Windows安全原理与技术

— 第一章：Windows系统安全概述

王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

Eric简介

- 工作单位：上海交通大学 信息安全学院
  网络攻防课题组
- 办公地点：闵行校区电信群楼1号楼111室
- 联系方式： 021-34205982
  Ericwyj@sjtu.edu.cn
- 研究方向：信息安全（网络攻防、系统安全、…）
- 科研成果：保密☹

课时安排（总共54课时，3个学分）

章节名称	讲授课时
第01章 - Windows系统安全概述	4
第02章 - Windows NT安全	3
第03章 - Windows 2000安全基础	1
第04章 - 活动目录	4
第05章 - 身份验证	2
第06章 - 访问控制	2
第07章 - 文件系统安全	4
补充内容 - 网络协议脆弱性分析	4
第08章 - 网络传输安全	4
第09章 - 应用服务安全	4
补充内容 - Windows 远程控制、Rootkit及检测分析	6
第10章 - 组策略	2
第11章 - 安全配置与分析	2
第12章 - 安全审核	2
第13章 - 公钥基础结构	4
补充内容 - Windows Vista安全	4
考试复习	2
总计	54

考核方式

- 平时考勤 15%
- 论文/课程设计 15%
- 期末考试 70%
  - 考试形式：闭卷。
  - 考试题型：判断、单选、多选，问答。

引言：Windows

- **Windows是什么？**

  当然是“操作系统”拉！

  - 窗口？
  - 硬件？
  - 软件？

引言：Windows的使用

- Windows的使用情况
  - Windows 95/98/Me
  - Windows NT
  - Windows 2000
  - Windows XP
  - Windows Server 2003
  - Windows Vista
  - Windows 2008
  - 非Windows，Linux，Unix，Mac…

引言：Windows的安全

- 是否考虑过Windows的安全？
  如何保证Windows的安全？

让我们讨论一下...

  - 个人主机上的Windows 系统。
  - 企业服务器上的Windows系统。
  - 移动设备上的Windows系统。
  - ...

引言：现今的网络攻击主流技术

- 缓冲区溢出
  - 服务器软件溢出
  - 客户端软件溢出
- 数据库SQL注入
- 跨站脚本攻击（XSS，CSRF）
- 数据嗅探
  - 以太网（包括交换环境）
  - 无线网
- 内核木马病毒（Rootkit）
  - 通信隐蔽、自启动项隐藏、文件隐藏、进程/模块隐藏、注册表隐藏、服务隐藏、端口隐藏等。

引言： Windows系统的安全需求

- 安全威胁的来源多种多样
  - 系统主机层面
  - 应用服务层面
  - 网络通讯层面
  - 安全管理层面

引言： Windows系统的安全需求

- 用户规模不同，其相应的安全需求也不尽相同
  - 单个用户
  - 小、中规模组织或单位
  - 大规模组织或单位

Windows系统的历史简介

Windows 9x内核系列的发展	Windows NT内核系列的发展
1983年11月：Windows宣布诞生	
1985年11月：Windows 1.0	
1992年4月：Windows 3.1	
	1993年5月：Windows NT 3.11
1994年2月：Windows 3.11	1994年9月：Windows NT 3.5
1995年8月：Windows 95	1995年6月：Windows NT 3.51
	1996年8月：Windows NT 4.0
	1997年9月：Windows NT 5.0 Beta 1
1998年6月：Windows 98	1998年8月：Windows NT 5.0 Beta 2
1999年5月：Windows 98 SE	1999年4月：Windows 2000 Beta 3
1999年11月：Windows Millennium Edition Beta 2	
2000年9月：Windows Me	2000年2月：Windows 2000
	2000年10月：Windows Whristler Beta 1
2001年1月：Windows 9x内核正式宣告终止	2001年10月：Windows XP
	2003年5月：Windows Server 2003
	2007年1月：Windows Vista
	2008年2月：Windows Server 2008

Windows的成功之处

- 直观、高效的面向对象的图形用户界面，易学易用。
- 用户界面统一、友好、美观。
- 多任务。
- 大量的函数调用。
- 和设备的无关性
- 内存管理
- 丰富的Windows软件开发工具。
- 面向对象式的程序设计思想。

Windows NT的基础与安全

- **Windows NT系统的历史使命**
  - 面向工作站、网络服务器和大型计算机的网络操作系统，也可作为个人计算机的操作系统。
- **Windows NT系统的版本**
  - Windows NT Workstation
  - Windows NT Server

Windows NT系统的特点

- 32位操作系统，多重引导功能，可与其他操作系统共存。
- “抢先式”（preemptive）多任务和多线程操作。
- 采用SMP（对称多处理）技术，支持多CPU系统。
- 支持多种硬件平台。
- 支持多种网络协议，可与各种网络操作系统互操作。
- 安全性达到美国国防部的C2标准。

Windows NT所引入的安全特性

- NTFS（Windows NT File System）
- 用户账户（User Account）
- 域（Domain）
- 工作组（Workgroup）
- 权限（Right）
- 许可（Permission）
- 共享权限 （Share Permission）
- 安全审核 （Security Audit）

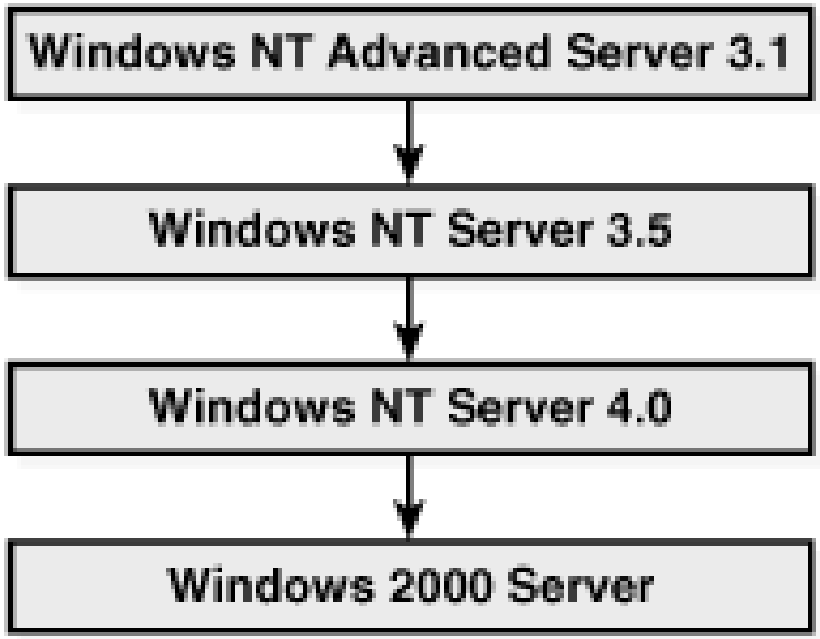
Windows 2000的基础与安全

- **Windows 2000系统**
  - 保留了部分NT系统的内核。
  - 增加了大量的内容，大部分集中在安全方面。
    - 以活动目录为核心。
    - 存在着安全功能的诸多新方面。

Windows 2000系统的版本

- **Windows 2000 Professional**
  - Windows NT 4.0 Workstation的替代产品
  - 桌面用户和移动用户
- **Windows 2000 Server**
  - Windows NT 4.0 Server的替代产品
  - 主流的工作组和部门商务服务器
- **Windows 2000 Advanced Server**
  - Windows NT 4.0 Server Enterprise Edition的替代产品
  - 中等应用范围的服务器解决方案
- **Windows 2000 Datacenter Server**
  - 新增
  - 针对企业部属与解决方案进行了优化

Windows 2000内核的发展过程



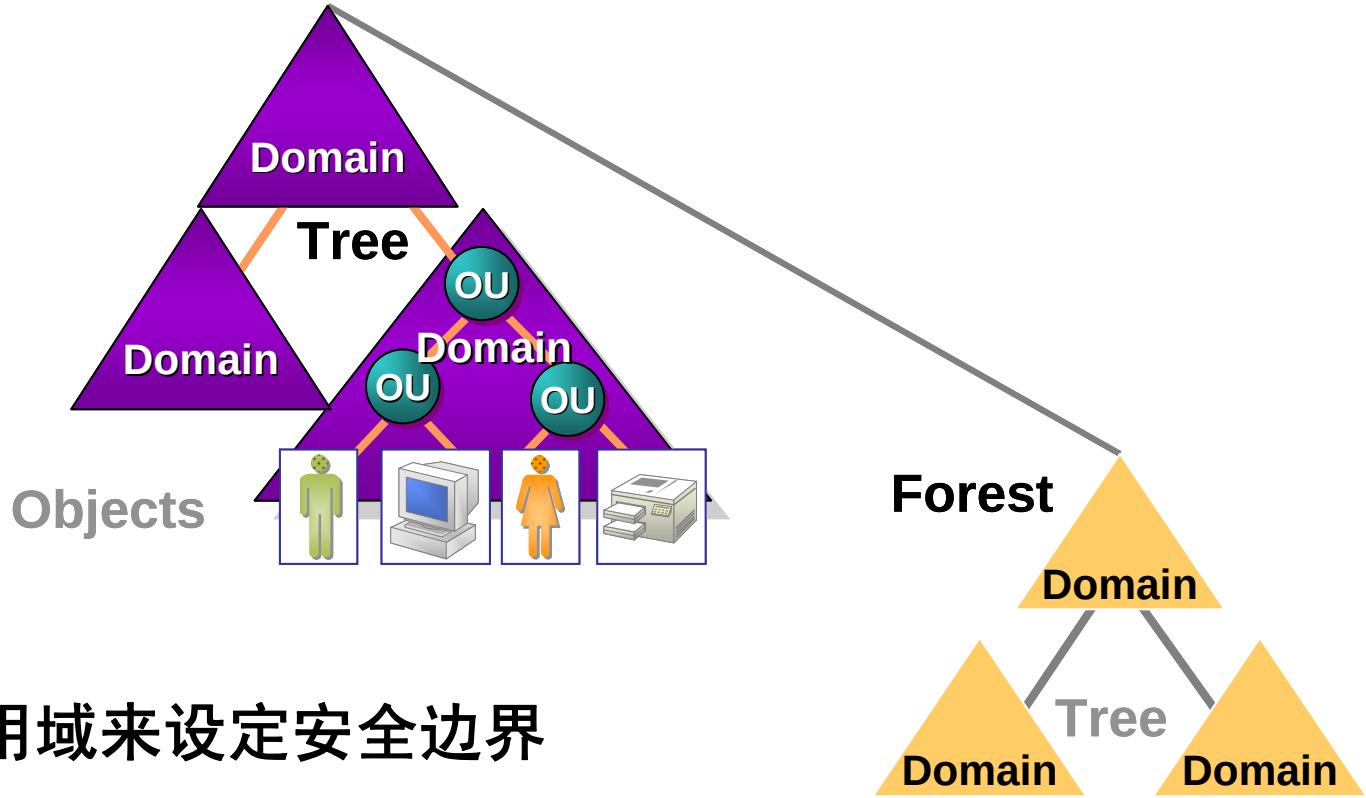
Windows 2000新增安全特性

- 活动目录（Active Directory, AD）
- 公钥基础结构（Public Key Infrastructure, PKI）
- 组策略对象（Group Policy Object, GPO）
- Kerberos协议
- IP安全协议（IPSec）
- 加密文件系统（EFS）
- 安全配置工具集

活动目录

- 活动目录提供了完全集成在Windows 2000中的一个安全、分布式、可扩展以及重复的分层目录服务。
  - Windows 2000安全模型灵活性与可扩展性的核心。
  - 提供了关于网络中所有对象的信息。
  - 简化了一般的管理任务。
- 活动目录包含的内容
  - 目录
  - 目录服务

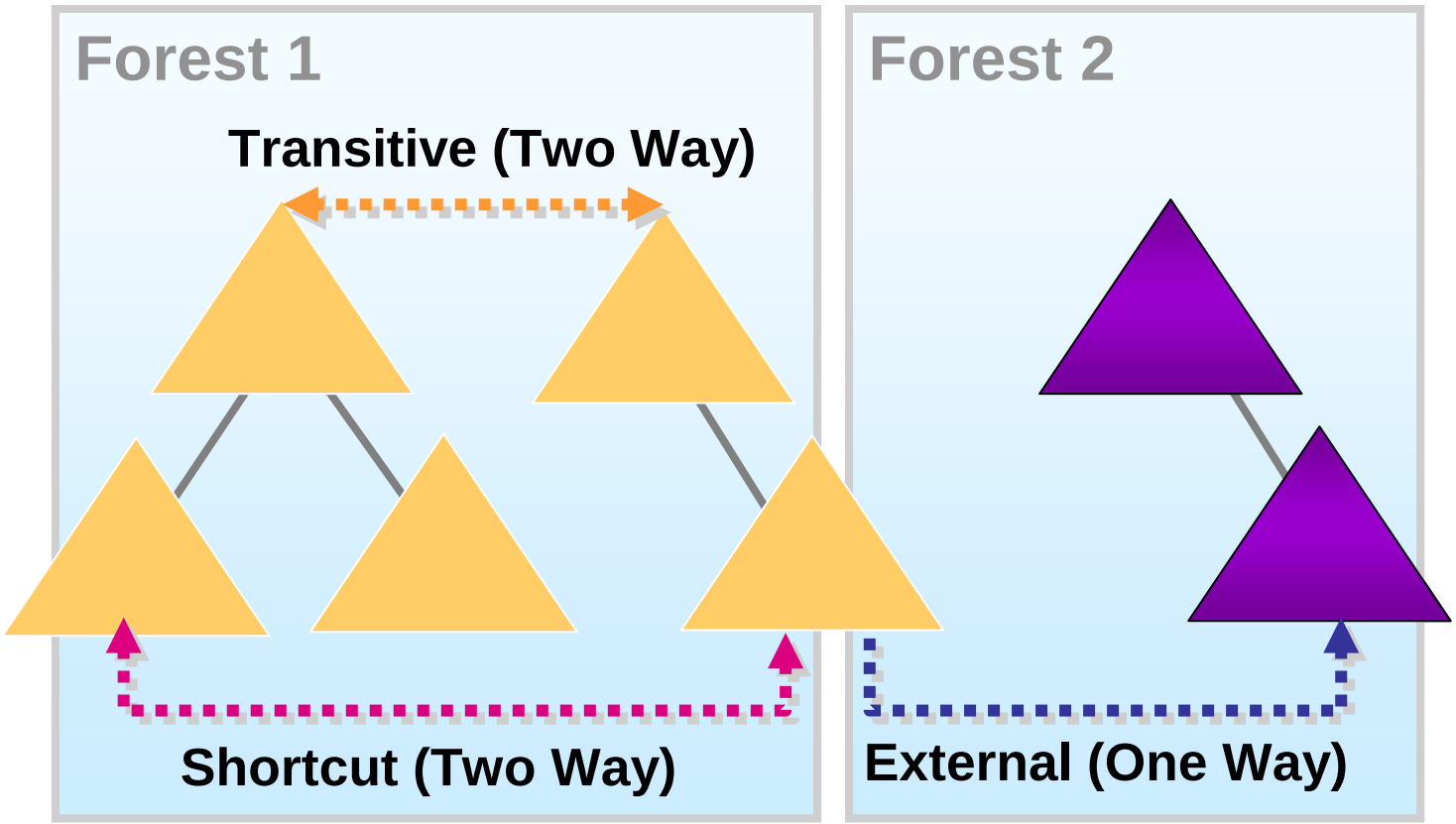
活动目录的层次结构



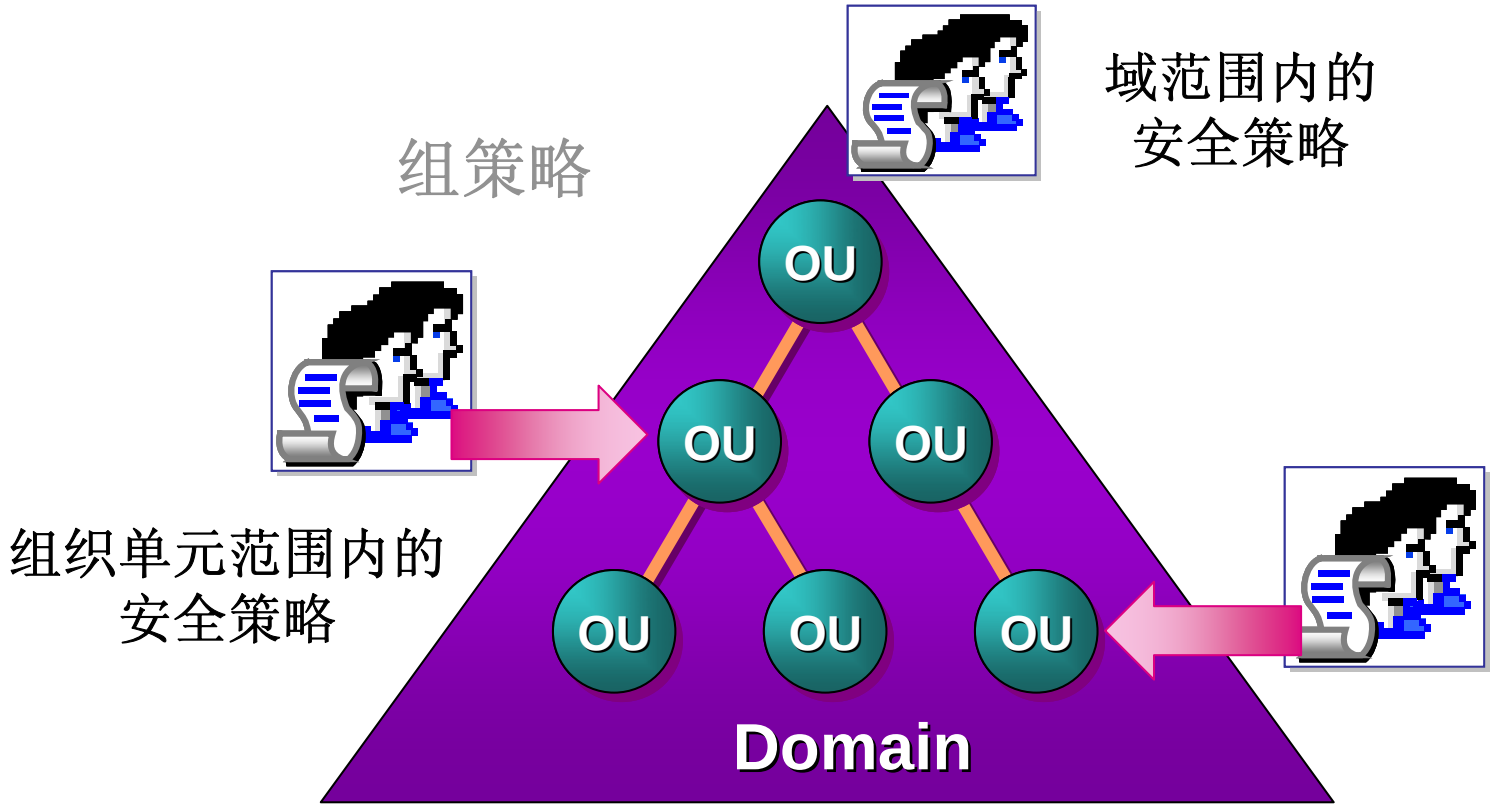
- 使用域来设定安全边界
- 使用组织单元来支持安全设置
- 提供管理员职责的授权和委派

信任关系

- 所有Windows 2000中的信任关系（在森林范围内）都是双向可传递的。



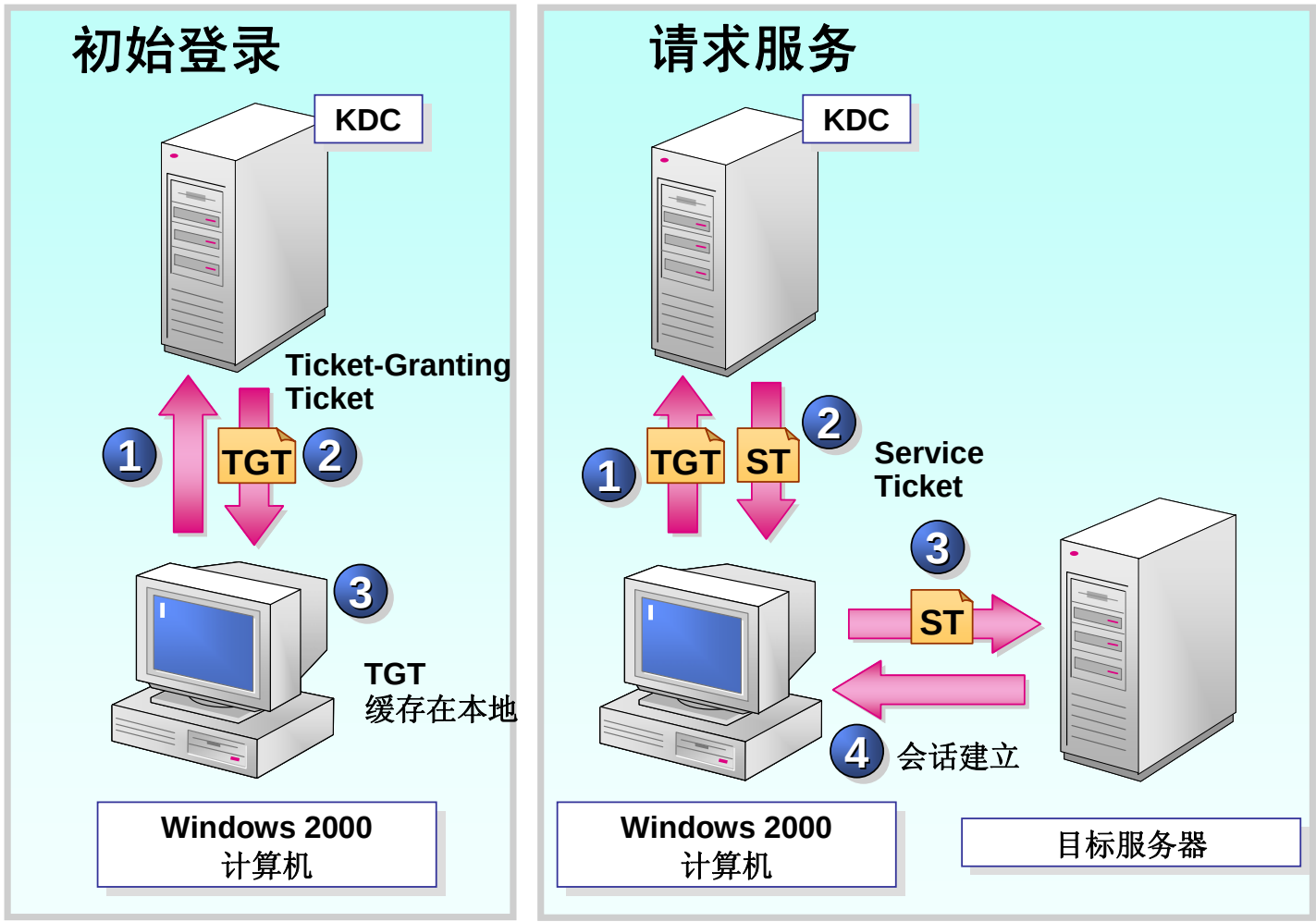
使用组策略进行管理



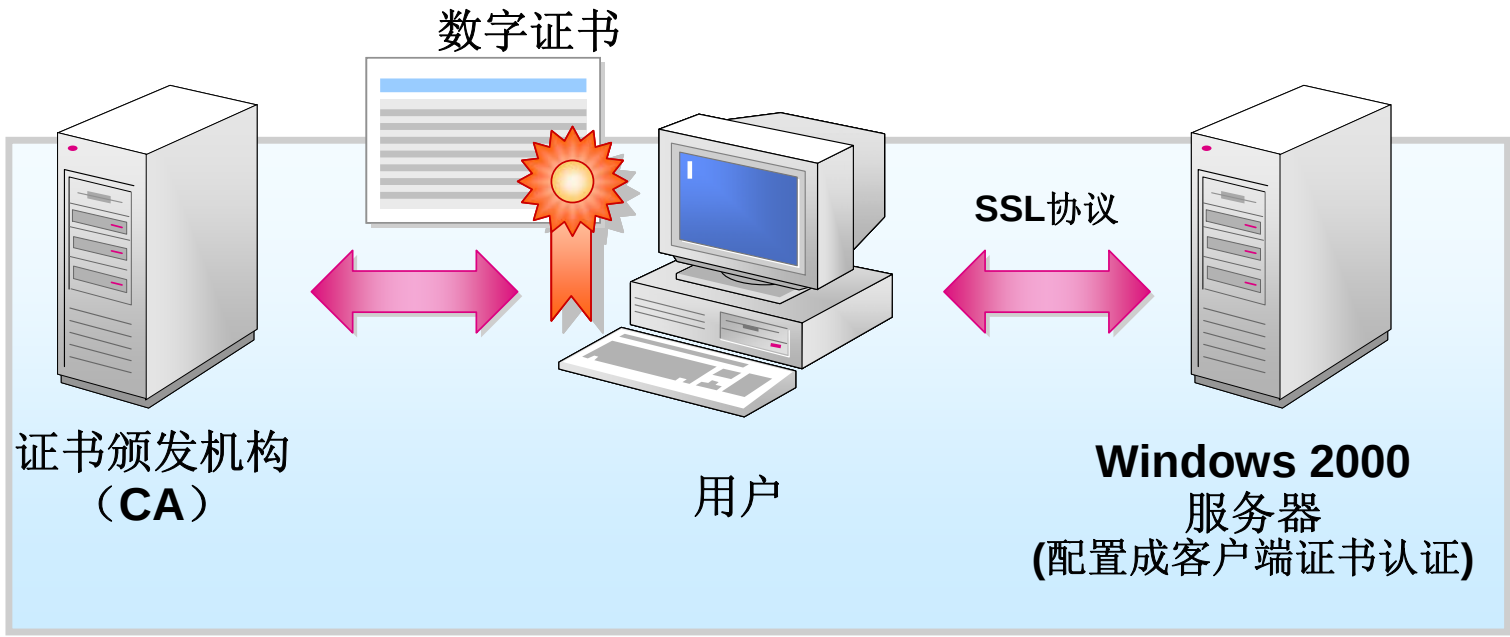
用户帐户的认证机制

- 基于Kerberos V5 协议的认证
- 基于数字证书的认证
- 基于NTLM协议的认证

基于Kerberos协议的认证

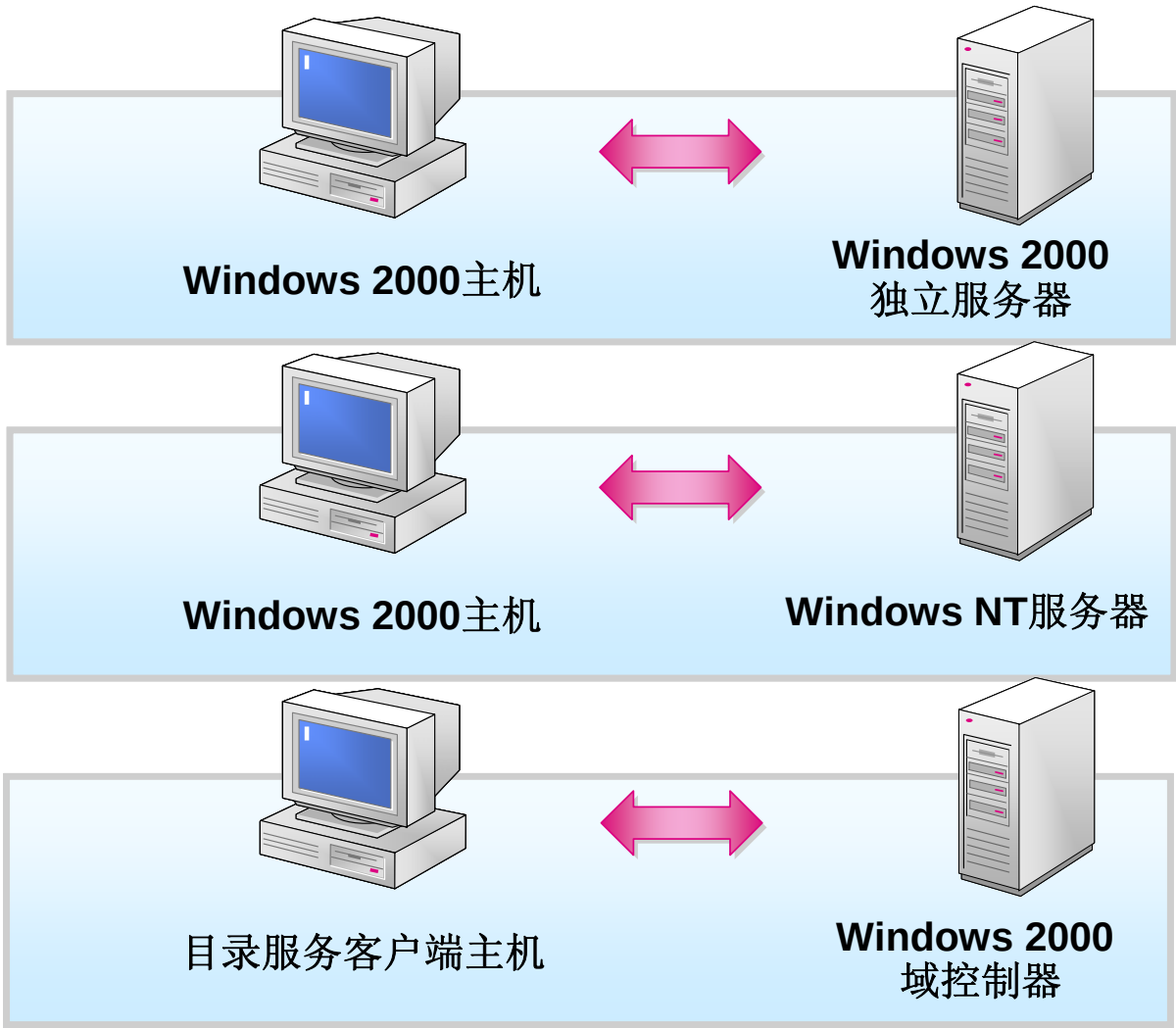


基于证书的认证



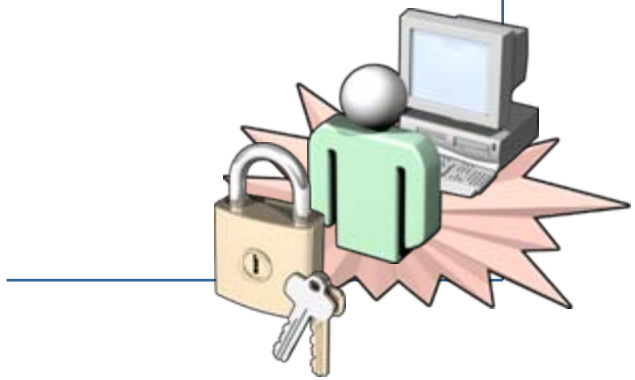
- 证书被映射成为活动目录帐户。
- 能够实现智能卡的认证。

基于NTLM协议的认证

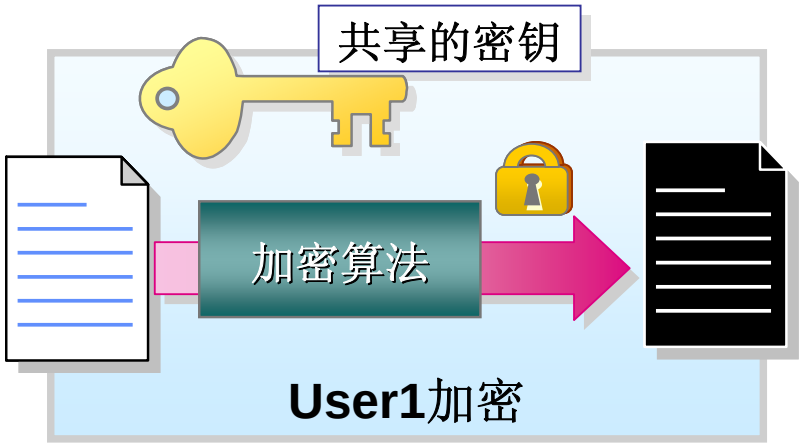


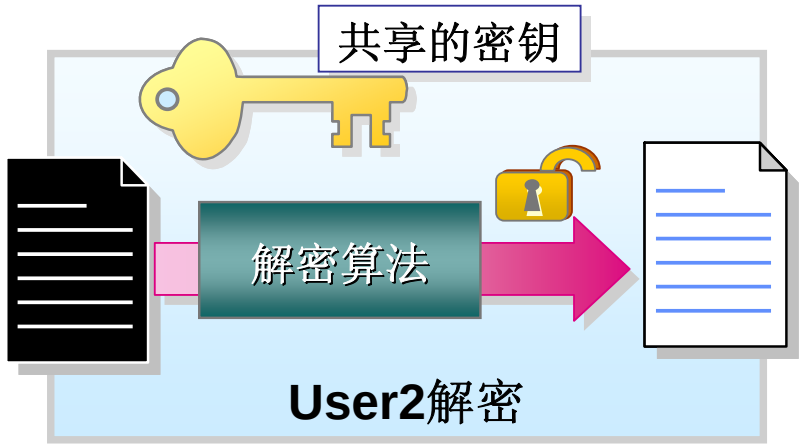
加密技术

- 加密技术
  - 对称加密
  - 公钥加密
  - 数字签名
- 加密应用
  - 加密存储在磁盘上的数据
  - 加密在网络上传输的数据

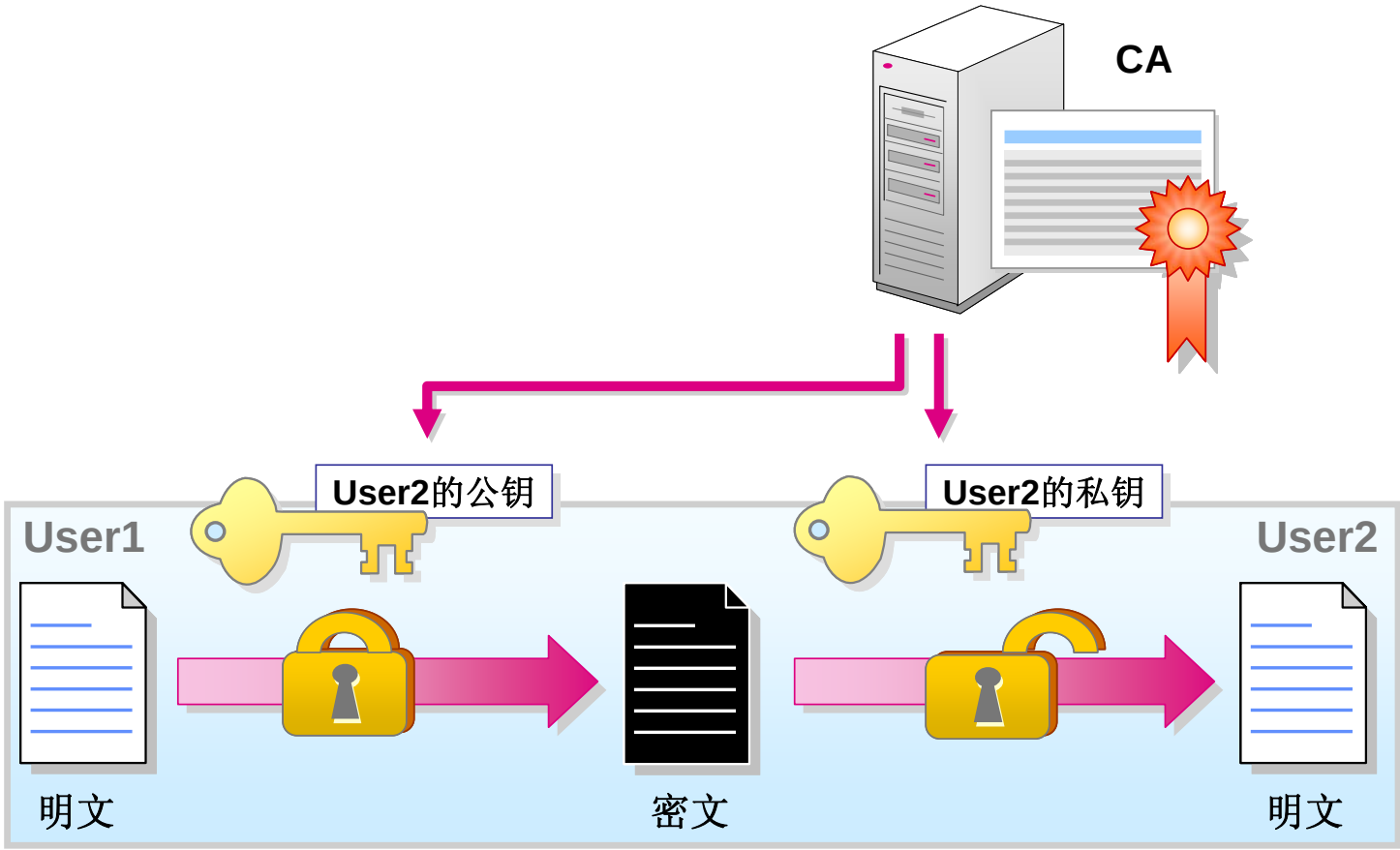


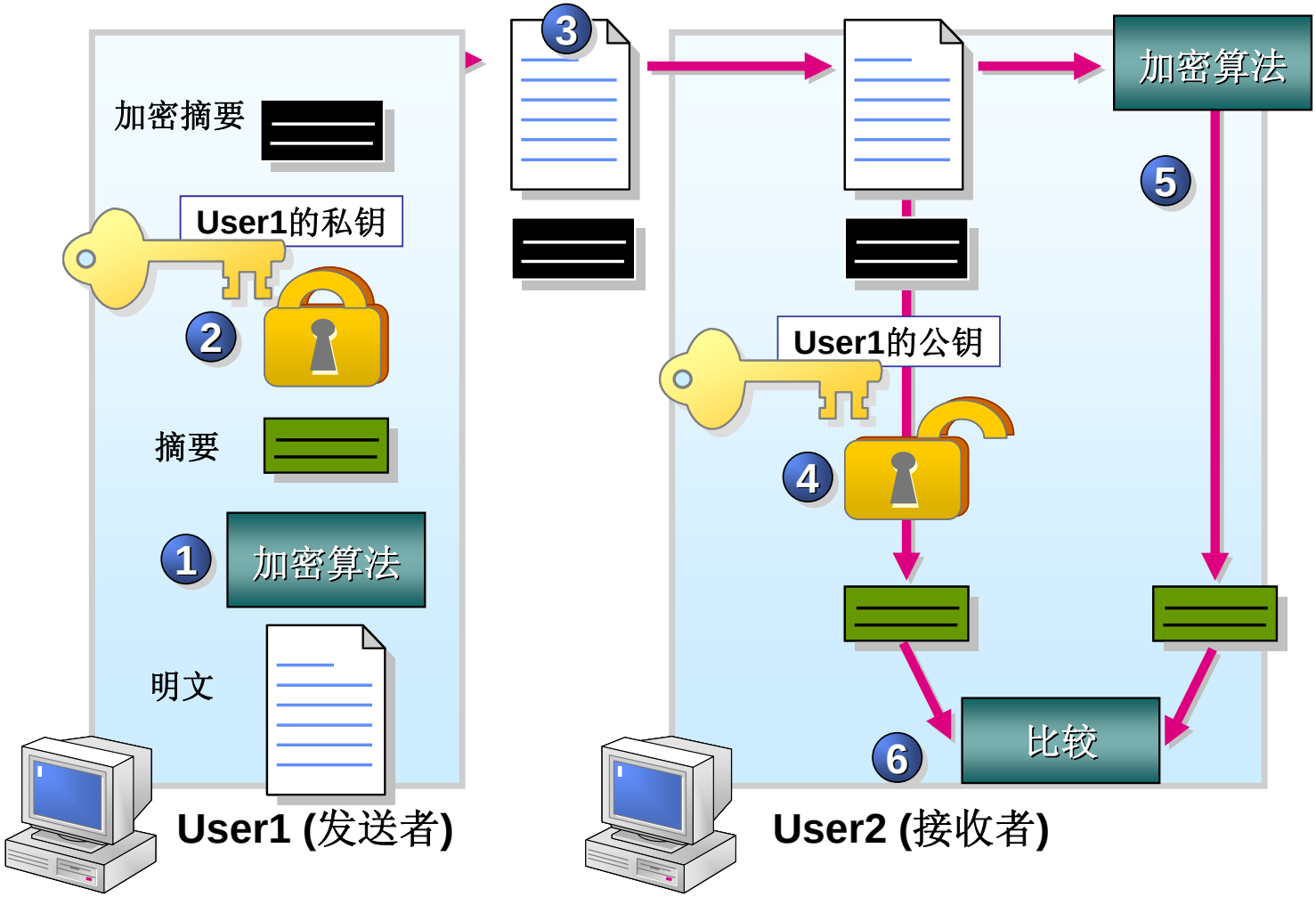
对称加密算法





公钥加密算法




加密摘要
User1的私钥
2
摘要
1
加密算法
明文
User1 (发送者)
3
加密算法
5
User1的公钥
4
6
比较
User2 (接收者)

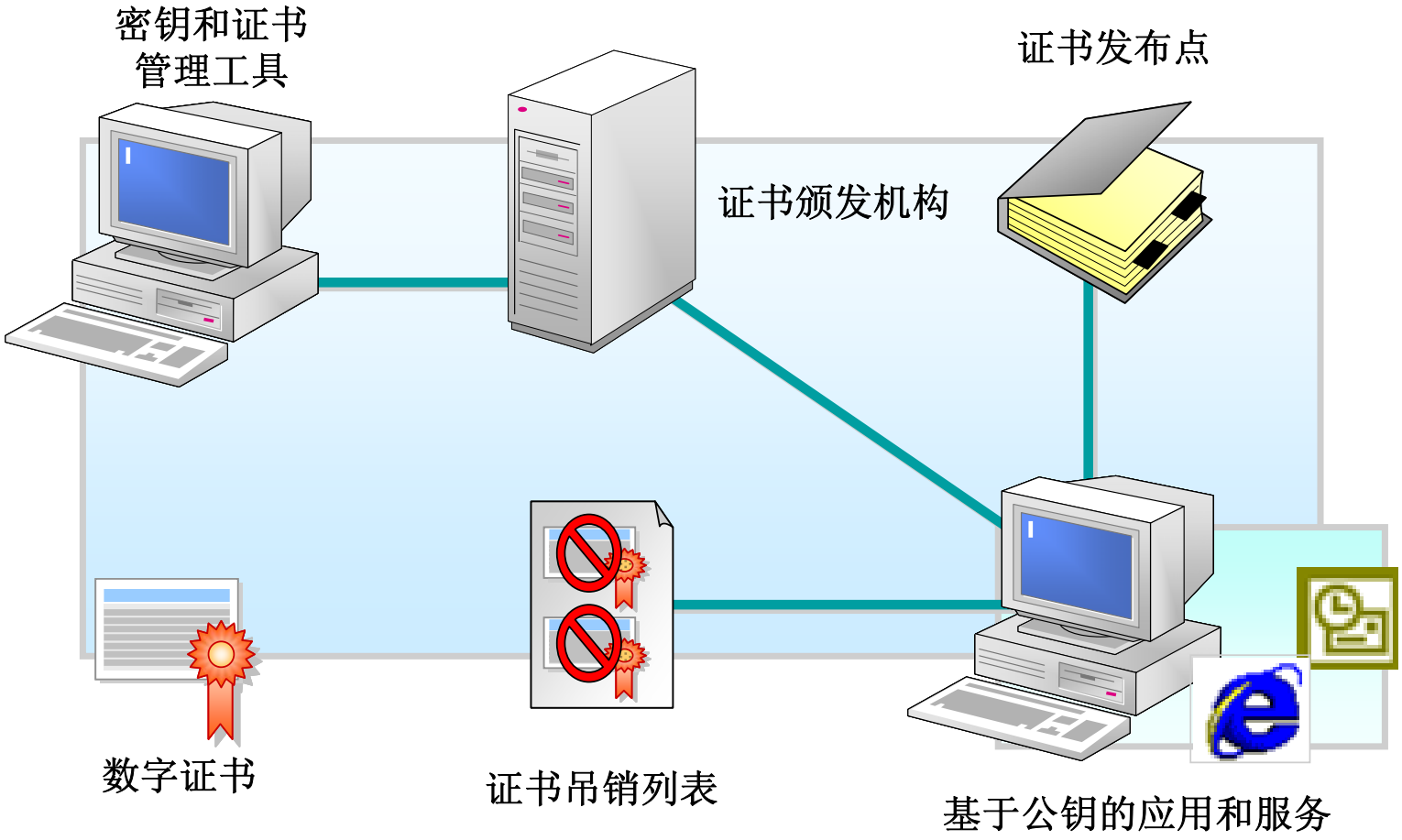
加密文件系统（EFS）

- EFS保护在磁盘上存储的数据。
- 使用“文件加密密钥”来加密数据。
- “文件加密密钥”也被以下的密钥进行加密：
  - 用户的公钥
  - EFS 恢复代理的公钥

网络上的加密保护

- IPSec在IP层加密数据
- SSL在应用层加密数据

PKI组件



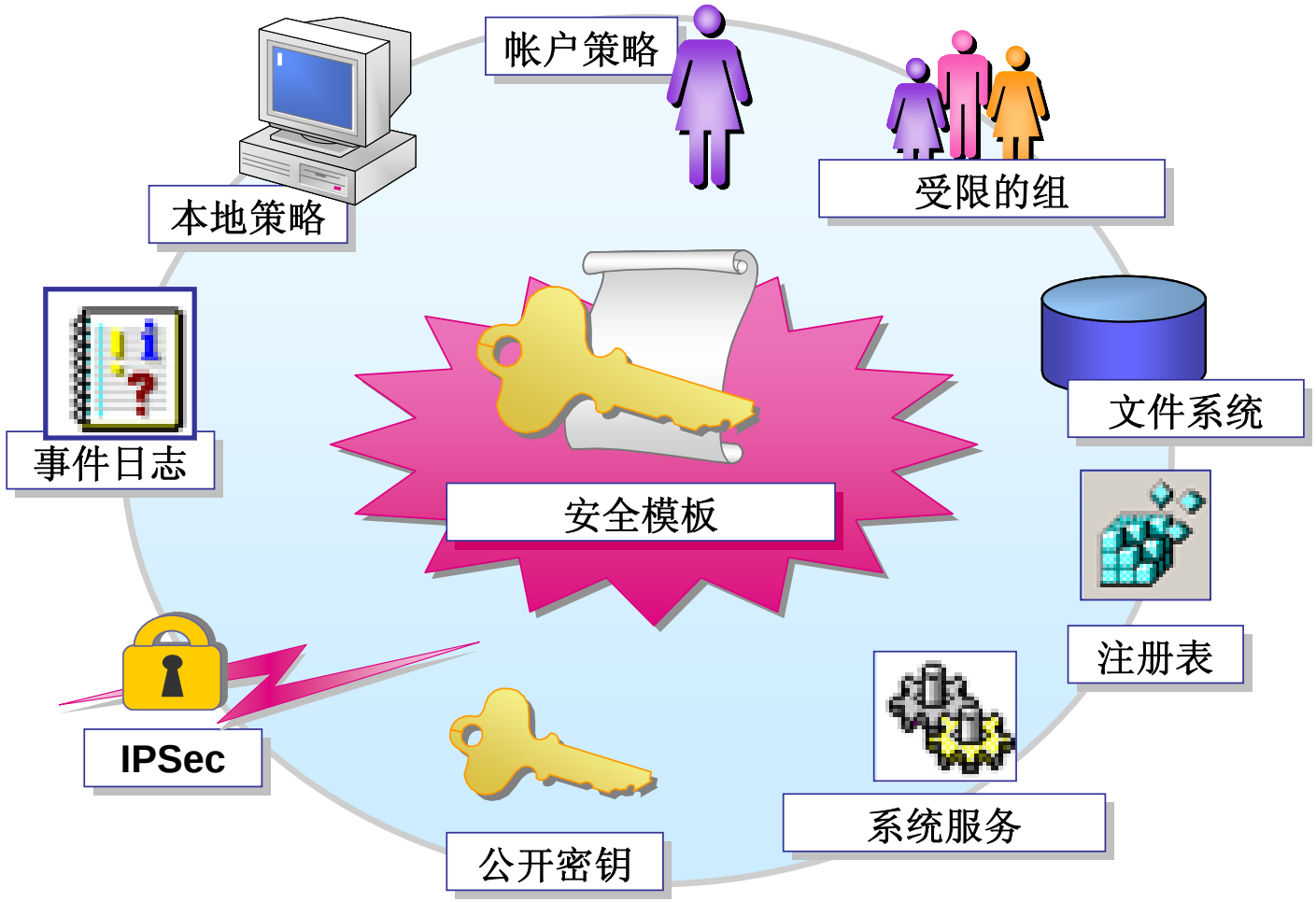
数字证书


客体标识
发布者标识
CA颁布的ID
扩展选项
Subject: eric
Issuer: CA-InfoSec
Subject's Public Key:
Serial Number: 29483756
Not Before: 6/18/03
Not After: 6/18/06
Secure E-mail Client Authentication
Signed: Cg6&^78
Subject的公钥值
有效期限
CA的数字签名

安全配置工具

- 安全模板
- 安全配置和分析工具

安全配置的区域



Windows 2000的其他安全性

- 核心模式写保护
- Windows文件保护
- 驱动程序签名

SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消