ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 27909.3—2011

银行业务　密钥管理(零售)
第3部分:非对称密码系统及其密钥管理和生命周期

Banking—Key management(retail)—
Part 3:Asymmetric cryptosystems—Key management and life cycle

(ISO 11568-4:2007,MOD)

2011-12-30 发布　　2012-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 27909《银行业务　密钥管理(零售)》分为以下3个部分：

——第1部分：一般原则；

——第2部分：对称密码及其密钥管理和生命周期；

——第3部分：非对称密码系统及其密钥管理和生命周期。

本部分是GB/T 27909的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分修改采用国际标准ISO 11568-4:2005《银行业务　密钥管理(零售)　第4部分：非对称密码系统及其密钥管理和生命周期》(英文版)。

在采用ISO 11568-4时做了以下修改：

——删除了“ISO 11568-4 附录A核准的算法”。

本部分还做了下列编辑性修改：

a)　对规范性引用文件中所引用的国际标准，有相应国家标准的，改为引用国家标准；

b)　删除ISO前言。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会(SAC/TC 180)归口。

本部分负责起草单位：中国金融电子化公司。

本部分参加起草单位：中国人民银行、中国工商银行、中国农业银行、中国银行、交通银行、中国光大银行、中国银联股份有限公司。

本部分主要起草人：王平娃、陆书春、李曙光、赵志兰、周亦鹏、赵宏鑫、程贯中、刘瑶、喻国栋、杨增宇、黄发国。

引　言

GB/T 27909 描述了在零售金融服务环境下密钥的安全管理过程，这些密钥用于保护诸如收单方和受理方之间，收单方和发卡方之间的报文。

本部分描述了在零售金融服务领域内适用的密钥管理要求，典型的服务类型有销售点/服务点(POS)借贷记授权和自动柜员机(ATM)交易。

GB/T 27909 各部分描述的密钥管理技术结合使用时，可提供 GB/T 27909.1 中描述的密钥管理服务。

这些服务包括：

——密钥分离；

——防止密钥替换；

——密钥鉴别；

——密钥同步；

——密钥完整性；

——密钥机密性；

——密钥泄露的检测。

本部分描述了使用非对称密码机制时，密钥安全管理中涉及的密钥生命周期。依据标准第 1 部分和本部分描述的密钥管理原则、服务和技术，本部分还规定了密钥生命期内各个阶段的要求和实现方法。本部分不涉及对称密码机制的密钥管理或生命周期，该方面的内容见 GB/T 27909.2。

本部分是 GB/T 27909、GB/T 21078.1、GB/T 20547、ISO 9564-2、ISO 9564-3、ISO 9564-4、ISO/TR 19038 等描述金融服务领域安全要求的标准之一。

银行业务　密钥管理(零售)
第3部分:非对称密码系统及其密钥管理和生命周期

1　范围

本部分规定了零售金融服务环境中使用非对称密码机制时,对称和非对称密钥的保护技术,也描述了与非对称密钥相关的生命周期管理。本部分适用于技术符合GB/T 27909.1中描述的原则。

本部分的零售金融服务环境仅限于下述实体之间的接口:

——卡受理设备与收单方;

——收单方与发卡方;

——集成电路卡(ICC)与卡受理设备。

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

GB/T 27909.2　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(GB/T 27909.2—2011,ISO 11568-2:2005,MOD)

GB/T 17964—2000　信息安全技术　分组密码算法的工作模式(ISO/IEC 10116:1997,IDT)

GB/T 20547.2　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(GB/T 20547.2—2006,ISO 13491-2:2005,MOD)

GB/T 21078.1　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(GB/T 21078.1—2007,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、要求和评估方法(GB/T 21079.1—2007,ISO 13491-1:1998,MOD)

ISO/IEC 9796-2:2002　信息技术　安全技术　实现报文恢复的数字签名方案

ISO/IEC 10118(所有部分)　信息技术　安全技术　哈希函数

ISO/IEC 11770-3　信息技术　安全技术　密钥管理　第3部分:使用非对称技术的机制

ISO/IEC 14888-3　信息技术　安全技术　带附录的签名　第3部分:基于离散对数的机制

ISO 15782-1:2003　银行业务　证书管理　第1部分:公钥证书

ISO/IEC 15946-3:2002　信息技术　安全技术　基于椭圆曲线的密码技术　第3部分:密钥的生成

ISO 16609:2004　银行业务:使用对称技术的报文认证要求

ISO/IEC 18033-2　信息技术　安全技术　加密算法　第2部分:非对称密码

ANSI X9.42-2003　金融业务的公钥密码　使用离散对数密码的对称密钥协议

3 术语和定义

GB/T 27909.1、GB/T 27909.2 界定的以及下列术语和定义适用于本文件。

3.1

非对称密码 asymmetric cipher

加密密钥和解密密钥不同的密码，并且从加密密钥推导出解密密钥在计算上不可行。

3.2

非对称密码系统 asymmetric cryptosystem

该密码系统由两个互补的操作组成，每一个操作利用不同但相关的密钥即公钥和私钥之一进行加密或解密，并且从加密密钥推导出解密密钥在计算上不可行。

3.3

非对称密钥对生成器 asymmetric key pair generator

用于生成非对称密钥的安全密码设备。

3.4

证书 certificate

由颁发证书的证书授权机构的私钥签署的一个实体的凭证，从而确保不可伪造。

3.5

认证机构(CA) certification authority(CA)

受一方或多方信任的创建、颁发和撤销证书的实体。

注：可选地，认证机构也可以给实体创建和分发密钥。

3.6

通信方 communicating party

发送或接收公钥，用于与公钥所有者通信的一方。

3.7

计算上不可行 computationally infeasible

计算在理论上可以实现，但就实现该计算所需要的时间或资源而言，这种计算是不可行的。

3.8

凭证 credentials

实体的认证数据，至少包括这个实体的惟一识别名和公钥。

注：也可以包括其他数据。

3.9

密码周期 cryptoperiod

一个特定的时间周期，在此时间周期内，特定密钥被授权使用或者密钥在给定系统中保持有效。

3.10

数字签名系统 digital signature system

提供数字签名生成和验证的非对称密码系统。

3.11

哈希函数 hash function

将一组任意的串集映射到一组固定长度的比特串集的单向函数。

注：抗冲突的哈希函数是具有如下特性的函数，即：要创建映射为同一输出的多个不同输入在计算上是不可行的。

3.12

独立通信 independent communication

指允许实体在产生证书之前，逆向验证凭证和鉴别文件的正确性的过程(例如，回呼、视觉鉴别等)。

3.13

密钥协商 key agreement

在实体间以不能预知密钥值的方式建立共享密钥的过程。

3.14

密钥分享组件 key share

与密码密钥相关的参数之一(参数至少2个)，在生成该密码密钥时，只有参数的数量达到阈值时才能组合形成密钥，参数数量小于阈值则不能提供有关该密钥的任何信息。

3.15

来源的不可否认性 non-repudiation of origin

在可接受的可信度上，报文和相关密码检验值(数字签名)的源发者无法否认自己曾发出该报文的这种特性。

4 零售金融服务系统中非对称密码系统的使用

4.1 概述

非对称密码系统包括非对称密码、数字签名系统以及密钥协商系统。

在零售金融服务系统中，非对称密码系统主要用于密钥管理：首先用于对称密码的密钥管理，其次用于非对称密码系统本身的密钥管理。本章描述了非对称密码系统的这些应用，第5章描述了与密钥管理及证书管理相关的这些应用所采用的技术，第6章描述了这些技术和方法是如何应用在密钥对生命周期的安全和实施相关要求中的。

4.2 对称密钥的建立和存储

对称密码密钥可以通过密钥传输或密钥协商来建立。密钥传输或密钥协商机制见ISO/IEC 11770-3。该机制应确保通信方的真实性。

对称密钥的存储要求见GB/T 27909.2。

4.3 非对称公钥的存储和分发

非对称密钥对的公钥需要分发给一个或多个用户或由他们存储，以便随后作为加密密钥和/或签名验证密钥使用，或者在密钥协商机制中使用。虽然这个密钥不需要防止泄露，但是分发和存储过程应确保如5.6.1所描述的密钥的真实性和完整性。

非对称公钥分发机制见ISO/IEC 11770-3。

4.4 非对称私钥的存储和传输

非对称密钥对的私钥不需要分发给任何实体，在某些情况下，它仅可以保存在生成它的安全密码设备内。

如果必须要从生成它的设备内输出(例如，为了传输给准备使用或备份它的其他安全密码设备)，则应至少使用以下技术中的一种来防止泄露：

——按照5.2定义的方式用另一个密钥加密(见5.2)；

——如果不进行加密且要输出到安全密码设备外，需使用可接受的密钥分割算法将非对称密钥对的私钥分成若干个密钥分享组件；

——输出到另一个准备使用的安全密码设备中，或是用于此目的的安全传输设备中。如果通信路径不是足够安全，则传输应只允许在安全环境中进行。

应采用 5.6.2 中定义的技术之一保证私钥的完整性。

5 提供密钥管理服务的技术

5.1 概述

本章描述了可以单独或组合使用的多项技术，这些技术提供了 GB/T 27909.1 中介绍的密钥管理服务。某些技术可以提供多种密钥管理服务。

非对称密钥对不宜用于多种目的，但是如果使用了，例如，用在数字签名和加密中，那么应使用特殊的密钥分离技术，通过使用密钥对的变换来确保系统不受到攻击。

所选的技术应在安全密码设备内实现，该密码设备的功能应确保技术的实现可达到预定的目的。

安全密码设备的特性和管理要求见 GB/T 21079.1。

5.2 密钥加密

5.2.1 概述

密钥加密是用一个密钥给另一个密钥加密的技术。由此得到的加密的密钥可以在安全密码设备之外安全地存在。用来实现这种加密技术的密钥被称为密钥加密密钥(KEK)。

这里描述了涉及非对称密钥和非对称密码的两种不同的密钥加密情况，分别是：

a) 用非对称密码给对称密钥加密；

b) 用对称密码给非对称密钥加密。

5.2.2 用非对称密码给对称密钥加密

用非对称密码的公钥给对称密钥加密典型地用于通过不安全信道分发该密钥。被加密的密钥可能是一个工作密钥，也可能本身是一个密钥加密密钥(KEK)。从而可建立起与对称和非对称密码密钥相结合的如 GB/T 27909.2 中描述的混合密钥分级结构。

对称密钥应格式化为适合于加密操作的数据分组。由于非对称密码的数据分组大小一般比对称密码密钥的更大，因此在加密时，在一个数据分组中通常可以包括一个以上的密钥。此外，数据分组中还应包括格式化信息、随机填充字符和冗余字符(见 ISO/IEC 18033-2)。

5.2.3 用对称密码给非对称密钥加密

可使用对称密码对非对称密钥进行加密。

由于非对称密码系统的密钥长度通常大于对称密码的分组，所以非对称密钥可以格式化为多个数据分组并使用密码分组链(CBC)操作模式(见 GB/T 17964)或等价的操作进行加密。

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平均 $2^{s-1}T$ 的时间进行攻击时，可称该算法能够提供 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 GB/T 17964 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。

注:当前,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。

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} 个已知明文/密文对)	1024	160
112	112 位 3-DEA(不带已知明文/密文对)	2048	224
	168 位 3-DEA		

5.3 公钥认证

密钥认证是一种技术,当按照 ISO 15782-1 的要求使用时,可通过为密钥和相关有效数据创建一个数字签名来保证公钥的真实性。在使用公钥前,接受者通过验证数字签名来检验公钥的真实性。

用户的公钥和相关有效数据统称为用户的凭证。有效数据通常包括用户和密钥标识数据,以及密钥有效性数据(例如,密钥有效期)。公钥证书由被称为"认证机构"的第三方发布。公钥证书通过用认证机构所拥有的私钥签署用户凭证来创建,认证机构的私钥只能用于签署证书。

应使用独立通信方式来验证密钥的标识及其所有者合法且经授权,这可能要求通过一个渠道获得原始信息,然后通过另一个不同的渠道获得确认。

在公钥向被授权的接受者分发或在密钥数据库存储期间,应保证它的真实性。

5.4 密钥分离技术

5.4.1 概述

为保证存储密钥仅用于其预定目的,应以下述一种或多种方式进行存储密钥的分离:

a) 将存储的密钥按照其预定的功能进行物理隔离;

b) 存储由密钥加密密钥加密的密钥,该密钥加密密钥用于特定类型的密钥加密;

c) 在密钥加密存储之前,按照其预定功能修改密钥信息或向密钥追加信息,即进行密钥标记。

5.4.2 密钥标记

5.4.2.1 概述

密钥标记是一种识别存在于现有安全密码设备以外的密钥的类型及其用途的技术。密钥值和它的权限应采用某种方式绑定在一起,该方式应能防止两者中的任何一个遭到无法检测的篡改。

5.4.2.2 显式密钥标记

显式密钥标记使用一个字段,该字段包含定义相关密钥权限及其密钥类型的信息。这一字段与密钥值应采用某种方式绑定在一起,该方式应能防止两者中的任何一个遭到无法检测的修改。

5.4.2.3 隐式密钥标记

隐式密钥标记不依靠包含定义相关密钥权限及其密钥类型信息的显式字段的使用,而是依靠系统

的其他特征，如密钥值在记录中的位置，或者确定和限制该密钥的权限的其他相关功能。

5.5 密钥验证

密钥验证是一种在不泄露密钥值并且不使用公钥证书的情况下检查和验证密钥值的技术。该项技术使用的密钥验证码(KVC)是通过抗冲突的单向函数与此密钥进行密码关联的。例如，参考 KVC 可以通过对公钥、私钥和相关数据使用 ISO/IEC 10118 定义的哈希算法进行运算获得。

在首次生成 KVC 后，该密钥可以再次输入单向函数。如果后来生成的 KVC 与最初产生的 KVC 完全相同，就可认定此密钥值未被改变。

可以用密钥验证来确定下列条件中的一项或多项已满足：

a) 密钥已正确输入密码设备；

b) 密钥已通过通信信道正确收到；

c) 密钥未被篡改或替换。

对公钥来说，只要 KVC 能够通过保证其完整性的信道分配，公钥就可以通过不安全的信道来分发。在安装使用公钥前，用户应通过计算 KVC 并与参考 KVC 进行比较来验证公钥。

应保证不可能篡改/替换 KVC 和公钥(及其相关数据)并使两者仍然保持一致。这可以通过下述方式之一来实现：

——通过确保 KVC 完整性的方式(见 ISO 16609)；

——通过将参考 KVC 进行独立存储/分发的方式。在该方式中可保证参考 KVC 的篡改/替换不与公钥(及其相关数据)的篡改/替换同步进行(例如，双重控制)。

5.6 密钥完整性技术

5.6.1 公钥

应采用下述的一项或多项技术来保证公钥的完整性：

——使用数字签名系统签名公钥和相关的数据，从而创建公钥证书。用于创建和验证证书的密钥的管理见第 5.3 及第 6 章；

——通过 ISO 16609 中定义的算法及保证公钥完整性的密钥为公钥及相关数据生成 MAC；

——将公钥存储在安全密码设备中(见 GB/T 21079.1 及 GB/T 20547.2)；

——在不受保护的信道上分发公钥，在受完整性保护的信道上分发公钥验证码及相关数据，例如，具有双重控制的经鉴别的信道。密钥验证内容见 5.5；

——使用经鉴别的加密方法。

5.6.2 私钥

应采用下述的一项或多项技术来保证私钥的完整性：

——通过 ISO 16609 中定义的算法及保证私钥完整性的密钥为私钥及相关数据生成 MAC；

——将私钥存储在安全密码设备中(见 GB/T 21079.1 及 GB/T 20547.2)；

——使用经鉴别的加密方法；

——以完整性受到保护的密钥组件的方式存储；

——通过使用密钥对中的两个密钥对任意数据进行加/解密转化并将结果与期望结果进行比较的方式，验证私钥和被鉴别公钥是否构成有效的密钥对。该操作应全部在安全密码设备中实现并销毁所有中间及最终转换结果。

6 非对称密钥生命周期

6.1 密钥生命周期的各个阶段

密钥生命周期包括三个阶段：

a) 使用前：该阶段密钥对产生并且可被传输；

b) 使用中：该阶段公钥被分发给一方或多方用于操作使用，私钥保留在安全密码设备(SCD)中；

c) 使用后：该阶段密钥对中的公钥被归档，私钥被终止使用。

图1和图2中分别给出了私钥(S)生命周期和公钥(P)生命周期的示意图。图中显示了密钥是如何通过特定的操作改变其状态的。有关公钥证书的生命周期见ISO 15782-1。

密钥可被认为是单个对象，它的多个实例可以以不同形式存在于多个不同的位置。下列操作之间有明显的区分：

——给通信方分发公钥(见6.4)；

——向没有能力产生密钥对的所有者一方传输密钥对(见6.5)。

以及：

——销毁单个私钥的实例(见6.11)；

——从给定的位置删除私钥，即销毁该密钥在此位置的所有实例(见6.12)；

——私钥的终止，即从所有位置删除密钥(见6.14)。

对密钥执行的每一项操作都会改变密钥的状态，本章详细说明了获得给定状态或执行一给定操作的要求。6.2详细说明了各个生命周期阶段的要求。

注1：对归档私钥的要求不包括在本部分范围内。归档私钥用于后续对由相应公钥所加密的数据进行解密。

注2：后续的要求依赖于密钥对生成方法的实施。特别指出的是，密钥对由第三方非对称密钥对生成器生成或密钥对由所有者生成并存储，各个生命周期阶段的要求是不一样的。

6.2 密钥生命周期——生成阶段

6.2.1 概述

非对称密钥对的生成是为特定的非对称密码系统生成新密钥对的过程，该密钥对包含一个私钥和其相关公钥。非对称密钥对的两个密钥以特定的非对称密码系统中定义的某种数学关系联系在一起；并且从公钥推导私钥在计算上是不可行的。

密钥对生成应由密钥对的所有者或其代理方完成。

每个私钥和私钥组件应以这样一种方式生成，该方式应不可预测任何私钥，也不可确定某些私钥比可能的私钥集中的其他私钥更具可能性，参见参考文献[4]。在产生私钥和私钥组件的过程中应引入随机或伪随机值。

非对称密钥对的生成方式应保证私钥的机密性以及公钥的完整性。对用于不可否认服务的非对称密钥对的生成，应可以向第三方来证明公钥的完整性以及私钥的机密性。

私钥不应以可读形式存在。

如果密钥对由不使用该密钥对的系统生成，则：

——在确认传输已经完成后，密钥对和所有相关的机密种子元素应被立即擦除；

——应确保私钥的完整性。

非对称密钥对在生成时应包含更换日期以建立密钥对的生命周期。

非对称密钥对的长度应足够大以使攻击在计算上不可行。

非对称密钥对的生成应由认证机构(CA)、密钥对所有者或第三方授权机构完成。6.2.2 至 6.2.4 描述了密钥对生成机构的角色和责任。

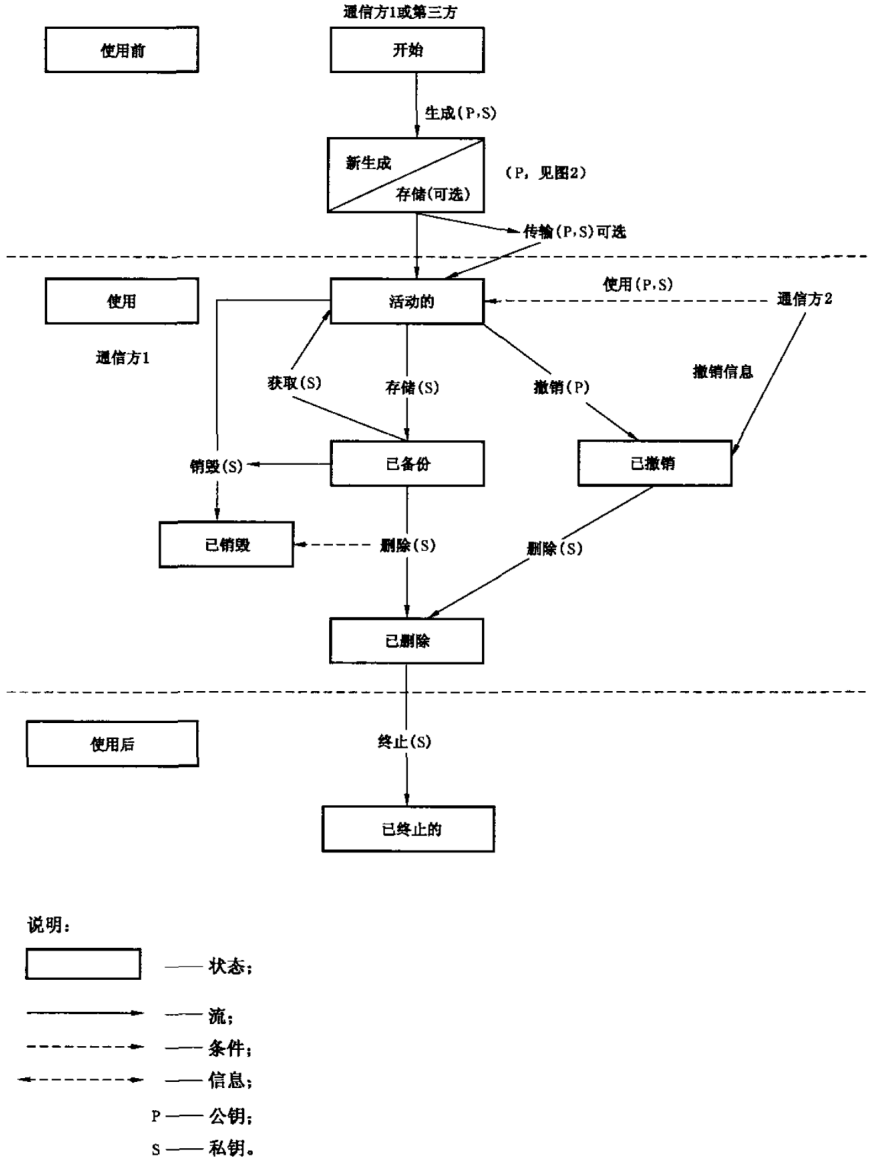

图 1　私钥生命周期

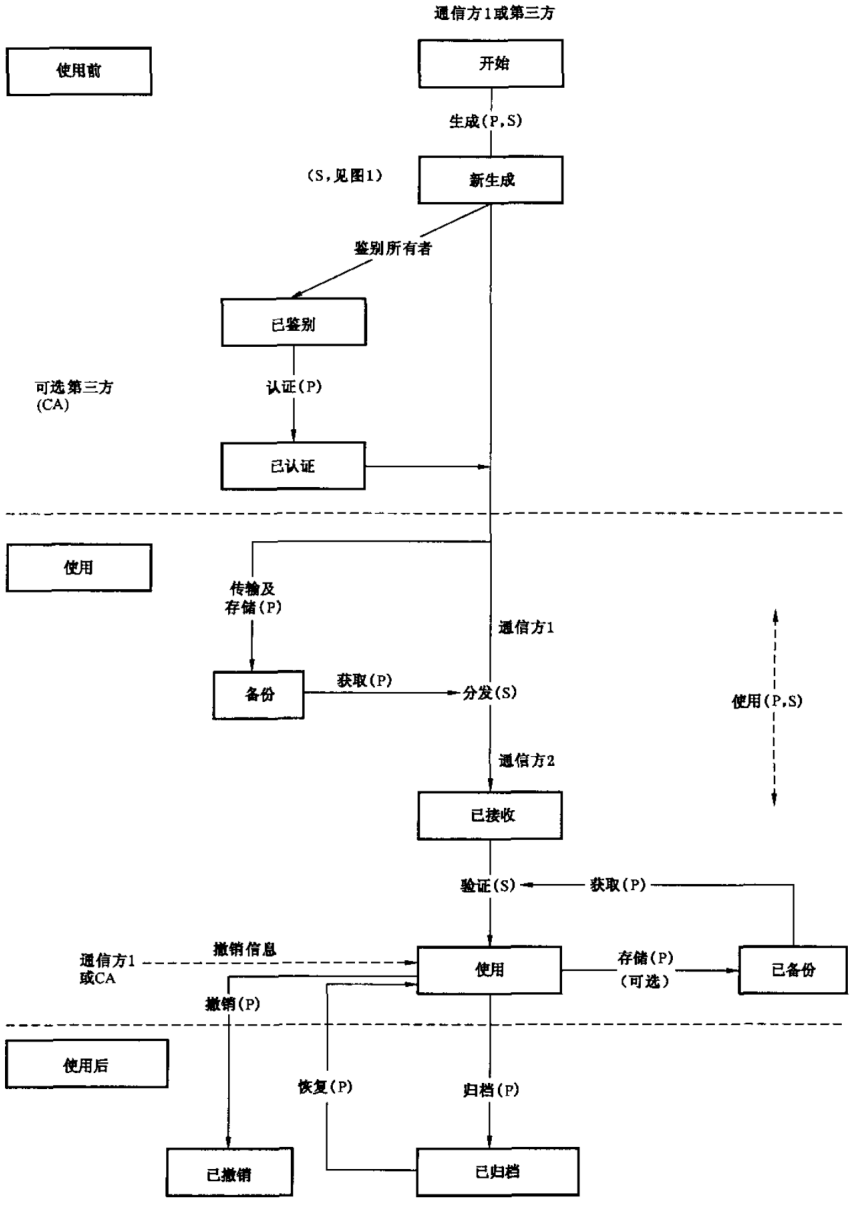
通信方1或第三方
使用前
开始
生成(P,S)
(S,见图1)
新生成
鉴别所有者
已鉴别
可选第三方
(CA)
认证(P)
已认证
使用
传输及
存储(P)
通信方1
备份
获取(P)
分发(S)
使用(P,S)
通信方2
已接收
验证(S)
获取(P)
通信方1
或CA
撤销信息
使用
存储(P)
(可选)
已备份
撤销(P)
使用后
恢复(P)
归档(P)
已撤销
已归档

图 2　公钥生命周期

6.2.2 认证机构

认证机构(CA)应在安全密码设备(SCD)中生成非对称密钥对,并将私钥按照 6.5 的要求传给密钥对所有者,将公钥以证书的形式传给密钥对所有者。

认证机构(CA)既不记录也不保留私钥及其他任何可能导致私钥泄露或重新生成的信息。

6.2.3 密钥对所有者

密钥对所有者应在安全密码设备中生成非对称密钥对,并满足下述要求之一:

——在使用密钥对的同一密码设备中生成该密钥对,或者;

——在能够安全地将私钥从生成它的密码设备传输到使用它的密码设备的设备中生成。

密钥对所有者应保留执行操作所需的最少私钥副本。

注:私钥实例越少,泄露的可能性越低,抗抵赖性越强。

6.2.4 第三方

第三方应在安全密码设备中生成非对称密钥对,并依据 6.5 中规定的要求将私钥传送给密钥对所有者。

第三方应根据 6.5.2 中规定的要求将公钥传送给密钥对所有者。

第三方不应记录和保留任何可能泄露私钥或者重新产生私钥的信息。

6.3 密钥存储

6.3.1 介绍

在密钥的存储过程中,应防止密钥非授权的泄露和替换,并且应提供密钥的分离机制。

私钥的存储要求保证机密性与完整性,公钥的存储要求保证真实性与完整性。

6.3.2 允许的私钥形式

6.3.2.1 概述

应当采用下述技术之一来存储私钥:

a) 明文密钥:在安全密码设备内;

b) 密钥共享组件:至少包含两个组件,其设计和管理方式应保证任何一方不可单独访问超过安全门限的组件数量(重建密钥需要的组件数量);

c) 加密的密钥:由密钥加密密钥进行加密。

6.3.2.2 明文私钥

明文私钥只允许存在于安全密码设备中。安全密码设备应遵循 GB/T 21079.1 描述的要求。

6.3.2.3 密钥分享组件

以至少两个单独的密钥分享组件形式存在的私钥应按照密钥分割和双重控制的原则进行保护。

对重构明文私钥的部分密钥分享组件的访问,不应泄露关于该私钥的任何信息。密钥分享组件应只被授权的个人或人员在所需的最短时间内访问。授权访问密钥某个组件的人不能访问该密钥的其他任何组件。

密钥分享组件应以对非授权访问有很高检出概率的方式存储。如果密钥分享组件以加密的方式存储,则密钥分享组件应满足对加密密钥的所有要求。密钥分享组件可以存储在密钥传输设备中(见

GB/T 20547.2)。

密钥分享组件应通过密钥信封或者密钥传送设备传输给被授权人。如果使用了密钥信封,密钥信封的印制方式应使得密钥分享组件在顺序编号的信封开启之前不可被获取。信封只应显示向被授权方传递密钥信封所需的最少信息。密钥信封的制作应当使收件人易于发现意外的或欺诈性的开启,在这种情况下,密钥分享组件应不再使用。如果密钥分享组件具有不安全的因素(例如,在密钥信封中以明文印制),应由唯一被授权人以单点方式及时访问,并且访问时间不超过组件被输入到安全密码设备所要求的时间。

6.3.2.4 加密的私钥

使用密钥加密密钥对密钥进行加密应在安全密码设备中进行。

私钥加密应按照 5.2.3 描述的方式进行。

6.3.3 允许的公钥形式

6.3.3.1 概述

非对称密码系统中对公钥的存储没有机密性的要求,但是应确保公钥的真实性与完整性。

应可以检测到任何对公钥或者相关信息的替换或篡改。

公钥只能以在 6.3.3.2 以及 6.3.3.3 中描述的明文或加密形式存储。

6.3.3.2 明文公钥

当公钥以明文形式作为证书存储时,应采用第 5 章描述的技术生成证书。

当公钥不以证书形式出现时,应对公钥的存储提供足够的保护,以确保可检测到任何对密钥值和其标识的修改,具体保护措施如下:

a) 以明文形式存储在可检测到未授权密钥替换的安全密码设备中,或者;

b) 采用 5.5 定义的密钥验证技术进行明文存储。

6.3.3.3 加密的公钥

在一些实例中,公钥的真实性和完整性可通过加密实现,例如,通过包含加密数据检验值。应按照 5.2 中定义的方式进行该类加密。

6.3.4 保护密钥在存储期间不被替换

当明文公钥不以证书的形式存储,或者证书经检验后而在使用时无需再次检验时,应根据 6.3.3 描述的方法以及第 5 章描述的技术保证密钥的完整性与真实性。

防止公钥在存储期间被替换是很重要的。例如,对用于加密的公钥的替换可对数据的机密性构成威胁。

防止公钥被替换的一种方法是采取与私钥相同的技术。另外一种方法就是将公钥存储在证书中,并允许在使用前对密钥的完整性与真实性进行验证。

应当通过以下一种或多种方法来防止对存储公钥的非授权替换:

a) 在物理上和流程防止对密钥存储区的非授权访问;

b) 根据使用目的不同将密钥加密存储,并且确保明文及其由该密钥加密密钥加密的相应密文不会均被知晓;

c) 保存包含公钥的证书,并在使用前验证证书。应保证用于验证此证书的公钥的真实性和完整性。

如果已知或怀疑有非授权的密钥替换发生,则应用正确的公钥进行更新。

6.3.5 密钥分离

为了确保非对称密钥对中的每个密钥只用于其预期目的，应通过以下一种或多种方法为存储的密钥提供密钥分离：

a) 根据使用目的不同对存储的密钥进行物理隔离；

b) 密钥存储前，由对特定类型密钥进行加密的密钥加密密钥进行加密；

c) 在对密钥加密存储前，根据使用目的不同修改或追加密钥信息；

d) 对于公钥，提供包含其用途的证书。

6.3.6 密钥备份

密钥备份指对密钥副本的存储，其目的是在密钥被意外破坏但尚未怀疑其泄露时进行密钥的恢复。

密钥副本应以允许的密钥存储形式保存。所有密钥副本应与当前使用的密钥保持相同或者更高的安全控制水平。

应使用与密钥存储相同的原则和技术来确保密钥副本的安全性。

6.4 公钥的分发

公钥分发是将公钥传输给准备使用公钥的通信方的过程。

公钥分发的方法(手工或自动)应保证公钥的完整性与真实性。

在分发过程中应防止公钥被替换，该目标可通过按照 6.3.3 描述的方式存储公钥来实现。

6.5 非对称密钥对的传输

6.5.1 过程

6.5.1.1 概述

非对称密钥对的传输是将密钥对和公钥证书传递给该密钥对的所有者的过程。该过程发生在密钥对的所有者没有能力生成密钥对时。

在传输密钥对之前应对所有者的身份进行鉴别。

公钥分发技术见 4.3。

密钥分发期间的防替换技术见第 5 章。

应使用本章描述的技术进行非对称密钥对公钥及私钥的传输，这些技术归纳在表 2 中。

ISO/IEC 11770-3 中提供了适用于公钥及私钥传输的有关技术。

表 2 允许的非对称密钥对传输技术

密钥形式	技术		
	手工	电子	
		直接	网络
明文密钥	P	P、S	P
密钥分享组件	P、S	P、S	P
加密密钥	P、S	P、S	P、S
证书	P	P	P
注：P 表示公钥；S 表示私钥。			

6.5.1.2 明文私钥

传输和导入明文私钥的通用要求为：

a) 密钥的传输过程应确保明文密钥的机密性和完整性；

b) 密钥的传输与导入过程应按照双重控制、密钥分割的原则进行；

c) 只有当安全密码设备至少鉴别了两个以上的被授权人身份时，如通过口令的方式，才可以传输明文私钥；

d) 只有确信安全密码设备在使用前没有受到任何可能导致密钥或敏感数据泄露的篡改时，才可以将明文私钥导入到安全密码设备中；

e) 只有确信安全密码设备接口处没有安装可能导致传输密钥的任何元素泄露的窃听装置时，才可以在安全密码设备之间进行明文私钥的传输；

f) 在生成密钥和使用密钥的设备间传输私钥时所使用的设备应是安全密码设备。在将密钥导入到目标设备后，密钥传送设备不应保留任何可能泄露该密钥的信息；

g) 当使用密钥传送设备时，密钥(如果使用显式密钥标识符，还包括密钥标识符)应从产生密钥的安全密码设备传输到密钥传送设备。这一便携设备应被物理运输到实际使用密钥的密码设备所在处。

对密钥传送设备应进行适当的监管，以确保私钥仅传送到预定的密钥使用设备。密钥(及其标识符)应由密钥传送设备传输到密钥使用设备内。

6.5.1.3 私钥分享组件

构成密钥的密钥分享组件应通过手工或密钥传输设备导入到设备中。

私钥分享组件传输与导入的通用要求为：

a) 密钥分享组件的传输过程不应向任何非授权的个人泄露密钥分享组件的任何部分；

b) 只有确信安全密码设备在使用前没有受到任何可能导致密钥或敏感数据泄露的篡改时，才可以将密钥分享组件加载到安全密码设备中；

c) 只有确信安全密码设备接口处没有设置可能导致传输的组件泄露的主动或被动的窃听机制时，才可以将密钥分享组件传输进安全密码设备；

d) 密钥的传输与导入过程应按照双重控制、密钥分割的原则进行；

e) 所需的密钥分享组件应由密钥分享组件持有者分别导入。
应使用 5.5 描述的密钥验证方法来验证密钥输入的正确性。当最后一个组件输入后，密码设备应执行构建密钥所要求的操作。

6.5.1.4 加密的私钥

加密的密钥可以通过通信信道以电子方式自动传输和导入。密钥加密密钥对密钥的加密应在安全密码设备中进行。该种情况应按照 5.2.3 中描述的要求实施。

加密的私钥的传输过程应防止密钥被替换或篡改。

密钥标识符和相关数据应随私钥一起传送。

6.5.2 公钥传输

公钥传输技术应确保密钥的真实性。

当密钥对不是由密钥所有者生成时，那么在分发公钥之前，密钥对所有者应验证所传输密钥对的正确性。验证过程是：通过使用密钥对中的一个对任意数据进行加密，使用另一个密钥进行解密并与预定结果进行比较来确认密钥对的正确性。验证操作应在安全密码设备中实现，并应将所有转换的中间和

最后的结果销毁。

6.6 使用前的真实性

在使用前应验证公钥的真实性和完整性，或公钥应以确保其操作期间的真实性和完整性的方式存在。

公钥应通过认证(见 5.3)或 5.5 描述的方法来提供上述保证。

6.7 使用

第 4 章对非对称私钥与公钥的使用进行了描述。

在非对称密码系统中，密钥对中的每个密钥都用于单独的功能。除非另有说明，密钥对的两个密钥应满足下述要求：

a) 应防止私钥的非授权使用；

b) 除去用于 5.1 描述的用途，一个密钥只能用于一个功能，例如，仅用于真实性或机密性；

c) 一个密钥只能在预定的位置用于预期的功能；

d) 私钥应存在于保持系统有效运行的最少位置上；

e) 密码周期结束或者已知或怀疑私钥已经泄露时，应停止密钥对的使用；

f) 公钥只有在其真实性与完整性经过验证并且正确时才可以使用；

g) 应保护私钥的机密性和完整性。因此，私钥不应在安全密码设备外使用；

h) 应实施物理控制和逻辑控制来防止密钥的非授权使用；

i) 公钥的接受者应在使用前验证公钥的完整性和真实性。

第 5 章给出了用于获得恰当的密钥分离和验证公钥完整性及真实性的技术列表。

应通过以下方式之一防止已被怀疑泄露的密钥的后续使用：

a) 从所有运行位置删除该密钥；

b) 阻断获得密钥的途径。

6.8 公钥的撤销

公钥的撤销是因以下原因之一而终止使用公钥的过程：

——私钥泄露；

——各种业务原因。

当发现私钥泄露时，相应的公钥应尽快撤销。如果被怀疑的密钥对是密钥加密密钥，那么在该密钥对级别下的所有密钥都应被终止。

出于各种业务原因，授权实体可以停止非对称密钥对的使用，在这种情况下，公钥应被撤销。

应通知公钥用户某个公钥已被撤销，一旦收到这样的通知，公钥用户应立即停止该公钥的使用。这样的通知可以是主动方式的，如向所有公钥用户发送公钥撤销信息；也可以是被动方式的，如将公钥撤销信息加入到公钥用户普遍访问的数据库中。

已被废除的公钥可能需要用来验证以前签名的信息，或者需要用于法律目的，此时公钥将从归档文件中恢复。

6.9 更换

密钥对的更换是新密钥对代替已撤销或已失效的密钥对的过程：

应通过重复适当的密钥生成、传输、分发和加载程序来实现密钥更换。

如果由于业务的原因引发密钥对失效或撤销，例如，更换安全密码设备的所有者，不必或不适合进行密钥对的更换。

在密钥对更换时，密钥对所有者应遵循密钥对生成的所有要求。

在密钥对更换时，密钥对所有者应遵循公钥注册的所有要求。

密钥更换应发生在：

a) 密码周期结束(当有效期到期)时；

b) 已知或怀疑私钥泄露时；

c) 按照业务需求。

在更换密钥的情况下，密钥对的公钥与私钥都应进行更换。

在认为可能对该密钥加密的数据成功实施攻击前，或者在通过密码分析攻击可能确定私钥前(参见参考文献[11])，应将密钥更换。这将取决于攻击时可用的具体实施方法和技术。

密钥对的更换应在该密钥对存在的所有操作位置进行。

被更换的密钥不应再激活使用。

密钥更换要求将旧的私钥销毁。

6.10 公钥失效

公钥在生成及签发使用前，拥有决定密钥对生命周期的失效日期。超过其失效日期后，不应再使用该公钥。

6.11 私钥的销毁

当私钥的实例不再需要处于激活状态时，则应将其销毁。私钥实例可通过擦除的方式销毁。但是，信息仍将驻留在操作位置，以便密钥随后还可恢复使用。

相应的公钥不应再分发给相关各方。如果公钥存储在相关各方所在的位置，则应通知他们相应的私钥已被销毁。

当安全密码设备从服务中永久删除时，设备中存储的全部私钥都应被销毁。

私钥的销毁可通过使用新密钥值或使用非机密值完全覆盖原密钥值实现，这样关于被擦除密钥的信息不会再保留。也可以按照 GB/T 21078.1 中描述的程序销毁密钥存储介质。

6.12 私钥的删除

当特定位置的某个私钥的所有实例都被销毁时，就会引起密钥删除。

私钥的删除可以通过在某一运行位置擦除所有形式的密钥来实现，无论该密钥是物理安全的、加密的还是密钥组件形式的。

当要删除以可读方式存在的密钥组件时，记录该密钥组件的介质应被焚毁或者以其他等效的方式销毁。

6.13 公钥的归档

公钥的归档是为了验证公钥撤销前发生的签名而进行的存储公钥的过程。在这样的验证之后，应销毁执行验证所需的密钥的实例。

只要存在可被该密钥验证的数据，则归档的公钥就应被安全存储以保证它的完整性。

应保证公钥归档的安全级别与公钥存储的安全级别相同(见 6.3)。

将归档密钥与活动密钥分离以及防止活动密钥被归档密钥替换，该方面的要求应按照 GB/T 27909.2 和 5.4 中描述的相应技术来完成。

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。

6.14 私钥的终止

当私钥在曾经出现的所有位置被删除时发生私钥终止。继私钥终止之后，任何可能重建该私钥的

信息都不应再存在。

注：不必进行私钥归档。

按照 6.12 中规定的要求与方式，在所有位置销毁所有的密钥实例即可实现私钥终止。

6.15 擦除概要

见表 3。

表 3 擦除的效果

操作	位置	影响的信息	
		密钥实例	重建信息
销毁	单一位置	擦除单一实例	—
删除	单一位置	擦除所有实例	擦除
终止	所有位置	擦除所有实例	擦除

6.16 可选的生命周期过程

6.16.1 公钥认证

公钥认证是通过称为认证机构的可信第三方，来建立公钥和其他相关信息与所有者之间的关联性证明的过程。

有关密钥认证与认证机构的详细信息见 5.3。

用于验证证书公钥的认证机构(CA)的公钥应使用一种经过鉴别的方式传输给用户。

6.16.2 密钥的重新获取

从备份中重新获得公钥的操作应根据 6.4 中描述的公钥分发和加载方法之一来实现。

从备份中重新获得私钥的操作应根据 6.3 中描述的私钥存储方法之一来实现。

参 考 文 献

[1] ISO/IEC 9797-1 信息技术 安全技术 报文鉴别码 第1部分:使用分组密码技术的机制

[2] ISO/IEC 9797-2 信息技术 安全技术 报文鉴别码 第1部分:使用哈希函数的机制

[3] ISO/IEC 11770-1:1996 信息技术 安全技术 密钥管理 第1部分:框架

[4] ISO/IEC 11770-2:1996 信息技术 安全技术 密钥管理 第2部分:使用对称技术的机制

[5] ISO/IEC 18032 信息技术 安全技术 素数生成

[6] ISO 21188 用于金融服务的公钥基础设施 实施和策略框架

[7] ANSI X9.57 金融服务业的公钥密码 证书管理

[8] 如何分享秘密,SHAMIR,A.编著,1979年11月 Communications of the ACM 出版

[9] ISO/IEC 18033-3 信息技术 安全技术 加密算法 第3部分:分组密码

[10] MENEZES,A.,VAN OORSCHOT,P.以及 VANSTONE,S.编著的实用密码学手册,1996年 CRC 出版社出版

[11] 特别报告(800-57) 密钥管理建议 第1部分:国家标准和技术机构

[12] ISO/IEC 9796-3 信息技术 安全技术 实现报文恢复的数字签名方案 第3部分:基于离散对数的机制

[13] ISO 9807 银行业务与相关金融服务 报文鉴别要求(零售)

[14] ANSI X9.30-1 金融服务业的公钥密码 第1部分:数字签名算法(DSA)

[15] BSR X9.102-200x 金融服务业的对称密钥密码 密钥及相关数据的封装

[16] AS 2805.5.3 电子资金转账 接口要求 密码 数据加密算法2(DEA 2)