Criptografia

Módulo II – Certificação e Public Key Infrastructure

M. B. Barbosa
mbb@di.uminho.pt

Departamento de Informática
Universidade do Minho

2006/2007

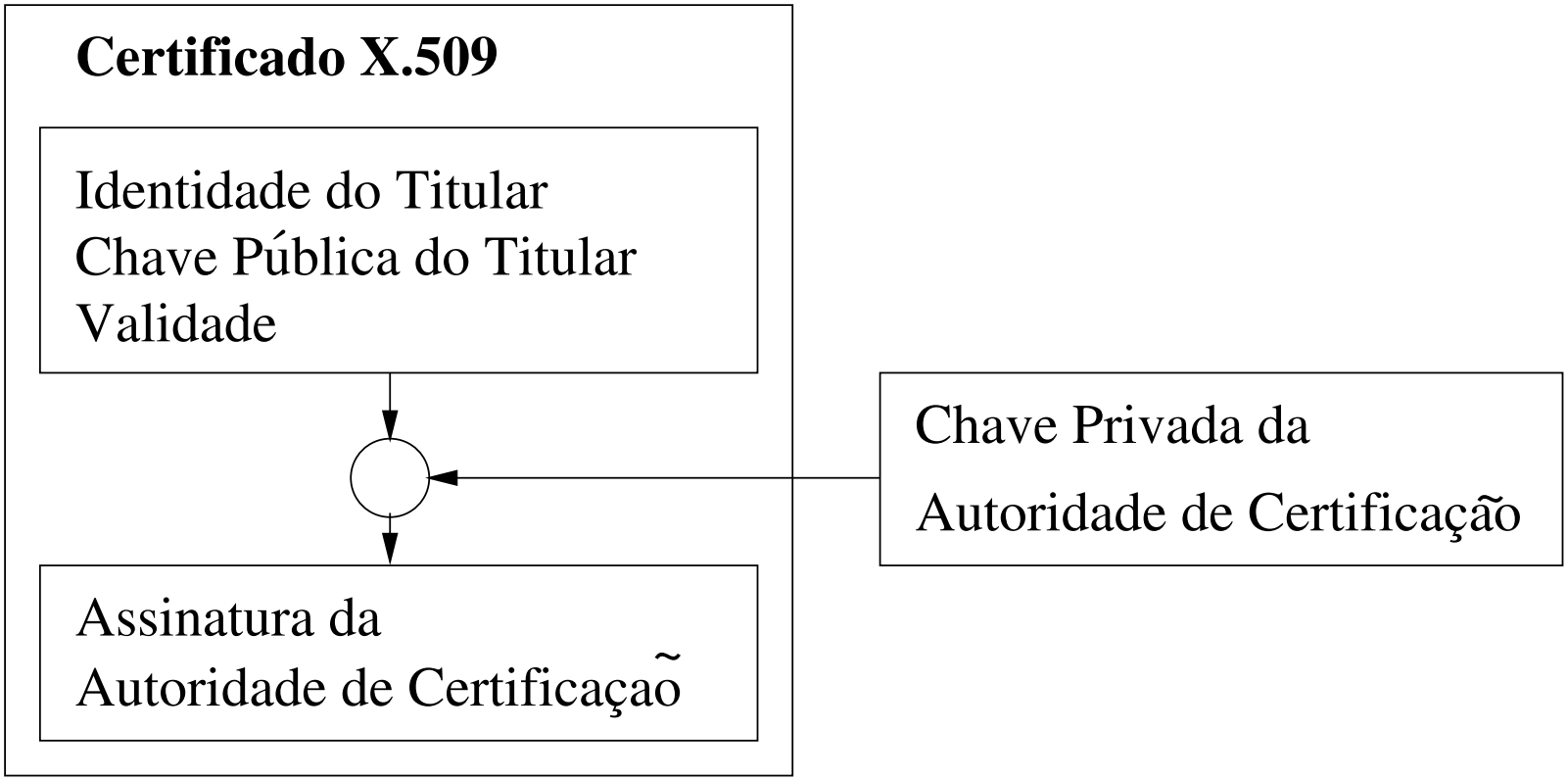
Introdução

- Esforços recentes para melhorar a segurança na Internet levaram ao aparecimento de um grupo de protocolos (S/MIME, IPSec, etc.) que utilizam a criptografia de chave pública para garantir:
  - Confidencialidade
  - Integridade
  - Autenticação
  - Não repúdio.
- Esta utilização baseia-se no conceito de Certificado (de chave pública ou de atributos).
- A Public Key Infrastructure (PKI) tem como objectivo a gestão segura e eficiente de chaves e certificados para permitir essa mesma utilização.

- A utilização da criptografia de chave pública nas telecomunicações é regulamentada pela recomendação X.509 da International Telecommunications Union (ITU).
- A aplicação dessa recomendação à Internet está definida num conjunto de Requests For Comments (RFCs) publicados pela IETF.
- A Internet Engineering Task Force é uma comunidade internacional de produtores, operadores, vendedores e investigadores das tecnologias de redes, interessados no funcionamento e evolução da Internet.
- Dentro da IETF, o grupo que gere os RFCs relacionados com o X.509 chama-se "*PKIX Working Group*". Este grupo de trabalho mantém um conjunto de documentos que se denomina "*Internet X.509 Public Key Infrastructure*".

Certificados de Chave Pública

- Os utilizadores numa PKI devem poder confiar que, cada vez que utilizam uma chave pública, o agente com quem querem comunicar possui a chave privada associada.
- Esta confiança é construída com base em Certificados de Chave Pública.
- Um Certificado de Chave Pública é uma estrutura de dados que associa uma chave pública a um determinado agente (a uma representação da sua identidade).
- A associação chave/agente é estabelecida por uma entidade terceira, uma Autoridade de Certificação, que assina digitalmente cada certificado.
- A utilidade de um certificado depende unicamente da **confiança** depositada na Autoridade de Certificação.


Certificado X.509
Identidade do Titular
Chave Pública do Titular
Validade
Assinatura da
Autoridade de Certificaçaõ
Chave Privada da
Autoridade de Certificação

- O utilizador do certificado confia que a Autoridade de Certificação verificou que a chave pública contida no certificado pertence de facto ao titular do certificado.
- A assinatura da Autoridade de Certificação assegura a autenticidade e integridade do certificado.
- Um Certificado de Chave Pública é válido durante um período de tempo bem definido. Esse período vem especificado no conteúdo assinado.
- Como a assinatura e a validade temporal de um certificado podem ser verificados independentemente por um utilizador, os certificados podem ser distribuídos por canais inseguros. Será isto verdade para todos os certificados?

- Os Certificados de Chave Pública são utilizados maioritariamente na validação de informação assinada digitalmente. Este processo consiste geralmente nos seguintes passos:
  1. O destinatário verifica que a identidade indicada pelo emissor está de acordo com a identidade indicada no certificado.
  2. O destinatário verifica que o certificado é **válido**:
     - que a assinatura do certificado é válida;
     - que foi efectuada por uma autoridade de certificação de confiança;
     - que o certificado está dentro do seu período de validade.
  3. O destinatário verifica que a informação que recebe está de acordo com as permissões/privilégios do emissor.
  4. O destinatário utiliza a chave pública contida no certificado para verificar a assinatura da informação recebida.

- Os Certificados de Chave Pública são utilizados maioritariamente na validação de informação assinada digitalmente. Este processo consiste geralmente nos seguintes passos:
  1. O destinatário verifica que a identidade indicada pelo emissor está de acordo com a identidade indicada no certificado.
  2. O destinatário verifica que o certificado é **válido**:
     - que a assinatura do certificado é válida;
     - que foi efectuada por uma autoridade de certificação de confiança;
     - que o certificado está dentro do seu período de validade.
  3. O destinatário verifica que a informação que recebe está de acordo com as permissões/privilégios do emissor.
  4. O destinatário utiliza a chave pública contida no certificado para verificar a assinatura da informação recebida.

- Se todos os passos anteriores forem executados sem problemas, o destinatário aceita que a informação foi assinada pelo emissor, e que essa informação permanece inalterada.
- Como é que se utiliza um certificado para proteger informação ao nível da confidencialidade?
- O certificado passa a ser utilizado pelo emissor, e contém informação relativa ao destinatário:
  1. o emissor valida o certificado e a identidade do destinatário;
  2. o emissor utiliza a chave pública contida no certificado para cifrar a informação;
  3. o emissor envia a informação cifrada ao destinatário que a decifra com a sua chave privada.

- Se todos os passos anteriores forem executados sem problemas, o destinatário aceita que a informação foi assinada pelo emissor, e que essa informação permanece inalterada.
- Como é que se utiliza um certificado para proteger informação ao nível da confidencialidade?
- O certificado passa a ser utilizado pelo emissor, e contém informação relativa ao destinatário:
  1. o emissor valida o certificado e a identidade do destinatário;
  2. o emissor utiliza a chave pública contida no certificado para cifrar a informação;
  3. o emissor envia a informação cifrada ao destinatário que a decifra com a sua chave privada.

Certificados X.509 (V1)

- Surgiram em 1988 com a primeira versão do X.509. Um certificado deste tipo contém os seguintes campos:
  - **Version** version
  - **CertificateSerialNumber** serialNumber
  - **AlgorithmIdentifier** signature
  - **Name** issuer
  - **Validity** validity
  - **Name** subject
  - **SubjectPublicKeyInfo** subjectPublicKeyInfo
- A assinatura do certificado é efectuada pela Autoridade de Certificação (CA) sobre uma codificação DER da representação desta estrutura de dados em ASN.1.

Certificados X.509 (V2)

- Surgiram na revisão de 1993 do X.509. Não chegaram a ser muito utilizados porque pouco tempo depois surgiu a versão actual (V3).
- Foram introduzidos dois novos campos:
  - **UniqueIdentifier** issuerUniqueID
  - **UniqueIdentifier** subjectUniqueID
- Estes campos tentam rectificar o problema de ser muito difícil garantir que os campos do tipo **Name** tenham valores únicos.
- A IETF recomenda que as CAs não utilizem estes campos e garantam, na medida do possível, a unicidade dos nomes. Por outro lado recomenda que estes campos, caso existam, não devem ser ignorados.

Certificados X.509 (V3)

- Esta é a versão utilizada hoje em dia. Foi standardizada em 1996 e é compatível com as versões anteriores.
- Esta versão veio colmatar as deficiências que as versões anteriores apresentavam para algumas aplicações e que consistiam básicamente na necessidade de mais atributos.
- Como inovação, esta versão introduziu um novo campo do tipo **Extensions**: uma colecção de elementos do tipo **Extension**.
- As extensões permitem associar atributos genéricos a um agente ou à sua chave pública, de forma flexível.
- Cada extensão é ela própria uma estrutura de dados com um identificador e um valor adequado ao tipo do atributo que representa.

Certificados X.509 (V3): Atributos

- **version** Tem de estar de acordo com o conteúdo do certificado.
- **serialNumber** Número único atribuido pela CA.
- **signature** Estrutura que identifica o algoritmo utilizado para gerar a assinatura da CA que acompanha o certificado.
- **validity** Estrutura com as duas datas que delimitam o período de validade do certificado.
- **subjectPublicKeyInfo** Estrutura contendo a chave pública do titular do certificado e identificação do algoritmo correspondente.

- Os atributos **issuer** e **subject** identificam a CA e o titular do certificado respectivamente. Ambos são do tipo **Name**.
- O tipo **Name** provém da norma X.501 e é utilizado porque permite a compatibilidade com os sistemas de directório definidos nas normas X.500 (e.g. DAP e LDAP).
- O tipo **Name** é uma colecção de atributos, geralmente *strings* da forma "$< nome > = < valor >$". Estes atributos definem um **Distinguished Name** para o agente titular.
- O **Distinguished Name** tem uma estrutura hierárquica. Inclui por exemplo, o país, a organização e o nome próprio do agente ou entidade.

- A norma X.520 standardiza alguns dos componentes de um Distinguished Name. Os seguintes são de reconhecimento obrigatório e são muito utilizados:
  - country (C)
  - organization (O)
  - organizational-unit (OU)
  - common name (CN)
  - serial number (SN)
- Algumas aplicações importantes utilizam também o endereço de e-mail como um dos atributos centrais da construção do Distinguished Name.
- Exemplo: C=PT, O=UMINHO, OU=DI, CN=MBB

Certificados X.509 (V3): Extensões

- As extensões são marcadas como **Critical** ou **Non Critical**.
- Uma aplicação que encontre uma extensão crítica que não reconheça tem de rejeitar o certificado.
- Não são permitidas várias instâncias da mesma extensão.
- O RFC3280 da IETF normaliza as extensões recomendadas para utilização na Internet, definindo o identificador (OBJECT IDENTIFIER) e o tipo de dados associado.
- São desaconcelhados desvios desta recomendação, nomeadamente no que diz respeito a extensões críticas, apesar de não haver qualquer limitação a nível do standard.

- **Subject Key Identifier** Serve para identificar o certificado que contém uma determinada chave pública e.g. quando um agente tem várias. É, em geral, um valor de hash derivado da chave pública que, caso esta extensão não conste do certificado, pode ser calculado em run-time.
- **Authority Key Identifier** Serve para identificar a chave pública da CA que assinou o certificado, caso existam várias, o que facilita a verificação de cadeias de certificação. Isto pode ser feito
  - identificando o certificado da CA através do seu **Subject** e **Serial Number**;
  - ou através da extensão **Subject Key Identifier** do certificado da CA.
- **Subject/Issuer Alternative Name** Permitem associar formas de identificação alternativas ao titular do certificado ou à CA que o emitiu (e-mail, DNS, endereço IP, URI, etc.).

- **Basic Constraints** Permite assinalar um certificado como pertencendo a uma CA e limitar o comprimento de cadeias de certificados.
- **Certificate Policies** Permite incluir informação relativa às políticas de certificação aplicáveis ao certificado:
  - Para certificados de utilizador, permite especificar em que condições o certificado foi emitido e quais as restrições associadas à sua utilização.
  - Para certificados de CAs, permite definir as políticas de certificação aplicaveis por CAs hierarquicamente inferiores.
- **Policy Mappings** Permite a uma CA declarar que algumas das suas políticas são equivalentes às políticas de certificação de outra CA.

(As hierarquias de CAs serão estudadas mais tarde.)

- **Key Usage** Permite restringir as utilizações do par de chaves associado ao certificado e.g. quando uma chave apenas pode ser utilizada para verificar assinaturas digitais. Contempla as seguintes utilizações:
  - **digitalSignature** Assinaturas digitais para autenticação e integridade de dados, excepto certificados e CRLs.
  - **nonRepudiation** Assinaturas digitais para não repúdio.
  - **keyEncipherment** Protecção da confidencialidade de chaves.
  - **dataEncipherment** Protecção da confidencialidade de dados.
  - **keyAgreement** Protocolos de acordo de chaves.
  - **keyCertSign** Assinatura de certificados.
  - **cRLSign** Assinatura de CRLs.
  - **encipherOnly**/**decipherOnly** Restringem a funcionalidade **keyAgreement**.

- **Extended Key Usage** Permite especificar ou restringir as utilizações previstas para o par de chaves associado ao certificado, em adição ou em alternativa à extensão **Key Usage**. Estão definidas diversas utilizações, bem como a sua relação com as especificadas na extensão **Key Usage**:
  - WWW server authentication
  - WWW client authentication
  - Signing of downloadable executable code
  - E-mail protection
  - ...
- **CRL Distribution Points** Serve para indicar ao utilizador de um certificado onde pode obter informação quanto à revogação do certificado na forma de **Certificate Revocation Lists** (CRLs).

Certificados X.509 (V3): Codificação

- Os certificados, como todas as estruturas de dados na PKI, são definidos e representados em ASN.1. A codificação é feita utilizando as Dinstinguished Encoding Rules (DER).
- O ficheiro que contém um certificado X.509 consiste na codificação DER da seguinte estrutura ASN.1:

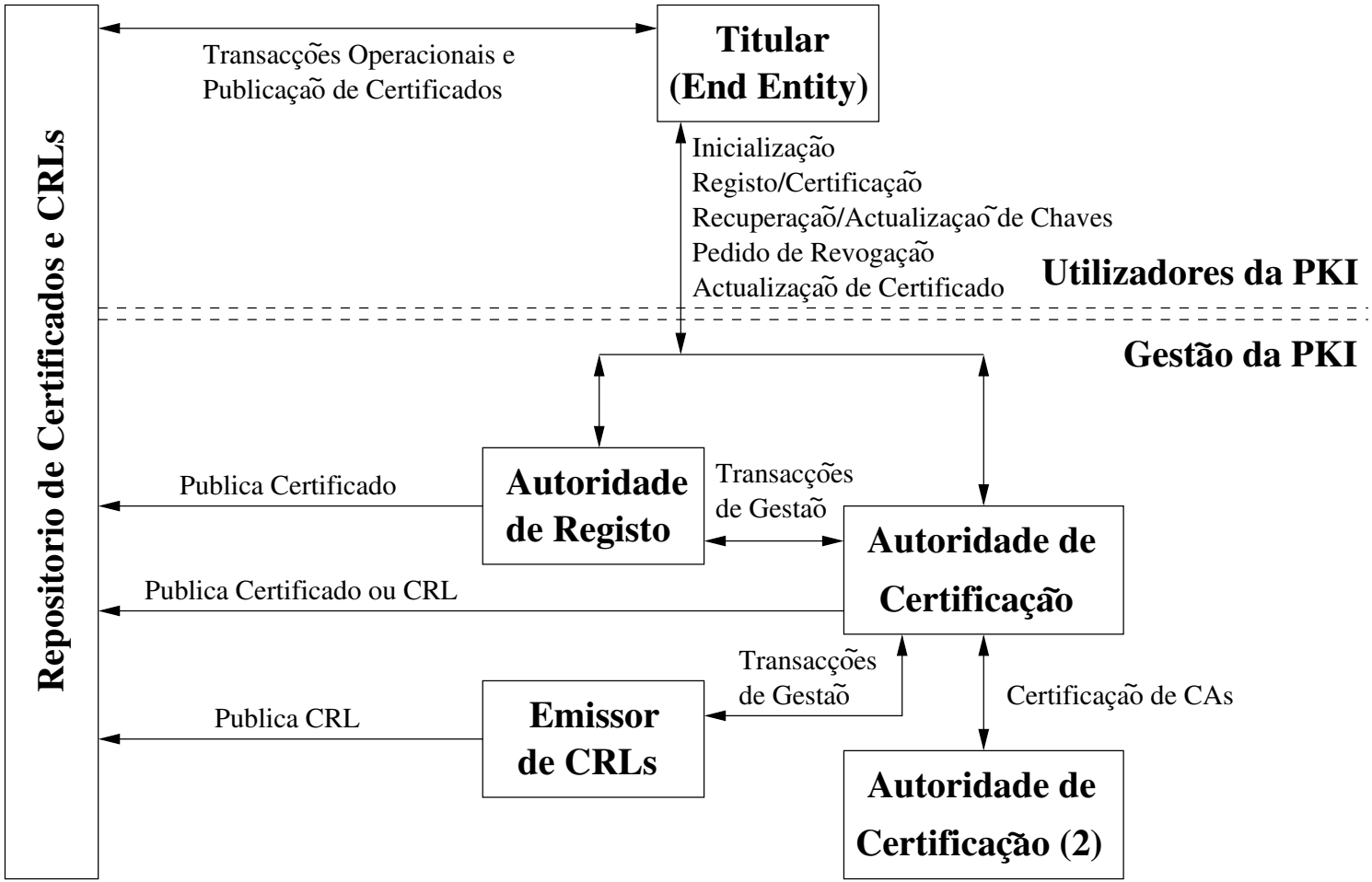
```
Certificate  ::=  SEQUENCE  {
       tbsCertificate       TBSCertificate,
       signatureAlgorithm   AlgorithmIdentifier,
       signatureValue       BIT STRING  }
```

- Além da estrutura de atributos apresentada nos slides anteriores (**tbsCertificate**), aparece também a assinatura da Autoridade de Certificação (**signatureAlgorithm** e **signatureValue**).

Introdução

- Uma Public Key Infrastructure define-se como o conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerir, armazenar, distribuir e revogar Certificados de Chave Pública.
- Uma PKI é composta por cinco tipos de componentes:
  - **Titulares de Certificados** Possuem as chaves privadas e as utilizam para decifrar mensagens e assinar documentos.
  - **Clientes** Utilizam a chave pública contida num certificado para cifrar mensagens e verificar assinaturas.
  - **Autoridades de Certificação** Emitem e revogam certificados.
  - **Autoridades de Registo** Garantem a associação entre chaves públicas e identidades de titulares (são opcionais).
  - **Repositórios** Armazenam e disponibilizam certificados e CRLs.

Arquitectura



- O funcionamento de uma PKI baseia-se em dois tipos de protocolos:
  - **Protocolos Operacionais** Estes protocolos são necessários para entregar certificados e CRLs aos sistemas que os utilizam. Estas operações podem ser efectuadas de diversas formas, incluindo o LDAP, HTTP e FTP. Para todos estes meios estão especificados protocolos operacionais que definem, inclusivamente, os formatos das mensagens.
  - **Protocolos de Gestão** Estes protocolos são necessários para dar suporte às interacções entre os utilizadores e as entidades de gestão da PKI, nomeadamente:
    - Inicialização.
    - Registo e Certificação.
    - Recuperação e Actualização de pares de chaves.
    - Pedido de revogação.
    - Certificação de CAs.

PKI: Operações

- **Inicialização** Processo inicial que permite ao utilizador comunicar com a PKI: toma conhecimento das CAs em que confia e adquire as chaves públicas e certificados correspondentes, gera o seu par de chaves, etc.
- **Registo** Um utilizador dá-se a conhecer a uma CA (directamente, ou através de uma RA) para que a CA lhe possa emitir um certificado; para isso fornece informação de identificação que deve ser verificada pela CA (RA).
- **Geração de Par de Chaves** Nalgumas implementações, as CAs encarregam-se de gerar o par de chaves.
- **Certificação** A CA recebe a chave pública do utilizador e a sua identificação e emite o respectivo certificado, segundo regras internas.

- **Publicação de Certificados e CRLs** Esta tarefa pode ser feita directamente pela CA, ou indirectamente por entidades como RAs. Além de colocar os certificados e CRLs em repositórios é muitas vezes necessário fazer estes documentos chegar aos utilizadores finais por outros meios (on-line ou não).
- **Revogação** Quando um certificado é emitido o seu período util de vida está pré-definido. No entanto, pode haver a necessidade de invalidar o certificado antes do fim desse período por diversos motivos (e.g. um despedimento, o comprometimento da chave privada, etc.). A revogação de certificados faz-se através de CRLs. As CRLs vão ser analizadas em detalhe mais tarde.

- **Recuperação de um Par de Chaves** Nalgumas implementações as CAs armazenam o par de chaves da entidade como *back-up* e protecção e.g. no caso de uma empresa e os seus empregados. Nestes casos o par de chaves pode ser restaurado em caso de extravio ou danificação do seu suporte.
- **Actualização de Par de Chaves** Todos os pares de chaves precisam de ser alterados, periódicamente por razões de segurança, ou simplesmente porque a segurança da chave privada foi corrompida.
- **Certificação de CAs** Os certificados das CAs chamam-se **cross certificates**. São utilizados para a validação de cadeias de certificados, mas também podem ser utilizados para outros fins e.g. comunicação segura entre uma entidade e a CA.

Cadeias de Certificação e Confiança

- Para utilizar um serviço que requeira o conhecimento de uma chave pública, é necessário obter e validar um certificado que a contenha.
- A validação do certificado implica, por sua vez, o conhecimento da chave pública da Autoridade de Certificação que o emitiu e, consequentemente, a obtenção e validação do certificado que a contém.
- A validação do certificado da CA poderá implicar o conhecimento da Chave Pública de outra CA que o tenha emitido, e assim sucessivamente.
- Chama-se a esta sequência uma **Cadeia de Certificação**.
- Confiança numa chave pública implica validar o certificado dessa chave, e zero ou mais certificados de CAs.

- A validação de um certificado segue o seguinte algoritmo:
  - Para todo o $x = 1, ..., n-1$, o `subject` do certificado x é o emissor do certificado $x+1$;
  - O certificado 1 é emitido pela **raiz da relação de confiança**;
  - O certificado n é o certificado a ser validado; e ...
  - Para todo o $x = 1, ..., n$, verifica-se que o certificado é válido na altura da sua utilização.
- Perguntas:
  - Onde termina a validação de uma cadeia de certificados?
  - O que é a raiz da relação de confiança?
  - Se cada chave pública implica um certificado, e vice-versa, o que aparece primeiro?

- As cadeias de certificação reflectem uma **hierarquia** de Autoridades de Certificação.
- As CAs hierarquicamente superiores emitem os certificados das CAs hierarquicamente inferiores.
- No topo da hierarquia reside uma CA denominada **Root** ou raiz. O certificado desta CA é emitido e assinado por ela própria: os campos `subject` e `issuer` do seu certificado são iguais.
- A confiança na chave pública de uma Root CA **não depende** de outra CA. é estabelecida por um meio externo à PKI.
- Por exemplo, a utilização de uma instalação comum do MS Windows implica a "confiança" em dezenas de Root CAs!

- Um utilizador conhece um número limitado de chaves públicas pertencentes a CAs (em geral Root CAs) e que funcionam como raizes das relações de confiança.
- Isso significa que o utilizador aceitará um certificado emitido por uma dessas CAs e que depositará um determinado nível de confiança no seu conteúdo.
- A validação de uma cadeia de certificados terminará quando for encontrado um certificado com essa característica.
- Conclusão: o grau de confiança depositada num certificado validado baseia-se apenas na confiança depositada na CA que funcionou como raiz da relação de confiança.

Políticas de Certificação

- A confiança que é depositada numa CA depende, em última instância, da sua política de certificação, e da forma como essa política é implementada.
- Essa confiança é influenciada por diversos factores internos e externos à PKI. Factores externos, como a credibilidade da instituição ou empresa que suporta a CA e o seu país de origem são obviamente importantes.
- No entanto, o conceito de PKI prevê uma forma de "ancorar"a confiança que se deposita numa CA, naquilo que de facto importa: as leis da sociedade em que a PKI opera.
- Isto é feito através das **Certificate Policies** ou CP.

Certificate Policies

- Uma CP é um conjunto de regras que define a aplicabilidade de certificados a uma determinada comunidade ou classe de aplicações:
  - A legislação em que se baseará a emissão e utilização dos certificados.
  - Os requisitos e as responsabilidades (nomeadamente legais e financeiras) associados a CAs e RAs.
  - Os requisitos e as responsabilidades associados a Titulares e Clientes.
  - Restrições ao conteúdo e utilização dos certificados e.g. somas máximas envolvidas numa transacção, etc.
  - Procedimentos a serem implementados relativamente a diversos aspectos do funcionamento de CAs e RAs.
- Cada CP é identificada por um `Object Identifier` que pode ser incluido na extensão **Certificate Policies**.

Certification Practice Statements

- Cada CA publica uma ou mais **Certification Practice Statements** (CPS), nas quais publicita as suas normas de operação internas. Uma CPS explica a forma como uma CA implementa um determinado conjunto de **CPs**.
- A acreditação de uma CA de acordo com uma determinada CPS implica uma auditoria efectuada por (ou em nome de) uma **Policy Management Authority**.
- Por exemplo, a PKI Governamental do Canadá define oito CPs correspondentes a quatro níveis de segurança na utilização de certificados em assinaturas digitais e protecção de dados. Uma CA que pretenda emitir certificados que em conformidade com estas políticas tem de ser credenciada pelo estado Canadiano.

Políticas de Certificação na Prática

- Uma parte significativa do RFC3280 é dedicada às políticas de certificação e ao efeito de uma política de certificação imposta num determinado ponto da hierarquia.
- Como foi já referido, esta especificação define também as extensões que permitem incluir este tipo de informação nos certificados X.509.
- De facto, associada a cada certificado pode estar uma lista de políticas aplicáveis à sua utilização ou, no caso do certificado de uma CA, uma lista das políticas aceitáveis para os certificados hierarquicamente inferiores.
- Durante a validação de um certificado é necessário propagar as políticas impostas desde o topo da hierarquia até à sua base.

- A informação contida nos certificados inclui uma componente processável num algoritmo de resolução deste problema, algoritmo esse que está também definido no RFC3280.
- A política em vigor na base da hierarquia de certificação resulta da reunião das políticas em vigor nos níveis superiores, com a ressalva de que uma política inserida num determinado nível não pode contradizer uma política de nível superior.
- Compete ao utilizador determinar se a política associada a um determinado certificado é aceitável ou não.
- É também possível incluir num certificado uma CPS, de forma directa ou referenciada, bem como informação dirigida ao utilizador final sobre as condições de emissão do certificado.