ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38629—2020

信息安全技术
签名验签服务器技术规范

Information security technology—
Technical specifications for signature verification server

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东得安信息技术有限公司、成都卫士通信息产业股份公司、无锡江南信息安全工程技术中心、兴唐通信科技有限公司、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、上海市数字证书认证中心有限公司、北京数字认证股份有限公司、北京创原天地科技有限公司、北京三未信安科技发展有限公司、北京信安世纪科技股份有限公司。

本标准主要起草人:马洪富、孔凡玉、罗俊、徐明翼、王妮娜、郑强、赵丽丽、韩玮、李述胜、肖青海、高志权、汪宗斌。

信息安全技术
签名验签服务器技术规范

1 范围

本标准规定了签名验签服务器的功能要求、安全要求和消息协议语法规则等内容。

本标准适用于签名验签服务器的研制和使用。

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 9813.3—2017 计算机通用规范 第3部分：服务器

GB/T 19713—2005 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 25069—2010 信息安全技术 术语

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—2017 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

GB/T 35291—2017 信息安全技术 智能密码钥匙应用接口规范

GB/T 36322 信息安全技术 密码设备应用接口规范

GM/T 0020 证书应用综合服务接口规范

GM/T 0028 密码模块安全要求

GM/T 0039 密码模块安全检测要求

3 术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

安全域 security domain

在信息系统中，单一安全策略下运行的实体的汇集。例如，由单个或一组认证机构采用同一安全策略创建的各公钥证书的汇集。

[GB/T 25069—2010，定义 2.2.1.17]

3.2

签名验签服务器 signature verification server

用于服务端的，为应用实体提供基于PKI体系和数字证书的数字签名、验证签名等运算功能的服务器，保证关键业务信息的真实性、完整性和不可否认性。

3.3

用户 user

与应用实体进行通信或认证的个人、机构或系统。