**动态口令生成算法说明**

**目 录**

[1. 动态口令生成算法 1](#_Toc486234098)

[1.1 登录口令 1](#_Toc486234099)

[1.1.1 算法描述 1](#_Toc486234100)

[1.2 基本挑战应答口令 1](#_Toc486234101)

[1.2.1 触发条件 1](#_Toc486234102)

[1.2.2 算法描述 2](#_Toc486234103)

[附录一、截位函数 3](#_Toc486234104)

[附录二、登录口令运算用例 4](#_Toc486234105)

[附录三、基本挑战应答口令运算用例 5](#_Toc486234106)

# 动态口令生成算法

## 登录口令

### 算法描述

动态口令的产生采用国密局《动态口令认证密码应用技术规范》中制定的算法：

**T=T0/Tc**

T是参与运算的时间因子，是一个8字节整数，T0是以UTC时间为标准的8字节整数，Tc是以秒为单位的口令变化周期。

**ID={T}**

ID是杂凑算法的输入信息，在右侧用0x00补足16字节。

**S=SM3(K｜ID)**

S是杂凑算法的输出结果，K为种子密钥密钥，长度为20字节。

**OD=Truncate(S)**

Truncate()是截位函数（详见附录），OD是其输出结果，长度为32比特。

**P=OD%(10^N)**

N是动态口令长度，P是最终显示的动态口令。

## 基本挑战应答口令

### 触发条件

开机验PIN成功后，在等待信息输入界面输入挑战信息，然后按“确认”键。

输入的挑战信息为1到40位，由0到9十个数字和小数点组成。

### 算法描述

动态口令的产生采用国密局《动态口令认证密码应用技术规范（征求意见稿）》中制定的算法：

**T=T0/Tc**

T是参与运算的时间因子，是一个8字节整数，T0是以UTC时间为标准的8字节整数，Tc是以秒为单位的口令变化周期。

**ID={T|Q}**

ID是杂凑算法的输入信息，在右侧用0x00补足16字节，Q是挑战数，由1到40个十进制数组成。

**S=SM3(K｜ID)**

S是杂凑算法的输出结果，K为种子密钥密钥，长度为20字节。

**OD=Truncate(S)**

Truncate()是截位函数（详见附录），OD是其输出结果，长度为32比特。

**P=OD%(10^N)**

N是动态口令长度，P是最终显示的动态口令。

# 附录一、截位函数

Truncate（）函数的详细实现如下：

S为32字节的串，定义8个4字节整数S1，S2，S3，S4，S5，S6，S7，S8，通过如下方法赋值：

S1 = S[0]<<24 | S[1]<<16 | S[2]<<8 | S[3]

S2 = S[4]<<24 | S[5]<<16 | S[6]<<8 | S[7]

S3 = S[8]<<24 | S[9]<<16 | S[10]<<8 | S[11]

S4 = S[12]<<24 | S[13]<<16 | S[14]<<8 | S[15]

S5 = S[16]<<24 | S[17]<<16 | S[18]<<8 | S[19]

S6 = S[20]<<24 | S[21]<<16 | S[22]<<8 | S[23]

S7 = S[24]<<24 | S[25]<<16 | S[26]<<8 | S[27]

S8 = S[28]<<24 | S[29]<<16 | S[30]<<8 | S[31]

OD = (S1 + S2 + S3 + S4 + S5 + S6 + S7 + S8) MOD 2^32

# 附录二、登录口令运算用例

|  |  |
| --- | --- |
| T0 | 1452067154 |
| TC | 30 |
| T=T0/TC | 0x 00 00 00 00 02 E2 8F 3E |
| ID={T} | 0x 00 00 00 00 02 E2 8F 3E 00 00 00 00 00 00 00 00 |
| K | 0xC11D0FB911530F706B6E67B0022EAAF405A34E67 |
| S=SM3(K|ID) | 0x 52 A2 51 0D 45 53 ED 3C BB 21 27 5F 54 99 DD 2F C8 E3 75 32 0B 83 B1 DA A8 09 AF 55 43 5F BB EB |
| OD=Truncate(S) | 1736561955 |
| P | 561955 |

# 附录三、基本挑战应答口令运算用例

|  |  |
| --- | --- |
| T0 | 1452067854 |
| TC | 30 |
| T=T0/TC | 0x 00 00 00 00 02 E2 8F 55 |
| Q | 1234 |
| ID={T|Q} | 0x00 00 00 00 02 E2 8F 55 31 32 33 34 00 00 00 00 |
| K | 0xC11D0FB911530F706B6E67B0022EAAF405A34E67 |
| S=SM3(K|ID) | 0xB2 ED 98 E6 12 C8 FE 72 E3 CC D0 E0 58 E7 35 6F 3A 55 41 B1 1A 77 86 F7 6C 37 39 2C 4D 9C 59 E2 |
| OD=Truncate(S) | 285931869 |
| P | 931869 |

|  |  |
| --- | --- |
| T0 | 1452068087 |
| TC | 30 |
| T=T0/TC | 0x 00 00 00 00 02 E2 8F 5D |
| Q | 1234567890. [11位，最后有一个小数点] |
| ID={T|Q} | 0x00 00 00 00 02 E2 8F 5D 31 32 33 34 35 36 37 38 39 30 2E |
| K | 0xC11D0FB911530F706B6E67B0022EAAF405A34E67 |
| S=SM3(K|ID) | 0x1B 3F DB 35 BD 64 9A 8F 7A B5 B9 6F 6C A6 67 39 E7 64 36 34 16 68 48 A3 4C 6E 55 2F 35 B7 1E C3 |
| OD=Truncate(S) | 1072859445 |
| P | 859445 |