ICS 33.050
CCS M 30

团　体　标　准

T/TAF 167—2023

网络设备密码应用通用测试方法

Cryptography application common test method for network devices

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、陈鹏、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。

网络设备密码应用通用测试方法

1 范围

本文件规定了网络设备在软件/固件安全、身份鉴别、访问控制、网络通信安全、数据安全、计算安全的密码应用测试方法与密码应用的性能测试方法。

本文件适用于在我国境内销售或提供的网络设备，也可为网络运营者采购网络设备时提供依据，还适用于指导网络设备的研发、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 082.1—2021 网络设备密码应用技术要求 通用要求

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

网络设备 network devices

网络设备指具备连接网络功能的实体（不包含消费类终端产品）。

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）
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）
SHA：安全散列算法（Secure Hash Algorithm）
UDP：用户数据报协议（User Datagram Protocol）

5 测试环境

测试环境如图1、图2所示。

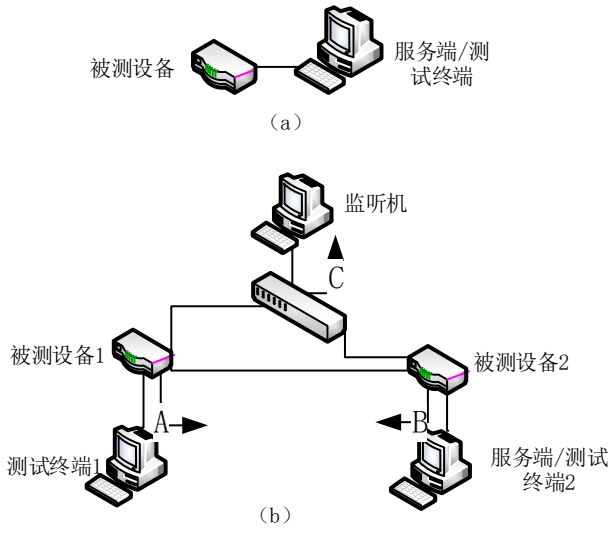

图1　测试环境1

测试环境1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。

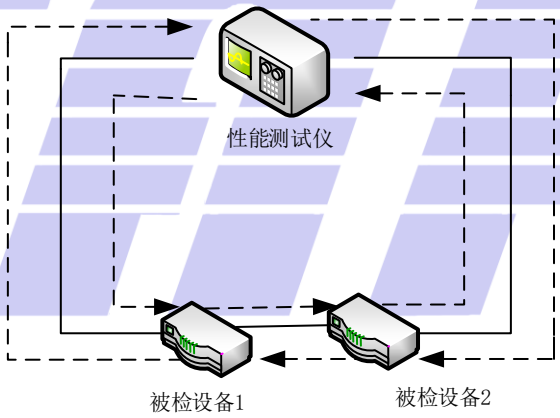

图2　测试环境2

测试环境2描述：性能测试仪用于模拟真实业务流量.

6　网络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 082.1—2021 4.1a））。

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 082.1—2021 4.2b））。

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固件/软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固件/软件的完整性保护，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 082.1—2021 4.3c））。

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） 检查是否采用有效的密码技术抵御反编译、重打包等攻击；

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） 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 082.1—2021 4.4d））。

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）使用厂商提供的预装软件更新包进行签名验证，若更新包与签名不匹配，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 082.1—2021 4.2a））。

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） 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 082.1—2021 4.2b））。

2） 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 082.1—2021 4.2c））。

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，生成用户身份鉴别信息，查看是否以加密方式存储；

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以加密方式传输；

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，身份鉴别信息以加密方式传输，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。

6.2.3 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 082.1—2021 4.2d））。

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：

可使用密码技术保障访问控制功能安全性（T/TAF 082.1—2021 4.3a））。

b） 预置条件：

1） 按测试环境 1 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） 检测设备授权的管理员（如系统管理员）下发和存储系统的访问控制策略时是否采用了密码技术；

2） 查看被测设备的访问控制功能在实施时所采用的密码技术是否能保障访问控制功能的安全性。

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，使用了密码技术来保证访问控制功能的安全性；

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。

6.3.2 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 082.1—2021 4.3b））；
   2) 可使用密码技术保证访问控制信息的不可否认性（T/TAF 082.1—2021 4.3c））。
b) 预置条件：
   1) 按测试环境 1 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 082.1—2021 4.3d））。
b) 预置条件：
   1) 按测试环境 1 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 网络通信可信信道/可信路径

网络通信可信信道/可信路径测试方法如下：

a） 安全要求：
   1） 应支持使用密码技术建立可信信道/可信路径（T/TAF 082.1—2021 4.4a））；
   2） 应使用密码技术保证通信传输过程中重要数据的保密性（T/TAF 082.1—2021 4.4b））；
   3） 应使用密码技术保证通信传输过程中重要数据的完整性（T/TAF 082.1—2021 4.4c））；
b） 预置条件：
   1） 按测试环境 1 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） 检测被测设备在建立可信信道/可信路径时所使用的密码技术；
   2） 重要数据在通信传输过程中的保密性和完整性测试方法详见 6.5.1 和 6.5.2；
   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，被测设备支持使用密码技术建立可信信道/可信路径；
   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。

6.4.2 非安全通道重要数据传输

非安全通道重要数据传输测试方法如下：

a） 安全要求：
   1） 可使用通信数据加密后再传输的方式保证信息不被泄露（T/TAF 082.1—2021 4.4d））；
   2） 应使用密码技术保证在非安全通道传输时重要数据的保密性与完整性（T/TAF 082.1—2021 4.4e））。
b） 预置条件：
   1） 按测试环境 1 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） 检测被测设备是否使用密码技术保证非安全通道传输的重要数据的保密性与完整性，如数据加密后再传输等方式；
   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，被测设备使用密码技术保证非安全通道传输的重要数据的保密性与完整性；
   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 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 082.1—2021 4.5a））。

b） 预置条件：

1） 按测试环境 1 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 082.1—2021 4.5b））。

b） 预置条件：

1） 按测试环境 1 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 082.1—2021 4.5c））。

b） 预置条件：

1） 按测试环境 1 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 082.1—2021 4.5d））。

b） 预置条件：

1） 按测试环境 1 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） 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 082.1—2021 4.5e））。
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） 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） 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 082.1—2021 4.6a））。
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技术名称、用途、何处使用及其实现方式。
c） 检测方法：
1） 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 082.1—2021 4.6b））。

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技术名称、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 082.1—2021 4.6c））。

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 密码算法安全强度

密码算法安全强度测试方法如下：

a） 安全要求：
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 082.1—2021 4.6d））。

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强密码算法，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的密码算法；
2） 检测被测设备是否正确使用了厂商申明的密码算法；
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，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；
2） 检测方法步骤 2）中，被测设备正确使用了厂商申明的密码算法；
3） 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。

6.7 性能测试

6.7.1 性能要求：算法支持

算法支持测试方法如下：

a） 安全要求：

应具有能够运行安全强度较高密码算法的相关性能，如SHA256/SM3、AES128/SM4等算法（T/TAF 082.1—2021 4.8a））。

b) 预置条件：

1) 按测试环境 1 搭建好测试环境；

2) 选择支持安全强度较高密码算法的相关性能运行环境，如 SHA256/SM3、AES128/SM4 等算法。

c) 检测方法：

1) 在客户端上强制选择对应的加密算法为指定算法；

2) 在被测设备上配置指定算法的安全策略，验证是否支持通过高强度的密码算法对被测设备进行运行管理.

3) 在被测设备上配置指定算法的安全策略，验证是否支持采用安全强度较高密码算法来保障加密传输业务。

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） 步骤 2）可支持通过高强度的密码算法对被测设备进行运行管理；

2） 步骤 3）可支持采用安全强度较高密码算法来保障加密传输业务的正常运行。

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。

6.7.2 性能要求：业务连续性

业务连续性测试方法如下：

a) 安全要求：

应具有在运行高强度加密、解密算法时不会出现因负载过高而造成不能正常提供服务的情况（T/TAF 082.1—2021 4.8b））。

b) 预置条件：

1) 按测试环境 2 搭建好测试环境；

2) 选择支持安全强度较高密码算法的相关性能运行环境，如 SHA256/SM3、AES128/SM4 等算法。

3) 厂商应提供被测设备密码技术应用的性能参数说明。

c) 检测方法：

1) 在客户端上强制选择对接的加密算法为指定算法；

2) 在被测设备上配置为指定算法的安全策略，实现从端到端的加密传输；

3) 测试被测设备的加密流量的吞吐量；

4) 使用测试仪表模拟构造 10%吞吐量的业务流量（如：UDP 512 字节），使用正确的用户名账户连续登录设备，观察设备运行状态；

5) 使用测试仪表模拟构造 80%吞吐量的业务流量（如：包长 64 字节的 UDP 报文、包长 512 字节的 UDP 报文、包长 1518 字节的 UDP 报文）持续 24 小时打流；

6) 有额外的要求时，可参照步骤 3）、4）构造业务流量进行测试。

d) 预期结果：

1) 步骤 3）能正常登录登出设备，登录时设备收发包不受影响，CPU 占用率的变化符合厂商申明的范围；

2） 步骤 4）被测设备 24 小时内运行稳定，未出现死机、重启等现象，CPU 占用率符合厂商的申明。

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。

6.7.3 性能要求：硬件加解密

硬件加解密测试方法如下：

a） 安全要求：

可具有硬件密码计算功能，能够满足高强度加解密算法的性能要求（T/TAF 082.1—2021 4.8c））。

b） 预置条件：

1） 按测试环境 2 搭建好测试环境；

2） 厂商应提供被测设备使用硬件进行密码计算的说明，说明内容应包含使用的密码计算硬件信息，该硬件支持的密码算法名称列表及使用场景。

c） 检测方法：

1） 拆机或者由厂家提供相关硬件的照片；

2） 根据厂家提供的说明材料，选取两个采用高强度加解密算法的硬件加解密使用场景，使用测试仪表模拟构造 80%吞吐量的业务流量（如：包长 64 字节的 UDP 报文、包长 512 字节的 UDP 报文、包长 1518 字节的 UDP 报文），进行业务验证，并记录 CPU 占用率。

3） 有额外的要求时，可参照步骤 2）构造业务流量进行测试。

d） 预期结果：

1） 通过拆机验证或者照片证明，相关密码计算硬件确实存在；

2） 使用硬件进行的加解密业务能正常运行，CPU 占用率符合厂家的申明。

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

网络设备密码应用通用测试方法

T/TAF 167—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