ICS 35.040
L 80
备案号：62995—2018

GM

# 中华人民共和国密码行业标准

GM/T 0060—2018

# 签名验签服务器检测规范

**Test specification for signature/verification server**

2018-05-02 发布　　2018-05-02 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、国家密码管理局商用密码检测中心、上海格尔软件股份有限公司、北京数字认证股份有限公司、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、北京创原天地科技有限公司。

本标准主要起草人：马洪富、孔凡玉、郑海森、邓开勇、罗鹏、李国友、刘常、谭武征、李述胜、徐明翼、李元正、王妮娜、王晓晨。

# 签名验签服务器检测规范

## 1 范围

本标准规定了签名验签服务器设备的检测内容、检测方法及检测要求等。

本标准适用于签名验签服务器设备的检测，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 17901 信息技术 安全技术 密钥管理

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918 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

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 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0020 证书应用综合服务接口规范

GM/T 0029—2014 签名验签服务器技术规范

GM/T 0039 密码模块安全检测要求

## 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 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，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。