安全芯片须支持安全的密钥协商机制来保证密钥更新过程的安全，且更新过程中传输的密钥的部分或全部信息应是密文形式。

3) 安全等级 3

同安全等级 2。

7.5 导入

1) 安全等级 1
   安全芯片能够正确、有效地导入密钥。
2) 安全等级 2
   在安全等级 1 的基础上，
   密钥导入需要相应的权限。
   安全芯片须支持以密文形式导入密钥。
3) 安全等级 3
   同安全等级 2。

7.6 导出

1) 安全等级 1
   安全芯片能够正确、有效地导出密钥。
2) 安全等级 2
   在安全等级 1 的基础上，
   密钥导出需要相应的权限。
   安全芯片须支持以密文形式导出密钥。
3) 安全等级 3
   同安全等级 2。

7.7 清除

1) 安全等级 1
   安全芯片能够根据需要正确、有效地清除所存储的密钥。
2) 安全等级 2
   在安全等级 1 的基础上，
   密钥清除需要相应的权限。
   密钥清除不得泄露密钥及密钥相关信息。
3) 安全等级 3
   在安全等级 2 的基础上，
   安全芯片须支持反复擦写等手段实现安全的密钥清除机制。

8 敏感信息保护

8.1 存储

1) 安全等级 1
   安全芯片能够正确、有效地存储敏感信息。
2) 安全等级 2
   在安全等级 1 的基础上，
   安全芯片须支持敏感信息以密文形式存储。
   安全芯片须具有对敏感信息的访问控制机制。
3) 安全等级 3
   在安全等级 2 的基础上，
   安全芯片须具有以硬件实现的对敏感信息的访问控制机制。
   不再转移的敏感信息不能从安全芯片读出。

8.2 清除

1) 安全等级 1

安全芯片能够根据需要正确、有效地清除敏感信息。

2) 安全等级 2

在安全等级 1 的基础上，

敏感信息清除需要有相应的权限。

敏感信息清除不得泄露敏感信息本身。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须支持反复擦写等手段实现安全的敏感信息清除机制。

8.3 运算

1) 安全等级 1

安全芯片能够正确、有效地运算敏感信息。

安全芯片在运算过程中不得输出敏感信息。

2) 安全等级 2

在安全等级 1 的基础上，

访问敏感信息运算过程使用的数据存储区需要相应的权限。

敏感信息运算过程使用的数据存储区在运算结束时须立即自行清零。

3) 安全等级 3

在安全等级 2 的基础上，

敏感信息的运算须在可控且专用的安全存储区域内进行。

8.4 传输

1) 安全等级 1

安全芯片能够根据需要正确、有效地输入或输出允许传输的敏感信息。

2) 安全等级 2

在安全等级 1 的基础上，

敏感信息的传输需要相应的权限。

允许传输的敏感信息须以密文形式传输。

对不允许传输的敏感信息，安全芯片须具有相应安全机制保证敏感信息只在安全芯片内部进行处理。

3) 安全等级 3

同安全等级 2。

9 固件安全

9.1 存储

1) 安全等级 1

安全芯片中的固件不得通过接口读出。

2) 安全等级 2

在安全等级 1 的基础上，

除固件本身外，其它代码不得读写固件的代码。

除固件本身外，其它代码读写固件中的数据需要相应的权限。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片中的固件须以密文形式存储。

9.2 执行

1) 安全等级 1

安全芯片能够正确、有效地实现声明的功能。

安全芯片固件不得实现未声明的功能。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片须采用异常处理机制等措施保证固件自身的健壮性和完整性。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须具有硬件实现的存储访问控制等系统级保护机制。

安全芯片须充分使用安全芯片硬件提供的保护机制，保证固件的安全可靠执行。

9.3 导入

1) 安全等级 1

安全芯片能够正确、有效地执行固件的导入。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片的固件不可再次导入。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片固件的初次导入须授权。

10 自检

1) 安全等级 1

安全芯片上电和复位时能够对支持的各种密码算法进行主动自检并生成自检状态。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片须支持在固件导入后对支持的密码算法进行主动自检并返回自检报告。

在外部指令要求下，安全芯片能够对支持的各种密码算法进行自检并返回自检报告。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须支持在检测到安全芯片面临风险时对支持的密码算法进行主动自检并返回自检报告。

11 审计

11.1 安全芯片标识

1) 安全等级 1

安全芯片须具有标识。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片须具有可校验的唯一标识。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须具有逻辑或物理的安全机制保证标识不被更改。

11.2 生命周期标识

1) 安全等级 1

无要求。

2) 安全等级 2

须定义安全芯片的生命周期模型，并对生命周期各阶段进行标识。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须具有相应的文档跟踪记录安全芯片所处的生命周期阶段。

安全芯片须具有相应的管理机制维护安全芯片的生命周期，并根据生命周期阶段的变化进行相应的处理。

12 攻击的削弱与防护

12.1 版图保护

1) 安全等级 1

无要求。

2) 安全等级 2

安全芯片上硬件实现的分组密码算法、公钥密码算法、序列密码算法和杂凑密码算法模块内混合布线。

安全芯片版图上各逻辑模块间不得有明显的通信链路。

安全芯片版图的布线须分多层实现。

安全芯片须具有屏蔽层。

安全芯片版图上对传输密钥和敏感信息的通信链路须设置防护措施。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须具有主动保护的屏蔽层。

安全芯片版图上所有自行设计的逻辑电路整体均须采用混合布线。

12.2 密钥及敏感信息的自毁

1) 安全等级 1

无要求。

2) 安全等级 2

安全芯片在接到外部合法自毁指令时，能够有效、可靠地完成密钥和敏感信息的自毁。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须具有主动完成密钥和敏感信息自毁的能力。

12.3 计时攻击的防护

1) 安全等级 1

无要求。

2) 安全等级 2

安全芯片须具有相应的防护措施以保证安全芯片支持的密码算法在运算时，运算时间与密钥和敏感信息之间没有明显的相关性。

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行描述和说明。

3) 安全等级 3

在安全等级 2 的基础上，

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行证明。

12.4 能量分析攻击的防护

1) 安全等级 1

无要求。

2) 安全等级 2

安全芯片须具有相应的防护措施以保证安全芯片支持的密码算法在运算时，能量消耗特征与密钥和敏感信息之间没有明显的相关性。

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行描述和说明。

3) 安全等级 3

在安全等级 2 的基础上，

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行证明。

12.5 电磁分析攻击的防护

1) 安全等级 1

无要求。

2) 安全等级 2

安全芯片须具有相应的防护措施以保证安全芯片支持的各种密码算法在运算时，电磁辐射特征与密钥和敏感信息之间没有明显的相关性。

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行描述和说明。

3) 安全等级 3

在安全等级 2 的基础上，

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行证明。

12.6 故障攻击的防护

1) 安全等级 1

无要求。

2) 安全等级 2

当安全芯片工作条件中的电压、频率、温度等可导致故障的工作参数的改变使安全芯片处于易受攻击状态时，安全芯片应能够发现这些工作条件的改变，并采取相应的防护措施保护密钥和敏感信息不泄露。

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行描述和说明。

3) 安全等级 3

在安全等级 2 的基础上，

安全芯片须具有对光攻击的抵抗能力，并能够采取相应的防护措施保护密钥和敏感信息

不泄露。

送检单位须通过文档或其它方式对相应的防护措施及其有效性进行证明。

13 生命周期保证

13.1 单位资质

1) 安全等级 1

具有国家密码管理局认定的资质。

2) 安全等级 2

同安全等级 1。

3) 安全等级 3

同安全等级 1。

13.2 文档

1) 安全等级 1

安全芯片的各类文档齐全。

2) 安全等级 2

在安全等级 1 的基础上，

安全芯片的各类文档分级管理，分开存放，访问不同级别的文档须具有相应权限。

安全芯片在生命周期的各个阶段须具有追踪记录文档。

3) 安全等级 3

在安全等级 2 的基础上，

对不同文档的访问须具有相应的访问许可及访问记录。

13.3 开发环境安全

1) 安全等级 1

安全芯片的开发环境须具有相应的规章制度及安全配置。

2) 安全等级 2

在安全等级 1 的基础上，

对安全芯片开发环境的访问须具有严格的人员控制。

安全芯片的开发环境须与外网物理隔离。

3) 安全等级 3

在安全等级 2 的基础上，

对安全芯片开发环境的访问须具有严格的记录。

对安全芯片开发环境的访问须具有严格的权限控制。

13.4 人员

1) 安全等级 1

安全芯片的生命周期的各个阶段所涉及的工作人员须具有明确的职能划分。

2) 安全等级 2

在安全等级 1 的基础上，

工作人员仅能接触与本人工作相关的信息。

接触敏感信息的工作人员须签署相关的保密合同。

3) 安全等级 3

在安全等级 2 的基础上，
严格控制工作人员接触的文档的传播范围。

13.5 开发流程

1) 安全等级 1
安全芯片的开发流程的各个阶段须明确界定。
对安全芯片开发过程中各阶段完成的任务及相应的输出须具有明确要求。
2) 安全等级 2
同安全等级 1。
3) 安全等级 3
同安全等级 1。

13.6 源文件

1) 安全等级 1
安全芯片的源文件须安全存放。
2) 安全等级 2
在安全等级 1 的基础上，
安全芯片的源文件的设计须具有规范的格式。
安全芯片的源文件须具有详细的设计文档。
安全芯片有关密码部分的源文件须提交检测机构进行备案和审核。
3) 安全等级 3
在安全等级 2 的基础上，
安全芯片源文件的设计须使用形式化的规则检查工具保证源文件的规范性。
安全芯片的源文件须提交检测机构进行备案和审核。