ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0123—2022

时间戳服务器密码检测规范

Cryptography test specification for time stamp server

2022-11-20 发布　　2023-06-01 实施

国家密码管理局　　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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：国家密码管理局商用密码检测中心、北京信安世纪科技有限公司、三未信安科技股份有限公司、北京数字认证股份有限公司、上海市数字证书认证中心有限公司、吉大正元信息技术股份有限公司、山东渔翁信息技术股份有限公司、鼎铉商用密码测评技术（深圳）有限公司、智巡密码（上海）检测技术有限公司。

本文件主要起草人：顾伟平、李国友、汪宗斌、刘盼盼、陈妍、李冬、邓开勇、郗楷、赵松、王春涛、许永欣、王腾飞、冯晔、王玉林、杨领波、钱维、宋志华、吴震、凌杭、谢明明、包斯刚、韩玮。

时间戳服务器密码检测规范

1 范围

本文件规定了时间戳服务器的检测内容、检测要求和检测方法。

本文件适用于时间戳服务器设备的密码检测，以及该类密码设备的研制，也可用于指导基于该类密码设备的应用开发。

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 9813（所有部分） 计算机通用规范

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0005 随机性检测规范

GM/T 0033—2014 时间戳接口规范

GM/T 0039 密码模块安全检测要求

GM/T 0050 密码设备管理 设备管理技术规范

GM/T 0062 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

时间戳 time stamp

对时间和其他待签名数据进行签名得到的数据，用于表明数据的时间属性。

3.2

应用实体 application entity

时间戳服务器的服务对象，可以是个人、机构或系统。

3.3

时间戳服务器 time stamp server

基于 PKI（Public Key Infrastructure，公钥基础设施）技术的对外提供精确可信的时间戳服务的服务器。

3.4

智能 IC 卡　smart card

实现密码运算和密钥管理的含 CPU(中央处理器)的集成电路卡。

4　缩略语

下列缩略语适用于本文件：

API：应用编程接口(Application Programming Interface)

HTTP：超文本传输协议(Hyper Text Transfer Protocol)

SOAP：简单对象访问协议(Simple Object Access Protocol)

UTC：协调世界时(Coordinated Universal Time)

5　检测环境要求

时间戳服务器常规检测平台应由检测控制台和运行测试程序的检测服务器组成，用于检测时间戳服务器的功能、性能，通过网口连接时间戳服务器。检测控制台向检测服务器上运行的测试程序发送测试指令，测试程序根据测试指令调用时间戳服务器的 API 接口对时间戳服务器功能及性能进行测试。

时间戳服务器检测环境用于测试时间戳服务器的功能、性能。检测环境拓扑见图 1。

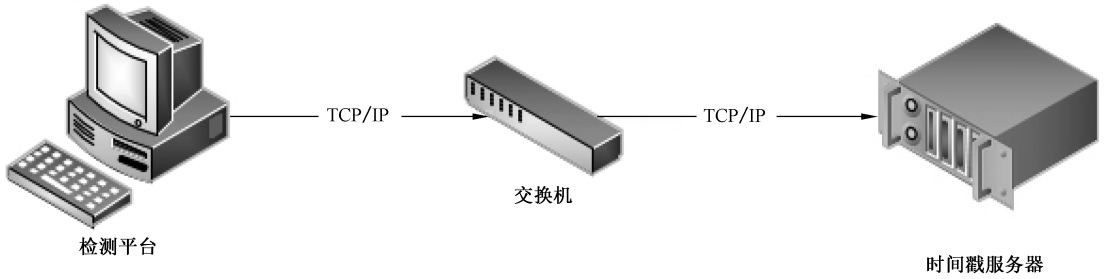

图 1　时间戳服务器的常规检测环境拓扑图

6　检测内容及检测方法

6.1　外观和结构的检查

根据产品的物理参数，对时间戳服务器的外观、尺寸、内部部件、密码运算部件、管理员身份验证设备及附件进行一致性检查。

a)　时间戳服务器应具备以下主要部件或接口：

1)　电源指示灯；

2)　状态指示灯，用于指示初始状态、就绪状态、错误状态等；

3)　故障指示灯或其他故障指示方式；

4)　至少 2 个网络接口(RJ45 或光口)；

5)　经商用密码检测认证的密码部件或模块，如加密卡、安全芯片等。

b)　时间戳服务器宜支持以下主要部件或接口：

1)　人机交互部件；

2)　冗余电源；

3） 手动密钥销毁开关；
4） 串口；
5） 授时天线。

6.2 功能检测

6.2.1 初始化功能检测

时间戳服务器应具备初始化功能，实现设备的初始状态到就绪状态的转换。

时间戳服务器的初始化操作主要包括系统初始配置、初始化管理员或操作员、初始密钥生成（或恢复）与安装。只有在初始化操作完成之后才能提供密码服务。经过初始化配置的时间戳服务器，可自动进入就绪状态，提供密码服务。

6.2.2 设备自检检测

时间戳服务器应具备自检功能，自检应包括上电/复位自检、周期自检和接收指令后的自检，检验时间戳服务器自身的密码部件、算法、随机数等软硬件状态，包括算法正确性检测、随机数发生器检测、存储密钥和数据的完整性检测，以及关键部件的正确性检测等。自检结束后应报告自检结果。自检成功，时间戳服务器应进入管理状态或工作状态。自检失败，时间戳服务器应报告自检结果并且停止对外提供密码服务。

6.2.3 密码运算检测

6.2.3.1 非对称算法检测

时间戳服务器应至少支持 SM2 非对称算法，对数据进行签名/验签运算，曲线参数应符合 GB/T 32918.5的规定。密码运算应在经商用密码检测认证的密码部件或模块内完成，应支持给定密钥、待签名消息，测试其运算结果的正确性：

a） 使用给定的密钥对待签名消息调用签名算法进行签名后，检测平台对签名结果进行验签，验签通过；
b） 使用给定的密钥对正确签名结果，调用验签算法进行验签运算，验签通过；
c） 使用给定的密钥对错误签名结果，调用验签算法进行验签运算，验签不通过。

6.2.3.2 杂凑算法检测

时间戳服务器应至少支持 SM3 算法，对消息进行杂凑运算，符合 GB/T 32905 的规定。对给定消息调用杂凑算法计算杂凑值，结果和给定杂凑值完全相同。

6.2.4 密钥管理检测

时间戳服务器应具备完善的密钥管理功能，密钥管理包括密钥的生成、存储、使用、更新、备份、恢复、归档和销毁。应保证密钥在生命周期的各个环节的安全性。时间戳签名密钥对的生成应采用经商用密码检测认证的密码部件或模块，时间戳签名私钥应安全存储在密码部件或模块内。

6.2.5 随机数检测

时间戳服务器应具备随机数生成功能。应采用经检测认证的具有物理噪声源功能的两个及以上独立芯片，用于实现随机数生成功能。采集 1000 个 128 KB 大小的随机数文件，对所采集的随机数文件进行检测，检测结果应符合 GM/T 0005 的要求。

随机数自检应符合 GM/T 0062 中的 E 类产品的上电检测和使用检测要求；自检失败，应停止提供

密码服务，进入错误状态，输出错误指示。

6.2.6 证书管理检测

时间戳服务器的证书管理和验证功能检测范围包括对应用实体证书、根证书或证书链的导入、存储、验证、使用、删除以及备份和恢复等操作，通过使用管理工具进行测试。

时间戳服务器的证书管理和验证功能检测时，SM2 证书应符合 GB/T 20518 的要求。

6.2.7 时间戳服务检测

6.2.7.1 通信方式

时间戳服务器应至少支持用户通过电子邮件、文件、Socket、HTTP、SOAP 中一种通信方式发送时间戳申请，并且通过相同方式向用户返回时间戳响应，应符合 GM/T 0033—2014 中第 8 章的要求。

6.2.7.2 请求和响应格式检测

时间戳服务器提供的时间戳服务，时间戳请求、时间戳响应的格式应符合 GM/T 0033—2014 中第 7 章规定的 ASN.1 数据格式，包括：

a) 对给定的正确的请求 ASN.1 编码格式，时间戳服务器应能正确响应；
b) 对给定的错误的请求 ASN.1 编码格式，时间戳服务器应能识别错误，并反馈响应的错误代码；
c) 对于时间戳服务器的请求成功响应，应是正确的 ASN.1 编码格式，检测其编码格式应符合 GM/T 0033—2014 中 7.1 的要求；
d) 对于时间戳服务器的请求失败响应，应是正确的 ASN.1 编码格式，检测其编码格式应符合 GM/T 0033—2014 中 7.2 的要求；
e) 时间戳服务器反馈的时间格式应是 UTC 格式。

6.2.7.3 时间戳接口

时间戳服务器的服务接口应符合 GM/T 0033—2014 中第 9 章的要求，且函数的返回值应符合 GM/T 0033—2014 附录 A 的要求。

时间戳服务器使用的签名算法标识应符合 GB/T 33560，SM2 签名算法数据的结构应符合 GB/T 35275 和 GB/T 35276 要求：

a) 调用初始化环境接口，时间戳服务器应成功建立时间戳环境，并返回 0，否则应反馈 GM/T 0033—2014 附录 A 中相应状态码；
b) 调用消除环境接口，时间戳服务器应成功清除时间戳环境，并返回 0，否则应反馈 GM/T 0033—2014 附录 A 中相应状态码；
c) 使用正确的密码杂凑算法标识调用生成时间戳请求接口，时间戳服务器应采用指定算法对时间戳请求信息进行密码杂凑运算，成功生成时间戳请求包，并返回 0；使用错误的密码杂凑算法调用生成时间戳请求接口，应反馈 GM/T 0033—2014 附录 A 中相应状态码，且不产生时间戳请求数据；生成的时间戳请求格式应通过 6.2.7.2 检测；
d) 使用正确的签名算法标识调用生成时间戳响应接口，时间戳服务器应成功地根据请求包生成时间戳响应包，并返回 0；使用错误的签名算法调用生成时间戳响应接口，应反馈 GM/T 0033—2014 附录 A 中相应状态码，且生成时间戳异常响应数据；生成的时间戳响应格式应通过 6.2.7.2 检测；
e) 使用正确的签名算法标识、密码杂凑算法标识调用验证时间戳有效性接口，时间戳服务器应成功地验证时间戳响应是否有效，并返回 0；使用错误的签名算法、密码杂凑算法标识调用验证

时间戳有效性接口，应反馈 GM/T 0033—2014 附录 A 中相应状态码；

f) 使用获取时间戳主要信息接口，时间戳服务器应成功获取时间戳的主要信息，并返回 0，否则应反馈 GM/T 0033—2014 附录 A 中相应状态码；

g) 使用正确的指定获取时间戳详细信息的项目编号调用解析时间戳详细信息接口，时间戳服务器应成功地解析时间戳的详细信息，并返回 0；使用错误的项目编号调用解析时间戳详细信息接口，应反馈 GM/T 0033—2014 附录 A 中相应状态码。

6.2.8 可信时间源

可信时间的源头应来源于国家权威时间部门(如国家授时中心)，或者使用国家权威时间部门认可的硬件和方法获取的时间。

可以使用以下的一种或多种方法获得时间。

a) 使用某种无线接收装置，通过无线手段获得国家权威时间部门的时间发布，如长波信号、卫星信号等。

b) 使用某种时间同步协议从一个指定网络地址获得时间。该网络地址发布的时间和使用的时间同步协议都应是可信的，且通过了国家权威时间部门认可。

c) 使用某种通过国家权威时间部门认证的硬件获取时间，如使用原子钟等。

时间戳服务器应能够自动同步时间，通过使用时间戳服务器的管理工具进行测试。时间源同步应满足 GB/T 20520—2006 中 6.3 的要求。

6.3 管理安全检测

6.3.1 配置管理检测

时间戳服务器应具备以下主要管理功能：

a) 网络地址配置功能，该功能包含但不限于配置 IP 地址、子网掩码以及网关地址；

b) 状态管理，该功能包含但不限于部件状态、软件状态、版本状态、当前状态；

c) 配置管理，该功能包含但不限于权限配置、访问控制配置等配置管理功能。

时间戳服务器权限配置应具备：

a) 不少于管理员、审计员两类角色管理；

b) 管理员负责设备的证书管理、访问控制、可信时间源配置等；

c) 审计员负责设备的日志管理操作。

6.3.2 管理员管理检测

时间戳服务器应能够设置管理员和审计员，管理员和审计员应采用智能密码钥匙、智能 IC 卡等硬件装置与登录口令相结合的方式登录系统，并使用证书进行身份验证。

6.3.3 设备访问控制检测

时间戳服务器应能够为内部存储的主体资源提供访问控制功能。通过管理工具进行系统配置和管理应具备完善的身份认证机制，不同的管理操作应有不同的操作权限，应拒绝任何不具备相应权限的访问或操作，防止未经授权的恶意人员进入，破坏设备的安全性。可配置 IP 地址访问控制列表。

对于存储在设备内部的私钥，应持有正确的私钥授权码才能使用。

宜支持由密码设备管理平台管理，符合 GM/T 0050 的规定，且对相应操作进行记录。

6.3.4 设备日志记录检测

时间戳服务器应提供日志记录、查看和导出功能，应对日志信息进行审计，防止日志内容被非法

修改。

时间戳服务器的日志内容应包括：

a） 管理员操作行为，包括登录认证、系统配置、密钥管理等操作；

b） 异常事件，包括认证失败、非法访问等异常事件的记录；

c） 对应用接口的调用进行日志记录。

6.4 性能检测

6.4.1 时间戳生成性能

将请求报文发送给时间戳服务器生成时间戳请求，根据时间戳请求进行时间戳签名操作，多线程（线程数 X）并行 N 次（N 可选择 100、1 000、10 000），测量其完成时间 T（秒）。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。性能指标公式为：$S=X*N/T$；单位为 TPS（次/秒）。

6.4.2 时间戳验证性能

将原文发送给时间戳服务器进行时间戳验证操作，多线程（线程数 X）并行 N 次（N 可选择 100、1 000、10 000），测量其完成时间 T。用于测试的数据由检测机构选取。测试应进行多次，结果取平均值。性能指标公式为：$S=X*N/T$；单位为 TPS。

6.5 设备安全性检测

时间戳服务器安全性检测应符合 GM/T 0039 的规定。

6.6 设备环境适应性检测

时间戳服务器的工作环境应根据实际需要符合 GB/T 9813 中关于“气候环境适应性”的规定。气候环境适应性包括高温工作下限、高温工作上限、低温工作下限、低温工作上限、高温贮存温度上限、低温贮存温度上限、高温贮存温度下限、低温贮存温度下限、湿热工作试验、湿热贮存条件试验。

6.7 设备可靠性检测

时间戳服务器的平均无故障工作时间宜不低于 10 000 h。平均修复时间宜不高于 30 min。

7 送检技术文档要求

研制单位按照商用密码检测认证机构要求提交相关文档资料，作为时间戳服务器的检测依据。

8 合格判定条件

本文件中，除 6.4、6.6 和 6.7 以外的各项检测中，其任意一项检测结果不合格，判定为产品不合格。