信息安全导论

第四讲 公开密钥基础设施

PKI（Public key infrastructure）

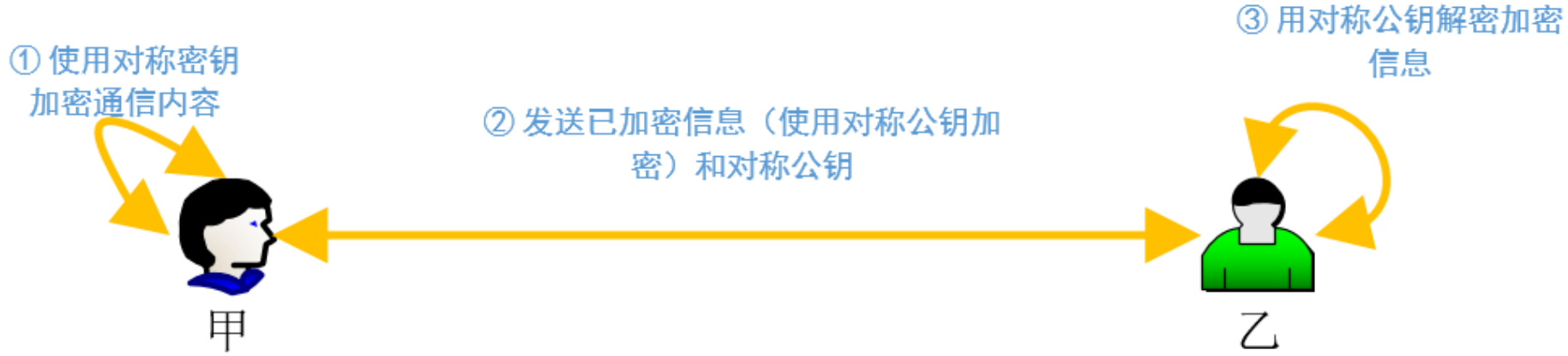
第四讲 PKI技术>主要内容

1. PKI的产生
2. PKI的概念
3. PKI的体系结构
4. PKI的组成
5. 信任模型

甲想将一份合同文件通过Internet发给远在国外的乙，此合同文件对双方非常重要，不能有丝毫差错，而且此文件绝对不能被其他人得知其内容。如何才能实现这个合同的安全发送？

问题1: 最自然的想法是，甲必须对文件加密才能保证不被其他人查看其内容，那么， 到底应该用什么加密技术，才能使合同传送既安全又快速呢?

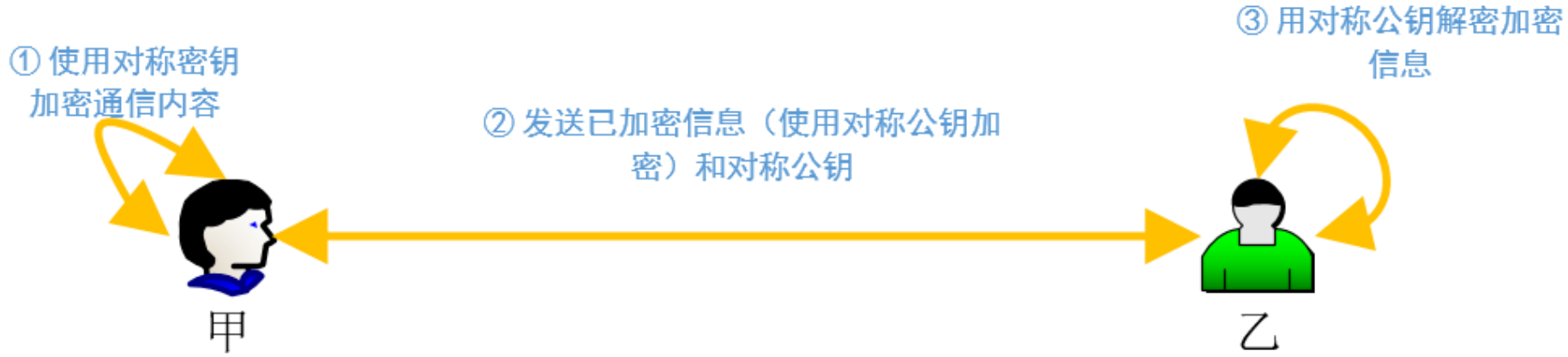
对称加密



甲想将一份合同文件通过Internet发给远在国外的乙，此合同文件对双方非常重要，不能有丝毫差错，而且此文件绝对不能被其他人得知其内容。如何才能实现这个合同的安全发送？

问题2：如果黑客截获此文件，是否用同一算法就可以解密此文件呢?

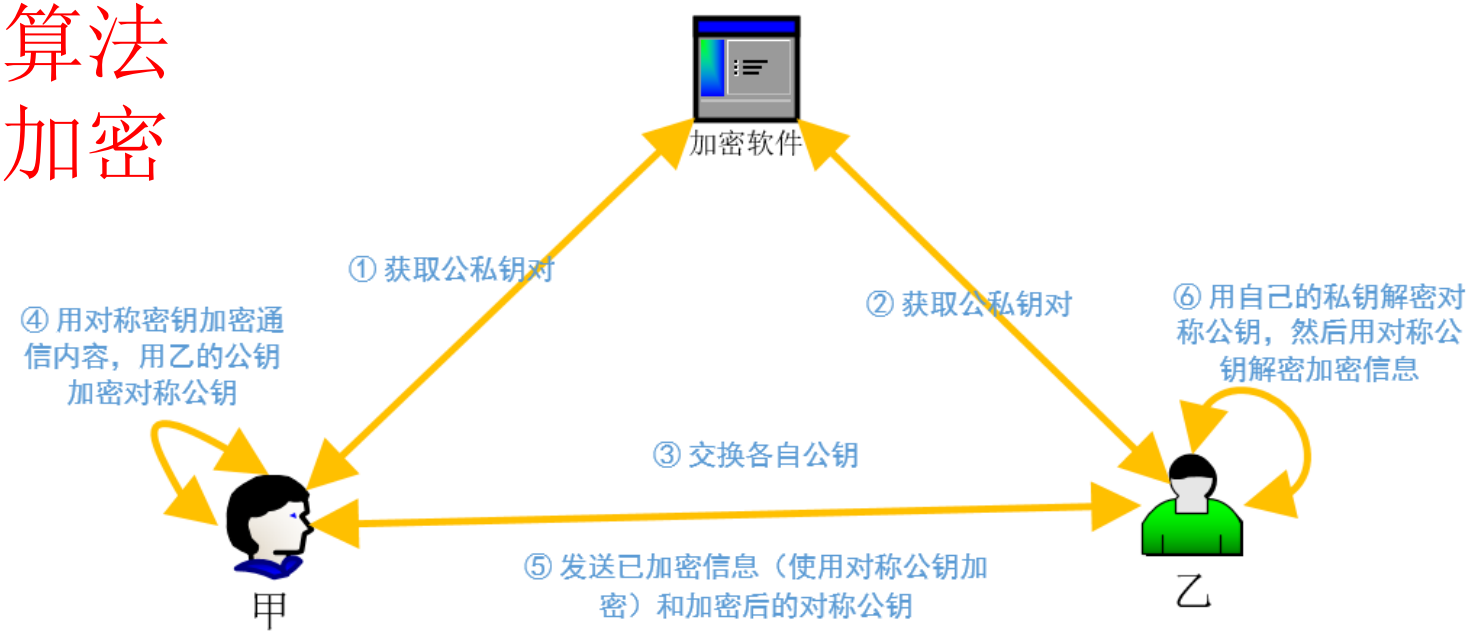
不可以，因为不知道对称密钥



甲想将一份合同文件通过Internet发给远在国外的乙，此合同文件对双方非常重要，不能有丝毫差错，而且此文件绝对不能被其他人得知其内容。如何才能实现这个合同的安全发送？

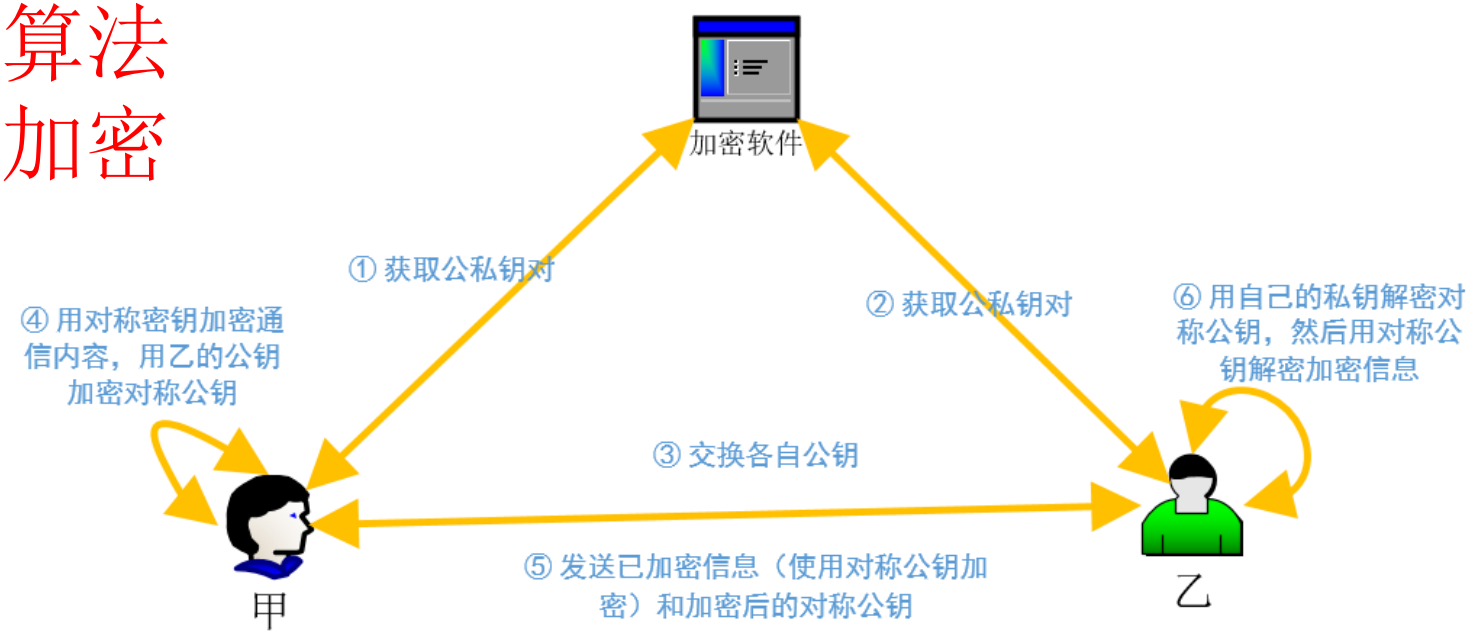
问题3：既然黑客不知密钥，那么乙怎样才能安全地得到其密钥呢？用电话通知，电话可能被窃听，通过Internet发此密钥给乙，可能被黑客截获，怎么办?

非对称加密算法对对称密钥加密后传输



甲想将一份合同文件通过Internet发给远在国外的乙，此合同文件对双方非常重要，不能有丝毫差错，而且此文件绝对不能被其他人得知其内容。如何才能实现这个合同的安全发送？

非对称加密算法对对称密钥加密后传输



甲想将一份合同文件通过Internet发给远在国外的乙，此合同文件对双方非常重要，不能有丝毫差错，而且此文件绝对不能被其他人得知其内容。如何才能实现这个合同的安全发送？

问题4：既然甲可以用乙的公钥加密其对称密钥，为什么不直接用乙的公钥加密其文件呢？这样不仅简单，而且省去了用对称加密算法加密文件的步骤？

不可以这么做。因为非对称密码算法有两个缺点:

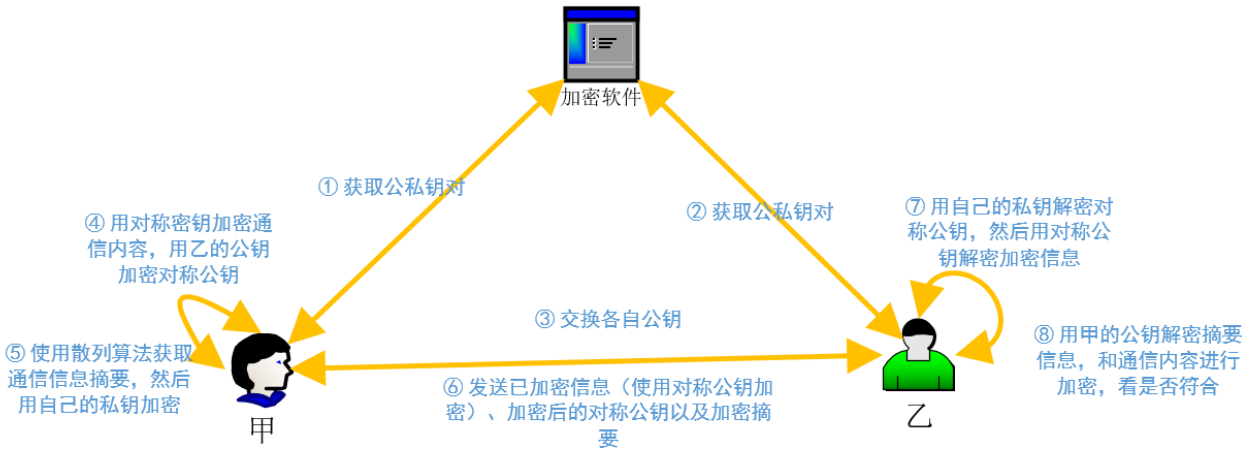
- 加密速度慢，比对称加密算法慢10～100倍，因此只可用其加密小数据（如对称密钥）
- 另外加密后会导致得到的密文变长。

现在一般指通信大都是指通过https协议进行网络通信，在 HTTPS 的场景中只有服务端保存了私钥，一对公私钥只能实现单向的加解密，所以HTTPS 中内容传输加密采取的是对称加密，而不是非对称加密。

甲想将一份合同文件通过Internet发给远在国外的乙，此合同文件对双方非常重要，不能有丝毫差错，而且此文件绝对不能被其他人得知其内容。如何才能实现这个合同的安全发送？

问题5：如果黑客截获到密文，同样也截获到用公钥加密的对称密钥，由于黑客无乙的私钥，因此他解不开对称密钥，但如果他用对称加密算法加密一份假文件，并用乙的公钥加密一份假文件的对称密钥，并发给乙，乙会以为收到的是甲发送的文件，会用其私钥解密假文件，并很高兴地阅读其内容，但却不知已经被替换。换句话说，乙并不知道这不是甲发给他的，怎么办?

数字签名证明其身份！



甲想将一份合同文件通过Internet发给远在国外的乙，此合同文件对双方非常重要，不能有丝毫差错，而且此文件绝对不能被其他人得知其内容。如何才能实现这个合同的安全发送？

问题6：通过对称加密算法加密其文件，再通过非对称算法加密其对称密钥，又通过散列算法证明其发送者身份和其信息的正确性，这样是否就万无一失了?

回答是否定的。问题在于乙并不能肯定他所用的所谓甲的公钥一定是甲的，解决办法是用**数字证书**来绑定公钥和公钥所属人。

PKI技术

- **PKI：Public Key Infrastructure，公钥基础设施**
- **PKI是一种遵循标准的、利用公钥加密技术的一套安全基础平台的技术和规范。**

PKI体系结构

- 简单的说，**PKI是基于公钥密码技术，支持公钥管理，提供真实性、保密性、完整性以及可追究性安全服务，具有普适性的安全基础设施**。
- PKI的核心技术围绕建立在公钥密码算法之上的数字证书的申请、颁发、使用与撤销等整个生命周期进行展开，**主要目的就是用来安全、便捷、高效地分发公钥**，为用户建立一个安全的网络环境，保证网络上信息的安全传输。

PKI应用系统的组成

- IETF的PKI小组制订了一系列的协议，定义了**基于X.509证书的PKI模型框架，称为PKIX**。PKIX系列协议定义了证书在Internet上的使用方式，包括证书的生成、发布、获取，各种密钥产生和分发的机制，以及实现这些协议的轮廓结构。
- 狭义的PKI一般指PKIX。
- 一个完整的PKI应用系统必须具有权威认证机构(CA，Certificate Authority)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口(API)等基本构成部分，如图3-9所示。
- 构建PKI也将围绕着这五大关键元素来着手构建。

PKI应用系统的组成

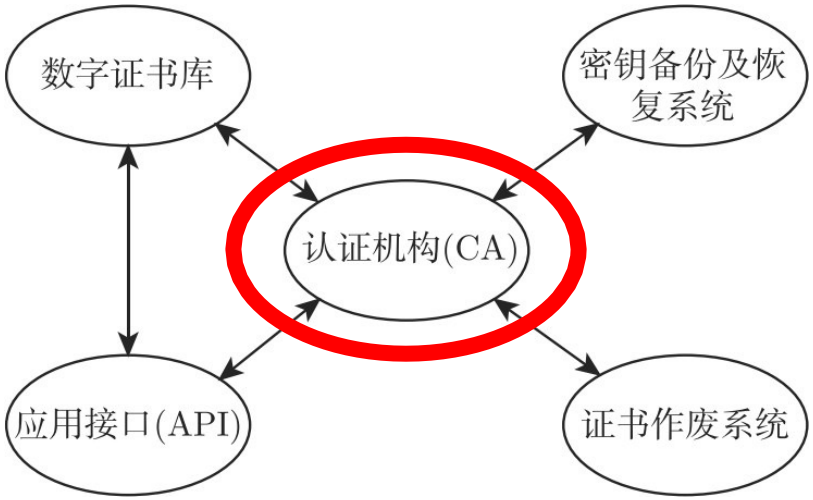


图3-9 PKI体系结构

- **认证机构(CA)**：CA是PKI的核心执行机构，　是PKI的主要组成部分，人们通常称它为**认证中心**。
- CA是数字证书生成、发放的运行实体，在一般情况下也是证书撤销列表(CRL)的发布点，在其上常常运行着一个或多个注册机构(RA)。
- CA必须具备权威性的特征。

PKI应用系统的组成

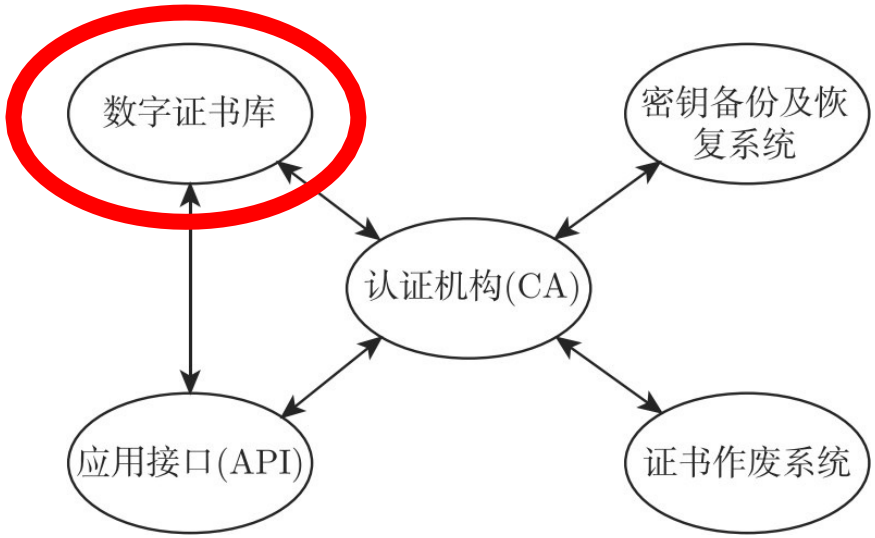


图3-9 PKI体系结构

- **数字证书库：证书库是CA颁发证书和撤销证书的集中存放地，可供公众进行开放式查询。**一般来说，查询的目的有两个：

① 其一是想得到与之通信实体的公钥；

② 其二是要验证通信对方的证书是否已进入“黑名单”。

- 证书库还提供了存取证书撤销列表(CRL)的方法。
- 目前广泛使用的是X.509证书。

PKI应用系统的组成

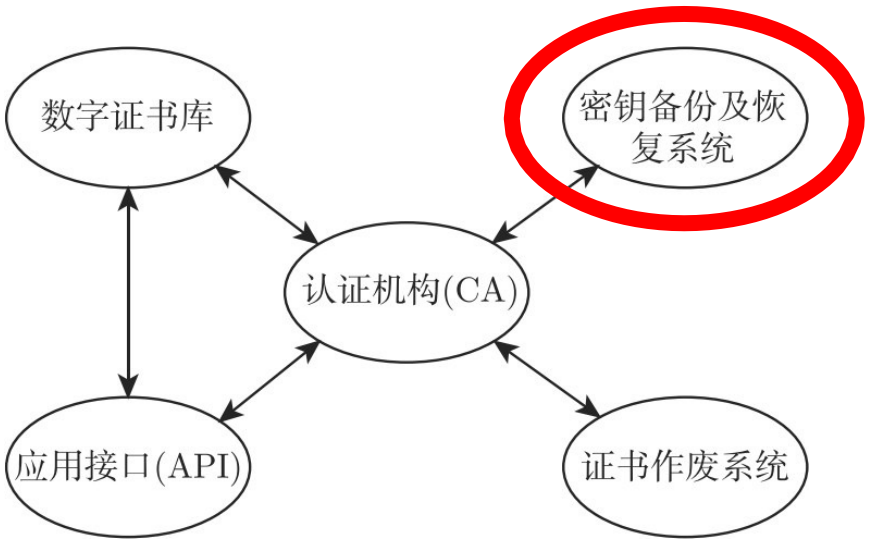


图3-9 PKI体系结构

- **密钥备份及恢复系统**：如果用户丢失了用于解密数据的密钥，则数据将无法被解密，这将造成合法数据丢失。
- 为避免这种情况， PKI提供备份与恢复密钥的机制。但是密钥的备份与恢复必须由可信的机构来完成。
- 密钥备份与恢复**只能针对解密密钥，签名私钥为确保其唯一性而不能够作备份**。

PKI应用系统的组成

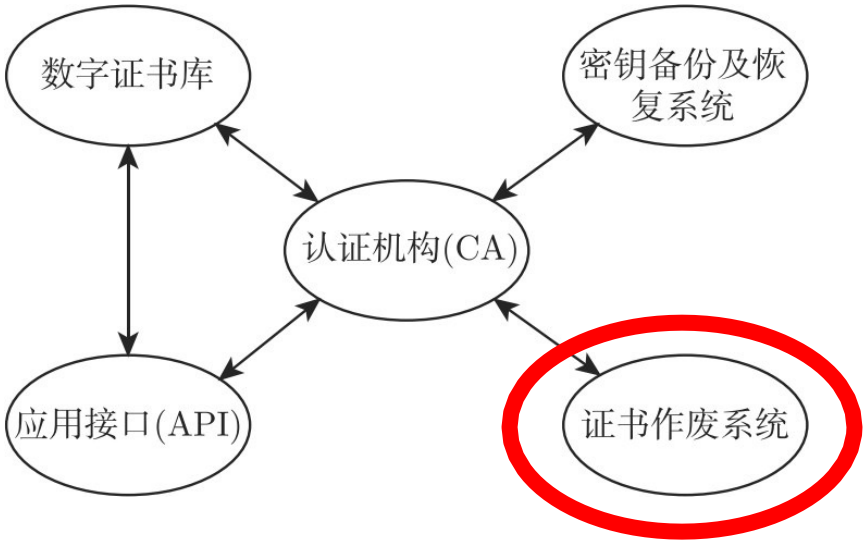


图3-9 PKI体系结构

- **证书作废系统**：证书作废处理系统是PKI的一个必备的组件。证书有效期以内也可能需要作废，原因可能是密钥介质丢失或用户身份变更等。在PKI体系中，**作废证书一般通过将证书列入作废证书表(CRL)来完成**。
- 通常，系统中由CA负责创建并维护一张及时更新的CRL，而由用户在验证证书时负责检查该证书是否在CRL之列。

PKI应用系统的组成

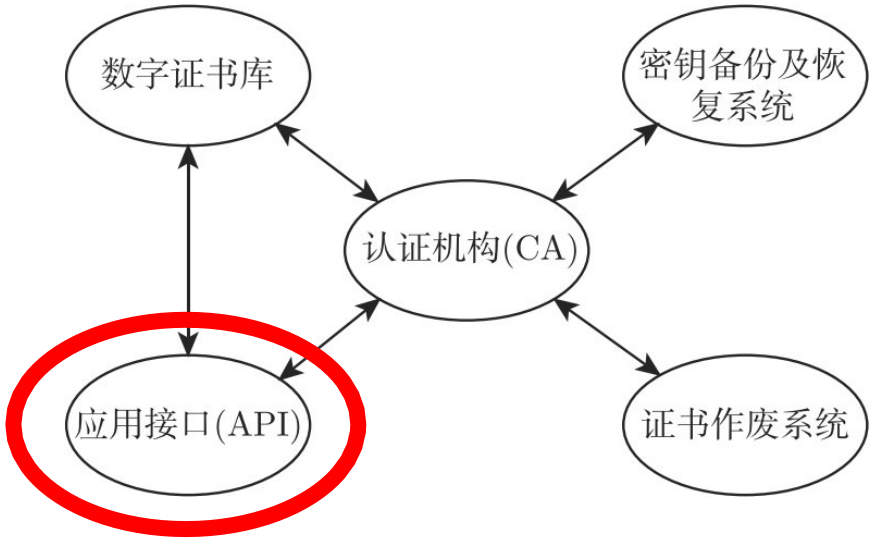


图3-9 PKI体系结构

- 应用接口(API)
- PKI的价值在于使用户能够方便地使用加密、数字签名等安全服务，因此，一个完整的PKI必须提供良好的应用接口系统，使得各种各样的应用能够以安全、一致、可信的方式与PKI交互，确保安全网络环境的完整性和易用性。

数字证书

公钥加密系统使我们能知道和谁在通信，但这个的前提是：**要知道（有）对方的公钥**。

那么，如果**对方不知道我的公钥怎么办**？ 这就轮到证书出场了。

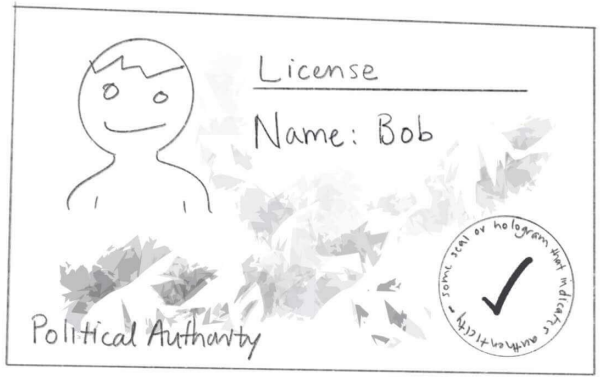
想一下，我们需求其实非常简单：

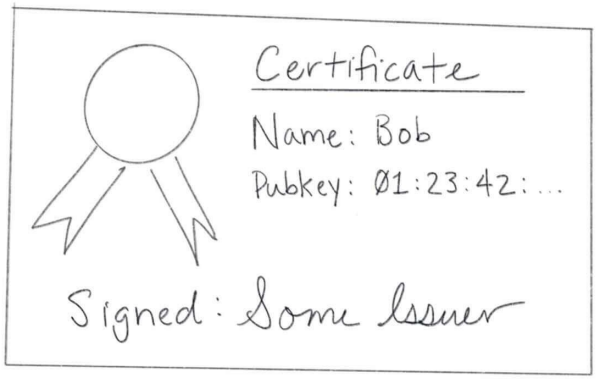
- 首先要将**公钥和它的 owner** 信息发给对方；
- 但光有这个信息还不行，**还要让对方相信这些信息**；
- 证书就是用来解决这个问题的，解决方式是**请一个双方都信任的权威机构** 对以上信息作出证明（签名）。

证书不过是一个将名字关联到公钥（bind names to public keys）的东西。

数字证书

计算机用**证书做类似驾照的事情**：如果之前从未和其他电脑通信，但信任 一些证书权威，那可以用证书来认证：
- 首先验证证书是合法的（用证书签发者的公钥检查签名等），
- 然后提取证书中的（subscriber 的）公钥和名字，
- 然后用 subscriber 的公钥，通过网络验证该 subscriber 的签名；
- 查看名字是否正确等等。





Issued by	DMV (Political Authority)	Certificate Authority
Verified by	Checking holograms & stuff	Checking signature & stuff
Trusted b/c	Trust DMV (lol)	Trust CA
Used to	Authenticate person / figure out name using picture	Authenticate entity / figure out name using public key

数字证书

PKI中广泛使用了X.509证书。一个X.509证书包含以下信息：

(1)版本号(Version)：

区分合法证书的不同版本。目前定义了三个版本，版本1的编号为0，版本2的编号为1，版本3的编号为2。

(2)序列号(Serial number)：

一个整数，和签发该证书的CA名称一起惟一标识该证书。

(3)签名算法标识(Signature algorithm identifier)

指定证书中计算签名的算法，包括一个用来识别算法的子域和算法的可选参数。

数字证书

PKI中广泛使用了X.509证书。一个X.509证书包含以下信息：

(1)版本号(Version)：

区分合法证书的不同版本。目前定义了三个版本，版本1的编号为0，版本2的编号为1，版本3的编号为2。

(2)序列号(Serial number)：

一个整数，和签发该证书的CA名称一起惟一标识该证书。

(3)签名算法标识(Signature algorithm identifier)

指定证书中计算签名的算法，包括一个用来识别算法的子域和算法的可选参数。

X.509数字证书

(4)签发者(Issuer name):

创建、签名该证书的CA的X.500格式名字。

(5)有效期(Period of validity):

包含两个日期，即证书的生效日期和终止日期。

(6)证书主体名(Subject name):

持有证书的主体的X.500格式名字，证明此主体是公钥的所有者。

(7)证书主体的公钥信息(Subject's public-key information):

主体的公钥以及将被使用的算法标识，带有相关的参数。

X.509数字证书

(8)签发者惟一标识(Issuer unique identifier):

版本2和版本3中可选的域，用于惟一标识认证中心CA。

(9)证书主体惟一标识(Subject unique identifier):

版本2和版本3中可选的域，用于惟一标识证书主体。

(10)扩展(Extensions):

仅仅出现在版本3中，一个或多个扩展域集。

(11)签名(Signature):

覆盖证书的所有其他域，以及其他域被CA私钥加密后的散列代码，以及签名算法标识。

- CA用它的私钥对证书签名，如果用户知道相应的公钥，则用户可以验证CA签名证书的合法性。

CA证书原理：

数字证书采用公钥体制；

私钥签名

是对版本号、序列号、有效期、用户公钥等所有证书信息进行hash，用CA私钥对hash值签名，放在证书的最后一段

从算法上讲，最重要的是CA私钥对用户公钥进行签名（实际上签了整个X.509除签名外的所有信息），所以课本及其他网上案例常把取得证书中的用户公钥称为：“认证（验证）得到用户公钥”

CA公钥公开，验证签名，确认证书合法性

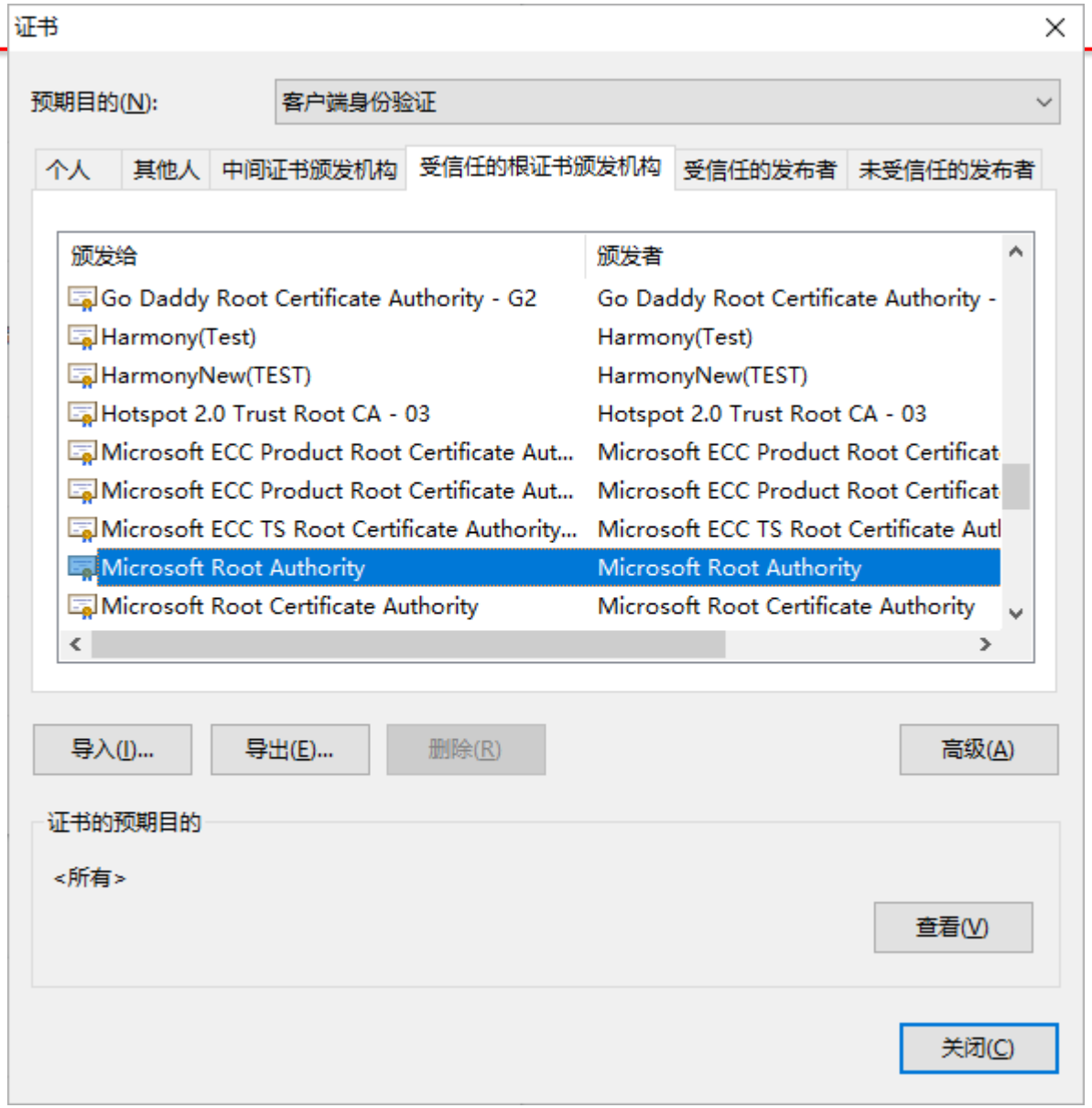
X.509证书格式：

- 版本号
- 序列号
  - 在CA内部唯一
- 签名算法标识符
  - 指该证书中的签名算法
- 证书发行机构名称
  - CA的名字
- 证书有效期
- 证书拥有者名称 X.500格式
- 证书拥有者的公钥信息
  - 算法
  - 参数
- 证书颁发者对证书的签名

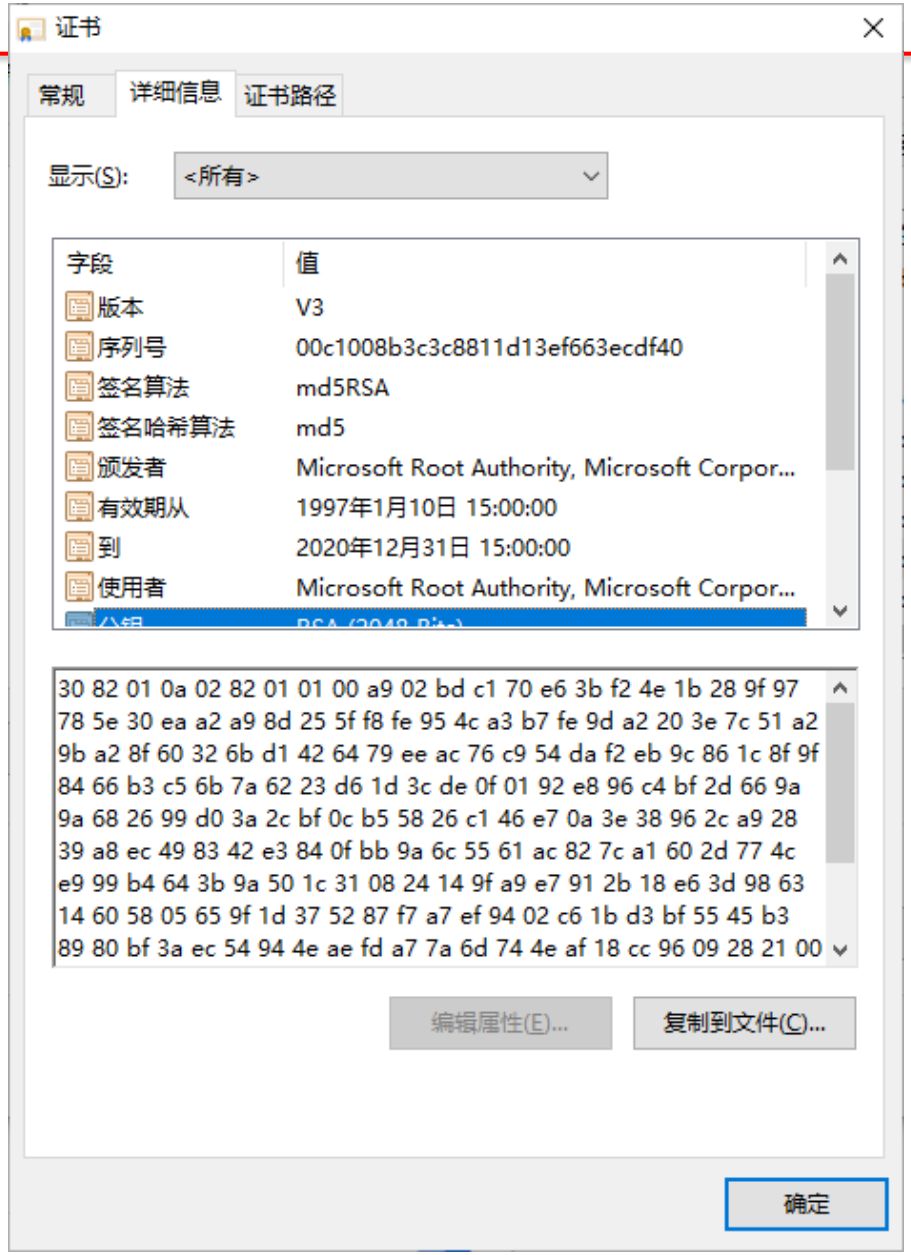
X.509 数字证书的结构

Version	version 1	version 2	version 3
Serial Number			
Signature Algorithm Identifier			
Issuer Name			
Validity Period			
Subject Name			
Subject Public Key Information			
Issuer Unique ID			
Subject Unique ID			
Extensions			
Certification Authority's Digital Signature			

Chrome浏览器中的证书



Chrome浏览器中的证书



3.4.3 认证机构

- PKI系统的关键是实现对公钥密码体制中公钥的管理。认证机构CA便是一个能够提供相关证明的机构。CA是基于PKI进行网上安全活动的关键，主要负责产生、分配并管理参与活动的所有实体所需的数字证书，其 功能类似于办理身份证、护照等证件的权威发证机关。CA必须是各行业、各部门及公众共同信任并认可的、权威的、不参与交易的第三方网上身份认证机构。
- 在PKI系统中，CA管理公钥的整个生命周期，其功能包括签发证书、规定证书的有效期限，同时在证书发布后，还要负责对证书进行撤销、更新和归档等操作。从证书管理的角度，每一个CA的功能都是有限的，需要按照上级CA的策略，负责具体的用户公钥的签发、生成和发布，以及CRL的生成和发布等职能。

CA的主要职能

① 制定并发布本地CA策略。但本地策略只是对上级CA策略的补充，而不能违背。

② 对下属各成员进行身份认证和鉴别。

③ 发布本CA的证书，或者代替上级CA发布证书。

④ 产生和管理下属成员的证书。

⑤ 证实RA的证书申请，返回证书制作的确认信息，或返回已制作的证书。

⑥ 接收和认证对所签发证书的撤销申请。

⑦ 产生和发布所签发证书和CRL。

⑧ 保存证书、CRL信息、审计信息和所制定的策略。

典型CA的构成

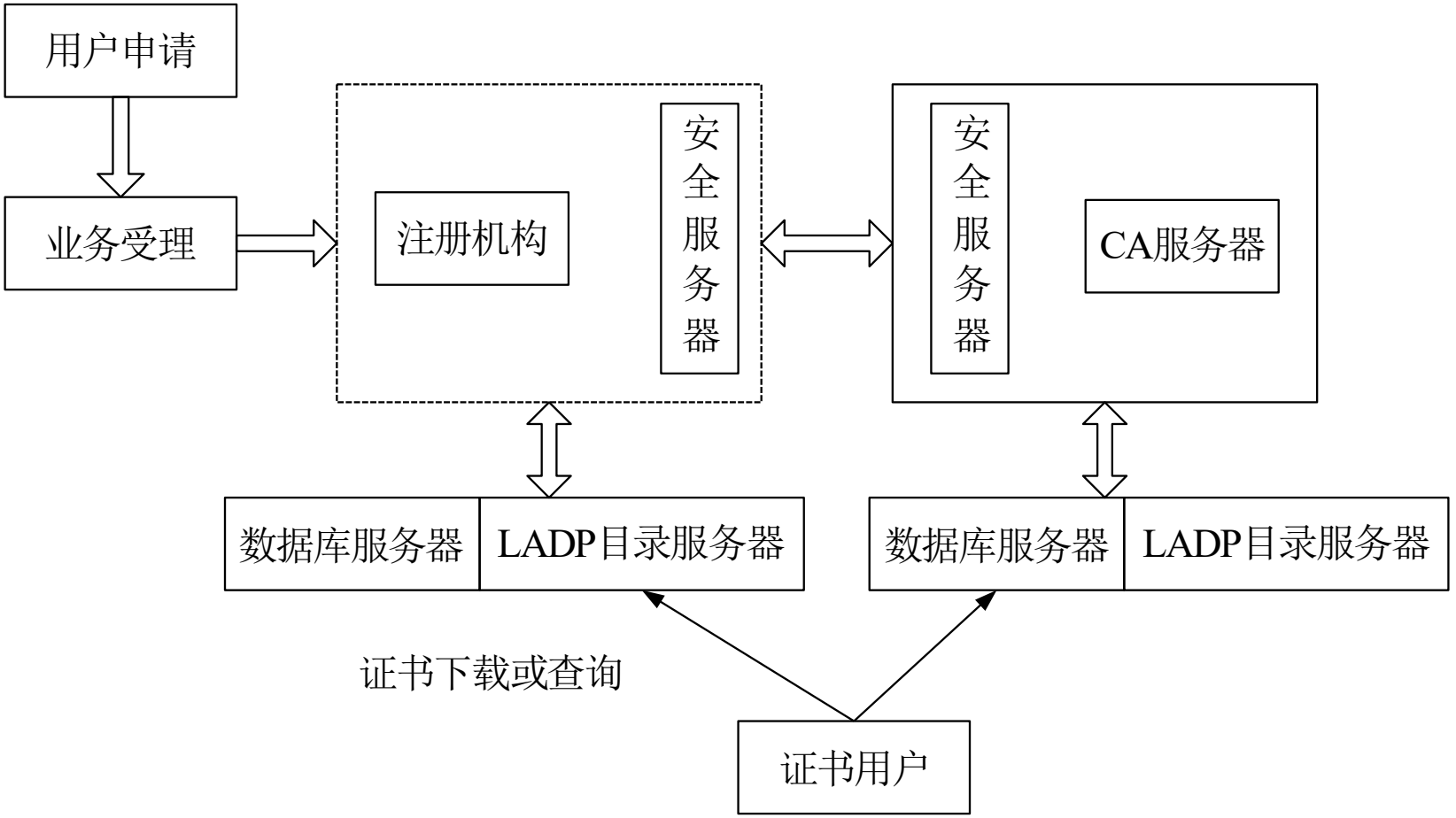


图3-10 典型CA的构成

3.4.4 PKIX相关协议

1) PKIX基础协议

- PKIX的基础协议以RFC2459和RFC3280为核心，定义了X.509 v3公钥证书和X.509 v2 CRL的格式、数据结构和操作等，用以保证PKI基本功能的实现。
- 此外，PKIX还在RFC2528、RFC3039、RFC3279等的基础上定义了基于X.509 v3的相关算法和格式等，以加强X.509 v3公钥证书和X.509 v2 CRL在各应用系统之间的通用性。

2) PKIX管理协议

- PKIX体系中定义了一系列的操作，它们是在管理协议的支持下进行工作的。管理协议主要完成以下的任务：

① 用户注册

② 用户初始化

③ 认证

④ 密钥对的备份和恢复

⑤ 自动的密钥对更新

⑥ 证书撤销请求

⑦ 交叉认证

3) PKIX安全服务和权限管理的相关协议

- PKIX中安全服务和权限管理的相关协议主要是进一步完善和扩展PKI安全架构的功能，通过RFC3029、RFC3161、RFC3281等定义。
- 在PKIX 中，**不可抵赖性**通过数字时间戳DTS(digital timestamp)和数据有效性验证服务器DVCS(data validation and certification server)实现。
- 在CA/RA中使用的DTS，是对时间信息的数字签名，主要用于确定在某一时间某个文件确实存在或者确定多个文件的时间上的逻辑关系，是实现不可抵赖性服务的核心。
- DVCS的作用则是验证签名文档、公钥证书或数据存在的有效性，其验证声明称为**数据有效性证书**。DVCS是一个可信第三方，是用来实现不可抵赖性服务的一部分。权限管理通过属性证书来实现。属性证书利用属性和属性值来定义每个证书主体的角色、权限等信息。

3.4.5 PKI信任模型

- 实体A信任B，即A假定实体B严格地按A所期望的那样行动。如果一个实体认为CA能够建立并维持一个准确地对公钥属性的绑定，则它信任该CA。
- 所谓**信任模型，就是提供用户双方相互信任机制的框架**，是PKI系统整个网络结构的基础。
- 信任模型主要明确回答了以下几个问题：
  ① 一个PKI用户能够信任的证书是怎样被确定的?
  ② 这种信任是怎样建立的?
  ③ 在一定的环境下，这种信任如何被控制?

1.层次模型

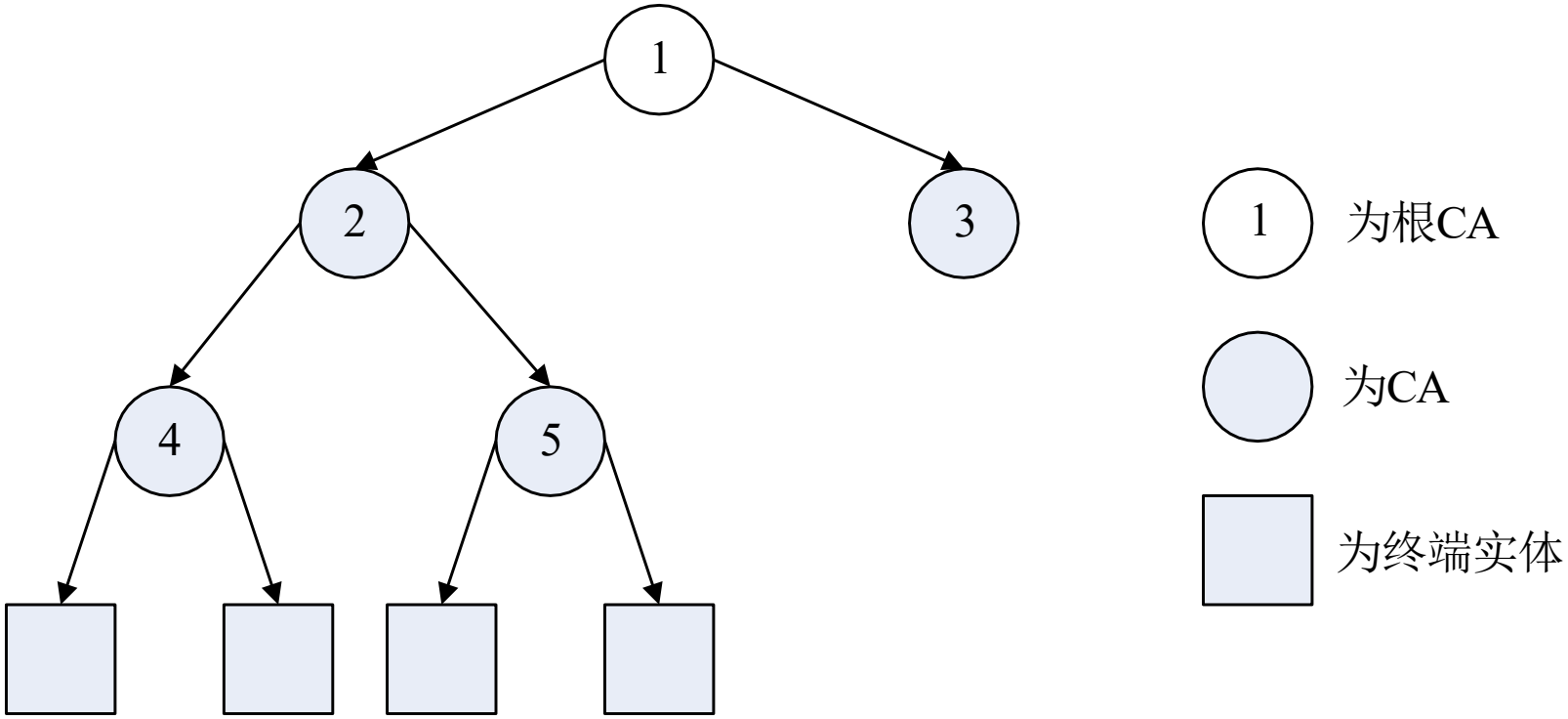


图3-12 层次模型

2.交叉模型

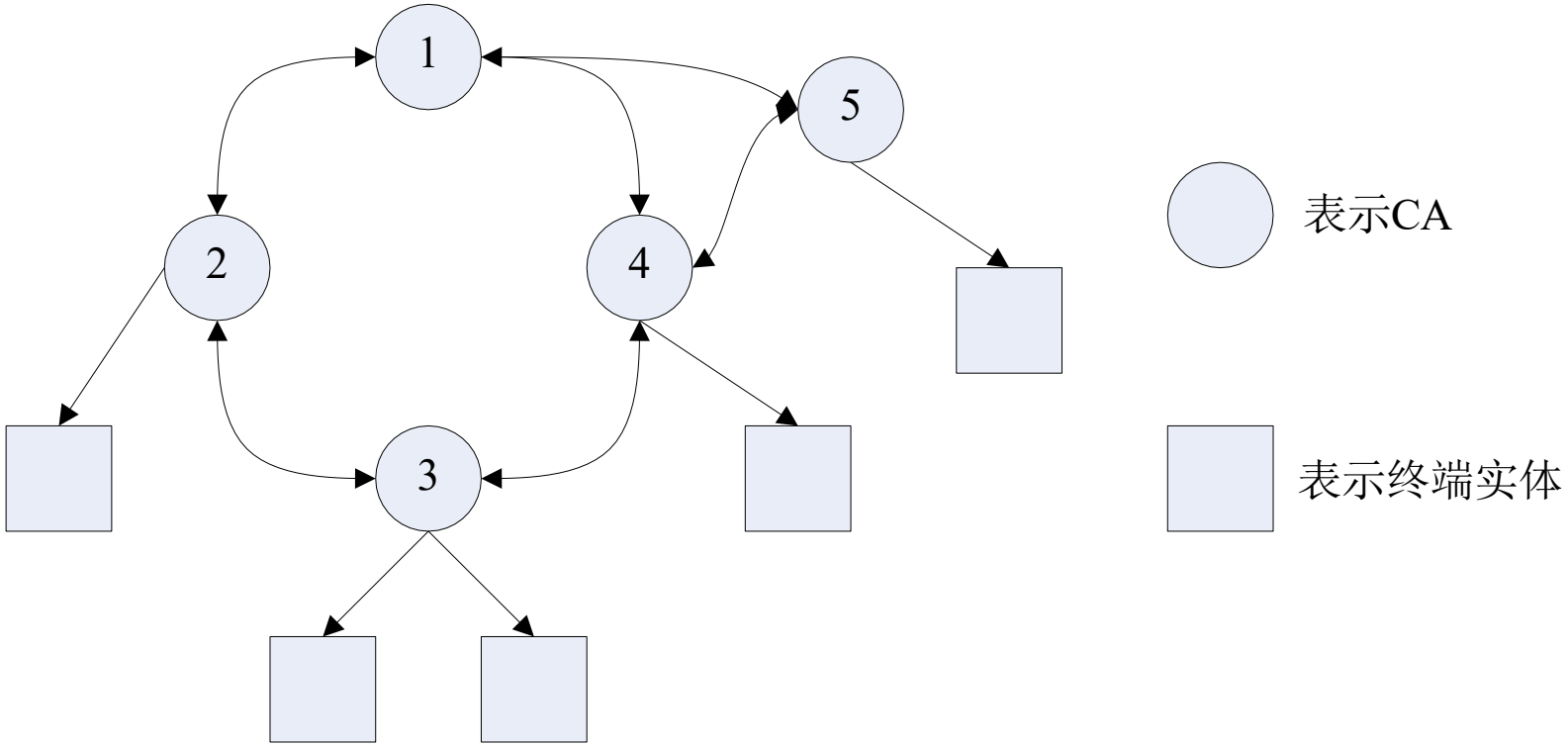


图3-12 交叉模型

3.混合模型

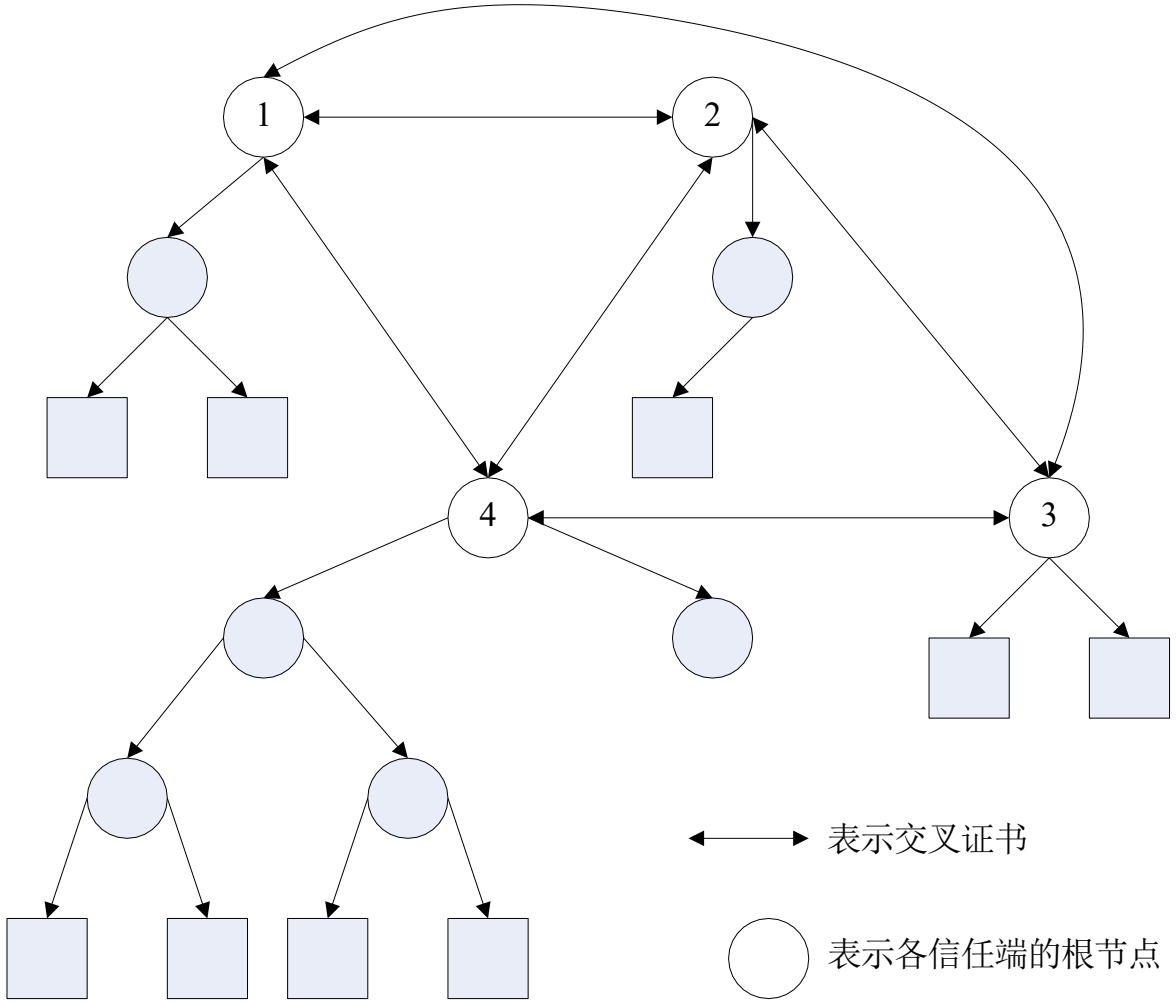


图3-13 混合模型

4.桥CA模型

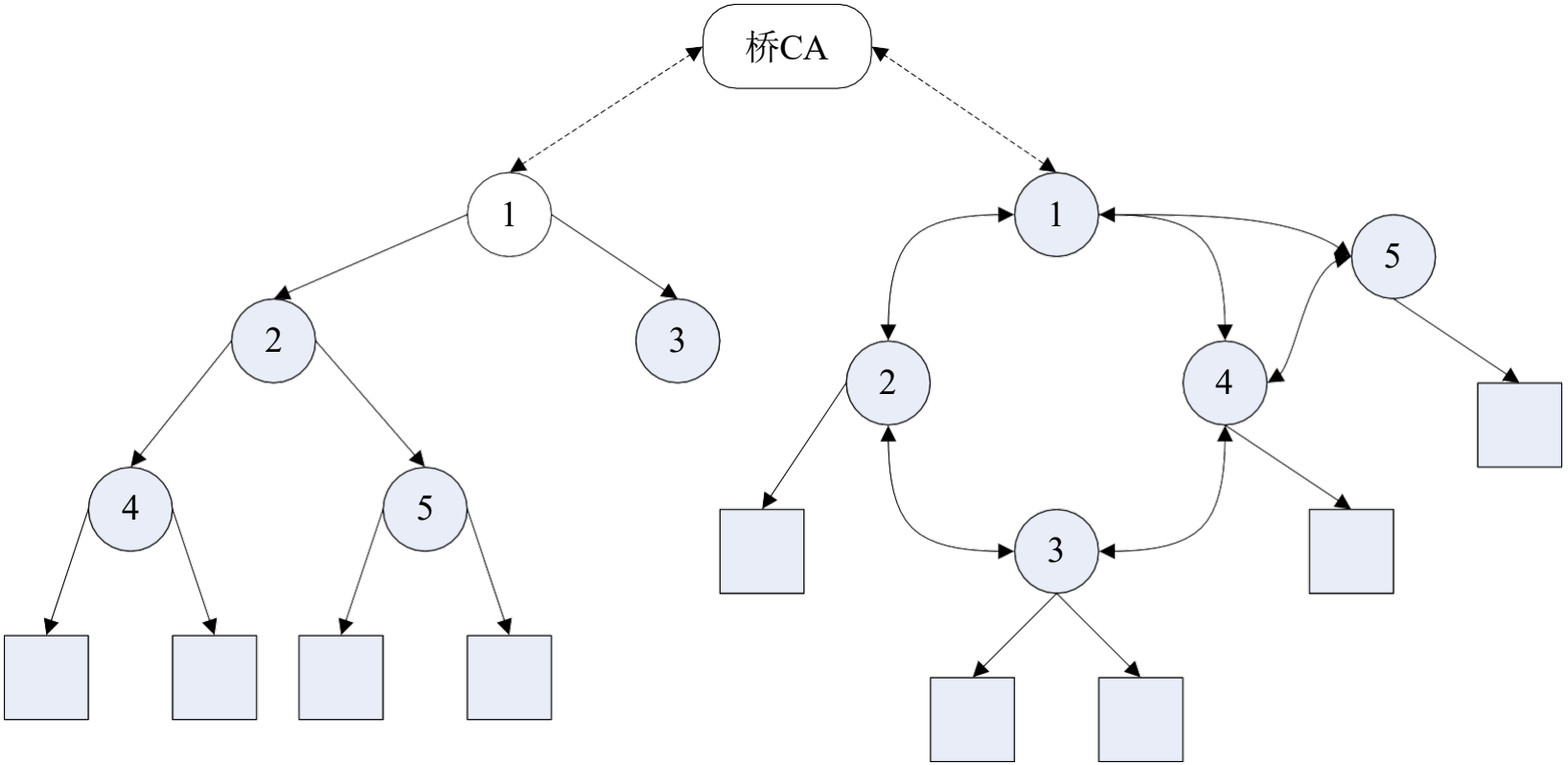


图3-14 桥模型

5.信任链模型

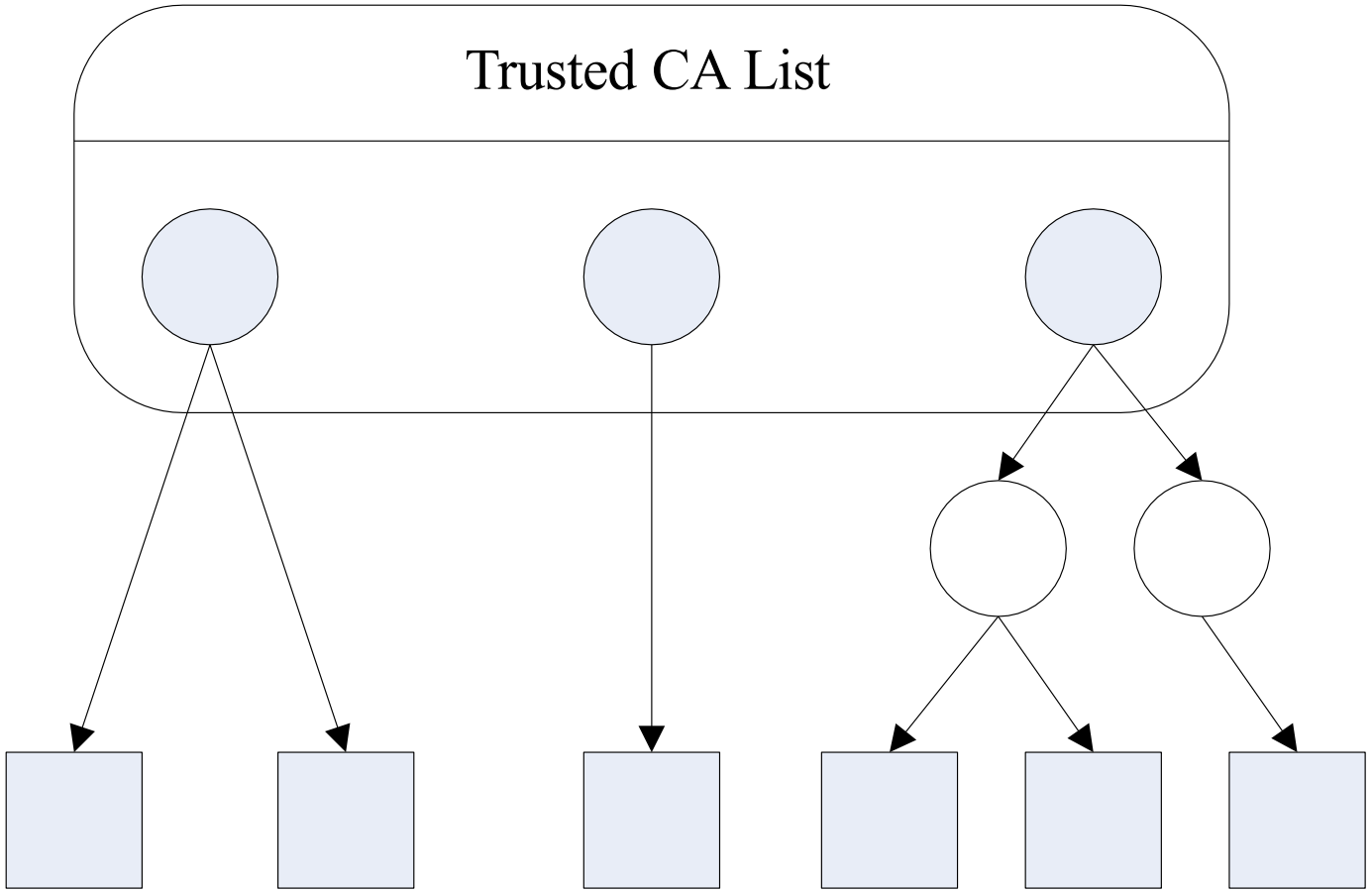


图3-15 信任链模型

1 信任

(1)定义:

实体A认定实体B将严格地按A所期望的那样行动，则A 信任B。（ITU-T推荐标准X.509的定义），称A是信任者，B是被信任者。

(2)信任的特点

时差性;

不确定性;

与风险是相联系性;

动态和非单调性;

信任是决策的重要因素，但不是唯一因素。

（3）信任分类

按有无第三方可信机构参与分：

直接信任、第三方信任。

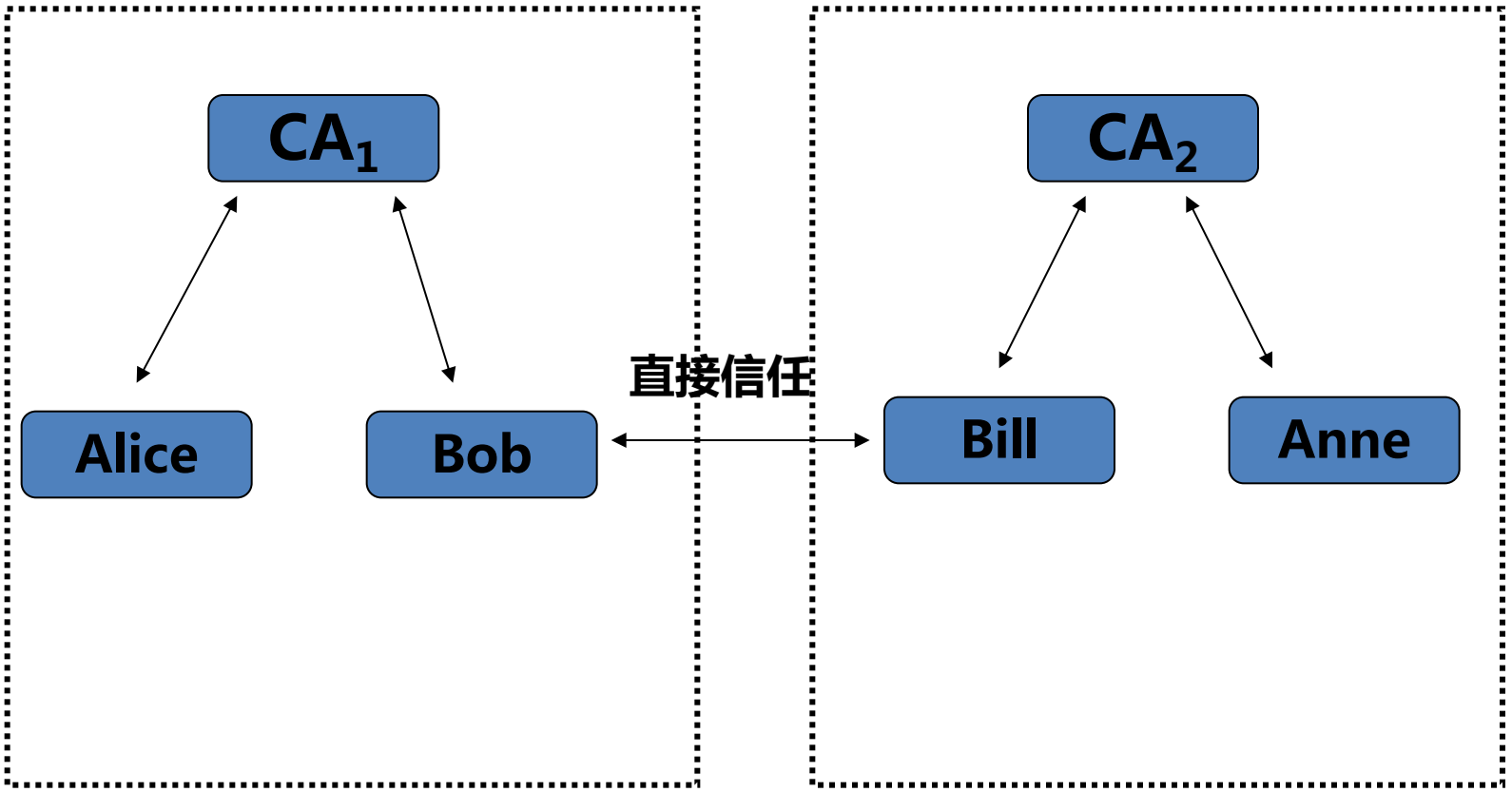
1）直接信任

直接建立信任关系。

最简单的形式。

① 直接信任根CA密钥；

② 不同的CA的实体进行安全通信，两个CA之间不能交叉认证时，这时也需要直接信任。

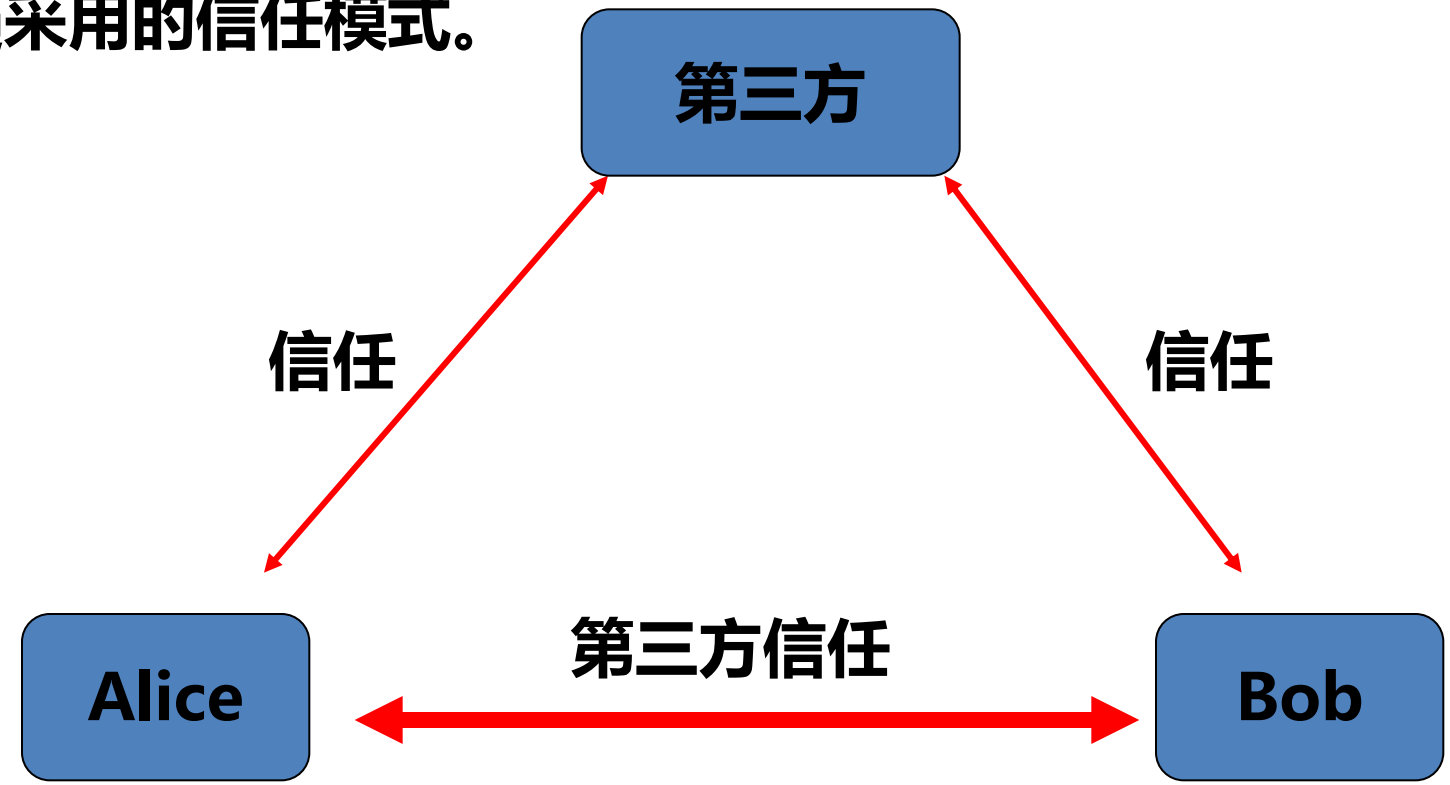

CA1
CA2
直接信任
Alice
Bob
Bill
Anne

2）第三方信任

通过第三方建立的信任关系。

实质是第三方的推荐信任。

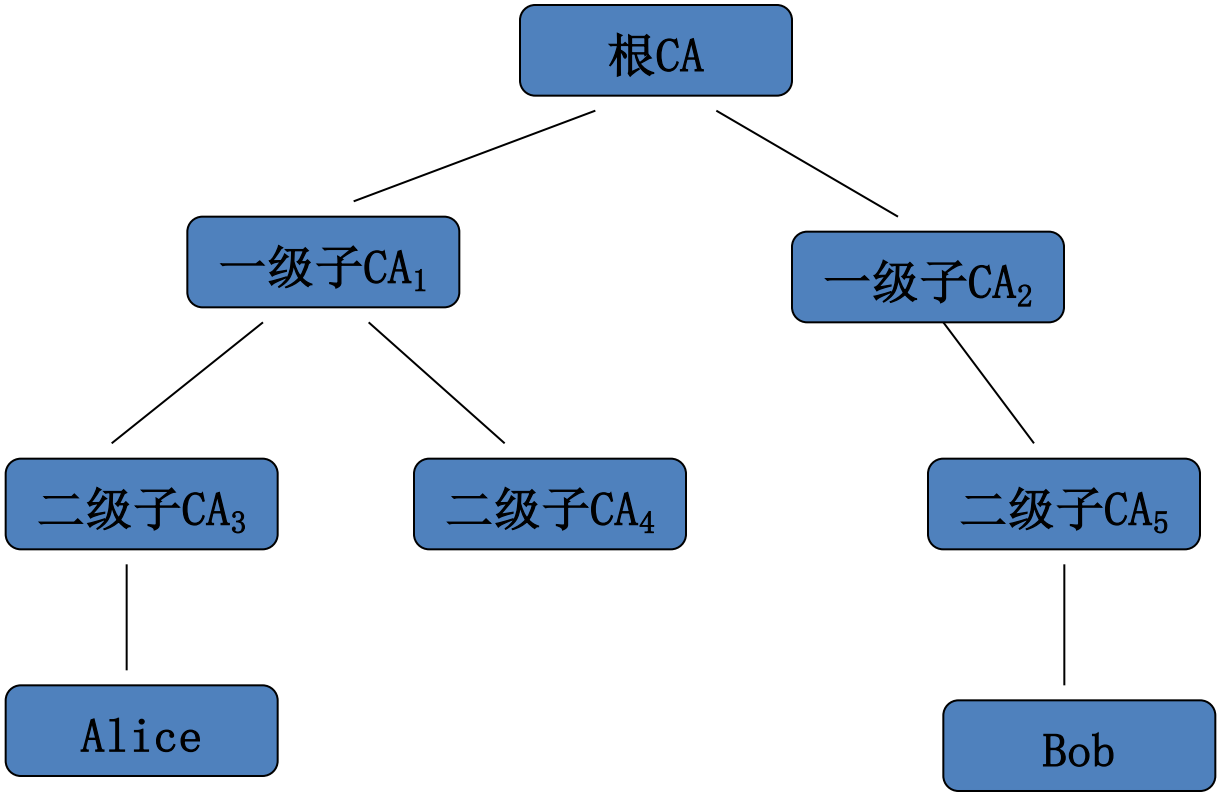
普遍采用的信任模式。



常用的四种信任模型：P91

- 严格层次模型
- 分布式模型
- Web模型
- 用户中心的模型

(1) 严格层次结构模型



这个层次结构按如下规则建立：

1) 根CA认证(创立和签发证书)直接连接在它下面的CA。

2）每个子CA认证直接在它下面的CA

3）倒数第二层的CA认证终端实体。

重要条件：

每个实体都必须拥有根CA的公钥；

每个CA的证书对各层次成员是公开的。

认证（证书检验）过程步骤：

1）Bob用CA的公钥K验证一级子CA_1的公钥K_1；

2）用K_1验证二级子CA_3的公钥K_3 ；

3）用K_3来验证Alice的证书，得到Alice的可信公钥K_A。

4) Alice用类似的方法得到Bob的可信公钥K_B。

Alice和Bob之间可以进行安全通信，

如Alice对发给Bob的消息加密;

验证自称是Bob的数字签名。

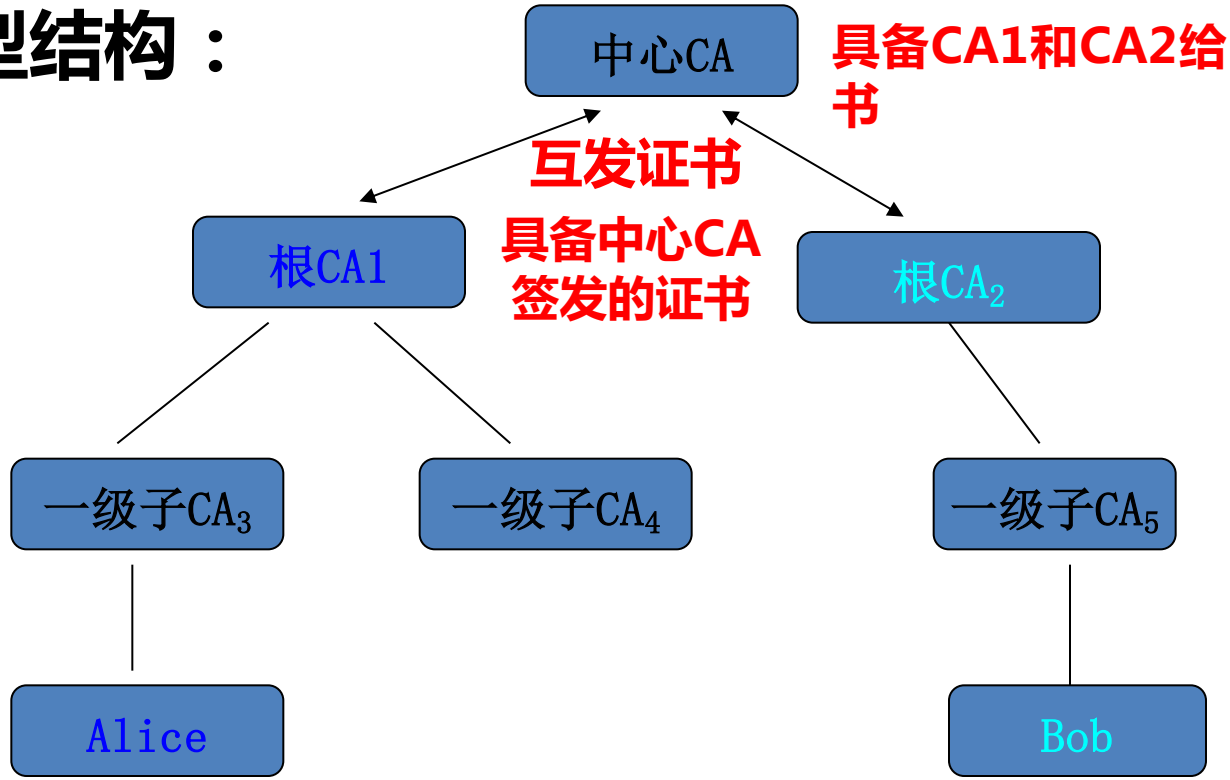
(2) 分布式信任模型

把信任分散到几个CA上。

有2种结构：

星型机构和网状结构。

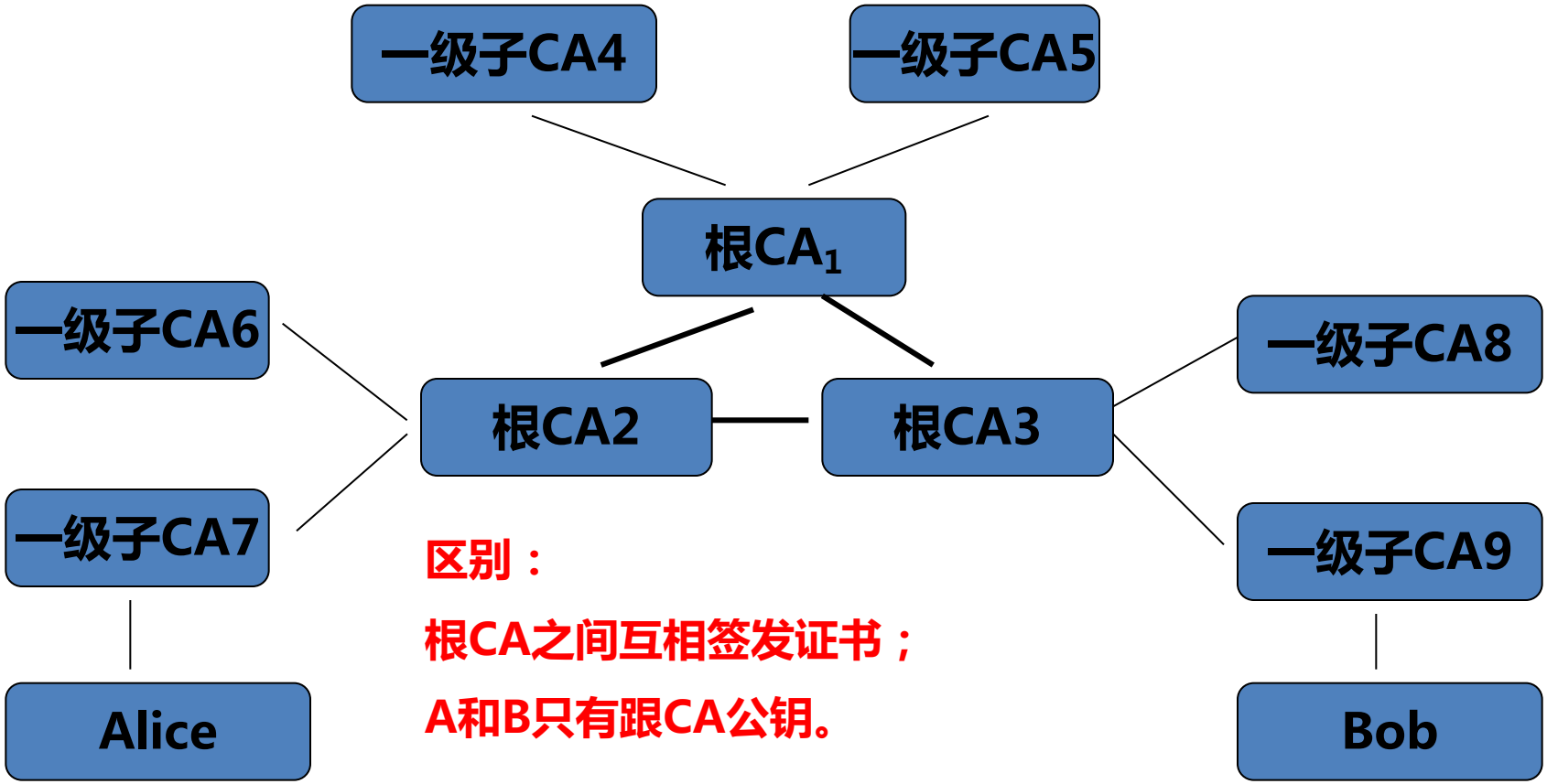
星型结构：



区别：

Alice和Bob没有中心CA公钥，而是他们各自的根公钥

网状结构：


一级子CA4
一级子CA5
根CA1
一级子CA6
根CA2
根CA3
一级子CA8
一级子CA7
一级子CA9
区别：
根CA之间互相签发证书；
A和B只有跟CA公钥。
Alice
Bob

(3) Web信任模型

依赖于浏览器，许多CA的公钥被预装在标准的浏览器上。

P93划线部分

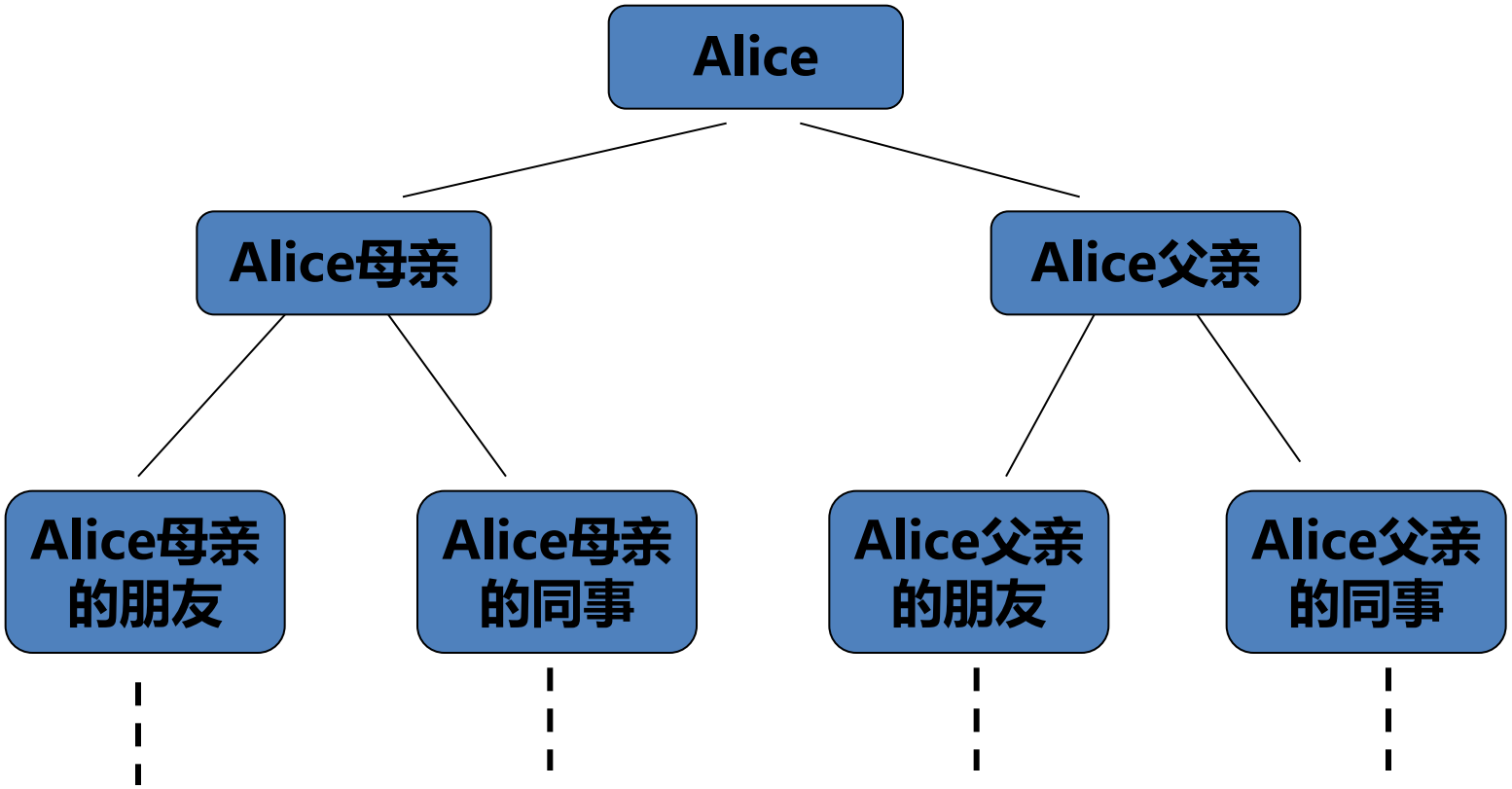
(4) 以用户为中心的信任模型

每个用户自己决定信任哪些证书。

最初信任对象：用户的朋友、家人或同事，但被许多因素所左右。

此模型依赖于用户行为、决策，不适于普通群体。

以用户为中心的信任模型：



（1）问题提出

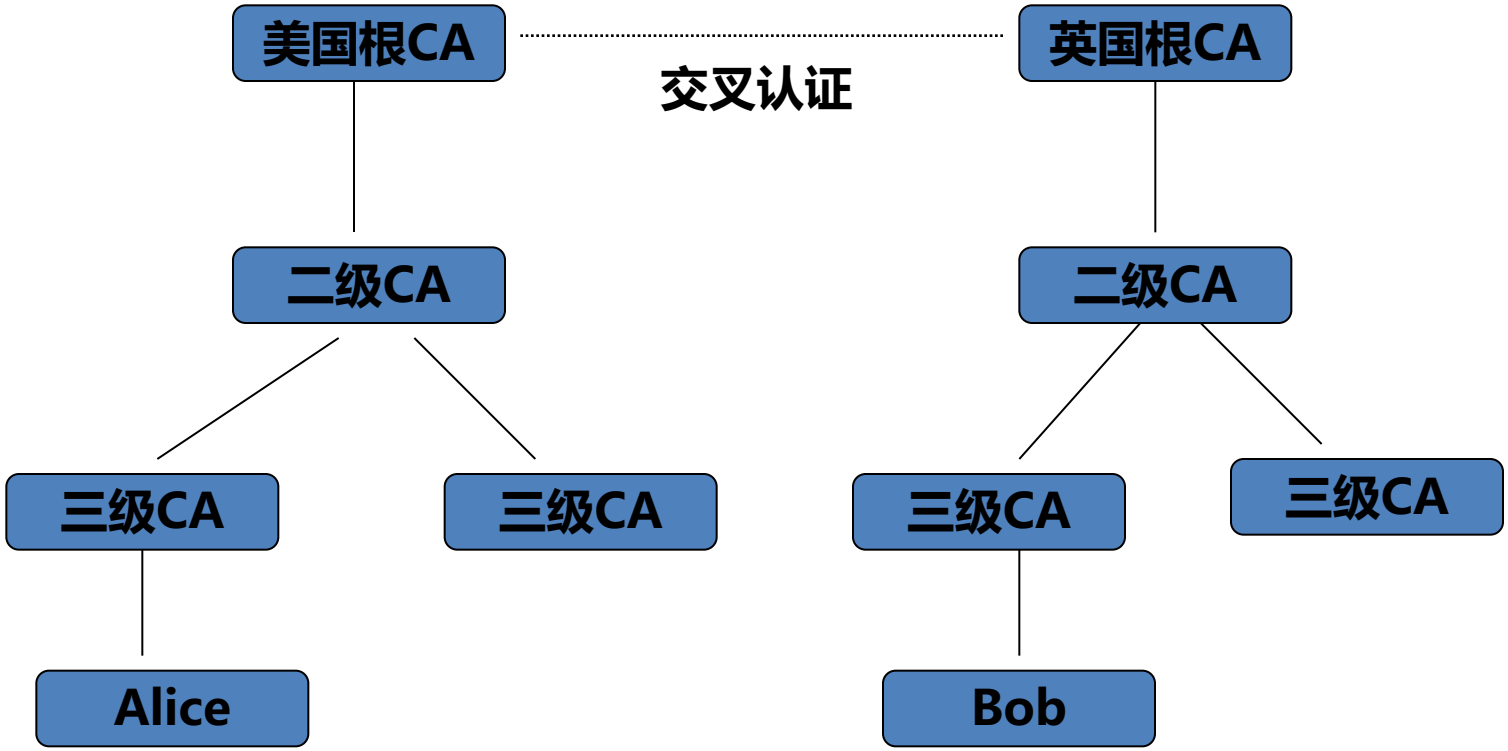
Alice是美国人，有美国CA签发的公钥和证书，

Bob是英国人，有英国CA签发的公钥和证书，

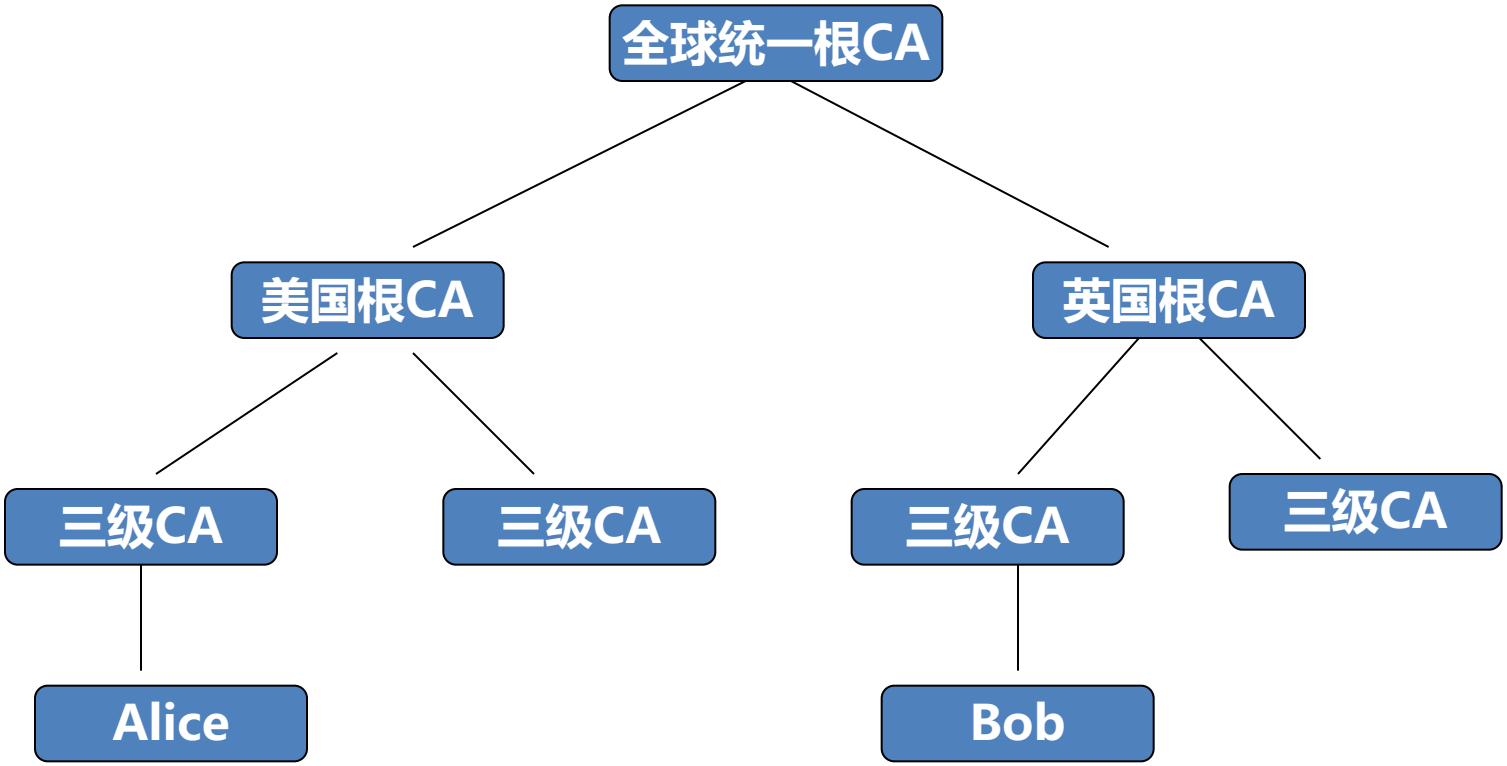
但她们不能相互认证。

（2）PKI有2种实现途径：

1）各PKI体系的根CA交叉认证（互签证书/主体CA/中间CA）



2) 全球性统一根CA



支付工具：现金→信用卡。

网上交易: 商家、消费者和银行通过Internet交互.

1996年6月，由IBM，Master Card International，Visa International，Microsoft，Netscape等共同制定的标准SET（Secure Electronic Transaction）.

规定了参加电子交易各方在交易中的行为规范和信息交换的过程和规则，

数字认证、数字签名等。

被用于B2C交易模式中。

五种实体：

✓持卡人：拥有信用卡的消费者；

✓商家：在Internet上提供商品或服务的商店；

✓支付网关：由金融机构或第三方控制，它处理持卡人购买和商家支付的请求；

✓收单行(Acquirer)：负责将持卡人的帐户中资金转入商家帐户的金融机构；

✓发卡行：负责向持卡人发放信用卡的金融机构。

SET协议流程：

1）用户向商家发订单和商家经过签名、加密的信托书。

信用卡号经过加密，商家无从得知；

2）收单银行收到商家发来的信托书，解密信用卡号，并通过认证验证签名；

3）收单银行向发卡银行查问，确认用户信用卡是否属实；

4）发卡银行认可并签证该笔交易；

5）收单银行认可商家并签证此交易；

6）商家向用户传送货物和收据；

7） 交易成功，商家向收单银行索款；

8） 收单银行按合同将货款划给商家；

9） 发卡银行向用户定期寄去信用卡消费账单。

拓展阅读

- 关于标识与认证，还有许多待研究的问题，感兴趣的同学可以通过中国科大图书库主页，在中国知网用“标识与认证”主题进行查询。
- 推荐阅读：

1宋玉龙,马文平,刘小雪.基于区块技术的权重标识的跨域认证方案[J].计算机应用与软件,2022,39(01):308-312.

2 王洒洒,戴炳荣,朱孟禄,李超.面向跨链系统的用户身份标识认证模型[J/OL].计算机工程与应用:1-8[2022-03-10].http://kns.cnki.net/kcms/detail/11.2127.TP.20211116.1918.004.html

3贾轶,包俊岭,吕永刚,张家华,欧阳震诤.可信身份认证和标识密码技术的跨网域建设与应用[J].电子技术与软件工程,2021(21):239-242.

4 戴斯达. 天地一体化信息网络标识认证协议设计与实现[D].北京邮电大学,2021.DOI:10.26969/d.cnki.gbydu.2021.002258.

5余果,王冲华,陈雪鸿,李俊.认证视角下的工业互联网标识解析安全[J].信息网络安全,2020,20(09):77-81.

6郑亚杰. 基于唯一标识图像认证技术的研究与应用[D].北京印刷学院,2020.DOI:10.26968/d.cnki.gbjyc.2020.000164.

7 赵茭茭. 云服务场景下可信标识签发及认证机制研究[D].西安电子科技大学,2018.

本讲到此结束，谢谢聆听！

Any question?

下一讲：入侵检测技术