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

目　　次

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。

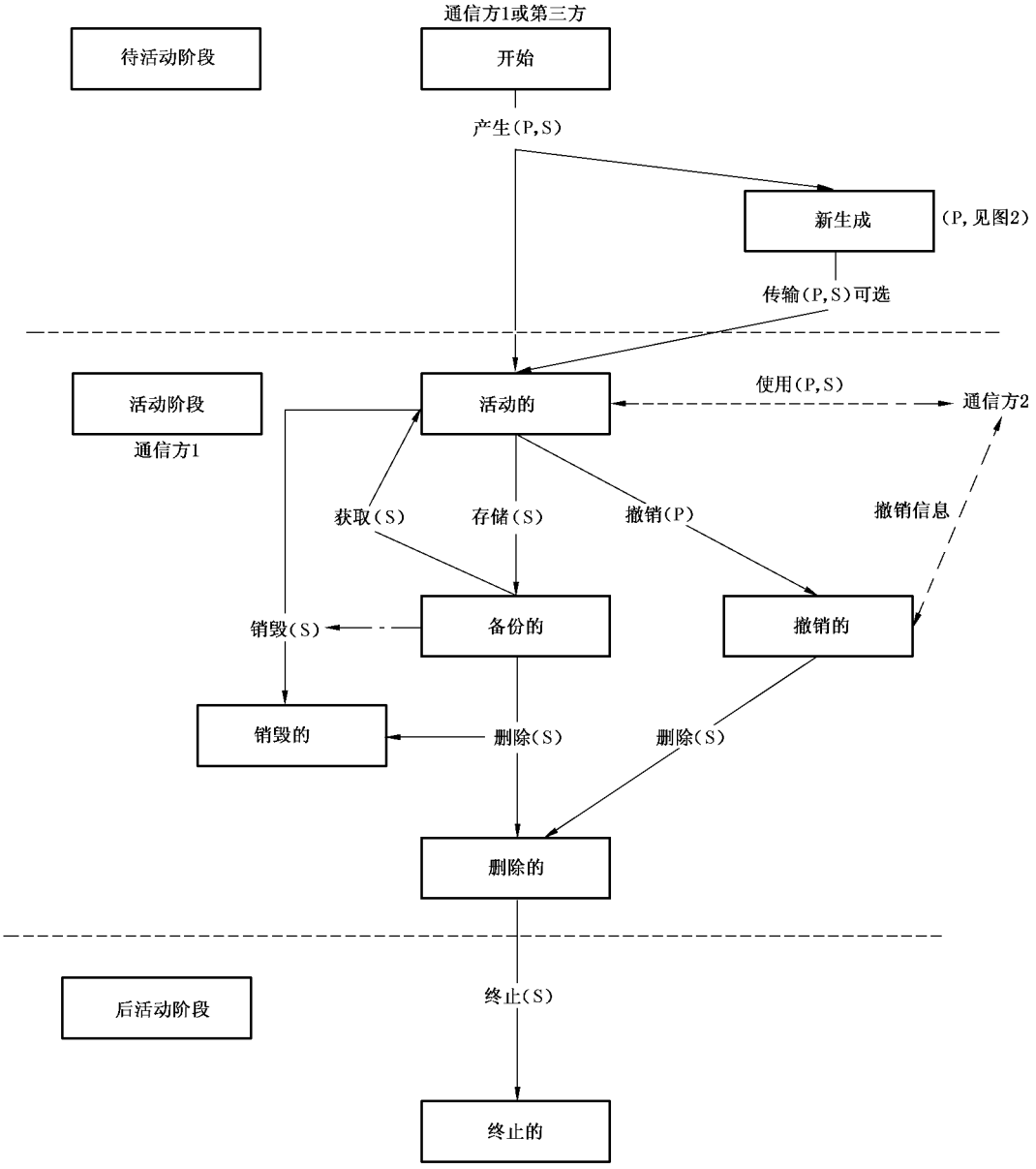
通信方1或第三方
待活动阶段
开始
产生(P,S)
新生成
(P,见图2)
传输(P,S)可选
活动阶段
通信方1
活动的
使用(P,S)
通信方2
获取(S)
存储(S)
撤销(P)
撤销信息
销毁(S)
备份的
撤销的
销毁的
删除(S)
删除(S)
删除的
后活动阶段
终止(S)
终止的
状态
动词
操作
流
条件
信息
P
公钥
S
私钥

图 1　私钥生命周期

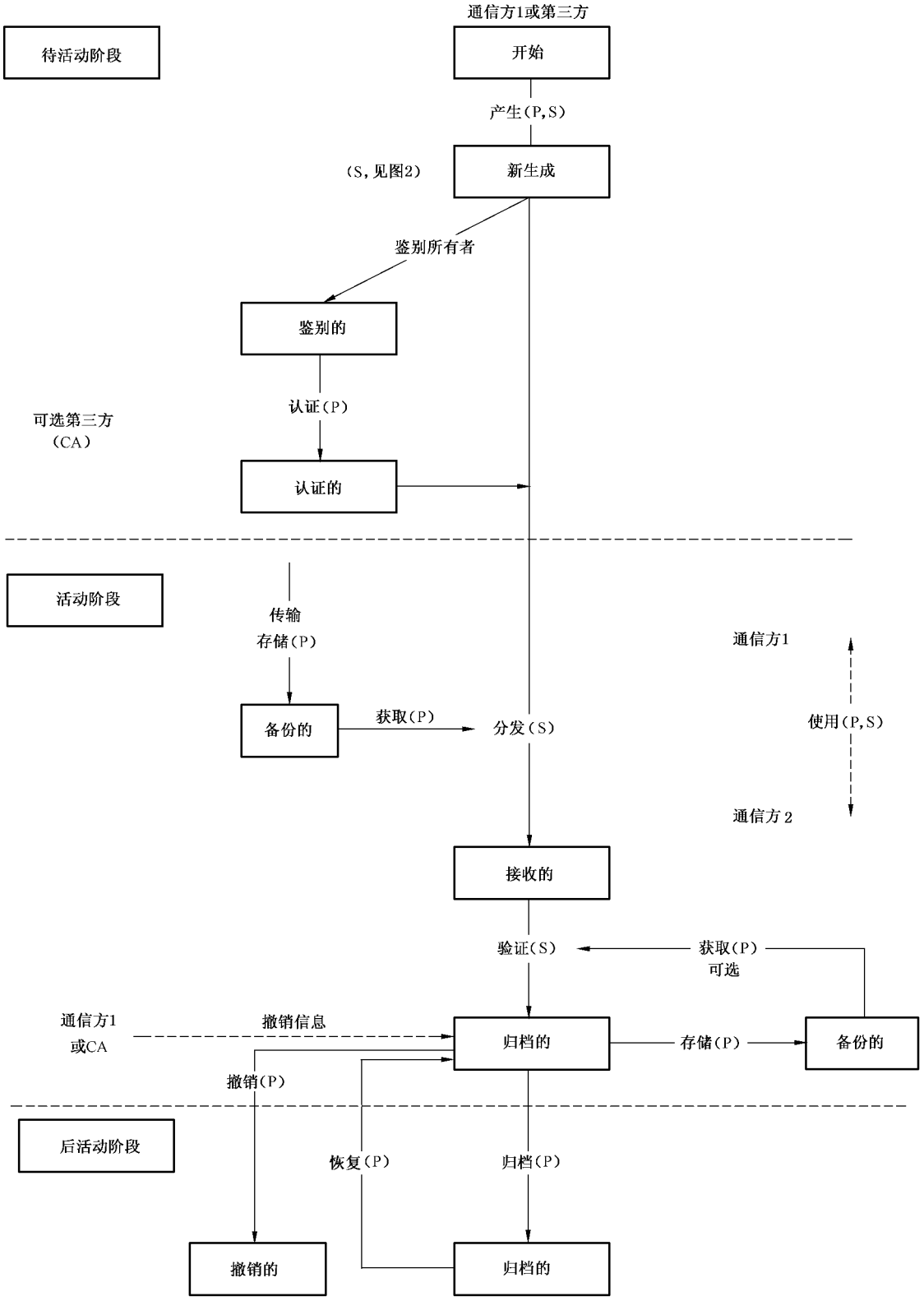
通信方1或第三方
待活动阶段
开始
产生(P,S)
(S,见图2)
新生成
鉴别所有者
鉴别的
认证(P)
可选第三方
(CA)
认证的
活动阶段
传输
存储(P)
通信方1
备份的
获取(P)
分发(S)
使用(P,S)
通信方2
接收的
验证(S)
获取(P)
可选
通信方1
或CA
撤销信息
归档的
存储(P)
备份的
撤销(P)
后活动阶段
恢复(P)
归档(P)
撤销的
归档的

图 2　公钥生命周期

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)。