ICS 35.040
L 80
备案号：

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

（报批稿）

2018-05-02 发布　　2018-05-02 实施

国家密码管理局 发布

目　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语与定义 1
4　符号和缩略语 3
5　检测内容及检测方法 3
5.1　动态口令生成算法 3
5.1.1　分组密码算法生成 3
5.1.2　杂凑密码算法生成 4
5.2　动态令牌检测 4
5.2.1　PIN 码机制检测 4
5.2.2　令牌功能检测 6
5.2.3　令牌生命周期评估 9
5.2.4　硬件动态令牌特性检测 10
5.3　动态令牌认证系统 12
5.3.1　动态口令认证 12
5.3.2　生成挑战码 12
5.3.3　挑战应答认证 12
5.3.4　生成激活码 13
5.3.5　认证系统管理功能 13
5.3.6　系统安全性 13
5.3.7　生命周期 13
5.3.8　性能检测 13
5.4　密钥管理系统 13
5.4.1　密钥管理系统合规性检测 13
5.4.2　系统登录 14
5.4.3　用户管理 14
5.4.4　保护密钥生成 14
5.4.5　序列号生成 15
5.4.6　种子密钥生成 15
5.4.7　令牌生产配置 15
5.4.8　系统时间同步 15
5.4.9　日志管理 16
5.4.10 接口检测 16
5.4.11 性能检测 16
6　送检技术文档要求 16

前　言

本标准依据 GB/T1.1—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，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。

GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907-2016 信息安全技术 SM4 分组密码算法

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、GM/Z 4001 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。

3.8

挂起 hung up

令牌被人为挂起后，处于挂起状态。

3.9

作废 invalidate

令牌执行作废操作后，进入作废状态。

3.10

自动解锁 automatically unlock

令牌被锁定以后，经过一定时间，令牌会自动解除锁定状态。

3.11

服务报表 service list

系统提供的，对于令牌和系统不同时间段对应的状态和结果的统计报表。

3.12

固件 firmware

固化在集成电路内部的程序代码，负责控制和协调集成电路的功能。

3.13

大窗口 large window

用于令牌时间与系统时间同步的窗口，窗口大小不应超过±10 分钟。

3.14

中窗口 middle window

用于令牌时间与系统时间同步的窗口，窗口大小不应超过±5 分钟。

3.15

小窗口 small window

用于令牌时间与系统时间同步的窗口，窗口大小不应超过±2 分钟。

3.16

主密钥 main key

某个动态口令系统的根密钥，用于分散产生厂商生产主密钥。

3.17

种子密钥加密密钥 encryption key for seed key

用于对种子密钥进行加密的密钥。

3.18

厂商生产主密钥 main key for manufacturer production

用于产生种子密钥加密密钥，由主密钥通过厂商代码密钥分散产生。

3.19

传输密钥 transmit key

用于加密保护厂商生产主密钥，保障其传输过程的安全。

4 符号和缩略语

下列符号适用于本文件。

key 长度不少于128比特的种子密钥

Km 主密钥

Kp 厂商生产主密钥

Ks 种子密钥加密密钥

Kt 传输密钥

mAh 毫安时（milliampere hour），电池电量单位

N 自然数

PIN 个人识别密码（Personal Identification Number），指用于使令牌工作并显示动态口令的一种口令，是一个6～16位长度的十进制数

PUK 解锁码（PIN Unlocking Key），用于解锁锁定PIN码状态

T 参与运算的时间因子

TPS 认证系统每秒处理能力单位（Transaction Per Second）

UTC 协调世界时（Universal Time Coordinated），是距1970年1月1日00:00时(格林尼治标准时间)的秒数

5 检测内容及检测方法

5.1 动态口令生成算法

5.1.1 分组密码算法生成

检测目的：

用分组密码算法SM4生成动态口令算法正确实现。

检测方法和流程：

a） 执行采用对称密码算法的运算指令，采用指定密钥进行运算；

b） 通过数据采集，还原运算的原始明文数据和密文结果；

c） 使用密码检测机构算法一致性工具软件对数据进行验证。

合格性判定条件：

a） 使用SM4算法；

b） 通过算法一致性的检测。

5.1.2 杂凑密码算法生成

检测目的：

选用杂凑算法 SM3 生成动态口令算法正确实现。

检测方法和流程：

a） 执行采用杂凑密码算法的运算指令，采用指定密钥进行运算；

b） 通过数据采集，还原运算的原始明文数据和密文结果；

c） 使用密码检测机构算法一致性工具软件对数据进行验证。

合格性判定条件：

a）使用 SM3 算法；

b）通过算法一致性的检测。

5.2 动态令牌检测

5.2.1 PIN 码机制检测

5.2.1.1 PIN 码保护

检测目的：

检测具有数字和功能按键的激活后的成品令牌 PIN 码保护功能，保证令牌不被他人非法使用。

检测条件：

激活后的成品令牌。

检测方法和流程：

a） 激活后的令牌应设置 6 至 16 位开机 PIN 码才能使用，如不设置开机 PIN 码则不能使用；

b） 令牌设置 PIN 码后，关机重新开机，应输入正确的开机 PIN 码才能使用令牌，如输入错误开机 PIN 码，则令牌不能使用，且记录错误次数；

c） 输入的 PIN 码有长度限制。

d） PIN 码具有超时自动关闭，在输入正确 PIN 码开机后，一段时间内（如 3 分钟）无操作令牌自动关闭，以防止被非法使用。

合格性判定条件：

a） 令牌应设置 6 至 16 位开机 PIN 码才能使用，当输入长度达到 16 位时不能继续输入；

b） 应输入正确的开机 PIN 码才能使用令牌；

c） 在输入正确 PIN 码开机后，一段时间内（如 3 分钟）无操作令牌自动关闭。

5.2.1.2 PIN 码锁定和永久锁定

检测目的：

a） 检测令牌 PIN 码锁定功能，当连续输入错误 PIN 码次数达到设定错误次数上限（如 6 次），令牌锁定，应解锁后才允许使用，防止他人恶意穷举尝试开机 PIN 码。

b） 当 PIN 码锁定次数达到设定错误次数上限（如 6 次），令牌永久锁定。

检测条件：

已设定开机 PIN 码的成品令牌。

检测方法和流程：

a） 输入错误开机 PIN 码，令牌应显示剩余尝试次数或已输入错误开机 PIN 码次数；

b） 连续输入小于设定错误次数上限（如 3 次）错误开机 PIN 码，再输入正确开机 PIN 码，开机 PIN 码错误次数应该清零。关机后再输入错误开机 PIN 码，显示的剩余尝试次数或已输入错误开机 PIN 码次数会重新开始计算；

c） 连续输入错误 PIN 码次数达到设定错误次数上限（如 6 次），令牌锁定，应解锁后才允许

使用。

d) 令牌第 6 次锁定后，被永久锁定，无法再次解锁使用。

合格性判定条件：

a) 输入错误开机 PIN 码，令牌显示剩余尝试次数或已输入错误开机 PIN 码次数；

b) 连续输入小于设定错误次数上限错误开机 PIN 码，再输入正确开机 PIN 码，开机 PIN 码错误次数清零。关机后再输入错误开机 PIN 码，显示的剩余尝试次数或已输入错误开机 PIN 码次数会重新开始计算；

c) 连续输入错误 PIN 码次数达到设定错误次数上限（如 6 次），令牌锁定。

d) 令牌锁定后通过解锁可以再次使用。

e) 令牌第 6 次锁定后，被永久锁定，无法再次解锁使用。

5.2.1.3 PIN 码解锁

检测目的：

检测令牌 PIN 码锁定后的解锁功能，防止用户不慎将令牌锁死，影响使用。

检测条件：

已设定开机 PIN 码的成品令牌，令牌锁定。

检测方法和流程：

a） 自动解锁：

1）到达设定自动解锁时间，令牌自动解锁，原 PIN 码保持不变，允许用户再次尝试输入 PIN 码；

2） 自动解锁到达设定上限后，令牌关闭 PIN 码自动解锁功能，只能通过手动解锁功能解锁令牌。

b） 手动解锁：

1） 令牌锁定后未达到自动解锁时间，可通过手动解锁功能解锁令牌；

2） 自动解锁到达设定上限后，令牌关闭 PIN 码自动解锁功能，可通过手动解锁功能解锁令牌；

3） 手动解锁后，需要重新设定开机密码，且自动解锁次数清零。

合格性判定条件：

PIN 码在锁定的条件下可以完成自动解锁和手动解锁。

5.2.1.4 PUK 码锁定

检测目的：

检测令牌 PUK 码输入错误后，PUK 码锁定功能。防止恶意穷举 PUK 码，非法解锁令牌。

检测条件：

已锁定开机 PIN 码的成品令牌。

检测方法和流程：

a) 连续输入错误 PUK 码次数达到设定错误次数上限（如 3 次），令牌一段时间内（如 10 分钟）不允许再次输入 PUK 码；

b) 到达 PUK 码锁定时间后（如 10 分钟），允许再次尝试 PUK 码输入。

c） 输入的 PUK 码有长度限制。

合格性判定条件：

当输入长度达到 16 位时不能继续输入。连续输入错误 PUK 码次数达到设定错误次数上限，令牌一段时间内不允许再次输入 PUK 码，PUK 码锁定自动解除后可继续尝试。

5.2.1.5 PIN码修改

检测目的：

检测令牌PIN码修改功能，保证令牌PIN码安全性。

检测条件：

已设定开机PIN码的成品令牌。

检测方法和流程：

a) 令牌开机，输入正确的开机PIN码，进入正常工作状态；

b) 按修改PIN码按键或组合键，进入PIN码修改状态。

c) 输入两次不同的新开机PIN码，修改开机PIN码失败，可重新输入；

d) 连续输入两次相同的新开机PIN码，修改开机PIN码成功。

合格性判定条件：

重新开机，输入原开机PIN码，验证不通过，输入修改后的新PIN码，验证通过。

5.2.1.6 PIN码修改保护

检测目的：

检测令牌PIN码修改保护功能，防止非法修改PIN码。

检测条件：

已设定开机PIN码的成品令牌。

检测方法和流程：

a) 令牌开机，输入正确的开机PIN码，进入正常工作状态；

b) 按修改PIN码按键或组合键，进入PIN码修改状态；

c) 在修改PIN码前，应输入原开机PIN码，防止意外修改PIN码。

合格性判定条件：

a) 在修改PIN码前，输入原开机PIN码才能进入正常工作状态。

b) 修改PIN码必须输入正确原PIN码,令牌修改PIN码后可以用新PIN码进入正常工作状态，原PIN码无法使用。

5.2.1.7 远程解PIN

检测目的：

检测远程解锁已锁定令牌功能。

检测条件：

已锁定开机PIN码、具备远程解PIN功能的成品令牌。

检测方法和流程：

a) 操作认证系统并产生解锁码PUK；

b) 将认证服务器产生的解锁码输入令牌，检测是否成功解锁。

合格性判定条件：

正确解锁码解锁成功，结果见5.2.1.3；错误解锁码解锁失败；超尝试次数解锁暂时锁定，结果见5.2.1.4。

5.2.2 令牌功能检测

5.2.2.1 激活功能

检测目的：

检测令牌激活功能，保证令牌能够正常激活并变换密钥。

检测条件：

未激活的成品令牌。

检测方法和流程：

a) 输入错误的激活码，令牌提示激活失败，并可重新尝试；

b) 输入正确的激活码，令牌激活成功。

合格性判定条件：

输入错误的激活码，令牌激活失败；输入正确的激活码，令牌激活成功。

5.2.2.2 开机 PIN 码

见 5.2.1.1。

5.2.2.3 时间口令认证

检测目的：

检测令牌时间口令是否正确。

检测条件：

已激活成品令牌。

检测方法和流程：

a) 操作令牌，产生时间型动态口令；

b) 将令牌产生的时间型动态口令输入认证服务器，检测是否通过认证。

合格性判定条件：

令牌成功通过认证。

5.2.2.4 挑战口令认证

检测目的：

检测令牌挑战口令是否正确。

检测条件：

已激活成品令牌。

检测方法和流程：

a) 操作令牌，输入认证服务器提供的挑战值，并产生挑战型动态口令；

b) 将令牌产生的挑战型动态口令输入认证服务器，检测是否通过认证。

合格性判定条件：

令牌成功通过认证。

5.2.2.5 其他参数口令认证

检测目的：

如令牌存在其他参与运算的因子（如：事件信息等），检测其口令是否正确。

检测条件：

已激活成品令牌。

检测方法和流程：

a) 操作令牌，并产生动态口令；

b) 将令牌产生的动态口令输入认证服务器，检测是否通过认证。

合格性判定条件：

令牌成功通过认证。

5.2.2.6 锁定、解锁

见 5.2.1.2、5.2.1.3、5.2.1.4。

5.2.2.7 修改开机密码

见 5.2.1.5、5.2.1.6。

5.2.2.8 令牌的同步

检测目的：

检测令牌认证系统动态同步计算是否正确。检测分为超小窗口未超中窗口、超中窗口未超大窗口两种情况。

检测条件：

已激活成品令牌、已登录认证系统。

检测方法和流程：

a) 操作令牌或软件模拟计算并产生两次连续动态口令；
b) 延时（或提前）小窗口至中窗口内时间，将产生的动态口令输入认证服务器，检测是否同步认证成功。
c) 操作令牌或软件模拟计算并产生两次连续动态口令；
d) 延时（或提前）中窗口至大窗口内时间，更高权限授权后，将产生的动态口令输入认证服务器，检测是否同步认证成功。

合格性判定条件：

令牌同步成功。

5.2.2.9 令牌状态

检测目的：

检测令牌认证系统中令牌状态变更是否正确。令牌工作状态分为：激活、锁定/解锁、挂起/解挂、废止状态，在认证系统中触发令牌状态变更为以上状态进行检测。

检测条件：

成品令牌。

检测方法和流程：

a) 操作认证系统界面，对未激活的令牌通过输入令牌的正确动态口令，验证动态口令成功后，令牌状态变更为就绪可用状态；
b) 通过认证系统的锁定服务设置就绪状态的令牌为锁定状态，锁定状态的令牌正确动态口令认证失败；
c) 通过认证系统的解锁服务将被锁定的令牌恢复为就绪状态，解锁需验证正确动态口令；
d) 通过认证系统的挂起服务设置就绪或锁定状态的令牌为挂起状态，挂起状态的令牌正确动态口令认证失败；
e) 通过认证系统的解挂服务将被挂起的令牌恢复为就绪状态，解挂需验证正确动态口令；
f) 通过认证系统的废止服务将被锁定、被挂起的令牌设置为废止状态，正确动态口令认证失败。

合格性判定条件：

令牌状态变更正确。

5.2.2.10 令牌系统数据

检测目的：

检测令牌认证系统的令牌系统数据是否正确。令牌系统数据为：序列号、密钥数据、令牌状态、上次使用时间、连续错误次数、令牌偏移量、其他配置参数等。

检测条件：

成品令牌。

检测方法和流程：

a) 操作认证系统查询令牌序列号；
b) 操作认证系统通过令牌序列号查询令牌种子密钥数据，种子密钥为加密数据；
c) 操作认证系统通过令牌序列号查询令牌状态；
d) 操作认证系统通过令牌序列号查询令牌上次使用时间；
e) 操作认证系统通过令牌序列号查询令牌连续错误次数；
f) 操作认证系统通过令牌序列号查询令牌当前时间偏移量。

合格性判定条件：

令牌系统数据正确。

5.2.3 令牌生命周期评估

5.2.3.1 种子密钥生成及管理周期

种子密钥由获得国家密码管理主管部门批准的硬件密码设备生成。

种子密钥为令牌重要安全要素，应保证种子密钥从生成、传输、加载入令牌、认证过程中安全使用直到废止、销毁的整个过程都有安全防护措施。

5.2.3.2 种子密钥传输安全

种子密钥的传输应采用安全方式传输。

5.2.3.3 种子密钥加载安全

种子密钥加载进入动态令牌时，该过程应在安全的环境中进行，具有安全的管理机制。

安全的生产环境，是指用于安装密钥管理系统的电脑应位于具有安全防护机制，能够保障密钥加载全过程安全保密的环境。

安全的管理机制，是指在生产过程中的安全管理措施。

5.2.3.4 种子密钥生命周期管理

令牌内部种子密钥生命周期管理见表 1：

表 1 内部种子密钥生命周期管理

生命周期	描述	说明
加载	种子密钥加载至动态令牌内。	种子密钥写入动态令牌的过程应在安全的生产环境中进行，具有安全的管理机制。种子密钥在写入令牌时应保证其写入线路的安全性。
存储	种子密钥在动态令牌内部的存储管理。	种子密钥写入动态令牌后应能够正确、有效地存储在安全存储区域内。 动态令牌内种子密钥可加密存储。
传输	种子密钥在动态令牌内部传输的管理。	动态令牌能够根据需要正确、有效在令牌内部传输种子密钥以供使用。

使用	种子密钥在动态令牌内部使用的管理。	动态令牌能够根据种子密钥的类型和使用场合等情况正确、有效的使用种子密钥。 动态令牌在密钥使用过程中，进行物理、逻辑隔离，要有措施防止非法设备接入。
废止	种子密钥在动态令牌内的销毁、删除。	动态令牌能够根据需要正确、有效地销毁、删除种子密钥。

5.2.3.5 令牌生命周期管理

令牌的生命周期管理见表 2：

表 2 令牌生命周期管理

生命周期	描述	检测方法
生产制造阶段	令牌制造，固件加载。	令牌制造阶段，不能提供正常的口令认证。
未激活阶段	令牌出厂时的状态，须激活后令牌才能进入就绪状态。	未激活令牌不能提供正常的口令认证。
使用阶段	令牌正常工作就绪状态	在使用阶段，令牌已激活，可用于口令认证。
锁定阶段	令牌因连续错误、重放攻击、人工方式等原因被锁定后处于锁定状态。	锁定状态的令牌不能提供正常的口令认证。
废止阶段	令牌损坏或失效，进入作废状态。	废止阶段，令牌不能提供正常的口令认证。可使用认证系统的废止服务将其废止。废止的令牌不可再用于用户的身份认证和交易验证。

5.2.4 硬件动态令牌特性检测

5.2.4.1 安全芯片合规性检测

硬件动态令牌涉及的处理器芯片，应是国家密码管理局批准产品型号证书的安全芯片。

5.2.4.2 令牌运算性能检测

检测目的：

检测令牌运算性能。

检测条件：

引出电源正负极的成品令牌。

检测方法和流程：

a） 将令牌通过电流表连接产品额定电源，写入种子密钥，并激活；

b） 检测令牌运算时间（高电流持续时间）。

合格性判定条件：

令牌口令生成的运算时间应小于 300ms。

5.2.4.3 令牌各状态功耗检测

检测目的：

检测令牌各状态功耗，保证令牌能够达到设计使用年限。

检测条件：

引出电源正负极的成品令牌。

使用场景：由于令牌库存功耗必然小于使用功耗，自出厂后至电池电量耗尽不少于 3 年计算最大功耗。假设令牌出厂后即使用，在 3 年里平均每天使用 10 次，每次操作 3 分钟，每次使用按键次数 30 次，每次按键 0.5s，每次使用运算 5 次密码，每次运算持续时间 0.3 秒(运算时间不得超过 0.3 秒)。电池容量有效系数 0.8。

检测方法和流程：

a） 将令牌接入额定电源，写入种子密钥，并激活；

b） 检测令牌各状态功耗，具体见表 3：

表 3 令牌各状态功耗

工作状态	检测值（uA）
运算状态工作电流	
待机状态工作电流	
按键状态工作电流	
显示状态工作电流	

合格性判定条件：

通过下面的运算公式计算，自出厂后至电池电量耗尽应不少于 3 年。

令牌使用年限 = (电池容量 mAh*1000*电池容量有效系数*3600)/(运算状态电流 uA*运算持续秒数*50+待机电流 uA*86400+按键电流 uA*150+显示电流 uA*3000)/365。

5.2.4.4 令牌开启所有安全功能时各状态功耗

检测目的：

检测令牌在开启各安全功能时各状态的功耗。

检测条件：

引出电源正负极的成品令牌。

检测方法和流程：

a） 将令牌接入额定电源，写入种子密钥，并激活；

b） 按照表 4 依次开启令牌具有的安全功能；

c） 检测令牌各状态功耗，具体见表 4：

表 4 令牌开启安全功能时各状态功耗

工作状态	检测值（uA）					
	无安全功能开启	自毁防护开启	计时攻击防护开启	能量攻击防护开启	故障攻击防护开启	所有安全功能开启
运算状态电流(uA)						
待机状态电流(uA)						

5.2.4.5 令牌硬件其他特性检测

按照 GM/T 0021-2012 第 7 章中所描述的动态令牌硬件要求实施检测，或提供有相关资质的第三方检测机构的检测报告。

5.3 动态令牌认证系统

5.3.1 动态口令认证

检测目的：

检测令牌认证系统动态口令计算是否正确。包括：静态口令+动态口令、动态口令。检测过程中需要进行正确口令检测、错误口令检测、窗口偏移量调整检测、重复正确口令检测、超小窗口正确口令检测、窗口内输入错误超过最大次数的情况检测。

检测条件：

已激活成品令牌或软件模拟、已登录认证系统。

检测方法和流程：

a) 操作令牌或软件模拟计算并产生动态口令（包括正确口令、错误口令、重复正确口令、超小窗口正确口令、有效窗口偏移量内正确口令、窗口内输入错误超过最大次数的情况检测）；

b) 将令牌产生的动态口令输入认证服务器，检测是否得到相应检测结果。

合格性判定条件：

正确口令成功认证、错误口令失败认证、重复正确口令失败认证、超小窗口正确口令失败认证、有效窗口偏移量内成功认证并进行窗口偏移量调整、窗口内输入错误超过最大次数口令失败认证。

5.3.2 生成挑战码

检测目的：

检测令牌认证系统挑战码产生是否正确。

检测条件：

已登录认证系统。

检测方法和流程：

a) 挑战码产生参数检查（格式类型和长度设置）

b) 操作认证系统产生挑战码；

c) 检查挑战码格式。

合格性判定条件：

挑战码参数设置正确，挑战码产生成功。

5.3.3 挑战应答认证

检测目的：

检测令牌认证系统动态口令计算是否正确。包括：正确口令检测、错误口令检测、重复正确口令检测、窗口偏移量调整检测、超小窗口正确口令检测、窗口内输入错误超过最大次数的情况检测。

检测条件：

已激活成品令牌或软件模拟、已登录认证系统。

检测方法和流程：

a) 操作令牌或软件模拟计算并产生动态口令（包括正确口令、错误口令、重复正确口令、超小窗口正确口令、有效窗口偏移量内正确口令、窗口内输入错误超过最大次数的情况检测）；

b) 将令牌产生的动态口令输入认证服务器，检测是否得到相应检测结果。

合格性判定条件：

正确口令成功认证、错误口令失败认证、重复正确口令失败认证、超小窗口正确口令失败认证、

有效窗口偏移量内成功认证并进行窗口偏移量调整、窗口内输入错误超过最大次数口令失败认证。

5.3.4 生成激活码

检测目的：

检测令牌认证系统激活码计算是否正确。包括：正确激活码和错误激活码检测。

检测条件：

未激活成品令牌、已登录认证系统。

检测方法和流程：

a) 操作认证系统产生激活码（正确激活码和错误激活码）；

b) 激活码输入令牌，检测是否正确激活。

合格性判定条件：

错误激活码激活失败，正确激活码激活成功。

5.3.5 认证系统管理功能

动态令牌认证系统管理功能符合 GM/T 0021-2012 第 8 章中描述的安全要求，通过操作界面检测实现。检测包括：权限管理、参数配置、日志管理、服务报表和种子导入。

5.3.6 系统安全性

系统本身的安全性符合 GM/T 0021-2012 第 8 章中描述的安全要求。动态令牌系统安全功能检测包括：接入端控制、通讯敏感字段加密、信息存储加密、日志安全、时间校准等，按照 GM/T 0021-2012 第 8.4 章中定义的安全要求，验证认证系统的安全性。

5.3.7 生命周期

认证系统须定义认证系统和令牌产品的生命周期模型，并对生命周期各阶段进行标识。

5.3.8 性能检测

认证系统的性能检测通过标准压力检测模型来实现，数据用来评估认证系统的性能，作为检测报告的参考数据。

标准压力检测模型定义：认证系统中存储一百万条令牌数据，令牌全部处于就绪状态，模拟客户端发起并发认证请求，模拟客户端并发数量可以选择：100、200、500、1000 四种情况进行检测。统计认证处理成功交易数量，除以总完成时间，得到认证系统每秒处理能力 TPS。以 TPS（100）=、TPS（200）=、TPS（500）=和 TPS（1000）=表示认证系统的并发能力。

5.4 密钥管理系统

5.4.1 密钥管理系统合规性检测

检测目的：

检测密钥管理系统的设计是否满足基本合规性要求。

检测条件：

密钥管理系统存在。密钥管理系统与动态令牌、认证系统可以是独立的，分别进行检测。

检测方法和流程：

a) 主密钥采用国家密码管理局批准的硬件密码设备生成、存储，无法导出。

b) 所有密钥的分散运算都在硬件密码设备中完成。

c) 种子密钥加密密钥由主密钥对令牌序号分散得到。

d) 厂商生产主密钥由主密钥对厂商代码分散得到。

合格性判定条件：

密钥管理系统满足 a)、b) 、c) 、d)要求。

5.4.2 系统登录

检测目的：

检测密钥管理系统用户登录是否正确。

检测条件：

未登录密钥管理系统。

检测方法和流程：

a) 操作密钥管理系统输入错误的用户名和随机的登录口令,登录口令非明文显示,登录失败；

b) 操作密钥管理系统输入正确的用户名和随机的登录口令,登录口令非明文显示,登录失败；

c) 操作密钥管理系统输入正确的用户名和正确的登录口令,登录口令非明文显示,登录成功；

d) 操作密钥管理系统连续输入正确的用户名和随机的登录口令，登录口令非明文显示，连续输入次数超密钥管理系统设置时登录锁定。

合格性判定条件：

用户可采用正确的用户名和口令登录。

5.4.3 用户管理

检测目的：

检测令牌密钥管理系统用户管理是否正确。

检测条件：

未登录密钥管理系统。

检测方法和流程：

a) 操作密钥管理系统输入正确的超级用户名和正确的登录口令，登录口令非明文显示，登录成功；

b) 操作密钥管理系统增加普通操作用户；

c) 操作密钥管理系统查询普通操作用户；

d) 操作密钥管理系统修改普通操作用户；

e) 操作密钥管理系统删除普通操作用户；

f) 超级用户退出登录；

g) 操作密钥管理系统输入正确的普通用户名和正确的登录口令，登录口令非明文显示，登录成功，不能对超级用户和其他普通用户进行管理。

合格性判定条件：

只有超级用户才能对普通操作用户进行操作。

5.4.4 保护密钥生成

检测目的：

检测令牌密钥管理系统保护密钥生成模块是否正确。

检测条件：

已登录密钥管理系统。

检测方法和流程：

a) 密钥管理系统连接密码模块设备。

b) 密钥管理系统生成密钥管理系统的根密钥；

c) 密钥管理系统生成密钥管理系统的传输密钥。

合格性判定条件：

密钥生成成功。

5.4.5 序列号生成

检测目的：

检测令牌密钥管理系统令牌序列号生成模块是否正确。

检测条件：

已登录密钥管理系统。

检测方法和流程：

a) 操作密钥管理系统生成令牌序列号；

b) 检查序列号和生成规则的一致性；

c) 检查序列号在密钥管理系统中的唯一性。

合格性判定条件：

令牌唯一序列号生成成功。

5.4.6 种子密钥生成

检测目的：

检测令牌密钥管理系统种子密钥生成模块是否正确。

检测条件：

已登录密钥管理系统。

检测方法和流程：

a) 验证硬件密码设备被使用；

b) 操作密钥管理系统生成密钥管理系统的种子密钥；

c) 验证密钥管理系统中的种子密钥为加密存储；

d) 生成的加密种子密钥文件可以被认证系统使用。

合格性判定条件：

种子密钥生成正确。

5.4.7 令牌生产配置

检测目的：

检测令牌密钥管理系统生产配置是否正确。

检测条件：

未配置半成品令牌和已登录密钥管理系统。

检测方法和流程：

a) 环境要求和安全措施见 5.3.3；

b) 密钥管理系统时间已同步；

c) 令牌序列号、种子密钥和其他参数通过接口写入动态令牌；

d) 动态令牌口令验证比对一致。

合格性判定条件：

令牌生产配置成功。

5.4.8 系统时间同步

检测目的：

检测令牌认证系统动态同步计算是否正确。

检测条件：

已登录密钥管理系统。

检测方法和流程：

a) 操作密钥管理系统界面与标准时钟源进行时钟同步；

b) 验证密钥管理系统的时间已经同步成功。

合格性判定条件：

密钥管理系统时间同步成功。

5.4.9 日志管理

检测目的：

检测令密钥管理系统日志管理是否正确。

检测条件：

未登陆密钥管理系统。

检测方法和流程：

a) 以超级用户身份登陆密钥管理系统；

b) 查询系统日志，日志记录完整、准确，用户登录、操作、认证均应由日志记载；

c) 修改、删除日志不成功。

合格性判定条件：

超级用户可以查看日志不能修改删除。

5.4.10 接口检测

动态令牌密钥管理系统接口类型符合 GM/T 0021-2012 第 9 章中描述的要求，接口定义依据相应厂商接口文档。动态令牌读写接口应检查种子密钥单向写入、接口权限控制、写入验证机制和接口纠错能力。

5.4.11 性能检测

密钥管理系统的性能检测，主要通过标准压力检测模型来实现，数据用来评估密钥管理系统的性能。

标准压力检测模型定义：密钥管理系统生成一百万条令牌种子密钥数据的时间，统计生成成功种子密钥数量，除以总完成时间，得到密钥管理系统每秒处理能力 TPS，即密钥管理系统每秒处理能力。以 TPS（key）=表示密钥管理系统的性能能力。

6 送检技术文档要求

动态令牌相关产品的研制单位按照国家密码管理主管部门检测要求提交技术工作总结报告、安全性设计报告、用户手册及密码检测材料等相关文档，作为动态令牌及动态令牌认证系统、密钥管理系统的检测依据。文档内容应包括但不限于以下内容：

a) 产品硬件组成的逻辑框图、各个功能模块或部件的结构框图以及相互之间的关系图；

b) 产品软件各功能模块的逻辑框图、流程图，基本功能的源代码；

c) 产品软件架构图及电路设计原理图、清晰可辨的主要元器件或部件图；

d) 产品的主要功能原理以及组成部分工作原理说明；

e) 密钥管理，包括敏感数据的生成、分发、使用、存储、备份、更换、销毁等生命周期管理说明；

f) 针对通信保护、安全认证、密钥协商的密码协议的用途、目标、要素、流程数据结构说明；

g) 物理防护措施说明。