ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0021—2023
代替 GM/T 0021—2012

动态口令密码应用技术规范

Technical specifications for one-time-password cryptographic application

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GM/T 0021—2012《动态口令密码应用技术规范》，与 GM/T 0021—2012 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了种子密钥管理系统的兼容性要求（见 2012 年版的 9.3.2）；

b) 增加了规范性引用文件 GB/T 2423.3—2016（见 6.2.3.4）、GB/T 2423.7—2018（见 6.2.3.6）、GB/T 15852.1—2020（见 5.2.3）、GB/T 17901.1—2020（见 5.5.1）、GB/T 32905（见 5.2.4）、GB/T 32907（见 5.2.4）、GB/T 32915（见 5.5.2）、GB/T 39786（见 6.3.3）、GM/T 0008（见 6.2.1.1）、GM/T 0028（见 5.5.5）、GM/T 0039（见 7.2.2）、GM/T 0051—2016（见 5.5.3）、GM/T 0061—2018（见 7.2.1.1）、GM/T 0062—2018（见 7.3.1.1）以及 GM/Z 4001（见第 3 章），删除了规范性引用文件 GB/T 2423.8—1995（见 2012 年版的 7.1.6）、GB/T 2423.9—2001（见 2012 年版的 7.1.4）、GB/T 18336.1—2008（见 2012 年版的 7.2.5）、GB/T 18336.2—2008（见 2012 年版的 7.2.5）、GB/T 18336.3—2008（见 2012 年版的 7.2.5）、GB/T 21079.1—2007（见 2012 年版的 7.2.5）、GM/T 0002—2012（见 2012 年版的 6.2.1）、GM/T 0004—2012（见 2012 年版的 6.2.1）以及 GM/T 0005—2012（见 2012 年版的 6.2.1）；

c) 删除了术语“静态口令”（见 2012 年版的 3.3）、“大端”（见 2012 年版的 3.7）、“认证系统”（见 2012 年版的 3.8）、“未激活”（见 2012 年版的 3.9）、“就绪”（见 2012 年版的 3.10）、“锁定”（见 2012 年版的 3.11）、“挂起”（见 2012 年版的 3.12）、“作废”（见 2012 年版的 3.13）、“自动解锁”（见 2012 年版的 3.14）、“密钥管理”（见 2012 年版的 3.15）、“硬件密码设备”（见 2012 年版的 3.16）、“密钥”（见 2012 年版的 3.17）、“服务报表”（见 2012 年版的 3.18）、“接口”（见 2012 年版的 3.19）、“大窗口”（见 2012 年版的 3.20）、“中窗口”（见 2012 年版的 3.21）、“小窗口”（见 2012 年版的 3.22）、“种子密钥加密密钥”（见 2012 年版的 3.23）、“厂商生产主密钥”（见 2012 年版的 3.24）、“主密钥”（见 2012 年版的 3.25）、“厂商代码”（见 2012 年版的 3.26）以及“内部挑战认证”（见 2012 年版的 3.27），增加了术语“置零”（见 3.6）、“动态口令系统”（见 3.7）、“SM3 算法”（见 3.8）、“SM4 算法”（见 3.9）、“声称方”（见 3.10）、“验证方”（见 3.11）以及“密码设备”（见 3.12）；

d) 增加了缩略语（见 4.2）；

e) 增加了“密钥管理”对密钥管理相关各方的描述和要求（见 5.5）；

f) 删除了动态口令鉴别系统（服务）与密码应用无关的功能要求（见 2012 年版的 8.3）；

g) 删除了种子密钥管理系统与密钥管理无关的功能要求（见 2012 年版的 9.3.1）；

h) 增加了“动态口令系统检测方法”（见第 7 章）。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：飞天诚信科技股份有限公司、上海复旦微电子集团股份有限公司、北京集联网络技术有限公司、格尔软件股份有限公司、北京宏思电子技术有限责任公司、北京天融信网络安全技术有限公司、西安交大捷普网络科技有限公司、山东渔翁信息技术股份有限公司、上海华虹集成电路有限责

任公司、上海林果实业股份有限公司。

本文件主要起草人：朱鹏飞、刘雅静、柳逊、刘岸、郑强、张文婧、刘治平、何建锋、郭刚、吴震、杨剑、韩玉佳、郭思建、詹榜华、谈剑锋、尤磊、陈达、张志茂、李阗、牛毅。

本文件及其所代替文件的历次版本发布情况为：

——2012 年首次发布为 GM/T 0021—2012；

——本次为第一次修订。

动态口令密码应用技术规范

1 范围

本文件规定了动态口令的基本原理、动态口令系统的技术要求以及动态口令系统的检测方法。

本文件适用于动态口令相关产品的研制、生产、应用，也可用于动态口令系统以及相关产品的密码应用合规性检测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15852.1—2020 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制

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 17901.1—2020 信息技术 安全技术 密钥管理 第1部分：框架

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

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GM/T 0008 安全芯片密码检测准则

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

GM/T 0051—2016 密码设备管理 对称密钥管理技术规范

GM/T 0061—2018 动态口令密码应用检测规范

GM/T 0062—2018 密码产品随机数检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及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。

3.2

动态口令令牌 one-time-password token;dynamic token

生成并显示动态口令的载体。

[来源:GM/Z 4001—2013,2.16]

3.3

种子密钥 seed key

计算动态口令的密钥。

3.4

挑战码 challenge code

可参与到动态口令生成过程中的一种数据。

注:挑战码即挑战因子。

3.5

UTC 时间 Universal Time Coordinated

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(格林尼治标准时间)的秒数。

注:又称协调世界时。

3.6

置零 zeroziration

销毁存储数据和未受保护的敏感安全参数,以防止数据恢复的方法。

3.7

动态口令系统 one-time-password system

对动态口令进行鉴别、对动态口令令牌及种子密钥进行管理的系统。

[来源:GM/Z 4001—2013,2.17,有修改]

3.8

SM3 算法 SM3 algorithm

一种密码杂凑算法,其输出为 256 比特。

[来源:GM/Z 4001—2013,2.119]

3.9

SM4 算法 SM4 algorithm

一种分组密码算法,分组长度为 128 比特,密钥长度为 128 比特。

[来源:GM/Z 4001—2013,2.120]

3.10

声称方 claimant

被鉴别的实体本身或者为了实现验证目标的某代表性实体。

注:声称方拥有鉴别交换时所必需的参数和私有数据。

[来源:GB/T 15843.1—2017,3.6]

3.11

验证方 verifier

要求鉴别其他实体身份的实体本身或实体代表。

注:验证方拥有从事鉴别交换所必需的参数。

[来源:GB/T 15843.1—2017,3.40]

3.12

密码设备　cryptography device

为密钥等秘密信息提供安全存储，并基于这些秘密信息提供秘密安全服务的设备。

[来源：GM/T 0051—2016，3.2]

4　符号和缩略语

4.1　符号

下列符号适用于本文件。

‖：拼接。

%：求余。

⊞：算术加，且不进位。

4.2　缩略语

下列缩略语适用于本文件。

AAA：鉴别、授权与计费(Authentication Authorization Accounting)

PAM：可插拔鉴别模块(Pluggable Authentication Modules)

PIN：个人识别码(Personal Identification Number)

RADIUS：远程认证拨号用户服务(Remote Authentication Dial In User Service)

5　动态口令基本原理

5.1　概述

动态口令鉴别的基本原理是：声称方与验证方采用相同的运算方法，分别使用各自的种子密钥以及当前运算因子(动态因子)，生成一次性的口令，并进行比对，从而完成整个鉴别过程。如图1所示。

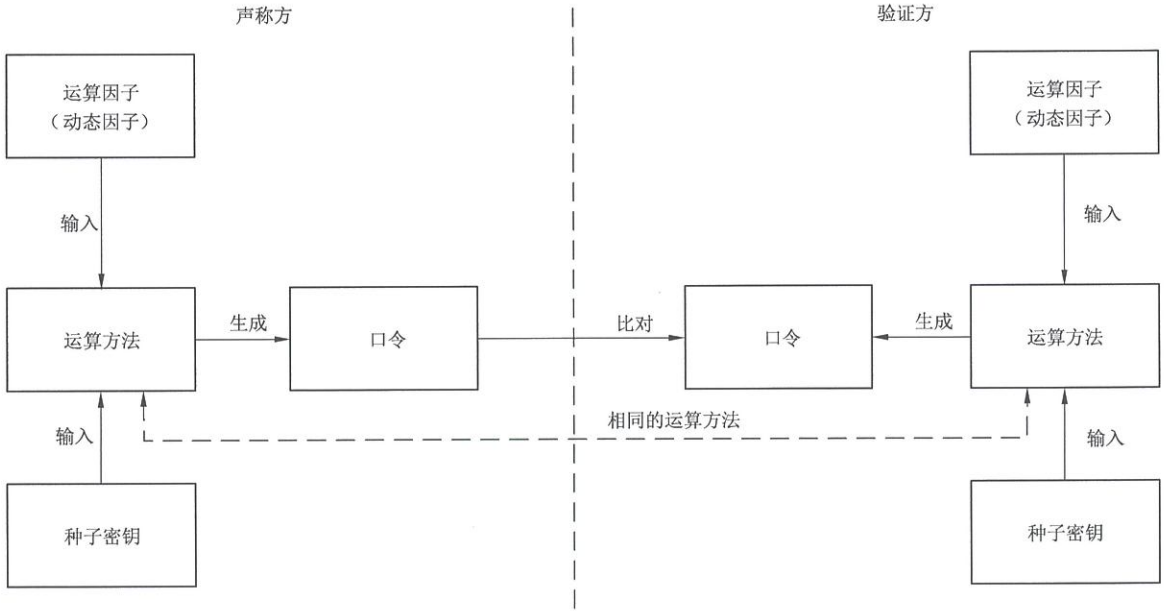

图1　动态口令基本原理

生成动态口令包括以下环节：

a） 计算运算因子；

b） 组装输入序列；

c） 计算一次性中间值；

d） 截位计算；

e） 计算动态口令。

其中，运算因子可包括以下一种或多种。

——时间因子：基于当前时间（例如 UTC 时间）计算而成（见 5.2.1）。

——事件因子：单向变化的计数值（例如每次生成动态口令递增一次）。

——挑战因子：由鉴别服务端生成的一次性字符串。

5.2 生成动态口令

5.2.1 计算时间因子

时间因子应按照公式（1）计算：

$$T = T_0 / T_c \quad \cdots\cdots (1)$$

式中：

T ——参与运算的时间因子，表示为一个 8 字节整数；

T_0 ——以 UTC 时间（或应用方选择的时间标准）为计量标准的当前时间，单位为秒（s）；

T_c ——口令变化周期，单位为秒（s）。

T_c 应不大于 60 s。宜选择 T_c=60 s 或 T_c=30 s。

5.2.2 组装输入序列

输入序列应按照公式（2）组装：

$$\mathrm{ID} = \{T \parallel C \parallel Q\} \quad \cdots\cdots (2)$$

式中：

ID ——杂凑密码算法或分组密码算法的输入序列；

T ——参与运算的时间因子（5.2.1 的计算结果）；

C ——参与运算的事件因子，表示为一个 4 字节整数；

Q ——鉴别双方通过协商输入的挑战因子（或其他类型参与运算的因子），使用 ASCII 码表示。

挑战因子应由可打印字符组成，应包括不少于 4 个字符。如包含英文字符，应区分大小写。不宜包含目视难以识别的字符（例如空格）或容易混淆的字符（例如数字 1 和字母 l、数字 0 和字母 O、字符’和字符 ’）。

输入序列的长度应不少于 128 比特，应至少包括 T、C 两个因子中的一个。Q 为可选参数。未包含的参数位置由后续参数补充。例如：

——输入序列由 T、Q 组成，则数据组装方式为 $T \parallel Q$；

——输入序列由 C、Q 组成，则数据组装方式为 $C \parallel Q$。

如组成输入序列的数据不足 128 比特，应在输入序列的数据末端填‘0’，至 128 比特。

5.2.3 计算一次性中间值

一次性中间值应按照公式（3）计算：

$$S = F(K, \mathrm{ID}) \quad \cdots\cdots (3)$$

式中：

K ——种子密钥；

ID ——输入序列(5.2.2 的组装结果)；

F ——算法函数；

S ——一次性中间值。

种子密钥的长度应不小于 128 比特。算法函数可使用 SM4 算法或 SM3 算法。一次性中间值的输出长度应为 128 比特(如果使用 SM4 算法)或 256 比特(如果使用 SM3 算法)。

使用 SM3 算法时，使用 $K \| ID$ 作为输入参数(如图 2 所示)。一次性中间值为使用 SM3 算法对 $K \| ID$ 计算得到的杂凑值。

图 2 使用 SM3 算法的计算过程

使用 SM4 算法时，K 为运算密钥，ID 为输入参数。运算过程如下。

a) 取 K 的前 128 比特数据(从高位记起)作为密钥参与运算。

b) 在 ID 末端填'0'，至 128 比特的整数倍长度(应符合 GB/T 15852.1—2020 中 6.3.2 的要求)，再将填充后的 ID 按 128 比特长度进行分组，高位在前，分别记作 ID_1、ID_2、ID_3……ID_m。

c) 将 ID_1 和 K 作为第一个分组运算的输入，通过 SM4 运算生成 S_1(应符合 GB/T 15852.1—2020 中 6.5.2 的要求)。将 S_1 与 ID_2 进行算术加运算(高位溢出舍去)，其结果与 K 一起用于第二个分组的输入，通过 SM4 运算生成 S_2。之后的运算以此类推。使用 SM4 算法的计算过程见图 3。

d) 将 S_m 作为一次性中间值输出(应符合 GB/T 15852.1—2020 中 6.8.2 的要求)。

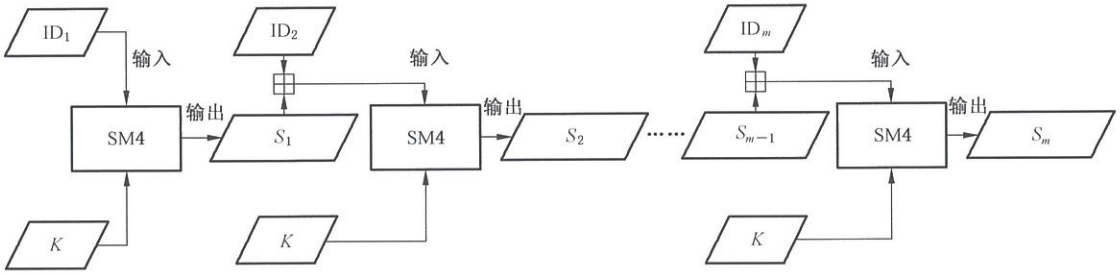

图 3 使用 SM4 算法的计算过程

5.2.4 截位计算

截位计算应按照公式(4)进行：

$$OD = Truncate(S) \quad \cdots\cdots(4)$$

式中：

OD ——截位函数的输出结果，OD 的长度应为 32 比特；

$Truncate()$——截位函数；

S ——一次性中间值(5.2.3 的输出)。

如选用 SM3 算法(应符合 GB/T 32905 的要求)作为算法函数，定义 $S1$、$S2$、$S3$、$S4$、$S5$、$S6$、$S7$、$S8$ 为 8 个 4 字节整数，通过公式(5)赋值：

$$S = S1 \| S2 \| S3 \| S4 \| S5 \| S6 \| S7 \| S8 \quad \cdots\cdots(5)$$

并使用公式(6)计算 OD：

$$OD=(S1+S2+S3+S4+S5+S6+S7+S8)\%2^{32} \quad \cdots\cdots(6)$$

如选用 SM4 算法(应符合 GB/T 32907 的要求)作为算法函数，截位计算应符合 GB/T 15852.1—2020 中 6.9.3 的要求。定义 $S1$、$S2$、$S3$、$S4$ 为 4 个 4 字节整数，通过公式(7)赋值：

$$S=S1\parallel S2\parallel S3\parallel S4 \quad \cdots\cdots(7)$$

并使用公式(8)计算 OD：

$$OD=(S1+S2+S3+S4)\%2^{32} \quad \cdots\cdots(8)$$

5.2.5 计算动态口令

动态口令应按照公式(9)计算：

$$P=OD\%10^{N} \quad \cdots\cdots(9)$$

式中：

P ——动态口令(通常显示为十进制数字)；

OD ——一次性中间值(5.2.4 的输出)；

N ——动态口令的位数。

动态口令的位数应不小于 6。

5.3 验证动态口令

声称方与验证方所使用的动态因子通常是同步变化的，但也有可能不同步(例如时间因子可能由于双方计时存在误差而不同步)。为了避免因为动态因子不同步而导致鉴别不通过，验证方可使用窗口机制：以当前动态因子为基准在一定范围(称作窗口)内浮动，得到一系列动态因子，分别生成若干动态口令，与声称方生成的动态口令分别进行比对。如果其中任意一个动态口令与声称方生成的动态口令一致，则鉴别通过。

如果使用时间因子，窗口大小应不超过±2 min。如果窗口中包含已经通过鉴别的动态口令对应的动态因子，则窗口应以该动态因子为界，不得包含已经通过鉴别的动态口令对应的动态因子及其之前的动态因子。因此：

——如果使用事件因子，应使用单向窗口(以当前动态因子为基准同向浮动)；

——如果使用挑战因子，应保证挑战码是一次性的(例如每次验证时生成新的挑战码，或每次验证后清除当前验证码)。

5.4 动态因子同步

为使声称方与验证方所使用的动态因子重新同步，可采用以下方式调整验证方所使用的动态因子当前值：以当前动态因子为基准在一定范围内浮动，得到一系列动态因子，分别生成若干动态口令，与客户端生成的连续多个(≥2 个)动态口令分别进行比对。如果存在多个动态口令均一致的情况，则将对应的动态因子最大值设为动态因子的当前值，或记录动态因子最大值与动态因子的当前值之间的偏移量，验证动态口令时在动态因子的当前值基础上增加偏移量作为基准。

时间因子同步所使用的浮动范围应为以下之一：

——大窗口：浮动范围不超过±10 min；

——中窗口：浮动范围不超过±5 min。

事件因子同步时，动态因子应使用单向窗口。

5.5 密钥管理

5.5.1 总体要求

密钥管理的对象是种子密钥。密钥管理涉及以下实体：

——生产方：生产动态口令产品（令牌、服务器等）；

——应用方：使用动态口令系统，使用、维护和管理种子密钥；

——制造方（可选）：受生产方委托制造动态口令令牌；

——建设方（可选）：受应用方委托部署动态口令系统；

——密钥管理中心：对种子密钥进行生命周期全过程管理。

密钥管理中心可设置在生产方或应用方，也可设置为独立第三方，但不应设置在制造方或建设方。密钥管理中心使用密码算法应符合密码国家标准、行业标准的相关要求，宜使用通过商用密码产品认证的密码设备提供的密码服务。

种子密钥的生命周期包括以下阶段：

——产生：种子密钥在密钥管理中心生成；

——待激活：种子密钥被安装到动态口令令牌及动态口令鉴别系统（服务）；

——可用（对应 GB/T 17901.1—2020 中 5.3.1 定义的“激活”状态）：种子密钥能够被正常使用；

——锁住（对应 GB/T 17901.1—2020 中 5.3.1 定义的“挂起”状态）：种子密钥暂停使用；

——丢弃：种子密钥脱离受控范围（例如动态口令令牌丢失）；

——过期：种子密钥的使用超过有效期，停止使用；

——销毁：种子密钥被置零。

种子密钥的有效期应不大于 5 年（60 个月）。

生命周期的各阶段逻辑关系如图 4 所示。

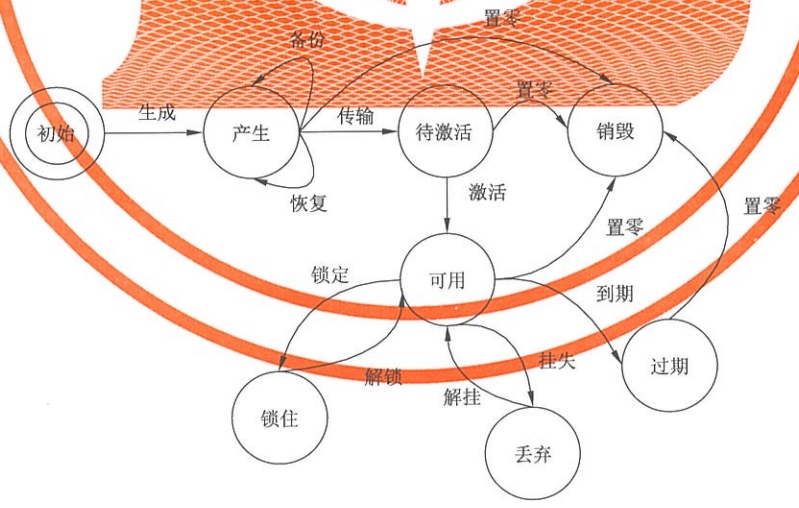

图 4 种子密钥生命周期

5.5.2 种子密钥生成

种子密钥的长度应不少于 128 比特。应使用随机数发生器生成种子密钥。随机数发生器应符合以下要求之一：

——是通过商用密码产品认证的密码产品；

——是通过商用密码产品认证的密码产品的组成部分，且该密码产品提供生成随机数服务；
——生成的随机数符合 GB/T 32915 要求。

5.5.3 种子密钥传输

种子密钥的传输包括：
——种子密钥在密钥管理中心的备份(归档)与恢复；
——种子密钥从密钥管理中心导出并传输到(一个或多个)生产方；
——种子密钥从生产方导出并传输到(一个或多个)制造方；
——种子密钥从(部署在制造方的)制造设备导入动态口令令牌；
——种子密钥从密钥管理中心导出并传输到应用方；
——种子密钥导入到部署在应用方的动态口令鉴别系统(由建设方操作)。

应使用密码技术保障种子密钥在各方之间传输的机密性和完整性。宜符合 GM/T 0051—2016 的要求。

导入硬件动态口令令牌的种子密钥不应从硬件动态口令令牌导出。

5.5.4 种子密钥存储

各方应采取有效的技术措施保证所存储种子密钥的机密性和完整性(见附录 A)。

种子密钥管理系统的种子密钥存储应使用以下方式之一：
——存储在密码设备内；
——加密后存储在密码设备以外的位置(例如数据库)，且加密所使用的密钥加密密钥存储在密码设备内。

5.5.5 种子密钥使用

生成动态口令可使用以下方式之一：
——种子密钥内置于通过商用密码产品认证、具有密码运算功能的密码产品(例如安全芯片、密码机、软件密码模块等)，使用密码产品进行生成动态口令所需的密码运算，基于密码运算结果生成动态口令；
——种子密钥内置于通过商用密码产品认证、具有生成动态口令功能的密码产品(例如动态口令令牌)，使用密码产品生成动态口令。

生成动态口令所使用的密码产品应符合 GM/T 0028 的要求。

注：使用 SM3 算法生成动态口令时，将种子密钥与动态因子拼接作为 SM3 算法的输入。这种方法不被密码机支持。

6 动态口令系统技术要求

6.1 系统组成

动态口令系统包括以下组成部分。
——动态口令令牌：生成动态口令。
——动态口令鉴别系统(服务)：验证动态口令，管理和维护种子密钥、动态因子等鉴别动态口令所需的信息，以及管理动态口令令牌等。此外还提供动态口令密码服务接口，从应用系统接收待鉴别的动态口令以及种子密钥索引(令牌序列号或用户标识)，以及发送鉴别结果。
——种子密钥管理系统：密钥管理中心的实现载体，生成和管理种子密钥。

动态口令系统组成框图如图 5 所示。

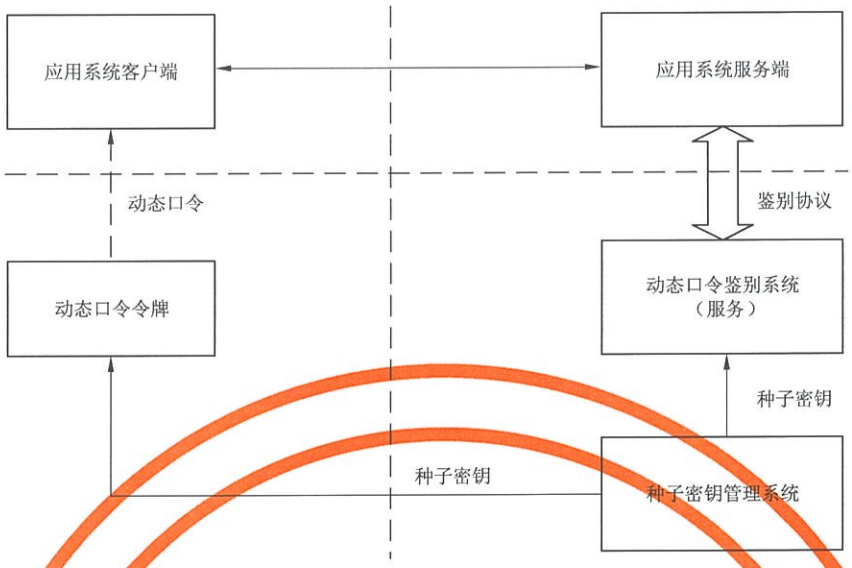

图 5　动态口令系统组成框图

6.2　动态口令令牌

6.2.1　密码服务功能要求

6.2.1.1　生成动态口令

生成动态口令的方法应符合 5.2 的要求。

注：GB/T 38556—2020 中的附录 D 提供了生成动态口令的实例。

支持时间因子的动态口令令牌，计时误差偏差应不大于 2 min/年。

生成动态口令所使用的密码产品应符合 5.5.5 的要求。

硬件动态口令令牌使用的安全芯片应符合以下条件之一：

——是通过商用密码产品认证的产品；

——符合 GM/T 0008 的要求。

6.2.1.2　用户鉴别、锁定与解锁

可支持用户鉴别功能（例如带有键盘，生成动态口令前输入 PIN）。如果用户鉴别连续多次不通过，动态口令令牌应锁定（种子密钥进入锁住状态，参见 5.5.1）。触发锁定的用户鉴别连续不通过次数应不大于 5 次。可支持解锁功能（例如一定时间后自动解锁）。如支持自动解锁，从锁定到解锁之间的间隔时间应不小于 1 h。

6.2.2　密码应用安全要求

动态口令令牌应符合 GM/T 0028 的要求。动态口令令牌的密码模块规格见附录 B。

动态口令令牌的有效期应与内置的种子密钥相同。如果内置的种子密钥过期，动态口令令牌宜失效。可通过更新种子密钥/重新安装种子密钥使动态口令令牌重新生效。应采取有效的技术措施保障更新种子密钥/重新安装种子密钥的安全性。

6.2.3 硬件动态口令令牌

6.2.3.1 高温

按照 GB/T 2423.2—2008 中试验方法 Bb 进行测试，严酷等级选择温度：+50 ℃，持续时间：2 h。测试结束后，硬件动态口令令牌应能正常使用。

6.2.3.2 低温

按照 GB/T 2423.1—2008 中试验方法 Ab 进行测试，严酷等级选择温度：−10 ℃，持续时间：2 h。测试结束后，硬件动态口令令牌应能正常使用。

6.2.3.3 高低温冲击

按照 GB/T 2423.22—2012 中试验方法 Na 进行测试，严酷等级选择高温温度：+50 ℃，低温温度：−10 ℃，暴露试验时间：10 min，转换时间：2 min～3 min，循环数：3 个。测试结束后，硬件动态口令令牌应能正常使用。

6.2.3.4 湿度

按照 GB/T 2423.3—2016 进行测试。严酷等级选择温度：30 ℃±2 ℃，相对湿度：93%±3%，试验时间：12 h。测试结束后，硬件动态口令令牌应能正常使用。

6.2.3.5 低气压

按照 GB/T 2423.21—2008 进行测试，严酷等级选择气压：55 kPa，持续时间：2 h。测试结束后，硬件动态口令令牌应能正常使用。

6.2.3.6 跌落

按照 GB/T 2423.7—2018 中的“自由跌落——方法 1”进行测试，严酷等级选择跌落高度：1 000 mm。测试结束后，硬件动态口令令牌应能正常使用。

6.2.3.7 防尘防水

应符合 GB/T 4208—2017 中 IP44 的要求。

6.2.3.8 标记和印刷

按照 GB/T 2423.53—2005 进行测试，试验液体：人工合成汗液，力的大小：1 N±0.2 N，循环次数：1 000 次。测试结束后进行目视检查，硬件动态口令令牌外壳所印刷的标记文字（包括但不限于序列号和有效期）应能被目视识别。

6.2.3.9 振动

按照 GB/T 2423.10—2019 中的扫频耐久试验进行测试，严酷等级选择频率：10 Hz～300 Hz，振动幅值：3.5 mm，扫频循环数：50。测试结束后，硬件动态口令令牌应能正常使用。

6.2.3.10 静电放电

按照 GB/T 17626.2—2018 中试验等级 3 进行测试。测试结束后，硬件动态口令令牌应能正常使用。

6.3 动态口令鉴别系统(服务)

6.3.1 密码服务功能要求

6.3.1.1 概述

应支持的功能包括但不限于以下内容。

——动态口令鉴别:按照 5.3 的要求验证动态口令。

——动态因子同步:按照 5.4 的要求进行动态因子同步。

——动态口令令牌管理:管理和维护动态口令令牌序列号与种子密钥的对应关系。

——用户管理(可选):管理和维护动态口令令牌与用户标识的对应关系。

6.3.1.2 动态口令鉴别

验证动态口令所使用的窗口应符合 5.3 的要求。

生成挑战码(如果支持挑战因子)应使用随机数。生成随机数所使用的随机数发生器应符合以下要求之一:

——使用通过商用密码产品认证的随机数发生器;

——使用通过商用密码产品认证且提供随机数生成服务的密码设备;

——所使用的随机数发生器生成的随机数符合 GB/T 32915 的要求。

如使用 SM4 算法生成动态口令,则应使用密码机进行加密运算。

宜具有时间校准的处理方法和措施。

6.3.1.3 动态因子同步

应符合 5.4 的要求。

6.3.1.4 动态口令令牌管理

应记录的动态口令令牌数据包括但不限于:令牌序列号、种子密钥索引、令牌状态、上次使用时间、连续错误次数、令牌动态因子偏移量等。还可记录令牌序列号对应的用户标识。

令牌的状态应与种子密钥的生命周期状态(见 5.5.1)一致,如表 1 所示。

表 1 令牌状态

状态	描述	说明
未激活	令牌出厂时的状态,应激活后令牌才能进入就绪状态	应不对未激活状态的令牌进行动态口令鉴别
就绪	令牌正常工作状态	就绪状态下令牌可用于口令鉴别
锁定	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	应不对锁定状态的令牌进行动态口令鉴别
挂起	令牌被人为挂起后,处于挂起状态	应不对挂起状态的令牌进行动态口令鉴别
作废	令牌内置的种子密钥过期或令牌被人为作废后,进入作废状态	应不对作废状态的令牌进行动态口令鉴别

应支持的令牌管理功能包括但不限于以下内容。

——增加:在系统中增加一个或多个动态口令令牌。

——删除：从系统中去掉一个或多个动态口令令牌。

——修改：调整系统中特定的动态口令令牌的数据，包括但不限于：

- 激活：将动态口令令牌的状态从“未激活”改为“就绪”；
- 锁定：将动态口令令牌的状态从“就绪”改为“锁定”；
- 解锁：将动态口令令牌的状态从“锁定”改为“就绪”；
- 挂起：将动态口令令牌的状态从“就绪”改为“挂起”；
- 解挂：将动态口令令牌的状态从“挂起”改为“就绪”；
- 废止：将动态口令令牌的状态从其他状态改为“作废”。

——查询：检索令牌的当前状态、上次使用时间、当前累计错误次数等。

如令牌连续多次鉴别动态口令不通过，应自动锁定该令牌。触发自动锁定的鉴别连续不通过次数应不大于5次。可在一定时间后自动解锁，从锁定到解锁之间的间隔时间应不小于1 h。

6.3.2 动态口令密码服务接口

可基于常见的鉴别协议封装动态口令密码服务接口，例如RADIUS(见附录C)。接口应支持动态口令鉴别和动态因子同步功能，可支持查询功能，不宜支持除查询之外的动态口令令牌管理功能。

注：如果接口支持查询之外的动态口令令牌管理功能，则密码应用安全要求将适用于这些接口。

6.3.3 密码应用安全要求

应用动态口令技术时，应根据应用系统的实际情况采取符合GB/T 39786相应等级要求的措施。为动态口令鉴别系统(服务)配置的网络安全保障措施应符合应用系统的网络安全要求。

应采取有效的技术措施保证所存储种子密钥的机密性和完整性。种子密钥存储应使用以下方式之一：

——存储在密码设备内；

——加密后存储在密码设备以外的位置(例如数据库)，且加密所使用的密钥加密密钥存储在密码设备内。

其他宜采取的信息安全保障措施包括但不限于以下内容。

——采取技术措施防止未授权的应用系统服务端接入。

——对动态口令鉴别系统(服务)和应用系统服务端之间的通讯数据做加密处理。

——记录系统日志。触发记录系统日志的事件包括但不限于：

- 动态口令令牌状态变更；
- 动态口令鉴别。

——采用密码技术保障系统日志的完整性。

6.3.4 系统管理功能要求

宜支持的系统管理功能包括但不限于以下内容。

——参数配置：对认证和管理功能参数进行配置。

——用户管理：对访问人员进行权限控制，例如不同角色的访问人员赋予不同的操作权限。

——日志管理：包括日志生成、查询等；每条日志至少记录事件的日期和时间、事件类型、主体身份、事件的结果(成功或失效)、日志级别。

——统计报表：对指定范围内的动态口令令牌使用情况进行统计分析。

6.4 种子密钥管理系统

6.4.1 功能要求

种子密钥管理系统的功能应符合 GM/T 0051—2016 中 6.5 的要求。

应支持的功能包括但不限于：

——种子密钥导入；

——种子密钥导出；

——种子密钥生成；

——种子密钥备份/恢复；

——种子密钥销毁。

各功能应符合 GM/T 0051—2016 中 5.2 的要求。

注：对于种子密钥管理系统而言，种子密钥属于 GM/T 0051—2016 中 3.4 定义的业务密钥。

6.4.2 信息安全要求

种子密钥的存储、分发等应符合 5.5 的要求。

系统安全应符合 GM/T 0051—2016 中 5.1 的要求。

7 动态口令系统检测方法

7.1 试验条件

7.1.1 环境条件

如未标明特殊要求，所有试验均在下述条件下进行。

——环境温度：15 ℃～35 ℃。

——相对湿度：40%～80%。

——大气压：86 kPa～106 kPa。

7.1.2 默认允差

除非另有规定，所给出的测量值的默认允差为±5%。

7.1.3 试验工装

试验工装包括以下内容。

——参照动态口令生成软件：具有生成动态口令功能，且应符合以下要求：

- 生成动态口令的方法符合 5.2 的要求；
- 能够基于任意指定的种子密钥以及动态因子生成动态口令。

——种子密钥数据集。其中包含的种子密钥数量应≥10^6，种子密钥的长度应符合 5.5.2 的要求。

——事件动态因子数据集。其中包含的动态因子数量应≥10^6。动态因子的值应≥1。

——挑战动态因子数据集。其中包含的种子密钥数量应≥10^6。

——参照授时服务器。

——参照种子密钥管理系统：内置种子密钥数据集。应符合 6.4 的要求。

——参照动态口令应用客户端：向动态口令鉴别系统发送动态口令并获取鉴别结果(可使用 RADIUS 消息格式或其他格式，见附录 C)。

种子密钥和挑战动态因子应使用通过商用密码产品认证的随机数发生器或使用通过商用密码产品

认证的密码产品提供的随机数生成服务生成。

注：GB/T 38556—2020 中的附录 F 提供了验证生成动态口令的方法是否符合要求的参考数据。

7.1.4 试验样品

动态口令令牌样品数量不少于 12 支。令牌中应导入相同的种子密钥(从参照种子密钥管理系统中选取)。如支持事件动态因子,初值应为 1;如支持时间因子,初值对应的 UTC 值应不超过当前时间的 UTC 值±2 min。从样品中选取 6 支进行测试,如果受试的样品在测试结束后能够生成动态口令且与未受试的样品一致,则判定为测试后能正常工作。

动态口令鉴别系统(服务)样品数量应为 1 套。样品中应导入指定的种子密钥(从参照种子密钥管理系统中选取),数量应不少于 10 个。

种子密钥管理系统样品数量应为 1 套。

7.2 动态口令令牌

7.2.1 密码服务功能测试

7.2.1.1 生成动态口令

生成动态口令的方法按照 GM/T 0061—2018 中 5.1 进行测试。将动态口令令牌样品生成的动态口令与参照动态口令生成软件使用相同参数生成的动态口令比对,如二者一致,则测试通过;否则不通过。

应核查动态口令令牌的安全芯片是否通过商用密码产品认证。

7.2.1.2 用户鉴别、锁定与解锁

用户鉴别按照 GM/T 0061—2018 中 5.2.1.1 进行测试。

锁定按照 GM/T 0061—2018 中 5.2.1.2 进行测试。

解锁按照 GM/T 0061—2018 中 5.2.1.3 进行测试。

7.2.2 密码应用安全测试

按照 GM/T 0039 进行测试。

7.2.3 硬件动态口令令牌

7.2.3.1 高温

按照 6.2.3.1 中的试验方法和参数进行测试。

7.2.3.2 低温

按照 6.2.3.2 中的试验方法和参数进行测试。

7.2.3.3 高低温冲击

按照 6.2.3.3 中的试验方法和参数进行测试。

7.2.3.4 湿度

按照 6.2.3.4 中的试验方法和参数进行测试。

7.2.3.5 低气压

按照 6.2.3.5 中的试验方法和参数进行测试。

7.2.3.6 跌落

按照 6.2.3.6 中的试验方法和参数进行测试。

7.2.3.7 防尘防水

按照 GB/T 4208—2017 进行测试。

7.2.3.8 标记和印刷

按照 6.2.3.8 中的试验方法和参数进行测试。

7.2.3.9 振动

按照 6.2.3.9 中的试验方法和参数进行测试。

7.2.3.10 静电放电

按照 6.2.3.10 中的试验方法和参数进行测试。

7.3 动态口令鉴别系统(服务)

7.3.1 密码服务功能测试

7.3.1.1 动态口令鉴别

按照 GM/T 0061—2018 中 5.3.1 进行测试。

如果支持挑战因子,按照 GM/T 0061—2018 中 5.3.3 进行测试,并按照 GM/T 0062—2018 中第 9 章(E 类产品)对其生成挑战因子所使用的随机数发生器进行测试。

7.3.1.2 动态因子同步

按照 GM/T 0061—2018 中 5.2.2.8 进行测试。

7.3.1.3 动态口令令牌管理

应被记录的动态口令令牌相关数据以及令牌信息查询按照 GM/T 0061—2018 中 5.2.2.10 进行测试。

应支持的令牌管理功能按照 GM/T 0061—2018 中 5.2.2.9 进行测试。

7.3.2 动态口令密码服务接口测试

使用参照动态口令生成软件,基于当前动态因子生成动态口令,使用参照动态口令应用客户端与动态口令鉴别系统建立连接,进行动态口令鉴别。如果鉴别结果为通过,则测试通过;否则测试不通过。

使用参照动态口令生成软件,基于当前动态因子偏移随机数量,连续生成两个动态口令;使用参照动态口令应用客户端与动态口令鉴别系统建立连接,进行动态因子同步,同步结束后进行动态口令鉴别。如果鉴别结果为通过,则测试通过;否则测试不通过。

7.4 种子密钥管理系统

种子密钥生成应按照 GM/T 0061—2018 中 5.4.6 进行测试。如所使用的随机数发生器未经商用密码产品认证,还应按照 GM/T 0062 对其随机数发生器进行测试。

附 录 A
（资料性）
种子密钥管理方案示例

总体架构如图 A.1 所示。密钥管理中心部署于应用方。应用方和生产方均部署服务器密码机（选用符合 GM/T 0030 要求且通过商用密码产品认证的产品）。动态口令令牌制造工装属于 GM/T 0051—2016 中 3.3 定义的被管设备，符合 GM/T 0051—2016 中关于被管设备的相关要求。

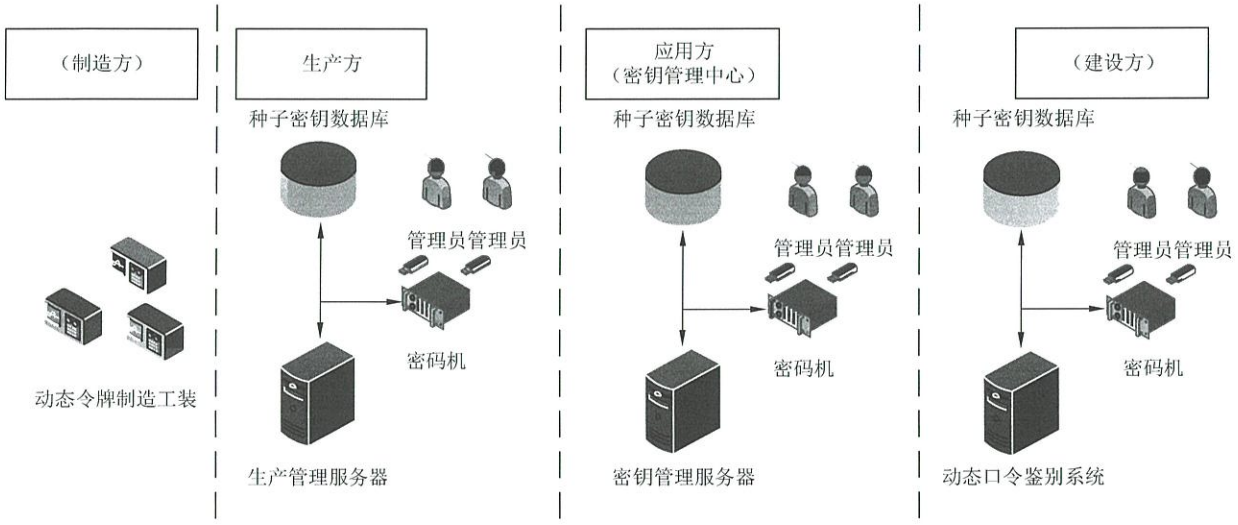

图 A.1 总体架构

种子密钥属于 GM/T 0051—2016 中 3.4 定义的业务密钥。除种子密钥之外，密钥管理中心使用的密钥包括：

——系统主密钥 K_m，在应用方的密码机中生成与存储、使用；

——建设方主密钥 K_s，由 K_m 基于建设方标识（例如统一社会信用代码）分散获得，用于对传递给建设方（并最终导入到动态口令鉴别系统的）种子密钥加密；

——建设方密钥加密密钥 K_{ss}，由 K_s 基于令牌序列号分散获得，用于对传递给建设方（并最终导入到动态口令鉴别系统的）种子密钥加密；

——生产方主密钥 K_p，由 K_m 基于生产方标识分散获得，通过 K_t 加密提供给生产方使用（即开发动态口令令牌时在固件中预置的动态口令令牌主密钥）；

——生产方密钥加密密钥 K_{ps}，由 K_p 基于令牌序列号分散获得，用于对传递给制造方（并最终写入动态口令令牌的）种子密钥加密。

管理密钥采用加密的密钥分量的方式保存，使用密钥分割技术把密钥分割成至少两个部分。每一部分采用不同的密钥加密密钥进行加密，并分别由不同的管理员保存（使用 IC 卡等安全存储介质）。在多个管理员同时操作的情况下，密码机能够解密得到管理密钥并存储。

种子密钥从密钥管理中心到动态口令令牌的传递过程包括：

——密钥管理中心（应用方）由 K_p 基于令牌序列号分散获得 K_{ps}，用 K_{ps} 对种子密钥计算鉴别码并加密，将令牌序列号和加密后的（带鉴别码的）种子密钥发给生产方；

——生产方检索匹配的动态口令令牌制造工装，将令牌序列号加密后的（带鉴别码的）种子密钥发给工装；

——工装对动态口令令牌进行初始化，将令牌序列号写入动态口令令牌，再将加密后的（带鉴别码

的)种子密钥发给动态口令令牌;

——动态口令令牌根据令牌序列号和设备认证密钥分散得到密钥加密密钥,对加密后的(带鉴别码的)种子密钥解密并基于鉴别码验证其完整性,验证通过后保存。

种子密钥从密钥管理中心到动态口令鉴别系统的传递过程包括:

——密钥管理中心由 K_s 基于令牌序列号分散获得 K_{ss},用 K_{ss} 对种子密钥计算鉴别码并加密,将令牌序列号和加密后的(带鉴别码的)种子密钥发给建设方;

——建设方在密码机中由 K_s 基于令牌序列号分散获得 K_{ss},对加密后的(带鉴别码的)种子密钥解密并基于鉴别码验证其完整性。验证通过后,随机生成密钥加密密钥,对种子密钥加密,由建设方将令牌序列号和加密后的种子密钥保存在种子密钥数据库。

根据 GM/T 0030 的定义,上述密钥在各方密码机中的类型如表 A.1 所示。

表 A.1 密钥类型

标识	应用方密码机	建设方密码机	生产方密码机
K_m	管理密钥	不涉及	不涉及
K_s	用户密钥	管理密钥	不涉及
K_{ss}	密钥加密密钥	密钥加密密钥	不涉及
K_p	用户密钥	不涉及	管理密钥
K_{ps}	密钥加密密钥	不涉及	密钥加密密钥
K_t	会话密钥	会话密钥	会话密钥

附 录 B
（资料性）
动态口令令牌的密码模块规格

B.1 硬件动态口令令牌描述为密码模块

硬件动态口令令牌的密码模块类型为硬件模块。密码边界是令牌的物理边线。密码边界内部的主要部件包括安全芯片、电池等。组成框图如图 B.1 所示（图上还标明了密码边界、物理端口和逻辑接口）。

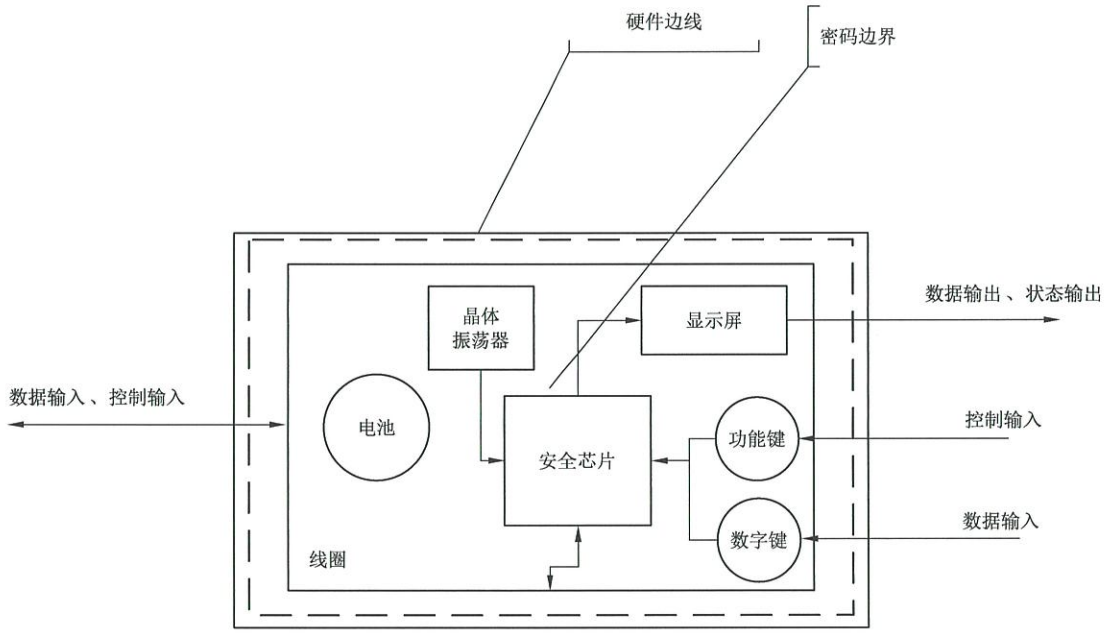

图 B.1 硬件动态口令令牌框图示例

物理端口及其对应的逻辑接口类型如表 B.1 所示。物理实体类型为单芯片。运行环境类型为不可修改的运行环境。

表 B.1 硬件动态口令令牌接口

物理端口	简介	逻辑接口类型
触发功能按键	触发令牌显示当前动态口令	控制输入
其他功能按键（可选）	触发令牌其他功能（如切换动态因子等）	控制输入
数字按键（可选）	输入 PIN、挑战值等	数据输入
显示屏	显示当前动态口令（以及其他信息，例如电量等）	数据输出、状态输出
线圈（或触点）	在生产时下载固件及种子密钥	数据输入、控制输入

敏感安全参数（SSP）包括设备序列号、种子密钥等。

角色与权限如表 B.2 所示。

表 B.2　角色与权限

角色	权限	鉴别机制
用户(可选)	生成动态口令、修改 PIN	基于 PIN
密码主管(CO)	初始化	基于设备认证密钥

B.2　软件动态口令令牌描述为密码模块

软件动态口令令牌的密码模块类型为软件模块。密码边界由可执行文件确定。示例如图 B.2 所示。运行环境类型为可修改的运行环境。

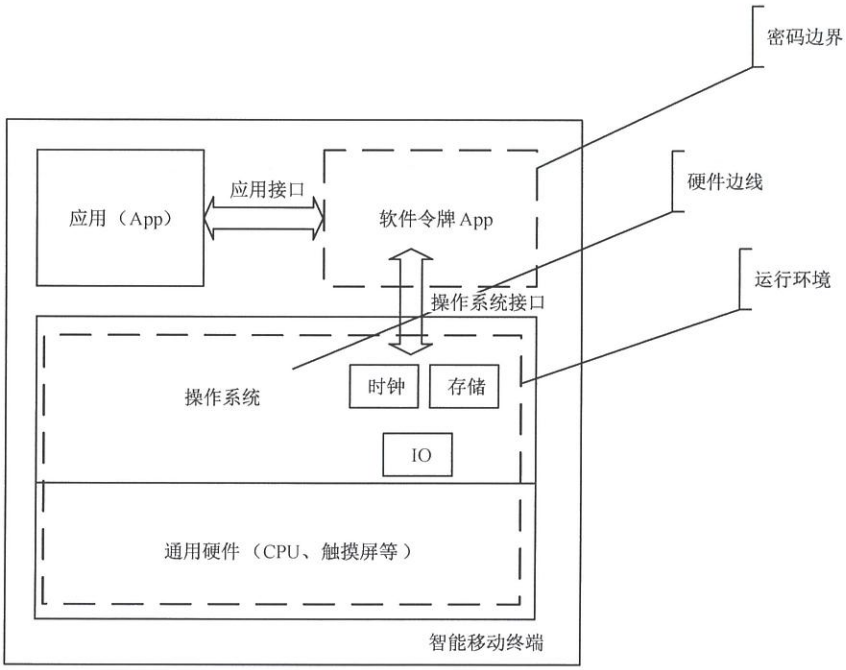

图 B.2　软件动态口令令牌框图示例

软件接口及其对应的逻辑接口类型如表 B.3 所示。

表 B.3　软件动态口令令牌接口

软件接口	简介	逻辑接口类型
获取动态口令	触发令牌输出当前动态口令	数据输出、数据输入(挑战码,可选)
身份鉴别(可选)	令牌输入当前动态口令所需的身份鉴别	控制输入
初始化	设置种子密钥、从操作系统获取动态因子初值	数据输入

附 录 C
（资料性）
动态口令系统与应用系统对接

C.1 RADIUS

RADIUS(Remote Authentication Dial In User Service,远程认证拨号用户服务)是一种应用广泛的 AAA(Authentication Authorization Accounting,鉴别、授权与计费)服务。RFC 2865 及 RFC 2866 对 RADIUS 进行了详细规定。RADIUS 的典型工作过程包括:

a) 用户向 RADIUS 客户端(或作为 RADIUS 客户端使用的 NAS)提供鉴别信息(例如用户名/口令);
b) RADIUS 客户端将用户提交的鉴别信息封装在接入请求数据包中(数据包中还包括客户端 ID 和用户访问端口的 ID),发给 RADIUS 服务器;
c) RADIUS 服务器进行用户鉴别,将鉴别结果回送给 RADIUS 客户端;
d) RADIUS 客户端如果收到鉴别结果为"允许接入",则为用户建立连接,对用户进行授权和提供服务;否则拒绝用户连接。

RADIUS 消息结构如图 C.1 所示。

图 C.1 RADIUS 消息结构

其中:

——Code 字段的长度为 1 字节,其值表示 RADIUS 消息的类型(请求接入、允许接入、拒绝接入等);
——Identifier 字段的长度为 1 字节,用于匹配请求消息与回复消息(请求消息与对应的回复消息的 Identifier 值相同);
——Length 字段的长度为 2 字节,其值为整个消息的长度(以字节为单位);
——Authenticator 字段的长度为 16 字节,其值为基于预共享密钥生成的消息鉴别码;
——Attributes 字段包括若干(0 个或多个)TLV 结构的内容(属性)。RADIUS 定义了包括用户名和口令在内的一系列属性,并且预留编码 26 作为自定义属性。

C.2 PAM

PAM(Pluggable Authentication Modules)是一种鉴别机制,在 Linux、UNIX 等操作系统得到广泛应用,国产操作系统(例如统信操作系统、优麒麟系统等)也普遍支持。PAM 使应用程序与鉴别机制的具体实现分离,当鉴别机制变更时,不需要修改应用程序,只需要系统管理员对配置文件进行修改即可。具体地:

——系统管理员通过 PAM 配置文件来制定各个应用程序的鉴别策略;
——应用程序开发者通过在源代码中调用 PAM API 来使用鉴别服务;
——PAM 服务模块的开发者通过实现 PAM SPI 与 PAM 接口库(libpam)对接;

——PAM 接口库(libpam)读取配置文件,将应用程序和相应的 PAM 服务模块联系起来。

如图 C.2 所示。其中,Pamh 是应用程序调用 PAM 所需的参数(句柄)。

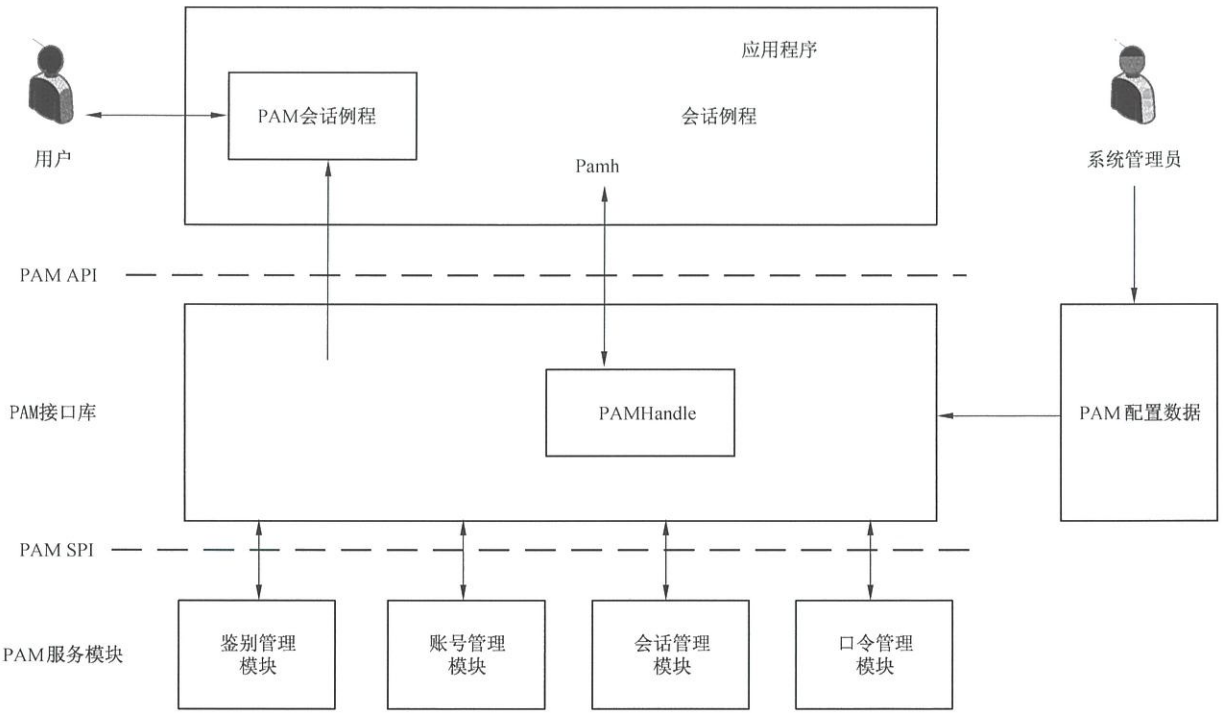

图 C.2 PAM 架构

PAM 服务模块包括以下类型:

——鉴别管理(authentication management),接收用户名和口令,基于用户名/口令进行鉴别;

——账户管理(account management),用于检查账户的权限,例如是否被允许登录系统、是否已经过期等;

——会话管理(session management),用于会话管理和计费;

——口令管理(password management),用于修改用户口令。

C.3 其他

可供应用系统与动态口令系统对接的框架还包括以下内容。

——OAuth:在传统的 C/S 身份验证模型中,客户端通过使用资源所有者的凭据向服务器进行身份验证来请求服务器上的访问受限资源(受保护资源)。为了使第三方应用程序能够访问受限资源,资源所有者需要与第三方共享其凭据。OAuth 通过引入授权层并将客户端的角色与资源所有者的角色分开来解决这些问题。在 OAuth 中,客户端通过获取访问令牌而不是使用资源拥有者的凭据来访问受限资源。授权服务器在资源所有者的批准下才会向第三方客户端颁发访问令牌。客户端使用访问令牌来访问资源服务器托管的受保护资源。RFC 6749 对 OAuth 进行了描述。GM/T 0068—2019 参考了 RFC 6749。

——SAML(Security Assertion Markup Language,安全断言置标语言):SAML 是一个基于 XML 的开源标准数据格式,它在当事方之间交换身份验证和授权数据,尤其是在身份提供者和服务提供者之间交换。SAML 定义了三个角色:委托人(用户)、身份提供者(IdP),服务提供者(SP)。委托人向服务提供者请求访问一项服务,服务提供者向身份提供者索取身份断言,并基于这一断言进行访问控制。GB/T 29242 有对 SAML 的相关要求。

参 考 文 献

[1] GB/T 7408—2005 数据元和交换格式 信息交换 日期和时间表示法

[2] GB/T 15843.1—2017 信息技术 安全技术 实体鉴别 第1部分:总则

[3] GB/T 29242 信息安全技术 鉴别与授权 安全断言置标语言

[4] GB/T 37937—2019 北斗卫星授时终端技术要求

[5] GB/T 38556—2020 信息安全技术 动态口令密码应用技术规范

[6] GM/T 0030 服务器密码机技术规范

[7] GM/T 0068—2019 开放的第三方资源授权协议框架

[8] GM/T 0107—2021 智能IC卡密钥管理系统基本技术要求

[9] IETF. RFC 2865: Remote Authentication Dial In User Service (RADIUS) [EB/OL]. https://datatracker.ietf.org/doc/rfc2865/,2020-01-21.

[10] IETF. RFC 2866: RADIUS Accounting [EB/OL]. https://datatracker.ietf.org/doc/html/rfc2866/,2020-01-21.

[11] IETF. RFC 6749: The OAuth 2.0 Authorization Framework [EB/OL]. https://datatracker.ietf.org/doc/rfc6749/,2012-10-08.

[12] OASIS. SAML V2.0 Protocol Extension for Third-Party Requests [EB/OL]. https://www.oasis-open.org/standards/,2007-05-23.