信息安全综合实践

第三讲 密码技术及应用

网络空间安全学院 孟魁

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

内容安排

密码学概述

- 密码学是一门古老而年轻的科学

“密码学是关于如何在敌人存在的环境中通讯”

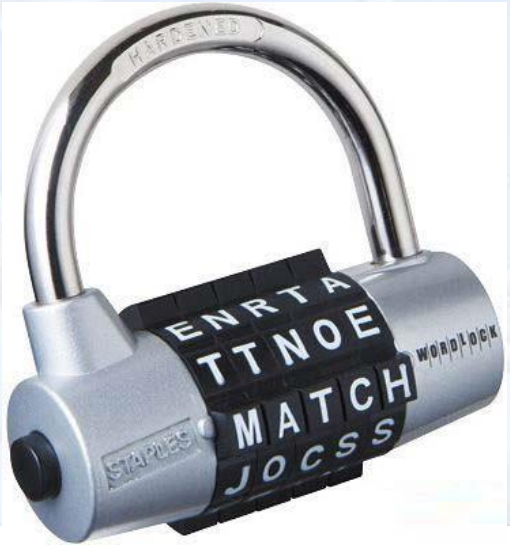
---Ron Rivest

“人类使用密码的历史几乎与使用文字的时间一样长”。

--美国学者戴维·卡恩《破译者》，1967

密码学概述

- 密码学(Cryptology)
  - 是数学的一个分支
  - 是密码编码学(Cryptography)和密码分析学(Cryptanalysis)的统称
    - 密码编码学：使消息保密的技术和科学，主要内容是密码体制的设计
    - 密码分析学：破译密文的科学和技术，主要内容是密码体制的破译



密码学发展史


计算强度小
加密算法需保密
计算量巨大
算法及密钥均可公开
手工阶段
• 古代加密方法
• 象形、隐写…
机械阶段
• 古典密码
• 1949年以前
• 密码机
计算机阶段
• 现代密码
• 1949～1975年
公钥阶段
• 公钥密码
• 1976年开始
新型密码
• 量子密码、DNA密码
• 对称密码发展
计算强度大
加密算法可公开
密钥需保密

密码算法分类

- 按保密内容分类
  - 受限制的算法：算法的保密性基于保持算法的秘密
  - 基于密钥的算法：算法的保密性基于对密钥的保密

- 按密钥的数量分类
  - 对称密码算法（传统密码算法，单密钥算法）
  - 非对称密钥算法（公开密钥算法）

密码算法分类

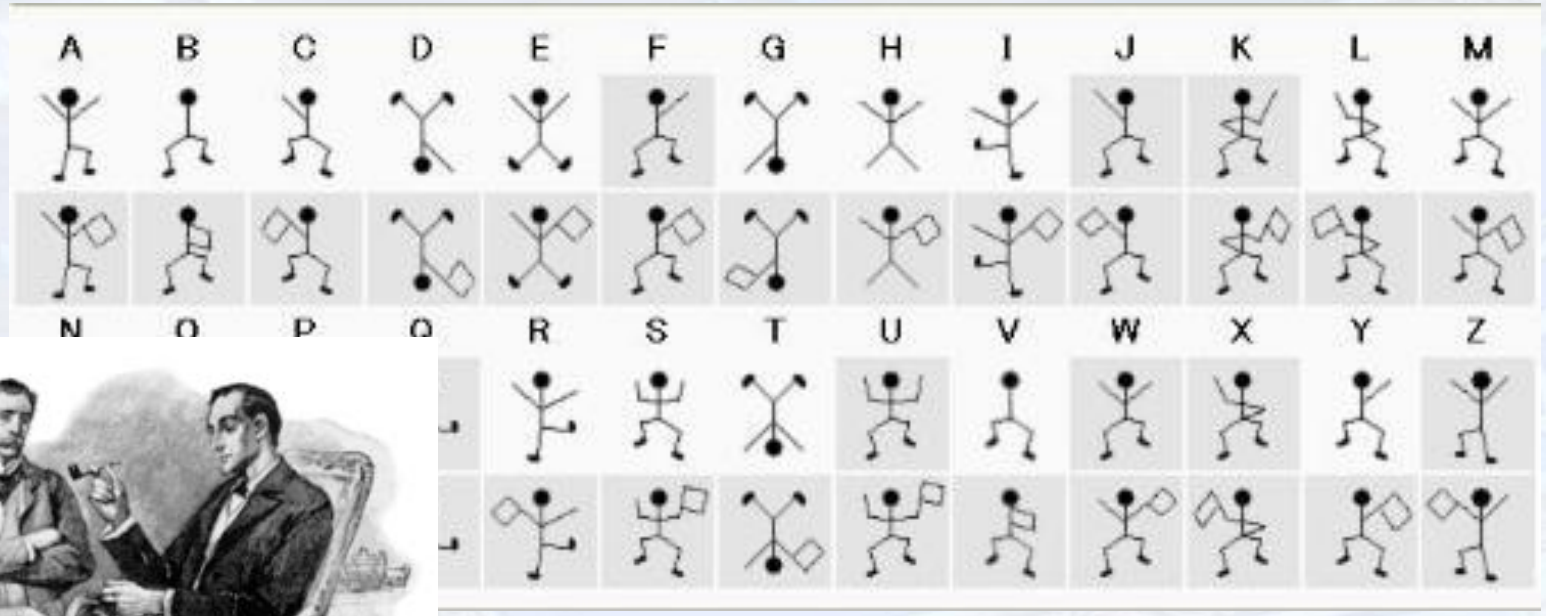
- 按明文的处理方法分类：
  - 流密码：又称序列密码，每次加密一位或一字节的明文。是手工和机械密码时代的主流。
  - 分组密码：将明文分成固定长度的组，用同一密钥和算法对每一块加密，输出也是固定长度的密文，如DES、IDEA、EES、AES…

密码分析

- 1412年，波斯人卡勒卡尚迪所编的百科全书中载有破译简单代替密码的方法。
- 16世纪末期，欧洲一些国家设有专职的破译人员，以破译截获的密信。
- 1863年普鲁士人卡西斯基《密码和破译技术》
- 1883年法国人克尔克霍夫《军事密码学》

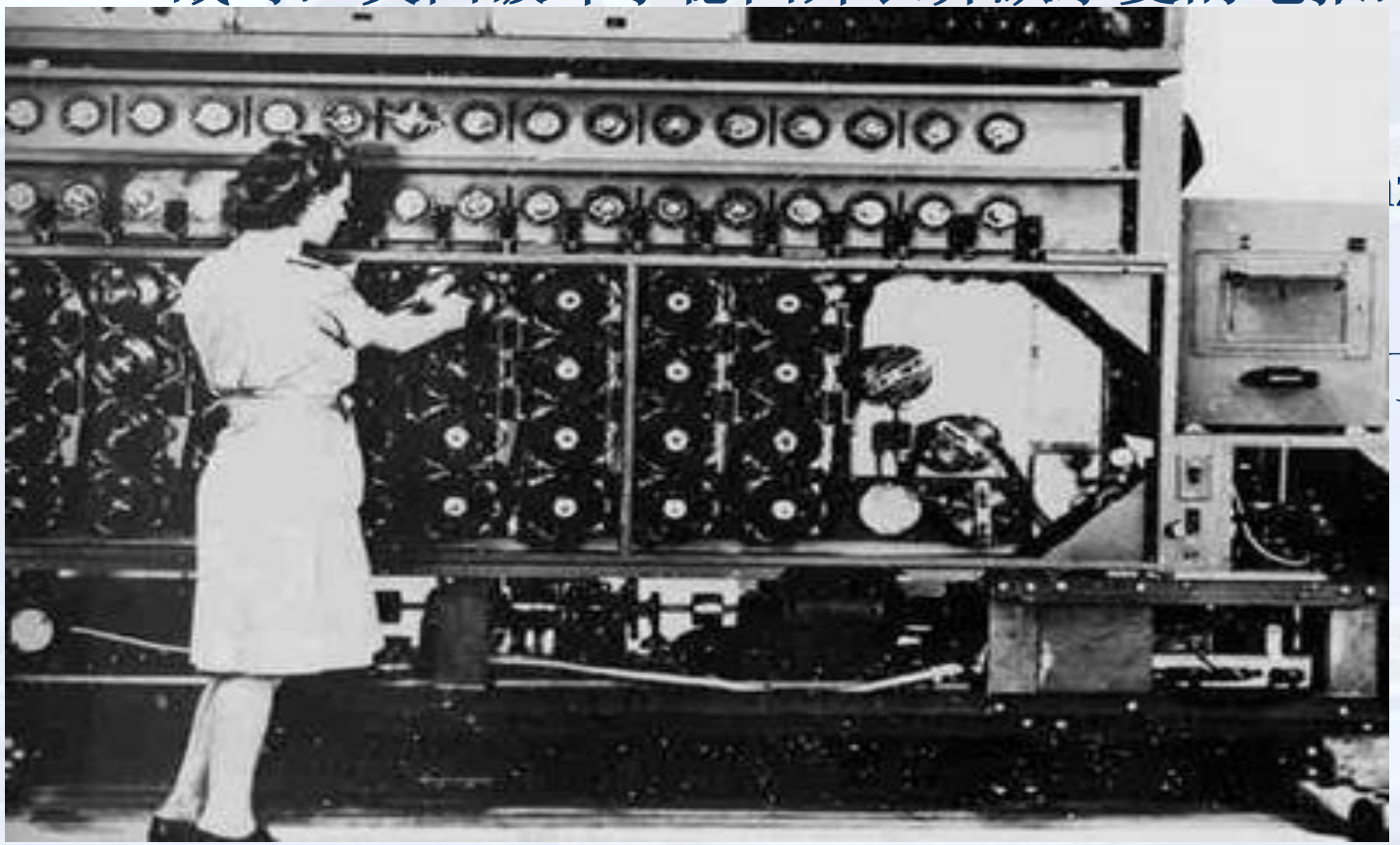
密码分析

- 频率分析法



密码分析

- 密码分析影响历史
  - 一战时，英国破译了德国外长齐默尔曼的电报，促成了美国对德宣战。



算法破解

- 1994年AT&T实验室的Peter Shor提出一种量子计算的方法，采用此方法能够在有限的时间内分解大的质因数，这意味着采用量子计算机将可以轻易的破译RSA算法。
- 1996年Bell实验室发现一种量子搜索算法，可以对现有的DES加密中的密钥进行快速穷举，从而破译密钥。

算法破解

- 2004年、2005年，山东大学数学系王小云教授带领的研究小组先后破解了MD5和SHA-1两大密码算法
  - 整个国际密码学界为之震惊，其研究成果引起了国际同行的广泛关注。
  - 美国国家标准与技术研究院宣布，美国政府5年内将不再使用SHA-1
- 王小云的研究成果表明了从理论上讲电子签名可以伪造，必须及时添加限制条件，或者重新选用更为安全的密码标准，以保证电子商务的安全。

密码分析

- 如果能够根据密文系统地确定出明文或密钥，或者能够根据明文-密文对系统地确定出密钥，则我们说这个密码是可破译的。
- 一个密码，如果无论密码分析者截获了多少密文和用什么方法进行攻击都不能被攻破，则称为是绝对不可破译的。
  - 绝对不可破译的密码在理论上是存在的。
  - 任何可实际使用的密码都是可破译的。
  - 信息论创始人C.E.Shannon论证了一般经典加密方法得到的密文几乎都是可破的

密码算法的安全性

无条件安全 (Unconditionally Secure)

- 无论攻击者拥有多少密文，他也无法破解出对应的明文；
- 即使解出了，也无法验证结果的正确性

计算安全 (Computationally Secure)

- 破译的代价超出信息本身的价值
- 破译的时间超出了信息的有效期

内容安排

1 密码学概述

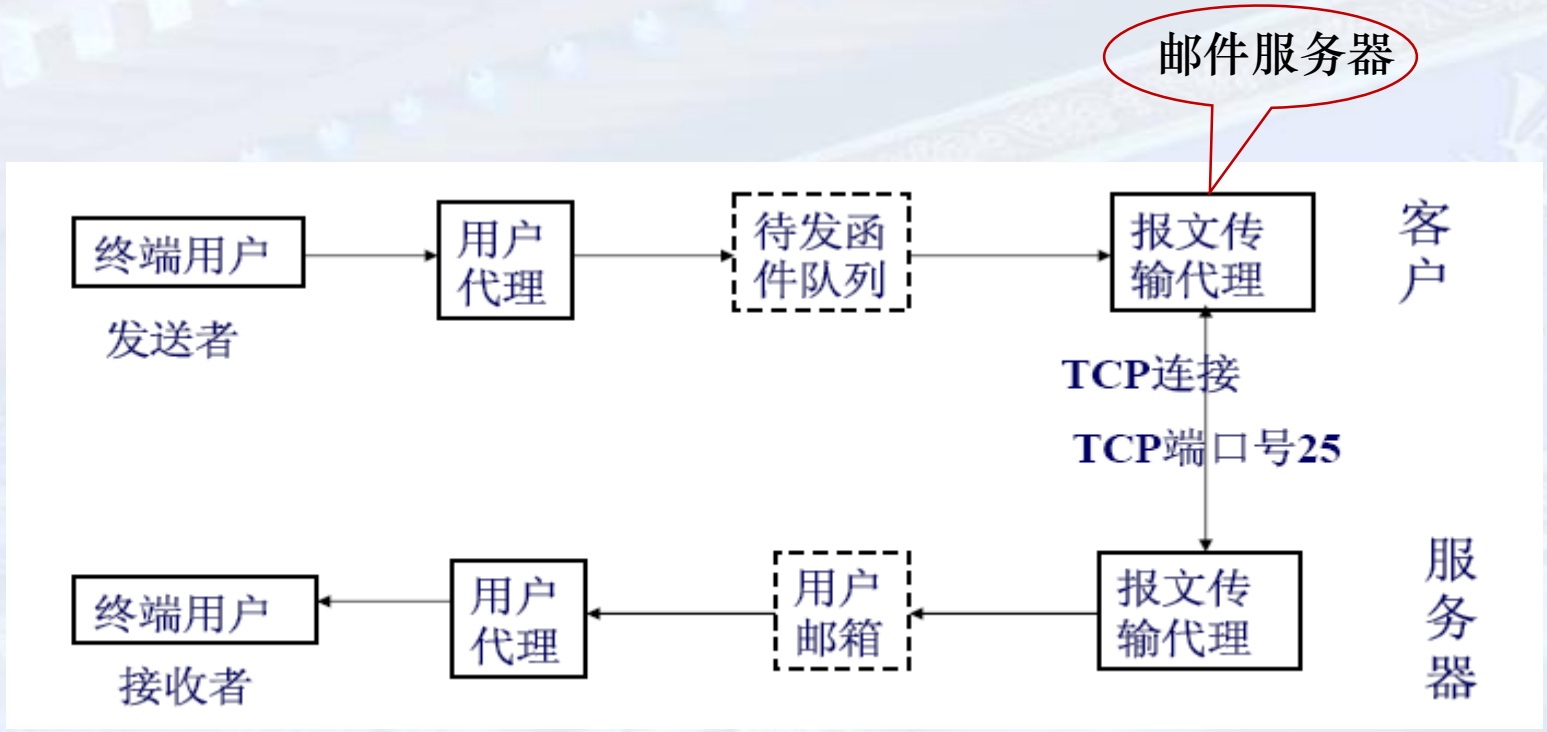
2 安全电子邮件

3 PGP

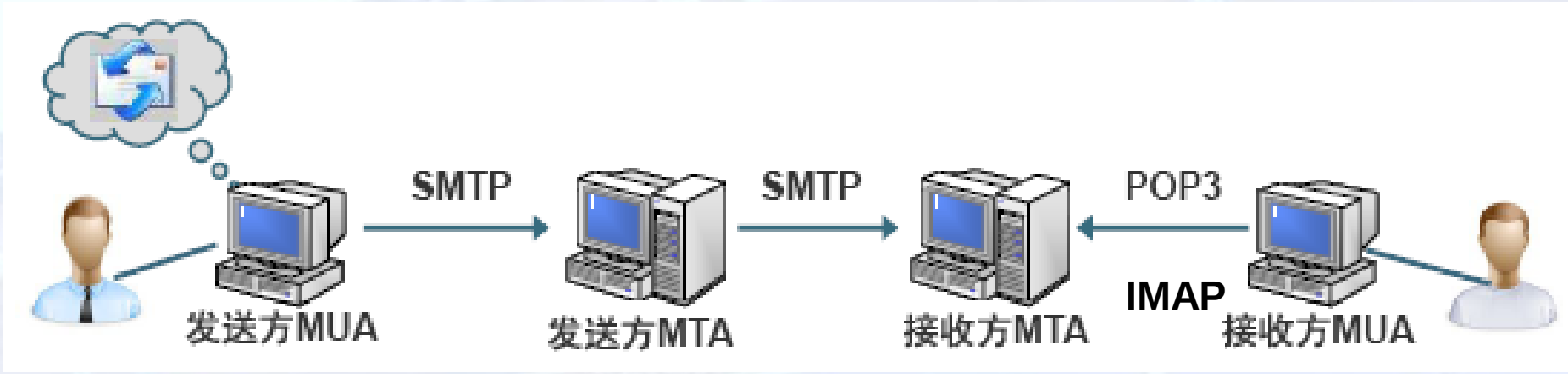
4 PKI技术

安全电子邮件

- 电子邮件　Email
  - Internet上最大的应用，也是唯一的广泛跨平台、跨体系结构的分布式应用。



安全电子邮件



- **MUA: 邮**
- **MTA: 邮**
- **邮件发送 Mail Transfer Protocol)**
- **邮件接收 fice Protocol 3)、IMAP(Internet Mail Access P**

安全需求？

安全风险？

安全电子邮件

- 安全需求
  - 发送邮件和接收邮件的安全登录
  - 安全的电子邮件：邮件保密性和完整性
  - 内容安全性——防止恶意邮件（病毒、钓鱼、不良信息...)

安全电子邮件

- 安全的邮件服务器
  - 对邮件服务器的攻击由来已久：WORM病毒
  - 网络入侵和拒绝服务
- 防范措施：
  - 防止来自外部的攻击：
    - 拒绝来自特定地址的连接请求、限制单个IP的连接数量
    - 拒绝从无法解析的域送来的邮件
    - 建立各种基于主机、用户、域的访问控制
    - 默认配置仅允许本地收发

安全电子邮件

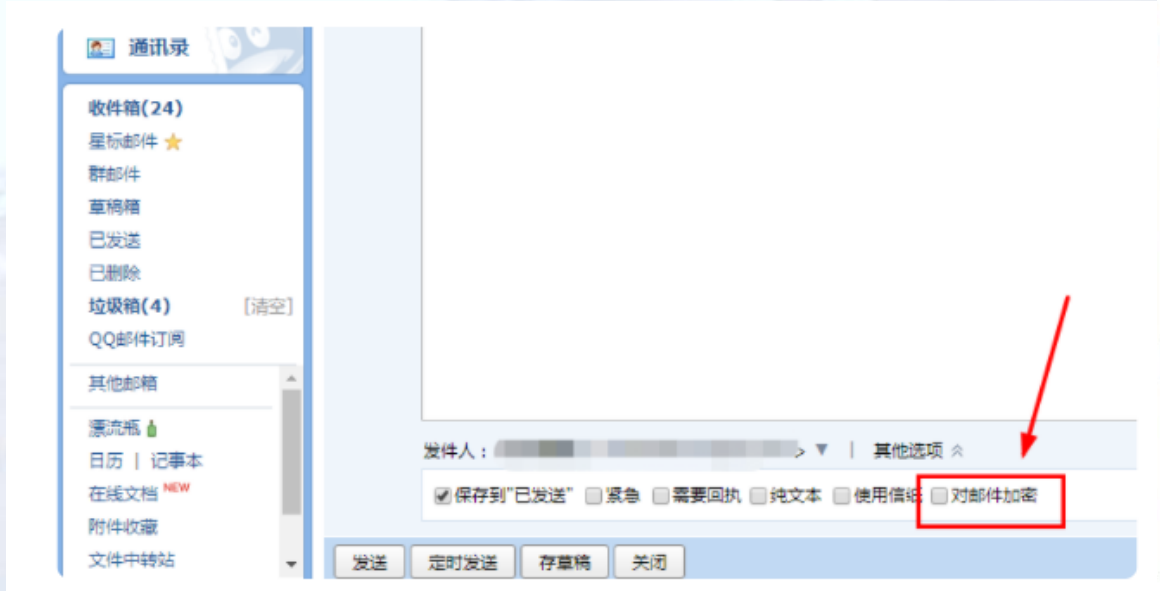
- 防范措施：
  - 防止来自内部的攻击：实现用户身份的鉴别
  - 反垃圾邮件策略
    - 默认情况下不做转发
    - 建立访问数据库
    - 检查邮件信头

安全电子邮件

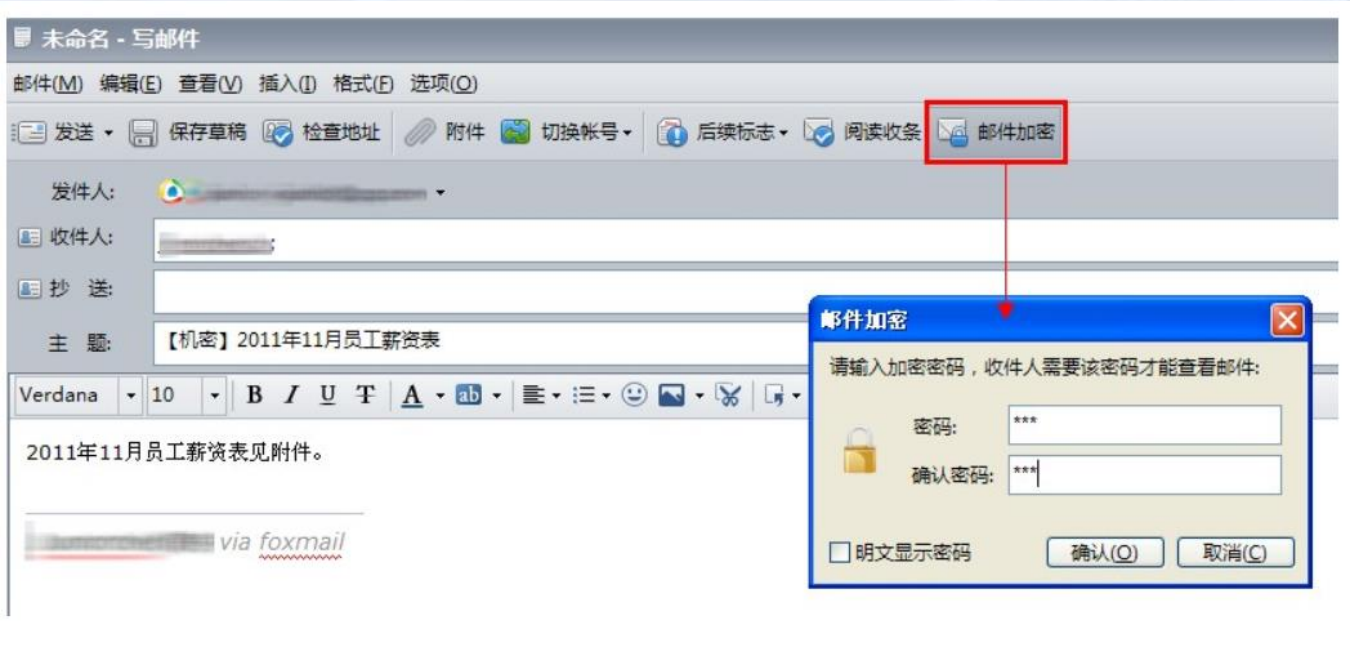
- 涉及到的问题：
  - 如何实现认证和信任管理
  - 安全算法的选择
  - 系统邮件的信息格式
  - 邮件服务器的可靠性
  - 。。。

安全电子邮件

▪ 邮件加密



QQ邮箱



Foxmail 邮件加密

安全电子邮件 —S/MIME

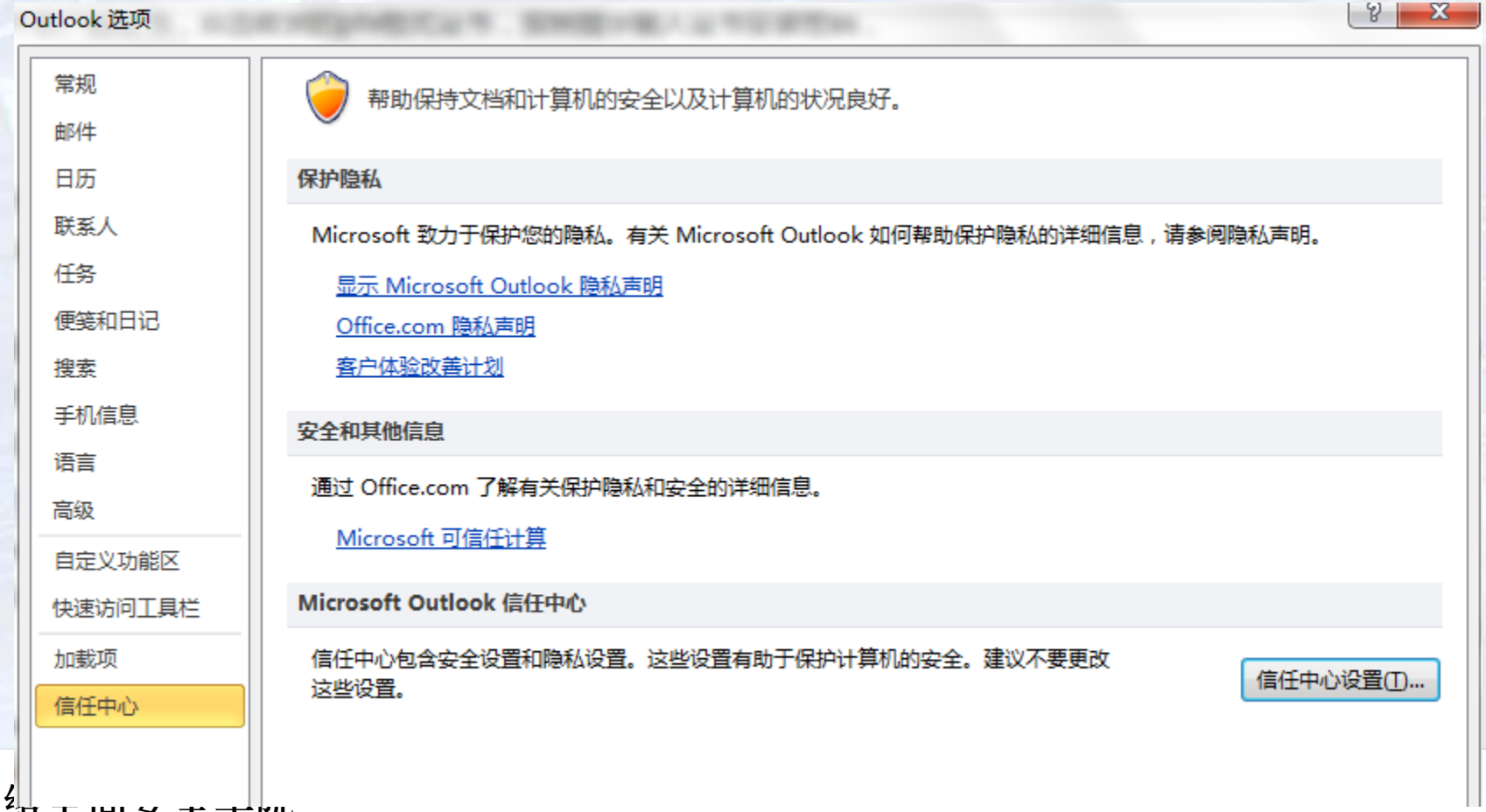
- **S/MIME: Secure Multipurpose Internet Mail Extensions**
- **是对MIME电子邮件格式的安全扩展**
- **为电子邮件提供：认证、完整性保护、鉴定及数据保密等安全服务**
- **证书格式采用X.509**
- **认证机制依赖于层次结构的证书认证机构**

安全电子邮件 —S/MIME

- S/MIME历史：
  - 从PEM （Privacy Enhanced Mail）和MIME（Internet邮件的附件标准）发展而来
  - 1995 年推出S/MIME第一版
  - 1998 年，S/MIME 2 推出，并被提交到 Internet 工程任务组 (IETF)。
  - 1999 年，IETF 提议使用 S/MIME 版本 3

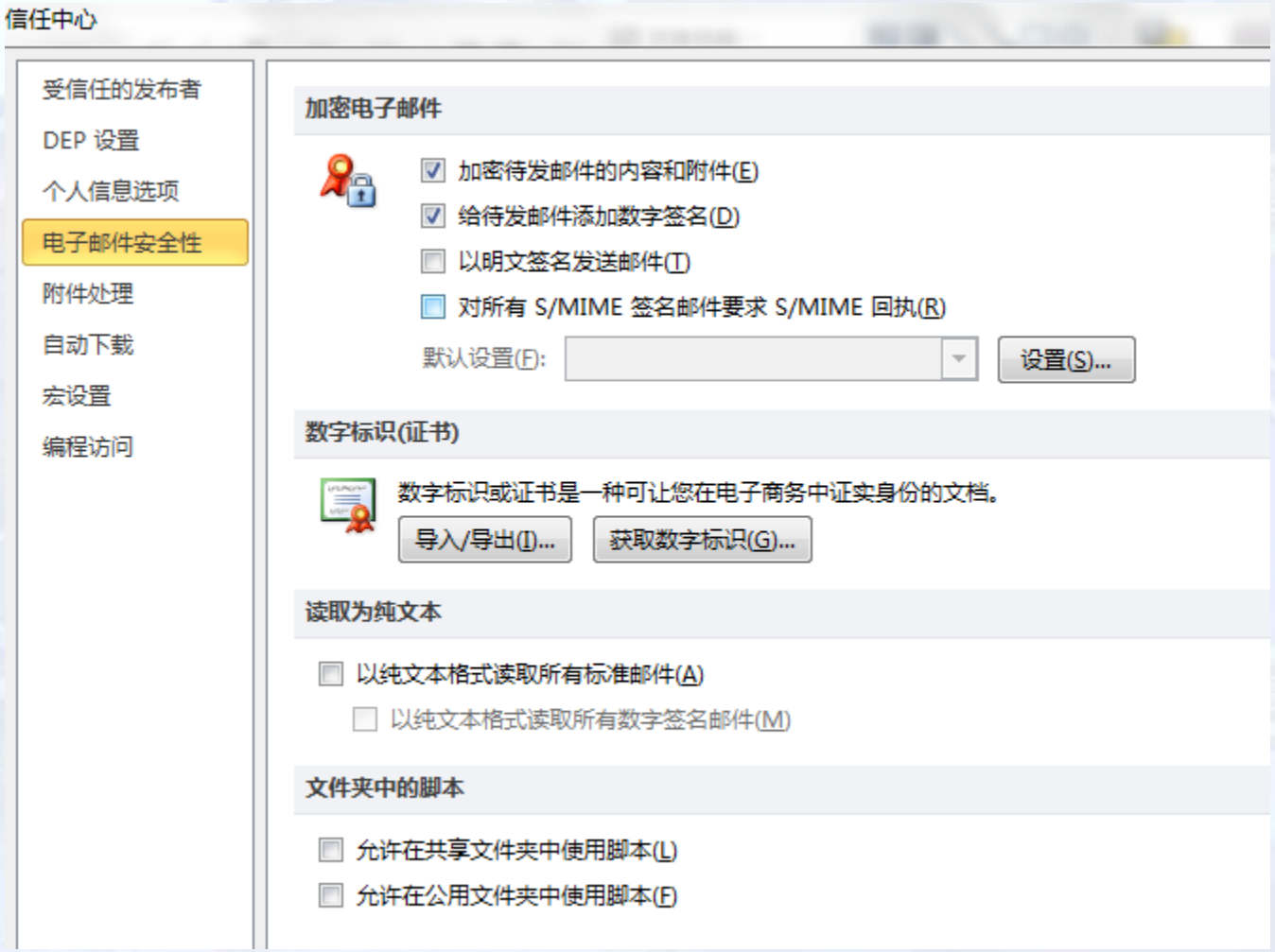
S/MIME应用

- **Outlook 加密所有传出邮件**
  - 在“文件”选项卡上，选择"选项>信任中心">"信任中心设置"。



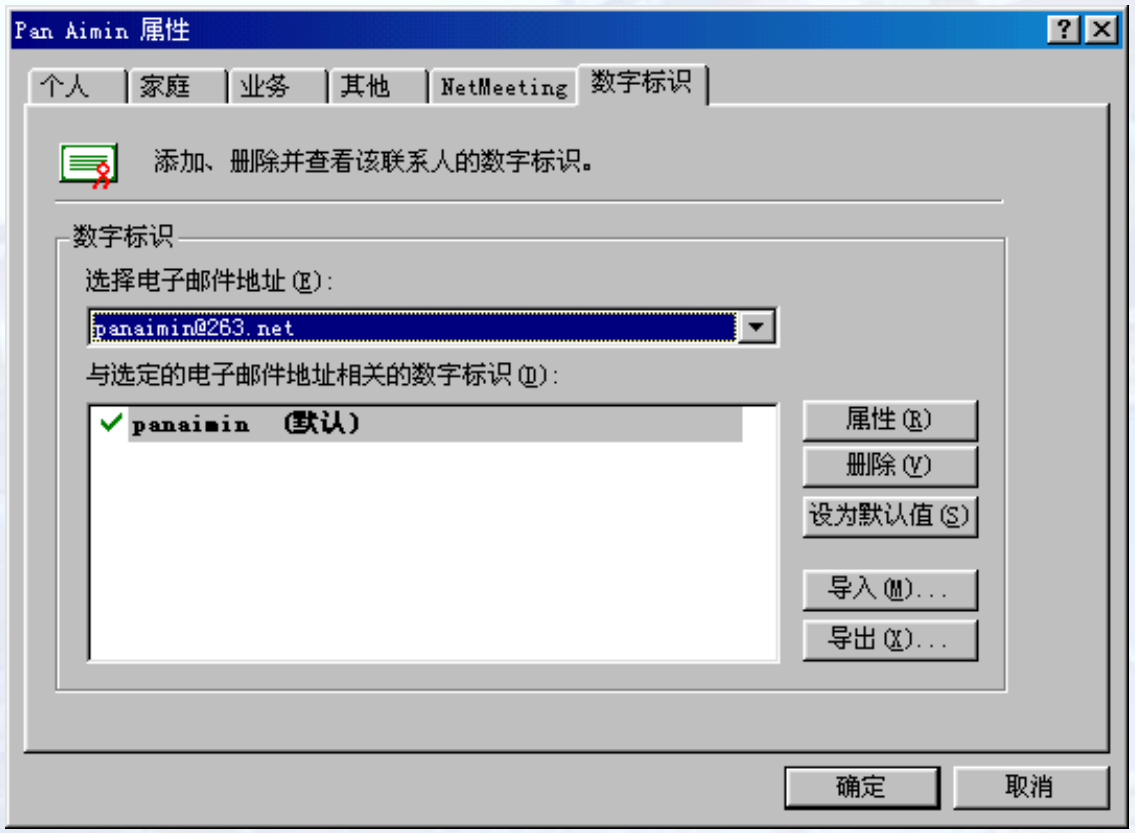
S/MIME应用

- **Outlook**

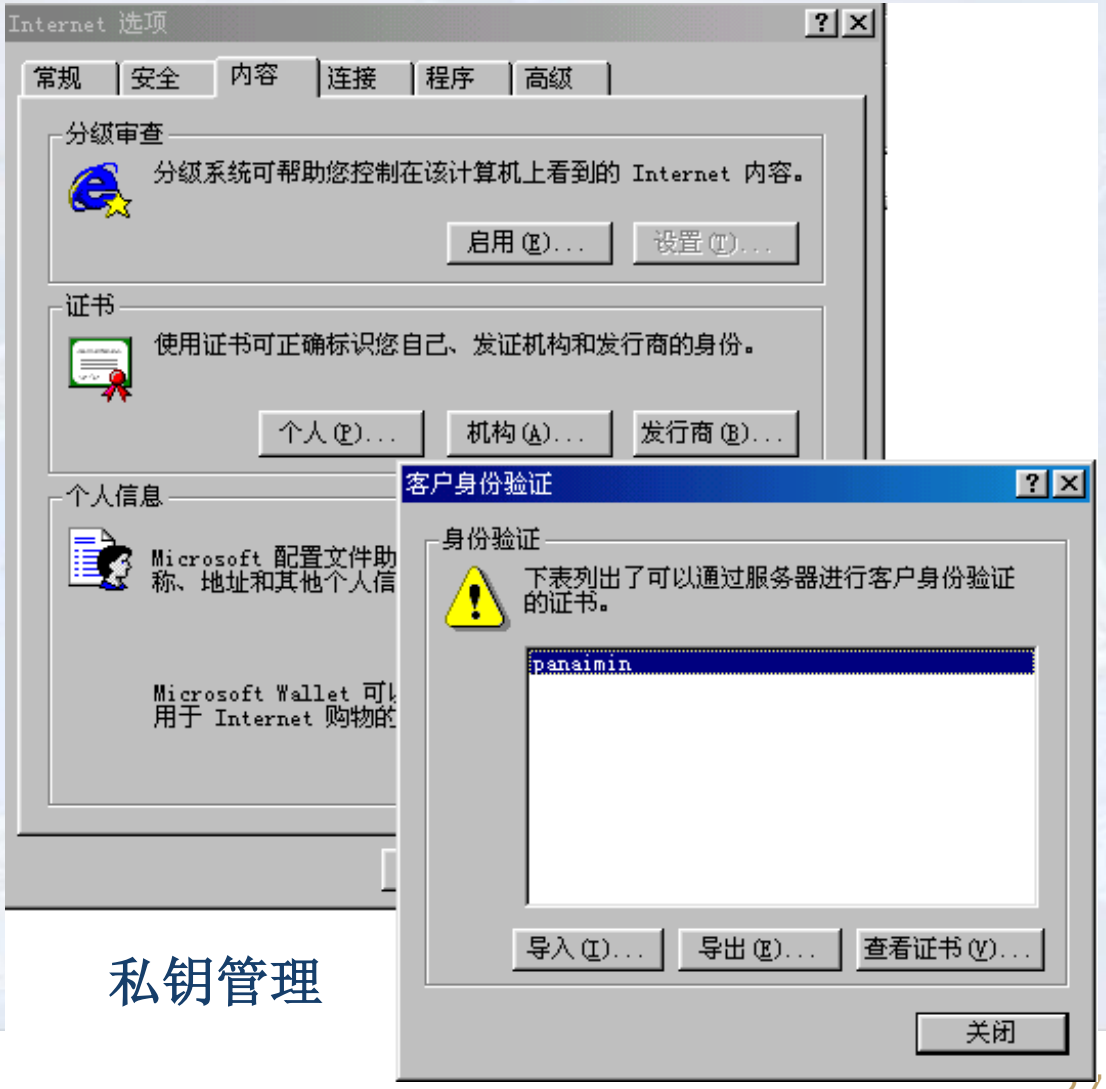


S/MIME应用

- **Outlook**



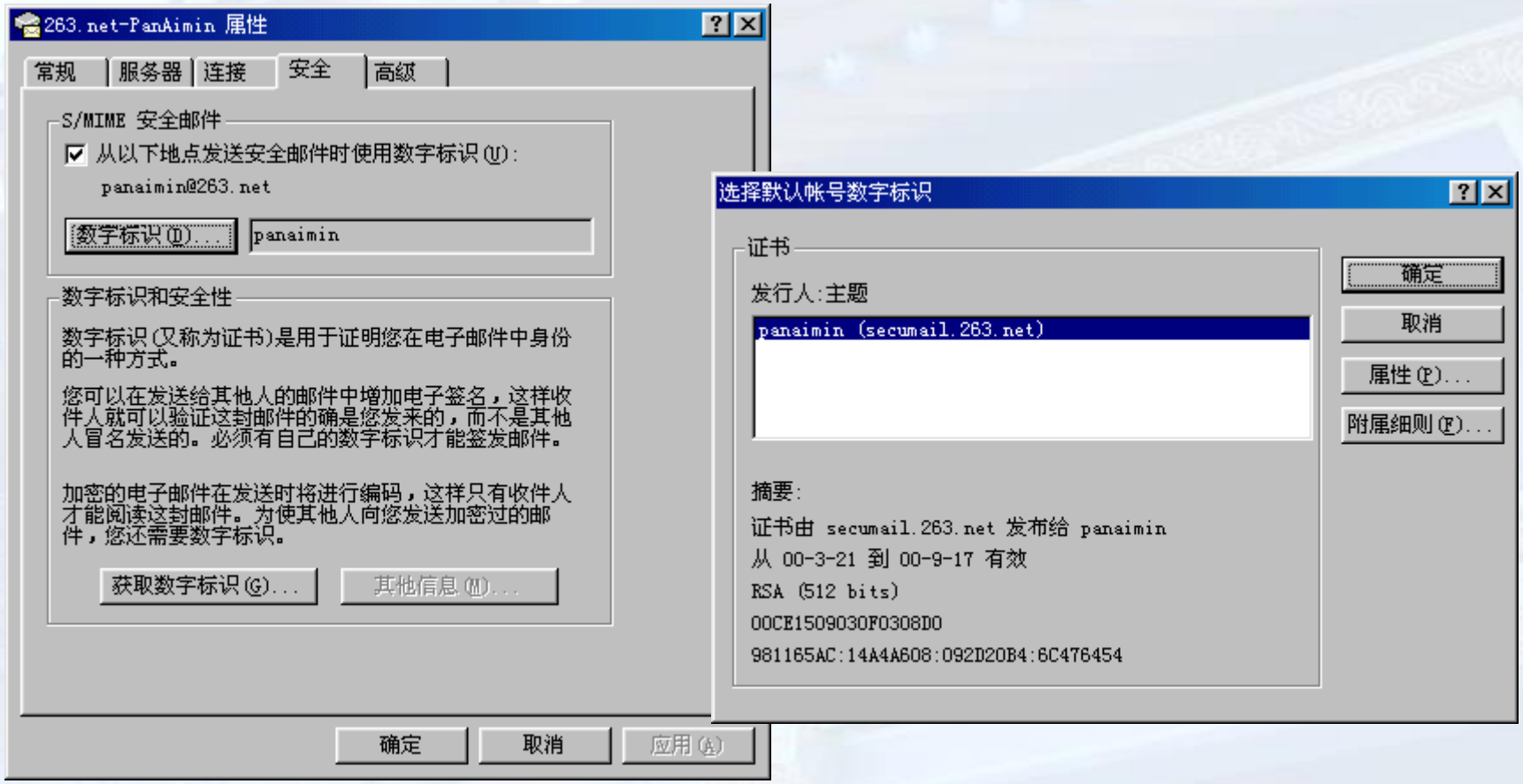
公钥管理



私钥管理

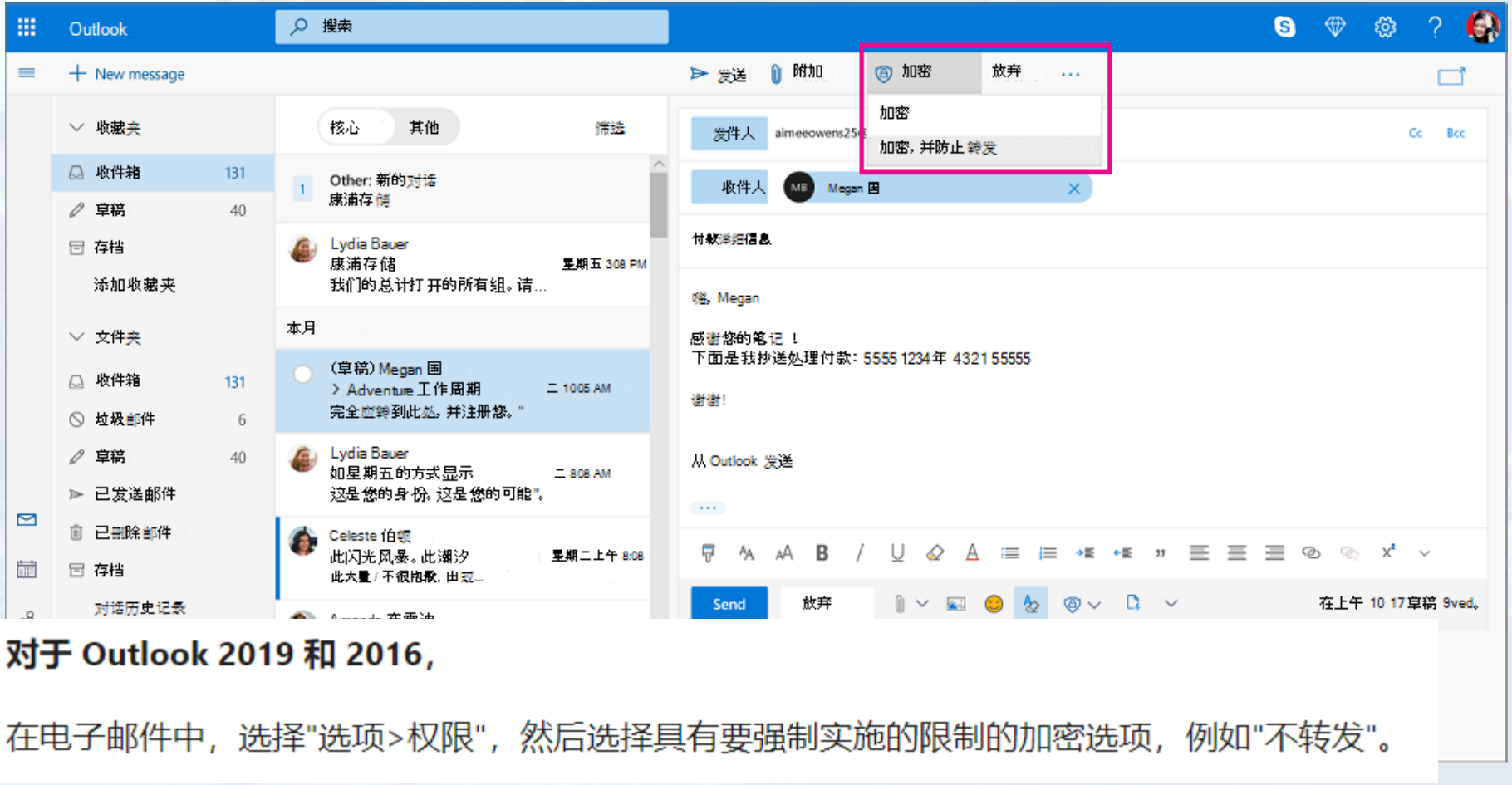
S/MIME应用

- **Outlook 把帐号与私钥关联起来**



S/MIME应用

- Microsoft 365中 outlook

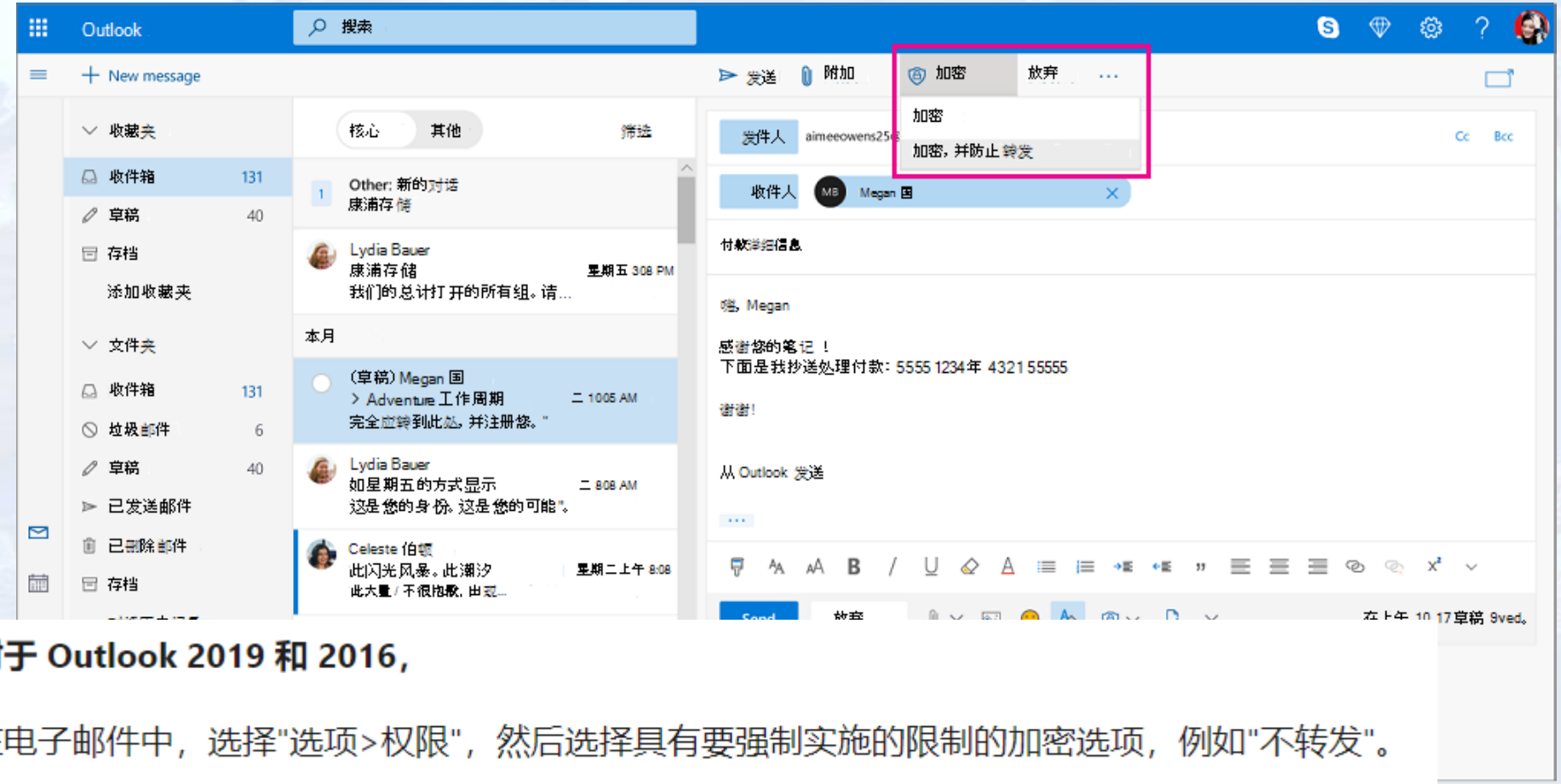


对于 Outlook 2019 和 2016，

在电子邮件中，选择"选项>权限"，然后选择具有要强制实施的限制的加密选项，例如"不转发"。

S/MIME应用

- Microsoft 365中 outlook

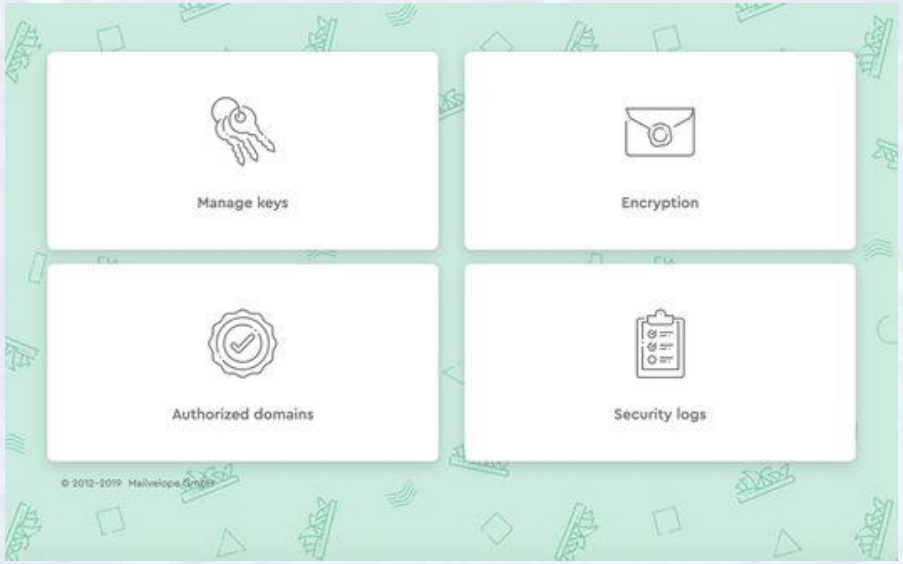


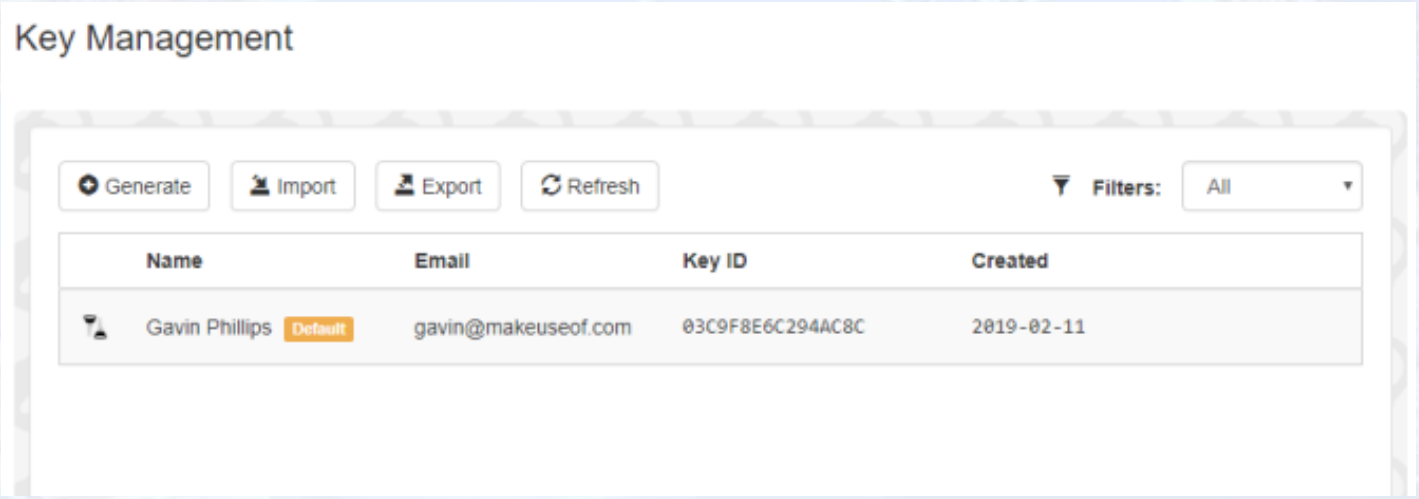
对于 Outlook 2019 和 2016，

在电子邮件中，选择"选项>权限"，然后选择具有要强制实施的限制的加密选项，例如"不转发"。

其它

- **Mailvelope**
  - **适用于Firefox和Chrome的浏览器，可在网络邮件提供商处加解密邮件**
  - **Mailvelope完全开源，基于OpenPGP标准**





内容安排

PGP

- **PGP: Pretty Good Privacy**
- **Phil Zimmermann，1991，世界上第一个信息加密传输工具，可以被个人使用的工具**
- **可以保护文件、邮件、磁盘等**
- **最初是免费的，后被赛门铁克公司收购，不再单独放出PGP版本的独立安装包形式，集成于诺顿等赛门铁克公司安全产品里。**
- **更名为 Symantec Encryption Desktop**

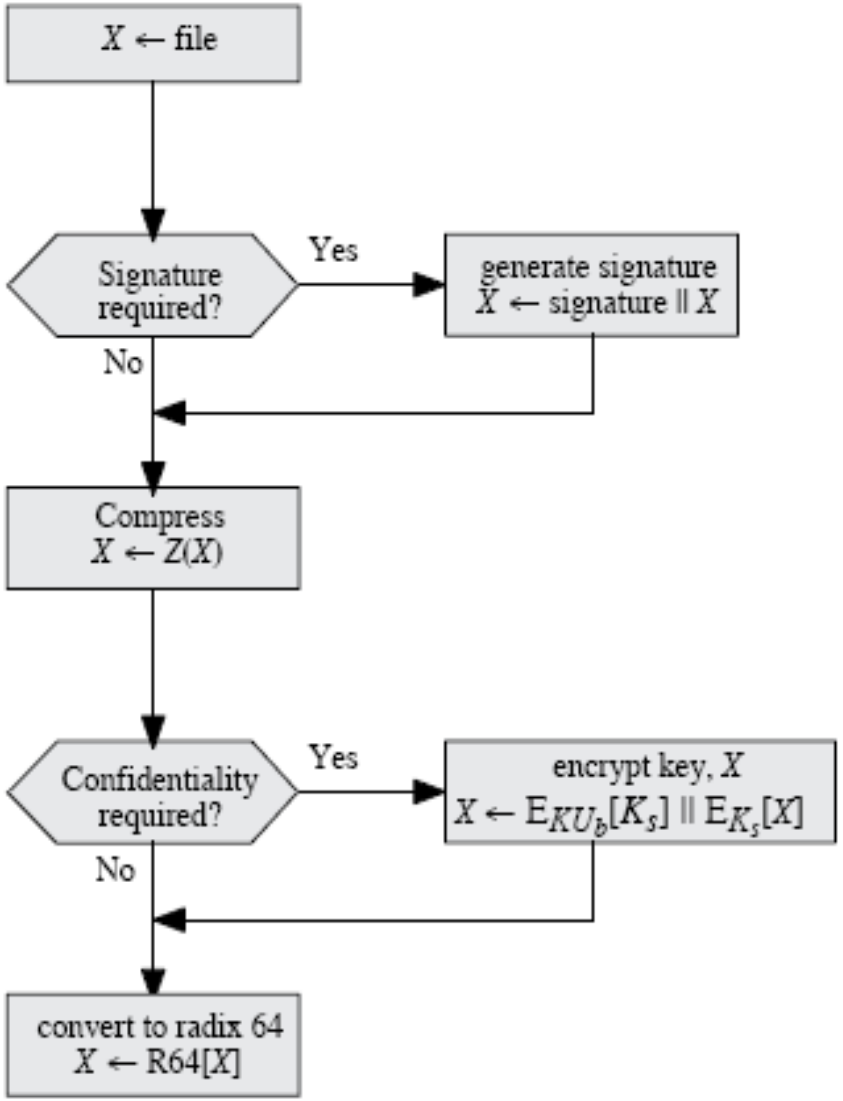
PGP功能

- **PGP功能**
  - 电子邮件加密
  - 加密与压缩功能
  - 全盘加密/网络磁盘加密
  - 文件签名
  - 。 。 。

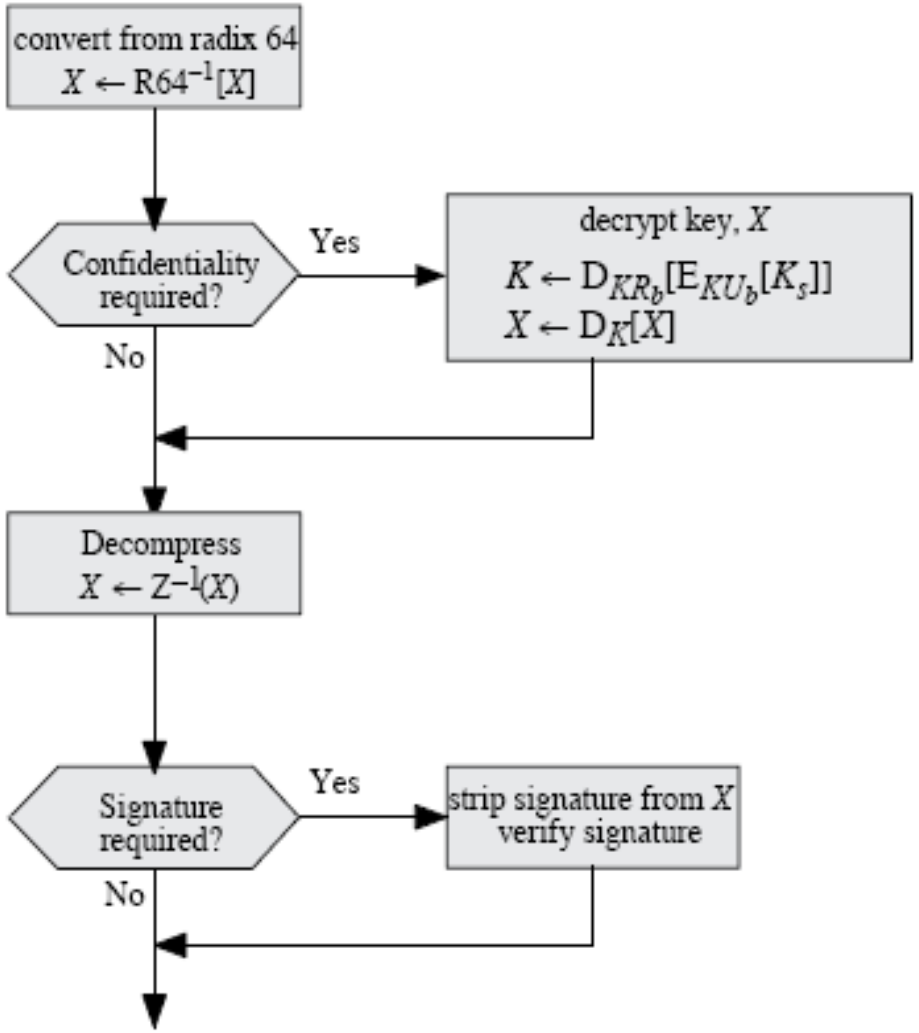
PGP

- **PGP成功原因**
  - 版本众多，包括各种系统平台，商业版本
  - 算法的安全性已经得到了充分的论证
  - 适用性强，公司可以选择用来增强加密文件和消息，个人可以选择用来保护自己与外界的通信
  - 不是由政府或者标准化组织所控制，可信性高
  - 据称绕过了美国政府限制出口的专利技术管理要求

PGP过程

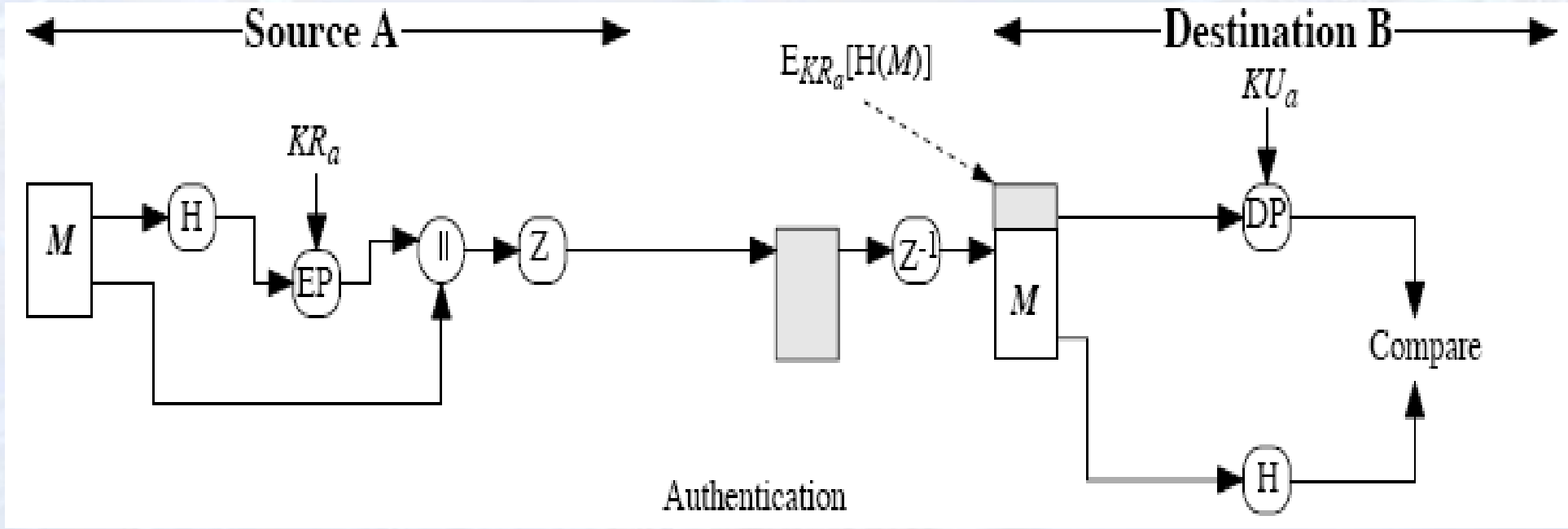


(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

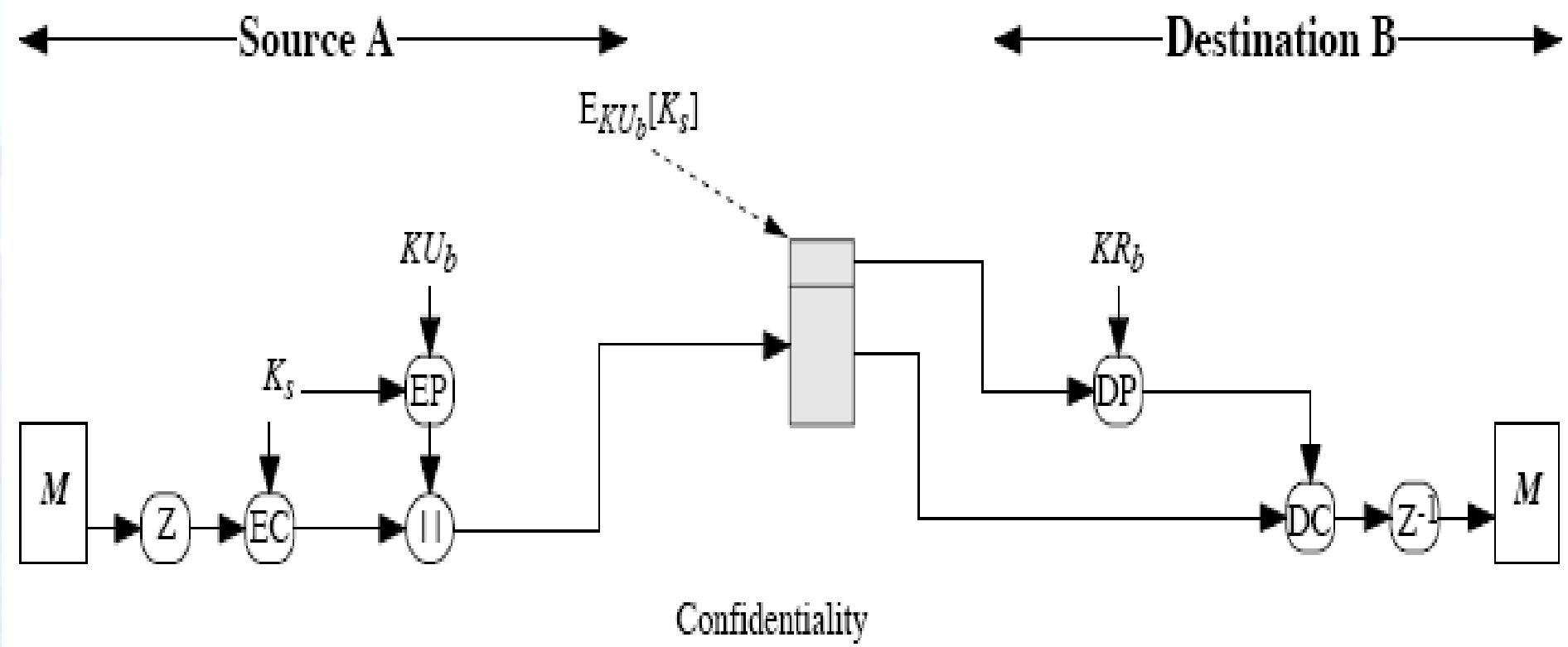
PGP功能：身份认证


Source A
Destination B
$E_{KR_a}[H(M)]$
KR_a
KU_a
M
H
EP
||
Z
Z^{-1}
M
DP
Compare
H
Authentication

PGP功能：身份认证

- 说明：
  - 1. 公钥算法（如RSA）的强度保证了发送方的身份
  - 2. HASH算法（如SHA-1）的强度保证了签名的有效性
  - 3. DSS/SHA-1可选替代方案
- 签名与消息可以分离
  - 对消息进行单独的日志记录
  - 可执行程序的签名记录，检查病毒
  - 文档多方签名，可以避免嵌套签名

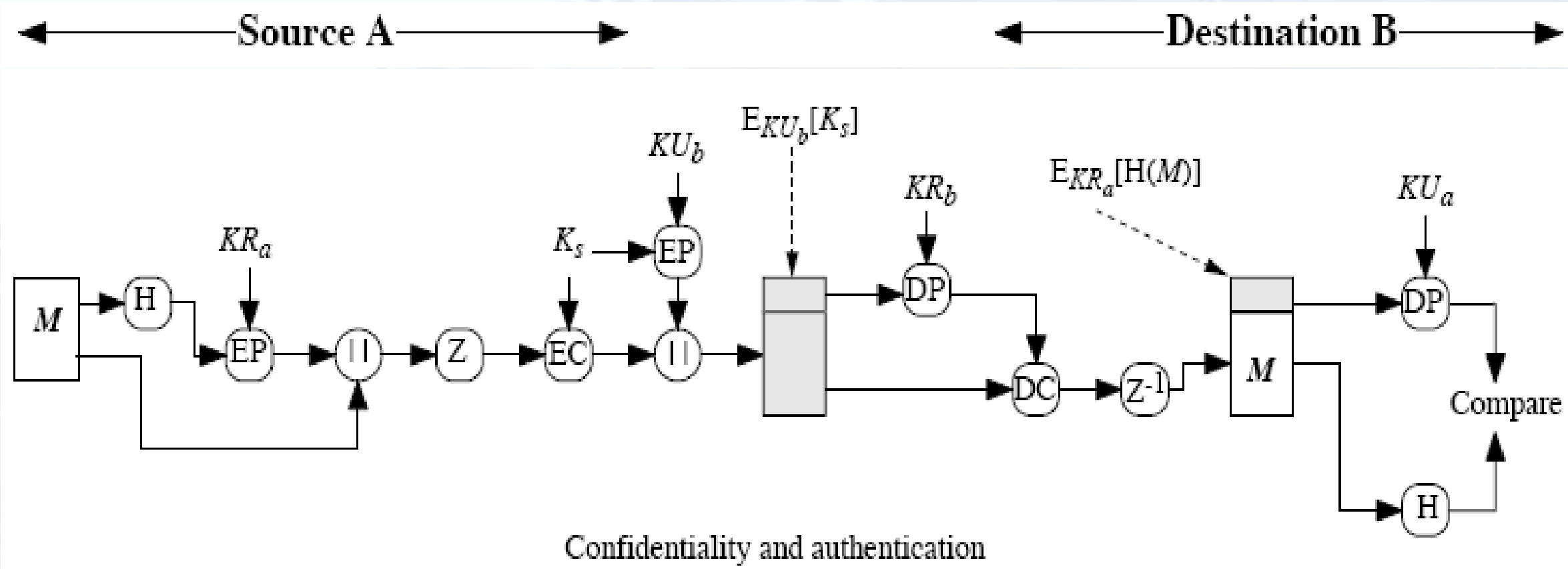
PGP功能：保密


Source A
Destination B
$E_{KU_b}[K_s]$
KU_b
KR_b
K_s
EP
DP
M
Z
EC
||
DC
Z-1
M
Confidentiality

PGP功能：保密

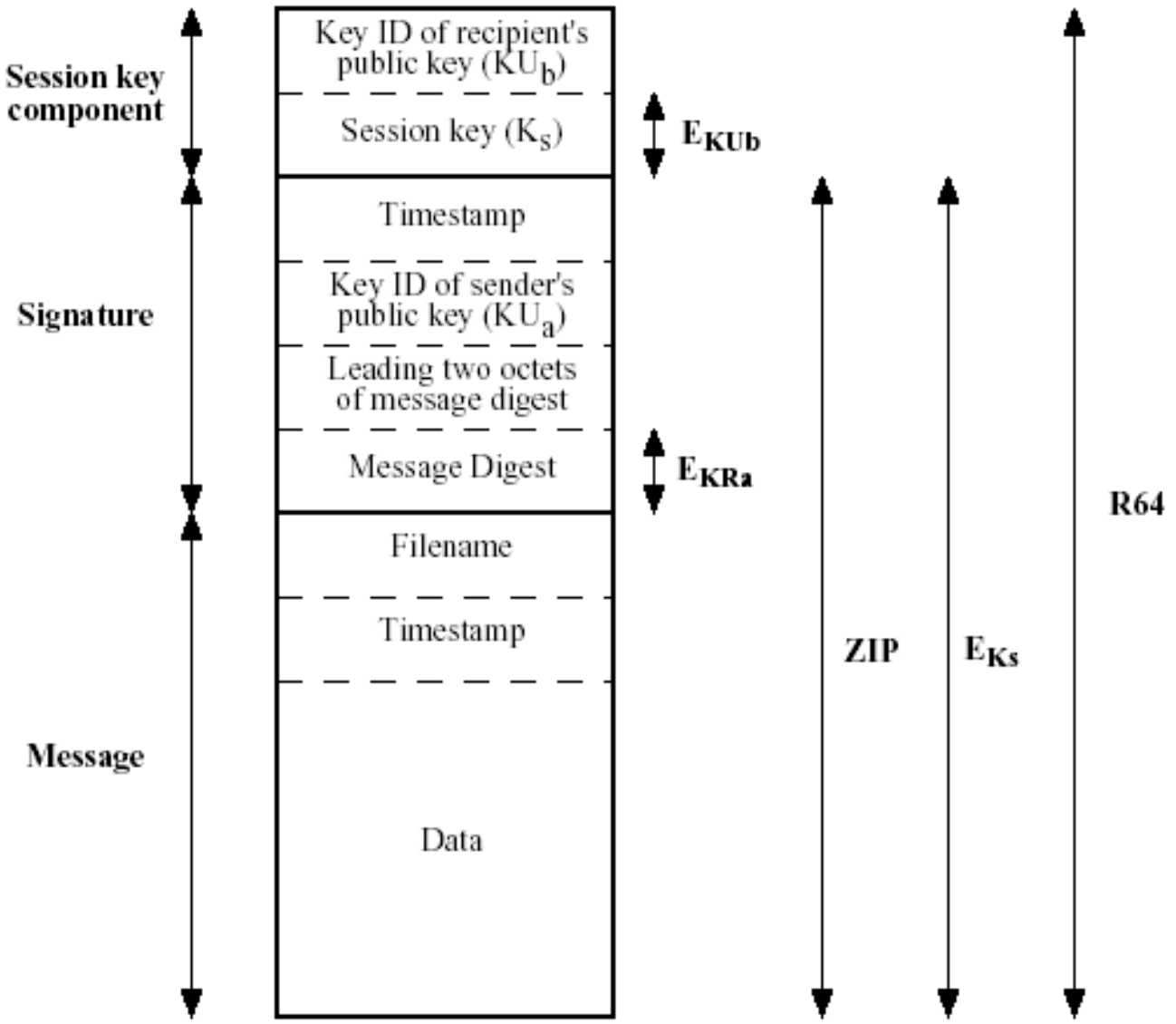
- 对称加密算法和公钥加密算法的结合可以缩短加密时间
- 用公钥算法解决了会话密钥的单向分发问题
  - 不需要专门的会话密钥交换协议
  - 由于邮件系统的存储-转发的特性，用握手方式交换密钥不太可能
- 每个消息都有自己的一次性密钥，进一步增强了保密强度。所以，每个密钥只加密很小部分的明文内容

PGP：保密与认证的结合



PGP中的密

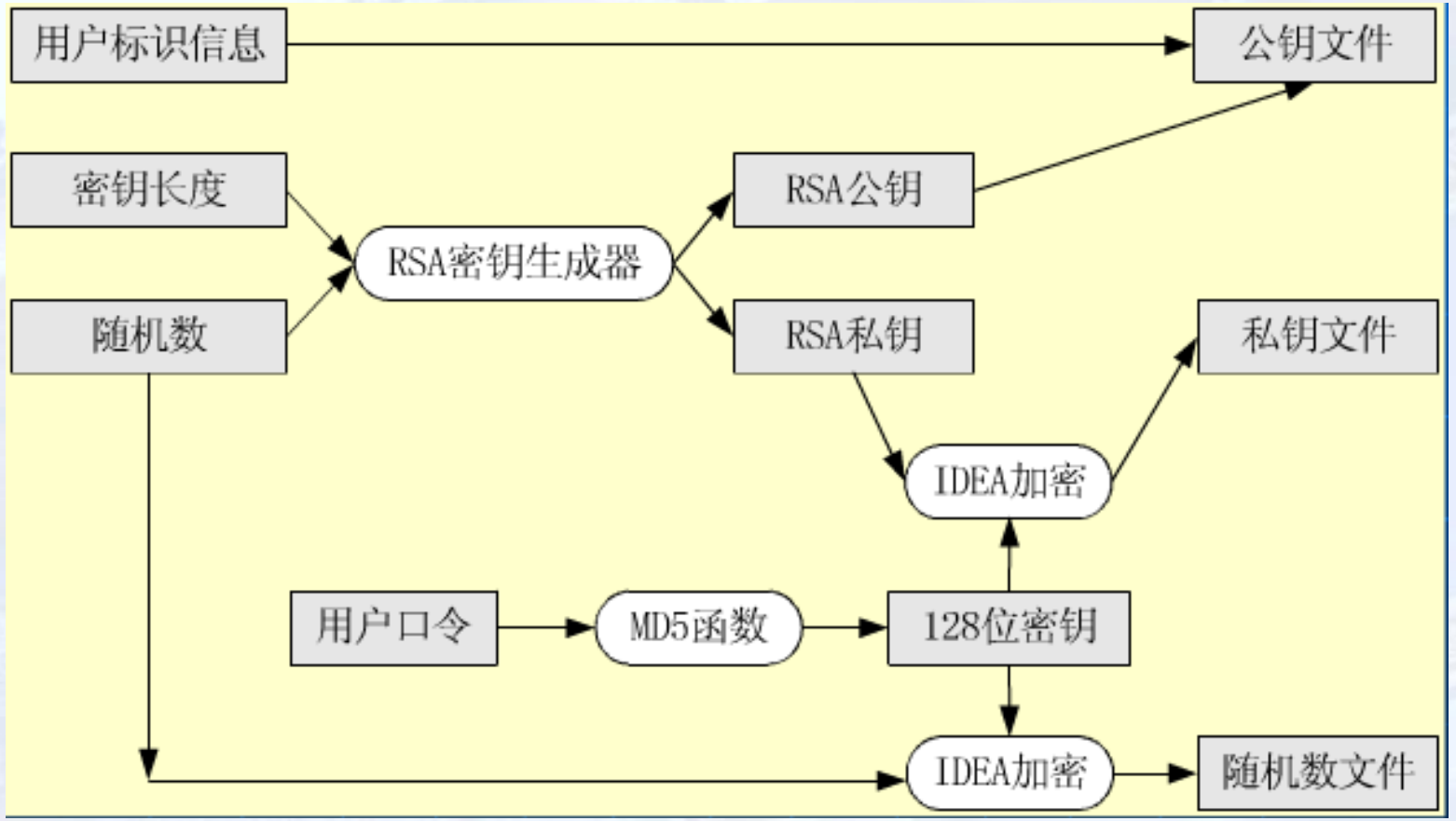
- 密钥标识符
  - 可能存在
  - 减少密钥
  - 管理公钥
  - PGP消息



PGP中的密钥

- 需要三种类型的密钥
  - 一次性会话密钥（对称密钥）
  - 公钥/私钥对（可以多对）
  - 基于口令的对称密钥

PGP中的密钥

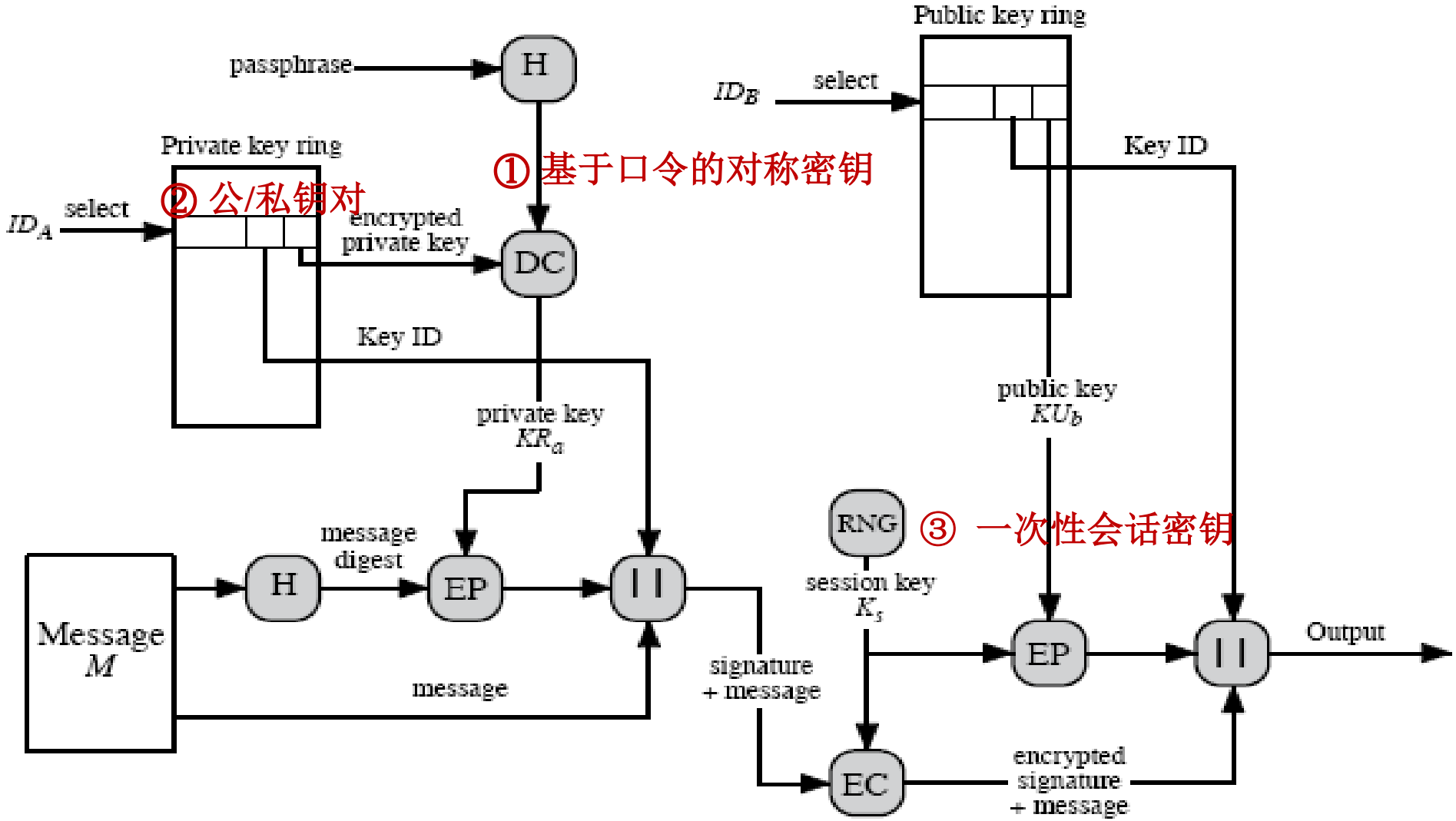


生成PGP公私钥对

PGP中的密钥

- 公开密钥环：Public key ring
  - 存储其他用户的公开密钥
- 私有密钥环：Private key ring
  - 存储用户自身的公开/私有密钥（可有多对）

PGP报文的生成

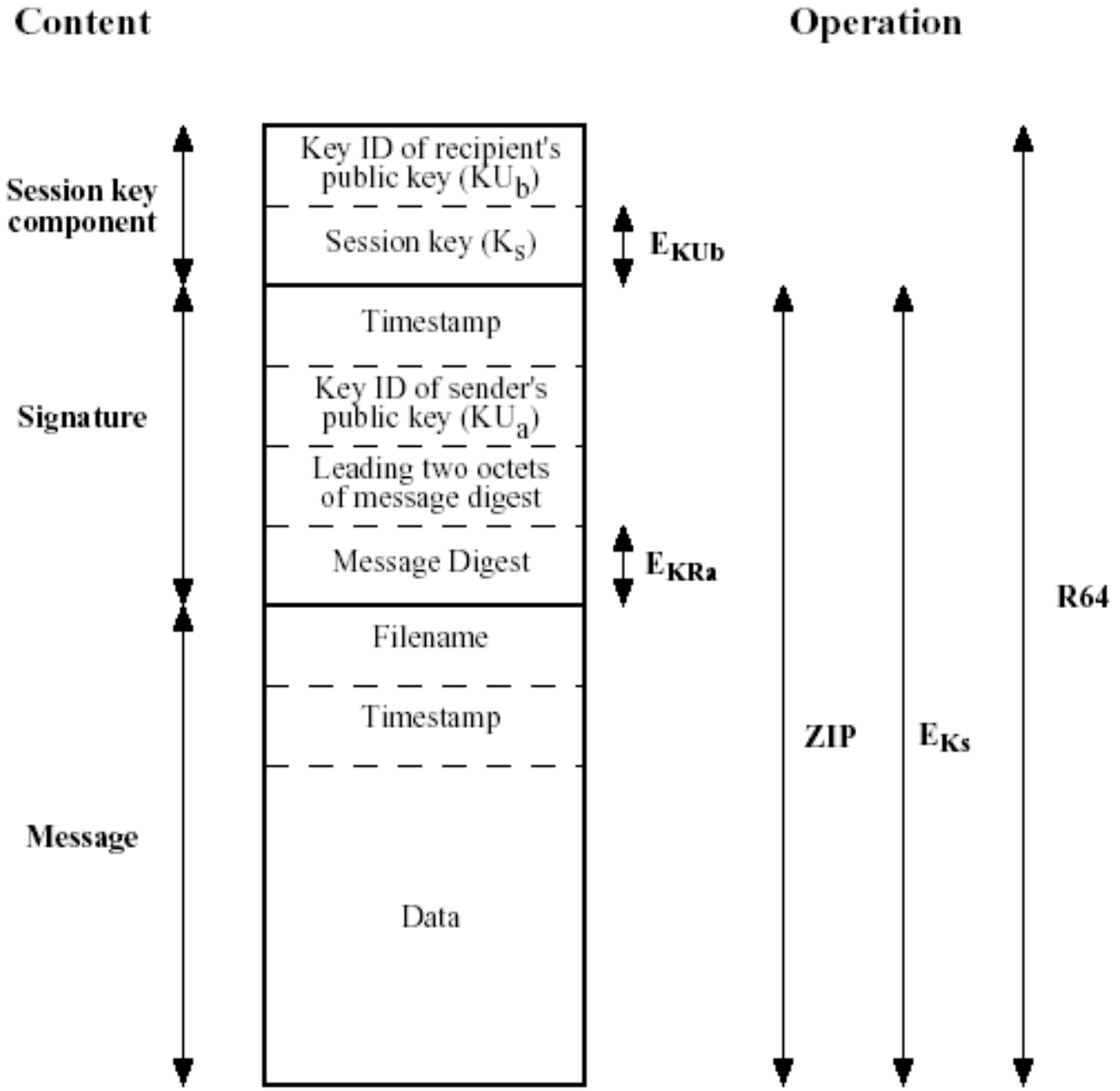


PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

PGP邮件数据处理

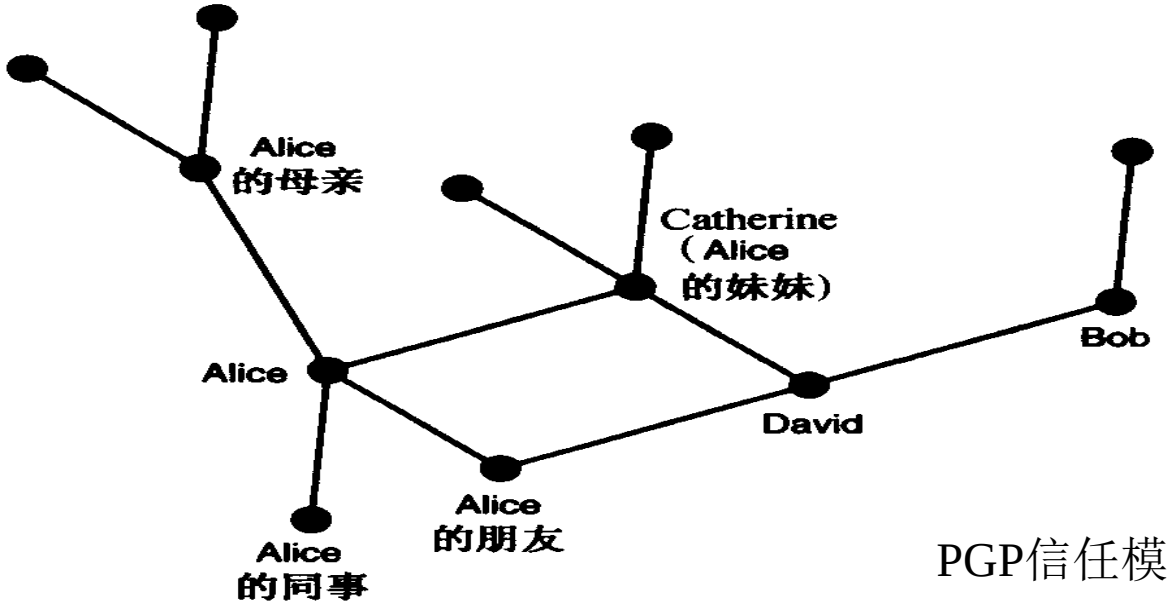
- 顺序：签名 — 压缩 —加密
- 签名后压缩
- 压缩
  - 存储、传输、减少运算、安全性
- 压缩之后再做加密

PGP


Content
Operation
Session key component
Signature
Message
Key ID of recipient's public key (KU_b)
Session key (K_s)
Timestamp
Key ID of sender's public key (KU_a)
Leading two octets of message digest
Message Digest
Filename
Timestamp
Data
E_{KUb}
E_{KRa}
ZIP
E_{Ks}
R64

PGP公钥管理

- 没有建立严格的公钥管理模式
- 私人方式的公钥介绍机制
  - 非官方，反映人类自然的社会交往



PGP信任模型

PGP信任模型

- 采用 Web of Trust 模型，由用户自己决定信任关系
  - 公开密钥环上的每个公开密钥都有一个密钥合法性字段，用来标识信任程度（完全信任、少量信任、不可信任和不认识的信任等）
  - 当新来一个公开密钥时，根据上面附加的签名来计算信任值的权重和，确定信任程度。
- 基于从旁观者角度和信息越多越好的思想，是一种累计的信任模型
  - 可以是直接信任
  - 可以是某种形式的信任链
  - 也可以通过多个介绍者
- 在公司、金融或政府环境下是不合适的

内容安排

1 密码学概述

2 安全电子邮件

3 PGP

4 PKI技术

PKI 的概念

- **PKI：Public Key Infrastructure，公钥基础设施**
- **学术定义：PKI是一个用公钥理论和技术来实施和提供安全服务的具有普适性的安全基础设施。**
- **工程定义：PKI是一个包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和证书的产生、管理、存储、分发和撤销等功能。（X.509标准）**

PKI应用

证书中心

5 接受各界查询证书资料，
提供证书注销查询

1 申请证书

2 核发证书

网 络

政府机关

4 向证书权威管理机构
查询证书有效期和真伪

纳税人

3 网络交易(如
电子报税)

企业

PKI组成

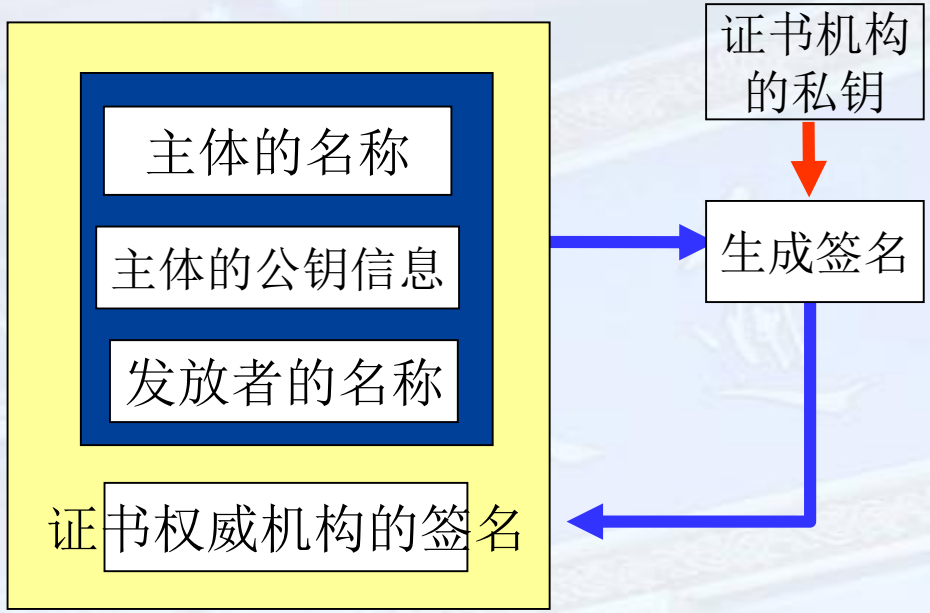
- **PKI组成：**
  - **证书管理机构 (CMA, Certificate Management Authority)**
    - 认证机构 (CA, Certificate Authority)
    - 注册机构 (RA, Registration Authority)
  - **证书存档 (Repository)**
    - 公钥证书 (PKC, Public Key Certificate)
    - 证书作废列表 (CRL, Certificate Revocation List)
  - **策略管理机构 (PMA, Policy Management Authority)**
  - **最终用户 (End User)**
    - 署名用户 (Subscriber)
    - 依赖方 (Relying party)

数字证书

- **Loren Kohnfelder，Towards a Practical Public-Key Cryptosystem, May 1978，MIT**
- **将对象身份和对象的公开密钥有效捆绑**
- **考虑身份证的原理**

数字证书

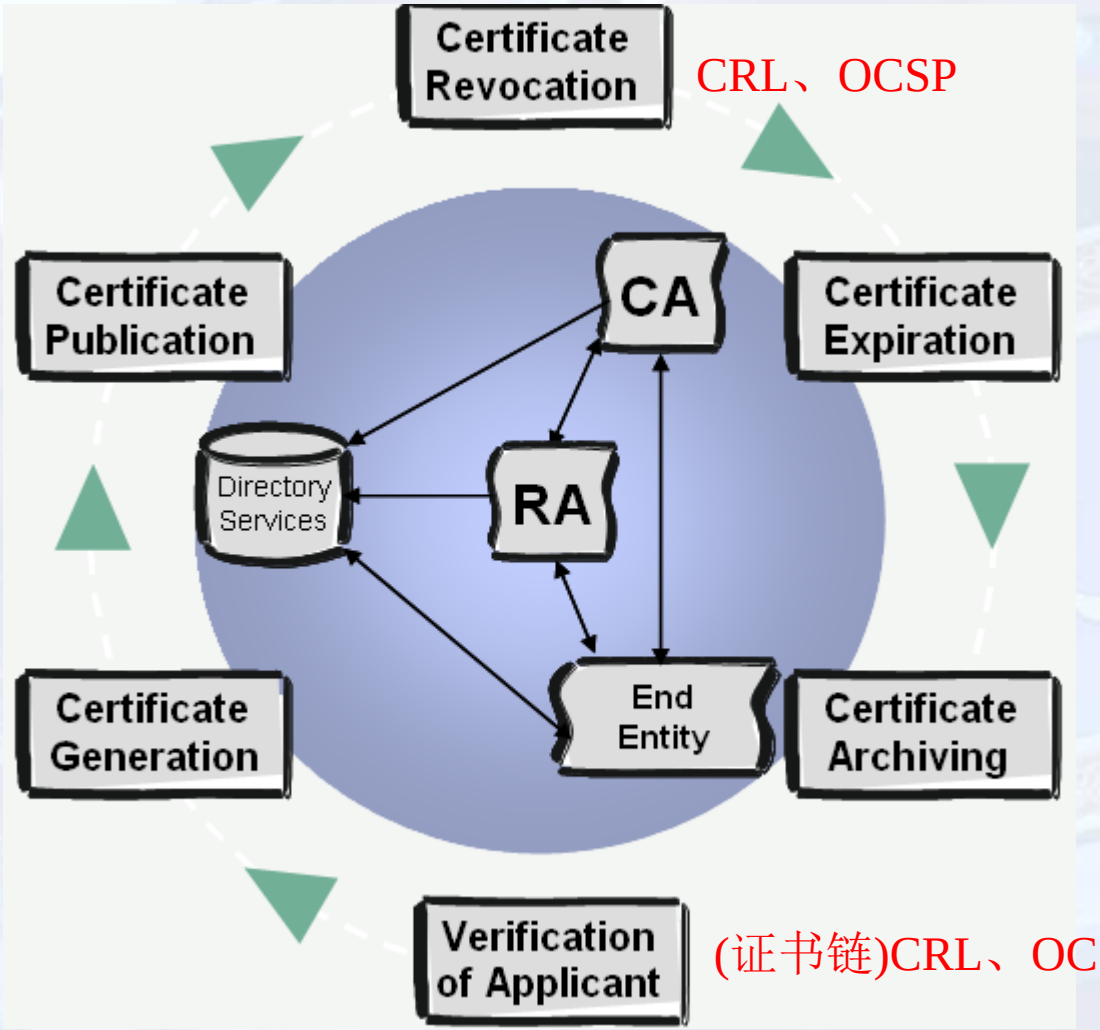
- 数字证书是一个由可信第三方（证书发放机构如CA）对证书主体（Subject）进行数字签名的结构化文档。证书中包含了证书主体的公钥信息。



PKI各组成实体的功能总结

- **CA: 颁发证书和证书撤消链CRL**
- **RA: 本身不颁发证书，但可以向颁发证书的CA登记或担保一个最终用户的身份**
- **Repository：存放证书和证书撤销列表CRL**
- **PMA：核实或协调各种机制，包括操作CA和RA的机制、颁发证书的机制等**
- **EE：证书主体实体和证书验证实体的统称，可以是人，也可以是机器。**

PKI证书生命周期


Certificate Revocation
CRL、OCSP
Certificate Publication
CA
Certificate Expiration
Directory Services
RA
Certificate Generation
End Entity
Certificate Archiving
Verification of Applicant
(证书链)CRL、OCSP

证书创建和分发

- 在验证信息的数字签名时，用户必须获取信息的发送者的公钥证书，以及一些需要附加获得的证书（如CA证书等，用于验证发送者证书的有效性）
- 获取方式：
  - 附加发送
  - 单独发送
  - 从证书发布的目录服务器获得
  - 直接从证书相关的实体获得

证书验证

- 签名验证的过程包括迭代的决定证书链中的下一个证书和它相应的上级CA证书。
- 在使用每个证书前必须检查相应的CRL
- 验证过程：
  - 验证证书链中每一个CA证书
  - 上级CA签名的有效性
  - 证书有效期
  - 是否作废：CRL、OCSP

密钥更新

- 何时应进行密钥更新
  - 密钥泄漏
  - 密钥到期
  - 密钥定时更换

PKI:撤消阶段

密钥/证书生命周期管理以取消阶段来结束。此阶段包括如下内容：

① 证书过期——证书生命周期的自然结束。

② 证书撤销——宣布一个合法证书（及其相关私有密钥）不再有效。

③ 密钥历史——维持一个有关密钥资料的记录（一般是关于终端实体的），以便被过期的密钥资料所加密的数据能够被解密。

④ 密钥档案——出于对密钥历史恢复、审计和解决争议的考虑所进行的密钥资料的安全第三方储存。

证书注销机制

- 由于各种原因，证书需要被注销
  - 比如，私钥泄漏、密钥更换、用户变化
- PKI中注销的方法
  - 证书撤消列表CRL(Certificate Revocation List)：在X.509中定义了一种称为证书撤消列表的机制。
  - 另外某些CA可以利用最新的在线证书状态协议(OCSP)，验证证书的状态。

证书撤消请求

- 证书撤消决定是由认证机构根据某些被授权人的请求决定的。
  - 谁有权撤消证书依赖于认证机构的准则.
  - 认证机构用户和通信各方都要了解这些准则。

证书撤消请求

- 谁有权撤消证书
  - 认证机构用户有权请求撤消自己的证书。
  - 认证机构官员有权撤消用户的证书：在某些规定的情况下，例如用户违反了职责或用户死亡时。
  - 其他人也可能有权请求撤消证书，例如，用户的雇主可以请求撤消雇佣关系证书。
- 认证机构必须能够鉴别任何撤消请求。
- 对撤消证书请求的评价，是赞成还是拒绝撤消请求，则是注册机构的职责。

证书撤消列表

- 在作出了撤消证书的决定后，认证机构必须通知可能的证书用户。
- 通知证书撤消的一般方法是：认证机构定期地公布一个称为证书撤消列表(CRL)的数据结构。
  - 该列表经过认证机构的数字签名，并能被证书用户获取。
  - 证书撤消列表是可以分发的
  - 在CRL列表中，每个已撤消的证书是用自己的证书序列号标识的，证书序列号是在证书发放时由发放证书的认证机构产生的，并包含在证书中。

证书撤消过程

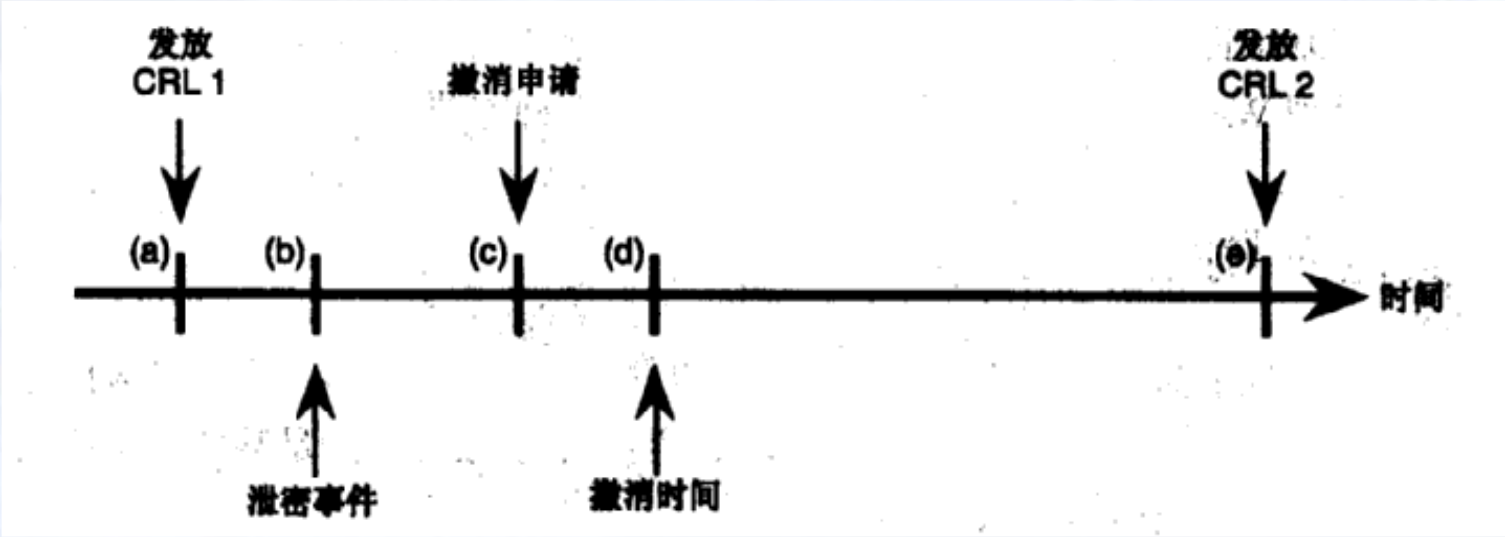
(a) 发放第一份证书撤消表;

(b) 密钥泄漏;

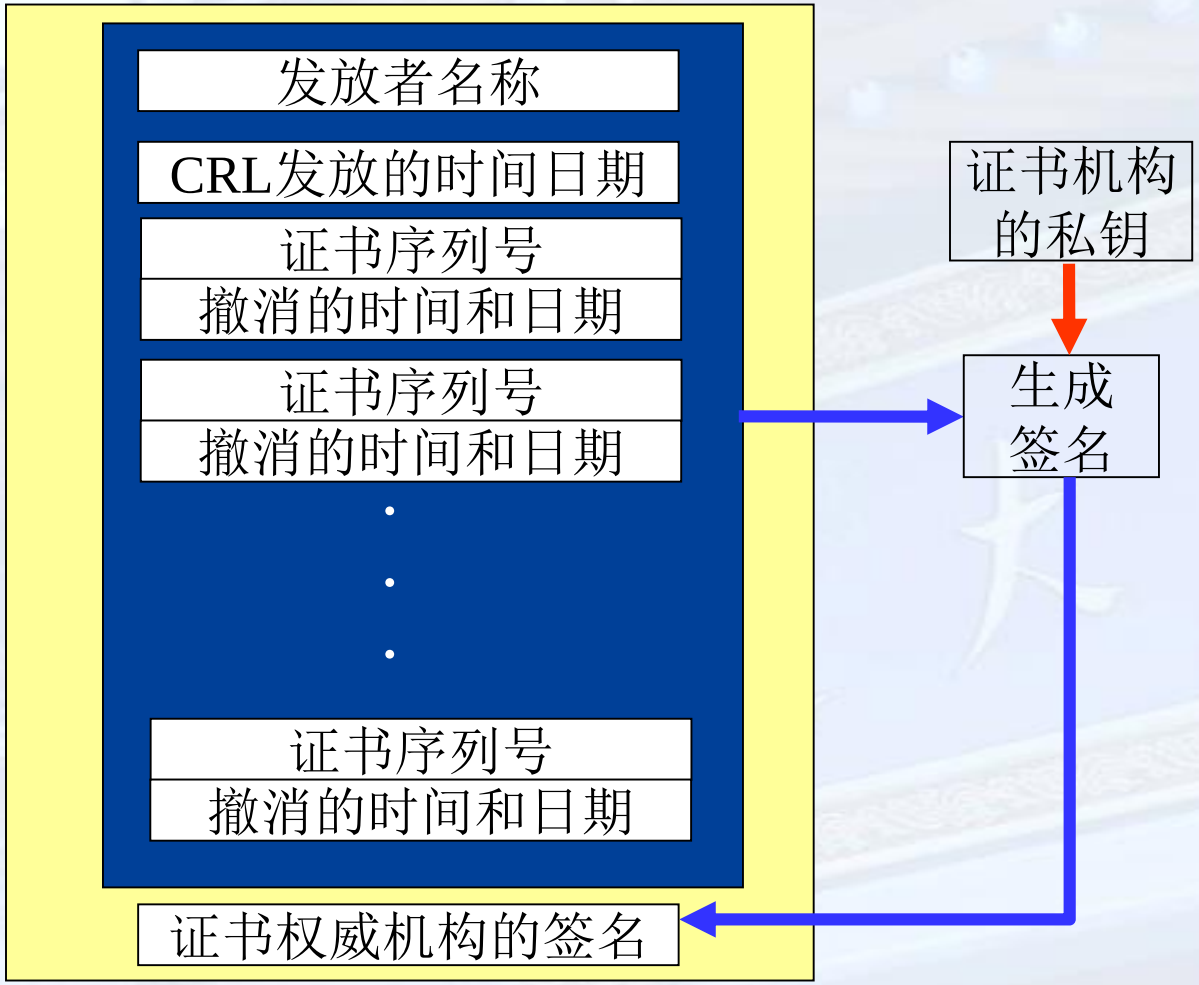
(c) 证书撤消请求;

(d) 撤消时间;

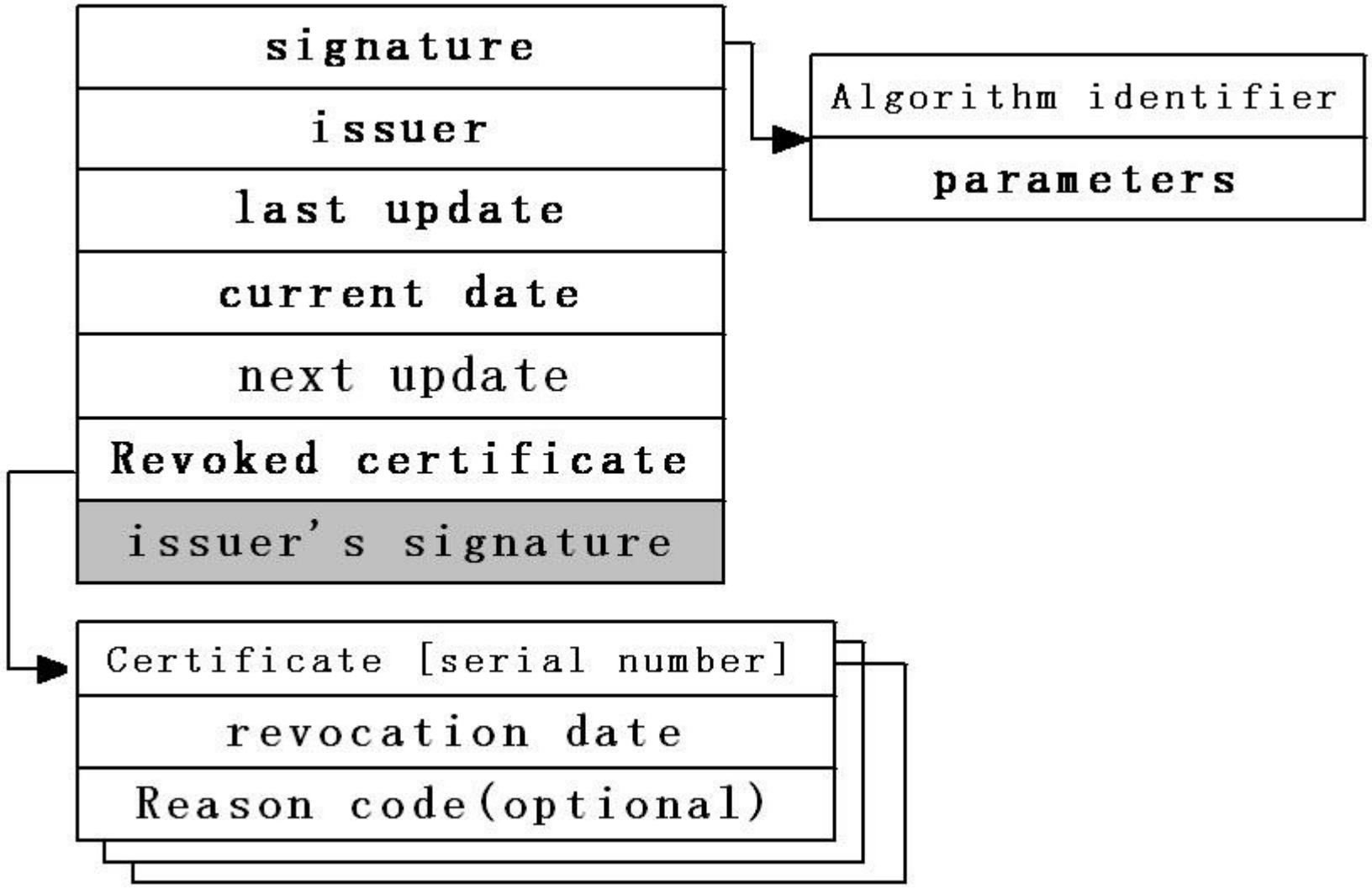
(e) 发放第二份证书撤消表。



撤消表的格式


发放者名称
CRL发放的时间日期
证书序列号
撤消的时间和日期
证书序列号
撤消的时间和日期
证书序列号
撤消的时间和日期
证书权威机构的签名
证书机构的私钥
生成签名

推荐的CRL格式


signature
issuer
last update
current date
next update
Revoked certificate
issuer's signature
Algorithm identifier
parameters
Certificate [serial number]
revocation date
Reason code(optional)

CRL机制

- CA维护CRL的操作：
  - 把新撤消的证书添加到CRL中
  - 把已到期（由证书上起止日期来表明）的证书从CRL中撤除
- 查询
  - 在线证书状态协议OCSP（Online Certificate Status Protocol）
  - 建立CRL分布点DP（Distribution Points）

其它机制

- 重定向CRL
- 增量CRL
- 间接CRL
- 证书撤消树CRT
  - 基于Merkle杂凑树
  - 美国Valicert公司创建
  - 唯一不基于证书撤消列表CRL的周期发布机制
  - 以一种很简洁的方式来表示大量的证书撤消信息

典型CA

- http://www.cfca.com.cn/

CFCA 中国金融认证中心

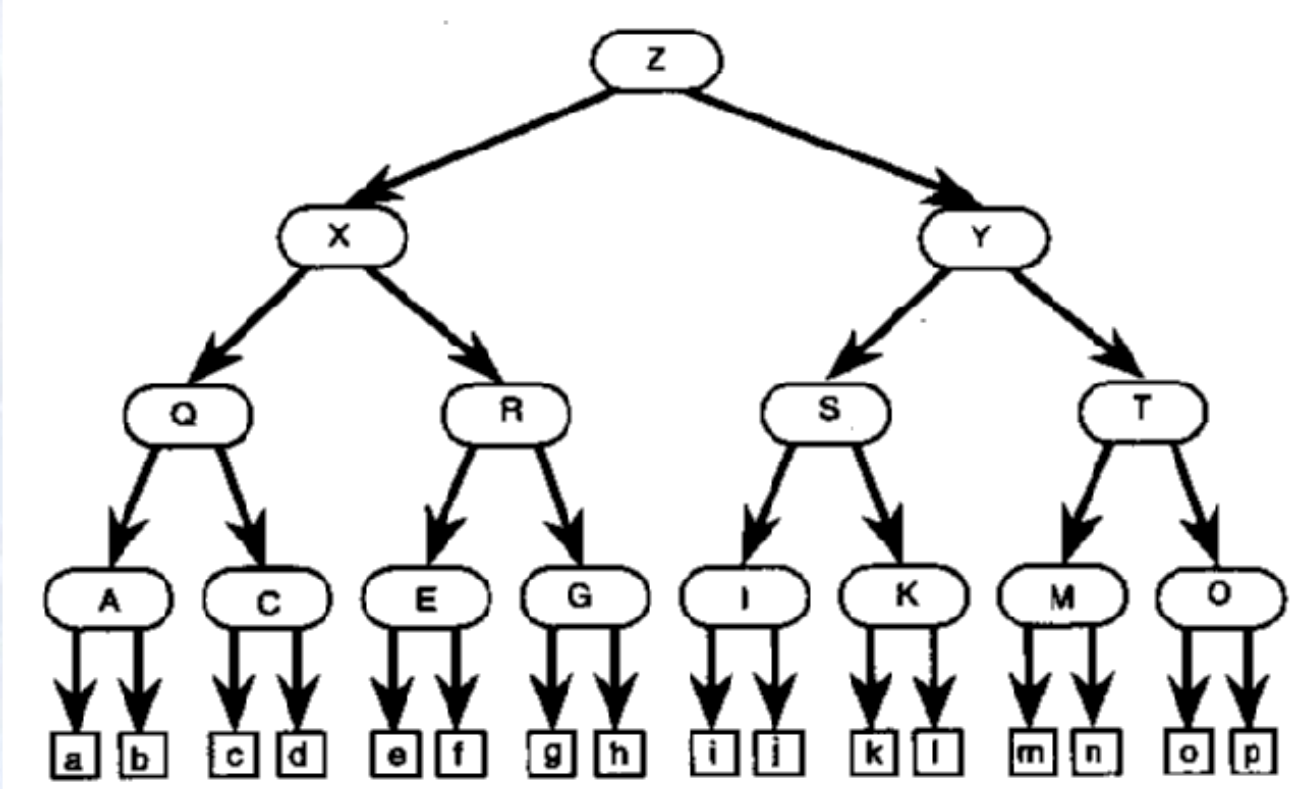
电子认证业务规则（CPS）

数字证书服务协议

- https://www.sheca.com/

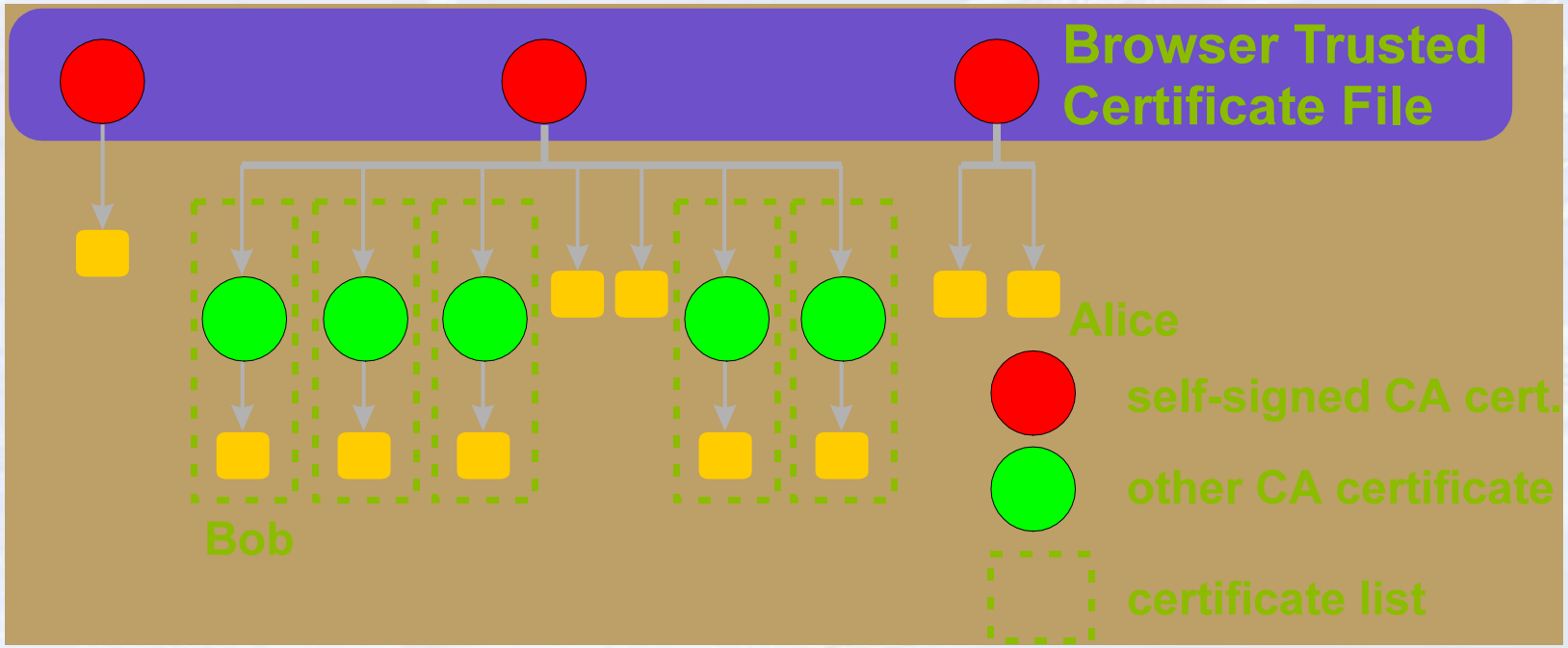
上海市数字证书认证中心有限公司
Shanghai Electronic Certificate Authority Center Co.Ltd.,

层次结构信任模型



Web可信列表

- 可信列表：
  - WEB浏览器和服务器产品
  - 浏览器中包含一个文件，该文件的内容是一些可信的自签名文件。



浏览器中的可信根CA列表

可信列表结构存在的问题

- Web可信列表结构在方便性和简单的互操作性方面有明显的优势。
- 这种模型中，许多CA的公钥被预装在正在被使用的标准浏览器上。
- 这些CA并不被浏览器厂商的根所认证，而是物理地嵌入软件来发布，作为对CA名字和它的密钥的安全绑定。
- 浏览器的用户自动地信任预安装的所有CA，如果这些CA中有一个是“坏”的，安全性将完全被破坏。
- 没有实用的机制来及时有效地撤销嵌入到浏览器中的CA根密钥。
- 不支持交叉认证。
- 不能自动进行证书路径查找和验证。

交叉认证

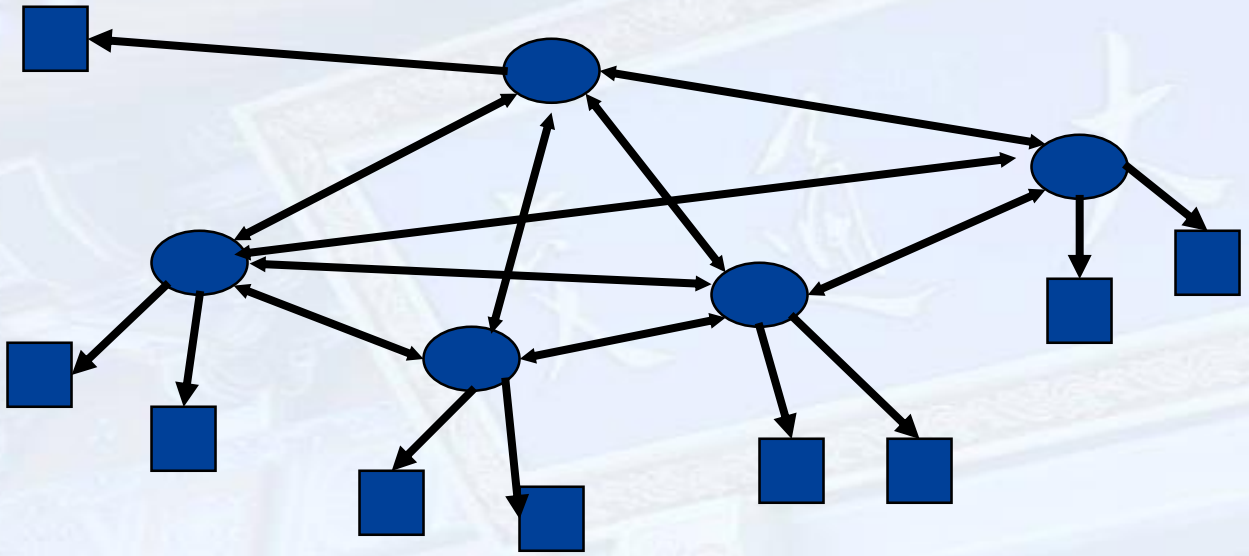
- 交叉认证是一种把以前无关的CA连接在一起的有用机制，从而使得在它们各自主体群之间的安全通信成为可能。
- 交叉认证的实际构成法除了最后交叉认证的主体和颁发者都是CA外与认证是相同的。
- 两个不同的CA层次结构之间可以建立信任关系
  - 单向交叉认证
    - 一个CA可以承认另一个CA在一定名字空间范围内的所有被授权签发的证书
  - 双向交叉认证

交叉认证

- 交叉认证可以分为
  - 域内交叉认证：如果两个CA属于相同的域
  - 域间交叉认证：如果两个CA属于不同的域(例如，当在一家公司中的CA认证了在另一家公司中的CA)。
- 交叉认证的约束
  - 名字约束
  - 路径长度约束
  - 策略约束

网状交叉认证信任模型

- 网状型：相互独立的CA之间可以交叉认证，从而形成CA之间的信任关系网络。
- 网状配置中，所有的根CA之间都可以进行交叉认证。



Any Questions?

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY