PKI 信任模型

实际网络环境中不可能只有一个 CA．多个认证机构之问的信任关系必须保证原有的 PKI 户不必依赖和信任专一的 CA，否则将无法进行扩展、管理和包含。信任模型建立的目的是确保一个认征机构签发的证书能够被另一个认证机构的用户所信任。常见的信任模型包括以下四种：

严格层次信任模型

严格层次信任模型是一个以主从 CA 关系建立的分级 PKl 结构√芭可以描绘为一棵倒转的树，在这棵树上，根代表一个对整个 PKI 域内的所有实体都有特别意义的 CA：根 CA，在根 CA 的下面是多层子 CA．与非 CA 的 PKI 实体相对应的树叶通常被称作终端用户

在严格层次信任模型中，上层 CA 为下层颁发证书，所有的实体都信任根 CA，以根 CA 作为信任点。信任关系是单向的，上层 CA 可以而且必须认证下层 CA，但下层 CA 不能认}j：E 上层 CA，根 CA 通常不直接为终端用户颁发证书而只为子 CA 颁发证书．两个不同的终端用户进行交互时，双方都提供自己的证书和数字签名，通过根 CA 来对证书进行有效性和真实性的认证．只要找到一条从根 CA 到一个证书的认证路径，就可以实现对证书的验证。

分布式信任模型

与严格层次信任模型中的所有实体都信任唯一 CA 相反，分布式信任模型把信任分布在两个或多个 CA 上，在分布式信任模型中，CA 间存在着交叉认证。因为存在多个信任点，单个 CA 安全性的削弱不会影响到整个 PKI．因此陔信任

模型具有更好的灵活性但其路径发现比较困难 .因为从终端用户到信任点建立证书的路径是不确定的。

以用户为中心的信任模型

在以用户为中心的信任模型中 ,每个用户自己决定信任哪些证书和拒绝哪些证书，没有可信的第三方作为 CA，用户就是自己的根 CA．通常，用户的信任对象一般为关系密切的用户．

以刚户为中心的信任模型具有安全性高和用户可控性强的优点 .但是其使其范闱较小，因为要依赖用户自身的行为和决策能力，这在技术水平较高的群体中是可行的，而在一般的群体中是不现实的

交叉认证模型

交叉认证是一种把以前无关的 cA 连接在一起的机制．可以使得它们各自终端用户之问的安全通信成为可能．有两种类型的交叉认证：域内交叉认证和域间交叉认证。