



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	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号	2
5 技术框架	3
5.1 总体框架	3
5.2 系统组成	4
6 动态口令生成	5
6.1 口令生成方式	5
6.2 算法使用说明	6
7 鉴别	7
7.1 鉴别模块说明	7
7.2 鉴别模块服务	8
7.3 鉴别模块管理功能	10
7.4 安全要求	10
8 密钥管理	11
8.1 概述	11
8.2 模块架构	11
8.3 功能要求	13
8.4 系统安全性设计	14
8.5 硬件密码设备接口说明	17
附录 A (规范性附录) 硬件动态令牌要求	19
附录 B (资料性附录) 动态口令鉴别原理	21
附录 C (资料性附录) 鉴别模块接口	22
附录 D (规范性附录) 运算参数与数据说明用例	27
附录 E (资料性附录) 动态口令生成算法 C 语言实现用例	28
附录 F (规范性附录) 动态口令生成算法计算输入输出用例	40