基于时间的动态口令令牌技术规范

（修改稿）

《基于时间的动态口令令牌技术规范》编写组

2011 年 02 月

目　　次

前　　言

基于时间的动态口令令牌产品因目前无国家标准和行业标准，本规范参照全国各地企业相关现有的技术规范，制定出本规范。本规范适用组织基于时间的动态口令令牌产品的生产和检测产品的依据，其中各项技术指标可随企业的技术进步和产品改进而提高标准。

本规范由上海市密码管理局提出。

本规范起草单位：上海众人网络安全技术有限公司，上海市信息安全行业协会。

本规范主要起草人：谈剑峰，尤磊，单蓉胜。

基于时间的动态口令令牌技术规范

1 范围

本规范规定了基于时间的动态口令令牌的相关规范，主要内容包括SM3-TOTP计算要求和认证实施过程与安全性要求。SM3-TOTP计算要求部分规范了符合和约定及算法，认证实施过程与安全性要求部分规范了时间同步、时间失步处理、令牌种子安全性等各项要求。

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。

电工电子产品环境试验国家标准汇编 GB/T2423

防尘防水特性的国际工业标准 IP67

HOTP: An HMAC-Based One-Time Password Algorithm RFC 4226

3 术语和定义

本规范确立及下列术语和定义只适用于本规范。

3.1 令牌

生成并显示动态口令的载体。

3.2 动态口令

由令牌种子与当前时间通过SM3算法运算生成的一次性口令，本规范中规定为6或8位数字。

3.3 令牌种子

即令牌密钥，用于与时间数据组装，通过特定算法运算获得当前时间的动态口令，同时存储于令牌和认证服务器中。令牌种子最小长度为128bit。

3.4 SM1 算法

一种对称加密算法，分组长度为128比特，密钥长度为128比特，在本规范中用于令牌种子的加密保护。

3.5 SM3 算法

一种杂凑算法，具体使用方法参考国家密码管理局发布的《SM3密码杂凑算法》。

3.6 SM3-TOTP 计算

一种基于SM3算法的时间同步一次性口令计算方法，其英文名为SM3 Time-Based One-Time Password。

3.7 当前时间

以UTC时间为标准的当前时间。

3.8 认证服务器

动态口令认证系统中负责接受动态口令认证请求，运算并对比口令，返回认证结果的服务器节点。

3.9 口令正常

动态口令令牌能按照本规范所规定的逻辑完成相应的功能，在令牌上可显示，并能够在时间窗口内认证通过，即判定为口令正常。

3.10 时间源服务器

以UTC时间为基准的时间服务器，可供其他系统和服务器进行时间校准。

4 技术要求

4.1 SM3-TOTP 计算要求

4.1.1 符号和约定

T0 是一个4字节整数，代表当前时间（以UTC时间为标准）。

X 口令变化周期，单位为秒，30秒或者60秒。

T 是一个4字节整数，当前时间除以X的值，公式描述为T = T0 / X。

P 一次性口令。

P0 SM3算法输出数据，32个字节。

D 十进制口令位数，6或者8位数字。

K 令牌种子。

S SM3算法输入数据。

SM3 SM3算法。

4.1.2 算法描述

计算T=T0/X。

组装SM3算法输入数据S，按T、K的顺序进行组装。

计算P0=SM3(S)。

设8个整数，依次按I1,I2,I3,I4,I5,I6,I7,I8表示，通过如下方法赋值：

I1 = P0[0] << 24 || P0[1] << 16 || P0[2] << 8 || P0[3]

I2 = P0[4] << 24 || P0[5] << 16 || P0[6] << 8 || P0[7]

I3 = P0[8] << 24 || P0[9] << 16 || P0[10] << 8 || P0[11]

I4 = P0[12] << 24 || P0[13] << 16 || P0[14] << 8 || P0[15]

I5 = P0[16] << 24 || P0[17] << 16 || P0[18] << 8 || P0[19]

I6 = P0[20] << 24 || P0[21] << 16 || P0[22] << 8 || P0[23]

I7 = P0[24] << 24 || P0[25] << 16 || P0[26] << 8 || P0[27]

I8 = P0[28] << 24 || P0[29] << 16 || P0[30] << 8 || P0[31]

I = (I1 + I2 + I3 +I4 +I5 +I6 + I7 +I8) MOD 2^32

计算P=I % (10^D)。10^D为10的D次方，P是一个D位的整数。

4.2 认证实施过程与安全性要求

4.2.1 时间同步要求

令牌时间和认证系统时间应保持同步，即认证系统时间应该为以UTC时间为标准的当前时间，令牌时间在发行时应该设定为与认证系统时间相同的时间。

4.2.2 时间失步处理要求

当令牌时间与认证系统时间失步时，应该对认证系统中该令牌时间进行误差修正，以保持该令牌时间与认证系统时间的同步。对时间误差的修正可以由合法用户自己完成或由令牌自动完成。

4.2.3 令牌种子安全性要求

4.2.3.1 生成要求

令牌种子应为真随机数，应符合《随机性检测规范》的要求。

4.2.3.2 分发要求

令牌制作过程中，必须由令牌种子生成的设备将令牌种子直接导入相应令牌中，该过程必须不涉及任何公共网络传输。令牌种子文件应该由令牌种子生成的设备，采用SM1算法进行加密，通过安全传输方式（如光盘）导入到相关认证系统中，该过程必须不涉及任何公共网络传输，并应该具有完整性校验。

4.2.3.3 存储要求

令牌种子在认证系统中应该采用SM1算法加密存储，在令牌中应该存储在令牌芯片的随机存取存储器（如保存在加密卡或加密机中）中，由令牌芯片保证其安全性。令牌芯片应当能够防止在芯片不掉电的情况下，通过调试接口直接读出RAM中的令牌种子，或者通过调试接口修改芯片程序，利用改编的程序读出RAM中的令牌种子。

4.2.3.4 使用要求

令牌种子在通过SM3-TOTP计算动态口令时，该过程必须在国家密码管理局认可的硬件设备中完成。

4.2.4 算法安全性要求

令牌芯片应当能够保证其程序存储器（Flash)中SM3算法的安全性，使得通过调试接口或者修改部分程序均不能读出并破译令牌的SM3算法。

4.2.5 认证服务器时间要求

认证服务器定期以时间源服务器为准，进行校准。

4.2.6 认证时间窗口要求

由于存在令牌时间误差的积累和认证数据传输的延时，为提高认证的成功率，服务器具有设置一个时间范围（窗口）的功能 ，在这个范围内的口令都可以认证成功。该时间范围可调整（调整范围为最大±5分钟）。

4.2.7 口令一次性有效要求

认证服务器对任何一个口令,只能认证一次。对本次认证和之前时间的动态口令不能再次认证成功。

4.2.8 误差自动追踪要求

认证服务器应该具有对令牌的时间误差进行追踪和记录的功能，并作为认证时间计算依据，以提高认证的成功率。

4.2.9 口令同步要求

令牌的时间误差超出认证服务器的追踪范围和认证时间窗口后,认证服务器应该可以重新进行令牌时间误差（即误差累计值）计算（误差范围为±6分钟/年）。

4.2.10 防电子侦听、暴力穷举等攻击要求

认证系统应该具有防电子侦听、暴力穷举攻击的功能。令牌连续认证失败超过一定次数后，认证服务器对此令牌进行一段时间的锁定保护，在此时间段内，不可再认证。可以在确认用户身份后进行解除锁定，或者过了保护时间段后自动解除锁定。上述认证失败次数可以设定，锁定保护的时间长度可以设定。

4.2.11 双因素认证要求

认证系统应该可以在认证服务器端为令牌设置一个PIN码,连同PIN码一起认证以达到双因素认证的效果，或者可以同时使用原来系统的静态口令认证，达到双因素认证效果。

4.2.12 防暴力拆解要求

令牌应该具备防暴力拆解特性，即通过强行打开令牌的方式会导致令牌中令牌种子不可恢复的销毁。

4.2.13 认证通信安全要求

认证通讯安全必须经过加密传输方式进行以确保认证代理与认证服务器之间通讯的机密性、完整性和不可抵赖性。

4.2.14 挑战应答机制

如需要采用挑战应答机制生成动态口令，则在4.1.2算法描述中，将挑战码数据C，按T、K、C的顺序进行组装，形成SM3算法输入数据S。其他生成动态口令的步骤，如4.1.2中所述。

附 录 A
（资料性附录）
SM3-TOTP 计算用例

C语言实现示例（4字节int类型，Small-endian环境，令牌种子是ausTokenID,长度为16字节）

```
unsigned char X=60;
unsigned int T0,T;
int D=6;
unsigned char sm3_in[20]     = {0};
unsigned char ausTokenID[16] = {0};
unsigned char S[20];
unsigned char P0[32];
unsigned int I1,I2,I3,I4,I5,I6,I7,I8,I;
unsigned int P;

T=T0/X;

unsigned char*  p = 0;
if (big_endian())
    T = big_to_small_32(T);

p = (unsigned char*)&T;
sm3_in[0]   = *(p + 3);
sm3_in[1]   = *(p + 2);
sm3_in[2]   = *(p + 1);
sm3_in[3]   = *(p + 0);
memcpy(sm3_in+4,ausTokenID,16);
SM3(S, P0);
I1 = P0[0] << 24 || P0[1] << 16 || P0[2] << 8 || P0[3]
I2 = P0[4] << 24 || P0[5] << 16 || P0[6] << 8 || P0[7]
I3 = P0[8] << 24 || P0[9] << 16 || P0[10] << 8 || P0[11]
I4 = P0[12] << 24 || P0[13] << 16 || P0[14] << 8 || P0[15]
I5 = P0[16] << 24 || P0[17] << 16 || P0[18] << 8 || P0[19]
I6 = P0[20] << 24 || P0[21] << 16 || P0[22] << 8 || P0[23]
I7 = P0[24] << 24 || P0[25] << 16 || P0[26] << 8 || P0[27]
I8 = P0[28] << 24 || P0[29] << 16 || P0[30] << 8 || P0[31]

I = (I1 + I2 + I3 +I4 +I5 +I6 + I7 +I8) MOD 2^32
P=I % (10^D); // 10的D次方
printf(“%d\n”, P);
```

附 录 B
（资料性附录）
SM3-TOTP 计算输入输出示例

输入参数必须为时间、密钥。
时间为UTC标准时间，密钥长度为16个字节。
具体见下表:

表 附录B-1 输入输出示例表

北京时间	UTC 标准时间	密钥（2 位为 1 个字节）	6 位密码	8 位密码
201010121701	1286874060	4225e56988184643c10ba5c2f52b84e8	367650	67367650
201010121702	1286874120	1f53de416ca79895086c64a7a2e5818a	151017	64151017
201010121703	1286874180	047a3ee066bf6990e76bdfbdc31e2ff3	974147	15974147
201010121704	1286874240	a18e3552720d1dc7882615c3b0ee18cd	160563	13160563
201010121705	1286874300	18a5416f1a069ac9ac5ae5d754d889c7	857910	18857910
201010121706	1286874360	2f601262b57155de23c9aac638c6875f	548506	94548506
201010121707	1286874420	24166b29e2d10fefc7a2edeadaafa649	178480	79178480
201010121708	1286874480	b6cd6d9ee072f631f159d4508ae504a6	480547	34480547
201010121709	1286874540	38624a407322bad665b04a1139403cb0	133012	98133012
201010121710	1286874600	25971966bac6e7c0dedcf1082a6ed266	585088	73585088

附 录 C
（资料性附录）
令牌其他特性

C.1 物理特性要求

C.1.1 温度

可承受温度：上限+70℃，下限-20℃。

工作温度在-10℃～+50℃之间，产品显示口令正常。储存温度在+70℃，下限-20℃之间。

温度超过+50℃或低于-10℃，产品可能显示口令不正常，但温度恢复到+50℃～-10℃之间，产品显示口令可恢复正常。

C.1.2 湿度

可承受湿度：上限90%RH，下限10%RH。

长时间湿度超过90%RH或低于10%RH，可能会对产品外壳形状或颜色产生影响，进而影响口令正常显示。不建议长时间放在超过此指标的环境下24小时。

C.1.3 抗震

可承受震动：水平振动及垂直震动；频率上限300HZ；振幅上限3mm；时间1小时。

C.1.4 防尘防水

达到IP67等级。具体数值请查阅相关标准资料。

C.1.5 抗挤压

可承受挤压：上限液压1000N或气压1000N；时间1小时。

C.1.6 抗跌落

可承受跌落：高1m；混凝土地表；跌落为自由跌落运动；产品各表面各为底面跌落至少1次；跌落次数为10次以上。

C.2 电磁特性要求

C.2.1 抗静电放电

可抗静电放电：空隙式放电12kV；接触式放电8kV。

C.2.2 抗电磁干扰

可抗工频50Hz，1安/米（A/m）连续磁场的干扰。

C.3 产品元件特性要求

C.3.1 电池电压

产品供电电压3V±10%。

C.3.2 晶振频率

晶振频率为32768HZ。

附 录 D
（资料性附录）
试验方法

D.1 试验条件

D.1.1 以下各项试验都采用试验设备，具体试验设备可自行采购，但试验设备应能满足各项性能的最大和最小边界值测试。

D.1.2 试验时如未规定浸泡、摆放或其他方式所需具体时间，则以 1 小时限。

D.2 技术要求试验

D.2.1 SM3-TOTP 计算测试

对SM3-TOTP计算采用国家密码管理局专用的测试平台进行试验检测。测试结果应达到的输入与输出数据符合测试预期。

D.2.2 认证实施过程与安全性要求

D.2.2.1 检测是否可以通过令牌芯片的调试接口读出完整的算法程序。

D.2.2.2 在令牌芯片不掉电的情况下，检测是否可以通过调试接口读出令牌芯片 RAM 中的令牌种子；在令牌芯片不掉电的情况下，写入新程序，检测令牌芯片 RAM 中保存令牌种子的区域是否已经清零，或者是否能够通过新程序读取保存在 RAM 中的令牌种子。

D.2.2.3 检测各项要求是否符合标准规定实施过程与安全性要求。

D.2.3 温度测试

按试验设备具体说明进行操作。

D.2.3.1 测试步骤

a. 设置温度+70℃，开启设备运行1小时。
b. 设置温度-20℃，开启设备运行1小时。
c. 分别记录测试后令牌硬件外观及口令显示状态。

D.2.3.2 试验输出

通过标准：硬件外观无变形、熔化等破坏性状态改变，并基本不影响产品外观；口令正常。

不通过标准：硬件外观变形、熔化等有破坏性状态改变，并对产品外观有较大影响；口令不正常。

D.2.4 湿度测试

按试验设备具体说明进行操作。

D.2.4.1 测试步骤

a. 设置湿度90%RH，温度10℃-35℃，开启设备运行1小时。
b. 设置湿度10%RH，温度10℃-35℃，开启设备运行1小时。
c. 分别记录测试后令牌硬件外观及口令显示状态。

D.2.4.2 试验输出

通过标准：硬件外观无变形、熔化等破坏性状态改变，并基本不影响产品颜色；口令正常。

不通过标准：硬件外观变形、熔化等有破坏性状态改变，改变产品颜色；口令不正常。

D.2.5 抗震测试

按试验设备具体说明进行操作。

D.2.5.1 测试步骤

a. 设置频率300HZ、振幅3mm；设置震动方向为6个方向，上下前后左右，每2个方向运行20分钟，开启设备运行1小时。
b. 记录测试后令牌硬件外观及口令显示状态。

D.2.5.2 试验输出

通过标准：硬件外观无变形、开裂、脱落等破坏性状态改变，并基本无影响产品外观现象出现；口令正常。

不通过标准：硬件外观变形、开裂、脱落等有破坏性状态改变，并对产品外观有较大影响；口令不正常。

D.2.6 防尘测试

按试验设备具体说明进行操作。

D.2.6.1 测试步骤

a. 环境条件：试验温度15℃～30℃，相对湿度25%～75%；大气压86～106KPa；
b. 金属筛网线径：50um，线间间距：75um，滑石粉用量：2kg/m3～3kg/m3，吹尘方向：上吹尘、下吹尘(浮尘试验)两种。
c. 开启设备上吹尘、下吹尘各运行半小时，共运行1小时。
d. 记录测试后令牌硬件外观及口令显示状态。

D.2.6.2 试验输出

通过标准：产品内部无粉尘；口令正常。

不通过标准：产品内部进入粉尘；口令不正常。

D.2.7 防水测试

按试验设备具体说明进行操作。

D.2.7.1 测试步骤

a. 环境条件：温度15℃～30℃，相对湿度25%～75%；大气压86～106KPa；水槽深度1M。
b. 把产品浸泡在1M深的设备中，开启设备运行2小时。
c. 记录测试后令牌硬件外观及口令显示状态。

D.2.7.2 试验输出

通过标准：产品内部无进水；口令正常。

不通过标准：产品内部进水；口令不正常。

D.2.8 抗挤压测试

按试验设备具体说明进行操作。

D.2.8.1 测试步骤

a. 液压方式：平板的挤压式传动1000N压力；产品分别挤压两侧、顶部、底部；产品被稳固夹住后，挤压力开始；持续时间1小时。
b. 气压方式：设备提供机械式施力恒定1000N压力；产品分别挤压两侧、顶部、底部；产品被稳固夹住后，挤压力开始；持续时间1小时。
c. 记录2种压力测试后令牌硬件外观及口令显示状态。

D.2.8.2 试验输出

通过标准：硬件外形无开裂、脱落等破坏性状态改变，并基本无影响产品外观现象出现；口令正常。

不通过标准：硬件外观变形、开裂、脱落等有破坏性状态改变，并对产品外观有较大影响；口令不正常。

D.2.9 抗跌落测试

按试验设备具体说明进行操作。

D.2.9.1 测试步骤

a. 跌落环境：设置跌落高度为1M；跌落面跟水平误差≤5°；跌落面为硬铁板（硬度高于混凝土）；产品各表面各为底面至少跌落1次。
b. 通电后，按键开始进行跌落测试，完成设置跌落次数后停止，跌落次数为10次以上。
c. 记录测试后令牌硬件外观及口令显示状态。

D.2.9.2 试验输出

通过标准：硬件外观无变形、开裂、脱落等破坏性状态改变，并基本无影响产品外观现象出现；口令正常。

不通过标准：硬件外观变形、开裂、脱落等有破坏性状态改变，并对产品外观有较大影响；口令不正常。

D.2.10 抗静电放电测试

按试验设备具体说明进行操作。

D.2.10.1 测试步骤

a. 测试1：空隙放电模式，设置为12kV，放电20pps(20次/秒)。

b. 测试2：接触放电模式，设置为8kV；放电20pps(20次/秒)。

c. 分别记录2次测试后口令显示是否正常。

D.2.10.2 试验输出

通过标准：口令正常。

不通过标准：口令不正常。

D.2.11 抗电磁干扰测试

按试验设备具体说明进行操作。

D.2.11.1 测试步骤

a. 将干扰源分别放置到令牌的正面、侧面和背面，按照引用标准进行测试。

b. 测试过程中及测试完成后，口令显示是否正常。

D.2.11.2 试验输出

通过标准：测试过程中及测试完成后，口令正常。

不通过标准：测试过程中或测试完成后，口令不正常。