ICS 35.040
L 80
备案号：62996—2018

GM

中华人民共和国密码行业标准

GM/T 0061—2018

动态口令密码应用检测规范

Detect specifications of one time password application

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：上海众人网络安全技术有限公司、国家密码管理局商用密码检测中心、北京集联网络技术有限公司、上海华虹集成电路有限责任公司。

本标准主要起草人：谈剑锋、李大为、邓开勇、罗鹏、尤磊、盛学明、刘文娟、莫凡、郭思建、周海京。

动态口令密码应用检测规范

1 范围

本标准规定了动态口令系统的口令算法、动态令牌、认证系统和密钥管理系统等相关的检测内容。本标准适用于动态口令相关密码产品的密码及安全功能检测。

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。

GM/T 0021—2012 动态口令密码应用技术规范

GM/Z 4001—2013 密码术语

3 术语与定义

GM/T 0021—2012、GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

3.1

挑战码 challenge code

即挑战因子，可参与到动态口令生成过程中的一种数据。

3.2

UTC 时间 universal time coordinated

协调世界时(Universal Time Coordinated)英文缩写，是由国际无线电咨询委员会规定和推荐，并由国际时间局(BIH)负责保持的以秒为基础的时间标度，是距 1970 年 1 月 1 日 00：00 时(格林尼治标准时间)的秒数。

3.3

种子密钥 seed key

即令牌种子密钥，计算动态口令的密钥。

3.4

认证系统 authentication system

对动态口令进行认证，对动态令牌进行管理的系统。

3.5

未激活 not activated

本状态为出厂时状态，成功激活后进入就绪状态。

3.6

就绪 ready

令牌为正常工作状态。

3.7

锁定 be locked

令牌因连续错误、重放攻击等原因被锁定后处于锁定状态。