

ICS 35.040
L 80
备案号:38319—2013



中华人民共和国密码行业标准

GM/T 0021—2012

动态口令密码应用 技术规范

One time password application of
cryptography algorithm

2012-11-22 发布

2012-11-22 实施

国家密码管理局 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号	3
5 动态口令系统	4
5.1 概述	4
5.2 总体框架	4
5.3 基本认证原理简述	5
6 动态口令生成方式	6
6.1 概述	6
6.2 算法使用说明	6
6.3 截位算法	7
7 动态令牌特性	8
7.1 令牌硬件要求	8
7.2 令牌安全特性	9
8 认证系统	10
8.1 系统说明	10
8.2 认证系统服务	11
8.3 认证系统管理功能	13
8.4 安全要求	13
9 密钥管理系统	14
9.1 概述	14
9.2 系统架构	14
9.3 功能要求	16
9.4 系统安全性设计	17
9.5 硬件密码设备接口说明	21
附录 A (资料性附录) 动态口令生成算法 C 语言实现用例	22
A.1 采用 SM3 的动态口令生成算法用例	22
A.2 采用 SM4 的动态口令生成算法用例	27
附录 B (资料性附录) 动态口令生成算法计算输入输出用例	34
B.1 采用 SM3 的动态口令生成算法输入输出用例	34
B.2 采用 SM4 的动态口令生成算法输入输出用例	34
附录 C (资料性附录) 运算参数与数据说明用例	36
附录 D (资料性附录) 认证系统接口	37

GM/T 0021—2012

D.1	服务报文格式	37
D.2	服务标识	39
D.3	数据标识	39
D.4	返回码	40
D.5	应用接口	41

前 言

本标准依据 GB/T 1.1—2009 给出的规则起草。

请注意本标准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。

本标准的附录 A、附录 B、附录 C、附录 D 为资料性附录。

本标准由国家密码管理局提出并归口。

本标准起草单位：上海众人网络安全技术有限公司，上海复旦微电子股份有限公司，飞天诚信科技股份有限公司，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，深圳同方电子设备有限公司，上海林果实业有限公司，上海格尔软件股份有限公司。

本标准主要起草人：詹榜华、谈剑锋、尤磊、柳逊、陈达、郭思建、张志茂、李阆、牛毅。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

动态口令密码应用 技术规范

1 范围

本标准规定了动态口令系统、动态口令生成方式、动态令牌特性、认证系统、密钥管理系统等的相关内容。

本标准适用于动态口令相关产品的研制、生产,也可用于指导相关产品的检测。

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 2423.1—2008 电工电子产品环境试验 第2部分:试验方法 试验 A:低温
- GB/T 2423.2—2008 电工电子产品环境试验 第2部分:试验方法 试验 B:高温
- GB/T 2423.8—1995 电工电子产品环境试验 第2部分:试验方法 试验 Ed:自由跌落
- GB/T 2423.9—2001 电工电子产品环境试验 第2部分:试验方法 试验 Cb 设备用恒定湿热
- GB/T 2423.10—2008 电工电子产品环境试验 第2部分:试验方法 试验 Fc:振动(正弦)
- GB/T 2423.21—1991 电工电子产品基本环境 试验规程:试验 M:低气压试验方法
- GB/T 2423.22—2002 电工电子产品环境试验 第2部分:试验方法 N:温度变化
- GB/T 2423.53—2005 电工电子产品环境试验 第2部分:试验方法 试验 Xb 由手的摩擦造成
标记和印刷文字的磨损
- GB/T 4208—2008 外壳防护等级(IP 代码)
- GB/T 17626.2—2006 电磁兼容试验和测量技术 静电放电抗扰度试验
- GB/T 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般
模型
- GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能
要求
- GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证
要求
- GB/T 21079.1—2007 银行业务 安全加密设备(零售) 第1部分 概念、要求和评估方法
- GM/T 0002—2012 SM4 分组密码算法
- GM/T 0004—2012 SM3 密码杂凑算法
- GM/T 0005—2012 随机数检测规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

动态令牌 dynamic password token; one time password token

生成并显示动态口令的载体。