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。