

***Software School of Shandong University***

# Security Protocols

--- PKI Principles and technology sd03032110  
(Chapter 3 Certificate And CRLs)



Instructor: Hou Mengbo 侯孟波

Email: houmb AT sdu.edu.cn

Office: Information Security Research Office.

Rm: Office Building 111

# Abstract

- 本章主要讲述ITU-T X.509标准公钥数字证书认证框架
  - ASN.1抽象语法标记/DER编码。
  - X.509标准中的Certificate和CRL的逻辑结构
  - X.509标准中的其他内容另章讲述。

# ASN.1

- 国际电联开放系统互联（OSI）抽象语法标记1（X.208）
- 基本思想是为描述数据结构而创建一种允许通过机器来产生数据编码解码器（codec）的系统
- 高层定义的结构描述规范，容易转换成二进制形式
- 非常灵活的定义一系列数据类型，从简单的整数、字符串到复杂结构的数据类型
- 复杂... 只须知道它是与C语言接近的语法和结构
- DER（Distinguished Encoding Rules）是ASN.1的一种从抽象标记到具体二进制转换的确定性编码方法。
- 数字证书和证书注销列表等相关对象采用ASN.1描述并采用DER编码方法进行编码。

# ASN.1 类(class)和标注(tag)

- 全局类 (universal) {00}
  - INTEGER [02]
  - BIT STRING [03]
  - OCTET STRING [04] 一串任意8元组
  - NULL [05]
  - Object Identifier [06] 一串整数表示
  - SEQUENCE/SEQUENCE OF [10]
  - SET / SET OF [11]
  - PrintableString [13]
  - IA5String [16] 任意ASCII 字符串
  - UTCTime [17]
  - .....
- 应用类型 (application) {01}
- 上下文特定类型 (context Specific) {10}
- 私有类型 (private) {11}

# BER & DER编码

- BER(Basic Encoding Rules)给出了一种或多种8元组串来表示ASN.1抽象内容的表示方法

BER编码的结构： 标识8元组 + 长度8元组 + 内容8元组 + （结束8元组）

3种分类:本原/有限长度 结构/有限长度 结构/无限长度

**标识：**（一般低标注） class (2位) + 0/1 （1位） + tag(5位)

本原/结构

**长度：**短形式长度在0 - 127之间， 1个8元组（高位0， 低7位为长度）；

长形式长度在 $0 \sim 2^{1008}-1$ ， 2 - 127个8元组， 第1个8元组高位1， 后7位代表接下来的长度8元组个数。

- 一个ASN.1描述对应一种确定的DER编码值

## 一些编码例子

- 位串(BITSTRING):     0110 1110 0101 1101 11   00 0000  
DER编码:     03 04 06               6e               5d               c0  
                ↑    ↑    ↑                                      ↑  
                标识 长度 填充                                      内容                                      -----
  - IA5String电子邮件地址:   test1@rsa.com  
DER编码:   16 0d   74 65 73 74 31 40 72 73 61 2e 63 6f 6d  
                                 t e s t 1 @ r s a . c o m
  - 整数(Integer):       16781473(hex: 010010a1)  
DER编码:   02 04   01 00 10 a1
  - NULL       0500
  - Object Identifier : v1,v2,.....,vn  
DER编码: 06 length 40\*v1+v2 v3 .....vn
- sha-1WithRsaEncryption               1.3. 14. 3. 2. 29
- 06 05 2b 0e 03 02 1d

# X.509 Certificate二进制编码图

```

00000000h: 30 82 04 48 30 82 03 B5 A0 03 02 01 02 02 04 01 ; 0?H0?缘.....
00000010h: 00 10 A1 30 09 06 05 2B 0E 03 02 1D 05 00 30 54 ; ..?...+.....OT
00000020h: 31 0B 30 09 06 03 55 04 06 13 02 43 4E 31 36 30 ; 1.0...U....CN160
00000030h: 34 06 03 55 04 0A 13 2D 53 68 61 6E 64 6F 6E 67 ; 4..U...-Shandong
00000040h: 20 44 69 67 69 74 61 6C 20 43 65 72 74 69 66 69 ; Digital Certifi
00000050h: 63 61 74 65 20 41 75 74 68 6F 72 69 74 79 20 43 ; cate Authority C
00000060h: 65 6E 74 65 72 31 0D 30 0B 06 03 55 04 03 13 04 ; enter1.0...U....
00000070h: 53 44 43 41 30 1E 17 0D 30 31 30 38 33 30 30 30 ; SDC10...01083000
00000080h: 30 30 30 30 5A 17 0D 30 32 30 38 32 39 30 30 30 ; 0000Z..020829000
00000090h: 30 30 30 5A 30 63 31 0D 30 0B 06 03 55 04 06 1E ; 000Z0c1.0...U...
000000a0h: 04 00 43 00 4E 31 0F 30 0D 06 03 55 04 08 1E 06 ; ..C.N1.0...U....
000000b0h: 00 33 00 37 00 30 31 0F 30 0D 06 03 55 04 03 1E ; .3.7.01.0...U...
000000c0h: 06 73 8B 91 D1 8D 85 31 0D 30 0B 06 03 55 04 07 ; .s娑禪?.0...U..
000000d0h: 1E 04 00 6A 00 6E 31 21 30 1F 06 09 2A 86 48 86 ; ...j.n!0...*唆?
000000e0h: F7 0D 01 09 01 16 12 78 69 6E 67 68 65 77 6A 63 ; ?.....xinghewjc
000000f0h: 40 32 31 63 6E 2E 63 6F 6D 30 81 9F 30 0D 06 09 ; @21cn.com0犬0...
00000100h: 2A 86 48 86 F7 0D 01 01 01 05 00 03 81 8D 00 30 ; *唆唯.....亘.0
00000110h: 81 89 02 81 81 00 BB 2F D6 05 84 DC D7 93 A5 69 ; 盲.三.??勳譜
00000120h: 12 2D 40 21 CD 7E 0E 9C 52 6B 17 49 EF 6C E8 97 ; .-0!蛭.凌k.I蹼研

```

# 数字证书



- 将对象身份和对象的公开钥有效捆绑。
- 考虑身份证的原理。
- 数字证书使用数字签名原理
- 证书标准: x509证书 WTLS 证书 PGP证书 属性证书...



# X509证书

- 1988年 ITU-T X.509 (原CCITT X509) 作为X.500目录服务系统的一部分。 Version 1
- 1993年 version 2 增加两个新字段
- 1997年 version 3 进一步完善, 增加扩展项。

# X509 V3数字证书

Certificate format version			version 3
Certificate serial number			12345678
Signature algorithm identifier for CA			RSA with MD5
Issuer X.500 name			c=US, o=ACME
Validity period			start=01/08/96, expiry=01/08/98
Subject X.500 name			c=US, o=ACME, cn=John Smith + ...
Subject public key information			 RSA with MD5
Issuer unique identifier			version 2
Subject unique identifier			version 2
version 3	Type	Criticality	Value
version 3	Type	Criticality	Value
version 3	Type	...	...
version 3	Type	Criticality	Value
CA Signature 			

Extensions

# 基本证书结构和语义 (1)

```
Certificate ::= SEQUENCE {  
    tbsCertificate      TBSCertificate,  
    signatureAlgorithm  AlgorithmIdentifier,  
    signatureValue      BIT STRING  
}
```

## 基本证书结构和语义 (2)

```
TBSCertificate ::= SEQUENCE {  
    version          [0] EXPLICIT Version DEFAULT v1(0),  
    serialNumber     CertificateSerialNumber,  
    signature        AlgorithmIdentifier,  
    issuer           Name,  
    validity         Validity,  
    subject          Name,  
    subjectPublicKeyInfo SubjectPublicKeyInfo,  
    issuerUniqueID    [1] IMPLICIT UniqueIdentifier OPTIONAL,  
                    -- If present, version shall be v2 or v3  
    subjectUniqueID   [2] IMPLICIT UniqueIdentifier OPTIONAL,  
                    -- If present, version shall be v2 or v3  
    extensions        [3] EXPLICIT Extensions OPTIONAL  
                    -- If present, version shall be v3  
}
```

# 基本证书结构和语义 (3)

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {  
    notBefore       Time,  
    notAfter        Time  
}

Time ::= CHOICE {  
    utcTime        UTCTime,  
    generalTime GeneralizedTime  
}

UniquelIdentifier ::= BIT STRING

# 基本证书结构和语义 (4)

```
SubjectPublicKeyInfo ::= SEQUENCE {  
    algorithm      AlgorithmIdentifier,  
    subjectPublicKey BIT STRING  
}
```

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
```

```
Extension ::= SEQUENCE {  
    extnID      OBJECT IDENTIFIER,  
    critical    BOOLEAN DEFAULT FALSE,  
    extnValue   OCTET STRING  
}
```

# 相关问题

- 证书版本 v1 v2 v3 区别和限制
- 证书序列号 大小无限制 产生方式
- 证书签发者和证书持有者 DN信息

Name ::= CHOICE { RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {

type AttributeType,

value AttributeValue

}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

DirectoryString ::= CHOICE {

teletexString TeletexString (SIZE (1..MAX)),

printableString PrintableString (SIZE (1..MAX)),

universalString UniversalString (SIZE (1..MAX)),

utf8String UTF8String (SIZE (1.. MAX)),

bmpString BMPString (SIZE (1..MAX))

}

# 相关问题

- DN信息组成 (X.500标准定义)

例如 这样一个DN: cn=Danny,ou=software development,o=ACME Corporation,c=CN

X.500名称常用的包含如下:

CountryName , 国家, 简写c;

StateOrProvinceName , 州名或省份名称, 简写st;

LocalityName , 城市名称, 简写l;      OrganizationName , 组织名称, 简写o;

OrganizationalUnitName , 部门名称, 简写ou;

CommonName , 通用名称, 简写cn;

StreetAddress , 街道地址;      PostalAddress , 邮政地址;

PostalCode , 邮政编码;      TelephoneNumber , 电话号码;

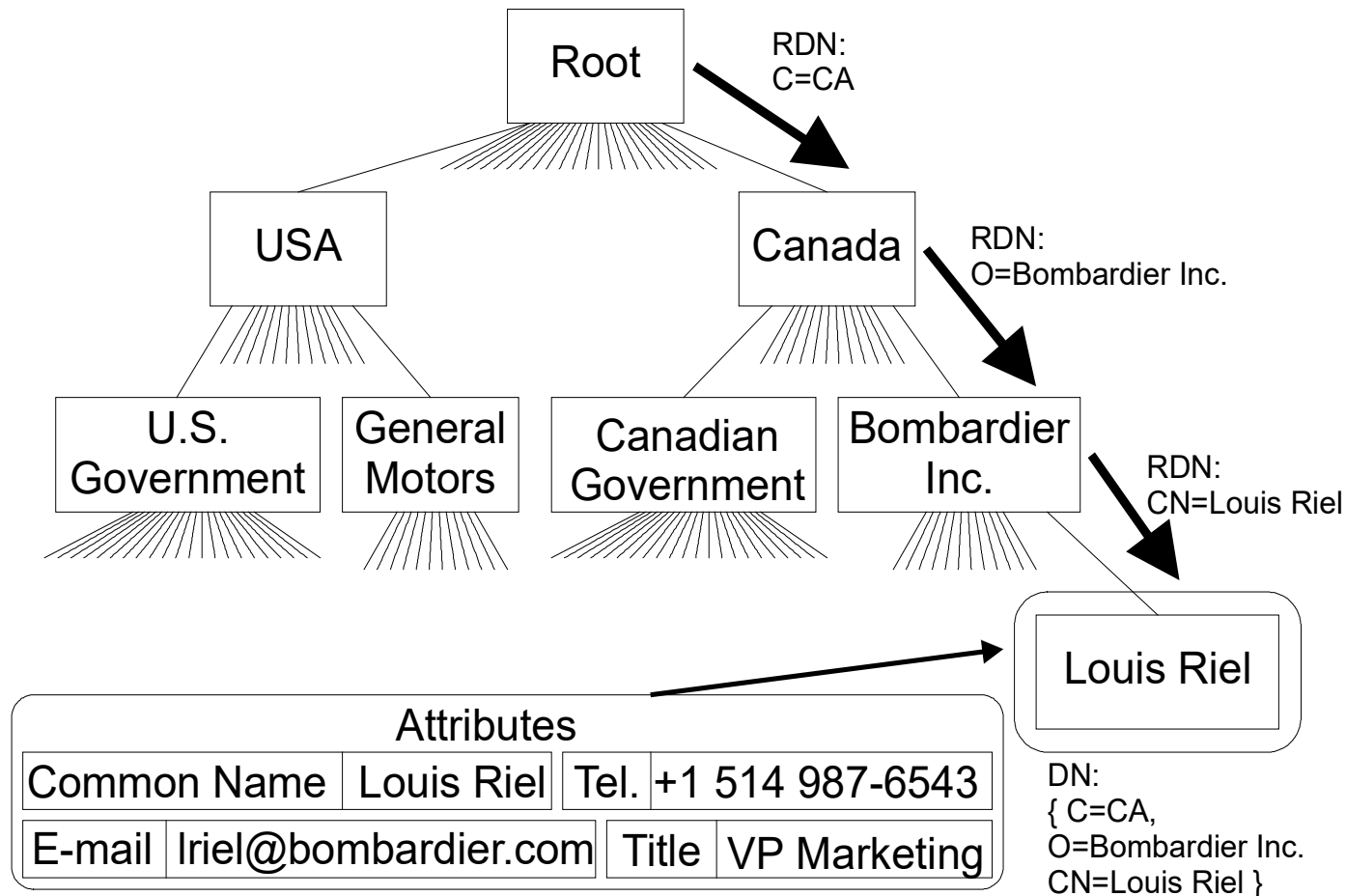
TelexNumber , 电传号码;      postOfficeBox , 信箱号码;

emailAddress , 电子邮箱地址。

.....



# The X.500 Directory Information Tree



# 相关问题

- 有效期

UTCTime: Universal Time YYMMDDHHMMSSZ 两位表示年精确到秒

GeneralizedTime: YYYYMMDDHHMMSSZ

2049年前, UTCTime

2050年后, GeneralizedTime

# 扩展信息

- 扩展ASN1描述

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {

    extnID        OBJECT IDENTIFIER,

    critical     BOOLEAN DEFAULT FALSE,

    extnValue    OCTET STRING

}

- 标准扩展 和私有扩展

# 扩展信息

- X509 v3证书中的扩展可以分为以下几类：
  - 密钥信息
  - 政策信息
  - 用户和CA属性
  - 证书路径限制

# 密钥信息扩展

## (i) Authority Key Identifier

它是CA用来签名证书的密钥的标识符，它应用于CA在生命周期中应用了多个密钥对时，帮助处理验证签名。

## (ii) Subject Key Identifier

它用于在区分与证书中的公钥相对应的特别的密钥对。当一个用户多次更新过它的密钥对时，它显得特别有用。

## (iii) Key Usage

它指明了密钥的用途。一般包括如下几种用途：

non-repudiation	不可抵赖	certificate signing	对证书签名
CRL signing	对CRL签名	Digital signature	数字签名
Symmetric key encryption	对称钥加密	Data encryption	数据加密
Diffie-Hellman key agreement	D-H	密钥交换	

## (iv) Private Key Usage Period

该项指明了用户的签名用私钥作为数字签名密钥的最后有效日期。

# 政策信息扩展

政策信息扩展项为CA发布关于一个特殊的证书应当怎样应用和怎样解释的信息提供了一种机制。它包括两个扩展：

## (i) Certificate Policies

证书政策域指明了证书是在什么样的政策下签发的，或证书适用于什么样的类型。证书政策由一个特殊格式的对象标识符标识，它必须由国际性标准组织注册。在一个证书中指派多个证书政策是可能的。一般的，对一个证书适用的政策不允许冲突。如果证书政策域设置成non-critical，则发放该证书的认证中心只是赋予该证书适用的政策，并不需要该证书仅仅适用于该政策；相反，则该证书只适用于该政策。

## (ii) Policy Mappings

相对于证书政策域适用于用户证书和CA交叉证书，该域只适用于交叉证书。当被一个不同的CA的公钥信息验证时，交叉证书就由一个CA产生。该域提供了一个为签名CA将其政策映射到一个交叉证书中的CA的政策机制。当一个应用程序处理跨CA范围的证书链时，该域设置成critical，一个应用程序应用映射信息来保证对证书链中的证书适用于连续的可接受的政策。

# 用户和CA属性扩展

- 用户和CA属性扩展为一个用户或CA提供鉴别信息提供了附加的机制。

## (i) **Subject Alternative Name**

该域对证书的拥有者提供了一个或多个确定的名称，允许的名称以下：

Internet e-mail address	互连网电子邮件地址
Internet domain name	互连网域名
Internet IP address	互连网IP地址
X. 400 e-mail address	X. 400电子邮件地址
EDI party name	EDI 成员名
URL	URL 网址

.....

## (ii) **Issuer Alternative Name**

该域对证书的发放者提供了一个或多个确定的名称，就象上面介绍的一样。

## (iii) **Subject Directory Attributes**

该域提供了用户证书中附加的一些X. 500目录属性。

# 证书路径限制扩展

- 证书路径限制扩展为使CA控制和限制在交叉认证环境中扩展的第三方提供了一种机制。有三种域：

## (i) Basic Constraints

该域指明了证书中的证书拥有者是作为一个终端用户还是作为一个CA。如果是一个CA，则该证书是一个交叉证书，一个交叉证书可能还指定可以接受的证书链的最大长度。如果长度指定为1，则用户只能验证在该交叉证书中指定的CA发放的终端用户的公钥和CRL。

## (ii) Name Constraints

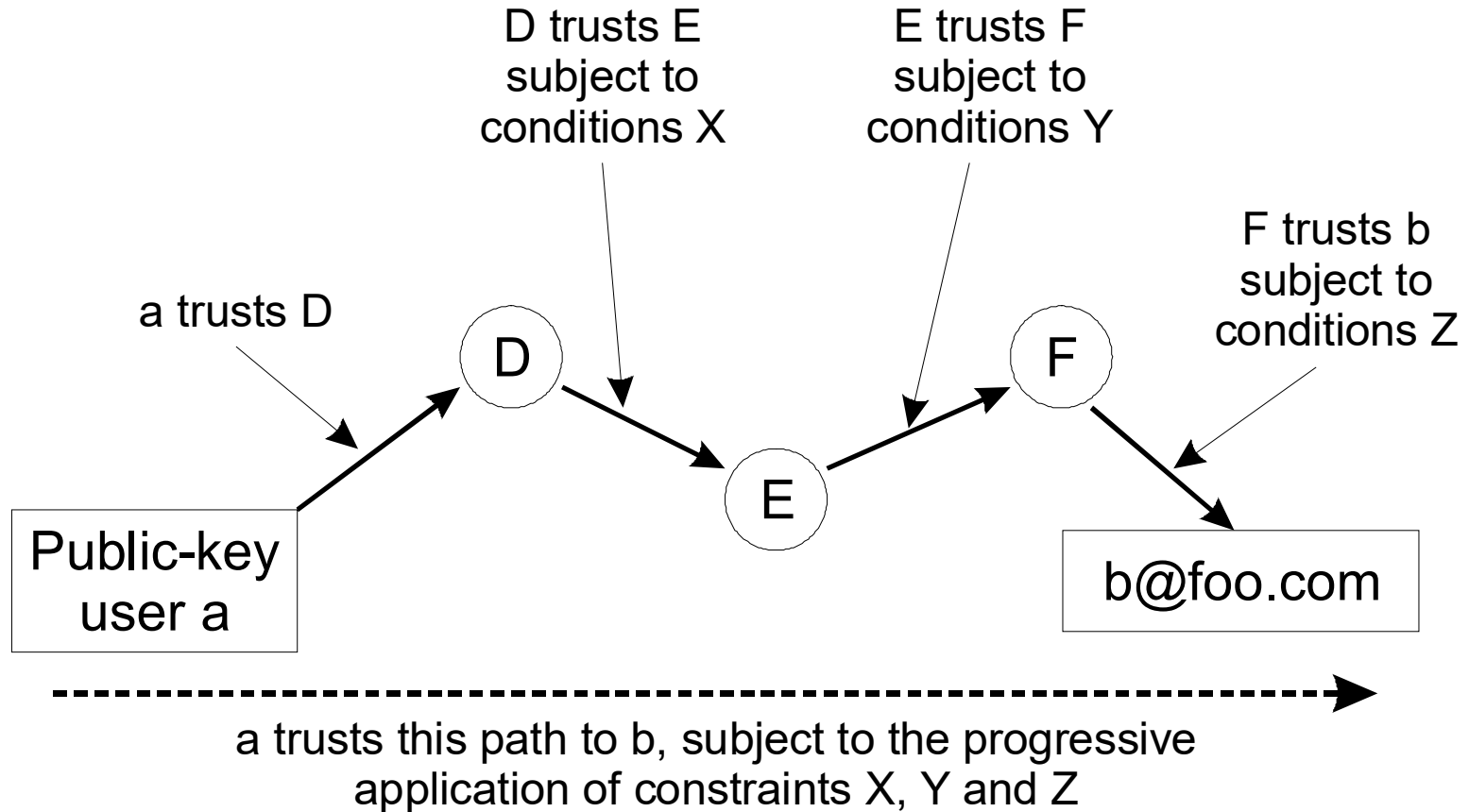
该域应用于交叉证书。该域为管理员提供了限制在交叉认证环境中可信名称的范围的能力。它相对于Basic Constraints更复杂。

## (iii) Policy Constraints

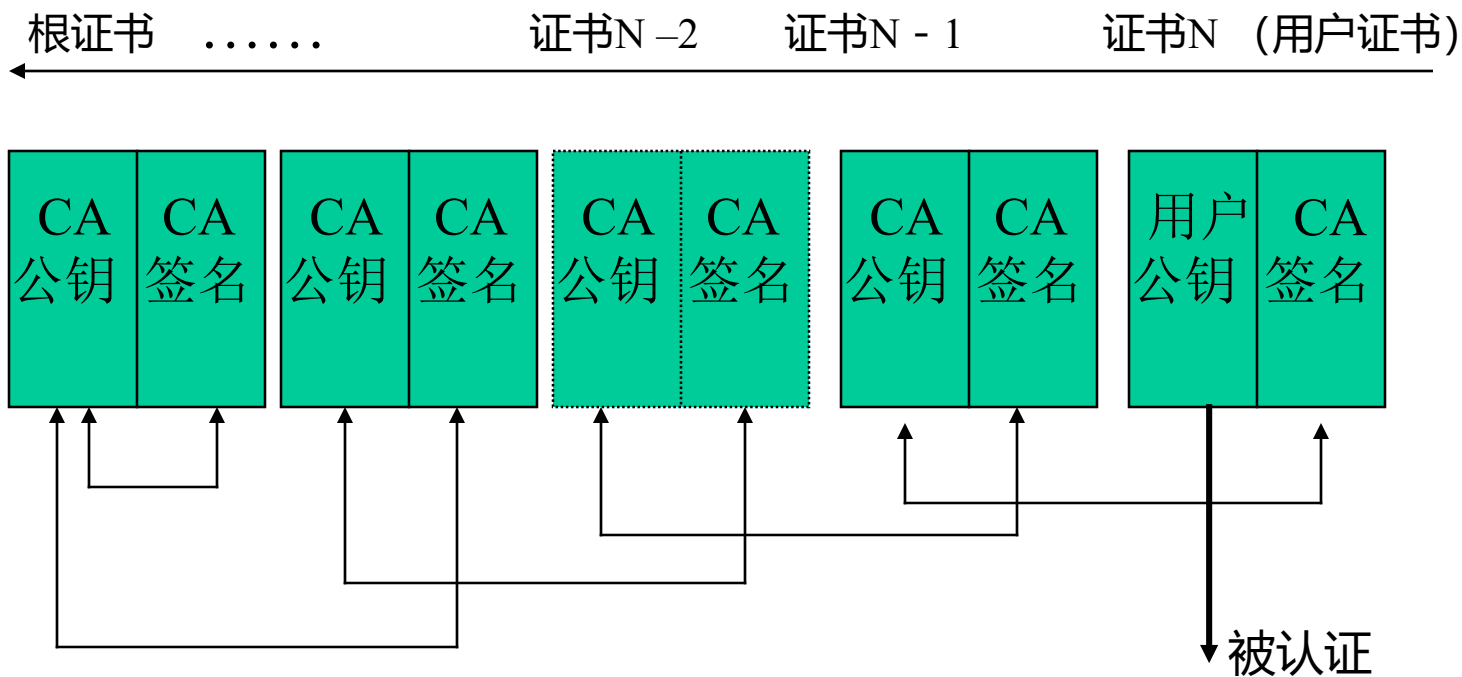
该域应用于交叉证书。该域为管理员提供了从一个交叉证书扩展的证书链中指定一系列可接受政策的能力。它可以指定是否证书链中所有的证书必须符合一个特定的政策，或者在处理证书链时是否约束policy mapping。



# A progressive-constrained trust chain



# 证书链问题



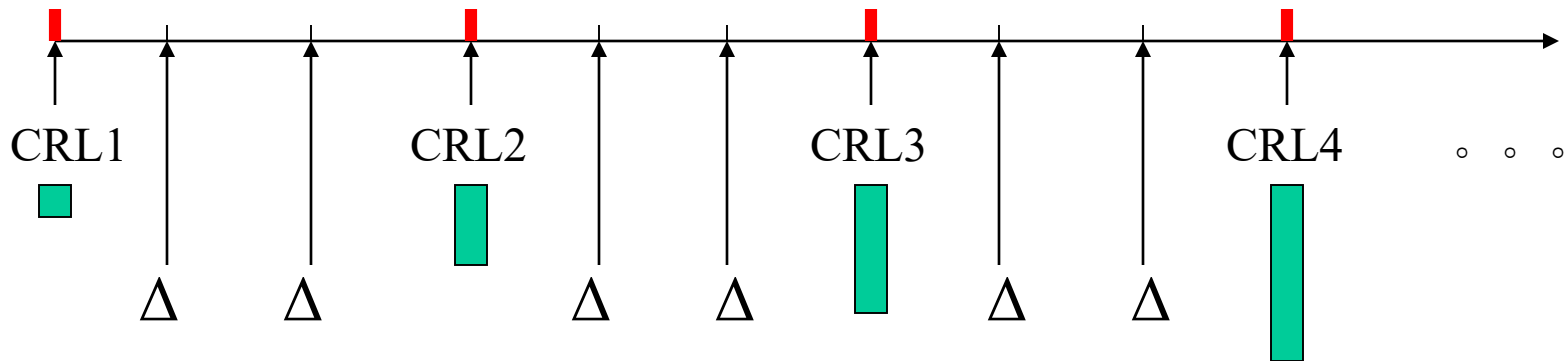
- ▲ 被认证公钥和签名密钥之间形成链状结构。
- ▲ 证书签发者和证书拥有者信息之间也是形成链状结构。

# 证书注销列表CRL

- CertificateList ::= SEQUENCE {  
    tbsCertList            TBSCertList,  
    signatureAlgorithm    AlgorithmIdentifier,  
    signatureValue BIT STRING  
}
- TBSCertList ::= SEQUENCE {  
    version            Version OPTIONAL,  
    signature          AlgorithmIdentifier,  
    issuer             Name,  
    thisUpdate        Time,  
    nextUpdate        Time OPTIONAL,  
    revokedCertificates SEQUENCE OF SEQUENCE {  
        userCertificate        CertificateSerialNumber,  
        revocationDate        Time,  
        crlEntryExtensions    Extensions OPTIONAL -- if present, shall be v2  
    } OPTIONAL,  
    crlExtensions        [0] EXPLICIT Extensions OPTIONAL -- if present, shall be v2  
}

# 增量CRL (Delta-CRL)

- 随着时间推移，注销证书逐渐增多。需要控制CRL下载及时性和下载规模
- 采取发布周期内基准点外的增量机制。



# 分段CRL和CRL发布点

- 为了控制CRL规模扩大和下载集中问题
- 将证书序列号进行某种规则的分段，每段形成一个规模较小的CRL，并分布式发布。
- 用户证书中包含CRL发布点，指明要下载的CRL位置。

# OCSP在线证书状态协议\*

- 解决CRL周期性发布机制存在的问题。 - - - 及时性  
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

# 属性证书

- AA, Attribute Certificate Authority的缩写, 即属性证书中心。它是一个为用户提供业务权限认证的可信赖的安全服务机构。由它为用户业务操作提供认证的属性证书, 与身份证书配合, 实现用户权限控制。
- **属性证书** 中包含了用户身份 (与身份证书中的身份相一致)、用户操作权限属性以及AA对其所做的数字签名。

采用属性证书实现权限控制是代替ACL (Access Control Lists) 的另一种权限控制安全方案。