ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 17901.1—2020
代替 GB/T 17901.1—1999

# 信息技术　安全技术　密钥管理
# 第1部分：框架

**Information technology—Security techniques—Key management—Part 1：Framework**

（ISO/IEC 11770-1：2010，MOD）

2020-03-06 发布　　2020-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

# 前　言

GB/T 17901《信息技术　安全技术　密钥管理》拟分为6个部分：

——第1部分：框架；

——第2部分：采用对称技术的机制；

——第3部分：采用非对称技术的机制；

——第4部分：基于弱秘密的机制；

——第5部分：群组密钥管理；

——第6部分：密钥派生。

本部分为GB/T 17901的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 17901.1—1999《信息技术　安全技术　密钥管理　第1部分：框架》，与GB/T 17901.1—1999相比，主要技术变化如下：

——在规范性引用文件中增加了新的引用文件(见第2章)；

——删除了“解密、加密、密钥确认、密钥控制、密钥分发中心(KDC)、密钥材料、密钥管理、密钥转换中心(KTC)、公开密钥信息、随机数、顺序号”的术语和定义，增加了“杂凑函数、密钥派生函数、密钥建立、密钥权标、消息鉴别码、签名系统”的术语和定义(见第3章，1999年版的第3章)；

——增加了第4章“符号和缩略语”(见第4章)；

——将1999年版的第4章“密钥管理综述”修改为第5章“密钥管理的一般模型”，删除了1999年版的4.1.2，增加了5.1、5.3.1，并对部分内容进行了修改(见第5章，1999年版的第4章)；

——将1999年版的第6章“密钥分发概念模型”修改为第7章“两实体间密钥分发的概念模型”，增加了7.1，并对部分内容进行了修改(见第7章，1999年版的第6章)；

——删除了1999年版的附录D，相关内容与现有国家标准和密码行业标准保持一致。

本部分使用重新起草法修改采用ISO/IEC 11770-1:2010《信息技术　安全技术　密钥管理　第1部分：框架》。

本部分与ISO/IEC 11770-1:2010相比在结构上有调整，增加了第2章，后续条款号依次改变，调整4.2.3～4.2.5为5.2.2、5.2.3.1和5.2.3.2，调整附录B为附录C，附录C为附录B。

本部分与ISO/IEC 11770-1:2010的技术性差异及其原因如下：

——增加了第2章规范性引用文件(见第2章)；

——删除了部分术语和定义(见ISO/IEC 11770-1:2010的第2章)；

——删除了“CA”和“RA”的符号(见ISO/IEC 11770-1:2010的3.1)；

——在第5章明确了“应采用国家密码管理部门认可的密码算法”，并将ISO/IEC 11770-1:2010所引用的密码算法标准修改为引用我国对应的密码算法标准，以便于使用(见第5章)。

本部分还做了下列编辑性修改：

——删除ISO/IEC 11770-1:2010的资料性附录D，相关内容与现有国家标准和密码行业标准保持一致。

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这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、

中关村无线网络安全产业联盟、国家密码管理局商用密码检测中心、北京大学深圳研究生院、中国电子科技集团公司第三十研究所、国家无线电监测中心检测中心、中国电子技术标准化研究院、中国通用技术研究院、中国网络安全审查技术与认证中心、天津市无线电监测站、北京计算机技术及应用研究所、天津市电子机电产品检测中心、重庆邮电大学。

本部分主要起草人：杜志强、李琴、郎元、朱跃生、刘科伟、周国良、陶洪波、王月辉、铁满霞、张变玲、彭潇、李冰、许玉娜、黄振海、布宁、张璐璐、于光明、颜湘、张国强、刘景莉、李冬、商钧、赵慧、王莹、朱正美、高德龙、郑骊、熊克琦、黄奎刚、龙昭华、吴冬宇。

本部分所代替标准的历次版本发布情况为：

——GB/T 17901.1—1999。

# 引　言

在信息技术中，采用密码机制保护数据不被非法窃取或篡改、实现实体鉴别和抗抵赖的需求与日俱增。这些机制的安全性和可靠性直接取决于对密钥的管理和保护。如果密钥管理有薄弱环节，那么将使其声称的密码功能都失效，因此安全管理密钥对于将密码功能集成到系统中至关重要。密钥管理的目的是提供用于对称或非对称密码机制中的密钥处理程序。

本部分修改采用 ISO/IEC 11770-1:2010《信息技术　安全技术　密钥管理　第1部分：框架》，适用于对通信密钥的管理。ISO/IEC 11770 定义了密钥管理的一般模型，它不依赖使用的特定密码算法。但是某些密钥分发机制取决于特定算法的特性，例如非对称算法特性。

如果密钥管理中需要使用抗抵赖功能，参见 GB/T 17903。

本部分描述了自动和人工两种密钥管理方法，包括数据元素框架以及用于获取密钥管理服务的操作流程，但对协议交换所需的细节不作详细说明。

同其他安全服务一样，密钥管理只在所定义的安全策略中提供密钥管理服务，但安全策略的定义超出本部分的范围。

密钥管理的根本问题是要参与各方确认密钥材料，向直接和间接用户保证其来源、完整性、即时性以及(秘密密钥情形下)保密性。密钥管理包括根据某一安全策略生成、存储、分发、删除和归档密钥(GB/T 9387.2—1995)等功能。

# 信息技术　安全技术　密钥管理
# 第1部分：框架

## 1　范围

GB/T 17901的本部分包含以下内容：

a）　建立密钥管理机制的通用模型；

b）　定义对GB/T 17901通用的密钥管理的基本概念；

c）　定义密钥管理服务的特征；

d）　规定对密钥在其生存周期内进行管理的通用原则；

e）　建立通信密钥分发的概念模型。

本部分适用于建立密钥管理模型和设计密钥管理方法。

## 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 15843(所有部分)　信息技术　安全技术　实体鉴别[ISO/IEC 9798(所有部分)]

GB/T 17903.2　信息技术　安全技术　抗抵赖　第2部分：采用对称技术的机制(GB/T 17903.2—2008，ISO/IEC 13888-2：1998，IDT)

GB/T 18794.1　信息技术　开放系统互连　开放系统安全框架　第1部分：概述(GB/T 18794.1—2002，idt ISO/IEC 10181-1：1996)

GB/T 32907　信息安全技术　SM4分组密码算法

GB/T 32918(所有部分)　信息安全技术　SM2椭圆曲线公钥密码算法

GB/T 37092—2018　信息安全技术　密码模块安全要求

ISO/IEC 18014(所有部分)　信息技术　安全技术　时间戳服务(Information technology—Security techniques—Time-stamping services)

ISO/IEC 18031　信息技术　安全技术　随机数生成(Information technology—Security techniques—Random bit generation)

## 3　术语和定义

下列术语和定义适用于本文件。

3.1

**非对称密码技术　asymmetric cryptographic technique**

采用两种相关的变换，由公钥定义的公开变换和由私钥定义的私有变换的密码技术。

注：这两个变换具有如下特性，即对给定的公钥导出私钥在计算上是不可行的。

3.2

**非对称密钥对　asymmetric key pair**

一对相关的密钥，其中私有密钥规定私有变换，公开密钥规定公开变换。

[ISO/IEC 11770-3：2008，定义3.3]

3.3

**私钥　private key**

在某一实体的非对称密钥对中，只由该实体使用的密钥。

3.4

**公钥　public key**

在某一实体的非对称密钥对中，能够公开的密钥。

3.5

**证书认证机构　certificate authority**

负责生成、签发和管理证书的、受用户信任的权威机构。

注：用户可以选择该机构为其创建特定密钥。

3.6

**数字签名　digital signature**

附加在数据单元上的数据，或是对数据单元所做的密码变换。

注：这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

3.7

**杂凑函数　hash function**

将比特串映射为固定长度的比特串的函数。

注：该函数满足下列两特性：

a）　对于给定输出，找出映射为该输出的输入，在计算上是不可行的。

b）　对于给定输入，找出映射为同一输出的第二个输入，在计算上是不可行的。

3.8

**密钥　key**

一种用于控制密码变换操作（例如加密、解密、密码校验函数计算、签名生成或签名验证）的符号序列。

3.9

**密钥协商　key agreement**

在实体之间建立一个共享的秘密密钥的过程，其中任何实体都不能预先确定该密钥的值。

3.10

**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，生成一个或多个共享秘密密钥的函数。

3.11

**密钥建立　key establishment**

为一个或多个实体生成一个可用的、共享的秘密密钥的过程，包括密钥协商、密钥传送等。

[ISO/IEC 11770-3:2008，定义 3.22]

3.12

**密钥权标　key token**

在密钥建立机制执行期间，一个实体向另一个实体发送密钥建立的消息。

3.13

**消息鉴别码　message authentication code**

消息鉴别码算法输出的比特串。

3.14

**原发鉴别　origin authentication**

对接收到的数据源与声称一致的确认。

3.15

**公钥证书　public key certificate**

由证书认证机构对一个实体签发并不可伪造的、有关其公钥信息的数据结构。

3.16

**秘密密钥　secret key**

用于对称密码技术中的一种密钥，并仅由一组规定实体所使用。

3.17

**签名系统　signature system**

基于非对称密码技术，其私有密钥用于签署变换，其公开密钥用于验证变换的系统。

3.18

**时间戳　time stamp**

根据公共的时间基准来表示某一时间点的时变参数。

3.19

**时变参数　time variant parameter**

用于验证数据并非重用的数据项，例如一个随机数、一个序列号或者时间戳。

注：在保持实体间时钟同步的情况下可使用时间戳。在维持和验证实体间序列号计数器同步的情况下可使用序列号。

3.20

**可信第三方　trusted third party**

在同安全相关的活动方面，被其他实体信任的安全机构或其代理。

## 4　符号和缩略语

### 4.1　符号

下列符号适用于本文件。

A，B：实体的可区分标示符。

DIR：目录维护认证机构。

KDC：密钥分发中心。

KG：密钥生成器。

KTC：密钥交换中心。

$S_A$：实体 A 的签名密钥。

$V_A$：实体 A 的验证密钥。

X：认证机构的可区分标识符。

### 4.2　缩略语

下列缩略语适用于本文件。

CA：认证机构(Certification Authority)

MAC：消息鉴别码(Message Authentication Code)

PIN：个人标识号(Personal Identification Number)

RA：注册机构(Registration Authority)

TTP:可信第三方(Trusted Third Party)

TVP:时变参数(Time Variant Parameter)

## 5 密钥管理的一般模型

### 5.1 概述

密钥管理的目标是安全地管理和使用密钥服务,密钥保护极其重要。

密钥管理过程取决于基本的密码机制、密钥的预期用途以及使用的安全策略。密钥管理还包括在密码设备中执行的功能。

凡涉及采用密码技术解决机密性、完整性、真实性、抗抵赖需求的应遵循密码相关国家标准和行业标准。

### 5.2 密钥保护

#### 5.2.1 密钥管理的基本概念

密钥在所有依赖于密码技术的安全系统中都是关键的部分。对密钥的适当保护取决于许多因素,如密钥的应用类型、面临的威胁、密钥可能出现的不同状态等,应保护密钥不被泄露、修改、销毁和重用,这取决于所使用的密码技术。密钥可能受到的威胁的示例参见附录 A,实际使用时可能需要多个保护技术抵抗这些威胁。密钥的有效性应在时间和使用次数上受限制,这些限制取决于进行密钥恢复攻击所需的时间和数据量,以及随着时间推移获取到的信息的价值。用于派生密钥的原始密钥比生成的密钥需要更多保护。密钥保护的另一个重要方面是避免滥用,如使用密钥加密密钥去加密数据。

#### 5.2.2 采用密码技术的保护

使用密码技术可抵抗对密钥的一些威胁。例如,用加密来抵抗密钥泄露和未授权使用;用数据完整性机制来抵抗篡改;用数据原发鉴别机制、数字签名和实体鉴别机制来抵抗伪造。

本部分应采用国家密码管理部门认可的密码算法。如,加密算法采用 GB/T 32907;数据完整性机制采用 GB/T 32918;数字签名采用 GB/T 32918;实体鉴别机制采用 GB/T 15843。

密码分隔机制可抵抗密钥滥用,按功能分类使用可以通过将信息与密钥的组合来完成。例如:控制信息与密钥的组合确保特定的密钥用于特定的任务(如密钥加密、数据完整性),采用对称密码技术的抗抵赖机制需要密钥控制。关于使用对称密码技术实现抗抵赖,见 GB/T 17903.2。密码应用的分类参见附录 B。

时间戳可以用来将密钥的使用限制在一定的有效期内,与序列号一起使用可抵抗对已记录的密钥协商信息的重放攻击。关于时间戳技术见 ISO/IEC 18014。

#### 5.2.3 采用其他手段的保护

##### 5.2.3.1 采用物理手段的保护

应对安全系统中密码设备所使用的密钥进行保护,防止被篡改、删除和泄露(公钥除外)等威胁。这些设备一般提供一个安全区用于密钥存储、密钥使用和密码算法的实现。提供的方法包括:

a) 从独立的安全密钥存储设备中加载密钥;

b) 与独立的安全设备(如智能卡)中的密码算法进行交互;

c) 脱机存储密钥(如存储卡)。

安全区一般通过物理安全机制加以保护。物理安全机制可包括:防止直接访问安全区的被动机制和在安全区可能受到入侵时破坏关键资料的主动篡改检测机制。所采用的物理安全机制取决于密钥的

重要性。密码设备的安全保护见 GB/T 37092—2018。

#### 5.2.3.2 采用组织手段的保护

密钥保护的一种方法是将其管理成一个密钥分级结构。除了该结构的最低级外，其他每级上的密钥只用于保护下级密钥。只有最低级密钥直接用于提供数据安全服务。这种分级方法限制密钥的使用，因此降低了泄露密钥的可能性，增加了攻击难度。例如，泄露单个会话密钥只会泄露该密钥所保护的信息。

允许获得密钥会导致一些严重问题，包括密钥泄露及密钥被滥用(尤其是抗抵赖)。仅在安全设备内部才可获得密钥明文。如需将它们输出，应采用一些特殊措施，例如，把该密钥分解为若干份，且不准许某个人获得所有部分。

密钥的使用也应控制，以防止泄露该密钥或其保护的信息。

### 5.3 密钥生存周期的一般模型

#### 5.3.1 密钥生存周期的定义

一个密钥将经历一系列状态，这些状态确定了其生存周期。有三种主要状态：

a) 待激活：在待激活状态，密钥已生成，但尚未激活使用；

b) 激活：在激活状态，密钥用于加密数据、解密或验证数据；

c) 挂起：在挂起状态，密钥仅可用于解密或验证。

若明确某个密钥已受到威胁后，应立刻将该密钥状态变为挂起状态，之后该密钥仅可用于解密或验证状态变化前收到的数据，不可用于其他用途。需要注意的是，确定受到威胁的密钥不能被再次激活，所以图 1 中密钥由挂起状态经再激活变为激活状态是有条件的可选操作。

当密钥确定受到未授权访问或控制时，可认为该密钥受到威胁。

这些状态及相应的转换如图 1 所示，图 1 给出了一个密钥生存周期的一般模型，其他生存周期模型可能附有上述三种状态的子状态。大多数生存周期需归档，根据生存周期的特定细节，这种归档可以和所有状态相关联。

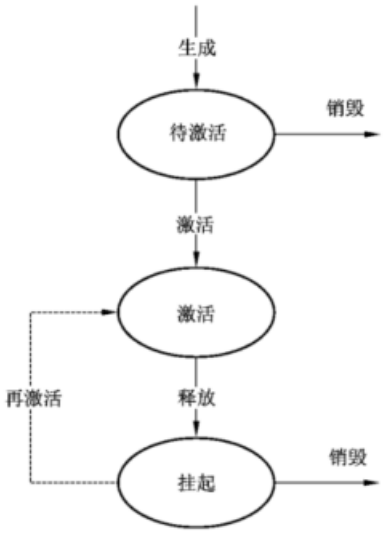


图 1 密钥生存周期

### 5.3.2 密钥状态间的转换

如图1，当密钥从一个状态迁移到另一个状态时，需经历下列转换：

a) “生成”：密钥生成过程。密钥生成应根据指定的密钥生成规则进行，该过程可能包括测试程序以验证是否遵守这些规则。需要注意的是，在密钥生成过程中使用不可预测的随机数是极其重要的，否则，即使使用最强的密码算法也不能提供足够的保护。关于随机数生成的方法，见ISO/IEC 18031。

b) “激活”：使密钥有效，可用于密码运算。

c) “释放”：限制密钥的使用，密钥过期或已被撤销都会发生这种情况。

d) “再激活”：允许挂起的密钥可重新用于密码运算。

e) “销毁”：终止密钥的生存周期，包括对密钥的逻辑销毁，也可包括物理销毁。

转换可由下列事件触发：需要新密钥、密钥受威胁、密钥过期、密钥生存周期结束等。所有这些转换都包括一系列的密钥管理服务。

### 5.3.3 密钥状态的转换与服务

用于特定密码技术的密钥在它的生存周期内将使用不同的服务组合。

对于对称加密技术，密钥生成后，从待激活状态到激活状态的转换包括密钥安装，也可包括密钥的注册和分发。在某些情况下，安装可涉及派生一个特殊的密钥。密钥的生存周期应限制在一个固定的期限内。释放终止激活状态，通常是因为密钥过期。如果发现处于激活状态的密钥受到威胁，撤销该密钥也可使它进入挂起状态。一个处于挂起状态的密钥可被归档。如果在某些条件下需再次使用已归档的密钥，它将被再激活，在它完全激活前，可能需再次安装和分发；否则，释放后，密钥可能会被注销和销毁。

对于非对称加密技术，一对密钥(公钥和私钥)生成后，这对密钥都会进入待激活状态。注意，这对密钥的生存周期有关联但不相同。在私钥进入激活状态之前，注册和分发给用户是可选的，但安装则是必需的。私钥在激活状态和挂起状态间的转换，包括释放、再激活和销毁，与上述对称密钥的情形类似。当签发公钥时，通常由CA生成一个包含公钥的证书，以确保公钥的有效性和所有权。该公钥证书可放在目录中或其他类似服务中用于分发，或传回给所有者进行分发。当所有者发送用其私钥签名的数据时，也可附上其证书。一旦公钥被验证，该密钥对就进入激活状态。当密钥对用于数字签名时，在私钥释放或销毁后，其相应的公钥可能不定期地处于激活状态或挂起状态。为了验证相关私钥在原定的有效期之内产生的数字签名，可能需要访问公钥。当采用非对称技术实现保密服务，且用于加密的密钥已释放或被销毁时，密钥对中所对应的密钥仍可能处于激活或挂起状态以用于其后的解密。

对于签名密钥，其对应的公开密钥将处于激活或挂起状态，对于加密密钥，其对应的私有密钥将处于激活或挂起状态。

密钥的使用或应用可决定与它相关的服务。例如，系统可决定不注册会话密钥，因为注册过程的时间可能比其生存周期还长。

## 6 密钥管理的基本内容

### 6.1 密钥管理服务

#### 6.1.1 密钥管理服务概述

密钥管理是对密钥生成、注册、认证、注销、分发、安装、存储、归档、撤销、派生以及销毁等服务的管理和使用。

密钥管理依赖于生成、注册、认证、注销、分发、安装、存储、归档、撤销、派生以及销毁等基本服务。这些服务可以是密钥管理系统的一部分，也可以由其他服务提供者提供。根据服务种类，服务提供者应

满足一定的由所有相关实体信任的最小安全要求(如安全交换)。例如,服务提供者可以是一个可信第三方(TTP)。密钥管理服务位于同一层,并可供各种用户(人或进程)使用,如图2所示。在不同的应用中,用户可利用不同的密钥管理设备,以满足其需求的服务。密钥管理服务见表1。

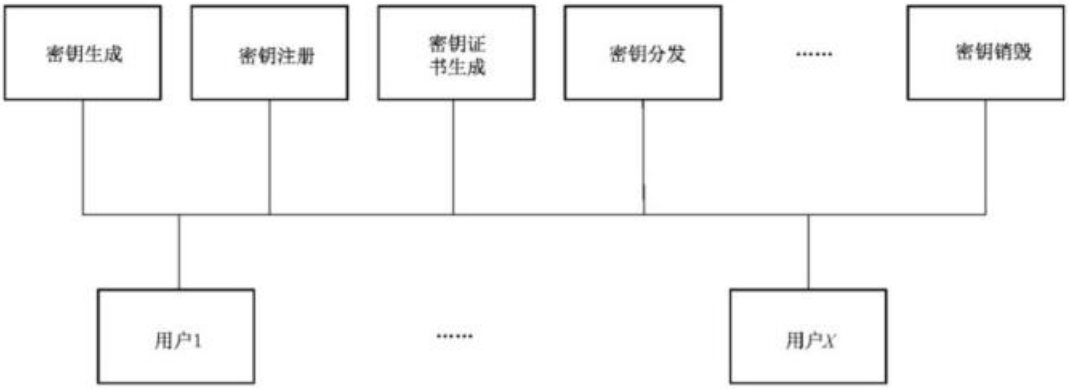


**图2 密钥管理服务**

转换和服务间的关系如表1所示,特殊的加密方法只需以下服务的子集。

**表1 转换和服务**

| 转换(按图1) | 服务 | 注释 |
|---|---|---|
| 生成 | 密钥生成 | 必选 |
| | 密钥派生 | 可选 |
| | 密钥注册 | 可选(在此处或激活时完成) |
| | 密钥证书生成 | 可选 |
| | 密钥分发 | 可选 |
| | 密钥存储 | 可选 |
| 激活 | 密钥证书生成 | 可选 |
| | 密钥分发 | 可选 |
| | 密钥派生 | 可选 |
| | 密钥安装 | 必选 |
| | 密钥存储 | 可选 |
| | 密钥注册 | 可选(在此处或生成时完成) |
| 释放 | 密钥存储 | 可选 |
| | 密钥归档 | 可选(在此处或销毁时完成) |
| | 密钥撤销 | 可选 |
| 再激活 | 密钥证书生成 | 可选 |
| | 密钥分发 | 可选 |
| | 密钥派生 | 可选 |
| | 密钥安装 | 必选 |
| | 密钥存储 | 可选 |

表 1（续）

| 转换（按图 1） | 服务 | 注释 |
| --- | --- | --- |
| 销毁 | 密钥注销 | 必选，如已注册 |
| | 密钥销毁 | 必选 |
| | 密钥归档 | 可选（在此处或释放时完成） |

### 6.1.2 密钥生成

密钥生成是为特定密码算法以安全的方式生成密钥的服务。这意味着密钥生成过程不能被篡改，生成方式不可预测，分发符合指定方法。某些密钥（如主密钥）的生成要求特别对待，因为知道这些密钥就能访问所有相关密钥或派生密钥。

密钥生成将涉及随机数生成器，随机数生成器不仅可生成不可预测的随机数，同时可生成均匀分布在整个算法密钥空间的随机数。例如，将一个 32 位熵的随机数生成器直接引入到密钥生成程序中，为一个对称算法生成 128 位密钥，密钥生成过程就有缺陷，随机数生成器见 ISO/IEC 18031。密钥派生函数及迭代次数见 GB/T 32918.3。

### 6.1.3 密钥注册

密钥注册服务将密钥和实体联系起来。它由一个注册机构提供，通常在使用对称密码技术时应用。如果实体需要注册密钥，它应与注册机构联系。密钥注册包括注册请求和注册确认。

注册机构以适当的安全方式保存密钥及其相关信息的记录。密钥管理信息的细节参见附录 C。由密钥注册机构提供的操作包括注册和注销。

### 6.1.4 密钥证书生成

由证书认证机构提供的密钥证书生成服务保证公钥和实体的联系。证书认证机构接受密钥的认证请求后，就生成公钥证书。公钥证书在本系列标准第 3 部分中有更详细的规定。

### 6.1.5 密钥分发

密钥分发是为已授权实体安全地提供密钥管理信息对象（参见附录 C）的一组过程。密钥分发的一种特殊情形是密钥交换，其中利用密钥交换中心在实体间建立密钥材料（见 7.3）。本系列标准的第 3 部分包括秘密密钥的密钥协商机制，以及秘密密钥和公开密钥的传输机制。

### 6.1.6 密钥安装

在使用密钥之前需要密钥安装服务。密钥安装是指以保护密钥不被泄露的方式在密钥管理设备内建立密钥。在极小的情况下，密钥安装只将密钥状态标记为“使用中”。

### 6.1.7 密钥存储

密钥存储服务为当前或近期使用的密钥或是备份密钥提供安全存储。物理上隔离的密钥存储通常具有优越性。例如，它确保密钥材料的保密性和完整性，以及公钥的完整性。存储可能发生在密钥生存周期的各种密钥状态（即待激活、激活和挂起）。根据密钥的重要性，可以选用下列机制中的一种来加以保护：

a) 物理安全（如在防篡改的设备中或用诸如存储卡等外部设备存储它们）；

b) 用密钥加密，这些加密密钥本身使用物理安全保护；

c) 用口令和 PIN 保护对它们的访问。

对所有密钥材料，应该能检测出任何试图泄露它们的行为。一般来说，当保护是完全基于密码或存储在软件上的 PIN 时，很难侦测到尝试性的密钥泄露。在这种情况下，受保护的密钥可被复制，在脱机情况下，密码和 PIN 可被破解，在实际应用中，这些都很难检测到。对这种情况，应根据应用考虑其他安全措施。

#### 6.1.8 密钥派生

密钥派生服务使用一个秘密的原始密钥(称为派生密钥)、非秘密的可变数据和一个变换过程(它也不需要保密)来生成大量的密钥。该过程的结果就是派生出的密钥。派生密钥需要特别的保护。派生过程应该是不可逆和不可预测的，这样才能保证泄露一个派生出的密钥不会导致泄露派生密钥或其他派生出的密钥。

#### 6.1.9 密钥归档

密钥归档在密钥正常使用之后提供一个安全且长期的存储过程。它可以使用密钥存储服务，但允许不同的实现，例如，脱机存储。在正常使用被中断后，为了证明或反驳某些声明，很久之后可能需要恢复已归档的密钥。

#### 6.1.10 密钥撤销

如果怀疑或已知某个密钥被泄露，密钥撤销服务能保证安全地将密钥释放。这项服务对于已经到期的密钥是必需的。密钥拥有者的情况发生变化时，也会撤销密钥。密钥被撤销后，它只用作解密和验证。密钥因为泄露被撤销，只有在泄露前处理的数据才可被解密或验证。

注：有些应用中对此服务称为密钥删除。

#### 6.1.11 密钥注销

由密钥注册机构提供的密钥注销服务解除密钥与实体的关系，它是销毁过程的一部分(见 6.1.12)。

#### 6.1.12 密钥销毁

密钥销毁服务是将不再需要的密钥安全地销毁。密钥销毁将删除该密钥管理信息对象的所有记录，在销毁之后将不再有任何信息可以用来恢复已销毁的密钥。销毁密钥还包括所有已归档的备份。然而，在销毁已归档的密钥之前，应进行检查以确保由这些密钥保护的已归档材料不再需要。

某些密钥可能存储于电子设备或系统之外。销毁这些密钥需要增加其他的管理措施。

### 6.2 支持服务

#### 6.2.1 密钥管理辅助服务

密钥管理服务可利用其他与安全有关的服务。这些服务包括：

a) 访问控制

访问控制服务保证密钥管理系统的资源只能由已授权的实体以授权方式访问。

b) 审计

审计用于对密钥管理系统中有关安全的行为进行跟踪。审计跟踪可能有助于分析安全风险和安全泄露。

c) 鉴别

鉴别服务用于确定实体为某一安全域的授权成员。

d) 密码服务

密码服务应当由密钥管理服务使用，以提供完整性、保密性、鉴别和抗抵赖。

e) 时间服务

时间服务是生成时变参数(如有效期)所必需的。

#### 6.2.2 面向用户服务

面向用户的服务提供一些必要的功能，例如，用户注册服务。这些服务与实现有关，但超出本部分的范围。

## 7 两实体间密钥分发的概念模型

### 7.1 密钥分发概述

在实体间分发密钥可能相当复杂，它受到通信链路的特性，涉及的可信关系和所用的密码技术的影响。实体可能直接通信也可能间接通信，可能属于同一安全域也可能属于不同安全域，可能使用或可能不使用可信机构的服务。下列概念模型说明了上述不同的情形如何影响密钥与信息的分发。

### 7.2 通信实体间的密钥分发

实体间的通信受实体间的链路、实体间的信任程度和所使用的密码技术的影响。

实体 A 与实体 B 之间存在一种连接，它们希望使用密码技术交换信息，这种通信连接如图 3 所示。


**图 3 两实体间的通信链路**

涉及直接通信实体的有密钥协商、密钥控制和密钥确认。

### 7.3 单域密钥分发

以下模型基于 GB/T 18794.1 中规定的带安全机构的安全域的概念。

该机构可以提供诸如密钥交换的密钥管理服务。当实体使用非对称技术进行信息的安全交换时，能区别以下情形：

a) 对于数据完整性和数据原发鉴别，接收方需要发送方相应的公钥证书；

b) 对于保密性，发送方需要接收方有效的公钥证书；

c) 对于鉴别、保密性和完整性，每一方都需要对方的公钥证书。这提供了相互抗抵赖手段。每个实体可能需要与其安全机构联系以获得合适的公钥证书。如果通信双方彼此信任并可以相互鉴别公钥证书，则不需要安全机构。

有些密码应用不涉及安全机构。在这种情况下，通信双方可能只需要安全地交换特定的公开信息，而不交换公钥证书。

当双方使用对称密码时，以下列两种方式中之一启动密钥生成：

a) 由一个实体生成密钥，并将其传给密钥交换中心(KTC)；

b) 一个实体请求密钥分发中心(KDC)生成用于后续分发的密钥。

如果由实体生成密钥，那么密钥的安全分发就由密钥交换中心来进行，如图 4 所示。图中数字代表

交换的步骤。KTC 接收来自实体 A 的已加密密钥(1),将它解密后用 KTC 与实体 B 的共享密钥重新加密。然后 KTC 可以将已加密密钥转发实体 B(2),或将已加密密钥传回给实体 A(3),实体 A 将其转发给实体 B(4)。

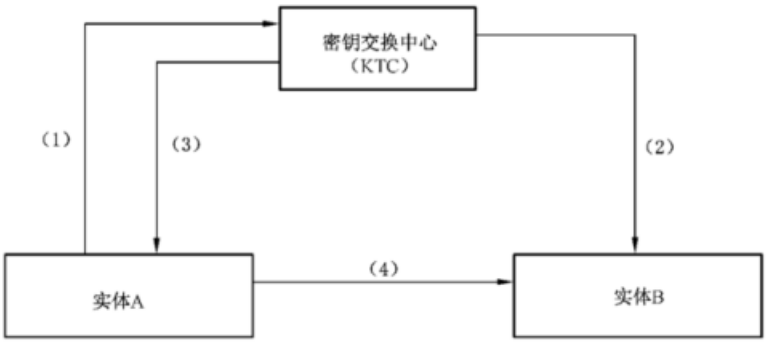


**图 4　密钥交换中心**

如果由可信第三方(TTP)生成密钥,有两种方法对通信双方进行后续的密钥分发,如图 5 密钥分发中心(KDC)的概念模型和图 6 实体 A 将密钥转发给实体 B 的密钥分发。

图 5 描述了密钥分发中心与两个实体均能进行安全通信的情形。在这种情况下,一旦密钥分发中心应一个实体的请求生成密钥,就应负责为两个实体安全地分发密钥。实体 A 向 KDC 请求与实体 B 的共享密钥(1),KDC 将密钥分发给通信双方实体 A(2a)和实体 B(2b)。

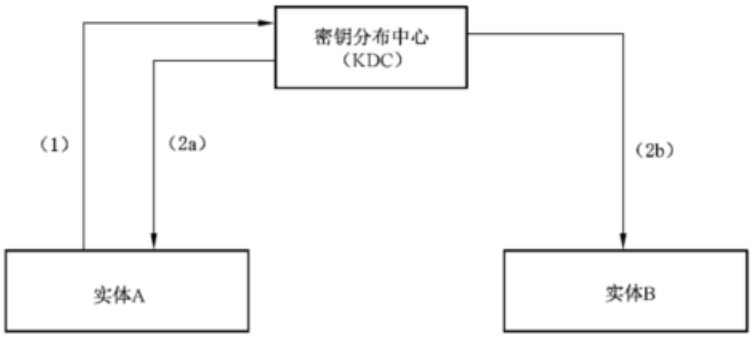


**图 5　密钥分发中心的概念模型**

如果只有实体 A 请求与实体 B 的共享密钥,则密钥分发中心可以采取两种方式。如果密钥分发中心与两个实体都能进行安全地通信,就如上所述将密钥分发给两个实体。如果密钥分发中心只能与实体 A 通信,那么实体 A 就负责把密钥传给实体 B。图 6 描述了后一种分发方式。实体 A 向 KDC 请求与实体 B 的共享密钥(1),KDC 将密钥分发给实体 A(2),由实体 A 将密钥转发给实体 B(3)。

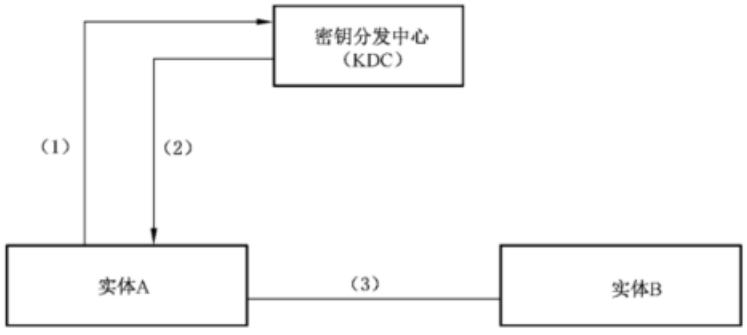


**图 6　实体 A 将密钥转发给实体 B 的密钥分发**

### 7.4 域间的密钥分发

域间的密钥分发模型包括归属不同安全域的实体 A 和实体 B，这两个安全域共用至少一种密码技术(即对称或者非对称技术)。图 7 描述了非对称情形，图 8 描述了对称情形。每个安全域都有自己的安全机构：一个被实体 A 信任，一个被实体 B 信任。如果实体 A 和实体 B 彼此信任或是信任对方的安全机构，那么密钥分发的方法则就依照 7.2 或 7.3。

在实体 A 与实体 B 之间建立密钥可分为两种情况：

a) 获取实体 B 的公钥证书(当适用时)；

b) 在实体 A 与实体 B 之间建立一个共享的秘密密钥。

在这些单元之间可能有各种密钥关系。这些密钥关系反映出单元之间的信任特征。

如果实体使用非对称技术进行信息交换，每一方需要取得对方的证书，如图 7 所示。当实体 A 的安全机构根据实体 A 的请求(1)颁发证书给实体 A (2)时，该证书通常由实体 A(3)或实体 A 的安全机构(3')发布在一个目录中。当实体 B 的安全机构根据实体 B 的请求(4)颁发证书给实体 B(5)时，该证书通常由实体 B(6)或实体 B 的安全机构(6')发布在一个目录中。目录可以是开放的，在这种情况下，实体 B 可以直接从实体 A 的目录获取实体 A 的证书(7)。如果实体 A 和实体 B 的安全机构有一个交叉发布协议(8)，那么实体 B 可通过实体 B 的安全机构(9)或在它自己的目录中找到实体 A 的证书(10)。如果没有找到，实体 A 将通过交换方式或作为密钥建立协议的一部分(11)将其证书发送给实体 B。

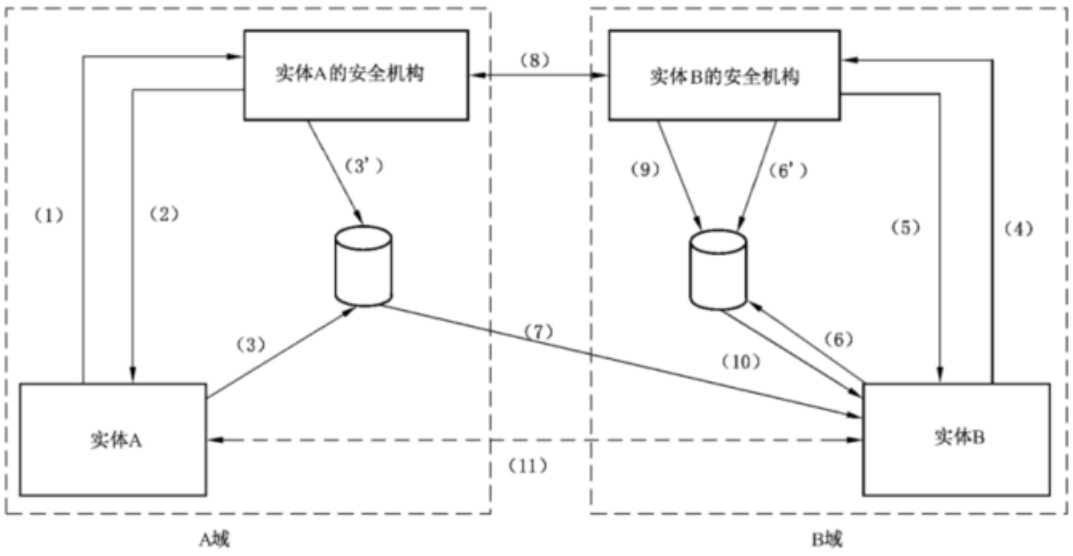


**图 7 通过非对称技术在两个域之间的密钥分发**

当实体间使用对称技术进行通信时，如图 8 所示，每个实体同样也应与各自的安全机构安全地联系(1)，以获得使他们能通信的一个秘密密钥。安全机构间协商一个供两个实体使用的共享秘密密钥(2)。如果把一个安全机构当作分发中心，另一个安全机构就可向两个实体分发该秘密密钥。前一安全机构也可提供密钥交换(2)和(3)。这样实体 A 和实体 B 就可以安全的直接通信(4)。

当只有实体 A 请求与实体 B 通信的秘密密钥时，安全机构可以采用两种方式：如果它能与双方通信，那么可采用上述方法，将秘密密钥分发给双方；如果它只能与一个实体通信，那么接收密钥的实体负责将密钥转发给另一个实体。

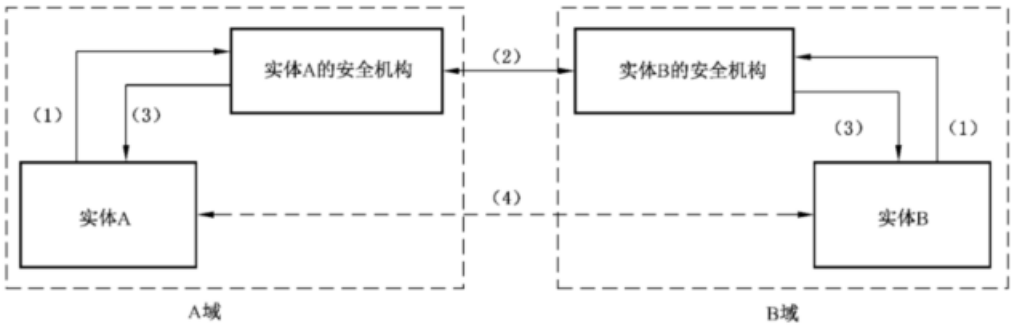


图 8　通过对称技术在两个域之间的密钥分发

有时实体 A 和实体 B 的安全机构既没有相互信任的关系也没有直接通信路径，那么就要借助双方都信任的机构 X，如图 9(2a)和(2b)所示。安全机构 X 可以生成密钥，将它分发给实体 A 和实体 B 的安全机构[如图 9(3a)和(3b)]，或者安全机构 X 可以将从实体 A 的安全机构接收到的秘密密钥或公钥证书[如图 9(2a)]转发给实体 B 的安全机构(3b)。然后这些安全机构应将接收到的密钥转发给各自的实体[如图 9(4a)和(4b)]，这样这些实体就可以安全地交换信息(5)。可能需要寻找一系列相关的安全机构，直至建立起信任链。

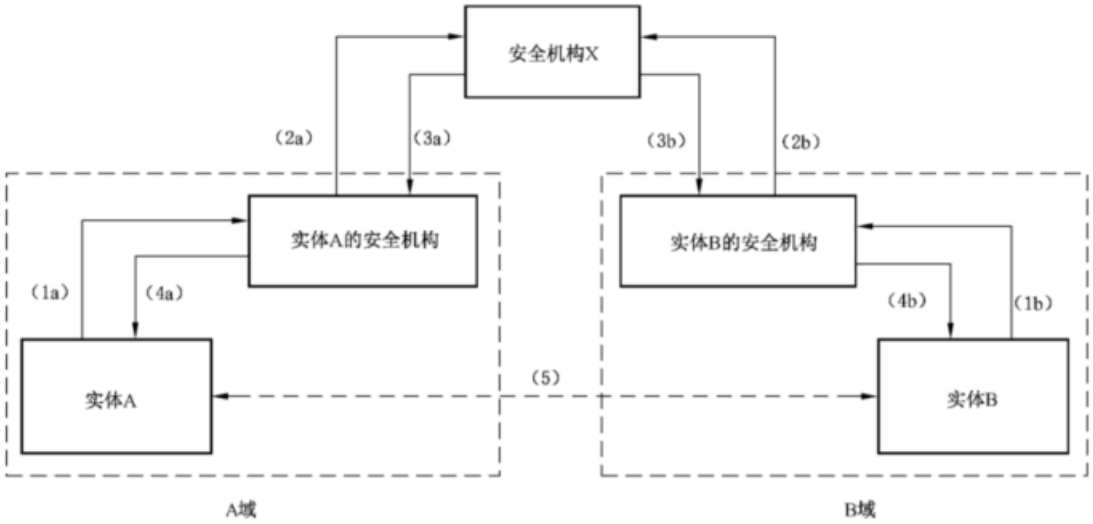


图 9　安全机构间的信任关系链

## 8　特定服务的提供者

密钥管理系统需要的某些服务可由外部服务提供者提供。可能的服务实体有：

a)　密钥注册机构或者密钥认证机构；

b)　密钥分发中心 KDC，KDC 用于为实体生成并分发密钥；

c)　密钥交换中心 KTC，KTC 不产生密钥，仅用于为实体间提供密钥交换服务。

# 附 录 A
（资料性附录）
## 密钥管理面临的安全威胁

密钥管理易受到许多威胁，包括以下几个方面：

a） 密钥材料的泄露

密钥材料或者是明文形式、未被保护并可以访问，或者虽已加密但可被解密。

b） 密钥材料的篡改

改变密钥材料，使之不能进行预定的运算。

c） 密钥材料的未授权删除

密钥或者密钥相关数据的删除。

d） 密钥材料的不完全销毁

可导致当前或者后续密钥的威胁。

e） 未授权撤销

直接或者间接删除有效密钥或者密钥材料。

f） 假冒

假冒授权的用户或者实体。

g） 延迟执行密钥管理功能

这可能导致生成、分发、撤销或者注册密钥的失败，密钥存储库及时更新失败，保持用户授权级别的失败等。前述威胁或与密钥相关设备的物理故障都会引起延迟威胁。

h） 密钥的滥用

- 将密钥用于未授权的目的，如用密钥加密密钥来加密数据；
- 将密钥管理设备用于未授权方的目的，如未授权的加密或者解密数据；
- 使用过期密钥；
- 过度使用某个密钥；
- 向未授权的接收者提供密钥。

# 附 录 B
（资料性附录）
密码应用分类

## B.1 常用密码系统的分类

密码系统通常按两种主要的密码技术来分类，即对称和非对称。因为密钥管理应支持这两种技术，所以需要另一种分类方法。下面根据技术所提供的功能对密码系统进行分类。

密码系统通常提供两种不同类型的密码服务：完整性和鉴别服务以及保密服务。机密性服务用于对信息进行密码保护，即提供数据机密性。完整性和鉴别服务主要是用于实体鉴别、数据原发鉴别、数据完整性和抗抵赖。密码系统的类型和相应的操作如图 B.1 所示。

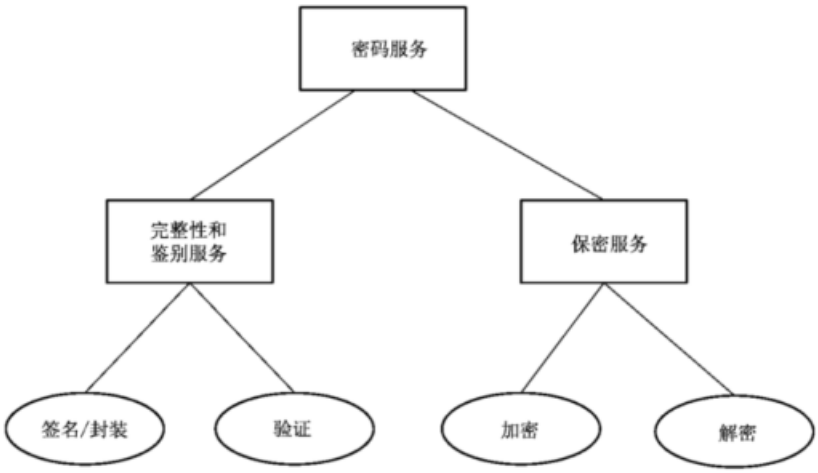


图 B.1 密码服务和相应机制

## B.2 完整性和鉴别服务以及密钥

完整性和鉴别服务提供对通信实体的鉴别（实体鉴别）、数据来源的鉴别（数据原发鉴别）抗抵赖性和数据完整性。该服务可以利用以下几个机制：

a） 数据单元封装
为数据完整性生成数据的密码校验值，如用对称算法生成一个消息鉴别码（MAC）。关于消息鉴别码，参见 GB/T 15852。

b） 数据单元签名
产生数字签名，用于数据原发鉴别、数据完整性和/或抗抵赖性。

c） 已封装数据单元的验证
计算数据单元的密码校验值，并与参考校验值比较（数据完整性的证明）。

d） 已签名数据单元的验证
验证数字签名，以确定该数据签名是否由声称的原发方生成，和（或）证明数据的完整性。

在完整性和鉴别服务中，签名与封装处理使用的信息或者是原发方私有的（即唯一且保密的），或者是只有原发方和接收方才知道的秘密。验证过程使用的程序或信息可以被公开获取，但从中不能推导

出原发方私有信息或者原发方和接收方使用的共享的秘密。签名的基本特征是只能使用原发方的私有信息(其私有密钥)才能生成。这样,当使用原发方的公开密钥对签名进行验证时,它可以随后向第三方(如公证机构)证明只有该私有信息的唯一持有者才能产生这一签名。

完整性和鉴别服务使用以下三类密钥中的两种:

a) 封装密钥:共享的、秘密密钥;

b) 签名密钥:与原发方有关的唯一的、私有的密钥;

c) 验证密钥:公开密钥和秘密密钥中的任何一种。

对于对称技术来说,完整性和鉴别服务使用一个封装密钥和一个验证密钥,它们是同一个秘密密钥;对非对称技术来说,使用签名密钥和验证密钥,一个是公开密钥,一个是私有密钥。

### B.3 机密性服务和密钥

机密性服务主要提供信息的机密性。它使用两种基本机制:

a) 加密:由已知数据产生密文;

b) 解密:由相应密文产生明文。

机密性服务可由所用的密码技术(即对称和非对称)决定。当使用对称技术时,加密和解密操作是由同一个密钥(共享秘密密钥)处理。当使用非对称时,加密和解密操作是由两个不同但相关的密钥(即公开和私有密钥)处理。

### B.4 组合服务

一些加密机制也提供机密性、数据完整性和(或)原发鉴别。特别是,ISO/IEC 19772 中描述的鉴别加密机制以及在 ISO/IEC 18033-4 中描述的流密码操作的 MULTI-SO1 模型都使用对称密码技术,提供机密性、数据完整性和原发鉴别。在 ISO/IEC 29150 中描述的签密技术使用非对称密码技术,提供机密性、数据完整性和原发鉴别。依靠使用的技术,也可能提供诸如鉴别和抗抵赖的安全功能。

# 附 录 C
（资料性附录）
## 密钥管理信息对象

密钥管理信息对象包括一个或者多个密钥，以及控制如何使用密钥的信息。控制信息不一定是显式的，可能隐含在控制密钥管理信息对象使用的惯例中（例如，非对称密码中，密钥对中的一个密钥使用受另一个的使用约定控制，一个用于加密，另一个就用于解密。）。

控制信息可以控制：

a） 密钥可能保护的对象类型（例如：数据或者密钥管理信息对象）；

b） 有效操作（例如：加密、解密）；

c） 授权的用户；

d） 可能使用密钥的环境；

e） 使用密钥管理信息对象的控制技术或者应用所持有的其他方面。

为达到优化的目的，密钥管理信息对象可能部分或全部在密钥生成过程中完成。

密钥证书是密钥生成信息对象的特例。它至少包括以下由认证机构签名的内容：

a） 公开密钥材料；

b） 能够使用相应的密钥管理信息对象的用户的身份；

c） 相应的密钥管理信息对象进行的操作（可能是隐含的）；

d） 有效期限；

e） 认证机构的身份。

# 参 考 文 献

[1] GB/T 9387.2—1985 信息处理系统 开放系统互联 基本参考模型 第2部分:安全体系结构

[2] GB/T 15852(所有部分) 信息技术 安全技术 消息鉴别码

[3] GB/T 17903(所有部分) 信息技术 安全技术 抗抵赖

[4] ISO/IEC 18033-4 Information technology—Security techniques—Encryption algorithms—Part 4: Stream ciphers)

[5] ISO/IEC 19772 Information technology—Security techniques—Authenticated encryption

[6] ISO/IEC 29150 Information technology—Security techniques—Signcryption