

# Certificados Digitais X.509

Dênio Mariz  
Outubro 2020

# Gerenciamento de Chaves Públicas

→ Chaves públicas não precisam ser secretas, mas precisam ser **autênticas**

- Suponha que Alice e Bob não se conhecem, como Bob vai saber a chave pública de Alice?
- Se alguém mandar pra Bob a chave pública de Alice, quem garante que ela é mesmo de Alice?

→ Solução:

- Bob deve confiar em alguém que garante que a chave pública é mesmo de Alice
- Bob confia em uma **autoridade certificadora**, que emite um **certificado** contendo a chave pública de Alice

# Certificado Digital

- É um **documento digital assinado** por **A** que afirma (certifica) que uma chave pública **P** pertence à entidade **E**
  - Assinado por uma **autoridade certificadora A**
  - O documento digital contém a chave pública **P**
  - Entidade = pessoa, site web, dispositivo IoT, empresa, Médico
  - Quem assinou atesta que a chave pertence a **E** (é autêntica)
  - Pode ser **revogado** (ex: o dono perdeu a chave privada)
- Premissa básica: você deve confiar na Autoridade Certificadora
- Vantagens
  - Atesta autenticação e integridade da chave pública (assinatura)
  - Permite estabelecer confidencialidade
- Desvantagens
  - Aplicações como sites web devem (quase sempre) **comprar um**

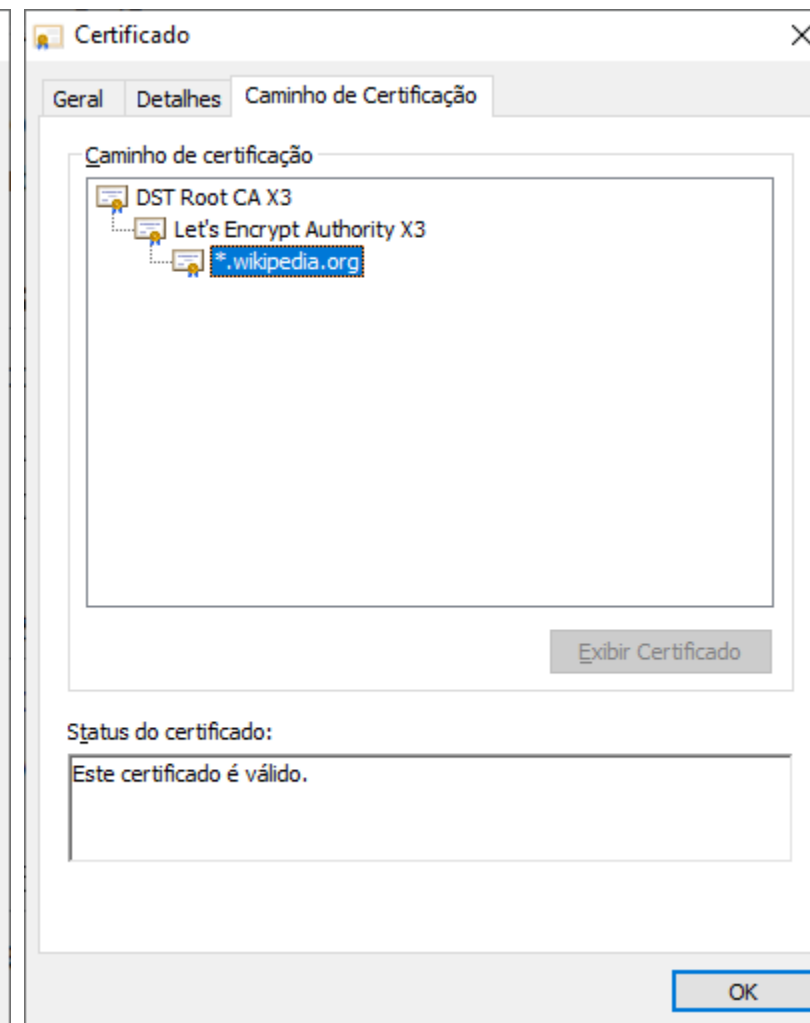
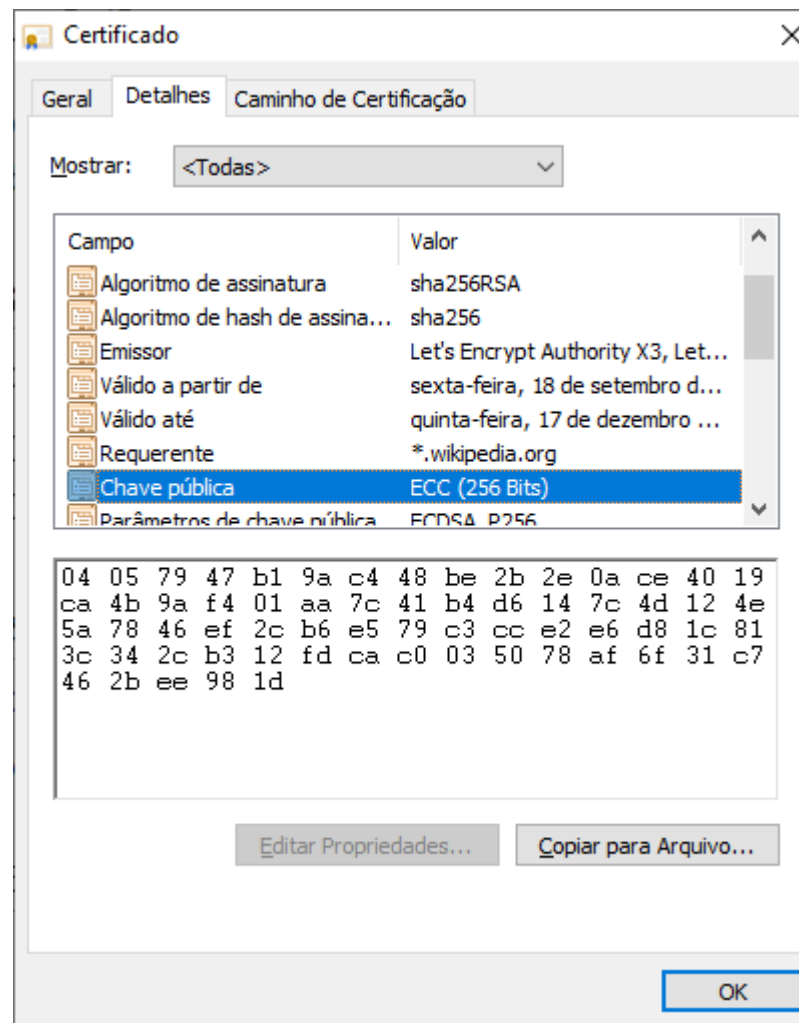
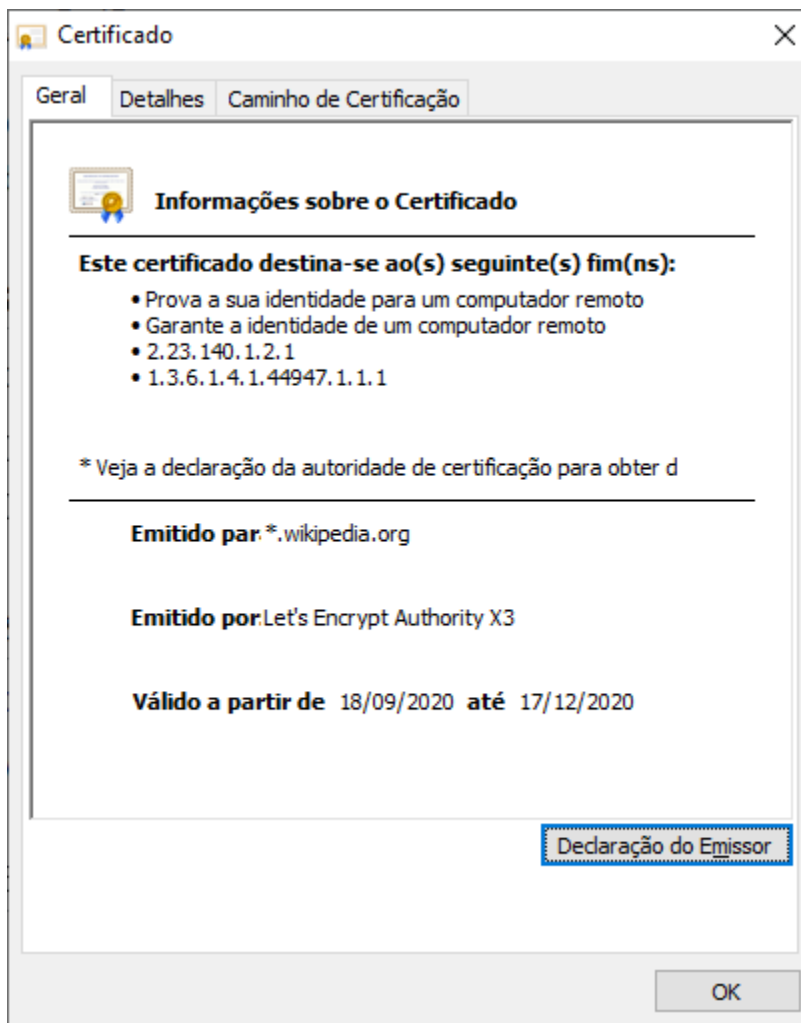
Veja opção  
gratuita em



# Certificado: padrão ITU X.509

Version	Versão do X.509 (atual=v.3)
Serial Number	Número único por CA (usado na revogação)
Issuer	Nome do CA (padrão X.500)
Validity period	Data de Início e fim da validade do certificado
Subject	Entidade para a qual a chave está sendo certificada
Public key	<b>A chave pública da entidade + ID do algoritmo</b>
Issuer ID	ID do emissor do certificado (opcional)
Subject ID	ID do dono do certificado (opcional)
Extensions	Muitas extensões foram definidas
Signature Algorithm	Algoritmo usado para assinar o certificado
Signature	<b>Assinatura do certificado (com a chave privada do CA)</b>

# Um Certificado Digital



# Um Certificado Digital

**Certificado**

Geral Detalhes Caminho de Certificação

**Informações sobre o Certificado**

Este certificado destina-se ao(s) seguinte(s) fim(ns):

- Prova a sua identidade para um computador remoto
- Garante a identidade de um computador remoto
- 2.23.140.1.2.1
- 1.3.6.1.4.1.44947.1.1.1

\* Veja a declaração da autoridade de certificação para obter d

Emitido por \*.wikipedia.org

Emitido por Let's Encrypt Authority X3

Válido a partir de 18/09/2020 até 17/12/2020

**Finalidade**

**Sujeito (dono)**

**Autoridade Certificadora**

**Validade**

**Certificado**

Geral Detalhes Caminho de Certificação

Mostrar: <Todas>

Campo	Valor
Algoritmo de assinatura	sha256RSA
Algoritmo de hash de assina...	sha256
Emissor	Let's Encrypt Authority X3, Let...
Válido a partir de	sexta-feira, 18 de setembro d...
Válido até	quinta-feira, 17 de dezembro ...
Requerente	*.wikipedia.org
Chave pública	ECC (256 Bits)
Parâmetros de chave pública	ECDSA P256

04 05 79 47 b1 9a c4 48 be 2b 2e 0a ce 40 19  
ca 4b 9a f4 01 aa 7c 41 b4 d6 14 7c 4d 12 4e  
5a 78 46 ef 2c b6 e5 79 c3 cc e2 e6 d8 1c 81  
24 2c b3 12 fd ca c0 03 50 78 af 6f 31 c7  
ee 98 1d

Editar Propriedades... Copiar para Arquivo...

OK

**Certificado**

Geral Detalhes Caminho de Certificação

Caminho de certificação

- DST Root CA X3
  - Let's Encrypt Authority X3
    - \*.wikipedia.org

Exibir Certificado

Status do certificado:  
Este certificado é válido.

OK

# Um Certificado Digital

The image displays three overlapping screenshots of a digital certificate viewer window, with red callout boxes highlighting specific details.

**Central Screenshot (Detailed View):**

- Tabs:** Geral, Detalhes, Caminho de Certificação.
- Mostrar:** <Todas>
- Table of Attributes:**

Campo	Valor
Algoritmo de assinatura	sha256RSA
Algoritmo de hash de assinatura	sha256
Emissor	Let's Encrypt Authority X3
Válido a partir de	sexta-feira, 18 de set
Válido até	quinta-feira, 17 de dezemb
Requerente	*.wikipedia.org
Chave pública	ECC (256 Bits)
Parâmetros de chave pública	ECDSA P256
- Hexadecimal Data:**

```

05 79 47 b1 9a c4 48 be 2b 2e 0a ce 40 19
4b 9a f4 01 aa 7c 41 b4 d6 14 7c 4d 12 4e
5a 78 46 ef 2c b6 e5 79 c3 cc e2 e6 d8 1c 81
3c 34 2c b3 12 fd ca c0 03 50 78 af 6f 31 c7
46 2b ee 98 1d

```

**Annotations:**

- Lista de atributos X.509:** Points to the table of attributes.
- Valor da chave pública:** Points to the 'Chave pública' row in the table.
- Tipo de Chave pública:** Points to the 'Parâmetros de chave pública' row in the table.

**Left Screenshot (Summary View):**

- Informações sobre o Certificado:**
  - Este certificado destina-se ao(s) seguinte(s) fim(ns):
    - Prova a sua identidade para um computador remoto
    - Garante a identidade de um computador remoto
    - 2.23.140.1.2.1
    - 1.3.6.1.4.1.44947.1.1.1
  - \* Veja a declaração da autoridade de certificação para obter d
  - Emitido por: \*.wikipedia.org
  - Emitido por: Let's Encrypt
  - Válido a partir de: 18/09/2020
- Buttons:** Declaração do Emissor, OK.

**Right Screenshot (Status View):**

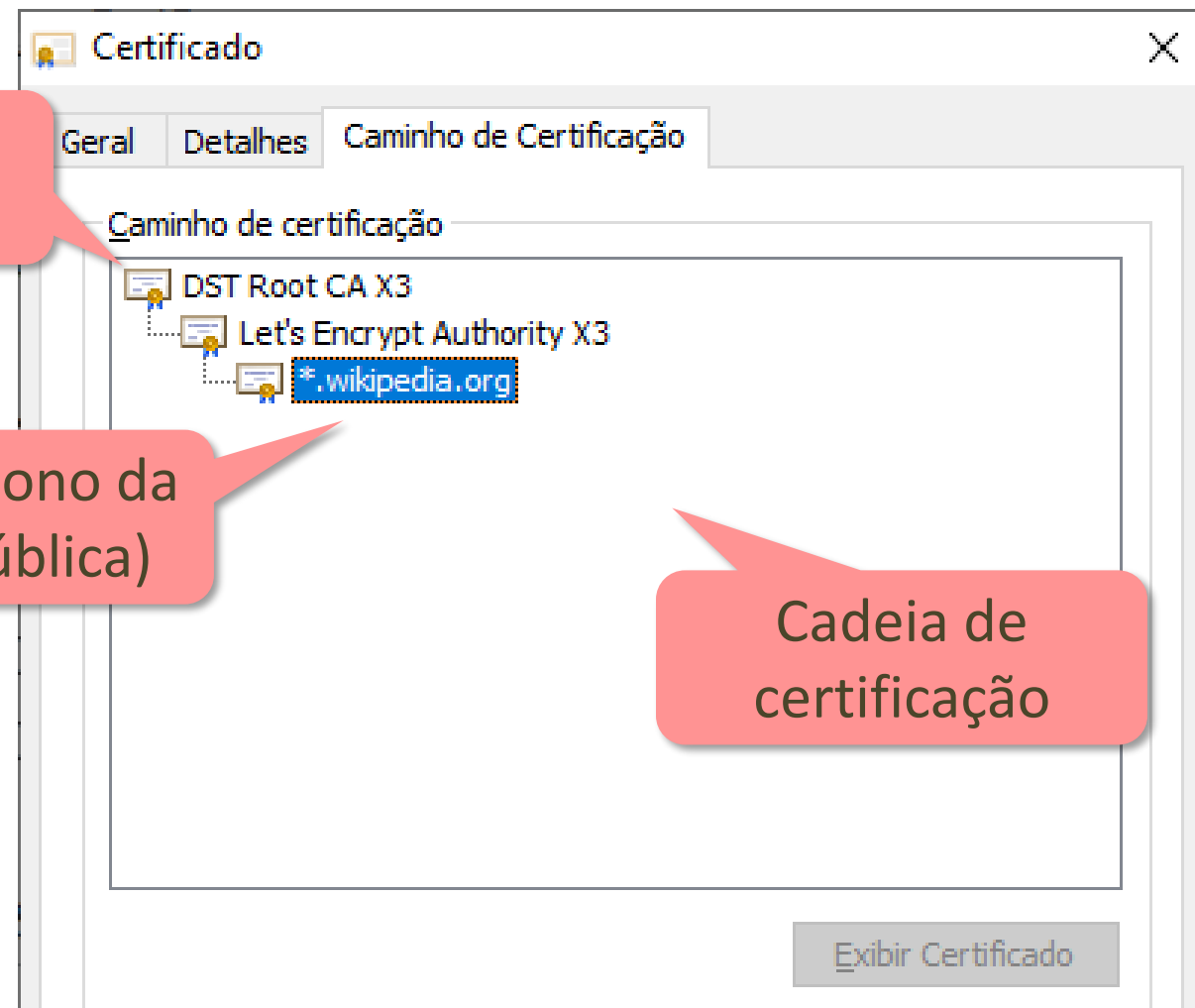
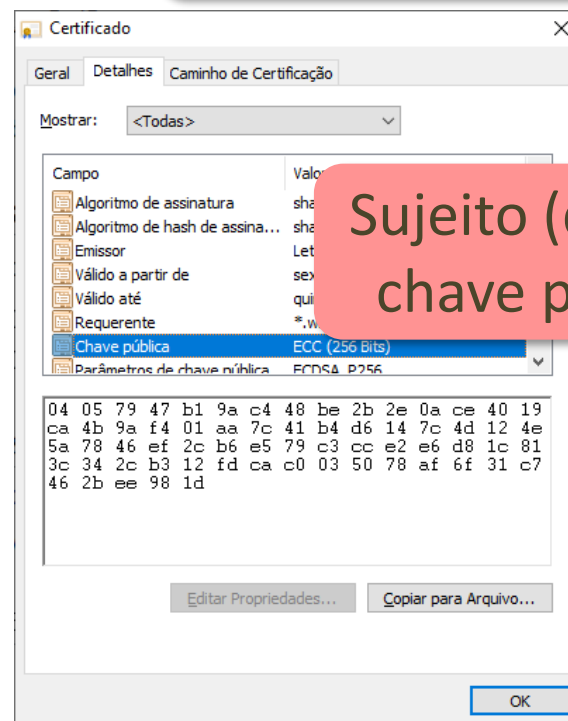
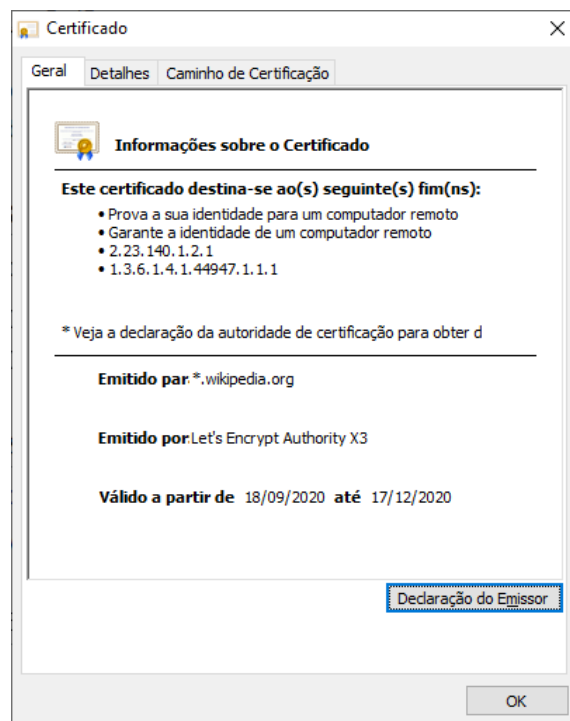
- Status do certificado:** Este certificado é válido.
- Buttons:** Exibir Certificado, OK.

# Um Certificado Digital

AC raiz

Sujeito (dono da  
chave pública)

Cadeia de  
certificação



Status do certificado:

Este certificado é válido.



# Extensões X.509 - Finalidade

Nome	Object ID	Finalidade
serverAuth	<b>1.3.6.1.5.5.7.3.1</b>	TLS Web server authentication
clientAuth	<b>1.3.6.1.5.5.7.3.2</b>	TLS Web client authentication
codeSigning	<b>1.3.6.1.5.5.7.3.3</b>	Code signing
emailProtection	<b>1.3.6.1.5.5.7.3.4</b>	E-mail protection
timeStamping	<b>1.3.6.1.5.5.7.3.8</b>	Timestamping
ocspSigning	<b>1.3.6.1.5.5.7.3.9</b>	OCSPstamping
...		

Fonte: RFC 3280

# Atributos do Certificado

## Emitido para:

Common Name (CN)	www.receita.fazenda.gov.br
Empresa (O)	ICP-Brasil
Unidade Organizacional (OU)	SUPCD
Número de série	27:1A

## Emitido por:

Common Name (CN)	Autoridade Certificadora do SERPRO - SRF
Empresa (O)	ICP-Brasil
Unidade Organizacional (OU)	Secretaria da Receita Federal - SRF

## Validade:

Emitido em	18/2/2005
Válido até	23/12/2005

## Assinaturas:

Assinatura SHA1	0D:88:BF:68:13:75:62:AF:25:90:D1:9C:19:E0:04:D5:4D:5E:74:12
Assinatura MD5	FF:BC:54:50:14:87:01:5E:23:81:CE:27:D1:02:60:8A

## Abreviações comuns para Atributos

**C**=Country  
**L**=Locality Name  
**S, ST**=State or province  
**MAIL**=Email address  
**O**=Organization  
**OU**=Organizational unit  
**CN**=Common name (subject or issuer)  
**STREET**=Street address

# Revogação de Certificados

- Certificados emitidos podem ser revogados em caso de quebra de confiança
  - Sua chave privada caiu na mão de terceiros
  - Você perdeu sua chave privada
  - Solicite à AC a revogação do seu certificado
- Certificate Revocation List (CRL)
  - Anunciados periodicamente pela AC (pushing)
  - Lista os números de série dos certificados revogados (cancelados)
  - CRL não precisa incluir certificados expirados
  - Ao receber um certificado, deve-se consultar a CRL

# Padrões de codificação de Certificados X.509

Codificação	Padrão	Extensão do arquivo
ASCII Base64	PEM Privacy Enhanced Mail	PEM CRT CER KEY (chave privada)
	PKCS#7 Public Key Cryptography Standards	P7B P7C
Binário	DER Distinguished Encoding Rules	DER CER
	PKCS#12 Public Key Cryptography Standards	PFX P12

# Formatos de Armazenamento de Certificado

- ➔ \*.PFX, \*.P12 - Personal Information Exchange Format (PKCS#12)
  - Pode armazenar múltiplos certificados (ex: toda a cadeia de certificação)
  - Suporta armazenamento de chaves pública + chave privada
- ➔ \*.CER, \*.CRT - Base64-encoded or DER-encoded binary X.509 Certificate
  - Armazena um único certificado
  - Não suporta armazenamento de chave privada
- ➔ \*.DER - DER-encoded binary X.509 Certificate
  - Armazena um único certificado
  - Não suporta armazenamento de chave privada
- ➔ \*.CSR - Certificate Signing Request
  - Não é um certificado
  - Reúne informações para solicitar um certificado a uma AC
- ➔ \*.P7B, \*.P7R, \*.SPC - Cryptographic Message Syntax Standard (PKCS#7)
  - Pode armazenar múltiplos certificados (ex: toda a cadeia de certificação)
  - Não suporta armazenamento de chave privada

# Exemplo: Privacy Enhanced Message

```
$ cat arquivo.PEM
```

```
-----BEGIN PUBLIC KEY-----
```

```
MIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA0gznhv/OGF3fEr1pDU/F  
mG0gy/Aked3a1R1ew7oz4nwfAxo5kkRHM72uQsR9cyKPmnqciR4ctRHXuVe7gYsf  
bM9azFL10TCAXGh910YPdcG6LC2BNmNFilPxQAr1t20Crw4cwK577hVR2GVSGBCO  
077yvsI5t2/P77yBp8LWe5v/mY3Y9E/xginea8e0oDdNvssrbBNA7692/BZ1fvSt  
7arSYGDtuaECKNXres0RpC/tTa6bAVsGeddnTahu/vb9Fd9JGAY6kGX5zn8qh8Y+  
YLeoXPF5tpoS0L2vgCcetTFG5RRh71t7Gb46Tvg1NIGE7yTvq0BID8EZ1qSsdBQm  
2wIDAQAB
```

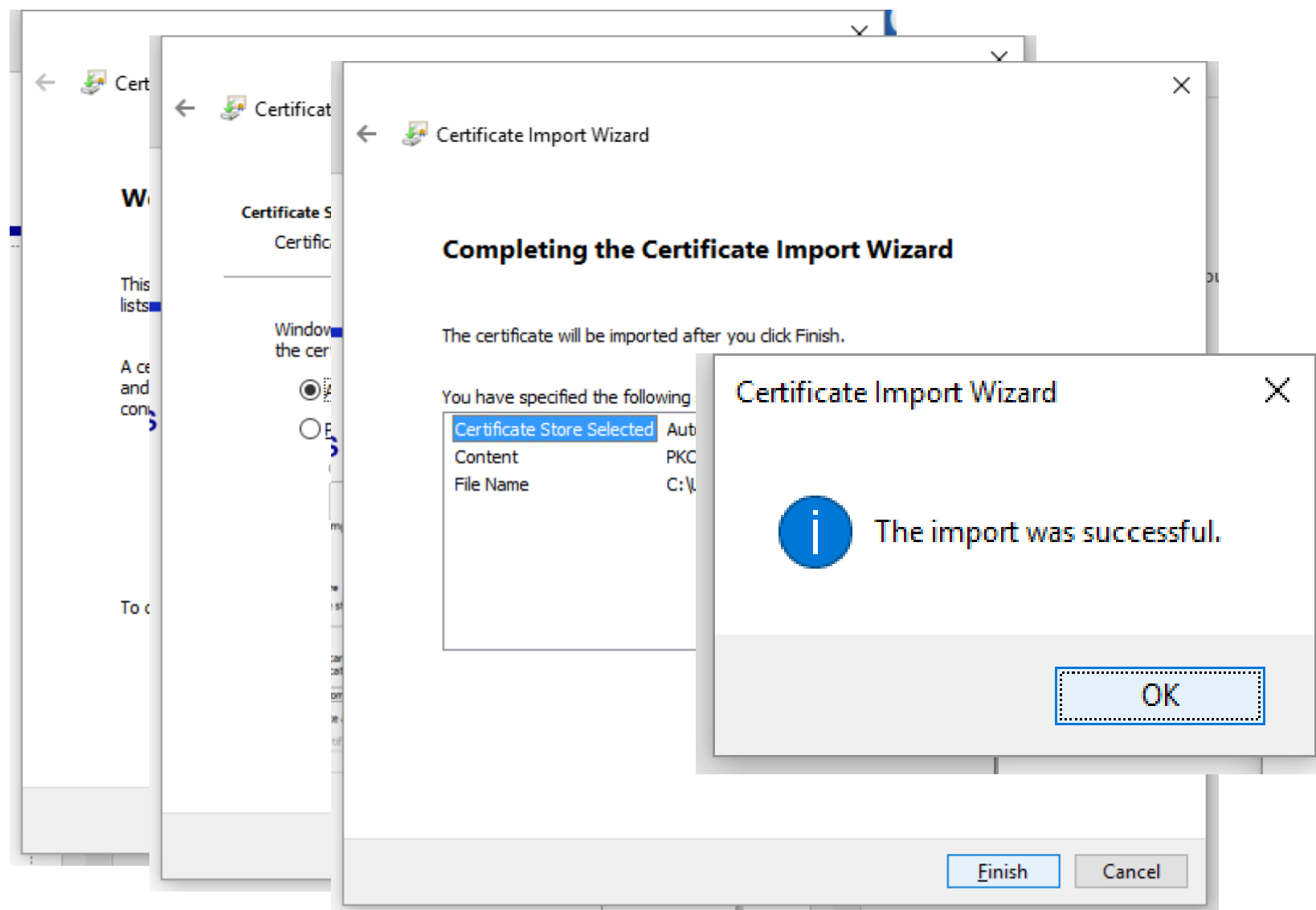
```
-----END PUBLIC KEY-----
```

```
$
```

Mecanismo  
Base64

Text content	M								a								n							
ASCII	77								97								110							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19								22								5							
Base64 Encoded	T								W								F							

# Instalando certificados



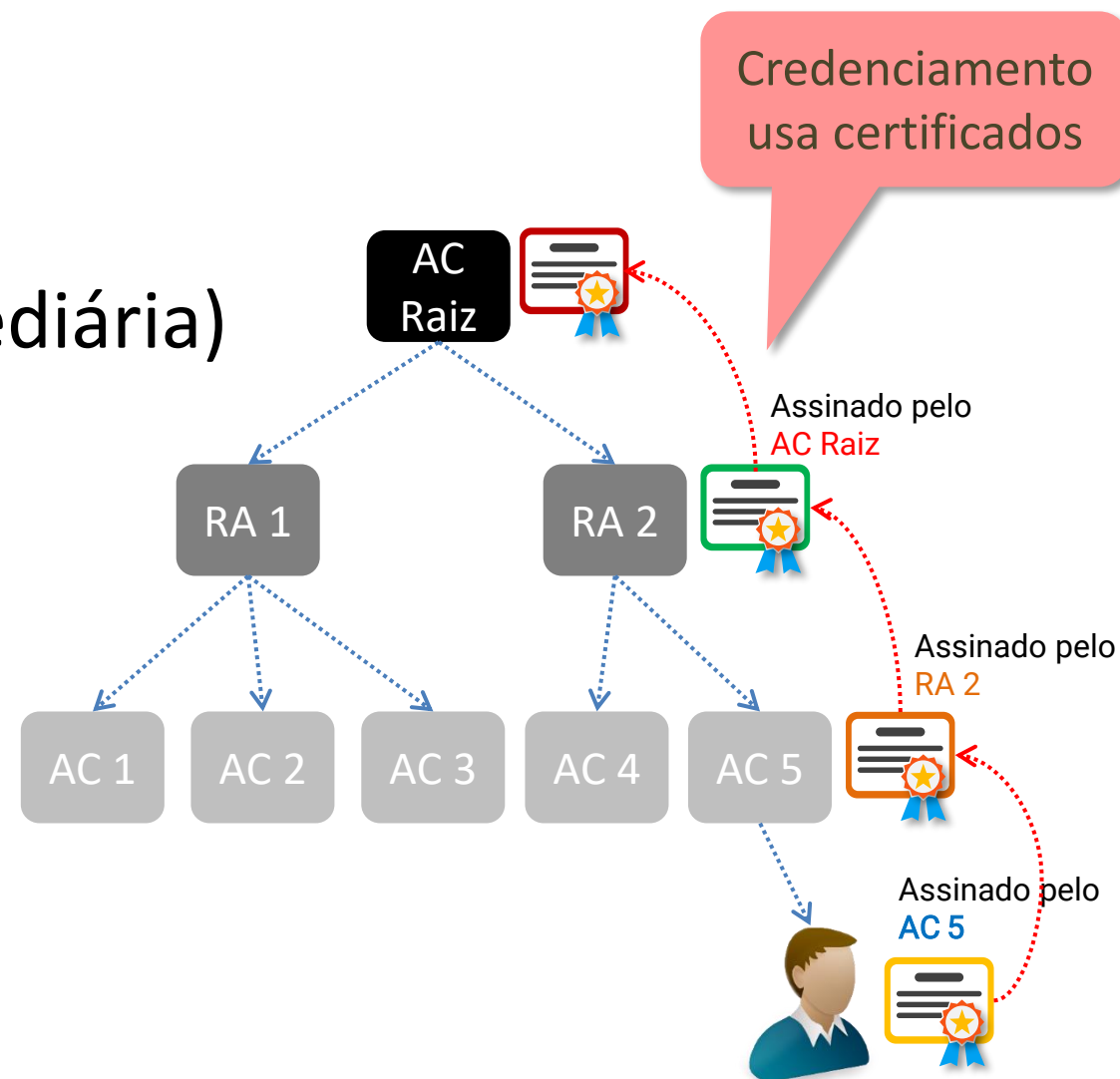
# Public Key Infrastructure (PKI) **ou** Infraestrutura de Chave Pública (ICP)


- Autoridades certificadoras (Certificate Authorities - CA)
  - Emitem e revogam certificados
- Autoridades de Registro (Registration Authorities - RA):
  - Verificam a ligação entre a chave pública e a identidade do dono (em certos casos pessoalmente)
- Assinante (ou dono, ou sujeito) do certificado
  - Pessoa, máquina, software [...] dono certificado (da chave pública nele contido)
- Repositórios
  - Armazenam e disponibilizam certificados e CRL (lista de revogação de certificados)



# PKI – Public Key Infrastructure

- Credenciamento hierárquico
- Nivel 1 = AC Raiz
- Nivel 2 = AC Regional (intermediária)
  - Pode haver vários níveis intermediários
- Nivel N = AC local
  - Ex: uma em cada estado





**ITI**  
 Instituto Nacional de  
 Tecnologia da Informação

Contrair estrutura

Pesquisar
 Detalhes

### DETALHES DA EMPRESA

CNPJ	00.360.305/0001-04
Nome	AC CAIXA SPB
Tipo	AC 2º Nível
Situação	Credenciado
Credenciamento	21/11/2014
Processo	00100.000299/2013-05
Telefone	(61) 3206-7277

### ENTIDADES VINCULADAS

AR	1
----	---

### ENDEREÇO

Logradouro	Setor Bancario Sul
Complemento	Quadra 4 Bloco A Lotes 3/4
Bairro	Asa Sul
CEP	70.092-900
Município	Brasília
UF	DF

AC RAIZ

AC 1 AC CAIXA

AC 2 AC CAIXA PF

AC 2 AC CAIXA PJ

AC 2 AC CAIXA PJ SSL

AC 2 AC CAIXA SPB

AR AR CAIXA

AC 1 AC CERTISIGN

AC 2 AC CERTISIGN MULTIPLA

AR AR ASSOCIAÇÃO COMERCIAL E EMPRESARIAL DE LARANJAL PAULISTA

AR AR CERTICONT

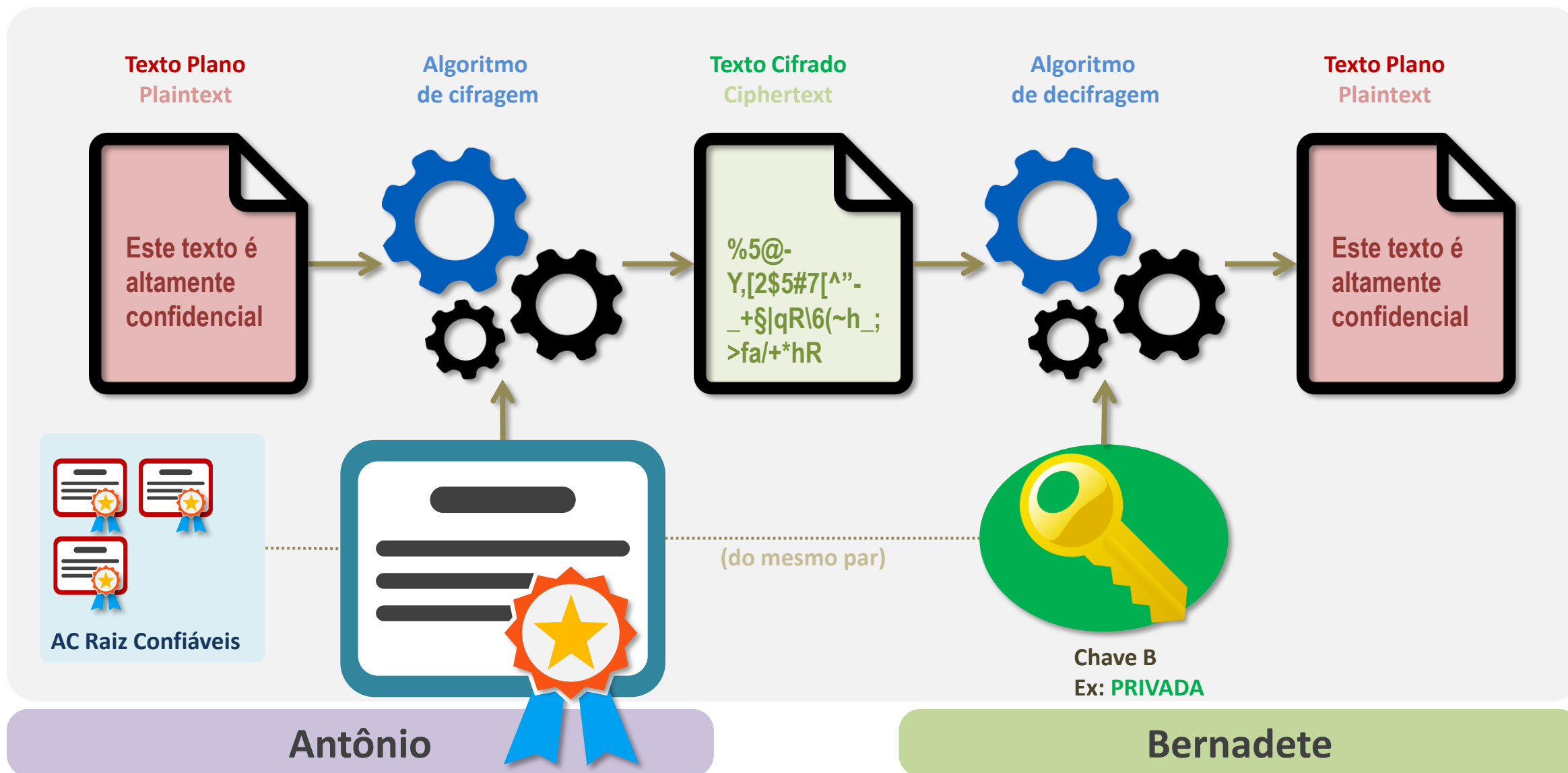
AR AR A.C.E.J.B.

Legenda

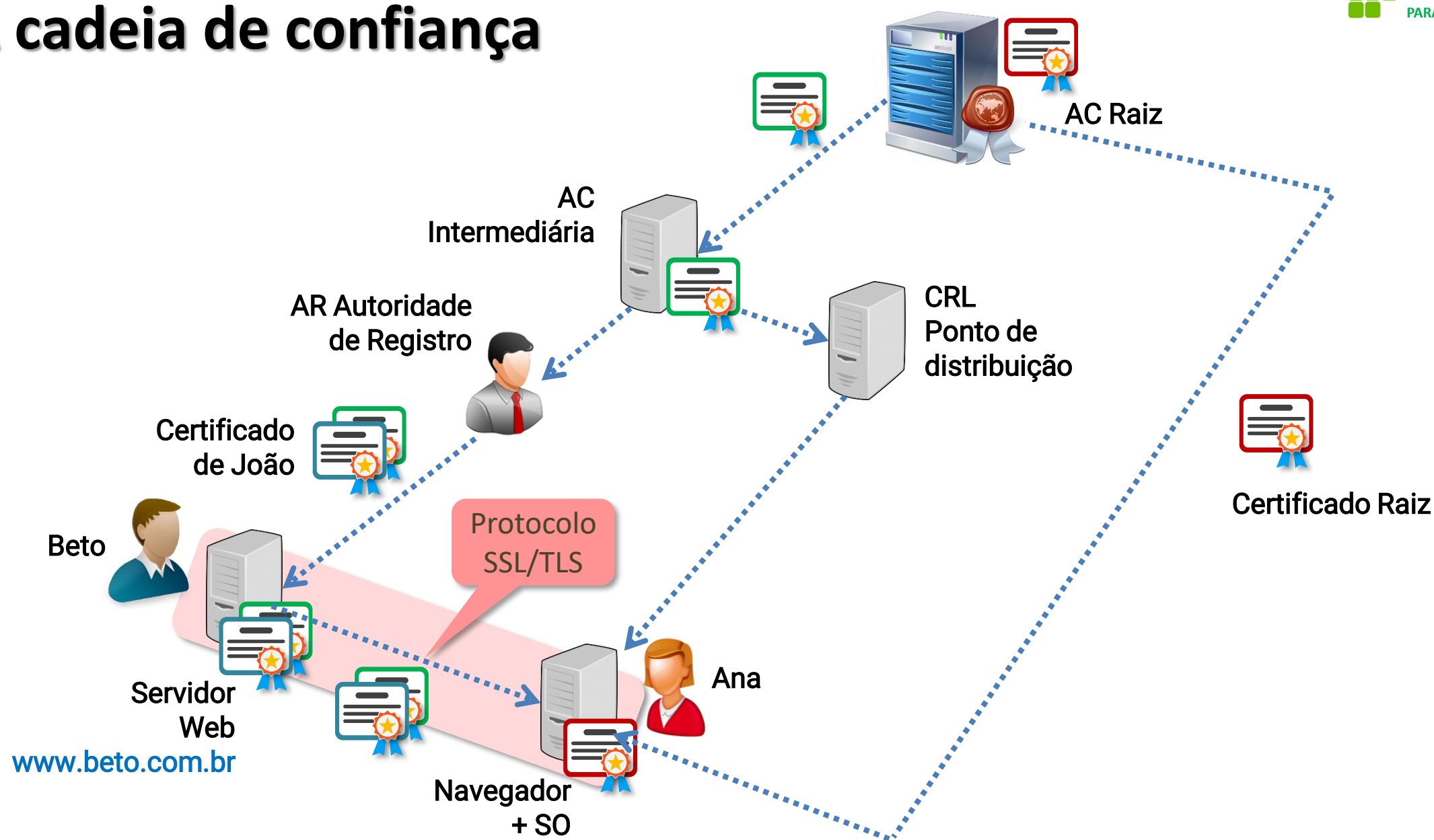
- Autoridade Certificadora Raiz
- Autoridade Certificadora de 1º Nível
- Autoridade Certificadora de 2º Nível
- Autoridade de Registro
- Em credenciamento

<https://estrutura.iti.gov.br/>

# Confidencialidade com Chaves Assimétricas



# A cadeia de confiança



Exemplo de Certificado Real  
**[www2.bancobrasil.com.br/aapf](http://www2.bancobrasil.com.br/aapf)**



# Certificados Digitais

Dênio Mariz  
[denio@ifpb.edu.br](mailto:denio@ifpb.edu.br)