ICS 35.040
L 80
备案号:44631—2014

GM

中华人民共和国密码行业标准

GM/T 0030—2014

服务器密码机技术规范

Cryptographic 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、海泰方圆科技有限公司。

本标准主要起草人：刘平、孔凡玉、李元正、徐强、李玉峰、谭武征、柳增寿。

服务器密码机技术规范

1 范围

本标准定义了服务器密码机的相关术语，规定了服务器密码机功能要求、硬件要求、软件要求、安全性要求和检测要求等有关内容。

本标准适用于服务器密码机的研制、使用，也可用于指导服务器密码机的检测。

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

GM/T 0005 随机性检测规范

GM/T 0018 密码设备应用接口规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

服务器密码机 cryptographic server

又称主机加密服务器，能独立或并行为多个应用实体提供密码服务和密钥管理的设备。

3.2

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.3

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开，另一个密钥(私钥)必须保密，且由公钥求解私钥是计算不可行的。

3.4

密码杂凑算法 cryptographic hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列三个特性：

(1)为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

(2)为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

(3)要发现不同的输入映射到同一输出是计算上困难的。

3.5

公钥/私钥 public key /private key

非对称密码算法中可以公开的密钥称为公钥。非对称密码算法中只能由拥有者使用的不公开密钥