# 银行业务　密钥管理(零售)
# 第2部分:对称密码及其密钥管理和生命周期

## 1　范围

本部分描述了在零售金融服务环境中,当使用对称密码机制时对称和非对称密钥的保护技术,也描述了与对称密钥相关的生命周期管理。本部分描述的技术符合 GB/T 27909.1 中描述的原则。

本部分描述的技术适用于任何对称密钥管理操作。

本部分所使用的符号见附录 A。

本部分描述的技术中所涉及到的算法应符合国家密码管理部门的有关规定。

## 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 27909.1—2011　银行业务　密钥管理(零售)　第1部分:一般原则(ISO 11568-1:2005,MOD)

GB/T 20547.2—2006　银行业务　安全加密设备(零售)　第2部分:金融交易中设备安全符合性检测清单(ISO 13491-2:2005,MOD)



GB/T 21078.1—2007　银行业务　个人识别码的管理与安全　第1部分:ATM 和 POS 系统中联机 PIN 处理的基本原则和要求(ISO 9564-1:2002,MOD)

GB/T 21079.1　银行业务　安全加密设备(零售)　第1部分:概念、需求和评估方法(GB/T 21079.1—2007,ISO 13491-1:1998,MOD)

ISO/IEC 10116　信息技术　安全技术　n位分组密码的操作方式

ISO 16609:2004　银行业务　使用对称技术的报文鉴别要求

ISO/IEC 18033-1　信息技术　安全技术　加密算法　第1部分:概要

ISO/TR 19038:2005　银行业务和相关金融服务　三重 DEA 操作模式　实施指南

ANSI X9.24 Part 1-2004　零售金融服务对称密钥管理　第1部分:使用对称技术

ANSI X9.65　三重数据加密算法(3-DEA),实施标准

## 3　术语和定义

下列术语和定义适用于本文件。

3.1

**密码　cipher**

在称为密钥的参数控制下,实现密文和明文间转换的一对操作。

注:加密操作将数据(明文)转换成不可读的密文形式;解密操作将密文恢复成明文。

3.2

**计数器 counter**

在两方间使用的累加计数，例如，可用于一个特定的密钥加密密钥控制连续的密钥分发。

3.3

**数据完整性 data integrity**

数据未以非授权的方式改变或破坏的性质。

3.4

**数据密钥 data key**

由随机或伪随机的方法产生的用来对数据加密、解密或鉴别的密钥。

3.5

**双重控制 dual control**

利用两个或更多的独立实体(通常是人)，协同操作以保护敏感功能和信息的过程。单独的实体不能存取和使用这些功能或信息(例如，密码密钥)。

3.6

**异或 exclusive-or**

见 3.15。

3.7

**十六进制数 hexadecimal digit**

用数字 0～9 以及字母 A～F(大写)表示的一个四比特串。

3.8

**密钥组件 key component**

至少两个随机或伪随机过程产生的参数中的一个，它们具有与一个或多个相似的参数结合形成一个密钥的密钥特征(例如，格式、随机性)，例如，通过模 2 加法形成密钥。



3.9

**密钥信封 key mailer**

用于向已获授权人员传送密钥组件的“防篡改”信封。

3.10

**密钥偏移 key offset**

密钥和计数器使用模 2 加法相加的结果。

3.11

**密钥空间 key space**

某一密码的所有可用密钥的集合。

3.12

**密钥转换设备 key transfer device**

提供密钥导入、存储和导出功能的安全密码设备。

3.13

**密钥转换 key transformation**

利用不可逆过程从已存在的密钥导出新的密钥。

3.14

**报文鉴别码(MAC) message authentication code (MAC)**

在发送方和接收方之间传输的报文内的代码。该代码用来验证发送源以及部分或全部报文文本。

注：该代码是按照协定方式计算得出的结果。

3.15

**模 2 加法　modulo-2 addition**

异或　exclusive-or(XOR)；

不带进位的二进制加法，运算规则如下：

0+0=0；

0+1=1；

1+0=1；

1+1=0。

3.16

**n 位分组密码　n-bit block ciper**

明文分组和密文分组在长度上都是 n 位的分组密码算法。

3.17

**公证　notarization**

为了鉴别发送方和最终接收方的身份而变化密钥加密密钥的方法。

3.18

**偏移　offset**

见 3.10 密钥偏移。

3.19

**发送方　originator**

负责生成密码报文的一方。

3.20

**伪随机　pseudo-random**

由算法生成但在统计上是随机的且本质上是不可预测的过程。



3.21

**接收方　recipient**

负责接收密码报文的一方。

3.22

**安全密码设备　secure cryptographic device**

为诸如密钥这样的秘密信息提供安全存储，以及基于这些秘密信息提供安全服务的设备。

3.23

**密钥分割　split knowledge**

两个或更多的实体分别地拥有密钥片断，仅通过单个密钥片段不能合成密钥信息。

## 4　密钥管理技术的一般环境

### 4.1　概述

本章描述密钥管理技术的操作环境并介绍一些通用的基本概念和操作。第五章描述用来提供密钥管理服务的技术，第六章描述密钥生命周期。

### 4.2　安全密码设备的功能

#### 4.2.1　概述

对称分组密码最基本的密码操作是使用所提供的密钥对一个数据分组进行加密或解密。对多分组

数据的操作可使用 ISO/IEC 10116 描述的密码操作模式。在这一层次上，并没有赋予数据任何涵义，也没有赋予密钥任何特定意义。

一般情况下，为了对密钥和其他敏感信息提供所要求的保护，安全密码设备应提供更高层的功能接口。这些功能接口的每项操作包括几个基本的密码操作，这些基本的密码操作使用密钥的某些组合以及由接口或中间结果获得的数据。这种复合的密码操作被称为功能，每一个功能只对适当类型的数据和密钥进行操作。

#### 4.2.2 数据类型

应用层密码系统给数据分配含义，特定含义的数据组成了一种数据类型。通过安全密码设备，不同含义的数据需要以不同的方式进行处理和保护。安全密码设备确保了以恰当的方式处理各种数据类型。

例如，PIN 是一种应保密的数据类型，然而其他的交易数据可构成需要鉴别但不必保密的数据类型。

密钥可被认为是一种特殊的数据类型。安全密码设备确保了密钥只以 4.7.2 中允许的形式存在。

#### 4.2.3 密钥类型

密钥按其操作的数据类型和操作方式分类。安全密码设备确保能够保持密钥分离，这样可使密钥不会与不恰当的数据类型一起使用或以不恰当的方式操作。例如，PIN 加密密钥是一种只用来对 PIN 加密的密钥类型，而密钥加密密钥(KEK)却是只用来加密其他密钥的密钥类型。同样，KEK 也需要分类，以便只对一种类型的密钥进行操作。例如，一种类型的 KEK 可以加密 PIN 加密密钥，而另一种可以加密报文鉴别码(MAC)密钥。

#### 4.2.4 密码功能



由安全密码设备支持的功能直接反映了具体应用的密码要求。它可能包括这些功能：

——加密 PIN；

——验证已加密的 PIN；

——生成 MAC；

——生成被加密的随机密钥。

安全密码设备的设计应保证不能使用单个功能获得未授权的敏感信息，另外，也不能使用组合功能获得这些信息，这样的设计被称为是逻辑安全的。

可能要求一个安全密码设备管理几种类型的密钥。用于这种系统的密钥可通过使用 KEK 以加密的形式存储，从而在密码设备外被安全的持有。KEK 或者存储在密码设备中，或者由更高级别的 KEK 加密。提供密钥分离的一项技术是使用不同类型的 KEK 对不同类型的密钥加密。当使用这项技术并且在一个加密密钥被传输到安全密码设备中时，应使用符合该密钥类型的 KEK 类型将这个密钥解密。如果密钥的类型不正确，即该加密密钥是用与其他密钥类型相应的 KEK 类型进行的加密，那么解密过程就会产生一个无意义的密钥值。

### 4.3 密钥生成

#### 4.3.1 概述

GB/T 27909.1 的密钥管理原则要求密钥应以某种过程生成，该过程应确保密钥的不可预测性或密钥在密钥空间中的等概率性。

为了遵循这个原则，密钥和密钥组件应使用随机或伪随机过程来生成。伪随机密钥的生成过程可

以是不可重复的，也可以是可重复的。

所用的随机或伪随机过程应保证不能够预测或确定某一个特定密钥的概率大于其他可能的密钥。

除了密钥变形、密钥的非可逆转换、由密钥加密的密钥或由密钥导出的密钥之外，一个秘密密钥的泄露不可提供与任何其他秘密密钥相关的有用信息。

#### 4.3.2 不可重复密钥的生成

不可重复密钥的生成过程涉及到不确定的值，如随机数生成器的输出值，或者该过程就是一个伪随机过程。

如下所示，Kx 是生成密钥的伪随机过程的实例，这里的 K 是为生成密钥而保留的秘密密钥，V 是保密的种子值，DT 是在每次密钥生成时更新的日期时间向量：

$Kx = eK(eK(DT) \oplus V)$

并且产生一个新的 V 值，如下所示：

$V = eK(Kx \oplus eK(DT))$

注：该种方法见 ISO 18031。

#### 4.3.3 可重复的密钥生成

使用可重复的过程可很方便地由单个密钥产生一个或多个甚至成千的密钥。这样的过程允许在拥有种子密钥和适当生成数据的情况下，根据要求重新生成任意密钥，并且显著减少需要人工管理、存储或分发的密钥数量。

如果初始密钥在密钥空间（如密钥管理原则所要求的）中是不可预测的，那么该过程生成的密钥也是不可预测的。

该过程可反复使用，如由一个初始密钥生成的密钥随后可用作生成其他密钥的初始密钥。

生成过程应是不可逆的，因此，一个已生成密钥的泄露，不能导致初始密钥和任何其他已生成密钥的泄露。该过程的一个实例是使用初始密钥对非秘密值进行加密。

### 4.4 密钥计算（变形）

使用可逆过程可由单个密钥获得大量密钥。密钥和非秘密值的模二加法即为该过程的一个实例。

密钥计算具有快速和简单的特点，但是以这种方式计算出的密钥一旦泄露会导致原始密钥和所有由它计算得到的其他密钥的泄露。

### 4.5 密钥分级

密钥分级是一个概念性的结构，在这个结构里，某些密钥的机密性依靠其他密钥的机密性。根据定义，密钥分级中某一级密钥的泄露不应导致更高一级密钥的泄露。

密钥加密引入了密钥分级概念，密钥加密密钥（KEK）是比它要加密的密钥更高一级的密钥。最简单的是两级结构，工作密钥由 KEK 来加密，KEK 自身存储在一个密码设备中。在三级结构中，这些 KEK 也通过使用更高一级的 KEK 以加密的形式被管理。这个概念可被扩展到四级或更多级以上。

类似地，当初始密钥或密钥生成密钥（KGK）通过某一过程参与其他密钥的生成时，会产生分级结构，这样 KGK 被认为是比它所生成的密钥更高一级的密钥。

在密钥分级结构中，上级密钥与它们所保护的密钥相比，安全级别应相等或更高。

评估各种密码算法等效强度时应考虑已知的攻击。一般来说，当已知的最快的攻击花费以平均 $2^{s-1}T$ 的时间进行攻击时，就认为该算法能够提供 s 比特的强度，其中 T 是执行一次明文加密并与相应密文值比较的时间。

例如：在 ISO/IEC 10116 中，提出了对 112 位 3-DEA 算法的攻击需要 O(k)空间和 $2^{120-\log k}$ 次操作，

其中 $k$ 是已知明文-密文对的数量。如参考文献[11]中所讨论的，给定 $2^{40}$ 个已知的明文密文对，则会将双密钥(112 位)3-DEA 的强度减小到 80 比特。表 1 中给出了标准发布时推荐的等效密钥长度。评估这些数值时，应考虑密码分析学、因数分解和计算技术的发展。

**表 1 加密算法 等效强度**

| 有效强度 | 对称密码 | RSA | 椭圆曲线 |
|---|---|---|---|
| 80 | 112 位 3-DEA(带 $2^{40}$ 个已知密钥对) | 1024 | 160 |
| 112 | 112 位 3-DEA(不带已知密钥对) | 2048 | 224 |
| | 168 位 3-DEA | | |
| 注：在标准颁布时，零售金融服务环境中的 3-DEA 密钥是用来保护其他密钥的，3-DEA 密钥可被变换，使得不可能收集足够数量的明文-密文对以削弱潜在的密码强度，因此，可以认为 112 位 3-DEA 为 168 位 3-DEA 和 2048 位 RSA 密钥提供了足够的安全保护。 | | | |

### 4.6 密钥生命周期

组成密钥生存期的各种状态统称为密钥的生命周期。密钥应在其生命周期中的任何阶段均受到保护。改变密钥生命周期状态的操作被称为生命周期操作。本节描述了获得一个给定状态或执行一个给定操作的要求。

密钥生命周期由以下三个阶段组成：

a) 使用前：该阶段生成并存储(可选地)密钥；

b) 使用中：该阶段将密钥分发到各个通信方使用；

在通信双方都生成新密钥的过程中，密钥的生成和分发紧密联系在一起；

有些密钥管理方案是为某作业过程中密钥自动变换而设计的；

c) 使用后：该阶段密钥进行归档或终止。

图 1 给出了密钥生命周期示意图，说明了密钥是如何经过的特定操作改变其状态的。

密钥可以被认为是单个对象，其多个实例可以在不同的位置以不同的形式存在。下列操作之间有明显的区分：

——销毁单个密钥的实例；

——从一个特定位置上把密钥删除，即意味着销毁这个密钥在该位置上的所有实例；

——终止一个密钥，即意味着从所有的位置上把这个密钥删除。

### 4.7 密钥存储

#### 4.7.1 概述

密钥安全存储的目标是防止密钥遭受未授权的泄露、修改和/或替换，并且提供密钥分离。

#### 4.7.2 允许的形式

##### 4.7.2.1 概述

密钥只应以如下形式存在：

——明文密钥；

——密钥组件；

——加密的密钥。

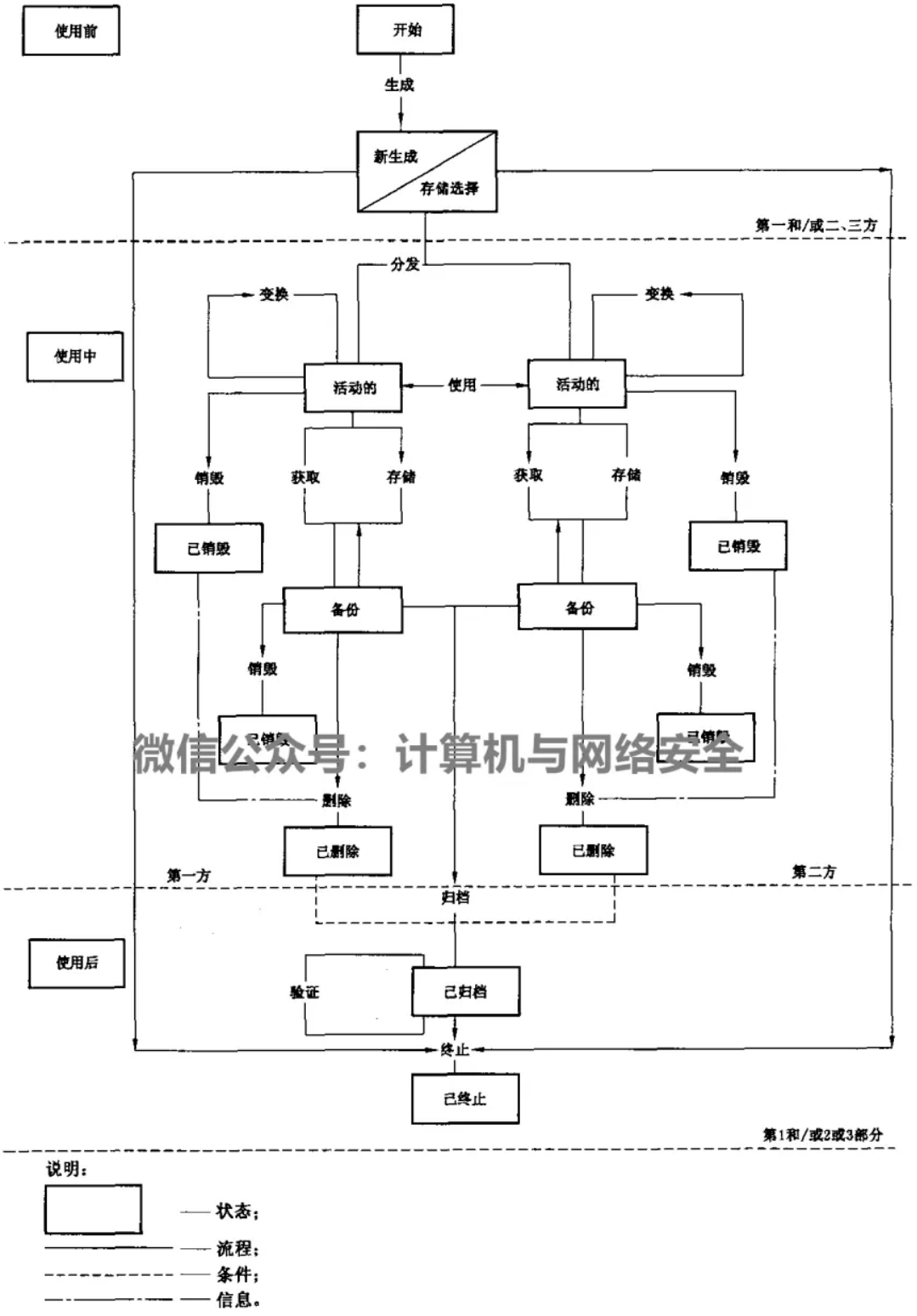




图 1 密钥生命周期示意图

#### 4.7.2.2 明文密钥

其泄露将会对多方造成影响的明文密钥只应存在于安全密码设备中。

泄露只会对一方造成影响的明文密钥只应存在于安全密码设备中，或者存放于由该方或该方代表所操作的物理安全环境中。

#### 4.7.2.3 密钥组件

以至少两个或更多分离的密钥组件形式存在的密钥应通过密钥分割和双重控制技术加以保护。对于基于主机的系统，建议一个密钥至少包含3个组件。

密钥组件应只允许获得信任的某个人或某一组人在必要的最短时段内访问。

如果密钥组件以人们可以理解的形式存在(例如，在密钥信封内以明文印制)，那么这个组件就应只被一个获得授权的人仅在某个时间点获知，并且知晓密钥组件的时间应不长于将密钥组件输入安全密码设备的时间。

授权访问一个密钥组件的人不允许访问此密钥的其他组件。

密钥组件应以某种方式保存，以便可以用很高的概率检测到未经授权的访问。

如果密钥组件以加密形式保存，则应符合加密的密钥的所有要求。

#### 4.7.2.4 加密的密钥

密钥加密密钥对密钥的加密应在安全密码设备中实现。

### 4.7.3 密钥完整性

应使用以下技术保护密钥的完整性：

a) 数字签名；

b) MAC；

c) 密钥分组绑定方法。

### 4.7.4 保护密钥不被替换

应采用下列方式中的一种或几种来防止对存储密钥的未授权的替换：

a) 从物理和流程上阻止对密钥存储区域的非授权访问；

b) 根据密钥的预期使用功能，将密钥加密存储；

c) 确保明文和相应的用密钥加密密钥加密的密文不被同时知晓。

### 4.7.5 密钥分离的规定

为了确保被存储的密钥只用于其预期用途，应采用以下一种或多种方法对密钥进行分离：

a) 按照预期功能从物理上将密钥分离；

b) 用对某种特定类型密钥加密的KEK对密钥进行加密后存储；

c) 在密钥加密存储以前，根据密钥的预期使用功能，修改或追加密钥信息。

## 4.8 备份密钥的重新获取

备份密钥存储了一个密钥的副本，以便密钥在意外损坏但还没有泄露时能够得到恢复。

备份密钥恢复的要求与在4.9中描述的密钥分发和导入的要求相同。

### 4.9 密钥的分发和导入

#### 4.9.1 概述

安全密码设备在导入一个或多个密钥之前应处于物理安全环境中。

密钥在分发和导入时应采用以下一种或多种形式的保护：

a) 明文只出现在密码设备中；

b) 以组件形式存在；

c) 加密。

#### 4.9.2 明文密钥

分发和导入密钥的最低要求如下：

a) 密钥分发过程不应泄露明文密钥的任何一个部分；

b) 只有在保证安全密码设备在此之前没有遭受到可能导致密钥或敏感数据泄露的破坏时，才能将明文密钥导入到该设备里；

c) 只有在保证接口处没有安装可能会泄露传输密钥的窃听装置时，明文密钥才可以在安全密码设备之间传输；

d) 只有对至少两个授权人进行了鉴别后（例如，通过口令的方法），安全密码设备才可以传输明文密钥；

e) 在生成和使用密钥的密码设备之间传输密钥的设备应是安全密码设备。在将密钥导入到目标设备以后，密钥传输设备不应保留任何可能泄露该密钥的信息。

#### 4.9.3 密钥组件

分发和导入密钥组件的最低要求：

a) 密钥组件的分发过程不应将密钥组件的任何部分泄露给未授权的人；

b) 只有保证安全密码设备在此之前没有遭受到可能导致密钥或敏感数据泄露的破坏时，才可将密钥组件导入到该设备里；

c) 只有保证接口处没有安装可能会泄露传输的密钥组件的窃听装置时，密钥组件才可在安全密码设备之间传输；

d) 密钥分发和导入过程应根据双重控制和密钥分割的原则来操作。

#### 4.9.4 加密的密钥

加密的密钥可通过通信信道实现电子化分发和导入。

加密的密钥的分发过程应确保密钥不被替换和修改。

注：完成上述要求的方法见 ISO/IEC 11770-2。

### 4.10 密钥使用

应防止密钥的未授权使用。密钥只应在其预定的位置上用于其预定的功能。然而，密钥的变形可以用于和原始密钥不同的功能。

一个密钥只应用于一种功能。

密钥应存在于保证系统有效运行的最少位置上。不同的交易发起设备应使用不同的密钥。

当确认或怀疑某个密钥泄露时，应停止使用该密钥。

### 4.11 密钥更换

当确认或怀疑密钥泄露时，密钥及其变形就应被更换。如果被怀疑的密钥是一个密钥加密密钥或能够导出其他密钥的根密钥，那么在此密钥级别下的所有密钥也都应被更换。

更换密钥的时间应小于成功实施字典攻击或穷举攻击的时间。该时间将取决于攻击时采用的的技术及手段。

密钥更换应在该密钥存在的所有运行位置上进行。

被更换的密钥不允许再被激活使用。

更换密钥有两种方法：

——分发一个新的密钥；

——对当前的密钥进行不可逆变换。

如果确定或怀疑密钥泄露，那么该密钥应通过分发新密钥进行更换而不是对原始的密钥进行不可逆变换。

密钥更换要求销毁旧密钥。

密钥的变换应防止反向推导，即当前密钥的泄露并不会导致先前使用密钥的泄露。

### 4.12 密钥销毁

如果一个密钥的某个实例不再被激活使用，那么该实例应被销毁。密钥的电子实例可以通过擦除来销毁。然而，信息还可以其他形式存在，以便该密钥随后还可再被恢复并激活使用。

如果一个密码设备永久不再投入使用，那么该设备里存储的所有密钥都应被销毁。

### 4.13 密钥删除

当一个密钥在某运行位置不再需要时，应删除该密钥。

当给定位置上密钥的所有实例都被销毁时，该密钥即被删除。



### 4.14 密钥归档

归档的密钥只应用于验证归档前交易的合法性。在这种验证之后，应销毁实施验证所必需的密钥实例。

归档的密钥不应再次投入使用。

在由归档密钥加密的数据（或密钥）的生命周期内，归档密钥应被安全地存储。

密钥归档应以不会增加使用中密钥的泄露风险的方式归档。

归档密钥应保留到密钥不再具有法律或业务用途时。

### 4.15 密钥终止

当密钥已经从它所存在的所有位置上删除了的时候，密钥即被终止。

随着密钥的终止，不应再存在可能会导致密钥重建的信息。

## 5 提供密钥管理服务的技术

### 5.1 介绍

本章描述的是可单独或组合使用的技术以提供 GB/T 27909.1 中介绍的密钥管理服务。某些技术提供了多种密钥管理服务。第 7 章中给出了密钥管理服务和技术之间的对照参考。

所选择的技术应在安全密码设备中实施（见 GB/T 21079.1 及 GB/T 20547.2），该密码设备确保了

预定的技术及安全目标的实现。

### 5.2 密钥加密

密钥加密是用一个密钥加密另一个密钥的技术，所生成的被加密的密钥可在密码设备保护的环境之外得到安全地管理。用来完成这种加密的密钥称为密钥加密密钥(KEK)。虽然密钥加密确保了密钥的机密性，但为了确保充分的密钥分离，防止密钥替换及确保密钥的完整性，需要其他技术与密钥加密联合使用。

若被加密密钥的长度超过密钥加密密码的分组的长度，那么每个被加密密钥分组应：

a) 具有完整性，每一个密钥分组从被授权生成、传输或存储时起，不能以非授权方式改变；

b) 以特定方式并按照特定的顺序使用；

c) 被视为一个固定的量，其中的每个分组都不能被单独操作，而其他分组保持不变；

d) 不能以任何非授权的目的分开使用。

### 5.3 密钥变形

密钥变形是从单个密钥获得一个密钥集的技术，每一个变形密钥具有各自的密钥类型。

该项技术提供了密钥分离，且不需要管理所需类型中的每一个分离的、不相关的密钥。如图 2 所示，通过使用可重复过程(f)，每一个变形密钥通过原始密钥和非秘密常量集内的一个常数来进行计算。可重复密钥计算过程在 4.3.3 中描述。

每一种密钥类型应对应常量集内某一惟一的常数，该密钥类型对应的密钥使用密钥变形技术由原始密钥计算得出。

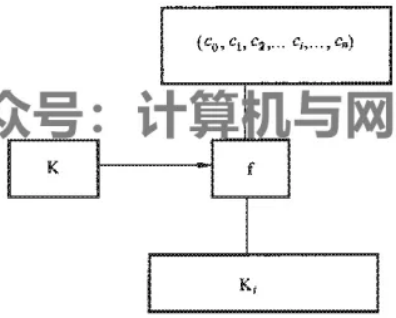




图 2 变形密钥计算

使用可逆过程计算的变形密钥应只存在于包含原始密钥的密码设备中。

密钥变形技术适用于密钥分级结构中的所有级别。用一个密钥可计算出一组不同类型的 KEK，每一个 KEK 可用来加密一种不同类型的密钥。或者，用一个密钥也可生成一组不同类型的工作密钥。

### 5.4 密钥衍生

密钥衍生是一种由一个初始密钥和非秘密可变数据生成(或导出)若干(可能是大量的)密钥的技术。其中每一个生成的密钥又作为另一种安全密码设备的初始密钥(典型的如 POS 终端的 PIN 键盘)。初始密钥被称为“衍生密钥”，同时每一个由它生成的密钥被称为“导出密钥”。密钥衍生通过为每一个密码设备生成(统计上)惟一的密钥来提供密钥分离，而无需管理大量分离的、不相关的密钥。因为当随后需要使用密钥时，它可从衍生密钥和适当的衍生数据中重新导出，所以密钥衍生就消除了将每一个初始密钥存储在收单方或接收节点的必要性。

导出密钥的生成程序利用了一个不可逆过程，如图 3 所示，该过程使用了衍生密钥和可惟一标识目

标密码设备的数据。

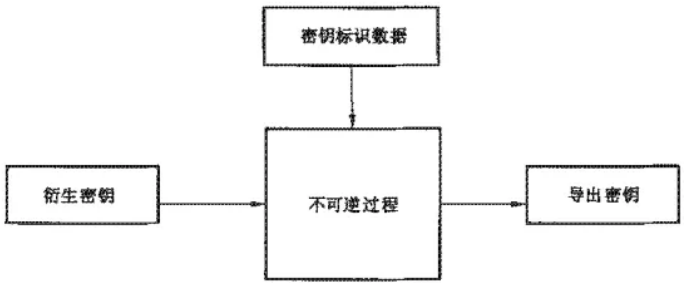


图 3 导出密钥的生成

不可逆过程的使用确保了导出密钥的泄露不会导致衍生密钥和任何其他导出密钥的泄露。然而，衍生密钥的泄露会导致所有由它导出的密钥的泄露。

应用可逆过程的密钥计算（见 4.4）不适合作为密钥衍生的方法。

## 5.5 密钥变换

密钥变换是这样一种技术，即安全密码设备（典型的如 POS 终端的 PIN 键盘）由当前密钥生成一个或多个未来的密钥并擦除当前密钥的所有痕迹，从而实现密钥更换。

密钥变换通过使密码设备在无需密钥分发过程的情况下频繁更换密钥（例如，每一次交易后），从而减轻了密钥泄露的影响。

如图 4 所示，使用当前密钥作为不可逆密钥生成过程中的初始密钥来完成密钥变换。该过程还涉及与实施相关的其他数据，例如，设备或交易相关数据，或密钥更换计数器。



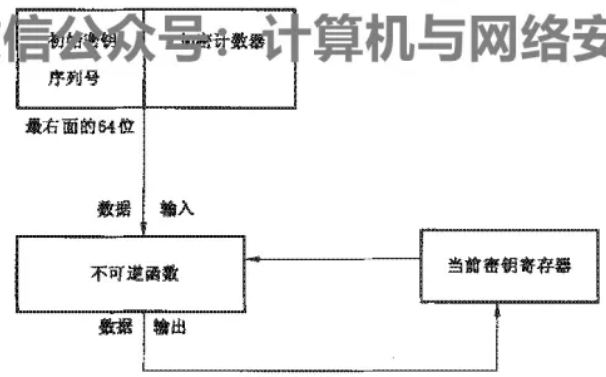


图 4 未来使用的密钥的生成

即使掌握所有曾存在于该设备之外（也不存在于其他密码设备内部）的相关数据，使用不可逆过程也能确保在使用变换密钥的密码设备泄密的情况下，不会导致该设备之前使用的任何密钥的泄露。

配有密钥变换装置的密码通信设备，通过以下方式之一判断该装置在任意时刻使用的密钥：

a) 与装置同步执行密钥变换过程，并且存储生成的密钥供后续使用；

b) 接收包含在该设备传送的交易数据中的密钥更换计数器的当前值，并由计数器和初始密钥来生成当前密钥。这个过程能够实现所有直接从初始密钥到各种当前密钥的密钥变换。特别的，即使密钥更换计数器会增加到一个很大的值（例如，100 万，见 ANSI X9.24 第 1 部分：2004，附录 A），但是它所需的转换次数也很小（例如，10）。

### 5.6 密钥偏移

密钥偏移是每当一个新加密的密钥被传输到接收节点时，由初始密钥计算出一个新 KEK 的技术。该项技术可防止用先前的(但已更换的)密钥替换通信双方交换的当前密钥。

用于记载更换密钥请求的递增计数器，通过一个可重复的过程(例如，模二加法)与初始 KEK 相结合，其生成的密钥为用以加密更换密钥的 KEK，如图 5 所示。

典型地，计数器的当前值与加密的密钥一起被传输到接收节点。

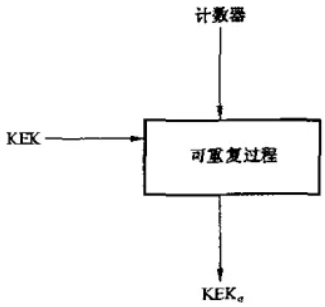


图 5 KEK 偏移量(KEKo)的计算

### 5.7 密钥公证

#### 5.7.1 概述

密钥公证是在密钥加密发生前将通信双方的标识融入 KEK 的一种技术。



密钥公证防止[illegible]。如果[illegible]的加密密钥，则对替换后的密钥的解密会产生一个不正确的结果。

密钥公证是用通信方的标识密封密钥的方法，它通过创建一个公证人密封(NS)实现。一旦公证后，通过下面描述的方法，密钥只能在掌握了用来公证的密钥(KP)及通信方的标识的情况下才能被恢复。密钥加密密钥(KEK)或者数据加密密钥(KD)可以通过使用公证密钥(KN)加密的方式进行公证，该公证密钥(KN)是由 KP 和 NS 进行模 2 加法形成的。

#### 5.7.2 方法

应使用惟一标识符来标识公证过程的每一方。如果有必要，标识符可复制以形成必要的 16 个字节。假设甲方希望给乙方发送一个密钥，设 FM1 为甲方标识符的高 8 个字节，FM2 为低 8 个字节，同样设 TO1 和 TO2 分别为乙方标识符的高 8 个和低 8 个字节。双方都已获知用于完成公证的共享秘密密钥的信息。

中间密钥(KI)是由 TO1 与 FM1 连接后再与 KP 进行模 2 加法形成的。

$KI=KP \oplus (TO1||FM1)$

公证人密封(NS)是由 TO2 和 FM2 与 KI 加密后的结果连接形成的。

$NS=eKI(TO2)||eKI(FM2)$

公证密钥 KN 是由 KP 和 NS 进行模 2 加法形成的。

$KN=KP \oplus NS$

则 KN 可用来公证(通过加密)KD 或者 KEK。

### 5.8 密钥标记

密钥标记是用相关标签来标识密码设备外存在的密钥类型的一种技术。密钥和它的标签以一种可以防止对密钥标签做不可检测的修改的方式绑定在一起。

密钥标记提供密钥分离。它与密钥加密结合使用，并且允许使用单个 KEK 对多密钥类型加密。

密钥标签由一个惟一却任意的常量构成。不同的密钥标签应被分配给每一个要被标记的密钥类型。当一个密钥在安全密码设备中生成时，作为密钥加密过程的一部分，它与和密钥类型相适应的标签绑定在一起，如图 6 所示。带标签的密钥随后可在密码设备外存储或分发。

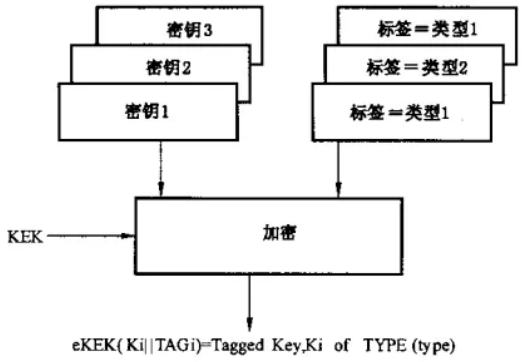


图 6 带标签的密钥生成

当一个带标签的密钥被传输到安全密码设备以用于特定功能时，它在设备内被解密并且密钥标签被恢复和并加以核查，如图 7 所示。如果密钥标签显示了该密钥类型不适合所要求的功能，则该功能应被终止。

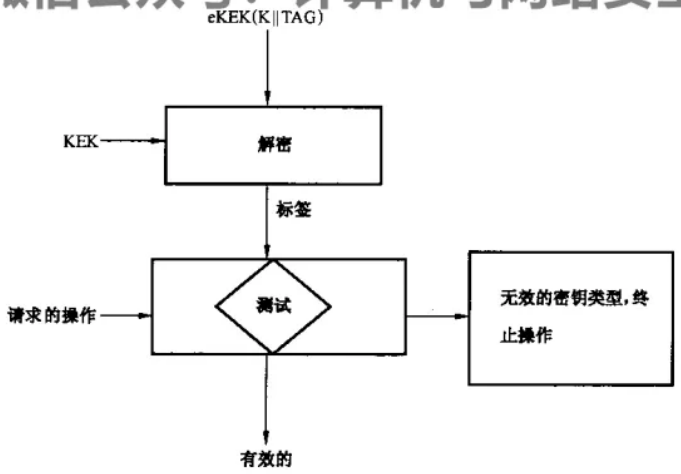


图 7 带标签密钥的使用

密钥和它的标签绑定的方式取决于它们组合后的长度是否超过用于密钥加密的密码分组的长度。如果没有超过，则密钥位和标签位可串联或交叉组合，作为结果的分组被加密。如果超过了，则密钥和标签占用不同的分组来进行加密。在这种情况下，应使用链式加密模型（见 ISO/IEC 10116）和完整性保护技术将密钥和其标签绑定在一起。

### 5.9 密钥验证

密钥验证码(KVC)是一个在密码技术上与密钥和一些附加的非秘密信息相关的值。当与适当的完整性保证机制一起使用时，KVC 可保证满足以下一种或多种情况：

a) 密钥已被正确地输入密码设备中；

b) 密钥通过通信渠道被正确地接收；

c) 密钥未被改变；

d) 密钥变换或密钥衍生的实例保持同步。

KVC 通常用于查找网络中密钥被修改或破坏的位置。任何没通过 KVC 测试的密钥都应被怀疑已遭到破坏或泄露。

一般的 KVC 实施实例(见图 8)是用受到怀疑的密钥对一个不变的公开的且非秘密的常量(例如，16 位的 16 进制值)进行加密，然后，截取产生的密文(例如，6 位 16 进制值)。

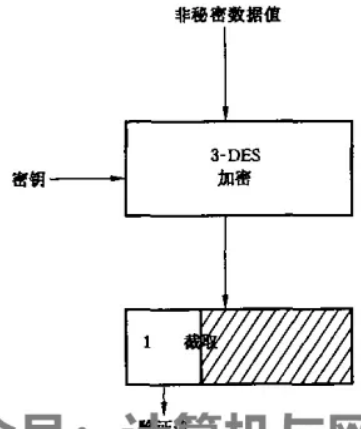




图 8 KVC 功能实例

KVC 通过一种确保完整性的方式(电子的或者其他方法)被传输到某个进行验证的位置，然后再输入到密码处理器中。需要验证的密钥可通过相同的或不同的路径被传送到该位置。对接收到的密钥执行同样的密码功能，并且将它的输出与密钥验证码进行比较。

应由生成 KVC 的密码设备来提供已知的非秘密值，并截取 KVC(例如，6 位数)，否则，产生 KVC 的能力可能被误用来加密已知的明文。

KVC 应只通过完整的密钥来计算得出。

### 5.10 密钥识别

密钥识别可使交易接收者能确定与交易有关的相应的密钥。有两种密钥识别的方法，即显式及隐式。

显式密钥识别是指在交易报文中，包含用于加密或鉴别报文中数据的密钥的信息。当许多具有惟一密钥的密码设备与单个设备通讯时，该技术尤为有用。这是因为它可使该设备确定对接收的任一给定报文使用哪一个密钥。

使用隐式密钥识别是从其他报文相关信息来确定报文使用的密钥，例如，终端标识符或接收报文的通信线路。

### 5.11 控制和审计

阻止安全泄露并非总是可能的或可行的。然而，如果能检测到泄露，则往往可以避免其影响。尤为

重要的是：

——检测密钥的泄露；

——检测合法密钥被替换成已泄露的密钥。

密钥泄露可通过以下方法来检测：

——对管理密钥和/或密码设备的人实施审计和控制，来检测可能引起密钥泄露的这些人之间的勾结；

——通过对传送未加密密钥或密钥组件的接口进行周期性的检查和控制来检测可能导致所传送密钥要素泄露的“利用缺陷”或“窃听装置”；

——通过对包含密钥的密码设备进行控制和审计来检测任何丢失的或被窃的设备。

如果已知或怀疑密码设备丢失或被窃，则认为该设备中包含的密钥已经泄露。

通过以下方法可检测密钥替换（使用泄露密钥的替换）：

a) 当使用显示密钥识别时，验证一个刚刚收到的密钥标识符是否具有所有期望的值；

b) 维护已知或怀疑泄露的密钥的“失效文件”，并且在恰当的场合对认为有效的密钥进行审计以确保没有任何一个被列在失效文件中；当使用显示密钥识别时，已泄露密钥的密钥标识符可用来识别属于“失效文件”条目中的密钥。否则可用密钥本身的加密版来识别“失效文件”条目中泄露的密钥；

c) 对认为有效的密钥进行周期性的审计以确保任何一个密钥只能与一个密码设备相联系（审计可使用加密的密钥或密钥标识符）。此方法可检测到对已泄露的密钥进行的复制。

当执行逆操作（例如，解密）的相应密码设备产生一个混乱或其他非法结果时，则可检测到相关密码设备（例如，加密）中已经发生未授权密钥的修改、删除和插入以及密钥替换的情况。

以上审计和控制措施也可用来防止一些安全泄露。更进一步，对密码设备的功能性审计还能确保设备只可执行授权的功能，从而防止密钥的误用。

### 5.12 密钥完整性



为满足 5.2 中所列出的密钥完整性要求，应采用以密码方式连接所有密钥位的技术。

确保加密密钥完整性的方法的示例见 ISO/TR 19038。

如果满足 5.2 的要求，也可使用其他方法。

## 6 对称密钥生命周期

### 6.1 概述

为防止或检测密钥泄露，确保其完整性，在密钥整个生命周期中，用于存储和管理密钥的设备和程序应受到控制和审计。

以下章节详细描述了生命周期各个阶段的不同要求。

### 6.2 密钥生成

密钥和密钥组件应通过 4.3 中描述的方式之一生成：

a) 不可重复的密钥生成；

1) 随机过程；

2) 伪随机过程。

b) 可重复的密钥生成；

1) 密钥变换；

2) 密钥衍生。

### 6.3 密钥存储

#### 6.3.1 概述

通过采用 4.7.2 中描述的密码安全存储方式可保护密钥不会在未授权的情况下泄露或替换。

应按照 6.3.3 中描述的过程更换已确认、怀疑或预计已被非法替换的密钥。

#### 6.3.2 允许的形式

##### 6.3.2.1 概述

以下描述了每一种允许形式的安全密钥的存储方法。

##### 6.3.2.2 明文密钥

明文密钥只能存储在符合 GB/T 21079.1 和 GB/T 20547.2 中规定要求的安全密码设备中。

##### 6.3.2.3 密钥组件

密钥组件应通过特定的密钥信封或密钥传输设备传送给被授权人。密钥信封的印制，应保证信封在开启后才能看到密钥组件。信封应只显示将密钥信封递交给授权人所必需的最少信息。密钥信封的结构应使得意外的或欺骗性的开启易于被接收方发现。如果出现这种情况，密钥组件就不应再使用。

当密钥组件输入安全密码设备以后，密钥信封应加以销毁或密封在另一个“防篡改”的密钥信封里，以备将来可能的使用。

应通过足够的访问控制（例如，口令）保护存储在密钥传输设备里的密钥组件。

##### 6.3.2.4 加密的密钥

密钥的加密应遵循 5.2 的具体规定。

#### 6.3.3 密钥替换——修正

如果根据攻击者已经获得的信息，可以确认、怀疑或预计已经发生了未经授权的密钥替换，则应遵循下列步骤进行密钥更换：

a) 擦除任何已经确认被替代的存储密钥的加密版本，确认现存的所有加密的密钥是否合法。如果有不合法的密钥，则应被删除；
b) 由某个新的密钥加密密钥对合法存储的加密的密钥重新加密；
c) 将旧的密钥加密密钥从所有运行位置上删除。

### 6.4 备份密钥的恢复

备份密钥的恢复应采用密钥分发和导入的方式来完成。

### 6.5 密钥分发和导入

#### 6.5.1 概述

本条描述了满足 4.9 中规定要求的每一种允许密钥形式的分发和导入的实现技术。

可以通过下述技术将密钥分发并导入到安全密码设备里。

a) 手工，例如，密钥组件经键盘导入；
b) 电子直接导入，例如，从生成设备或密钥传输设备通过电缆直接导入密钥；
c) 网络分发和导入，如通过网络实现的远程的密钥传送。表 2 中用对钩指出了将不同密钥形式的密钥导入到安全密码设备里所允许的技术。

表 2 允许的密钥分发和导入技术

| 密钥形式 | 人工 | 电子 | |
|---|---|---|---|
| | | 直接 | 网络 |
| 明文密钥 | | √ | |
| 密钥组件 | √ | √ | |
| 加密的 | √ | √ | √ |

### 6.5.2 明文密钥

当某个明文密钥在两个安全密码设备之间以电子形式直接进行传输时，应确保这些设备之间是直连的（没有中间分接装置），并且应在持续的双重控制下操作。

当使用显式密钥识别时，密钥标识符（非机密的）应和密钥（机密的）同时传输。

当使用密钥传输设备时，密钥（及其标识符，如果使用显式密钥识别的话）从源安全密码设备传输到密钥传输设备里。该便携设备就可以被物理运输到真正使用这个密钥的安全密码设备的位置。然后，密钥及其标识符应从密钥传输设备传输到密钥使用设备里。如果密钥使用设备是一个交易发起设备，那么密钥应立即从密钥传输设备里擦除。明文密钥的传输应按照电子直接导入的具体规定实现。

密钥传输设备可接受多个互不相同的密钥（如果可能的话，每一个都有其标识符），从而可用于给多个远程的密码设备提供初始密钥。

密钥传输设备的另一种做法是采用一套密钥生成机制，在与单一中央密码设备通信的多个远程密码设备之间建立惟一的密码关系。在初始化过程中，密钥传输设备连接到中央密码设备接收初始密钥，然后密钥传输设备应使用该密钥的不可逆衍生方法为远程密码设备生成惟一密钥，并以物理形式直接运输到这些远程密码设备。在生成和导入密钥后，密钥生成设备不应保留任何可能导致密钥泄露的信息。



如果有密钥验证码，应在密钥导入后对其加以验证。

### 6.5.3 密钥组件

当使用该技术时，构成密钥的组件应手工输入到设备里。当密钥组件以可读的形式分发时，每一个密钥组件都应通过在开启前不会泄露密钥组件值的密钥信封进行分发。

在输入密钥组件之前，应检查密钥信封有无被篡改的迹象。如果组件之一被篡改，这一套密钥组件就不应被使用，且应遵循 GB/T 21078.1 中说明的程序将其销毁。

密钥组件应由密钥组件的每一个持有者单独输入并应运用 5.9 中描述的密钥验证方法来验证密钥组件的输入是否正确。当最后一个组件输入以后，密码设备将按照要求构造新的密钥。如果提供了利用 5.9 中描述的方法生成的密钥验证码，则应用该值验证密钥构造是否正确。

### 6.5.4 加密的密钥

在网络中分发加密的密钥可能需要传送专门的密码服务报文，发起密钥变化的一方通过这种方法通知其他各方。应注意避免密码不同步的问题。

一个密钥加密密钥的安全级别应至少与它保护的密钥持平或更强。

注：如 4.5 中注释，在标准发布时，零售金融服务环境的 3-DEA 密钥被用于保护其他密钥，3-DEA 密钥可被更换，这样就不可能收集足够数量的明文/密文对以削弱潜在的密码强度。可以认为 112 位 3-DEA 为 168 位 3-DEA 和 2048 位 RSA 密钥提供了足够的安全保护，见表 1。

为防止密钥在操作过程中被误用，应使用本部分中描述的技术来防止密钥替换和修改。

被加密密钥的发送者和接收者都需要获知用于加密其他密钥的密钥。

### 6.6 密钥使用

4.7.4 包含了用于获得恰当的密钥分离的技术列表。

一个密钥最多只应被两个通信方使用。

应防止继续使用被怀疑泄露的密钥。这可能需要：

a) 从所有的运行位置上删除这个密钥；

b) 阻断用于导出该密钥的方法。

### 6.7 密钥更换

密钥更换可以通过下列任何一种方法进行：

a) 重复适当的密钥生成、分发和导入过程；

b) 将由密钥加密密钥加密的工作密钥传输到安全密码设备中，该密钥加密密钥此前已经由初始密钥分发过程导入到该设备中；

c) 在设备里生成一个新的交易密钥，该密钥由前一密钥的不可逆变换得出。该技术的具体实例见 5.5；

1) 一个可能的目标是自动地为每笔交易生成一个惟一的密钥。交易密钥或生成交易密钥所需的数据只能在单一的交易过程中或两个连续的交易之间存在；

2) 当采用“每笔交易一个密钥”技术时，在一个交易结束后，无法从包含在安全密码设备里的信息里确定任何先前使用的交易密钥。

d) 作为固定密钥和交易数据的函数，通过在安全密码设备里计算一个新交易密钥的方法隐式分发新密钥。

如果进行密钥更换是为了防止对加密数据的穷举攻击，则 4 种方法均可使用。



如果进行密钥更换是为了减小未来安全密码设备物理泄露造成的影响，则应采用方法 a)或 c)。

如果进行密钥更换是因为已知的或怀疑受到的泄露，则应采用方法 a)或 b)。

### 6.8 密钥销毁、删除、归档和终止

#### 6.8.1 密钥擦除技术

密钥的擦除可通过将一个全新的，或一个不包含被擦除的密钥中的信息的密钥值重新写入到已暴露的密钥存储器当中；或是按照 GB/T 21078.1 中的规定销毁密钥存储介质来实现。

当要删除一个可读的密钥组件时，记录该密钥组件的存储介质应当用焚烧或与其等效的方法销毁，也可按照 GB/T 21078.1 中的规定的方法进行销毁。

#### 6.8.2 密钥销毁

密钥销毁的实施见 6.8.1，密钥销毁针对单个密钥实例进行操作。

#### 6.8.3 密钥删除

密钥删除的实施见 6.8.1，密钥删除针对给定位置的的所有密钥实例进行操作。

#### 6.8.4 密钥归档

##### 6.8.4.1 概述

密钥可以通过 4.7 中描述的任何一种允许的存储形式进行归档：

a) 在安全密码设备内部以明文形式；
b) 至少两种分离的密钥组件形式；
c) 使用密钥加密密钥加密的形式。

#### 6.8.4.2 明文密钥

载有归档密钥的安全密码设备，应只允许这些密钥用于验证归档之前发生交易的合法性。

归档密钥和活动密钥之间的分离或者活动密钥免于被归档密钥所替代，可以通过采用 4.7.4 中描述的相应技术来实现。

#### 6.8.4.3 密钥组件

对归档的密钥组件应建立一套程序以实施足够的访问控制。

归档的密钥要素应与使用的密钥要素分开存储。

#### 6.8.4.4 加密的密钥

在归档过程中应考虑密钥管理方案的分级。这意味着用于归档密钥加密密钥的密钥不应用于归档其他级别的明文密钥。

用于归档过程的密钥加密密钥不应与任何用于加密活动密钥的密钥加密密钥相同。

归档的密钥要素应与使用中的密钥要素分开存储。

### 6.8.5 密钥终止

依据 6.8.1 对该密钥的所有实例在所有位置实施密钥终止。

## 7 密钥管理服务的对照参考



表 3 为 GB/T 27909.1 中定义的安全服务和第 5 章中详述的技术之间的对照参考。然而，应注意服务、技术的有效性将最终依赖于具体用户的实施。

**表 3 密钥管理服务的对照参考**

| 服务技术 | 分离 | 替换的防止 | 识别 | 同步(可用性) | 完整性 | 机密性 | 泄露的检测 |
|---|---|---|---|---|---|---|---|
| 加密 | | | | | | 5.2 | |
| 变形 | 5.3 | | | | | | |
| 密钥衍生 | 5.4 | 5.4 | | 5.4 | | | |
| 密钥变换 | 5.5 | 5.5 | | 5.5 | | | |
| 偏移 | | 5.6 | | | | | |
| 公证 | | 5.7 | | | | | |
| 标记 | 5.8 | | | | | | |
| 密钥验证 | | 5.9 | | 5.9 | 5.9 | | |
| 密钥识别 | | | 5.10 | | | | 5.10 |
| 审计和控制 | | | | | | | 5.11 |
| 密钥完整性 | | | | | 5.12 | | |

# 附 录 A
（规范性附录）
本部分使用的符号

## A.1 操作符

操作符可表示如下：

e——加密；

d——解密；

‖——连接；

⊕——模 2 加法。

## A.2 密钥的后缀字母

后缀字母定义如下：

o——有密钥偏移的密钥；

S——正被发送的密钥；

R——正被接收的密钥。

如果不用作后缀，这些字母可用于其他任何目的。

# 附 录 B
（规范性附录）
缩 略 语

表 B.1 中的缩略语适用于本部分。

表 B.1 缩略语表

| 缩略语 | 含 义 | 描 述 |
|---|---|---|
| DEA | 数据加密算法 | 见 ANSI X9.65 |
| f | 函数 | 数据、密钥和密码操作的交互作用 |
| K | 密钥 | 与算法结合使用以实现验证、鉴别、加密、解密的目的的参数 |
| KD | 数据密钥 | 用来加密/解密数据的密钥 |
| KEK | 密钥加密密钥 | 用于对密钥加密和解密的密钥 |
| KGK | 密钥生成密钥 | 在生成其他密钥时，用来确保比特流不可预测的密钥（也称为“初始密钥”） |
| KVC | 密钥验证码 | 加密一个值为随后通过比较来验证一个密钥而产生的代码 |
| MAC | 报文鉴别码 | 如 ISO 16609 中定义 |
| PIN | 个人识别码 | 一个与主账号(PAN)或者卡号关联在一起作为鉴别卡持有者的验证参数的秘密数值 |
| T | 时间 | 用做过程或函数的可变输入的时间参数 |
| 3-DEA | 三重 DEA | 如 ISO/IEC 18033-3 中定义 |
| XOR | 模 2 加法 | 不带进位的二进制加法 |