ICS 35.040
L 80
备案号:49741—2015

GM

中华人民共和国密码行业标准

GM/T 0042—2015

三元对等密码安全协议测试规范

Test specification for cryptography and security protocol in tri-element peer architecture

2015-04-01 发布　　2015-04-01 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：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、中国电信集团公司、中国航天科工集团第二研究院七〇六所、中国电子科技集团公司第十五研究所、国家信息中心、总参第六十一研究所、北京市政务网络管理中心、WAPI 产业联盟、广州杰赛科技股份有限公司、深圳市明华澳汉科技股份有限公司、公安部信息安全等级保护评估中心、北京中电华大电子设计有限责任公司。

本标准主要起草人：曹军、李琴、黄振海、李大为、邓开勇、胡亚楠、宋起柱、高波、孔雷、罗鹏、李国友、李光、吴亚非、杨林、李延春、秦志强、周涛、朱正美、姚蕊、詹葆荣、沈宇超、潘琪、师倩俊、杜志强、颜湘、王月辉、张变玲、铁满霞、张强、张国强、李明、张莎、丁启枫、刘鹄、杨峰、黄丽、潘毅明、童伟刚、王磊等。

引　言

三元对等架构(Tri-element Peer Architecture,TePA)是我国自主提出的普适性网络安全技术架构,其核心技术于2010年6月1日获国际标准化组织ISO/IEC批准发布为国际标准(标准号:ISO/IEC 9798-3:1998/Amd.1:2010),并被批准发布为国家标准(标准号:GB/T 28455—2012)。

三元对等架构是网络与信息安全领域基础共性技术架构,可扩展应用于有线网络、无线移动网络、近距离通信网络、IP安全、数据安全与隐私等多个应用领域,并且支持国家密码管理主管部门认可的密码算法。

本标准的主要目的是针对符合国际标准ISO/IEC 9798-3:1998/Amd.1:2010和国家标准GB/T 15843.3、GB/T 28455—2012的基于三元对等架构的密码安全协议(以下简称三元对等密码安全协议),提出一套测试要求及方法。

本标准是与三元对等架构对应的框架性测试规范,可为三元对等密码安全协议的设计提供参考,提高符合三元对等架构的相关产品的互操作性。

三元对等密码安全协议测试规范

1 范围

本标准规定了三元对等密码安全协议对相关密码算法与安全协议应满足的基本技术要求和对应的测试方法,适用于三元对等密码安全协议相关产品的检测。主要包括如下内容:

a) 密码算法实现的正确性和一致性的技术要求及测试方法;

b) 协议实现的符合性和互操作性的基本技术要求及测试方法。

本标准适用于符合 ISO/IEC 9798-3:1998/Amd.1:2010 和 GB/T 15843.3、GB/T 28455—2012 的设备,用于检测其密码算法和协议实现是否符合上述标准的要求。

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 15843.3 信息技术 安全技术 实体鉴别 第3部分:采用数字签名技术的机制

GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

GM/T 0002 SM4 分组密码算法

GM/T 0003 SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

GM/T 0005 随机性检测规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

GM/Z 4001 密码术语

CBWIPS/Z 021—2010 无线局域网网络设备标识规范

ISO/IEC 9798-3:1998/Amd.1:2010 信息技术 安全技术 实体鉴别 第3部分:采用数字签名技术的机制 补篇1(Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques—Amendment 1)

3 术语和定义

GM/Z 4001 和 GB/T 28455—2012 所界定的以及下列术语和定义适用于本文件。

3.1

被测设备 tested equipment

实现三元对等密码安全协议的设备。

3.2

测试平台 test platform

提供三元对等密码安全协议测试的平台,用于收集和分析处理测试数据,按照测试规范的要求对测