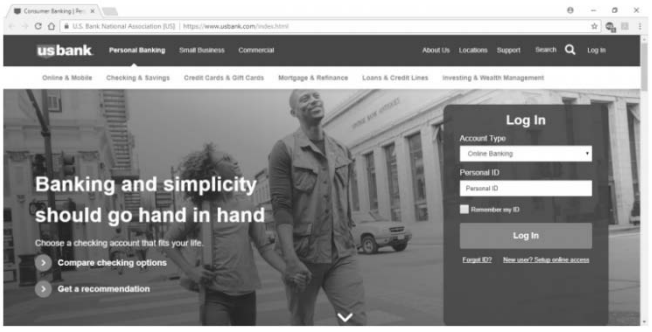
第 5 章　公钥基础设施

启蒙案例

如何判断网站是否可信呢？哪些网站是官方的？哪些是合法的？哪些是安全的？能借助哪些简单技术进行判断呢？举个例子，美国居民需要登录自己的银行账户，在浏览器的地址栏中键入银行的网站地址或 URL，如 ww.usbank.com，将打开如下的网页。

虚假钓鱼网站的故事人们耳熟能详，如果下面的是虚假网站该怎么办呢？



幸运的是，有一种非常简单的技术可以判断网站是否真实。在网站地址栏中，我们可以看到有一个小挂锁的符号，由于这是一个黑白页面，无法看到网站地址栏的颜色是否为绿色，如果不是绿色，则可能是警告符号；如果是绿色的，则表示该网站是安全的。

此外，用户可以单击挂锁符号，获得网站有效性的更多详细信息。单击挂锁符号后，将出现小对话框，可以查看网站的数字证书，如下所示。

对话框内容清楚地表明，网站已获得受信证书颁发机构颁发的证书，其有效期至 2019 年 8 月 2 日。单击上面窗口中的 Details 选项卡，会看到证书的更多详细信息。

任何用户都可以用这种简单的技术判断网站是否是欺诈性网站，避免被欺骗。

本章将学习公钥基础设施这一重要概念背后的关键技术。

学习目标

- 理解公钥基础设施（PKI）技术。
- 学习数字证书的概念及其用途。
- 了解证书签发机构（CA）的角色。
- 通过使用证书吊销列表（CRL）、在线证书状态协议（OCSP）和简单证书验证协议（SCVP），理解数字证书验证。
- 掌握如何管理公钥和私钥。

5.1 数 字 证 书

5.1.1 简介

我们已经详细讨论了密钥协商或密钥交换的问题，还介绍了为其专门设计的 Diffie-Hellman 之类的密钥交换算法如何解决这个问题，存在哪些缺点。非对称密钥加密是一个非常好的解决方案，但也有一个未解决的问题，即双方（即消息的发送方和接收方）如何互换公钥。显然，双方不能公开交换公钥，否则会引发针对公钥的中间人攻击！

因此，密钥交换或密钥协商的问题是个难题，事实上也是设计基于计算机的密码解决方案的最难解决的挑战之一。历经思考与多年的沉淀，**数字证书**（digital certificate），这一革命性的思想解决了这一难题，下面进行详细的介绍。

从概念上讲，数字证书相当于护照或驾照等证件。护照或驾照能确定持有人的身份，毫无疑问，护照至少可以证明如下信息。

- 姓名。
- 国籍。
- 出生日期和地点。
- 照片与签名。

同样，数字证书也能证明一些非常关键的信息，下面将仔细学习。

5.1.2 数字证书的概念

数字证书只是一个小型计算机文件。例如，笔者的数字证书实际上是一个计算机文件，文件名为 atul.cer，其中.cer 是 certificate 的前三个字母。当然，这只是一个例子，实际的文件扩展名可以不同。护照证明笔者与姓名、国籍、出生日期与地点、照片和签名等的关联，而数字证书证明笔者与公钥的关联，数字证书的概念如图 5.1 所示，注意，这只是一

个概念图，没有描述数字证书的实际内容。

我们没有指定用户与用户数字证书之间的关联是由谁正式批准的。显然，它必须是权威的，各方都信任的。想象一下，假设护照不是由政府机构签发，而是由普通店主签发，人们还会相信护照吗？ 同样，数字证书必须由某个受信任的实体签发，否则没人会信任数字证书。

正如前面所述，数字证书建立了用户与其公钥之间的关联。因此，数字证书必须包含用户名和用户的公钥，证明特定的公钥属于特定的用户。除此之外，数字证书还包含什么呢？图 5.2 给出了数字证书示例的简化图。

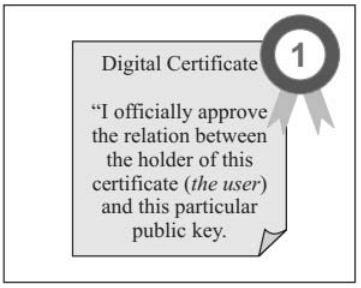


图 5.1　数字证书的概念图

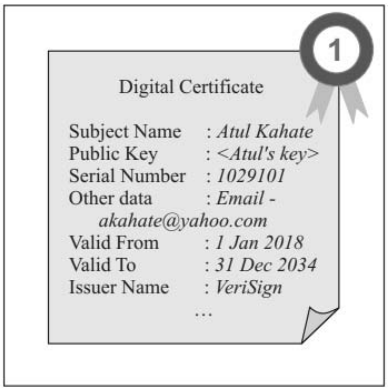


图 5.2　数字证书示例

注意这里有一些有趣的事情。首先，笔者的姓名显示为**主体名**（subject name）。事实上，数字证书中的任何用户名都称为主体名，因为数字证书可以颁发给个人、团体或组织。此外，还有另一个有趣的信息，称为**序列号**（serial number），在后面适当时候会分析它的含义。证书还包含其他信息，如证书的有效期和**签发者名**（issuer name）。下面通过与护照项的比较，理解数字证书各项的含义，如图 5.3 所示。

护照项	对应的数字证书项
姓名	主体名
护照号	序列号
有效期的起始日期	相同
有效期的终止日期	相同
签发者	签发者
照片与签名	公钥

图 5.3　护照与数字证书的相似处

如图 5.3 所示，实际上数字证书与护照非常相似。如每本护照都有一个唯一的护照号，每个数字证书也都有一个唯一的序列号。众所周知，相同颁发机构（如政府）签发的护照不会重号，同样，同一颁发者签发的数字证书也不会重号，谁颁发这些数字证书呢？下面给出答案。

5.1.3 证书机构（CA）

证书机构（Certification Authority，CA）是可以颁发数字证书的受信任机构。谁能成为 CA 呢？显然，不是任何人（如 Tom、Dick 和 Harry）都能作为 CA。CA 是必须受到每个人的信任，因此，各国政府能决定谁能作为 CA，谁不能作为 CA。通常，CA 是著名的组织，如邮局、金融机构、软件公司等。世界上最著名的两个 CA 是 VeriSign 和 Entrust。Safescrypt 有限公司是 Satyam Infoway 有限公司的子公司，于 2002 年 2 月成为印度的第一家 CA。

因此，CA 有权向个人和组织颁发数字证书，使其能在非对称密钥加密应用程序中使用数字证书。

5.1.4 数字证书技术细节

下面从技术角度，分析数字证书的内容。前面已从概念上进行了介绍，现在将从技术角度分析数字证书。读者可以跳过这部分内容，内容连贯性不会有任何损失。

X.509 标准定义了数字证书的结构。国际电信联盟（ITU）于 1988 年提出了这一标准，当时放在 X.500 标准中。从那时起，X.509 于 1993 年和 1995 年进行了两次修订，当前版本是第 3 版，称为 X.509V3。互联网工程任务组（IETF）于 1999 年发布了 X.509 标准的 RFC 2459，图 5.4 给出了 X.509V3 数字证书的结构。

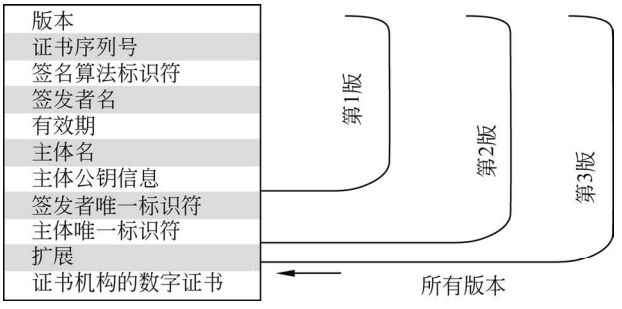


图 5.4 数字证书的内容

图 5.4 不仅给出了 X.509 标准数字证书的各个字段，还指定了哪一版的标准应包含哪些字段。如我们所见，X.509 标准的第 1 版包含 7 个基本字段，第 2 版增加了 2 个字段，第 3 版增加了 1 个字段。这些附加字段分别称为第 2 版和第 3 版的**扩展**（extensions）或**扩展属性**（extended attributes）。当然，所有版本最后都有一个额外的公共字段，下面分析这些字段，分别如图 5.5（a）、图 5.5（b）和图 5.5（c）所示。

第 2 版增加了两个新字段，处理因时间推移，签发者名（即 CA 名）和主体名（即证书持有者的姓名）可能会出现重复的问题。数字证书标准（RFC 2459）要求签发者名、主体名是不能重复的。因此，虽然第 2 版添加了这两个字段，但不鼓励使用，这两个字段都是可选的。如果需要使用，则仅用于区分无意中重复的签发者名和主体名。

X.509 标准第 3 版的数字证书结构增加许多扩展，如图 5.5（c）所示。

字段	说明
版本（Version）	标识数字证书所用的 X.509 协议的版本，目前，该字段值为 1、2、3 之一
证书序列号（Certificate Serial Number）	由 CA 生成的唯一整数值
签名算法标识符（Signature Algorithm Identifier）	标识 CA 签署证书的算法（稍后介绍）
签发者名（Issuer Name）	标识 CA 的**专有名**（Distinguished Name，DN），CA 创建并签署证书
有效期（Validity）（Not Before/Not After）	包含两个日期时间值：Not Before 和 Not after，指定证书的有效时间范围，其值指定日期和时间，精度是秒或毫秒
主体名（Subject Name）	标识数字证书所指的最终实体的 DN，即用户或组织。该字段不能为空，除非第 3 版扩展中定义了备用名称
主体公钥信息（Subject Public Key Information）	包含主体的公钥和与该密钥相关的算法。该字段不能为空

图 5.5（a）　X.509 数字证书各字段说明——第 1 版

字段	说明
签发者唯一标识符（Issuer Unique Identifier）	如果随着时间的推移，两个或多个 CA 使用相同的签发者名，则用该字段唯一标识 CA
主体唯一标识符（Subject Unique Identifier）	如果随着时间的推移，两个或多个主体使用相的主体名，则用该字段唯一标识主体

图 5.5（b）　X.509 数字证书各字段说明—— 第 2 版

字段	说明
机构密钥标识符（Authority Key Identifier）	CA 可能有多个私钥-公钥对。该字段定义这个证书使用哪个密钥对签名和验证
主体密钥标识符（Subject Key Identifier）	主体可能有多个私钥-公钥对，原因稍后解释。该字段定义了哪些密钥对用于签名和验证
密钥用途（Key Usage）	定义了这个证书的公钥操作范围。例如，可以指定这个公钥用于所有加密操作，或仅用于加密，或仅用于 Diffie-Hellman 密钥交换，或仅用于执行数字签名，或上述用途的一些组合等
扩展密钥用途（Extended Key Usage）	该字段可以补充或代替密钥用途字段，指定此证书能与哪些协议互操作，稍后分析。这些协议的示例有安全传输层（TLS）协议、客户端身份认证、服务器身份认证、时间戳等
私钥使用期（Private Key Usage Period）	定义证书对应的私钥/公钥的使用期限。如果此字段为空，则证书对应私钥的有效时间与公钥一样
证书策略（Certificate Policies）	定义 CA 对证书指定的策略和可选限定符信息，在此不讨论
策略映射（Policy Mappings）	仅在给定证书的主体也是 CA 时使用。即，当 CA 向另一个 CA 颁发证书时，指定认证的 CA 必须遵循哪些策略
主体备用名（Subject Alternative Name）	为证书主体定义一个或多个备用名。但是，如果主证书格式的主体名字段为空，此字段必须不能为空
签发者备用名（Issuer Alternative Name）	可选地，为证书的签发者定义一个或多个备用名
主体目录属性（Subject Directory Attributes）	用于提供有关主体的附加信息，例如主体的电话/传真号码、电子邮件 ID 等

图 5.5（c）　X.509 数字证书各个字段说明——第 3 版

字段	说明
基本约束（Basic Constraints）	表示此证书的主体是否能作为 CA。该字段还指定主体是否允许其他主体成为 CA。例如，如果 CA X 颁发此证书给另一个 CA Y，则 X 不仅可以指定 Y 是否能作为 CA，给其他主体颁发证书，还可以指定 Y 是否能指定别的主体作为 CA
名称约束（Name Constraints）	指定名称空间，这里不讨论
策略约束（Policy Constraints）	仅用于 CA 证书，这里不讨论

图 5.5（c） （续）

5.1.5 生成数字证书

5.1.5.1 相关各方

在了解数字证书概念与技术之后，下面介绍生成数字证书要执行的典型过程。参与各方是谁，它们需要各做些什么？这个过程涉及三方，一方是主体，即最终用户；一方为签发者，即 CA；第三方（可选）为参与证书的创建和管理的 RA。

由于 CA 要执行的各种任务太多，如颁发新证书、维护旧证书、撤销失效的证书等，因此 CA 可以委托第三方，即**注册机构** （Registration Authority，RA）分担一些它的任务。从最终用户角度来看，CA 和 RA 几乎没有区别。从技术上讲，RA 是最终用户和 CA 之间的中间实体，它协助 CA 完成日常工作，如图 5.6 所示。

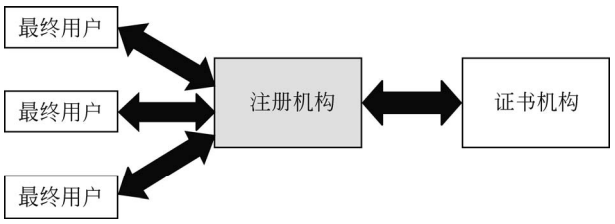


图 5.6 注册机构（RA）

RA 通常提供如下服务。

- 接收和验证新用户有注册信息。
- 代表最终用户生成密钥。
- 接收和授权密钥备份和恢复请求。
- 接收和授权证书撤销请求。

在最终用户和 CA 之间使用 RA 的另一个非常重要的用途是：使 CA 成为隔离的实体，保护 CA 免遭攻击。由于最终用户只与 RA 通信，所以可以重点保护 RA 和 CA 之间的通信，使得攻击者没有可乘之机。

但要注意的是，设立 RA 主要是为了方便最终用户和 CA 之间的交互。RA 不能颁发数字证书，必须由 CA 完成。此外，签发证书后，CA 负责所有证书的管理，例如，跟踪证书状态，对因故无效的证书发出撤销通知等。

5.1.5.2 证书生成步骤

生成数字证书包括几个步骤，如图 5.7 所示。

下面逐一介绍生成数字证书所需的步骤。

第 1 步：密钥生成

首先，是主体（即用户/组织）需要取得证书，可以使用下面两种不同的方法。

（1）主体可以使用某些软件生成私钥和公钥对，这个软件通常是 Web 浏览器或 Web 服务器的一部分，或者使用特殊的软件程序。主体必须保密所生成的私钥，然后将公钥连同关于自己的其他信息和证明发送给 RA，如图 5.8 所示。

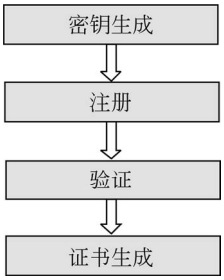


图 5.7　数字证书生成步骤

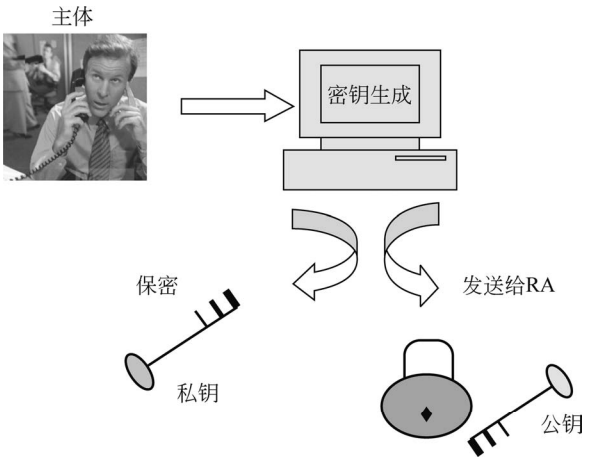


图 5.8　主体生成自己的密钥对

（2）RA 可以代表主体（用户）生成密钥对。之所以这样做，原因之一可能是用户不能生成密钥对；另一种可能是要求所有密钥必须由 RA 集中生成和分发，以便于执行一致的安全策略和密钥管理。当然，这种方法的主要缺点是 RA 知道用户的私钥。此外，在私钥生成后，将它发送给用户的传输过程中也有可能暴露，如图 5.9 所示。

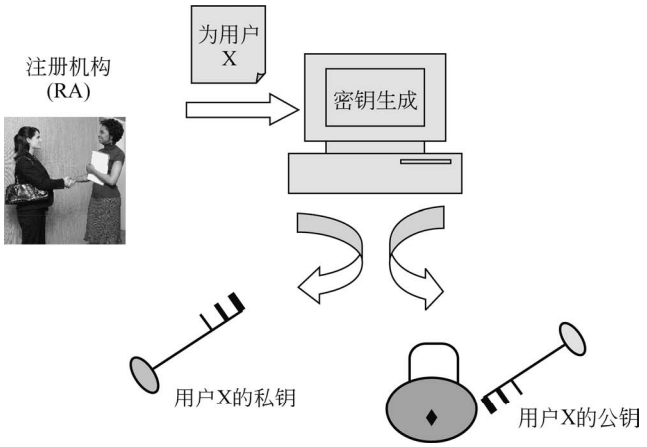


图 5.9　RA 代表主体生成密钥对

第 2 步：注册

只有当在第 1 步中是由用户生成密钥对时，才需要这一步，如果是 RA 代表用户生成密钥对，则这一步在第 1 步就完成了。

假设用户生成了密钥对，要将公钥、相关的注册信息（例如主体名，要出现在数字证

书中）以及所有关于用户的证明发送给 RA。为此，软件提供了一个向导，用户按提示输入数据，并在所有数据正确后提交，这些数据通过 Internet 传输给 RA。证书请求的格式已标准化，称为**证书签名请求**（Certificate Signing Request，CSR），这是**公钥加密标准**（Public Key Cryptography Standard，PKCS）之一，后面将要学习，CSR 也称为 PKCS#10。

但证明可能不是计算机数据，通常是纸质文件，如护照、商业文件的副本、收入/税务报表等，如图 5.10 所示。

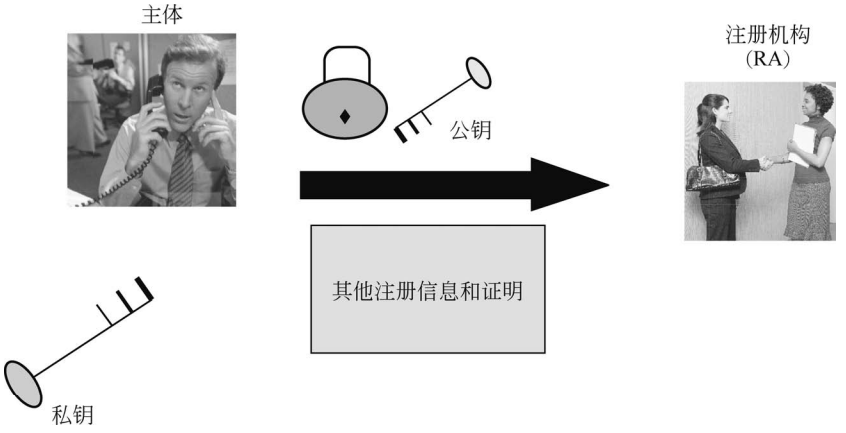


图 5.10　主体向 RA 发送公钥和证明

注意，用户不能将私钥发送给 RA，用户必须安全地保存它。实际上，私钥绝对不能离开用户的计算机。

在现实生活中，实际的证书请求页面如图 5.11 所示。

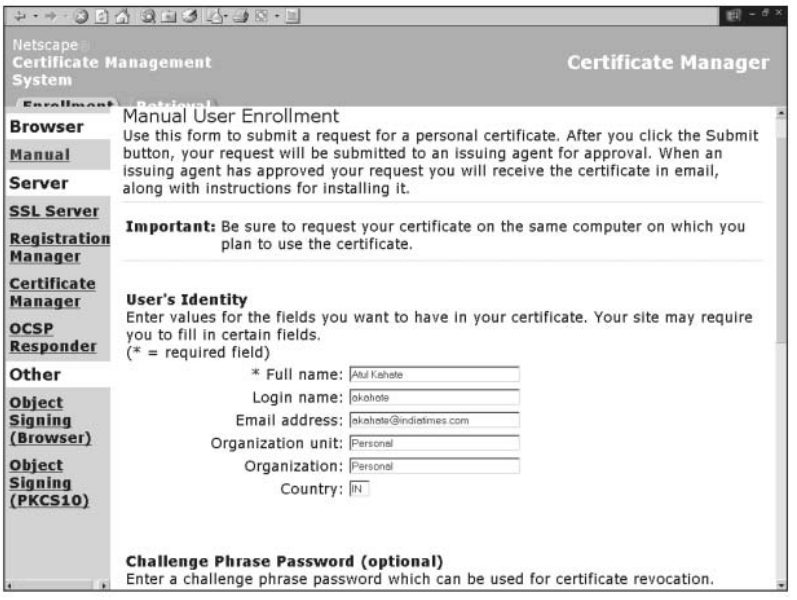


图 5.11　数字证书请求页面

之后，用户会得到请求标识符，用于跟踪证书请求的进度，如图 5.12 所示。

图 5.12　CA 收到证书请求的收据

第 3 步：验证

注册完成后，RA 必须验证用户的凭据，验证分为如下两方面。

（1）RA 需要验证用户的凭据，例如，提供的证明是否正确，RA 是否可以接受。如果实际用户是组织，那么 RA 要查看组织的业务记录、历史文件和信用证明。如果是个人用户，则进行的检查很简单，就是验证邮政地址、电子邮件 ID、电话号码、护照或驾照等。

（2）要保证请求证书的用户确实拥有私钥，这个私钥与向 RA 提出请求证书的公钥相对应，这一点非常重要。因为，必须有记录证明用户拥有与给定公钥相对应的私钥，否则，可能会造成法律问题，即如果用户声称自己从未拥有过私钥，则用其私钥签名的文件必然造成法律问题，这种检查称为检查私钥的**拥有证明**（Proof of Possession，POP）。RA 如何执行这种检查呢？可以有许多方法，主要如下。

- RA 可以要求用户必须用自己的私钥对其**证书签名请求**（Certificate Signing Request，CSR）进行数字签名。如果 RA 能用这个用户的公钥验证签名的正确性，则可以相信用户确实拥有私钥。
- 在这个阶段，RA 也可以生成随机数挑战；用这个用户的公钥加密随机数挑战，再将其发送给用户。如果用户能用其私钥解密，则 RA 相信用户拥有正确的私钥。
- 此外，RA 还可以为用户生成虚拟证书，用这个用户的公钥加密，再将其发送给用户。只有用户能解密这个加密证书，才能得到明文证书。

第 4 步：生成证书

假设，到目前为止，上述所有步骤都已完成，RA 会将用户的所有详细信息传递给 CA。CA 进行必要的验证，并为用户生成数字证书。有一些程序可以生成 X.509 标准格式的证书。 CA 将证书发送给用户，并保留一份证书副本作为自己的记录。CA 的证书副本保存在**证书目录**（certificate directory）中。证书目录是由 CA 维护的中央存储位置。证书目录的内容类似于电话目录的内容，用于证书管理和分发的单点访问。

目前没有描述证书目录结构的单一标准。但 X.500 标准已成为一种流行的选择，它不

仅可以存储数字证书，还可以存储有关服务器、打印机、网络资源的信息和用户的个人信息，如电话号码/分机号、电子邮 ID 等，以受控方式集中在中央位置。目录客户端可以使用目录协议，如**轻量级目录访问协议**（Lightweight Directory Access Protocol，LDAP），请求访问这个中央存储库的信息。LDAP 允许用户和应用程序根据自己的权限访问 X.500 目录。

然后 CA 将证书发送给用户，可以附加到电子邮件中；CA 也可以给用户发送电子邮件，通知证书已准备好，让用户从 CA 网站下载，后者如图 5.13 所示，用户从截屏可知，自己的数字证书已经准备好，可以从 CA 网站下载了。

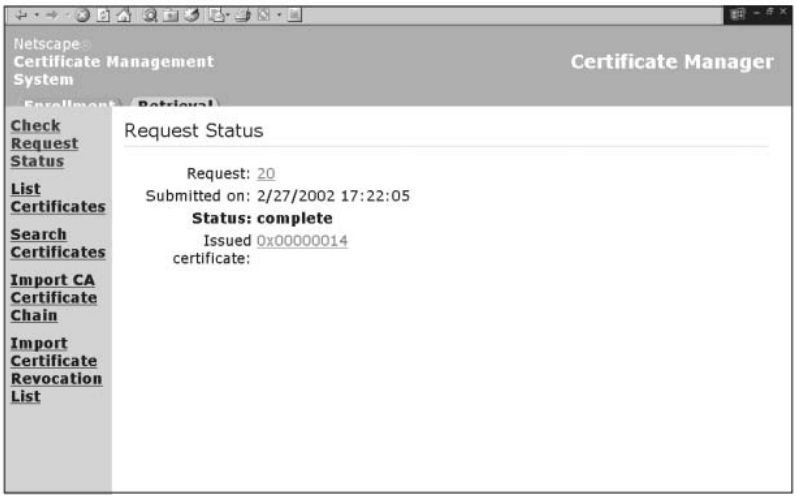


图 5.13　CA 通知用户证书已准备好，可以下载

用户选择下载此证书后，会看到如图 5.14 所示的截屏。注意，此截屏给出了版本、序列号、用于计算消息摘要和签署证书的算法、签发者、有效性、主体的详细信息等。

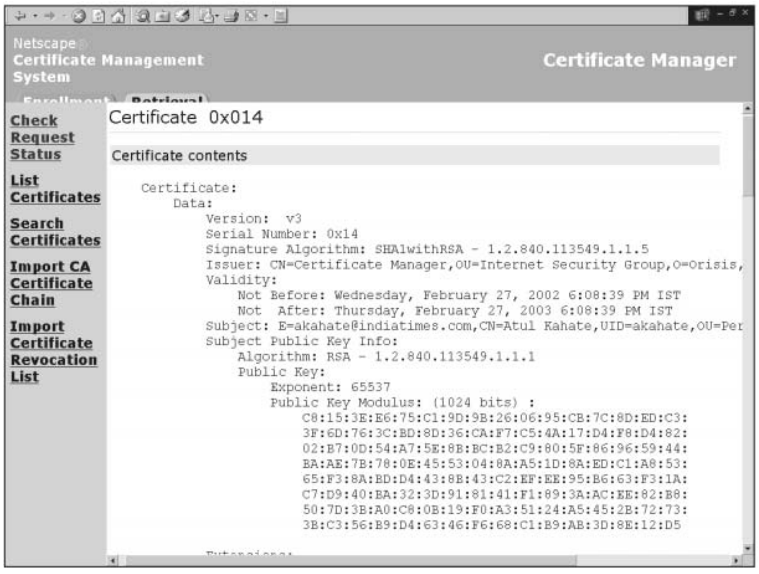


图 5.14　证书内容