ICS 35.040
L 80

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 sign and verify server

2018-05-02 发布　　2018-05-02 实施

国家密码管理局　　发布

目　次

前　言

本标准依据 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 17901.1-1999 信息技术 安全技术 密钥管理 第一部分

GB/T 17901.2-1999 信息技术 安全技术 密钥管理 第一部分

GB/T 17901.3-1999 信息技术 安全技术 密钥管理 第一部分

GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法

GB/T 32915-2016 信息安全技术 二元序列随机性检测规范

GB/T 32918.1-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第一部分

GB/T 32918.2-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第二部分

GB/T 32918.3-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第三部分

GB/T 32918.4-2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第四部分

GB/T 33560-2017 信息安全技术 密码应用标识规范

GM/T 0009-2012 SM2 密码算法使用规范

GM/T 0010-2012 SM2 密码算法加密签名消息语法规范

GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范

GM/T 0020-2012 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 0039-2015 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 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。

3.4

SM2 算法　SM2 algorithm

由 GB/T 32918 定义的一种算法。

3.5

SM3 算法　SM3 algorithm

由 GB/T 32905 定义的一种算法。

4　符号和缩略语

下列缩略语适用于本文件。

API　应用程序接口 (Application Program Interface)
CRL　证书撤销列表(Certificate Revocation List)
LDAP　轻量级目录访问协议(Lightweight Directory Access Protocol)
NTP　网络时间协议(Network Time Protocol)
OCSP　在线证书状态查询协议(Online Certificate Status Protocol)
PKI　公钥密码基础设施(Public Key Infrastructure)
PKCS　公钥密码标准(The Public-Key Cryptography Standards)

5　检测环境要求

5.1　常规检测环境

签名验签服务器的常规检测环境，用于测试签名验签服务器的功能和性能，检测环境拓扑可参考图 1。

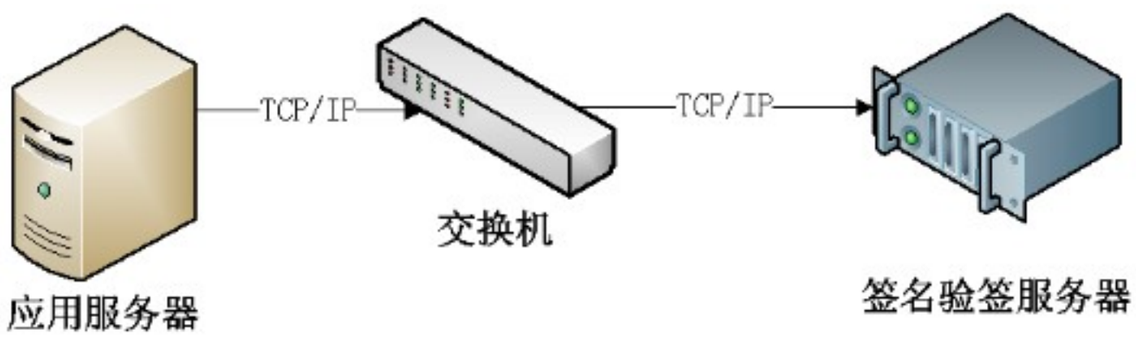

图 1　签名验签服务器的常规检测环境拓扑图

5.2　跨网段检测环境

签名验签服务器的跨网段检测环境，用于测试签名验签服务器的跨网段服务能力，检测环境拓扑可参考图 2。

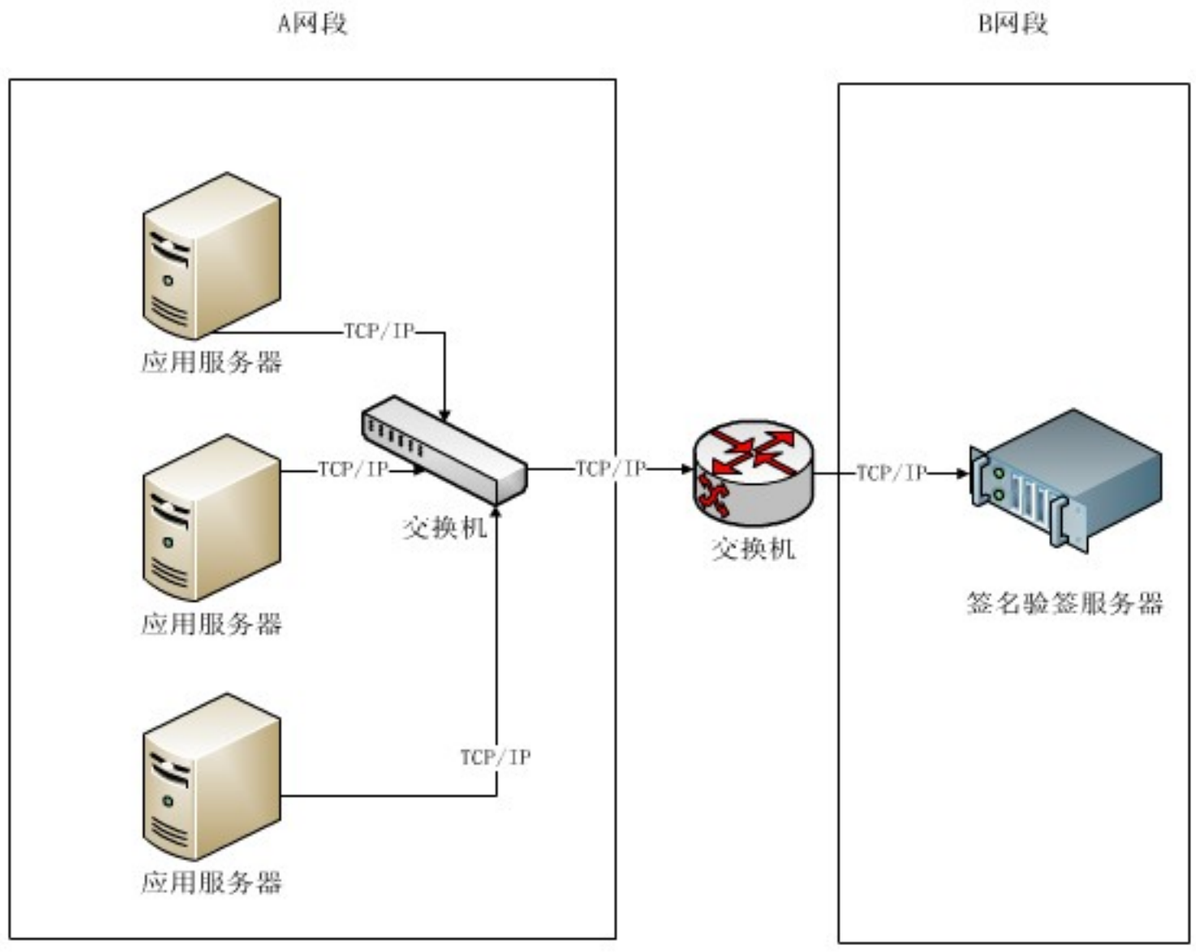

图 2　签名验签服务器的跨网段检测环境拓扑图

6　检测内容及检测方法

6.1　外观和结构的检查

根据产品的物理参数，对签名验签服务器的外观、尺寸、内部部件、密码运算部件、管理员身份验证设备及附件进行检查。

签名验签服务器应具备以下主要部件或接口：

a)　具备电源指示灯；

b)　具备状态指示灯；

c)　具备故障指示灯；

d)　具备至少 2 个 RJ45 网络接口。

签名验签服务器宜具备以下主要部件或接口：

a)　宜具备人机交互部件；

b)　宜具备冗余电源；

c)　宜具备密钥销毁按钮或插销，只有当签名验签服务器中的所有密钥已确定不再使用等情况下，才能使用密钥销毁按钮或插销；

d)　宜具备串口。

6.2　功能检测

6.2.1 初始化功能检测

签名验签服务器能正常启动，对签名验签服务器进行初始化功能检测。初始化主要包括系统配置、生成管理员，使设备处于正常工作状态。签名验签服务器应能够正常初始化。

6.2.2 与公钥基础设施的连接功能检测

签名验签服务器与公钥基础设施的连接功能检测范围包括 CRL 连接配置、OCSP 连接配置等操作，通过使用签名验签服务器的管理工具进行测试。

6.2.3 应用管理功能检测

签名验签服务器的应用管理功能检测范围主要包括应用实体的注册和用户信息(应用实体名称、配置的密钥索引号、设置的私钥授权码和导入的证书等)的存储和销毁，通过使用签名验签服务器的管理工具进行测试。

6.2.4 证书管理和验证功能检测

签名验签服务器的证书管理和验证功能检测范围包括对应用实体证书、用户证书、根证书或证书链的导入、存储、验证、使用、删除以及备份和恢复等操作，包括对密钥的产生、导入、存储、销毁以及备份和恢复等操作，通过使用签名验签服务器的管理工具进行测试。

签名验签服务器的证书管理和验证功能检测时，SM2 证书应符合 GM/T 0015 要求。

6.2.5 数字签名功能检测

签名验签服务器的数字签名功能测试程序由检测方提供。检测方法是将签名验签服务器的密码运算与检测方提供的检测平台对接，如果与检测平台对接成功，则测试通过；否则，测试失败。

数字签名功能检测的范围应包括签名验签服务器提供的每个公钥密码算法的每个功能函数，如：数据、消息、文件等多种格式的运算方式，按照 GM/T 0029-2014 附录 A、附录 B 或 GM/T 0020 的要求进行测试。签名验签服务器应支持 SM2 算法的数字签名功能测试。

签名验签服务器数字签名功能测试时使用的签名算法标识，详见 GB/T 33560。

签名验签服务器数字签名功能 SM2 算法测试时，数据的结构应符合 GB/T 32905、GM/T 0009 和 GM/T 0010 要求。

6.2.6 访问控制功能检测

签名验签服务器应能够为内部存储的主体资源提供访问控制功能。通过管理工具进行系统配置和管理应具备完善的身份认证机制，不同的管理操作应有不同的操作权限，签名验签服务器应拒绝任何不具备相应权限的访问或操作，防止未经授权的恶意人员进入，破坏设备的安全性。

对于存储在设备内部的私钥，应持有正确的私钥授权码才能使用。

6.2.7 日志管理功能检测

签名验签服务器应提供日志记录、查看、审计和导出功能。日志内容应包括：

a) 管理员操作行为，包括登录认证、系统配置、密钥管理等操作；
b) 异常事件，包括认证失败、非法访问等异常事件的记录；
c) 如与设备管理中心连接，则对相应操作进行记录；
d) 对应用接口的调用也可进行日志记录。

6.2.8 系统自检功能检测

签名验签服务器应具备自检功能，检验签名验签服务器自身的密码部件、算法、随机数等软硬件状态,包括算法正确性检测、随机数发生器检测、存储密钥和数据的完整性检测，以及关键部件的正确性检测等。

自检功能应在每次加电启动后自动执行，自检结束后应报告检测结果。

自检成功，签名验签服务器进入管理状态或工作状态。

自检失败，签名验签服务器停止工作并报告检测结果。

6.2.9 NTP 时间源同步功能检测

签名验签服务器应能够与时间源服务器进行连接配置，自动同步时间，通过使用签名验签服务器的管理工具进行测试。

6.2.10 服务接口检测

签名验签服务器的服务接口应遵循 GM/T 0029-2014 附录 A、附录 B 或 GM/T 0020 的要求。

签名验签服务器对于正确的调用环境和调用过程，API 函数应返回正确的结果，并完成相应功能；对于设定的不正确的调用环境和调用过程，API 函数应返回相应的错误代码。

6.2.11 管理工具功能检测

签名验签服务器提供的管理工具应具备以下主要管理功能：

a） 网络地址配置功能，该功能包含但不限于配置 IP 地址、子网掩码以及网关地址；

b） 状态管理，该功能包含但不限于部件状态、软件状态、版本状态、当前状态；

c） 配置管理，该功能包含但不限于权限配置、访问控制配置等配置管理功能。

签名验签服务器权限配置应具备：

a）不少于管理员、审计员两类角色管理；

b）管理员负责设备的应用管理、证书管理、访问控制、私钥授权码、与公钥基础设施连接配置和 NTP 配置等；

c）审计员负责设备的日志管理操作。

签名验签服务器访问控制配置可具备：

a）IP 地址访问控制授权表配置。

6.2.12 管理员管理功能检测

签名验签服务器应能够设置管理员和审计员，管理员和审计员应采用智能密码钥匙、智能 IC 卡等硬件装置与登录口令相结合的方式登录系统，并使用证书进行身份验证。管理员通过身份鉴别后执行应用管理、证书管理、系统配置等管理操作。

6.2.13 随机数随机性检测

签名验签服务器使用的密码设备应至少采用两个独立的物理噪声源芯片，用于实现随机数生成功能。随机数随机性检测按照 GB/T 32915 的要求进行检测，本标准不作另行要求。

6.2.14 密钥管理检测

签名验签服务器应依据相关技术规范的要求，具备完善的密钥管理功能，密钥管理包括密钥的产生、存储、更换、备份、恢复和销毁。签名验签服务器应保证密钥在生命周期的各个环节的安全性。密钥管理检测按照 GB/T 17901 的要求进行检测，本标准不作另行要求。

6.2.15 算法正确性与一致性检测

6.2.15.1 对称算法检测

签名验签服务器应支持 SM1 或 SM4 对称密码算法，对每种算法应至少提供 ECB、CBC、OFB 三种工作模式，同时可扩展支持其他工作模式。

签名验签服务器应能按照指定的工作模式对数据进行加解密运算，应能支持各模式下分别给定密钥和明文（密文），测试其运算结果的正确性，包括：

a) 签名验签服务器对给定的密钥和明文经对称算法 ECB 模式加密，结果和给定密文完全相同；
b) 签名验签服务器对给定的密钥和密文经对称算法 ECB 模式解密，结果和给定明文完全相同；
c) 签名验签服务器对给定的密钥和明文经对称算法 CBC 模式加密，结果和给定密文完全相同；
d) 签名验签服务器对给定的密钥和密文经对称算法 CBC 模式解密，结果和给定明文完全相同。
e) 签名验签服务器对给定的密钥和明文经对称算法 OFB 模式加密，结果和给定密文完全相同；
f) 签名验签服务器对给定的密钥和密文经对称算法 OFB 模式解密，结果和给定明文完全相同。

6.2.15.2 非对称算法检测

签名验签服务器应支持 SM2 公钥密码算法。签名验签服务器应能够使用 SM2 算法对数据进行加解密、签名/验签和密钥协商运算。应能支持给定密钥和明文、待签名消息、密钥协商参数，测试其运算结果的正确性，包括：

a) 签名验签服务器对给定的密钥和明文使用 SM2 算法加密后，检测平台对密文进行解密运算，解密结果和给定明文完全相同；
b) 签名验签服务器对给定的密钥和明文使用 SM2 算法加密后，再经 SM2 解密运算，解密结果和给定明文完全相同；
c) 签名验签服务器使用给定的密钥对待签名消息进行 SM2 算法签名后，检测平台对签名结果进行验签，验签通过；
d) 签名验签服务器使用给定的密钥对待签名消息调用 SM2 算法签名后，再经 SM2 算法进行验签运算，验签通过；
e) 签名验签服务器使用给定的密钥和密钥协商参数，调用 SM2 密钥协商算法与检测平台进行密钥协商，协商结果正确。

6.2.15.3 杂凑算法检测

签名验签服务器应支持 SM3 算法，对给定的消息和参数，能够调用 SM3 算法对消息进行杂凑运算，测试方法包括：

a) 签名验签服务器对给定消息调用 SM3 算法计算杂凑值，结果和给定杂凑值完全相同；
b) 签名验签服务器对给定消息和参数调用 SM3 算法计算杂凑值，结果和给定杂凑值完全相同。

6.3 性能检测

6.3.1 数字签名性能检测

签名验签服务器的数字签名运算可实现 SM2 数字签名、SM2 验证签名（CRL/OCSP）、SM2 文件签名、SM2 验证文件签名（CRL/OCSP）、SM2 加密/解密、SM2 文件加密/解密、SM2 消息签名、SM2 验证消息签名（CRL/OCSP）等功能，并满足一定的速度指标。用于测试的数据由检测机构选取，测试应进行多次，结果取各次的平均值。

a) SM2 数字签名、SM2 验证签名（CRL/OCSP）、SM2 文件签名、SM2 验证文件签名（CRL/OCSP）、SM2 消息签名、SM2 验证消息签名（CRL/OCSP）等性能测试：

将一个定长数据报文（数据长度可以选择 32 字节、128 字节、256 字节、1024 字节等），

发送给签名验签服务器进行数字签名/验证，重复操作 N 次，测量其完成时间 T。根据各个测试项的具体耗时情况，依照等比序列来选取测试次数，例如：测试次数 N 可以选择 1 次、10 次、100 次、1000 次等，分别测试后得到不同测试次数时的性能序列，性能的计算如下式所示：

$$S = \frac{N}{T}$$

其中，S 为速度，单位为 tps（次/秒）；N 为测试次数；T 为测量所耗费的时间，单位为秒。

b) SM2 加密/解密、SM2 文件加密/解密等性能测试：

将一个长度为 L(L 可以选择 32 字节、128 字节、256 字节、1024 字节等)的数据报文，发送给签名验签服务器进行加密/解密操作，重复操作 N 次，测量其完成时间 T（秒）。

公式为：$S = \frac{8LN}{1024 \times 1024T}$；单位为 Mbit/s(兆比特每秒)。

如签名验签服务器支持多种公钥密码算法，应测试所支持的所有公钥密码算法及其各种应用模式。

6.3.2 算法性能检测

签名验签服务器的各项算法应满足一定的速度指标。

a) 签名验签服务器 SM2 算法密钥对生成性能测试：测试 SM2 算法的密钥对生成速度；重复操作 N 次，测量其完成时间 T（秒），计算公式为：

$$S = \frac{N}{T}$$

其中，S 为速度，单位为 tps（次/秒）；N 为测试次数；T 为测量所耗费的时间，单位为秒。

b) 签名验签服务器 SM2 算法签名/验证性能测试：测试 SM2 算法的签名/验证速度；将杂凑后 32 字节的数据报文，发送给签名验签服务器进行签名/验证操作，重复操作 N 次，测量其完成时间 T（秒）。，计算公式为：

$$S = \frac{N}{T}$$

其中，S 为速度，单位为 tps（次/秒）；N 为测试次数；T 为测量所耗费的时间，单位为秒。

c) 签名验签服务器 SM2 算法加密/解密性能测试：测试 SM2 算法的加密/解密速度；将一个长度为 L(L 可以选择 32 字节、128 字节、256 字节、1024 字节等)的数据报文，发送给签名验签服务器进行加密/解密操作，重复操作 N 次，测量其完成时间 T(秒)。

公式为：$S = \frac{8LN}{1024 \times 1024T}$；单位为 Mbit/s(兆比特每秒)。

d) 签名验签服务器 SM3 算法运算性能测试：测试 SM3 算法运算速度；将一个长度为 L（L 可以选择 32 字节、128 字节、256 字节、1024 字节等）的数据报文，发送给签名验签服务器进行摘要运算，重复操作 N 次，测量其完成时间 T（秒）。

公式为：$S = \frac{8LN}{1024 \times 1024T}$；单位为 Mbit/s(兆比特每秒)。

e) 签名验签服务器 SM1 或 SM4 对称密码算法加解密性能测试：测试 SM1 或 SM4 对称算法所支持的工作模式的加/解密速度；将一个长度为 L（L 可以选择 32 字节、128 字节、256 字节、1024 字节等）的数据报文，发送给签名验签服务器进行加/解密操作，重复操作 N次，测量其完成时间 T（秒）。

公式为：$S = \frac{8LN}{1024 \times 1024T}$；单位为 Mbit/s(兆比特每秒)。

6.3.3 并发性能检测

签名验签服务器应满足一定的并发连接数要求，支持多连接并发测试。

参考 6.3.1 节和 6.3.2 节的要求，并配置连接数 M（M可以选择 16、32、64、128 等）进行各种算法性能测试。计算公式为 6.3.1 节和 6.3.2 节描述公式的基础上乘以 M。

例如，SM2 算法加密/解密的公式为：$S = \frac{8LNM}{1024 \times 1024T}$；单位为 Mbit/s(兆比特每秒)。

6.4 其它检测

6.4.1 设备网络适应性测试

签名验签服务器对使用主体的服务模式应具备良好的适应性和扩展性，至少应满足四种模式的应用要求，包括：

a) 一台应用服务器对应一台签名验签服务器；
b) 一台应用服务器对应多台签名验签服务器；
c) 多台应用服务器对应一台签名验签服务器；
d) 多台应用服务器对应多台签名验签服务器。

应使用交换机等网络设备分别搭建以上四种应用模式，测试签名验签服务器是否在每种应用模式中正常工作。

6.4.2 设备安全性测试

签名验签服务器设备安全性测试遵照 GM/T 0039 的要求。

6.4.3 设备环境适应性测试

签名验签服务器设备环境适应性测试应达到 GM/T 0029-2014 第 6.8 节的要求。

6.4.4 设备可靠性测试

签名验签服务器设备可靠性测试应达到 GM/T 0029-2014 第 6.9 节的要求。

7 送检技术文档要求

签名验签服务器研制单位按照国家密码管理主管部门检测要求提交相关文档资料，作为签名验签服务器的检测依据。文档资料应包含但不限于以下内容：

a) 后台服务程序、应用程序接口和客户端管理软件的结构框图、流程图和基本功能的源代码；
b) 开机自检的工作原理说明；
c) 自测程序的工作原理说明；
d) 敏感数据信息的存储和使用说明；

e) 物理防护措施说明；
f) 技术工作总结报告；
g) 安全性设计报告；
h) 安装使用说明；
i) 算法自检说明；
j) 随机数自检原理说明。

附 录 A
（规范性附录）
测试项目列表

A.1 外观结构测试

外观结构测试项目见表 A.1。

表 A.1 外观结构测试项目列表

测试项目	测试子项目
外观和结构的检查	根据产品的物理参数，对签名验签服务器的外观、尺寸、内部部件、密码运算部件、管理员身份验证设备及附件进行检查
	设备应具备以下部件或接口： a)电源指示灯； b)状态指示灯； c)故障指示灯； d)至少 2 个 RJ45 网络接口。
	设备宜具备以下部件或接口： a)人机交互部件； b)冗余电源； c)密钥销毁按钮或插销； d)串口。

A.2 提交文档测试

提交文档测试项目见表 A.2。

表 A.2　提交文档测试项目列表

测试项目	测试子项目
提交文档的检查	文档资料应包含以下内容： a)后台服务程序、应用编程接口和客户端管理软件的结构框图、流程图和基本功能的源代码； b)开机自检的工作原理说明； c)自测程序的工作原理说明； d)敏感数据信息的存储和使用说明； e)物理防护措施说明； f)技术工作总结报告； g)安全性设计报告； h)安装使用说明； i)算法自检说明； j)随机数自检原理说明； k)基本功能的源代码中开源代码的比例审查（具体比例依据国家密码管理局要求）。

A.3 功能检测测试

功能检测测试项目见表 A.3。

表 A.3　功能检测测试项目列表

测试项目	测试子项目
初始化功能检测	设备能正常启动
	设备可以进行系统配置、生成管理员，设备能处于正常工作状态
与公钥基础设施的连接功能检测	设备能正常进行 CRL 连接配置操作并连接正常
	设备能正常进行 OCSP 连接配置操作并连接正常
应用管理功能检测	设备能进行应用实体的注册和用户信息的存储、销毁
	设备可以查询应用实体的注册信息
证书管理和验证功能检测	设备可以对多个根证书或证书链（SM2）进行导入、存储和删除
	设备可以对应用实体证书、用户证书进行导入、存储、删除并使用导入的根证书或证书链验证其有效性
	设备可以对应用实体证书、用户证书、根证书或证书链进行备份和恢复
	设备可以产生、导入、存储、销毁以及备份和恢复密钥
数字签名功能检测	设备 SM2 算法数字签名与第三方设备进行互通测试
	设备 SM2 算法文件签名与第三方设备进行互通测试
	设备 SM2 算法加密数据与第三方设备进行互通测试
	设备 SM2 算法文件加密与第三方设备进行互通测试
	设备 SM2 算法消息签名与第三方设备进行互通测试
访问控制	登录设备应具备完善的身份认证机制
	无正确私钥授权码不能使用指定的设备内部私钥进行运算
	已许可 IP 的主机可正常调用设备功能
	未许可 IP 的主机不可正常调用设备功能
日志管理功能检测	设备对管理员操作行为具备日志记录
	设备对异常事件提供日志记录
	设备对与设备管理中心连接情况提供日志记录
	设备对应用接口的调用提供日志记录
	日志可查看、可导出、可审计
系统自检检测	设备开机自动进行自检功能
	设备自检成功自动进入管理状态或工作状态
	设备自检失败，签名验签服务器停止工作，报告检测结果。
NTP 时间源同步功能检测	设备应能够进行时间源服务器的连接配置，自动同步时间。
服务接口检测	设备应用编程接口应遵循 GM/T 0029-2014 附录 A 、附录 B 或 GM/T 0020 要求返回正确结果或正确的错误码。
	签名验签服务器对于正确的调用环境和调用过程，API 函数应返回正确的结果，并完成相应功能。
	签名验签服务器对于设定的不正确的调用环境和调用过程，API 函数应返回相应的错误代码。

表 A.3（续）

测试项目	测试子项目
管理工具功能检测	设备地址配置功能，该功能包含但不限于配置 IP 地址、子网掩码以及网关地址。
	设备状态管理，该功能包含但不限于部件状态、软件状态、版本状态、当前状态。
	设备权限配置应具备： a)应不少于管理员、审计员两类角色管理； b)管理员负责设备的应用管理、证书管理、访问控制、私钥授权码、与公钥基础设施连接配置和 NTP 配置操作； c)审计员负责设备的日志管理操作。
	设备访问控制配置可具备： a)IP 地址访问控制授权表配置。
管理员管理功能检测	签名验签服务器应能够设置管理员和审计员
	管理员和审计员应采用智能密码钥匙、智能 IC 卡等硬件装置与登录口令相结合的方式登录系统，并使用证书进行身份验证。
	各管理员通过身份鉴别后执行应用管理、证书管理、系统配置等管理操作。
设备随机数随机性测试	采用的密码模块应至少两个独立随机源
	对设备产生的随机数进行随机性检测满足 GB/T 32915 要求
密钥管理检测	签名验签服务器应保证密钥在生命周期各个环节的安全性
算法正确性与一致性检测	对称算法正确性与一致性
	非对称算法算法正确性与一致性
	杂凑算法算法正确性与一致性

A.4 性能检测测试

性能检测测试项目见表 A.4。

表 A.4 性能检测测试项目列表

测试项目	测试子项目
数字签名性能检测	设备 SM2 算法数字签名
	设备 SM2 算法验证签名(CRL 和 OCSP 均不验证模式)
	设备 SM2 算法验证签名(CRL 验证模式)
	设备 SM2 算法验证签名(OCSP 验证模式)
	设备 SM2 算法文件签名
	设备 SM2 算法验证文件签名(CRL 和 OCSP 均不验证模式)
	设备 SM2 算法验证文件签名(CRL 验证模式)
	设备 SM2 算法验证文件签名(OCSP 验证模式)
	设备 SM2 算法加密数据
	设备 SM2 算法解密数据
	设备 SM2 算法文件加密
	设备 SM2 算法文件解密
	设备 SM2 算法消息签名
	设备 SM2 算法验证消息签名(CRL 和 OCSP 均不验证模式)
	设备 SM2 算法验证消息签名(CRL 验证模式)
	设备 SM2 算法验证消息签名(OCSP 验证模式)
算法性能检测	设备 SM2 算法密钥对生成性能
	设备 SM2 算法签名性能
	设备 SM2 算法验证性能
	设备 SM2 算法加密性能
	设备 SM2 算法解密性能
	设备 SM3 算法性能（不带 ID）
	设备 SM3 算法性能（带 ID）
	设备对称算法 ECB 模式性能
	设备对称算法 CBC 模式性能
	设备对称算法 OFB 模式性能
	设备对称算法 CFB 模式性能

A.5 其它检测测试

其它检测测试项目见表 A.5。

表 A.5 其它检测测试项目列表

测试项目	测试子项目
设备网络适应性测试	一台应用服务器对应一台签名验签服务器
	一台应用服务器对应多台签名验签服务器
	多台应用服务器对应一台签名验签服务器
	多台应用服务器对应多台签名验签服务器
设备安全性测试	对设备安全性检测满足 GM/T 0039 的要求
设备环境适应性测试	对设备环境适应性检测达到 GM/T 0029-2014 第 6.8 节的要求
设备可靠性测试	对设备可靠性检测达到 GM/T 0029-2014 第 6.9 节的要求。