

Certificados Digitais

Tecnologia Criptográfica

José Bacelar Almeida (jba@di.uminho.pt)
Universidade do Minho



Plano

1. Arquitectura e aspectos operacionais
2. Certificados X509
3. Perfis e Políticas de Certificados
4. Revogação de Certificados e OCSP

...relembrando...

- › A combinação de técnicas criptográficas simétricas e assimétricas permite ultrapassar um aspecto crítico limitativo da aplicabilidade em larga escala das primeiras – **a pré-distribuição de chaves**.
- › Mas a segurança das segundas depende da correcta associação entre chaves públicas e identidades.
- › Para garantir essas associações, faz-se uso de uma entidade externa de confiança (EC):
 - Os Certificados de Chave Pública, assinados pela EC, atestam essa associação;
 - Os utilizadores aceitam como válida essa associação (por via da confiança depositada na EC).
- › Os utilizadores, de cada vez que necessitarem de uma chave pública, solicitam o respectivo certificado:
 - Confirmam a validade do certificado verificando a assinatura nele contido
 - utilizando para isso a chave pública da EC (essa sim, terá de ser distribuída de forma segura)



3

- › Não são necessários canais seguros para transmitir os certificados
- › Interessa reforçar o papel crítico que as Entidade de Certificação exercem na segurança de todo o sistema.

?e porquê?

- › É por isso normal impôr-se nas ECs padrões de segurança muito elevados (utilização de HSMs; segurança física; planos de segurança rigorosos; etc.)
- › Para operacionalizar todos estes aspectos, torna-se necessário fixar toda uma série de formatos, regras e procedimentos relativos aos mecanismos de certificação das chaves públicas que são adoptados pela comunidade – a **Infraestrutura de Chave Pública (ICP)**

4



Infra-estrutura de Chave Pública (ICP) (*Public-Key Infrastructure - PKI*)

5



Preâmbulo

6



Enquadramento

- › A utilização em larga escala de Certificados de Chave Pública pressupõe uma base sólida de fixação e sistematização de:
 - Formatos e tecnologia;
 - Convenções e assumpções;
 - Práticas e procedimentos;
 - Enquadramento normativo e legal;
 - Etc.
- › De facto, uma ICP faz a ponte entre conceitos e elementos de natureza tecnológica (chaves criptográficas) com aspectos que no limite detém um cariz "social" (identidade; individualidade; personalidade).
- › Por outro lado, e quando considerada em toda a sua abrangência, envolve questões que tocam aspectos tão diversos quanto:
 - Tecnológicos (especificação de formatos, protocolos, etc.);
 - Comerciais (direitos de propriedade, vantagens competitivas, cotas de mercado, etc.);
 - Políticas (supervisão e controlo, jurisdição, soberania, etc.)
 - ...

7



- › Trata-se pois de um área que, em grande medida, tem evoluído em resposta a estímulos localizados e bem sucedidos na solução de problemas concretos, que depois de suficientemente estabilizados/amadurecidos são "adoptados" para abordar questões mais abrangentes...
 1. Definições básicas: âmbito e objectivos; formatos; codificações; etc.
 2. Processos: interações ao nível dos intervenientes "locais" (EC e utilizadores); operações e ciclo de vida; protocolos de gestão; etc.
 3. Inter-operacionalidade: mecanismos de interação e inter-relação entre diferentes utilizações e comunidades; impacto nas relações de confiança e validade; etc.
 4. Regulamentação e acreditação: boas práticas, regras, organismos, etc.
 5. Enquadramento legal: jurisdisção, direitos e responsabilidades; valor jurídico de operações electrónicos; etc.
 6. ICPs públicas: suporte aos organismos actividades dos estados e cidadãos

8



Origem Histórica

- › O primeiro esforço bem sucedido para standardização dos Certificados de Chave Pública aconteceu no âmbito dos protocolos associados ao serviço de directoria X500. Em 1988, surge o standard X509 responsável por estabelecer os mecanismos de autenticação para o X500.
- › Por se tratar da primeira proposta abrangente e sistemática para o mecanismo de certificação, acabou por servir de base para muito do trabalho de normalização e standardização relacionado com ICP.
- › É assim que hoje, os Certificados X509 estão na base de praticamente todas as abordagens à ICP (com honrosas excepções, como o esquema de certificação do PGP).
- › O Grupo de Trabalho IETF-PKIX-WG foi constituído em 1995 para promover o desenvolvimento de standards técnicos (RFCs) que suportassem a ICP baseada em certificados X509



- › O PKIX-WG, assim como outros organismos e consórcios (e.g. NIST, W3C, ...), produziu um vasto conjunto de documentos que constituem o suporte tecnológico para a ICP (e.g. <https://datatracker.ietf.org/wg/pkix/documents/>)
- › Certos domínios de aplicação exerceram também um papel catalizador na adopção das propostas tecnológicas que iam sendo desenvolvidas (como navegação segura na web, correio electrónico, etc.), promovendo elas próprias avanços nessas tecnologias.
- › Em termos comerciais, a área atraiu muita interesse, assistindo-se a uma explosão da oferta de serviços, e contribuindo para a sua consolidação.
- › Por último, assistiu-se também a um impulso significativo promovido por organismos públicos (e.g. as iniciativas da Comunidade Europeia na promoção da economia digital, etc.), que alargaram a adopção e aplicabilidade da tecnologia.

Âmbito das ICP

- › Interessa reforçar que, mesmo com todo o volume de normas e standards que prevêem ICPs de âmbito verdadeiramente global, continua a fazer sentido considerarem-se ICPs de âmbito local com atribuições específicas
- › Os requisitos e os procedimentos são nesses casos ajustados de acordo com a criticidade do sistema
- › Diferentes âmbitos para uma EC:
 - EC *in-house* (doméstica)
 - EC comercial
 - EC em *outsourcing*
 - EC comercial com atribuições especiais
 - EC pública



EC *in-house*

- › EC criada para dar resposta à necessidade de certificação locais à organização.
- › Requisitos e procedimentos associados à EC são normalmente muito simplificados, que resulta num ponto de falha crítico para segurança do sistema.
- › Por norma, é benéfico adoptar os mesmos formatos/procedimentos/etc. estabelecidos pelos standards, por forma a permitir a (re)utilização de software standard.
- › Vantagens:
 - Flexibilidade
 - Cadeia de confiança não depende de terceiros
 - Começa a existir suporte nos sistemas operativos
- › Desvantagens:
 - Requer recursos humanos qualificados
 - Tendência para “relaxar demasiado” aspectos da segurança
- › Utilizações típicas:
 - Projectos piloto
 - Segurança de Intranets

EC comercial

- › Empresas comerciais que fornecem o serviço de emitirem certificados de chave pública
- › Por regra, essas entidades estão acreditadas para o efeito, pelo que é credível que ofereçam níveis de credibilidade/segurança aceitáveis
- › Organismos “adquirem” os certificados que necessitam dessas ECs
- › Vantagens:
 - Simplicidade e baixo custo
 - Grande oferta (escolha)
 - Garantia de padrões de segurança/qualidade
 - Certificados das ECs são por norma válidos na configurações standard dos sistemas operativos
- › Desvantagens:
 - Dependência de terceiros na cadeia de confiança
- › Utilizações típicas:
 - Sítio de comércio electrónico
 - Email seguro

13



EC em *outsourcing*

- › Um serviço que as empresas certificadoras também oferecem é o de alojarem/gerirem ECs de clientes
- › Dessa forma, recursos e know-how é da empresa certificadora, sendo que o controlo sobre os certificados emitidos se mantém no cliente
- › Vantagens:
 - Controle sobre a EC
 - Garantia de padrões de segurança/qualidade
 - Certificados das ECs são por norma válidos na configurações standard dos sistemas operativos
- › Desvantagens:
 - Custo
 - Dependência de terceiros na cadeia de segurança
- › Utilizações típicas:
 - Certificados para colaboradores/serviços de uma organização (email, TLS, etc.)

14



EC comercial com atribuições especiais

- › Certas empresas de certificação estão habilitadas a emitir certificados com atribuições especiais
- › Normalmente, pressupõe um processo de acreditação específico.
- › O suporte desses certificados é muitas vezes um *token criptográfico* (e.g. *smartcard*)
- › Vantagens:
 - Ter acesso à atribuição especial concreta...
 - ECs estão por norma obrigadas a requisitos específicos e/ou mais apertados.
- › Desvantagens:
 - Escolha limitada (ou inexistente)
- › Utilizações típicas:
 - Emissão de certificados qualificados (aptos para assinatura qualificada)
 - Certificados para *code-signing* em sistemas fechados

15



EC pública

- › EC da responsabilidade de organismos públicos para suprir necessidades próprias
- › Ainda que, muitas vezes, sejam geridas em regime de *outsourcing* por entidades privadas
- › Utilizações típicas:
 - Emissão de certificados para documentos electrónicos (e.g. cartão cidadão, passaporte, etc.)

16



Organismos do Estado Português relacionados com a Certificação Digital

- › Entidade responsável pela credenciação das Entidades de Certificação em Portugal é o Gabinete Nacional de Segurança.
- › A lista das Entidades de Certificação credenciadas encontra-se disponível em <http://www.gns.gov.pt/trusted-lists.aspx>.
- › Entidade Certificadora Comum do Estado (CEGER) — entidade responsável pelo sistema de certificação electrónica do estado, servindo de topo à hierarquia das ECs dos organismos públicos, como sejam:
 - Entidade de Certificação do Cartão de Cidadão
 - Passaporte Electrónico Português
 - Entidade certificadora do Ministério da Justiça
 - Rede Nacional de Segurança Interna

17



Arquitectura de uma ICP

18



Normas e Standards

- › O esforço de normalização, standardização e regulação das ICPs é levado a cabo por organismos internacionais com competências nas diferentes áreas envolvidas. Ao nível técnico, destacam-se:
 - International Telecommunications Union (ITU), responsável pela recomendação X.509 que introduz a utilização de certificados em sistemas de telecomunicações;
 - Internet Engineering Task Force (IETF), uma comunidade internacional de produtores, operadores, vendedores e investigadores das tecnologias de redes, que são responsáveis por expressar a aplicação das tecnologias criptográficas num conjunto de Requests For Comments (RFCs);
 - PKIX Working Group, um grupo da IETF que gere os RFCs relacionados com os certificados X.509. Este grupo de trabalho mantém um conjunto de documentos que se denomina "Internet X.509 Public Key Infrastructure";
 - ETSI – European Telecommunications Standard Institute, responsável pela standardização Europeia nas áreas das tecnologias de informação e comunicação.

19



Infraestrutura de Chave Pública (ICP)

- › Uma **Infraestrutura de Chave Pública (ICP)** define-se como o conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerir, armazenar, distribuir e revogar **Certificados de Chave Pública**.
- › Intervêm numa ICP diferentes entidades:
 - **Titulares de Certificados:** possuem as respectivas chaves privadas que utilizam para decifrar mensagens ou produzir assinaturas digitais.
 - **Clientes:** Utilizam a chave pública contida num certificado para cifrar mensagens e verificar assinaturas.
 - **Entidades de Certificação:** Emitem/renovam/revogam certificados.
 - **Autoridades de Registo:** Garantem a associação entre chaves públicas e identidades de titulares (opcionais).
 - **Repositórios:** Armazenam e disponibilizam certificados e outra informação relevante (como certificados revogados, etc.).

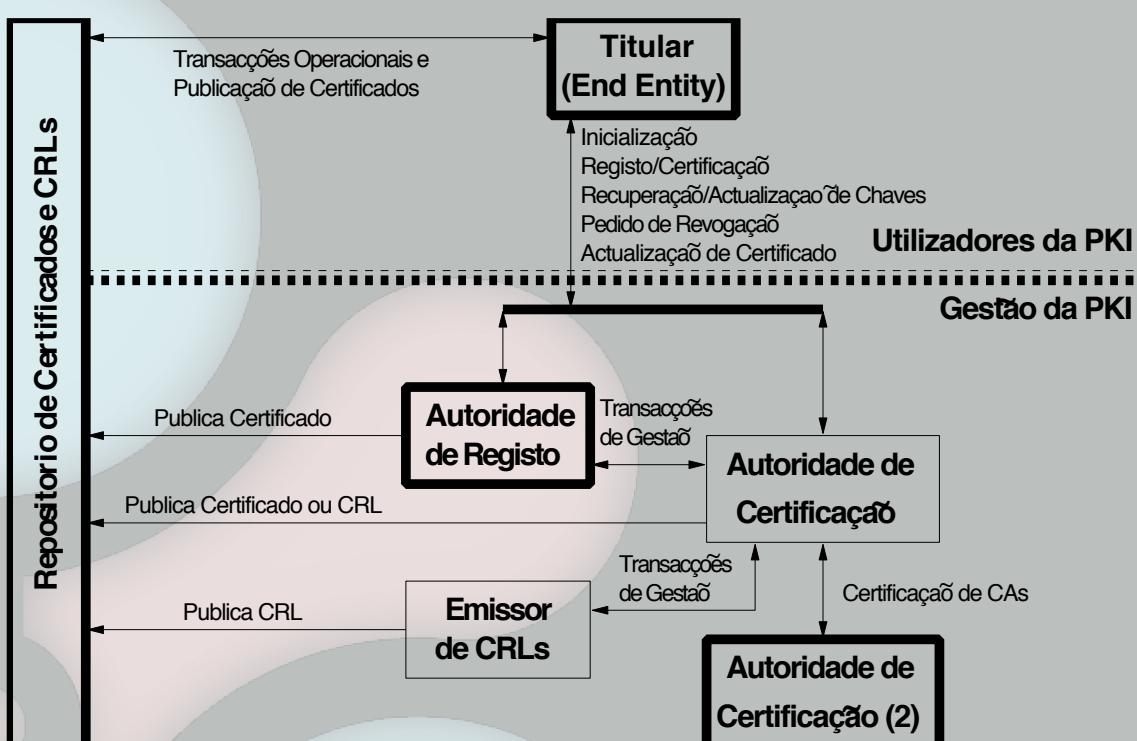
20



- › 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.
 - Renovação e Actualização de pares de chaves.
 - Pedido de revogação.
 - Certificação de CAs.

21

Arquitectura



22

Operações

- › **Inicialização:** Processo inicial que permite ao utilizador comunicar com a PKI: toma conhecimento das ECs em que confia e adquire as chaves públicas e certificados correspondentes.
- › **Pedido de Certificado:** O utilizador, dispondo do seu par de chaves, solicita a uma EC a certificação da sua chave pública por meio de um pedido de certificado.
- › **Registo:** Um utilizador dá-se a conhecer a uma EC (directamente, ou através de uma RA) para que a EC lhe possa emitir um certificado; para isso fornece informação de identificação que deve ser verificada pela EC (RA).
- › **Geração de Par de Chaves:** Em algumas implementações, as ECs encarregam-se de gerar os pares de chaves dos utilizadores, que enviam de forma segura junto com o certificado.

- › **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. atributos deixam de ser aplicáveis, o comprometimento da chave privada, etc.).

- › **Recuperação de um Par de Chaves:** Em algumas implementações as ECs armazenam de forma segura 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.
- › **Renovação de certificados e/ou actualização de Par de Chaves:** Uma vez esgotada a validade de um certificado, existe necessidade de construir um novo certificado. Neste processo pode ou não ser mantido a chave pública do utilizador.

Estrutura dos Certificados X509

Certificado de Chave Pública

- › Recordemos o conteúdo básico de um certificado de chave pública:
 - Dados Informativos:
 - **Identificação do titular** do certificado (i.e. quem detém a chave privada associada a essa chave pública certificada);
 - **Chave pública** do titular;
 - A identificação da EC;
 - Outra informação relevante para a operacionalização do conceito (número de série; datas de validade; etc.)
 - **Assinatura** dos dados realizada pela EC.
- › Os Certificados X509 são uma instância de certificados de chave pública que foram introduzidos para autenticar os nós do serviço de X500.
- › Os dados são representados como estruturas de dados “atributo/valor” (dicionários).
- › As codificações desses dados está standardizada, garantindo a sua interoperabilidade.
 - **DER** - formato binário definido pelo standard (notação ASN.1)
 - **PEM** - representação da informação contido no formato DER em caracteres imprimíveis
- › A assinatura do certificado é efectuada pela Entidade de Certificação (EC) sobre a codificação DER dos dados nele contidos.

27



Certificados X.509v3

- › A versão de certificados utilizada actualmente (standardizada em 1996) veio colmatar as deficiências que as versões anteriores apresentavam em alguns domínios de aplicações, e que se traduziam essencialmente na necessidade de mais atributos.
- › Esta versão introduziu um novo campo do tipo **Extensions**, equipando assim os certificados com a flexibilidade necessária às novas utilizações.
- › As extensões permitem associar atributos genéricos a uma entidade ou à sua chave pública.
- › Cada extensão é, ela própria, uma estrutura de dados com um identificador e um valor adequado ao tipo do atributo que representa.

28



Atributos básicos

- › **version** – Versão do standard X509 (v3).
- › **serialNumber** – Número único atribuído pela EC ao certificado.
- › **subject** – Identificação do titular da chave pública contida no certificado.
- › **subjectPublicKeyInfo** – Estrutura contendo a chave pública do titular do certificado e identificação do algoritmo correspondente.
- › **issuer** – Identificação da EC que emite o certificado.
- › **signature** – Estrutura que identifica o algoritmo utilizado para gerar a assinatura da EC que acompanha o certificado.
- › **validity** – Estrutura com as duas datas que delimitam o período de validade do certificado.

29



Identificadores

- › Os atributos **issuer** e **subject** que identificam a EC e o titular do certificado respectivamente 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 (DN)** para o agente titular.
 - O **DN** tem uma estrutura hierárquica. A norma X.520 standardiza alguns dos componentes de um DN. Os seguintes são de reconhecimento obrigatório e muito utilizados:
 - Country (C)
 - organization (O)
 - organizational-unit (OU)
 - common name (CN)
 - serial number (SN)
- › Exemplo: "C=PT, O=UMINHO, OU=DI, CN=JOE"

30



Certificados X.509 (V3): Extensões

- › Permitem personalizar os dados contidos no certificado (e certificados pela EC por via da respectiva assinatura)
- › As extensões são marcadas como **Critical** ou **Non Critical**. Uma aplicação que encontre uma extensão crítica que não reconheça deve rejeitar o certificado.
- › O RFC-5280 da IETF normaliza as extensões recomendadas para utilização na Internet, definindo como estas devem ser codificados no certificado.
- › São desaconselhados desvios desta recomendação, nomeadamente no que diz respeito a extensões críticas, apesar de não haver qualquer limitação a nível do standard.

31



- › **Basic Constraints** permite assinalar um certificado como pertencendo a uma (sub-)EC, 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 aplicáveis por CAs hierarquicamente inferiores.

32



- › **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).

Formato textual

```
Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number: 1 (0x1)  
Signature Algorithm: md5WithRSAEncryption  
Issuer: C=PT, ST=Minho, L=Braga, O=UM,  
OU=LMF, CN="Dummy CA"  
Validity  
Not Before: Oct 5 16:49:16 2001 GMT  
Not After : Oct 5 16:49:16 2003 GMT  
Subject: C=PT, ST=Minho, L=Braga, O=UM,  
OU=LMF, CN="Dummy CA"  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public Key: (1024 bit)  
Modulus (1024 bit):  
00:d7:.....  
.....  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
.....  
.....  
Signature Algorithm: md5WithRSAEncryption  
43:fe:bd:3d:0a:4c:71:30:46:78:93:63:c1:52:31:a9:49:b7:  
0f:07:d9:79:1e:fb:cf:5d:cd:ca:0d:df:f4:68:09:51:7c:bf:  
d9:33:ba:.....
```

Formato PEM

```
-----BEGIN CERTIFICATE-----  
MIICizCCAfSgAwIBAgIFdMMs9fEwDQYJKoZIhvcNAQE  
ZXJsyW5nQ0ExIDAeBhgkhkiG9w0BCQEWEWRlc3RlckB  
VQQHEwlTdG9ja2hvbG0xCzAJBgNVBAYTA1NFMQ8wDQY  
BgNVBAstC3Rlc3RpbcgZGVwMCIYDzIwMTAwOTAxMDA  
MDAwMDBaMH0xETAPBgNVBAMTCGVybGFuZ0NBMSAwHgY  
ZXJAZZXJsYW5nLm9yZzESMBAGA1UEBxMJu3RvY2tob2x  
MA0GA1UEChMGZXJsYW5nMRQwEgYDVQQLEwt0ZXN0aW5  
9w0BAQEFAAOBjQAwgYkCgYEAgmHw2xApZqdzZOOPTzw  
.....  
.....  
4Sr+EcjROkqe8jE0DmbwmM6lzpwsJscxte+V6HvGR==  
-----END CERTIFICATE-----
```

Cadeias de Certificação e de 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 Entidade de Certificação que o emitiu.
- › Aqui, existem duas alternativas:
 1. A chave pública já é do conhecimento do utilizador (e.g. foi pré-instalada de forma segura)
 2. ou é também fornecida por via de um certificado emitido por uma outra EC
- › Naturalmente que, no segundo caso, há necessidade de proceder à verificação de validade desse certificado.

Que resulta num procedimento de validação recursivo!

Que só termina quando se encontrar um certificado de uma EC que já se confia!

- › A esta sequência de certificados envolvidos no processo de validação dá-se o nome de **Cadeia de Certificação**.
 - › Note que, numa cadeia de certificação bem formada, o issuer de um certificado deverá ser o subject do antecessor.
-
- › As cadeias de certificação reflectem uma **hierarquia** de Entidades de Certificação: as ECs hierarquicamente superiores emitem os certificados das ECs hierarquicamente inferiores.
 - › No(s) topo(s) da hierarquia reside uma EC denominada **Root** ou raiz. O certificado desta EC é emitido e assinado por ela própria – ou seja, um certificado **auto-assinado**, i.e. os campos subject e issuer do seu certificado são iguais.
 - › A confiança na chave pública de uma Root EC é estabelecida por um meio externo à ICP.
 - › Por exemplo: sistemas operativos comuns (e.g. *MS Windows*) incluem certificados de dezenas de Root ECs!

37



Validação de Certificados

- › Para cada certificado da **cadeia de certificação** bem formada, verificar:
 1. validade da assinatura
 2. a aplicabilidade do certificado (face às extensões)
 3. se não foi revogado (e.g. consultando CRLs)
- › A raiz da cadeia de certificação deverá ser de uma EC que já se conheça a chave pública – designa-se por **raiz** ou **âncora** da relação de confiança.
- › A convenção é que os certificados de “raiz” são **auto-assinados** (subject é igual ao issuer).

38



Âncoras de Confiança

- › Um utilizador conhece um número limitado de chaves públicas pertencentes a ECs (em geral Root CAs) e que funcionam como raízes 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 termina então quando for encontrado um certificado com essa característica. Esses são normalmente certificados auto-assinados.

Conclusão: o grau de confiança depositada num certificado válido baseia-se, em última análise, na confiança depositada na EC que funcionou como raiz da relação de confiança.

39



- › A gestão da lista com âncoras de confiança, assim como do próprio processo de validação das cadeias de certificados, é normalmente assegurada pelo próprio Sistema Operativo.
- › Em particular, a compilação dos certificados Root adoptados, assim como a sua actualização/manutenção, é assegurada pelo fabricante.
- › Torna o processo de utilização de certificados praticamente transparente para o utilizador.
 - **O que é bom!** porque, quer os conceitos envolvidos na certificação, quer a própria manipulação dos certificados é complexa.
 - **O que é mau!** porque toda a segurança que supostamente eles suportam fica comprometida se não houver plena consciência das relações de confiança envolvidas.

40



Perfis e Políticas de Certificados



Perfis de Certificados (*Certificate Profiles*)

- › O standard X509v3 oferece flexibilidade para se definirem extensões à medida das necessidades
- › A semântica desses atributos é assim “aberta”, mas que deve ser fixada por regras que estabeleçam, num dado contexto (cenário de utilização, aplicação, protocolo, etc.), quais os atributos que devem estar presentes e qual o seu significado.
- › Um **Perfil de Certificados** denota uma classe de certificados, e compreende:
 - Quais os atributos/extensões de podem ou devem estar presentes e qual a criticidade desses atributos;
 - Qual o significado desses atributos e gama de valores admissível;
 - Quais os algoritmos criptográficos suportados e tamanho de chaves correspondentes;
 - Formato de nomes adoptado e restrições que se lhe devem impôr;
 - *Política de Certificados* associada e respectiva identificação;
 - Regras de validação para as extensões críticas consideradas.

Políticas de Certificados (*Certificate Policies*)

- › A confiança depositada numa EC depende desde:
 - Factores externos, como a credibilidade da instituição ou empresa que suporta a EC e o seu país de origem; etc.
 - Informação sobre as práticas adoptadas pela EC, e garantias que elas cumprem os requisitos apropriados (e.g. por via de acreditação)
- › Mas a confiança que é depositada num certificado individual depende, em última instância, do critério adoptado pela EC na emissão do respectivo certificado.
- › Obs: note que uma EC pode emitir certificados para diferentes fins (perfis), sendo que é concebível que esses diferentes perfis ofereçam garantias distintas...
- › Numa ICP, prevê-se a forma de basear a confiança que se deposita num certificado incluindo nele explicitamente a referência para a respectiva **Política de Certificados** e respectiva documentação.

43



- › Uma **Política de Certificados** é um conjunto de regras que define a aplicabilidade de certificados a uma determinada comunidade ou classe de aplicações com requisitos de segurança comuns.
 - A legislação em que se baseará a emissão e utilização dos certificados.
 - Os requisitos e as responsabilidades (nomeadamente legais e financeiras) associados a ECs e RAs.
 - Os requisitos e as responsabilidades associados a Titulares e Clientes.
 - Restrições ao conteúdo e utilização dos certificados
 - Procedimentos a serem implementados relativamente a diversos aspectos do funcionamento de ECs e RAs.
- › As Política de Certificação permitem:
 - aos utilizadores ajuizarem se devem, num contexto específico, confiar no certificado em questão.
 - que a EC limite a sua responsabilidade explicitando o âmbito de utilização, enquadramento legal, etc. dos certificados por si emitidos.
- › As Política de Certificação:
 - são documentos disponibilizados pelas ECs para serem consultados pelos utilizadores das ICPs
 - devem ser explicitamente referenciadas no certificado por recurso às extensões apropriadas.

44



Políticas de Certificação na validação de certificados

- › Uma parte significativa do RFC-5280 é dedicada às políticas de certificação e ao efeito de uma política de certificação imposta num determinado ponto da hierarquia de certificação.
- › 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 EC, 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 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.

45



Declaração de Práticas de Certificação (Certification Practice Statement)

- › Está ainda previsto que as ECs publiquem um documento onde explicitam as práticas seguidas na emissão e gestão dos certificados por si emitidos.
- › Cada EC publica então uma ou mais **Declaração de Práticas de Certificação** (CPS), nas quais publicita as suas normas de operação internas.
- › Em particular, explica a forma como a EC implementa um determinado conjunto de **Políticas de Certificação**.
- › A acreditação de uma EC 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 em conformidade com estas políticas tem de ser credenciada pelo estado Canadiano.
- › É também possível (e recomendado) incluir nos certificado referência explícita à CPS.

46



Exemplos de Documentos

- › O RFC-3647 fornece um padrão que se recomenda que seja seguido na elaboração dos documentos de Política de Certificados e nas Declarações de Práticas de Certificação.
- › Exemplos de Políticas de Certificação:
 - https://pki.cartao-decidadao.pt/publico/politicas/PJ.CC_24.1.2_0009_pt_AsC.pdf
 - https://acedicom.edicongroup.com/eu/CAEDICOM01_CP_TLSCertificatesPolicy.pdf
 - https://www.actalis.it/area-download-doc/ssl_client_smime_certs_policy_v1-0-en.pdf
- › Exemplos de Declaração de Práticas de Certificação:
 - <https://cacert.org/policy/CertificationPracticeStatement.html>
 - https://pki.cartao-decidadao.pt/publico/politicas/PJ.CC_24.1.1_0002_pt_AsC.pdf

47



Exemplos de Perfis de Certificados

1. Protecção de Email (S/MIME)
2. Autenticação de Sítios (TLS-server)
3. Autenticação em Serviços (TLS-client)
4. Assinatura Qualificada de Documentos

48



Certificados TLS: classificação do Método de Validação (CA/browser forum)

1. **Domain Validation (DV)** - identidade verificada unicamente com base em evidência de controlo do domínio DNS.
2. **Organization Validation (OV)** - verifica existência/controlo de uma organização (e.g. empresa, organismo público, etc.)
3. **Extended Validation (EV)** - critérios mais rigorosos de validação fornecendo evidência de *controlo legal* sobre a entidade.

49



Certificados TLS: Certificate Transparency Motivação:

1. PKIX não prevê um mecanismo simples e efectivo de auditar se certificados são emitidos com lacunas no processo de validação (quer por omissões da CA, ou por comprometimento desta);
2. ...esses problemas tem ocorrido com frequência crescente e com impacto significativo...
3. ...tornando evidente que é “demasiadamente simples” uma CA incorrer em falhas sem terem consciência da gravidade das possíveis consequências.

50



Certificados TLS: Certificate Transparency

Objectivos:

1. Impossibilita (dificulta) a capacidade de CAs emitirem certificados sem conhecimento dos detentores dos domínios DNS correspondentes;
2. Disponibiliza um mecanismo aberto de “registo” e “monitorização” que permite controlar se um certificado foi emitido de forma incorrecta ou maliciosa;
3. Protege os utilizadores de serem induzidos em erro por certificados incorrectamente/maliciosamente emitidos.



Certificados TLS: Certificate Transparency

Arquitectura:

1. Logs:
 - mantém registo incremental assegurado criptograficamente e publicamente auditável de certificados;
 - operados por intervenientes interessados na confiabilidade do sistema (CAs, ISPs, etc.)
2. Monitors:
 - servidores que periodicamente contactam os servidor de Logs por forma validarem consistência e identificarem eventuais certificados suspeitos;
3. Auditors:
 - componentes de software (incorporado em, e.g., web browsers) capazes de interrogar e verificar integridade dos Logs
 - ...verificando em particular se contém o certificado pretendido.

Revogação de Certificados

- › Por vezes há necessidade de revogar certificados que ainda se encontram no seu período de validade
- › Motivos para a revogação de certificados:
 - Chave privada comprometida;
 - Circunstância que justificava associação do `issuer` à chave pública já não se verifica (e.g. `issuer` é o detentor de um cargo temporário)
 - Dados contidos no certificado deixam de ser correctos (e.g. atributo já não se aplica)
 - Etc.
- › Mecanismo originalmente previsto para a revogação de certificados são as **Listas de Revogação de Certificados** (CRL)

53



Certificate Revocation Lists (CRL)

- › As **Certificate Revocation Lists (CRL)** são o canal previsto no X.509 para a revogação de certificados dentro do período de validade. Uma CRL diz-se:
 - **Base CRL** quando lista todos os certificados revogados por uma EC que ainda estão no seu período de validade.
 - **Delta CRL** quando apenas lista os certificados revogados desde a publicação de uma Base CRL referenciada.
- › As CRLs são emitidas e assinadas, em geral, pelas próprias ECs. É possível que a EC delegue esta função numa outra autoridade denominada **CRL Issuer**.
- › Cada CRL tem um contexto específico (o conjunto de certificados passíveis de aparecerem no seu conteúdo), que deve estar bem definido.

54



- › A segurança de uma ICP depende da eficácia com que são revogados os certificados que se tornaram inválidos. Este facto sugere que, assim que um certificado se torna inválido, uma nova CRL deva ser publicada.
- › No entanto, desta forma, um utilizador nunca saberia qual a CRL mais recente.
- › Admitindo que o atacante controla o meio de comunicação que liga o utilizador ao ponto de publicação de uma CRL, possibilitaria ataques do tipo:
 - Vamos admitir que o utilizador pretende utilizar um certificado cuja chave privada foi comprometida, e que é conhecida pelo intruso.
 - O utilizador tenta obter a CRL mais recente, que revogaria o certificado.
 - Mas o intruso fornece uma versão antiga da CRL onde ainda não aparece a revogação desse certificado.
 - O utilizador aceita o certificado porque não tem como saber que a CRL que utilizou estava desactualizada.

- › De facto, a utilidade de uma CRL depende do facto de ela ser publicada periodicamente (e.g. diariamente, semanalmente, mensalmente, etc.)
- › Isto permite também que a CRL seja pública, e distribuída por canais não seguros.
- › Compete ao utilizador estar ao corrente da frequência de publicação das CRLs, e definir uma política sobre o que é uma CRL “suficientemente recente”.
- › O atributo nextUpdate permite indicar na própria CRL a altura a partir da qual é garantida a publicação de uma nova CRL.

- › O utilizador está consciente de que, a menos que obtenha a última versão da CRL, estará a correr o risco de aceitar certificados inválidos.
- › Isto não quer dizer que não possam ser publicadas CRLs extraordinárias, fora da frequência normal de publicação.
- › Isto pode ocorrer, por exemplo, se um certificado importante tem de ser revogado porque a chave privada correspondente foi comprometida (e.g. o certificado de uma EC hierarquicamente inferior).
- › No entanto, a granularidade garantida nunca é inferior ao período de publicação da CRL: não é possível garantir que os utilizadores obtenham a CRL extraordinária antes da data de publicação da próxima CRL periódica.

Online Certificate Status Protocol (OCSP)

- › Os riscos associados à utilização indevida de um certificado revogado podem não ser aceitáveis.
- › Em alternativa ou adição à consulta de uma CRL, pode ser necessária informação actual sobre o estado de revogação de um certificado.
- › O OCSP (definido no [RFC-6960](#)) permite a uma aplicação determinar o estado de um certificado com maior frescura temporal.
- › O Cliente OCSP emite um pedido a um Responder OCSP (Servidor) e suspende a aceitação do certificado até que este forneça uma resposta.
- › Estão ainda previstos serviços análogos ao OCSP para *Delegated Path Validation* e *Delegated Path Discovery* ([RFC-3379](#)).

Referências

- › *Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure.* Carl Ellison and Bruce Schneier. Computer Security Journal • Volume XVI, Number 1, 2000 (<https://www.schneier.com/academic/paperfiles/paper-pki.pdf>)
- › Adams, Carlisle & Lloyd, Steve (2003). *Understanding PKI: concepts, standards, and deployment considerations*. Addison-Wesley Professional. ISBN 978-0-672-32391-1.
- › Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (<https://tools.ietf.org/html/rfc5280>)
- › CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (<https://cabforum.org/baseline-requirements-documents/>)
- › Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (<https://tools.ietf.org/html/rfc3647>)