GB

国家标准汇编

2005年制定

中 国 国 家 标 准 汇 编

316

GB 19714～19753

(2005 年制定)

中 国 标 准 出 版 社

2006

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。本《汇编》在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2. 本《汇编》收入我国正式发布的全部国家标准。各分册中如有顺序号缺号的，除特殊情况注明外，均为作废标准号或空号。

3. 由于本《汇编》的出版时间与新国家标准的发布时间已达到基本同步，我社将在每年出版前一年发布的新制定的国家标准，便于读者及时使用。出版的形式不变，分册号继续顺延。

4. 由于标准不断修订，修订信息不能在本《汇编》中得到充分和及时的反应，根据多年来读者的要求，自1995年起，在本《汇编》汇集出版前一年发布的新制定的国家标准的同时，新增出版前一年发布的被修订的标准的汇编版本，视篇幅分设若干分册。这些修订标准汇编的正书名、版本形式与《中国国家标准汇编》相同，但不占总的分册号，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样，作为本《汇编》的补充。读者配套购买则可收齐前一年制定和修订的全部国家标准。

5. 由于读者需求的变化，自第201分册起，仅出版精装本。

本分册为第316分册，收入国家标准GB 19714～19753的最新版本。

中国标准出版社

2006年3月

目　　录

ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 19714—2005

信息技术 安全技术 公钥基础设施 证书管理协议

Information technology—Security technology—Internet public key infrastructure—Certificate management protocol

2005-04-19 发布　　2005-10-01 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

前　言

本标准是依据 IETF RFC 2510 制定的。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准中引用的 RSA、SHA1、DH 密码算法均为举例性说明，具体使用时均须采用国家商用密码管理委员会批准的相应算法。

本标准的附录 B、附录 C、附录 F 为规范性附录，附录 A、附录 D、附录 E、附录 G 为资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会(TC260)归口。

本标准主要起草单位：北京创原天地科技有限公司、中国电子技术标准化研究所。

本标准主要起草人：林雪焰、吴志刚、王炳艳、陈震琦、张科研、李 丹、罗锋盈、陈 星。

引　言

本标准描述了公钥基础设施(PKI)证书管理协议，定义了与证书产生和管理相关的各方面所需要的协议消息，主要包括：申请证书、撤销证书、密钥更新、密钥恢复、交叉认证等等。

公钥基础设施中总共有四类实体：CA、RA、终端实体、证书/CRL 库，如何保证四实体之间的通信安全、在证书业务中如何对四类实体进行管理，这些问题是本标准解决的主要问题。

信息技术　安全技术　公钥基础设施　证书管理协议

1　范围

本标准描述了公钥基础设施(PKI)中的证书管理协议，定义了与证书产生和管理相关的各方面所需要的协议消息，这些消息主要包括申请证书、撤销证书、密钥更新、密钥恢复、交叉认证等。

本标准主要适用于在安全或不安全环境中实施 PKI 组件并实施管理，可作为 PKI 运营机构、PKI 组件开发者的参考指南。

2　规范性引用文件

下列文件中的条款通过本标准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标准，然而，鼓励根据本标准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标准。

GB/T 16264.8—2005　信息技术　开放系统互连　目录　第 8 部分：公钥和属性证书框架(ISO/IEC 9594-8:2001，IDT)

RFC2511 因特网 X.509 公开密钥基础设施证书消息格式

3　术语和定义

下列术语和定义适用于本标准。

3.1

抽象语法记法一(ASN.1)　Abstract Syntax Notation 1(ASN.1)

用来组织复杂数据对象的表示法。

3.2

公钥证书　public key certificate

用户的公钥连同其他信息，并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

3.3

证书持有者　certificate holder

有效证书的主体对应的实体。

3.4

证书用户　certificate user

需要确切地知道另一实体的公开密钥的某一实体。

3.5

证书认证机构(CA)　Certificate Authority(CA)

负责创建和分配证书，受用户信任的权威机构。用户可以选择该机构为其创建密钥。

3.6

证书认证路径　certification path

一个 DIT 中对象证书的有序序列，通过处理该有序序列及其起始对象的公钥可以获得该路径的末端对象的公钥。

3.7

认证业务说明(CPS)　Certification Practice Statement(CPS)

证书认证机构发放证书时遵循的业务说明。

3.8

交叉证书　cross-certificate

两个 CA 间为交叉认证所互相签发的数字证书。

3.9

CRL 分布点　CRL distribution point

一个 CRL 目录项或其他 CRL 分发源;由 CRL 分布点分发的 CRL 可以包括仅对某 CA 所发证书全集某个子集的撤销条目,或者可以包括有多个 CA 的撤销条目。

3.10

证书撤销列表(CRL)　Certificate Revocation List(CRL)

一个已标识的列表,它指定了一套证书发布者认为无效的证书。除了普通 CRL 外,还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

3.11

发证　certify

颁发一个证书的行为。

3.12

可辨别编码规则(DER)　Distinguished Encoding Rules(DER)

对 ASN.1 对象进行编码的规则。

注:本标准中使用 DER 对 ASN.1 对象进行编码。

3.13

数字签名　digital signature

允许接收者验证签名人的身份和数据完整性的数据单元。

3.14

目录服务(DS)　Directory Service(DS)

分布在网络中的各种节点或服务器提供的分布式数据库服务。

3.15

终端实体　end entity

不以签署证书为目的而使用其私钥的证书主体或者是依赖(证书)方。

3.16

散列函数　hash function

哈希函数

将值从一个大的(可能很大)定义域映射到一个较小值域的(数学)函数。"好的"散列函数是把该函数应用到大的定义域中的若干值的(大)集合的结果可以均匀地(和随机地)被分布在该范围上。

3.17

散列码　Hash code

散列函数的输出比特串。

3.18

消息认证码(MAC)　Message Authentication Code(MAC)

通过密码技术由消息产生的认证数据。

3.19

消息摘要 message digest

散列一个消息后得到的固定长度数据。

3.20

个人安全环境(PSE) Personal Security Environment (PSE)

证书及私钥的终端实体的安全本地存储。

3.21

拥有证明(POP) Proof of Possession (POP)

终端实体用以证明自己拥有(即能够使用)与为之申请证书的公钥相对应的私钥。

3.22

策略映射 policy mapping

当某个域中的一个 CA 认证另一个域中的一个 CA 时,在第二个域中的特定证书策略可能被第一个域中的证书认证机构认为等价(但不必在各方面均相同)于第一个域中认可的特定证书策略。

3.23

注册机构(RA) Registration Authority(RA)

为用户办理证书申请、身份审核、证书下载、证书更新、证书注销以及密钥恢复等实际业务的办事机构或业务受理点。

3.24

资料库 repository

存储证书和 CRL 等信息,并提供无需验证的信息检索服务的数据库。

3.25

自颁发证书 self-issued certificate

证书的主体和颁发者相同的 CA 证书。

4 缩略语

下列缩略语适用于本标准:

CA 证书认证机构

CRL 证书撤销列表

PKCS 公钥密码系统

PKI 公钥基础设施

POP 拥有证明

PSE 个人安全环境

RA 注册机构

TCP 传输控制协议

5 PKI 管理概述

5.1 PKI 管理模型

在详细阐述特定的消息格式和流程之前,首先要定义一下 PKI 管理中所涉及到的实体以及它们之间的交互行为(根据 PKI 管理所需的功能)。然后再对这些功能进行归类,以包含可以确定的不同类型的终端实体。

5.2 PKI 实体的定义

PKI 管理中所涉及到的实体包括终端实体和证书认证机构。注册机构也可以被包括在内。

5.2.1 主体和终端实体

终端实体是不以签署证书为目的而使用其私钥的证书主体或者是依赖(证书)方。

“主体”在此处是指被授予证书的实体,一般在证书的主体或主体可替换名字段中指定。当要区分主体所使用的工具和/或软件时(例如:一个本地的证书管理模块),使用术语“主体设施”。通常优先使用术语“终端实体”而不是“主体”,以防止与证书字段名中的主体相混淆。

需要着重指出的是:终端实体在此处不仅包括应用软件的使用者,也包括软件本身(例如 IPSec 的情况)。这一因素影响着 PKI 管理操作所使用的协议。例如,与个人用户相比,应用软件更有可能确切知道需要使用证书中的哪个扩展项。PKI 管理实体也被看作为一个终端实体,因为它们有时候也在证书(或交叉证书)的主体或主体可替换名字段中被指定。如无特殊说明,术语“终端实体”将不会被用来指代 PKI 管理实体。

所有的终端实体都需要安全可靠的访问一些本地信息,至少包括:实体自己的名字和私钥,被该实体直接信任的 CA 的名字及其公钥(或公钥指纹,如果可以通过其他的方式得到自签名证书)。软件实现可以使用安全本地存储机制存储上述信息,但不限于上述信息(例如:还可以包括用户自己的证书以及应用软件特有的信息)。存储方式也可以不同,例如普通的文件或抗攻击的密文存储介质。像这样安全的本地存储在这里被称之为终端实体的个人安全环境。

尽管有关 PSE 格式的内容已经超出本标准的范围(与设备及其他信息相关),但这里定义了一种通用的 PSE 数据交换格式 —— 认证响应消息。

5.2.2 证书认证机构(CA)

证书认证机构是负责创建和分配证书,受用户信任的权威机构。用户可以选择该机构为其创建密钥。

从终端实体的角度出发,CA 可以是,也可以不是一个事实上真正的“第三方”。绝大多数情况下,CA 与其所服务的终端实体属于同一个机构。

同样,我们使用术语“CA”指代证书中签发者(issuer)字段所代表的实体。当需要与 CA 所使用的软硬件工具相区分时,我们使用术语“CA 设施”。

CA 设施一般包括离线模块和在线模块,只有 CA 的离线模块可以使用 CA 的私钥。尽管是否这样做与 CA 的策略相关,但这取决于软件实现者。

我们使用术语“根 CA”来指代被终端实体直接信任的 CA;即安全地获取根 CA 的公钥需要一些额外的步骤。这一术语并不意味着根 CA 必须处于 CA 体系层次的顶层,它只是说明该 CA 是被终端实体直接信任的。

“下级 CA”(子 CA)不是终端实体的根 CA。通常,下级 CA 不是任何实体的根 CA,但这并不是强制的。

5.2.3 注册机构(RA)

注册机构是为用户办理证书申请、身份审核、证书下载、证书更新、证书注销以及密钥恢复等实际业务的办事机构业务受理点,亦称证书注册审核中心。

除了终端实体和 CA 之外,很多应用环境要求把注册机构从证书认证机构中独立出来。(RA 存在的原因参见附录 A。)RA 所具有的功能将因情况不同而有所不同,可能包括个人身份鉴别、介质分发、作废报告、名称分配、密钥产生、密钥归档等等。

本标准将 RA 作为可选的组成部分,当 RA 不存在时,假定 CA 可以实现 RA 的功能。从终端实体的观点看,它们都使用相同的 PKI 管理协议。

同样,当需要区分 RA 和 RA 所使用的工具时,使用“RA 设施”这个术语。

应该注意到 RA 本身也是一个终端实体,一个被验证了的终端实体,它有自己的私钥进行数字签名和身份认证。CA 设施如何把某些终端实体认定为 RA 则是一个实现问题(本标准不阐述特定的 RA 认证操作)。并不强制 RA 必须可以被与其正通信的 CA 所认证(所以一个 RA 可以只被认证一次,与多

个 CA 协同工作)。

在某种情况下,即使存在 RA,终端实体可能仍然需要和 CA 直接通信。例如,在 RA 进行登记和接受审核,而直接与 CA 通信来更新证书。

5.3 PKI 管理要求

PKI 管理的要求如下:

a) PKI 管理必须符合 GB/T 16264.8—2005 及相关修订补篇(指证书扩展项);

b) PKI 管理必须符合 PKI 系列草案的其他标准;

c) 必须能够在不影响其他密钥对的前提下定期地更新任意密钥对;

d) 为了使调整简单易行,在 PKI 管理协议中应尽可能少的使用加密;

e) PKI 管理协议必须允许使用不同的工业标准加密算法。这意味着,原则上,任何给定的 CA、RA 或终端实体,可以使用任何适合其所拥有的密钥对的算法;

f) PKI 管理协议一定不能排除密钥对由相关的终端实体或 RA 或 CA 产生。密钥产生也可以在其他地方完成,出于 PKI 管理的目的,我们可以认为密钥生成发生在密钥第一次出现的地方:终端实体、RA 或 CA;

g) PKI 管理协议必须能够支持相关终端实体或 RA、CA 进行证书发布。在不同实现和不同的环境下可以采用上面任何一种方法;

h) PKI 管理协议必须允许通过认证的终端实体请求作废证书,以签发 CRL。这一功能必须能够尽可能防止拒绝服务攻击;

i) PKI 管理协议必须能够使用各种不同的传输机制,特别是邮件传输协议、HTTP、TCP/IP 和 FTP;

j) 签发证书的最终决定权属于 CA。RA 或终端实体都不能假定 CA 签发出来的证书符合它们的全部要求。CA 可以根据其运营策略,改变一个证书字段的值,或者添加、删除、修改证书扩展项。换句话说,所有的 PKI 实体(终端实体、RA、CA)都必须能够处理那些与其请求不一致的证书响应(例如:CA 可能会缩短证书有效期)。CA 策略可能作出规定,在证书请求者检查并接受新签发的证书之前,CA 机构不能发布或分发该证书(通常使用证书确认消息完成这一功能);

k) PKI 管理协议必须能够支持未泄密的 CA 密钥对的更新(即 CA 密钥更新)。如果 CA 发生密钥泄露,那么该 CA 所辖的全部实体都必须重新进行初始化操作。在 CA 密钥更新以后,PSE 中包含 CA 新公钥的终端实体,必须仍然能够验证使用旧的 CA 公钥能够验证的证书。直接信任旧的 CA 密钥对的终端实体,也必须能够验证新的 CA 私钥所签发的证书;

l) 在某些实现或情况下,RA 的功能可能会由 CA 来承担。PKI 管理协议的设计,必须满足下面的条件:终端实体不管与 CA 还是与 RA 通信都应该使用相同的协议;

m) 当终端实体发出的证书请求带有公钥时,必须能够证明拥有相应的私钥。完成此项工作可以用不同方法,究竟采用哪一种取决于认证请求的类型。关于证书管理协议消息中定义的带内方法完成以上工作的详细内容见 6.3。

5.4 PKI 管理操作

图 1 描述了 PKI 管理操作所定义的各个实体间的关系。可以沿着字母标明的线路发送 PKI 消息。

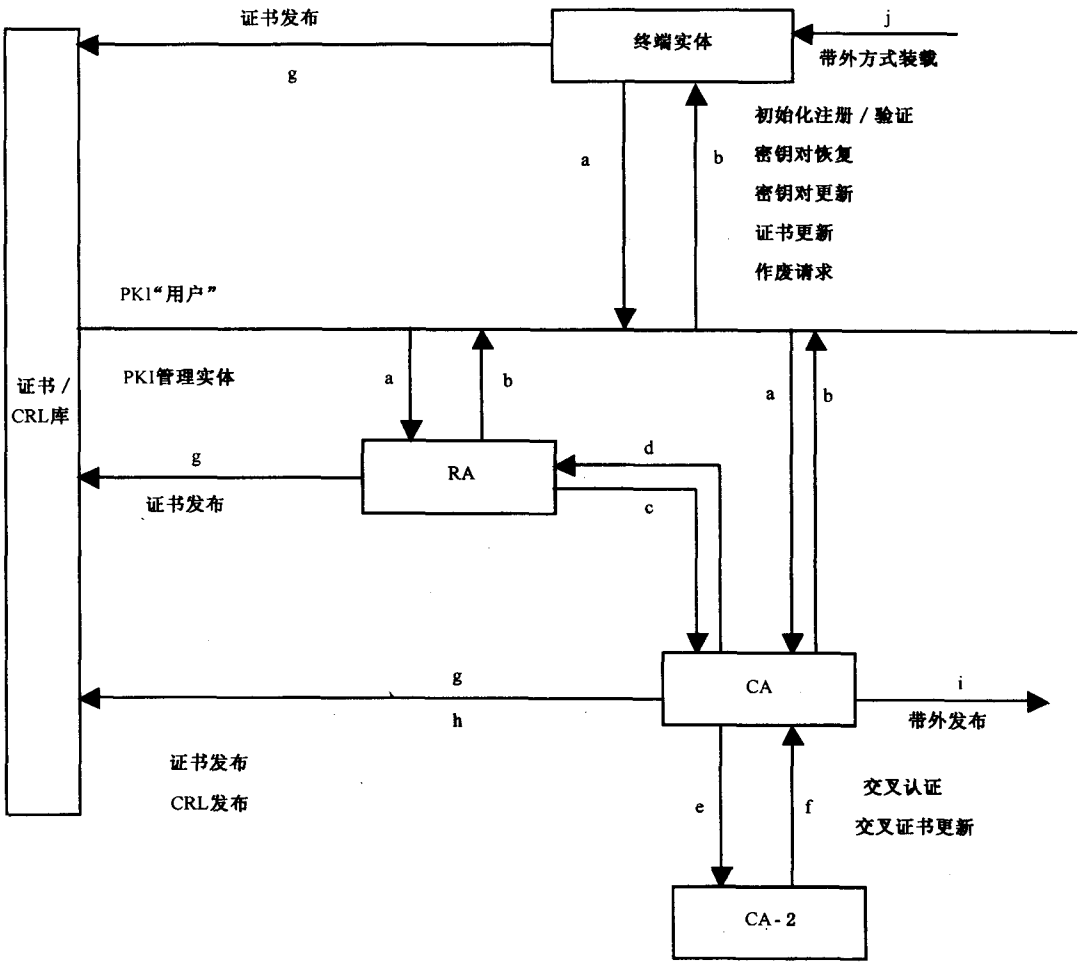

图 1 PKI 实体

在上层，各种 PKI 操作可以按下列方式分组：

a) CA 的建立。当建立一个新的 CA 时，需要完成一些必要的操作（例如：发布初始 CRL，导出 CA 公钥）。

b) 终端实体初始化：包括导入根 CA 公钥，以及获得 PKI 管理实体所支持的可选项信息。

c) 认证：各种操作都将导致创建新的证书：

1) 初始注册和认证：终端实体在 CA 为它签发证书之前第一次向 CA 或 RA 表明自己的身份。这一过程成功时的最终结果是 CA 为终端实体的公钥签发证书，并将该证书返回给终端实体和/或将该证书发布到公共的数据仓库中。这一过程通常包括多个“步骤”，还可能包括终端实体设施的初始化过程。例如，终端实体设施必须能够安全地导入 CA 公钥，以用来验证证书路径。此外，终端实体通常还需要导入自己的密钥对。

2) 密钥对更新：任何密钥对都需要定期更新（即用新的密钥对替换旧的密钥对），因此需要签发一个新的证书。

3) 证书更新：由于证书会过期，如果其他相关信息没有变化，那么证书就可以被“刷新”。

4) CA 密钥对更新：同终端实体一样，CA 密钥对也需要定期更新，但需要不同的机制。

5) 交叉认证请求：一个 CA 请求另一个 CA 签发一个交叉证书。“交叉证书”的主体 CA 与签发者 CA 完全不同，主体公钥信息(SubjectPublicKeyInfo)字段包含着验证密钥(即该证书是为主体 CA 的签名密钥对签发的)。交叉证书细致的区分时使用下面的术语：“域间交叉证书” —— 如果交叉证书的主体 CA 和签发者 CA 属于不同的管理域；其他的交叉证书则称作“域内交叉证书”。

注 1：上面所定义的“交叉证书”与 X.509 中定义的“CA 证书”是并列的。注意不要把“交叉证书”同 X.509 中的“cACertificate”属性相混淆，它们之间没有联系。

注 2：除非特别说明，否则一般认为术语“交叉证书”指的就是“域间交叉证书”。

注 3：交叉证书的签发可以是相互的(但并非必须这样做)；换句话说，两个 CA 可能彼此为对方签发交叉证书。

6) 交叉证书更新：与普通证书更新类似，不同之处就在于它操作的是交叉证书。

d) 证书/CRL 搜索操作：某些 PKI 管理操作将导致发布证书或 CRL。

1) 证书发布：产生证书之后，就需要通过一些方法发布这些证书。PKIX 中定义的方法可以是 7.3.13～7.3.16 中规定的方法，或者是 RFC2559、RFC2585(PKIX 系列规范的“操作协议”方案)中描述的其他方法(例如：LDAP)。

2) CRL 发布：与证书发布类似。

e) 恢复操作：当一个 PKI 实体“丢失”它的 PSE 时，需要通过某些 PKI 操作完成恢复工作。

密钥对恢复：作为可选操作，用户密钥资料(例如用户的解密密钥)可以由 CA、RA 或与 CA 或 RA 相关的密钥备份系统进行备份。如果一个实体需要恢复它已经备份的密钥资料(例如忘记了私钥保护密码或丢失了密钥链文件)，就需要一个支持密钥恢复的协议消息。

f) 撤销操作：某些 PKI 操作将需要创建新的 CRL 条目或新的 CRL。

撤销请求：一个经过授权的人向 CA 发出异常情况警告并要求撤销证书。

g) PSE 操作：PSE 操作(例如转移 PSE、更改口令等)的定义超出了本标准的范围，这里我们还是定义了一个 PKI 消息(CertRepMessage)，它可以作为该操作的基础。

注：在线协议并非是实现以上操作的唯一途径。对任何一个操作来说，离线方法可以达到同样的效果，本标准也并不强制使用在线协议。例如：当使用硬件介质时，很多操作都通过物理介质的传送来完成。

后面将定义一组支持以上操作的标准消息。关于在不同环境中传送这些消息的传输协议(基于文件的、在线、E-mail 和 WWW)的定义，已经超出了本标准的范围，将在其他文档中单独说明。

6 前提与限制

6.1 终端实体初始化

对于每一个终端实体，在与 PKI 管理实体进行交互之前，首先要申请获得一些信息，包括获得 PKI 系统所支持的功能、安全获得相关根 CA 的公钥。

6.2 初始注册/认证

终端实体的初始化注册和认证有很多种方案。由于 CA 执行的策略各不相同，并且终端实体的类型也有所不同，因此没有一种方案能适应所有的环境。

初始化注册前，终端实体与 PKI 还没有任何的联系。当终端实体已经拥有认证过的密钥对时，就可以进行简化或选择其他的方案。

以下对本标准支持的初始化注册和认证方案进行分类。方案中一部分为强制性的，一部分为可选择的。强制性的方案能够覆盖到大多数的实际应用，而可选方案满足那些不是很常用的应用。这样，在系统的灵活性和系统实现的简便上进行了折衷。

6.2.1 所用的准则

6.2.1.1 注册/认证的启动

就产生的 PKI 消息而言，初始化注册/认证的启动发生在产生第一条与终端实体相关的 PKI 消息

的地点。可能的场所是在终端实体，RA 或者 CA。

6.2.1.2 终端实体消息的最初认证

终端实体产生的请求证书的在线消息认证与否都可以，但要求对最初终端实体发给 PKI(CA/RA)的任何消息进行认证。

在本标准中，PKI(CA/RA)通过带外方式向终端实体发放秘密数据(初始认证密钥)和参考数据(用于识别密钥)来完成。然后初始认证密钥就可以用来保护相关的 PKI 消息了。

因此，通过判断在线消息是否经过初始鉴别从而对初始注册/认证方案进行分类。

注 1：本标准不讨论对 PKI 系统发给终端实体的消息的认证，因为在所有情况下，在终端实体设施安装根 CA 的公钥或基于初始认证密钥都可以实现这一认证。

注 2：如果终端实体发送的消息通过带外方式被鉴别，那么可以认为初始注册/认证流程是安全的。

6.2.1.3 密钥产生的地点

在本标准中，认为“密钥产生”的地点是密钥(无论是公钥还是私钥)第一次在 PKI 消息中出现的地方。注意，这不排除有一个密钥集中产生的服务，密钥可以在其他地方产生，然后使用一个(自定义的或者标准的)密钥产生请求/响应协议(该协议不在本标准的讨论范围之内)导入到终端实体、RA 或 CA 中。

密钥产生的地点有三种可能：终端实体、RA 或者 CA。

6.2.1.4 成功认证的确认

在为一个终端实体创建初始证书以后，通过让终端实体显示确认成功地接收到了包含证书(或表明证书已生成)的消息，从而可以得到附加的保证。当然，这个确认消息必须受到保护(通过初始认证密钥或者其他方式)。

这又提供了两种可能性：确认的或者未确认的。

6.2.2 强制的方案

上面的标准考虑到了大多数的初始注册/认证方案。要求符合本标准的 CA 设施、RA 设施和终端实体设施必须支持下面的第二种方案。如果需要，任何实体还可以支持其他的方案。

6.2.2.1 集中方案

按照上面的分类标准，这种方案可能是最简单的：

—— 启动发生在进行认证的 CA；

—— 不要求在线消息的认证；

—— 密钥由进行认证的 CA 产生(见 6.2.1.3)；

—— 不要求确认消息。

从消息流的角度来看，本方案意味着只要求一个由 CA 发送给终端实体的消息。这个消息必须包含终端实体的全部 PSE 信息。该消息使用加密传输，通过带外方式通知终端实体(如用电话通知消息的保护口令)，使终端实体认证并解密接收到的消息。

6.2.2.2 基本认证方案

按照上面的分类标准，本方案如下：

—— 启动发生在终端实体；

—— 要求进行消息认证；

—— 密钥由终端实体产生(见 6.2.1.3)；

—— 要求确认消息。

从消息流的角度来看，基本认证方案见图 2：