没有网络安全，
就没有国家安全！

第4章 身份认证

授课人：翟健宏

课前思考问题

- **了解一个会议软件，如腾讯会议、钉钉、Zoom、腾讯课堂等，如何实现身份认证的，安全性如何（易受干扰、会议保密性等），你给安全性打个分。**

主要内容

4.1 概述

- 问题的提出
- 身份认证
  - 身份认证是证实用户的真实身份与其所声称的身份是否相符的过程。
- 认证依据：应包含只有该用户所特有的、并可以验证的特定信息。
  - 用户所知道的或所掌握的信息（Something the user know），如密码、口令等；（基于口令的认证技术）
  - 用户所拥有的特定东西（Something the user possesses），如身份证、护照、密钥盘等；（基于密码学的认证技术）
  - 用户所具有的个人特征（Something the user is or How he behaves），如指纹、笔迹、声纹、虹膜、DNA等。（生物特征的认证技术）

身份认证的分类

- 根据认证条件的数目分类
  - 仅通过一个条件的相符合来证明一个人的身份，称之为单因子认证；
  - 通过两种不同条件来证明一个人的身份，称之为双因子认证；
  - 通过组合多种不同条件来证明一个人的身份，称之为多因子认证。
- 根据认证数据的状态来看，
  - **静态数据认证**:指用于识别用户身份的认证数据事先已产生并保存在特定的存储介质上；
  - **动态数据认证**:指用于识别用户身份的认证数据不断动态变化，每次认证使用不同的认证数据，即动态密码。

4.2 认证协议

- 技术基础
  - 以网络为背景的认证技术的核心基础是密码学
  - 对称密码和公开密码是实现用户身份识别的主要技术
- 实现机制
  - 实现认证必须要求示证方和验证方遵循一个特定的规则来实施认证，这个规则被称为认证协议。
- 认证安全
  - 认证过程的安全取决于认证协议的完整性和健壮性。

4.2.1 基于对称密钥的认证协议

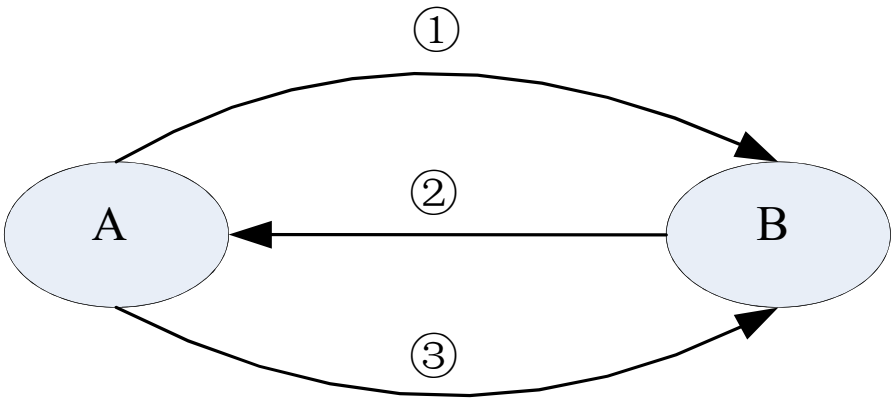
基于对称密码体制下的认证

① 示证方和验证方共享密钥，通过共享密钥来维系彼此的信任关系，实际上认证就是建立某种信任关系的过程。

② 在只有少量用户的封闭式网络系统中，各用户之间的双人共享密钥的数量有限，可以采用挑战-应答方式来实现认证；

③ 对于规模较大的网络系统，一般采用密钥服务器的方式来实现认证，即依靠可信的第三方完成认证。

基于挑战-应答方式的认证协议



① A ⟶ B：IDa ‖ IDb

② B ⟶ A：Nb

③ A ⟶ B：E_k(Nb)

Needham-Schroeder认证协议

- 适用条件
  - 所有的使用者共同信任一个公正的第三方，此第三方被称为认证服务。
  - 每个使用者需要在认证服务器AS(Authentication Server)上完成注册，
  - AS保存每一个用户的信息并与每一个用户共享一个对称密钥。

Needham-Schroeder 协议描述

① A → KDC： $ID_A||ID_B||N_1$ ；
- A通知KDC要与B进行安全通信，N_1为临时值。

② KDC → A： $EK_a[Ks||ID_B||N1||EKb[Ks||ID_A]]$ ；

③ A → B： $EK_b[Ks||ID_A]$ ；
- A转发KDC给B的内容。

④ B → A： $EKs[N_2]$ ；
- B用Ks加密挑战值N_2，发给A并等待A的回应认证信息。

⑤ A → B： $EKs[f(N_2)]$ ； * End
- A还原N_2后，根据事先的约定f(x)，计算$f(N_2)$，使用Ks加密后，回应B的挑战，完成认证，随后A和B使用Ks进行加密通讯。

安全问题

- 攻击方C已经掌握A和B之间通信的一个老的会话密钥
- C可以在第3步冒充A利用老的会话密钥欺骗B
- 除非B记住所有以前使用的与A通信的会话密钥，否则B无法判断这是一个重放攻击。

Kerberos

- 设计目标
  - 通过使用对称密钥系统为客户机/服务器应用程序提供强大的第三方认证服务。
- 前提条件
  - 每个用户或应用服务器与Kerberos分享一个对称密钥。
- 结构&机制
  - 认证服务器AS（Authentication Server）和票据授予服务器TGS（Ticket Granting Server）。
  - 票据Ticket是客户端用于证明自己身份。
    - AS负责签发访问TGS服务器的票据，TGS负责签发访问其它应用服务器的票据。
  - 允许一个用户通过交换加密消息在整个网络上与另一个用户或应用服务器互相证明身份，Kerberos给通讯双方提供对称密钥。

KerBeros协议

- **第一阶段 身份验证服务交换**

– C → AS：$ID_C||ID_{tgs}||TS_1$

– AS → C：$E_{KC}[K_{c,tgs}||ID_{tgs}||TS_2||Lifetime_2||Ticket_{tgs}]$

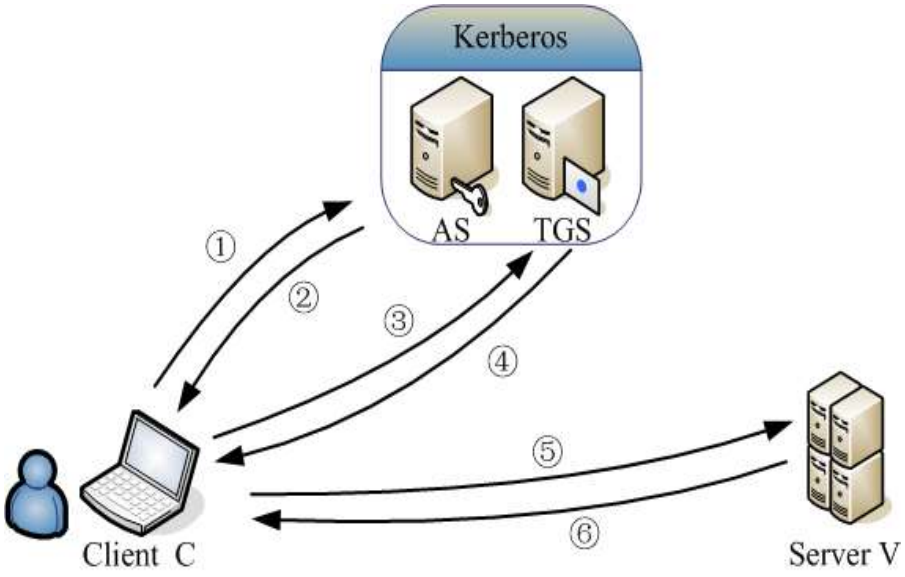
✧$Ticket_{tgs} = E_{Ktgs}[K_{c,tgs}||ID_C||AD_C||ID_{tgs}||TS_2||Lifetime_2]$

- **第二阶段 票据授予服务交换**
  - C → TGS：$ID_V||Ticket_{tgs}||Authenticator_c$
  - TGS → C：$E_{Kc,tgs}[K_{c,v}||ID_v||TS_4||Ticket_v]$

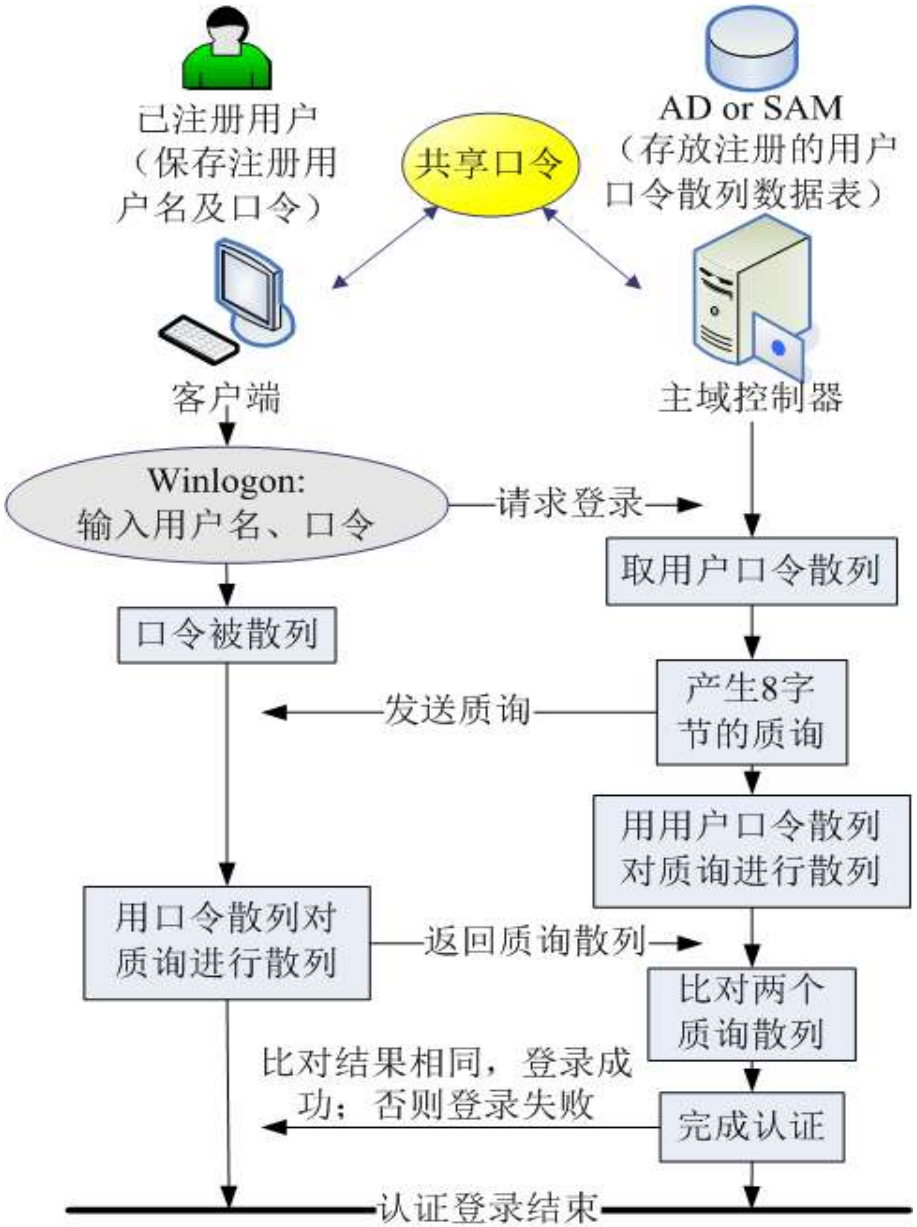
  ✧$Authenticator_c = E_{Kc,tgs}[ID_c||Ad_c||TS_3]$。

  ✧$Ticket_v = E_{KV}[K_{c,v}||ID_C||AD_C||ID_v||TS_4||Lifetime_4]$
- **第三阶段 客户与服务器身份验证交换**
  - C → V：$Ticket_v||Authenticator_c$
  - V → C：$E_{Kc,v}[TS_5+1]$ (for mutual authentication)

  ✧$Authenticator_c = E_{Kc,v}[ID_c||AD_c||TS_5]$



Windows系统的安全认证



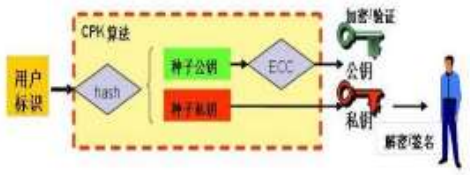
课堂问题

- KerBeros能够解决什么问题（多选）
  - A. 统一身份认证
  - B. 一次认证，访问多个服务器
  - C. 访问可靠性
  - D. 访问传输安全问题
  - E. 多密码问题

4.2.2 基于公开密钥的认证协议

基于公开密钥体制下的认证协议通常有两种认证方式

- 【方式一】实体A需要认证实体B，A发送一个明文挑战消息（也称挑战因子，通常是随机数）给B，B接收到挑战后，用自己的私钥对挑战明文消息加密，称为签名；B将签名信息发送给A，A使用B的公钥来解密签名消息，称为验证签名，以此来确定B是否具有合法身份。



- 【方式二】实体A将挑战因子用实体B的公钥加密后发送给B，B收到后，用自己的私钥解密还原出挑战因子，并将挑战因子明文发还给A，A可以根据挑战因子内容的真伪来核实B的身份。

Needham-Schroeder公钥认证

① A → B：$E_{KUb}[ID_a||R_a]$；

- A使用B的公钥加密A的标识ID_a和挑战R_a，确保只有B才能使用私钥解密。

② B → A：$E_{KUa}[R_a||R_b]$；

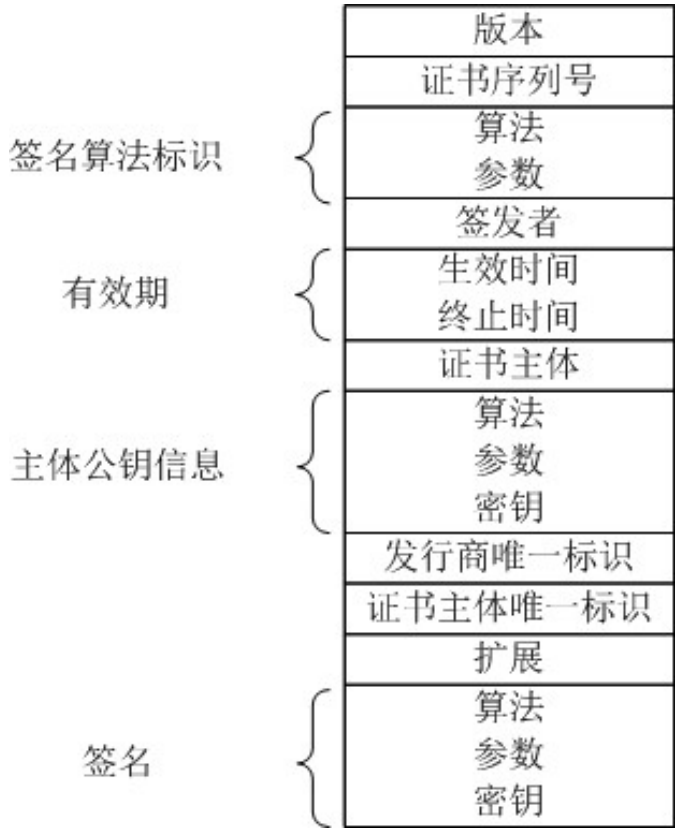
- B使用A的公钥加密A的挑战R_a和B的挑战R_b，发送给A，确保只有A才能使用其私钥解密。

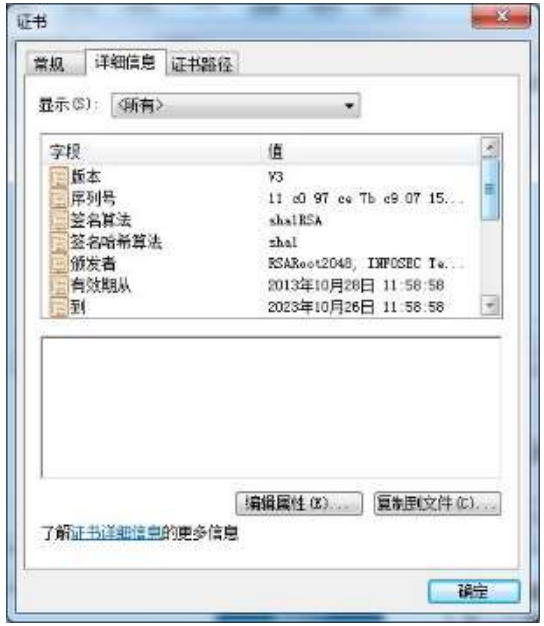
③ A → B：$E_{KUb}[R_b]$；

- A还原出R_b后，再使用B的公钥加密R_b，作为验证应答信息发送给B。

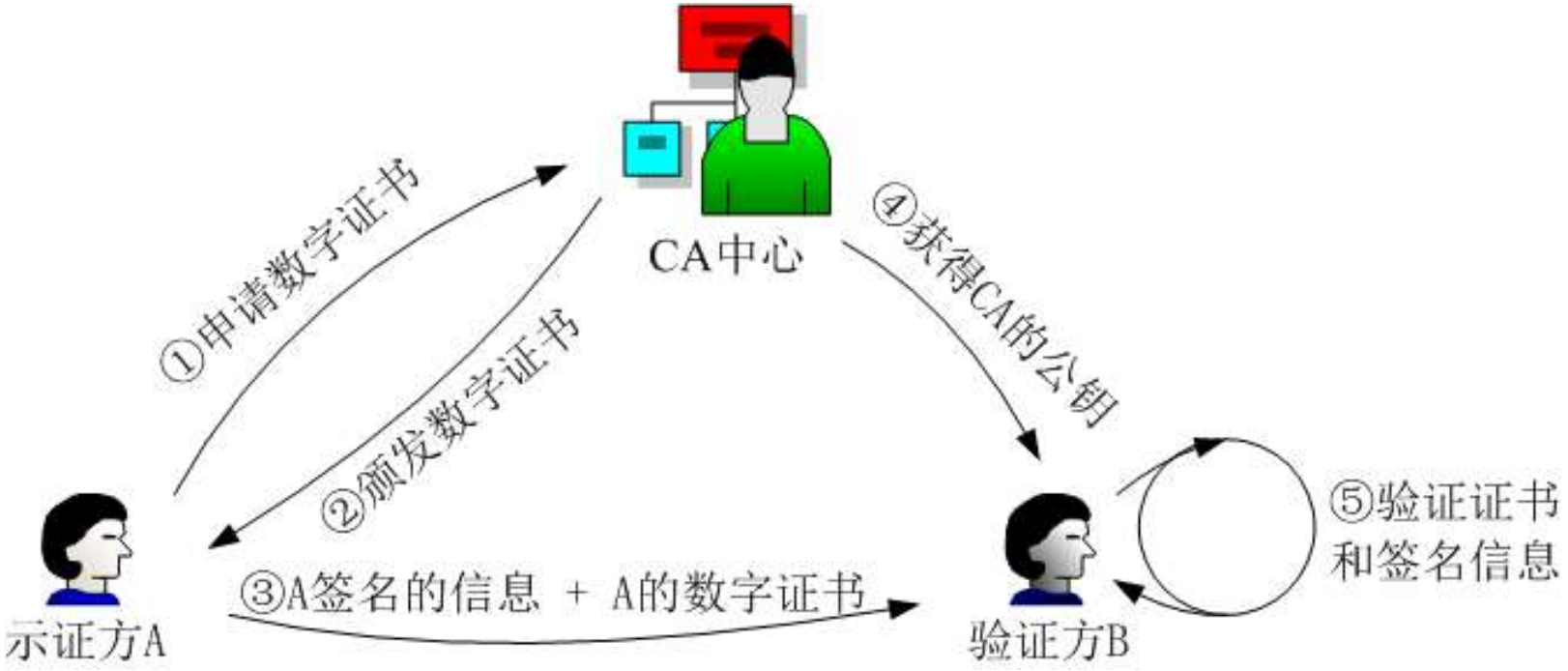
基于CA数字证书的认证协议

- 数字证书是一个经过权威的、可信赖的、公正的第三方机构（CA认证中心）签名的包含拥有者信息及公开密钥的文件。
- CA：Certificate Authority





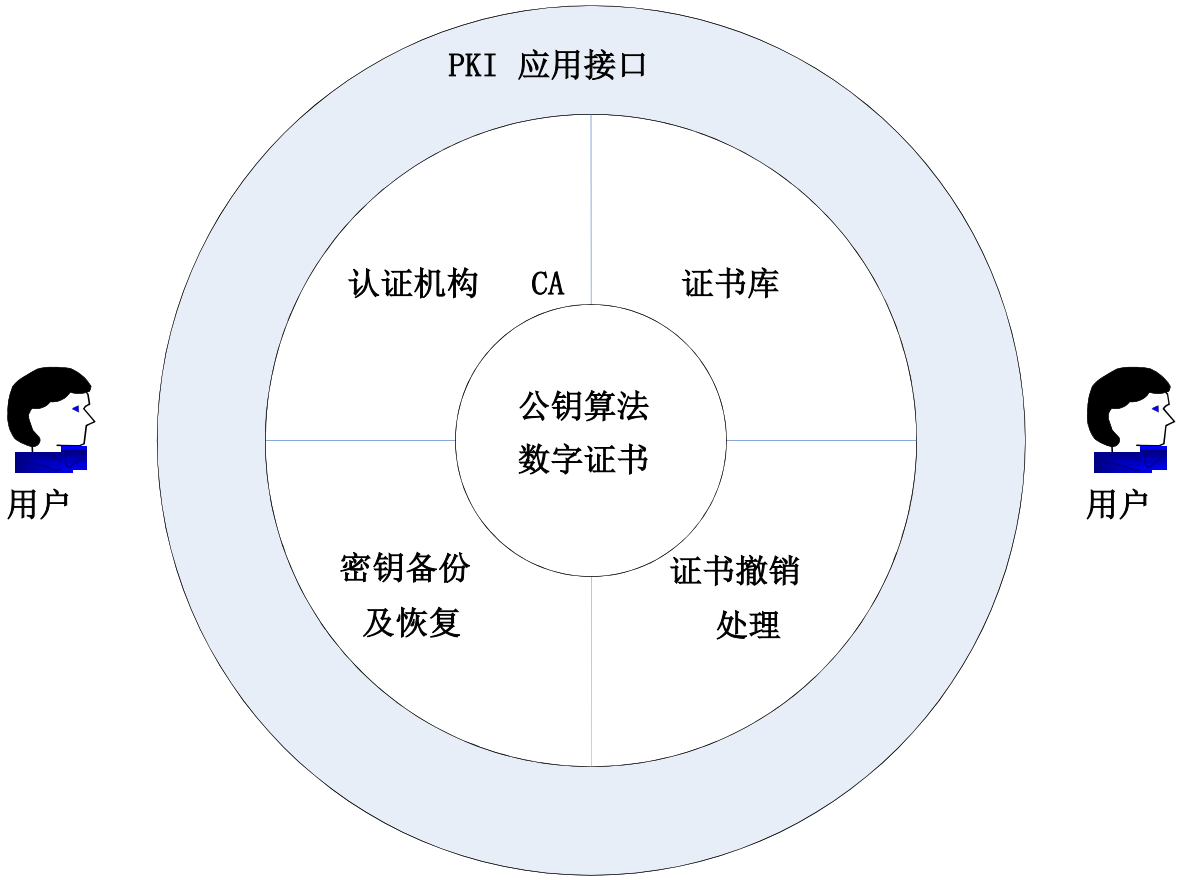
基于数字证书进行身份认证的过程



4.3 公钥基础设施PKI

- PKI是一种遵循一定标准的密钥管理基础平台，为所有网络应用提供加密和数字签名等密码服务所必需的密钥和证书管理。
  - PKI就是利用公钥理论和技术建立的提供安全服务的基础设施。
  - 用户可利用PKI平台提供的服务进行安全的电子交易、通信和互联网上的各种活动。

4.3.1 PKI体系结构

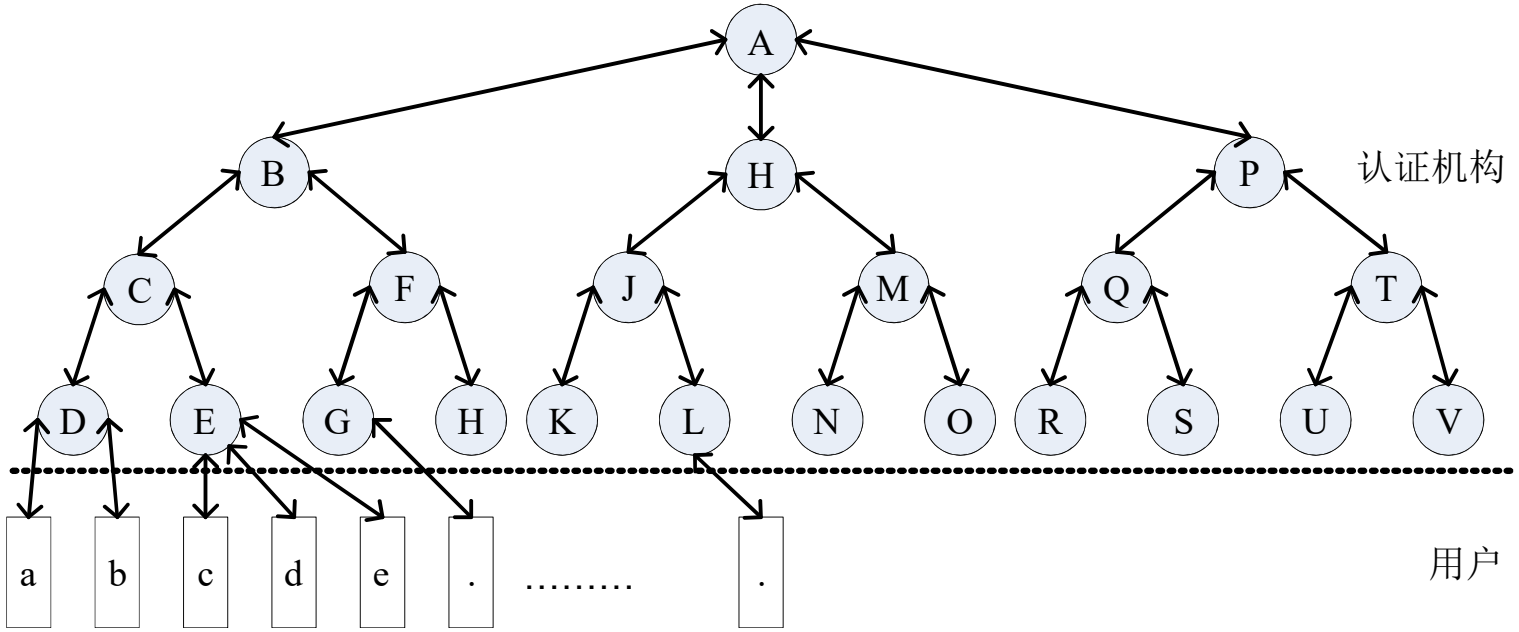


4.3.2 基于X.509的PKI系统

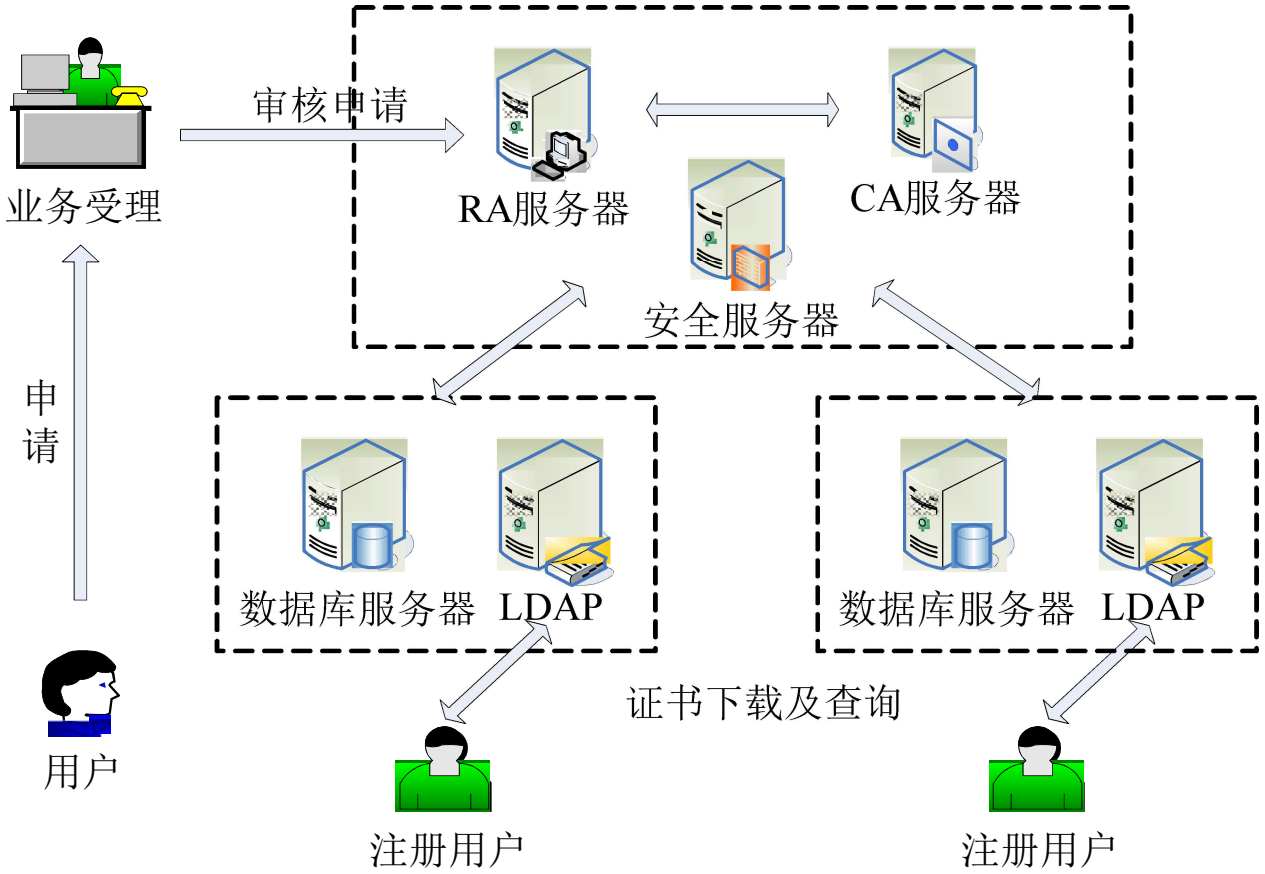
- X.509是国际电信联盟-电信（ITU-T）部分标准和国际标准化组织（ISO）的证书格式标准。
- X.509的主要作用
  - 确定了公钥证书结构的基准
  - X.509 V3证书包括一组按预定义顺序排列的强制字段，还有可选扩展字段，即使在强制字段中，X.509证书也具有很大的灵活性，因为它为大多数字段提供了多种编码方案。

X.509的CA目录的层次结构

用户a的证书链可以使用下面的形式表达：
KR_A《CA_B》KR_B《CA_C》KR_C《CA_D》KR_D《CA_a》



一个典型的PKI模型


审核申请
业务受理
RA服务器
CA服务器
安全服务器
申请
数据库服务器
LDAP
数据库服务器
LDAP
证书下载及查询
用户
注册用户
注册用户

PKI系统功能

- 接收验证用户数字证书的申请；
- 确定是否接受用户数字证书的申请；
- 向申请者颁发（或拒绝颁发）数字证书；
- 接收、处理用户的数字证书更新请求；
- 接收用户数字证书的查询、撤销；
- 产生和发布证书的有效期；
- 数字证书的归档；
- 密钥归档；
- 历史数据归档。

课堂问题

- CA证书是不是安全，主要取决什么？ （多选）
  - A. 可信第三方公私钥的安全性
  - B. 用户CA证书的相应私钥的机密性
  - C. CA证书被盗
  - D. CA证书使用过于频繁

Thanks!