ICS 33.050
CCS M 30

团　体　标　准

T/TAF 218—2024

网络设备密码应用技术要求
服务器设备

Cryptography application technical requirement for network devices—Server

2024-02-23 发布　　2024-02-23 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：浪潮电子信息产业股份有限公司、中国信息通信研究院、新华三技术有限公司、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、上海泰峰检测认证有限公司、中兴通讯股份有限公司、武汉网锐检测科技有限公司、北京通和实益电信科学技术研究所有限公司、成都泰瑞通信设备检测有限公司、博鼎实华(北京)技术有限公司。

本文件主要起草人：刘雁鸣、张治兵、童天予、李汝鑫、刘为华、王瑾、宋祥烈、周继华、陈玺、何伟、赵媛、袁玉东、吴翔宇、刘向东、刘献伦、徐潇、宋桂香、苏振宇、李勇、曹柱、齐园。

引　　言

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。为推进《网络安全法》的落地实施，本文件提出服务器设备密码应用应满足的相关技术要求。

网络设备密码应用技术要求　服务器设备

1　范围

本文件规定了服务器设备在固件自身安全、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服务器设备，也可为网络运营者采购服务器设备时提供依据，还适用于指导服务器设备的研发、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

GB/T 39680—2020　信息安全技术　服务器安全技术要求和测评准则

3　术语和定义

GB/T 25069—2022、GB/T 39680—2020中界定的以及下列术语和定义适用于本文件。

3.1

重要数据　important data

主要指支持服务器设备自身运行管理所涉及的重要信息，包括访问控制信息、身份鉴别信息、重要日志信息、重要配置信息、重要个人信息和密钥等，具体参见附录A。

4　缩略语

下列缩略语适用于本文件。

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

KVM：键盘、视频、鼠标（Keyboard Video Mouse）

Rest API：表现层状态转化应用程序编程接口（Representational State Transfer Application Programming Interface）

SNMP：简单网络管理协议（Simple Network Management Protocol）

SSH：安全外壳协议（Secure Shell）

VNC：虚拟网络控制台（Virtual Network Console）

5　服务器设备密码应用技术要求

5.1 基本要求

服务器设备基本要求如下：

a) 设备使用的密码技术（指本文件规定范围内的密码应用技术）应支持使用安全强度较高的密码算法，不宜使用安全强度弱的密码算法；

b) 设备使用的密码技术（指本文件规定范围内的密码应用技术）应支持使用安全强度较高的密码协议，不宜使用安全强度弱的密码协议。

5.2 固件自身安全

服务器设备固件自身安全要求如下：

a） 远程升级时，应使用密码技术保证固件升级包的完整性与来源真实性；

b） 宜使用密码技术保证固件包的保密性；

c） 宜使用密码技术保证固件包的完整性；

d） 宜使用密码技术保证固件抵御常见的攻击，如反编译、重打包等。

5.3 身份鉴别

服务器设备身份鉴别要求如下：

a） 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；

b） 应支持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） 应支持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） 对于不需要还原的身份鉴别信息，应使用密码散列加随机盐值等不可逆密码技术处理后存储；

g） 可使用密码技术对口令认证中身份鉴别信息进行加密后再传输；

h） 可使用密码技术来抵御常见的重放攻击。

5.4 访问控制

服务器设备访问控制要求如下：

a） 可使用密码技术实现访问控制功能，如数字证书等；

b） 可使用密码技术保证访问控制信息的完整性；

c） 可使用密码技术保证访问控制信息的不可否认性；

d） 可使用密码技术来抵御常见的越权攻击，如会话劫持等。

5.5 网络通信安全

服务器设备网络通信安全要求如下：

a） 应使用密码技术保证通信传输过程中重要数据的保密性,可使用通信数据加密后再传输的方式保证信息不被泄露；

b） 可使用密码技术保证通信传输过程中重要数据的完整性；

c） 远程管理或日志外发时，应支持使用密码技术建立可信信道/可信路径；

1）在支持Web或Rest API管理时，应支持HTTPS；

2）在支持SSH管理时，应支持SSHv2；

3）在支持SNMP管理时，应支持SNMPv3，并使用鉴权及加密模式；

4）在支持VNC、基于IP的KVM等控制台重定向管理时，应支持加密通道；

5）在支持syslog外发日志管理时，可使用加密通道，可使用密码技术进行双向身份鉴别。

5.6 数据安全

服务器设备数据安全要求如下：

a） 宜使用密码技术保证重要数据在存储过程中的保密性；

b） 可使用密码技术保证重要数据在存储过程中的完整性；

c） 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。

5.7 计算安全

服务器设备计算安全要求如下：

a） 宜使用可信计算技术建立可信计算环境，以支持在设备启动时对服务器引导固件和主引导分区/初始化程序加载器进行完整性检测；

b） 宜使用密码技术保证操作系统和驱动程序完整性与来源真实性；

c） 可使用符合GB/T 32915—2016标准的随机数生成器。

附 录 A
（资料性）
重要数据说明

表A.1列举了服务器设备涉及的重要数据。服务器设备重要数据包括但不限于访问控制信息、身份鉴别信息、重要日志信息、重要配置信息、重要个人信息和密钥等。

表A.1 服务器设备涉及的重要数据示例

序号	重要数据类型	备注
1	访问控制信息	引导固件及带外管理模块固件的访问控制策略等
2	身份鉴别信息	引导固件及带外管理模块固件中的各类用户口令等
3	重要日志信息	带外管理模块固件的审计日志等
4	重要配置信息	License、各类安全策略配置等
5	重要个人信息	邮箱、手机号等
6	密钥	私钥、对称密钥等

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] GB/T 39680—2020 信息安全技术 服务器安全技术要求和测评准则
[6] GM/T 0014—2012 数字证书认证系统密码协议规范
[7] T/TAF 082.1—2021 网络设备密码应用技术要求 通用要求

电信终端产业协会团体标准

网络设备密码应用技术要求　服务器设备

T/TAF 218—2024

*

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