



Certificação

Criptografia (MIETI)
José Carlos Bacelar Almeida
(jba@di.uminho.pt)



Certificados digitais de chave pública

Documento assinado contendo uma associação entre uma dada entidade (identidade) e uma chave pública.

Objecto: entidade detentora de um par de chaves.

Assinante: *Autoridade de Certificação* a quem se reconhece autoridade (e se confia) para estabelecer as referidas associações entre identidades e chaves públicas.

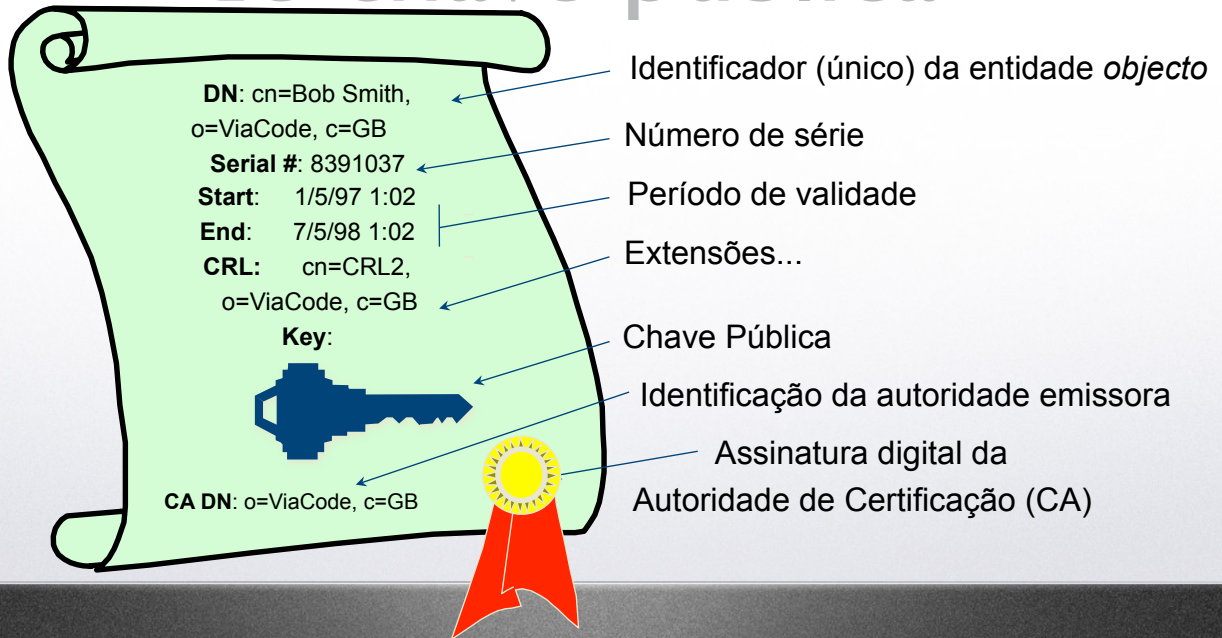
Verificador: utilizador de técnicas criptográficas assimétricas que necessita de garantias que a chave pública corresponde à entidade presumida.

Outra informação contida nos certificados:

- Data de validade (do certificado e da chave nele contida)
- Aplicabilidade (da chave pública) do certificado
- ...



Estrutura de um certificado de chave pública



Alguns *standards* de certificados de chave pública

- **X509(v3)** - originalmente concebido para dotar o serviço de directoria X500 de mecanismos seguros de autenticação. Foi posteriormente adoptado como base para os mais populares esquemas de certificação (PKIX; em protocolos sobre a *Web*; correio electrónico; etc.)
- **PGP** - certificados utilizados na popular aplicação de *mail* (*Pretty Good Privacy*).
- **SPKI/SDSI** - certificados vocacionados para autenticação.



Identities...

- A associação de uma chave pública a uma entidade é realizada por intermédio de uma *identificação*.
 - deve a identificação de uma entidade ser globalmente única (se sim, será isso possível?)
 - são realmente imprescindíveis?
- Por motivos históricos os certificados X509 herdaram o esquema de nomes dos nós serviço de directoria X500 - *Distinguished Names (DNs)*
C=PT / P=Minho / O="Universidade do Minho" / OU="Departamento de Informática" / CN="José"
- Hierarquia implícita nos nomes (prefixação)
- Muitas vezes é preferível utilizar nomes mais informativos... (e.g. xpto@abc.org; ...)



Modelos de Confiança

Modelo Rígido: utilizadores dispõem da chave pública da(s) entidade(s) autorizadas a emitir certificados. (Intranet; WEB)

Modelo Hierárquico rígido: uma só CA que dispõe da capacidade de delegar noutras (sub-)CAs a capacidade de emissão de certificados. (e.g. X509 PEM)

Modelo Hierárquico distribuído: um conjunto de hierarquias coabitam podendo existir certificação cruzada entre essas árvores. (e.g. X509 PKIX; WEB)

Modelo em Rede: é dada a cada utilizador a capacidade de emitir certificados, cabendo assim a quem faz uso desses certificados avaliar o grau de confiança que esses certificados lhe merecem. (e.g. PGP)



Componentes de uma *PKI*

- É normal identificarmos os seguintes componentes numa Infra-estrutura de Chave Pública:
 - **Autoridade de Certificação (CA)** - que detém a responsabilidade de emitir; revogar; manter e disponibilizar a informação dos certificados.
 - **Autoridade de Registo (RA)** - que serve de *interface* entre os “clientes” da autoridade de certificação e a CA. É normal serem estas entidades as responsáveis pela validação da informação contida nos certificados.
 - **Repositório** - onde se mantém a informação de todos os certificados emitidos (e dos revogados - CRLs) e se disponibiliza mecanismos de acesso a essa informação (e.g. LDAP; FTP; HTTP).
 - **Arquivo** - onde se guardam os certificados (mesmo caducados) para permitir a verificação de assinaturas “antigas”.



Estrutura base de um certificado X509 (v3)

Version	2 (V1=0, V2=1, V3=2)
Serial Number	56
Signature Algorithm	sha1RSA
Issuer DN	C=US;S=UTAH;O=DST;OU=DSTCA;CN=RootCA
Validity Period	05/02/2000 08:00:00 to 05/02/2001 08:00:00
Subject DN	C=US;O=GOV;O=NIH;OU=CIT;CN=Mark Silverman
Subject Public Key	RSA, 3081 8902 8181 ... 0001
Issuer UID	Usually omitted
Subject UID	Usually omitted
Extensions	Optional Extensions
Signature Algorithm	sha1RSA (same as above)
Signature	302C 0258 AE18 7CF2 ... 8D48



Extensões...

- Fornecem informação adicional sobre o objecto do certificado
 - Email; DNS name; etc.
 - Pontos de acesso da Certificate Revocation List (CRL); Certificate Practice Statement (CPS); etc.
 - Caracterizar aplicabilidade do certificado (e.g. se pode emitir certificados; se só pode ser utilizado para assinatura digital; etc.)
- Algumas das extensões mais utilizadas:
 - altName** - identificação alternativa para objecto do certificado.
 - keyUsage; nsCertType** - caracteriza aplicabilidade do cert.
 - basicConstrains; nameConstrains** - determina se entidade objecto pode (ou não) emitir certificados (i.e. se é sub-CA).
 - policyId** - identificador da *Policy* do certificado.
- Extensões podem ser **críticas**...
- *Profiles* - estabelecem a estrutura dos certificados...



Exemplo...

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=PT, ST=Minho, L=Braga, O=UM, OU=LMF (Dummy CA)/Email=root@localhost
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 (Dummy CA)/Email=root@localhost
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:d7:.....
      .....
    Exponent: 65537 (0x10001)
X509v3 extensions:
  Netscape Comment:
    This CA issues SSL server certificates.
  Netscape CA Policy Url:
    https://localhost/ServerCerts/policy.html
  Netscape Cert Type:
    SSL CA
  X509v3 Basic Constraints:
    CA:TRUE
```

X509v3 Subject Key Identifier:

3A:F7:61:90:F9:B3:CE:A0:82:18:B9:8A:91:C7:6C:21:B2:EE:C6:EF

X509v3 Authority Key Identifier:

keyid:46:49:CE:A6:16:CC:A9:86:61:9B:E3:92:47:A4:8E:43:75:2B:57:4B

DirName:/C=PT/ST=Minho/L=Braga/O=UM/OU=LMF (Dummy CA)/Email=root@localhost
serial:00

X509v3 Key Usage:

Certificate Sign, CRL Sign

X509v3 Extended Key Usage:

Netscape Server Gated Crypto, Microsoft Server Gated Crypto

X509v3 Subject Alternative Name:

URI:https://localhost/pyca/get-cert.py/ServerCerts/ca.crt

X509v3 Issuer Alternative Name:

URI:https://localhost/pyca/get-cert.py/Root/ca.crt

X509v3 Certificate Policies:

Policy: 1.2.3.4

CPS: https://localhost/ServerCerts/policy.html

User Notice:

Organization: Looser Org. with bad CA admin.

Numbers: 4, 2

Explicit Text: This CA issues SSL server certificates.

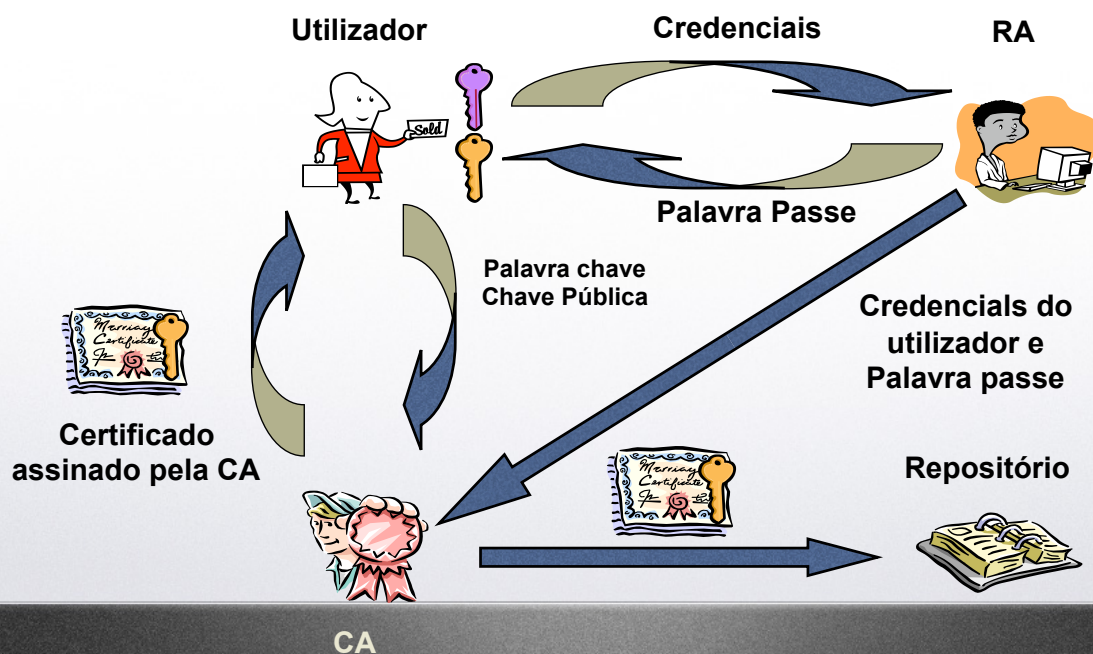
Signature Algorithm: md5WithRSAEncryption

43:fe:bd:3d:0a:4c:71:30:46:78:93:63:c1:52:31:a9:49:b7:

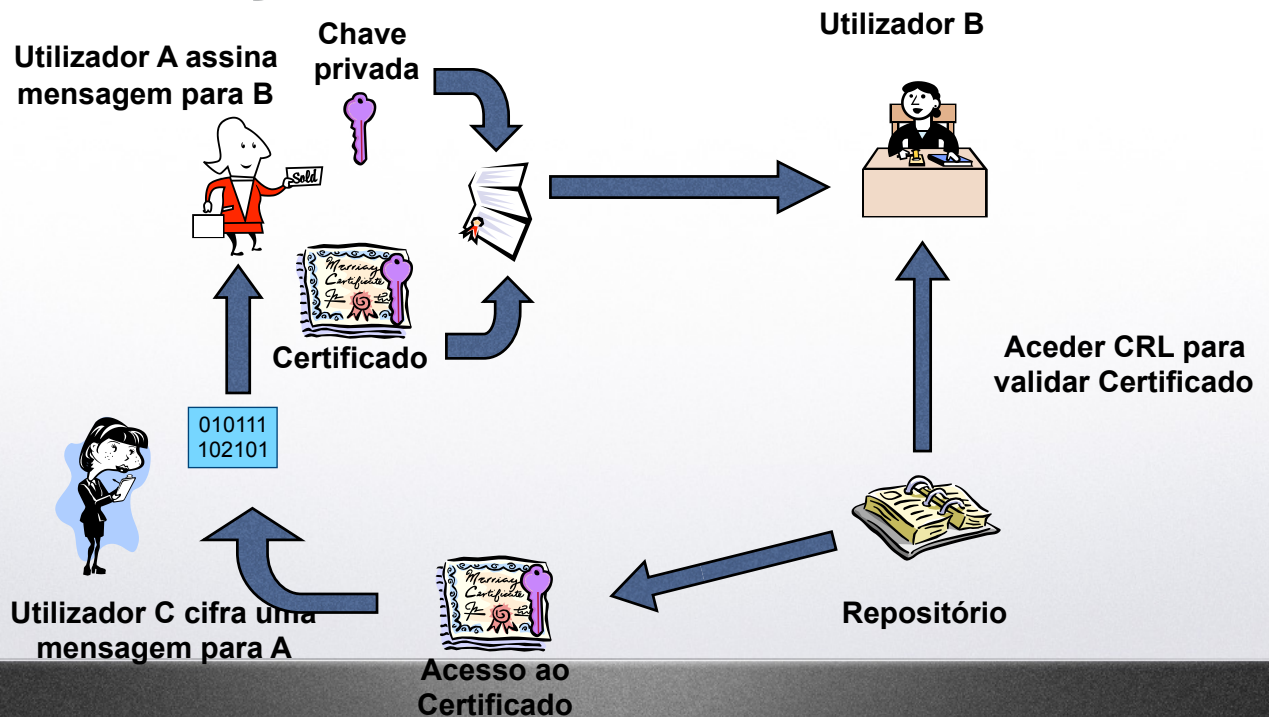
0f:07:d9:79:1e:fb:cf:5d:cd:ca:0d:df:f4:68:09:51:7c:bf:

d9:33:ba:.....

Pedido de certificados...



Utilização dos certificados...



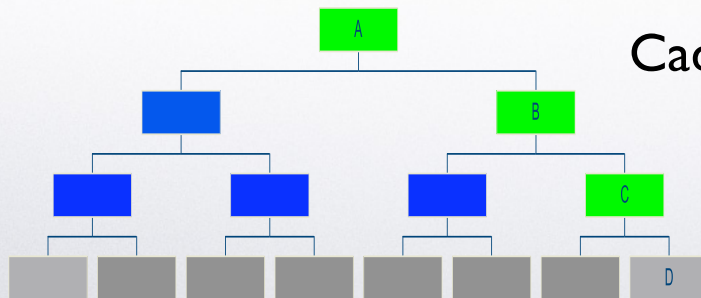
Revogação

- Se uma chave privada é comprometida torna-se necessário “ANULAR” o certificado emitido para a respectiva chave pública.
- Uma *Certificate Revocation List* (CRL) consiste numa lista de certificados revogados por uma dada CA numa determinada data (assinada por esta) - tal como as “listas negras” dos cartões de crédito.
- O mecanismo de acesso às CRLs é um ponto fraco:
 - um intruso pode “impedir” o acesso ao ponto de distribuição
 - um intruso pode “enviar” uma lista desatualizada
- ...por isso, é conveniente as CRLs serem distribuídas com uma periodicidade fixa.
- Surgiram já esquemas alternativos que minimizam estes problema (On-line Certificate Status Protocol; etc.)



Cadeia de certificação

- Num modelo hierárquico, designa-se por **cadeia de certificação** a sequência de certificados envolvidos entre o certificado do utilizador final e a raiz da hierarquia de certificação.
- É normal os topos das hierarquias de certificação fazerem uso de certificados **auto-assinados**.

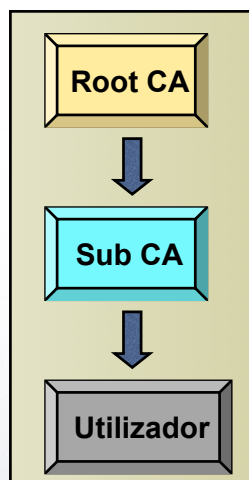


Cadeia de certificação:
A/B/C/D



Cadeia de Certificação

Auto-assinado



Informação da RootCA

Assinatura de Root

← Chave privada da RootCA

Informação da SubCA

Assinatura de Root



Informação do Utilizador

Assinatura SubCA

← Chave privada da SubCA



Documento alvo

Assinatura do utilizador

← Chave privada do utilizador





Verificação de Certificados

- ◆ Para cada certificado da **cadeia de certificação** (da raiz para a certificado alvo):
 - Verificar a validade da assinatura
 - Verificar a aplicabilidade do certificado (face às extensões)
 - Verificar se não foi revogado (e.g. consultando CRLs)



Outros esquemas de certificação...

Algumas críticas apontadas ao modelo PKIX:

- Certificados foram desenhados para “identificação” e são normalmente utilizados para “autenticação”.
- Modelo hierarquico é rígido e não reflete estruturas sociais comuns.

○ grande argumento a favor...

- foi adoptado como “standard *de facto*” pelos protocolos “da WEB” (i.e. pelos fabricantes dos browsers...)

Algumas alternativas/extensões

- Certificados de atributos
- PGP *web of trust*
- SPKI/SDSI



Certificados de Atributos

- Standard que complementa os certificados de chave pública com vista a responder convenientemente a utilizações envolvendo “autorizações”.
- Certificados *light* em que se associa uma identidade a determinados atributos (e.g. permissões de acesso; recibos de pagamentos; etc.)
- Dado que os certificados de atributos não dispõem de chave pública, estes são utilizados juntamente com certificados X509 normais (certificados de chave pública são responsáveis pela “identificação”, e os de atributos pela “autorização”).
- ... podem ser entendidos como “acrescentos” aos certificados de chave pública.
- Autoridade emissora dos certificados de atributos não necessita ser a mesma que emite os certificados de chave pública.



PGP *web of trust*

- A todas as entidades é permitida a produção de certificados (i.e assinar digitalmente uma associação entre chaves públicas e identidades).
- Cada utilizador atribui um determinado “grau de confiança” aos certificados assinados com uma determinada chave de sua confiança (*pub-ring*).
- Avaliação da confiabilidade de novas chaves é estabelecida por intermédio de heurísticas (e.g. três derivações com nível de confiança “médio” permitem derivar uma com nível “bom”)



SPKI/SDSI

- Proposta de esquema de certificação vocacionado para “controlo de acessos”
- Adota um âmbito meramente local para os identificadores.
- Principal motivação é a definição simples e efectiva das regras de acesso a servidores *web*.
- Permite representar aspectos como “delegação”; grupos de utilizadores; ACLs...



Referências web

- <http://www.pki-page.org/>
- <http://www.pkilaw.com/>
- <http://world.std.com/~cme/html/spki.html>
- <http://www.ietf.org/html.charters/pkix-charter.html>
- <http://www.pgpi.org/>