Computer Science&Technology School of Shandong University

Security Protocols & Standards

--- PKI Principles and technology sd03031340

(Chapter 6 PKI Standards:X.509/PMI/PKIX)

Instructor: Hou Mengbo 侯孟波
Email: houmb AT sdu.edu.cn
Office: Information Security Research Office.
Rm: Office Building 421

PKI相关标准背景

- PKI标准有很多不同的标准制定机构,主要包括:
  - ITU-T :　ITU-T Recommendation X.509, *Information technology – Open Systems Interconnection – The Directory: Authentication framework*. (X.509V1(88) \ V2(93) \ V3(97) \ V4(00))
  - ISO/IEC: ISO/IEC 9594-8:　, *Information technology – Open Systems Interconnection – The Directory: Authentication framework*.(98 \ 01)
  - Internet Engineering Task Force (IETF).　PKIX

标准涉及的内容

- 公钥数字证书\证书注销列表的格式(标准内容与扩展)
- PKI消息管理协议
- 证书存储与发布操作协议
- 证书状态以及注销
- 时间戳\数据认证和验证服务
- 证书政策与实施

公钥数字证书、证书注销列表的格式

- 在前面章节已经对X.509标准中的数字证书和证书注销列表的逻辑字段构成、ASN1描述以及DER编码方法作了详细阐述.
- X509[V4]标准中主要涉及以下几方面:
  - 公钥数字证书认证框架 PUBLIC-KEY CERTIFICATE FRAMEWORK
  - **属性证书认证框架 *** ATTRIBUTE CERTIFICATE FRAMEWORK
  - 使用证书的目录认证框架 Directory use of public-key & attribute certificate frameworks

- 本节主要讲述X509标准中有关 **使用证书的目录认证框架。**

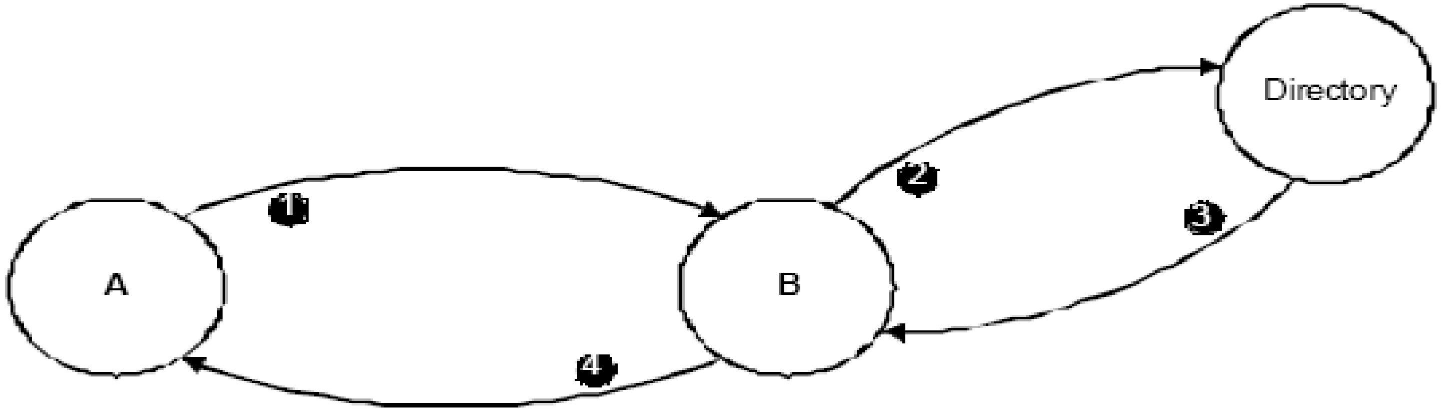
X509认证

- 认证方式包括两类：
  - 简单认证
    - 用于安全性要求比较低的环境
    - 基于用户名／口令方式
  - 强认证
    - 用于安全性要求比较高的环境
    - 使用数字证书

X.509 简单认证

- 通过用户名和口令（ID / password）实现
- 以有限的保护对本地系统的使用者进行认证以及认证后继授权进行管理
- 使用范围： 本地授权 / 本地用户/封闭环境
- 方法:
  - 用户名 / 口令明文认证传送
  - 使用单向函数保护的 认证传送
  - 二次单向函数保护的认证传送
  - 其他挑战应答方法

用户名／口令明文认证传送



The unprotected simple authentication procedure

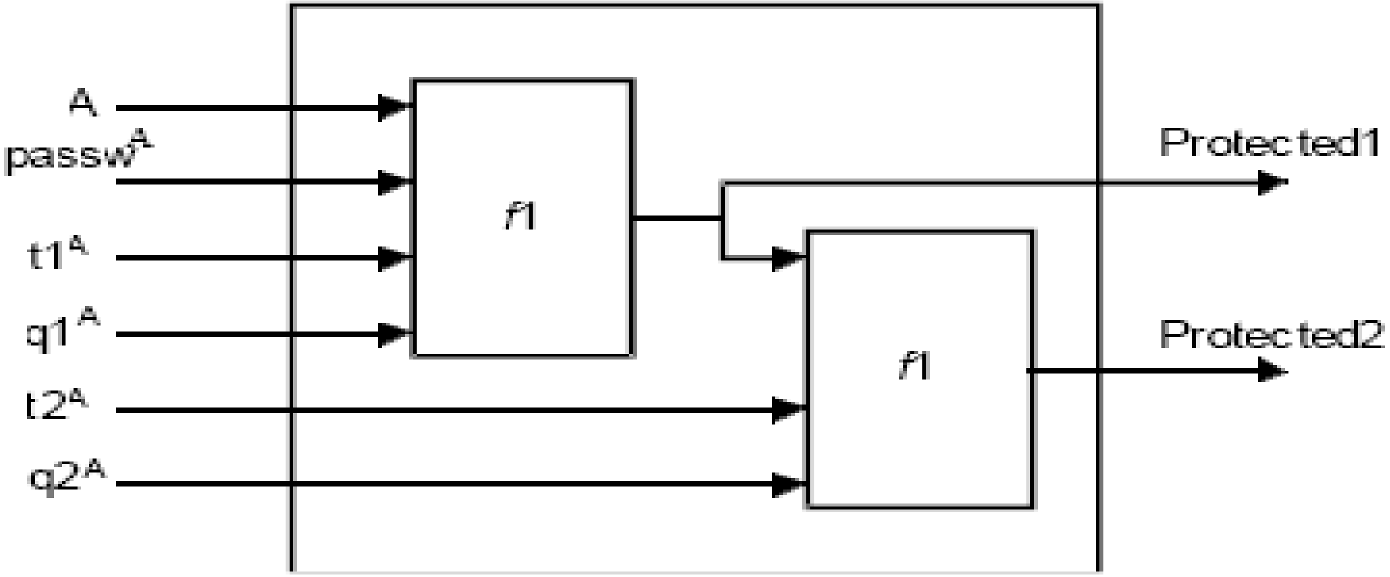
1) A将用户名和口令明文传送给验证者B;

2) B 将A的用户名和口令传给目录服务者D，D根据本地存储信息验证是否符合;

3) D将验证结果（Y/N）回送B;

4) B将验证结果（Y/N）回送A.

使用单向函数的保护



A	User's distinguished name
t^A	Timestamps
$passw^A$	Password of A
q^A	Random numbers, optionally with a counter included

Protected simple authentication

使用单向函数的保护

- 方法一：

  $\text{Protected}_1 = f_1\ (t1^A, q1^A, A, \text{passw}^A)$

  $\text{Authenticator}_1 = t1^A, q1^A, A, \mathbf{Protected_1}$

- 方法二：

  $\text{Protected}_2 = f_2\ (t2^A, q2^A, \mathbf{Protected_1})$

  $\text{Authenticator}_2 = t1^A, t2^A, q1^A, q2^A, A, \mathbf{Protected_2}$

注：Authenticator：认证符； t : 时间戳; q： 随机数
passw : 口令; A: 用户名; Protected:保护符

其他简单认证(非X509方法)

- 采用单向函数对口令进行HASH ,传送HASH认证.
  - 问题: 容易网上重放攻击
- 随机数挑战应答式
  - 服务器先向客户端发送一个随机数,客户端向服务器传送HASH(用户名+口令+随机挑战字)
  - 好处是避免重放攻击
  - 缺点是多了一次传输
- 基于时间标志的认证
  - 将服务器随机挑战字变成时间标志
  - 好处是避免一次通信
  - 缺点是时间很难同步
- 基于HASH和对称加密的挑战应答方法
  - 将用户名+口令作为对称密钥,加密服务器发来的挑战字

X509 强认证

- 开放式网络环境,认证要求更高
- 采用公钥密码技术
- 三种强认证方式
  - 单向认证
  - 双向认证
  - 三向认证

获取用户公钥

- 强认证方法使用公开钥密码方法，也就是使用一对密钥（KEY PAIR），一个是公开钥，一个是秘密钥。
- 认证还依赖于每个对象要有一个唯一的用户标识，通常该标识通过命名中心（NA，Naming Authority）获得，每个用户都会相信NA不会给不同用户分配重复的命名。
- 每个用户通过拥有它的秘密钥来鉴别。
- 在认证过程中，首要的是要从一个可信源安全的获取对方的公开钥。这个可信源一般是CA（Certificate Authority），
- CA通过公钥技术来认证用户的公钥,产生数字证书.
- 数字证书的原理决定了其不可伪造性,因而数字证书可以公开发布(如目录服务).

单向认证 （One-way Authentication）

- 包含一条从A到B的传输信息
- 过程：
  - 1.A产生随机数 r^A，时间戳t^A （当前时间和有效期）
  - 2.A向B发送：B ，A ｛ t^A， r^A， B｝ （签名）

    或者 B , data , A ｛ t^A， r^A， B，signData｝ 带签名

    或者B, data , B_P[encData] , A ｛ t^A， r^A， B，signData，B_P[encData]｝ 带加密数据
  - 3.B 获得A的公钥A^p （检查证书有效性）

    验证签名

    检查B确实是接收者

    检查时间戳t^A

    检查不是r^A重放攻击

双向认证（Two-way Authentication）

- 包含一条请求消息和一条响应消息（交互）
- 过程:
  - 1 - 3 同上
  - 4. B产生随机数 r^B
  - 5.B 发送A： A,B { t^B， r^B， A， r^A }

    或者： A,data,B { t^B， r^B， A， r^A ， signData }

  或者: A,data, A_P[encData] ,B { t^B， r^B， A， r^A ， signData ,A_P[encData] }
  - 6.A 验证签名

    检查A确实是接收者

    检查时间戳t^B

    检查不是r^B重放攻击

三向认证（ Three-way Authentication ）

- 包含一条请求消息、一条响应消息和一条再响应消息
- 过程：
  - 1- 6 同上
  - 7. A检查接收到的r^A 和发出去的r^A 是否一样的
  - 8. A 发送B：A{r^B,B}
  - 9. B 检查签名

    检查接收到的r^B 和发出去的r^B是否一样的

密钥和证书的管理

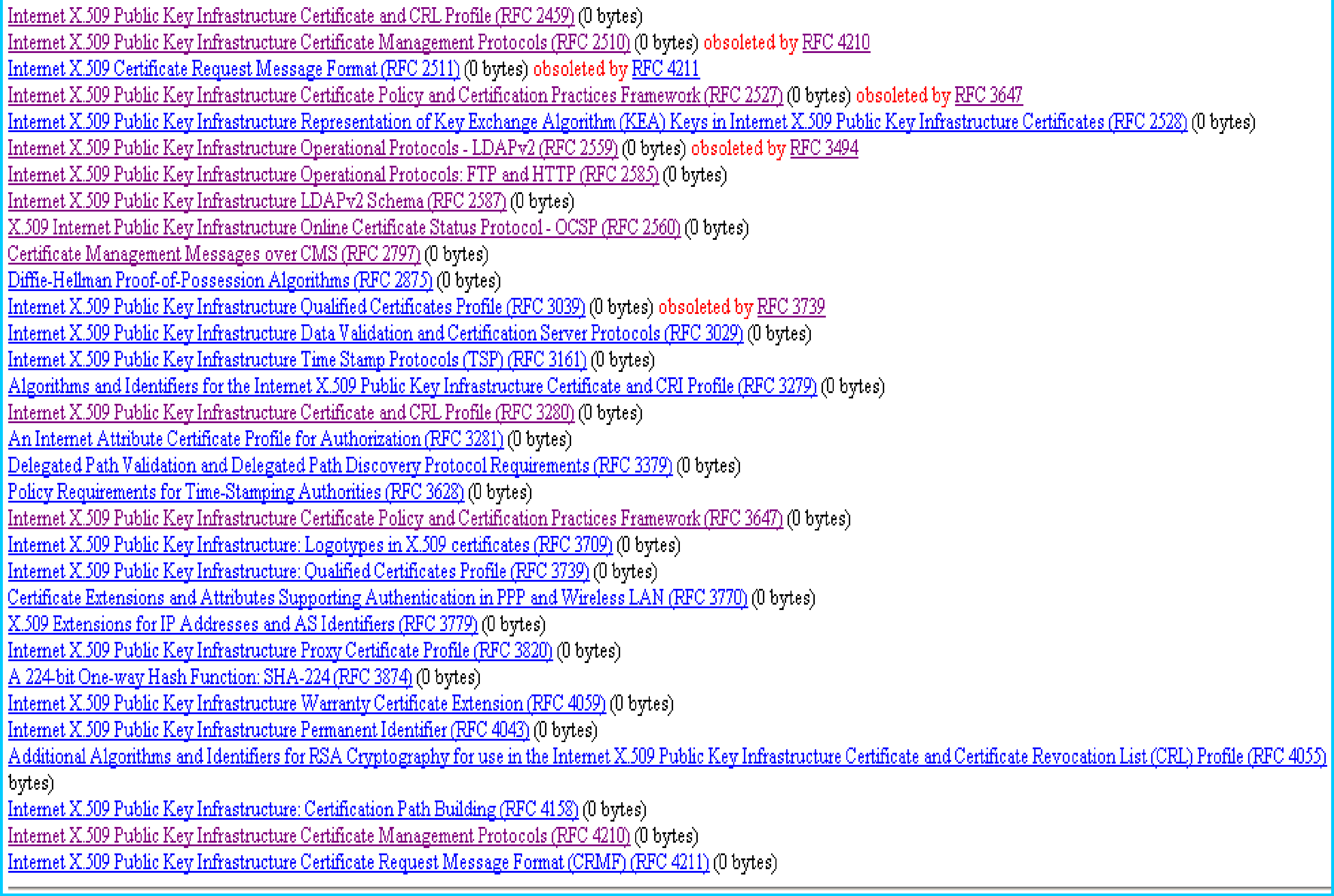
- 密钥的生成
  - 存储形式　　软件安全文件口令保护 / 智能卡 / 其他硬件
  - 产生形式　　自己产生 / 第三方产生 / CA产生

- 证书管理
  - CA保证给用户唯一的名字，保证不会给同名用户重复发证。
  - 保证发证过程中的消息不会被危及安全。

PMI (Privilege Management Infrastructure)

PKIX系列标准

- IETF工作组Security Area PKIX Work Group 成立于1995年，旨在开发基于X509标准的PKI。
- IETF标准系列（Standard Track）文档的制定需要三个阶段：
  - 建议标准 Proposed Standard
  - 标准草案Draft Standard
  - 标准 Standard
- 主要协议和标准涉及：
  - 数字证书\证书注销列表的格式(标准内容与扩展) RFC2459
  - PKI管理协议 **RFC2510（CMP, RFC4210） RFC2511（CRMF, RFC4211）** RFC2797 (CMC)
  - 证书政策与实施 RFC3647（RFC2527,CP&CPS）
  - 证书存储与发布操作协议 RFC2585(FTP/HTTP), /RFC2559-3494(LDAPv2) , RFC2587 (LDAPv2 Schema)
  - 证书状态以及注销 RFC2560(OCSP)
  - 时间戳\数据认证和验证服务 RFC3161(TSP)



Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459) (0 bytes)
Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510) (0 bytes) obsoleted by RFC 4210
Internet X.509 Certificate Request Message Format (RFC 2511) (0 bytes) obsoleted by RFC 4211
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527) (0 bytes) obsoleted by RFC 3647
Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates (RFC 2528) (0 bytes)
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 (RFC 2559) (0 bytes) obsoleted by RFC 3494
Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP (RFC 2585) (0 bytes)
Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2587) (0 bytes)
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560) (0 bytes)
Certificate Management Messages over CMS (RFC 2797) (0 bytes)
Diffie-Hellman Proof-of-Possession Algorithms (RFC 2875) (0 bytes)
Internet X.509 Public Key Infrastructure Qualified Certificates Profile (RFC 3039) (0 bytes) obsoleted by RFC 3739
Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (RFC 3029) (0 bytes)
Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP) (RFC 3161) (0 bytes)
Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile (RFC 3279) (0 bytes)
Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 3280) (0 bytes)
An Internet Attribute Certificate Profile for Authorization (RFC 3281) (0 bytes)
Delegated Path Validation and Delegated Path Discovery Protocol Requirements (RFC 3379) (0 bytes)
Policy Requirements for Time-Stamping Authorities (RFC 3628) (0 bytes)
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647) (0 bytes)
Internet X.509 Public Key Infrastructure: Logotypes in X.509 certificates (RFC 3709) (0 bytes)
Internet X.509 Public Key Infrastructure: Qualified Certificates Profile (RFC 3739) (0 bytes)
Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN (RFC 3770) (0 bytes)
X.509 Extensions for IP Addresses and AS Identifiers (RFC 3779) (0 bytes)
Internet X.509 Public Key Infrastructure Proxy Certificate Profile (RFC 3820) (0 bytes)
A 224-bit One-way Hash Function: SHA-224 (RFC 3874) (0 bytes)
Internet X.509 Public Key Infrastructure Warranty Certificate Extension (RFC 4059) (0 bytes)
Internet X.509 Public Key Infrastructure Permanent Identifier (RFC 4043) (0 bytes)
Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4055)
bytes)
Internet X.509 Public Key Infrastructure: Certification Path Building (RFC 4158) (0 bytes)
Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 4210) (0 bytes)
Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) (RFC 4211) (0 bytes)

RFCxxxx

数字证书/证书注销列表概貌－RFC2459

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile RFC 2459 （1999.01）
- 给出了X.509 v3 certificate and X.509 v2 CRL for use in the Internet.
- 是对X509标准中定义的证书和CRL的进一步明确和约束。

证书管理协议CMP－ RFC4210

- Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) RFC4210（2005.09）(取代 RFC2510) (1999.03)
- 协议消息定义了 X509证书的创建和管理
- 提供了PKI组件间在线交互,包含CA和客户端系统之间的交换以及两个CA之间的交叉认证.

有关涉及的实体在本标准中的含义

- Subject （主体）：被签发证书的实体，主要指证书中的subject 或 subjectAltName 域。其使用的工具和软件称为主体设备（subject equipment）。
- End entities（终端实体）：包括应用程序的使用人和应用本身。一般PKI的管理实体不包括在内。
- Personal Security Environment (PSE，个人安全环境)：指的是在终端实体本地的可信存储的信息。如文件或者防篡改令牌等。
- CA（认证中心）：这里（从终端实体角度看）不一定指的是第三方，也可以属于同一组织内部。CA所用的软件或者硬件工具，一般称为 CA设备。可以是在线或离线部件。

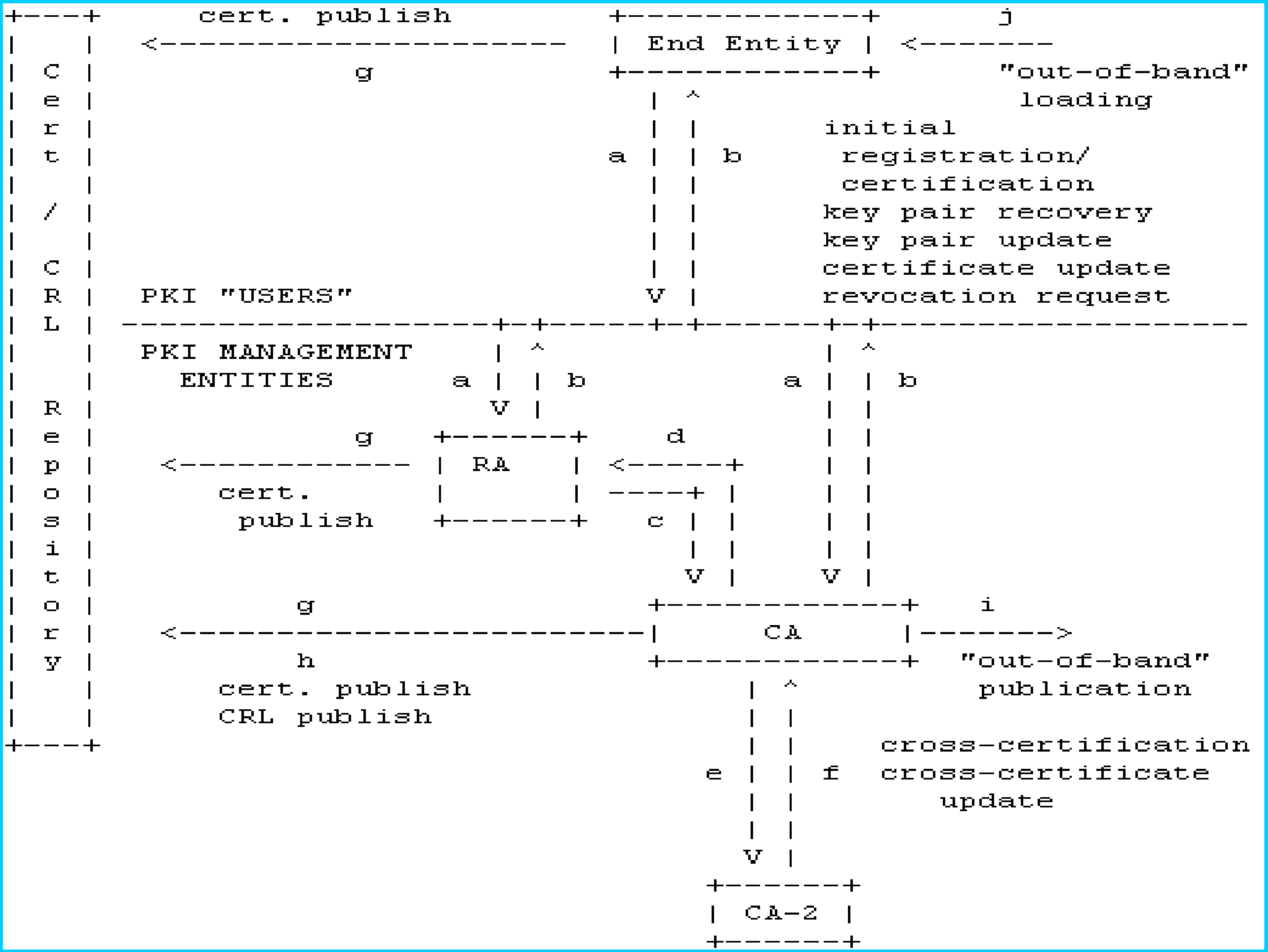
有关涉及的实体在本标准中的含义

- Root CA（根CA）：直接被终端实体所信任的CA（通常要获取根CA的公钥需要通过带外步骤），并不一定特指在信任层次的最顶端。
- Registration Authority（登记中心）：功能视情况而定，可能包含个人认证、令牌发放、注销报告、命名分配、密钥产生、密钥归档等，如果没有RA，其功能通常由CA完成。在RA存在时，也不一定要求终端实体一定要和RA直接通信，也可以和CA直接通信。

PKI管理需求

- 符合 ISO/IEC 9594-8/ITU-T X.509标准
- 密钥更新 不影响其他密钥对
- 尽量减少管理协议中机密性的要求
- 允许使用不同的工业标准加密算法，可以任意选择
- 允许密钥产生可以发生在终端实体、RA、CA
- 允许证书发布可以由终端实体、RA、CA
- 必须支持认证的终端实体的证书注销申请来产生CRL
- 必须支持多种传输机制（如mail, http, TCP/IP and ftp）
- 证书产生的最终决定在CA，CA可以根据自己的政策改变证书中的相关内容，和请求的内容不一定完全一致。
- 必须支持CA密钥的更新（终端实体能顺利过渡)
- 管理协议不会因为独立CA或CA / RA模式而改变
- 如果终端实体的请求信息里包含了公钥，终端实体就应准备证明它拥有相应的私钥

PKI管理操作



```
+---+     cert. publish        +------------+      j
|   |  <---------------------  | End Entity | <-------
| C |             g            +------------+      "out-of-band"
| e |                            | ^                loading
| r |                            | |      initial
| t |                          a | | b     registration/
|   |                            | |       certification
| / |                            | |      key pair recovery
|   |                            | |      key pair update
| C |                            | |      certificate update
| R |  PKI "USERS"               V |      revocation request
| L | -------------------+-+-----+-+------+-+-------------------
|   |  PKI MANAGEMENT    | ^              | ^
|   |    ENTITIES      a | | b          a | | b
| R |                    V |              | |
| e |             g   +------+    d       | |
| p |   <------------ | RA   | <-----+    | |
| o |      cert.      |      | ----+ |    | |
| s |       publish   +------+   c | |    | |
| i |                              | |    | |
| t |                              V |    V |
| o |          g                 +------------+   i
| r |   <------------------------|     CA     |-------->
| y |          h                 +------------+  "out-of-band"
|   |      cert. publish              | ^         publication
|   |      CRL publish                | |
+---+                                 | |    cross-certification
                                    e | | f  cross-certificate
                                      | |       update
                                      | |
                                      V |
                                    +-------+
                                    | CA-2  |
                                    +-------+
```

PKI管理操作的协议消息分类

- CA建立

  当建立一个新CA的时候，需要确定的步骤（如产生初始CRL，发布公钥等）
- 终端实体初始化

  输入根CA公钥、PKI管理实体支持的请求信息等
- 认证

  包括所有新证书创建需要的操作
  - 初始登记和认证　注册、审查、签证、下载、发布
  - 密钥对更新 （周期性，新证书签发）
  - 证书更新（周期性，即使终端实体信息未变）
  - CA密钥更新
  - 交叉认证请求
  - 交叉认证更新

PKI管理操作的协议消息分类

- 证书 / CRL发现操作
  证书发布 / CRL发布
- 恢复操作　　密钥恢复
- 注销操作　　注销请求
- 个人安全环境操作

管理协议的数据结构

- 包括PKI消息的一般结构、PKI消息头、PKI消息体、PKI消息保护以及其他一些公共数据结构和操作规定数据结构。

```
PKIMessage ::= SEQUENCE {
    header          PKIHeader,
    body            PKIBody,
    protection   [0] PKIProtection OPTIONAL,
    extraCerts   [1] SEQUENCE SIZE (1..MAX) OF CMPCertificate
                 OPTIONAL
}
PKIMessages ::= SEQUENCE SIZE (1..MAX) OF PKIMessage
```

PKI消息头

```
PKIHeader ::= SEQUENCE {
     pvno              INTEGER     { cmp1999(1), cmp2000(2) },
     sender            GeneralName,
     recipient         GeneralName,
     messageTime     [0] GeneralizedTime        OPTIONAL,
     protectionAlg   [1] AlgorithmIdentifier    OPTIONAL,
     senderKID       [2] KeyIdentifier          OPTIONAL,
     recipKID        [3] KeyIdentifier          OPTIONAL,
     transactionID   [4] OCTET STRING           OPTIONAL,
     senderNonce     [5] OCTET STRING           OPTIONAL,
     recipNonce      [6] OCTET STRING           OPTIONAL,
     freeText        [7] PKIFreeText            OPTIONAL,
     generalInfo     [8] SEQUENCE SIZE (1..MAX) OF
                  InfoTypeAndValue    OPTIONAL
  }
  PKIFreeText ::= SEQUENCE SIZE (1..MAX) OF UTF8String
```

PKI消息体（1）

```
PKIBody ::= CHOICE {
      ir        [0]  CertReqMessages,                     --Initialization Req
      ip        [1]  CertRepMessage,                      --Initialization Resp
      cr        [2]  CertReqMessages,                     --Certification Req
      cp        [3]  CertRepMessage,                      --Certification Resp
      p10cr     [4]  CertificationRequest,              --PKCS #10 Cert.  Req.
      popdecc   [5]  POPODecKeyChallContent            --proof-of-possession
                                                                 Challenge
      popdecr   [6]  POPODecKeyRespContent,                  --pop Response
      kur       [7]  CertReqMessages,                    --Key Update Request
      kup       [8]  CertRepMessage,                     --Key Update Response
      krr       [9]  CertReqMessages,                    --Key Recovery Req
```

PKI消息体（2）

```
krp      [10] KeyRecRepContent,      --Key Recovery Resp
rr       [11] RevReqContent,         --Revocation Request
rp       [12] RevRepContent,         --Revocation Response
ccr      [13] CertReqMessages,       --Cross-Cert.  Request
ccp      [14] CertRepMessage,        --Cross-Cert.  Resp
ckuann   [15] CAKeyUpdAnnContent,    --CA Key Update Ann.
cann     [16] CertAnnContent,        --Certificate Ann.
rann     [17] RevAnnContent,         --Revocation Ann.
crlann   [18] CRLAnnContent,         --CRL Announcement
pkiconf  [19] PKIConfirmContent,     --Confirmation
nested   [20] NestedMessageContent,  --Nested Message
genm     [21] GenMsgContent,         --General Message
genp     [22] GenRepContent,         --General Response
error    [23] ErrorMsgContent,       --Error Message
certConf [24] CertConfirmContent,    --Certificate confirm
pollReq  [25] PollReqContent,        --Polling request
pollRep  [26] PollRepContent         --Polling response
}
```

PKI管理消息的传输方式

- 基于文件的方式
- 基于TCP的方式
- 基于EMAIL的方式
- 基于HTTP的方式

证书请求消息格式CRMF－ RFC4211

- Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) RFC4211 （2005.09）(取代RFC2511) (1999.03)
- 本协议描述了X.509证书请求的消息格式语法和语义
- 所谓的证书请求是指用于向CA提交的（可能经过RA）用于产生证书的请求消息，一般是包括申请认证的终端实体的公钥和终端实体的注册身份信息。

证书请求消息CertReqMessages

```
CertReqMessages ::= SEQUENCE SIZE (1..MAX) OF CertReqMsg
 CertReqMsg ::= SEQUENCE {
          certReq   CertRequest,
          popo      ProofOfPossession  OPTIONAL,     -- content depends upon key type
          regInfo   SEQUENCE SIZE(1..MAX) of AttributeTypeAndValue   OPTIONAL
 }
```

a) A CertRequest object is constructed.

b) If required, a proof-of-possession value is calculated.

c) Additional registration information

d) The CertReqMessage is securely communicated to a CA.

CertRequest / CertTemplate

```
CertRequest ::= SEQUENCE {
    certReqId     INTEGER,        -- ID for matching request and reply
    certTemplate  CertTemplate, --Selected fields of cert to be issued
    controls      Controls OPTIONAL } -- Attributes affecting issuance

CertTemplate ::= SEQUENCE {
    version      [0] Version              OPTIONAL,
    serialNumber [1] INTEGER              OPTIONAL,
    signingAlg   [2] AlgorithmIdentifier  OPTIONAL,
    issuer       [3] Name                 OPTIONAL,
    validity     [4] OptionalValidity     OPTIONAL,
    subject      [5] Name                 OPTIONAL,
    publicKey    [6] SubjectPublicKeyInfo OPTIONAL,
    issuerUID    [7] UniqueIdentifier     OPTIONAL,
    subjectUID   [8] UniqueIdentifier     OPTIONAL,
    extensions   [9] Extensions           OPTIONAL }
```

Controls

Controls ::= SEQUENCE SIZE(1..MAX) OF AttributeTypeAndValue

The following controls are defined by this document:

regToken	Registration Token Control
authenticator	
pkiPublicationInfo	Publication Information Control
pkiArchiveOptions	Archive Options Control
oldCertID	OldCert ID Control
protocolEncrKey	Protocol Encryption Key Control

Certificate Management Messages over CMS(CMC)

- Certificate Management Messages over CMS RFC 2797(2000.04)
- 该协议用于尽可能支持已有的实现,包括PKCS#10、PKCS#7和CRMF
- 使用一个简单的请求和响应完成一次往返的事务操作.
- 与CMP不同,CMC不创建操作的特殊案例.

证书政策与认证实施－ RFC3647

- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework RFC3647（2003.11）取代RFC2527
- 该文档描述了一个框架，来帮助撰写证书政策CP和认证实施声明CPS，这两方面的内容都是服务于PKI参与者（包括认证中心、政策中心以及依赖于证书的团体）的。
- CA要正常运作，必须确定其运作方式，CP和CPS是其中重要的内容。

证书政策CP

- Certificate Policy (CP)： a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements.
- A CP may be used by a relying party to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.
- 例如： 一份特定的证书限定在B2B电子交易中商品的价格范围等。

认证实施声明CPS

- A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a certification practice statement (CPS) published by or referenced by the CA.
- CPS： A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
- In general, CPSs also describe practices relating to all certificate lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying), and CPSs provide details concerning other business, legal, and technical matters.

证书政策CP

- 当CA签发了一份终端实体的证书后，证书用户需要判断其依赖的CA的陈述，也就是如何使用证书是恰当的。
- 描述类型：
  - 对特定用户的适用性
  - 对满足一般安全需求的应用类型的适用性
- 举例： 如国际航空运输联盟IATA至少可以制定两类证书政策
  - 普通CP：用于保护IATA内部个人的一般信息保护（如EMAIL），则可以限定证书密钥的存储方式可以为软件系统，可用于B/S和一般应用，所以证书签发范围可以遍及IATA的任何雇员。
  - 商业级CP：用于保护IATA商业交易和合同交换，则可以限定证书密钥的存储方式为硬件令牌，

证书政策在X509证书中的体现

- X509证书中的扩展域可以描述证书政策项
  - Certificate Policies extension;
  - Policy Mappings extension;
  - Policy Constraints extension.

认证实施声明CPS

- A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate 。
- 有时候CA也不一定提供一份完整详尽的描述，也可以通过其他形式说明，如subscriber agreement, relying party agreement, or agreement combining subscriber and relying party terms 这些也可视同CPS。
- 由于CPS可能涉及系统敏感信息，所以CA不一定要把完全的CPS公布，也可发布一个CPS摘要（CPS Summary），其中主要描述和用户有关的内容，如各方责任、证书周期等。

CP和CPS的关系

- CP描述了PKI各方面对用户强加的需求和标准 ，也就是目的在于说明参与者必须做什么.
- CPS描述了CA和参与者在既定环境下如何在过程和控制中实现对CP的要求达到满足，也就是其目的在于揭示参与者如何执行其功能和实现控制。
- 一个CP可以应用于多个CA，多个组织。
- 一个CPS只适用于一个CA，一个组织。
- 一个CA应支持多个CP，多个CA可能支持同一个CP。
- CPS的描述比CP更加细致。

CP和CPS的关系

(a) A PKI uses a CP to establish requirements that state what participants within it must do. A single CA or organization can use a CPS to disclose how it meets the requirements of a CP or how it implements its practices and controls.

(b) A CP facilitates interoperation through cross-certification, unilateral certification, or other means. Therefore, it is intended to cover multiple CAs. By contrast, a CPS is a statement of a single CA or organization. Its purpose is not to facilitate interoperation (since doing so is the function of a CP).

(c) A CPS is generally more detailed than a CP and specifies how the CA meets the requirements specified in the one or more CPs under which it issues certificates.

CP&CPS描述框架

1. Introduction
2. Publication and Repository
3. Identification and Authentication
4. Certificate Life-Cycle Operational Requirements
5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. Certificate, CRL, and OCSP Profile
8. Compliance audit
9. Other Business and Legal Matters

CPS撰写模板

1. INTRODUCTION

1.1 Overview

1.2 Document name and identification

1.3 PKI participants

- 1.3.1 Certification authorities
- 1.3.2 Registration authorities
- 1.3.3 Subscribers
- 1.3.4 Relying parties
- 1.3.5 Other participants

1.4 Certificate usage

- 1.4.1. Appropriate certificate uses
- 1.4.2 Prohibited certificate uses

1.5 Policy administration

- 1.5.1 Organization administering the document
- 1.5.2 Contact person
- 1.5.3 Person determining CPS suitability for the policy
- 1.5.4 CPS approval procedures

1.6 Definitions and acronyms

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

2.2 Publication of certification information

2.3 Time or frequency of publication

2.4 Access controls on repositories

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Anonymity or pseudonymity of subscribers

3.1.4 Rules for interpreting various name forms

3.1.5 Uniqueness of names

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.2 Authentication of organization identity

3.2.3 Authentication of individual identity

3.2.4 Non-verified subscriber information

3.2.5 Validation of authority

3.2.6 Criteria for interoperation

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

3.3.2 Identification and authentication for re-key after revocation

3.4 Identification and authentication for revocation request

4.CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

- 4.1.1 Who can submit a certificate application
- 4.1.2 Enrollment process and responsibilities

4.2 Certificate application processing

- 4.2.1 Performing identification and authentication functions
- 4.2.2 Approval or rejection of certificate applications
- 4.2.3 Time to process certificate applications

4.3 Certificate issuance

- 4.3.1 CA actions during certificate issuance
- 4.3.2 Notification to subscriber by the CA of issuance of certificate

4.4 Certificate acceptance

- 4.4.1 Conduct constituting certificate acceptance
- 4.4.2 Publication of the certificate by the CA
- 4.4.3 Notification of certificate issuance by the CA to other entities

4.5 Key pair and certificate usage

- 4.5.1 Subscriber private key and certificate usage
- 4.5.2 Relying party public key and certificate usage

4.6 Certificate renewal

- 4.6.1 Circumstance for certificate renewal
- 4.6.2 Who may request renewal
- 4.6.3 Processing certificate renewal requests
- 4.6.4 Notification of new certificate issuance to subscriber
- 4.6.5 Conduct constituting acceptance of a renewal certificate
- 4.6.6 Publication of the renewal certificate by the CA
- 4.6.7 Notification of certificate issuance by the CA to other entities

4.7 Certificate re-key

- 4.7.1 Circumstance for certificate re-key
- 4.7.2 Who may request certification of a new public key
- 4.7.3 Processing certificate re-keying requests
- 4.7.4 Notification of new certificate issuance to subscriber
- 4.7.5 Conduct constituting acceptance of a re-keyed certificate
- 4.7.6 Publication of the re-keyed certificate by the CA
- 4.7.7 Notification of certificate issuance by the CA to other entities

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

4.8.2 Who may request certificate modification

4.8.3 Processing certificate modification requests

4.8.4 Notification of new certificate issuance to subscriber

4.8.5 Conduct constituting acceptance of modified certificate

4.8.6 Publication of the modified certificate by the CA

4.8.7 Notification of certificate issuance by the CA to other entities

4.9 Certificate revocation and suspension

- 4.9.1 Circumstances for revocation
- 4.9.2 Who can request revocation
- 4.9.3 Procedure for revocation request
- 4.9.4 Revocation request grace period
- 4.9.5 Time within which CA must process the revocation request
- 4.9.6 Revocation checking requirement for relying parties
- 4.9.7 CRL issuance frequency (if applicable)
- 4.9.8 Maximum latency for CRLs (if applicable)
- 4.9.9 On-line revocation/status checking availability
- 4.9.10 On-line revocation checking requirements
- 4.9.11 Other forms of revocation advertisements available
- 4.9.12 Special requirements re key compromise
- 4.9.13 Circumstances for suspension
- 4.9.14 Who can request suspension
- 4.9.15 Procedure for suspension request
- 4.9.16 Limits on suspension period

4.10 Certificate status services

- 4.10.1 Operational characteristics
- 4.10.2 Service availability
- 4.10.3 Optional features

4.11 End of subscription

4.12 Key escrow and recovery

- 4.12.1 Key escrow and recovery policy and practices
- 4.12.2 Session key encapsulation and recovery policy and practices

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

- 5.1.1 Site location and construction
- 5.1.2 Physical access
- 5.1.3 Power and air conditioning
- 5.1.4 Water exposures
- 5.1.5 Fire prevention and protection
- 5.1.6 Media storage
- 5.1.7 Waste disposal
- 5.1.8 Off-site backup

5.2 Procedural controls

- 5.2.1 Trusted roles
- 5.2.2 Number of persons required per task
- 5.2.3 Identification and authentication for each role
- 5.2.4 Roles requiring separation of duties

5.3 Personnel controls

- 5.3.1 Qualifications, experience, and clearance requirements
- 5.3.2 Background check procedures
- 5.3.3 Training requirements
- 5.3.4 Retraining frequency and requirements
- 5.3.5 Job rotation frequency and sequence
- 5.3.6 Sanctions for unauthorized actions
- 5.3.7 Independent contractor requirements
- 5.3.8 Documentation supplied to personnel

5.4 Audit logging procedures

- 5.4.1 Types of events recorded
- 5.4.2 Frequency of processing log
- 5.4.3 Retention period for audit log
- 5.4.4 Protection of audit log
- 5.4.5 Audit log backup procedures
- 5.4.6 Audit collection system (internal vs. external)
- 5.4.7 Notification to event-causing subject
- 5.4.8 Vulnerability assessments

- 5.5 Records archival
  - 5.5.1 Types of records archived
  - 5.5.2 Retention period for archive
  - 5.5.3 Protection of archive
  - 5.5.4 Archive backup procedures
  - 5.5.5 Requirements for time-stamping of records
  - 5.5.6 Archive collection system (internal or external)
  - 5.5.7 Procedures to obtain and verify archive information
- 5.6 Key changeover
- 5.7 Compromise and disaster recovery
  - 5.7.1 Incident and compromise handling procedures
  - 5.7.2 Computing resources, software, and/or data are corrupted
  - 5.7.3 Entity private key compromise procedures
  - 5.7.4 Business continuity capabilities after a disaster
- 5.8 CA or RA termination

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

- 6.1.1 Key pair generation
- 6.1.2 Private key delivery to subscriber
- 6.1.3 Public key delivery to certificate issuer
- 6.1.4 CA public key delivery to relying parties
- 6.1.5 Key sizes
- 6.1.6 Public key parameters generation and quality checking
- 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

6.2.2 Private key (n out of m) multi-person control

6.2.3 Private key escrow

6.2.4 Private key backup

6.2.5 Private key archival

6.2.6 Private key transfer into or from a cryptographic module

6.2.7 Private key storage on cryptographic module

6.2.8 Method of activating private key

6.2.9 Method of deactivating private key

6.2.10 Method of destroying private key

6.2.11 Cryptographic Module Rating

6.3 Other aspects of key pair management

6.3.1 Public key archival

6.3.2 Certificate operational periods and key pair usage periods

- 6.4 Activation data
  - 6.4.1 Activation data generation and installation
  - 6.4.2 Activation data protection
  - 6.4.3 Other aspects of activation data
- 6.5 Computer security controls
  - 6.5.1 Specific computer security technical requirements
  - 6.5.2 Computer security rating
- 6.6 Life cycle technical controls
  - 6.6.1 System development controls
  - 6.6.2 Security management controls
  - 6.6.3 Life cycle security controls
- 6.7 Network security controls
- 6.8 Time-stamping

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

- 7.1.1 Version number(s)
- 7.1.2 Certificate extensions
- 7.1.3 Algorithm object identifiers
- 7.1.4 Name forms
- 7.1.5 Name constraints
- 7.1.6 Certificate policy object identifier
- 7.1.7 Usage of Policy Constraints extension
- 7.1.8 Policy qualifiers syntax and semantics
- 7.1.9 Processing semantics for the critical Certificate Policies extension

7.2 CRL profile

- 7.2.1 Version number(s)
- 7.2.2 CRL and CRL entry extensions

7.3 OCSP profile

- 7.3.1 Version number(s)
- 7.3.2 OCSP extensions

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

8.2 Identity/qualifications of assessor

8.3 Assessor's relationship to assessed entity

8.4 Topics covered by assessment

8.5 Actions taken as a result of deficiency

8.6 Communication of results

9. OTHER BUSINESS AND LEGAL MATTERS

- 9.1 Fees
  - 9.1.1 Certificate issuance or renewal fees
  - 9.1.2 Certificate access fees
  - 9.1.3 Revocation or status information access fees
  - 9.1.4 Fees for other services
  - 9.1.5 Refund policy
- 9.2 Financial responsibility
  - 9.2.1 Insurance coverage
  - 9.2.2 Other assets
  - 9.2.3 Insurance or warranty coverage for end-entities
- 9.3 Confidentiality of business information
  - 9.3.1 Scope of confidential information
  - 9.3.2 Information not within the scope of confidential information
  - 9.3.3 Responsibility to protect confidential information

- 9.4 Privacy of personal information
  - 9.4.1 Privacy plan
  - 9.4.2 Information treated as private
  - 9.4.3 Information not deemed private
  - 9.4.4 Responsibility to protect private information
  - 9.4.5 Notice and consent to use private information
  - 9.4.6 Disclosure pursuant to judicial or administrative process
  - 9.4.7 Other information disclosure circumstances
- 9.5 Intellectual property rights
- 9.6 Representations and warranties
  - 9.6.1 CA representations and warranties
  - 9.6.2 RA representations and warranties
  - 9.6.3 Subscriber representations and warranties
  - 9.6.4 Relying party representations and warranties
  - 9.6.5 Representations and warranties of other participants
- 9.7 Disclaimers of warranties
- 9.8 Limitations of liability
- 9.9 Indemnities

- 9.10 Term and termination
  - 9.10.1 Term
  - 9.10.2 Termination
  - 9.10.3 Effect of termination and survival
- 9.11 Individual notices and communications with participants
- 9.12 Amendments
  - 9.12.1 Procedure for amendment
  - 9.12.2 Notification mechanism and period
  - 9.12.3 Circumstances under which OID must be changed
- 9.13 Dispute resolution provisions
- 9.14 Governing law
- 9.15 Compliance with applicable law
- 9.16 Miscellaneous provisions
  - 9.16.1 Entire agreement
  - 9.16.2 Assignment
  - 9.16.3 Severability
  - 9.16.4 Enforcement (attorneys' fees and waiver of rights)
  - 9.16.5 Force Majeure
- 9.17 Other provisions

Operational Protocols – LDAPv3(RFC2251)

- Lightweight Directory Access Protocol, version 3 is an Internet Protocol used to access X.500-based directory services.
- 最新RFC3494给出建议，抛弃LDAPV2,使用LDAPV3，以提高操作安全性。
- 本节将讲述LDAPV3 协议内容以及与证书有关的Schema。

目录服务

- 目录服务的种类：
  - 电话号码本：基于印刷形式的目录服务
  - 114信息服务：基于电话查询的目录服务
  - 网上黄页：基于Internet的目录服务
- 集中了大量为人们所感兴趣的数据,提供了方便，快捷，高效的访问机制，使得人们可以有效的利用这些数据
- 目录服务＝ 数据 ＋访问机制

基于网络的目录服务

- X.500目录服务标准：1988年，DDITT制定了第一版X.500标准，全面描述了这一模型。1993年，ITU-T对第一版作了显著的修改和补充，产生了第二版建议（1997年作了进一步修改）。ISO接受了这个建议，把它作为ISO/IEC9594标准。如同ISO的网络七层参考模型一样，它是所有目录服务的标准。
- 协议内容非常庞大，要求很高，实现起来非常困难.
- 提供大量繁杂的操作：对于开发者和使用者来说都是负担.
- 致命问题：不支持TCP/IP版本的目录访问协议，而是使用专有的DAP目录访问协议访问目录

基于网络的目录服务

- 现有的主要目录访问协议的框架都是建立在X.500之上的
- LDAP目录服务可以说就是X.500的简化版本
- Microsoft的Active Directory目录服务的主体框架也是X.500的

轻量级目录服务LDAP

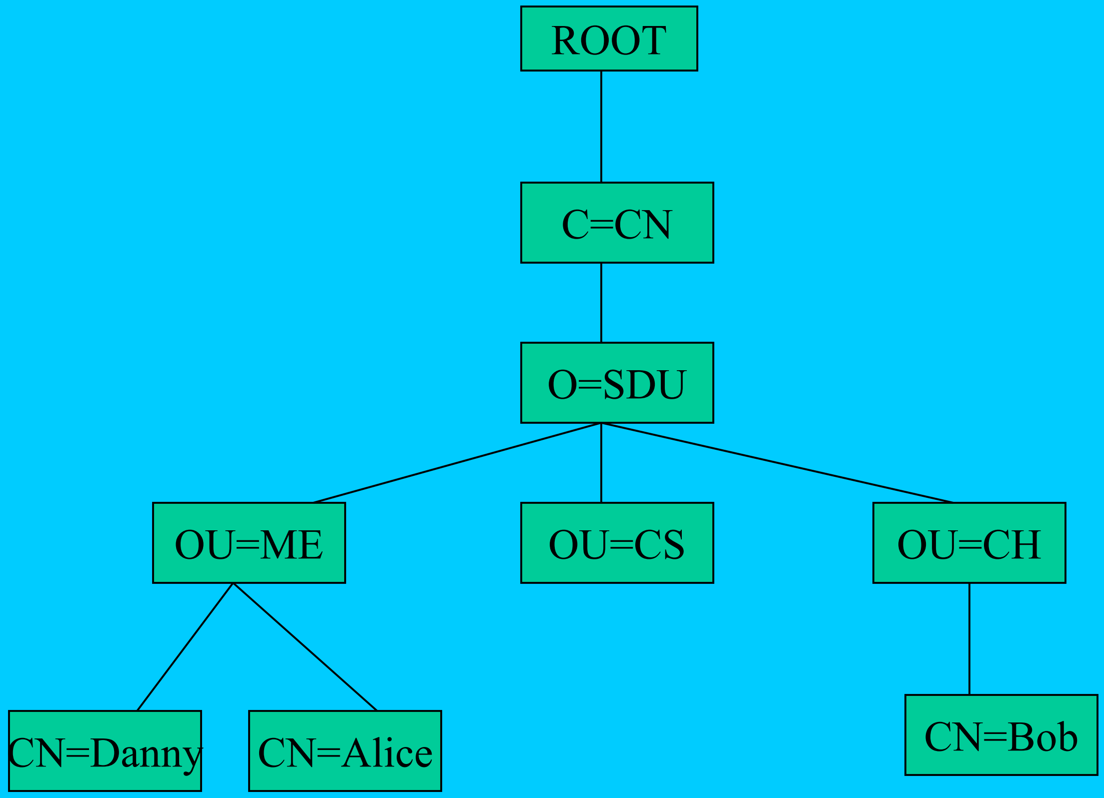
- 由于X.500系列协议存在的诸多问题，IEIF下的ASID制定了Light Weight Directory Access Protocol，也就是LDAP
- LDAP的设计目标就是用较小的代价在Internet上实现X.500的大多数功能
- LDAP用相当于X.500 10%的代价实现了它90%的功能
- 到目前为止，LDAP协议已经发展到了第3版本
- 描述LDAP v3的RFC主要有：

RFC2251-2256,2829-2831

LDAP使用的数据模型

- LDAP使用的数据模型有点类似于DNS：都是一个树形结构
- 每个资源都是这个树中的一个叶子结点
- Directory Information Tree(DIT)及其相关概念构成了LDAP使用的数据模型
- 树中的每个节点都是一个Entry(条目，入口)
- 某个条目本身有一个名称，称为Relative Distinguished Name(相关辨识名)。它被用来区别同级的其它条目
- 从某个入口到根的直接下级的RDN序列构成了该入口的Distinguished Name(辨识名)，用来在整个树中标识这个节点

一棵典型的目录信息树



LDAP的功能模型

- LDAP的功能模型中指定其支持如下操作：

  search add delete modify modify DN bind unbind 等操作
- 在LDAP v3中，增加了扩展操作的机制，允许定义协议中没有的操作，如数字签名等

常见的LDAP系统

- **OpenLDAP** -- Are you a DIYer? This one is free! Since it's source code open, you can compile this for most computer platforms
- **Messaging Direct's M-Vault LDAP server** -- For Solaris, NT, IRIX, AIX, and Linux
- **iPlanet / Netscape Directory Server** -- For Solaris, NT, HP-UX, AIX, IRIX, and Linux
- **Novell NDS eDirectory**
- **IBM Directory**
- **Microsoft Active Directory**
- **南开创元 iTec - LDAP**

OpenLDAP系统简介

- OpenLDAP系统是一个源码开放的LDAP服务器软件
- 它是目前能得到的较好的LDAP服务器软件之一
- OpenLDAP主要被应用在类Unix平台上
- 目前最高的版本是2.3.11
- 从版本2.0开始就支持LDAP v3

可用的LDAP地址服务资源

- Bigfoot (ldap.bigfoot.com)
- InfoSpace (ldap.infospace.com)
- Verisign (directory.verisign.com)
- WhoWhere (ldap.whowhere.com)
- Yahoo! People Search (ldap.yahoo.com)
- 可以利用支持LDAP的客户端使用这些服务

LDAP在PKI中的应用

- 公钥就是要让所有需要的人知道，所以要把它发布出去发布出去之后要能使用户方便，高效地得到它,所以关键在于发布的手段.选择目录服务是不错的选择.
- 为方便、高效、透明地使用PKI提供的公钥基础设施创造了条件,比如：得到用户的证书(包含用户的公钥)、使用证书注销列表CRL、方便CA之间进行交叉认证.

PKI中使用LDAP的优点

- 可以在许多应用中提供透明性要求，方便用户使用
- 不依赖于底层数据库系统，方便实现大规模分布式要求

Operational Protocols- FTP and HTTP (RFC2585)

- 该协议描述了用FTP和HTTP协议从证书和证书注销列表存储仓库（Repository）获取证书和证书注销列表的机制。
- 在证书和CRL的扩展项中， 使用URI 形式的 GeneralName 用来描述获取签发的证书和的位置.
- Internet 用户可以把URI reference发布 到一个文件里，里面包含了他们的证书位置.
  - ftp://ftp.netcom.com/sp/spyrus/housley.cer
  - http://www.netcom.com/sp/spyrus/housley.cer

Online Certificate Status Protocol –OCSP (RFC2560)

- 解决CRL周期性发布机制存在的问题。 - 及时性

  CRL可能存在安全风险?
- 实时获取证书状态
- 协议的基本过程描述

  (1) 请求　协议版本/服务请求/目标证书标识/扩展项

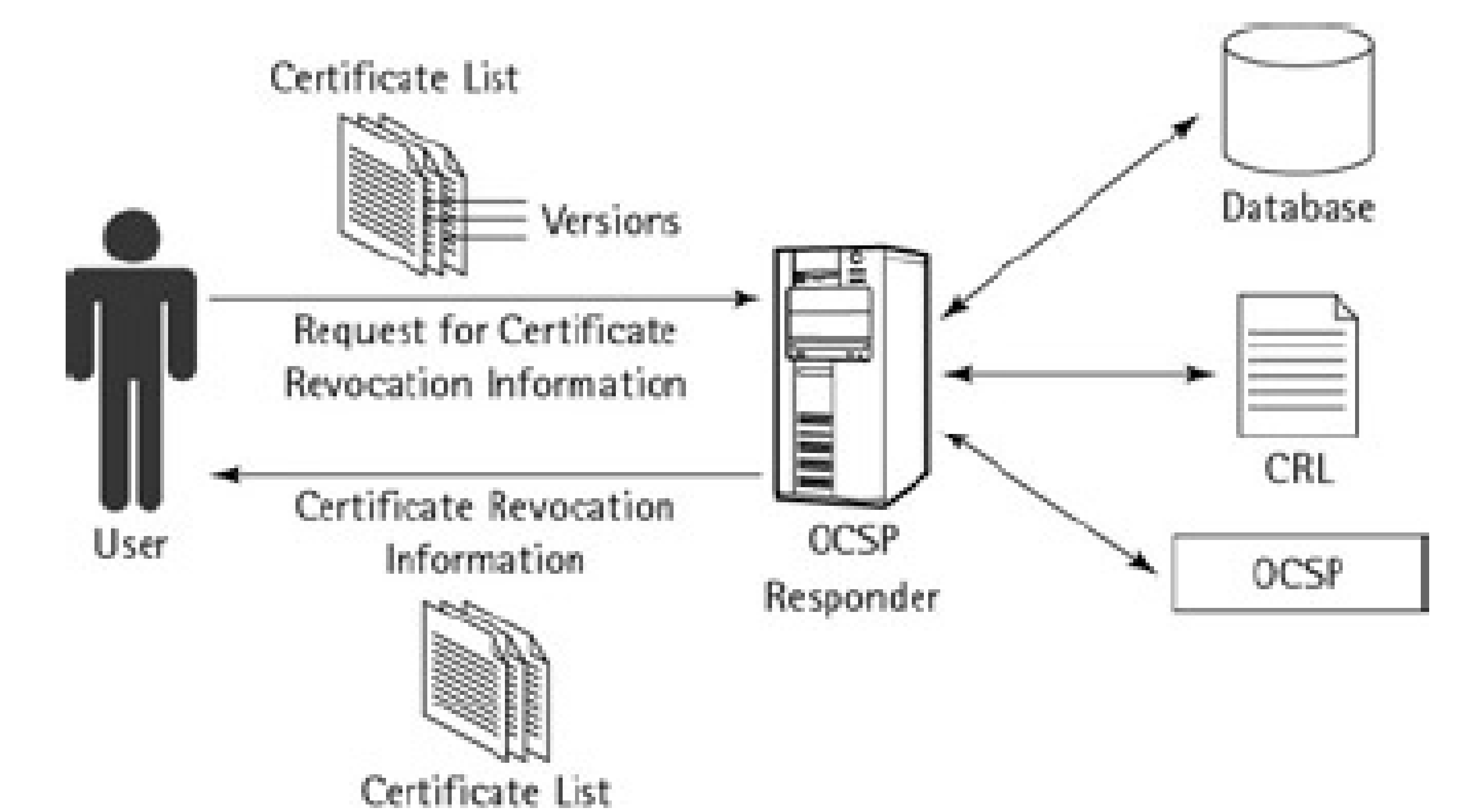
  (2) 回复　版本/响应器名称/证书状态回复/扩展/签名算法标识/签名

证书状态回复:　证书标识/证书状态值/回复有效期/扩展

证书状态值:　良好/已撤销/未知

例外情况:请求非法/内部错误/稍后再试/需要签名/未授权

OCSP


Certificate List
Versions
User
Request for Certificate Revocation Information
Certificate Revocation Information
Certificate List
OCSP Responder
Database
CRL
OCSP

OCSP请求消息ASN1描述(1)

```
OCSPRequest ::= SEQUENCE {
      tbsRequest                  TBSRequest,
      optionalSignature           [0] EXPLICIT Signature OPTIONAL }
TBSRequest ::= SEQUENCE {
      version                [0] EXPLICIT Version DEFAULT v1,
      requestorName     [1] EXPLICIT GeneralName OPTIONAL,
      requestList           SEQUENCE OF Request,
      requestExtensions [2] EXPLICIT Extensions OPTIONAL }
Signature ::= SEQUENCE {
      signatureAlgorithm      AlgorithmIdentifier,
      signature                      BIT STRING,
      certs                          [0] EXPLICIT SEQUENCE OF Certificate
    OPTIONAL}
```

OCSP请求消息ASN1描述(2)

```
Version ::= INTEGER { v1(0) }
Request ::= SEQUENCE {
      reqCert                                  CertID,
      singleRequestExtensions     [0] EXPLICIT Extensions OPTIONAL }
CertID ::= SEQUENCE {
        hashAlgorithm               AlgorithmIdentifier,
        issuerNameHash              OCTET STRING, -- Hash of Issuer's DN
        issuerKeyHash             OCTET STRING, -- Hash of Issuers public
    key
        serialNumber                CertificateSerialNumber
        }
```

OCSP回复消息ASN1描述(1)

```
OCSPResponse ::= SEQUENCE {
      responseStatus            OCSPResponseStatus,
      responseBytes            [0] EXPLICIT ResponseBytes OPTIONAL }
OCSPResponseStatus ::= ENUMERATED {
         successful             (0), --Response has valid confirmations
         malformedRequest   (1), --Illegal confirmation request
         internalError           (2), --Internal error in issuer
         tryLater                (3), --Try again later
                                        --(4) is not used
         sigRequired            (5), --Must sign the request
         unauthorized            (6) --Request unauthorized
        }
```

OCSP回复消息ASN1描述(2)

```
ResponseBytes ::= SEQUENCE {
        responseType       OBJECT IDENTIFIER,
        response            OCTET STRING
       }

  id-pkix-ocsp           OBJECT IDENTIFIER ::= { id-ad-ocsp }
  id-pkix-ocsp-basic    OBJECT IDENTIFIER ::= { id-pkix-ocsp 1 }
```

OCSP回复消息ASN1描述(3)

```
BasicOCSPResponse ::= SEQUENCE {
        tbsResponseData          ResponseData,
        signatureAlgorithm       AlgorithmIdentifier,
        signature                BIT STRING,
        certs                    [0] EXPLICIT  SEQUENCE OF
                               Certificate OPTIONAL
       }

ResponseData ::= SEQUENCE {
      version               [0] EXPLICIT Version DEFAULT v1,
      responderID           ResponderID,
      producedAt            GeneralizedTime,
      responses               SEQUENCE OF SingleResponse,
      responseExtensions      [1] EXPLICIT Extensions OPTIONAL }
```

OCSP回复消息ASN1描述(4)

```
ResponderID ::= CHOICE {
         byName                [1] Name,
         byKey                 [2] KeyHash }
KeyHash ::= OCTET STRING -- SHA-1 hash of responder's public key
   (excluding the tag and length fields)
SingleResponse ::= SEQUENCE {
      certID               CertID,
      certStatus            CertStatus,
      thisUpdate           GeneralizedTime,
      nextUpdate           [0] EXPLICIT GeneralizedTime OPTIONAL,
      singleExtensions   [1] EXPLICIT Extensions OPTIONAL }
CertStatus ::= CHOICE {
      good                    [0] IMPLICIT NULL,
      revoked                 [1] IMPLICIT RevokedInfo,
      unknown                 [2] IMPLICIT UnknownInfo }
RevokedInfo ::= SEQUENCE {
      revocationTime            GeneralizedTime,
      revocationReason          [0] EXPLICIT CRLReason OPTIONAL }
UnknownInfo ::= NULL
```

Time Stamp Protocols -TSP(RFC3161)

- 时间戳服务是什么?
  - 提供一个数据在某个时间之前的存在性证明（proof-of-existence）。
- 为什么需要时间戳服务?
  - 数字签名 + 时间戳 提供抗否认服务。
- PKI中时间戳的基本原理
  - 对数据的摘要和公正时间进行权威绑定，并可以验证。
- 用户和时间戳认证中心（Time Stamping Authority， TSA)之间的交互协议

时间戳认证中心 需求

1. 可信时间源.
2. 每个产生的时间戳里包含一个可信时间.
3. 每个产生的时间戳里包含一个唯一标识.
4. 针对每个有效的时间戳请求，产生一个有效的时间戳.
5. 时间戳认证并不包含对请求者的认证。
6. 在每个时间戳里包含产生时间戳的认证政策.
7. 对认证的数据只包含其唯一的指纹数据（HASH）.
8. 用时间戳认证服务专用的密钥对时间戳进行数字签名.
9. 必要时，可以包含认证扩展信息.

时间戳认证中心交互协议

- 时间戳请求者向时间戳认证中心发送请求（TimeStampReq）。
- 时间戳认证中心向时间戳请求者发送响应（TimeStampResp）。
- 时间戳请求者验证响应
  - 检查响应状态码（出错则失败）
  - 检查验证返回的时间戳（数字签名和各个域内容）
  - 检查TSA证书的有效性

A time-stamping request Format

```
TimeStampReq ::= SEQUENCE  {
      version                    INTEGER  { v1(1) },
      messageImprint        MessageImprint,
                     --a hash algorithm OID and the hash value of the data to be time-stamped
      reqPolicy                TSAPolicyId             OPTIONAL,
      nonce                      INTEGER                   OPTIONAL,
      certReq                   BOOLEAN                  DEFAULT FALSE,
      extensions              [0] IMPLICIT Extensions  OPTIONAL
}
MessageImprint ::= SEQUENCE  {
          hashAlgorithm                AlgorithmIdentifier,
          hashedMessage                OCTET STRING
}
```

A time-stamping response Format(1)

```
TimeStampResp ::= SEQUENCE  {
     status                    PKIStatusInfo,
     timeStampToken        TimeStampToken     OPTIONAL  }

PKIStatusInfo ::= SEQUENCE {
     status       PKIStatus,
     statusString  PKIFreeText     OPTIONAL,
     failInfo      PKIFailureInfo  OPTIONAL  }

PKIStatus ::= INTEGER {
     granted                   (0),  -- when a TimeStampToken, as requested, is present.
     grantedWithMods         (1),  -- when a TimeStampToken, with modifications, is present.
     rejection                 (2),
     waiting                   (3),
     revocationWarning       (4),  -- contains a warning that a revocation is  imminent
     revocationNotification (5)   -- notification that a revocation has occurred  }
```

A time-stamping response Format(2)

```
PKIFailureInfo ::= BIT STRING {
  badAlg                  (0),    -- unrecognized or unsupported Algorithm Identifier
  badRequest              (2),    -- transaction not permitted or supported
  badDataFormat           (5),    -- the data submitted has the wrong format
  timeNotAvailable    (14),    -- the TSA's time source is not available
  unacceptedPolicy    (15),    -- TSA policy is not supported by the TSA
  unacceptedExtension (16),    -- the extension is not supported by the TSA
  addInfoNotAvailable (17)     -- the additional information requested could not
                                      be understood or is not available
  systemFailure           (25)   -- the request cannot be handled due to system failure
 }
```

TimeStampToken(时间戳)

```
TimeStampToken ::= ContentInfo
ContentInfo ::= SEQUENCE {
  contentType      ContentType,          -- contentType is id-signedData ([CMS])
  content          SignedData ([CMS])
}
SignedData ::= SEQUENCE {
     version                CMSVersion,
     digestAlgorithms       DigestAlgorithmIdentifiers,
     encapContentInfo        EncapsulatedContentInfo,
     certificates           [0] IMPLICIT CertificateSet OPTIONAL,
     crls                   [1] IMPLICIT CertificateRevocationLists OPTIONAL,
     signerInfos            SignerInfos
}
EncapsulatedContentInfo ::= SEQUENCE {
     eContentType              ContentType,
     eContent                  [0] EXPLICIT OCTET STRING OPTIONAL
                         --for TimeStampToken ,it is the DER-encoded value of TSTInfo
}
```

SignerInfo

```
SignerInfo ::= SEQUENCE {
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifier,
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signature SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}
```

TSTInfo

```
TSTInfo ::= SEQUENCE  {
          version                 INTEGER  { v1(1) },
          policy                  TSAPolicyId,
          messageImprint          MessageImprint,  -- MUST have the same value as the
                                                     similar field in TimeStampReq
          serialNumber            INTEGER,         -- TSA MUST be ready to accommodate
                                                     integers up  to 160 bits.
          genTime                 GeneralizedTime,
          accuracy                Accuracy               OPTIONAL,
          ordering                BOOLEAN                DEFAULT FALSE,
          nonce                   INTEGER                OPTIONAL,
                                  -- MUST be present if the similar field was present
                        -- in TimeStampReq.  In that case it MUST have the same value.
          tsa                     [0] GeneralName        OPTIONAL,
          extensions              [1] IMPLICIT Extensions   OPTIONAL
 }
```

时间戳消息传输机制

- 目前还没有强制标准,以下为可选的
  - Time-Stamp Protocol Using E-mail
  - File Based Protocol
  - Socket Based Protocol
  - Time-Stamp Protocol via HTTP

补：Cryptographic Message Syntax (CMS) RFC3369

- 该文档描述了密码消息语法，功能用于数字签名、摘要、认证和加密任意消息内容等。
- 描述了数据保护的封装语法，支持数字签名和加密。
- 允许多次封装即嵌套封装
- 该标准是由PKCS＃7 （V1.5）发展而来的（保持向前兼容）。
- 本文档定义了一个保护对象：ContentInfo
- ContentInfo的内容类型定义了6个：
  - data
  - signed-data
  - enveloped-data
  - digested-data
  - encrypted-data
  - authenticated-data

ContentInfo ASN.1语法

```
ContentInfo ::= SEQUENCE {
        contentType            ContentType,
        content                [0] EXPLICIT ANY DEFINED BY contentType
}

 ContentType ::= OBJECT IDENTIFIER
```

以下描述 内容类型ContentType：

（1）Data 内容类型

- 任意的octet strings，无内部结构。

（2）Signed-data内容类型

```
SignedData ::= SEQUENCE {
      version        CMSVersion,
      digestAlgorithms        DigestAlgorithmIdentifiers,
      encapContentInfo        EncapsulatedContentInfo,
      certificates        [0] IMPLICIT CertificateSet OPTIONAL,
      crls                    [1] IMPLICIT CertificateRevocationLists
                                  OPTIONAL,
      signerInfos      SignerInfos
}
EncapsulatedContentInfo ::= SEQUENCE {
      eContentType                ContentType,
      eContent                     [0] EXPLICIT OCTET STRING OPTIONAL }
```

```
SignerInfo ::= SEQUENCE {
     version                 CMSVersion,
     sid                     SignerIdentifier,
     digestAlgorithm         DigestAlgorithmIdentifier,
     signedAttrs             [0] IMPLICIT SignedAttributes OPTIONAL,
     signatureAlgorithm          SignatureAlgorithmIdentifier,
     signature               SignatureValue,
     unsignedAttrs           [1] IMPLICIT UnsignedAttributes OPTIONAL
}
```

（3）Enveloped-data内容类型

```
 EnvelopedData ::= SEQUENCE {
        version                        CMSVersion,
        originatorInfo                 [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos                 RecipientInfos,
        encryptedContentInfo           EncryptedContentInfo,
        unprotectedAttrs           [1] IMPLICIT UnprotectedAttributes OPTIONAL }
OriginatorInfo ::= SEQUENCE {
        certs                      [0] IMPLICIT CertificateSet OPTIONAL,
        crls                    [1] IMPLICIT CertificateRevocationLists OPTIONAL }
RecipientInfos ::= SET SIZE (1..MAX) OF RecipientInfo
RecipientInfo ::= CHOICE {
       ktri KeyTransRecipientInfo,
       kari [1] KeyAgreeRecipientInfo,
       kekri [2] KEKRecipientInfo,
       pwri [3] PasswordRecipientinfo,
       ori [4] OtherRecipientInfo }
```

```
EncryptedContentInfo ::= SEQUENCE {
        contentType            ContentType,
        contentEncryptionAlgorithm        ContentEncryptionAlgorithmIdentifier,
        encryptedContent            [0] IMPLICIT EncryptedContent OPTIONAL }

EncryptedContent ::= OCTET STRING
```

（4）Digested-data内容类型

```
DigestedData ::= SEQUENCE {
      version                    CMSVersion,
      digestAlgorithm        DigestAlgorithmIdentifier,
      encapContentInfo     EncapsulatedContentInfo,
      digest                      Digest
}

    Digest ::= OCTET STRING
```

（5）Encrypted-data内容类型

- 与Enveloped-data内容类型不同，它不存在接收者，也不存在内容加密密钥信息，通常用于本地数据加密保护（也许密钥是从口令演化出来的）。

```
EncryptedData ::= SEQUENCE {
    version                 CMSVersion,
    encryptedContentInfo    EncryptedContentInfo,
    unprotectedAttrs        [1] IMPLICIT UnprotectedAttributes OPTIONAL }
EncryptedContentInfo ::= SEQUENCE {
    contentType ContentType,
    contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
    encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL }

EncryptedContent ::= OCTET STRING
```

（6）Authenticated-data内容类型

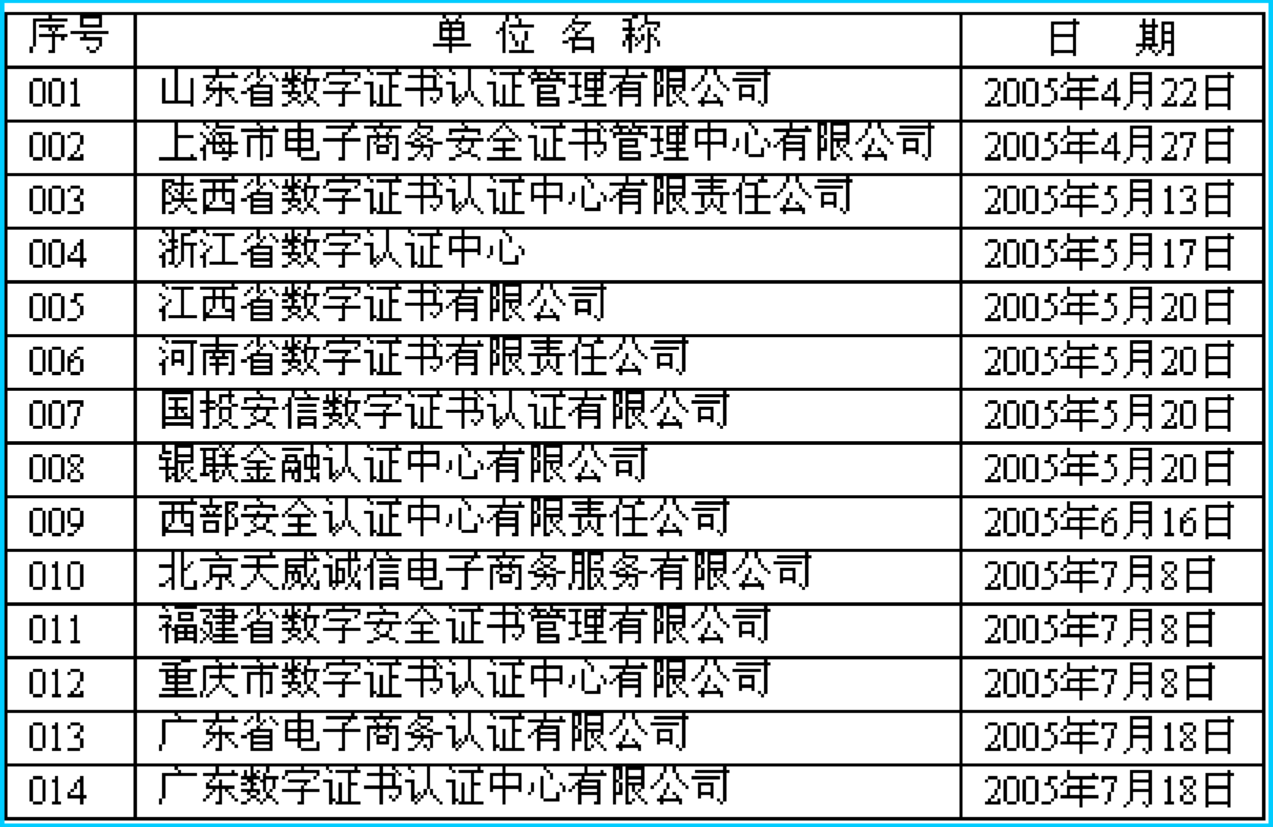
- 包含内容、MAC以及加密认证密钥

```
AuthenticatedData ::= SEQUENCE {
      version                 CMSVersion,
      originatorInfo          [0] IMPLICIT OriginatorInfo OPTIONAL,
      recipientInfos          RecipientInfos,
      macAlgorithm            MessageAuthenticationCodeAlgorithm,
      digestAlgorithm         [1] DigestAlgorithmIdentifier OPTIONAL,
      encapContentInfo        EncapsulatedContentInfo,
      authAttrs               [2] IMPLICIT AuthAttributes OPTIONAL,
      mac                     MessageAuthenticationCode,
      unauthAttrs             [3] IMPLICIT UnauthAttributes OPTIONAL
}
```

PMI *

国内CA机构

- 国家刚通过了几个获得电子认证服务使用密码许可证的单位



序号	单位名称	日期
001	山东省数字证书认证管理有限公司	2005年4月22日
002	上海市电子商务安全证书管理中心有限公司	2005年4月27日
003	陕西省数字证书认证中心有限责任公司	2005年5月13日
004	浙江省数字认证中心	2005年5月17日
005	江西省数字证书有限公司	2005年5月20日
006	河南省数字证书有限责任公司	2005年5月20日
007	国投安信数字证书认证有限公司	2005年5月20日
008	银联金融认证中心有限公司	2005年5月20日
009	西部安全认证中心有限责任公司	2005年6月16日
010	北京天威诚信电子商务服务有限公司	2005年7月8日
011	福建省数字安全证书管理有限公司	2005年7月8日
012	重庆市数字证书认证中心有限公司	2005年7月8日
013	广东省电子商务认证有限公司	2005年7月18日
014	广东数字证书认证中心有限公司	2005年7月18日