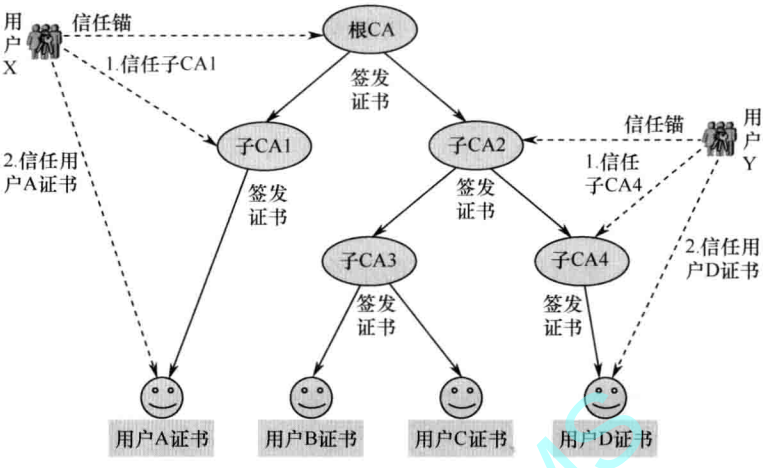

图 2-5　PKI 根 CA 信任模型

2.7.2　交叉认证信任模型

该信任模型下，根 CA 之间可以互相签发交叉认证证书，该交叉认证证书等同于子 CA 证书。在不增加信任锚的前提下，就可将信任关系传递到其他 CA 管理域。一般情况下，只有根 CA 之间签发交叉认证证书，子 CA 之间不签发交叉认证证书。

如图 2-6 所示，根 CA1 给根 CA2 签发交叉认证证书根 CA2(1)，根 CA2 给根 CA1 签发交叉认证证书根 CA1(2)。

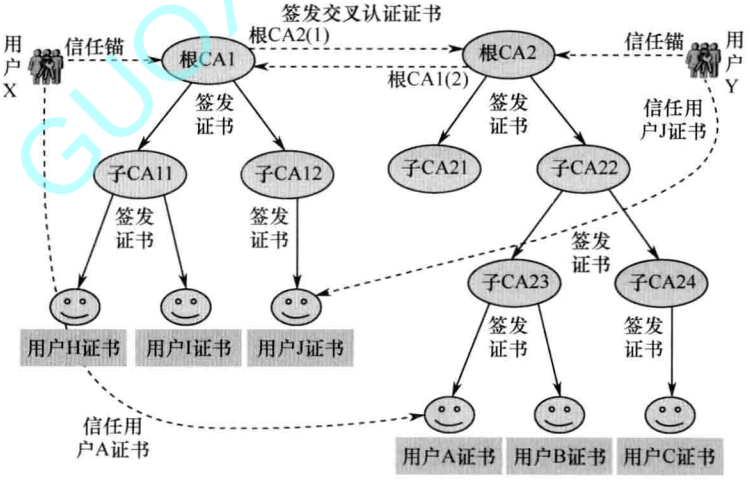

图 2-6　PKI 交叉认证信任模型

用户 X 的信任锚为根 CA1，因此它可信任根 CA2 管理域内的用户 A 证书。于是，从用户 X 的角度，用户 A 证书的信任链为：根 CA1→根 CA2(1) →根 CA2→子 CA22→子 CA23→用户 A 证书。

用户 Y 的信任锚为根 CA2，因此它可信任根 CA1 管理域内的用户 J 证书。于是，从用

户 Y 的角度，用户 J 证书的信任链为：根 CA2→根 CA1(2) →根 CA1→子 CA12→用户 J 证书。

交叉认证信任模型中，当有 N 个根 CA 时，最多需要签发 $N(N-1)$个交叉认证证书。

2.7.3　桥 CA 信任模型

该信任模型下，引入独立的桥 CA 中心，等同于虚拟的根 CA。所有根 CA 与桥 CA 之间互相签发交叉认证证书。在不增加信任锚的前提下，就可将信任关系传递到其他 CA 管理域。

如图 2-7 所示，根 CA1 与桥 CA 之间的交叉认证证书为：根 CA1(q)和桥 CA(1)；根 CA2 与桥 CA 之间的交叉认证证书为：根 CA2(q)和桥 CA(2)。

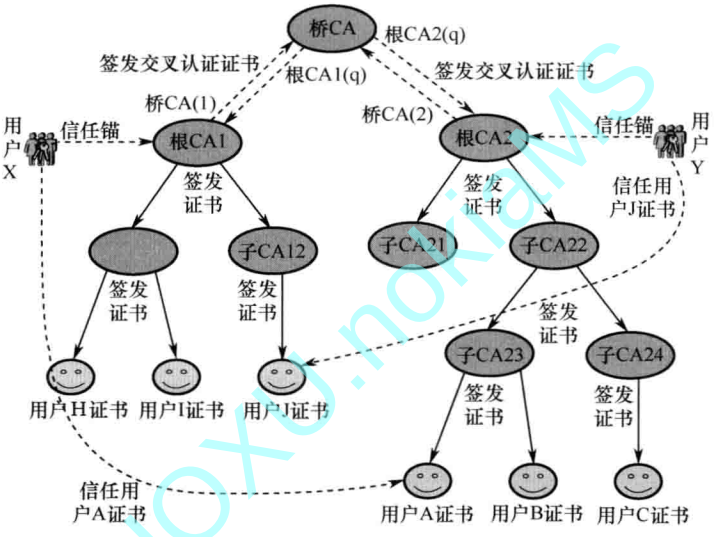

图 2-7　PKI 桥 CA 信任模型

用户 X 的信任锚为根 CA1，因此它可信任根 CA2 管理域内的用户 A 证书。于是，从用户 X 的角度，用户 A 证书的信任链为：根 CA1→桥 CA(1)→桥 CA→根 CA2(q)→根 CA2→子 CA22→子 CA23→用户 A 证书。

用户 Y 的信任锚为根 CA2，因此它可信任根 CA1 管理域内的用户 J 证书。于是，从用户 Y 的角度，用户 J 证书的信任链为：根 CA2→桥 CA(2)→桥 CA →根 CA1(q) →根 CA1→子 CA12→用户 J 证书。

桥 CA 信任模型中，当有 N 个根 CA 时，最多只需要签发 $2N$ 个交叉认证证书。

2.7.4　信任列表信任模型

该信任模型下，用户可以拥有多个信任锚，如图 2-8 所示。

用户 X 的信任锚为根 CA1 和子 CA22，因此它可信任根 CA1 管理域内的用户 H 证书，也可信任子 CA22 管理域内的用户 A 证书。于是，从用户 X 的角度，用户 H 证书的信任链为：根 CA1→子 CA11→用户 H 证书；用户 A 证书的信任链为：子 CA22→子 CA23→用户 A 证书。

用户 Y 的信任锚为根 CA2 和根 CA1，因此它可信任根 CA2 管理域内的用户 C 证书，也可信任根 CA1 管理域内的用户 J 证书。于是，从用户 Y 的角度，用户 C 证书的信任链为：

根 CA2→子 CA22→子 CA24→用户 C 证书；用户 J 证书的信任链为：根 CA1→子 CA12→用户 J 证书。

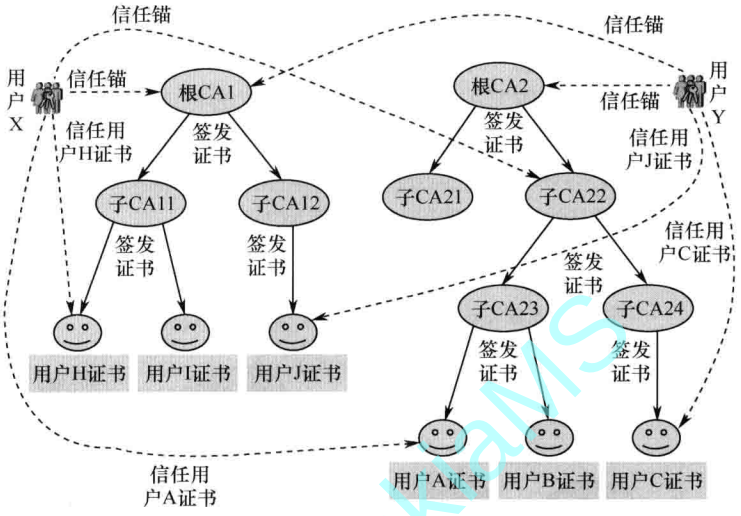

图 2-8　PKI 信任列表信任模型

Web 浏览器属于典型的信任列表信任模型，已经内置了多个信任锚，如图 2-9 所示。

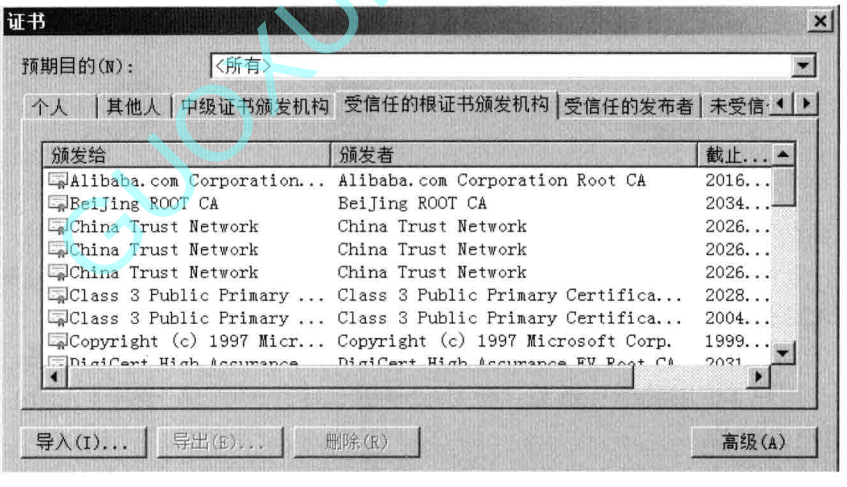

图 2-9　Web 浏览器已内置多个信任锚

第 3 章　其他非对称密钥管理体系

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，本书中 PKI 均指 PKIX。

3.1　PGP

1．PGP 简介

PGP 是 Pretty Good Privacy 的简称，字面含义是完美隐私。PGP 实际是一个基于公钥算法的加密软件，提供文件安全保护、安全电子邮件、VPN 安全通信等功能。文件安全保护主要包括文件或文件夹加密、硬盘或虚拟磁盘加密、文件粉碎或擦除等功能。安全电子邮件主要包括邮件内容加密、邮件发送者身份认证等功能。

PGP 诞生于 1991 年，由原作者 Philip Zimmermann 发表，属于开源且免费软件。由于受 Symantec 公司收购影响，PGP 从 10.0.2 版本开始将不再独立发布，而是以安全插件形式集成于 Symantec 公司的安全产品中，如 Norton。

2．PGP 密钥格式：密钥环

PGP 为每个节点（或用户）提供一对数据结构，一个用于存放本节点（或用户）自身的公私钥对，另一个用于存放本节点知道的其他用户的公钥，即私钥环（Private Key Ring）和公钥环（Public Key Ring），如图 3-1 所示。

私钥环

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
⋮	⋮	⋮	⋮	⋮
Ti	KU_i mod 2^{64}	KU_i	$E_{H(P_i)}[KR_i]$	User i
⋮	⋮	⋮	⋮	⋮

公钥环

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
Ti	KU_i mod 2^{64}	Ku_i	trust_flag$_i$	User $_i$	trust_flag$_i$		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

*=field used to index table

图 3-1　PGP 私钥环和公钥环

其中，User ID 表示用户名称，通常用邮件地址表示；Private Key 表示私钥，使用口令加密存储，保存于 Encrypted Private Key 中；Public Key 表示公钥；Key ID 表示密钥唯一标识；Timestamp 表示时间戳。私钥环和公钥环可以用 User ID 或 Key ID 进行索引。

3．PGP 密钥管理

为有效解决好密钥与用户映射关系的难题，PGP 引入了公钥介绍机制，基本原理是：

（1）公钥信任级别分为：最高信任（ultimate trust）、完全信任（complete trusted）、接近信任（marginally trusted）、不信任（untrusted）、不认识（unknown）。

（2）每个用户可以使用自己的私钥对他人的公钥进行签名。每个公钥可以拥有多个他人的签名。

（3）向公钥环新增公钥时，如果能完全确认该公钥的拥有者，则该公钥的信任级别设置为 Ultimate Trust。

（4）如果新增公钥拥有多个签名，则通过公钥环中这些签名对应公钥的信任级别，来确定该新公钥的信任级别。

PGP 密钥管理实际是模拟现实社会中人们的交往关系。公钥可以由单个朋友或多个朋友推荐，根据推荐者的信任程度自动将公钥分为不同的信任级别，最后由用户参考决定对该公钥的信任程度。

4．PGP 密钥应用

PGP 密钥应用主要包括六种基本功能或服务：认证、保密、认证与保密、压缩、邮件兼容性、分段，如表 3-1 所示。

表 3-1　PGP 基本功能或服务

基本功能	使 用 算 法	说　　明
认证	RSA SHA	将消息按照 SHA1 算法产生消息摘要，使用发送者私钥对消息摘要按照 RSA 算法加密（签名）。 将消息明文、签名一起发送
保密	RSA CAST、IDEA、3DES	按照算法 CAST-128、IDEA 或 3DES 产生会话密码后将消息加密，使用接收方公钥按照 RSA 算法加密会话密钥。 将消息密文、会话密钥密文一起发送
认证+保密	RSA SHA CAST、IDEA、3DES	将消息按照 SHA1 算法产生消息摘要，使用发送者私钥对消息摘要按照 RSA 算法加密（签名）；按照算法 CAST-128、IDEA 或 3DES 产生会话密码后将消息与签名加密，使用接收方公钥按照 RSA 算法加密会话密钥。 将消息与签名密文、会话密钥密文一起发送
压缩	ZIP	消息在传送或存储或加密前用 ZIP 压缩
邮件兼容性	Base 64	为了对电子邮件应用提供透明性，使用 Base 64 算法将消息明文或密文转换成 ASCII 字符串
分段	无	为了符合最大消息尺寸限制，对消息进行分段和重新组装

3.2　EMV

1．EMV 简介

EMV 组织由 EUROPAY、MASTERCARD、VISA 国际组织共同成立，负责管理、维护和修订 EMV 标准，制定相关检测案例，以保证其可在全球范围内通用。2002 年 EUROPAY