IB00168 网络空间安全基础

授课教师：姜婧妍

jiangjingyan@sztu.edu.cn

2023年

第三章 数字签名与身份认证

授课教师：姜婧妍

jiangjingyan@sztu.edu.cn

2023年

第3章 身份认证（安全基础设施技术）

1. 用户认证
    1. 基于口令的认证
    2. 基于智能卡的认证
    3. 基于生物特征的认证
2. 认证协议
    1. 单向认证
3. PKI技术
    1. PKI体系结构
    2. X.509数字证书
    3. 认证机构
    4. PKIX相关协议
    5. PKI信任模型

身份认证

- **Authentication** is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity.（认证是确认一个实体声称为真的一段数据的属性的真实性的行为）
- **身份认证：确认某个实体是所声称的实体的行为。**

- 根据被认证实体的不同，身份认证包括两种情况：
  ① **计算机认证人**的身份，称之为**用户认证**；
  ② **计算机认证计算机**，主要出现在通信过程中的认证握手阶段，称之为**认证协议**。

3.1 用户认证

- 用户认证是由计算机对用户身份进行识别的过程，用户向计算机系统出示自己的身份证明，以便计算机系统**验证确实**是所声称的用户，允许该用户访问系统资源。
- **用户认证是对访问者授权的前提**。

- 用户认证的依据主要包括以下三种：
  A. 所知道的信息，比如身份证号码、账号密码、口令等。
  B. 所拥有的物品，比如IC卡、USBKey等。
  C. 所具有的独一无二的身体特征，比如指纹、虹膜、声音等。

3.1.1 基于口令的认证

- 基于用户名 / 口令的身份认证是最简单、最易实现、最易理解和接受的一种认证技术，也是目前应用最广泛的认证方法。
- 包括静态口令和动态口令。

1.静态口令

- 是指**用户口令是静态的**。
  - 例如，操作系统及诸如邮件系统等一些应用系统的登录和权限管理，都是采用“用户账户加静态口令”的身份识别方式。
  - 口令是一种根据**“所知道的信息”**实现身份认证的方法，其优势在于实现的简单性，无须任何附加设备，成本低、速度快。

静态口令的认证必须解决两个问题

1) 口令存储

- 如果口令以**明文方式**存储，则**易受字典攻击**，也就是使用一个预先定义好的单词列表，逐一地尝试所有可能的口令的攻击方式。
- 一般系统的**口令文件存储的是口令的散列值**，即使攻击者得到口令文件，由于散列函数的单向性，也**难于得到口令明文**。

2) 口令传输

- 在网络环境中，基于口令的身份认证系统一般采用客户 / 服务器模式，如各种Web应用。服务器统一管理多个用户账户，用户口令要从客户机传送到服务器上进行验证。为了保证传输过程中口令的安全，一般**采用双方协商好的加密算法或单向散列函数对口令进行处理后传输**。

静态口令的认证方式存在的安全问题

① 它是一种单因素的认证方式，安全性全部依赖于口令，口令一旦被泄露，用户即可被冒充。

② 为了便于记忆，用户往往选择简单、容易被猜测的口令，如生日。这使得口令被攻击的难度大大降低。

③ 口令在网络上传输的过程中可能被截获。

④ 系统中所有用户的口令以文件形式存储在认证方，攻击者可以利用系统中存在的漏洞获取系统的口令文件。

⑤ 用户在访问多个不同安全级别的系统时，都要求用户提供口令，用户为了记忆的方便，往往采用相同的口令。

⑥ 口令方案无法抵抗重放攻击。

⑦ 只能进行单向认证，即系统可认证用户，而用户无法对系统进行认证，攻击者可能伪装成系统骗取口令。

静态口令实例：操作系统的用户认证

- ubuntu linux系统
- 用adduser username增加用户并设置口令：
  - sudo adduser test
- 用id username查看用户标
- 识：
  - id test
- 用passwd username更改用户口令：
  - sudo passwd test

- Windows系统
- 用net user name passwd增加用户并设置口令：
  - net user test 123456
- 用net user name 查看用户
- 信息：
  - net user test
- 用net localgroup Administrators test /add将用户加入管理员组：
  - net localgroup Administrators test /add

2.动态口令

- 为了有效地改进口令认证的安全性，人们提出了各种基于动态口令的身份识别方法。
- 动态口令又叫做**一次性口令**，是指在用户登录系统进行身份认证的过程中，送入计算机系统的**验证数据是动态变化的**。

- **动态口令的主要思路是在登录过程中加入不确定因素**，如时间。系统执行某种加密算法**E(用户名+密码+不确定因素（时间）)**，**产生一个无法预测的动态口令**，以提高登录过程的安全性。

动态口令的产生

1)共享一次性口令表

- 系统和用户共享一个秘密口令表，每个口令只使用一次。用户登录时，系统需要检查用户的口令是否使用过。

2)口令序列

- 用户拥有一个长度为N、单向的、根据某种**单向 算法**前后相关的口令序列，每个口令只使用一次。用户用第M个口令登录时，计算机系统用**单向算法**计算第M个口令，并与用户输入的第M个口令 比对，实现对用户的认证。用户登录N次后，必 须重新初始化口令序列。

3)挑战—响应方式

- 用户登录时，系统产生一个随机数发送给用户。用户使用某种单向算法将自己的口令和随机数混 合起来运算，结果发送给系统。系统用同样的方 式进行运算，并通过结果比对实现对用户的认证。

4)时间—事件同步机制

- 这种方式可以看做挑战—响应方式的变形，区别在于以用户登录时间作为随机因素。这种方式要求双方的时间要同步。

基于电子令牌卡生成口令的工作原理

A. 用户和计算机系统之间**共享同一个用户口令**。用户还拥有一种叫做**动态令牌**的专用硬件，内置电源、密码生成芯片和显示屏，密码生成芯片运行专门的密码算法。

B. 当用户向认证系统发出登录请求时，认证系统向用户发送**挑战数据**。挑战数据通常是由两部分组成的，一部分是种子值，它是分配给用户的在系统内具有唯一性的一个数值，而另一部分是随时间或次数不断变化的数值。

C. 用户接收到挑战后，将**种子值、随机数值和用户口令**输入到动态令牌中进行计算，并把结果作为应答发送给远程认证系统。远程认证系统使用相同的算法和数据进行计算，与从用户那里接收到的应答数据作对比，认证用户的合法性。

动态口令

- 动态口令具有以下几个技术特点：

① **动态性**，登录口令是不断变化的。

② **随机性**，口令的产生是随机的，具有不可预测性。

③ **一次性**，每个口令只使用一次，以后不再使用。

④ **方便性**，用户不需记忆口令。

FTGS132

3.1.2 基于智能卡的认证

- **智能卡(smart card)**是一种集成的带有智能的电路卡，内置可编程的微处理器，可存储数据，并提供硬件保护措施和加密算法。

- 在智能卡中存储用户个性化的秘密信息，同时在验证服务器中也存放该秘密信息，进行认证时，用户输入PIN(Personal Identification Number，个人身份识别码)，智能卡认证PIN成功后，即可读出智能卡中的秘密信息，进而利用该秘密信息与主机之间进行认证。
- 其中，基于USB Key的身份认证是当前比较流行的智能卡身份认证方式。

USB Key

- USB Key是一种USB接口的硬件设备。它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的**私钥以及数字证书**，利用USB Key内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因此保证了用户认证的安全性。
- USB Key结合了现代密码学技术、智能卡技术和USB技术，具有以下4个主要特点。

∴**(1)双因子认证**。每一个USB Key都具有**硬件和PIN码**保护，PIN码和硬件构成了用户使用USB Key的两个必要因素，即所谓“**双因子认证**”。

USB Key的特点

- **(2)带有安全存储空间**。USB Key具有8～128kB的安全数据存储空间，可以存储数字证书、用户密钥等秘密数据，对该存储空间的读写操作必须通过程序实现，用户无法直接读取。其中用户私钥是不可导出的，杜绝了复制用户数字证书或身份信息的可能性。
- **(3)硬件实现加密算法**。USB Key内置CPU或智能卡芯片，可以实现数据摘要、数据加解密和签名的各种算法，加解密运算在USB Key内进行，保证了用户密钥不会出现在计算机内存中，从而杜绝了用户密钥被黑客截取的可能性。
- **(4)便于携带、安全可靠**。如拇指般大的USB Key非常便于随身携带，并且密钥和证书不可导出；USB Key的硬件不可复制，更显安全可靠。

基于USB Key的身份认证主要方式

(1)基于挑战 / 应答的双因子认证方式

- 先由客户端向服务器发出一个验证请求，服务器接到此请求后生成一个随机数（此为挑战）并通过网络传输给客户端。客户端将收到的随机数通过USB接口提供给**USB Key的计算单元**，由计算单元使用该随机数与存储在安全存储空间中的密钥进行运算并得到一个结果（此为应答）作为认证证据传给服务器。
- 与此同时，服务器也使用该随机数与存储在服务器数据库中的该客户密钥进行相同运算，如果服务器的运算结果与客户端回传的响应结果相同，则认为客户端是一个合法用户。
- 密钥运算分别在**USB Key的硬件计算单元**和服务器中运行，不出现在客户端内存中，也不在网络上传输，从而保护了密钥的安全，也就保护了用户身份的安全。

(2)基于数字证书的认证方式

- 随着PKI技术日趋成熟，许多应用中开始使用数字证书进行身份认证与数据加密。
- **数字证书是由权威公正的第三方机构（即CA中心）签发的，由用户的身份与其所持有的公钥相结合的计算机文件。**
- 以数字证书为核心的加密技术，可以对网络上传输的信息进行加密、解密、数字签名和签名验证，确保网上传 递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性。
- USB Key作为数字证书的存储介质，可以保证数字证书不被复制，并可以实现所有数字证书的功能。

USB Key实物

3.1.3 基于生物特征的认证

- 基于生物特征识别的认证方式**以人体具有的唯一的、可靠的、终生稳定的生物特征为依据**，利用计算机图像处理和模式识别技术来实现身份认证。生物特征识别技术目前主要利用指纹、声音、虹膜、视网膜、脸形、掌纹这几个方面的特征进行识别。
- 与传统的身份认证技术相比，基于生物特征的身份认证技术具有以下优点：
  ① 不易遗忘或丢失。
  ② 防伪性能好，不易伪造或被盗。
  ③ “随身携带”，方便使用。
- 目前，已有的生物特征识别技术主要有指纹识别、掌纹识别、手形识别、人脸识别、虹膜识别、视网膜识别、声音识别和签名识别等。

指纹识别

- 指纹识别是最早研究并利用的，且是最方便、最可靠的生物识别技术之一。
- 指纹识别主要包括三个过程：指纹图像读取、特征提取、比对。

① 首先，通过指纹读取设备读取到人体指纹的图像，进行初步的处理，使之清晰；

② 然后，通过指纹图像进行指纹特征数据的提取，这是一种单方向的转换；

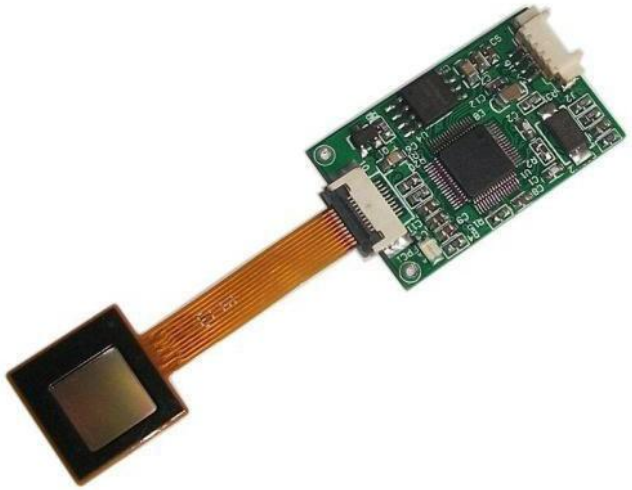
③ 最后，计算机通过某种指纹匹配算法进行比对，得到两个指纹的匹配结果。

其他的用于认证的生物特征

- 此外，人们还研究了其他的一些生物特征，如手部静脉血管模式、DNA、耳形、身体气味、击键的动态特性、指甲下面的真皮结构等。这些技术与上述的几大技术相比，普遍性较差，主要用于一些特定的应用领域。

- 尽管生物学特征的身份验证机制提供了很高的安全性，但其生物特征信息采集、认证装备的成本较高，只适用于安全级别比较高的场所。

基于生物特征的认证实例：基于指纹的认证



难于抵抗指纹克隆技术的攻击!

日常生活中的用户认证

- 智能手机的解锁屏幕

  指　　纹　　解　　锁

  人　　脸　　识　　别

  锁　　屏　　密　　码

  图形解锁

- 网络银行的多因素认证：

  登录网页：用户名/口令认证

  转账确认：

  - 手机短信验证码+网银口令
  - 手机短信验证码+动态口令
  - USB Key + PIN

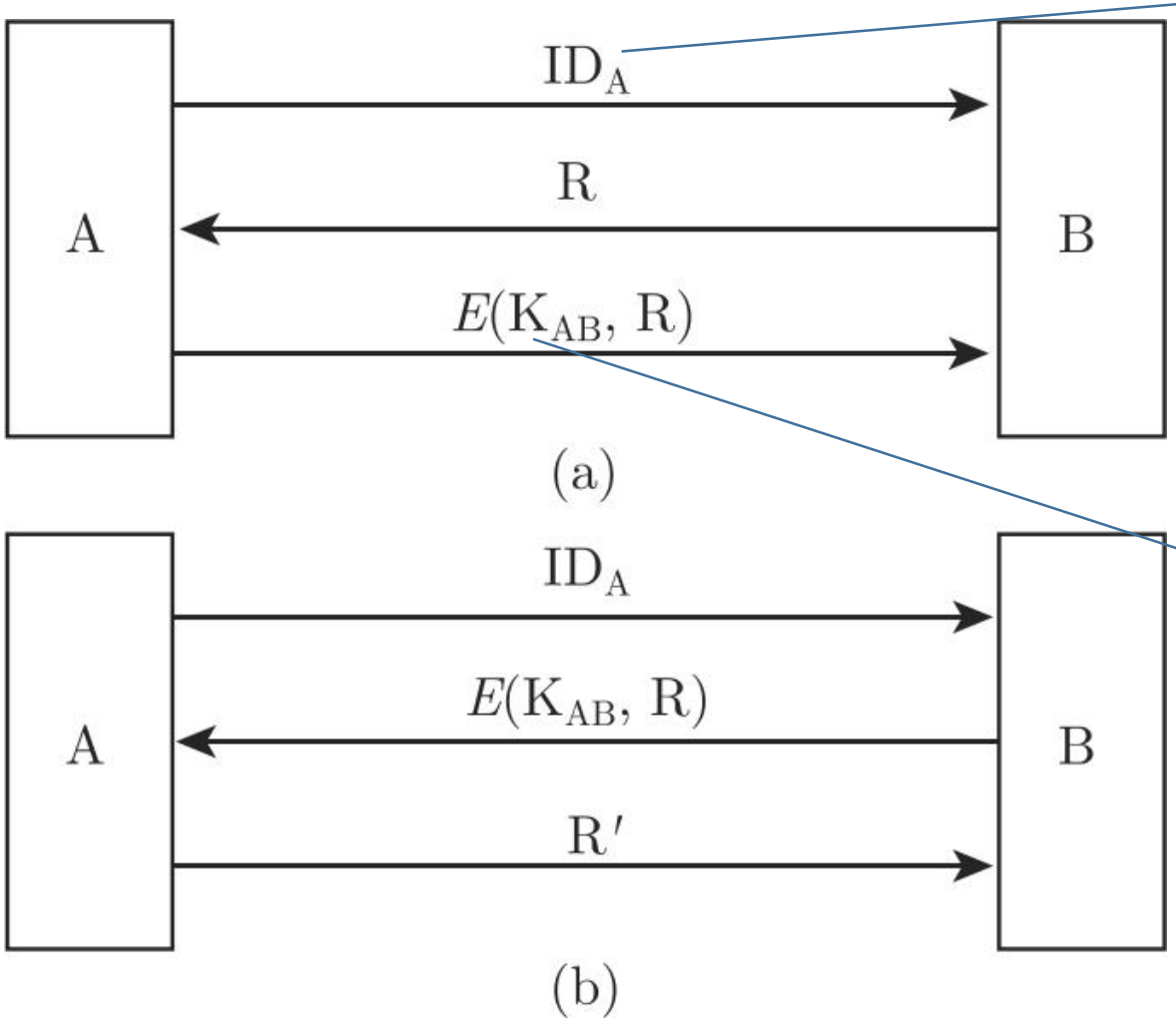
3.2 认证协议

- 认证协议通过一定的过程，保证使合法的协议一方（或双方彼此）**确信对方确实是其所声称的那个实体。身份认证协议的实质是抗身份欺诈。**

3.2.1 单向认证

- 单向认证是指通信双方中，**只有一方对另一方进行认证**。通常，单向认证(**B认证A**)协议包括三个步骤：
  ① 应答方B通过网络发送一个挑战；
  ② 发起方A回送一个对挑战的响应；
  ③ 应答方B检查此响应，然后再进行通信。
- 单向认证既可以采用对称密码技术实现，也可以采用公钥密码技术实现。

基于对称加密的单向认证方案



ID_A:
A的唯一标识

B认证A:
B随机选择一个挑战**R**

K_{AB}:
A和B的共享密钥

图3-1 基于对称加密的单向认证

基于对称加密的、KDC干预的单向认证

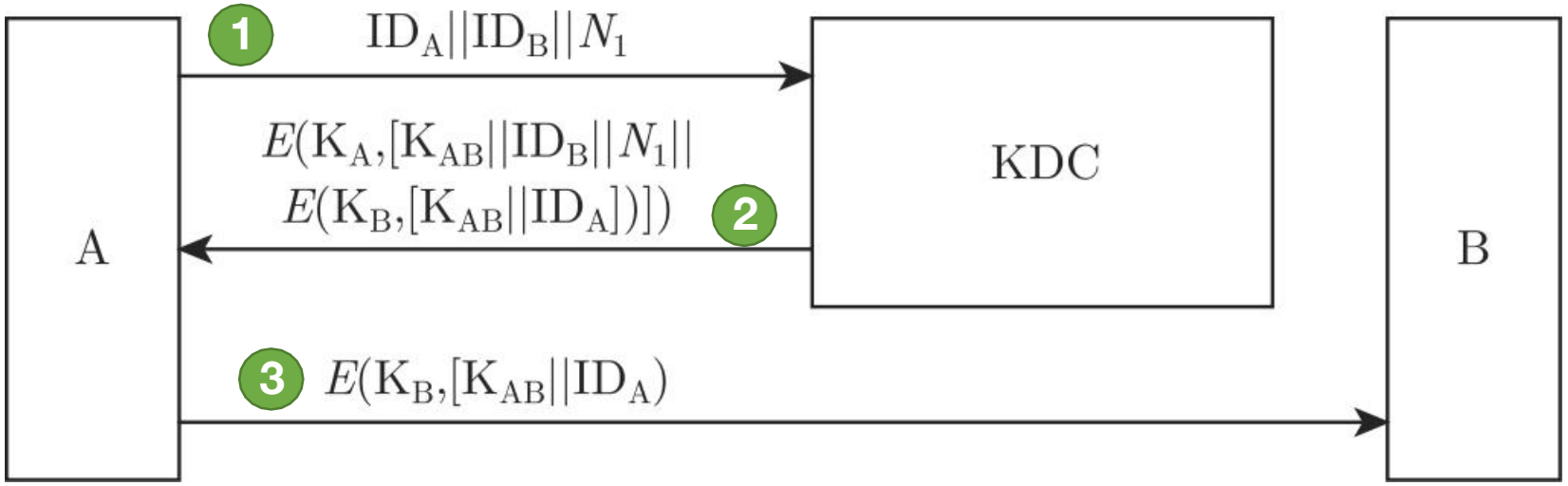


图3-2 基于对称加密的、KDC干预的单向认证

- 每个用户与**密钥分配中心(KDC)**共享唯一的主密钥：
  A有一个除了它外只有KDC知道的密钥K_A，
  同样，B有一个与KDC共享的密钥K_B。
- 假设A要与B建立一个逻辑连接，需要用一个一次性的**会话密钥K_{AB}**来保护数据的传输。

(1) A向KDC请求一个会话密钥以保护与B的逻辑连接。消息中有A和B的标识及唯一的标识N_1，这个标识我们称为临时交互号(nonce，不重复数)。

(2) KDC以用K_A加密的消息做出响应。消息中有两项内容是给A的。

- 一次性会话密钥K_{AB}，用于会话。
- 原始请求消息，包括临时交互号，以使A使用适当的请求匹配这个响应。

此外，消息中有两项内容是给B的。

- 一次性会话密钥K_{AB}，用于会话。
- A的标识符ID_A。

- 这两项用K_B(KDC与B共享的主密钥)加密。它们将发送给B，以建立连接并证明A的标识。

(3) A存下会话密钥备用，并将消息的后两项发给B，即$E(K_B, [K_{AB}||ID_A])$。现在B已知道会话密钥K_{AB}，知道它稍后的通话伙伴是A(来自ID_A)，且知道这些消息来自于KDC(因为它是用K_B加密的)。至此，B实现了对A的认证过程。

基于公钥加密的简单单向认证方案

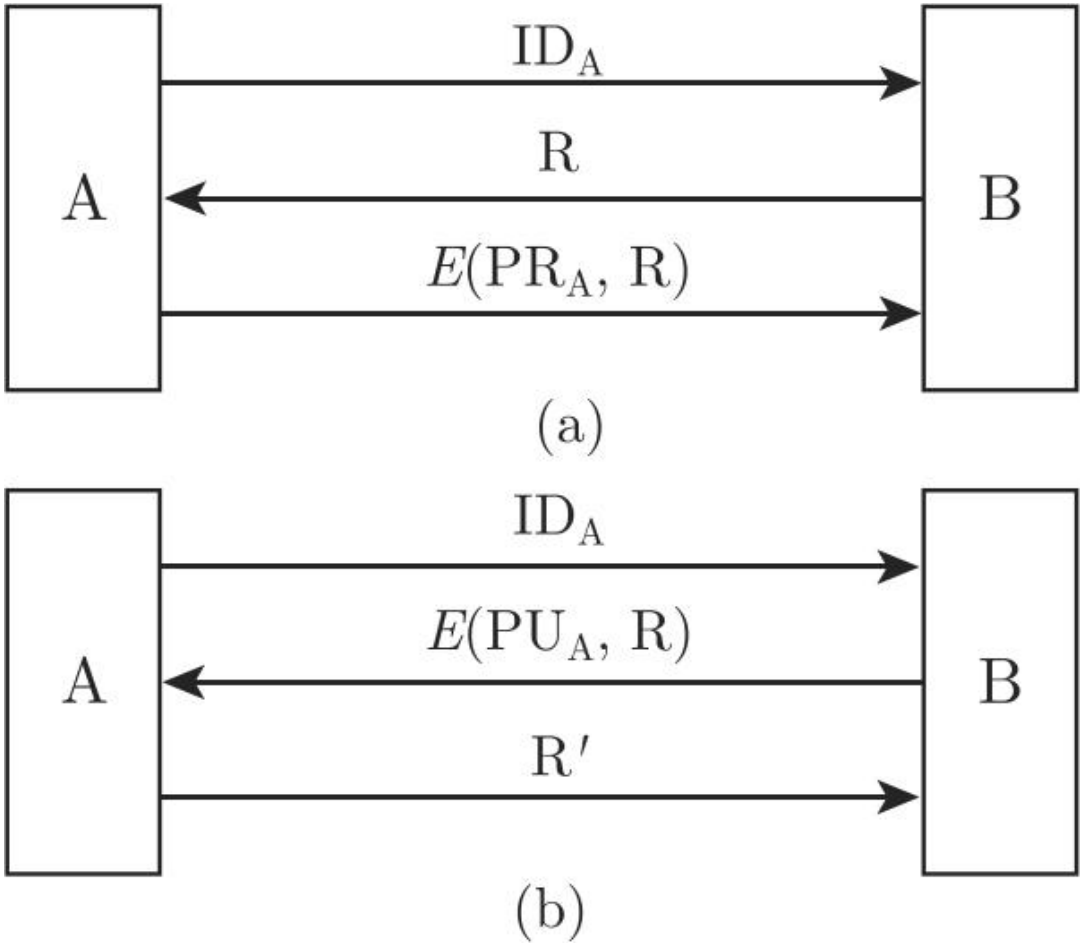
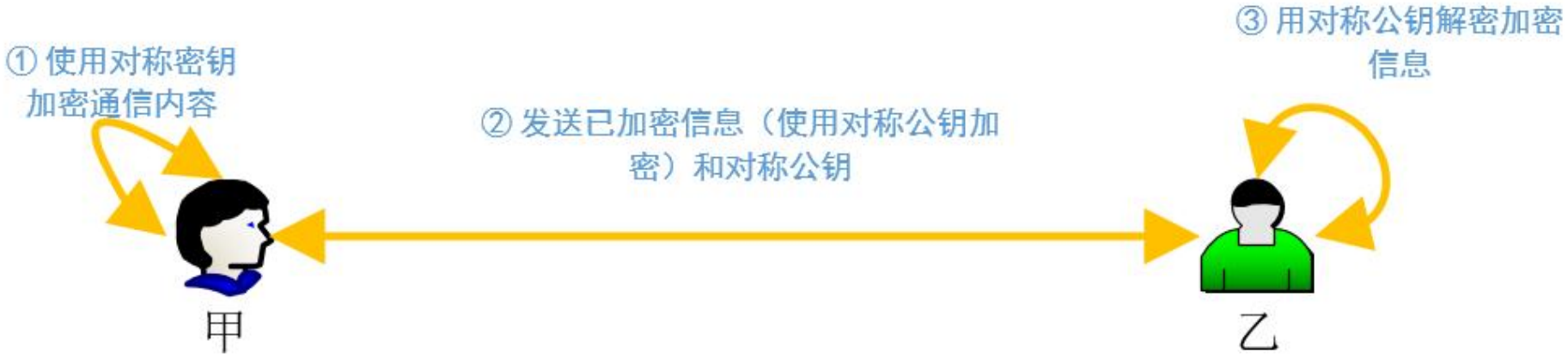


图3-3 基于公钥加密的单向认证

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？

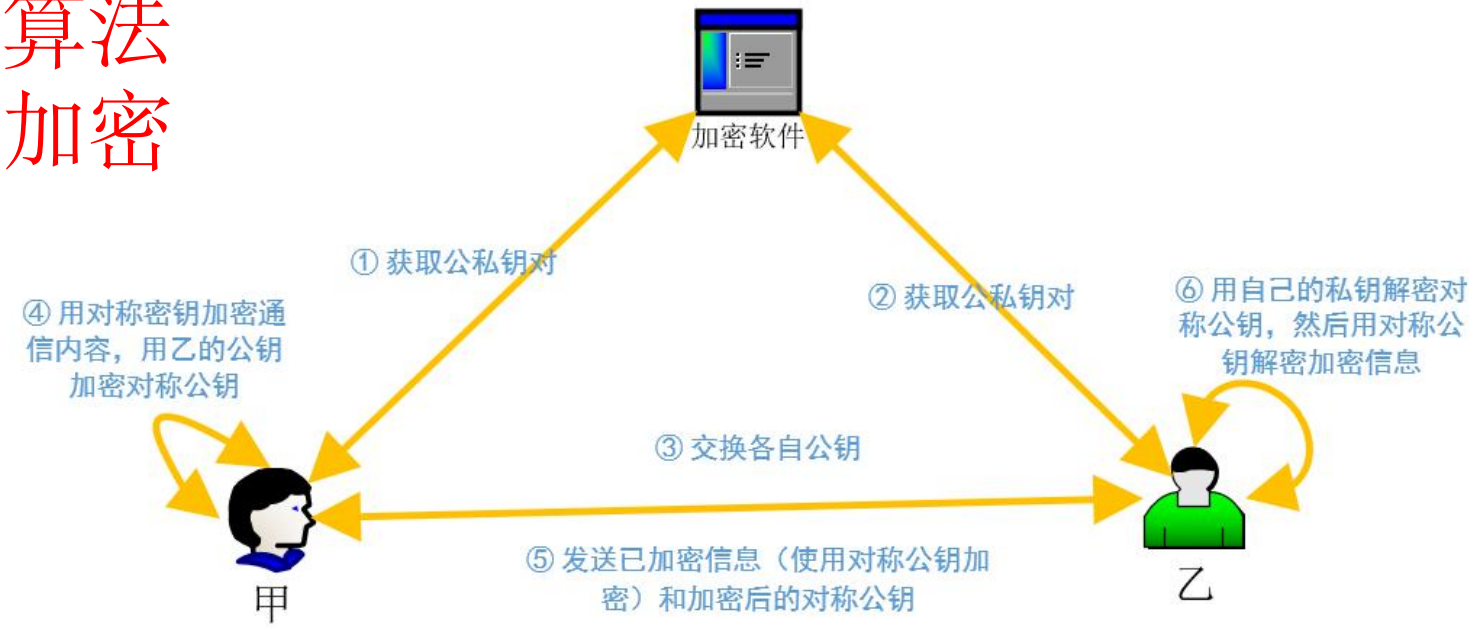
问题2：如果黑客截获此文件，是否用同一算法就可以解密此文件呢？

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？

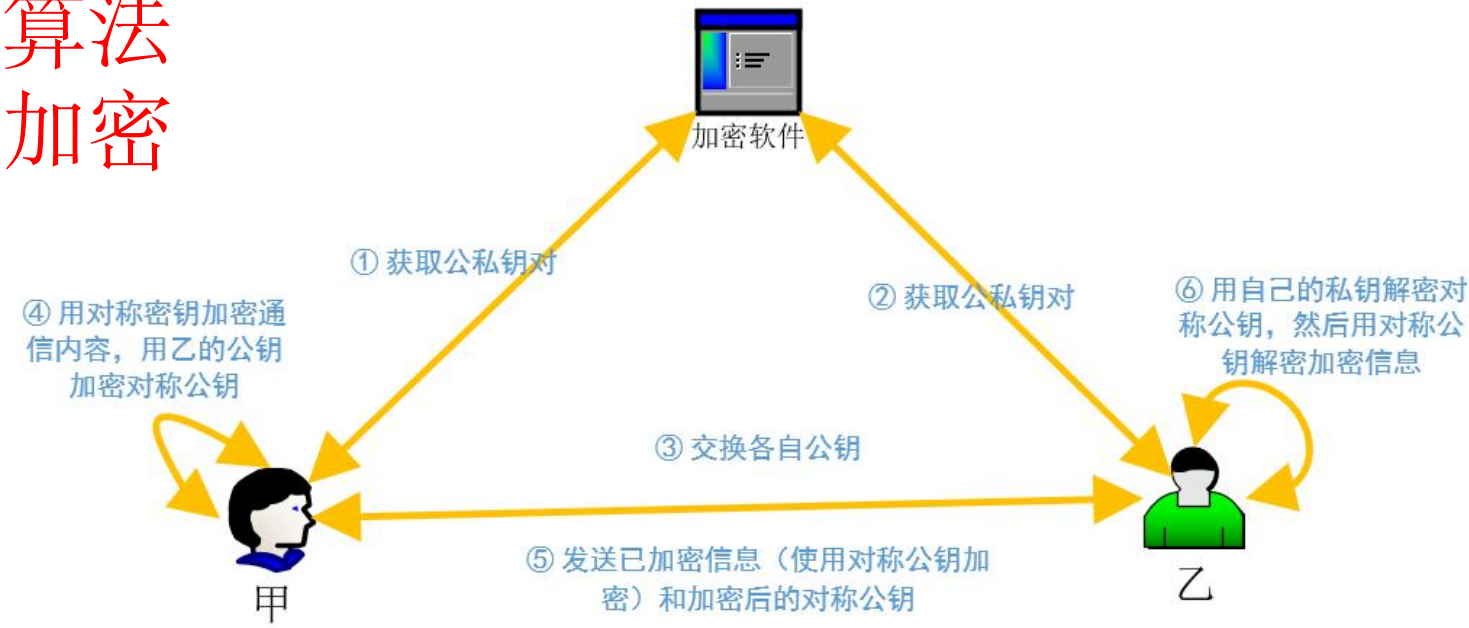
问题3：既然黑客不知密钥，那么乙怎样才能安全地得到其密钥呢？用电话通知，电话可能被窃听，通过Internet发此密钥给乙，可能被黑客截获，怎么办？

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:

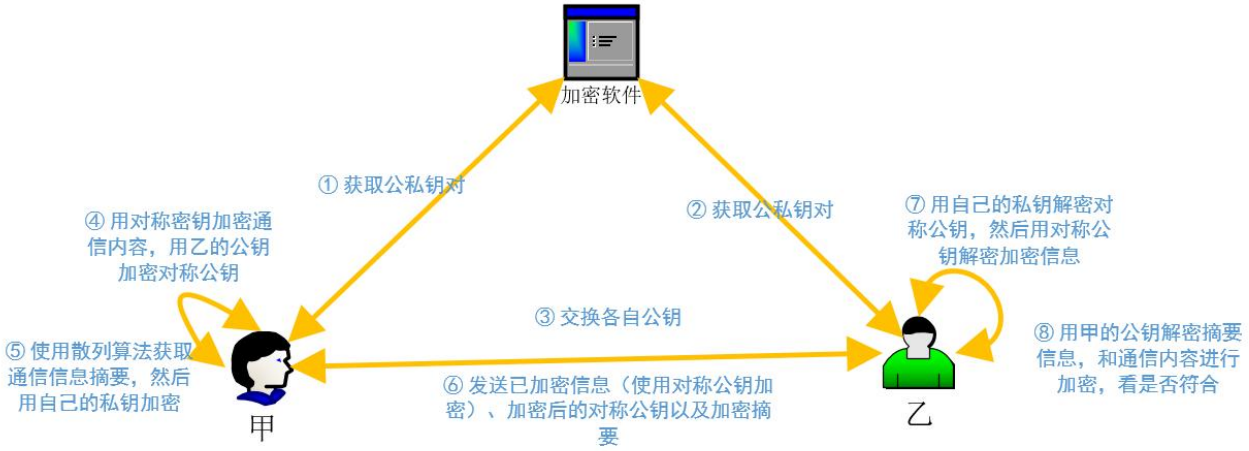
- 加密速度慢，比对称加密算法慢10～100倍，因此只可用其加密小数据（如对称密钥）
- 另外加密后会导致得到的密文变长。

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。

3.4 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。**

3.4.1 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

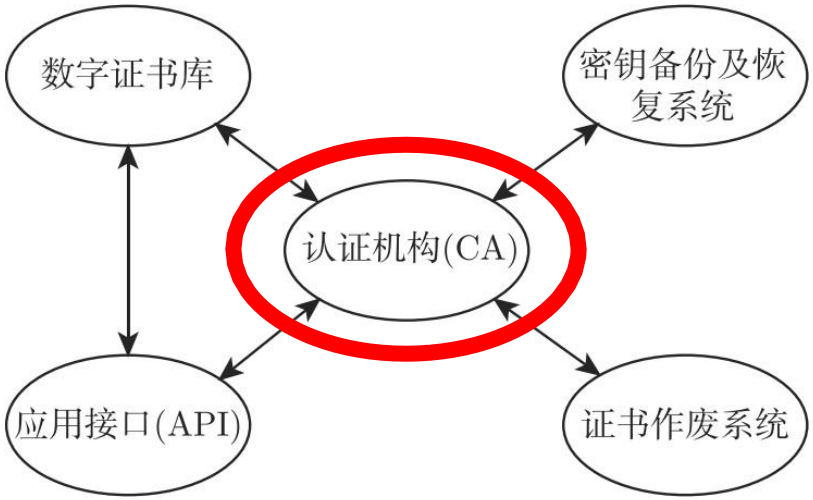


图3-9 PKI体系结构

- **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

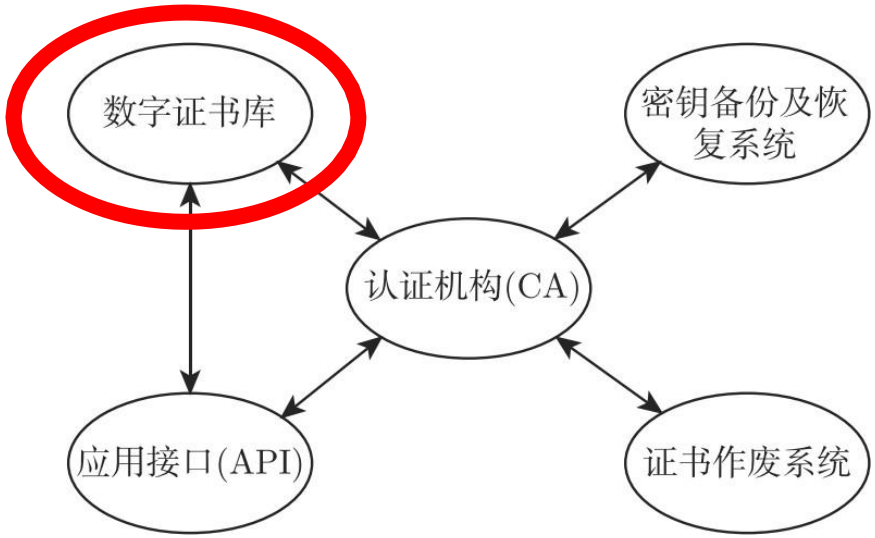


图3-9 PKI体系结构

- **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

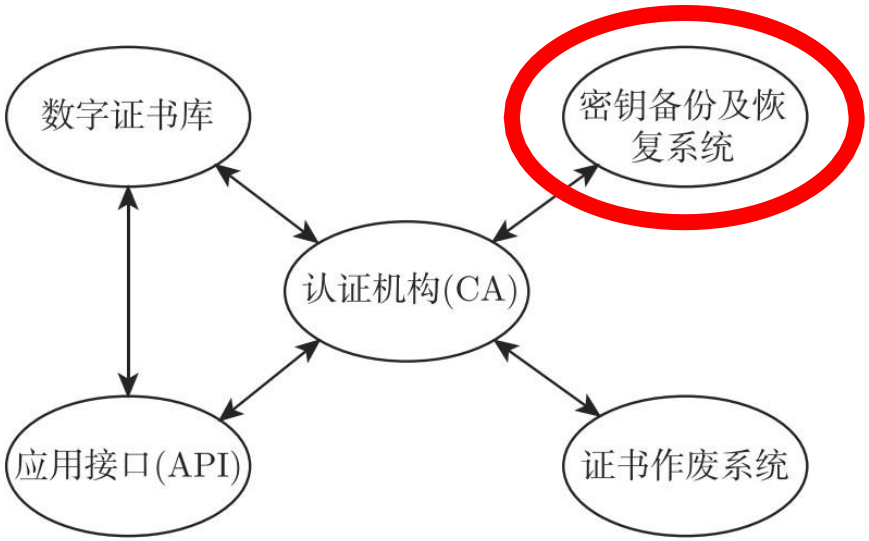


图3-9 PKI体系结构

- **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

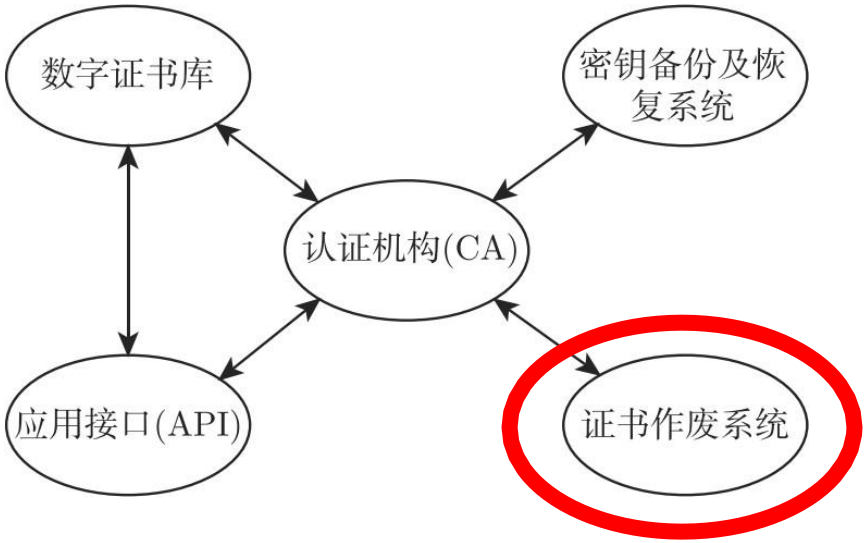


图3-9 PKI体系结构

- **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

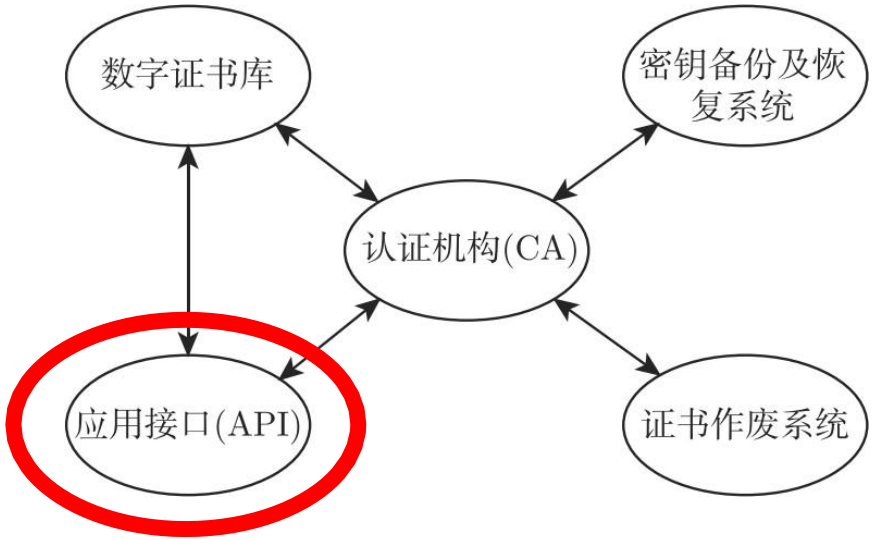


图3-9 PKI体系结构

- 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。

3.4.2 X.509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):**

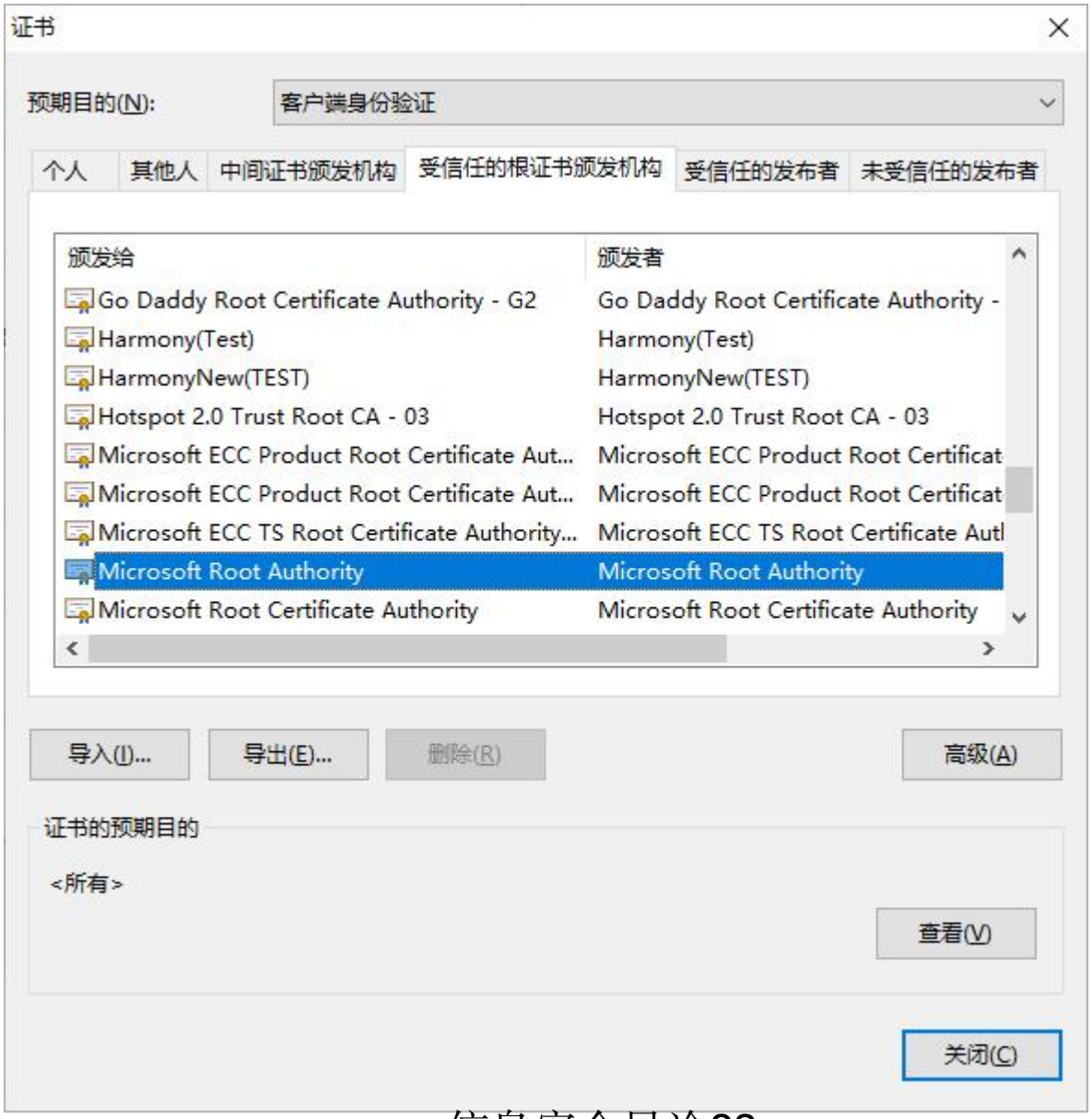
覆盖证书的所有其他域，以及其他域被CA私钥加密后的散列代码，以及签名算法标识。

- 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。

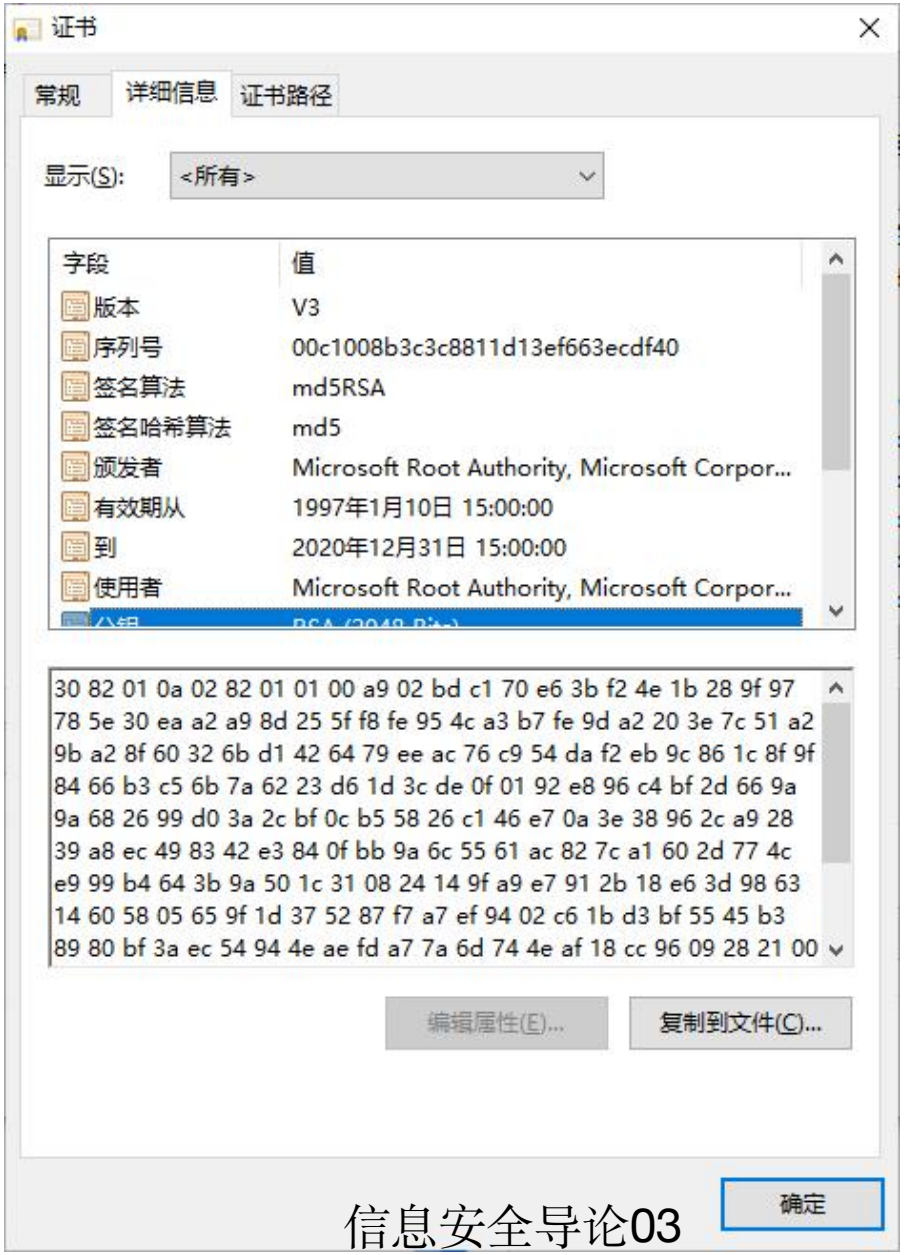
X.509 数字证书的结构

	version 1	version 2	version 3
Version			
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

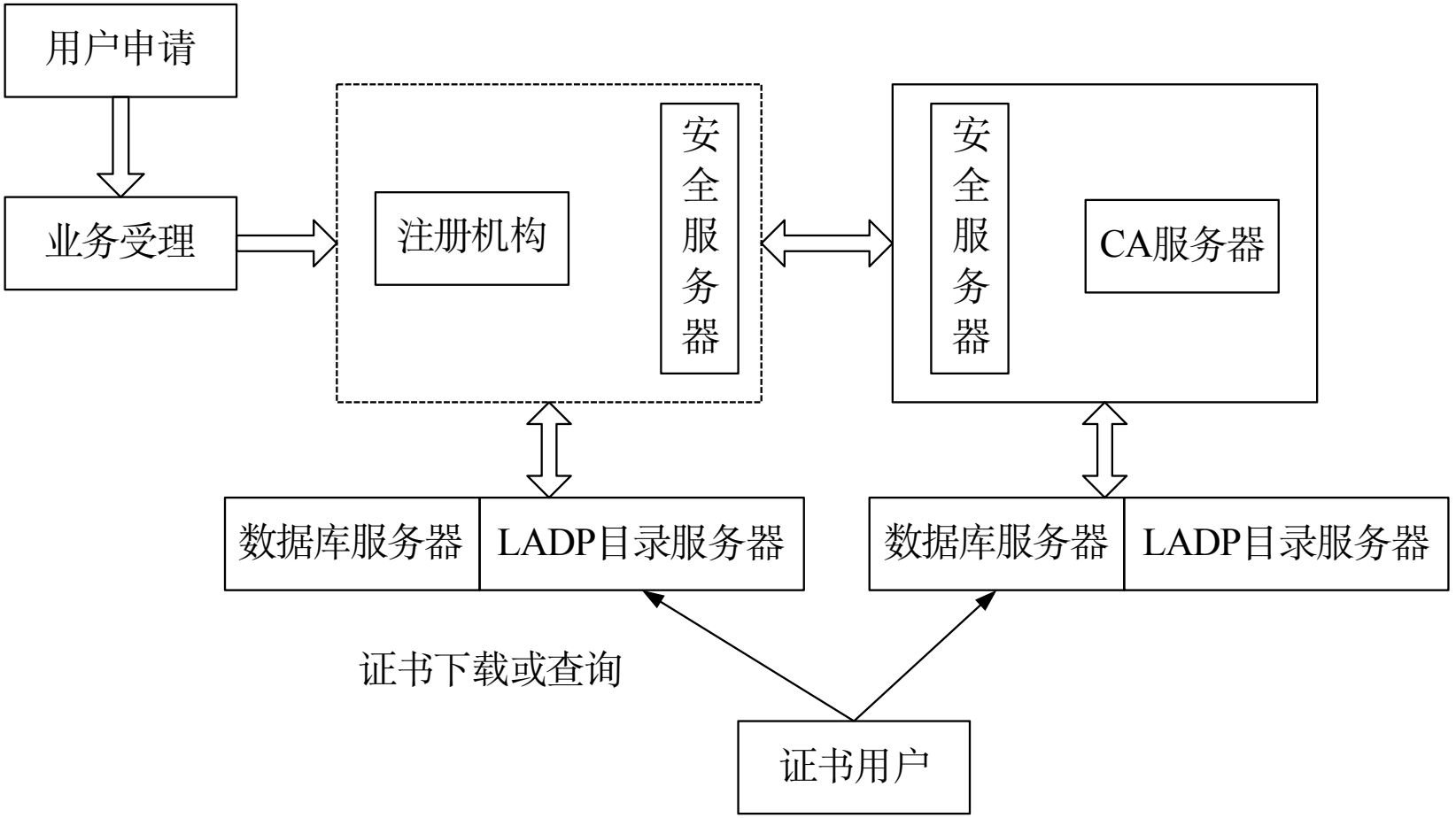


图3-10 典型CA的构成

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

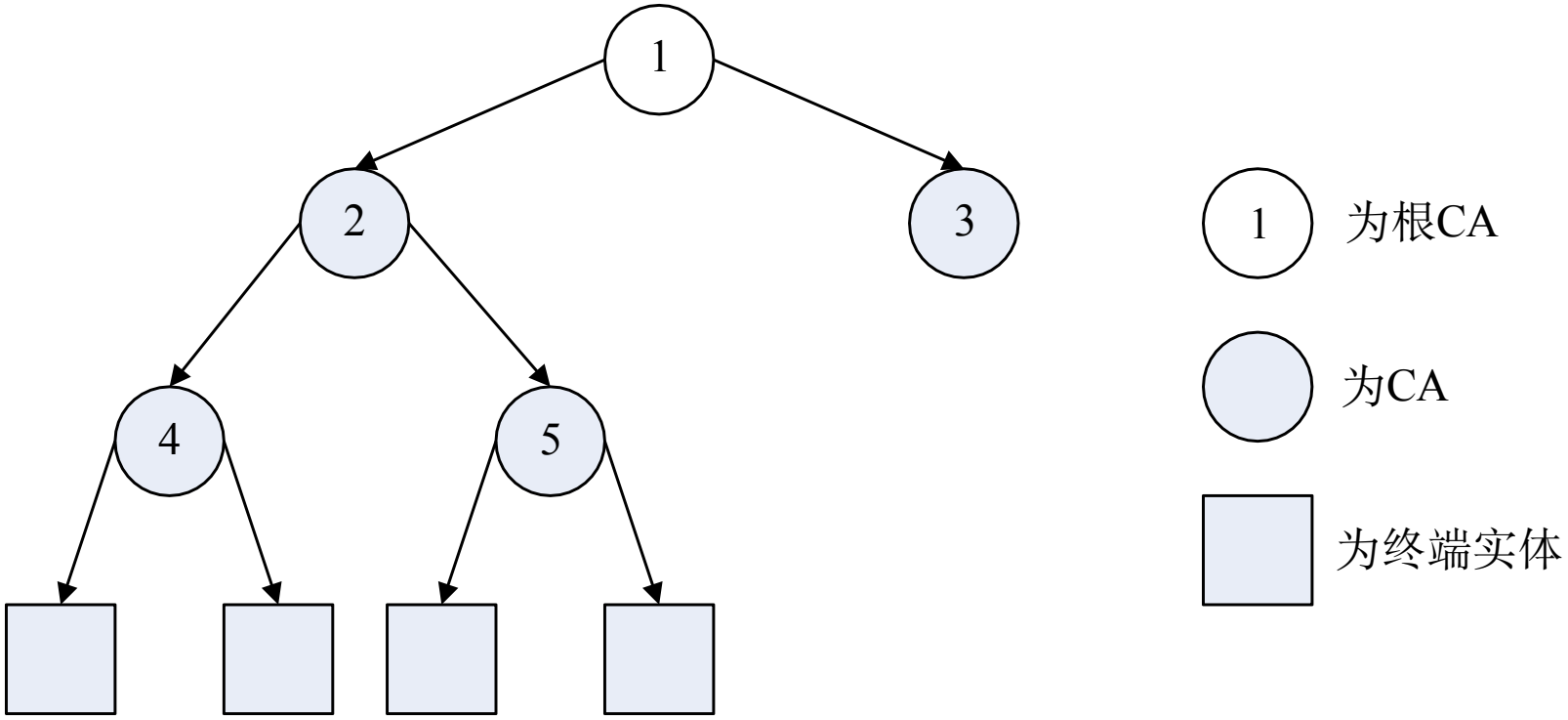


图3-12 层次模型

2.交叉模型

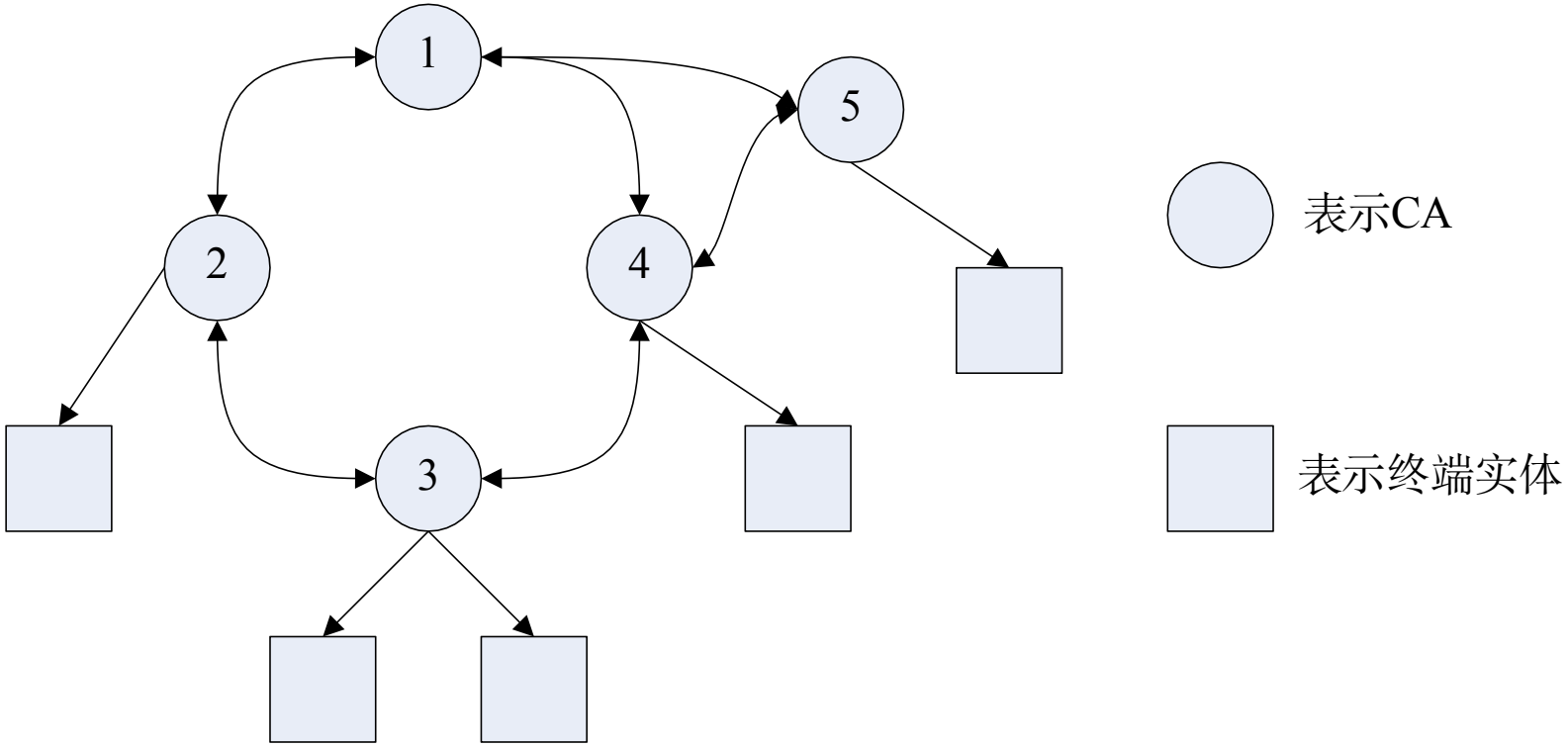


图3-12 交叉模型

3.混合模型

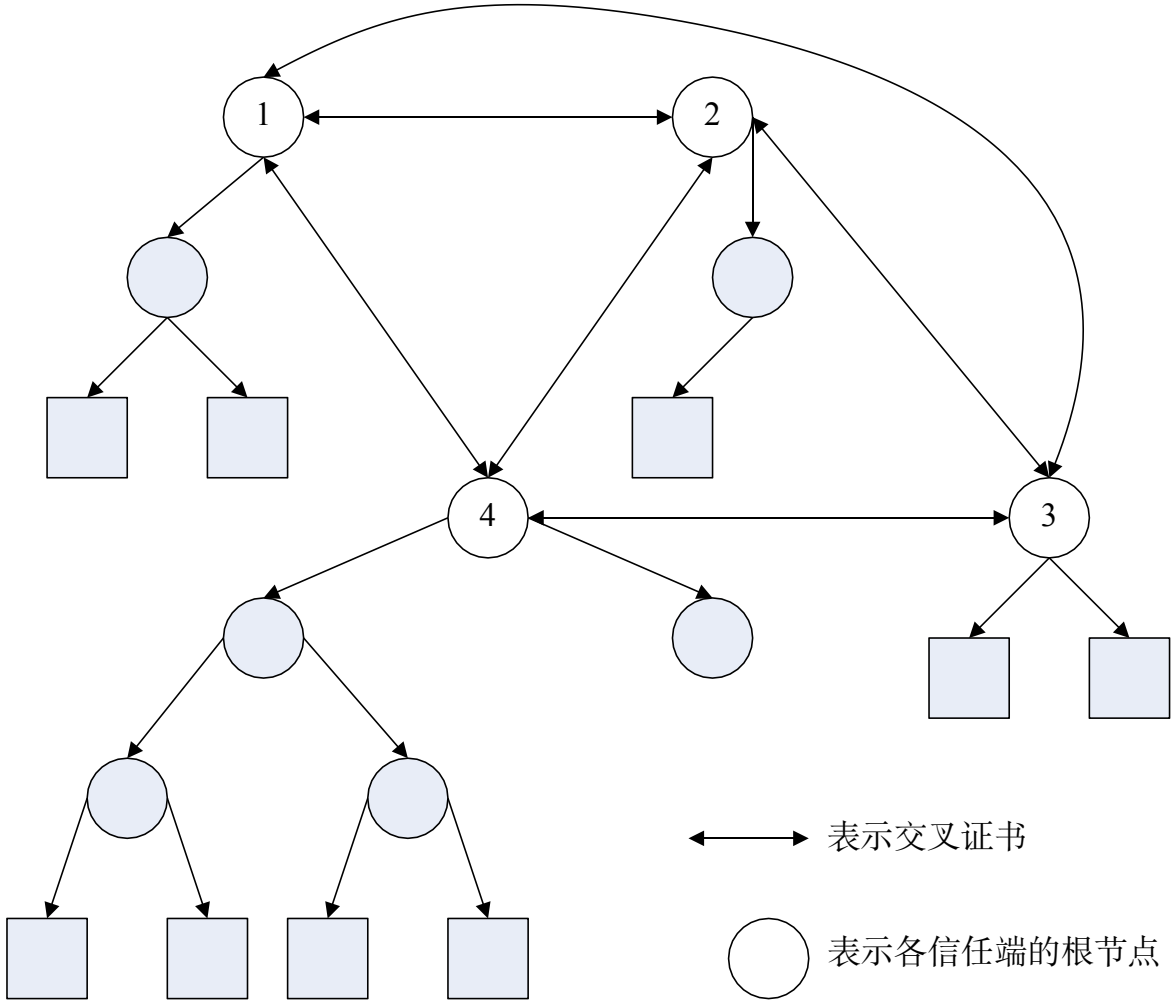


图3-13 混合模型 信息安全导论03

4.桥CA模型

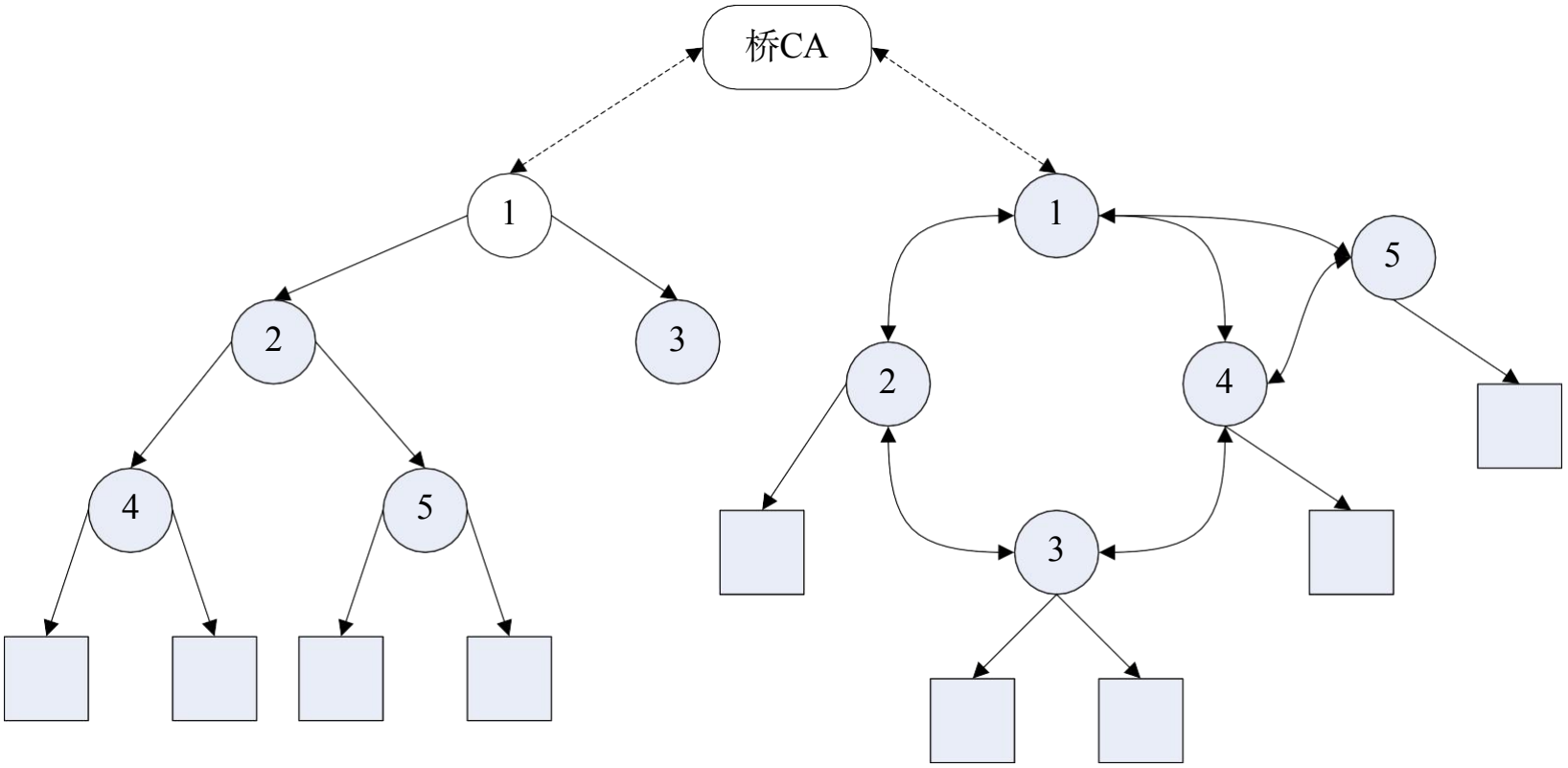


图3-14 桥模型

5.信任链模型

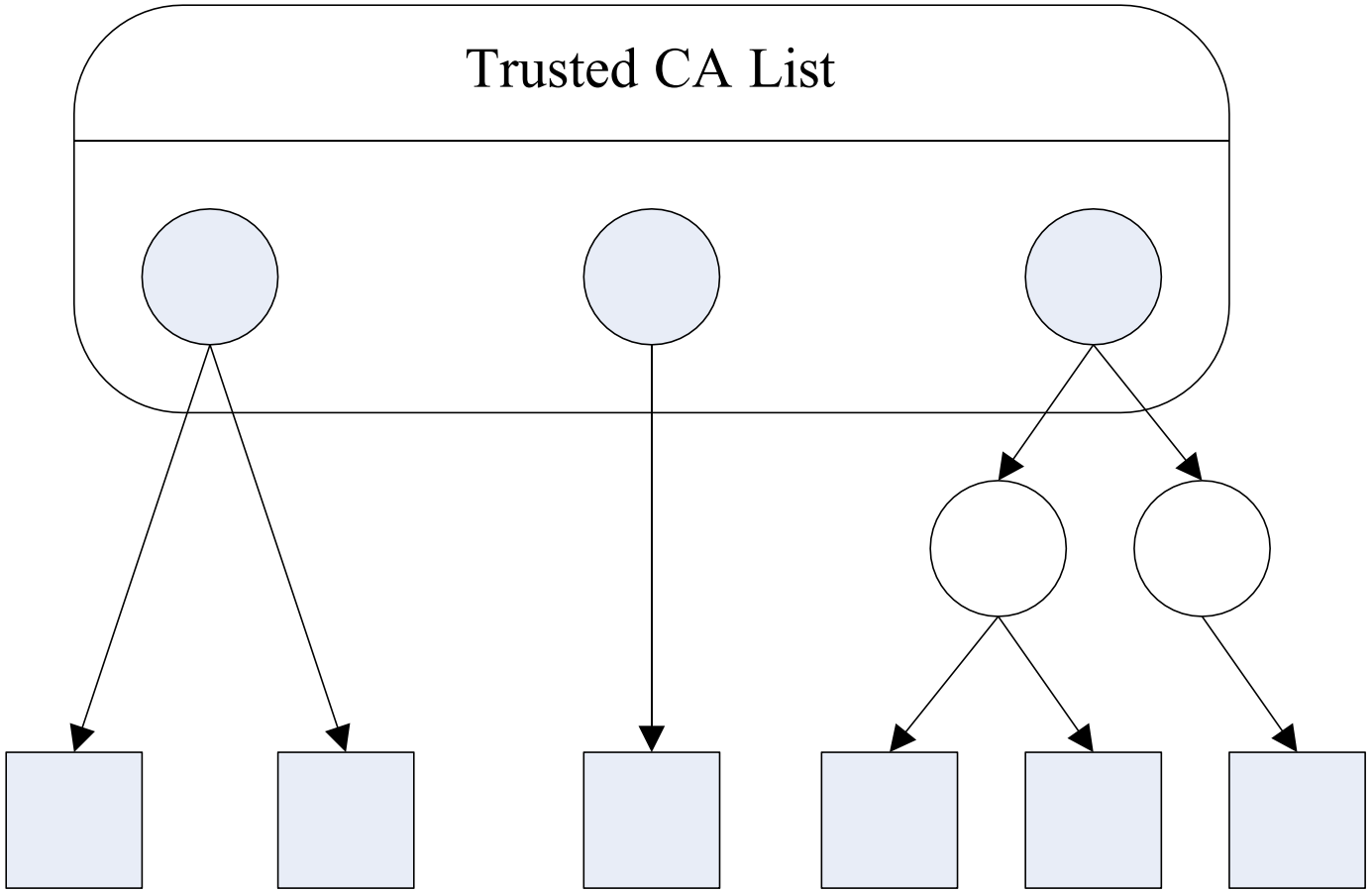


图3-15 信任链模型

思考：如何保证根证书可信？

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.


谢谢！