ICS 35.040
L 80
备案号:44634—2014

GM

中华人民共和国密码行业标准

GM/T 0033—2014

时间戳接口规范

Interface specifications of time stamp

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：上海市数字证书认证中心有限公司、北京市数字证书认证中心有限公司、上海格尔软件股份有限公司、长春吉大正元信息技术股份有限公司、北京海泰方圆科技有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、兴唐通信科技有限公司、上海颐东网络信息有限公司、万达信息股份有限公司、飞天诚信科技股份有限公司、北京华大智宝电子系统有限公司、北京握奇智能科技有限公司、山东得安信息技术有限公司、国家信息安全工程技术研究中心、国家密码管理局商用密码检测中心。

本标准起草人：刘平、刘承、崔久强、李述胜、谭武征、赵丽丽、柳增寿、徐强、李元正、王妮娜、夏东山、李海杰、于华章、陈跃、胡俊义、孔凡玉、袁峰、李志伟。

时间戳接口规范

1 范围

本标准规定了面向应用系统和时间戳系统的时间戳服务接口，包括时间戳请求和响应消息的格式、传输方式和时间戳服务接口函数。

本标准适用于规范基于公钥密码基础设施应用技术体系框架内的时间戳服务相关产品，以及时间戳服务的集成和应用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件，凡是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 20520 信息安全技术 公钥基础设施 时间戳规范

GM/T 0006 密码应用标识规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

GM/T 0019 通用密码服务接口规范

RFC 3066 Tags for the Identification of Languages

RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

RFC 3369 Cryptographic Message Syntax (CMS)

3 术语和定义

下列术语和定义适用于本文件。

3.1

证书认证机构 certification authority;CA

对数字证书进行全生命周期管理的实体。也称为电子认证服务机构。

3.2

密码杂凑算法 cryptographic hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

(1)为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

(2)为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的。

(3)要发现不同的输入映射到同一输出是计算上困难的。

3.3

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。