ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0091—2020

基于口令的密钥派生规范

Password-based key derivation specification

2020-12-28 发布　　2021-07-01 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。

请注意本标准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：北京信安世纪科技股份有限公司、格尔软件股份有限公司、北京数字认证股份有限公司、长春吉大正元信息技术股份有限公司、兴唐通信科技有限公司、卫士通信息产业股份有限公司、国家信息安全工程技术研究中心、山东得安信息技术有限公司、北京创原天地科技有限公司。

本文件主要起草人：汪宗斌、刘婷、郑强、傅大鹏、赵丽丽、王妮娜、赵闪、罗俊、张旭、周淑静、张庆勇、焦靖伟、史晓峰、马洪富。

基于口令的密钥派生规范

1 范围

本文件规定了基于口令的密钥派生规范，包括基于口令的密钥派生函数、基于口令的加密方案、基于口令的消息鉴别码。

本文件适用于证书与密钥迁移时利用口令来保护被迁移的密钥。

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 15852.2 信息技术 安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制

GB/T 25069—2010 信息安全技术 术语

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/Z 4001 密码术语

3 术语和定义

GB/T 25069—2010和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

算法标识 algorithm identifier

用于对密码算法进行唯一标识的符号。

3.2

密钥派生函数 key derivation function

通过作用于共享秘密和双方都知道的其他参数，产生一个或多个共享秘密密钥的函数。

[来源：GB/T 25069—2010，2.2.2.124]

3.3

伪随机函数 pseudo random function

产生伪随机数的函数。

3.4

盐值 salt

作为单向函数或加密函数的二次输入而加入的随机变量，可用于导出口令验证数据。

[来源：GB/T 25069—2010，2.2.2.186]

注：盐值也称添加变量。

4 符号和缩略语

下列符号和缩略语适用于本文件。

C:密文,字节串。
c:迭代次数,正整数。
DK:派生密钥,字节串。
dkLen:派生密钥的字节数,正整数。
EM:经过编码的消息,字节串。
hLen:伪随机函数输出的字节数,正整数。
n:派生密钥的分组数,正整数。
IV:初始化向量,字节串。
K:加密密钥,字节串。
M:消息,字节串。
P:口令,字节串。
PS:填充串,字节串。
psLen:填充串的长度,正整数。
S:盐值,字节串。
T:消息鉴别码,字节串。
T1,…,Ti,U1,…,Uc:中间值,字节串。
0x01, 0x02, …, 0x10:值为 0x1, 0x2, …, 0x10 的字节。
⊕:两个字节串按位异或。
|| x ||:求串中字节个数的算子。
||:连接算子。
HMAC:散列消息鉴别码(Hash Message Authentication Code)
KDF:密钥派生函数 (Key Derivation Function)
PBKDF:基于口令的密钥派生函数(Password-Based Key Derivation Function)
PBES:基于口令的加密方案(Password-Based Key Encryption Scheme)
PBMAC:基于口令的消息鉴别码(Password-Based Message Authentication Code)
PRF:伪随机函数 (Pseudo Random Function)

5 OID 定义

本文件对 3 个对象 PBKDF、PBES 和 PBMAC 的标识符进行了定义,见表 1。

表 1 OID 定义

对象标识符 OID	对象标识符定义
1.2.156.10197.6.1.4.1.5	基于口令的密钥派生规范
1.2.156.10197.6.1.4.1.5.1	基于口令的密钥派生函数 PBKDF
1.2.156.10197.6.1.4.1.5.2	基于口令的加密方案 PBES
1.2.156.10197.6.1.4.1.5.3	基于口令的消息鉴别码 PBMAC

6 基于口令的密钥派生函数

密钥派生函数 KDF 通常使用一个口令和其他参数得到派生密钥。

基于口令的密钥派生函数 PBKDF 中，其他两个参数分别是盐值和迭代次数，盐值位不小于 64 比特的随机比特串，迭代次数不小于 1024 次（具体说明见附录 A 的 A.1）。

基于口令的密钥派生函数主要应用于 7 和 8。密钥派生函数（KDF）典型应用一般包括以下步骤：

a） 选择一个盐值 S 和一个迭代次数 c（选择原则见 A.1）；

b） 选择派生密钥的长度 dkLen（字节数）；

c） 将口令 P、盐值 S、迭代次数 c 和密钥长度 dkLen 用于 KDF，产生一个派生密钥；

d） 输出派生密钥。

通过调整盐值 S，可以从一个口令派生出任意数量的密钥，见 A.1 所述。

本文件规定的 PBKDF 使用一个伪随机函数 PRF（见 A.2）来派生密钥，不限定派生密钥的长度。

KDF（P，S，c，dkLen）

选项：	PRF	伪随机函数（hLen 表示伪随机函数输出的字节数）
输入：	P	口令（Password），字节串
	S	盐值（Salt），字节串
	c	迭代次数，正整数
	dkLen	派生密钥的长度（字节数），正整数，最大为 $(2^{32}-1)\times$hLen
输出：	DK	派生密钥，长度为 dkLen 的字节串

步骤：

a） 如果 dkLen $>(2^{32}-1)\times$hLen，输出“派生密钥的长度过长”，停止程序；

b） 将派生密钥的长度按 hLen 个字节进行分块，向下取整，令 n 为分块数。令 r 为最后一块的字节数：

$n=dkLen / hLen$，

$r=dkLen-(n-1)\times hLen$；

c） 将口令 P、盐值 S、迭代次数 c 和块的序号代入到下面定义的函数 F 中，分别计算出派生密钥的各个块：

$T1=F(P, S, c, 1)$，

$T2=F(P, S, c, 2)$，

…

$Tn=F(P, S, c, n)$，

其中，F 定义为伪随机函数 PRF 作用于口令 P、盐值 S 与块序号 i 的连接串的前 c 次迭代结果的异或和：

$F(P, S, C, i) = U1 \oplus U2 \oplus \cdots\cdots \oplus Uc$

其中：

$U1=PRF(P, S \,||\, INT(i))$，

$U2=PRF(P, U1)$，

…

$Uc=PRF(P, Uc-1)$

这里，INT（i）是整数 i 的 4 字节编码，首字节为最高位；

d） 连接所有的块，提取前面的 dkLen 字节作为派生密钥 DK：

$DK=T1 \,||\, T2 \,||\, \cdots\cdots \,||\, Tn\langle 0..r-1\rangle$；

e） 输出派生密钥 DK。

7 基于口令的加密方案

7.1 加密操作

基于口令 P 的加密操作具体包含以下步骤：

a) 选定 KDF 和基础加密方案(见 A.3)；

b) 选择一个盐值 S 和一个迭代次数 c(见第 6 章)；

c) 选择将要在基础加密方案中使用的派生密钥的字节数 dkLen；

d) 将口令 P、盐值 S 和迭代次数 c 代入选定的 KDF 中得到一个 dkLen 字节长的派生密钥 DK：
DK＝KDF (P, S, c, dkLen)；

e) 在基础加密方案中，使用派生密钥 DK 将消息 M 加密为密文 C；(根据基础加密方案的不同，本步骤可能涉及对初始向量和填充串等参数的选择)

f) 输出密文 C。

盐值 S、迭代次数 c、密钥长度 dkLen 和密钥派生函数 KDF 及基础加密方案的标识符可用一个算法标识传送给解密方 (按附录 B 的 B.2)。

7.2 解密操作

基于口令 P 将密文 C 解密为消息 M 的步骤如下：

a) 获取操作中的盐值 S；

b) 获取密钥派生函数中的迭代次数 c；

c) 获取基础加密方案中派生密钥的字节数 dkLen；

d) 将口令 P、盐值 S 和迭代次数 c 代入选定的密钥派生函数(见第 6 章)，得到一个 dkLen 字节长的派生密钥 DK：
DK＝KDF (P, S, c, dkLen)；

e) 在基础加密方案中，用派生密钥 DK 将密文 C 解密为消息 M。如果解密函数输出“解密出错”，则输出“解密出错”并终止程序；

f) 输出解密后的消息 M。

8 基于口令的消息鉴别码

8.1 MAC 的生成

基于口令 P 生成消息 M 的消息鉴别码 T 的具体步骤如下：

a) 选定密钥派生函数 KDF 和基础消息鉴别方案(见 A.4)；

b) 选择一个盐值 S 和一个迭代次数 c(选择原则见 A.1)；

c) 选择基础消息鉴别方案中使用的派生密钥的字节长度 dkLen；

d) 将口令 P、盐值 S 和迭代次数 c 代入选定的密钥派生函数中，得到一个字节长度为 dkLen 的派生密钥 DK：
DK＝KDF (P, S, c, dkLen)；

e) 在基础消息鉴别方案中使用派生密钥 DK 生成消息 M 的消息鉴别码 T；

f) 输出消息鉴别码 T。

盐值 S、迭代次数 c、密钥长度 dkLen 和密钥派生函数 KDF 及基础消息鉴别方案的标识符可用一个算法标识传送给消息验证方(见 A.3)。

实现者应注意基于口令的密钥派生函数与基于口令的消息鉴别码所使用的口令和盐值需要互相独立，不要相互混淆。

8.2 MAC 的验证

基于口令 P 对消息 M 进行处理，验证消息鉴别码 T 的步骤如下：

a) 获取盐值 S 和迭代次数 c；

b) 获取基础消息鉴别方案中派生密钥的字节长度 dkLen；

c) 将口令 P、盐值 S 和迭代次数 c 代入选定的密钥派生函数，得到一个字节长度为 dkLen 的派生密钥 DK：DK = KDF (P, S, c, dkLen)；

d) 将派生密钥 DK 运用到基础消息鉴别方案中对消息 M 进行处理，从而对消息鉴别码 T 进行验证。

如果消息鉴别码通过了验证，则输出“正确”，否则输出“错误”。

附 录 A
（资料性）
辅助技术

A.1 盐值和迭代次数

A.1.1 盐值

由于盐值和迭代次数是本文件的关键技术，本附录对其进行深入的讨论。

在基于口令的密码中，对于给定的口令，盐值常用来与口令一起生成密钥集，并从密钥集中根据盐值随机选取一个密钥。

使用以下的密钥派生函数从密钥集中选择一个密钥：

DK＝KDF（P，S）

其中，DK 是派生密钥，P 是口令，S 是盐值。

这会带来两个好处。

a） 攻击者根据口令字典难于计算出所有可能的密钥。例如，假设盐值的长度为 64 比特，则每个口令能够派生 2^{64} 个密钥。经过一次基于口令的操作后，即使盐值已知，攻击者也只能对口令进行搜索。

b） 同一密钥基本不可能被选到两次。如果盐值的长度为 64 比特，根据“生日悖论”，只有选择了 2^{32} 个密钥后，出现“碰撞”的概率才会显著提高。因此，不必担心在某些加密和消息鉴别应用中同一个密钥会被重复选用。

基于口令的加密方案，当使用口令派生密钥时，加密方只要选择一个很长的、随机性强的盐值，就能满足上述两点。这同样也适用于消息鉴别。但解密方或消息验证方难以确定对方所提供的盐值是否随机。在某种情况下，应用为了利用对同一密钥重复使用所产生的影响，可能使用从另一个基于口令的操作中复制得到的盐值。例如，假设合法的双方交换一条经过 80 比特长的密钥加密的消息，其中的密钥由合法双方共用的口令和同一个盐值派生得到。攻击者就可能将这个盐值作为一个用于生成 40 比特长密钥的盐值提供给一个合法方。如果该合法方公开了用 40 比特长的密钥解密的结果，攻击者就能计算出这个密钥。若这个 40 比特长密钥正好是那个 80 比特长的密钥的前半部分，攻击者就很容易计算出密钥的后半部分。

为了抵抗这种攻击，应对重复使用同一密钥所产生的影响进行仔细地分析，或者将一些能明确区分不同操作的数据加入盐值。例如，可以用一个非随机的字节来说明一个生成密钥的用途：加密、消息鉴别或其他，然后把这个字节包含到盐值中。

基于以上论述，对盐值的选择提出了以下建议。

a） 在基于口令的加密和消息鉴别方案中，对于一个给定的口令，如果不必考虑对派生密钥（或密钥前缀）的重复使用所产生的影响，则盐值可以随机生成，接收方也不必对其进行详细的格式检查。盐值的长度至少应为 8 字节（64 比特）。

b） 如果需要考虑重复使用派生密钥所产生的影响，盐值就应包含一些能明确区分不同操作和不同密钥长度的数据。该数据的长度至少应是 8 字节，而且接收方应对其进行检查或重新生成。例如，盐值可以包含一个附加的非随机字节来说明派生密钥的用途。或者，用一个结构来描述派生密钥的详细信息（如，加密或鉴别技术，派生密钥的序列号等），并将这个结构的编码包含到盐值中。这种附加数据的特定格式由应用程序来决定。

注：推荐使用硬件随机数发生器生成盐值(或盐值的随机部分)。如果无法取得一个(伪)随机数生成器来生成盐值(或盐值的随机部分)，一种替代的方法是将口令和待处理的消息 M 代入到一个基于口令的密钥派生函数中。比如说盐值可以通过计算 S=KDF(P，M)得到。若消息 M 的消息空间(如“Yes” or “No”)较小，由于生成盐值的数量太少，则不建议采用该替代方法。

A.1.2 迭代次数

迭代次数通常被用来增加从口令派生密钥的计算代价，从而增加攻击的难度。从计算角度看，迭代次数 c 通过 $\log_2(c)$位来增加密码的安全强度，以对抗暴力攻击或字典攻击等基于审判的攻击。

为迭代次数选择一个合理的值取决于环境和应用场景。在用户可接受的范围内，迭代次数 c 应尽可能选择大的，派生密钥的时间尽量长的。

在本文件推荐的最小迭代次数是 1024。对生成单个密钥来说，并不会产生明显影响，但对口令的穷举攻击却是严重的负担。对于特别重要的密钥，或者从用户感知角度来说，对系统性能不是很挑剔的，推荐 10000000 的迭代次数。

A.2 伪随机函数

本文件规定的 PBKDF 使用一个 PRF 来派生密钥，PRF 可产生伪随机序列，本附录介绍了 PRF 的一个实例 HMAC-SM3，HMAC 算法按 GB/T 15852.2 执行。

HMAC-SM3 为基于 SM3 密码杂凑算法计算消息鉴别码的函数，可作为一个 PRF 使用。与计算 HMAC 相同，该 PRF 的第一个参数用作 HMAC 的“密钥”，第二个参数用作 HMAC 的“明文”，输出为杂凑值的全部长度。在本文件的 PBKDF 中，“密钥”就是口令，而“明文”就是盐值。HMAC-SM3 的密钥长度可变，输出长度为 32 字节(256 位)。

HMAC-SM3 对密钥长度没有限制，但当密钥长度大于 256 位时，HMAC-SM3 把它杂凑到 256 位。所以，即使很长的派生密钥是由一个密钥经过多个伪随机函数得到，该派生密钥的有效搜索空间最多为 256 位。

对象标识符 id-hmacWithSM3 标识伪随机函数 HMAC-SM3 算法：

id-hmacWithSM3 OBJECT IDENTIFIER ::= {digestAlgorithm(401) 3 1}

在 AlgorithmIdentifier 与该 OID 相关联的参数域应有类型 NULL。该对象标识符使用在对象集 PBKDF-PRFs。

A.3 基础加密方案

本文件规定的 PBES 需要使用一个基础加密方案，本附录介绍了基础加密方案的一个实例 SM4-CBC，SM4 分组密码算法按 GB/T 32907—2016 执行。

基础加密方案 SM4-CBC 的填充方案 SM4-CBC-Pad，如下：

将消息 M 和填充串 PS 连接得到编码消息 EM = M || PS。其中，填充串 PS 由 16-(||M|| mod 16)个值都为 16-(||M|| mod 16)的字节构成，||M||标识消息 M 的字节长度，能满足下面的条件之一：

PS = 0x01 — 如果 ||M|| mod 16=15；

PS = 0x02 0x02 —如果 ||M||mod 16=14；

……

PS = 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 0x10 —如果 ||M||mod 16 = 0。

编码后的消息长度将为 16 的倍数，并能将其恢复为消息 M。

基础加密方案 SM4-CBC 的初始向量，虽然作为明文传送给解密方，但也要保证初始向量是随机

的，初始向量长度为 16 字节。可以输入口令、盐值、迭代次数和限定密钥长度为 16 字节，通过本文件定义的 PBKDF 派生得到密钥，作为初始向量使用。

在本条给出的对象标识符预期在对象集合 PBES-Encs 中应用。

A.4 基础消息鉴别方案

本文件规定的 PBMAC 需要使用一个基础消息鉴别方案，本附录介绍了基础消息鉴别方案的一个实例 HMAC-SM3，HMAC 算法与 GB/T 15852.2 一致，仅杂凑函数使用 SM3 算法，SM3 密码杂凑算法按 GB/T 32905—2016 执行。

HMAC-SM3 是基于 SM3 散列函数的 HMAC 消息鉴别方法。HMAC-SM3 的密钥长度是可变的，输出一个 32 字节(256 位)消息鉴别码。

对象标识符 id-hmacWithSM3 标识 HMAC-SM3 消息鉴别方法。该标识符预期在对象集合 PBMAC-Macs 中应用。商用密码领域相关 OID 定义见表 A.1。

表 A.1 商用密码领域相关 OID 定义

对象标识符	对象标识符定义	备注
1.2.156.10197.1.401.3.1	id-hmacWithSM3	SM3 密码杂凑算法，有密钥使用
1.2.156.10197.1.104.1	SM4-CBC	SM4 分组密码算法 CBC 链接模式

一个证书与密钥封装格式消息鉴别的实例片段如下：

MFgwMDAMBggqgRzPVQGDEQUABCASTp8IJ3X0+oIb4N+wzlKPu1tqyTOLqQ38kw0wm883twQgeXHpagos8kyyRmRoNBGH3w5/fybc+ebylqCQP/Xj3cMCAicQ

解析后的结构为：

SEQUENCE
  SEQUENCE
    SEQUENCE
      OBJECT IDENTIFIER 1.2.156.10197.1.401-杂凑算法
      NULL
    OCTET STRING (32 byte) 124E9F082775F4FA821BE0DFB05……B6AC9338BA90DFC930D3-杂凑值
  OCTET STRING (32 byte) 7971E96A0A2CF24CB2466468341……187D6DCF9E6F296A0903FF-盐值
  INTEGER 10000-迭代次数

附 录 B
（规范性）
ASN.1 语法

B.1 PBKDF 结构

对象标识符 id-PBKDF 标识了 PBKDF(见第 5 章)。

id-PBKDF OBJECT IDENTIFIER ::= {1 2 156 10197 6 1 4 1 5 1}

在算法标识中与这个 OID 相对应的参数域里应包含 PBKDF-params 类型的参数：

```
PBKDF-params ::= SEQUENCE {
    salt CHOICE {
        specified OCTET STRING,
        otherSource AlgorithmIdentifier {{PBKDF-SaltSources}}
    },
    iterationCount          INTEGER (1..MAX),
    dkLen INTEGER (1..MAX) OPTIONAL,
    prf AlgorithmIdentifier {{PBKDF-PRFs}} DEFAULT id-hmacWithSM3
}
```

其中：

PBKDF-SaltSources ALGORITHM-IDENTIFIER ::= { ... }

在算法 ID 或应用程序中，SaltSources 被用来表示盐值是如何生成的。例如，salt-source 可以表示可用 A.1.1 的方法生成盐值：用一个结构来描述派生密钥的详细信息，并用该结构的编码来生成盐值。完整的 ASN.1 结构定义按附录 C 执行。

PBKDF-PRFs ALGORITHM-IDENTIFIER::={{NULL IDENTIFIED BY id-hmacWithSM3}, ... }

id-hmacWithSM3 AlgorithmIdentifier {{PBKDF-PRFs}} ::=

{algorithm id-hmacWithSM3, parameters NULL : NULL}

PBKDF-params 类型组成见表 B.1。

表 B.1 PBKDF-params 数据类型

字段名称	数据类型	含义
salt	Salt	指定盐值，或指定盐值的来源。即一个字节串或一个 OID
iterationCount	INTEGER	迭代次数
dkLen	INTEGER	派生密钥的字节长度，可选域
prf	PRFs	Prf 标识伪随机函数，并且在 PBKDF-PRFs 集合中有一个相应的 OID。本文件中，prf 是 id-hmacWithSM3 或其他由应用定义的 OID 构成

B.2 PBES 结构

对象标识符 id-PBES 标识了 PBES 加密方案(见第 5 章)。

id-PBES OBJECT IDENTIFIER ::= {1 2 156 10197 6 1 4 1 5 2}

在算法标识中与该 OID 对应的参数域应包含 PBES-params 类型：

PBES-params ::= SEQUENCE {

keyDerivationFunc AlgorithmIdentifier {{PBES-KDFs}},

encryptionScheme AlgorithmIdentifier {{PBES-Encs}}

}

其中：

PBES-KDFs ALGORITHM-IDENTIFIER::={{PBKDF-params IDENTIFIED BY id-PBKDF}, ... }

PBES-Encs ALGORITHM-IDENTIFIER ::= {

pbeWithSM3AndSM4-CBC OBJECT IDENTIFIER ::= {1.2.156.10197.6.1.4.1.12.1.1}

}

PBES-params 类型的域有以下含义，见表 B.2。

表 B.2　PBES-params 数据类型

字段名称	数据类型	含义
keyDerivationFunc	KeyDerivationFunc	指定密钥派生函数，是一个在 PBES-KDFs 中定义了 OID 的算法 ID（见 B.1）
encryptionScheme	EncryptionScheme	指定基础加密方案，是一个算法 ID，并且在 PBES-Encs 中有一个 OID，在应用中对其进行定义。A.3 中给出了基础加密方案的实例

B.3　PBMAC 结构

对象标识符 id-PBMAC 标识了 PBMAC 消息鉴别方案（见第 5 章）。

id-PBMAC OBJECT IDENTIFIER ::= {1 2 156 10197 6 1 4 1 5 3}

在算法标识中与该 OID 对应的参数域应包含 PBMAC-params 类型：

PBMAC-params ::= SEQUENCE {

keyDerivationFunc AlgorithmIdentifier {{PBMAC-KDFs}},

messageAuthScheme AlgorithmIdentifier {{PBMAC-MACs}}

}

其中：

PBMAC-KDFs ALGORITHM-IDENTIFIER ::={{PBKDF-params IDENTIFIED BY id-PBKDF}, ... }

PBMAC-MACs ALGORITHM-IDENTIFIER ::= { ... }

PBMAC-params 域的含义见表 B.3。

表 B.3　PBMAC-params 数据类型

字段名称	数据类型	含义
keyDerivationFunc	KeyDerivationFunc	除了 OID 集是 PBMAC-KDFs 外，keyDerivationFunc 域与 PBES-params 中的对应域有相同的含义
messageAuthScheme	MessageAuthScheme	基础消息鉴别方案，是一个算法 ID，并且在 PBMAC-MACs 中有一个 OID，在应用中对其进行定义

附 录 C
（规范性）
ASN.1 结构定义

本附录将前面各条中的 ASN.1 语法在这里作为 ASN.1 结构定义给出。

```
-- ASN.1 Module
-- Jan.2, 2018
DEFINITIONS ::= BEGIN

    -- Basic object identifiers
    cstc            OBJECT IDENTIFIER ::= {iso(1) member-body(2) cn(156) cstc(10197)}
    q5      OBJECT IDENTIFIER ::= { iso(1) member-body(2) cn(156) cstc(10197) ss(6)
bc(1) sm(4) 1 5}

    -- Basic types and classes
    AlgorithmIdentifier { ALGORITHM-IDENTIFIER:InfoObjectSet } ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL
    }

    -- PBKDF
    PBKDFAlgorithms ALGORITHM-IDENTIFIER ::={ {PBKDF-params IDENTIFIED BY
id-PBKDF}, ...}
    id-PBKDF OBJECT IDENTIFIER ::= {q5 1}
    algid-hmacWithSM3 AlgorithmIdentifier {{PBKDF-PRFs}} ::={algorithm id-hmacWithSM3,
parameters NULL : NULL}
    PBKDF-params ::= SEQUENCE {
        salt CHOICE {
        specified           OCTET STRING,
        otherSource     AlgorithmIdentifier {{PBKDF-SaltSources}}
        },
        iterationCount          INTEGER (1..MAX),
        keyLength           INTEGER (1..MAX) OPTIONAL,
        prf                 AlgorithmIdentifier {{PBKDF-PRFs}} DEFAULT algid-hmacWithSM3
    }

    PBKDF-SaltSources   ALGORITHM-IDENTIFIER ::= { ... }
    PBKDF-PRFs          ALGORITHM-IDENTIFIER ::={ {NULL IDENTIFIED BY id-
hmacWithSM3}, ... }

    -- PBES
    PBESAlgorithms ALGORITHM-IDENTIFIER ::={ {PBES-params IDENTIFIED BY id-
```

```
PBES}, ...}
        id-PBES OBJECT IDENTIFIER ::= {q5 2}
        PBES-params ::= SEQUENCE {
            keyDerivationFunc AlgorithmIdentifier {{PBES-KDFs}},
            encryptionScheme AlgorithmIdentifier {{PBES-Encs}}
        }
        PBES-KDFs ALGORITHM-IDENTIFIER ::= { {PBKDF-params IDENTIFIED BY id-
PBKDF}, ... }
        PBES-Encs ALGORITHM-IDENTIFIER ::= { ... }

        -- PBMAC
        PBMACAlgorithms ALGORITHM-IDENTIFIER ::={ {PBMAC-params IDENTIFIED BY
id-PBMAC}, ...}
        id-PBMAC OBJECT IDENTIFIER ::= {q5 3}
        PBMAC-params ::= SEQUENCE {
            keyDerivationFunc AlgorithmIdentifier {{PBMAC-KDFs}},
            messageAuthScheme AlgorithmIdentifier {{PBMAC-MACs}}
        }

        PBMAC-KDFs ALGORITHM-IDENTIFIER ::= { {PBKDF-params IDENTIFIED BY id-
PBKDF}, ... }
        PBMAC-MACs ALGORITHM-IDENTIFIER ::= { ... }

        -- Supporting techniques
        digestAlgorithm          OBJECT IDENTIFIER ::= { iso(1) member-body(2) cn(156)
cstc(10197) algorithm(1) sm3(401)}
        encryptionAlgorithm      OBJECT IDENTIFIER ::= { iso(1) member-body(2) cn(156)
cstc(10197) algorithm(1) sm4(104)}
        SupportingAlgorithms     ALGORITHM-IDENTIFIER ::= {
    {NULL IDENTIFIED BY id-hmacWithSM3}|
    {OCTET STRING (SIZE(8)) IDENTIFIED BY SM4-CBC } , ...
        }
        id-hmacWithSM3     OBJECT IDENTIFIER ::= {digestAlgorithm(401) withKey(2)}
        SM4-CBC          OBJECT IDENTIFIER ::= {encryptionAlgorithm SM4(104) CBC(1)}

        END
```

参 考 文 献

[1] RFC 8018 PKCS #5: Password-Based Cryptography Specification Version 2.1.

[2] D. Balenson. RFC 1423: Privacy Enhancement for Internet Electronic Mail: Part Ⅲ: Algorithms, Modes, and Identifiers. IETF, February 1993.

中华人民共和国密码
行业标准
基于口令的密钥派生规范
GM/T 0091—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 33 千字
2021年4月第一版 2021年4月第一次印刷
*
书号:155066·2-35938 定价 24.00 元

GM/T 0091-2020

码上扫一扫 正版服务到