

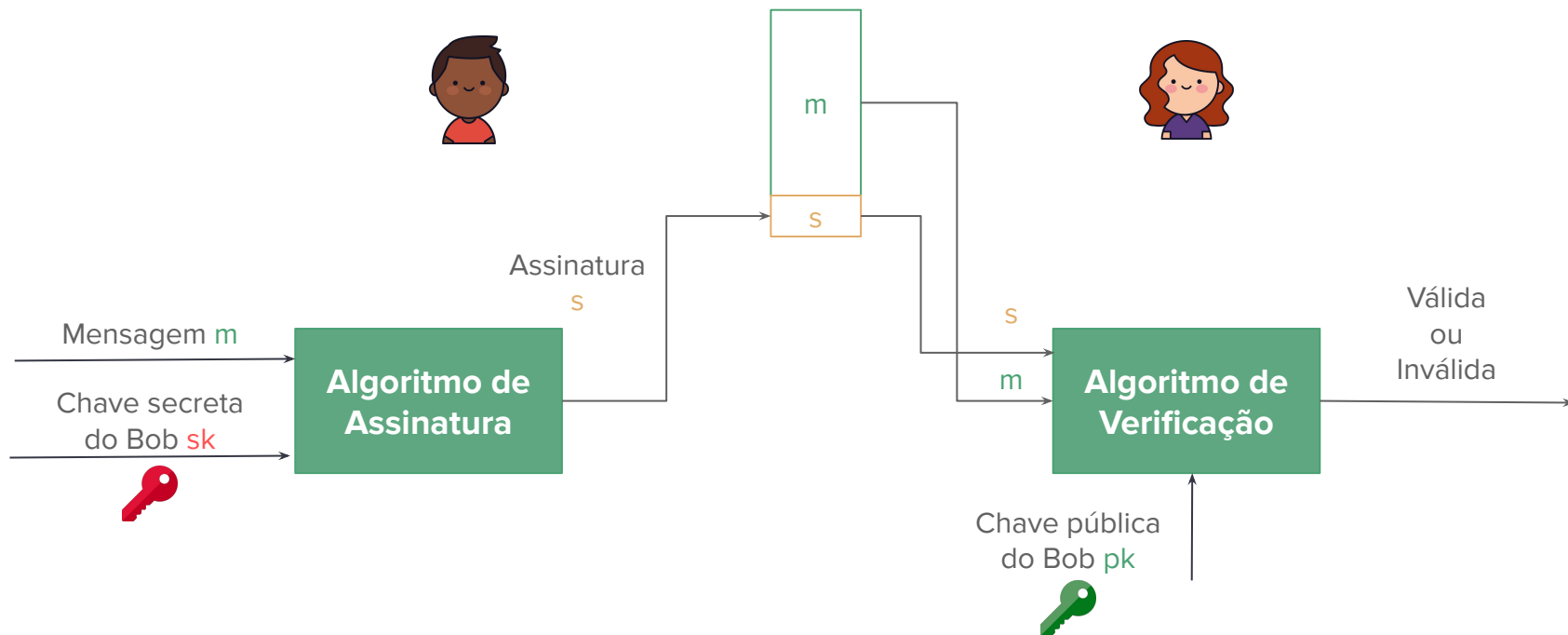
Criptografia Aplicada

Certificação Digital

Sumário

- Autoridades Certificadoras e Autoridades de Registro
- Infraestrutura de Chaves Públicas
- Certificados Digitais

Assinatura Digital



Como Alice sabe que essa chave é do Bob?

Assinatura Digital



Assinatura Digital



Assinatura Digital



Alternativa

- **Autoridade confiável** verifica a identidade do Bob e a vincula com a sua chave pública
- Vinculação entre usuário e chave é feita através de um **certificado digital**
- Bob distribui o seu certificado
- Alice consegue verificar a validade do certificado de Bob

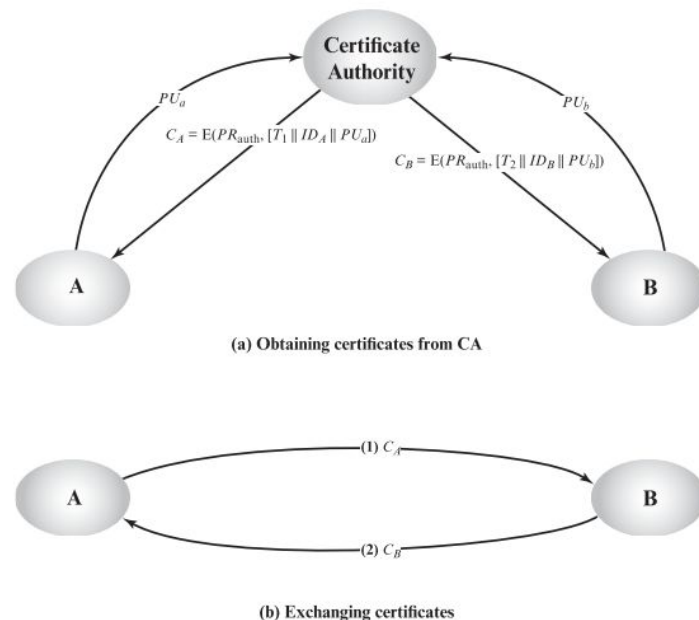


Figure 14.13 Exchange of Public-Key Certificates

Fonte: W. Stallings. *Cryptography and network security*. Cap 14.3

Requisitos

- Qualquer participante pode ler o certificado e determinar o nome e a chave pública do seu dono.
- Qualquer participante pode verificar que o certificado foi gerado pela autoridade confiável e não é falsificado
- Apenas a autoridade confiável pode gerar certificados
- Qualquer participante pode verificar a validade do certificado

Autoridade Certificadora (AC)

- A autoridade confiável é chamada de **Autoridade Certificadora (AC)**
- Cada AC tem um par de chaves
 - chave privada usada para assinar certificados
 - chave pública usada para verificar assinaturas
- Seu papel consiste em:
 - Verificar a identidade do dono do par de chaves
 - Emitir um certificado digital, que vincula dono à chave pública
 - assinando esses certificados com a sua chave privada
 - Revogar certificados
 - e consequentemente manter a lista de certificados revogados (LCR)

Emissão de Certificados

- Um certificado digital contém
 - identidade do dono par de chaves,
 - chave pública,
 - data de validade,
 - assinatura da AC,
 - etc.
- AC emite o certificado
 - **verifica a identidade** do usuário
 - **assina** o certificado com a sua chave privada

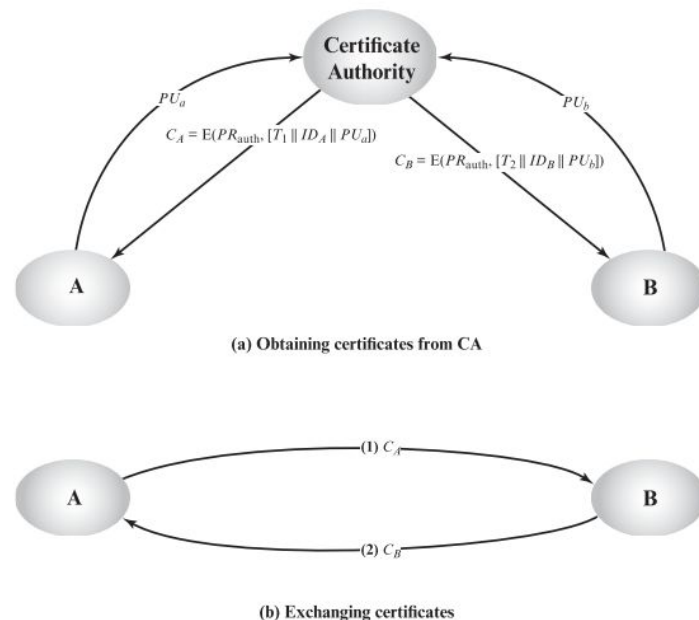


Figure 14.13 Exchange of Public-Key Certificates

Fonte: W. Stallings. *Cryptography and network security*. Cap 14.3

Verificação de Certificados

- Bob distribui o seu certificado.
- Alice não precisa confiar em Bob, só precisa confiar na AC
 - ela possui uma lista de chaves públicas de ACs que ela confia
 - Alice **verifica** a assinatura contida no certificado de Bob utilizando a chave pública da AC
 - caso haja modificações nas informações do certificado, Alice consegue identificar
- Alice não guarda a lista de todos os certificados dos seus colegas
 - guarda apenas as chaves das ACs que ela confia
 - ao chegar um novo certificado, ela verifica, usa e descarta

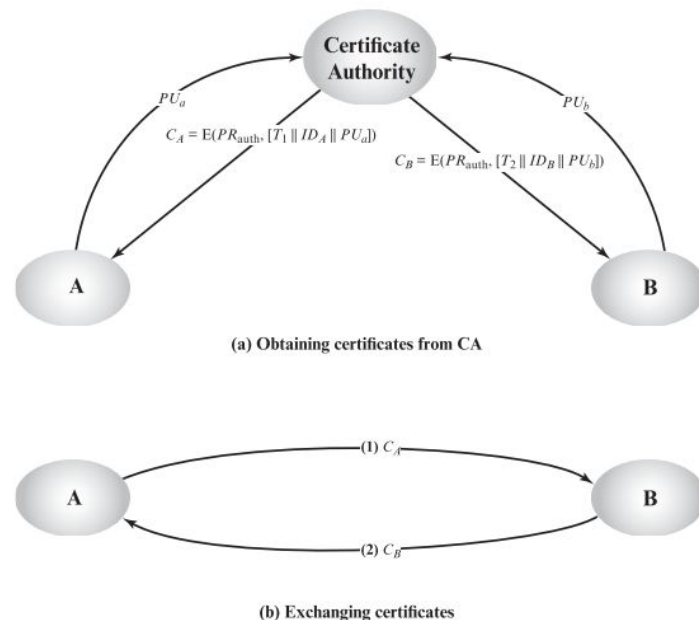


Figure 14.13 Exchange of Public-Key Certificates

Fonte: W. Stallings. *Cryptography and network security*. Cap 14.3

Autoridade de Registro (AR)

- Componente opcional que pode auxiliar a AC em atividades administrativas
- Responsável pela interface entre usuário final e AC
- Seu papel consiste em:
 - Verificar a identidade e cadastrar os usuários
 - Encaminhar solicitações de certificados às ACs

Sumário

- Autoridades Certificadoras e Autoridades de Registro
- **Infraestrutura de Chaves Públicas**
- Certificados Digitais

Infraestrutura de Chaves Públicas (ICP)

- Conjunto de hardware, software, pessoas, políticas e procedimentos necessários para gerenciar, armazenar, distribuir e revogar certificados [\(RFC4949\)](#)
- Tem por objetivo desenvolver uma maneira segura, conveniente e eficiente de obter certificados digitais

Infraestrutura de Chaves Públicas (ICP)

- Entidades de uma ICP:
 - **autoridades certificadoras**
 - **autoridades de registro**
 - **entidade final**: o usuário final, que pode ser uma pessoa, dispositivo, computador, etc.
 - **emissor de LCRs**: opcional, pode ser a AC ou alguma outra entidade
 - **repositório**: local de armazenamento de certificados e LCRs

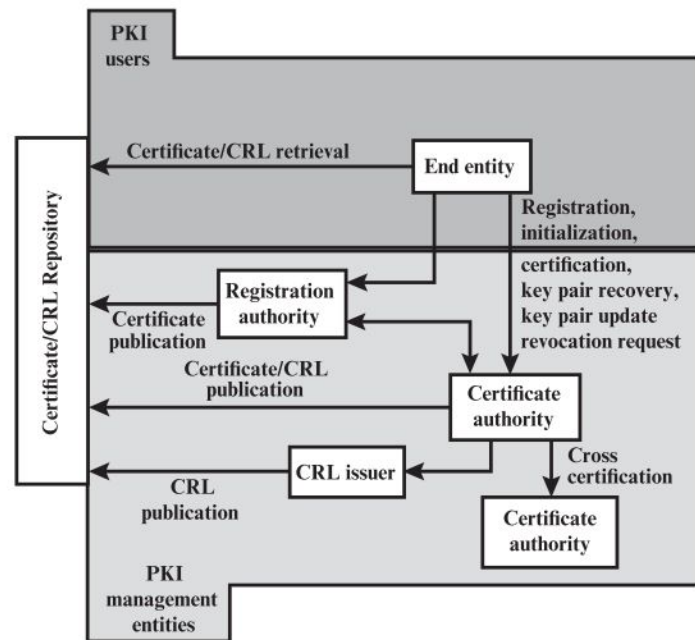
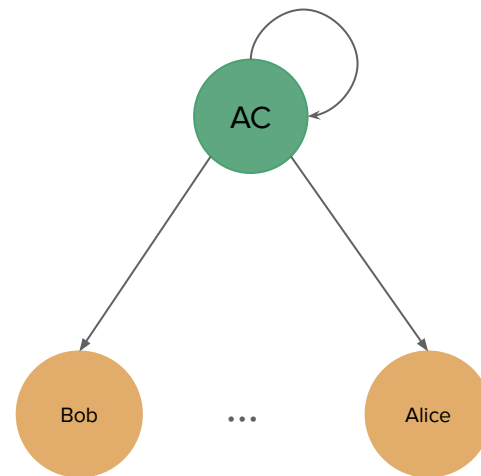


Figure 14.17 PKIX Architectural Model

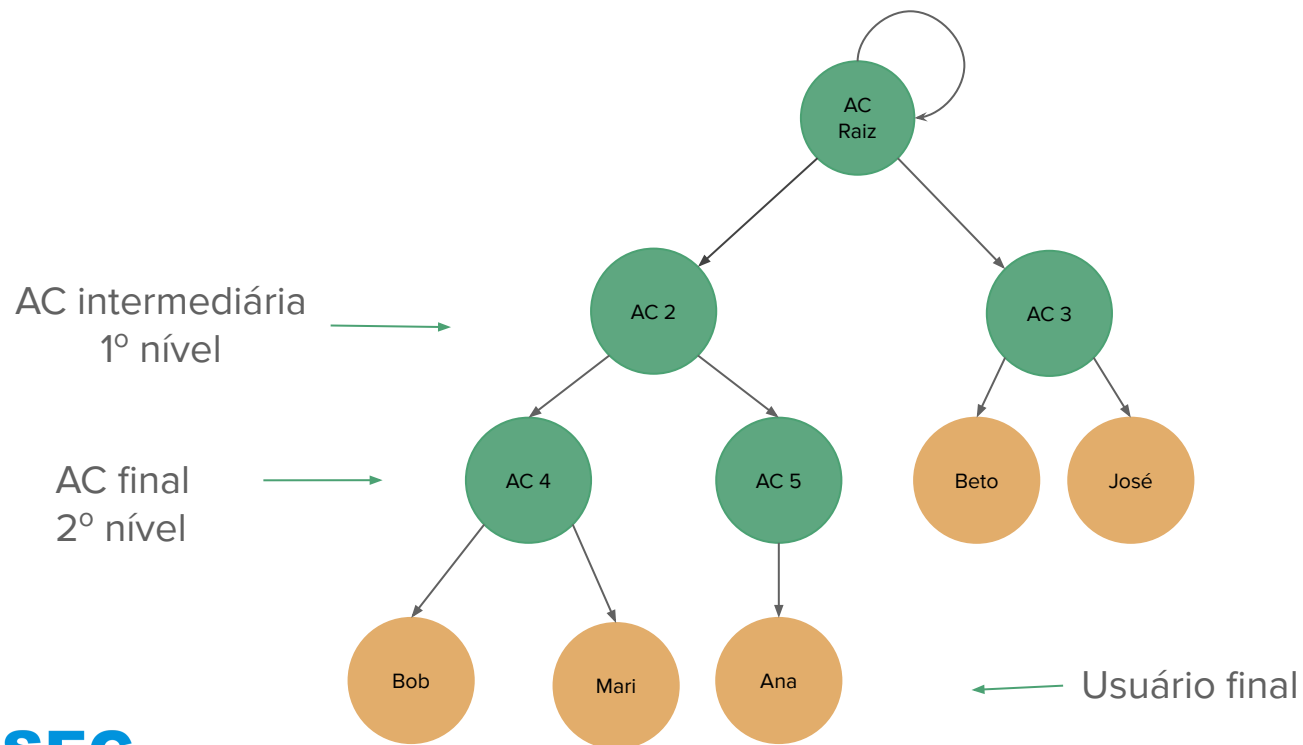
Fonte: W. Stallings. *Cryptography and network security*. Cap 14.5

ICPs hierárquicas

- Uma AC também possui um certificado
 - vincula a identidade da AC à sua chave pública
 - é utilizado na verificação dos certificados emitidos por ela
- Esse certificado é auto-assinado e armazenado em um repositório público
- Uma AC é responsável pela emissão de todos os certificados?



ICPs hierárquicas



ICP-Brasil

- A ICP-Brasil é uma infraestrutura que segue o padrão hierárquico
- Possui AC raiz, autoridades certificadoras de primeiro nível, de segundo nível e autoridades de registro
 - link para a estrutura completa:
<https://estrutura.iti.gov.br/>
- Exemplos de aplicações:
 - sistema financeiro, poder judiciário, sistema tributário, receituário e dispensação de medicamentos, etc.



Imagem:

https://www.gov.br/iti/pt-br/assuntos/icp-brasil/EcosystemaICPBrasil_240822.pdf

ICPEdu

- Serviço de certificação oferecido pela Rede Nacional de Ensino e Pesquisa (RNP)
- Provê estrutura para emissão de certificados para alunos, professores e servidores de universidades brasileiras
 - desde que tenha acesso à comunidade acadêmica federada (CAFe)
- Possui uma AR automatizada
 - a identidade dos usuários é obtida e verificada pelas instituições de ensino
 - as informações cadastradas na universidade são utilizadas na emissão do certificado
- Mais informações:
 - Link para os certificados das ACs: <https://repositorio.icpedu.rnp.br/public/ac>
 - Link para emissão de certificados: <https://pessoal.icpedu.rnp.br/home>



Emitir certificado digital

1
Dados

2
Senha

3
Salvar

Confira seus dados de usuário

Confirme os dados fornecidos pela sua instituição. Caso os dados não estejam de acordo, entre em contato diretamente com o operador da sua instituição.

Dados do usuário

Nome do usuário: Thais

Bardini Idalino

CPF:

E-mail:

thaisidalino@gmail.com

Nascimento:

Cancelar

Informações do certificado

Dados da autoridade certificadora

Autoridade: AC PESSOAS

Instituição: UFSC -

Universidade Federal de Santa Catarina

Data de emissão:

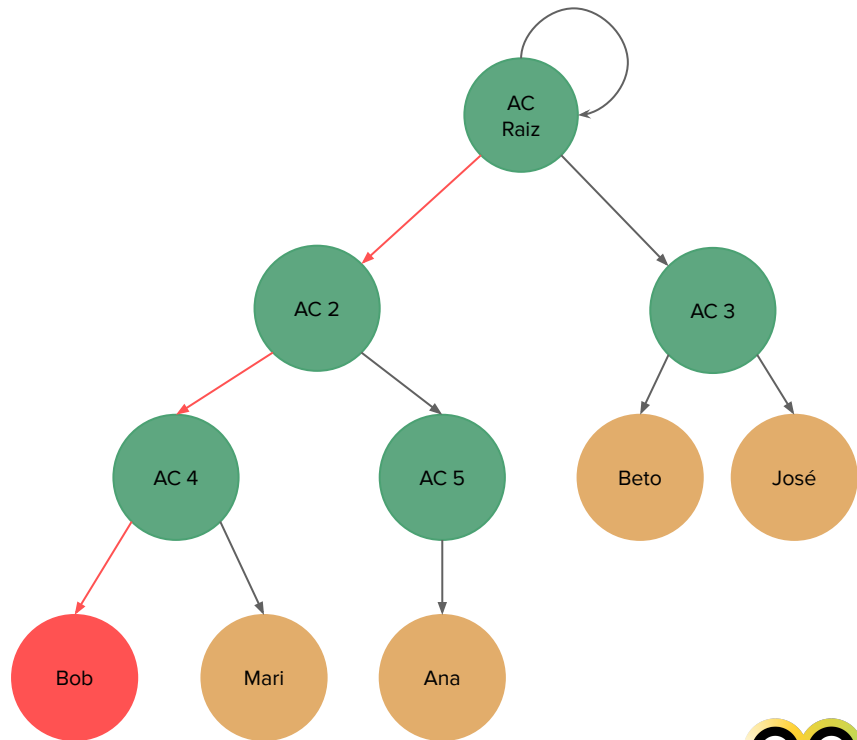
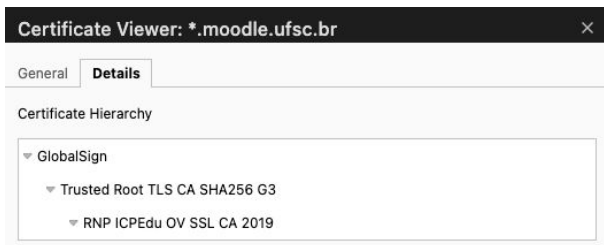
07/11/2024

Data de expiração:

07/11/2025

Caminho de certificação

- Agora a verificação do certificado do Bob envolve alguns passos extras
- A Alice precisa fazer 4 verificações de certificado para verificar a validade o certificado de Bob
 - ela confia apenas na AC Raiz
 - precisa validar a cadeia de certificados que leva o certificado de Bob até a raiz



Sumário

- Autoridades Certificadoras e Autoridades de Registro
- Infraestrutura de Chaves Públicas
- **Certificados Digitais**

Certificados Digitais

- Baseados em criptografia de chaves públicas e assinaturas digitais
- Seguem o padrão X.509
 - define a estrutura do certificado e protocolos de autenticação
 - padrão utilizado em uma variedade de contextos, ex: SSL/TLS, S/MIME, IPSec
- O padrão não requer o uso de algoritmos de assinatura digital ou de hash específicos

Geração de certificados X.509

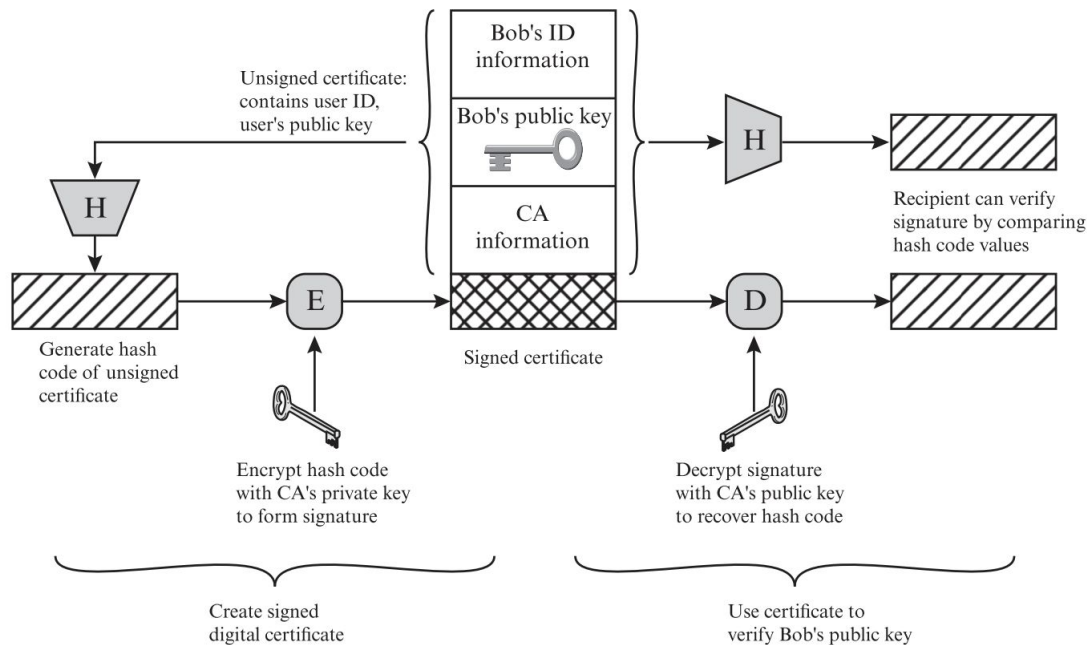
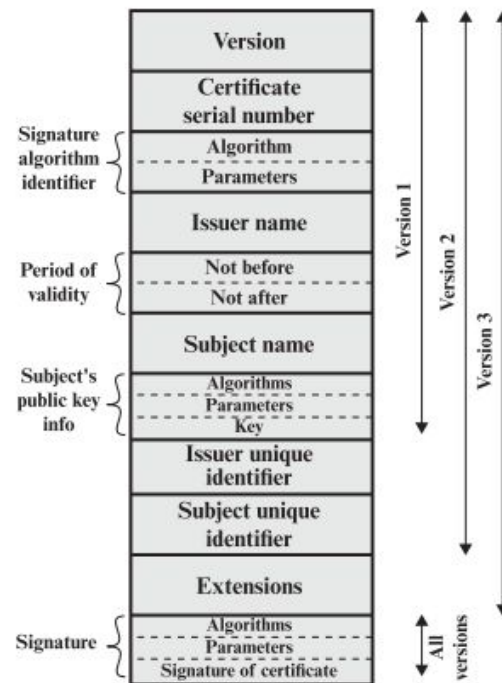


Figure 14.14 X.509 Public-Key Certificate Use

Campos de um certificado digital

Principais campos de um certificado:

- **Version:** versão do formato do certificado.
- **Certificate serial number:** inteiro que identifica unicamente o certificado na AC que o emitiu
- **Signature algorithm identifier:** algoritmo usado para assinar o certificado
- **Issuer name:** identificação da AC que criou e assinou
- **Period of Validity:** datas de emissão e validade



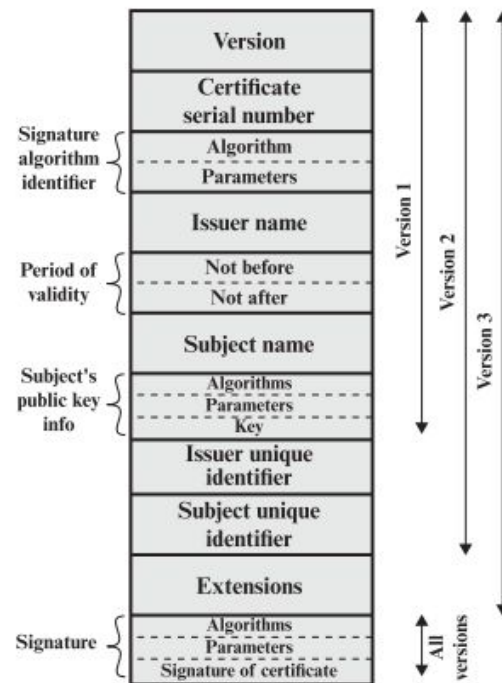
(a) X.509 certificate

Figure 14.15 X.509 Formats

Campos de um certificado digital

Principais campos de um certificado:

- **Subject name:** nome do dono do certificado
- **Subject's public key info:** chave pública, identificador do algoritmo e os parâmetros
- **Issuer unique identifier:** identificador único da AC
- **Subject unique identifier:** identificador único do usuário
- **Extensions:** conjunto de campos com informações adicionais
- **Signature:** assinatura aplicada em todos os outros campos do certificado



(a) X.509 certificate

Figure 14.15 X.509 Formats

Extensões

- O campo de extensões é flexível e permite a inclusão de diversos tipos de extensões.
- Cada extensão contém um identificador (OID), um indicador de criticidade, e o valor da extensão.
- Elas podem ser divididas em três categorias:
 - **Informações de chave e política:** informações adicionais sobre as chaves do emissor e do sujeito, e indicadores da política do certificado;
 - **atributos do certificado do sujeito e emissor:** trazem informações adicionais sobre o sujeito e emissor, que reforçam sua identidade;
 - **restrições do caminho de certificação:** permitem que especificações de restrição sejam incluídas em certificados emitidos por ACs para outras AC

Certificado de entidade final

AC que emitiu o certificado



Assinatura do certificado pela AC




Validade do certificado



Informações sobre a minha chave pública



**Thais Bardini Idalino**
Issued by: AC PESSOA SC
Expires: Friday, 7 November 2025 at 13:15:46 Brasilia Standard Time
✔ This certificate is valid

> Trust
> Details

Subject Name
Common Name Thais Bardini Idalino
Organizational Unit UFSC - Universidade Federal de Santa Catarina
Organization ICPEdu
Country or Region BR

Issuer Name
Common Name AC PESSOA SC
Country or Region BR
Organization RNP
Organizational Unit ICPEDU

Serial Number 1730996147053355358
Version 3
Signature Algorithm SHA-512 with RSA Encryption (1.2.840.113549.1.1.13)
Parameters None

Not Valid Before Thursday, 7 November 2024 at 13:15:46 Brasilia Standard Time
Not Valid After Friday, 7 November 2025 at 13:15:46 Brasilia Standard Time

Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 256 bytes : AE B1 45 5B 79 BA 79 71 ...
Exponent 65537
Key Size 2.048 bits
Key Usage Encrypt, Verify, Wrap, Derive
Signature 512 bytes : 4A 96 32 11 9E ED 4A F6 ...

Extension Key Usage (2.5.29.15)
Critical YES
Usage Digital Signature, Non-Repudiation, Key Encipherment

Certificado de AC intermediária



AC PESSOA SC

Intermediate certificate authority

Expires: Tuesday, 24 January 2040 at 15:18:26 Brasilia Standard Time

⚙ This certificate is marked as trusted for this account

> Trust



✓ Details

Subject Name	
Common Name	AC PESSOA SC
Country or Region	BR
Organization	RNP
Organizational Unit	ICPEDU
Issuer Name	
Country or Region	BR
Organization	RNP
Organizational Unit	GSER
Common Name	ac-raiz-v3
State/Province	Santa Catarina
Locality	Florianopolis
Email Address	gopac@rnp.br
Serial Number	
Version	3
Signature Algorithm	SHA-512 with RSA Encryption (1.2.840.113549.1.1.13)
Parameters	None
Not Valid Before	Wednesday, 29 January 2020 at 15:18:26 Brasilia Standard Time
Not Valid After	Tuesday, 24 January 2040 at 15:18:26 Brasilia Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	512 bytes : C3 1D DA 28 0B 76 EA 69 ...
Exponent	65537
Key Size	4.096 bits
Key Usage	Verify
Signature	512 bytes : 1E CF C5 8C 35 33 65 5F ...
Extension Key Usage (2.5.29.15)	
Critical	NO
Usage	Digital Signature, Key Cert Sign, CRL Sign

Certificado de AC raiz

ver mais em:

<https://repositorio.icpedu.rnp.br/public/ac>

**ac-raiz-v3**
Root certificate authority
Expires: Friday, 20 January 2045 at 17:33:43 Brasilia Standard Time
 This certificate is marked as trusted for all users

> Trust

> Details

Subject Name

Country or RegionBR

OrganizationRNP

Organizational UnitGSER

Common Nameac-raiz-v3

State/ProvinceSanta Catarina

LocalityFlorianopolis

Email Addressgopac@rnp.br

Issuer Name

Country or RegionBR

OrganizationRNP

Organizational UnitGSER

Common Nameac-raiz-v3

State/ProvinceSanta Catarina

LocalityFlorianopolis

Email Addressgopac@rnp.br

Serial Number1

Version3

Signature AlgorithmSHA-512 with RSA Encryption (1.2.840.113549.1.1.13)

ParametersNone

Not Valid BeforeMonday, 27 January 2020 at 17:33:43 Brasilia Standard Time

Not Valid AfterFriday, 20 January 2045 at 17:33:43 Brasilia Standard Time

Public Key Info

AlgorithmRSA Encryption (1.2.840.113549.1.1.1)

ParametersNone

Public Key512 bytes : D6 45 97 20 1D B7 F2 F5 ...

Exponent65537

Key Size4.096 bits

Key UsageVerify

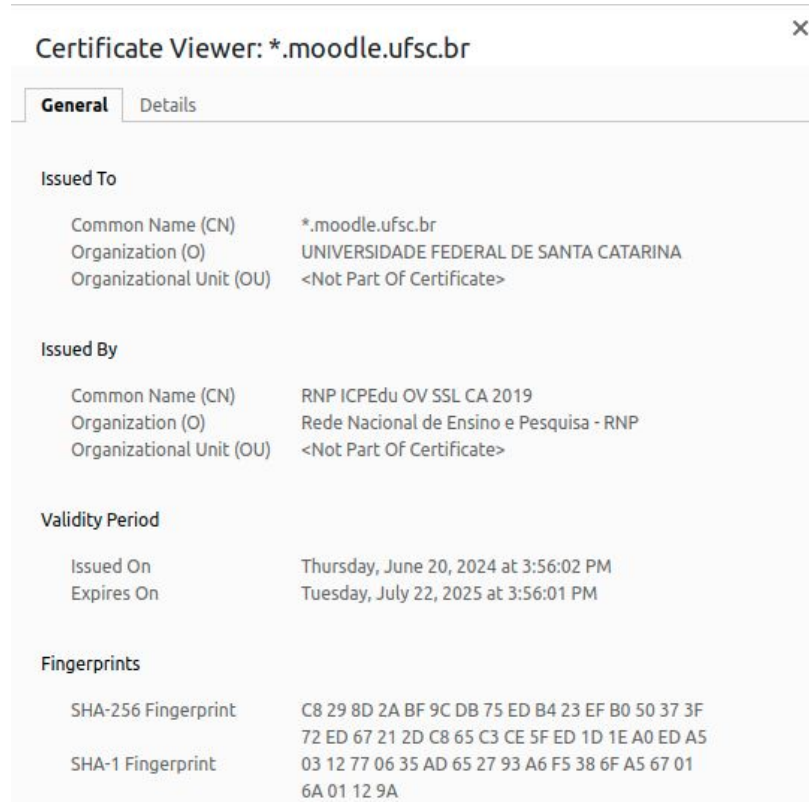
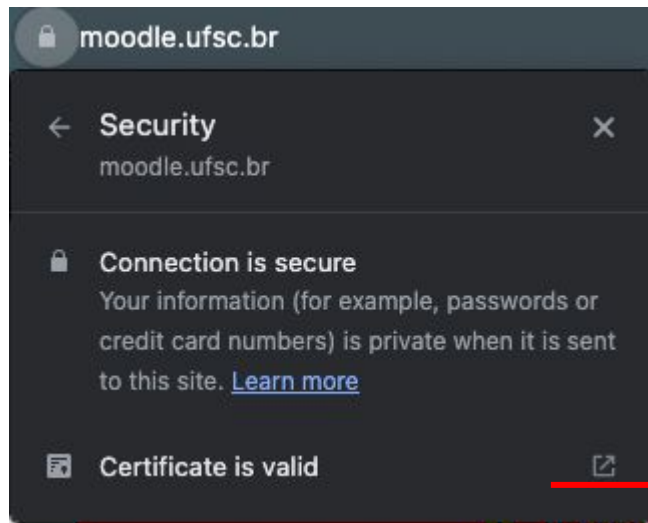
Signature512 bytes : 21 F0 8F 1D D4 AA 74 EE ...

ExtensionKey Usage (2.5.29.15)

CriticalNO

UsageKey Cert Sign, CRL Sign

Certificado SSL



Revogação de certificados

- Existem situações onde deseja-se invalidar um certificado antes do seu prazo de expiração
- Motivos de revogação:
 - Comprometimento da chave privada
 - Alterações nos atributos ou permissões do titular
 - Certificado emitido incorretamente
 - Término do relacionamento entre entidade e AC
- A AC mantém a Lista de Certificados Revogados (LCR) emitida por ela
 - Emitida periodicamente
 - Contém emissor, data de criação, data programada da próxima emissão de LCR, lista de certificados revogados

Thais Bardini Idalino:07448185918

Purpose #1 Client Authentication (1.3.6.1.5.7.3.2)

Purpose #2 Email Protection (1.3.6.1.5.5.7.3.4)

Extension Subject Key Identifier (2.5.29.14)

Critical NO

Key ID 4C 7E 60 DA 13 9A D9 E8 27 6B E0 92 6A 01 03 0F 95 B3 53 95

Extension Authority Key Identifier (2.5.29.35)

Critical NO

Key ID AE D7 C0 C3 F7 30 6C E2 E2 A8 BC 28 8F 67 A1 FA 00 F2 33 4E

Extension Subject Alternative Name (2.5.29.17)

Critical NO

RFC 822 Name thaisidalino@gmail.com

Other Name

Type ID (2.16.76.1.3.1)

Value A0 39 04 37 31 37 31 32 ...

Other Name

Type ID (2.16.76.1.3.6)

Value A0 0E 04 0C 30 30 30 30 30 30 30 30 30 30 30 30

Other Name

Type ID (2.16.76.1.3.5)

Value A0 2B 04 29 30 30 30 30 ...

Extension Certificate Policies (2.5.29.32)

Critical NO

Policy ID #1 (1.3.6.1.4.1.15996.1.1.4)

Qualifier ID #1 Certification Practice Statement (1.3.6.1.5.7.2.1)

CPS URI <https://repositorio.icpedu.rnp.br/ac-pessoa/doc-ac-pessoa.pdf>

Extension CRL Distribution Points (2.5.29.31)

Critical NO

URI <https://pessoal.icpedu.rnp.br/public/crl/download/last>

Extension Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)

Critical NO

Method #1 CA Issuers (1.3.6.1.5.5.7.48.2)

URI <https://repositorio.icpedu.rnp.br/ac-pessoa/ac-pessoa-chain>

Method #2 Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

URI <https://pessoal.icpedu.rnp.br/public/ocsp/status>

Atividade: Gerando certificados

- Vamos utilizar as chaves RSA criadas anteriormente:
 - `openssl genrsa -aes256 -out seunome.privada.pem 2048`
 - `openssl rsa -pubout -in seunome.privada.pem -out seunome.publica.pem`
- Gere uma solicitação de assinatura de certificado
 - `openssl req -new -key seunome.privada.pem -out csr.pem`
 - aqui será necessário entrar algumas informações, como país, estado, empresa, nome e email
 - o arquivo `csr.pem` é a requisição de certificado
- Gere um certificado autoassinado
 - `openssl req -x509 -days 365 -key seunome.privada.pem -in csr.pem -out certificate.crt`
 - esse certificado pode ser visualizado no seu sistema operacional ou pelo `openssl`
- Verifique as informações do certificado
 - `openssl x509 -noout -text -in certificate.crt`

Referências

- W. Stallings. *Cryptography and network security*. 7a edição.
 - capítulos 14.3, 14.4, 14.5
- ICP-Brasil:
 - <https://estrutura.it.gov.br/>
 - https://www.gov.br/iti/pt-br/assuntos/icp-brasil/EcosistemaICPBrasil_240822.pdf
 - <https://www.gov.br/iti/pt-br/assuntos/icp-brasil/icp-brasil-18-anos>
- ICPEdu
 - Link para os certificados das ACs: <https://repositorio.icpedu.rnp.br/public/ac>
 - Link para emissão de certificados: <https://pessoal.icpedu.rnp.br/home>
- Caminho de certificação: [RFC 5280](#)
- imagens: Flaticon.com