的信任关系网啊！

2）一旦 CA 验证了某个实体的身份，这个 CA 会生成一个把其身份和实体的公钥绑定起来的**证书**（certificate）。这个证书包含这个公钥和公钥所有者全局唯一的身份标识信息（例如，一个人的名字或一个 IP 地址）。由 CA 对这个证书进行数字签名。这些步骤显示在图 8-14 中。

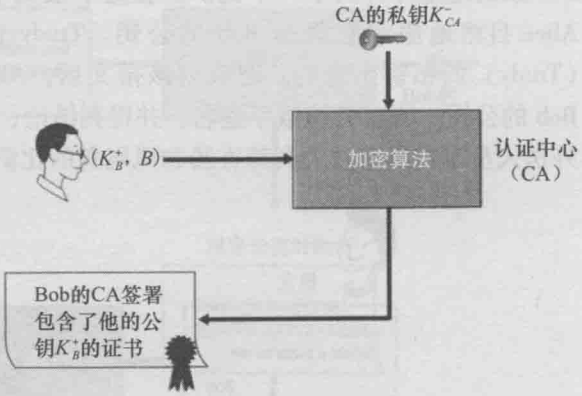

图 8-14 Bob 获得一份来自 CA 的证书

我们现在来看怎样使用认证来对抗“比萨订购”中的恶作剧者（如 Trudy）和其他意外情况。当 Bob 下订单的同时，他也发送了其 CA 签署的证书。Alice 使用 CA 的公钥来核对 Bob 证书的合法性并提取 Bob 的公钥。

国际电信联盟（International Telecommunication Union，ITU）和 IETF 都研发了用于 CA 的系列标准。ITU X.509［ITU 2005a］规定了证书的鉴别服务以及特定语法。［RFC 1422］描述了安全因特网电子邮件所用的基于 CA 的密钥管理。它和 X.509 兼容，但比 X.509 增加了密钥管理体系结构的创建过程和约定内容。表 8-4 显示了一份证书中的某些重要字段。

表 8-4 在 X.509 和 RFC 1422 公钥证书中的部分字段

字段名	描述
版本（Version）	X.509 规范的版本号
序列号（Serial Number）	CA 发布的证书的独特标识符
签名（Signature）	规定了由 CA 所用的对该证书签名的算法
颁发者名称（Issuer Name）	发行该证书的 CA 的标识符，用的是区别名（DN）格式［RFC 4514］
有效期（Validity period）	证书合法性开始和结束的时间范围
主题名（Subject name）	其公钥与该证书相联系的实体标识符，用 DN 格式
主题公钥（Subject public key）	该主题的公钥以及该公钥使用的公钥算法（及其参数）的指示

8.4 端点鉴别

端点鉴别（end-point authentication）就是一个实体经过计算机网络向另一个实体证明其身份的过程，例如一个人向某个电子邮件服务器证明其身份。作为人类，我们通过多种方式互相鉴别：见面时我们互相识别对方的面容，打电话时我们分辨对方的声音，海关的检查官员通过护照上的照片对我们进行鉴别。

在本节中，我们讨论经网络通信的双方如何能够鉴别彼此。此处我们重点关注当通信实际发生时鉴别“活动的”实体。一个具体的例子是一个用户向某电子邮件服务器鉴别他或她自己。这与证明在过去的某点接收到的报文确实来自声称的发送方稍有不同，如 8.3 节所述。

当经网络进行鉴别时，通信各方不能依靠生物信息比如外表、声波纹等进行身份鉴别。的确，我们会在后面的实例研究中看到，诸如路由器、客户/服务器进程等网络元素