ICS 35.240.40
A 11

0800235

中华人民共和国国家标准

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

Banking—Key management(retail)—
Part 4:Key management techniques using public key cryptography

(ISO 11568-4:1998,MOD)

华南理工大学 图书馆藏书

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

数码防伪

中 华 人 民 共 和 国
国 家 标 准
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
GB/T 21082.4—2007
*
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 1.5 字数 32 千字
2007年12月第一版 2007年12月第一次印刷
*
书号:155066·1-30268 定价 20.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533

GB/T 21082.4-2007

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4部分。

本部分修改采用国际标准ISO 11568-4:1994《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》(英文版)。

考虑到我国国情,在采用ISO 11568-4时做了以下修改：

删除了“ISO 11568-4附录A核准的算法和算法审核程序”,在第1章中说明应遵循我国密码管理部门的有关规定。

为便于使用,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。

本部分的附录A为规范性附录,附录B、附录C为资料性附录。

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是描述在零售银行业务环境下密钥安全管理过程的一系列标准，这些密钥用于保护诸如收单行和受卡方之间，或收单行和发卡行之间的报文。用于集成电路卡的密钥管理不包括在GB/T 21082标准中。

鉴于批发银行环境中的密钥管理是以在安全系数相对高的安全环境中的密钥交换为特征的，本标准描述了在零售银行服务涉及的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)借记支付，信用卡凭证支付和自动柜员机(ATM)交易。

GB/T 21082的本部分主要描述适用于公开密钥密码系统的密钥管理技术。在组合使用时，这些技术将提供ISO 11568-1中描述的密钥管理服务。这些服务是：

——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；

——密钥泄露检测。

STANDARDS PRESS OF CHINA

目　次

此为试读，需要完整PDF请访问：www.ertongbook.com

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

1　范围

GB/T 21082的本部分详细描述了在零售银行业务环境下对公开密钥密码系统密钥的使用和保护技术。

它适用于任何在密钥生命周期内负责执行密钥保护程序的组织。GB/T 21082的本部分描述的技术符合ISO 11568-1描述的原则。

注:在密钥生命周期每一阶段所要求的保护公开密钥密码系统的保护细节在ISO 11568-1中有详细描述。

公开密钥密码系统包括非对称密码、数字签名系统和公开密钥分发系统。虽然本部分主要描述在密钥管理中应用这些系统的技术,但其中一些技术也同样适用于数据的安全管理。

本部分描述的技术主要针对一般的公开密钥密码系统。针对某个特定系统的具体标准见附录。

批准与本部分中描述的技术一起使用的算法和算法的审批程序应遵从国家密码管理相关机构的规定。

附录A概述了公钥证书管理的标准化。

附录B描述了属性证书,这项技术能加强公钥证书的功能。

附录C介绍了上面提到的三种公开密钥密码系统。

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部分的条款。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 15843.3—1998　信息技术　安全技术　实体鉴别　第3部分:用非对称签名技术的机制(idt ISO/IEC 9798-3:1993)

GB/T 17964—2000　信息技术　安全技术 n位块密码算法的操作方式(idt ISO/IEC 10116:1997)

ISO/IEC 8824:1990　信息技术　开放系统互连　抽象语法记数法一(ASN.1)规范

ISO/IEC 8825:1990　信息技术　开放系统互连　抽象语法记数法一(ASN.1)基本编码规则规范

ISO 8908:1993　银行业务及相关金融服务　词汇和数据元

ISO/IEC 9594-8:1990　信息技术　开放系统互连　目录　第8部分:鉴别框架

ISO 9807:1991　银行业务和相关金融服务　报文鉴别要求(零售)

ISO 11166(所有部分)　银行业务　采用非对称算法的密钥管理

ISO 11568-1　银行业务　密钥管理(零售)　第1部分:密钥管理介绍

ISO 11568-2　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/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 13491-1:1999　银行业务　安全密码设备(零售)　第1部分:概念、要求和评估方法

3　术语和定义

ISO 8908:1993中给出的以及下列术语和定义适用于本部分。

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

非对称密钥对　asymmetric key pair

在一个公开密钥密码系统下创建和使用的公钥及其相关私钥。

3.3

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。

3.4

证书授权机构　certification authority；CA

授权创建和颁发证书的可信中心。

注：可选地，证书授权机构也可以选择创建和分发密钥给实体。

3.5

计算上不可行　computationally infeasible

计算在理论上可以实现，但在当前或可预测的计算机能力下，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。

3.6

凭证　credentials

实体的密钥认证数据，至少包括这个实体的唯一识别名和公钥。

注：也可以包括其它数据。

3.7

数字签名　digital signature

对一个数据单元进行密码变换，使数据单元的接收者能证明它的来源和完整性，防止发送者的数据单元遭到第三方或接收者的伪造。

3.8

数字签名系统　digital signature system

创建和验证数字签名的公开密钥密码系统。

3.9

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

3.10

密钥约定　key agreement

建立一个公共密钥无需参照另一个公共密钥。

3.11

密钥对的所有者　key pair owner

拥有密钥对的一方。

3.12

来源的不可否认性　non-repudiation of origin。

报文和相关密码校验值(数字签名)的源发者，在可接受的可信度上，随后不能否认自己曾发出该报文的这种特性。

3.13

公开密钥密码系统　public key cryptosystem

由两个互补操作组成的密码系统，每个操作使用两个截然不同但互相联系的密钥（公钥和私钥）中的一个，它们具有在计算上不可能由公钥来确定私钥的特性。

3.14

公开密钥分发系统　public key distribution system

允许两个通信实体共同创建一个密钥的公开密钥密码系统。

3.15

公钥用户　public key user

将另一方的公钥用于密码系统服务的一方。

注：证书授权机构并不是公钥用户。

4　零售银行系统中公开密钥密码系统的使用

零售银行业务系统中，公开密钥密码系统主要用于密钥管理：首先用于对称密码系统的密钥管理，其次用于公开密钥密码系统本身的密钥管理。本章描述了公开密钥密码系统的这些应用，支持这些应用所采用的技术在第5章中进行描述。

4.1　对称密钥的分发

一个或多个对称密码密钥的分发可以通过密钥传输或通过密钥约定。

注：对称密钥的分发机制在ISO/IEC 11770-3:1999中描述，在该标准中，密钥分发被称为密钥建立。

4.1.1　密钥传输

当使用密钥传输时，对称密钥应使用非对称密码进行加密，所产生的加密的密钥块被传输给预定的接收方。密钥加密确保了对称密钥在分发过程中的机密性；密钥块或完整的传输报文的真实性、完整性可以通过数字签名系统对该密钥块或报文进行签名来保证。

密钥加密在第5章中进行描述。

注：ISO 11166-1描述了对称密钥传输的协议。该协议同时使用了密钥加密和数字签名。

4.1.2　密钥约定

当使用密钥约定时，对称密码系统的密钥应使用公开密钥分发系统（参见附录C）建立。所使用的机制应确保通信实体的真实性。

4.2　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，或者在密钥约定机制中使用。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维护密钥的真实性和完整性。

注：某些应用的设计中，所需的安全性依赖于公钥的不被泄露。

以下方法之一都可以用于确保公钥在存储或分发过程中的真实性和完整性：

a）　使用数字签名系统对公钥和相关数据签名，从而创建了公钥证书，公钥证书及用于创建和验证证书的密钥管理在5.3和第6章中描述；

b）　使用ISO 9807:1991中定义的算法以及仅用于此目的的密钥，为公钥和相关数据产生MAC；

c）　使用对称或非对称密码加密公钥和相关数据。

密钥加密在5.2中描述。

以下附加方法可以用于只在分发过程中确保公钥的真实性和完整性：

通过无保护的信道分发公钥，通过带双重控制的被鉴别信道分发公钥的密钥验证值和相关数据。密钥验证在5.5中描述。

4.3　非对称私钥的存储和传输

因为非对称密钥对的私钥不需要提供给用户以外的其他地点，所以某些情况下它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),则应至少使用以下三种技术中的一种来防止它被泄露:

a) 用另一个密钥加密(见 5.2);

b) 分割为两个或多个组件,这样受保护密钥中的每一位都依赖于所有组件;

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

5 提供密钥管理服务的技术

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 ISO 11568-1 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。

由于常常需要(或希望)将公钥对用于多种目的,例如数字签名和加密,所以在这些情况下,应使用密钥分散技术,它通过使用密钥对的变换来避免系统受到攻击。

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以达到该技术的目的。

安全密码设备的特征和管理要求在 ISO 13491-1:1999 中定义。

5.1 非对称密钥对的产生

正如特定公开密钥密码系统的设计所定义的那样,一个非对称密钥对的两个密钥在数学上是相关的。由公钥推导私钥在计算上是不可行的。

大部分公开密钥密码系统都基于模运算。模的大小不仅决定了数据和密钥块的大小,而且也决定了攻破该系统的难度。因为系统的强度直接和模的大小相关,因此应选择足够大的模数以使攻击在计算上是不可行的。

在确保两个密钥之间的关系的同时,密钥生成应采用随机或伪随机过程,这样,就不可能预测任何密钥,或者不可能在密钥空间内确定哪些密钥比其他密钥具有更大的可能性。

注:在某些密码系统内,可能使用某个已知的常数值作为公钥的一部分。这与上面的要求并不冲突。

5.2 密钥加密

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被安全地管理(确保密钥的机密性和/或真实性)。用来实现这种加密技术的密钥被称为密钥加密密钥(KEK)。

这里描述了包括非对称密钥和密码的三种不同的密钥加密情况,它们分别是:

a) 用非对称密码给对称密钥加密;

b) 用非对称密码给非对称密钥加密;

c) 用对称密码给非对称密钥加密。

注:ISO 11568-2 描述了用对称密码给对称密钥加密的密钥加密技术。

虽然密钥加密技术能保证密钥的机密性,但在密钥加密过程中,为了确保密钥充分分散,还需要使用其他技术,如密钥标记(见 5.4)等。

5.2.1 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。加密了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)。这样就可以建立对称和非对称密码密钥相结合的混合密钥分级结构。

注:密钥分级结构在 ISO 11568-2 中有详细描述。

对称密钥必须格式化为适合于加密操作的数据块。由于非对称密码的数据块大小一般比对称密码密钥的大小更大,因此在加密时,在一个数据块中通常可以包括一个以上的密钥。此外,数据块中还可能包括格式化信息、随机填充字符和冗余字符。

5.2.2 用非对称密码给非对称密钥加密

非对称密码的公钥或私钥都可以用非对称密码进行加密。

5.2.3 用对称密码给非对称密钥加密

可以要求用对称密码给非对称密码的公钥或私钥进行加密。

由于非对称密码的密钥一般比对称密码的数据块更大，非对称密钥必须格式化成多个数据块才能进行加密，因此必须将密码块链操作模式用于加密操作。

注 1：GB/T 17964—2000 规定了 n 位分组密码算法的操作模式。

在非对称钥的加密过程中应该使用双长度密钥。

注 2：用双长度密钥加密在 ISO 11568-2 中有详细论述。

5.3 密钥认证

在向被授权的接收者分发密钥，或在密钥数据库中存储密钥时，必须保证用户公钥的真实性。

密钥认证是一种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真实性的技术。在使用公钥前，接收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识别数据，以及密钥有效性数据(例如，密钥有效期)。公钥证书由被称为“证书授权机构”的第三方发布。公钥证书通过用证书授权机构所拥有的私钥签署用户凭证来创建，并且只能用于上述目的。

附录 A 详细描述了对公钥证书的管理。

5.4 密钥分散技术

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。将密钥值和它的属性和权限采用某种方式捆绑在一起，以防止两者中的任何一个遭到无法检测的修改。

5.4.1 显式密钥标记

显式密钥标记使用一个字段，它包含定义相关密钥的属性、权限限制和密钥类型的信息。将这一字段与密钥值采用某种方式捆绑在一起，以防止两者中的任何一个遭到无法检测的修改。

5.4.2 隐式密钥标记

隐式密钥标记并不依赖于使用包含定义相关密钥属性、权限限制和密钥类型信息的显式字段，而是依靠系统的其他特征，如密钥值在记录中的位置或相关功能，来决定和限制该密钥的权利和属性和权限。

5.5 密钥验证

密钥验证是一种在不泄露密钥值的情况下检查和验证密钥值的技术。这项技术使用密钥验证码(KVC)，该密钥验证码通过抗冲突的单向函数与此密钥是密码相关的。

在首次产生 KVC 后的任何时候，该密钥可以再次输入单向函数。如果后来产生的 KVC 与最初产生的 KVC 完全相同，就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) 通过通信信道已正确收到密钥；

c) 密钥未改变。

对私钥来说，密钥验证可以用来保证加密的密钥在传输或变换过程中没有遭到破坏，或在存储过程中没有被破坏或改写。

对公钥来说，密钥验证还能为密钥完整性检查提供方便。只要 KVC 通过保证完整性的信道分配，公钥就可以通过不安全的信道来分发。

6 公钥证书管理

为了一个实体以可接受的可信度使用另一个实体的公钥，可以使用公钥证书。公钥证书为公钥的完整性和真实性提供保障级别。公钥证书由证书授权机构(CA)颁发。公钥所有者向 CA 注册，确定个人身份和相应的公钥。CA 把上述实体的身份与它的公钥联结起来。用户可以直接从 CA 或公钥所有者那里获得公钥证书。要获得更多信息，见附录 A。

附 录 A
（规范性附录）
公钥证书的管理

A.1 引言

为了在密钥对的所有者和公钥之间建立和维持联系，应该使用公钥证书管理。公钥证书为公钥的完整性、真实性和所有权提供较高程度的保障。

该规范性附录提供以下信息，分列为三项条款：

A.2 描述这些实体是谁，列举相关文件，并解释证书管理中的这些关系。

A.3 描述这些过程是什么，对证书管理过程中每个实体的责任进行定义。

A.4 定义公钥证书内部包含的强制性、推荐性和选择性数据元。

有关证书管理和证书数据元的额外信息可以在详细说明公钥证书的 ANSI X9.57 中找到。两种标准均使用 ISO/IEC 8824:1990，ISO/IEC 8825:1990 和 ISO/IEC 9594-8:1990 中描述的抽象语法记数法(ASN.1)。

A.2 实体和文件

A.2.1 身份文件

身份文件是递交给证书授权机构，建立密钥对的所有者身份的物理或电子文件。

A.2.2 凭证

凭证是递交给证书授权机构，建立公钥身份的物理或电子文件。见 A.4.2。

A.2.3 公钥证书

公钥证书是通过数字签名，确保密钥对所有者和相应公钥之间关系的物理或电子文件，其中数字签名由证书授权机构和它自身的私钥产生。见 A.4.1。

A.2.4 证书授权机构(CA)

证书授权机构(CA)是经授权提供下列服务的机构：

a) 确认密钥对所有者的身份；

b) 检验公钥的正确性[1)]；

c) 创建公钥证书；

d) 为密钥对所有者签发公钥证书(相应的，密钥对所有者可能向公钥用户分发公钥证书)；

e) 有可能向公钥用户分发公钥证书或使这些用户可以获得公钥证书。

A.2.5 密钥对所有者(KPO)

密钥对所有者是私钥和公钥对的所有者，同时还是私钥的使用者。他或者产生非对称密钥，或者从可信第三方安全地获得非对称密钥。

A.2.6 公钥用户(PKU)

公钥用户是公钥的使用者，这里所指的公钥来自证书授权机构最初发布的公钥证书。公钥用户通过用 CA 的公钥来检验它的签名，鉴别公钥证书的真实性。公钥证书意味着密钥对所有者的身份得到确认，从而提供了所有者身份和他的公钥的完整性。

---

1) 例如，密钥对所有者可以用私钥创建数字签名，CA 可以用公钥检验数字签名。另一个例子是：CA 可以用公钥对信息进行加密，与此同时，密钥对所有者可以用私钥对信息解密。在上述两个例子中，CA 假设密钥对所有者持有相应的私钥。

此为试读，需要完整PDF请访问：www.ertongbook.com

公钥用户在最初获得 CA 的公钥时应该确保公钥的真实性和完整性已经建立。这可以通过使用另一个已经建立公钥的 CA 发布的公钥证书，或人工交换 CA 的公钥（因为数据不具有保密性），或其他密码技术（包括对称和非对称密钥管理方案）来完成。

A.2.7 实体和文件的关系

图 A.1 形象描述了上面讨论的实体和文件之间的关系。

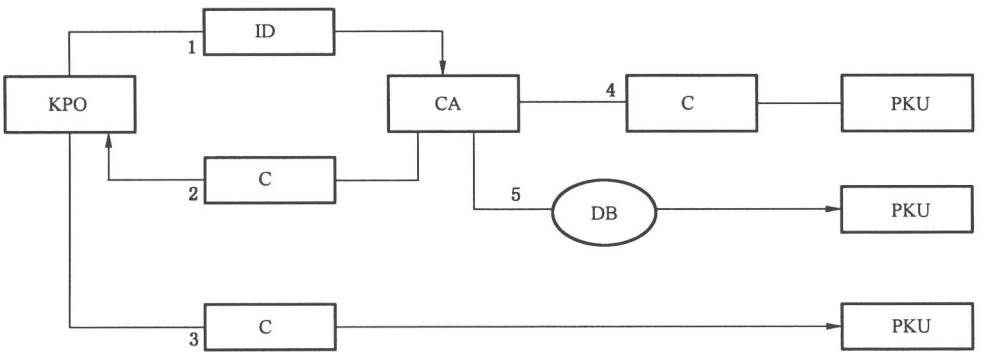

图 A.1

a) 密钥对所有者（KPO）向证书授权机构（CA）注册正确的身份文件（ID）和凭证[2)]；

b) CA 产生公钥证书（C）并传送证书的副本给所有者（KPO）；

c) 所有者可以向一个或多个公钥用户（PKU）分发证书（C）的副本；

d) CA 也可以向一个或多个用户（PKU）分发证书的副本；

e) 作为选择，CA 可以将证书放置到数据库（DB）或公共目录中，向用户公开。

A.3 过程和责任

这一节描述了每一实体在以下证书管理过程中的责任：

a) 密钥对所有者的注册；

b) 证书的产生和传输；

c) 证书的分发；

d) 证书的撤销；

e) 公钥用户对证书的使用。

注：证书授权机构的所有活动都应记录在审计日志中并周期性审查。

A.3.1 密钥对所有者的注册

注册是通过验证所有者的凭证和身份文件而建立公钥身份和所有者身份的过程。

恰当的身份文件和凭证应该直接提交给 CA 或者提交给 CA 认定的本地注册授权机构（LRA），由它对身份文件进行验证。LRA 的功能由 CA 或者第三方组织行使。

LRA 应验证身份文件并为密钥对所有者创建或核实唯一名称。如果 LRA 不属于 CA，则应采取安全措施保证在由 LRA 向 CA 传输期间所有者身份和凭证的真实性、完整性。

应采用独立的通告来证实所提交的身份文件及凭证是正确并被认可的。这需要从其他渠道获得的书面或口头的确认，这一渠道要不同于最初取得文件的渠道。

CA 颁发的每一个公钥证书都要采取这一注册过程。

A.3.2 证书的产生和传输

证书产生是由 CA 创建公钥证书的过程。

在成功完成注册过程后，CA 签署适当的信息创建证书，如 A.4 的定义，并且将数字签名合并到被签名的数据之后。证书的发布保证了所有者身份和公钥的可信性，数字签名提供了对该信息完整性的保护。

2) 注意：如果由 CA 生成 KPO 的非对称密钥对，因为凭证不包含公钥，所以 KPO 不需要向 CA 注册他的凭证。

传输是公钥证书返回到密钥对所有者手中的过程。

CA 可以在证书产生时或稍后通过分发机制颁发公钥证书给密钥对所有者。

另外，CA 可以向密钥对所有者发送独立的通告，通知证书已经颁发。

A.3.3 证书的分发

分发是指公钥用户获得公钥证书的过程。证书可以包含有效期，指明证书使用的终止日期。

证书可以从密钥对所有者或者从 CA 取得。实际的分发方式可以多种多样，包括邮寄文件，电子媒介和在线数据库。不论何种情况，公钥用户必须知晓 CA 的公钥，来对证书进行验证。

A.3.4 证书的撤销

撤销是在证书过期前终止证书使用的过程。证书可能因为某些安全原因而被撤销，如实体的私钥或者 CA 的私钥可能泄露或被怀疑泄露，也可能是其他商业原因。证书撤销列表(CRL)应由 CA 维护。不论因何种原因而被终止使用，撤销的证书都要被加入到该列表之中。

CRL 应对所有的公钥用户都可用。例如，CA 可以将撤销通知直接发给公钥用户，或者维护一个 CRL 的在线数据库。

CA 应维护 CRL 的完整性，确保每个条目的真实性。CRL 的完整性和真实性应该通过对整个 CRL 进行签名，或者采用 ISO 9807:1991 中定义的报文鉴别来维护，以保证它的完整性并提供独立的验证。如果撤销信息被单个地分发，它们也应该由 CA 进行签名。

另外，CA 应向密钥对所有者发送独立签名的撤销通知，说明某个证书已经被撤销。

A.3.5 公钥用户对证书的使用

证书使用是指公钥用户采用公钥证书的过程。在公钥用户可以使用证书之前，应对证书进行验证。这是通过以下方式来完成的：

a) 确保选择了正确的公钥证书；

b) 检查证书没有出现在 CRL 当中，确保证书没有被撤销；

c) 如果证书当中包含有起始日期和终止日期，则确保该证书有效；

d) 确保证书信息的完整性(即，用 CA 的公钥验证数字签名)。

A.4 证书的数据元

本节定义了证书内的数据元。数据元的选项有如下定义：

M：应有的强制性数据元

R：应有的推荐性数据元

O：可以出现的可选数据元

如 A.4.1 所述，以一些分层次的表来显示信息，高级代表公钥证书本身。更详细的信息见 A.4.2 和 A.4.3。

A.4.1 公钥证书数据元

表 A.1 公钥证书数据元

选项	数据元
M	1. 密钥对所有者资格凭证[3)]
O	2. 证书序列号
O	3. 证书起始日期
R	4. 证书终止日期
R	5. 证书授权机构信息[3)]
O	6. 属性证书指示项
M	7. 数字签名

3) 这些数据元素的定义分别在 A.4.2 和 A.4.3 中进一步阐述。

A.4.1 中出现的数据元按推荐的顺序排列。下面是对每个数据元的描述：

A.4.1.1 密钥对所有者资格凭证

见 A.4.2 的描述。

A.4.1.2 证书序列号

这是 CA 分配的号码，以唯一地识别由 CA 发布的每个证书，号码具有唯一性。证书序列号可以和证书存储或与属性证书结合使用。

A.4.1.3 证书起始日期

这是公钥证书开始生效的日期，一般情况下是 CA 发布公钥证书的日期。参考 A.3.2。

A.4.1.4 证书终止日期

这是公钥证书失效的日期，由 CA 指定。见 A.3.4。

A.4.1.5 CA 信息

见 A.4.3 的描述。

A.4.1.6 属性证书指示项

该值表明存在着一个或多个相应的属性证书，它们对 KPO 的非对称密钥对的使用做出进一步规定。

A.4.1.7 数字签名

这是从公开密钥密码算法生成的值。一般情况下，首先对数据采用散列函数缩短数字签名的长度。但在某些情况下，不用散列函数也能得出数字签名。

A.4.2 密钥对所有者凭证

表 A.2 密钥对所有者凭证

选项	数据元
M	1. 相对识别名
M	2. 公钥值
R	3. 公钥长度
R	4. 公钥名称
R	5. 公钥参数：模数
R	6. 公钥参数：算法标识符
R	7. 公钥参数：散列函数标识符
O	8. 提交时间和日期

注：A.4.2 中出现的数据元是以可选的次序排列的。以下是对每个数据元的描述。

A.4.2.1 相对识别名

这是密钥对所有者的名字，相对于在同一个证书授权机构注册的所有密钥对所有者是唯一的。

A.4.2.2 公钥值

这是密钥对所有者的公钥值，一般用二进制或十六进制数字表示。

A.4.2.3 公钥长度

这是公钥的长度，一般用二进制位数表示。

A.4.2.4 公钥名称

这是公钥的名字，相对于每个密钥对所有者的所有公钥是唯一的。

下列数据元是与特定的公开密钥算法相对应的推荐参数。额外的参数对于完整定义该算法可能是必需的。

A.4.2.5 公钥参数：模数

这是公开密钥算法中使用的模数值，一般属于非密数据。

A.4.2.6 公钥参数:算法标识符

这是识别与所有者的公钥一起使用的特定公开密钥算法的值。

A.4.2.7 公钥参数:散列函数标识符

这是识别与密钥对所有者的公钥一起使用的进行数字签名的特定散列函数的值。

A.4.2.8 提交时间和日期

这是密钥对所有者在 LRA 或 CA 注册的时间和日期,它不一定和证书起始日期一致。

A.4.3 CA 信息

表 A.3 CA 信息

选项	数据元
R	1. CA 的唯一识别名
O	2. CA 的公钥参数:模数
O	3. CA 的公钥参数:算法标识符
O	4. CA 的公钥参数:散列函数标识符

注:A.4.3 中出现的数据元是以可选次序排列的。下面是对每个数据元的描述。

A.4.3.1 CA 的唯一识别名

这是 CA 的名称,与其他所有证书授权机构相比,相对唯一。

A.4.3.2 CA 的公钥参数:模数

这是 CA 的公开密钥算法所使用的模数值。

A.4.3.3 CA 的公钥参数:算法标识符

这是识别 CA 的公钥所使用的公开密钥算法的值。

A.4.3.4 CA 的公钥参数:散列函数标识符

这是标识在签署证书时与 CA 的公钥一起使用的具体散列函数的值。

附 录 B
（资料性附录）
属 性 证 书

B.1 属性证书

属性证书是一种加强公钥证书的功能，同时维持与现有证书，如国际电信联盟（ITU）标准 X.509 中定义的那些证书互操作的技术。

公钥证书中的属性证书指示项表示公钥证书中存在着一个或多个属性证书。相反，每个属性证书都包含公钥证书中的证书序列号。

公钥证书的作用是为公钥用户提供有效的公钥，该公钥用来加密信息或者用来验证信息上的签名；属性证书中规定了上述信息使用的目的。

B.2 属性证书实例

例如，一个公钥证书允许某个商户或收单机构检验小额交易的签名，验证密钥对所有者的真实性。但公钥证书本身可能无法授权密钥对所有者进行这样的交易。

在这个例子中，另一个被称为“属性授权机构”的实体可以向密钥对所有者颁发一个或多个属性证书。注意：属性授权机构（AA）和证书授权机构（CA）不一定是同一个实体。

AA 可能发布一个包含公钥证书序列号的属性证书，授权从事小额交易的密钥对所有者购买不超过一定金额的货物。这样，商户或公钥证书持有者在验证签名和审查属性证书后可以批准这项零售交易。

此外，同一个属性证书可以包含对于不同类型零售交易的多个金额限制，像现金预付、旅馆、饭店等等。

同一个 AA 可能会针对不同国家，发布含有类似金额信息的另一个属性证书。

不同的 AA 可能会针对不同的金融机构发布含有类似金额信息的另一个属性证书。

B.3 角色和职责

属性证书的角色和职责类似于公钥证书的角色和职责。

B.3.1 证书授权机构

证书授权机构（CA）的职责与公钥证书管理中描述的相同（见 A.2.4）。

B.3.2 密钥对所有者

密钥对所有者的职责是保证 AA 拥有他所需要的公钥证书和其他适当的信息。

B.3.3 属性授权机构

AA 的职责如下：

a） 采用密钥初始化过程或证书获得 CA 的公钥；

b） 从密钥对所有者或从初始的 CA 获得公钥证书；

c） 验证密钥对所有者的公钥证书上的 CA 签名；

d） 向密钥对所有者详述颁发证书所必需的适当信息；

e） 从密钥对所有者获得适当的信息，最好是由密钥对所有者签名的；

f） 若信息进行了签名，则验证密钥对所有者的签名；

g） 如 B.4 所述，产生并颁发属性证书。

B.4 描述了格式和数据内容。

B.3.4 公钥用户

公钥用户的职责如下：

a) 通过密钥初始化过程或证书获得 CA 和 AA 的公钥；

b) 从密钥对所有者或者分别从 CA 和 AA 获得公钥证书和属性证书；

c) 验证 CA 在密钥对所有者的公钥证书上的签名；

d) 验证 AA 在密钥对所有者的属性证书上的签名；

e) 验证密钥对所有者对交易的签名；

f) 如果适当，就批准交易或执行所要求的功能。

B.4 属性证书数据元

表 B.1 属性证书数据元

选项	数据元
O	1. 密钥对所有者凭证[4)]
R	2. 证书序列号[4)]
O	3. 证书起始日期
R	4. 证书终止日期
R	5. 属性授权机构信息
M	6. 属性信息
M	7. 数字签名

B.4.1 密钥对所有者凭证

与附录 A 中讨论的信息相同。如果原始的公钥证书不包含证书序列号，那么应存在这些数据元，以确保其唯一性。

B.4.2 证书序列号

与附录 A 中讨论的信息相同，推荐它作为指针指回原公钥证书。

B.4.3 证书起始日期

除非由属性授权机构规定这一数据，这部分信息与附录 A 中讨论的相同。

B.4.4 证书终止日期

除非由属性授权机构规定这一数据，这部分信息与附录 A 中讨论的相同。

B.4.5 属性授权机构信息

这部分与附录 A 中对证书授权机构讨论的信息类似。

B.4.6 属性信息

这是规定密钥对所有者的私钥实际用途的信息。

B.4.7 数字签名

除非 AA 用它的私钥产生数字签名，这部分内容与附录 A 中讨论的信息相同。

4) 注意必须存在这些数据元中的一个，以便和相应的公钥证书相关联。

此为试读，需要完整PDF请访问：www.ertongbook.com