ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 21082.5—2007/ISO 11568-5:1998

银行业务　密钥管理(零售)　第5部分：公开密钥密码系统的密钥生命周期

Banking—Key management (retail)—
Part 5:Key life cycle for public key cryptosystems

(ISO 11568-5:1998,IDT)

2007-09-05 发布　　2007-12-01 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

中 华 人 民 共 和 国
国 家 标 准
银行业务 密钥管理(零售) 第5部分:
公开密钥密码系统的密钥生命周期
GB/T 21082.5—2007/ISO 11568-5:1998
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
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 34千字
2007年12月第一版 2007年12月第一次印刷
*
书号:155066·1-30269 定价 18.00元

GB/T 21082.5-2007

前　言

GB/T 21082《银行业务　密钥管理(零售)》分为如下6个部分：

——第1部分　密钥管理介绍；

——第2部分　对称密码的密钥管理技术；

——第3部分　对称密码的密钥生命周期；

——第4部分　使用公开密钥密码的密钥管理技术；

——第5部分　公开密钥密码系统的密钥生命周期；

——第6部分　密钥管理方案。

本部分是GB/T 21082的第5部分。

本部分等同采用国际标准ISO 11568-5:1998《银行业务　密钥管理(零售)　第5部分:公开密钥密码系统的密钥生命周期》(英文版)。

为便于使用,对于ISO 11568-5:1998本部分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归口管理。

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、招商银行、华北计算技术研究所、启明星辰有限公司。

本部分主要起草人:谭国安、杨竑、陆书春、李曙光、林中、张启瑞、史永恒、赵宏鑫、李红新、徐伟、董永乐、王林立、周亦鹏、熊少军。

本部分为首次制定。

引　言

GB/T 21082 描述了在零售银行环境下，对用于保护诸如收单行和受卡方之间，或收单行和发卡方之间的报文的密钥进行安全管理的过程。用于集成电路卡的密钥管理不包括在 GB/T 21082 标准中。

鉴于批发银行交易环境下的密钥管理以相对的高安全性环境中的密钥交换为特征，而本标准描述的密钥管理要求适用于零售银行服务中可访问区域。这种典型的服务有销售点/服务点(POS)的借记、贷记授权以及自动柜员机交易。

GB/T 21082 本部分描述了公开密钥密码系统密钥安全管理中的密钥生命周期。

公开密钥密码系统使用公钥和私钥。这些密钥在 GB/T 21082 本部分中合称为密钥对。

第 4 章陈述了密钥对生命周期各个阶段的通用安全要求，采用了 ISO 11568-1:1994 和 ISO 11568-4:1998 中描述的密钥管理原则、服务和技术。

第 5 章规定了对与这些总体安全要求相关的实施方法的要求。

密钥生命周期包括三个阶段：

1. 待活动阶段：期间密钥对被产生并且可被传输。
2. 活动阶段：期间公钥被分发给至少一方或多方用于操作使用。
3. 后活动阶段：期间密钥对中的公钥被归档，私钥被终止使用。

私钥(S)生命周期和公钥(P)生命周期的示意图相应地在图 1 和图 2 中分别给出。图中显示了对密钥的特定操作是如何改变其状态的。

密钥可以被认为是单个对象，其多个实例可以以不同的形式存在于多个不同的位置。在以下操作之间可以做出明显的区分：

——给通信方分发公钥；

——在所有者一方没有能力产生密钥对的实现方法中，向其所有者传输密钥对。

和：

——销毁单个私钥的实例；

——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；

——私钥的终止，即从所有位置删除密钥。

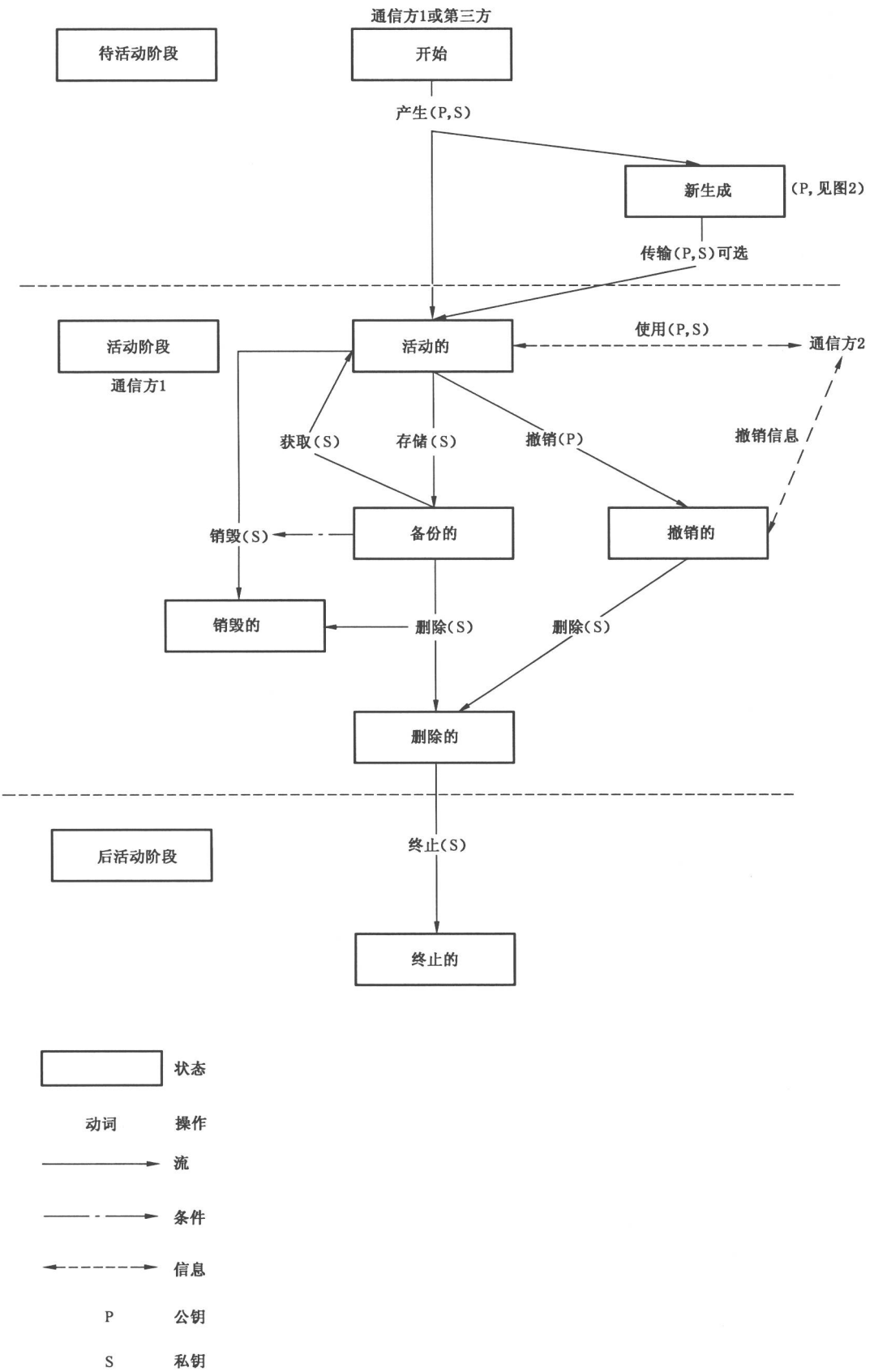

图 1　私钥生命周期

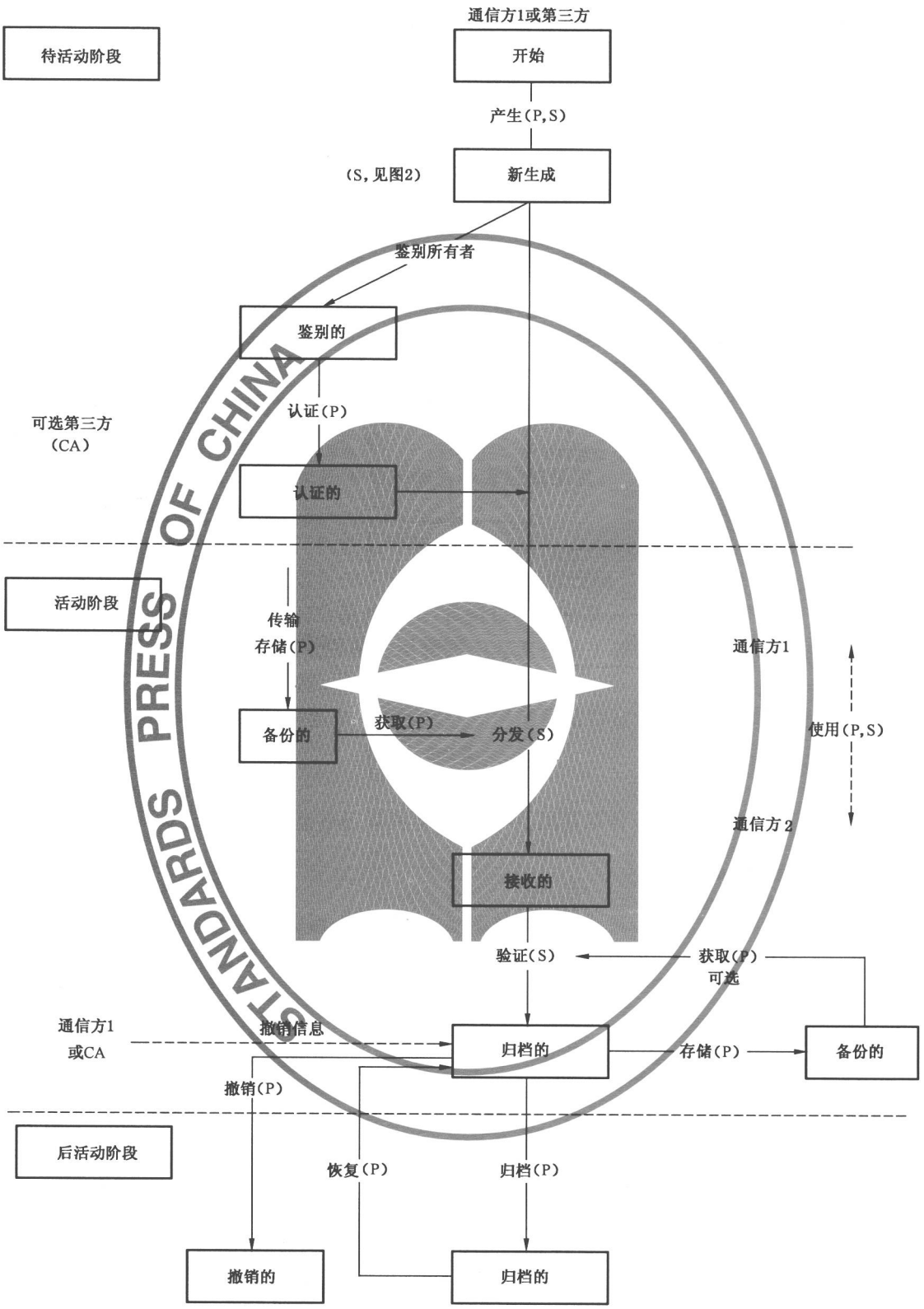
通信方1或第三方
待活动阶段
开始
产生(P,S)
(S,见图2)
新生成
鉴别所有者
鉴别的
认证(P)
可选第三方
(CA)
认证的
活动阶段
传输
存储(P)
通信方1
备份的
获取(P)
分发(S)
使用(P,S)
通信方2
接收的
验证(S)
获取(P)
可选
通信方1
或CA
撤销信息
归档的
存储(P)
备份的
撤销(P)
后活动阶段
恢复(P)
归档(P)
撤销的
归档的

图 2 公钥生命周期

目　次

银行业务　密钥管理(零售)　第5部分：公开密钥密码系统的密钥生命周期

1　范围

本部分详细描述了在零售银行业务环境下的安全要求，以及对非对称密钥对的私钥和公钥在密钥生命周期中每一阶段的实现方法。

本部分适用于任何实现密钥管理技术的机构，它所管理的公开密钥密码系统用于实现对数据的保护。

2　规范性引用文件

下列文件中的条款通过GB/T 21082的本部分的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB/T 17901.1—1999　信息技术　安全技术　密钥管理　第1部分：框架(idt ISO/IEC 11770-1:1996)

GB/T 21082.4—2007　银行业务　密钥管理(零售)　第4部分：使用公开密钥密码的密钥管理技术

ISO 8908:1993　银行业务及相关金融服务　词汇和数据元

ISO 9564-1:2002　银行业务　个人识别码的管理与安全　第1部分：个人识别码(PIN)的保护原则与技术

ISO 11568-1:1994　银行业务　密钥管理(零售)　第1部分：密钥管理介绍

ISO 11568-2:1994　银行业务　密钥管理(零售)　第2部分：对称密码的密钥管理技术

ISO 11568-3:1994　银行业务　密钥管理(零售)　第3部分：对称密码的密钥生命周期

ISO/IEC 11770-3:1999　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 13491(所有部分)　银行业务　安全密码设备(零售)

3　术语和定义

ISO 8908:1993标准中确立的以及以下术语和定义适用于本部分。

3.1

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

用于生成非对称密钥对的安全密码设备。

3.2

通信方　communicating party

接收公钥，用于与公钥所有者通信的一方。

3.3

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、视觉鉴别等等)。

4 通用要求

对密钥进行的每一步操作都会改变密钥的状态。本章详细说明了为获得特定状态或实施特定操作的要求。

在以下子条款中规定了生命周期内各阶段中适用的要求。

值得注意的是,此后的要求可能取决于生成密钥对的实现过程。尤其是当密钥对由第三方的非对称密钥对生成器生成时或者当密钥对所有者生成并存储了自己的密钥对时,那么这些要求将会不同。

4.1 非对称密钥对的生成

非对称密钥对的生成是产生可以在特定非对称密码系统中使用,包含一个私钥和相关公钥的新密钥对的过程。在这一过程中,也可能产生其它的非对称密钥信息。这一过程的输入可能还需要预先设定的值。

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的一种方式生成,这种方式使预测任何私钥或者确定某些私钥比可能的私钥集中的其他私钥更具可能性都是不可行的。在适当的情况下,根据非对称密码算法的特点,产生私钥和私钥组件的过程应结合随机或伪随机值。

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。

私钥在生成过程中,不应在任何时候以可理解的方式对任何人可用。

如果密钥对由不使用该密钥对的系统生成,则:

a) 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删除;

b) 此外,应确保私钥的完整性。

非对称密钥对在生成时应有有效期以建立密钥对的生命周期。

密钥对的生成过程应符合 GB/T 21082.4—2007 中规定的要求。

注:附加信息,例如所有者身份、密钥类型、有效期,应结合到公钥中,以避免通过公钥替换进行否认。

4.2 使用前的真实性

在使用前以及整个生命周期内,应确保公钥的真实性。应通过认证提供相应的保证。

4.3 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。

密钥认证与认证机构在 GB/T 21082.4—2007 中作出了详细说明。

用于验证证书公钥的 CA 公钥应使用一种经过鉴别的方式传输给密钥对的所有者。

4.4 非对称密钥对的传输

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认证。

4.4.1 私钥的传输

私钥只能通过本节中规定的下述形式之一进行传输:

a) 明文私钥;

b) 私钥组件;

c) 加密的私钥。

4.4.1.1 明文私钥

传输和加载明文私钥的通用要求为:

a) 密钥的传输过程不应泄露明文密钥的任何部分;

b) 密钥的传输与加载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，才可以将明文私钥加载到安全密码设备中；

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

f) 当使用一个设备在生成密钥的密码设备和使用密钥的密码设备之间传输私钥时，此设备应是安全密码设备。在将密钥加载到目标设备后，密钥传输设备不应保留任何可能泄露该密钥的信息。

4.4.1.2 私钥组件

私钥组件传输与加载的通用要求为：

a) 密钥组件的传输过程不应向任何非授权的个人泄露密钥组件的任何部分；

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可能导致传输的组件泄露的窃取装置时，才可以将密钥组件传输进安全密码设备；

d) 密钥的传输与加载过程应按照双重控制、密钥分割的原则进行。

4.4.1.3 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加载。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。

这种情况下应采用在 ISO 11568-2:1994 和 GB/T 21082.4—2007 中描述的要求。

加密的私钥的传输过程应防止密钥被替换或更改

4.4.2 公钥的传输

公钥的传输技术应确保密钥的真实性。这些技术应与私钥的传输中所使用的技术相同。

4.5 密钥存储

在密钥的存储过程中，应防止密钥非授权的泄露和替换。应提供密钥的分散。

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。

4.5.1 允许的私钥形式

私钥只能以 4.4.1 中定义的形式存储。

4.5.1.1 明文私钥

明文私钥只允许存在于安全密码设备中。

4.5.1.2 密钥组件

以至少两个单独的密钥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。

所形成的密钥的每一位都应是所有密钥组件的函数。

当在多个场合必须生成相同的密钥值时，应使用不同的密钥组件集。如果产生新的组件，这些密钥组件中任意一个的值都不应相同，除非偶然。

密钥组件应只被授权的个人或人员组在所需的最短时间内访问。

若密钥组件以人可以理解的形式存在(例如在密钥信封中以明文打印)，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，并且时间长短只能是将密钥组件输入到安全密码设备中所需的时间。

能访问密钥的某一个组件的人不能访问该密钥的其它任何组件。

密钥组件应以对非授权访问有很高检测概率的方式存储。如果密钥组件以加密的方式存储，对加

密的密钥的所有要求都应采用。

4.5.1.3 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。

在这种情况下，应采用 ISO 11568-2:1994 和 GB/T 21082.4—2007 中规定的要求。

4.5.2 允许的公钥形式

非对称密码中对公钥的存储没有机密性的要求，但是真实性与完整性是必需的。

对于替换或更改任何公钥或者相关信息的行为都应该可以检测得到。

考虑到这些要求，公钥只能以下列形式存储：

a) 证书内的明文密钥；

b) 加密的密钥。

由于公钥不需要保密，密钥组件的使用相应地也就不再具有价值。

4.5.2.1 明文公钥

如果公钥不被认证，则其存储方式应提供充分的保护，确保可以检测到密钥值和它的标识的修改。

在以电子方式存储公钥时，强烈希望对公钥进行认证。

4.5.2.2 加密的公钥

尽管公钥不需要机密性，而保证公钥真实性与完整性的一个途径就是以加密形式对密钥进行存储。在这种情况下，应采用 ISO 11568-2:1994 和 GB/T 21082.4—2007 中规定的要求。

4.5.3 保护密钥在存储期间不被替换

当明文公钥不以证书的方式存储，或者其证书已被核对，使用时无需再次检验证书时，应根据 5.5.3 描述的方法以及 GB/T 21082.4—2007 中描述的技术保证密钥的完整性与真实性。

4.5.4 密钥分散的规定

为保证给定的密钥只能用于指定的目的，应当根据 5.5.4 中规定的方法以及 GB/T 21082.4—2007 中描述的技术(例如密钥标记)进行密钥分散。

4.5.5 密钥备份

密钥备份是存储密钥的副本，其目的是在密钥被意外破坏但未怀疑其泄露时进行恢复。

备份的副本应以允许的密钥存储形式之一保存。所有密钥备份副本的安全控制水平应与当前使用的密钥相同或者更高。

如果私钥备份副本保留在安全密码设备中，应采用有效的用户验证(例如访问标识符和口令或其他方式)控制对存储数值的访问，防止非授权地使用该密钥。

4.6 密钥的重新获取

从备份重新获取公钥的要求与 4.7 中描述的公钥分发的要求相同。

从备份重新获取私钥的要求与私钥的传输要求相同。

4.7 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。

公钥可以手工分发或通过通信信道自动分发。

对公钥进行分发的过程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，最好采用密钥认证的方法。

注：密钥认证在 GB/T 21082.4—2007 中说明。

4.8 公钥证书验证

公钥证书验证过程是指通信方验证收到的公钥属于预定的所有者并将用于指定的用途。

有关密钥验证将在 5.8 中进行描述。

4.9 密钥的使用

GB/T 21082.4—2007 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，以下要求对密钥对的两个密钥都适用。

应防止密钥的非授权使用，因此：

a) 一个密钥只能用于一个功能；

b) 一个密钥只能在预期的位置用于预期的功能；

c) 私钥应存在于保持系统有效运行的最少位置上；

d) 在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；

e) 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。

4.10 公钥注册

公钥注册是为了达到真实性的目的，密钥对所有者向授权机构注册适当凭证和相应公钥的过程。

值得注意的是，授权机构可以是使用公钥证书提供真实性证明的认证机构。

密钥对所有者应向公钥用户提供他们的公钥的真实性证明。

密钥对所有者应在授权机构，如认证机构注册他们自己的公钥。

4.11 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：

a) 公钥有效期过期；

b) 私钥泄露；

c) 各种业务原因。

公钥在生成并发布使用的时候有一个有效期限，该期限确定密钥对的生命周期。超出有效期的公钥应不再使用并自动撤销。

当发现私钥泄露时，相应的公钥应被撤销。

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。

公钥用户应被告知[1]某个公钥已被废除，收到这样的通知应立即停止该公钥的使用。

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。

4.12 密钥的更换

密钥更换应发生在：

a) 密码周期结束(当有效期到期)时，或者

b) 已知或怀疑私钥泄露时。

在更换密钥的情况下，密钥对的公钥与私钥都应进行更换。如果受怀疑的密钥对被用作密钥加密密钥，则在该密钥对之下的各级密钥也都应被更换。

在更换密钥的情况下，相应的密钥证书也应如 GB/T 21082.4—2007 中所描述的那样予以撤销。

在认为可能对该密钥加密的数据成功实施字典攻击的时间内，或者在通过密码分析攻击确定私钥的时间内，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。

如果确信或已知用于解密的密钥已经泄露，则应通知通信方不再使用该密钥对。

在密钥存在的所有操作位置都应该进行密钥对的更换。

被更换的密钥不应再激活使用。

只应通过分发新的公钥来更换密钥对。密钥更换要求将旧的私钥销毁。

4.13 私钥的销毁

当私钥的实例不再需要处于激活使用状态时，则应将其销毁。私钥的电子化实例可以通过擦除的方式销毁。但是，信息仍将驻留在操作位置，以便密钥日后还可以恢复使用。

---

1) 通知可以是主动的，如向所有公钥用户广播某个公钥已经撤销，也可以是被动的，如在通常可访问的数据库中发布撤销公告。

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。

当安全密码设备可以访问，并且已知将从服务中永久删除时，在曾经用于或可能用于任何密码目的的设备中存储的全部私钥都应被销毁。

4.14 私钥的删除

当在特定操作位置不再需要私钥时，私钥应被删除。

当在特定位置某个私钥的所有实例都被销毁时，就会引起密钥删除。

4.15 私钥的终止

当私钥在曾经产生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。

4.16 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。

只要可被该密钥验证的数据存在，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 4.5)。

4.17 密钥对的恢复

密钥对的恢复是用新密钥对更换已撤销的密钥对的过程。

如果密钥对已经过期或者因业务原因而被撤销，密钥对的更换可能不是必需或适合的。

如果私钥被泄露，则应立即撤销公钥，并且可以用新生成的密钥对进行替换。

在密钥对恢复期间，密钥对所有者应遵循有关密钥对生成的所有要求。

在密钥对恢复期间，密钥对所有者应遵循有关公钥注册的所有要求。

5 实现的要求

在整个密钥生命周期中，应对用于存储和管理密钥的设备和程序进行控制和审计，以防止或检测密钥的泄露。

5.1 非对称密钥对的产生

应按照在 GB/T 21082.4—2007 中描述的要求来生成密钥对和密钥组件。

应使用适当的非对称密钥对生成器来实现非对称密钥对的生成。

应使用随机或伪随机过程以保证生成不重复的密钥对。

非对称密钥对的生成过程由认证机构(CA)、密钥对所有者或者授权第三方来完成。

以下三个子条款分别描述了认证机构、密钥对所有者、授权第三方的角色和责任。

5.1.1 认证机构

CA 应在安全密码设备中生成非对称密钥对，并依据 4.4 中规定的要求将私钥传送给密钥对所有者。

CA 应通过证书将公钥传送给密钥对所有者。

CA 不应记录和保留任何可能泄露私钥或者允许重新产生私钥的信息。

5.1.2 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，并且应：

a) 在使用密钥对的同一密码设备中生成该密钥对；

b) 或者直接将私钥从生成此私钥的设备注入到使用该私钥的设备中。

密钥对所有者应保留执行操作所需的最少私钥副本[2)]。

2) 私钥的实例越少，泄露的可能性越低，抗抵赖性越强。

5.1.3 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 5.4.1 中规定的要求将私钥传送给密钥对所有者。

第三方应根据 5.4.2 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。

5.2 使用前的真实性

如果证书准备开始使用，应使用 GB/T 21082.4—2007 中描述的程序来确保密钥及其所有者的真实性和完整性。

应使用独立通信来验证密钥及其所有者的身份信息正确无误并已经授权。该过程需要通过与最初获得信息的信道不同的其他信道来获得确认。

5.3 公钥认证

GB/T 21082.4—2007 中描述了公钥认证的实现。

5.4 非对称密钥对的传输

应通过下述技术之一进行非对称密钥对的传输。

应当在安全密码设备中存储密钥对，例如 ISO 13491-1 中描述的密钥传输设备。

允许的非对称密钥对传输方式在表 1 中描述。

5.4.1 私钥的传输

5.4.1.1 明文私钥

当明文私钥以电子方式直接在两个安全密码设备之间进行传输时，应保证这些设备彼此直接连接（没有窃取装置介入）并且在持续的双重控制下运行。

应保护私钥不被泄露和替换。直到私钥已经成功安装时才可以进行公钥的分发。

表 1 允许的非对称密钥对传输方式(P:公钥，S:私钥)

技术 密钥形式	手工的	电子化的		
		直接	设备	网络
明文密钥	P	P,S	P,S	P
密钥组件	P,S	P	P	P
加密的密钥	P,S	P,S	P,S	P,S
证书	P	P	P	P

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。对密钥传送设备应进行恰当的监管，以确保私钥仅传送到预定的密钥使用设备。然后，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。如果该密钥使用设备是一个交易发起设备，则该密钥应立即从密钥传送设备擦除。明文密钥的传送应根据以上电子化直接密钥载入的规定进行。

5.4.1.2 私钥组件

当使用密钥组件时，形成密钥的组件应手工地或使用密钥传送设备输入到设备内。当密钥组件以人可理解的形式分发时，每个这样的组件应在一个文件内进行分发，该文件在打开之前不能泄露组件的值。

密钥组件输入前应检查该文件是否有篡改的痕迹。如果发现对任何一个组件的篡改，则整套组件都不应使用，且应根据 ISO 9564-1:2002 概述的程序进行销毁。

密钥组件应由每个密钥组件持有人单独输入。应使用 ISO 11568-3:1994 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，密码设备应实现构建密钥所要求的动作。如果提供按照 ISO 11568-3:1994 描述的方法产生的密钥验证码，就应使用该密钥验证码来验证密钥输入的正

确性。

如果可行,每个密钥组件和所生成的密钥的密钥验证码都应被验证。

5.4.1.3 加密的私钥

密钥标识符和相关数据应随私钥一起传送。私钥应按照 GB/T 21082.4—2007 的描述进行加密。

5.4.2 公钥传输

公钥传输技术应确保密钥的真实性;它们应与私钥传输所使用的技术相同。

当密钥对不是由密钥所有者生成时,那么在分发公钥之前,密钥对所有者应使用私钥来验证公钥传输的正确性。

5.5 密钥存储

本节描述了每一种允许形式的安全密钥存储的实施。

通过实施 5.5.1 中描述的一种安全密钥存储形式来保护私钥免遭非授权的泄露。

通过 5.5.2 中描述的一种安全密钥存储形式来防止对私钥和公钥的替换。

对已知、怀疑或预计已经被替换了的密钥进行更换时需要执行 5.10 描述的程序。

5.5.1 允许的私钥形式

应当使用如下所述的技术之一来存储私钥:

a) 明文密钥:在安全密码设备内;

b) 密钥组件:包含至少两个组件,其设计保证即使知晓除一个组件以外的其他所有组件,也不能对密钥轻易造成攻击。各密钥组件应当分离存储并被不同的实体所控制;

c) 加密的密钥:由密钥加密密钥进行加密。

5.5.1.1 明文私钥

安全密码设备应遵循 ISO 13491-1 描述的要求。

5.5.1.2 密钥组件

密钥组件应通过密钥信封或者密钥传送设备传输给被授权人。

密钥信封的打印方式应使密钥组件在信封拆封之前不可以被观察到。信封只应显示向被授权方传递密钥信封所需的最少信息。密钥信封的构建应当使收件人易于发现意外的或欺诈性的打开,在这种情况下,密钥组件应不再使用。

当密钥组件被输入到安全密码设备后,密钥信封应被销毁。

存储在密钥传送设备中的密钥组件应当通过充分的访问控制进行保护,例如通过口令的方式。

5.5.1.3 加密的私钥

私钥的加密应当按照 ISO 11568-2:1994 和 GB/T 21082.4—2007 中的规定实施。

当使用对称密码对密钥对的私钥进行加密时,相应的密钥加密密钥应当是双长度密钥。而且,由于私钥的长度通常大于块的大小,因此应当使用密码块链模式。

5.5.2 允许的公钥形式

5.5.2.1 明文公钥

当公钥以明文形式作为证书存储时,应采用 GB/T 21082.4—2007 中描述的技术用于证书的生成。

当公钥不作为证书呈现时,应当以明文形式存储在经过设计、可检测到非授权的密钥更换的安全密码设备中。

5.5.2.2 加密的公钥

在某些实施中,可以将公钥加密存储以保证其完整性。这种情况下应采用 ISO 11568-2:1994 和 GB/T 21082.4—2007 中描述的技术。

5.5.3 防止密钥在存储期间被替换

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导致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此公钥存储在证书中，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) 从物理上和程序上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，并且确保选定的明文及其由该密钥加密密钥加密的相应密文不会都被知晓；

c) 保存包含公钥的证书，并在使用前验证密钥。

实现防止密钥替换的技术在 GB/T 21082.4—2007 中有更为详细的描述。

如果已知或怀疑有非授权的密钥替换发生，则应重新分发公钥。

5.5.4 密钥分散的规定

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散：

a) 根据使用目的不同对存储的密钥进行物理隔离；

b) 密钥由指定用于对特定类型密钥进行加密的密钥加密密钥加密后存储；

c) 在对密钥加密存储前，根据使用目的不同对密钥修改或附加相关信息；

d) 对于公钥，提供包含其用途的证书。

5.5.5 密钥备份

使用与密钥存储相同的原则和技术来确保密钥备份。

5.6 密钥的重新获得

从备份中重新获得公钥应根据 5.7 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应根据 5.5 中描述的私钥存储方法之一来实现。

5.7 公钥分发

用于公钥分发的技术在 GB/T 21082.4—2007 中描述。

分发过程中保护免遭替换的技术在 GB/T 21082.4—2007 中描述，它们是：

a) 使用证书；

b) 为公钥附加报文鉴别码(MAC)或使用数字签名技术；

c) 加密公钥；

d) 通过独立信道确认密钥值和相关信息。

5.8 公钥验证

公钥真实性的验证应通过以下任意一种方法来实现：

a) 通过对称密码关系的安全通道；

b) 在证书内分发公钥；

c) 通过独立信道确认密钥值和相关信息。

实现公钥证书验证的技术在 GB/T 21082.4—2007 中描述。

5.9 密钥使用

私钥用于解密密钥或产生数字签名；公钥用于加密密钥或验证签名。

应保护私钥的机密性。因此，私钥不应在安全密码设备外使用。

固定设备，如主机安全模块，可以用于操作私钥。如果密钥被存储，这样在线访问是可能的，则应采用安全方法防止密钥的非授权使用。

应实施物理控制和逻辑控制来防止密钥的非授权使用。

接收公钥应在使用前验证其完整性和真实性。

GB/T 21082.4—2007 包含用于获得恰当的密钥分散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怀疑泄露密钥的后续使用：