ICS 35.240
L 70

DB43

湖　南　省　地　方　标　准

DB43/T 1841—2020

信息安全技术
区块链加密安全技术测评要求

Information security technology - Evaluation requirements for blockchain encryption security technology

2020-09-30发布　　2020-12-30实施

湖南省市场监督管理局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020给出的规则起草。

本文件由中共湖南省委网络安全和信息化委员会办公室提出。

本文件由湖南省区块链和分布式记账技术标准化技术委员会（筹）归口。

本文件起草单位：湖南链信安科技有限公司、湖南天河国云科技有限公司、湖南省东方区块链安全技术检测中心、湖南省人民政府发展研究中心、湖南天河云链科技有限公司。

本文件主要起草人：杨征、李财、陈昕、谭林、聂璐璐、梁琪、梁亮、汪武、聂朗、尹海波、黄帅、柳兴、郭慧、殷新文、丁雅琪、沈浪、张祥、宋姝、姜载乐、刘齐平、郑婷婷、胡钦、邹曼瑜等。

信息安全技术　区块链加密安全技术测评要求

1　范围

本文件规定了区块链加密安全技术测评指标要求。包括第一级、第二级、第三级、第四级区块链加密安全技术测评要求。

本文件适用于测评机构对区块链加密安全进行的测评工作，也适用于区块链技术开发者参考使用。

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 17964—2008　信息安全技术　分组密码算法的工作模式

GB/T 25069—2010　信息安全技术　术语

GB/T 28448—2019　信息安全技术　网络安全等级保护测评要求

GM/T 0050—2016　密码设备管理　设备管理技术规范

3　术语和定义

GB/T 17964—2008、GB/T 25069—2010、GB/T 28448—2019 界定的下列术语和定义适用于本文件。

3.1

测评对象　target of testing and evaluation

等级测评过程中不同测评方法作用的对象，主要涉及相关配套制度文档、设备设施及人员等。

[GB/T 28448—2019]

3.2

等级测评　testing and evaluation for classified cybersecurity protection

测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对未涉及国家秘密的网络安全等级保护状况进行检测评估的活动。

[GB/T 28448—2019]

3.3

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

[GB/T 17964—2008]

3.4

解密　decipherment/decryption

加密过程对应的逆过程。

[GB/T 17964—2008]

3.5

密钥　key

密钥是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数。

[GB/T 17964—2008]

3.6

密钥管理　key management

根据安全策略，实施并运用对称密钥材料进行产生、等级、认证、注销、分发、安装、存储、归档、撤销、衍生、销毁和恢复的服务。

[GB/T 17964—2008]

3.7

公开密钥/公钥　public key

在某一实体的非对称密钥对中，能够公开的密钥。

[GB/T 25069—2010]

3.8

数字签名　digital signature

附加在数据单元上的数据，或是对数据单元所做的密码变换，这种数据或变换允许数据单元的接受者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接受者）伪造或抵赖。

[GB/T 25069—2010]

4　等级测评概述

4.1　等级测评方法

等级测评实施的基本方法是针对待定的测评对象，采用相关的测评手段，遵从一定的测评规程，获取需要的证据数据，给出是否达到特定级别安全保护能力的评判。

本标准中针对每一个要求项的测评就构成一个单项测评，针对某个要求项的所有具体测评内容构成测评实施。根据调研结果，分析等级保护对象的业务流程和数据流，确定测评工作范围。结合等级保护对象的安全级别进行综合分析，测评对象可以根据类别加以描述，包括密码算法、加密设备、密钥管理以及账本安全。

本标准账中每个级别测评要求都包括密码算法安全测评要求、加密设备及配置测评要求、密钥管理安全测评要求以及账本安全测评要求四部分内容。

4.2　单项测评

单项测评是针对各安全要求项的测评，支持测评结果的可重复性和可再现性。本标准中单项测评包括测评指标、测评对象、测评实施和单元判定结果构成。

5　第一级测评要求

5.1　密码算法使用安全测评要求

5.1.1　对称加密算法

该测评单元包括以下要求：

a） 测评指标：使用对称加密算法时应保证数据的安全加密。
b） 测评对象：对称加密算法模块。
c） 测评实施包括以下内容：
1） 是否使用国际 AES 或国密 SM4、SM7 等安全级别及以上的对称加密算法。
d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.1.2 非对称加密算法

a） 测评指标：使用非对称加密算法时应保证数据的安全加密。
b） 测评对象：非对称加密算法模块。
c） 测评实施包括以下内容：
1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的非对称加密算法。
d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.1.3 数字签名验签算法

该测评单元包括以下要求：
a） 测评指标：使用数字签名验签算法时应保证安全性。
b） 测评对象：数字签名验签算法模块。
c） 测评实施包括以下内容：
1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的加密算法进行数字签名/验签；
2） 是否支持基于硬件实现的数字签名/验签设备。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.1.4 数字摘要算法

该测评单元包括以下要求：
a） 测评指标：使用数字摘要算法时应保证安全性。
b） 测评对象：数字摘要算法模块。
c） 测评实施包括以下内容：
1） 是否使用国际 SHA256 或国密 SM3 安全级别及以上的哈希散列算法；
d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2 加解密设备及配置安全测评要求

5.2.1 加密设备物理结构

该测评单元包括以下要求：
a） 测评指标：应保证加密设备物理结构安全性。
b） 测评对象：加密设备物理结构
c） 测评实施包括以下内容：
1） 加密设备是否具有防拆、防撬结构设计。

d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.2.2 加密设备配置

该测评单元包括以下要求：

a） 测评指标：应保证加密设备使用时的安全性。

b） 测评对象：加密设备配置策略。

c） 测评实施包括以下内容：

1） 加密设备使用的加密算法是否符合本文档5.1的要求。

d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.3 密钥管理安全测评要求

5.3.1 密钥生成

该测评单元包括以下要求：

a） 测评指标：应保证系统产生密钥的安全性。

b） 测评对象：密钥生成方式。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数发生器、密钥导出函数、标准的密钥协商机制等安全的方式生成密钥。

d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.3.2 密钥使用

该测评单元包括以下要求：

a） 测评指标：保证密钥使用的安全性。

b） 测评对象：密钥使用方式。

c） 测评实施包括以下内容：

1） 密钥是否通过密文形式进行分发；

2） 所有涉及密钥的敏感操作是否避免使用分支操作；

3） 是否能够正确、有效地导入密钥。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.3.3 密钥更新

该测评单元包括以下要求：

a） 测评指标：保证系统密钥更新的安全性。

b） 测评对象：密钥更新方式。

c） 测评实施包括以下内容：

1） 是否具有密钥更新策略；

2） 系统管理员是否可以手动更新密钥；

3） 是否设置系统定期自动更新密钥策略，且系统管理员定期检查更新状态并手动更新密钥。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.3.4 密钥存储

该测评单元包括以下要求：

a） 测评指标：保证密钥存储的安全性。

b） 测评对象：密钥存储方式。

c） 测评实施包括以下内容：

1） 密钥是否以密文形式存储；

2） 密钥在内存中是否只保留一份；

3） 密钥存储是否具备校验能力。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.3.5 密钥备份

该测评单元包括以下要求：

a） 测评指标：保证密钥备份的安全性。

b） 测评对象：密钥备份机制。

c） 测评实施包括以下内容：

1） 是否具有密钥备份机制。

d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.3.6 密钥销毁

该测评单元包括以下要求：

a） 测评指标：保证密钥正确销毁。

b） 测评对象：密钥销毁机制。

c） 测评实施包括以下内容：

1） 是否能够根据实际需求，正确、有效地清除所存储的密钥；

2） 密钥销毁过程是否不会泄露密钥相关信息。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

5.4 账本安全测评要求

5.4.1 账本存储

该测评单元包括以下要求：

a） 测评指标：保证区块链账本存储具备持久化。

b） 测评对象：区块链账本存储方式。

c） 测评实施包括以下内容：

1） 区块链账本是否具备存储持久化能力，例如利用账本存储数据的时间长短等方式判断。

d） 测评判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

5.4.2 账本记录

该测评单元包括以下要求：

a） 测评指标：保证账本记录的完整性、一致性。

b） 测评对象：区块链账本记录方式。

c） 测评实施包括以下内容：

1） 每个节点是否拥有完整的数据记录；

2） 拥有完整数据记录的各节点的数据是否保持一致。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6 第二级测评要求

6.1 密码算法安全测评要求

6.1.1 对称加密算法

该测评单元包括以下要求：

a） 测评指标：使用对称加密算法时应保证数据的安全加密。

b） 测评对象：对称加密算法模块。

c） 测评实施包括以下内容：

1） 是否使用国际 AES 或国密 SM4、SM7 等安全级别及以上的对称加密算法；

2） 对称加密算法密钥长度是否符合用户实际需求级别。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.2 非对称加密算法

该测评单元包括以下要求：

a） 测评指标：使用非对称加密算法时应保证数据的安全加密；

b） 测评对象：非对称加密算法模块；

c） 测评实施包括以下内容：

1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的非对称加密算法；

2） 非对称加密算法密钥长度是否符合用户实际需求级别。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.3 数字签名验签算法

该测评单元包括以下要求：

a） 测评指标：使用数字签名验签算法时应保证安全性。

b） 测评对象：数字签名验签算法模块。

c） 测评实施包括以下内容：

1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的加密算法进行数字签名/验签；

2） 是否采用本地签名方式；

3） 是否未使用已被证明不安全的加密算法。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.1.4 数字摘要算法

该测评单元包括以下要求：

a） 测评指标：使用数字摘要算法时应保证安全性。

b） 测评对象：数字摘要算法策略结构文档、数字摘要算法功能说明文档等。

c） 测评实施包括以下内容：

1） 是否使用国际 SHA256 或国密 SM3 安全级别及以上的哈希散列算法；

2） 是否未使用已被证明不安全的数字摘要算法。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.2 加解密设备及配置安全测评要求

6.2.1 加密设备物理结构

该测评单元包括以下要求：

a） 测评指标：应保证加密设备物理结构安全性。

b） 测评对象：加密设备物理结构。

c） 测评实施包括以下内容：

1） 加密设备是否具有防拆、防撬结构设计；

2） 加密设备是否具备紧急情况下人工毁钥装置。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.2.2 加密设备配置

该测评单元包括以下要求：

a） 测评指标：应保证加密设备使用时的安全性。

b） 测评对象：加密设备使用。

c） 测评实施包括以下内容：

1） 加密设备使用的加密算法是否符合本文档 6.1 的要求；

2） 加密设备是否得到国家密码管理主管部门认证。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3 密钥管理安全测评要求

6.3.1 密钥生成

该测评单元包括以下要求：

a） 测评指标：保证系统产生的密钥安全性。

b） 测评对象：密钥生成方式。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数发生器、密钥导出函数、标准的密钥协商机制等安全的方式生成密钥；
2） 如果采用安全的随机数发生器方式时，密钥是否由符合 GM/T 0050 要求的随机数产生相关标准内容。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.2 密钥使用

该测评单元包括以下要求：

a） 测评指标：保证密钥使用的安全性。
b） 测评对象：密钥使用方式。
c） 测评实施包括以下内容：
1） 密钥是否通过密文形式进行分发；
2） 所有涉及密钥的敏感操作是否避免使用分支操作；
3） 是否能够正确、有效地导入密钥；
4） 是否只能使用密码算法访问密钥。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.3 密钥更新

该测评单元包括以下要求：

a） 测评指标：保证系统密钥更新的安全性。
b） 测评对象：密钥更新方式。
c） 测评实施包括以下内容：
1） 是否具有密钥更新策略；
2） 系统管理员是否可以手动更新密钥；
3） 是否设置系统定期自动更新密钥策略，且系统管理员定期检查更新状态并手动更新密钥；
4） 是否严格按照密钥更新策略进行更新。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.4 密钥存储

该测评单元包括以下要求：

a） 测评指标：保障密钥存储的安全性。
b） 测评对象：密钥存储方式。
c） 测评实施包括以下内容：
1） 密钥是否以密文形式存储；
2） 密钥在内存中是否只保留一份；
3） 密钥存储是否具备校验能力；
4） 存储的密钥相关信息是否存放在可控且专用的存储区域，且具有防止通过物理接口和逻辑接口对密钥进行非法访问的安全机制；
5） 需要长期存储的明文密钥是否存储于物理安全模块中，当物理安全模块失效时，明文密钥应立即失效。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.5 密钥备份

该测评单元包括以下要求：

a） 测评指标：保证密钥备份的安全性。

b） 测评对象：密钥备份机制。

c） 测评实施包括以下内容：

1） 是否具有密钥备份机制；

2） 备份密钥是否通过密文形式进行存储。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.3.6 密钥销毁

该测评单元包括以下要求：

a） 测评指标：保证密钥正确销毁。

b） 测评对象：密钥销毁机制。

c） 测评实施包括以下内容：

1） 是否能够根据实际需求，正确、有效地清除所存储的密钥；

2） 密钥销毁过程是否不会泄露密钥相关信息；

3） 在接到外部合法自毁指令时是否能够有效、可靠地完成密钥和敏感信息的自毁。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

6.4 账本安全测评要求

6.4.1 账本存储

该测评单元包括以下要求：

a） 测评指标：保证区块链账本存储具备持久化能力。

b） 测评对象：区块链账本存储方式。

c） 测评实施包括以下内容：

1） 区块链账本是否具备存储持久化能力，例如利用账本存储数据的时间长短等方式判断。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

6.4.2 账本记录

该测评单元包括以下要求：

a） 测评指标：应保证账本记录的完整性、一致性。

b） 测评对象：区块链账本记录类文档及操作说明文档。

c） 测评实施包括以下内容：

1） 每个节点是否拥有完整的数据记录；

2） 拥有完整数据记录的各节点的数据是否保持一致。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分

符合本测评单元指标要求。

7 第三级测评要求

7.1 密码算法安全测评要求

7.1.1 对称加密算法

该测评单元包括以下要求：

a） 测评指标：使用对称加密算法时应保证数据的安全加密。

b） 测评对象：对称加密算法模块。

c） 测评实施包括以下内容：

1） 是否使用国际 AES 或国密 SM4、SM7 等安全级别及以上的对称加密算法；

2） 对称加密算法密钥长度是否符合用户实际需求级别；

3） 对称加密算法模块是否可切换、可替换。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.2 非对称加密算法

该测评单元包括以下要求：

a） 测评指标：使用非对称加密算法时应保证数据的安全加密。

b） 测评对象：非对称加密算法模块。

c） 测评实施包括以下内容：

1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的非对称加密算法；

2） 非对称加密算法密钥长度是否符合用户实际需求级别；

3） 非对称加密算法模块是否可切换、可替换。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.3 数字签名验签算法

该测评单元包括以下要求：

a） 测评指标：使用数字签名验签算法时应保证安全性。

b） 测评对象：数字签名验签算法模块。

c） 测评实施包括以下内容：

1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的加密算法进行数字签名/验签；

2） 是否支持基于硬件实现的数字签名/验签设备；

3） 是否采用本地签名方式；

4） 是否未使用已被证明不安全的加密算法；

5） 数字签名算法安全性是否达到用户实际需求级别。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.1.4 数字摘要算法

该测评单元包括以下要求：

a） 测评指标：使用数字摘要算法时应保证安全性。

b） 测评对象：数字摘要算法模块。

c） 测评实施包括以下内容：

1） 是否使用国际 SHA256 或国密 SM3 安全级别及以上的哈希散列算法；

2） 是否支持基于硬件实现的哈希散列求解设备；

3） 是否未使用已被证明不安全的数字摘要算法。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2 加解密设备及配置安全测评要求

7.2.1 加解密设备物理结构

该测评单元包括以下要求：

a） 测评指标：应保证加密设备物理结构安全性。

b） 测评对象：加密设备物理结构。

c） 测评实施包括以下内容：

1） 加密设备是否具有防拆、防撬结构设计；

2） 加密设备是否具备紧急情况下人工毁钥装置；

3） 加密设备随意开关电源是否不会造成系统损坏、崩溃等后果。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.2.2 加密设备配置

该测评单元包括以下要求：

a） 测评指标：应保证加密设备使用时的安全性。

b） 测评对象：加密设备使用。

c） 测评实施包括以下内容：

1） 加密设备使用的加密算法是否符合 7.1 的要求；

2） 加密设备是否得到国家密码管理主管部门认证；

3） 加密设备的私钥是否不能被导出。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3 密钥管理安全测评要求

7.3.1 密钥生成

该测评单元包括以下要求：

a） 测评指标：保证系统产生的密钥安全性。

b） 测评对象：密钥生成方式。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数发生器、密钥导出函数、标准的密钥协商机制等安全的方式生成密

钥；

2） 如果采用安全的随机数发生器方式时，密钥是否由符合 GM/T 0050 要求的随机数产生；

3） 如果采用密钥导出函数时，是否使用 Bcrypt 算法、Scrypt 算法或 Argon2 算法等足够复杂的密钥生成算法；

4） 如果采用标准的密钥协商机制方式时，是否采用多方参与密钥协商方式一同决定密钥。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.2 密钥使用

该测评单元包括以下要求：

a） 测评指标：保证密钥使用的安全性。

b） 测评对象：密钥使用方式。

c） 测评实施包括以下内容：

1） 密钥是否通过密文形式进行分发；

2） 所有涉及密钥的敏感操作是否避免使用分支操作；

3） 是否能够正确、有效地导入密钥；

4） 是否只能使用密码算法访问密钥；

5） 是否能够根据密钥类型和使用场景合理的使用密钥。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.3 密钥更新

该测评单元包括以下要求：

a） 测评指标：保证系统密钥可更新。

b） 测评对象：密钥生成方式。

c） 测评实施包括以下内容：

1） 是否具有密钥更新策略；

2） 系统管理员是否可以手动更新密钥；

3） 是否设置系统定期自动更新密钥策略，且系统管理员定期检查更新状态并手动更新密钥；

4） 是否严格按照密钥更新策略进行更新；

5） 密钥更新是否不会增加其它密钥的泄露风险。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.4 密钥存储

该测评单元包括以下要求：

a） 测评指标：保障密钥存储的安全性。

b） 测评对象：密钥存储方式。

c） 测评实施包括以下内容：

1） 密钥是否以密文形式存储；

2） 密钥在内存中是否只保留一份；

3） 密钥存储是否具备校验能力；

4） 存储的密钥相关信息是否存放在可控且专用的存储区域，且具有防止通过物理接口和逻辑接口对密钥进行非法访问的安全机制；
5） 需要长期存储的明文密钥是否存储于物理安全模块中，当物理安全模块失效时，明文密钥应立即失效；
6） 密钥分量在生命周期内是否隔离存储于不同介质中。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.5 密钥备份

该测评单元包括以下要求：

a） 测评指标：保证密钥备份的安全性。
b） 测评对象：密钥备份机制。
c） 测评实施包括以下内容：
1） 是否具有密钥备份机制；
2） 备份密钥是否通过密文形式进行存储。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.3.6 密钥销毁

该测评单元包括以下要求：

a） 测评指标：保证密钥正确销毁。
b） 测评对象：密钥销毁机制。
c） 测评实施包括以下内容：
1） 是否能够根据实际需求，正确、有效地清除所存储的密钥；
2） 密钥销毁过程是否不会泄露密钥相关信息；
3） 在接到外部合法自毁指令时是否能够有效、可靠地完成密钥和敏感信息的自毁。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4 账本安全测评要求

7.4.1 账本存储

该测评单元包括以下要求：

a） 测评指标：保证区块链账本存储具备持久化、可追溯性。
b） 测评对象：区块链账本存储方式。
c） 测评实施包括以下内容：
1） 区块链账本是否具备存储持久化能力，例如利用账本存储数据的时间长短等方式判断；
2） 区块链账本是否能溯源原始数据位置。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

7.4.2 账本记录

该测评单元包括以下要求：

a） 测评指标：保证账本记录的完整性、一致性、安全性。
b） 测评对象：区块链账本记录方式。
c） 测评实施包括以下内容：
1） 每个节点是否拥有完整的数据记录；
2） 拥有完整数据记录的各节点的数据是否保持一致。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8 第四级测评要求

8.1 密码算法使用安全测评要求

8.1.1 对称加密算法

该测评单元包括以下要求：
a） 测评指标：对称加密算法使用时应保证数据的安全加密。
b） 测评对象：对称加密算法使用模块。
c） 测评实施包括以下内容：
1） 是否使用国际 AES 或国密 SM4、SM7 等安全级别及以上的对称加密算法；
2） 对称加密算法密钥长度是否符合用户实际需求级别；
3） 对称加密算法模块是否可切换、可替换。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.2 非对称加密算法

该测评单元包括以下要求：
a） 测评指标：非对称加密算法使用时应保证数据的安全加密。
b） 测评对象：非对称加密算法使用模块。
c） 测评实施包括以下内容：
1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的非对称加密算法；
2） 非对称加密算法密钥长度是否符合用户实际需求级别；
3） 非对称加密算法模块是否可切换、可替换。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.3 数字签名验签算法

该测评单元包括以下要求：
a） 测评指标：数字签名验签算法使用时应保证安全性。
b） 测评对象：数字签名验签算法使用模块。
c） 测评实施包括以下内容：
1） 是否使用国际 RSA、ECC 或国密 SM2、SM9 等安全级别及以上的加密算法进行数字签名/验签；
2） 是否支持基于硬件实现的数字签名/验签设备；

3） 是否采用本地签名方式；
4） 是否未使用已被证明不安全的加密算法；
5） 数字签名算法安全性是否达到用户实际需求级别。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.1.4 数字摘要算法

该测评单元包括以下要求：

a） 测评指标：数字摘要算法使用时应保证安全性。
b） 测评对象：数字摘要算法使用模块。
c） 测评实施包括以下内容：
1） 是否使用国际 SHA256 或国密 SM3 安全级别及以上的哈希散列算法；
2） 是否支持基于硬件实现的哈希散列求解设备；
3） 是否未使用已被证明不安全的数字摘要算法；
4） 数字摘要算法是否达到用户实际需求级别。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.2 加密设备及配置安全测评要求

8.2.1 物理加密设备

该测评单元包括以下要求：

a） 测评指标：加密设备物理结构应保证安全性。
b） 测评对象：加密设备物理结构。
c） 测评实施包括以下内容：
1） 加密设备是否具有防拆、防撬结构设计；
2） 加密设备是否具备紧急情况下人工毁钥装置；
3） 加密设备随意开关电源是否不会造成系统损坏、崩溃等后果。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.2.2 加密设备配置

该测评单元包括以下要求：

a） 测评指标：加密设备使用应保证安全性。
b） 测评对象：加密设备使用。
c） 测评实施包括以下内容：
1） 加密设备使用的加密算法是否符合本标准中 8.1 的要求；
2） 加密设备是否得到国家密码管理主管部门认证；
3） 加密设备的私钥是否不能被导出。
d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3 密钥管理安全测评要求

8.3.1 密钥生成

该测评单元包括以下要求：

a） 测评指标：保证系统产生的密钥安全性。

b） 测评对象：密钥生成方式。

c） 测评实施包括以下内容：

1） 是否使用安全的随机数发生器、密钥导出函数、标准的密钥协商机制等安全的方式生成密钥；

2） 如果采用安全的随机数发生器方式时，密钥是否由符合 GM/T 0050 要求的随机数产生；

3） 如果采用密钥导出函数时，是否使用 Bcrypt 算法、Scrypt 算法或 Argon2 算法等足够复杂的密钥生成算法；

4） 如果采用标准的密钥协商机制方式时，是否采用多方参与密钥协商方式一同决定密钥。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.2 密钥使用

该测评单元包括以下要求：

a） 测评指标：保证密钥使用的安全性。

b） 测评对象：密钥使用方式。

c） 测评实施包括以下内容：

1） 密钥是否通过密文形式进行分发；

2） 所有涉及密钥的敏感操作是否避免使用分支操作；

3） 是否只能使用密码算法访问密钥；

4） 是否能够正确、有效地导入密钥；

5） 是否能够根据密钥类型和使用场景合理的使用密钥；

6） 在密钥使用过程中，物理接口和逻辑接口是否不会泄露密钥相关信息。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.3 密钥更新

该测评单元包括以下要求：

a） 测评指标：保证系统密钥更新的安全性。

b） 测评对象：密钥更新方式。

c） 测评实施包括以下内容：

1） 是否具有密钥更新策略；

2） 系统管理员手动更新密钥；

3） 设置系统定期自动更新密钥，且系统管理员定期检查更新状态并手动更新密钥；

4） 是否严格按照密钥更新策略进行更新；

5） 新密钥是否不可逆向推导出旧密钥；

6） 密钥更新是否不会增加其它密钥的泄露风险。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.4 密钥存储

该测评单元包括以下要求：

a） 测评指标：保障密钥存储的安全性。

b） 测评对象：密钥存储方式。

c） 测评实施包括以下内容：

1） 密钥是否以密文形式存储；

2） 密钥在内存中是否只保留一份；

3） 密钥存储是否具备校验能力；

4） 存储的密钥相关信息是否存放在可控且专用的存储区域，且具有防止通过物理接口和逻辑接口对密钥进行非法访问的安全机制；

5） 需要长期存储的明文密钥是否存储于物理安全模块中，当物理安全模块失效时，明文密钥应立即失效；

6） 密钥分量在生命周期内是否隔离存储于不同介质中；

7） 若密文秘钥存储于密码设备外，是否经过授权才能访问。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.5 密钥备份

该测评单元包括以下要求：

a） 测评指标：保证密钥备份的安全性。

b） 测评对象：密钥备份机制。

c） 测评实施包括以下内容：

1） 是否具有密钥备份机制；

2） 备份密钥是否通过密文形式进行存储。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.3.6 密钥销毁

该测评单元包括以下要求：

a） 测评指标：保证密钥正确销毁。

b） 测评对象：密钥销毁机制。

c） 测评实施包括以下内容：

1） 是否能够根据需要正确、有效地清除所存储的密钥；

2） 密钥销毁过程是否不会泄露密钥相关信息；

3） 在接到外部合法自毁指令时是否能够有效、可靠地完成密钥和敏感信息的自毁；

4） 是否不可从销毁结果中恢复原密钥。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4 账本安全测评要求

8.4.1 账本存储

该测评单元包括以下要求：

a） 测评指标：保证区块链账本存储具备持久化、可追溯性。

b） 测评对象：区块链账本存储方式。

c） 测评实施包括以下内容：

1） 区块链账本是否具备存储持久化能力，例如利用账本存储数据的时间长短等方式判断；

2） 区块链账本是否能溯源原始数据位置。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

8.4.2 账本记录

该测评单元包括以下要求：

a） 测评指标：保证账本记录的完整性、一致性、真实性。

b） 测评对象：区块链账本记录方式。

c） 测评实施包括以下内容：

1） 每个节点是否拥有完整的数据记录；

2） 拥有完整数据记录的各节点的数据是否保持一致；

3） 账本记录是否受密码学保护。

d） 测评判定：如果以上测评实施内容均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

9 测评结论

9.1 风险分析和评价

等级测评报告中应对整体测评之后单项测评结果中的不符合项或部分符合项进行风险分析和评价。

采用风险分析的方法对单项测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，综合评价这些不符合项或部分符合项对定级对象造成的安全风险。风险分析和评价应根据特定的条件和场景下展开，并对高风险的测试项予以预警。

9.2 等级测评结论

等级测评报告应给出等级保护对象的等级测评结论，确认等级保护对象达到相应等级保护要求的程度。

应结合各类的测评结论和对单项测评结果的风险分析给出等级测评结论：

a） 符合：定级对象中未发现安全问题，等级测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为0。

b） 基本符合：定级对象中存在安全问题，部分符合和不符合项的统计结果不全为0，但存在的安全问题不会导致定级对象面临高等级安全风险。

c） 不符合：定级对象中存在安全问题，部分符合项和不符合项的统计结果不全为0，而且存在的安全问题会导致定级对象面临高等级安全风险。

参 考 文 献

[1] CBD-Forum-001-2017 区块链 参考架构.

[2] 中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书，2018.

[3] GA/T 988—2012 信息安全技术 文件加密产品安全技术要求.

[4] GB/T 36624—2018 信息技术安全技术 可鉴别的加密机制.

[5] GB/T 35275—2017 信息安全技术 SM2 密码算法加密签名消息语法规范.

[6] 杨璐，叶晓俊. 云服务环境下的密钥管理问题和挑战[J]. 计算机科学，2017(03):9-15.

[7] 赵翔. 数字签名综述[J]. 计算机工程与设计，2006，027(002):195-197.

[8] Diffle W, Hellman M. New direction in cryptography[C]. IEEE Tran Inform Theory IT-22, 1976.664-654.

[9] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19.

[10] 万武南，陈豪，陈俊，等. 区块链的椭圆曲线密码算法侧信道安全分析[J]. 应用科学学报，2019 (2): 5.

[11] 朱兴雄. 区块链加密算法研究[J]. 生态互联 数字电力——2019 电力行业信息化年会论文集，2019.