ICS 35.040
L 80

中华人民共和国国家标准

GB/T 17901.1—1999
idt ISO/IEC 11770-1:1996

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

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局 发布

前　言

本标准等同采用国际标准 ISO/IEC 11770-1:1996《信息技术　安全技术　密钥管理　第 1 部分：框架》。

本系列标准规定了密钥管理框架，适合于我国使用。

GB/T 17901 在总标题《信息技术　安全技术　密钥管理》下，包含以下几个部分：

——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

本标准的附录 A、附录 B、附录 C、附录 D 和附录 E 都是提示的附录。

本标准由国家信息化办公室提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位：电子工业部第三十研究所。

本标准主要起草人：雷利民、龚奇敏、方姝姝、鲍振东、吴娅若、杜明钰。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了世界范围内的标准化专门体系。ISO或IEC的成员国,通过由处理特殊技术活动领域的各个组织所建立的技术委员会来参与国际标准的开发。ISO和IEC的技术委员会在共同感兴趣的领域内合作,其他与ISO和IEC有联络的官方和非官方国际性组织,也参与这项工作。

在信息技术领域内,ISO和IEC已建立了一个联合技术委员会ISO/IEC JTC1。被联合技术委员会接受的国际标准草案送给各成员国表决。一个国际标准的发布,需要至少75%的成员国投赞成票。

国际标准ISO/IEC 11770-1是由信息技术联合技术委员会ISO/IEC JTC1的IT安全技术SC 27分委员会制定的。

ISO/IEC 11770的总标题《信息技术　安全技术　密钥管理》下,包含以下部分:

——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

可能有后续部分。

附录A、附录B、附录C、附录D和附录E只作为参考。

引　言

在信息技术中，采用密码机制保护数据不被非授权地泄露或窜改、实现实体鉴别和抗抵赖功能的需求与日俱增。这些机制的安全性和可靠性直接取决于对密钥这一安全参数的管理和保护。如果密钥管理有薄弱环节，那么即使是最完善的安全概念都将不起作用，因此安全地管理这些密钥对于将密码功能集成到系统中去是至关重要的。密钥管理的目的是提供对用于对称或非对称密码机制中的密码密钥材料的处理程序。

根本问题是要确定密钥材料，向直接和间接用户保证其来源、完整性、即时性和(秘密密钥情形下的)保密性。密钥管理包括根据某一安全策略产生、存储、分发、删除和归档密钥材料(GB/T 9387.2—1995)等功能。

本标准与开放系统安全框架(ISO/IEC 10181)有着特殊的关系。所有这些框架，包括本框架，确定涵盖安全各个方面的机制的基本概念和特性。本标准介绍作为对称和非对称密码机制基础的密钥管理的一般模型。

目　　次

中华人民共和国国家标准

信息技术　安全技术　密钥管理
第1部分：框架

GB/T 17901.1—1999
idt ISO/IEC 11770-1:1996

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

1　范围

本标准：

1）确定密钥管理的目标；

2）描述作为密钥管理机制基础的一般模型；

3）定义对 GB/T 17901 所有部分通用的密钥管理基本概念；

4）定义密钥管理服务；

5）确定密钥管理机制的特性；

6）规定对密钥材料在其生存期内进行管理的需求；

7）描述对密钥材料在其生存期内进行管理的框架。

本框架定义了与任何特定密码算法的使用无关的密钥管理一般模型，但是某些密钥分发机制可能与特定的算法特性（如非对称算法的特性）有关。

具体的密钥管理机制在本系列标准的其他部分阐述。其中，第2部分阐述对称体制，第3部分阐述非对称体制。本标准的内容是理解第2和第3部分的基础。ISO 8732 和 ISO 11166 中有使用密钥管理机制的范例。如果密钥管理需要抗抵赖功能，应采用 GB/T 17903。

本标准对密钥的自动与人工管理都进行了阐述，包括用来获得密钥管理服务的数据元素和操作顺序的概貌，但对可能需要的协议交换的细节未作规定。

和其他安全服务一样，只有在已定义的安全策略中才能提供密钥管理服务。安全策略的定义超出了 GB/T 17901 的范围。

2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分：安全体系结构（idt ISO 7498-2:1989）

GB 15843.1—1995　信息技术　安全技术　实体鉴别机制　第1部分：一般模型（idt ISO/IEC 9798-1:1991）

ISO/IEC 10181-1:1996　信息技术　开放系统互连　开放系统的安全框架：概述

国家质量技术监督局 1999-11-11 批准　　2000-05-01 实施

3 定义

下列定义与 GB/T 9387.2 中相同：

数据完整性 data integrity

数据原发鉴别 data origin authentication

数字签名 digital signature

下列定义与 GB/T 15843.1 中相同：

实体鉴别 entity authentication

下列定义与 ISO/IEC 10181-1 中相同：

安全机构 security authority

安全域 security domain

可信第三方 trusted third party (TTP)

除以上定义外，本标准还采用下列定义：

3.1 非对称密码技术 asymmetric cryptographic technique

使用两个相关的变换的密码技术，一个公开变换(由公开密钥定义)和一个私有变换(由私有密钥定义)。这两种变换具备这样的特性：给定公开变换，要推导出私有变换在计算上是不可行的。

3.2 认证机构 certification authority (CA)

产生和确定公开密钥证书的可信中心。认证机构也可以为实体产生和确定密钥。

3.3 解密 decipherment

与加密对应的逆。

3.4 加密 encipherment

通过密码算法对数据进行(可逆的)变换来产生密文，即隐藏数据的信息内容。

3.5 密钥 key

控制密码变换(如加密、解密、密码校验函数计算、签名产生或签名验证)运算的符号序列。

3.6 密钥协定 key agreement

两个实体间以双方都无法预先决定密钥的值的方式来确定共享秘密密钥的过程。

3.7 密钥确认 key confirmation

某实体确信另一个已识别的实体拥有正确的密钥。

3.8 密钥控制 key control

选择密钥或选择用于计算密钥的参数的能力。

3.9 密钥分发中心(KDC) key distribution centre (KDC)

一个可信实体，产生或获得密钥，并将密钥分发给每个与 KDC 有共享密钥的实体。

3.10 密钥材料 keying material

确立和维持密码密钥关系所必需的数据(如密钥，初始化值)。

3.11 密钥管理 key management

根据安全策略，实施并运用对密钥材料进行产生、登记、认证、注销、分发、安装、存储、归档、撤消、衍生和销毁的服务。

3.12 密钥转换中心(KTC) key translation centre (KTC)

实体间转换密钥的可信实体，每个实体与 KTC 共享一个密钥。

3.13 私有密钥 private key

在实体的非对称密钥对中只能由该实体使用的密钥。

注：私有密钥一般不能泄露。

3.14 公开密钥 public key

在实体的非对称密钥对中可以公开的那个密钥。

3.15 公开密钥证书 public key certificate

由认证机构签署的某一实体的不可伪造的公开密钥信息。

3.16 公开密钥信息 public key information

单一实体专用的信息，至少包括该实体的可区分标识符，以及该实体的至少一个公开密钥。可能还包含与认证机构、实体和公开密钥信息中的公开密钥有关的其他信息，例如公开密钥的有效期、相关私有密钥的有效期或是所涉及算法的标识符。

3.17 随机数 random number

其值是不可预测的时变参数。

3.18 秘密密钥 secret key

用于对称密码技术并只能由一组特定实体使用的密钥。

3.19 顺序号 sequence number

其值是从一定时间内不重复的规定顺序中取出的时变参数。

3.20 对称密码技术 symmetric cryptographic technique

原发者和接收者均采用同一秘密密钥进行变换的密码技术。若不知道秘密密钥，要计算出原发者或接收者的变换在计算上是不可行的。

3.21 时间标记 time stamp

根据公共的时间基准来表示某一时间点的时变参数。

3.22 时变参数 time variant parameter

实体用来检测消息并非重用的数据项，如随机数、顺序号或时间标记。

4 密钥管理综述

密钥管理是对密钥材料的产生、登记、认证、注销、分发、安装、存储、归档、撤消、衍生和销毁等服务的实施和运用。

密钥管理的目标是安全地实施和运用这些密钥管理服务，因此密钥的保护是极其重要的。

密钥管理程序依赖于基本的密码机制、预定的密钥使用以及所用的安全策略，密钥管理还包括在密码设备中执行的那些功能。

4.1 密钥的保护

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。要对密钥进行恰当的保护取决于许多因素，例如使用密钥的应用类型，它们所面临的威胁、密钥可能出现的不同状态等等。主要地，必须防止密钥不被泄露、窜改、销毁和重用，这取决于密码技术。附录A给出了密钥可能面临的威胁的例子。应通过时间和使用次数来限制密钥的有效性，这取决于进行恢复密钥攻击所需的时间和数据量，以及被保护信息的战略价值。用于产生密钥的密钥比它所产生的密钥更需要保护。密钥保护的另一个重要方面是要防止它们被误用，例如使用密钥加密密钥去加密数据。

4.1.1 采用密码技术的保护

可以采用密码技术来对抗对密钥材料的某些威胁。例如：用加密来对抗密钥泄露和未授权使用；用数据完整性机制来对抗窜改；用数据原发鉴别机制、数字签名和实体鉴别机制对抗冒充。

密码分隔机制可对抗滥用，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。

4.1.2 采用非密码技术的保护

时间标记可以用来将密钥的使用限制在一定的有效期限内，还可以与顺序号一起对抗对已记录的密钥协定信息的重用攻击。

4.1.3 采用物理手段的保护

安全系统中的每个密码设备通常需要保护它所使用的密钥材料不受下列威胁：窜改、删除以及泄露(公开密钥除外)。典型地，这些设备将为密钥存储、密钥使用和密码算法实现提供安全区，可能提供以下手段：

——从独立的安全密钥存储设备中装载密钥材料；

——与独立的智能安全设备(如智能卡、存储卡)中的密码算法进行交互；

——脱机存储密钥材料(如磁盘)。

通常由物理安全机制来保护安全区。

4.1.4 采用组织手段的保护

一种保护密钥的方法是从组织上将它们按级别划分。除最低级密钥外，每级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。这种分级方法能限制密钥的使用，从而减少了泄露范围，增加了攻击难度。例如，泄露单个会话密钥就只会泄露该密钥所保护的信息。

使用安全区是为了对抗未授权实体进行密钥泄露、窜改和删除的威胁。然而，授权对密钥管理服务执行特定管理功能的系统管理员有可能滥用他们拥有的访问特权，因而这种威胁仍然存在，尤其是他们有可能获得主密钥(最高级密钥)。主密钥的泄露可能导致暴露或窜改所有由该密钥保护的密钥(即该特定的密钥分级结构中的所有其他密钥)。因此最好是将对主密钥的访问减至最少，例如使任何单一用户都不能访问。密钥分割(双重或是 n 重控制)或使用专用密码方案(秘密共享方案)可以满足这一需求。

4.2 密钥生存期一般模型

一个密钥将经历一系列状态，这些状态确定了其生存期。三种主要的状态是：

待激活：在待激活状态，密钥已产生好但并未激活供使用；

激　活：在激活状态，密钥用于按密码术处理信息；

次激活：在本状态，密钥将只用于解密或验证。

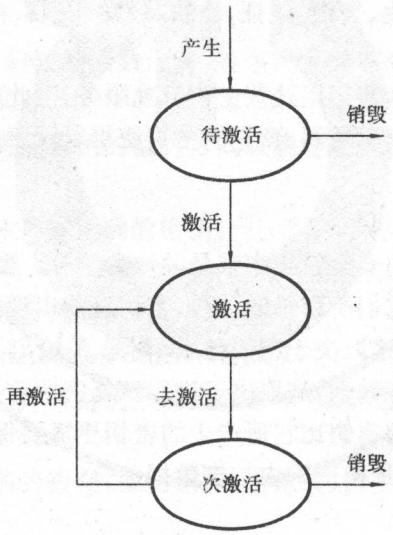

图 1　密钥生存期

注：次激活状态密钥的用户应确信，数据在该密钥进入去激活状态之前已经用密码学方法处理过。这种保证一般是由可信的时变参数提供的。

若已知某个密钥已被泄露，应马上变为次激活状态，并可能需要进行特殊处理。当已知或怀疑密钥被未授权使用时，认为该密钥已泄露。

图 1 表明了这些状态和相应的转移。

图 1 表示密钥生存期的一般模型。其他的生存期模型可能附有上述三种状态的子状态。大多数生存期都需要归档，根据生存期的具体细节，这种归档可以和所有状态相关联。

4.2.1 密钥状态间的转移

当密钥由一种状态向另一种状态变化时，它将经历如图1所示的下述转移：

产生是指产生密钥的过程。密钥产生应根据指定的密钥产生规则进行；这一过程可能包含测试程序，以验证是否遵守了这些规则。

激活是使密钥生效，以便进行密码运算。

次激活是限制密钥的使用。发生这种情况可能是因为密钥已过期或已被撤消。

再激活是使一个次激活密钥可重新用于密码运算。

销毁是终止密钥的生存期。它包括密钥的逻辑销毁，也可能包括物理销毁。

转移可能由下述事件触发，如需要新密钥、密钥泄露、密钥过期、以及密钥生存期结束。所有这些转移都包括一系列密钥管理服务，转移与服务之间的关系见表1，第5章中有对服务的解释。

任何特定的密码方法只需要表1所给出服务的一个子集。

4.2.2 转移、服务与密钥

用于特定的密码技术的密钥在其生存期内将使用不同的服务组合，下面给出两个例子。

对于对称密码技术，在产生密钥之后，从待激活状态到激活状态的转移包括密钥安装，并也可能包括密钥登记和分发。在某些情况下，安装可能涉及到衍生一个特殊的密钥。密钥的生命期应限制在一个固定的期限内。去激活将终止激活状态，通常是因为密钥过期。如果怀疑或已知某个处于激活状态的密钥被泄露，撤消该密钥也使它进入次激活状态。可以对次激活状态的密钥进行归档。如果重新需要一个已归档的密钥，它将被再激活，在它完全激活之前可能需要再次安装和分发。否则，在去激活之后该密钥可能被注销并销毁。

对于非对称密码技术，产生一对密钥(公开的和私有的)，并且都进入待激活状态。注意，这两个密钥的生存期相关但不相同。在私有密钥进入待激活状态之前，登记和分发给用户是可选的，但安装总是必需的。私有密钥的激活和次激活状态之间的转移包括去激活、再激活和销毁，与上述对称密钥的情形类似。当签发公开密钥时，通常由CA产生一个包含公开密钥的证书，以确保公开密钥的有效性与所有权。该公开密钥证书可能放在目录或其他类似服务中用于分发，或是传回给所有者进行分发。当所有者发出用其私有密钥签名的信息时，他可附上他的证书。一旦签发了公开密钥，密钥对就进入激活状态。当密钥对用于数字签名时，在去激活或销毁相关的私有密钥之后，公开密钥可能仍不定期地处于激活或次激活状态。为了验证相关私有密钥在原定的有效期之内产生的数字签名，可能需要访问公开密钥。当非对称技术用于加密，且用于加密的密钥已被次激活或已销毁时，密钥对中对应的密钥可能仍处于激活或次激活状态以用于以后的解密。

密钥的使用或应用可决定对它的服务。例如，系统可决定不登记会话密钥，因为登记过程可能比它们的生存期还长。相反，当对称技术用作数字签名时，必需登记秘密密钥。

表1 转移和服务

转　移	服　务	注　释
产　生	密钥产生	必备
	密钥登记	可选(在此处或在激活处)
	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
	密钥衍生	可选

表 1(完)

转　移	服　务	注　释
	密钥安装	必备
	密钥存储	可选
	密钥登记	可选(在此或在产生处)
去激活	密钥存储	可选
	密钥归档	可选(在此或在销毁处)
	密钥撤消	可选
再激活	密钥证书生成	可选
	密钥分发	可选
	密钥衍生	可选
	密钥安装	必备
	密钥存储	可选
销　毁	密钥注销	如果已登记,必备
	密钥销毁	必备
	密钥归档	可选(在此或在去激活处)

5　密钥管理概念

5.1　密钥管理服务

为帮助了解密钥管理服务以及它们如何互相配合与支持,本章描述密钥管理的一般结构。

密钥管理依赖于密钥的产生、登记、认证、分发、安装、存储、衍生、归档、撤消、注销和销毁等基本服务。这些服务可以是密钥管理系统的部分,也可以由其他服务提供者提供。根据服务的种类,服务提供者必须满足一定的由所有有关实体信赖的最小安全需求(如安全交换)。例如,服务提供者可以是一个可信第三方。图 2 表明所有密钥管理服务位于同一层,并可供各种各样的用户(人或进程)使用。在不同的应用中,这些用户可利用不同的密钥管理设备,以满足其需求的服务。密钥管理服务列于表 1 中。

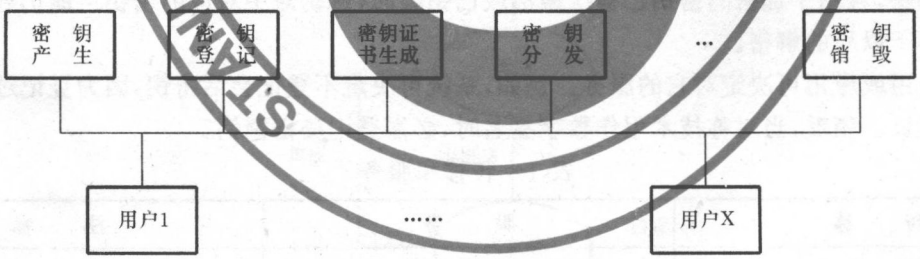

图 2　密钥管理服务

5.1.1　密钥产生

产生密钥是为特定密码算法以安全的方式产生密钥的服务。这意味着密钥产生过程不会被窜改,产生方式不可预测,分发符合指定方法。使用密钥的密码算法和密钥的密码保护级别将影响分发过程。某些密钥(如主密钥)的产生要求特别对待,因为知道这些密钥就能访问所有相关密钥或衍生密钥。

5.1.2　密钥登记

登记密钥服务将密钥与实体联系起来。它由一个登记机构提供,通常是在使用对称密码技术时应用。如果实体希望登记密钥,它必须与登记机构联系。密钥登记包括登记请求和对登记的确认。

登记机构以适当的安全方式保存密钥及相关信息的记录。附录 B 给出了密钥管理信息的细节。

由密钥登记机构提供的操作有登记和注销。

5.1.3 密钥证书生成

由认证机构提供的生成密钥证书服务保证公开密钥与实体的联系。认证机构接受密钥的认证请求后，就生成密钥证书。公开密钥证书在本系列标准第3部分中有更详细的讨论。

5.1.4 密钥分发

分发密钥是为已授权实体安全地提供密钥管理信息客体(见附录B中的实例)的一组过程。密钥分发的一种特殊情形是密钥转换，其中利用密钥转换中心在实体间建立密钥材料(见6.2)。本系列标准的第2部分给出在实体间建立密钥的各种机制。本系列标准的第3部分包括秘密密钥的密钥协定机制，以及秘密和公开密钥的传输机制。

5.1.5 密钥安装

在使用密钥之前总是需要密钥安装服务。密钥的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。

5.1.6 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，以及公开密钥的完整性。存储可能发生在密钥生存期的各种密钥状态(即待激活、激活和次激活)。根据密钥的重要性，可以选用下列机制中的一种来保护它们：

——物理安全(如，在一个防拆设备中或用诸如磁盘或存储卡等外部设备存储它们)；

——用密钥加密，这些密钥本身用物理安全保护；

——用口令或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。

5.1.7 密钥衍生

密钥衍生服务使用一个秘密的原始密钥(称为衍生密钥)、非秘密的可变数据和一个变换过程(它也不需要保密)来产生大量的密钥。该过程的结果就是衍生出的密钥。衍生密钥需要特别的保护。衍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衍生出的密钥不会导致泄露衍生密钥和其他衍生出的密钥。

5.1.8 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，如脱机存储。在正常使用被中断之后，为了证实或反驳某些声明，很久之后可能需要恢复已归档的密钥。

5.1.9 密钥撤消

如果怀疑或已知某个密钥被泄露，密钥撤消服务能保证安全地将密钥去激活，这项服务对于已经到期的密钥是必需的。密钥持有者的情况发生变化时，也会撤消密钥。密钥被撤消后，可能只用于解密和验证。密钥撤消服务不适用于基于证书的方案，因为密钥生存期受控于证书的期限。

注：某些应用以术语“密钥删除”代表本服务。

5.1.10 密钥注销

由密钥登记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5.1.11密钥销毁)。当实体希望注销某个密钥时，可与登记机构联系。

5.1.11 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客体的所有记录，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。销毁密钥还包括销毁所有已归档备份。然而，在销毁已归档密钥之前，必须进行检查以确保由这些密钥保护的已归档材料不再需要。

注：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。

5.2 支持服务

可能需要其他一些服务来支持密钥管理。

5.2.1 密钥管理辅助服务

密钥管理 服务可以利用其他与安全有关的服务。这些服务包括：

访问控制 该服务保证密钥管理系统的资源只能由授权实体以授权的方式访问。

审计 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漏。

鉴别 该服务确定实体为某一安全域的授权成员。

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。

时间服务 该服务是产生时变参数(如有效期)所必需的。

5.2.2 面向用户的服务

密码体制和设备可能需要其他服务，如用户登记服务。这些服务与实现有关，超出了本标准的范围。

6 密钥分发概念模型

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。以下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。

6.1 通信实体间的密钥分发

实体间的通信受到实体间的链路、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，这种通信连接见图3。一般来说，密钥分发必须在逻辑上与通信业务信道不同的安全信道上进行。

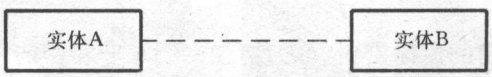

图3 两个实体间的通信链路

涉及直接通信实体的有密钥协商、密钥控制和密钥确认，详见本系列标准的第2部分(信息技术 安全技术 密钥管理 第2部分：采用对称技术的机制)和第3部分(信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制)。

6.2 单域密钥分发

以下模型基于ISO/IEC 10181-1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转换的密钥管理服务。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：

——对于数据完整性或数据原发鉴别，收方需要发方相应的公开密钥证书；

——对于保密性，发方需要收方有效的公开密钥证书；

——对于鉴别、保密性和完整性，每一方都需要对方的公开密钥证书，这就提供了相互抗抵赖手段。

每个实体都可能需要与其安全机构联系以获得合适的公开密钥证书。如果通信双方彼此信任并可以相互鉴别公开密钥证书，则不需要安全机构。

注：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，而不交换公开密钥证书。

当双方使用对称密码时，以下列两种方式中之一启动密钥产生：

——由一个实体产生密钥，并将其传给密钥转换中心(KTC)；

——一个实体请求密钥分发中心产生用于后续分发的密钥。

如果由实体产生密钥，那么密钥的安全分发就由密钥转换中心来进行，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

——将已加密密钥转发给实体 B(2),或者

——将它传回给实体 A(3),实体 A 再传给实体 B(4)。

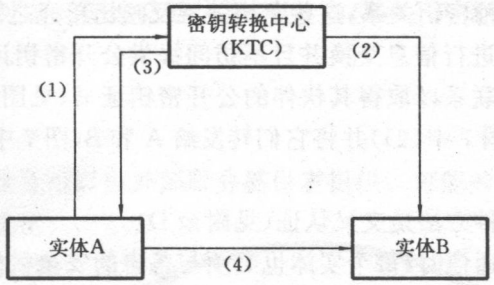

图 4 密钥转换中心

如果由可信第三方产生密钥,有两种方法对通信双方进行后续的密钥分发,见图 5——密钥分发中心的概念模型和图 6——实体 A 将密钥转发给实体 B 的密钥分发。

图 5 说明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产生出密钥,就负责为两个实体安全地分发该密钥。(1)表示请求共享密钥,(2a)和(2b)表示将密钥分发给通信双方。

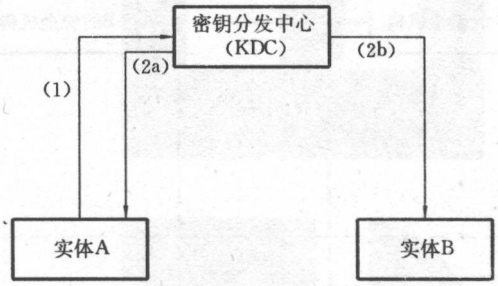

图 5 密钥分发中心的概念模型

如果只有实体 A 请求与 B 的共享秘密密钥,则 KDC 可以采取两种方式:如果它与两个实体都能安全地通信,就如上所述将秘密密钥分发给两个实体;如果 KDC 只能与 A 通信,那么实体 A 就负责将密钥传给实体 B。图 6 表示了后一种分发方式。(1)表示请求共享密钥,(2)表示将密钥分发给实体 A,(3)表示由 A 将密钥转发给 B。

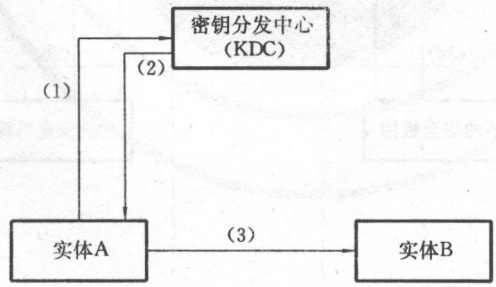

图 6 实体 A 将密钥转发给实体 B 的密钥分发

6.3 域间的密钥分发

这种模型涉及属于不同安全域的实体 A 和 B,这两个安全域共用至少一种密码技术(即对称或非对称)。每个安全域各有自己的安全机构:一个被 A 信任,一个被 B 信任。如果 A 和 B 彼此信任或是信任对方域的安全机构,那么密钥分发的方法就依照 6.1 或 6.2。

在 A 和 B 之间建立密钥可分为两种情况:

——获得 B 的公开密钥证书(当可利用时);

——在 A 与 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并且不访问提供公开密钥证书的公用目录服务,那么每个实体都应该与各自的安全机构联系以取得其伙伴的公开密钥证书(见图 7 中(1))。A 和 B 的机构交换实体 A 与 B 的公开密钥证书(图 7 中(2))并将它们转发给 A 和 B(图 7 中(3))。这样 A 和 B 就可以安全且直接地通信(图 7 中(4))。

交换公开密钥证书的另一种方法是交叉认证(见附录 D)。

当实体使用对称技术进行通信时,每个实体也必须与各自的安全机构安全地联系(图 7 中(1))以获得使他们能通信的一个秘密密钥。这些安全机构商定一个供这两个实体使用的共享秘密密钥(图 7 中(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,前者也可以提供密钥转换(图 7 中(2)和(3))。

当只有实体 A 请求与实体 B 通信的秘密密钥时,安全机构可以采取两种方式:如果它能够与双方通信,可将秘密密钥如上所述分发给双方;如果安全机构只能与一方进行通信,接收密钥的实体负责将密钥转发给另一实体。

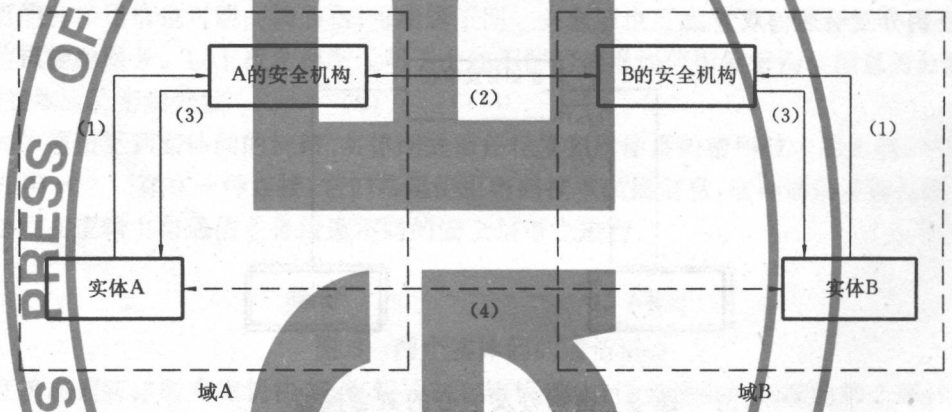

图 7 两个域间的密钥分发

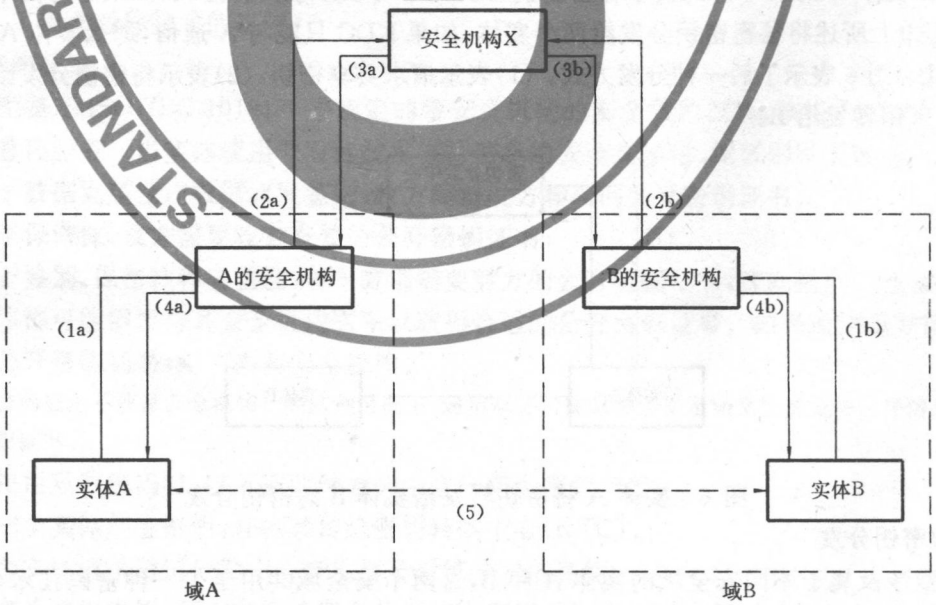

图 8 安全机构间的信任关系链

有时 A 和 B 的安全机构既没有相互的信任关系也没有直接的通信路径,那么就要借助双方都信任的机构 X,如图 8 所示(见箭头(2a)和(2b))。机构 X 可以产生一个密钥,将它分发给 A 和 B 的机构(见

图 8 中的箭头(3a)和(3b)),或者,机构 X 可以将从 A 的机构接收到的秘密密钥或公开密钥证书(例如图 8 中(2a))转发给 B 的机构(3b),然后这些机构必须将接收到的密钥转发给各自的实体(见图 8 中的(4a)和(4b)),这样这些实体就可以安全地交换信息(图 8 中(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。

7 专门的服务提供者

密钥管理系统需要的某些服务可以由外部服务提供者提供。可能的服务实体有:

——密钥登记机构或认证机构;

— ISO/IEC 8732 中定义的密钥分发中心;

— ISO/IEC 8732 中定义的密钥转换中心。

附 录 A
（提示的附录）
对密钥管理的威胁

密钥管理易受到许多威胁，包括以下几种。

泄露密钥材料：密钥材料或者是明文形式、未被保护并可以访问，或者是虽已加密但可被解密。

窜改密钥材料：改变密钥材料，使之不能进行预定的运算。

未授权删除密钥材料：删除密钥或与密钥有关的数据。

不彻底销毁密钥材料：这可能导致当前或后续密钥的损害。

未授权撤消：直接或间接地删除有效密钥或密钥材料。

假冒：冒充某个授权用户或实体。

延迟执行密钥管理功能：这可能导致产生、分发、撤消或登记密钥的失败，及时更新密钥库的失败，保持用户授权级别的失败等等。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。

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的目的，如非法加密或解密数据；

——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
（提示的附录）
密钥管理信息客体

密钥管理信息客体由一个或几个密钥以及控制如何使用密钥的信息组成（最后一项为可选项）。控制信息不一定是显式的，可能隐含于控制密钥管理信息客体使用的惯例中（例如，非对称密码中，密钥对中的一个密钥的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：

——密钥可能保护的客体类型（如数据或密钥管理信息客体）；

——合法的操作（如加密、解密）；

——允许的用户；

——可能使用密钥的环境；

——使用密钥管理信息客体专门的控制技术或应用所特有的其他方面。

为达到优化的目的，密钥管理信息客体可能部分或全部在密钥产生过程中生成。

密钥证书是密钥管理信息客体的一个特例。它至少包含以下由认证机构签名的内容：

——密钥材料；

——能够使用相应的密钥管理信息客体的用户的身份；

——相应的密钥管理信息客体进行的操作（可能是隐含的）；

——有效期限；

——认证机构的身份。

以下的 ASN.1 定义是密钥管理信息客体的一个例子，但密钥管理信息客体还可能包含其他与实现有关的参数。