第15章 身份认证

一 身份证明

二 口令认证系统

三 一次性口令认证技术

四 个人生物特征的身份认证技术

五 基于证书的认证

六 智能卡技术及应用

第15章 身份认证

一 身份证明

二 口令认证系统

三 一次性口令认证技术

四 个人生物特征的身份认证技术

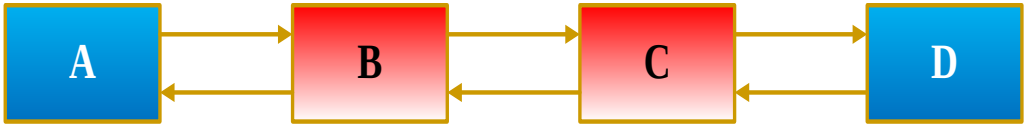
五 基于证书的认证

六 智能卡技术及应用

15.1 身份认证概述

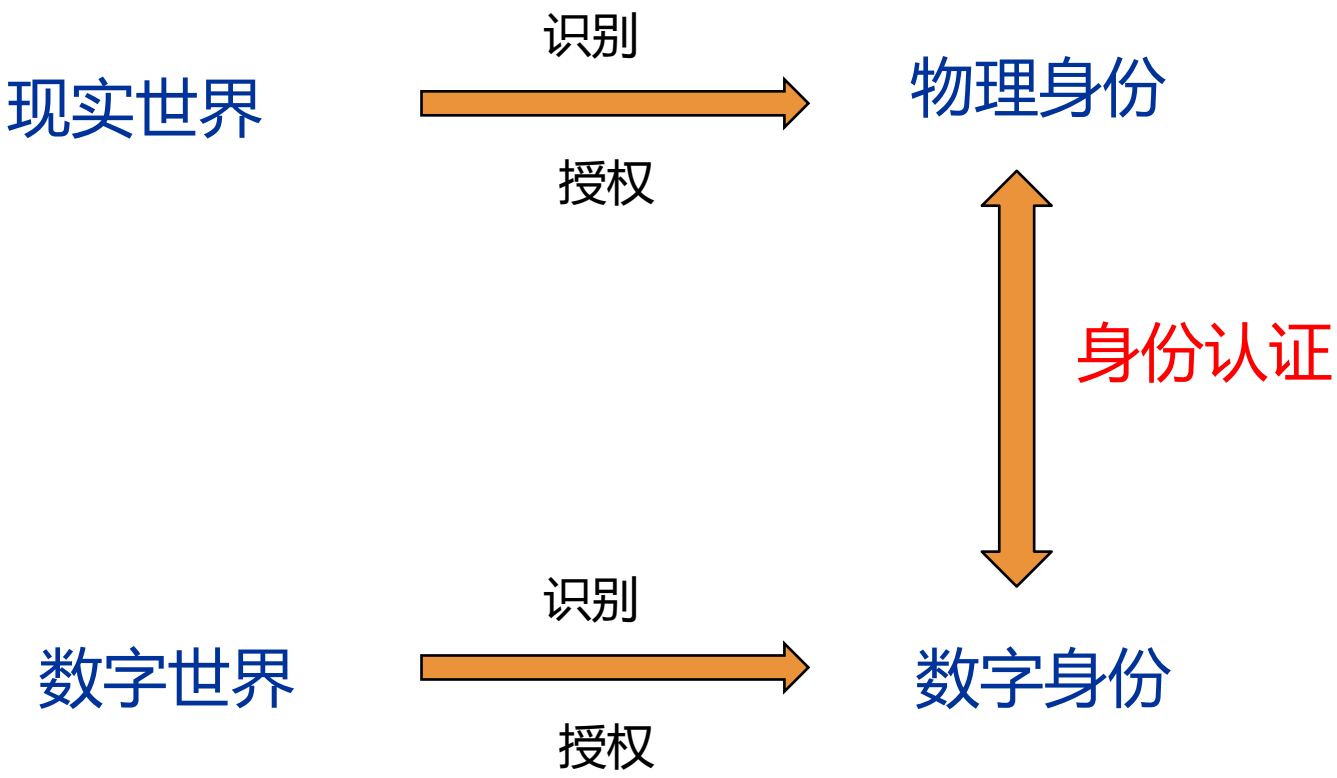
1. 中间人欺诈

2. 中间人合伙欺诈



4. 多身份欺诈

15.1 身份认证概述



15.1 身份认证概述

必要性

- 防止身份欺诈
- 通信和数据系统的安全性
- 计算机的访问和使用
- 安全区的出入

热点

实现安全、准确、高效和低成本的数字化认证

15.1 身份认证概述

- 在现实生活中，我们个人的身份主要是通过各种证件来确认的，比如：身份证、户口本等。
- 认证是对网络中的主体进行验证的过程，用户必须提供他是谁的证明。
- 认证(authentication)是证明一个对象的身份的过程。授权(authorization)是决定把什么特权附加给该身份。

15.1.2 身份证明系统的组成

示证者P(Prover)	出示证件的人
验证者V(Verifier)	检验证件的合法性和正确性
攻击者A(Attacker)	窃听并伪装示证者骗取验证者的信任

- 必要时，有第四方参与，即可信者，参与纠纷调解

身份证明系统的组成

- 实体认证: 对通信主体的认证，识别通信双方的真实身份，防止假冒

- 消息认证: 对通信数据的认证，验证收到的消息确实是来自真正的发送方且未被修改的消息

15.1.2 身份证明系统的要求

1.最大可能正确识别合法示证者

2.不具有可传递性

3.最大可能防止攻击者伪装欺骗

4.计算有效性

5.通信有效性

6.秘密参数能安全存储

7.交互识别

8.第三方实时参与

9.第三方的可信性

10.可证明安全性

15.1.3 身份证明的基本分类

你是否是你
所声称的你?

1.身份验证

（Identity verification）

2.身份识别

（Identity recognition）

我是否知
道你是谁?

15.1.4 实现身份证明的基本途径

通过这三者之一或组合实现

服务质量评价指标：拒绝率（FRR）、漏报率（FAR）

第15章 身份认证

一 身份证明

二 口令认证系统

三 一次性口令认证技术

四 个人生物特征的身份认证技术

五 基于证书的认证

六 智能卡技术及应用

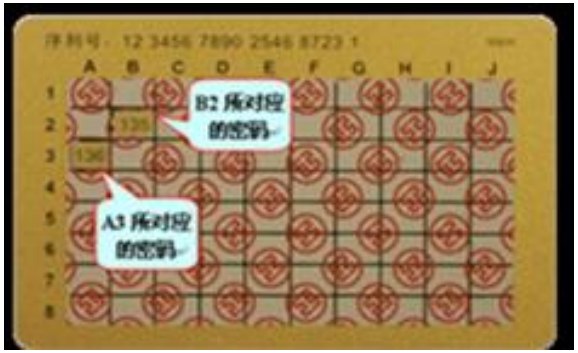
15.2.1 口令认证系统概述

定义：根据已知事物验证身份的方法，被广泛使用。

选择原则：易记；难以猜中或发现；能抵御蛮力破解攻击。

防止泄露的措施：

- 个人身份和口令用软件加密，如Bell的UNIX系统就用加密方式。
- 采用通行短语（Pass Phrases）代替口令，通过密钥碾压（Key Crunching）技术生成较短的随机性密钥。



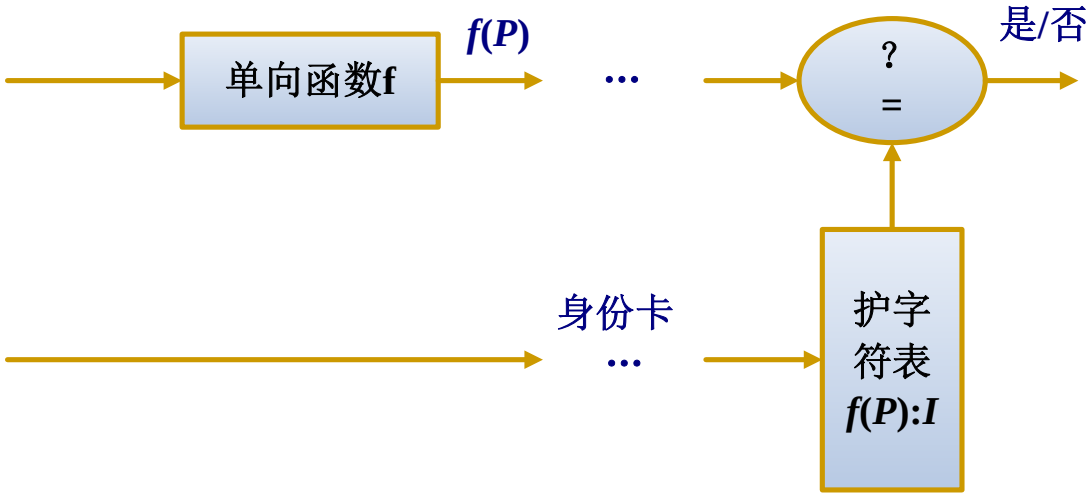
15.2.1 口令认证系统概述（续）

口令分发系统的安全性也不容忽视

- 通常采用邮寄方式。
- 银行系统通常采用夹层信封，由计算机将护字符印在中间纸层上，只有拆封才能读出。
- 在使用口令时，我们还应注意防止别人骗取口令。
- 为了安全，系统常常限定尝试输入口令的次数。

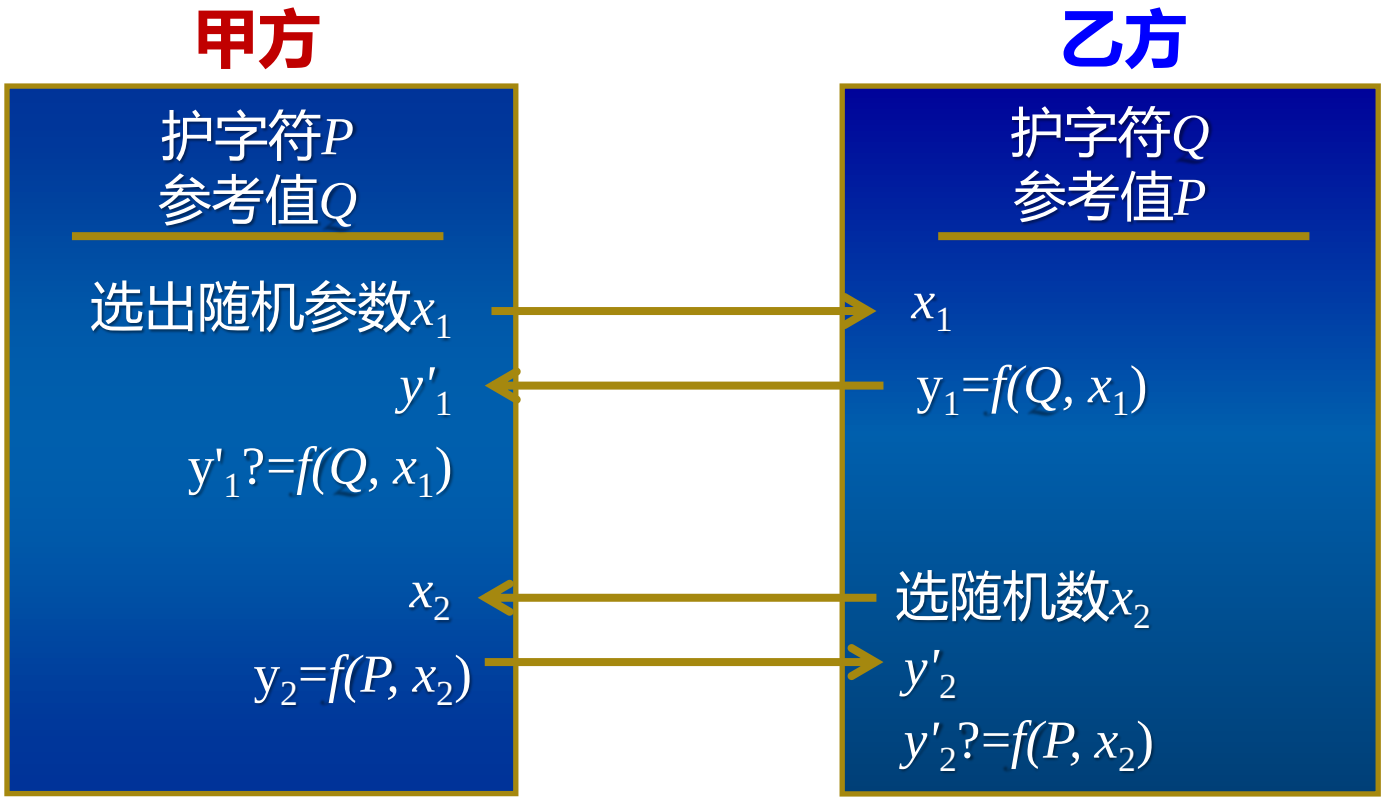
15.2.1 口令认证系统概述（续）

一种单向函数检验口令框图



- 系统检验用户的口令。
- 有时需双向验证，用户也要检验系统口令。

15.2.2 一种双方互换口令的安全验证方法



- 甲乙分别以P、Q作为护字符。
- 为验证，双方彼此知道对方的口令，并通过一个单向函数f进行响应。

15.2.3 口令的控制措施

15.2.3 口令的检验

口令的检验

- 用户选择口令，程序检验，若易于猜中须重新选择
- 可猜中性与安全性之间折中

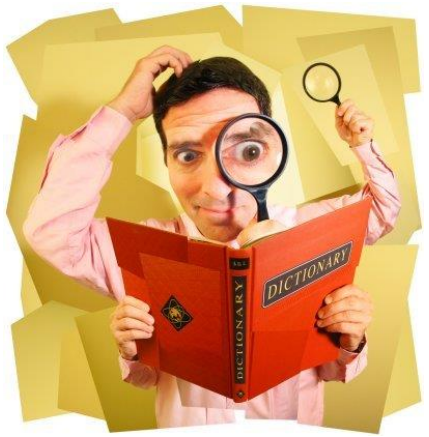
易猜测的口令

- 使用用户名或其变换形式作为口令。
- 使用自己或者亲友的生日作为口令
- 使用常用的英文单词作为口令
- 使用5位或5位以下的字符作为口令

15.2.3 口令的检验

安全的口令

- 位数>6位。
- 大小写字母混合。
- 字母与数字混合。
- 口令有字母、数字以外的符号。



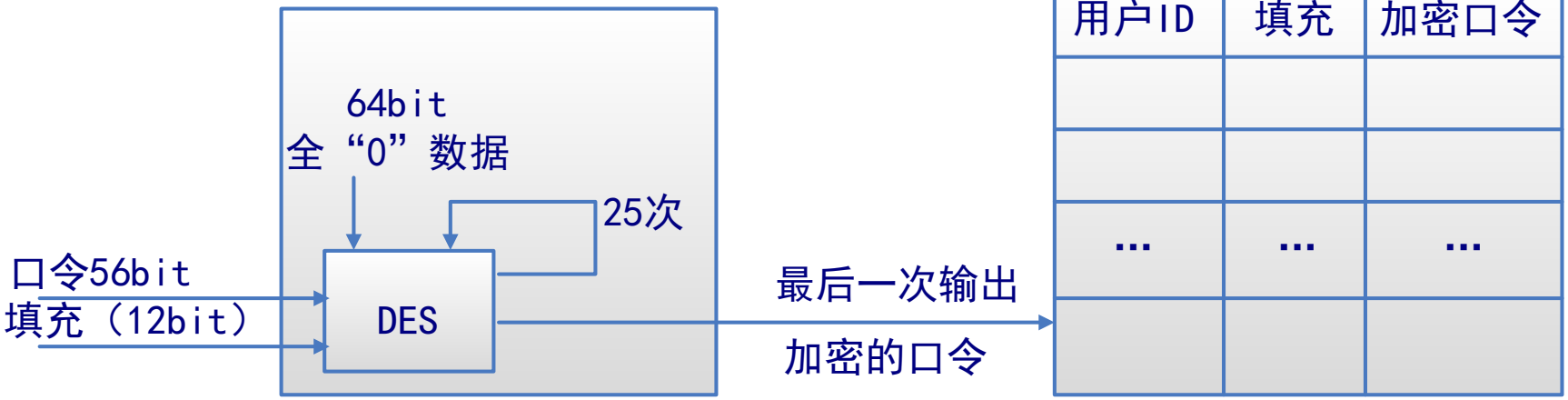
15.2.4 口令的安全存储

一般方法

- 以口令加密方式存储
- 存储口令的单向杂凑

UNIX系统中的口令存储

- 口令为8个字符：7bitASCII码（56bit）+12bit填充（用户输入口令的时间）
- 第一次输入64bit全0进行加密，再以第一次的加密结果为输入，迭代25次
- 最后一次变换成11个字符作为口令密文。
- 检验时用户发送ID和口令。



15.2.4 口令的安全存储

用智能卡令牌（Token）产生一次性口令

- 本质上是由一个随机数生成器产生的，可以由安全服务器用软件生成。
- 一般用于第三方认证。
- 即使口令被截获也难以使用。
- 用户需要输入PIN码（持卡人知道）难以用来进行违法活动。
- 美国的Secure Dynamics Inc.的Secure ID和RSA公司的SecurID令牌。

第15章 身份认证

一 身份证明

二 口令认证系统

三 一次性口令认证技术

四 个人生物特征的身份认证技术

五 基于证书的认证

六 智能卡技术及应用

15.3 一次性口令认证

- 背景：信息化水平的提高，电子商务的普及，成为黑客的攻击对象。
- 攻击的主要方式：窃取系统口令文件和窃听网络连接，以获取用户ID和口令。
- 攻击的主要目的：设法得到用户ID和用户密码。


15.3 一次性口令认证

- OTP(One Time Passord）认证: 确保在每次认证中所使用的口令不同，以对付重放攻击。
- OTP 的主要思路：在登陆过程中加入不确定因素，使每次登录过程中传送的信息都不相同，以提高登录过程安全性。
- OTP认证机制：
  - 挑战/响应机制
  - 口令序列机制
  - 时间同步机制
  - 事件同步机制

15.3.1 挑战/响应机制-流程

15.3.1 挑战/响应机制-举例

输入 Challenge

输入 PIN 来启动认证卡

login: Smith

challenge: 6729330

response: 2188655

输入 response

开启认证卡电源

你现在已认证成功 ！

15.3.1 挑战/响应机制-优缺点

优点

- 可以保证很高的安全性
- 没有同步的问题
- 一个认证卡可以支持不同的认证服务器系统

缺点

- 需多次手工输入，易造成失误
- 客户端和服务器交互次数多

15.3.2 口令序列机制-原理

口令序列(S/key)机制是挑战/响应机制的一种实现

- 在口令重置前，允许用户登录n次，那么主机需要计算出$F_n(x)$，并保存该值，其中F为一个单向函数。
- 用户第一次登录时，需提供$F_{n-1}(x)$。系统计算$F(F_{n-1}(x))$，并验证是否等于$F_n(x)$。如果通过则重新存储$F_{n-1}(x)$。下次登录时，则验证$F_{n-2}(x)$，依此类推。
- 计算顺序：$F_1(x) \rightarrow F_2(x) \ldots F_{n-1}(x) \rightarrow F_n(x)$
- 口令使用顺序：n　n-1　2　1

15.3.2 口令序列机制

说明

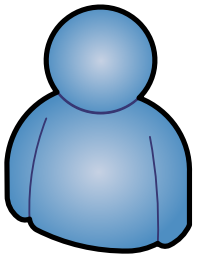
- 为方便用户使用，主机把$F_{n-1}(x) \sim F_1(x)$计算出来，编成短语打印在纸条上。用户只需按顺序使用这些口令登录即可。
- 纸条一定要保管好，不可遗失。
- 由于n有限，用户用完这些口令后，需重新生成新口令序列。

缺点

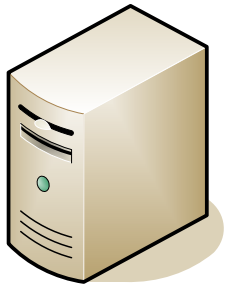
- 只支持服务器对用户的单方面认证，无法防范假冒的服务器欺骗合法用户。
- 当迭代值递减为0或用户的口令泄露后必须对S/key系统重新进行初始化。

15.3.3 时间同步机制-流程

以用户登录时间作为随机因素



用户



服务器

3 将动态口令Rc传送给服务器

5.服务器返回认证结果

4 服务器根据登录ID，取出密钥K,根据当前时间和K生成Rs，比较Rc与Rs

1 用户登陆 启动令牌

2 生成口令Rc

令牌由当前时间和密钥K

令牌

令牌与服务器时间一致

15.3.3 时间同步机制-优缺点

优点

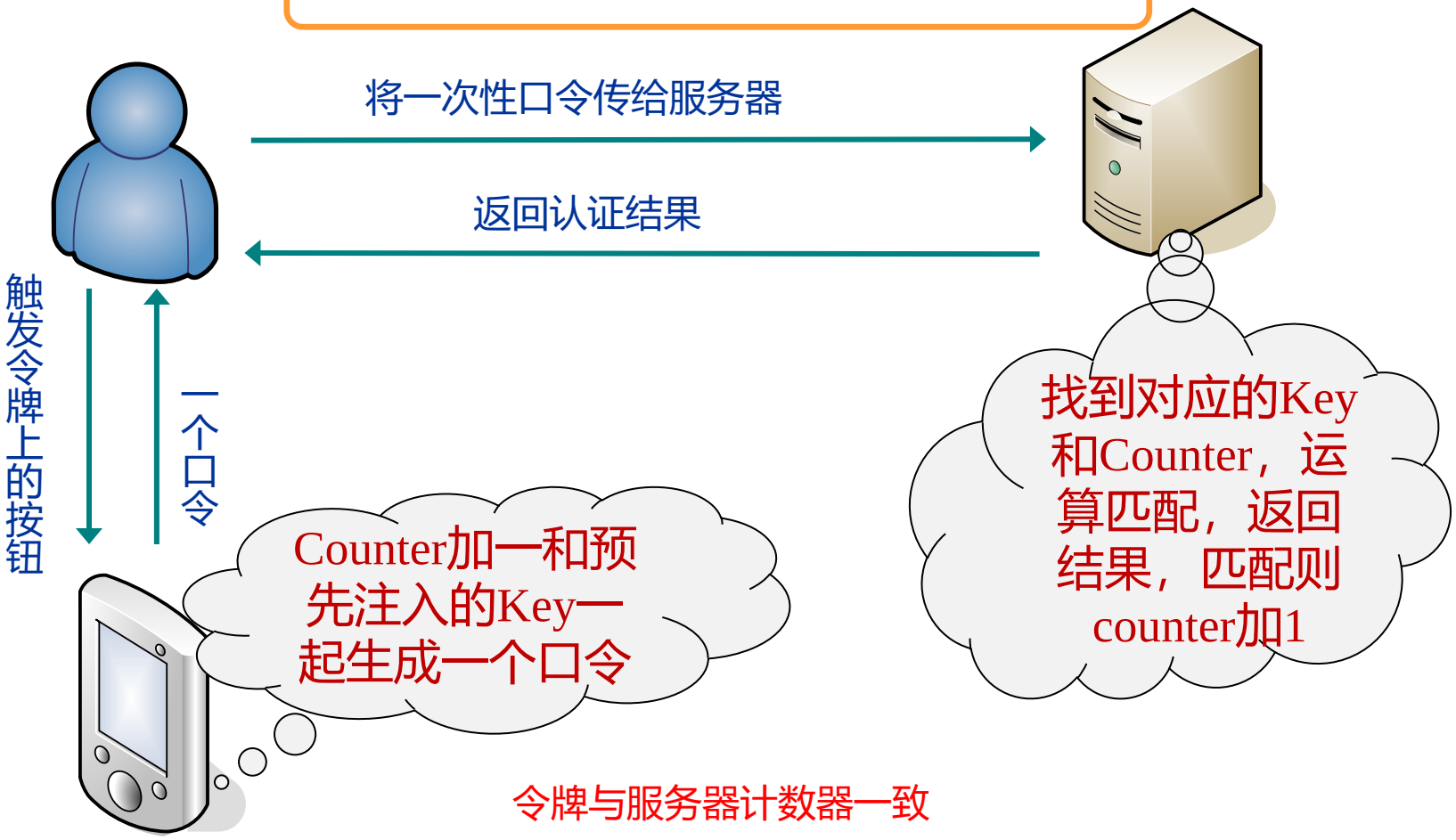
- 用户使用简单、方便，不用频繁输入数据
- 通信数据小，服务器计算量不大

缺点

- 时间同步比较困难，软件认证卡采用PC的时间，很可能随时被修改，常常需要与服务器重新对时
- 对设备的时钟精度要求比较高，设计成本较高
- 安全性不如挑战/响应机制

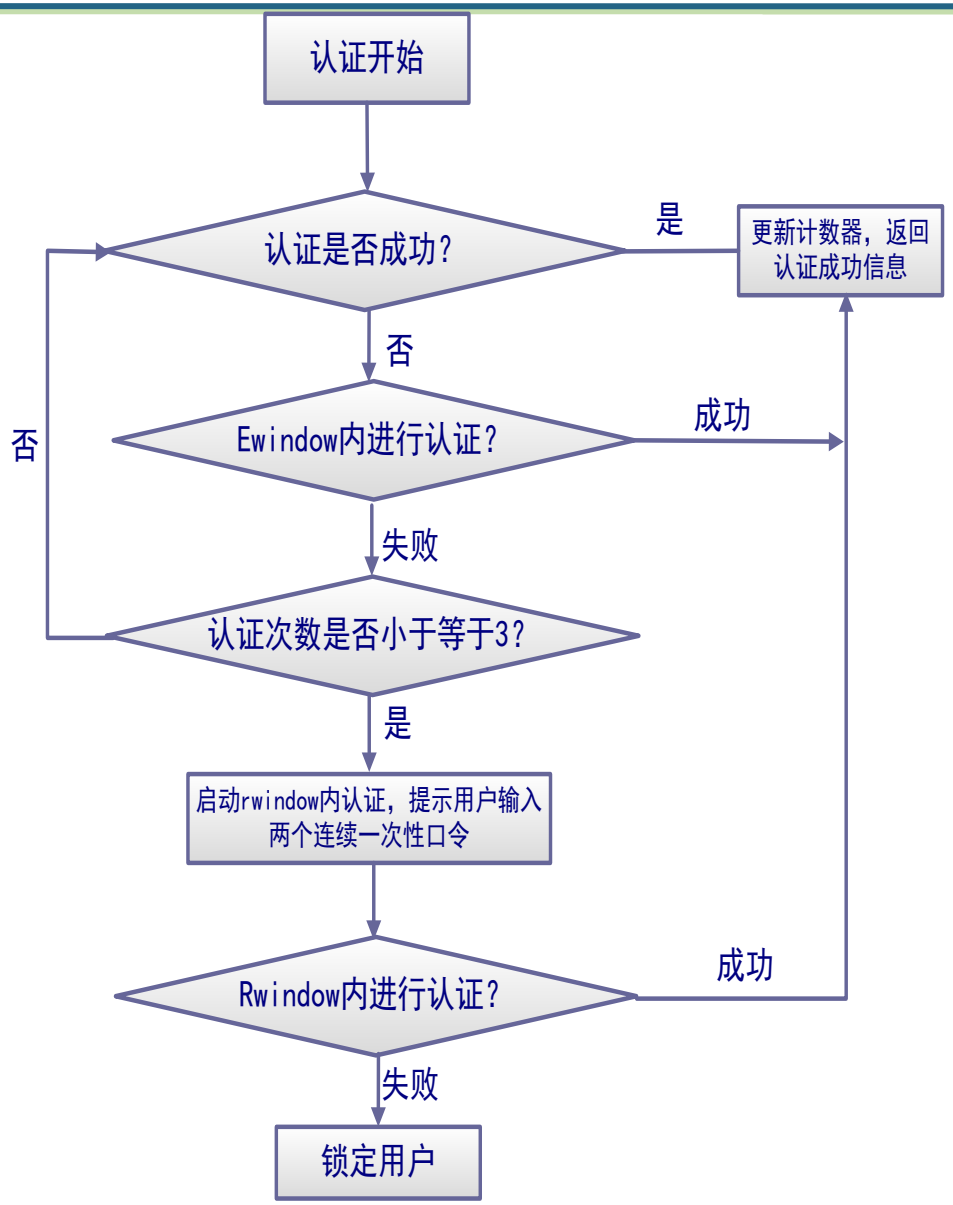
15.3.4 事件同步机制-流程

以用户使用次数作为随机因素



令牌与服务器计数器一致

15.3.4 事件同步机制-重同步方法



- 用户和服务器很容易失去同步
- 解决：设置窗口值**ewindow**

- 令牌Counter远远超前于服务器Counter，靠窗口值**rwindow**重同步
- 令牌计数器超出ewindow范围启用rwindow机制
- 超过rwindow则只能去注册中心办理重同步业务

15.3.4 事件同步机制-优缺点

优点

- 用户操作简单
- 一次认证过程通信量小
- 可以防止小数攻击
- 系统实现较简单，对时钟精度没要求

缺点

- 服务器计算量稍大

15.3.5 几种一次性口令实现机制的比较

- 时间同步和事件同步的优势比较明显，目前市场上很多公司的产品采用的大都是基于时间同步和事件同步的方案。

机　制	通 信 量	系统实现复杂度	机制安全性	服务器计算量
挑战/响应	较大	较简单	较好	较大
S/key	较大	较简单	较差	较大
时间同步	较小	较复杂	较好	较小
事件同步	较小	较简单	较好	适中

第15章 身份认证

一 身份证明

二 口令认证系统

三 一次性口令认证技术

四 个人生物特征的身份认证技术

五 基于证书的认证

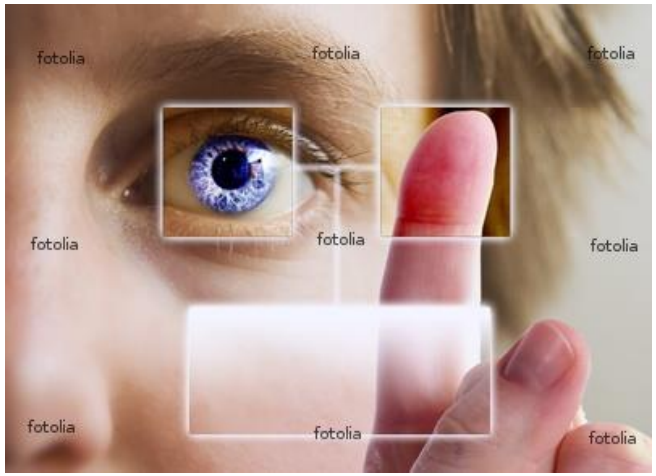
六 智能卡技术及应用

15.4 个人生物特征的身份认证技术

- 安全性要求高时，护字符和持证等提供的安全性不能满足要求；
- 新的生物统计学（Biometrics）方法正在成为实现个人身份认证最简单而安全的方法。

优点

- 可信度高
- 个人特征因人而异，难以伪造
- 随身携带，不易丢失
- 已用于刑事案件侦查



15.4 个人生物特征的身份认证技术

生物识别依据人类自身所固有的生理或行为特征

- 生理特征：与生俱来，多为先天性的，如指纹、视网膜、面容、掌纹、声音、手形等；
- 行为特征：则是习惯使然，多为后天性的，如笔迹、步态、签名等。

- 最可靠的生物识别方式：视网膜识别、指纹识别

15.4.1 手书签字验证

- 依据：每个人的签名动作和字迹具有明显的个性，手书签名可作为身份验证的可靠依据。
- 发展：机器自动识别手书签字的研究，是模式识别的重要课题之一。

应用举例

- 英国物理实验室的VERISIGN系统
- IBM公司的加速度动态识别方法
- Cadix公司的笔迹识别系统（软件Penop）

可能的伪造签字类型

- 不知真迹时按得到的信息随手签的字
- 已知真迹时的模仿签字或映描签字

15.4.2 指纹验证

依据：没有两个人（包括孪生儿）的指纹完全相同，且指纹形状不随时间变化，提取方便。

应用举例

- 美国Fingermatrix公司指纹阅读机（Ridge Reader）
- 个人接触证实PTV-Personal Touch Verification系统
- Identix公司的Identix System
- FBI已成功将小波理论应用于压缩和识别指纹图样
- 自动指纹身份识别系统（AFIS）

15.4.3 语音验证

- **依据：**每个人的语音都各有其特点，而人对于语音的识别能力是很强的，适用于个人身份认证。
- **发展：**机器自动识别语言认证的研究，主要依据的语音特征为语声纹。

应用举例

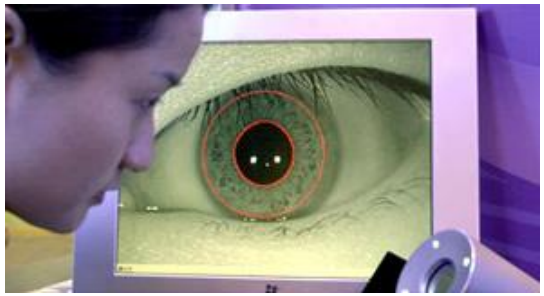
- 美国Texas仪器公司曾设计一个16个字集的系统
- 美国AT&T公司为一种语音口令系统（VPS）
- 科大讯飞的语音识别
- 语声纹识别技术可用于防止黑客进入语音函件和电话服务系统

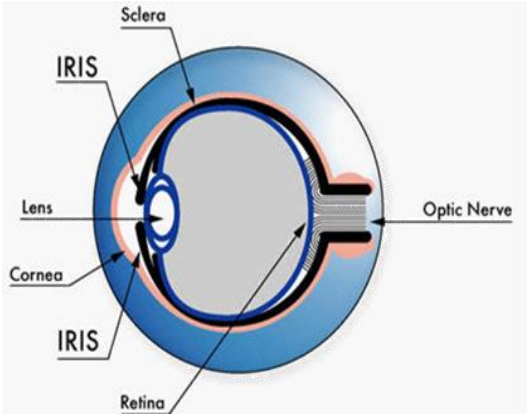
15.4.4 视网膜图样验证

- **依据：**人的视网膜血管图样（即视网膜脉络）具有良好的个人特征。

发展

- 视网膜血管图样的身份识别系统。
- 系统的成本较高，目前仅在军事系统和银行系统中采用。





15.4.5 虹膜图样验证

- **依据：** 具有个人特征，可以提供比指纹更细致的信息。
- **发展：** 视网膜血管图样的身份识别系统。

应用举例

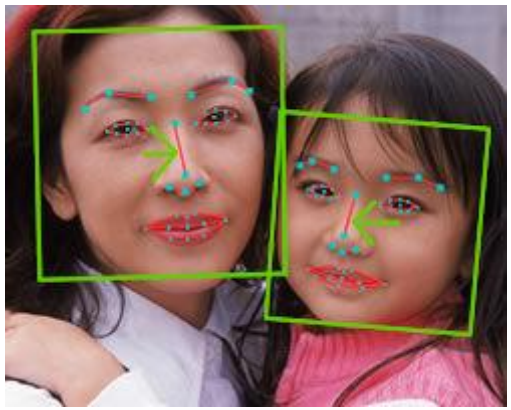
- 可用于安全入口、接入控制、信用卡、POS、ATM、护照等的身份认证
- 美国IriScan Inc.已研发出此种产品

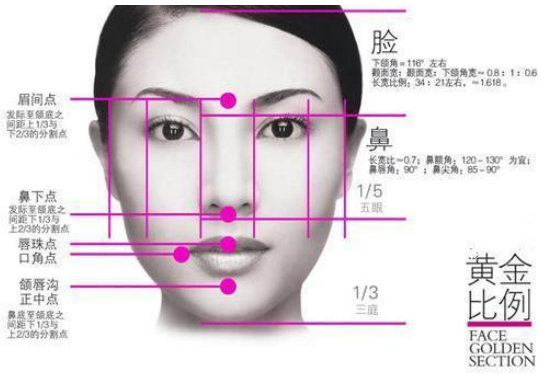
15.4.6 脸型验证

- **依据：**用照片识别人脸轮廓（还可扩展到对人耳形状的识别）。
- **发展：**脸型自动验证系统，用图像识别、神经网络和红外扫描探测人脸的“热点”进行采样、处理并提取图样信息。

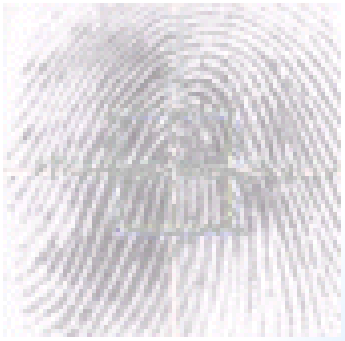
应用举例

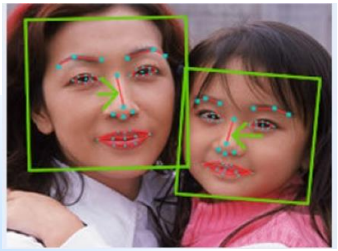
- 高铁站的人脸识别
- 支付宝的人脸支付





基于生物特征的身份认证的优点和不足





优点：

1. 绝对无法仿冒的使用者认证技术。

缺点：

1. 较昂贵。
2. 不够稳定(辩识失败率高)。

15.4.7 身份证明系统的设计

美国国家标准局（NBS）的自动身份验证技术的评价指南提出了下述12个需要考虑的问题：

1. 抗欺诈能力
2. 伪造容易程度；
3. 对设陷的敏感性；
4. 完成识别的时间；
5. 方便用户；
6. 识别设备及运营的成本；
7. 设备使用的接口数目；
8. 更新所需时间和工作量；
9. 所需计算机系统的处理工作；
10. 可靠性和可维护性；
11. 防护器材费用；
12. 分配和后勤支援费用。

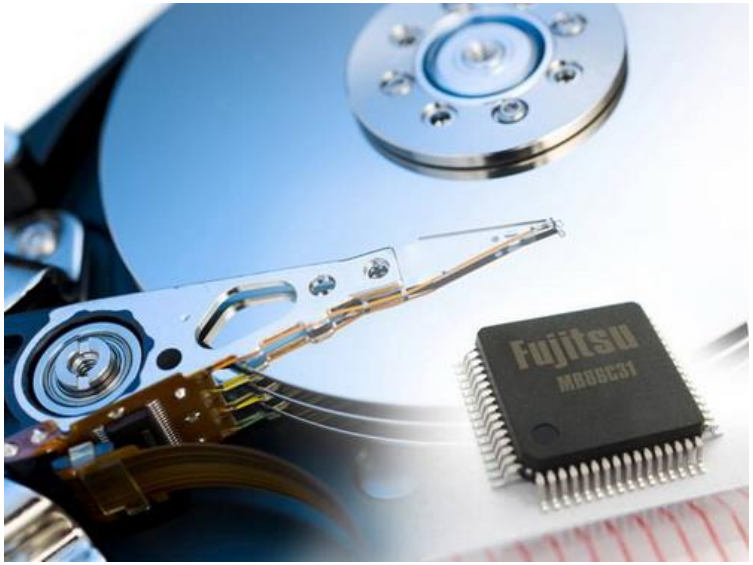
主要考虑

- 设备系统强度
- 用户可接受性
- 系统成本

第15章 身份认证

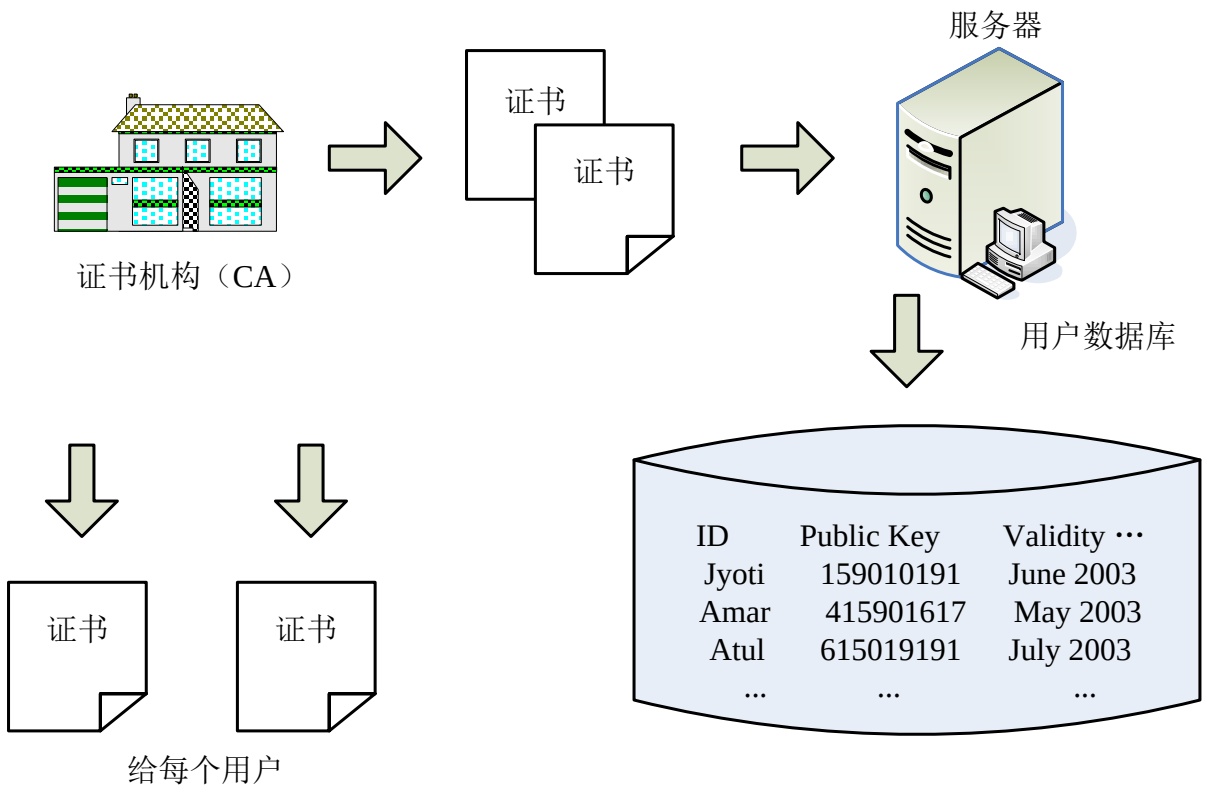
15.5.1 简介

- 基于证书比基于口令的认证机制更安全。
- 基于证书的认证采用公私钥密码机制，破解难度更大



15.5.2 基于证书认证的工作原理

Step 1 生成、存储和发布数字证书

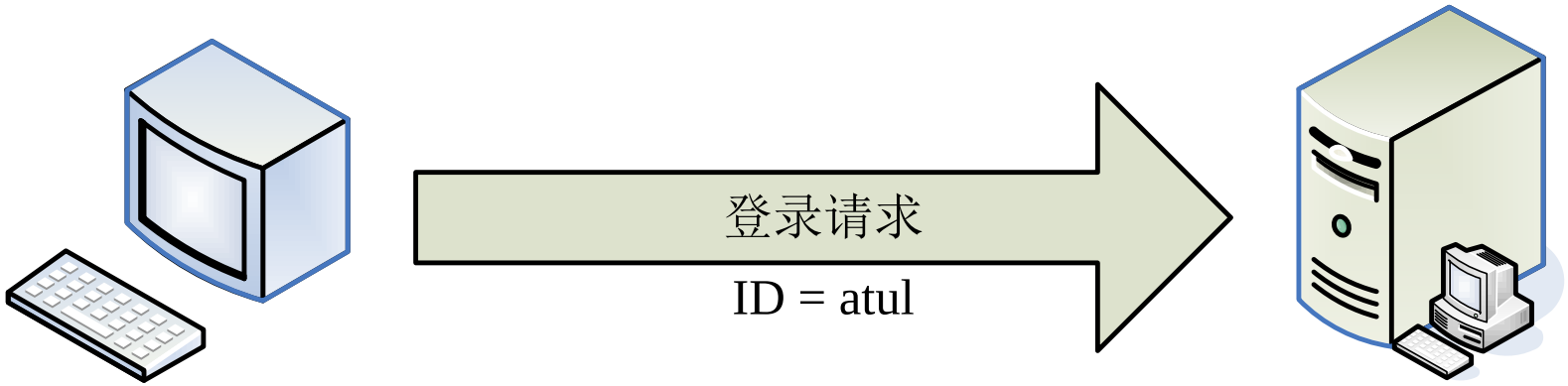


- CA为每个用户生成数字证书，将其发给相应的用户。
- 数据库存储证书的副本，便于用户登录时验证用户的证书。

数字证书的生成、存储与发布过程

15.5.2 基于证书认证的工作原理

Step 2 用户发出登录请求



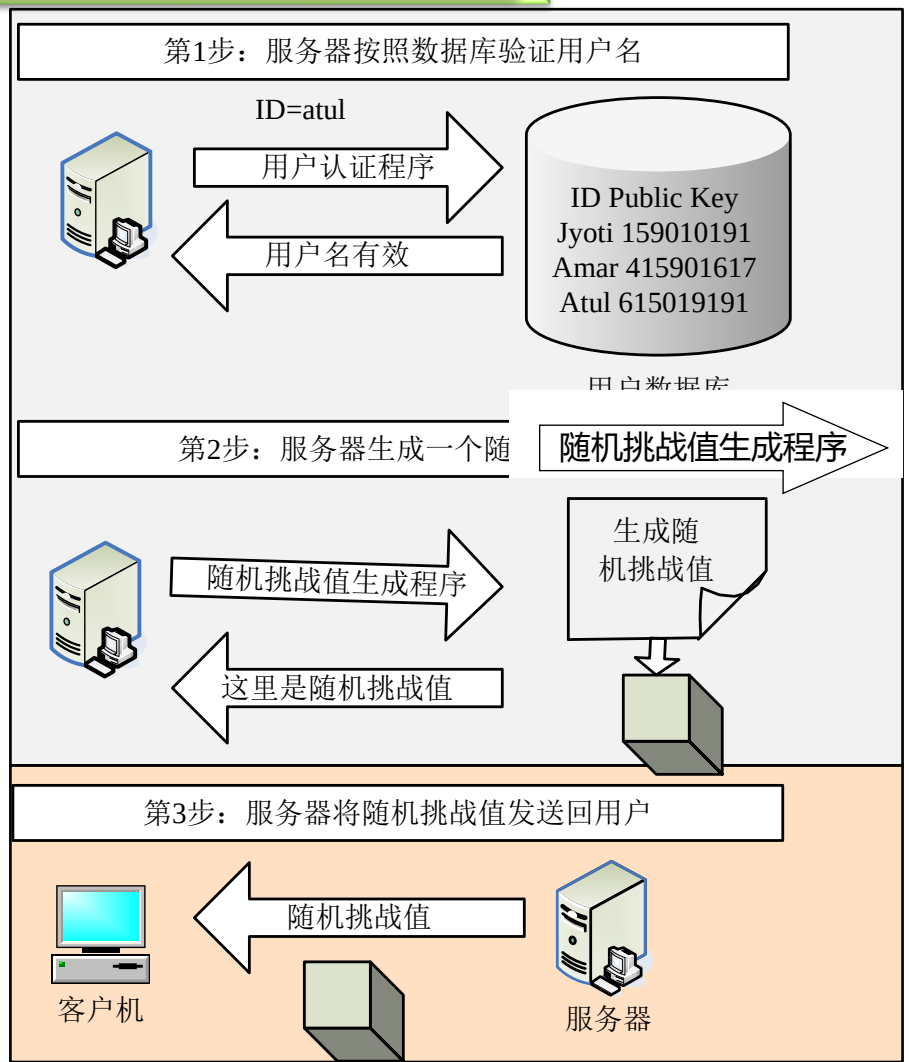
登录请求

- 登录服务器时，用户发送用户名和数字证书至服务器。

15.5.2 基于证书认证的工作原理

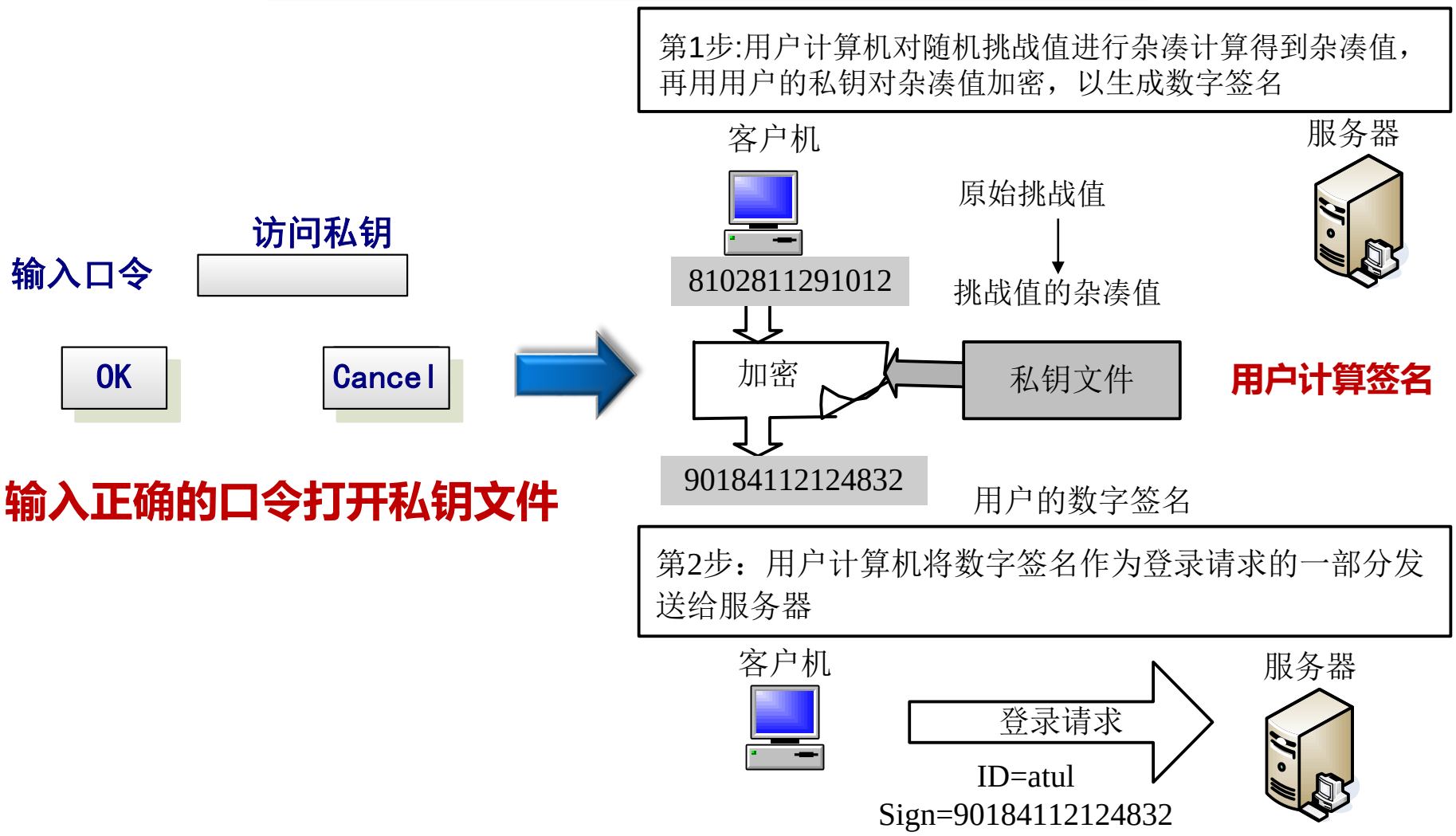
Step 3 服务器随机生成挑战值

- 服务器收到登录请求，首先验证证书，检查用户是否有效。
- 若有效，则调用伪随机数生成程序，生成一个随机挑战值。
- 服务器将随机挑战值传送到用户计算机。



15.5.2 基于证书认证的工作原理

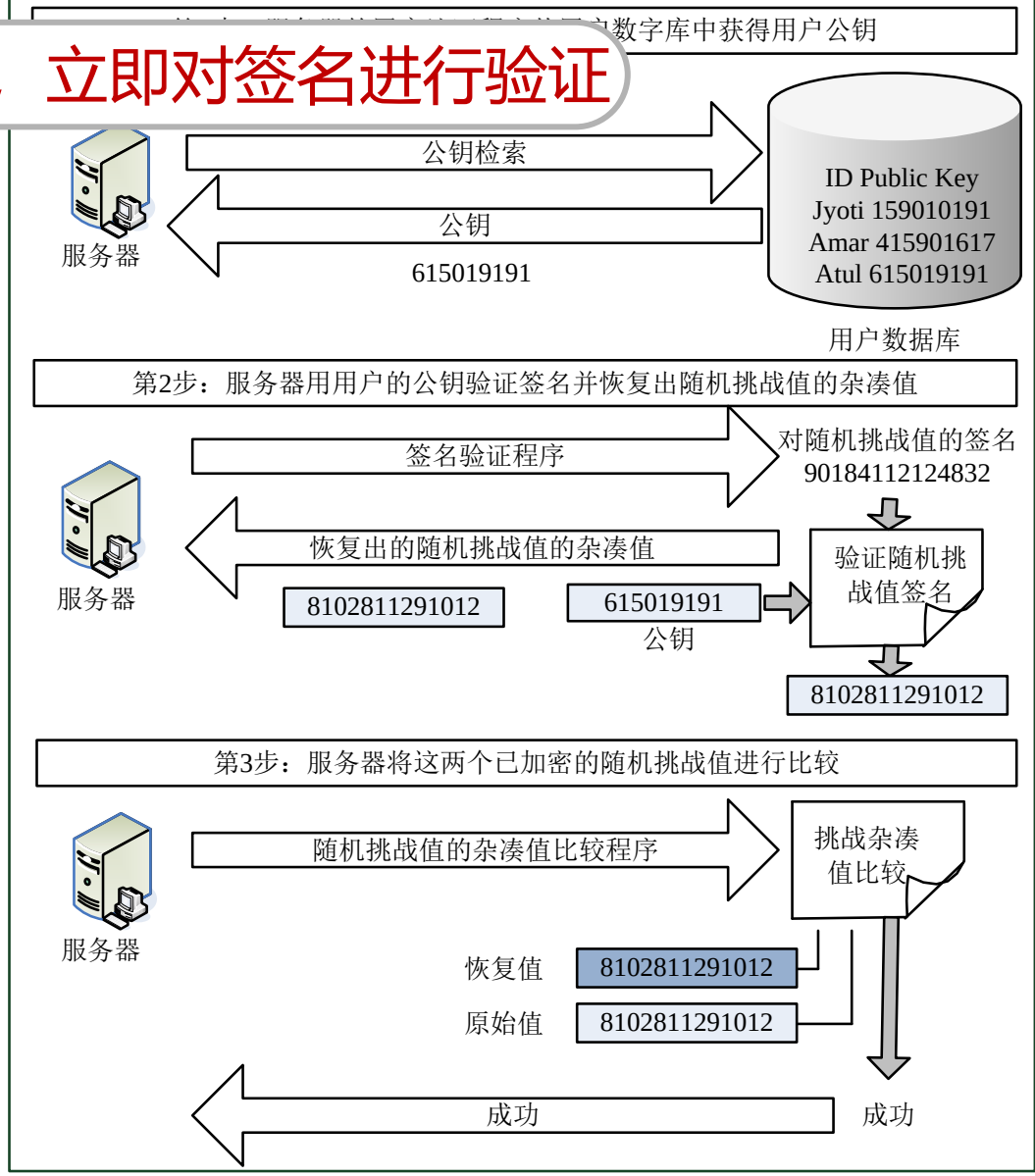
Step 4 用户对随机挑战值签名



15.5.2 基于证书认证的工作原理

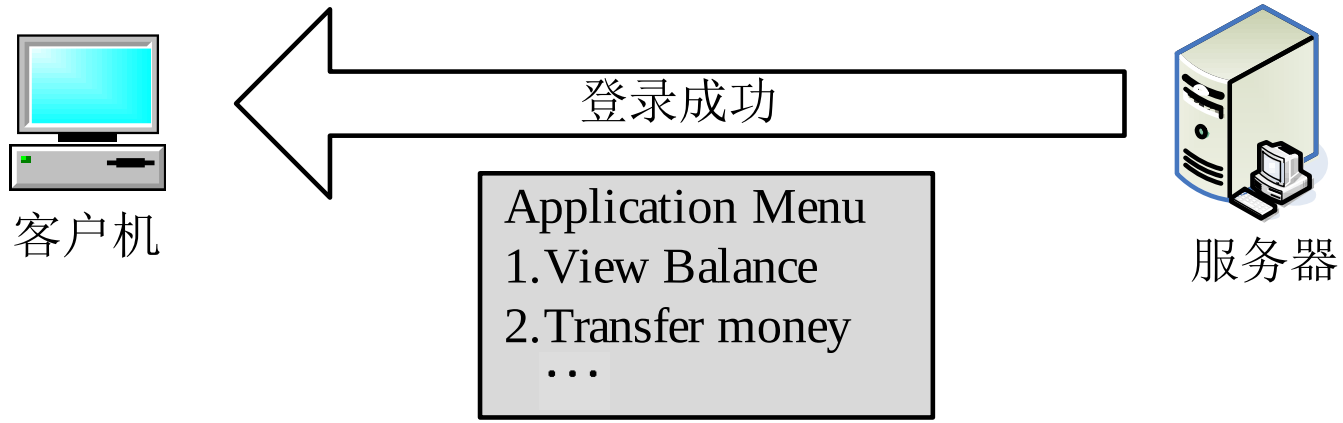
服务器在收到用户签名后，立即对签名进行验证

- 服务器的用户认证程序从用户数据库取得用户公钥；
- 服务器用用户的公钥验证此签名，并恢复出挑战值的杂凑值；
- 服务器将这两个随机挑战值的杂凑值进行比较



15.5.2 基于证书认证的工作原理

Step 5 服务器向用户返回相应的消息



- 根据上述验证是否通过，服务器向用户返回相应的消息，以通知用户认证是否成功。
- 此后，用户可使用网上银行业务开始电子商务活动。

USB Key认证

- 软硬件相结合
- 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，可以存储用户的私钥或数字证书，利用USB Key内置的密码学算法实现对用户身份的认证
- 私钥只能用于计算，不能取出
- 工行叫U盾，农行叫K宝，建行叫网银盾，光大银行叫阳光网盾

第15章 身份认证

一 身份证明

二 口令认证系统

三 一次性口令认证技术

四 个人生物特征的身份认证技术

五 基于证书的认证

六 智能卡技术及应用

15.6.1 智能卡技术概述

身份认证的工具

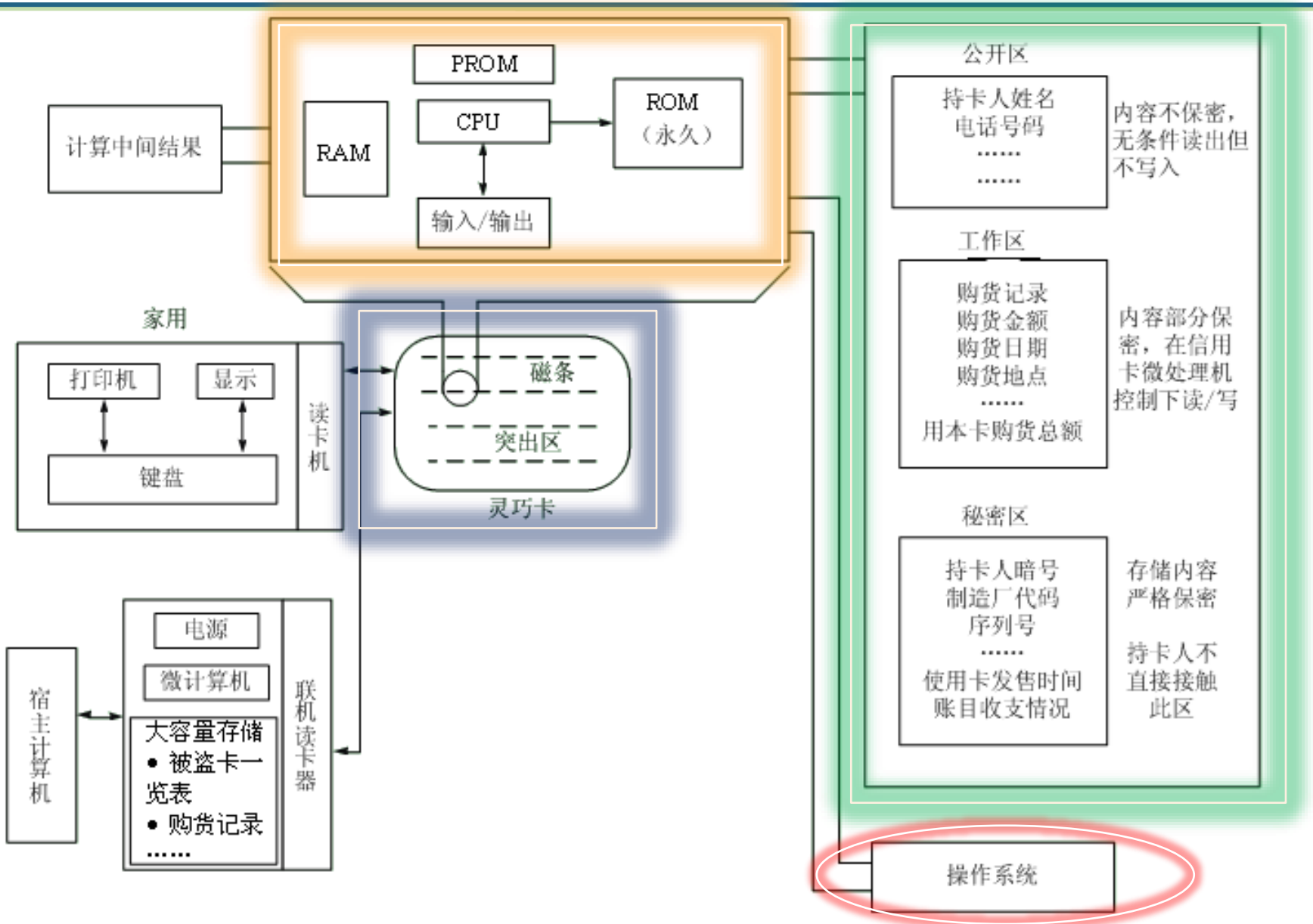
- 令牌
- 磁卡
- 智能卡（IC卡）

ID卡

磁卡与智能卡的比较

- 嵌有磁条的塑卡数据易于被转录
- 智能卡将微处理器芯片嵌在塑卡上代替无源存储磁条，安全性比无源卡有了很大提高。

15.6.2 智能卡的工作原理框图



15.6.3 智能卡的设计

智能卡发行时都要经过个人化（Personalization）或初始化（Initialization）阶段。

个人化的几个方面

- 软/硬件逻辑的格式化
- 写入系统和个人信息
- 在卡上印制名称、照片

智能卡安全设计的方面

- 芯片的安全技术
- 卡片的安全制造技术
- 软件的安全技术
- 安全密码算法
- 安全可靠协议的设计
- 管理系统的安全设计
- 智能卡防复制、防伪造

15.6.4 智能卡的应用

目前的应用方面

- 电子货币、电子商务
- 劳动保险、医疗卫生
- 银行系统
- 在付费电视系统
- 制作电子护照、二代身份证、公交一卡通、校园一卡通、电话/电视计费卡、个人履历记录、电子门禁系统等

扩大的应用范围

- 个人签字、指纹、视网膜图样等信息就可能存入智能卡，成为身份验证的更有效手段。

谢谢！