ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38556—2020

信息安全技术
动态口令密码应用技术规范

Information security technology—Technical specifications for one-time-password cryptographic application

2020-03-06 发布　　2020-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)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、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、紫光同芯微电子有限公司、上海林果实业股份有限公司北京科技分公司、格尔软件股份有限公司。

本标准主要起草人:谈剑锋、尤磊、李坤、柳逊、郑强、朱鹏飞、田敏求、吕春梅、郭思健、陈岩、李阗、周学庆、王凤珍。

信息安全技术
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技术框架，动态口令生成算法、鉴别和密钥管理等的相关内容。

本标准适用于动态口令相关产品的研制、生产、应用，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 2423.3—2016 环境试验 第2部分：试验方法 试验Cab：恒定湿热试验

GB/T 2423.7—2018 环境试验 第2部分：试验方法 试验Ec：粗率操作造成的冲击(主要用于设备型样品)

GB/T 2423.10—2019 环境试验 第2部分：试验方法 试验Fc：振动(正弦)

GB/T 2423.21—2008 电工电子产品环境试验 第2部分：试验方法 试验M：低气压

GB/T 2423.22—2012 环境试验 第2部分：试验方法 试验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—2017 外壳防护等级(IP代码)

GB/T 17626.2—2018 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 18336.1 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 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能组件

GB/T 18336.3 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保障组件

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

动态口令 one-time-password；dynamic password

由种子密钥与其他数据，通过特定算法，运算生成的一次性口令。