Universidade da Beira Interior
Faculdade de Engenharia
Departamento de Informática

Segurança Informática
Aula 6
Licenciatura em Engenharia Informática
Licenciatura em Informática Web

Computer Security
Lecture 6
Degree in Computer Science and Engineering
Degree in Web Informatics

Sumário
Gestão de chaves públicas: o problema associado à confiança de chaves públicas, estrutura e objetivos dos certificados X.509, a infraestrutura de chaves públicas, e as listas de revogação de certificados.

Summary
Management of public keys: the trust issue associated with public key management, structure and objectives of X.509 certificates, Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs).

1 Certificados X.509
X.509 Certificates

1.1 Introdução e Motivação
Introduction and Motivation

Anteriormente foram discutidos vários algoritmos e mecanismos da criptografia de chave pública, nomeadamente cifra e troca de chaves de sessão, e assinaturas digitais. Da discussão deve resultar uma noção mais ou menos clara das enormes vantagens e possibilidades que o uso destes algoritmos e mecanismos têm em várias áreas de aplicação:

1. é a criptografia que chave pública que permite trocar segredos sem existir qualquer contacto prévio[1]
2. é também a que permite a construção de assinaturas digitais sem recurso a agentes de confiança e;
3. embora, não discutido, é ela que suporta métodos novos de autenticação de entidades bem mais seguros que o conhecido método baseado na combinação de um nome de utilizador e uma palavra-passe;
4. etc.

Contudo, **a utilização destas novas técnicas** e mecanismos acarreta **um problema novo**, **o da gestão das chaves**:

1. O facto de cada entidade ter duas chaves em vez de uma não parece ser grave.
2. O facto do par de chaves pública/privada ser muito maior que o tamanho das respetivas chaves de cifra simétricas já constitui um problema maior, mas não inteiramente limitativo hoje em dia[2]. Este subproblema contudo, levará inevitavelmente ao pensamento de como é que um humano poderá usar chaves tão grandes na prática, já que recordá-las é impraticável. O uso de dispositivos que guardam estas chaves (e.g., Cartão do Cidadão) podem resolver este problema.
3. **O grande problema está na confiança** ou, por outras palavras, na **garantia de que determinada chave pública é da entidade que a diz possuir**.

Repare no seguinte: se o Bob quiser falar com a Alice, pede-lhe a sua chave pública, gera uma chave de cifra simétrica aleatoriamente, cifra-a com a chave que recebeu da Alice usando *Optimal Assymmetric Encryption Padding* (OAEP) e envia-lha. O problema está na parte em que o Bob pede ou procura a chave da Alice e obtém uma. **Quem é que garante ao Bob que ele obteve, seguramente, a chave pública da Alice, e não a chave pública da Claire, disfarçada de Alice?**

Repare-se que **o problema antes indicado afeta todas as aplicações deste tipo de mecanismos**, nomeadamente a assinatura digital. Neste caso, a questão é: *como é que podemos ter a certeza de que foi a Alice que assinou um documento, se há a hipótese da Claire o ter feito e nos enviar a chave dela, dizendo que é a da Alice?*

1.2 A Recomendação X.509
The X.509 Recommendation

Quando foi **inicialmente pensada e implementada**, a *Internet*[3] **não incorporava mecanismos de segurança**

[1] Esta afirmação não é inteiramente verdade, e será discutida aqui.

[2] Alguns esquemas de cifra de chave pública homomórfica definem chaves que são, de facto, limitativas em termos de utilização prática.

[3] A rede que interliga redes locais a nível mundial.

nativos, principalmente porque se desconheciam o sucesso e importância que esta rede teria para a **humanidade** a curto/médio prazo. Esforços relativamente recentes, feitos no sentido de **melhorar a segurança** na *Internet*, levaram à **criação e desenvolvimento de vários protocolos** (e.g. *Secure/Multipurpose Internet Mail Extensions* (S/MIME), *Internet Protocol Security* (IPSec)) que usam criptografia simétrica e assimétrica para garantir a segurança das comunicações.

Muitos destes protocolos **elaboram no conceito de certificado de um conjunto de parâmetros**, que mais não é do que um **documento eletrónico assinado digitalmente que liga dois ou mais valores entre si**, como por exemplo, o nome de uma pessoa e uma chave pública. Esses certificados são gerados e geridos por via de uma Infraestrutura de Chave Pública (*Public Key Infrastructure* (PKI)), discutida em baixo.

O uso de criptografia de chave pública nas telecomunicações é regulado pela **recomendação X.509 do *International Telecomumunications Union* (ITU)**. A aplicação desta recomendação à organização algo mais flexível da *Internet* **é definida num conjunto de** *Requests for Comments* **(RFCs) publicados pela** *Internet Engineering Task Force* **(IETF)**, uma comunidade internacional de fabricantes, operadores, vendedores e investigadores de tecnologias de redes, interessados no funcionamento e evolução da *Internet*.

Dentro do IETF, **o grupo que gere os RFCs relacionados com o X.509 chama-se *PKIX Working Group***. Este grupo de trabalho alimenta uma série de documentos chamados X.509 *Public Key Infrastructure*. Entre outros detalhes, a norma X.509 **especifica a sintaxe dos certificados de chave pública, das listas de revogação de certificados e dos certificados de atributos, bem como o algoritmo de validação dos certificados**, discutido adiante, e conhecido por validação do **caminho de certificação**.

Os mecanismos e conceitos definidos nesta norma **fornecem as respostas a questões como**:

1. Como é que as chaves públicas são guardadas?
2. Como é que obtenho uma dada chave pública?
3. Como é que o Bob sabe ou confia que uma determinada chave pública pertence, de facto, à Alice?

1.3 História Resumida
Brief History

A norma X.509 foi **inicialmente submetida a 3 de Julho de 1988**, e começou como **um ramo da norma X.500**. A norma **assume um sistema estritamente hierárquico de Autoridades Certificadoras** (ACs) para **emissão de certificados**, contrastando com **outros modelos de confiança**, como o definido pelo sistema *Pretty Good Privacy* (PGP) (falaremos do PGP mais adiante).

O X.509 vai agora **na sua 3ª versão**, está especificado no **RFC 5280**, e é normalmente referido como **PKIX para a Infraestrutura de Chave Pública** (X.509).

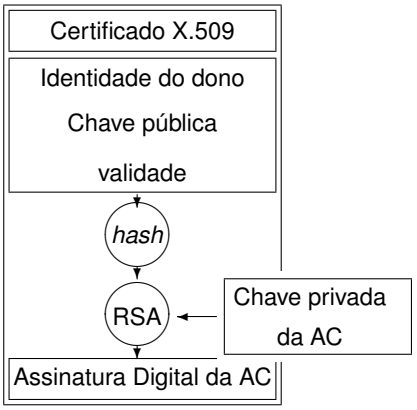
1.4 O Certificado X.509
A X.509 Certificate

O preenchimento dos objetivos da norma X.509 e o funcionamento da PKI **presumem que os sistemas que vão usar chaves públicas se associam à PKI** o que, no fundo, **significa serem compatíveis e usarem os mecanismos definidos na norma**. O utilizador de determinada PKI **deve ficar em condições de confiar** que, cada vez que usa uma chave pública, esta pertence à entidade com quem deseja comunicar ou para quem deseja verificar a assinatura digital (por outras palavras, fica certo de que a entidade com quem quer comunicar tem a respetiva chave privada).

Já foi dito que a **confiança** é construida recorrendo certificados de chave pública:

> Um certificado de chave pública é uma **estrutura que associa uma chave pública a uma** entidade em particular (ou a uma **representação da sua identidade**). A associação chave / entidade **é estabelecida por um terceiro**, designado na literatura por **Autoridade de Certificação** (AC), que assina digitalmente cada certificado.

No fundo, esta autoridade é quem assegura ao recetor do certificado que determinada chave pertence a determinada entidade. Assim, **a utilidade** de um certificado **depende**, apenas e só, **da confiança que as entidades têm relativamente à Autoridade de Certificação**.



O certificado é assinado digitalmente pela **Autoridade Certificadora**, que **utiliza**, para o efeito e obviamente, **a sua chave privada**.

1.5 Representação Simplista de um Certificado X.509
Simplified Representation of an X.509 Certificate

Em baixo inclui-se uma representação simplificada de um certificado X.509:

```
Certificate:
 Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e95)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town,
```

```
        O=Thawte Consulting cc, OU=Certification
        Services Division, CN=Thawte Server
        CA/emailAddress=server-certs@thawte.com

    Validity
        Not Before: Jul  9 16:04:02 1998 GMT
        Not After : Jul  9 16:04:02 1999 GMT

    Subject: C=US, ST=Maryland, L=Pasadena,
        O=Brent Baccala, OU=FreeSoft,
        CN=www.freesoft.org/emailAddress=
            baccala@freesoft.org

    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:
                c8:bb:33:35:19:d5:0c:64:b9:3d:41:b2:96:
                fc:f3:31:e1:66:36:d0:8e:56:12:44:ba:75:
                eb:e8:1c:9c:5b:66:70:33:52:14:c9:ec:4f:
                91:51:70:39:de:53:85:17:16:94:6e:ee:f4:
                d5:6f:d5:ca:b3:47:5e:1b:0c:7b:c5:cc:2b:
                6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:8f:
                a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:
                e3:d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:
                10:bc:b8:e8:35:1c:9e:27:52:7e:41:8f
            Exponent: 65537 (0x10001)

Signature Algorithm: md5WithRSAEncryption
    93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:
    5d:9d:92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:
    ef:63:2f:92:ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:
    be:f6:ea:8e:9c:67:d0:a2:40:03:f7:ef:6a:15:09:79:
    a9:46:ed:b7:16:1b:41:72:0d:19:aa:ad:dd:9a:df:ab:
    97:50:65:f5:5e:85:a6:ef:19:d1:5a:de:9d:ea:63:cd:
    cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:8f:0e:fc:ba:
    1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:68:9f
```

1.6 Propriedades do Certificado X.509

Properties of a X.509 Certificate

A utilização de uma PKI e de certificados X.509 assenta nas seguintes propriedades e factos:

- (facto) **A entidade** que requisitou e possui o certificado **confia que a Autoridade Certificadora verificou que a chave pública expressa no certificado pertence**, de facto, **ao proprietário**. Presume-se que, quando uma autoridade certificadora emite um certificado, só o faz quando tem a certeza de que a chave pública pertence ao *subject* constante no documento.
- (propriedade) A assinatura digital anexa ao certificado assegura a sua **autenticidade** e **integridade**. I.e., não foi alterada, portanto, tudo o que contém é verdade, se assinatura digital verificar.
- (propriedade) Um certificado de chave pública é válido para **um período de tempo bem definido**. Este período **é especificado no conteúdo assinado**.
- (propriedade) Como a assinatura e a validade temporal de um certificado podem ser verificadas independentemente por um utilizador, os certificados **podem ser distribuídos por canais inseguros**.

1.7 X.509 – Verificação de Assinaturas Digitais

X.509 – Verification of Digital Signatures

Normalmente, para além de conterem a chave pública, o período de validade e o identificador do dono, os certificados de chave pública **contêm também um campo que indica para que efeitos pode ser usada a chave** nele contida, nomeadamente: **assinatura digital, autenticação, troca de chaves de sessão ou verificação de assinaturas de outros certificados** (caso o certificado seja o de uma autoridade certificadora – ver em baixo).

Dado que temos agora **mais uma estrutura de dados que é necessário verificar** aquando de uma das operações criptográficas antes descritas, o processo de verificação de uma assinatura digital e de cifra de chaves de sessão **fica mais complexo** (e ainda vai complicar mais adiante). Por exemplo, considere que o Bob recebeu uma mensagem e uma assinatura digital da entidade que se anuncia como Alice no contexto da comunicação. **Os passos da verificação dessa assinatura passam a ser** (estes passos ainda não estão completos):

1. **O Bob procura obter o certificado da Alice contendo a chave pública** necessária à verificação **assinado por uma entidade de confiança.**
2. O Bob verifica que o certificado é válido:
   (a) **Verifica que a assinatura do certificado é válida**;
   (b) Que **foi emitida por uma entidade certificadora de confiança** e;
   (c) que **ainda está dentro do prazo de validade**.
3. O Bob **verifica que a informação que recebe é consistente com as permissões** / privilégios da Alice;
4. Finalmente, **Bob usa a chave pública contida no certificado para verificar a assinatura digital recebida**[4].

2 Infrastrutura de Chave Pública

Publik Key Infrastructure

2.1 Definição de PKI

Definition of PKI

*A Public Key Infrastructure (PKI) is a **set of hardware**, **software**, **people**, **policies** and **procedures** needed **to create**, **manage**, **store**, **distribute and revoke Public Key Certificates (PKCs) based on publickey cryptography**.*[5]

[4] Repare que, antes, só se fazia este último passo.

[5] Adaptado de RFC4158 (ver `http://www.ietf.org/rfc/rfc4158.txt`).

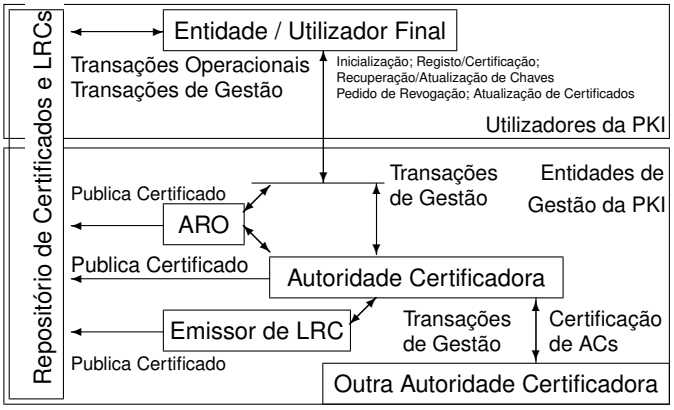
A Infraestrutura de Chave Pública (Public Key Infrastructure (PKI)) é o conjunto de hardware, software, pessoas, políticas e procedimentos necessários à criação, gestão, distribuição, utilização, armazenamento e revogação de certificados digitais.

2.2 Componentes e Arquitetura da PKI
PKI Components and Architecture

De acordo com o que está normalizado no RFC5280, a PKI é composta por cinco tipos de componentes:

1. **Entidade terminal ou cliente** – aquela que utiliza os certificados PKI ou sistema a que se refere determinado certificado;
2. **Autoridade Certificadora (ou de Certificação) (AC)** – aquela que emite ou revoga certificados;
3. **Autoridades de Registo Organizacional (ARO)** – um sistema opcional ao qual as ACs delegam certas funções de gestão.
4. **Emissor de Listas de Revogação de Certificados (LRC)** – um sistema que gera e assina LRCs;
5. **E o Repositório** – um sistema ou coleção de sistemas distribuídos que guardam certificados e LRCs, e que servem como um meio de distribuição destes certificados e LRCs a entidades terminais.

Os componentes referidos antes podem estruturar-se como se mostra na figura seguinte, que concretiza a arquitetura da PKI:



2.3 Protocolos da PKI
PKI Protocols

O funcionamento da PKI assenta em dois tipos diferentes de protocolos:

1. **Protocolos Operacionais** – Necessários para entregar certificados e LRCs (ou informação de *status*) a utilizadores cliente do sistema. É necessário recorrer a vários meios para entrega de certificados e LRCs, como procedimentos de distribuição LDAP, HTTP, FTP, e X.500.
2. **Protocolos de Gestão** – Necessários para suportar interações em linha entre utilizadores cliente e entidades de gestão ou entre entidades de gestão. O conjunto de operações que precisam ser suportadas por protocolos de gestão incluem, mas não estão confinadas, às seguintes:
   - Registo;
   - Inicialização;
   - Certificação;
   - Recuperação / atualização de chaves;
   - Pedido de Revogação;
   - Certificação Mútua entre ACs.

As **operações do protocolo de gestão são as que melhor ilustram o funcionamento da PKI**, e explicam-se com um pouco mais de detalhe a seguir:

- **Registo** – processo através do qual um utilizador se faz conhecer à Autoridade de Certificação (diretamente, ou através de um ARO), antes mesmo de ser emitido um ou mais certificados a esse utilizador.
- **Inicialização** – antes que o cliente possa operar de modo seguro, é necessário instalar todo o material relativo a chaves de cifra, relacionadas com as chaves guardadas noutros sítios da infraestrutura (neste processo, o cliente precisa de ser inicializado com uma chave pública e com outra informação relativa à raíz de confiança).
- **Geração de Chaves** – em algumas implementações, a Autoridade de Certificação fornece o serviço de gerar um par de chaves (pública / privada) para o cliente.
- **Certificação** – processo através do qual a Autoridade de Certificação emite um certificado para a chave pública de determinado utilizador, e transmite esse certificado para o cliente ou publica-o num repositório público adequado.
- **Publicação de Certificados e LRCs** – a publicação pode ser feita diretamente pela Autoridade de Certificação, ou indiretamente por entidades como as AROs. Para além de colocar os certificados e LRCs nos repositórios, também é comum tomar as providências necessárias para notificar os utilizadores terminais de qualquer mudança importante.
- **Revogação** – quando um certificado é emitido, a sua validade também é especificada. Contudo, pode ser necessário revogar o certificado antes do tempo por várias razões (e.g., despedimento do empregado, comprometimento da chave privada, etc.). Neste caso, uma entidade autorizada avisa a Autoridade de Certificação que uma situação que requer revogação de determinado certificado ocorreu. O certificado revogado passa então a ser publicado em LRCs.

- **Recuperação de Par de Chaves** – o sistema pode estar, opcionalmente, dotado com a possibilidade de guardar uma cópia do par de chaves dos clientes remotamente. Se um utilizador precisar de as recuperar, um protocolo interativo pode ajudar a verificar se o utilizador é quem ele realmente diz que é, e fornecer-lhe as cópias de segurança.
- **Atualização do Par de Chaves** – todas as chaves de cifra precisam de ser atualizadas com regularidade, i.e., substituídas por um novo par, e os respetivos certificados emitidos.
- **Certificação Cruzada** – duas Autoridades de Certificação trocam informação no sentido de estabelecer um certificado cruzado (adaptação de *cross-certificate*). Um certificado cruzado é um certificado emitido por uma Autoridade de Certificação para outra.

2.4 Caminho de Certificação
Certification Path

Conforme discutido antes, para usar um serviço que dependa do conhecimento de determinada chave pública, o utilizador deve primeiro obter e validar um certificado dessa chave. A utilização da criptografia de chave pública é, portanto, mais complexa por si só. Contudo, há detalhes que ainda não foram discutidos.

Por exemplo, **a validação de um certificado de um utilizador envolve**, **por sua vez**, o **conhecimento da chave pública da AC1 que emitiu o certificado** e, consequentemente, **requer a obtenção do certificado que contém a chave pública do AC**.

1. A validação do certificado do AC1 pode precisar da chave pública **de outro**
   (a) AC2 (que emitiu o certificado para este AC1),
      i. **e assim por diante**.

Esta **cadência de certificados necessários à validação** de uma determinada chave pública é denominada de **caminho de certificação** (*certificate validation path*).

Basicamente, de modo a confiar que determinada chave pública pertence, de facto, a determinada entidade, **é preciso validar o certificado para esta chave, e para uma ou mais Autoridades Certificadoras**.

O processo de validação do caminho verifica, entre outros detalhes, que um caminho de certificação (i.e., uma sequência de n certificados $\{X.509_1, X.509_2, ..., X.509_n\}$) satisfaz as seguintes condições:

- Para todo o x em $\{X.509_1, X.509_2, ..., X.509_n\}$, o *subject* do certificado x_i é *issuer* do certificado x_{i+1};
- **O Certificado 1 é emitido pela Raíz de Confiança.**
- O Certificado n é o certificado que necessita ser validado (i.e., aquele certificado que queremos usar);
- Verifica-se que, para todo o x em $\{X.509_1, X.509_2, ..., X.509_n\}$, o certificado está dentro do prazo de validade.

É claro que, dada a situação, podem imediatamente surgir algumas dúvidas, nomeadamente:

- **Onde é que o caminho acaba? Qual é a Raiz da Confiança?**
- Se cada chave pública precisa de um certificado, e cada certificado necessita de uma chave pública, o que é que vem primeiro, o ovo ou a galinha?

Os caminhos de certificação concretizam, de modo explícito, **uma hierarquia de Autoridades Certificadoras**. As **ACs superiores**, em termos hierárquicos, **emitem certificados de ACs de níveis inferiores**. **No topo da hierarquia descansa serenamente a AC Raiz de Confiança**. Um certificado desta AC **é emitido e assinado por ela própria**, o que basicamente **significa que os campos *subject* e *issuer*** deste certificado contêm **o mesmo valor**.

A confiança depositada na chave pública de uma AC Raiz de Confiança não depende de outra AC. **A confiança é estabelecida por critérios externos à PKI**. Por exemplo, a instalação típica do sistema operativo Windows define, automaticamente, a confiança em dezenas de ACs Raiz de Confiança. O mesmo é válido para *browsers* (e.g., *Mozilla* mantém uma lista de, pelo menos 36 Autoridades de Certificação Raiz de Confiança em `http://www.mozilla.org/projects/security/certs/included/`).

Um utilizador (um *browser*) **conhece um número limitado de chaves públicas** pertencendo a ACs (normalmente ACs raiz — *root* CAs) **em quem confia**. Neste caso, estas ACs são a raiz de confiança. Isto significa que o utilizador passa a aceitar certificados de uma destas ACs e passa a depositar um certo nível de confiança no que esses certificados atestam. Também significa que **a validação de um caminho de certificação termina quando um certificado com essa propriedade (raiz da confiança) é encontrado**. O grau de confiança depositado num certificado validado é baseado na confiança que o utilizador tem relativamente à AC que serviu como raiz.

3 Listas de Revogação de Certificados
Certificate Revogation Lists

Quanto um **certificado** é emitido, espera-se que este esteja em **utilização durante todo** o tempo definido no **período de validade**. Contudo, o certificado **pode tornar-se inválido** durante esse período devido a diferentes motivos, nomeadamente:

1. A mudança do nome (do titular);
2. Mudança de associação entre o titular e a Autoridade de Certificação (e.g., um empregado termina o contrato de trabalho com a empresa que lhe dava o certificado);
3. Ou o comprometimento (ou só suspeita de comprometimento) da chave privada.

Nestas circunstâncias, a Autoridade de Certificação **precisa de um mecanismo que permita revogar certificados antes da sua validade terminar**.

3.1 Definição de Lista de Revogação de Certificados

Definition of Certificate Revogation List

A norma X.509 engloba um mecanismo para revogação de certificados. Este mecanismo requer que cada Autoridade de Certificação emita **uma estrutura de dados chamada Lista de Revogação de Certificados** (LRC) **periodicamente**.

> Uma LRC é **uma lista com selo temporal que identifica certificados revogados**, **é assinada por uma Autoridade de certificação** ou por um emissor dedicado de LRC, e é **disponibilizada num repositório público**.

Cada certificado revogado é **identificado** na LRC **pelo seu número de série**. Quando um sistema-utilizador de certificados usa um certificado, deve sempre:

1. Verificar a assinatura do certificado e a sua validade; Esta verificação inclui, como já foi visto antes, validar a própria assinatura do certificado, bem como os detalhes nele constantes, e os de todos os certificados que formam a cadeia de certificação.
2. **Para além disso**, deve ainda adquirir uma LRC *recente* e verificar se o número de série do certificado que está a usar não está nessa CRL.

O **significado de LRC *recente* pode variar com a política local aplicada**, mas normalmente significa a LRC **emitida mais recentemente**. Uma LRC é emitida **periodicamente** (e.g., hora-a-hora, diariamente ou semanalmente). Uma das vantagens deste método de revogação é que as LRCs podem ser **distribuídas através dos meios usados para os certificados**, nomeadamente via servidores públicos e **canais inseguros**.

A sintaxe de uma LRC representada na figura em baixo. Para o cálculo da assinatura, os dados são codificados na notação ASN.1 DER. Na figura, os campos `signatureAlgorithm` e `signatureValue` têm o mesmo significado que para os certificados.

```
CertificateList  ::=  SEQUENCE  {
    tbsCertList                 TBSCertList,
    signatureAlgorithm          AlgorithmIdentifier,
    signatureValue              BIT STRING  }
```

```
TBSCertList  ::=  SEQUENCE  {
 version                 Version OPTIONAL,
                         (if present, MUST be v2)

 signature               AlgorithmIdentifier,
 issuer                  Name,
 thisUpdate              Time,
 nextUpdate              Time OPTIONAL,

 revokedCertificates SEQUENCE OF SEQUENCE{
    userCertificate      CertificateSerialNumber,
    revocationDate       Time,
    crlEntryExtensions   Extensions OPTIONAL
                         (if present, version MUST be
                             v2)
 } OPTIONAL,

 crlExtensions  [0] EXPLICIT Extensions OPTIONAL
                    (if present, version MUST be v2)
}
```

O campo *version* é opcional, mas quando presente deve ter valor superior a 2, dado que **as LRCs foram introduzidas apenas na segunda versão** do X.509.

As LRCs são emitidas por emissores de LRCs. **Em geral, o emissor de LRCs é a própria Autoridade de Certificação.** As Autoridades de Certificação publicam as LRCs de modo a fornecer o estado dos certificados que elas anteriormente emitiram. Contudo, uma Autoridade de Certificação **pode delegar esta responsabilidade a outra autoridade de confiança** e, nesse caso, a LRC é designada por **LRC indireta**. Cada LRC **tem um âmbito** particular, que é composto pelo **conjunto de certificados que podem aparecer** nessa lista. Por exemplo, o âmbito pode ser *todos os certificados emitidos pela AC X* ou *todos os certificados emitidos pela AC X revogados por motivos de comprometimento de chave.* Também pode ser um conjunto de certificados definido por restrições, e.g., de localidade, como por exemplo *todos os certificados emitidos aos empregados do NIST localizados em Boulder*.

Qual pode ser a **causa que leva à revogação de uma grande quantidade** de certificados digitais simultaneamente?

3.2 LRCs Base e Delta

Base and Delta CRLs

Uma LRC pode ser de um de **dois tipos** possíveis:

- Uma LRC **completa** lista **todos** (dentro do seu domínio de atuação) os certificados que ainda não expiraram mas que foram revogados por uma das razões de revogação cobertas no âmbito da LRC. **Esta lista completa é normalmente designada por LRC Base**.
- Uma **LRC *Delta*** lista **apenas** aqueles certificados que, dentro do seu domínio de atuação, **mudaram o**

seu estado relativo à revogação (ou ficaram revogados, ou saíram da revogação), **desde a emissão de uma LRC Base**. O **âmbito** de uma LRC *Delta* **deve ser o mesmo que** o âmbito da **LRC Base** que referência.

Nota: o conteúdo exposto na aula e aqui contido não é (nem deve ser considerado) suficiente para total entendimento do conteúdo programático desta unidade curricular e deve ser complementado com algum empenho e investigação pessoal.