ICS 33.050
CCS M 30

团　体　标　准

T/TAF 168—2023

网络设备密码应用测试方法　交换机设备

Cryptography application test method for network devices—Switch

2023-04-26 发布　　2023-04-26 实施

电信终端产业协会　发布

目　　次

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。

请注意本文件中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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、中兴通讯股份有限公司、郑州信大捷安信息技术股份有限公司、浪潮电子信息产业股份有限公司、新华三技术有限公司、成都泰瑞通信设备检测有限公司、上海泰峰检测认证有限公司。

本文件主要起草人：张治兵、刘雅闻、吴荣春、叶郁柏、周继华、刘为华、陈泽、宋桂香、童天宇、刘欣东、吴萍、吴翔宇、宋祥烈、康亮。

网络设备密码应用测试方法　交换机设备

1　范围

本文件规定了交换机设备在软件/固件安全、身份鉴别、访问控制、网络通信安全、数据安全、计算安全、物理安全与性能等方面的密码应用测试方法。

本文件适用于在我国境内销售或提供的交换机设备，也可为网络运营者采购交换机设备时提供依据，还适用于指导交换机设备的研发、测试等工作。

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 25069—2022　信息安全技术　术语

GB/T 32915—2016　信息安全技术　二元序列随机性检测方法

GM/T 0005—2021　随机性检测规范

T/TAF 082.3—2021　网络设备密码应用技术要求　交换机设备

3　术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

交换机　switch

交换机是一种用于连接各个网络节点，能够在通信系统中完成信息交换功能的设备。

3.2

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.3

解密　decipherment/decryption

对密文进行密码变换以产生数据的过程。

3.4

密钥　key

控制密码算法运算的关键信息或参数。

3.5

保密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.6

数据完整性 data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.7

不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的性质。

3.8

重要数据 important data

重要数据包括身份鉴别信息、访问控制信息、设备信息、配置信息等。

3.9

可信计算环境 trusted execution environment

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

3.10

固件 firmware

固件(Firmware)是写入EPROM（可擦写可编程只读存储器）或EEPROM(电可擦可编程只读存储器)中的程序。

4 缩略语

AES：高级加密标准（Advanced Encryption Standard）
DES：数据加密标准（Data Encryption Standard）
HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）
KAT：已知答案测试（Known Answer Test）
MAC：消息鉴别码（Message Authentication Code）
MD5：信息摘要算法（Message-Digest Algorithm）
OSPF：开放式最短路径优先（Open Shortest Path First）
RIP：路由选择信息协议（Routing Information Protocol）
SHA：安全散列算法（Secure Hash Algorithm）
SSH：安全外壳协议（Secure Shell）
SNMP：简单网络管理协议（Simple Network Management Protocol）

5 测试环境

测试环境如图1、图2所示。

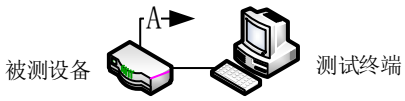

图1 测试环境1

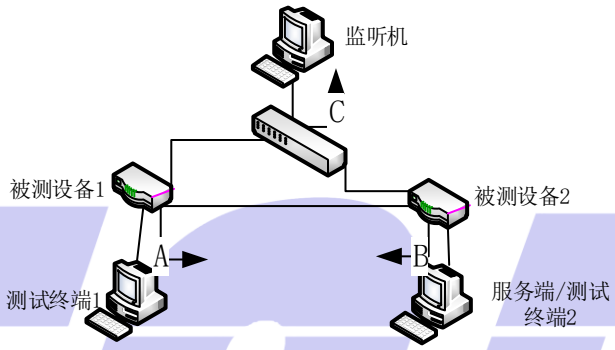

图2 测试环境2

测试环境描述：监听机用于监听实际业务流量，A、B、C为测试工具接入点。

6 交换机设备密码应用测试方法

6.1 软件/固件密码应用测试

6.1.1 软件/固件保密性

软件/固件保密性测试方法如下：

a) 安全要求：

可使用密码技术保证软件/固件保密性（T/TAF 082.3—2021 4.1a））。

b) 预置条件：

1) 按图 1 搭建好测试环境；
2) 厂商提供被测设备预装软件，并完成安装；
3) 厂商应提供被测设备保证软件/固件保密性采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c) 检测方法：

1) 检查是否可采用密码技术的加解密功能对软件/固件进行保护，并验证保护机制是否有效；
2) 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d) 预期结果：

1） 检测方法步骤1）中，可以采用加解密功能进行保护，保护机制有效；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合6.6.4节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.1.2 软件/固件完整性

软件/固件完整性测试方法如下：

a） 安全要求：
可使用密码技术保证软件/固件完整性（T/TAF 082.3—2021 4.1b））。

b） 预置条件：
1） 按图1搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备保证软件/固件完整性采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 检查是否可采用密码技术对软件/固件的完整性进行保护，并验证保护机制是否有效；；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤1）中，可以采用密码技术进行软件/固件的完整性保护，保护机制有效；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合6.6.4节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.1.3 软件/固件抵御攻击能力

软件/固件抵御攻击能力测试方法如下：

a） 安全要求：
可使用密码技术保证软件/固件抵御常见的攻击，如反编译、重打包等（T/TAF 082.3—2021 4.1c））。

b） 预置条件：
1） 按图1搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备保证软件/固件加固（如反编译、重打包等）采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 查看厂商提供的说明资料，检查是否采用有效的密码技术抵御反编译、重打包等攻击，并验证抵御机制是否有效；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤1）中，有效采用了密码技术抵御反编译、重打包等攻击；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合6.6.4节要求。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.1.4 软件/固件升级

软件/固件升级测试方法如下：

a） 安全要求：
远程升级时，应使用密码技术保证固件/软件升级包的完整性与身份校验（T/TAF 082.3—2021 4.1d））。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商提供被测设备预装软件的更新包；
3） 厂商提供签名验证的工具或指令；
4） 厂商应提供被测设备保证软件/固件远程升级采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 检查厂商发布更新软件包时是否同时发布更新软件包和数字签名；
2） 使用工具或指令验证厂商提供的更新包，检查是否通过签名验证；
3） 修改厂商提供的预装软件更新包，使用工具或指令验证修改过的更新包，检查是否可以通过完整性校验。
4） 修改预装软件升级包的数字签名，检查是否能通过签名验证；
5） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 更新包与签名一同发布；
2） 使用工具或指令进行签名验证，若更新包与与签名不匹配，则验证不通过，输出错误信息；若匹配，则输出验证通过信息；
3） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.2 身份鉴别密码应用测试

6.2.1 身份鉴别功能

身份鉴别功能测试方法如下：

a） 安全要求
应使用密码技术对访问控制实体进行身份鉴别，可使用密码技术进行双向身份鉴别（T/TAF 082.3—2021 4.2a））。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备身份鉴别功能采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查是否采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对访问控制实体进行身份鉴别/双向身份鉴别；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，采用密码技术进行身份鉴别/双向身份鉴别；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.2.2 身份鉴别信息保护

身份鉴别信息保护测试方法如下：

a） 安全要求
1） 应使用密码技术保证身份鉴别信息传输过程中的保密性（T/TAF 082.3—2021 4.2b））；
2） 可使用密码技术保证身份鉴别信息传输过程中的完整性（T/TAF 082.3—2021 4.2c））；
3） 应使用密码技术保证身份鉴别信息存储过程中的保密性（T/TAF 082.3—2021 4.2d））；
4） 可使用密码技术保证身份鉴别信息存储过程中的完整性（T/TAF 082.3—2021 4.2e））；
5） 可使用密码技术对口令认证中身份鉴别信息进行加密（T/TAF 082.3—2021 4.2f））；
6） 可使用密码技术对口令认证中身份鉴别信息的传输进行加密(T/TAF 082.3—2021 4.2g))。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备身份鉴别信息安全保护中采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 按照厂商提供说明材料，生成口令认证、数字签名等功能中的用户身份鉴别信息，查看是否以加密方式存储，是否可以采用密码技术进行完整性保护；
2） 按照厂商提供说明材料，传输用户身份鉴别信息，通过抓包或其他有效的方式查看是否采用加密方式传输，查看是否采用密码技术进行信息的完整性保护；
3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）、2）中，身份鉴别信息以加密方式存储和传输；
2） 检测方法步骤 1）、2）中，身份鉴别信息可以进行完整性保护；
3） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.2.3 抵御重放攻击

抵御重放攻击测试方法如下：

a） 安全要求
可使用密码技术来抵御常见的重放攻击（T/TAF 082.3—2021 4.2h））。

b） 预置条件：

1） 按图 2 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备防重放功能采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 查看厂商提供的说明资料，检查是否论证了所采用密码技术抵御重放攻击的技术原理，验证特定场景抗重放的能力；
2） 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，厂商提供的说明资料正确且充分地论证了所采用密码技术抵御重放攻击的技术原理，并且在特定场景下能够通过抗重放攻击的验证；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.3 访问控制密码应用测试

6.3.1 访问控制功能

访问控制功能测试方法如下：

a） 安全要求：
1） 可使用密码技术实现访问控制功能，如数字证书等（T/TAF 082.3—2021 4.3a））；
2） 可使用密码技术实现用户分级分权控制机制（T/TAF 082.3—2021 4.3b））。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商应提供被测设备在实现访问控制功能时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 按照厂商提供说明材料，检测是否采用数字证书等密码技术实现访问控制功能；
2） 按照厂商提供说明材料，检测是否采用密码技术实现用户的分级分权控制机制；
3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，可使用数字证书等密码技术实现访问控制功能；
2） 检测方法步骤 2）中，可使用密码技术实现用户的分级分权控制机制；
3） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.3.2 访问控制信息保护

访问控制信息保护测试方法如下：

a） 安全要求：
1） 可使用密码技术保证访问控制信息的完整性（T/TAF 082.3—2021 4.3c））；

2） 可使用密码技术保证访问控制信息的不可否认性（T/TAF 082.3—2021 4.3d））。

b） 预置条件：

1） 按图 2 搭建好测试环境；

2） 厂商应提供被测设备在执行访问控制功能时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检测设备在下发和存储访问控制策略时是否采用密码技术保证访问控制策略的完整性；

2） 检测设备在下发和存储系统的访问控制策略时是否采用密码技术保证访问控制信息的不可否认性；

3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）、2）中，被测设备在下发和存储访问控制策略时，使用密码技术来保证访问控制功能的完整性和不可否认性；

2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；

2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.3.3 访问控制抵御攻击能力

访问控制抵御攻击能力测试方法如下：

a） 安全要求

可使用密码技术来抵御特定的越权攻击，如会话劫持等（T/TAF 082.3—2021 4.3e））。

b） 预置条件：

1） 按图 2 搭建好测试环境；

2） 厂商应提供被测设备在执行访问控制功能时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1) 查看厂商提供的说明资料，检查是否论证了所采用密码技术抵御越权攻击的技术原理，验证特定场景抗越权攻击的能力；

2) 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：

1) 检测方法步骤 1）中，厂商提供的说明资料正确且充分地论证了所采用密码技术抵御越权攻击的技术原理，并且在特定场景下能够通过抗越权攻击的验证；

2) 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；

2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.4 网络通信密码应用测试

6.4.1 保密性

保密性测试方法如下：

a） 安全要求：

1） 应使用密码技术保证通信传输过程中数据的保密性（T/TAF 082.3—2021 4.4b））；
2） 可使用重要数据加密后再传输的方式保证信息不被泄露（T/TAF 082.3—2021 4.4i））。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商应提供被测设备网络通信时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 按照厂商提供说明材料，查看重要数据是否可以在传输前进行加密，保证信息不被泄露；
2） 使用工具从网络层面截取传输的数据，检测设备的数据在传输过程中是否采用密码技术进行机密性保护；
3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，被测设备可使用通信数据加密后再传输的方式保证信息不被泄露；
2） 检测方法步骤 2）中，被测设备使用网络层数据加密技术保证数据传输时的保密性；
3） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.4.2 完整性

完整性测试方法如下：

a） 安全要求：
可使用密码技术保证通信传输过程中数据的完整性（T/TAF 082.3—2021 4.4c））。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商应提供被测设备网络通信时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 使用工具从网络层面截取传输的数据，检测设备的数据在传输过程中是否可采用密码技术进行完整性保护，并验证完整性校验机制是否有效；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，被测设备在进行网络通信时，可否使用密码技术来保证通信传输过程中数据的完整性；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.4.3 远程管理安全

远程管理安全测试方法如下：

a） 安全要求：
1） 远程管理时，应支持使用密码技术建立可信信道/可信路径（T/TAF 082.3—2021 4.4a））；

2） 在支持 web 管理时，应支持 HTTPS，并避免使用安全强度弱的密码算法与加密模式（T/TAF 082.3—2021 4.4d））；
3） 在支持 SSH 管理时，应支持 SSHv2，并避免使用安全强度弱的密码算法与加密模式（T/TAF 082.3—2021 4.4e））；
4） 在支持 SNMP 管理时，应支持 SNMPv3，应使用 authPriv 模式（T/TAF 082.3—2021 4.4f））；
5） 在支持 Netconf 管理时，安全传输层应避免使用安全强度弱的密码算法与加密模式（T/TAF 082.3—2021 4.4g））。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商应提供被测设备网络通信时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 使用 HTTPS、SSHv2 协议对设备进行管理操作，通过抓包等有效方式对协议、加密方式和加密强度进行检查；
2） 使用 SNMPv3 协议、authPriv 模式对设备进行管理操作，通过抓包等有效方式对协议和安全模式进行检查；
3） 使用 Netconf 协议对设备进行管理操作，通过抓包等有效方式对协议、加密方式和加密强度进行检查；
4） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）、2）、3）中，被测设备如果支持对应的管理方式，则支持要求的协议管理操作，并且未使用安全强度弱的密码算法或加密模式；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.4.4 路由协议认证安全

路由协议认证安全测试方法如下：

a） 安全要求：
在支持路由功能时，应使用密码技术保证非明文路由认证功能（T/TAF 082.3—2021 4.4h））。

b） 预置条件：
1） 按图 2 搭建好测试环境；
2） 厂商应提供被测设备在执行访问控制功能时所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 启用路由协议，测试路由协议的安全认证功能；
2） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，被测设备采用了非明文的路由认证方式；
2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；

2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.5 数据安全密码应用测试

6.5.1 数据传输保密性

数据传输保密性测试方法如下：

a） 安全要求：

应使用密码技术保证重要数据在传输过程中的保密性（T/TAF 082.3—2021 4.5a））。

b） 预置条件：

1） 按图 2 搭建好测试环境；

2） 厂商提供在传输过程中为保护重要数据所使用的密码算法说明文档材料；

3） 厂商提供被测设备所涉及的重要数据清单。

c） 检测方法：

1） 身份鉴别信息的保密性测试方法详见 6.2.2；

2） 通过人工查看和工具验证，检查传输的数据是否有保密性保护措施，是否通过密码算法保证重要数据的保密性；

3） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 2）中，被测设备支持使用密码技术保证数据传输保密性；

2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；

2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.5.2 数据传输完整性

数据传输完整性测试方法如下：

a） 安全要求：

可使用密码技术保证数据在传输过程中的完整性（T/TAF 082.3—2021 4.5b））。

b） 预置条件：

1） 按图 2 搭建好测试环境；

2） 厂商提供在传输过程中为保护重要数据所使用的密码算法说明文档材料；

3） 厂商提供被测设备所涉及的重要数据清单。

c） 检测方法：

1） 访问控制信息的完整性测试方法详见 6.3.2；

2） 查看被测设备是否应用了密码技术来保障重要数据传输的完整性；

3） 设备通信过程中，通过网络截取通信报文等方式对传输的重要数据进行检测；

4） 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 2）、3）中，被测设备支持使用密码技术保证数据传输完整性；

2） 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；

2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.5.3 数据存储保密性

数据存储保密性测试方法如下：

a) 安全要求：

应使用密码技术保证重要数据在存储过程中的保密性（T/TAF 082.3—2021 4.5c））。

b) 预置条件：

1) 按图 1 搭建好测试环境；
2) 厂商提供在存储过程中为保护重要数据所使用的密码算法说明文档材料；
3) 厂商提供被测设备所涉及的重要数据清单。

c) 检测方法：

1) 身份鉴别信息保密性测试方法详见 6.2.2；
2) 通过下载、导出或在设备系统中查看存储的重要数据；
3) 检测被测设备是否应用了密码技术来保障重要数据存储的保密性；
4) 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 2）、3）中，被测设备支持使用密码技术保证重要数据在存储过程中的保密性；
2) 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e) 判定原则：

1) 测试结果应与预期结果相符，否则不符合要求；
2) 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.5.4 数据存储完整性

数据存储完整性测试方法如下：

a) 安全要求：

可使用密码技术保证数据在存储过程中的完整性（T/TAF 082.3—2021 4.5d））。

b) 预置条件：

1) 按图 1 搭建好测试环境；
2) 厂商提供在存储过程中为保护重要数据所使用的密码算法说明文档材料；
3) 厂商提供被测设备所涉及的重要数据清单。

c) 检测方法：

1) 访问控制信息的完整性测试方法详见 6.3.2；
2) 通过下载、导出或在设备系统中查看存储的重要数据；
3) 检测被测设备是否应用了密码技术来保障重要数据存储的完整性；
4) 检查并记录该功能使用的密码算法名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 2）、3）中，被测设备支持使用密码技术保证重要数据在存储过程中的完整性；
2) 记录的密码算法信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e) 判定原则：

1) 测试结果应与预期结果相符，否则不符合要求；
2) 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.5.5 数据安全防御能力

数据安全防御能力测试方法如下：

a) 安全要求

可使用密码技术保证设备抵御常见的攻击，防止密钥等重要数据泄露，如计时攻击等（T/TAF 082.3—2021 4.5e））。

b) 预置条件：

1) 按图 2 搭建好测试环境；
2) 厂商提供被测设备预装软件，并完成安装；
3) 厂商应提供被测设备抵御常见攻击所采用密码技术的说明，内容应包含使用的技术名称、原理、用途、何处使用及其实现方式。

c) 检测方法：

1) 查看厂商提供的说明资料，检查是否论证了所采用密码技术抵御常见攻击的技术原理；
2) 若被测设备使用了开源的密码算法实现，检查该开源实现是否存在可利用的公开漏洞；
3) 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 1）中，厂商提供的说明资料正确且充分地论证了所采用密码技术抵御常见攻击的技术原理；
2) 检测方法步骤 2）中，被测设备中使用的开源密码算法实现不存在可利用的公开漏洞；
3) 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e) 判定原则：

1) 测试结果应与预期结果相符，否则不符合要求；
2) 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.6 计算安全密码应用测试

6.6.1 随机数生成

随机数生成测试方法如下：

a) 安全要求

应使用符合GB/T 32915-2016标准的随机数生成器，显著性水平指标参考GM/T 0005-2021（T/TAF 082.3—2021 4.6a））。

b) 预置条件：

1) 按图 1 搭建好测试环境；
2) 厂商提供被测设备预装软件，并完成安装；
3) 厂商应提供被测设备中随机数生成器的输入输出接口或指令；
4) 厂商应提供被测设备生成随机数所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c) 检测方法：

1) 检查是否采用密码技术实现随机数生成器，并使用 GB/T 32915-2016 标准的检测方法验证被测设备生成的随机数是否达到了 GM/T 0005-2021 的测试指标要求；
2) 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d) 预期结果：

1) 检测方法步骤 1）中，随机数生成器应能够通过 GB/T 32915-2016 标准的检测，达到 GM/T 0005-2021 的测试指标要求；
2) 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；

2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.6.2 可信计算环境

可信计算环境测试方法如下：

a） 安全要求

可使用可信计算技术建立可信计算环境（T/TAF 082.3—2021 4.6b））。

b） 预置条件：

1） 按图 1 搭建好测试环境；

2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备可信计算环境的说明，说明内容应包括计算环境的功能架构、可信密码模块结构、完整性度量机制、身份标识机制和数据安全保护机制；

4） 厂商应提供被测设备可信计算环境与外部环境的接口说明；

5） 厂商应提供被测设备建立可信计算环境所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查是否可采用密码技术建立可信计算环境，并验证可信计算环境的完整性度量机制、身份标识机制和数据安全保护机制有效；

2） 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：

1） 检测方法步骤 1）中，采用密码技术建立可信计算环境，可信计算环境的完整性度量机制、身份标识机制和数据安全保护机制有效；

2） 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：

1） 测试结果应与预期结果相符，否则不符合要求；

2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.6.3 计算完整性保护

计算完整性保护测试方法如下：

a） 安全要求

可使用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证（T/TAF 082.3—2021 4.6c））。

b） 预置条件：

1） 按图 1 搭建好测试环境；

2） 厂商提供被测设备预装软件，并完成安装；

3） 厂商应提供被测设备中重要可执行程序的范围，以及对程序进行完整性保护和真实性验证的凭据；

4） 厂商应提供被测设备保护可执行程序完整性所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式；

5） 厂商应提供被测设备验证可执行程序来源所采用密码技术的说明，说明内容应包含使用的密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：

1） 检查设备在执行重要可执行程序前是否采用密码技术对其来源真实性和完整性进行保护，并验证保护机制是否有效；
2） 篡改对重要可执行程序来源进行真实性验证的凭据（如数字签名），调用该程序；
3） 篡改用于对重要可执行程序进行完整性保护的凭据（如杂凑值），调用该程序；
4） 检查并记录该功能使用的密码技术名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，可以采用密码技术对重要可执行程序的完整性和来源的真实性进行保护，保护机制有效；
2） 检测方法步骤 2）中，可执行程序无法通过来源的真实性验证，被测设备提示相应错误信息；
3） 检测方法步骤 3）中，可执行程序的完整性校验失败，被测设备提示相应错误信息；
4） 记录的密码技术信息应与厂商提供的材料一致，密码算法安全强度符合 6.6.4 节要求。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

6.6.4 密码安全强度

密码安全强度测试方法如下：

a） 安全要求
1） 以上使用的密码技术应使用安全强度较高的密码算法，不应使用md5、SHA1、DES等（T/TAF 082.3—2021 4.6d））；
2） 以上使用的密码技术应使用安全强度较高的密码协议（T/TAF 082.3—2021 4.6e））。

b） 预置条件：
1） 按测试环境 1 搭建好测试环境；
2） 厂商提供被测设备预装软件，并完成安装；
3） 厂商应提供被测设备密码算法的调用接口或指令；
4） 厂商应提供被测设备采用密码技术的说明，说明内容应包含使用的密码协议和密码算法名称、用途、何处使用及其实现方式。

c） 检测方法：
1） 检查以上使用的密码技术是否使用了安全强度高的密码协议和密码算法，即当前在业界普遍认可，且具有可证明安全性或在当前的算力环境下显著不可破解；
2） 检测被测设备是否正确使用了厂商申明的密码协议和密码算法；
3） 检查并记录该功能使用的密码协议、密码算法的名称、用途、何处使用及其实现方式。

d） 预期结果：
1） 检测方法步骤 1）中，上述使用的密码技术使用了安全强度较高的密码协议；
2） 检测方法步骤 1）中，上述使用的密码技术使用了强密码算法，没有发现使用 md5、SHA1、DES 等；
3） 检测方法步骤 2）中，被测设备正确使用了厂商申明的密码协议和密码算法；
4） 记录的密码技术信息应与厂商提供的材料一致。

e） 判定原则：
1） 测试结果应与预期结果相符，否则不符合要求；
2） 密码算法合规性可根据使用方要求或其他相关规定进行判定。

参 考 文 献

[1] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[2] GB/T 37092—2018 信息安全技术 密码模块安全要求
[3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[4] GB/T 32915—2016 信息安全技术 二元序列随机性检测方法
[5] GM/T 0014—2012 数字证书认证系统密码协议规范
[6] GM/T 0005—2021 随机性检测规范

电信终端产业协会团体标准

网络设备密码应用测试方法 交换机设备

T/TAF 168—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：82052809
电子版发行网址：www.taf.org.cn