ICS 33.050
M 30

团　体　标　准

T/TAF 082.3-2021

网络设备密码应用技术要求
交换机设备

Cryptography application technical requirement for network devices—Switch

2021-01-18 发布　　2021-01-18 实施

电信终端产业协会　发布

目　　次

5

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。

本文件是网络设备密码应用技术要求系列标准之一，该系列标准结构预计如下：

《网络设备密码应用技术要求 通用要求》

《网络设备密码应用技术要求 路由器设备》

《网络设备密码应用技术要求 交换机设备》

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。

本文件对交换机设备提出密码应用技术要求。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：中国信息通信研究院、中兴通讯股份有限公司、新华三技术有限公司、华为技术有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：秦书锴、张治兵、张亚薇、周继华、童天予、万晓兰、吴萍、陈鹏、吴荣春、刘为华、薄菁、叶郁柏。

引　　言

为推进《网络安全法》与《密码法》的落地实施，本文件提出交换机设备密码应用技术应满足的通用安全技术要求。

密码技术是网络安全的核心技术，是信息保护和网络信息体系建设的基础，是保障网络空间安全的关键技术。本文件对交换机设备提出密码应用技术要求。

网络设备密码应用技术要求 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、数据安全与计算安全等方面的密码应用技术的要求。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 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

GB/T 37092—2018 信息安全技术 密码模块安全要求

3 术语和定义

GB/T 25069-2010与GB/T 37092—2018中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

重要数据包括认证口令、管理指令、设备信息等，具体参见附录B。

4 交换机设备密码应用技术要求

4.1 软件/固件安全

交换机设备：

a） 可使用密码技术保证软件/固件保密性；
b） 可使用密码技术来保证固件/软件完整性；
c） 可使用密码技术保证软件/固件抵御常见的攻击；
d） 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来源真实性。

4.2 身份鉴别

交换机设备：

a） 应使用密码技术对访问控制实体进行身份鉴别，必要时使用密码技术进行双向身份鉴别；
b） 应使用密码技术保证身份鉴别信息传输过程中的保密性；
c） 可使用密码技术保证身份鉴别信息传输过程中的完整性；
d） 应使用密码技术保证身份鉴别信息存储过程中的保密性；
e） 可使用密码技术保证身份鉴别信息存储过程中的完整性；
f） 可使用密码技术对口令认证中身份鉴别信息进行加密；
g） 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；
h） 可使用密码技术来抵御常见的重放攻击。

4.3 访问控制

交换机设备：

a） 可使用密码技术实现访问控制功能，如数字证书等；
b） 可使用密码技术实现用户分级分权控制机制；

c） 可使用密码技术保证访问控制信息的完整性；
d） 可使用密码技术保证访问控制信息的不可否认性；
e） 可使用密码技术来抵御常见的越权攻击。

4.4 网络通信安全

交换机设备：
a） 远程管理时，应支持使用密码技术建立可信信道/可信路径；
b） 应使用密码技术保证通信传输过程中数据的保密性；
c） 可使用密码技术保证通信传输过程中数据的完整性；
d） 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；
e） 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；
f） 在支持SNMP管理时，应支持SNMPv3，应使用authPriv模式；
g） 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；
h） 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；
i） 可使用通信数据加密后再传输的方式保证信息不被泄露。

4.5 数据安全

交换机设备：
a） 应使用密码技术保证重要数据在传输过程中的保密性；
b） 可使用密码技术保证重要数据在传输过程中的完整性；
c） 应使用密码技术保证重要数据在存储过程中的保密性；
d） 可使用密码技术保证重要数据在存储过程中的完整性；
e） 可使用密码技术保证设备抵御常见的侧信道攻击，防止密钥等重要数据泄露，如计时攻击等。

4.6 计算安全

交换机设备：
a） 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 0005-2012；
b） 可使用可信计算技术建立可信计算环境；
c） 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；
d） 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；
e） 以上使用的密码技术应使用安全强度较高的密码协议。

附录 A
（资料性）
重要数据说明

重要数据包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据和重要个人信息等。

参 考 文 献

[1] 信息安全技术 信息系统密码应用基本要求（征求意见稿）
[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—2012 随机性检测规范

电信终端产业协会团体标准

网络设备密码应用技术要求 交换机设备

T/TAF 082.3-2021

*

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：010-82052809
电子版发行网址：www.taf.org.cn