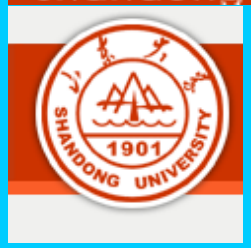
山东大学
Shandong University



Computer Science&Technology School of Shandong University

PKI Principles and Technology

(Chapter 4 Trust Models)

Instructor: HouMengbo 侯孟波
Email: houmb AT sdu.edu.cn
Office: Information Security Research Office.
Research Building Room 217,Software School of SDU

信任模型

- 解决实体之间信任的证书如何确定，如何建立信任，如何控制信任
- 讨论几种信任关系模型
  - 单一直接信任
  - 严格层次结构
  - 对等结构
  - 网状结构
  - 用户为中心的结构
  - 混合模型

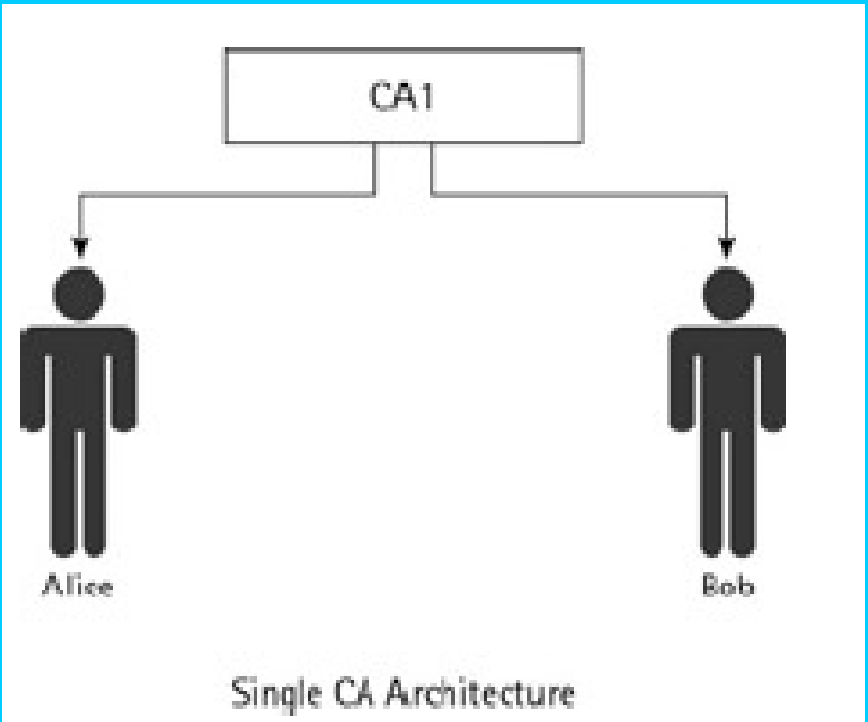
信任-相关概念

- **信任**: 如果一个实体假定另一个实体会严格的像它期望的那样行动,就称它**信任**那个实体.信任包含双方的一种关系以及对该关系的期望.
  - Predictability
  - Assets
  - Uncertainty

信任-相关概念

- **信任水平(信任度)**:描述了信任的一方对另一方的信任程度,信任水平高低的情况,可能需要引入第三方.信任总是与风险相联系
- **信任模型** 规定了最初信任的建立,以及它允许对基础结构的安全性以及被这种结构所强加的限制进行更详尽的推理.
- **信任域**: 是公共控制下或服从于一组公共策略的系统集,策略可以通过明确规定,也可通过操作过程指定.信任域可以按照组织或地理界限来划分.
- **信任锚**：信任模型中，直接确定一个身份或通过可信实体签发证明身份，方能作出信任决定。这个可信实体称为信任锚。
- **直接信任、外部信任锚**（传递信任）
- **信任关系**：信任模型描述了信任关系的方法，信任关系可以是单向的，也可以是双向的
- **信任路径**越短，通常越容易建立信任关系

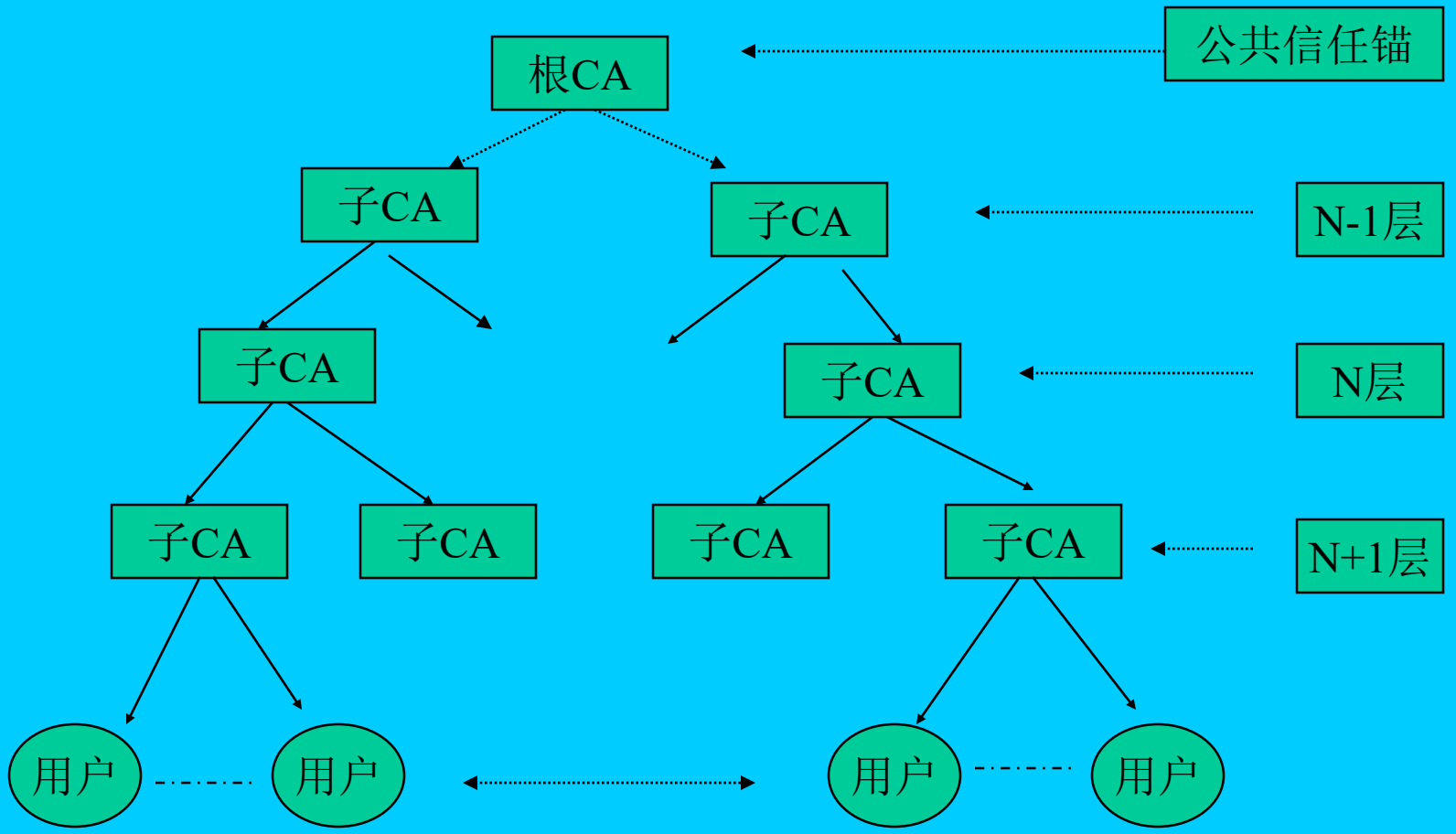
信任模型－ Single CA



Single CA Architecture

All the entities in this architecture communicate with each other in a trusted environment, as there is a common point of trust, which is the CA； but suffers from scalability issues.

信任模型一 Enterprise (Hierarchical) CA

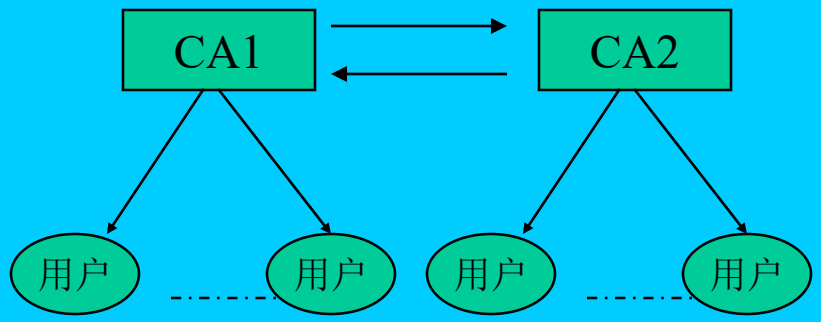


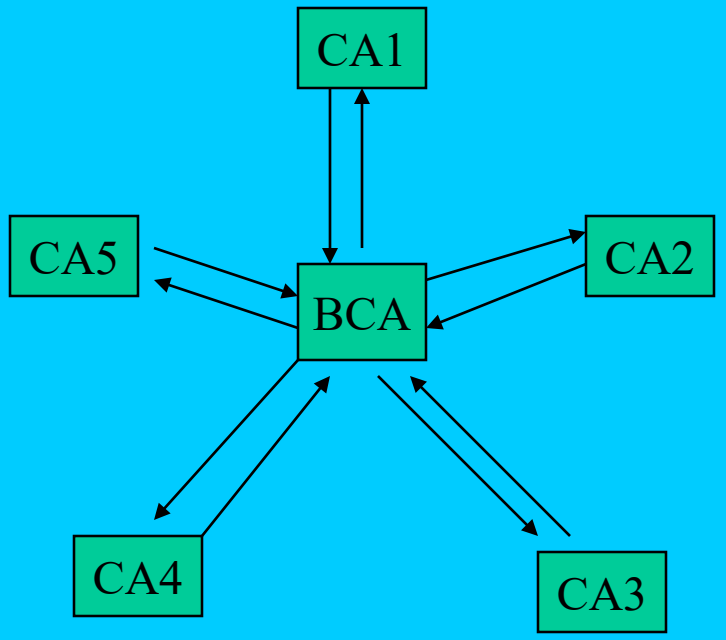
严格层次结构

- 使用最为广泛的信任模型
- 证书路径长度平均只有层次树高的一半
- 缺点是： 虽然在小规模群体容易形成公共根CA达成一致信任，但是不可能在全局范围达成一致信任。

信任模型—对等结构（交叉认证）

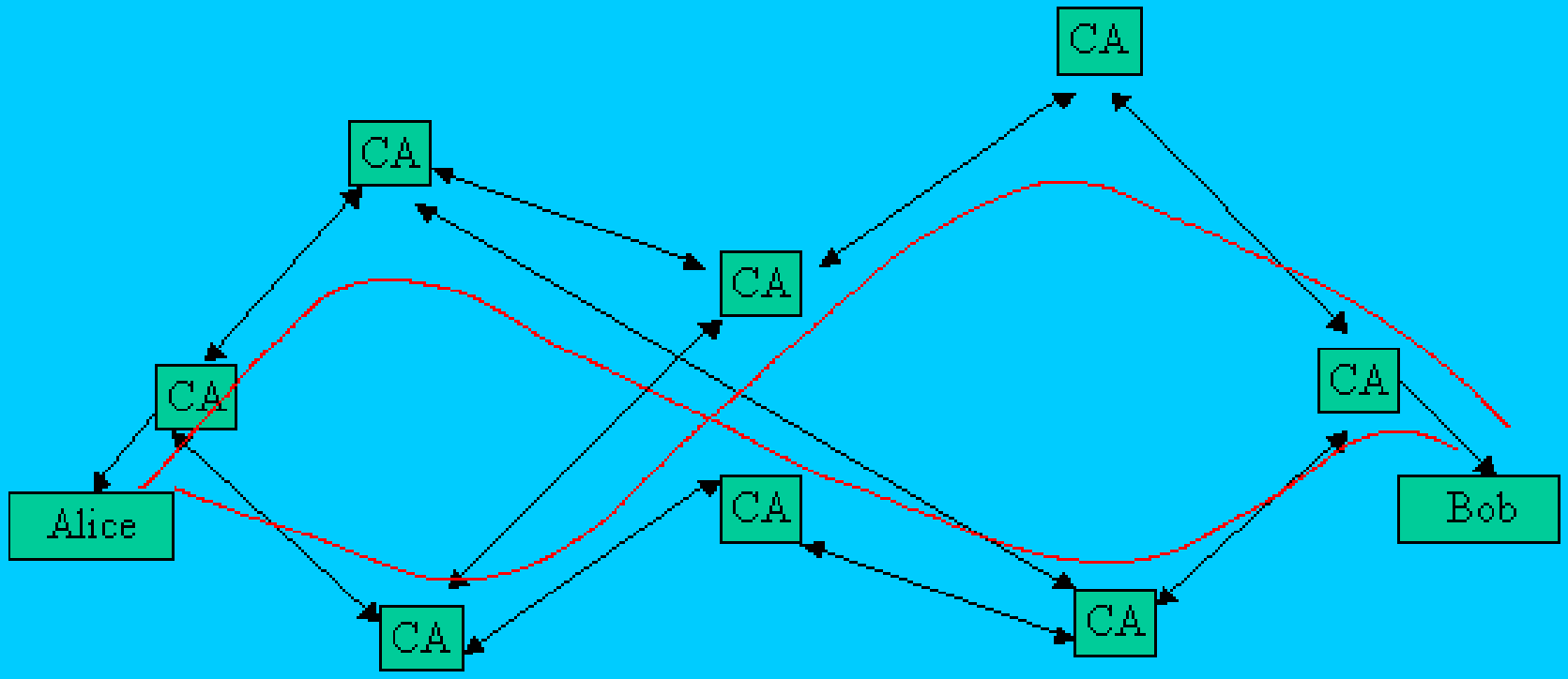
- 网状交叉认证: N个CA，需要C^2_N个交叉认证





- 桥式交叉认证: N个CA，需要N个交叉认证

信任模型一 Mesh CA



信任模型－网状结构

- 为建立一组信任关系，对等交叉认证关系中的每个参与者与其他对等方进行交叉认证，通过允许证书路径经过多个CA而创建一种建立长证书链的通用机制。
- 为确定使用何种信任关系，需要对许多可选路径进行计算
- 既然跨越大量中介CA的信任关系不可取，就要选择两端点间的最优路径。（在一条较长路径上执行的安全策略也可能提供较高的保证水准）
- 我们要寻找满足证书用户策略限制的最短路径

信任模型—用户为中心

- 用户自己决定信赖关系
- PGP是典型，是现实中信任关系的反应
- 浏览器模式

信任模型－ Hybrid CA