ICS 35.040
L 80
备案号:44630—2014

GM

中华人民共和国密码行业标准

GM/T 0029—2014

签名验签服务器技术规范

Sign and verify server technical specification

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：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、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、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、山东渔翁信息技术股份有限公司。

本标准主要起草人：刘平、孔凡玉、李元正、王妮娜、谭武征、赵丽丽、刘承、李述胜、王晓晨、高志权、宋志华。

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、接口要求、检测要求和消息协议语法规范等有关内容。

本标准适用于签名验签服务器的研制设计、应用开发、管理和使用，也可用于指导签名验签服务器的检测。

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 微型计算机通用规范

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

GM/T 0006—2012 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0018 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 0030 服务器密码机技术规范

PKCS #1 RSA 密码算法使用规范

PKCS #7 RSA 密码算法消息语法规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

签名验签服务器 sign and verify 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，可以保证关键业务信息的真实性、完整性和不可否认性。

3.2

应用实体 application entity

签名验签服务器的服务对象，可以是个人、机构或系统，其私钥存储在签名验签服务器的密码设备中，能够使用签名验签服务器进行签名及验签运算。

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，其数字证书可导入到签名验签服务器中。