ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0082—2020

可信密码模块保护轮廓

Trusted cryptography module protection profile

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　TOE 描述 …… 2
6　TOE 安全环境 …… 2
7　TOE 安全目的 …… 4
8　IT 安全要求 …… 5
9　基本原理 …… 19
参考文献 …… 29

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学院软件研究所、同方股份有限公司、国民技术股份有限公司。

本文件主要起草人：赵世军、秦宇、初晓博、冯伟、刘孜文、胡浩、常德显、张倩颖、邵健雄、郑必可、刘鑫、汪丹。

可信密码模块保护轮廓

1 范围

本文件以GB/T 29829和GB/T 18336为基础，构建可信密码模块的保护轮廓，对符合评估保障级第3级的TOE的定义、安全环境、安全目的、安全要求等进行了详细说明，并给出相应的基本原理说明。

本文件适用于可信密码模块相关产品的生产、测评与应用开发。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336(所有部分) 信息技术 安全技术 信息技术安全评估准则

GB/T 29829 信息安全技术 可信计算密码支撑平台功能与接口规范

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2椭圆曲线公钥密码算法

GM/T 0012 可信计算可信密码模块接口规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信计算平台 trusted computing platform

构建在计算系统中，用于实现可信计算功能的支撑系统。

3.2

可信密码模块 trusted cryptography module

可信计算平台的硬件模块，为可信计算平台提供密码运算功能，具有受保护的存储空间。

3.3

密码模块密钥 TCM endorsement key

可信密码模块的背书密钥。

3.4

存储主密钥 storage master key

用于保护平台身份密钥和用户密钥的存储主密钥。

3.5

可迁移密钥 migratable key

可被迁移到其他特定可信密码模块的密钥。

3.6

不可迁移密钥　non-migratable key

不能够被迁移到特定可信密码模块外部的密钥。

3.7

SM2 算法

由 GB/T 32918 定义的一种公钥密码算法。

3.8

SM3 算法

由 GB/T 32905 定义的一种密码杂凑算法。

3.9

SM4 算法

由 GB/T 32907 定义的一种分组加密算法。

3.10

HMAC 算法

利用密码杂凑算法和秘密信息产生的消息验证码，本文件采用的密码杂凑算法为 SM3 算法。

4　缩略语

下列缩略语适用于本文件。

EK：密码模块密钥(TCM Endorsement Key)

IT：信息技术(Information Technology)

SF：安全功能(Security Function)

SFP：安全功能策略(Security Function Policy)

SMK：存储主密钥(Storage Master Key)

SOF：功能强度(Strength of Function)

TCM：可信密码模块(Trusted Cryptography Module)

TOE：评估对象(Target of Evaluation)

TSC：TSF 控制范围(TSF Scope of Control)

TSF：TOE 安全功能(TOE Security Functions)

TSP：TOE 安全策略(TOE Security Policy)

5　TOE 描述

本文件的安全要求适用于 TCM。本文件所指的 TOE 是 TCM，在 GB/T 29829 和 GM/T 0012 中定义。

6　TOE 安全环境

6.1　使用和环境假设

TOE 使用假设是对 TOE 使用方式的假设，也是本文件中各项安全要求合理性和完整性的基础之一，TOE 使用假设见表 1。

表 1　使用假设

序号	假设名称	描述
1	正确配置	TOE需要被正确的安装以及配置

TOE环境假设是对TOE运行环境的假设，也是本文件中各安全要求合理性和完整性的基础之一，TOE环境假设见表2。

表 2　环境假设

序号	假设名称	描述
1	篡改留证	TOE只提供篡改的证据。它并不提供对诸如简单能量分析攻击、差分能量分析攻击、外部信号干扰和高温等物理威胁的保护。物理保护假设由TOE所处的环境来提供

6.2　威胁

威胁是本文件中各安全要求需要应对和克服的主要对象，与TOE安全目的之间存在紧密的对应关系，TOE所面临的威胁见表3。

表 3　威胁

序号	威胁	描述
1	攻击	一个攻击者会试图执行一个没有被授权的操作，从而使得TOE未能检测到对加密数据的威胁
2	旁路	一个未经授权的用户可能会篡改安全属性或其他数据，以绕过TOE的安全功能，从而未经授权而访问TOE数据
3	导出	一个用户或攻击者可能会将数据导出而不附带安全属性或附带的安全属性不够安全，造成导出的数据是错误的并且无效
4	密码破解	密码算法可能没有被正确实现，因此一个用户可能会获取TOE生成的密钥，并未经授权用此密钥去访问被加密的数据
5	物理破解	通过与TOE物理交互并在物理环境中利用其弱点，一个未经授权的用户可能在未经授权的情况下获取或修改TOE数据
6	冒名	一个未经授权的用户可能伪装成一个已由TOE授权的用户，从而获得访问TOE数据、密钥以及执行操作的能力
7	导入	一个用户或者攻击者可能会将不带有安全属性或带有错误安全属性的数据导入，造成所有权和鉴别的错误、系统故障或者非安全运行
8	密钥生成和销毁	密钥可能通过一种不安全的方式产生或销毁，从而对密钥构成危害
9	功能异常	TOE出现故障时，TOE的数据可能会被未经授权的TOE的用户修改或者访问
10	修改	一个攻击者可能会修改TSF或者用户数据，例如存储的安全属性以及密钥，从而获得访问TOE以及TOE的数据的能力
11	无安全属性	用户可能会创建一个没有安全属性值的数据客体，例如没有安全属性值的密钥
12	安全属性变化	用户或攻击者可能未经授权而改动数据的安全属性

表 3 威胁（续）

序号	威胁	描述
13	未受保护的安全属性	用户可能会为一个客体设置一个未受保护的安全属性值
14	残留数据	当一个数据不再被 TOE 管理的时候（即产生了“残留”数据），用户可能未经授权而获得这个数据
15	重放	一个未经授权的个体，可能通过重放攻击以及中间人攻击而获得已经通过鉴别的数据，从而能够非法访问系统以及机密数据
16	否认	一个数据的生成者可能会否认某数据由其生成的事实，以逃避其应承担的责任
17	自检失败	TOE 可能以一个不安全的状态启动或者启动后进入了一个不安全的状态，使得攻击者能够获得机密数据或者威胁系统

7 TOE 安全目的

7.1 TOE 安全目的

TOE 安全目的是本文件中各安全要求所要达到的最终目的，与安全威胁之间存在紧密的对应关系，TOE 安全目的见表 4。

表 4 TOE 安全目的

序号	目的	描述
1	安全密钥管理	TOE 应以一种安全的方式产生和销毁密钥
2	执行密码操作	TOE 应能够执行与密码学相关的操作，这些操作包括 SM2、SM3、SM4、HMAC、密钥生成（遵循一定的算法和密钥的长度，密钥的长度应足够大以保证公私密钥对不被破解）
3	自检	TOE 应具备自检功能，检验密码功能是否按照设计的模式运行
4	自主访问控制	TOE 应能够通过特定的访问控制策略来控制和限制用户对 TOE 数据的访问
5	安全导出	当数据被导出 TOE 时，TOE 应保证安全属性与数据一起被导出，并且保证这些与数据相关的安全属性值之间密切关联
6	故障时安全	TOE 应保证在发生与密码学相关的操作失败情况时，或发生其他故障时，系统仍然处于一个安全状态
7	完整性检查	TOE 应对系统完整性和用户数据完整性进行周期性检查
8	消息校验	TOE 应提供检测安全属性或其他数据是否被更改的功能
9	身份标识	TOE 应能够识别各用户的唯一身份，并且在授权用户访问 TOE 功能之前，TOE 应鉴别用户所声称的身份
10	安全导入	当数据被导入 TOE 时，TOE 应保证与数据关联的安全属性也一同被导入，并且保证这些数据来自一个合法的授权方。此外，TOE 应根据 TSF 访问控制规则对这些安全属性进行校验
11	功能调用	TSF 应被 TOE 的行为所调用

表 4　TOE 安全目的（续）

序号	目的	描述
12	限制操作	TOE 在核实用户身份之前，应限制用户进行任何操作
13	消息判定	当 TOE 与一个远程的系统交换数据时，应支持对数据的完整性和消息的不可否认性的判定
14	无可重用信息	TOE 应保证没有“可重用”的资源。例如通过将资源重复分配给不同的用户时，应保证在信息容器中或者系统资源中没有“残留”的信息
15	默认安全属性	当一个客体被创建时，TOE 要求其拥有默认的安全属性
16	修改安全属性	TOE 应允许一个授权用户修改某一个已被创建的客体的默认安全属性
17	可靠的安全属性	TOE 应管理安全属性，并且保证这些安全属性必须具有安全值
18	安全属性管理	TOE 应只允许授权用户初始化和修改客体的安全属性值
19	安全角色	TOE 应管理与安全相关的角色以及与这些角色相关联的用户
20	受保护的功能	TSF 应拥有属于其自身的一块区域用于执行安全功能操作，以避免外部干扰、篡改以及未经授权的信息泄露
21	一次性鉴别	TOE 应提供一次性鉴别的机制，通过要求重新鉴别来防止重放攻击和中间人攻击
22	篡改识别	TOE 应具有让用户检测系统部件是否被物理篡改的特性

7.2　环境安全目的

环境安全目的见表 5。

表 5　环境安全目的

序号	目的名称	目的描述
1	正确配置	TOE 应被恰当的安装和配置，以保证 TOE 启动状态的安全性
2	物理安全	环境应提供可接受的物理安全级别，以保证 TCM 不会被篡改以及不会遭受诸如能量分析攻击、时间分析攻击等多种形式的旁路攻击

8　IT 安全要求

8.1　概述

本章定义了 TOE 安全功能要求和安全保证要求，这些要求的具体内容、描述形式以及相互间依赖关系均遵循和抽取自 GB/T 18336，并根据 GB/T 18336 的规定进行了具体规则的选择、赋值以及提炼。在下述具体要求描述中，这些选择、赋值以及提炼的操作都通过下划线标识出来。

8.2　TOE 安全功能要求

8.2.1　FCO 类：通信

FCO_NRO.2　强制性原发证明

从属于:FCO_NRO.1 选择性原发证明。

FCO_NRO.2.1 TSF 在任何时候都应对传送的使用身份密钥签名的 TCM 数据强制生成原发证据。

FCO_NRO.2.2 TSF 应能将信息起源者的身份与证据适用的信息的 TCM 数据相关联。

FCO_NRO.2.3 TSF 应能为只有通过请求者正确鉴别才可用的证据的接收者提供验证原发证据的能力。

依赖关系:FIA_UID.1 标识定时。

8.2.2 FCS 类:密码支持

8.2.2.1 FCS_CKM.1 密钥产生

从属于:无其他组件。

FCS_CKM.1.1 TSF 应根据特定的密钥产生算法 SM2/SM4 和规定的密钥长度 256/128 比特来生成密钥;

依赖关系:FCS_COP.1 密码运算,FCS_CKM.4 密钥销毁,FMT_MSA.2 安全属性。

8.2.2.2 FCS_CKM.4 密钥销毁

从属于:无其他组件。

FCS_CKM.4.1 TSF 应根据特定密钥销毁算法擦除含有密钥的存储区域来销毁密钥;

依赖关系:FCS_COP.1 密码运算, FMT_MSA.2 受保护的安全属性。

8.2.2.3 FCS_COP.1:1 密码运算

8.2.2.3.1 SM2/SM4 加密和解密

从属于:无其他组件。

FCS_COP.1.1;1 TSF 应根据特定的密码算法 SM2/SM4 和密钥长度 256/128 比特来执行加密运算和解密运算。

8.2.2.3.2 FCS_COP.1:2 SM2 签名和签名校验

从属于:无其他组件。

FCS_COP.1.1;2 TSF 应根据特定的密码算法 SM2 和密钥长度 256 比特来执行签名和签名校验。

8.2.2.3.3 FCS_COP.1:3 SM3

从属于:无其他组件。

FCS_COP.1.1;3 TSF 应根据特定的密码算法 SM3 和一定长度的密钥来执行 SM3 密码杂凑运算。

8.2.2.3.4 FCS_COP.1:4 HMAC

从属于:无其他组件。

FCS_COP.1.1;4 TSF 应根据特定密码算法 SM3 和 256 比特长度的密钥来执行 HMAC 运算。

依赖关系:FCS_CKM.1 密钥产生,FCS_CKM.4 密钥销毁, FMT_MSA.2 受保护的安全属性。

8.2.3 FDP 类：用户数据保护

8.2.3.1 FDP_ACC.1 子集访问控制

从属于：无其他组件。

FDP_ACC.1.1 TSF 应对下列内容实施受保护的操作的访问控制：主体为用户执行的命令；客体为密钥和用户数据；操作包括签名、加密、解密。

依赖关系：FDP_ACF.1 基于安全属性的访问控制。

8.2.3.2 FDP_ACF.1 基于安全属性的访问控制

从属于：无其他组件。

FDP_ACF.1.1 TSF 应基于安全属性 TCM-AUTH-DATA-USAGE，TCM-KEY-FLAGS，TCM-KEY-USAGE 对客体依据 SFP 实施受保护的操作的访问控制。

FDP_ACF.1.2 TSF 应实施以下规则，以决定受控主体与受控客体间的操作是否被允许：对密钥和数据的访问被定义为基于安全属性 TCM-AUTH-DATA-USAGE 的值只被所有者访问或只被所有用户访问；每一个密钥的密码操作都要基于安全属性 TCM-KEY-USAGE 进行限制。

FDP_ACF.1.3 TSF 应基于以下附加规则明确授权主体对客体的访问：基于安全属性明确授权主体访问客体的规则。

FDP_ACF.1.4 TSF 应基于以下规则明确拒绝主体对客体的访问：基于安全属性明确拒绝主体访问客体的规则。

依赖关系：FDP_ACC.1 子集访问控制，FMT_MSA.3 静态属性初始化。

应用注释：FDP_ACF.1.3，FDP_ACF.1.4 中的赋值操作应由安全目标制定者定义。

8.2.3.3 FDP_ETC.2 有安全属性的用户数据输出

从属于：无其他组件。

FDP_ETC.2.1 TSF 在 SFP 控制下输出用户数据到 TSC 之外时，应受保护的操作的访问控制。

FDP_ETC.2.2 TSF 应输出用户数据且带有用户数据关联的安全属性。

FDP_ETC.2.3 TSF 在安全属性输出到 TSC 之外时，应确保其与输出的数据确切关联。

FDP_ETC.2.4 TSF 在用户数据从 TSC 输出时应执行：只有当 TCM-KEY-FLAGS 中的可迁移标志位被设置时，一个密钥才能够被加密迁移。[赋值：其他的输出控制规则]

应用注释：在输出之前，安全属性会被加密到数据块中。作为经过加密过的数据块的一部分，安全属性明确地与数据关联。

依赖关系：FDP_ACC.1 子集访问控制。

8.2.3.4 FDP_ITC.2 有安全属性的用户数据输入

从属于：无其他组件。

FDP_ITC.2.1 TSF 在 SFP 控制下从 TSC 之外输入用户数据时，应实施受保护的操作的访问控制。

FDP_ITC.2.2 TSF 应使用与输入数据相关的安全属性。

FDP_ITC.2.3 TSF 应确保使用的协议在安全属性和接收的用户数据之间提供了明确的

联系。

FDP_ITC.2.4　TSF 应确保对输入的用户数据的安全属性的解释与用户数据源的解释是一致的。

FDP_ITC.2.5　TSF 在 SFP 控制下从 TSC 之外导入用户数据时，应执行：[赋值：附加的输入控制策略]。

应用注释：安全属性作为被加密过的数据块的一部分一同输入。作为数据块的一部分，安全属性与数据确切关联；FDP_ITC.2.5 中的赋值操作应由安全目标的制定者定义。

依赖关系：FDP_ACC.1，子集访问控制，FTP_TRP.1，可信路径，FPT_TDC.1，TSF 间基本 TSF 数据的一致性。

8.2.3.5　FDP_RIP.2 完全残余信息保护

从属于：FDP_RIP.1　子集残余信息保护。

FDP_RIP.2.1　TSF 应确保对所有客体释放资源时，使该资源任何以前的信息内容不再使用。

依赖关系：无依赖关系。

8.2.4　FIA 类：标识和鉴别

8.2.4.1　FIA_ATD.1　用户属性定义

从属于：无其他组件。

FIA_ATD.1.1　TSF 应保存属于每个用户的下列安全属性：鉴别数据，角色。

依赖关系：无依赖关系。

8.2.4.2　FIA_UAU.1　鉴别定时

从属于：无其他组件。

FIA_UAU.1.1　在用户鉴别前，当实体所有者基于 TCPA_AUTH_DATA_USAGE 的值得到全局访问权时，TSF 应允许其访问密钥和数据；当它代表用户执行时，应允许其对以下几个命令的访问：TCM-SelfTestFull，TCM-ContinueSelfTest，TCM-GetTestResult，TCM-PcrRead。

FIA_UAU.1.2　对于任何其他由 TSF 所协调的并能代表该用户的操作，在允许执行这些操作前，TSF 应要求该用户已被合法鉴别。

依赖关系：FIA_UID.1　标识定时。

8.2.4.3　FIA_UAU.4　一次性鉴别机制

从属于：无其他组件。

FIA_UAU.4.1　TSF 应防止与独立客体授权协议和特定客体授权协议有关的鉴别数据的重用。

依赖关系：无依赖关系。

8.2.4.4　FIA_UAU.6　重鉴别

从属于：无其他组件。

FIA_UAU.6.1　在每一个需要鉴别用户才能执行的命令条件下，TSF 应重新鉴别用户。

依赖关系：无依赖关系。

8.2.4.5 FIA_UID.1 标识定时

从属于：无其他组件。

FIA_UID.1.1 在用户鉴别前，当实体所有者基于 TCPA_AUTH_DATA_USAGE 的值得到全局访问权时 TSF 应允许其访问密钥和数据；当它代表用户执行时应允许其对以下几个命令的访问：TCM-SelfTestFull，TCM-ContinueSelfTest，TCM-GetTestResult，TCM-PcrRead。

FIA_UID.1.2 对于任何其他由 TSF 所统一协调的并能代表该用户的操作，在允许执行这些操作前，TSF 应要求用户能够成功地标识自己。

依赖关系：无依赖关系。

8.2.5 FMT 类：安全管理

8.2.5.1 FMT_MOF.1 安全功能行为的管理

从属于：无其他组件。

FMT_MOF.1.1 TSF 应限制 TCM 所有者对功能[赋值：功能列表]进行允许或禁止的能力。

依赖关系：FMT_SMR.1 安全角色。

应用注释：赋值应由安全目标的制定者来定义。

8.2.5.2 FMT_MSA.1 安全属性的管理

从属于：无其他组件。

FMT_MSA.1.1 TSF 应实施受保护的操作的访问控制，以仅限于资源所有者能够对安全属性与特定资源相关的安全属性进行控制，包括 TCM-KEY-USAGE，TCM-AUTH-DATA-USAGE，可迁移标志以及易变性标志进行创建。

依赖关系：FMT_SMR.1 安全角色，FDP_ACC.1 子集访问控制。

8.2.5.3 FMT_MSA.2 受保护的安全属性

从属于：无其他组件。

FMT_MSA.2.1 TSF 应确保安全属性只接受安全的值。

依赖关系：ADV_SPM .1，非形式化的 TOE 安全策略模型，FMT_SMR.1，安全角色，FDP_ACC.1 子集访问控制，FMT_MSA.1 安全属性的管理。

8.2.5.4 FMT_MSA.3 静态属性初始化

从属于：无其他组件。

FMT_MSA.3.1 TSF 应实施受保护的操作的访问控制，以便为用于执行 SFP 的安全属性提供特定的默认值。

FMT_MSA.3.2 TSF 应允许资源所有者为生成的客体或信息指定替换性的初始值以代替原来的默认值。

应用注释 安全属性的默认值由生产厂商指定，生产厂商应在制定相关的安全目标中应详细说明。

依赖关系：FMT_SMR.1 安全角色，FMT_MSA.1 安全属性的管理。

8.2.5.5 FMT_MTD.1：1 TSF 数据的管理——TCM 所有者修改

从属于：无其他组件。

FMT_MTD.1.1:1　TSF 应限制修改 TSF 数据的能力:与密码模块密钥和存储根密钥相关的标识与鉴别数据;向 TCM 所有者迁移的授权数据。

8.2.5.6　FMT_MTD.1:2　TSF 数据的管理——TCM 所有者创建

从属于:无其他组件。

FMT_MTD.1.1:2　TSF 应限制产生 TSF 数据的能力:为 TCM 所有者产生存储根密钥和 TCM 证据。

8.2.5.7　FMT_MTD.1:3　TSF 数据的管理——资源所有者

从属于:无其他组件。

FMT_MTD.1.1:3　TSF 应限制修改 TSF 数据的能力:为资源所有者修改与资源相关的标识与鉴别数据。

8.2.5.8　FMT_MTD.1:4　TSF 数据的管理——生产厂商

从属于:无其他组件。

FMT_MTD.1.1:4　TSF 应限制产生 TSF 数据的能力:为 TCM 厂商或设计者产生密码模块密钥。

依赖关系:FMT_SMR.1 安全角色。

8.2.5.9　FMT_SMR.2　安全角色限制

从属于:FMT_SMR.1 安全角色。

FMT_SMR.2.1　TSF 应维护的角色:TCM 所有者,资源所有者,TCM 生产厂商。

FMT_SMR.2.2　TSF 应能够把用户和角色关联起来。

FMT_SMR.2.3　TSF 应确保条件:满足正确的鉴别数据能够被表述。

依赖关系:FIA_UID.1 标识定时。

8.2.6　FPT 类:TSF 保护

8.2.6.1　FPT_FLS.1　带保存安全状态的失败

从属于:无其他组件。

FPT_FLS.1.1　TSF 在下列失败发生时应保存一个安全状态:a)任何密码运算的失败;b)任何命令或内部操作的失败。

依赖关系:ADV_SPM.1　非形式化的 TOE 安全策略模型。

8.2.6.2　FPT_PHP.1　物理攻击的被动检测

从属于:无其他组件。

FPT_PHP.1.1　TSF 应对可能危及 TSF 的安全的物理篡改提供明确的检测。

FPT_PHP.1.2　为 TSF 提供判断 TSF 设备或 TSF 元件是否已被物理篡改的能力。

依赖关系:FMT_MOF.1　安全功能行为的管理。

8.2.6.3　FPT_RCV.4　功能恢复

从属于:无其他组件。

FPT_RCV.4.1　TSF 应确保 TCM 命令有如下特征,即 SF 或者被成功完成,或者对指明的失

败情况恢复到一致的安全状态。

依赖关系：ADV_SPM.1　非形式化的 TOE 安全策略模型。

8.2.6.4　FPT_RPL.1　重放检测

从属于：无其他组件。

FPT_RPL.1.1　TSF 应检测以下实体的重放：包含随机数的命令请求。

FPT_RPL.1.2　检测到重放时，TSF 应执行销毁会话。

依赖关系：无依赖关系。

8.2.6.5　FPT_TDC.1　TSF 间基本 TSF 数据的一致性

从属于：无其他组件。

FPT_TDC.1.1　当 TSF 与其他可信 IT 产品共享 TSF 数据时，TSF 应提供对 TCM 命令和响应一致性解释的能力。

FPT_TDC.1.2　当解释来自其他可信 IT 产品的 TSF 数据时，TSF 应使用可信密码模块规范。

依赖关系：无依赖关系。

8.2.6.6　FPT_TST.1　TSF 检测

从属于：无其他组件。

FPT_TST.1.1　TSF 应运行一套自检程序：1)在初始化启动期间；2)在正常工作时周期性地；3)授权用户要求；4)满足以下条件时：先于第一次对功能调用的执行以表明 TSF 操作的正确性。

FPT_TST.1.2　TSF 为授权用户提供对 TSF 数据完整性的验证能力。

FPT_TST.1.3　TSF 为授权用户提供对存储的 TSF 可执行代码完整性的验证能力。

应用注释　FPT_TST.1.1 中的授权用户应被解释为一个用户。对于运行自检或基于自检来校验系统正确性的用户来说不需要经过鉴别。

依赖关系：FPT_AMT.1　抽象机测试。

8.2.7　FTP 类：可信路径

FTP_TRP.1：可信路径

从属于：无其他组件。

FTP_TRP.1.1　TSF 应在它自身和远程或本地用户之间提供一条通信路径，此路径在逻辑上与其他路径不同，并且确保对其端点提供鉴别，并保护通信数据免遭修改和泄露。

FTP_TRP.1.2　TSF 应允许 TSF、本地用户或远程用户经可信路径发起通信。

FTP_TRP.1.3　对于初始化用户鉴别、所有 TCM 命令、所有用户命令及 TSF 响应，TSF 应要求经由可信路径发起通信。

依赖关系：无依赖关系。

8.2.8　功能强度要求

TOE 鉴别功能的威胁程度假定为基本功能强度。密码算法的强度不在信息技术安全性评估准则范围之内。功能强度仅用于非密码的、概率或置换机制。功能强度要求适用于 TOE 内部的标识与鉴别功能。

8.3 TOE 安全保证要求

8.3.1 ACM 类：配置管理

8.3.1.1 ACM_CAP.3：授权控制

依赖关系：ACM_SCP.1 TOE CM 范围，ALC_DVS.1 安全度量标识。

开发者行为元素：

ACM_CAP.3.1D	开发者应为 TOE 提供一个参照号。
ACM_CAP.3.2D	开发者应使用 CM 系统。
ACM_CAP.3.3D	开发者应提供 CM 文档。

证据的内容和形式元素：

ACM_CAP.3.1 C	TOE 参照号对 TOE 的每一个版本应是唯一的。
ACM_CAP.3.2C	应给 TOE 标记上其参照号。
ACM_CAP.3.3C	CM 文档应包括一个配置清单和一个 CM 计划。
ACM_CAP.3.4C	配置清单应描述组成 TOE 的配置项。
ACM_CAP.3.5 C	CM 文档应描述用以唯一标识配置项的方法。
ACM_CAP.3.6C	CM 系统应唯一标识所有配置项。
ACM_CAP.3.7C	CM 计划应描述 CM 系统是如何使用的。
ACM_CAP.3.8C	证据应论证 CM 系统的运作与 CM 计划相一致。
ACM_CAP.3.9C	CM 文档应提供证据以证明在 CM 系统下有效地维护了所有的配置项。
ACM_CAP.3.10C	CM 系统应提供措施使得对配置项只能进行授权修改。

评估者行为元素：

ACM_CAP.3.1E	评估者应确认所提供的信息满足证据的内容和形式的所有要求。

8.3.1.2 ACM_SCP.1 TOE CM 范围

依赖关系：ACM_CAP.3 授权控制。

开发者行为元素：

ACM_SCP.1.1D	开发者应提供 CM 文档。

证据的内容和形式元素：

ACM_SCP.1.1C	CM 文档应说明 CM 系统至少能跟踪以下几项：TOE 实现表示，设计文档，测试文档，用户文档，管理员文档和 CM 文档。
ACM_SCP.1.2C	CM 文档应描述 CM 系统是如何跟踪配置项的。

评估者行为元素：

ACM_SCP.1.1E	评估者应确认所提供的信息满足证据的内容和形式的所有要求。

8.3.2 ADO 类：交付和运行

8.3.2.1 ADO_DEL.1 交付过程

依赖关系：无依赖关系。

开发者行为元素：

ADO_DEL.1.1D	开发者应将把 TOE 及其部分交付给用户的程序文档化。
ADO_DEL.1.2D	开发者应使用交付程序。

证据的内容和形式元素：

ADO_DEL.1.1 C　交付文档应描述，在给用户分配 TOE 的版本时，用于维护安全所必需的所有程序。

评估者行为元素：

ADO_DEL.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.2.2 ADO_IGS.1 安装，生成和启动过程

依赖关系：AGD_ADM.1 管理员指南。

开发者行为元素：

ADO_IGS.1.1D　开发者应将 TOE 安全地安装、生成和启动所必要的程序文档化。

证据的内容和形式元素：

ADO_IGS.1.1C　文档应描述 TOE 安全地安装、生成和启动所必要的步骤。

评估者行为元素：

ADO_IGS.1.1　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADO_IGS.1.2E　评估者应决定安装，生成和启动程序最终产生了安全的配置。

8.3.3 ADV 类：开发

8.3.3.1 ADV_FSP.1 非形式化功能规范

依赖关系：ADV_RCR.1 非形式化对应性论证。

开发者行为元素：

ADV_FSP.1.1D　开发者应提供功能规范。

证据的内容和形式元素：

ADV_FSP.1.1C　功能规范应使用非形式化的风格来描述 TSF 及其外部接口。

ADV_FSP.1.2C　功能规范应是内在一致的。

ADV_FSP.1.3C　功能规范应描述所有外部 TSF 的接口的用途及使用方法，适当的时候，要提供产生的影响、例外情况和错误消息的细节。

ADV_FSP.1.4C　功能规范应完备地表示 TSF。

评估者行为元素：

ADV_FSP.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADV_FSP.1.2E　评估者应决定功能规范是 TOE 安全功能要求的一个精确且完备的实例。

8.3.3.2 ADV_HLD.2 安全加强的高层设计

依赖关系：ADV_FSP.1 非形式化功能规范，ADV_RCR.1 非形式化对应性论证。

开发者行为元素：

ADV_HLD.2.1 D　开发者应提供 TSF 的高层设计。

证据的内容和形式元素：

ADV_HLD.2.1C　高层设计的表示应是非形式化的。

ADV_HLD.2.2 C　高层设计应是内在一致的。

ADV_HLD.2.3 C　高层设计应按子系统来描述 TSF 的结构。

ADV_HLD.2.4 C　高层设计应描述 TSF 的每一个子系统所提供的安全功能。

ADV_HLD.2.5 C　高层设计应标识 TSF 所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示。

ADV_HLD.2. 6C　高层设计应标识 TSF 子系统的所有接口。

ADV_HLD.2.7 C　高层设计应标识 TSF 子系统的哪些接口是外部可见的。

ADV_HLD.2. 8C　高层设计应描述 TSF 子系统所有接口的用途与使用方法，并适当提供影响，例外情况和错误消息的细节。

ADV_HLD.2. 9C　高层设计应描述把 TOE 分成 TSP-实施和其他子系统的这种分离。

评估者行为元素：

ADV_HLD.2. 1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADV_HLD.2. 2E　评估者应决定功能规范是 TOE 安全功能要求的一个精确且完备的实例。

8.3.3.3 ADV_RCR.1 非形式化对应性论证

依赖关系：无依赖关系

开发者行为元素：

ADV_RCR.1.1D　开发者应在所提供的 TSF 表示的所有相邻对之间提供其对应性分析。

证据的内容和形式元素：

ADV_RCR.1.1C　对于所提供的 TSF 表示的每个相邻对，分析应论证：较为抽象的 TSF 表示的所有相关安全功能都在较不抽象的 TSF 表示中得到正确且完备地细化。

评估者行为元素：

ADV_RCR.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.3.4 ADV_SPM.1 非形式化 TOE 安全策略模型

依赖关系：ADV_FSP.1 非形式化功能规范。

开发者行为元素：

ADV_SPM.1.1D　开发者应提供一个 TSP 模型。

ADV_SPM.1.2D　开发者应论证功能规范和 TSP 模型之间的对应性。

证据的内容和形式元素：

ADV_SPM.1.1C　TSP 模型应是非形式化的。

ADV_SPM.1.2C　TSP 模型应描述所有可模型化的 TSP 策略的规则与特征。

ADV_SPM.1.3C　TSP 模型应包括一个基本原理，即论证该模型对与所有可模型化的 TSP 策略来说，是与其一致而且是完备的。

ADV_SPM.1.4C　TSP 模型和功能规范之间的对应性论证应说明：所有功能规范中的安全功能对于 TSP 模型来说，是与其一致而且是完备的。

评估者行为元素：

ADV_SPM.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.4 AGD 类：指导性文档

8.3.4.1 AGD_ADM.1 管理员指南

依赖关系：ADV_FSP.1 非形式化功能规范。

开发者行为元素：

AGD_ADM.1.1D　开发者应提供针对系统管理员的管理员文档。

证据的内容和形式元素：

AGD_ADM.1.1 C　管理员指南应描述 TOE 管理员可使用的管理功能和接口。

AGD_ADM.1.2 C　管理员指南应描述如何以安全的方式管理 TOE。

AGD_ADM.1.3 C　管理员指南应包含在安全处理环境中应进行控制的功能和权限的警告。

AGD_ADM.1.4 C　管理员指南应描述所有与 TOE 的安全运行有关的用户行为的假设。

AGD_ADM.1.5 C　管理员指南应描述所有受管理员控制的安全参数，合适的情况下应指明安全值。

AGD_ADM.1.6 C　管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件，包括改变 TSF 所控制的实体的安全特性。

AGD_ADM.1.7 C　管理员指南应与为评估而提供的其他所有文档保持一致。

AGD_ADM.1.8 C　管理员指南应描述与管理员有关的 IT 环境的所有安全要求。

评估者行为元素：

AGD_ADM.1.1 E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.4.2　AGD_USR.1　用户指南

依赖关系：ADV_FSP.1　非形式化功能规范

开发者行为元素：

AGD_USR.1.1 D　开发者应提供用户指南。

证据的内容和形式元素：

AGD_USR.1.1 C　用户指南应描述 TOE 的非管理员可用的功能和接口。

AGD_USR.1.2 C　用户指南应描述 TOE 提供的用户可访问的安全功能的用法。

AGD_USR.1.3 C　用户指南应包含在安全处理环境中所控制的用户可访问的功能和权限的警告。

AGD_USR.1.4 C　用户指南应清晰地阐述 TOE 安全运行中用户所应负的职责，包括有关在 TOE 安全环境阐述中找得到的用户行为的假设。

AGD_USR.1.5 C　用户指南应与为评估而提供的其他所有文档保持一致。

AGD_USR.1.6 C　用户指南应描述与用户有关的 IT 环境的所有安全要求。

评估者行为元素：

AGD_USR.1.6 E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.5　ALC 类：生命周期支持

8.3.5.1　ALC_DVS.1　安全度量标识

依赖关系：无依赖关系。

开发者行为元素：

ALC_DVS.1.1 D　开发者应提供开发安全文档。

证据的内容和形式元素：

ALC_DVS.1.1 C　开发安全文档应描述在 TOE 的开发环境中，为了保护 TOE 设计和实现的保密性和完整性面需要在物理，程序，人员以及其他方

面应采取的必要安全措施。

ALC_DVS.1.2 C　开发安全文档应提供在 TOE 的开发和维护过程中执行安全措施的证据。

评估者行为元素：

ALC_DVS.1.1 E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ALC_DVS.1.2 E　评估者应确认应用了安全措施。

8.3.5.2 ALC_FLR.1 基本缺陷纠正

依赖关系：无依赖关系。

开发者行为元素：

ALC_FLR.1.1 D　开发者应将缺陷纠正的程序文档化。

证据的内容和形式元素：

ALC_FLR.1.1 C　缺陷纠正程序文档应描述用以跟踪所有在 TOE 发布时已被报告的安全缺陷的程序。

ALC_FLR.1.2 C　缺陷纠正程序应要求描述所提供的每个安全缺陷的性质和效果，以及更正缺陷的情况。

ALC_FLR.1.3 C　缺陷纠正程序应要求标识每个安全缺陷所采取的纠正措施。

ALC_FLR.1.4 C　缺陷纠正程序文档应描述为 TOE 用户的更正行为所提供的信息，更正和指导的方法。

评估者行为元素：

ALC_FLR.1.1 E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.6 ATE 类：测试类

8.3.6.1 ATE_COV.2 范围分析

依赖关系： ADV_FSP.1 非形式化功能规范，ATE_FUN.1 功能测试。

开发者行为元素：

ATE_COV.2.1D　开发者将提供测试覆盖范围的分析。

证据的内容和形式元素：

ATE_COV.2.1C　测试覆盖范围的分析应论证测试文档中所标识的测试和功能规范中所描述的 TSF 之间的对应性。

ATE_COV.2.2C　测试覆盖范围的分析应论证功能规范中所描述的 TSF 和测试文档中所标识的测试之间的对应性是完备的。

评估者行为元素：

ATE_COV.2.1 E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.6.2 ATE_DPT.1 测试：高层设计

依赖关系：ADV_HLD.1，概述性高层设计，ATE_FUN.1，功能测试。

开发者行为元素：

ATE_DPT.1.1D　开发者应提供测试深度分析。

证据的内容和形式元素：

ATE_DPT.1.1 C　深度分析应论证测试文档中所标识的测试足以论证该 TSF 运行和高层设计是一致的。

评估者行为元素：

ATE_DPT.1.1　　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.6.3　ATE_FUN.1　功能测试

依赖关系：无依赖关系。

开发者行为元素：

ATE_FUN.1.1 D　　开发者应测试 TSF，并将结果文档化。

ATE_FUN.1.2 D　　开发者应提供测试文档。

证据的内容和形式元素：

ATE_FUN.1.1 C　　测试文档应包括测试计划，测试程序描述，预期的测试结果和实际的测试结果。

ATE_FUN.1.2 C　　测试计划应标识要测试的安全功能，描述要执行的测试目标。

ATE_FUN.1.3 C　　测试过程描述应标识要执行的测试，并描述每个安全功能的测试情况，这些概况包括对于其他测试结果的顺序性依赖。

ATE_FUN.1.4 C　　预期的测试结果应标明成功测试运行后的预期输出。

ATE_FUN.1.5 C　　开发者执行测试的结果应论证每个被测试的安全性功能已按照规定进行了运作。

评估者行为元素：

ATE_FUN.1.1 E　　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

8.3.6.4　ATE_IND.2　独立性测试——抽样

依赖关系：ADV_FSP.1，非形式化功能规范，AGD_ADM.1，管理员指南，AGD_USR.1，用户指南，ATE_FUN.1，功能测试。

开发者行为元素：

ATE_IND.2.1D　　开发者应提供用于测试的 TOE。

证据的内容和形式元素：

ATE_IND.2.1 C　　TOE 应与测试相适应。

ATE_IND.2.2 C　　开发者应提供一个与开发者的 TSF 功能测试中使用的资源相当的集合。

评估者行为元素：

ATE_IND.2.1 E　　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ATE_IND.2.2 E　　评估者应适当测试一个 TSF 子集，以确认 TOE 相应的按照规范运行。

ATE_IND.2.3 E　　评估者应抽样执行测试文档里的测试样本，以验证开发者测试的结果。

8.3.7　AVA 类：脆弱性评定

8.3.7.1　AVA_MSU.1　指南审查

依赖关系：ADO_IGS.1，安装，生成和启动过程，ADV_FSP.1，非形式化功能规范，AGD_ADM.1，管理员指南，AGD_USR.1，用户指南。

开发者行为元素：

AVA_MSU.1.1D　　开发者应提供指导性文档。

证据的内容和形式元素：

AVA_MSU.1.1 C　指导性文档应确定对 TOE 的所有可能的运行方式(包括失败和操作失误后的运行),它们的后果以及对于保持安全运行的意义。

AVA_MSU.1.2 C　指导性文档应是完备的,清晰的,一致的,合理的。

AVA_MSU.1.3 C　指导性文档应列出所有目标环境的假设。

AVA_MSU.1.4 C　指导性文档应列出所有外部安全措施(包括外部程序的,物理的或人员的控制)的要求。

评估者行为元素：

AVA_MSU.1.1 E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

AVA_MSU.1.2 E　评估者应重复所有配置与安装程序,以确认只使用所提供的指导性文档就可让 TOE 安全配置和使用。

AVA_MSU.1.3 E　评估者应决定指导性文档的使用能检测到所有不安全状态。

8.3.7.2 AVA_SOF.1 TOE 安全功能强度评估

依赖关系：ADV_FSP.1 非形式化功能规范,ADV_HLD.1 概述性高层设计。

开发者行为元素：

AVA_SOF.1.1D　开发者应对安全目标中标识的每个具有 TOE 安全功能强度声明的安全机制进行 TOE 安全功能强度分析。

证据的内容和形式元素：

AVA_SOF.1.1 C　对于具有 TOE 安全功能强度声明的每个安全机制,TOE 安全功能强度分析应说明该机制达到或超过保护轮廓/安全目标定义的最低强度。

AVA_SOF.1.2 C　对于具有特定 TOE 安全功能强度声明的每个安全机制,TOE 安全功能强度分析应说明该机制达到或超过保护轮廓/安全目标定义的最低强度。

评估者行为元素：

AVA_SOF.1.1 E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

AVA_SOF.1.2 E　评估者应确认强度声明是正确的。

8.3.7.3 AVA_VLA.1 开发者脆弱性分析

依赖关系：ADV_FSP.1 非形式化功能规范,ADV_HLD.1 概述性高层设计,AGD_ADM.1 管理员指南,AGD_USR.1 用户指南。

开发者行为元素：

AVA_VLA.1.1 D　开发者应分析 TOE 的可交付材料,以寻找用户违反 TSP 的明显途径,并将分析结果文档化。

AVA_VLA.1.2 D　开发者应将明显的脆弱性分析文档化。

证据的内容和形式元素：

AVA_VLA.1.1C　对所有已标识的脆弱性,文档应能说明在所期望的 TOE 环境中无法利用这些脆弱性。

评估者行为元素：

AVA_VLA.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

AVA_VLA.1.2E　评估者应在开发方脆弱性分析的基础上实施穿透性测试,确保已经表述了明显的脆弱性。

9 基本原理

9.1 安全目的基本原理

安全目的基本原理，通过安全目的与威胁之间的关系证明安全目标的合理性和完整性。安全假设向安全威胁的映射关系见表6，所有假设和威胁都至少映射到一个目的。对应的，安全目标向安全假设和威胁的映射规定见表7，所有的目标都至少映射到一个假设或威胁。表7后的文字说明了对抗每一个威胁的安全目的。

表6 TOE安全环境与安全目的映射关系

序号	假设/威胁	目的
1E	正确配置	环境应正确配置
2E	篡改留证	环境篡改留证
1	攻击	自主访问控制，身份标识，安全角色，受保护的功能
2	旁路	消息校验，安全属性管理，功能调用
3	导出	安全导出
4	密码破解	执行密码操作
5	物理破解	篡改识别
6	冒名	身份标识，安全角色，安全导入
7	导入	安全导入
8	密钥生成和销毁	安全密钥管理
9	功能异常	故障时安全
10	修改	限制操作，安全属性管理，安全角色，自主访问控制
11	无安全属性	默认安全属性
12	安全属性变化	修改安全属性
13	未受保护的安全属性	可靠的安全属性
14	残留数据	无可重用信息，安全密钥管理
15	重放	一次性鉴别
16	否认	消息判定
17	自检失败	自检，完整性检查

表7 安全目的与假设和威胁映射关系

序号	目的	假设/威胁
1E	环境正确配置	正确配置
2E	环境篡改留证	篡改留证
1	安全密钥管理	密钥生成和销毁
2	执行密码操作	密码破解

表 7　安全目的与假设和威胁映射关系（续）

序号	目的	假设/威胁
3	自检	自检失败
4	自主访问控制	攻击，修改
5	安全导出	导出
6	故障时安全	功能异常
7	完整性检查	自检失败
8	消息校验	旁路
9	身份标识	攻击，冒名
10	安全导入	导入，冒名
11	功能调用	旁路
12	限制操作	修改
13	消息判定	否认
14	无可重用信息	残留数据
15	默认安全属性	无安全属性
16	修改安全属性	安全属性变化
17	可靠的安全属性	未受保护的安全属性
18	安全属性管理	修改，旁路
19	安全角色	攻击，修改，冒名
20	受保护的功能	攻击
21	一次性鉴别	重放
22	篡改识别	物理破解

攻击：一个攻击者会试图执行一个未授权操作，从而导致 TOE 没有检测到针对加密数据的威胁。“攻击”作为一个威胁，可通过“自主访问控制”“身份标识”“安全角色”和“受保护的功能”四个安全目的来消除。这些目的限制了用户的操作能力，只允许用户进行经过授权的活动：

——自主访问控制：TOE 应能够通过特定的访问控制策略来控制和限制用户对 TOE 数据的访问，该安全目的通过定义的访问控制策略来限制攻击者执行未经授权的操作；

——身份标识：TOE 应唯一的识别所有的用户，并且在授权用户访问 TOE 功能之前，TOE 需要鉴别用户所宣称的身份；

——安全角色：TOE 应管理与安全相关的规则以及与这些规则相关联的用户，该安全目的通过将每一个用户与一个角色关联起来（并据此赋予特定的访问控制策略）来更进一步的支持访问控制策略；

——受保护的功能：TSF 应拥有属于其自身的一块区域用于执行安全功能操作，以避免外部的干扰、篡改以及未经授权的泄露。

旁路：一个未经授权的用户可能会篡改安全属性或其他数据以绕过 TOE 的安全功能，从而未经授权而访问 TOE 的数据。“旁路”作为一个威胁，可通过“消息校验”“安全属性管理”“功能调用”三个目的消除。这三个安全目的使得 TOE 能够检测到数据的篡改，以及阻止未经授权的用户对安全属性或其他数据的篡改：

——消息校验：TOE 应提供检测安全属性或其他数据是否被更改的功能，从而为系统提供了检测数据是否被篡改的能力；

——安全属性管理：TOE 只允许授权用户初始化和修改客体的安全属性值，从而消除了非授权用户进行这些更改的威胁；

——功能调用：TSF 应被 TOE 各功能调用，由于此安全目的要求 TOE 各功能都要调用 TSF，并且不准许被任何用户绕过，因此保护系统免遭非授权用户的篡改。

导出：一个用户或攻击者可能会将数据导出而不附带安全属性或附带的安全属性不够安全，造成导出的数据是错误的并且不能使用。“导出”作为一个威胁，可通过“安全导出”来消除：

——安全导出：当数据被导出 TOE 时，TOE 应保证安全属性随着数据一起被导出，并且这些与数据相关的安全属性值是无歧义的。

密码破解：密码算法可能没有被正确的实现，因此一个用户可能会解密由 TOE 生成的密钥，并未经授权用此密钥去访问加密的数据。“密码破解”作为一个威胁，可通过“执行密码操作”来消除；

——执行密码操作：TOE 应能够执行与密码学相关的操作，这些操作包括 SM3 密码杂凑、HMAC、SM2 数字签名以及签名校验、SM2 加密与解密、SM2 密钥的生成（遵循一定的算法和密钥的长度，密钥的长度应足够大以保证公私密钥对不被破解）。

物理破解：通过与 TOE 物理交互，在物理环境中利用其脆弱性，一个未经授权的个体或 TOE 的用户可能未经授权而泄露或修改 TOE 数据。“物理破解”作为一个威胁，可通过“物理破解”来消除。

——篡改识别：TOE 应具有让用户检测系统部件是否被物理篡改的特性。尽管这个安全目的并不能阻止物理篡改，但它能够在对 TOE 进行物理检查的时候检测出篡改。

冒名：一个未经授权的个体可能伪装成一个已由 TOE 授权的用户，从而获得访问 TOE 数据、密钥以及操作的能力。“冒名”作为一个威胁，可通过“身份标识”“安全角色”和“安全导入”来消除。这三个安全目的要求用户需要通过标识与鉴别，并且限制了用户只能在与之所属角色相关的访问控制策略下进行操作。

——身份标识：TOE 应唯一的识别所有的用户，并且在授权用户访问 TOE 功能之前，TOE 需要鉴别用户所宣称的身份。该安全目的要求鉴别每一个用户以确定每一个用户所属的角色适用的特定的访问控制规则。

——安全角色：TOE 应管理与安全相关的规则以及与这些规则相关联的用户。该安全目的更进一步地将每一个用户与一个角色关联起来，并据此赋予特定的访问控制策略。

——导入：当数据被导入 TOE 时，TOE 应保证与数据关联的安全属性也一同被导入，并且这些数据来源于一个已经被授权的资源。此外，TOE 应根据 TSF 访问控制规则校验这些安全属性。

导入：一个用户或者攻击者可能会将不带有安全属性或带有错误的安全属性的数据导入，造成所有权和鉴别的不确定或错误、系统故障或者运行方式不安全。“导入”作为一个威胁，可通过“安全导入”消除。

——安全导入：当数据被导入 TOE 时，TOE 应保证与数据关联的安全属性也一同被导入，并且这些数据来源于一个已经被授权的资源。此外，TOE 应根据 TSF 访问控制规则校验这些安全属性。

密钥生成和销毁：密钥可能通过一种不安全的方式产生或销毁，从而对密钥构成了危害。“密钥生成和销毁”作为一个威胁，可通过“安全密钥管理”消除。

——安全密钥管理：TOE 应以一种安全的方式产生和销毁密钥。

功能异常：TOE 出现故障时，TOE 的数据可能会被未经授权的个体或者 TOE 的用户修改或者访问。功能异常通过故障时安全消除。

——故障时安全：TOE 应保证在出现与密码学相关的操作失败时或其他故障时，系统仍然处于一个安全状态。

修改：一个攻击者可能会修改 TSF 或者用户数据，例如存储的安全属性或密钥，从而获得访问 TOE 以及 TOE 的数据的能力。攻击者未经授权的更改或破坏信息对信息的完整性构成威胁。“修改”作为一个威胁，可通过“限制操作”“安全属性管理”“安全角色”和“自主访问控制”消除。这些安全目的支持 TOE 限制未经授权的用户的访问，还支持 TOE 通过对一些经过加密的特殊数据进行管理来维护数据和系统的完整性：

——受限操作：TOE 在核实用户身份之前，应限制用户能够进行的操作；

——安全属性管理：TOE 只允许授权用户初始化和修改客体的安全属性值；

——安全角色：TOE 应管理与安全相关的规则以及与这些规则相关联的用户；

——自主访问控制：TOE 应能够通过特定的访问控制策略来控制和限制用户对 TOE 数据的访问。

无安全属性：用户可能会创建一个没有安全属性值的客体。“无安全属性”作为一个威胁，可通过“默认安全属性”消除。

——默认安全属性：当一个客体被创建时，TOE 要求其拥有默认的安全属性。

安全属性变化：用户或攻击者可能未经授权而改动客体的安全属性。“安全属性变化”作为一个威胁，可通过“修改安全属性”消除。

——修改安全属性：TOE 应允许一个授权用户修改某一个已被创建的客体的默认安全属性。

未受保护的安全属性：用户可能会为一个客体设置一个未受保护的安全属性值。“未受保护的安全属性”作为一个威胁，可通过“可靠的安全属性”消除。

——可靠的安全属性：TOE 管理安全属性，并且只允许这些安全属性具有安全的值。

残留数据：当一个数据不再被 TOE 管理的时候（“残留”数据），用户可能未经授权而获得这个数据。残留数据通过无可重用信息，安全密钥管理消除。无可重用信息用于确保在缓冲区或者系统区域中没有残留的数据。安全密钥管理决定了密钥销毁应被执行：

——无重用数据：TOE 应保证没有“可重用”的资源，例如通过将资源重分配给不同的用户，保证在信息容器中或者系统资源中没有“残留”的信息；

——安全密钥管理：TOE 应以一种安全的方式产生和销毁密钥。

重放：一个未经授权的个人，可能通过重放攻击以及中间人攻击而获得标识与鉴别数据，从而能够非法访问系统以及机密数据。“重放”可通过“一次性鉴别”消除。

——一次性鉴别：TOE 应提供一次性鉴别的机制，通过要求重新鉴别来防止重放攻击和中间人攻击。

否认：一个数据的生成者可能会否认产生过此数据以逃避其应承担的责任。“否认”作为一个威胁，可通过“消息判定”来消除。

——消息判定：当 TOE 与一个远程的系统交换数据时，应保证数据的完整性、消息的鉴别以及消息的不可否认性。

自检失败：TOE 可能以一个不安全的状态启动或者进入了一个不安全的状态，使得攻击者能够获得机密数据或者威胁系统。“自检失败”作为一个威胁，可通过“自检”和“完整性检查”来消除。这些安全目的要求 TOE 具有自检和检查数据完整性的功能，以便检测在启动时或正常操作时的不正常状态：

——自检：TOE 应具备检验密码功能是否按照设计的模式运行的能力；

——完整性检查：TOE 应提供对系统完整性和用户数据完整性的周期性检查。

9.2 安全要求基本原理

9.2.1 安全功能要求原理

安全功能要求基本原理，通过安全目的同安全功能要求之间的关系说明了安全功能要求的合理性

和完整性。安全目的至功能组件的映射见表8。

表8 安全目的映射功能组件

序号	目的	功能组件
1	安全密钥管理	FCS_CKM.1 ,FCS_CKM.4
2	执行密码操作	FCS_COP.1
3	自检	FPT_AMT.1,FPT_TST.1
4	自主访问控制	FDP_ACC.1,FDP_ACF.1,FMT_MOF.1,FMT_MTD.1
5	安全导出	FDP_ETC.2
6	故障时安全	FPT_FLS.1,FPT_RCV.4
7	完整性检查	FPT_AMT.1,FPT_TST.1
8	消息校验	FCS_COP.1:4
9	身份标识	FIA_UAU.1,FIA_UID.1,FIA_ATD.1
10	安全导入	FDP_ITC.2,FPT_TDC.1,FTP_TRP.1
11	功能调用	FPT_RVM.1
12	限制操作	FIA_UAU.1,FIA_UID.1
13	消息判定	FCO_NRO.2,FDP_ETC.2
14	无可重用信息	FDP_RIP.2
15	默认安全属性	FMT_MSA.3
16	修改安全属性	FMT_MSA.3
17	可靠的安全属性	FMT_MSA.2,FPT_TDC.1
18	安全属性管理	FMT_MSA.3,FMT_MSA.1
19	安全角色	FMT_SMR.2,FIA_ATD.1
20	受保护的功能	FPT_SEP.1
21	一次性鉴别	FIA_UAU.4,FIA_UAU.6,FPT_RPL.1
22	篡改识别	FPT_PHP.1

安全密钥管理:TOE应以一种安全的方式产生和销毁密钥。作为一个安全目的,“安全密钥管理”映射到如下安全功能要求:

——FCS_CKM.1:密钥产生,TOE应按照SM2/SM4算法,生成指定长度的密钥;

——FCS_CKM.4:密钥销毁,TOE应依据安全的密钥销毁方法销毁密钥。

执行密码操作:TOE应能够执行与密码学相关的操作,这些操作包括SM3密码杂凑、HMAC、SM2数字签名以及签名校验、SM2/SM4加密与解密、SM2/SM4密钥的生成。作为一个安全目的,“执行密码操作”映射到如下安全功能要求:

——FCS_COP.1:密码运算,TOE应能够执行各类密码运算,包括SM3密码杂凑、SM2加解密操作、SM2签名和签名校验、HMAC以及SM4对称密码的加解密操作,覆盖了所有必需遵循的密码运算、密钥长度和标准。

自检:TOE应具备检验密码功能是否按照设计的模式运行的能力。作为一个安全目的,“自检”映射到如下安全功能要求:

——FPT_AMT.1:抽象机测试,TOE应能够测试在抽象机下的密码运算部分;

——FPT_TST.1：TSF 检测，TOE 应能够实施自检，以确保密钥运算正确运行。检测在启动期间或周期性的进行，这些测试包括对密码运算的已知答案测试，以及对随机数的统计测试。额外的测试可包括公私密钥对的生成，以及密钥对的加解密一致性测试、密钥入口测试和密钥完整性测试。

自主访问控制：TOE 应能够通过特定的访问控制策略来控制和限制用户对 TOE 数据的访问。作为一个安全目的，“自主访问控制”映射到如下安全功能要求：

——FDP_ACC.1：子集访问控制，TOE 应加强对主体、客体和运算的保护性访问控制；

——FDP_ACF.1：基于安全属性的访问控制，TOE 应能够基于 TCM 内部属性值 TCM_AUTH_DATA_USAGE 和 TCM_KEY_USAGE 的实施访问控制；

——FMT_MOF.1：安全功能行为的管理，安全目标的制定者应指定由 TCM 的所有者限制的功能列表；

——FMT_MTD.1：TSF 数据的管理，TOE 应确保 TSF 数据对于授权用户是可访问的。

安全导出：当数据被导出 TOE 时，TOE 应保证安全属性随数据一起被导出，并且这些与数据相关的安全属性值是无歧义的。作为一个安全目的，“安全导出”映射到如下安全功能要求：

——FDP_ETC.2：有安全属性的用户数据输出，数据输出到 TSF 外时，安全属性与数据应确切关联。

故障时安全：TOE 应保证在出现与密码学相关的操作失败时或其他故障时，系统仍然处于一个安全状态。作为一个安全目的，“故障时安全”映射到如下安全功能要求：

——FPT_FLS.1：带保存安全状态的失败，TSF 应在失败发生时保存一个安全状态；

——FPT_RCV.4：功能恢复，TOE 的功能执行应能够被成功完成，或者针对指明的失败情况恢复到安全状态。

完整性检查：TOE 应提供对系统完整性和用户数据完整性的周期性检查。作为一个安全目的，“完整性检查”映射到如下安全功能要求：

——FPT_AMT.1：抽象机测试，TOE 应测试在抽象机下的密码运算部分；

——FPT_TST.1：TSF 检测，TOE 应执行自检过程以确保密钥运算正确运行。检测应在启动时或周期性地进行，这些测试包括对密码运算的已知答案测试，以及对随机数的统计测试。额外的测试可包括公私密钥对的生成，以及密钥对的加解密一致性测试、密钥入口测试、密钥完整性测试。

消息校验：TOE 应提供检测安全属性或其他数据是否被更改的功能。作为一个安全目的，“消息校验”映射到如下安全功能要求：

——FCS_COP.1.1：TOE 应根据引用的标准提供 HMAC 功能，使其具有检测安全属性或其他数据被改动的能力。

身份标识：TOE 应唯一的识别所有的用户，并且在授权用户访问 TOE 功能之前，TOE 需要鉴别用户所宣称的身份。作为一个安全目的，“身份标识”映射到如下安全功能要求：

——FIA_UAU.1：鉴别定时，除了一些已经明确定义的行为，用户在进行其他行为之前应被成功的鉴别；

——FIA_UID.1：标识定时，除了一些已经明确定义的行为，用户在进行其他行为之前应被成功的识别；

——FIA_ATD.1：用户属性定义，通过要求用户属性来支持 FIA_UAU.1 和 FIA_UID.1。鉴别数据被定义为用户属性，在这里，鉴别数据与一个代表用户的特定密钥相关联。

安全导入：当数据被导入 TOE 时，TOE 应保证与数据关联的安全属性也一同被导入，并且这些数据来源于一个已经被授权的资源。此外，TOE 应根据 TOE 访问控制规则校验这些安全属性。“安全导入”映射到如下安全功能要求：

——FDP_ITC.2：有安全属性的用户数据输入，导入至 TOE 的数据应具有安全属性，这些安全属性包括基于密钥的鉴别数据。

——FPT_TDC.1：TSF 间基本 TSF 数据的一致性，定义了安全属性，当导入数据时这些安全属性应被一致性解释。

——FTP_TRP.1：可信路径，TOE 应确保接收的数据来源于一个已被授权的数据源。FDP_ITC.2 依赖于可信路径，数据的导入需要一条可信路径。

功能调用：TSF 应被所有的活动调用。作为一个安全目的“功能调用”映射到如下安全功能要求：

——FPT_RVM.1：TSP 的不可旁路性，保证 TSC 范围内的功能操作被执行前，TSP 功能被调用并成功执行。

限制操作：TOE 在核实用户身份之前，应限制用户能够进行的操作。作为一个安全目的“限制操作”映射到如下安全功能要求：

——FIA_UAU.1：鉴别定时，除了一些已经明确定义的行为，用户在进行其他行为之前应被成功的鉴别。

——FIA_UID.1：标识定时，除了一些已经明确定义的行为，用户在进行其他行为之前应被成功的识别。

消息判定：当 TOE 与一个远程的系统交换数据时，应保证数据的完整性，消息的鉴别以及消息的不可否认性。作为一个安全目的“消息判定”映射到如下安全功能要求：

——FCO_NRO.2：强制原发证明；

——FDP_ETC.2：有安全属性的用户数据输出。

无可重用信息：TOE 应保证没有“可重用”的资源。例如通过将资源重分配给不同的用户，保证在信息容器中或者系统资源中没有“残留”的信息。作为一个安全目的“无可重用信息”映射到如下安全功能要求：

——FDP_RIP.2：完全残余信息保护，任何资源所承载的过往信息都应不可再用。

默认安全属性：当一个客体被创建时，TOE 要求其拥有默认的安全属性。作为一个安全目的“默认安全属性映射到如下安全功能要求：

——FMT_MSA.3：静态属性初始化，TOE 应确保安全属性已被生成并且已经设置了默认值。

修改安全属性：TOE 应允许一个授权用户修改某一个已被创建的客体的默认安全属性。作为一个安全目的“修改安全”属性映射到如下安全功能要求：

——FMT_MSA.3：静态属性初始化，确保安全属性已被生成并且已经设置了默认值，授权用户可更改默认值。

可靠的安全属性：TOE 管理安全属性，并且只允许这些安全属性具有安全的值。作为一个安全目的“可靠的安全属性”映射到如下安全功能要求：

——FMT_MSA.2：受保护的安全属性，安全属性应只能具有安全的值；

——FPT_TDC.1：TSF 间基本 TSF 数据应保持一致性。

安全属性管理：TOE 只允许授权用户初始化和修改客体的安全属性值。作为一个安全目的“安全属性管理”映射到：

——FMT_MSA.3：静态属性初始化，TOE 应确保安全属性已被生成且已经设置了默认值；

——FMT_MSA.1：安全属性的管理，TOE 中数据等访问客体应具有安全属性。

安全角色：TOE 应管理与安全相关的规则以及与这些规则相关联的用户。作为一个安全目的“安全角色”映射到如下安全功能要求：

——FMT_SMR.2：安全角色限制，TSF 应管理角色以及与这些角色相关联的用户；

——FIA_ATD.1：用户属性定义，鉴别所依赖的数据被定义为用户属性，鉴别数据应与一个代表用户的特定密钥相关联。

受保护的功能：TSF 应拥有属于其自身的一块区域用于执行安全功能操作，以避免外部的干扰、篡改以及未经授权的泄露。作为一个安全目的“受保护的功能”映射到如下安全功能要求：

——FPT_SEP.1：TSF 域分离，TSF 应实现自我保护。

一次性鉴别：TOE 应提供一次性鉴别的机制，通过要求重新鉴别来防止重放攻击和中间人攻击。作为一个安全目的“一次性鉴别”映射到如下安全功能要求：

——FIA_UAU.4：一次性鉴别机制，TOE 应防止鉴别数据的重用；

——FIA_UAU.6：重鉴别，对于每一个要求鉴别用户的命令，TOE 都应对用户再次进行鉴别；

——FPT_RPL.1：重放检测，TOE 应防止重放攻击。

篡改识别：TOE 应具有让用户检测系统部件是否被物理篡改的特性。作为一个安全目的“篡改识别”映射到如下安全功能要求：

——FPT_PHP.1：物理攻击的被动检测，TOE 的物理篡改应是可检测的。

9.2.2 安全保证要求原理

本文件选择 GB/T 18336 中的评估保证级 3 级作为对 TOE 的安全要求。这种选择的原因在于，TOE 自身要求达到中等级别的安全等级，能够对 TOE 和它的开发过程的全面的审查，但是不需要为达到该安全等级重新设计和实现 TOE。

评估保证级 3 级利用 TOE 功能和接口规范、用户指南、高层设计来理解安全行为，并通过分析安全功能来提供保证安全。该分析过程由以下各部分提供支持：TOE 安全功能独立性测试、基于功能规范和高层设计的开发者测试的证据、对开发者测试结果的选择性独立地确认、功能强度分析、开发者寻找明显的脆弱性的证据。

增强的评估保证级 3 级增加了 ADV_SPM.1 组件和 ALC_FLR.1 组件。增加 ADV_SPM.1 组件是因为安全功能组件 FMT_SMR.2 依赖该组件。增加的 ALC_FLR.1 用于提供基本缺陷纠正。

9.2.3 依赖性原理

本文件所使用的安全功能要求及其所依赖的组件关系见表 9。

表 9 安全功能要求依赖

序号	功能要求	依赖的组件
1	FCO_NRO.2	FIA_UID.1
2	FCS_CKM.1	FCS_COP.1，FCS_CKM.4，FMT_MSA.2
3	FCS_CKM.4	FCS_CKM.1，FMT_MSA.2
4	FCS_COP.1	FCS_CKM.1，FCS_CKM.4，FMT_MSA.2
5	FDP_ACC.1	FDP_ACF.1
6	FDP_ACF.1	FDP_ACC.1，FMT_MSA.3
7	FDP_ETC.2	FDP_ACC.1
8	FDP_ITC.2	FDP_ACC.1，FTP_TRP.1，FPT_TDC.1
9	FDP_RIP.2	无依赖性
10	FIA_ATD.1	无依赖性
11	FIA_UAU.1	FIA_UID.1
12	FIA_UAU.4	无依赖性

表 9　安全功能要求依赖（续）

序号	功能要求	依赖的组件
13	FIA_UAU.6	无依赖性
14	FIA_UID.1	无依赖性
15	FMT_MOF.1	FMT_SMR.1
16	FMT_MSA.1	FDP_ACC.1，FMT_SMR.1
17	FMT_MSA.2	ADV_SPM.1，FDP_ACC.1，FMT_MSA.1,FMT_SMR.1
18	FMT_MSA.3	FMT_MSA.1，FMT_SMR.1
19	FMT_MTD.1	FMT_SMR.1
20	FMT_SMR.2	无依赖性
21	FPT_AMT.1	无依赖性
22	FPT_FLS.1	ADV_SPM.1
23	FPT_PHP.1	FMT_MOF.1
24	FPT_RCV.4	ADV_SPM.1
25	FPT_RPL.1	无依赖性
26	FPT_RVM.1	无依赖性
27	FPT_SEP.1	无依赖性
28	FPT_TDC.1	无依赖性
29	FPT_TST.1	FPT_AMT.1
30	FTP_TRP.1	无依赖性

9.2.4　以安全目的为基础的安全功能要求

本文件中涉及的安全功能要求与对应的安全目的的映射关系见表 10。

表 10　安全功能要求映射安全目的

序号	功能要求	目的
1	FCO_NRO.2	消息判定
2	FCS_CKM.1	安全密钥管理
3	FCS_CKM.4	安全密钥管理
4-1	FCS_COP.1;1	执行密码操作
4-2	FCS_COP.1;2	执行密码操作
4-3	FCS_COP.1;3	执行密码操作
4-4	FCS_COP.1;4	执行密码操作，消息校验
5	FDP_ACC.1	自主访问控制
6	FDP_ACF.1	自主访问控制
7	FDP_ETC.2	安全导出，消息判定

表 10　安全功能要求映射安全目的（续）

序号	功能要求	目的
8	FDP_ITC.2	安全导入
9	FDP_RIP.2	无可重用信息
10	FIA_ATD.1	身份标识，安全角色
11	FIA_UAU.1	身份标识，限制操作
12	FIA_UAU.4	一次性鉴别
13	FIA_UAU.6	一次性鉴别
14	FIA_UID.1	身份标识，限制操作
15	FMT_MOF.1	自主访问控制
16	FMT_MSA.1	安全属性管理
17	FMT_MSA.2	可靠的安全属性
18	FMT_MSA.3	安全属性管理，默认安全属性，修改安全属性
19	FMT_MTD.1	自主访问控制
20	FMT_SMR.2	安全角色
21	FPT_AMT.1	自检，完整性检查
22	FPT_FLS.1	故障时安全
23	FPT_PHP.1	篡改识别
24	FPT_RCV.4	故障时安全
25	FPT_RPL.1	一次性鉴别
26	FPT_RVM.1	功能调用
27	FPT_SEP.1	受保护的功能
28	FPT_TDC.1	可靠的安全属性，安全导入
29	FPT_TST.1	自检，完整性检查
30	FTP_TRP.1	安全导入

参 考 文 献

[1] 《可信计算密码支撑平台功能与接口规范》，2007.

[2] 《可信计算平台密码技术规范》(简称 TCM/TSM 规范)，2007.

[3] Common Criteria for Information Technology Security Evaluation，Part 1：Introduction and General Model；Version 3.1，Revision 1，CCMB-2006-09-001，September 2006.

[4] Common Criteria for Information Technology Security Evaluation，Part 2：Security Functional Requirements；Version 3.1，Revision 2，CCMB-2007-09-002，September 2007.

[5] Common Criteria for Information Technology Security Evaluation，Part 3：Security Assurance Requirements；Version 3.1，Revision 2，CCMB-2007-09-003，September 2007.

[6] Common Methodology for Information Technology Security Evaluation Methodology，Evaluation Methodology，Version 3.1，Revision 2，CCMB-2007-09-004，September 2007.

[7] IEEE P1363-2000，Standard Specifications for Public Key Cryptography，Institute of Electrical and Electronics Engineers，Inc.(note reaffirmation PAR is actual running).

[8] Trusted Computing Platform Alliance (TCPA)，Trusted Platform ModuleProtection Profile，Version 1.9.7，July 1，2002.

[9] Trusted Computing GroupProtection Profile，PC Client Specific Trusted Platform ModuleTPM Family 1.2；Level 2，Version：1.1；July 10，2008.

中华人民共和国密码
行业标准
可信密码模块保护轮廓
GM/T 0082—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.25 字数 64 千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35973 定价 36.00 元

GM/T 0082-2020

码上扫一扫 正版服务到