第 2 章　PKI 包括哪些内容

2.1　PKI 体系框架

PKI 是 Public Key Infrastructure 的缩写，主要功能是绑定证书持有者的身份和相关的密钥对（通过为公钥及相关的用户身份信息签发数字证书），为用户提供方便的证书申请、证书作废、证书获取、证书状态查询等，并利用数字证书及相关的各种服务（证书发布，黑名单发布，时间戳服务等）实现通信中各实体的身份认证、完整性、抗抵赖性和保密性。

根据数字证书格式及密钥管理方式的不同，PKI 也包括多种模式，如 X.509 模式、PGP 模式、IBE/CPK 模式、EMV 模式等。X.509 模式的 PKI 也称作 PKIX。由于 X.509 标准已经成为数字证书格式的事实标准，因此大部分情况下 PKI 特指 PKIX。如非特殊说明，本文中 PKI 均指 PKIX。

PKI 体系框架主要包括三部分内容。

1．数字证书与私钥

用户或系统只有拥有自己的公钥和私钥后，才能实现数字签名和加解密功能。由于公钥是随机产生的，因此从公钥无法直接判断属于哪个用户。

为解决公钥与用户映射关系问题，PKI 引入了数字证书，用于建立公钥与用户之间的对应关系。数字证书实际上是一种特殊的文件格式，包含用户身份信息、用户公钥信息和 CA 私钥的数字签名。X.509 标准规定了数字证书的具体格式。数字证书中只包含公钥，并不包括私钥。由于数字证书中包含 CA 私钥的数字签名，因此数字证书具有防伪性。由于数字证书中不包含秘密信息，因此数字证书具有公开性。数字证书作为网络身份证，可有效解决网络世界中“你是谁”的问题。

为保证私钥的安全性，一般将私钥保存在硬件密码设备中（如个人的私钥可保存在 USB Key 或 IC 卡中，系统的私钥可保存在加密机或加密卡中），而且不允许私钥导出硬件密码设备；通过口令、指纹等方式来访问控制该硬件密码设备。如果将私钥保存在硬盘文件中，则需要通过口令进行加密保护，但私钥文件容易被复制。

2．数字证书的管理

为解决数字证书的签发问题，PKI 引入 CA，对数字证书进行集中签发。CA 是 Certificate Authority 的缩写，字面含义是证书权威，也称作 CA 中心、认证中心。CA 中心拥有自己的公钥和私钥，使用其私钥给用户（包含 CA 中心自己）签发数字证书。

CA 实际是一种特殊的公钥管理中心，负责数字证书的安全性，对数字证书的全生命周期进行管理，主要包括：数字证书的签发、数字证书的作废（注销、撤销或吊销）、数字证书的冻结（挂失）和解冻、数字证书的更新、数字证书的下载、数字证书状态查询等。

当私钥丢失时，如果没有备份和恢复机制，将导致公钥加密的所有数据都无法解密，可能给用户带来损失。为解决私钥的备份与恢复问题，PKI 引入了 KMC，用于对私钥的全生命周期进行管理。KMC 是 Key Management Center 的缩写。用户公私钥对可由 KMC 产生，提交 CA 签发数字证书后，将私钥和数字证书同时安全移交给用户，而 KMC 将私钥留作备份，可按需要给用户恢复。用户公私钥对也可由用户自己产生（使用软件或密码设备），在向 CA 中心申请数字证书时，可将私钥安全提交 KMC 留作备份。

为防止用户身份被冒用，应保证用户私钥的唯一性，不允许备份恢复。为防止公钥加密后的数据无法解密，应提供用户私钥的备份恢复机制。为解决这两种矛盾的应用需求，PKI 引入双证书机制：签名证书和加密证书。签名证书及私钥只用于签名验签，不能用于加密解密，该公私钥对必须由用户自己产生，KMC 不备份签名私钥。加密证书及私钥只用于加密解密，不能用于签名验签，该公私钥对必须由 KMC 产生，且 KMC 对加密私钥进行备份。

CA 中心存储着所有数字证书，并通过公开服务形式供用户随时查询或下载。为解决数字证书查询或下载的性能问题，避免 CA 中心成为性能瓶颈，PKI 引入了 LDAP 技术，通过 LDAP 方式对外提供高速证书查询或下载服务。LDAP 为轻量目录访问协议，是 Light-weight Directory Access Protocol 的缩写。

当用户私钥泄露后，CA 中心有责任将该用户的证书标记为失效。但用户如何获得对方证书是否失效的状态呢？为方便用户获得证书状态，PKI 引入了 CRL 和 OCSP 技术。CRL 为证书作废列表，是 Certificate Revocation List 的缩写，也称作证书黑名单。OCSP 为在线证书状态协议，是 Online Certificate Status Protocol 的缩写。

在保证 CA 系统安全性的前提下，为方便证书业务远程办理、方便证书管理流程与应用系统结合，PKI 引入了 RA，专门用于对用户提供面对面的证书业务服务，负责用户证书办理/作废申请、用户身份审核、制作证书并移交用户等功能，而涉及证书签发时则提交 CA 系统集中处理。RA 是 Registry Authority 的缩写，又称作 RA 中心、注册中心。有时候，证书管理流程会与应用业务流程结合，并不单独体现出来，如对于网上银行，证书管理流程就会融合到网银业务流程中。

为保证 CA 系统在数字证书管理方面的规范性、合规性和安全性，PKI 引入电子认证服务机构，以第三方运营的方式对外提供数字证书相关服务。《电子签名法》规定："电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。"显然，电子签名法不仅赋予了电子签名的法律效力，而且明确了电子认证服务提供者的法律地位。电子认证服务提供者，又称作电子认证服务机构或 CA 中心，需要独立运营，不仅需要满足政策法规的各项要求，而且需要满足业务运营的业务需求。

3．数字证书的应用

基于数字证书可实现四种基本安全功能：身份认证、保密性、完整性和抗抵赖性。

基于证书接口中间件（模块或组件），应用系统可以很方便地使用数字证书技术，从而提高应用系统的身份认证强度、保证应用系统中各种敏感数据的保密性、保证应用系统中各种敏感数据和交易记录的完整性、用户各种操作或交易的不可否认性（抗抵赖性）。

PKI 技术经过 30 多年的发展历程，已经形成比较完善的标准规范体系，几乎覆盖应用系统的各个方面，目前很多软件都已经支持数字证书技术，如操作系统、数据库系统、Web 服

务器、应用服务器等。由于受应用环境多样性和应用技术复杂性的影响或限制，在不同的应用环境和应用技术下，数字证书技术应用的方式可能差异很大。

网上报税和网上银行是数字证书应用的典型案例。国内大部分省份上千万家企业已经通过数字证书在进行网上报税。数字证书（俗称 U 盾）已经成为国内网上银行的标准配置。如果没有数字证书，企业用户将不允许使用网上银行。上亿个人用户已经通过数字证书访问网上银行实现转账或汇款等资金操作。

PKI 体系框架如图 2-1 所示。

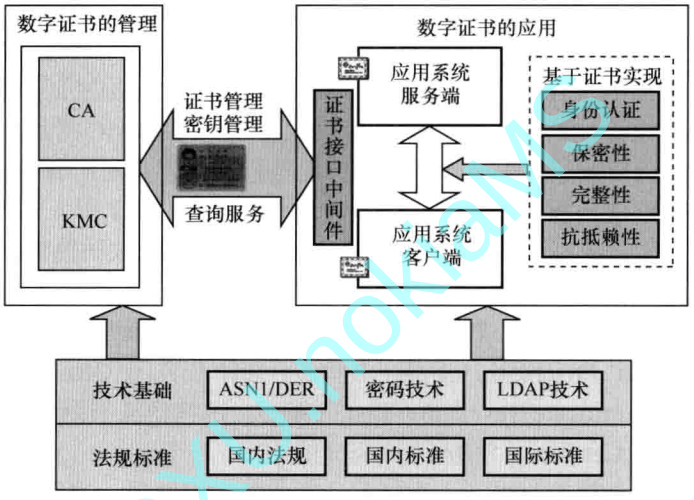

图 2-1　PKI 体系框架

2.2　PKI/数字证书与私钥

1. 数字证书的最初目的是建立公钥与用户之间的对应关系

由于公钥是随机产生的，从公钥无法直接判断属于哪个用户。为解决公钥与用户映射关系问题，PKI 引入数字证书，用于建立公钥与用户之间的对应关系。

数字证书实际是一种特殊的文件格式，包含用户身份信息、用户公钥信息和 CA 私钥的数字签名。用户身份信息由姓名或名称、单位、城市、国家等组成。X.509 标准规定了数字证书的具体格式。

由于数字证书中包含用户身份信息和公钥信息，根据数字证书就可直接判断该公钥属于哪个用户。如某数字证书包含用户信息“诸葛亮”和公钥 PK，则可判断公钥 PK 就是诸葛亮的。

由于数字证书中包含 CA 私钥的数字签名，使用 CA 公钥对数字证书中 CA 私钥的数字签名进行解密处理后，就可立刻判断该数字证书是否被篡改，因此数字证书具有防伪性，于是，数字证书中公钥和用户之间对应关系也值得可信。当然，数字证书防伪性的前提是公钥算法和 CA 私钥都是安全的。

由于数字证书中不包含秘密信息，因此数字证书可公开发布。

数字证书主要内容显示如图 2-2 所示，其中，“使用者”为用户身份信息，“公钥”为用户公钥信息，“有效期”属于附加策略。

图 2-2　数字证书主要内容显示

2. 数字证书可作为网络身份证

现实生活中，公安部为每人颁发一张二代身份证，身份证上包含姓名、性别、出生日期、省份、身份证号、照片等信息。当购票、住店、坐飞机时，身份证持有人（或持证人）只需出示身份证即可证明自己的身份。只有通过以下四个方面的合法性验证，才能完全确认持证人的合法身份：

（1）验证身份证是否伪造。需要专门的二代身份证读写设备来验证。

（2）验证身份证信息是否正确。需要查询身份证数据库，需要公安部门提供；也可由公安部门在发放身份证时保证。

（3）验证身份证是否与持证人一致。需要对比身份证上照片与持证人的长相。

（4）验证身份证是否在黑名单上。需要查询黑名单数据库，如公安部通缉犯清单，需要公安部门提供。

既然数字证书包含用户身份信息，而且具有防伪性且可以公开，那么数字证书持有人（或持证人）在网络世界中能否也像现实生活中一样，只需出示数字证书即可证明自己身份呢？答案是肯定的。如果能通过类似二代身份证的四个方面合法性验证，数字证书就可作为网络身份证。下面来确认一下，数字证书能否通过四个方面的合法性验证：

（1）验证数字证书是否伪造。可通过 CA 公钥验证。

（2）验证数字证书中信息是否正确。可由 CA 中心在签发数字证书时保证。

（3）验证数字证书是否与持证人一致。可要求持证人使用私钥对特定数据进行加密或签名，然后使用数字证书中的公钥来解密该数据或验签，从而可验证持证人是否持有与数字证书中的公钥对应的私钥。

（4）验证数字证书是否在黑名单上。可通过查询黑名单数据库来实现，但需要 CA 中心提供黑名单。

因此，数字证书作为网络身份证，可有效解决网络世界中“你是谁”的问题。由于数字证书采用公钥密码技术实现，从技术上保证了每个人“钥匙”的唯一性，既不重复也无法复制，所以数字证书比现实生活中的各种钥匙安全很多。

3．数字证书可附加很多策略

由于数字证书具有防伪性和公开性，因此数字证书中不仅可包含用户身份信息和用户公钥信息，而且还可以附加其他策略信息，这些信息同样具有防伪性和公开性。

X.509 数字证书标准中规定常用策略信息主要包括：

（1）有效期。包括起始时间和终止时间。

（2）密钥用途。表示该公钥和私钥用于什么目的，如数据签名、数据加密、签发证书、用于安全电子邮件等。

（3）别名。包括持证人别名和 CA 中心别名。

（4）黑名单地址。

（5）是否 CA 中心的数字证书。如果是 CA 中心的数字证书，则规定能签发几级证书。

4．CA 中心的数字证书

用户在验证数字证书是否被篡改时，必须首先获得 CA 中心的公钥。为方便用户识别 CA 中心的公钥，CA 中心也为自己签发数字证书。该证书包含 CA 中心公钥、CA 中心身份信息和 CA 中心私钥的签名。CA 中心的数字证书有时也称作 CA 证书。

由于 CA 证书是验证其他证书合法性的前提和基础，所以 CA 证书的正确性至关重要。尽管可通过网络直接下载获取 CA 证书，但为避免被欺骗，需要通过其他方式验证 CA 证书的正确性。可通过电话方式、官方报纸或官方电视公布 CA 证书的摘要值，用户通过核对该摘要值即可确认该证书的正确性。

5．私钥

对于公钥密码技术，公钥和私钥是成对出现的。公钥以数字证书形式存在，可以公开，但私钥必须保密。为保证私钥的安全性，一般将私钥保存在硬件密码设备中（如个人的私钥可保存在 USB Key 或 IC 卡中，系统的私钥可保存在加密机或加密卡中），而且不允许私钥导出硬件密码设备；通过口令、指纹等方式来访问控制该硬件密码设备。如果将私钥保存在硬盘文件中，则需要通过口令进行加密保护，但私钥文件容易被复制。

为保证私钥的唯一性，可只允许在硬件密码设备内产生公私钥对，通过硬件技术保证私钥无法导出，然后只导出公钥提交 CA 中心签发数字证书。

2.3 PKI/CA 与 KMC

1．CA 最初目的是签发数字证书

为解决数字证书的签发问题，PKI 中引入了 CA，用于对数字证书进行集中签发。CA 是 Certificate Authority 的缩写，字面含义是认证机构，也称作 CA 中心、认证中心。CA 中心拥