Information Security Engineering

2017.11.29

Access Control

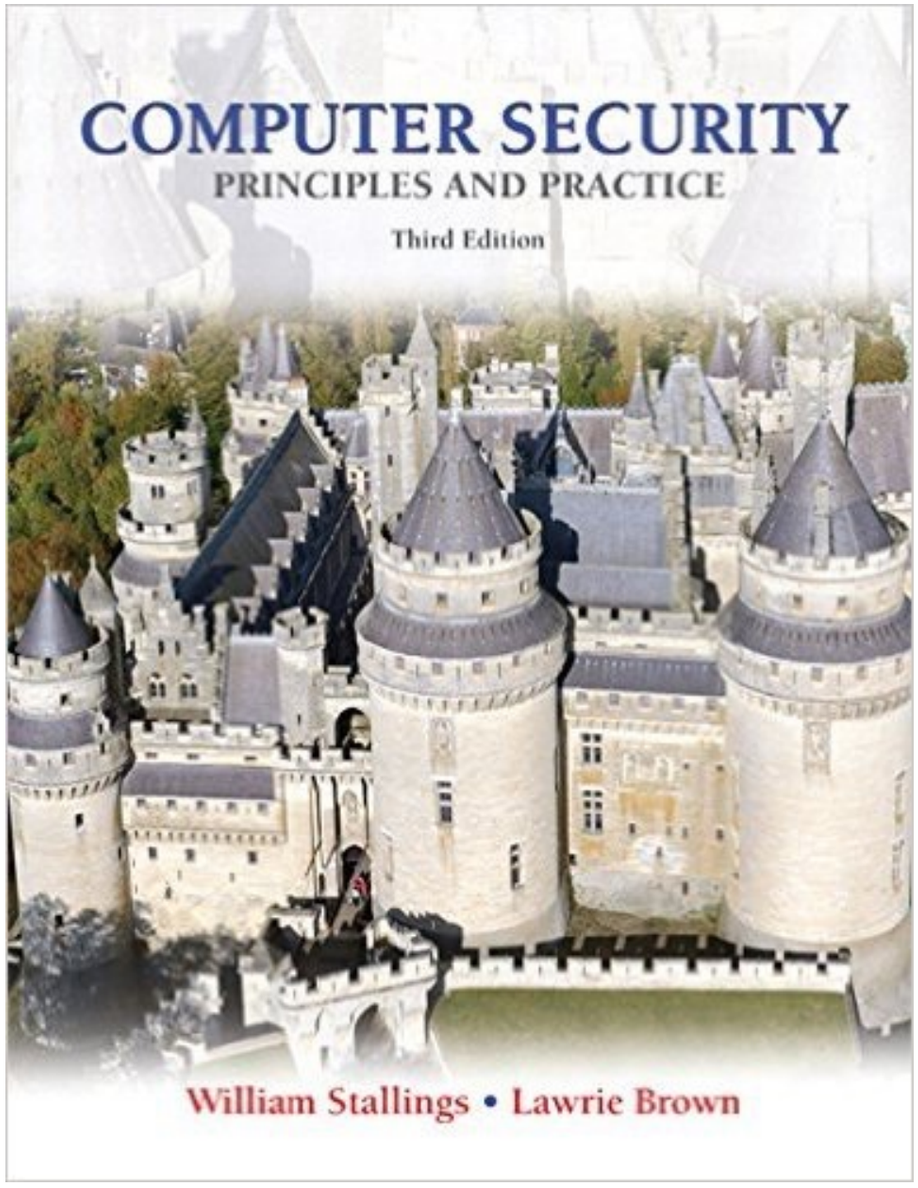
北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

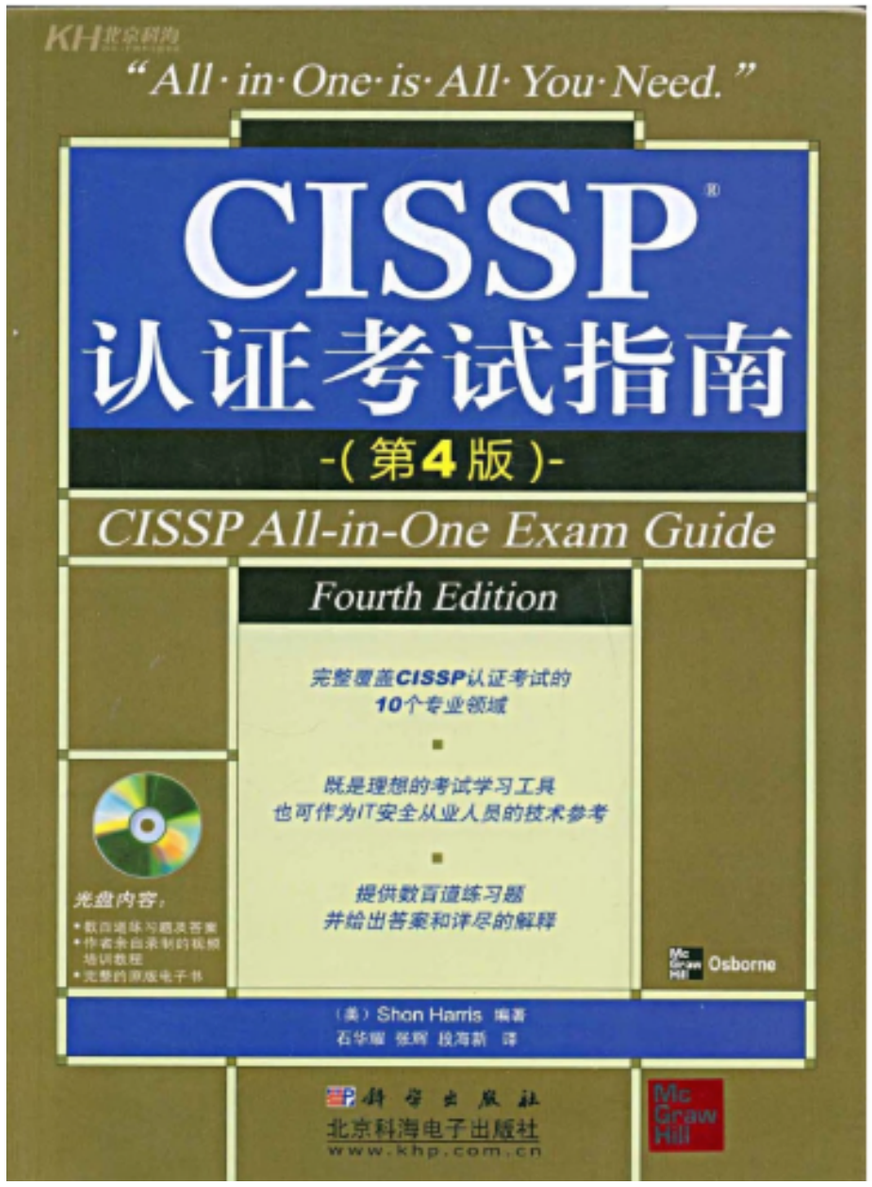
Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

主要内容

- 访问控制介绍
- 访问控制模型
- 访问控制技术
- 访问控制例子
- 身份管理介绍

参考书


COMPUTER SECURITY
PRINCIPLES AND PRACTICE
Third Edition
William Stallings • Lawrie Brown


"All·in·One·is·All·You·Need."
CISSP
认证考试指南
-(第4版)-
CISSP All-in-One Exam Guide
Fourth Edition
完整覆盖CISSP认证考试的
10个专业领域
既是理想的考试学习工具
也可作为IT安全从业人员的技术参考
提供数百道练习题
并给出答案和详尽的解释
光盘内容：
Osborne
(美) Shon Harris 编著
北京科海电子出版社
www.khp.com.cn

第四章

访问控制简介

访问控制定义

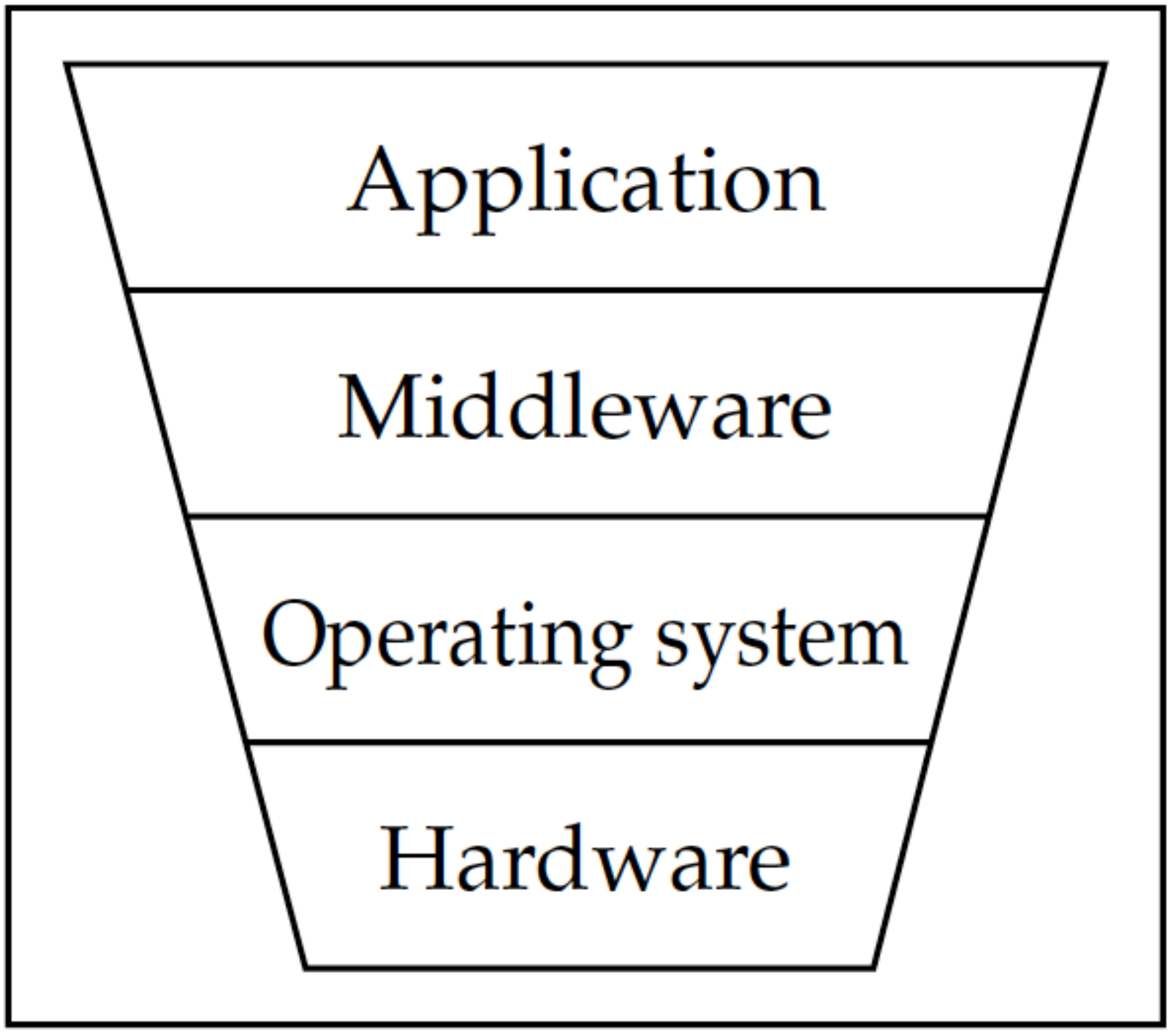
- The process of granting or denying specific requests to:
  - ✴ obtain and use information and related information processing services; and
  - ✴ enter specific physical facilities.

NIST IR 7298

- A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.

RFC 4949

不同层次的访问控制



访问控制与其余安全功能的关系

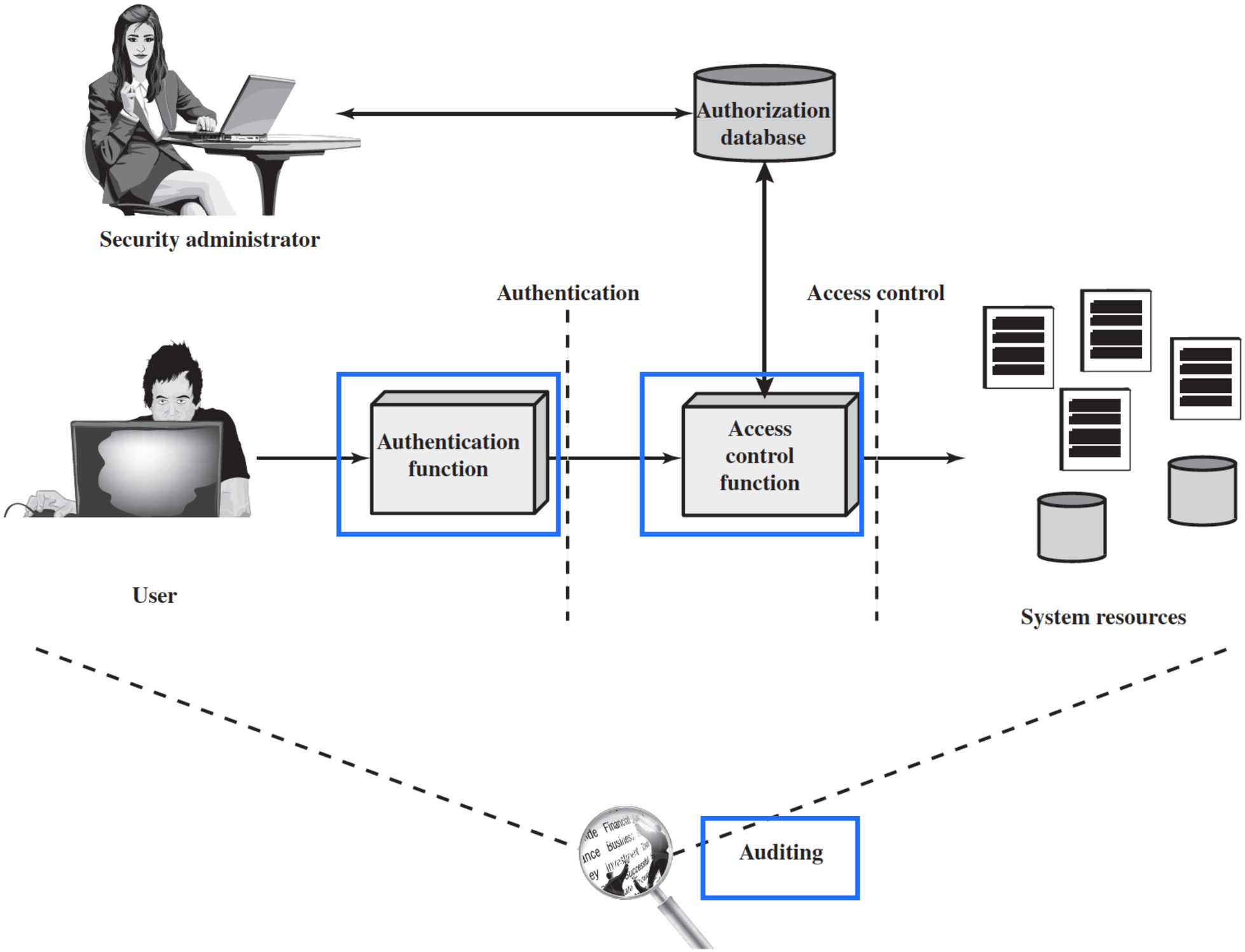
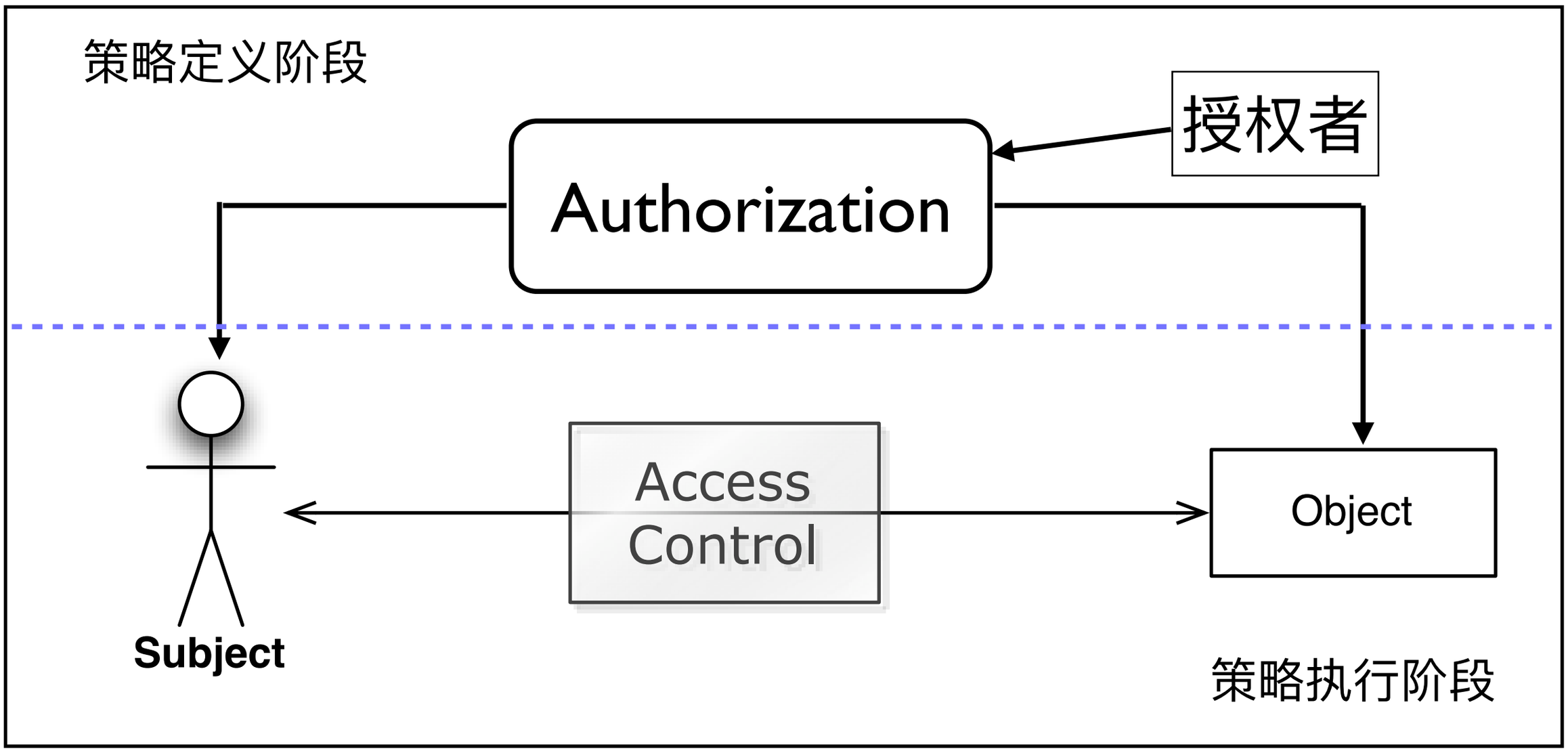


Figure 4.1 Relationship Among Access Control and Other Security Functions
Source: Based on [SAND94].

访问控制策略和机制

通过控制信息资源如何被访问来防范资源泄露或未经授权的修改



能够保护系统和资源免受未经授权的访问

控制用户和系统与其他的系统和资源进行通信和交互

主体和客体

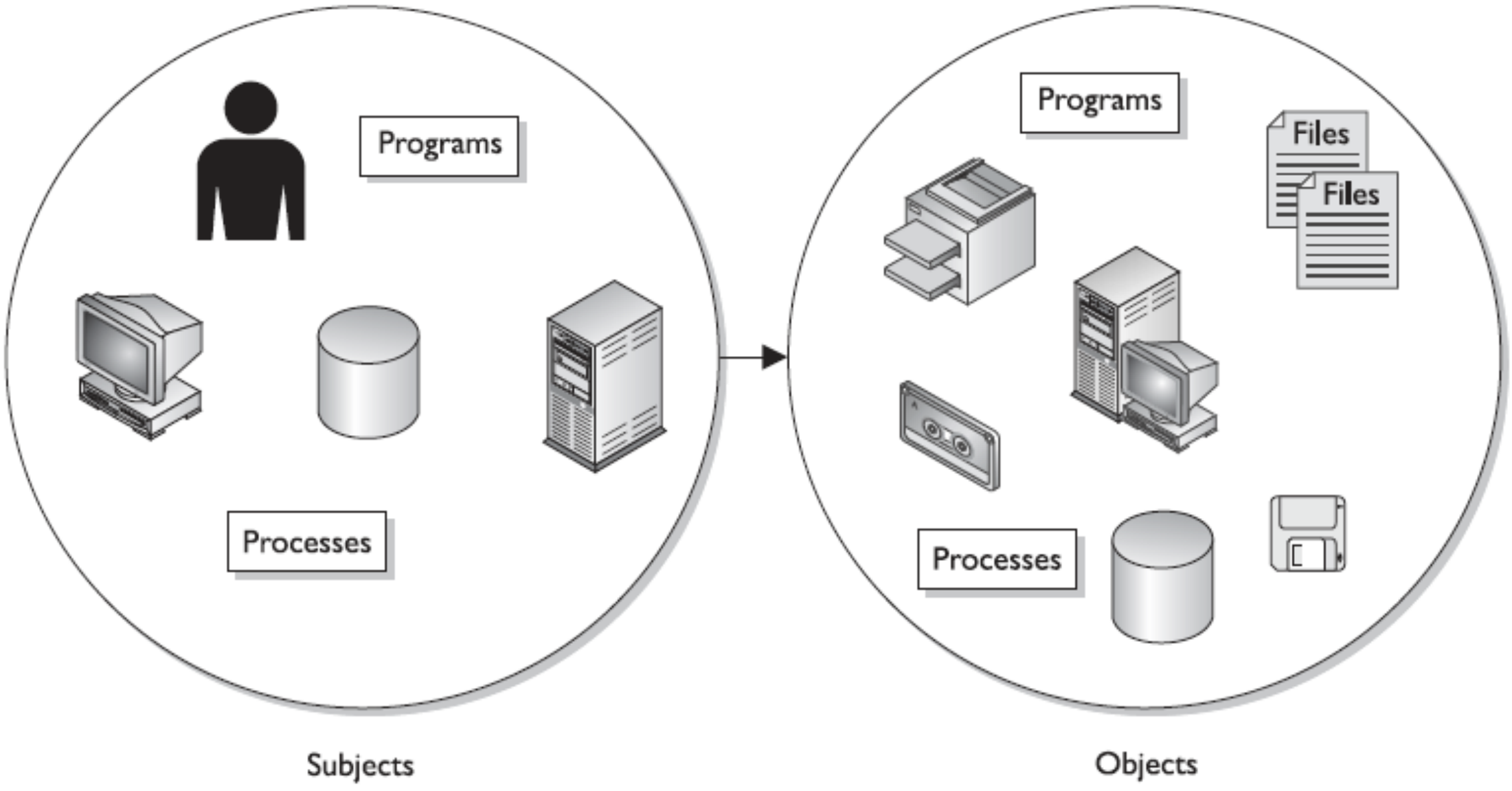
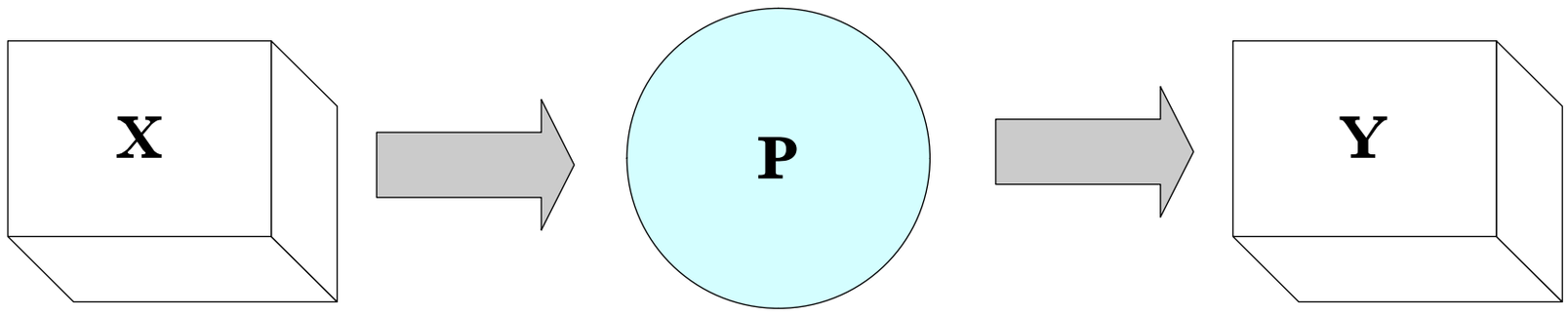


Figure 4-1 Subjects are active entries that access objects, while objects are passive entities.

权限



权限是对某一对象的可操作权利

可以用一个三元组 (X,Y,P)来表示权限

X表示一个主体，Y表示一个客体

P表示X对于Y的操作权利集合

最小权限

不应该给用户除他们需要完成必须功能之外的访问控制

最小特权原则

- 每一个模块仅能访问满足它合法目的必须的信息和资源
  - ✴角色划分：系统管理员 vs 备份管理员
  - ✴个人计算机：管理员账户 vs 普通账户
- 好处：稳定、安全、部署
- 真正的最小特权无法证明并不存在
  - ✴系统可控制力度
  - ✴环境变化

http://web.mit.edu/Saltzer/

Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.

一个简单的例子

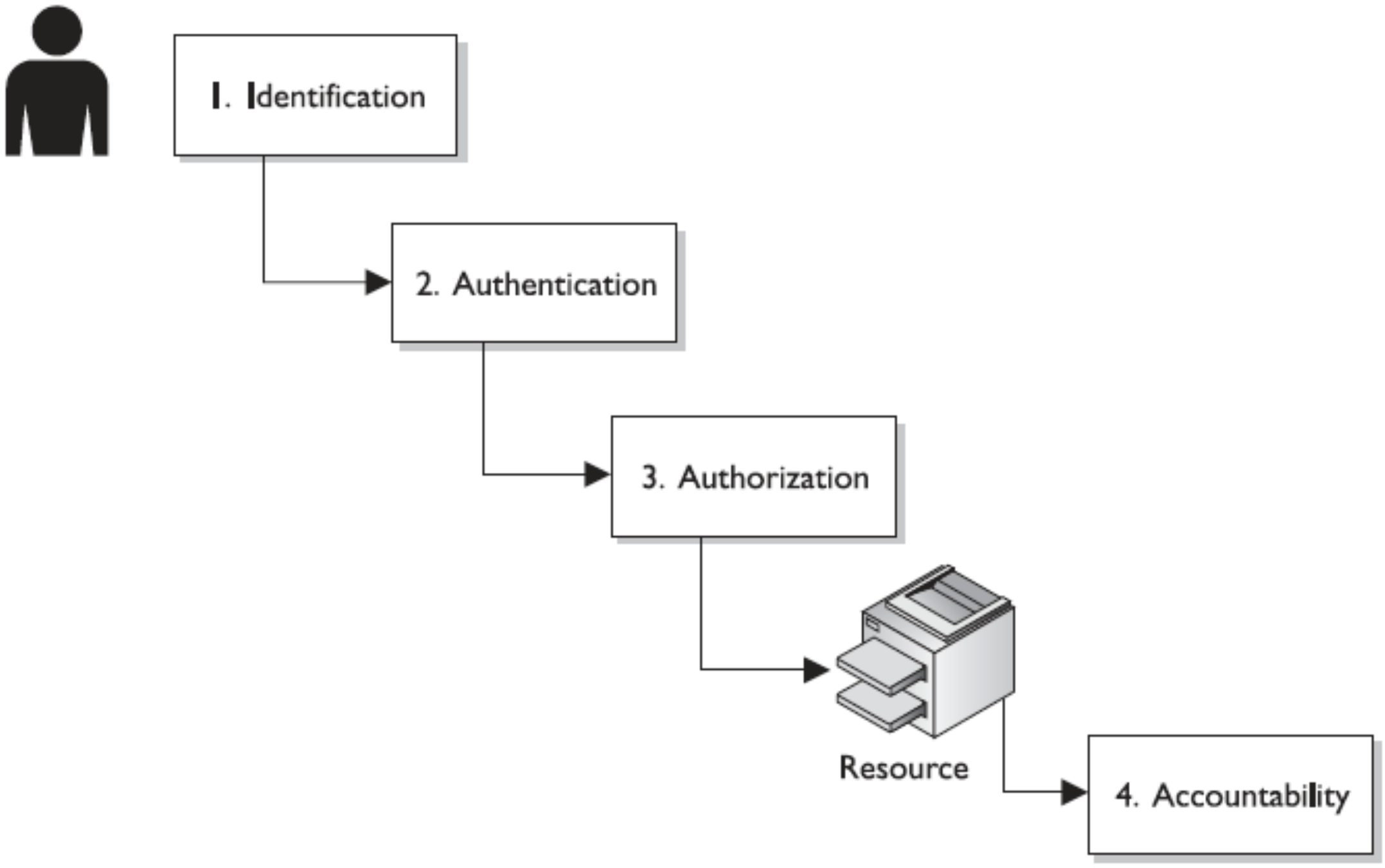


Figure 4-2 Four steps must happen for a subject to access an object: identification, authentication, authorization, and accountability.

访问控制模型

Access Control Model

访问控制模型

- Access Control Model
- 描述主体访问客体的一种框架
- 通过访问控制技术和安全机制来实现模型的规则和目标

- DAC：自主访问控制
- MAC：强制访问控制
- RBAC：基于角色的访问控制
- ABAC：基于属性的访问控制

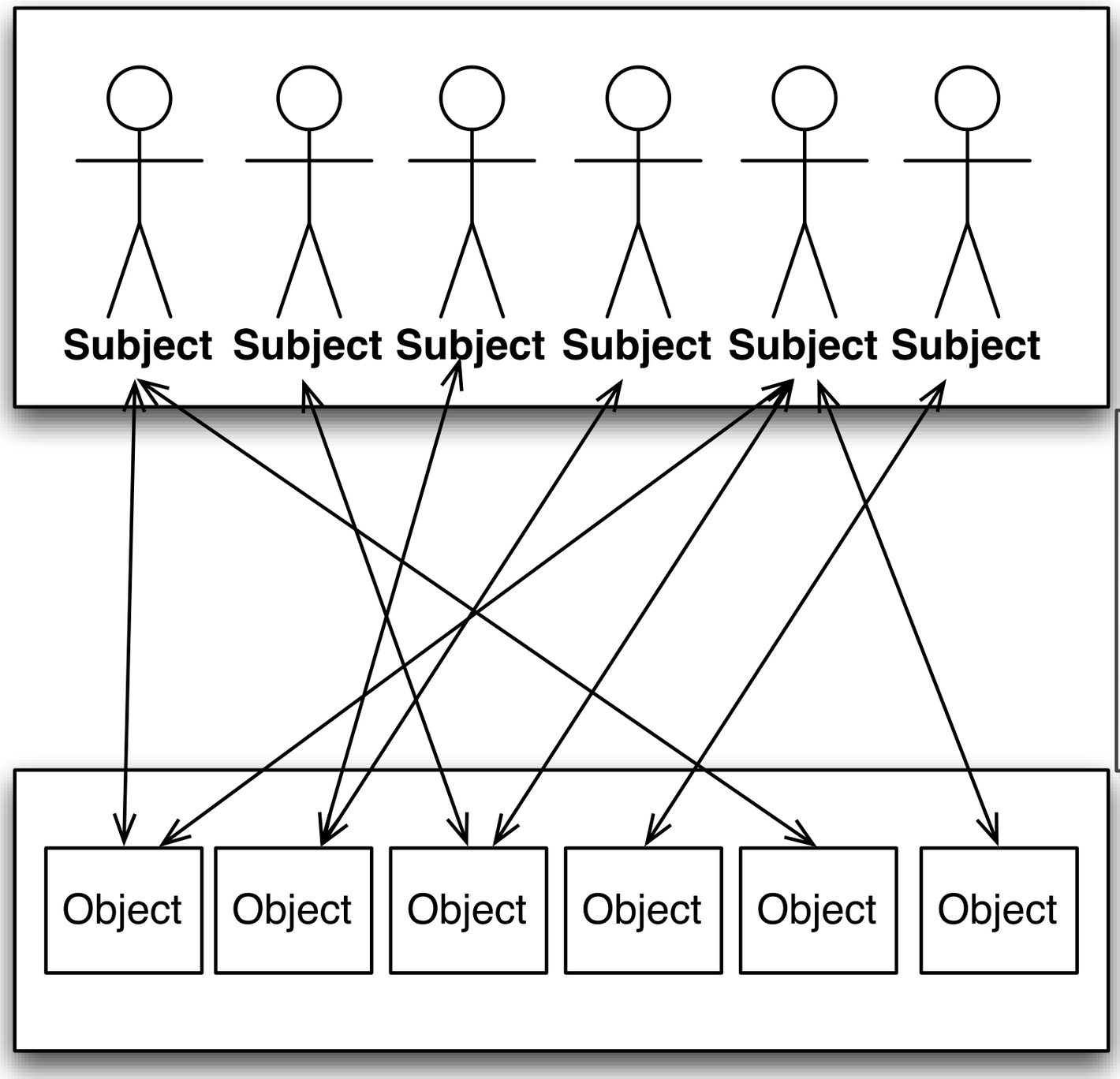
Access Control Model

自主访问控制模型

客体的拥有者指定哪些主体可以访问客体

最常见的形式是访问控制列表

动态的



Discretionary Access Control

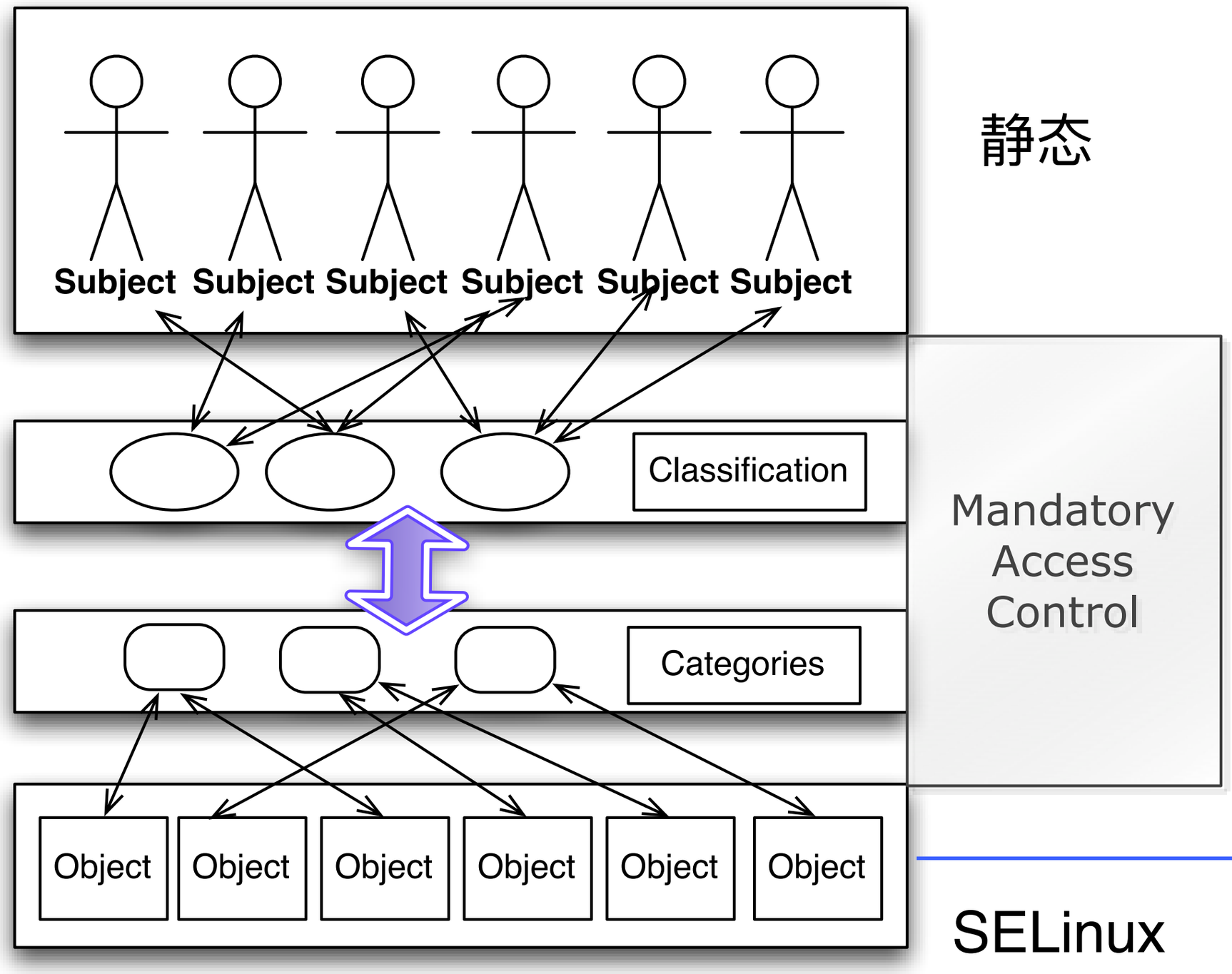
Access Control Model

强制访问控制模型

主体和客体均没有权限决定谁来访问客体

一般基于安全标签系统来实现，客体和主体绑定一个安全标签

应用于对信息分类和机密性要求较高的环境中

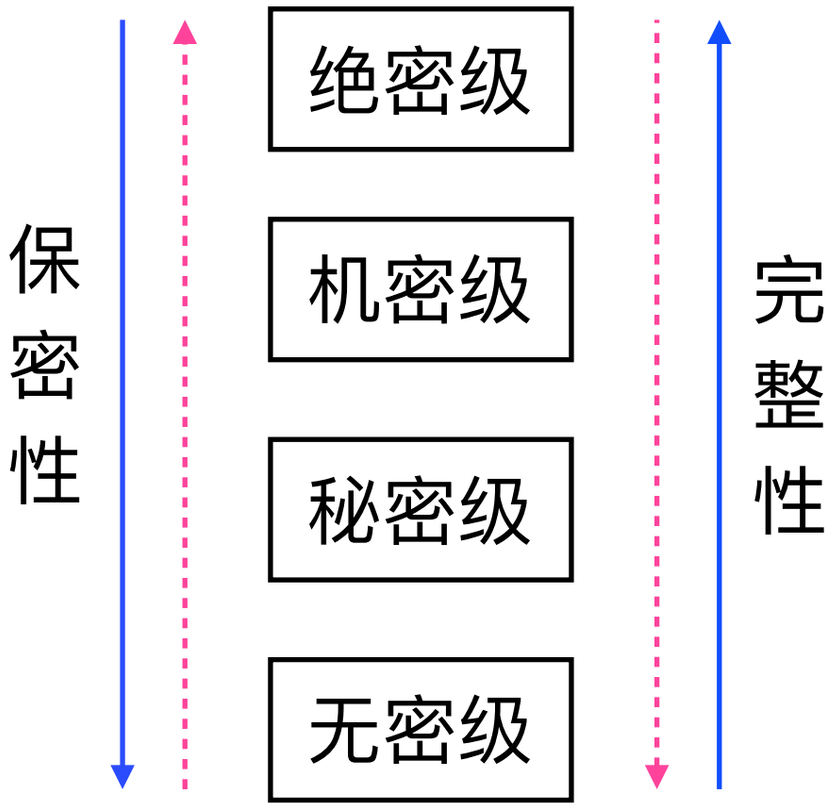


静态

SELinux
可信Solaris

MAC

多级安全



Bell-LaPadula

不上读

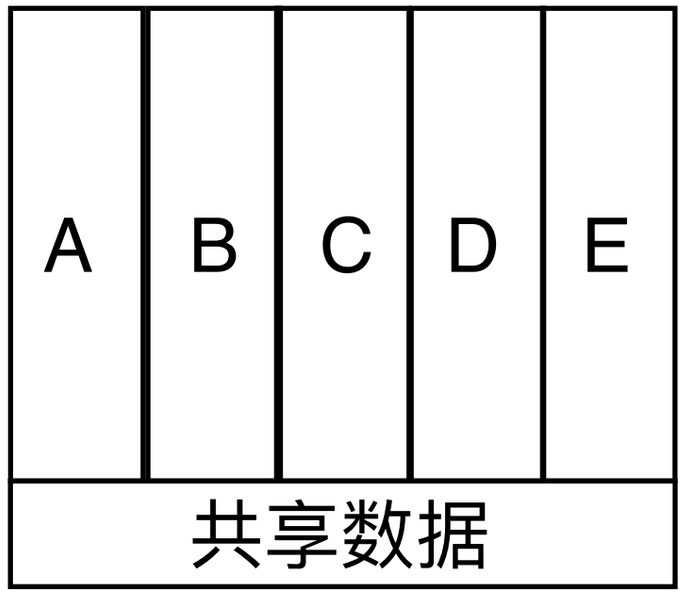
不下写

Biba

不上写

不下读

多边安全



分割和网格模型

BMA模型

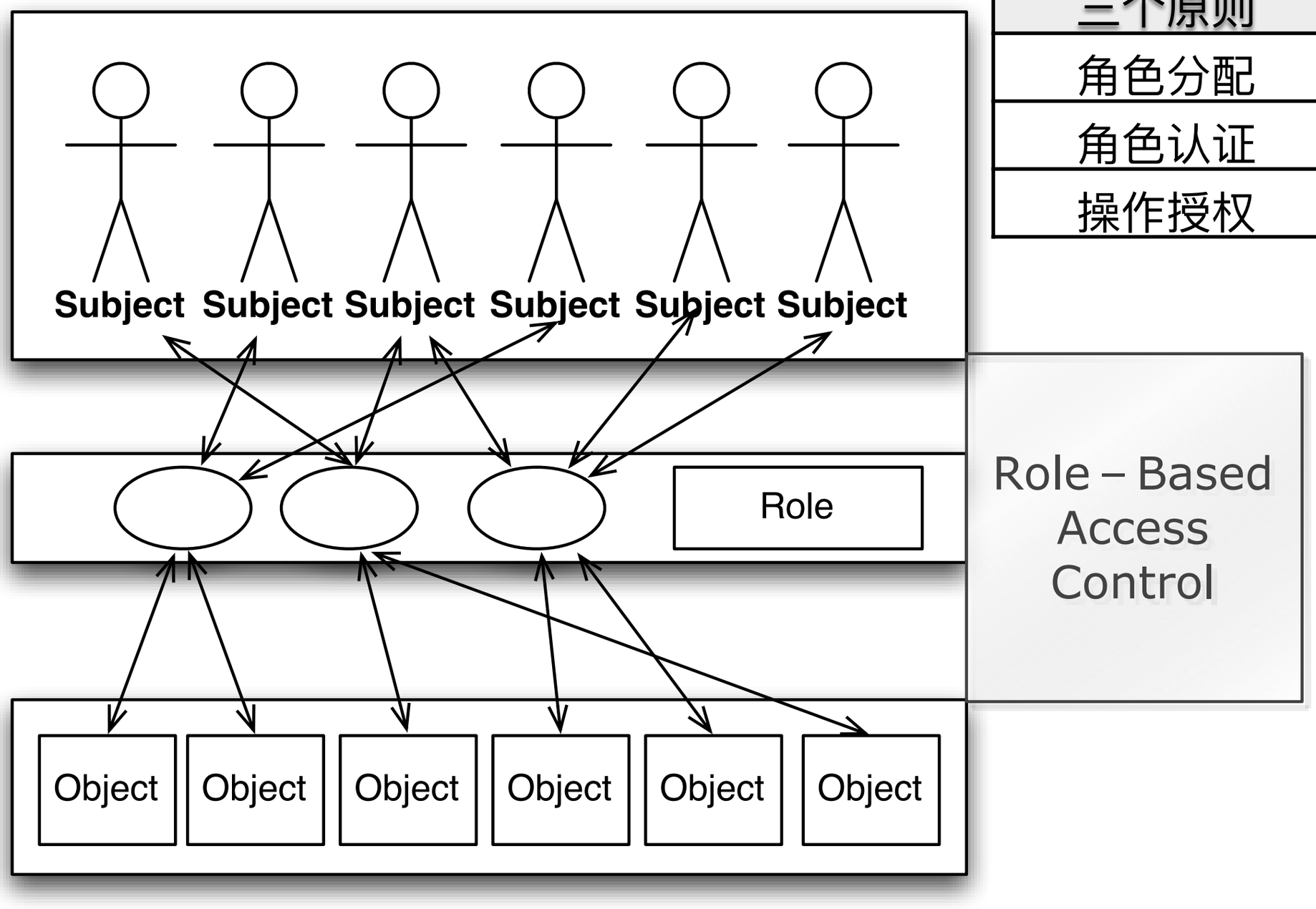
Access Control Model

基于角色访问控制模型

非自主型访问控制
集中管理

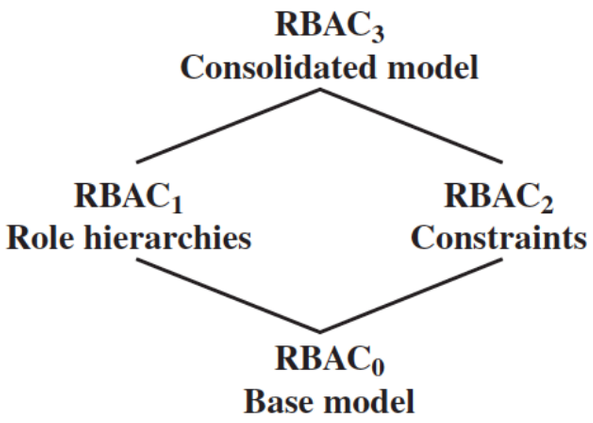
权限和角色挂钩
适合于员工流动性高的组织

企业级应用
当前最广泛的访问控制机制



http://csrc.nist.gov/rbac

RBAC模型



(a) Relationship among RBAC models

(b) RBAC models

基于属性的访问控制

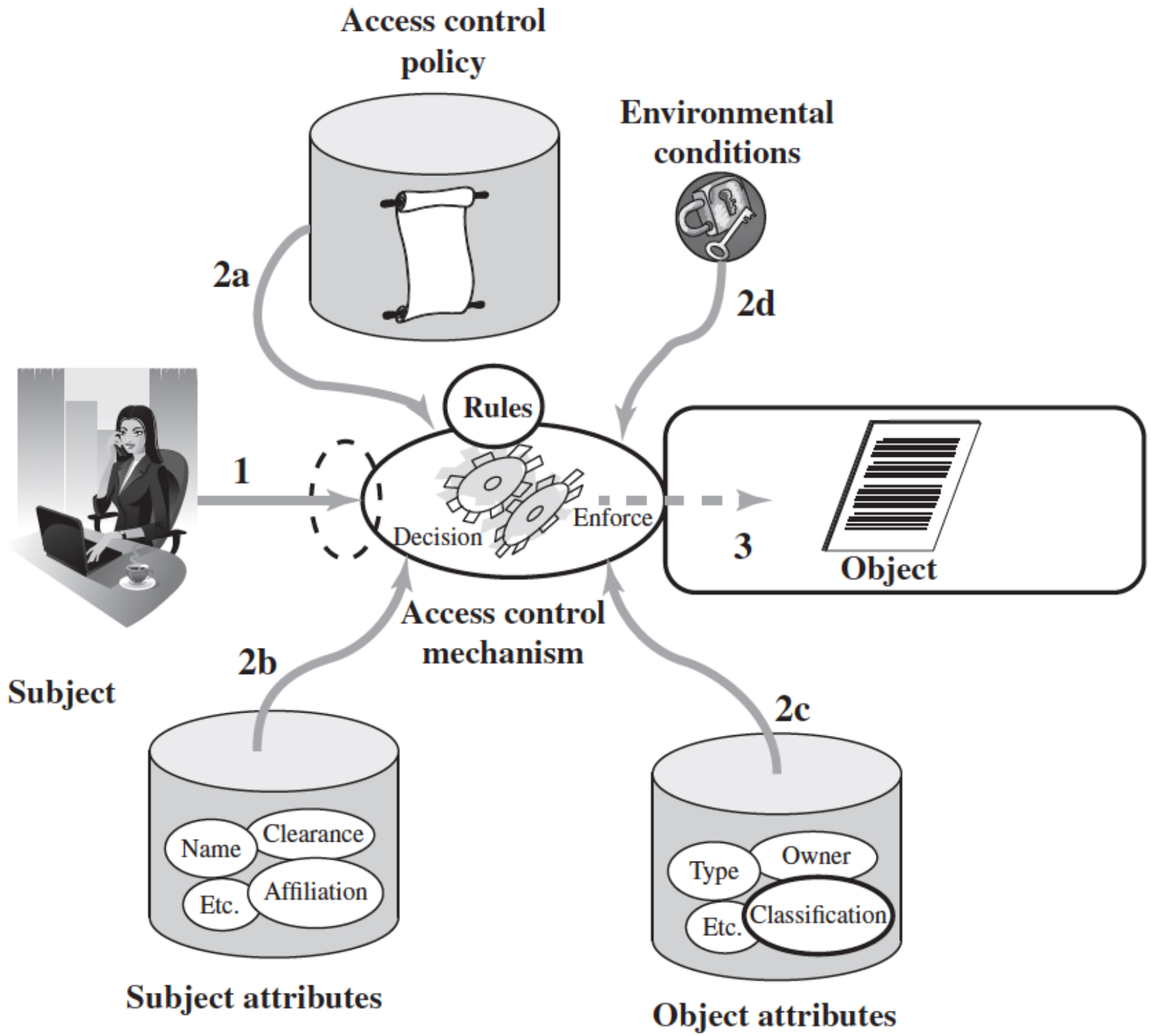


Figure 4.10 **Simple ABAC Scenario**

属性例子

- 主体：ID、角色、组、部门、...
- 环境：时间、位置、...
- 客体：密级、类型、...
- 例子
  - 网页URI
  - 网页内部的Object类型和Object属性
  - 标签系统中的标签

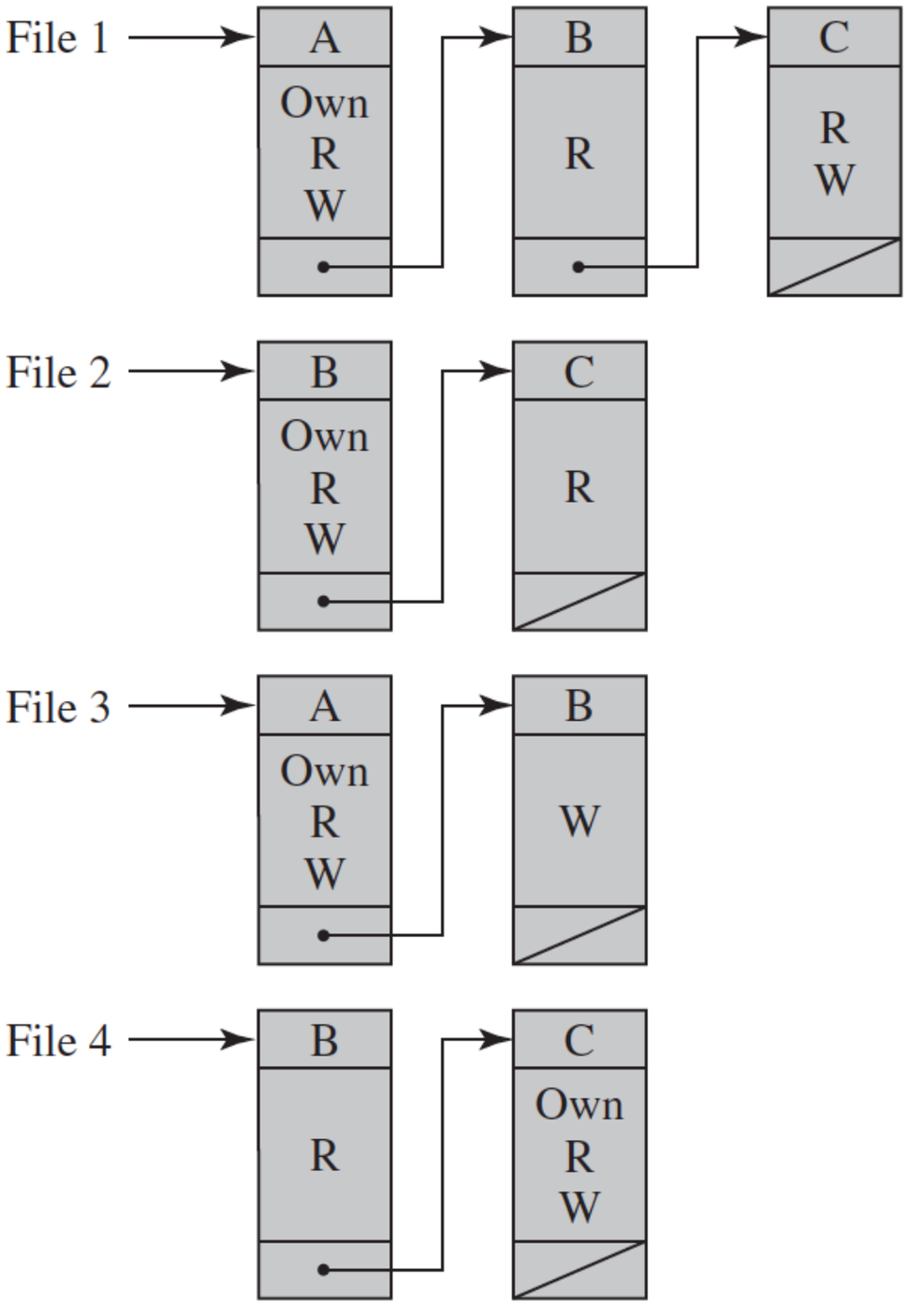
访问控制技术

访问控制矩阵

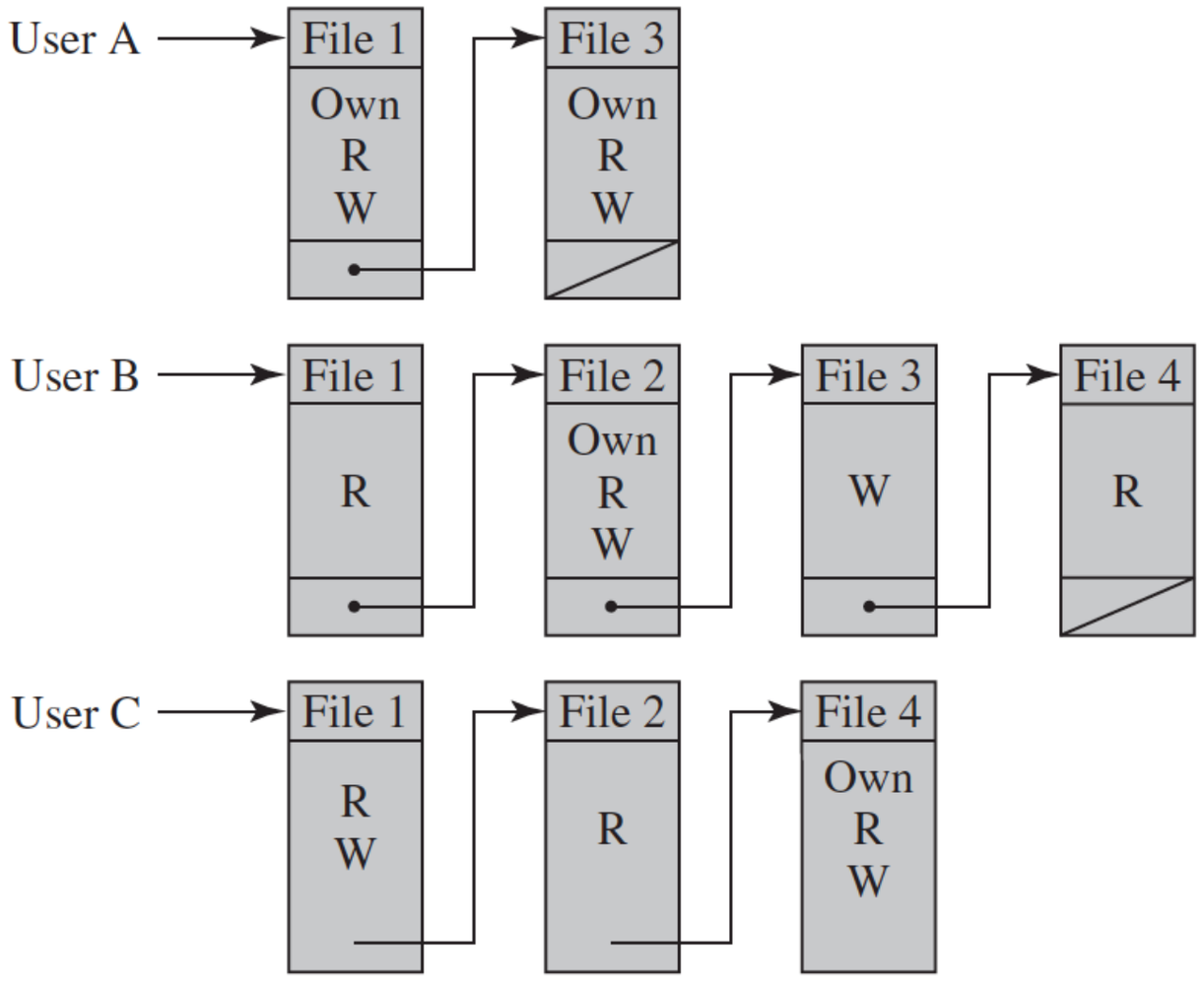
		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

访问控制列表 vs 访问能力表



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)

UNIX的文件访问控制

- 用户和组对资源都有权限，用户属于组，文件归属于所有者和组，每一个权限级别都可以设置给文件所有者、文件所在组和其它用户
- Unix文件系统：读、写、执行


```
#ls -l install.log
-rw-r--r--   1  root    root    26195 Dec 17 10:42 install.log
```

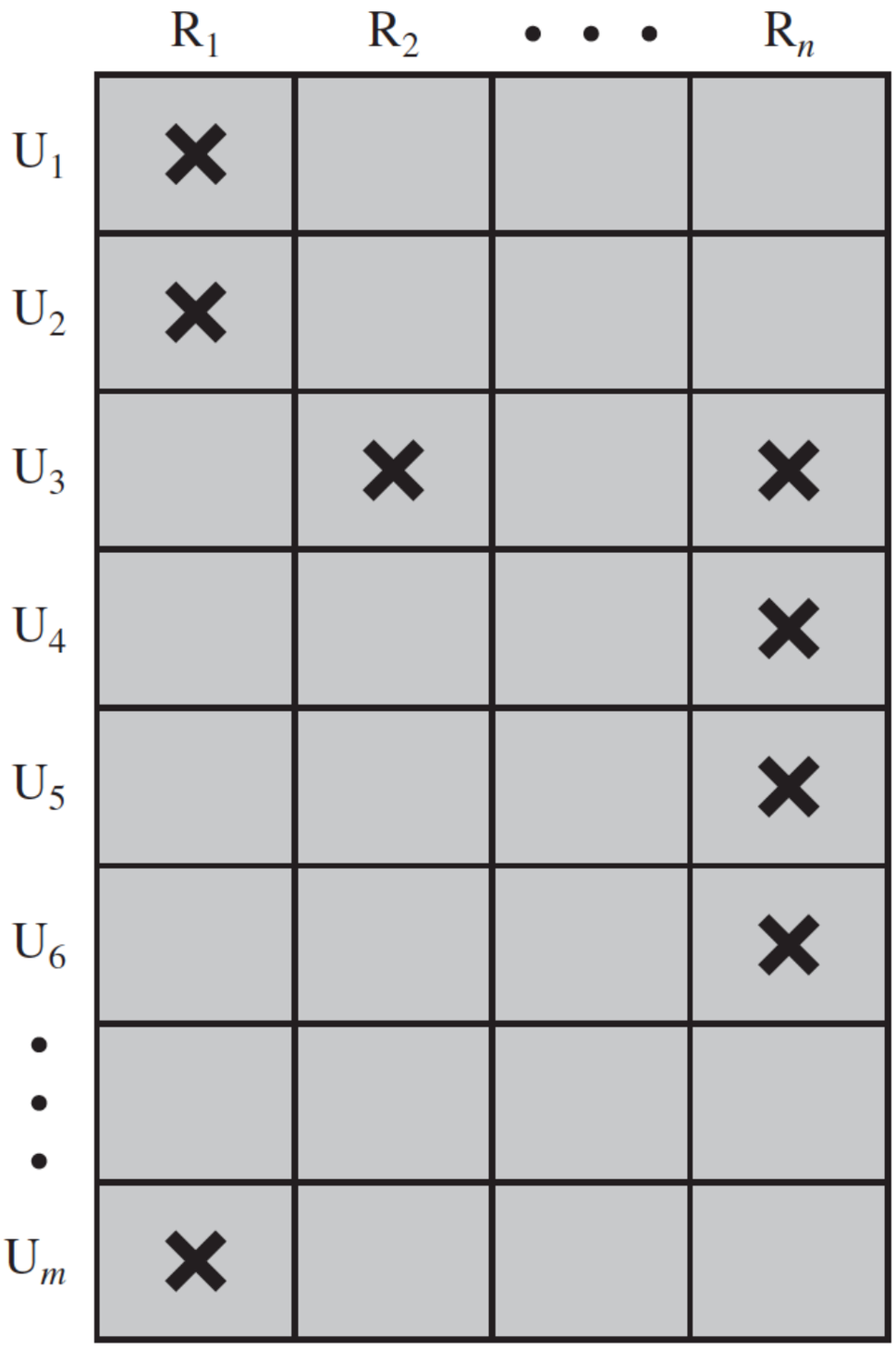
权限表示

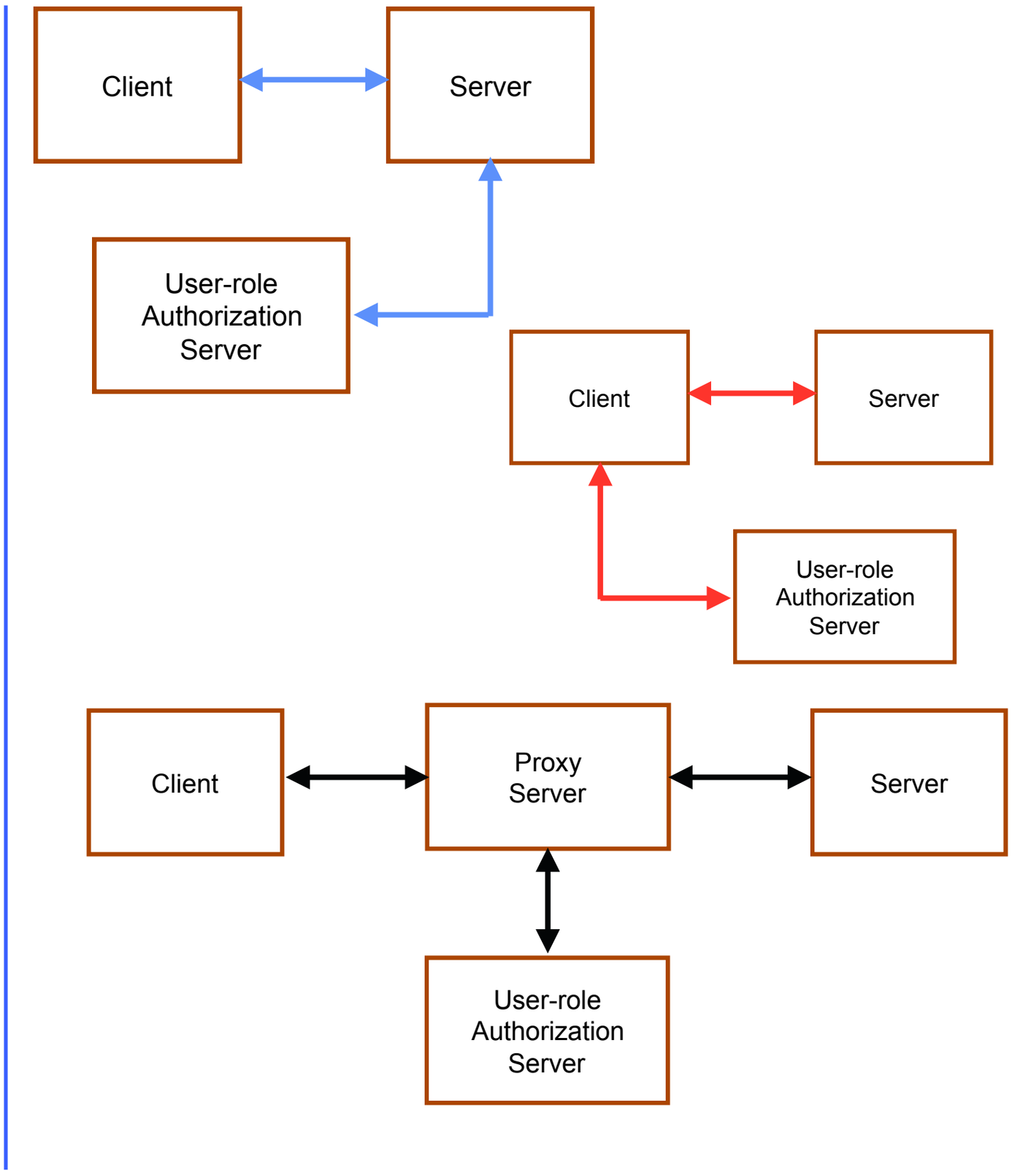
文件权限（-rw--r--r--）

权限项	读	写	执行	读	写	执行	读	写	执行
字符表示	(r)	(w)	(x)	(r)	(w)	(x)	(r)	(w)	(x)
数字表示	4	2	1	4	2	1	4	2	1
权限分配	文件所有者			文件所属组用户			其他用户		

- 忘记正确分组
- 缺少分组工具
- 权限关联资源
- 管理员设置

RBAC: 用户和角色映射





RBAC: 角色和客体

ROLES	R_1	R_2	R_n	F_1	F_2	P_1	P_2	D_1	D_2
		OBJECTS							
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
•									
•									
•									
R_n			control		write	stop			

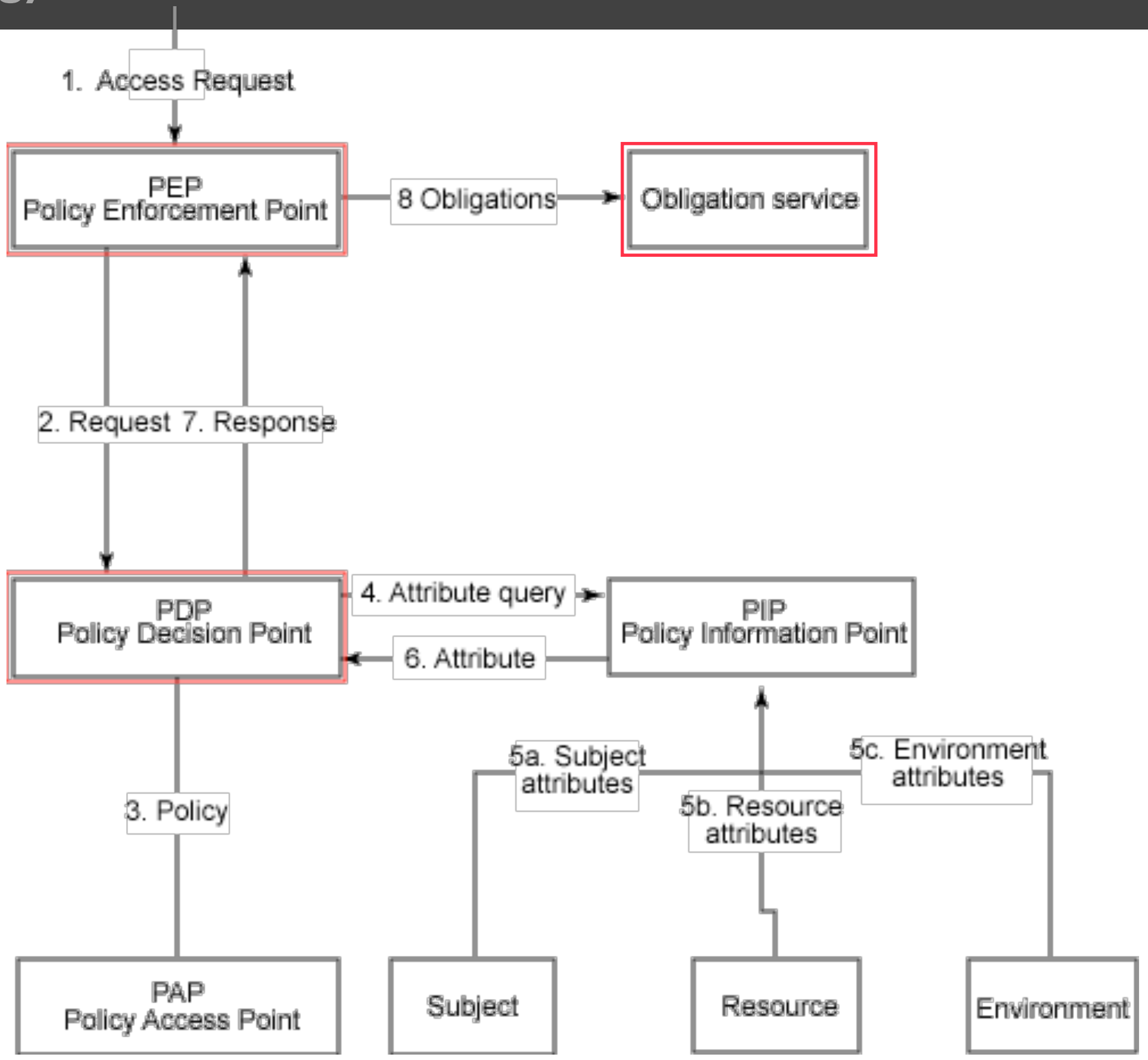
Figure 4.7 Access Control Matrix Representation of RBAC

XACML

- XACML是OASIS制定的一个用以整合各方面（比如IBM和米兰大学）努力成果的一个标准。它和SAML共同使用，它提供了一种标准化XML文件接入控制决定的工具。
- XACML是用来决定是否允许一个请求使用一项资源，比如它是否能使用整个文件，多个文件，还是某个文件的一部分。
- XACML允许组织为了存取在线资源和信息而传递他们的策略
  - ✴ 哪个客户端可以存取信息
  - ✴ 哪些信息是客户端可以使用的
  - ✴ 什么时间客户端可以存储这些信息
  - ✴ 如何来存取这些信息

http://www.oasis-open.org/committees/xacml/

XACML


1. Access Request
PEP
Policy Enforcement Point
8 Obligations
Obligation service
2. Request 7. Response
PDP
Policy Decision Point
4. Attribute query
PIP
Policy Information Point
6. Attribute
3. Policy
5a. Subject attributes
5b. Resource attributes
5c. Environment attributes
PAP
Policy Access Point
Subject
Resource
Environment

其余技术：基于规则的访问控制

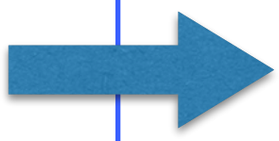
- 使用特定的规则来规定主体和客体之间可以做什么，不可以做什么
- 应用于强制访问控制
- 一个例子：
  - ✳ 电子邮件的附件不能大于5M
  - ✳ 张三的电子邮件附件可以大于5M，但不能超过10M
- 路由器和防火墙的数据包通过规则
- 管理员制定，用户不能修改

其余技术：限制用户接口

- 通过不允许提交某些功能、信息或访问某些系统资源来限制用户的访问能力
  - ✴ 菜单和命令：限制用户能执行的命令和程序
  - ✴ 数据库视图：限制用户访问数据库中数据
  - ✴ 物理限制接口：ATM提款机

张三	4500	10日
李四	6000	11日
王五	6500	12日

薪水数据库视图



张三	工作1	10日
李四	工作2	11日
王五	工作2	12日

经理数据库视图

其余

- 基于内容的访问控制
  - ✴ 对客体的访问主要取决于客体内容
  - ✴ 基于内容的过滤
  - ✴ 数据库视图
- 基于情形的访问控制
  - ✴ 根据一组信息的情形做出访问决定
  - ✴ 通信协议
  - ✴ 基于行为的一个特例

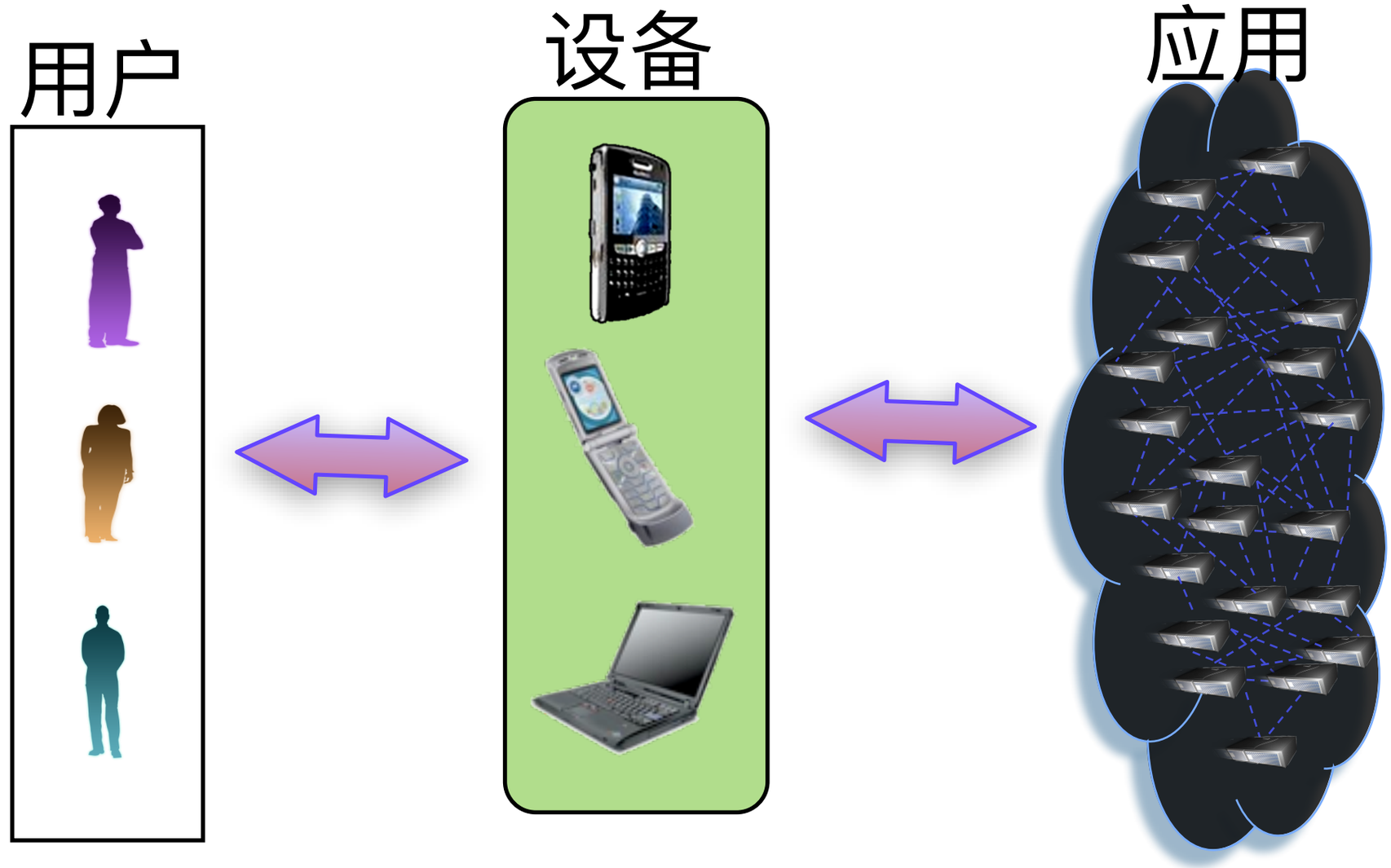
- 基于上下文
- 基于任务
- 基于时间
- 基于信任
- 基于风险
- UCON
- …… ……

访问控制例子

Access Control Example

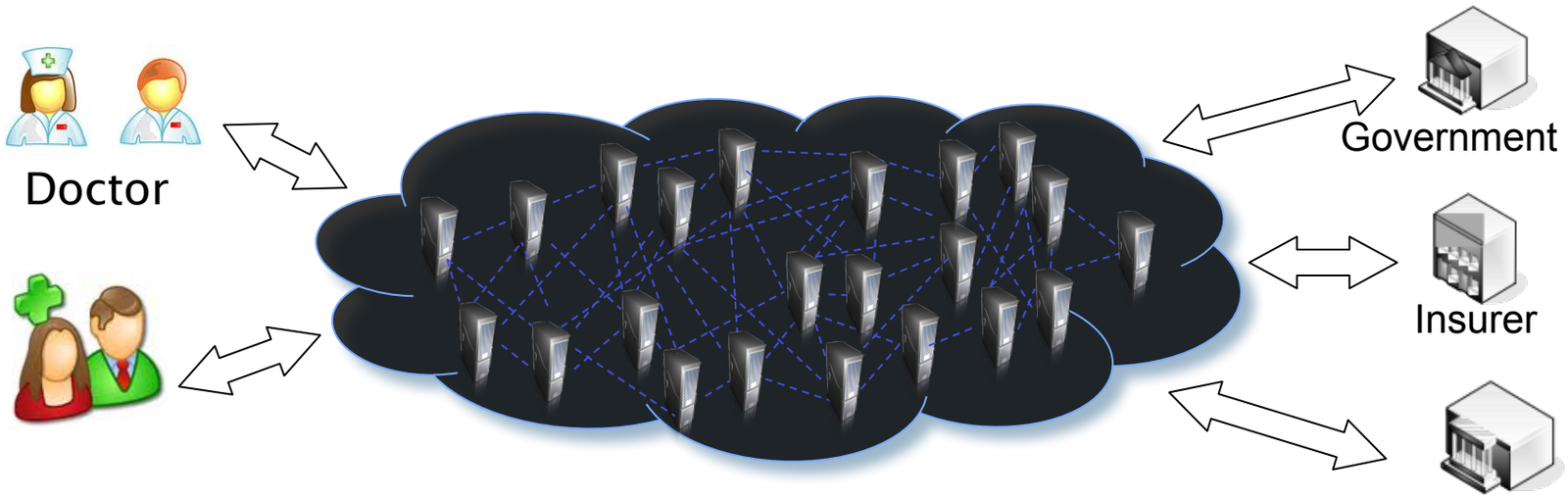
访问控制面临挑战

- 细粒度
- 海量
- 分布式
- 环境多变
- 管理简单
- 个性化
- 互联互通



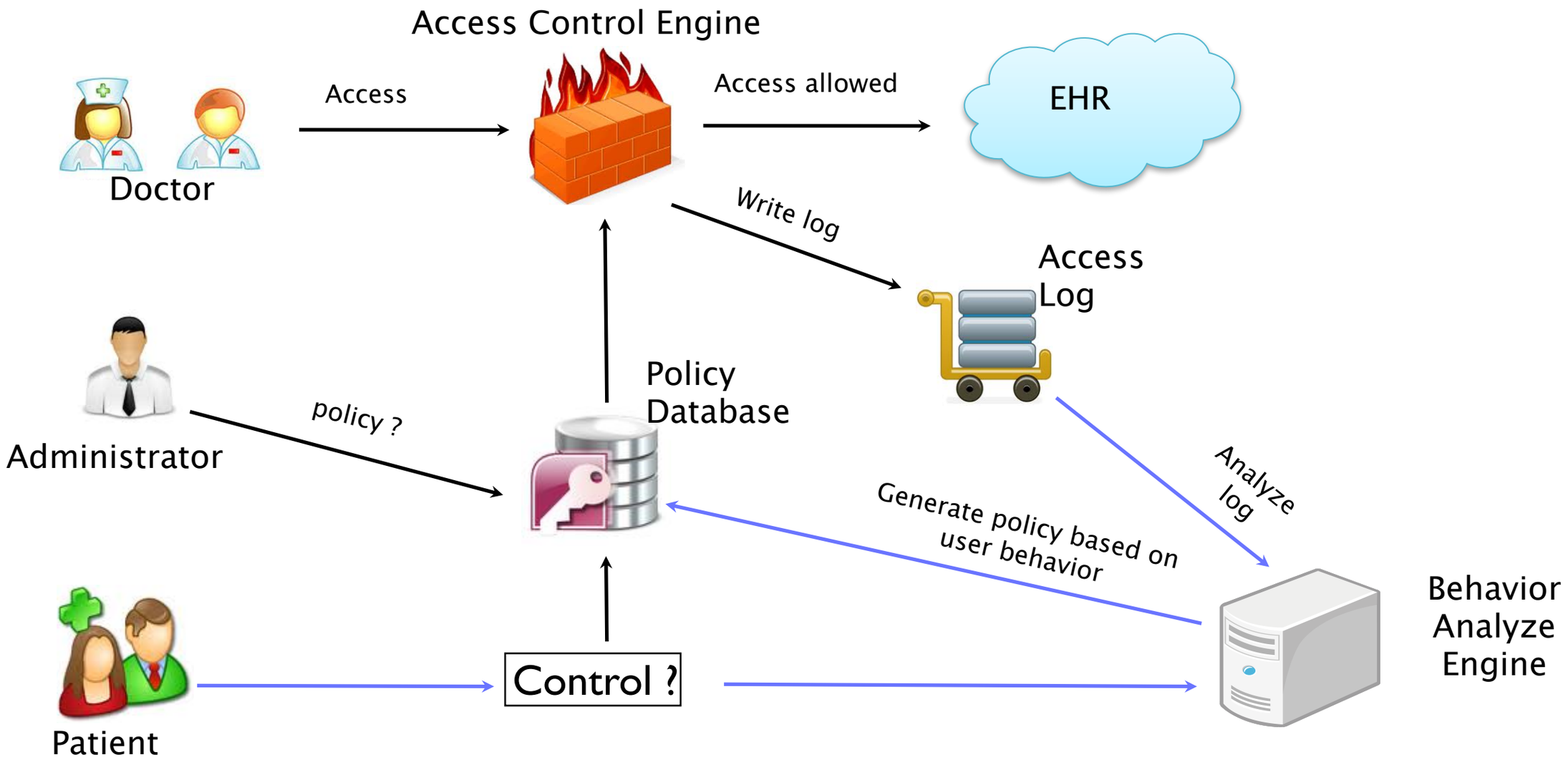
Access Control Example

基于行为



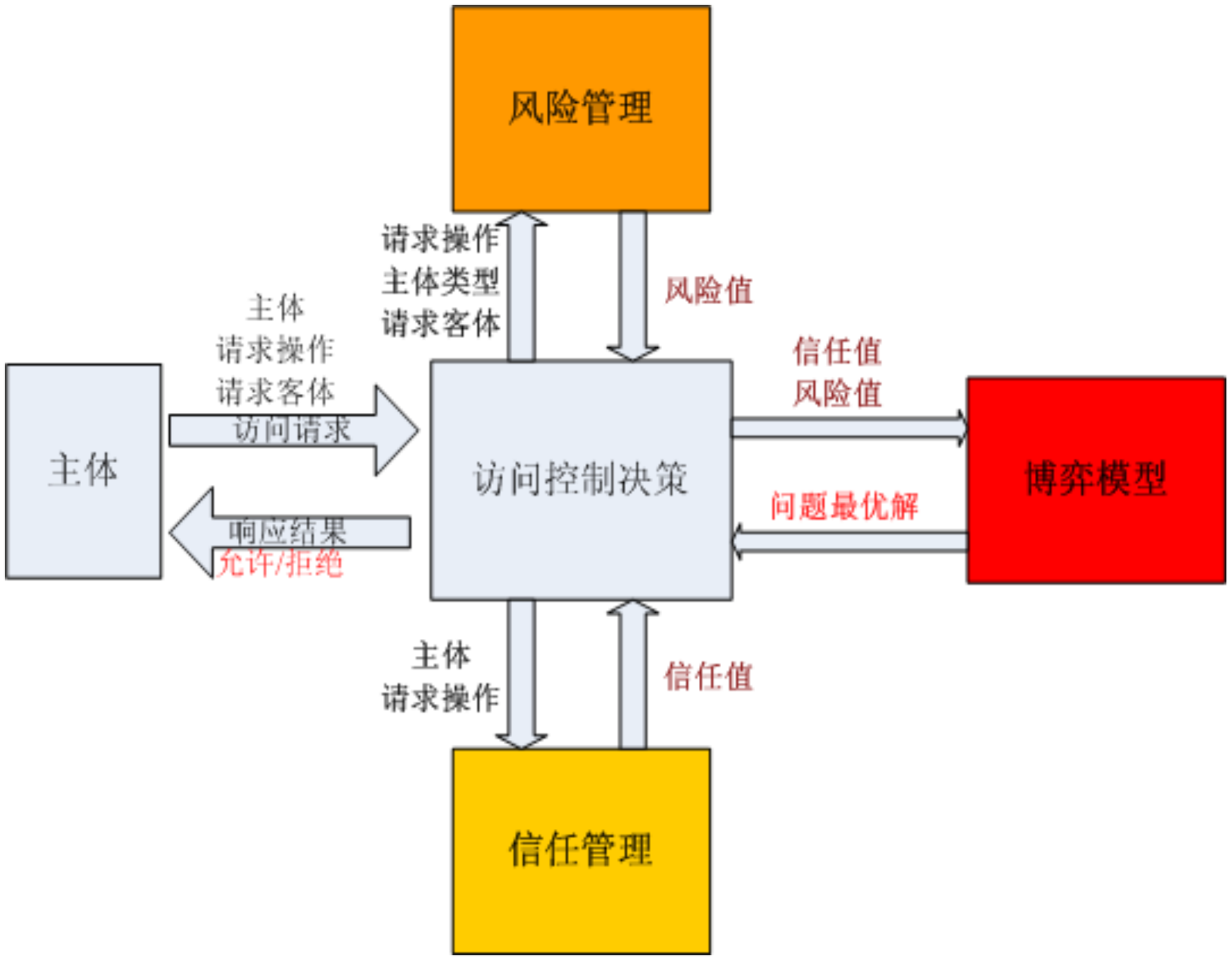
Google health beta

Microsoft HealthVault



Access Control Example

基于信任 + 风险 + 博弈

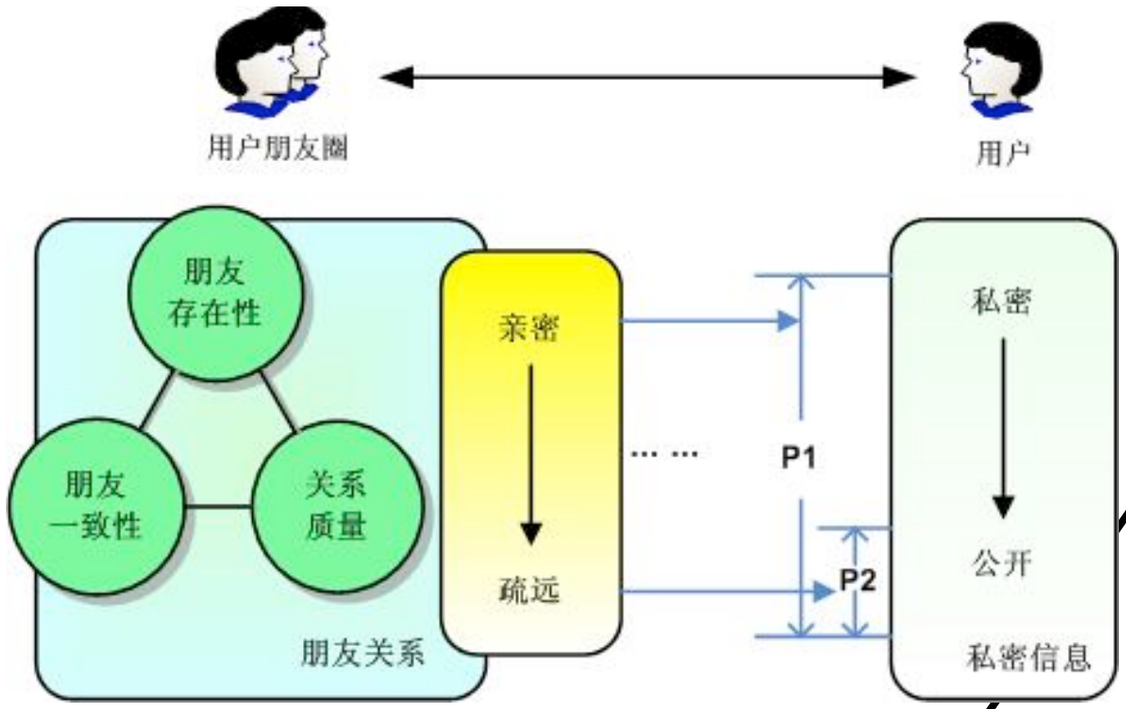


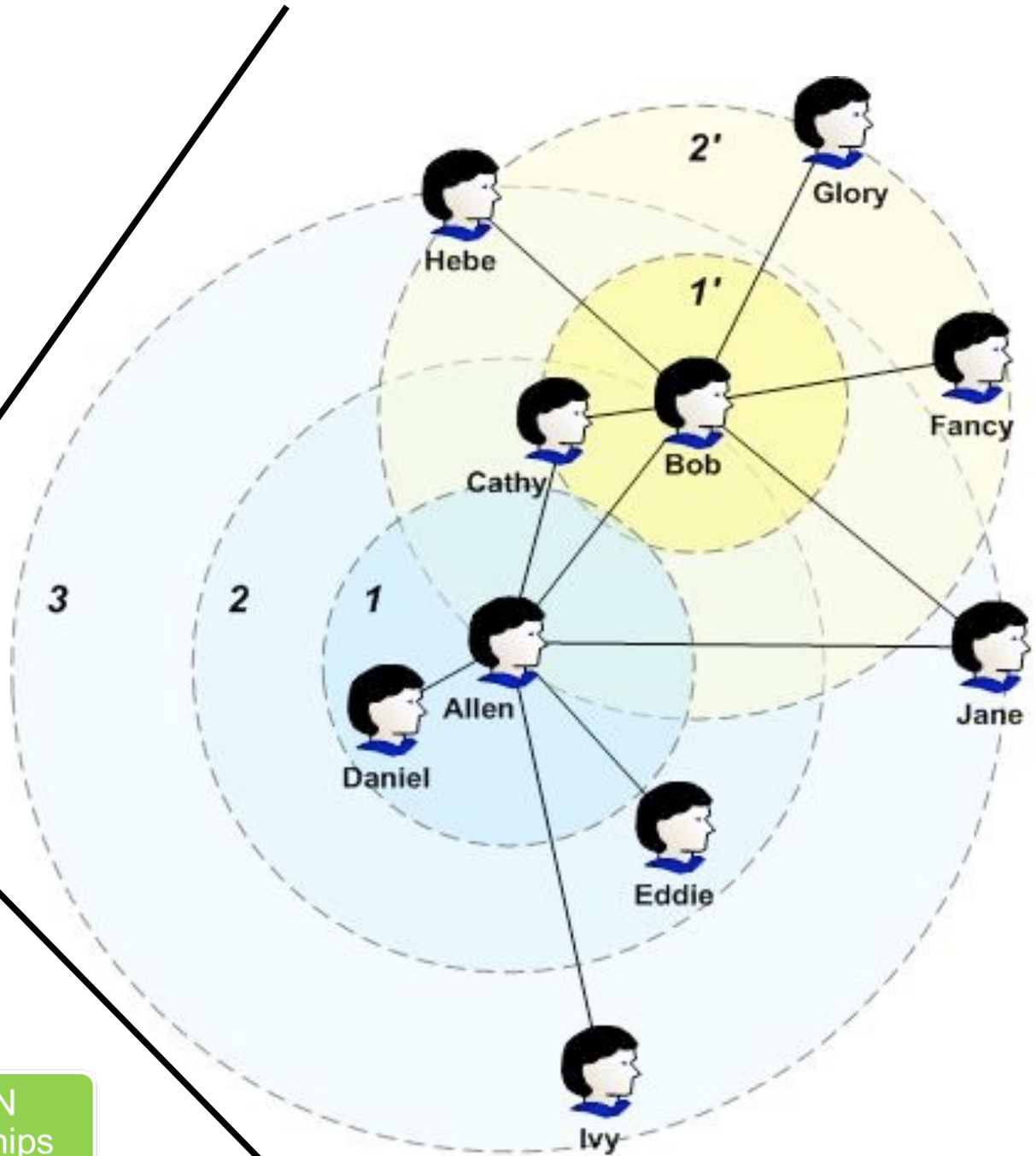
隐私设定问题

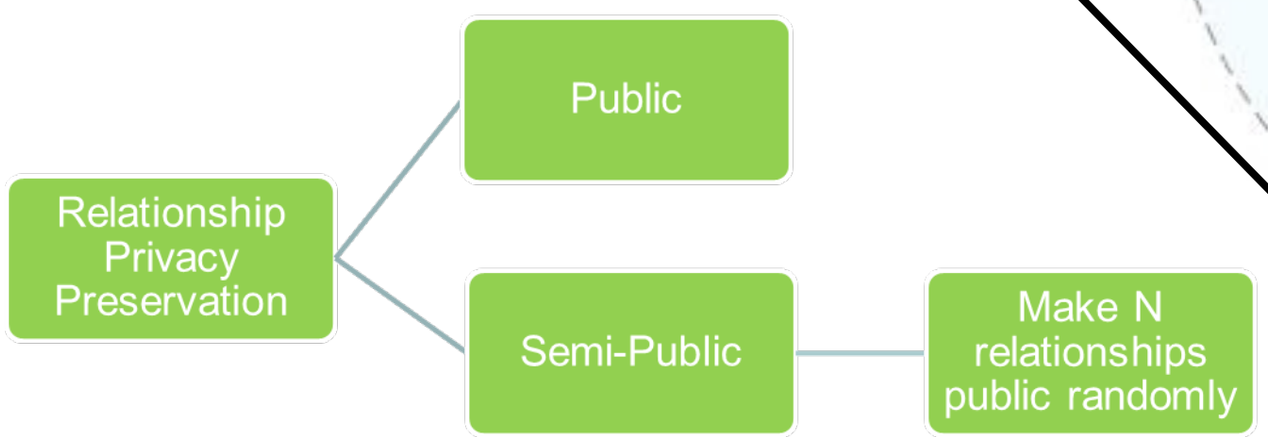
- OSN面临的主要问题
  - ✴用户保护自己的信息 vs 信息共享
  - ✴用户自己设定不现实 vs 系统设定复杂
- 现在的解决方法
  - ✴更好力度的隐私设定
  - ✴可视化的隐私设定
  - ✴自动化的隐私设定
  - ✴缺省隐私设定

Access Control Example

基于朋友亲密度的SNS隐私控制

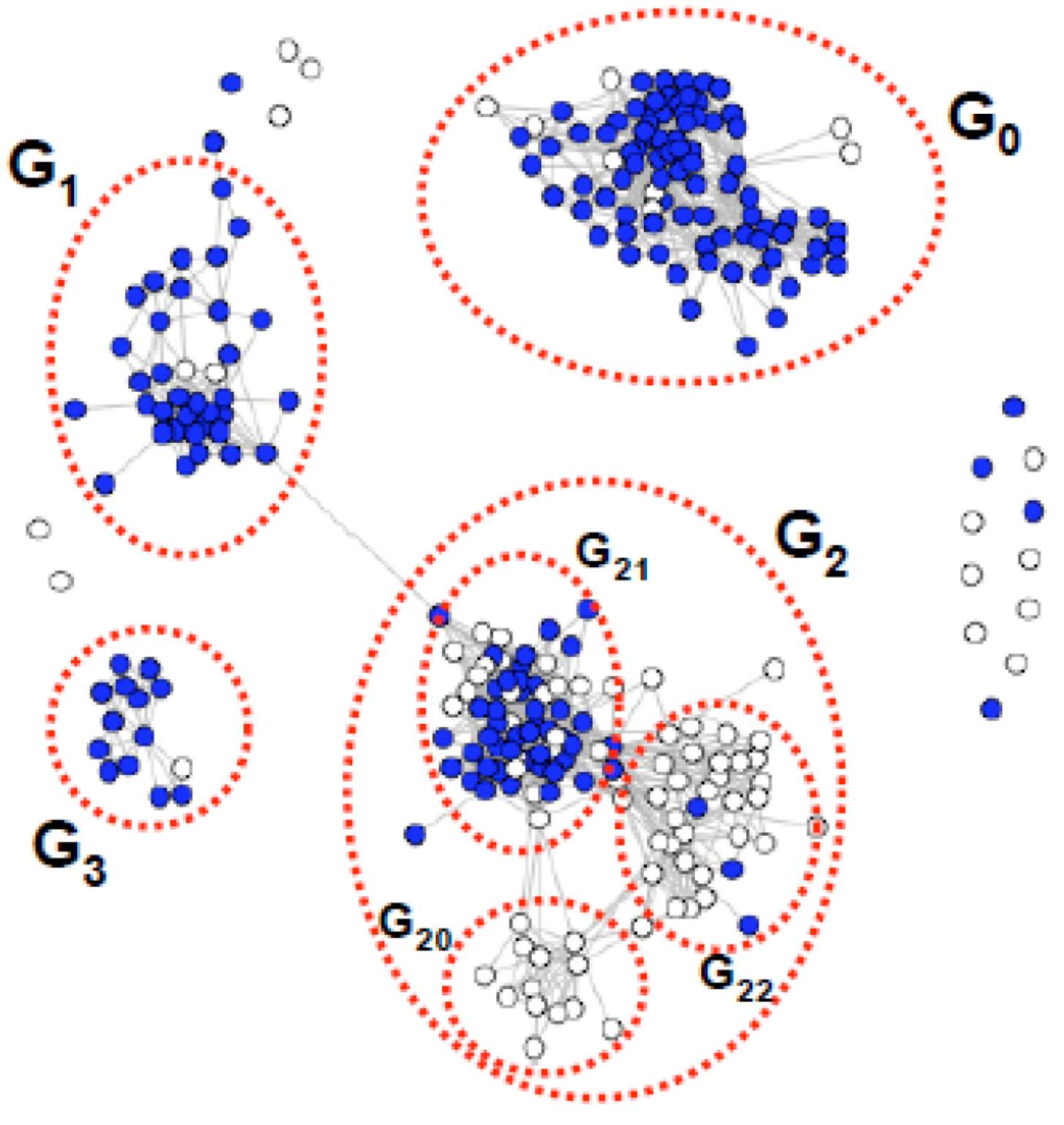






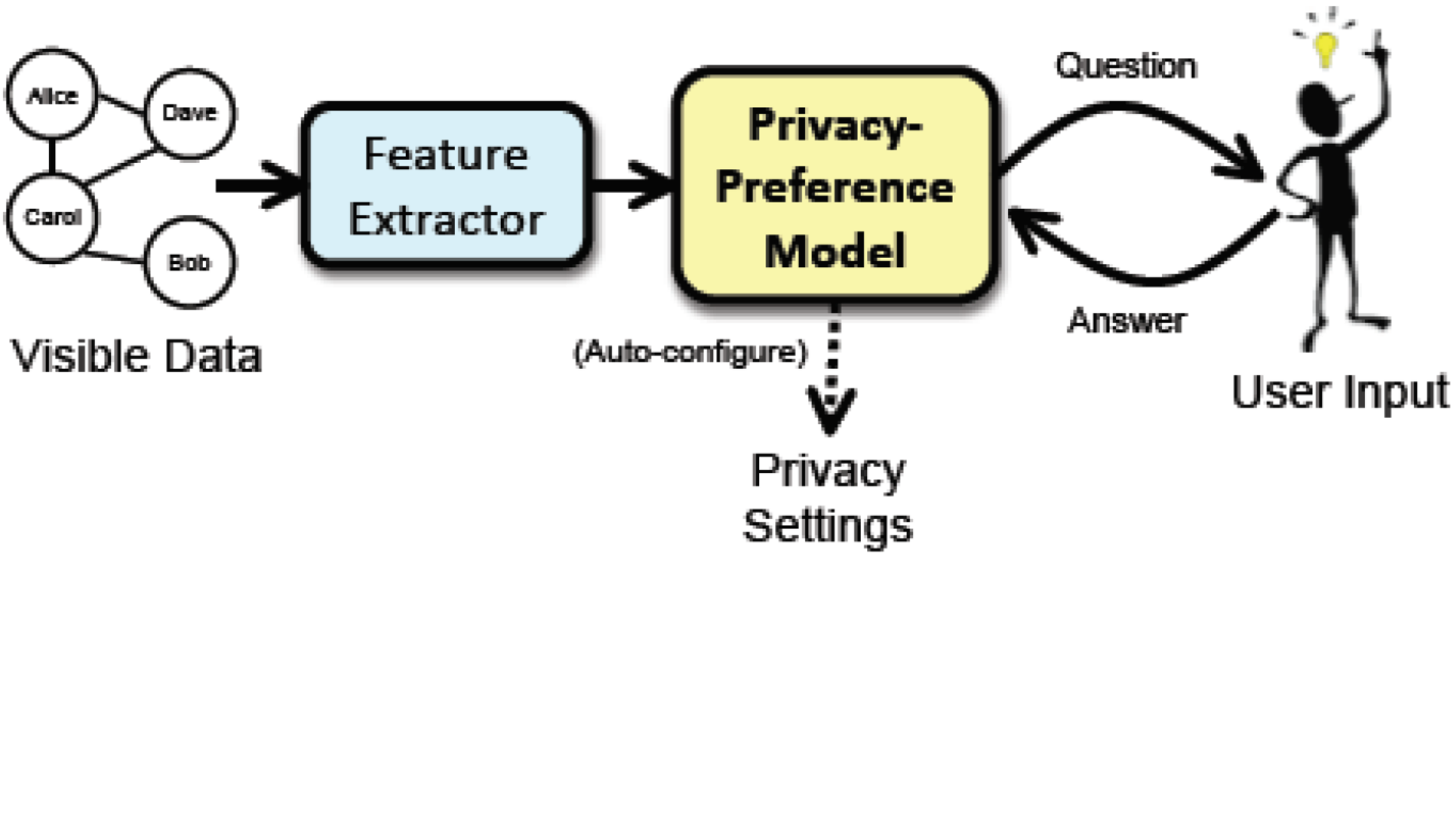
访问控制设定推荐向导

圈子



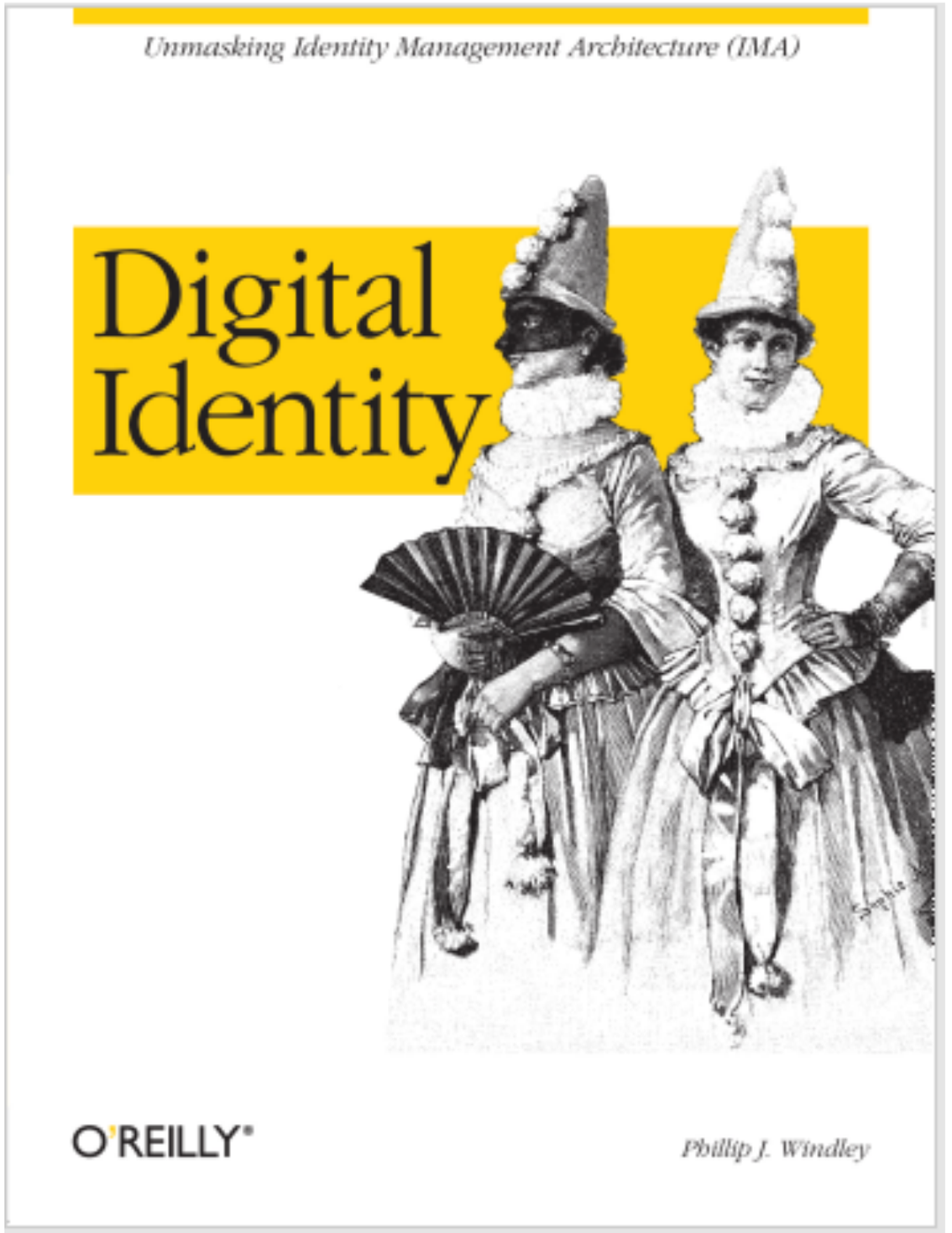
隐私设定推荐向导

利用机器学习技术推荐隐私设定



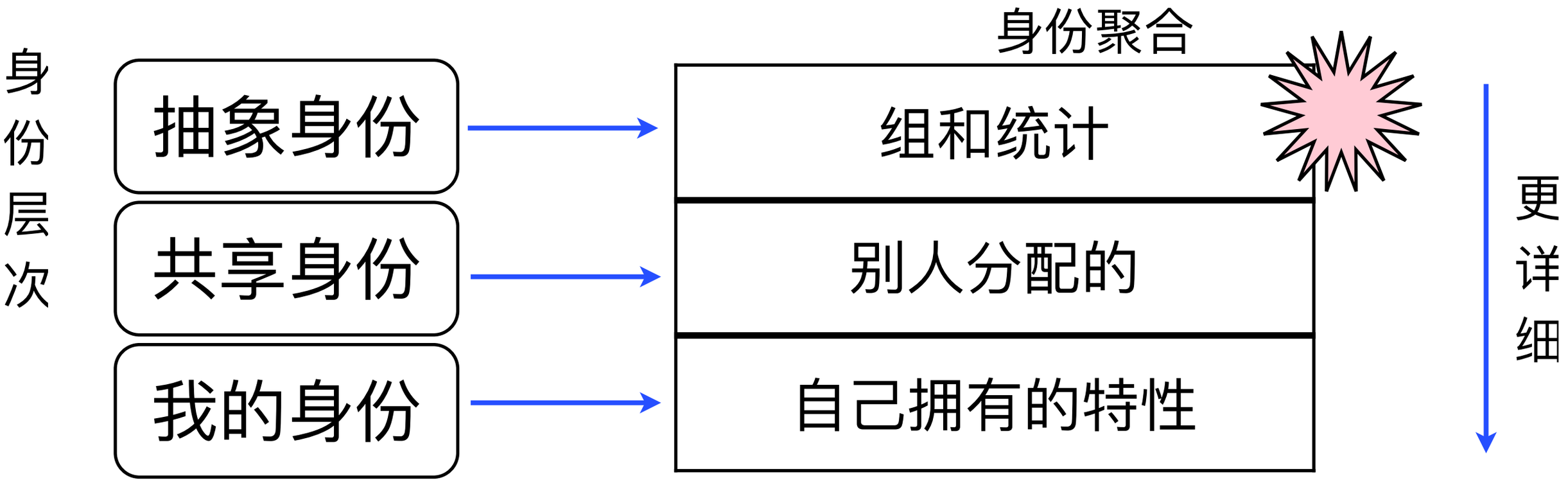
身份管理介绍

参考书

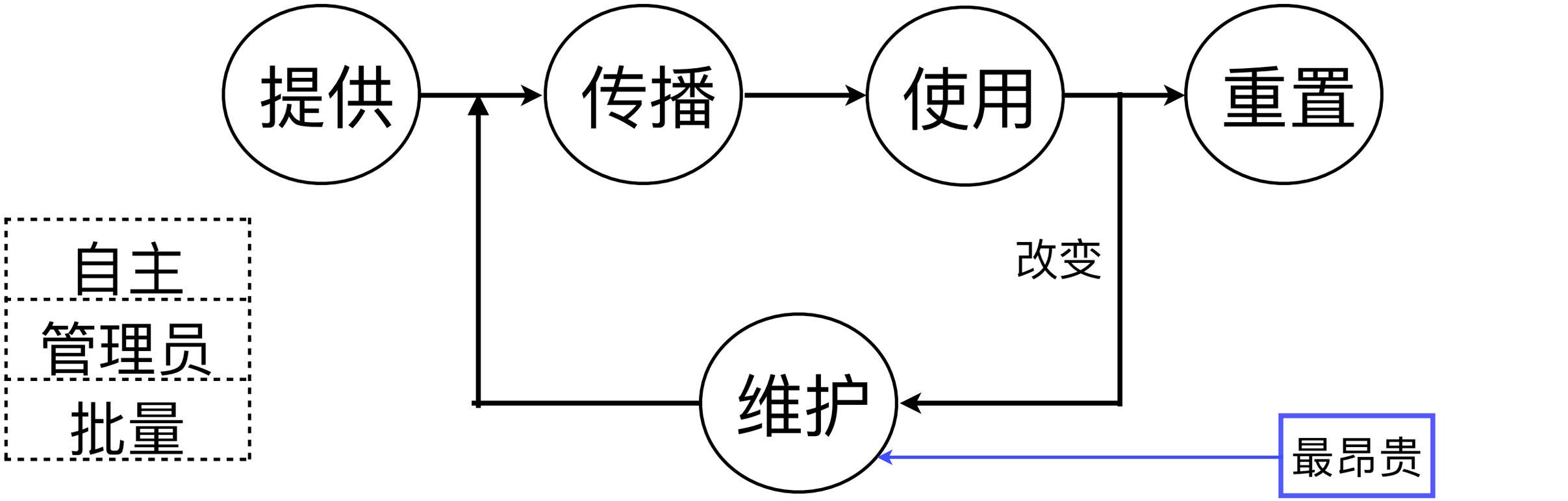

Unmasking Identity Management Architecture (IMA)
Digital Identity
O'REILLY®
Phillip J. Windley

数字身份

- 数字身份是一个实体的属性、喜好和特性的数据集合
  - 属性：病历、存款、信用、尺码、年龄等
  - 喜好：航班座位、商品牌子等
  - 特性：先天固有的



数字身份生命周期



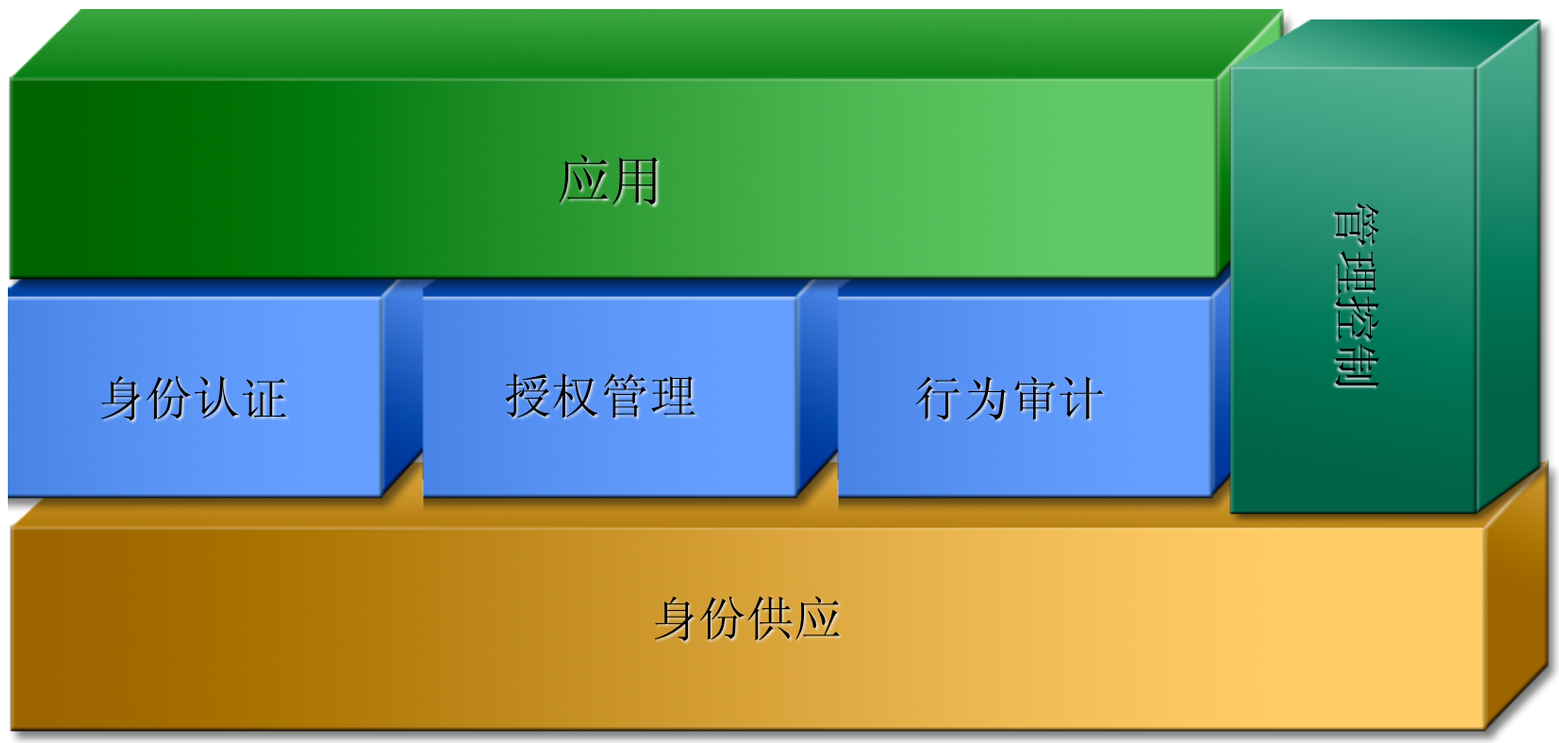
定义

- 定义

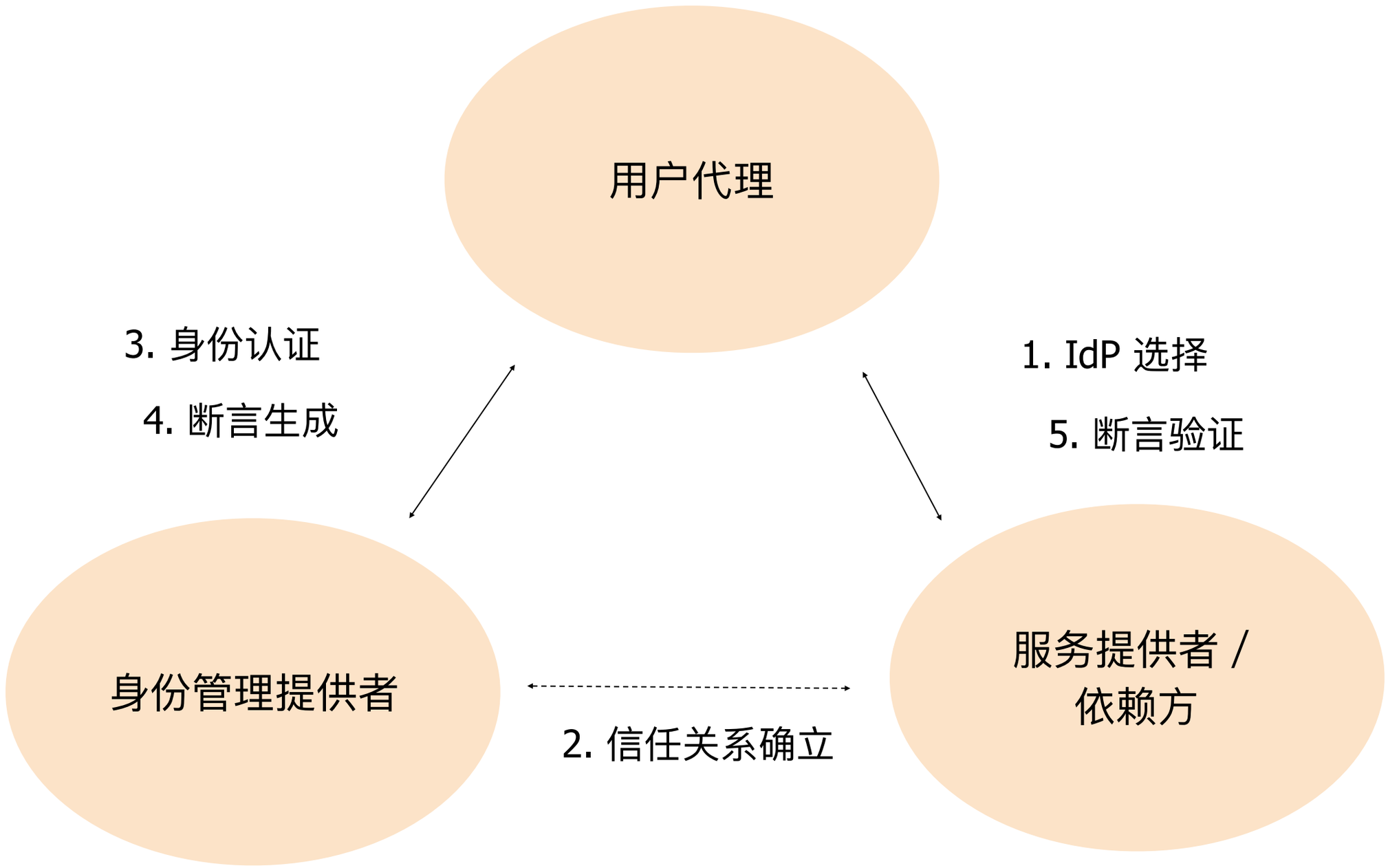
✴一系列创建、维护、管理和使用数字标识的软件、硬件、人员、管理、过程的集合

✴又称为身份和存取管理、IDM、IAM、AIM等

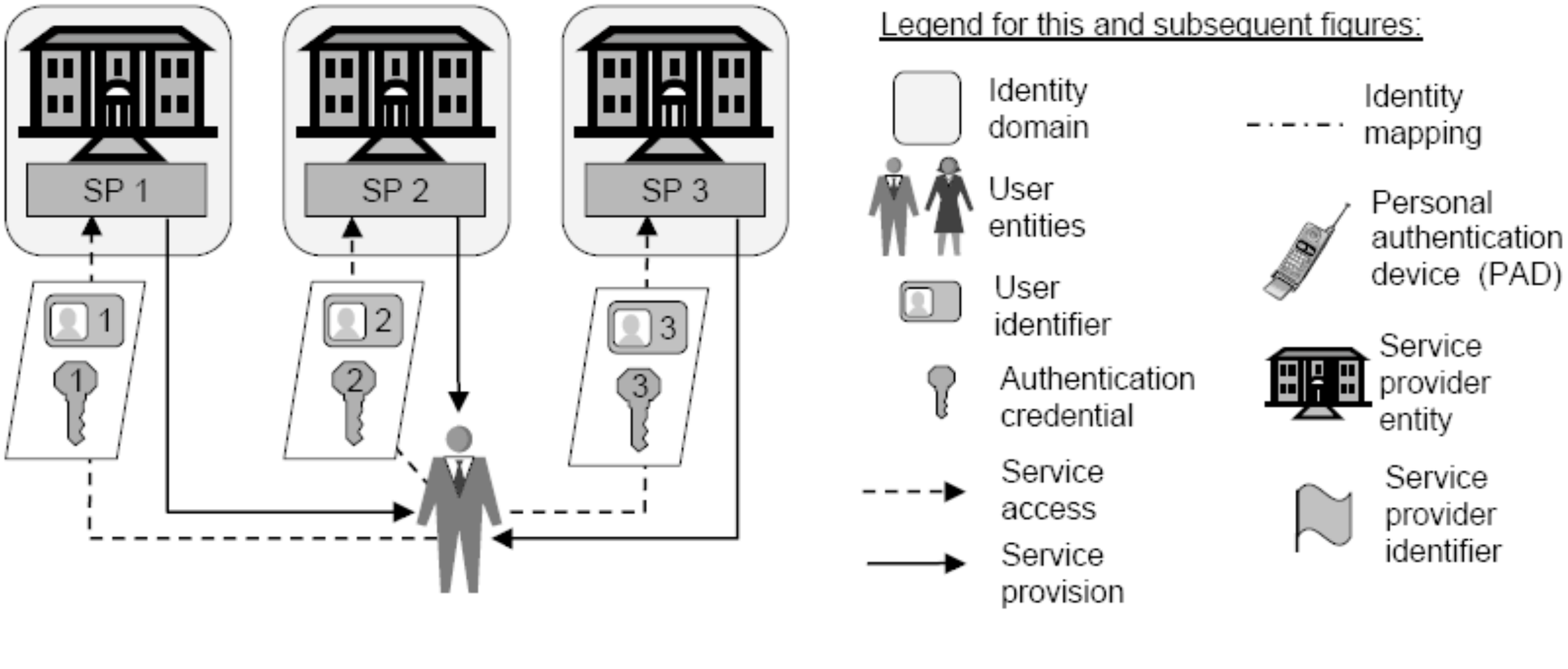
✴包括身份标识、身份认证、授权管理、访问控制、行为审计、责任认定、单点登录、隐私保护、信任管理等



身份管理参与方



孤立的IDM



Identifier和Credential均来自同一个服务提供商

服务提供商实现最简单，但是用户难于管理

Audi Josang and Simon Pope. *User Centric Identity Management.* In Proc. AusCERT'2005

联盟的IDM

需要一系列的协议、标准和技术来保证联盟域的互通

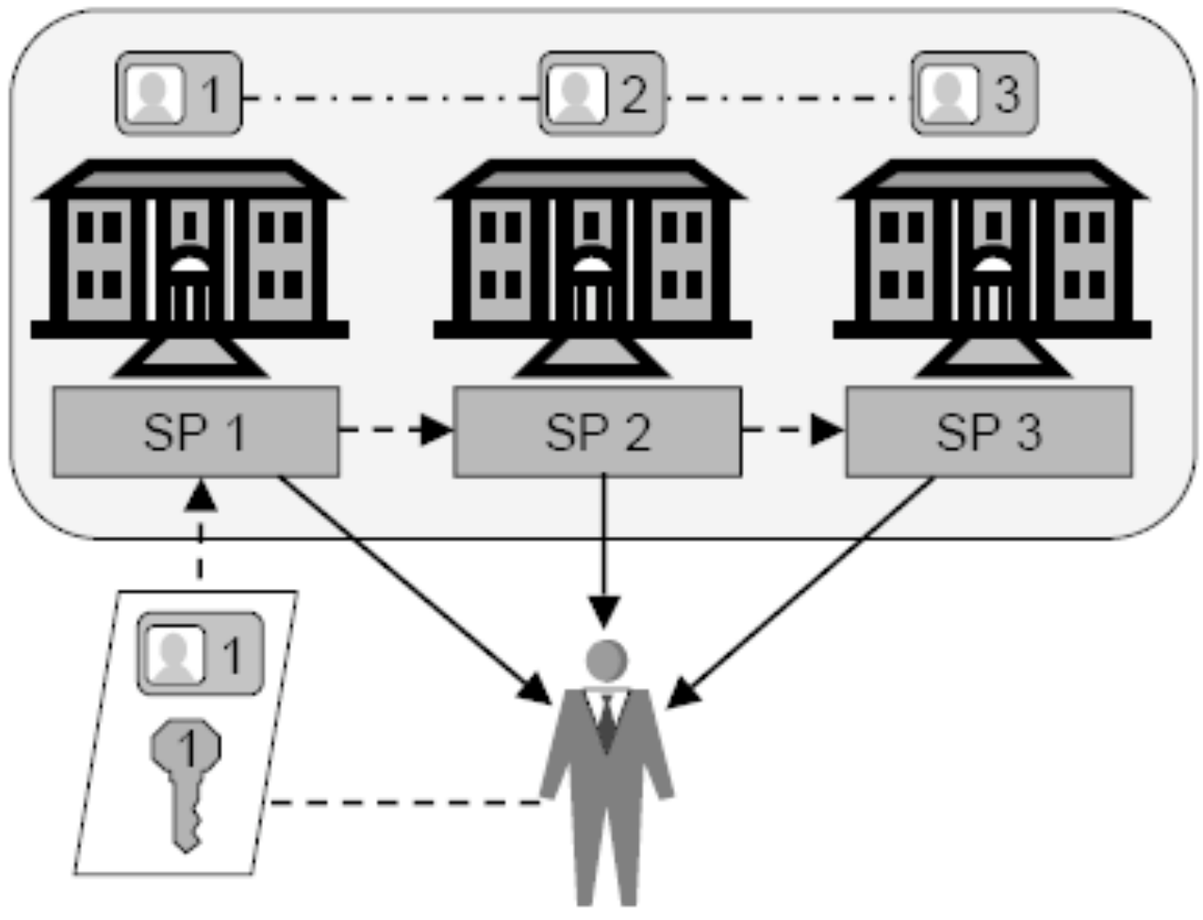
需要不同服务提供者之间建立信任管理，并通过传递Assertion实现存取

提供单点登录

SAML

Liberty Allicance

Shibboleth



集中的IDM

让一个独立的实体或者单一的权威来作为独家身份标识和凭证的服务提供墒

CA是最常见的形式

规模是最大的挑战

名字空间是否可控

常见的身份管理模型

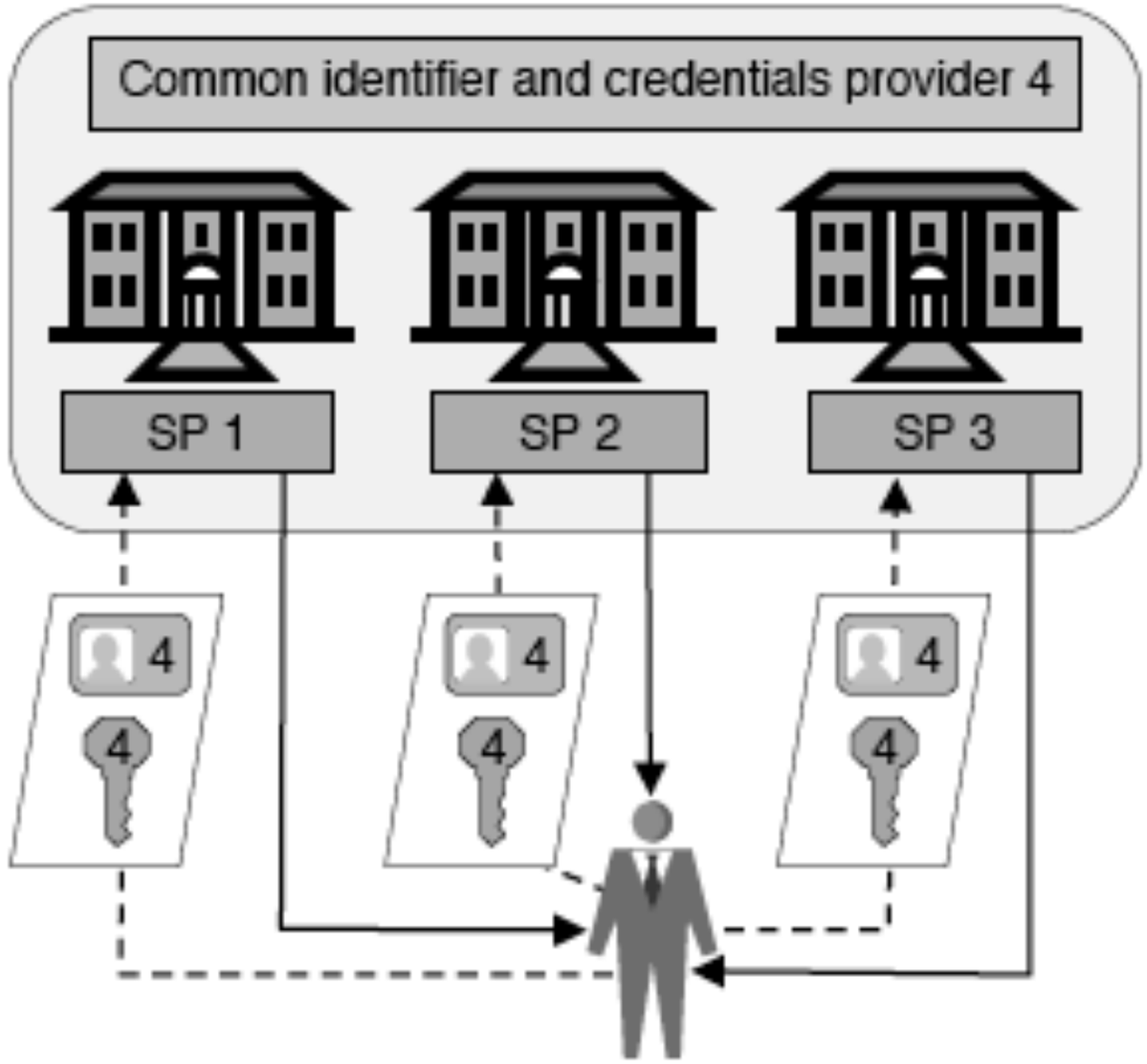


Figure 4: Common user identity model.

单点登录的IDM

一个服务提供商来提供用户认证，其余服务提供商认同这个认证结果

Kerberos

Microsoft Passport

单点登录身份管理模型

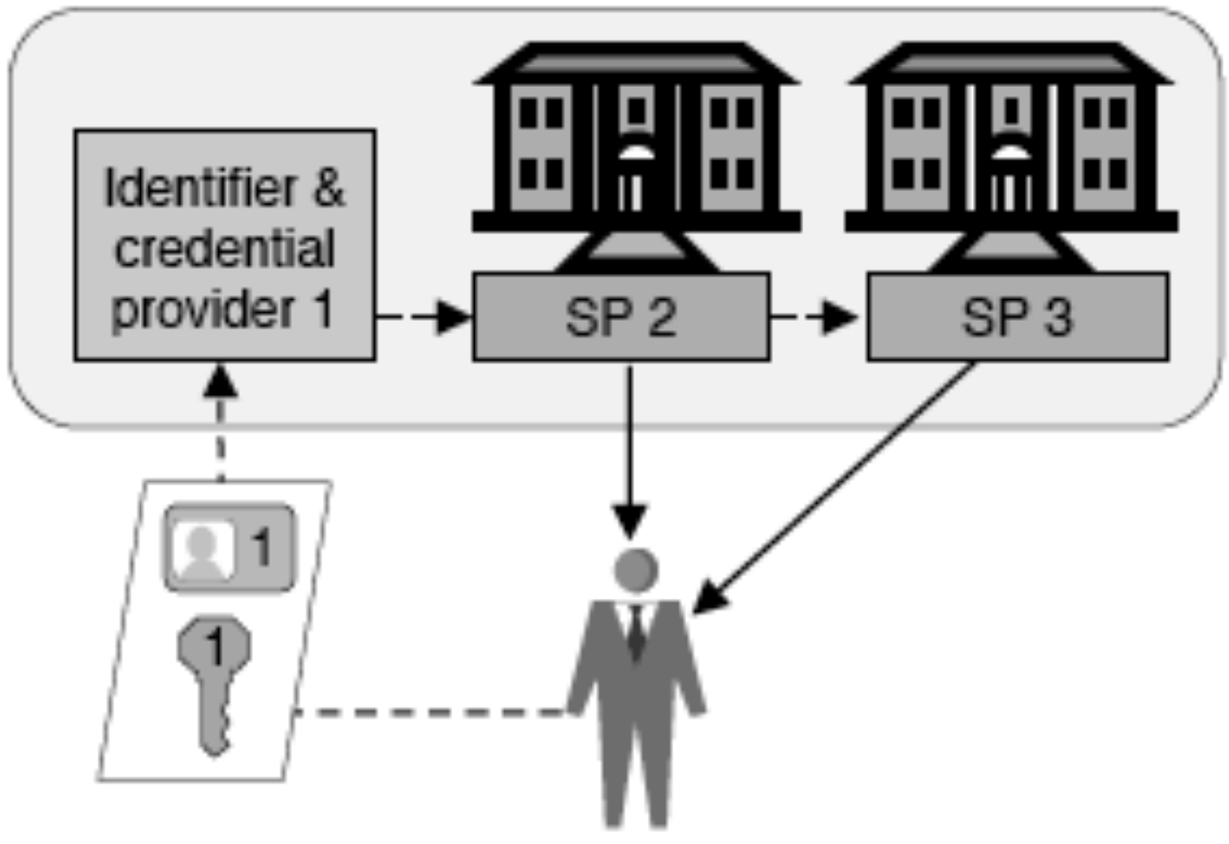


Figure 6: SSO identity model.

标准

- 可能需要的任何工具
- 需要在抑制统一的基础上创建的事物
- 为了做我们一致同意的事情，需要完成的工作

- 一些要素
  - ✶ 谁制定标准
  - ✶ 谁使用标准
  - ✶ 如何使用该标准

IEC

SAC

IETF

IEEE

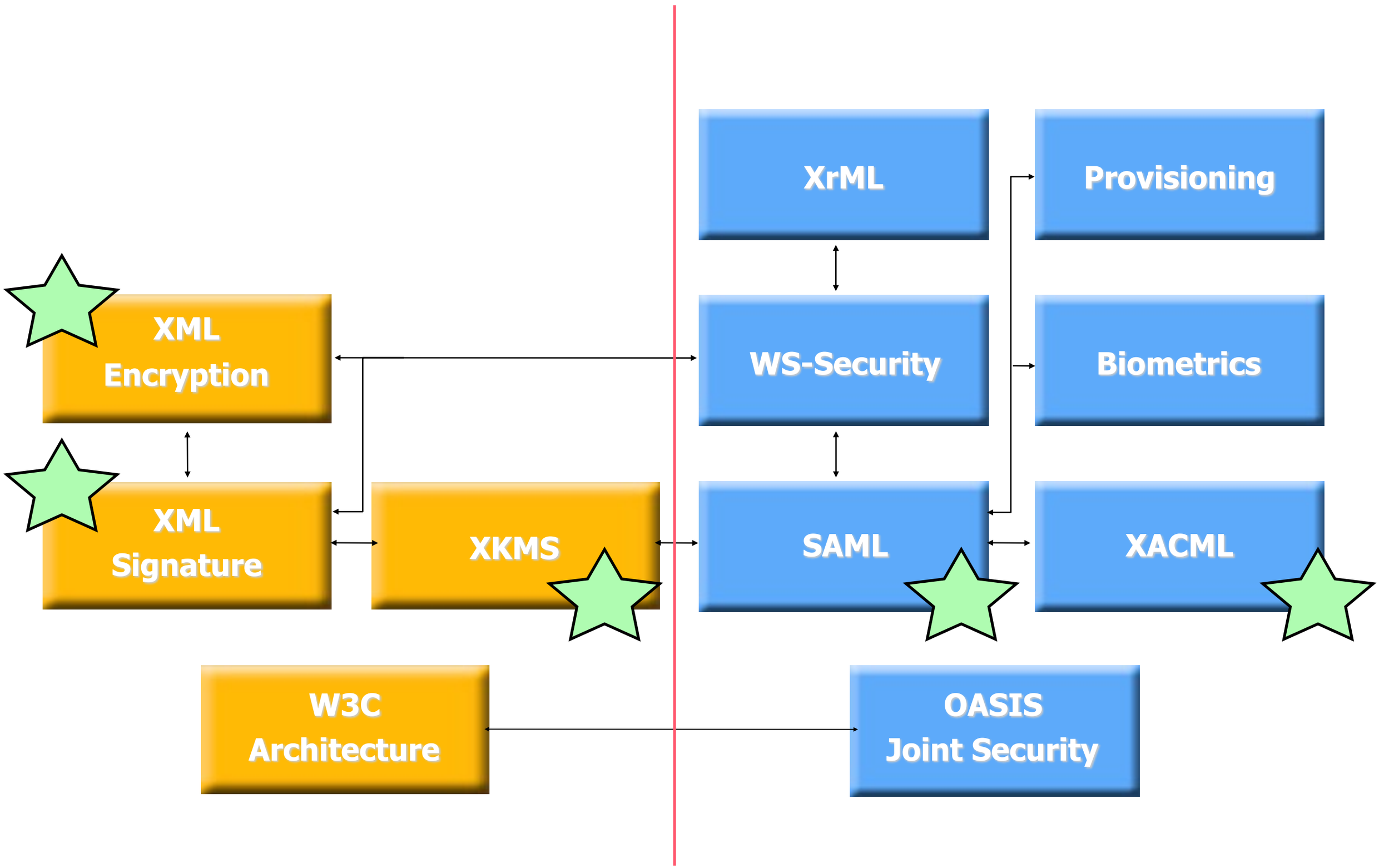
ISO International Organization for Standardization

OASIS

- 法定标准
  - ✶ 国际、区域、国家、行业、地方、企业
- 事实标准
  - ✶ 垄断标准
  - ✶ 联盟标准
    - ➡ 开放标准
    - ➡ 封闭标准

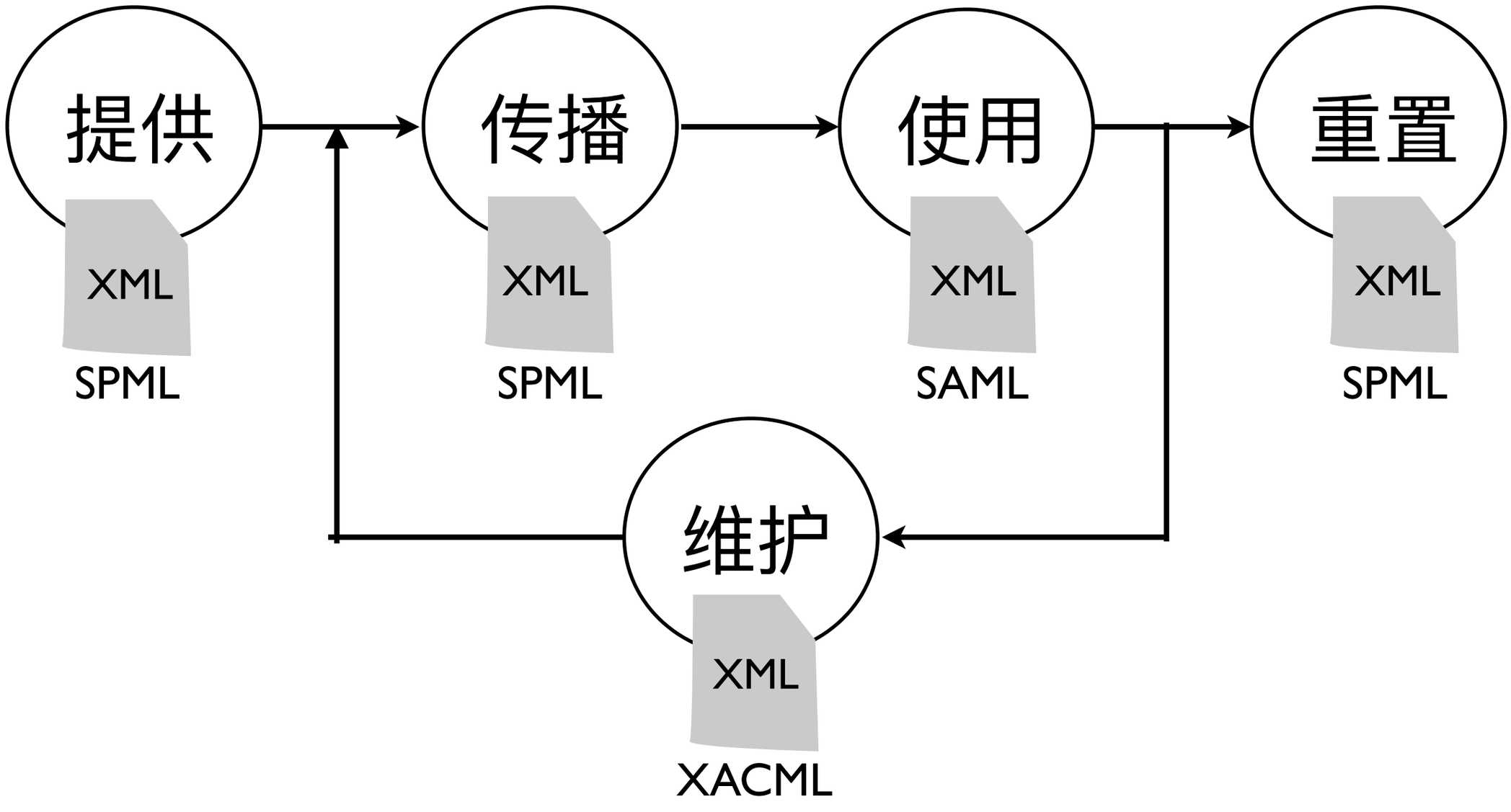
Identity Management

Web服务安全标准



Identity Management

身份管理标准



SPML

- Service Provisioning Markup Language、服务配置标记语言
- SPML的作用
  - ✴自动化IT配置任务
  - ✴不同配置系统之间的互操作性
- 一个场景
  - ✴拥有成千上万员工和大量IT系统、应用系统和外部伙伴系统的大公司
  - ✴公司和部门合并、新系统、新员工
  - ✴物理领域、数字环境

SPML

核心操作
ListTargets
Add
Lookup
Modify
Delete

异步
- status
- cancel

成批
- batch
- bulkModify
- BulkDelete

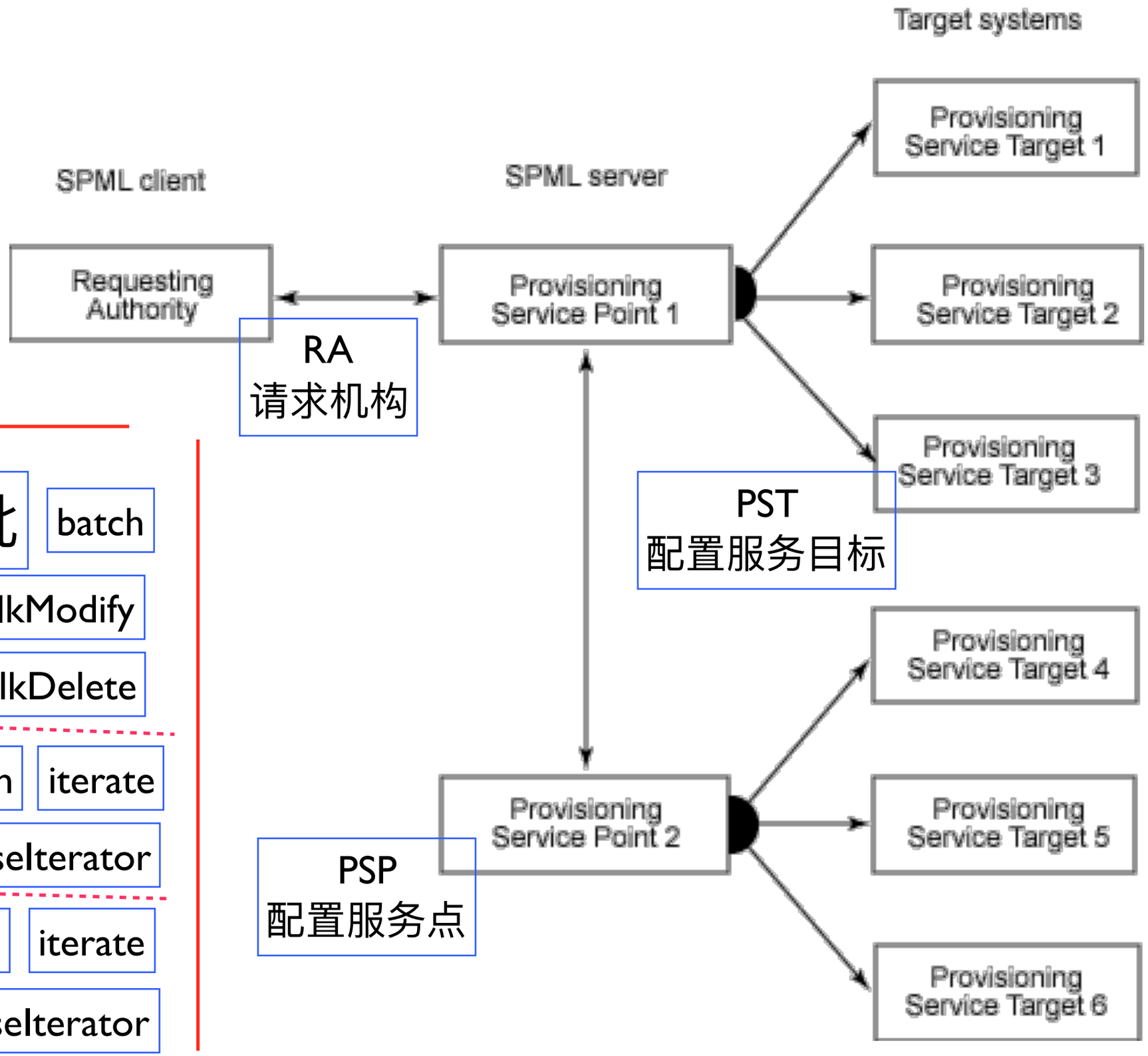
- setPassword
- expirePassword
- resetPassword
- validatePassword

- search
- iterate
- closeIterator

- suspend
- resume

active

- update
- iterate
- closeIterator



SAML

- Service Assertion Markup Language、安全断言标记语言
- SAML的作用

  ✴为了解决Web浏览去单点登录

  ✴用于不同安全域之间交换认证和授权数据

- 断言

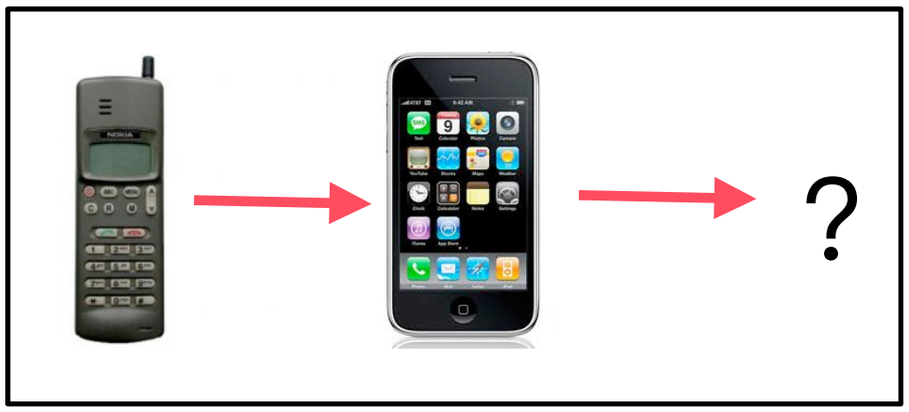
  ✴认证断言：确定用户身份

  ✴属性断言：确定特定主体信息

  ✴授权断言：确定特定主体是否得到授权

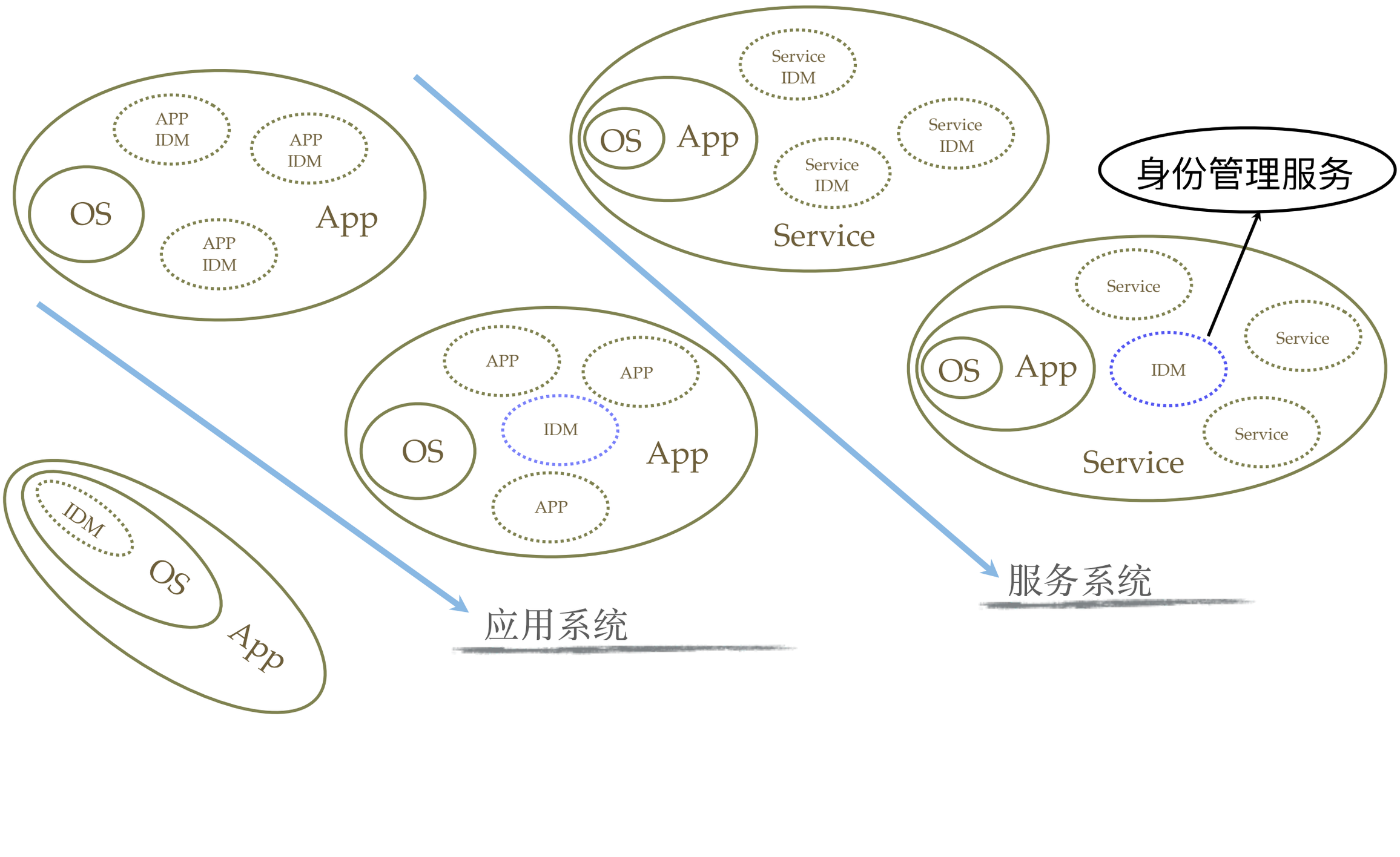
  ✴决定断言：报告一个特定授权请求的结果

计算模式变迁



Identity Management

身份管理服务



Homework 课后作业

- 要求阅读如下论文：

➡ *PACMAN: Personal Agent for Access Control in Social Media. In IEEE Internet Computing 2017.*

下次上课测试！

谢谢！

孙惠平

sunhp@ss.pku.edu.cn