Software School of Shandong University

Security Protocols

--- PKI Principles and technology sd03032110

(Chapter 2 PKI Concepts and Architecture)

Instructor: HouMengbo 侯孟波
Email: houmb AT sdu.edu.cn
Office: Information Security Research Office.
Rm: Office Building 111

PKI (Public Key Infrastructure)

- Internet安全系统解决方案, PKI采用数字证书机制管理公钥，通过第三方可信机构CA，把用户的公开钥和身份信息进行有效捆绑，在Internet上有效验证用户的身份。
- 借助数字证书机制分发密钥，通过各种密码学算法和对要传输的信息进行安全处理，通过构造密码安全协议保证信息传输的机密性、完整性、真实性、不可否认性，实现身份认证，以及访问控制，从而全面保证数据存储安全和传输安全安全。

PKI 发展

- 1976，RSA
- 20世纪80年代，美国学者提出PKI概念
- 美国在1996年成立了联邦PKI指导委员会
- 1999年，国际PKI论坛成立
- 2000年4月，美国国防部宣布要采用PKI安全倡议方案。签署《全球及全国商业电子签名法》
- 2000年10月成立欧洲桥CA指导委员会，2001粘月成立欧洲桥CA
- 2001年6月13日，在亚洲和大洋洲推动PKI进程的国际组织 “亚洲PKI论坛” 宣告成立，宗旨是在亚洲地区推动PKI标准化，为实现全球范围的电子商务奠定基础。

PKI 发展

- 我国PKI技术起步于1998年，独立实体运营的SHECA成立。2001年PKI技术列为“十五”863计划重大项目，2002年成立中国PKI论坛。
- 1999年10月7日，《商用密码管理条例》正式由国务院颁布施行，对商用密码产品的科研、生产、销售和使用实施管理。
- 2002年国家商用密码办公室成立，专门负责全国商用密码管理工作，包括商用密码技术与标准化、产品服务和进出口审批、密码应用、监督管理、检测认证等。
- 2005年，发布实施《**中华人民共和国电子签名法**》（2015年修订）
- 2011年成立了密码行业标准化技术委员会。
- 截止2002年，全国成立全国性和区域性行业性CA机构60余家。
- 2002年成立全国信息安全标准化技术委员会，成立“PKI/PMI（WG4）”工作组

PKI 发展

- 2000年至今，中国PKI技术和应用大发展
  - 技术体系标准化　商密SM系列标准
  - 专业公司蓬勃发展，有2000多款商用密码通用产品，上千家从业单位
  - 产品适应 传统因特网、移动终端、无线网络、云计算、物联网等环境
  - 2017年，国家密码管理局起草了《中华人民共和国密码法（草案征求意见稿）》
- 国际标准 PKIX 系统化 标准化
  - PKIX系列标准(Public Key Infrastructure on X.509)是由因特网网络工程技术小组(Internet Engineering Task Force)的PKI小组制定，PKIX标准化是建立互操作的基础。标准主要定义基于X.509的PKI框架模型，并以RFC形式发布。

基础设施

- 基本概念

  新华字典解释: 为工农业生产部门提供服务的各种基本设施。如铁路、公路、运河、港口、桥梁、机场、电力、邮电、煤气、供水、排水等设施。广义的还包括教育、科研、卫生等部门。因其建设投资大、周期长，一般由政府投资或支持。

  是普适性基础平台，是大环境里的基本框架. 如：信息时代的网络基础设施等.

- 地位

  应用支撑功能，通用 / 实用性

- 特性
  - 易于使用 / 众所周知的用户界面
  - 可预测 / 有效的服务
  - 应用设备无需知道设施工作原理

网络基础设施

- 电力通信网络中，用于连接计算机互联互通的一切基础元素的集合。
  - 所有的硬件
  - 所有的软件
  - 所有的人员
  - 所有的执行策略
  - 所有的规程
  - ……

网络安全基础设施

- 提供网络安全基本框架，可以被组织内任何需要安全服务的应用和对象使用
- 接入点是统一的，便于使用的
- 适应多种环境框架 / 互操作能力
- 可管理 / 透明性
- 安全一致性
- 保证数据和资源的本地安全以及传输安全

安全基础设施服务

- 安全登录(认证)

  认证:确认一个实体确实是其向他人声明的.

  用户标识 / 认证信息（口令或其他机密信息)

  防止口令截取 / 监听 / 重放攻击

  选择好的口令：长度 / 质量 / 经常修改

  口令不在网络上直接传输

  单点登录

安全基础设施服务

- 终端用户透明

  基础设施是个黑盒子，无需知道提供服务的细节

  用户只需知道是成功还是失败.

安全基础设施服务

- 全面的安全性
  - 单一、可信的安全技术　如:公钥密码技术
  - 机密性　　如:对称加密　公钥加密
  - 完整性　　如:HASH函数　MAC码　数字签名
  - 身份认证　　如:数字证书　CA
  - 抗否认　　如:数字签名
  - 访问控制　　如:属性证书

安全基础设施在信息基础设施中的地位

- 信息基础设施容易遭受攻击和破坏
  - 攻击数据
  - 攻击控制系统　　众多案例
- 安全基础设施是保证信息基础设施的有利保障

公钥基础设施PKI

- 通俗的说，Public Key Infrastructure, PKI是一个用非对称密码算法原理和技术实现并提供全面安全服务的具有通用性的安全基础设施。是一种遵循标准的利用公钥技术为电子商务、电子政务的开展提供一整套安全解决方案的基础设施。
- PKI采用数字证书机制管理公钥，通过第三方可信机构－CA，把用户的公开钥和身份信息进行有效捆绑，在Internet上验证用户的身份。通过数字证书，通过对要传输的信息进行加密和签名，保证信息传输的机密性、完整性、真实性、不可否认性，实现身份认证，从而全面保证信息安全传输。

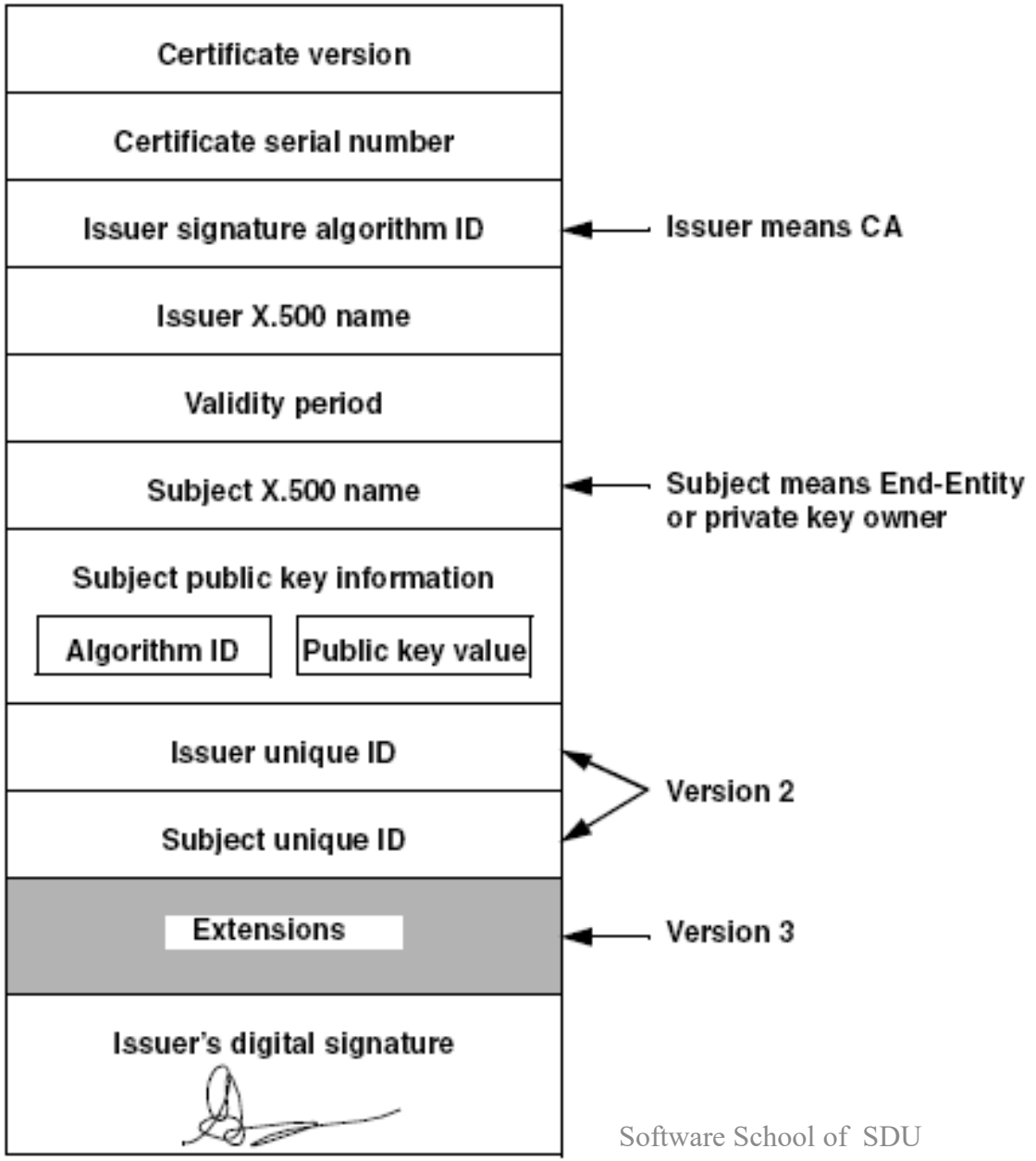
PKI

- PKI is a framework that consists of security policies, encryption mechanisms, and applications that generate, store, and manage keys. PKI also provides procedures to generate, distribute, and utilize keys and certificates. PKI provides a mechanism to publish the public keys that are part of public key cryptography. It describes the policies, standards, and software that are used to regulate certificates, public keys, and private keys.
- the core security functions provided by cryptography are confidentiality, non-repudiation, authentication, and integrity.
- In addition, Policies that specify rules for operating cryptographic systems, Mechanisms for managing, storing, and creating keys. Guidelines for managing, storing, distributing, and creating keys and certificates should also be provided.

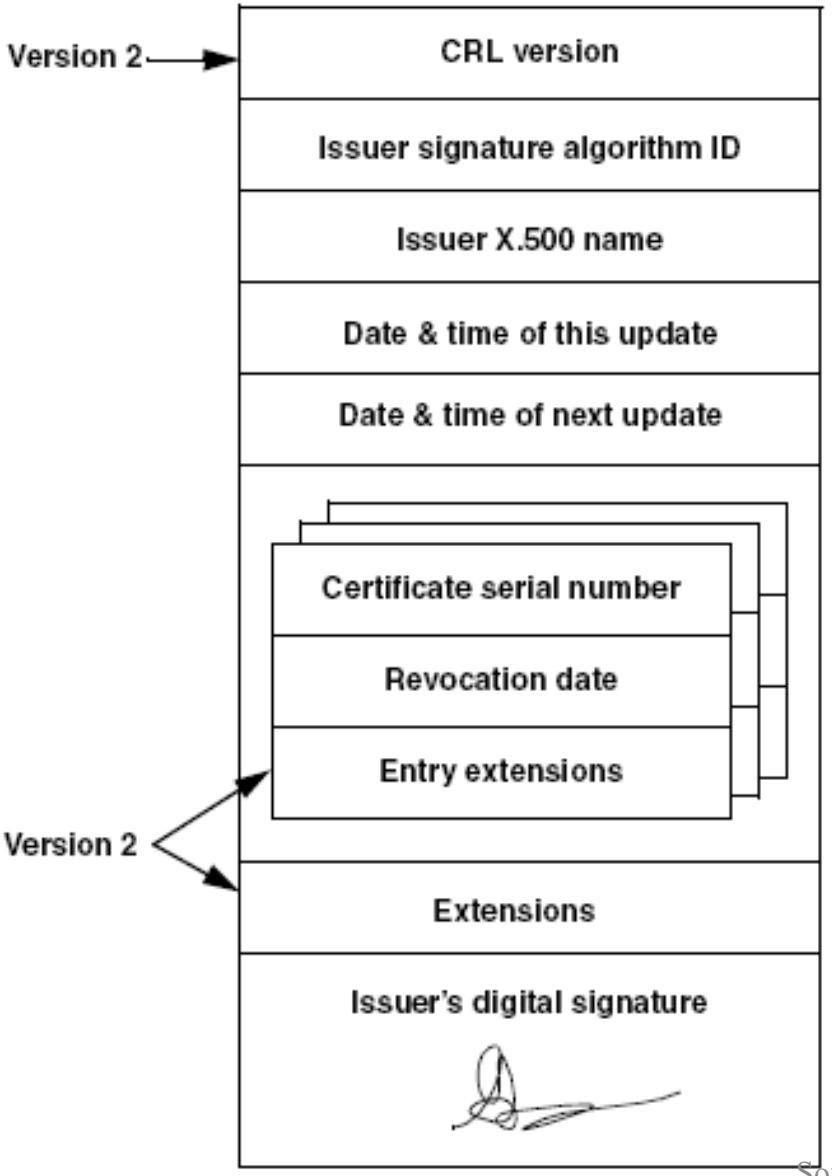
概念1: Certificate

- issued by a Certification Authority (CA), containing:
  - version (1, 2, or 3)
  - serial number (unique within CA) identifying certificate
  - signature algorithm identifier
  - issuer X.500 name (CA)
  - period of validity (from - to dates)
  - subject X.500 name (name of owner)
  - subject public-key info (algorithm, parameters, key)
  - issuer unique identifier (v2+)
  - subject unique identifier (v2+)
  - extension fields (v3)
  - signature (of hash of all fields in certificate)

X.509 Certificate



CRLs, Certificate Revocation Lists



主观题 10分

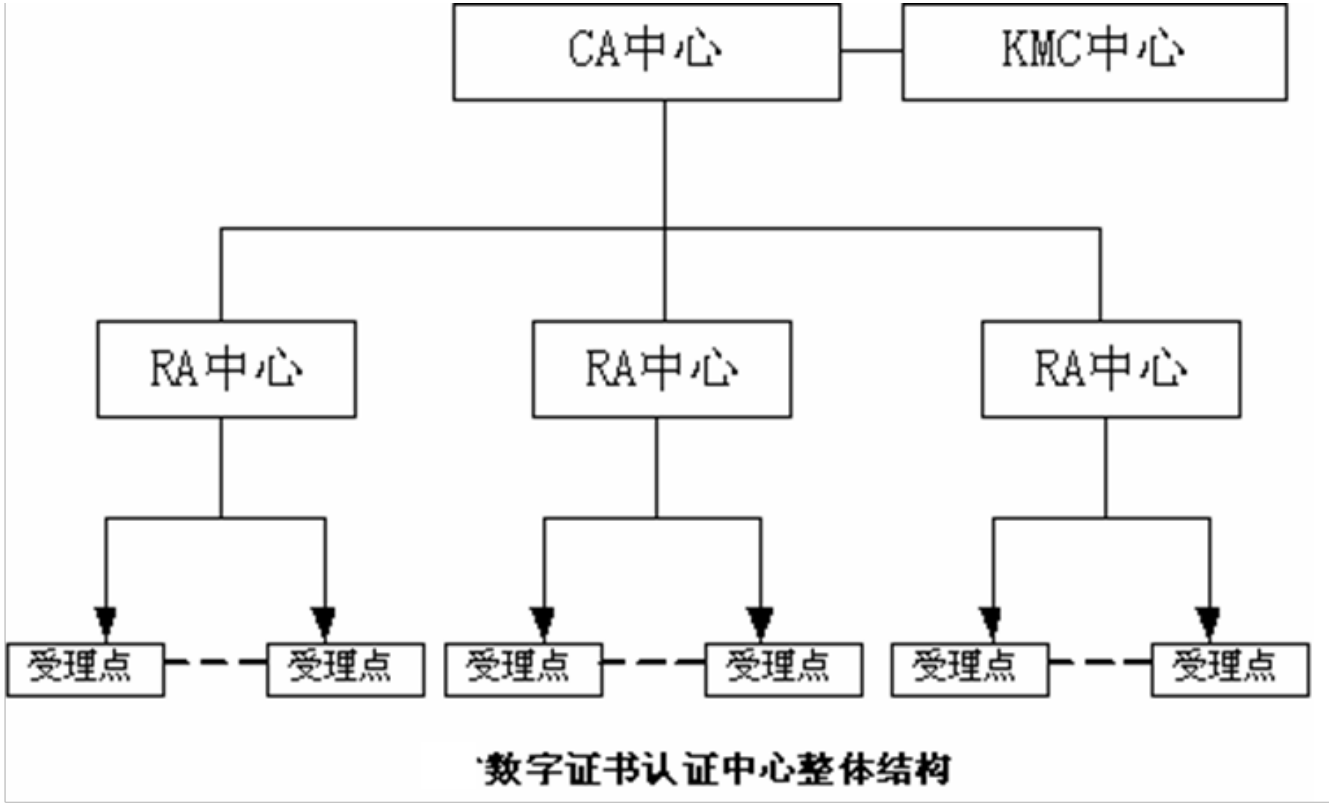
设置

请问数字证书的合法有效性验证包含哪些方面?

正常使用主观题需2.0以上版本雨课堂

作答

概念2: CA, Certificate Authority



数字证书认证中心整体结构

概念3: Attribute Certificate

- **属性证书(Attribute Certificate)**

是采用数字签名技术将用户的身份信息和相关属性(如用户角色/权限等)进行有效捆绑形成的认证对象。通过与身份证书的结合使用，实现网络身份认证和访问控制。

PKI服务的突出优势

- 节省费用(单一\标准\独立\重用)
- 企业内部互操作性\企业间互操作性
- 一致的解决方案(兼容性)
- 实际安全性(标准化\成熟性)
- 安全服务提供者的选择(可度量\可靠性\认证管理)

PKI 面临挑战

- 现有应用并不支持PKI，由于PKI属于基础设施,与应用的集成性较差,因而部署困难
- PKI基于数字信任状实现信任和认证，对高层信任至关重要.
- PKI实现需要专用复杂技术来实现，由于与应用集成性差, 所以并非所有PKI以及应用是无缝和交互友好的。
- PKI的ROI (Return of Investment)自身是零,因为它是基础设施而不是终端用户应用。ROI应基于PKI上层应用。

PKI服务的认证性实现

- 前提是: 安全的获得对方的公开密钥(方式)
- 认证手段
  - 公共可信时间环境中：请求信息签名方案
  - 防范重放攻击环境中：挑战信息签名方案

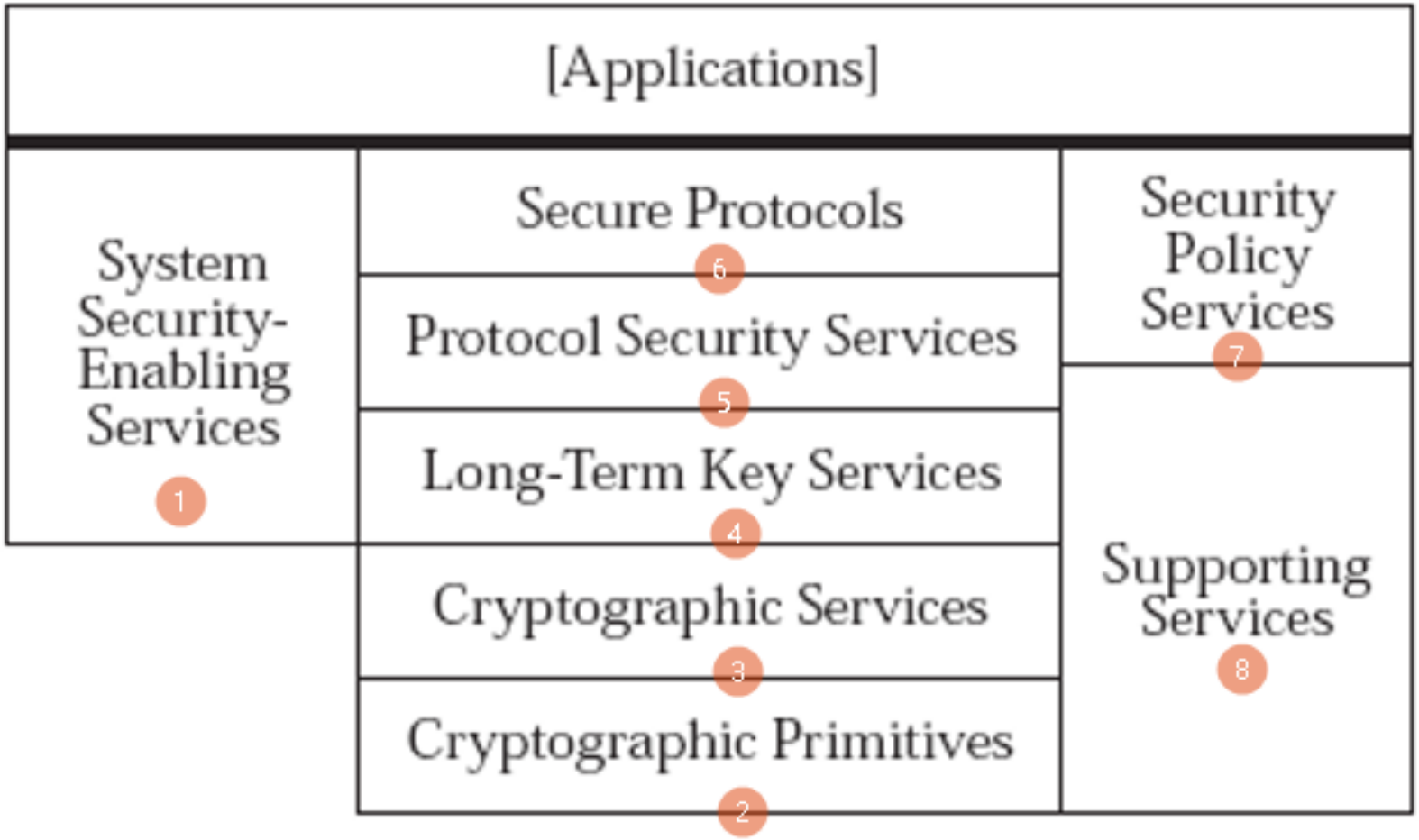
PKI服务的保密性实现

- 生成一个对称密钥（密钥协商协议）
- 用对称密钥加密数据（使用分组密码）
- 加密后的数据发送给对方

PKI服务的不可否认性实现

- 数字签名 + 时间戳服务
- 证据（原始数据 + 签名信息 + 密钥 + 时间戳）

PKI Architecture

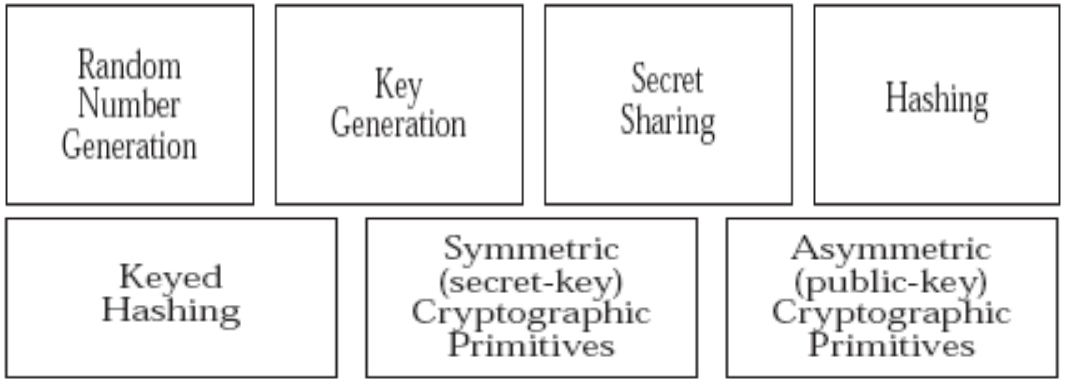


1. System Security-Enabling Components

•Functions

System functions (e.g. operating system functions) are needed to support user logon, user credential acquisition, and association of security state information with user processes and threads. For example, once a user has acquired credentials by authenticating himself to a Smartcard, that user's processes should be able to use the Smartcard interface to sign data using a private key stored on the smartcard. This will only be possible (and secure) if the system has maintained security state information associating the user's processes with the handle returned when the user authenticated himself to the smartcard.

2. Cryptographic Primitive Components



- **Functions**

These components provide access to low-level cryptographic primitives such as key generation, hash function application to a data buffer, encryption of a data buffer using secret-key or public key algorithms, decryption of a data buffer using secret-key or public-key algorithms, etc.

- **Interfaces**
  - The RSA BSafe library interface
  - RSA PKCS-11
  - CSSM API (from CDSA, The Common Security Services Manager (Version 2.0)
  - The Microsoft CryptoAPI 2.0 etc.

3. Cryptographic Service Components

Interfaces

· CSSM API (from CDSA, Version 2.0)
· Microsoft CryptoAPI 2.0
· SESAME CSF API
· Advanced Encryption Standard (AES)

Others include:

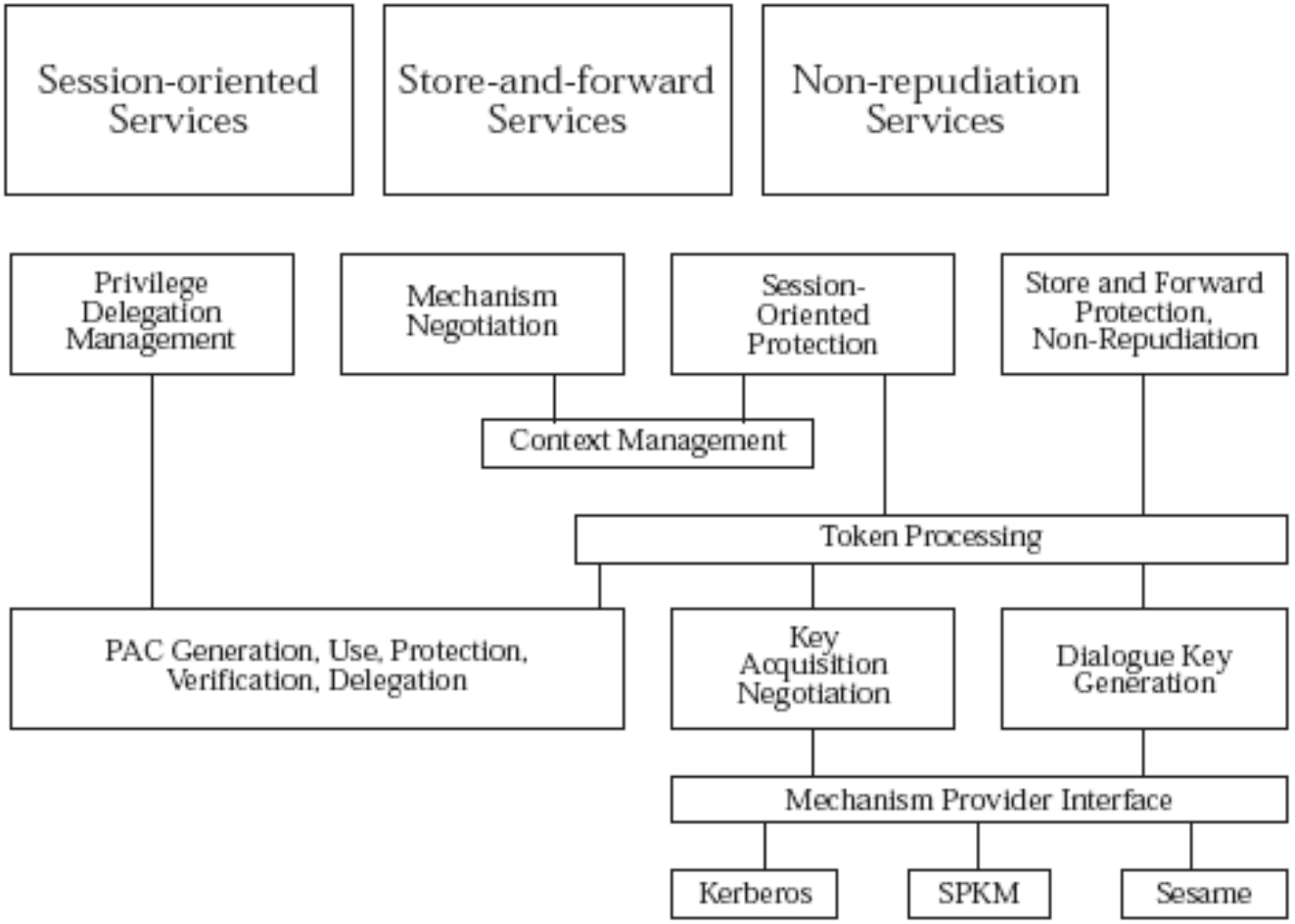
· Cryptoki
· RSA BSAFE

4. Long-Term Key Services Components

Interfaces :

CSSM (from CDSA, Version 2.0)

5. Protocol Security Services Components



Protocol Security Service Structure

Protocol Security Services Components

- **Interface**
  - **Session-Oriented Protocol Security Services**

    IETF RFC 2078: The GSS-API, Version 2.
  - **Store-and-Forward Protocol Security Services**

    IETF RFC 2479:IDUP-GSS-API.
  - **Non-Repudiation Services**

    IETF RFC 2479: IDUP-GSS-API.
- Other interfaces include:
  - Microsoft SSPI
  - OMG CORBA Security
  - TIPEM
  - SHTTP

6. Secure Protocol Components

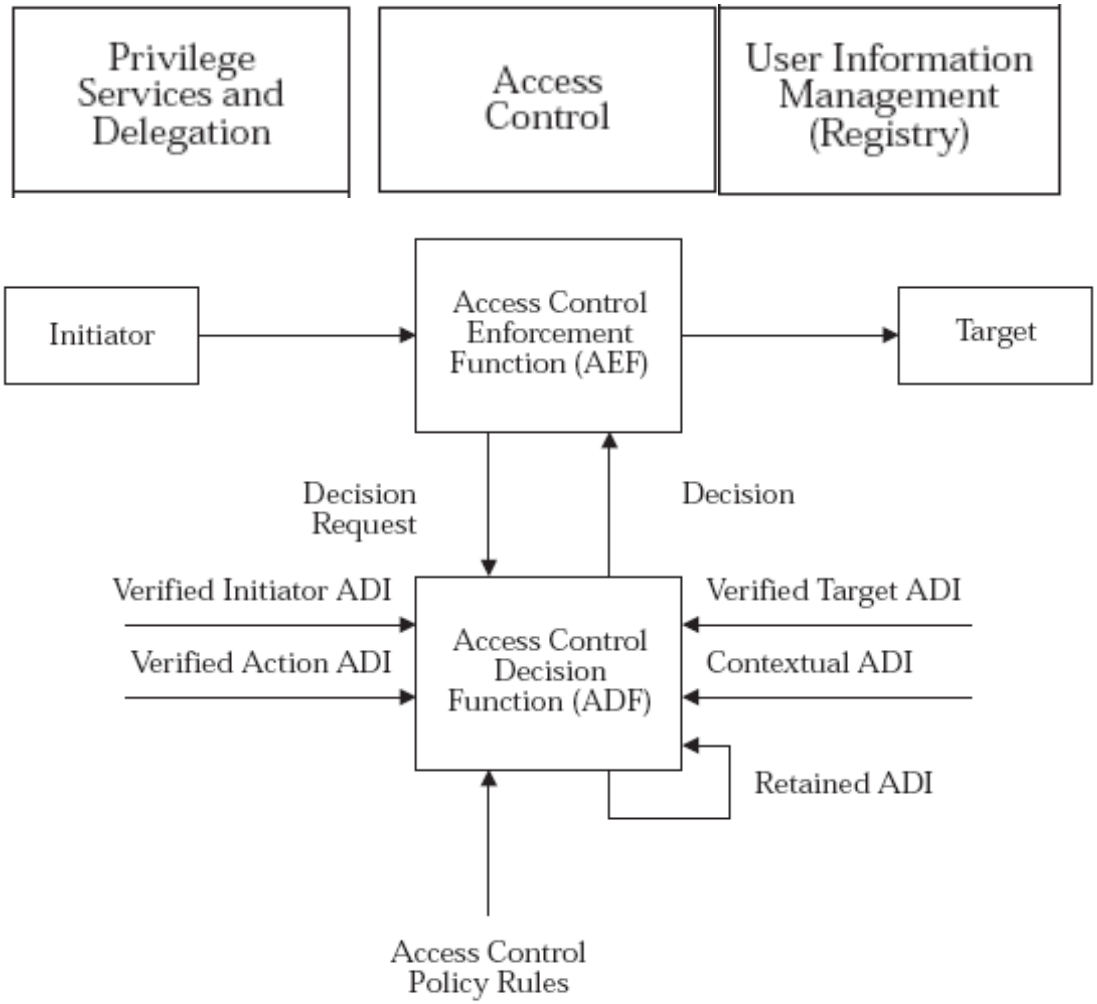
Protocols:

· *Connection-oriented peer-to-peer*: ONC GSS RPC, TLS, SHTTP, HTTPS, OMG SECIOP

· *Connectionless peer-to-peer*: IPsec

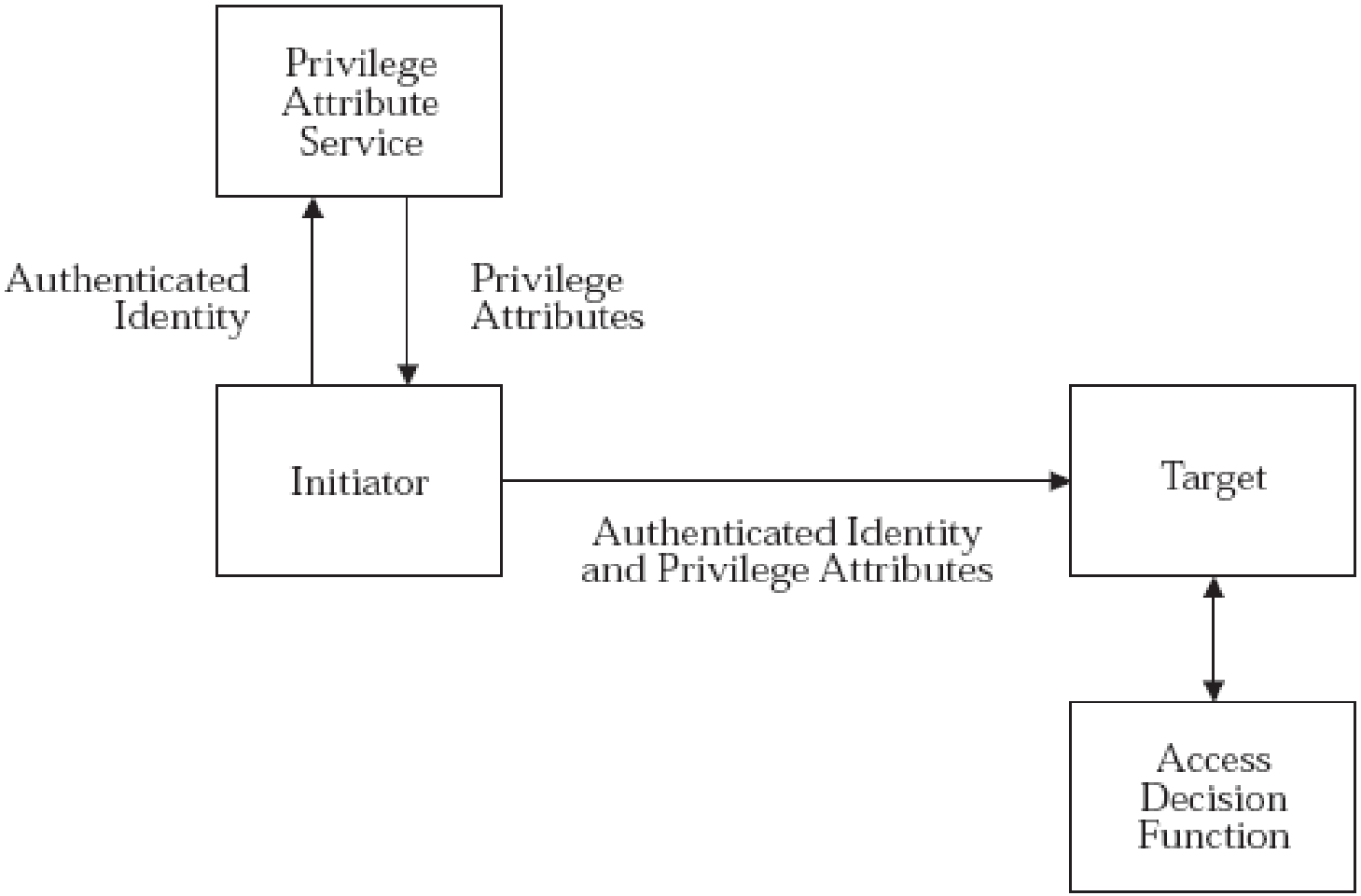
· *Connectionless multicast*: S/MIME, Open PGP, Secure multicast

7. Security Policy Services Components

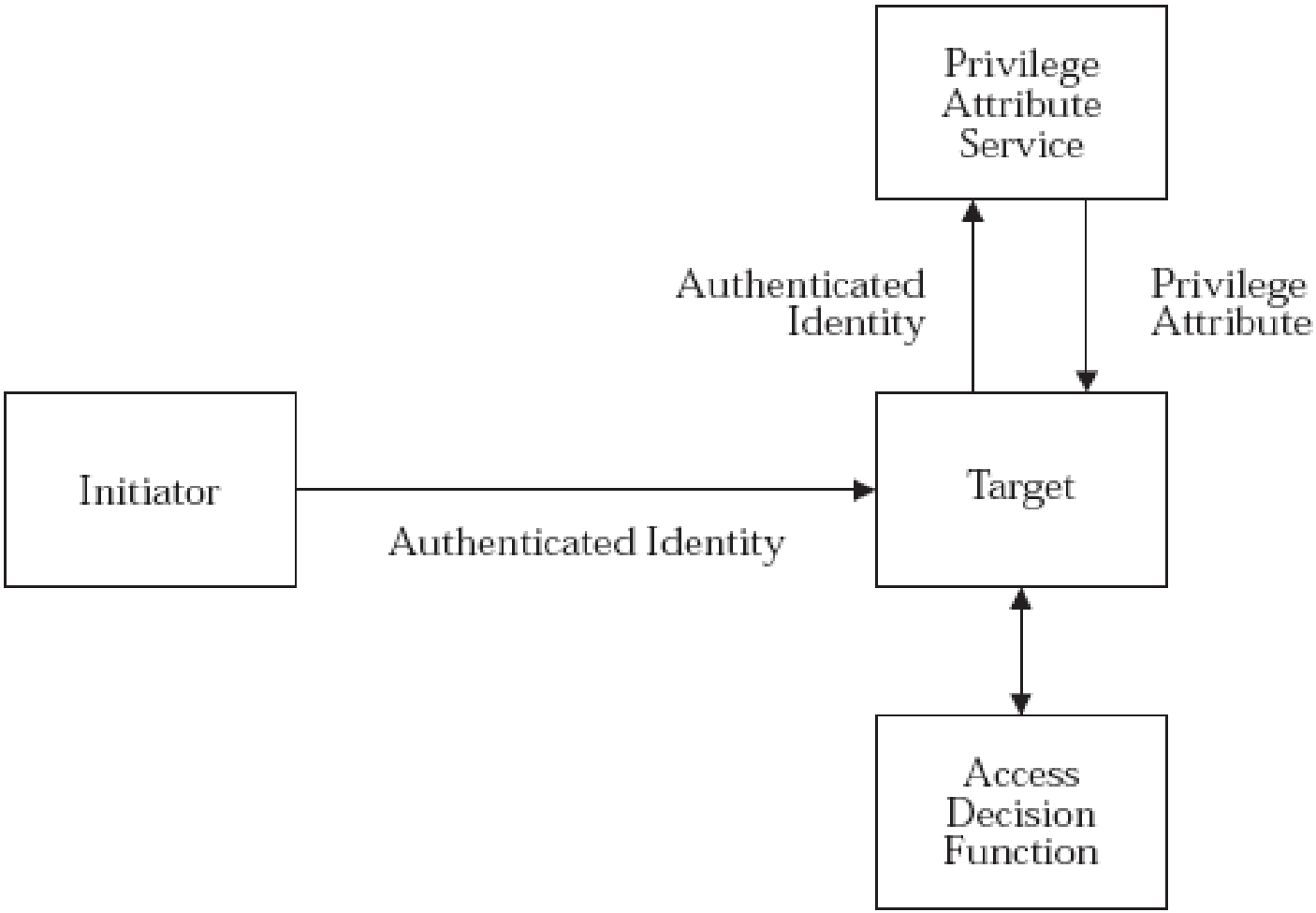


Access Control Decision Model

Privilege Attribute Service: *Push model*



Privilege Attribute Service: *Pull model*



8. Supporting Services Components

- **Security Auditing Services**

  support accountability within the PKI Architecture and may also support notarization services.
- **Time Service**

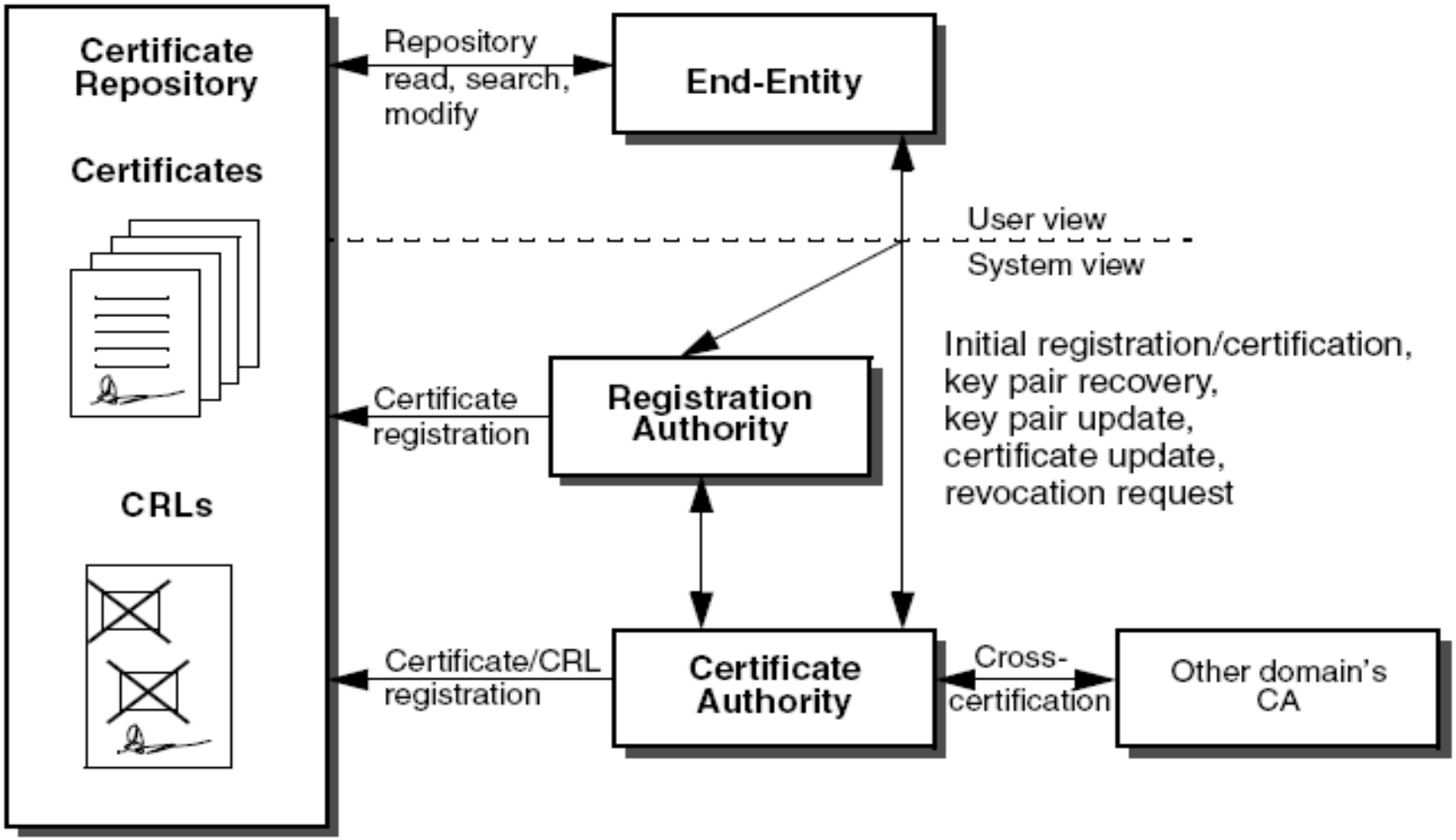
  fundamental to the synchronization of time within a distributed PKI Architecture and the basis of time stamps that may be incorporated into security certificates and also be used by a notarization service.
- **Directory Services**

  necessary to support the location of PKI Architecture users and components and the retrieval of attributes applicable to them.

PKI系统结构组成

- **Certificate Authority(CA) &Registration Authority (RA)**
  - 证书的申请和签发机构，是PKI的核心，是PKI应用中权威的、可信的、公正的第三方机构。
- **Keys Backup & Recovery System**
  - 对用户的解密密钥进行备份，当丢失时进行恢复，而签名密钥不能备份和恢复。
- **Certificate Revocation System**
  - 证书由于某种原因需要作废，终止使用，须将证书列入CRL中。
- **Certificate Distribution System (CDS) or Repository(CR)**
  - 证书的集中存放地，提供公众查询。
- **End Entities and PKI application Interfaces**
  - 为各种应用提供安全、一致、可信任的方式与PKI交互。

General PKI structure



典型PKI应用系统实现

- 认证中心CA　certificate/CRL 创建注销　密钥管理
  - X.509数字证书/证书注销列表CRL
  - CA/RA操作协议
  - CA管理协议
  - CA政策制定
- X.500目录服务　Certificates/CRLs 发布,状态管理
- 高强度安全的WEB Server/WEB Client
  - 标准WEB接口SSL协议
- Client/Server 结构安全应用接口

PKI服务要处理好的几个方面

- 良好密钥的安全生成(生成安全\保存安全)
- 初始身份的确认(审核等级)
- 证书颁发\更新\终止(证书生命周期管理)
- 证书有效性检查(完善的检查步骤和内容)
- 证书等相关信息的分发(分发方式\方便性\及时性)
- 密钥的安全存档和恢复(备份\周期管理)
- 数字签名和数字时间戳的产生
- 信任关系的建立和管理-CA

认证中心CA

- 是PKI的信任基础，权威、可信的第三方TTP
- 基于数字签名技术，其签名公钥高效安全发布
- 高安全性和可用性
- 数字证书和密钥管理(全周期)

认证中心CA功能

- 证书申请\审核\签发\发布
- 证书更新
- 证书注销
- CA证书更新/密钥更新
- 证书验证
- 生成和发布证书注销列表
- 证书状态查询服务 - OCSP
- 数字证书归档
- 密钥归档
- 历史数据归档
- 数字时戳服务

CA模块

- 签发服务器
- 密钥管理服务器
- 证书管理服务器
- 证书发布和CRL发布服务器
- OCSP服务器
- 时间戳服务器(可选)
- WEB服务器

CA密钥管理

- CA签名密钥

  用于签发用户证书，安全度最高，生命周期很长。
- CA签名密钥更新

用户密钥管理

- 密钥种类
  - 签名密钥对

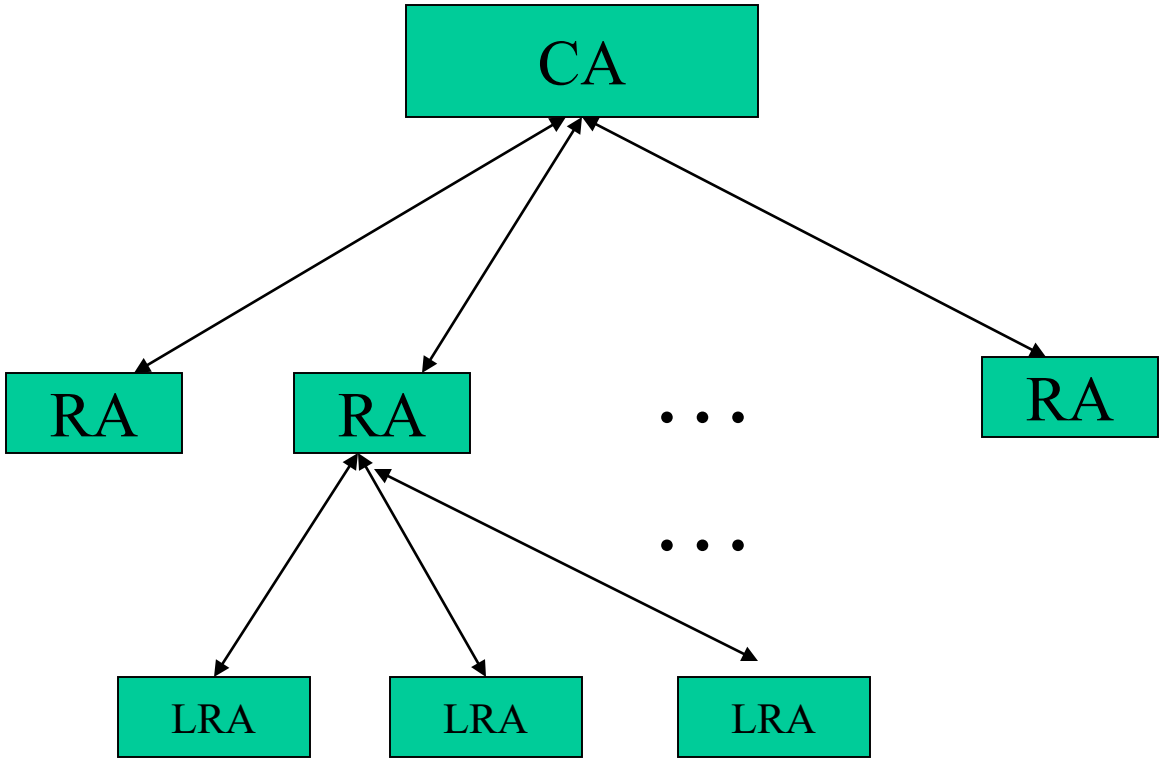
    由签名私钥 / 签名公钥组成，一一对应。用于用户信息签名和验证签名。对应的证书称为签名证书。
  - 加密密钥对

    由加密共钥 / 解密公钥组成，一一对应。用于用户信息加密 / 解密，密钥交换等。对应的证书称为加密证书。
- 生成方式
  - 用户自己产生　一般是指签名密钥对。
  - CA密钥管理中心产生并分发　一般是指加密密钥对。

CA中心基本结构

- 一般三级结构
  - CA系统　签发管理　目录服务 / 数据库服务 / OCSP服务 / 数字时戳服务
  - RA系统　注册登记　　负责某一区域 / 行业
  - LRA系统　本地受理点　面向最终用户

CA结构



RA中心

- RA(Registry Authority)是数字证书注册审批机构，是CA管理功能的延伸。
- 负责证书申请者的信息录入、审核等工作。
- 证书介质管理：IC卡、USB - KEY、文件等

RA功能

- 支持确定或确认签署者身份：
  - 主体注册证书的个人认证
  - 确认主体所提供的信息有效性
  - 对被请求证书属性确定主体的权利
  - 确认主体确实拥有注册的私钥
  - 在需要撤销时报告密钥泄露或终止事件。
  - 为识别身份的目的分配名字。
  - 在注册初始化和证书获得阶段产生共享秘密。
  - 产生公 /私密钥对。
  - 认证机构代表最终实体开始注册过程。
  - 私钥归档。
  - 开始密钥恢复处理。
  - 包含私钥的物理环网（例如智能卡）的分发。

证书注册实现

- 初始化
  - 最终实体获得服务要连接的地方
  - 连接的PKI是否提供已告知服务
  - 最终实体对RA进行认证
  - 最终实体要产生自己的密钥对，在注册请求时使用
- 初始信任　RA对最终实体进行认证
  - 手工方式 证件检查，然后提交注册管理员签名过的申请。 安全度高
  - 在线方式　分配 用户名 / 口令 认证
- 注册要求

  注册期间利用的信息不会全部体现在证书中，保证隐私

证书注册实现

- 私钥拥有者确认
  - 如果密钥是用于数字签名，则可通过签名申请信息来证明
  - 如果密钥是用于加密
    - 使用智能卡产生，私钥安全保存，导出公钥
    - RA使用随机质询，用申请者公钥加密，申请者解密确认
    - CA产生密钥，安全传递给申请者

证书签发

- 离线证书签发
  - 用户向RA面对面提交审查资料,由RA提交CA签发证书.
- 在线证书签发
  - 用户将申请信息在线提交CA,在CA认可后,用户根据回馈的信息即时生成密钥,即时下载并安装证书.(需要基本的认证机制)
- 证书签发类别
  - **User certificates**

    Person/Organization/VPN/SSL/Device Manufacturing/Code signing/Wireless Device…
  - **CA certificates**
  - **Cross certificate**

浏览器申请证书过程

- WEB页面提供申请界面和申请表单
- 页面上提供密钥生成程序，并可选择密钥长度
- 提交表单，页面程序将产生密钥对，私钥本地密钥存储区安全存储，公钥将和页面参数一起传递给WEB服务器，通常上传信息包含该密钥的签名值。
- WEB服务器端接收申请信息和公钥，并验证签名
- 检查信息合法性，并根据证书政策实施约束
- 生成证书，返回用户（即时 / 指导下载）
- 浏览器在本地证书库加载该证书

证书撤销

- 证书废止原因:
  - 密钥泄密
  - 相关信息变更
  - 终止使用
  - CA原因
- CRL 原理
  - 定期签发CRL,用户定期下载

密钥生成、备份和恢复

- 原因
  - 遗失保护口令/介质破坏
- 一个用户要使用PKI系统,首先要在初始化阶段生成属于自己的密钥对.
- 由于密钥空间的特点,生成的密钥一般是唯一的,不重复的.
- 密钥备份方式: 自己备份/托管备份/强制托管
- 密钥恢复发生在需要该密钥而该密钥已经不在手上, 往往向CA中心或密钥管理中心申请.

证书注销列表CRL处理

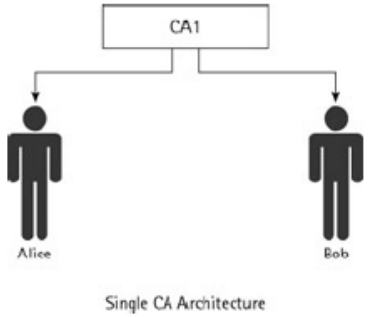
- 该列表记录尚在有效期之内,但是因各种原因而注销的证书.
- 由CA中心签名
- 注明证书注销时间/原因/签发日期等信息

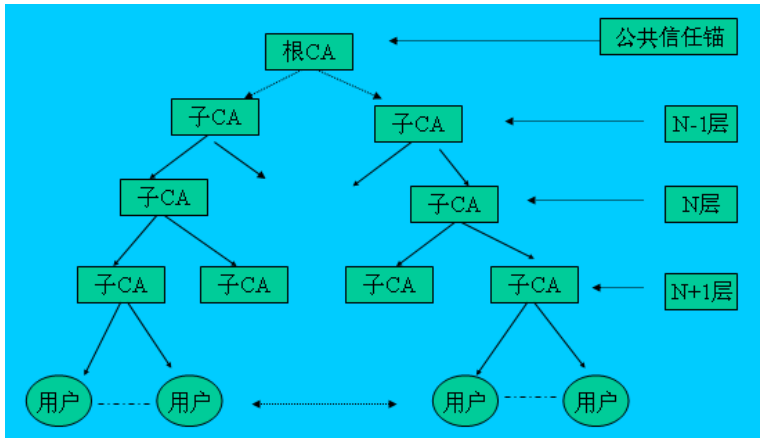
信息发布

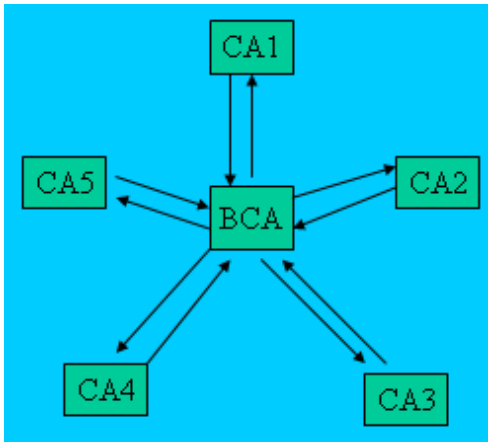
- 证书/CRL分发方式
  - 私下分发
  - 集中分发 目录服务

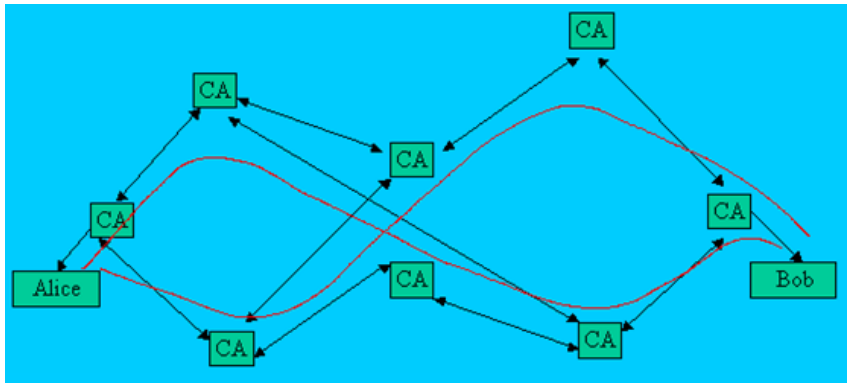
CA认证结构—信任模型

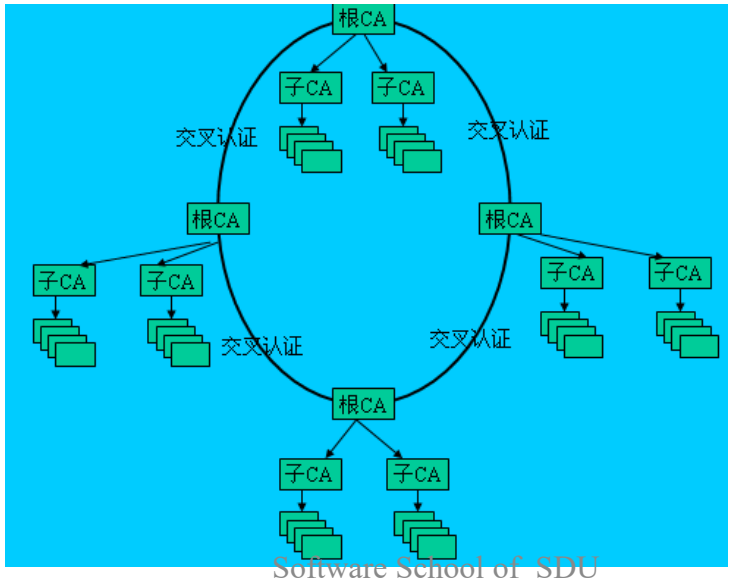
- Single CA architecture / Enterprise PKI architecture / Hybrid PKI architecture



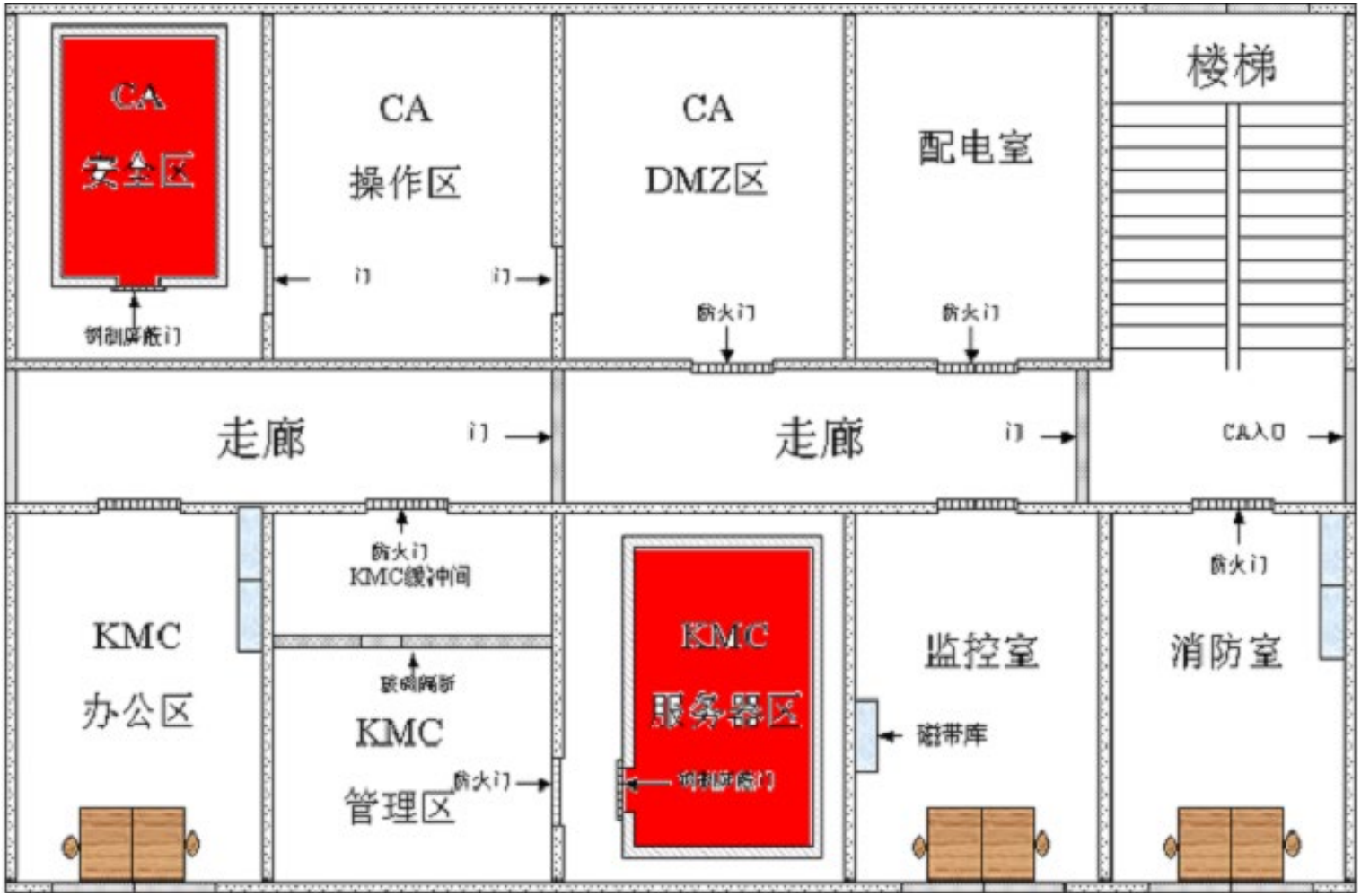




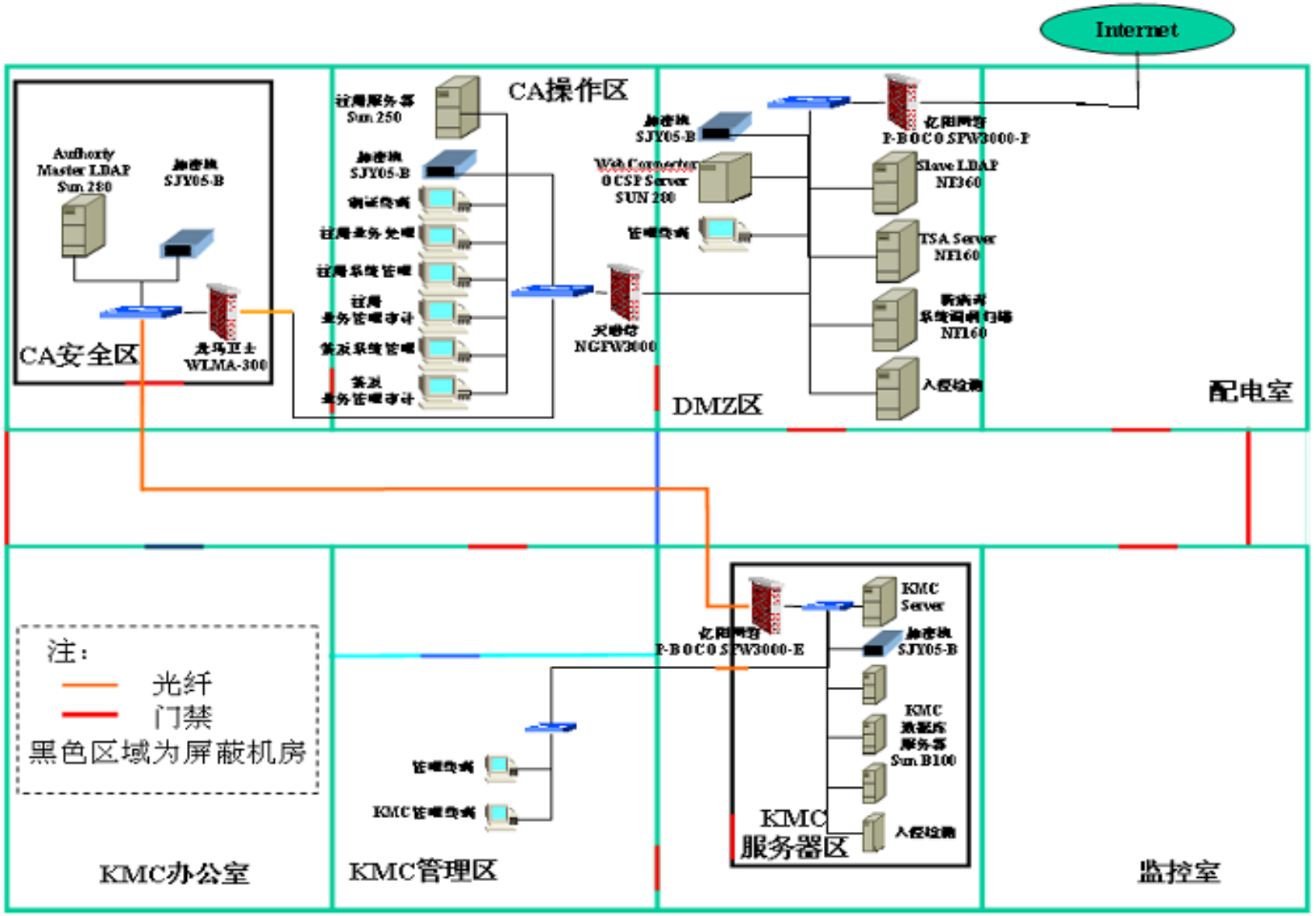




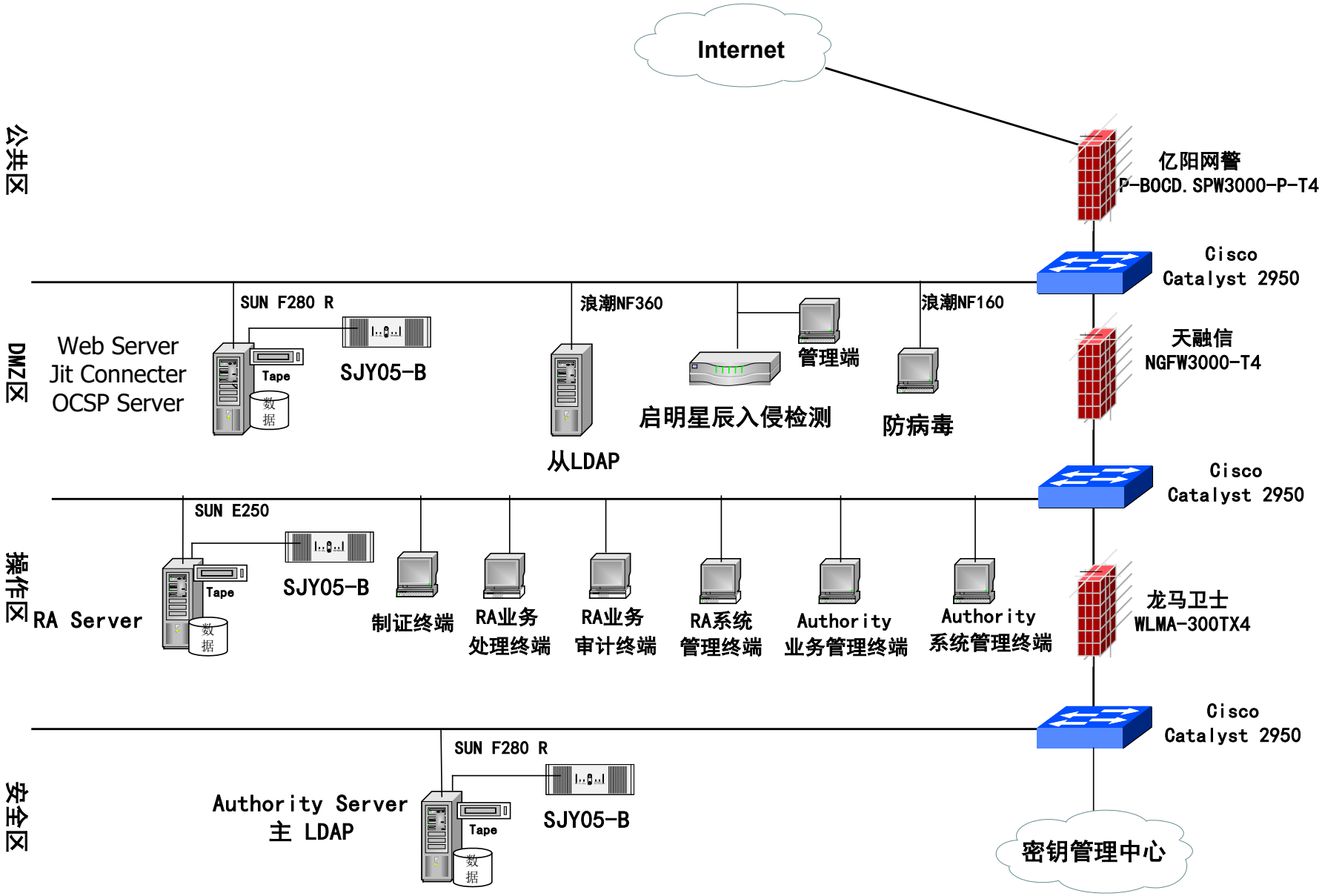
CA认证中心物理环境布置



CA中心系统布置


Internet
CA操作区
Authority
Master LDAP
Sun 280
SJY05-B
CA安全区
WLMA-300
Sun 250
SJY05-B
NGFW3000
SJY05-B
Web Connector
OCSP Server
SUN 280
P-BOCO SFW3000-F
Slave LDAP
NF360
TSA Server
NF160
NF160
DMZ区
配电室
注：
光纤
门禁
黑色区域为屏蔽机房
P-BOCO SFW3000-E
KMC
Server
SJY05-B
KMC
Sun B100
KMC
服务器区
KMC办公室
KMC管理区
监控室

CA系统逻辑布置


Internet
公共区
亿阳网警
P-BOCD.SPW3000-P-T4
Cisco
Catalyst 2950
DMZ区
SUN F280 R
Web Server
Jit Connecter
OCSP Server
Tape
数据
SJY05-B
浪潮NF360
从LDAP
管理端
启明星辰入侵检测
浪潮NF160
防病毒
天融信
NGFW3000-T4
Cisco
Catalyst 2950
操作区
SUN E250
RA Server
Tape
数据
SJY05-B
制证终端
RA业务
处理终端
RA业务
审计终端
RA系统
管理终端
Authority
业务管理终端
Authority
系统管理终端
龙马卫士
WLMA-300TX4
Cisco
Catalyst 2950
安全区
SUN F280 R
Authority Server
主 LDAP
Tape
数据
SJY05-B
密钥管理中心