PUC Minas

Plataforma Node.js

Fundamentos de Segurança

Prof. Rommel Vieira Carneiro

Autenticação *vs* Autorização

Autenticação

Verifica se o usuário é quem diz ser

Autorização

Verifica as permissões de acesso do usuário

Fontes:

- Authentication vs. Authorization (okta)

Autenticação Multi-Fator (MFA)

A Autenticação multi-fator é um mecanismo de segurança que utiliza várias estratégias para identificar um usuário em sistemas eletrônicos.

Fatores de Identificação

Conhecimento

Algo que você sabe

Exemplos

- Senhas
- PIN
- Padrões

Posse

Algo que você possui

Exemplos

- Smartcard
- Telefone celular
- Tokens

Herança

Algo que você é

Exemplos

- Íris do olho
- Digitais
- Voz
- Face

Localização

Onde você está

Exemplos

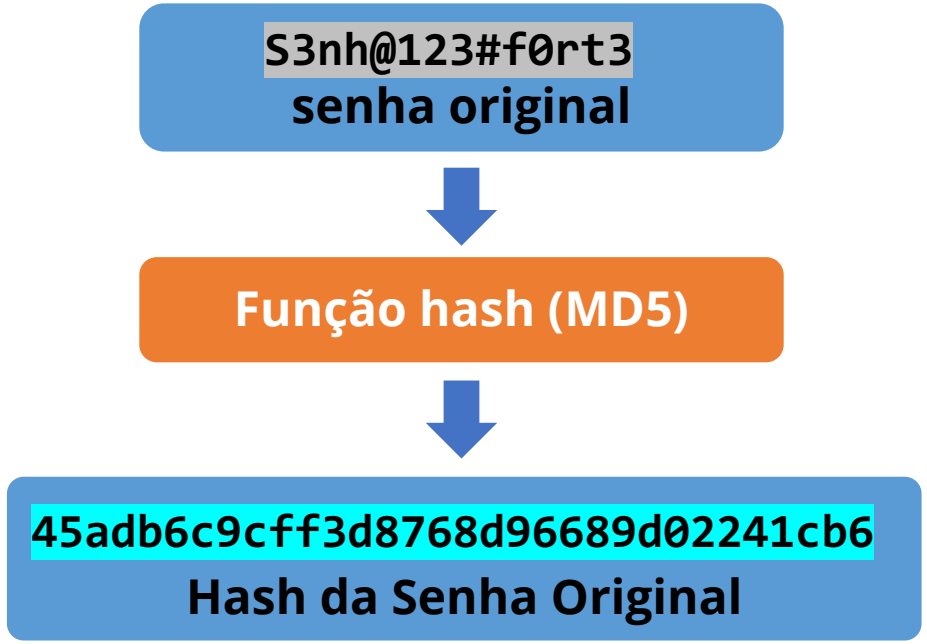
- Coordenadas GPS
- Endereço IP

Message Digest – Função Hash

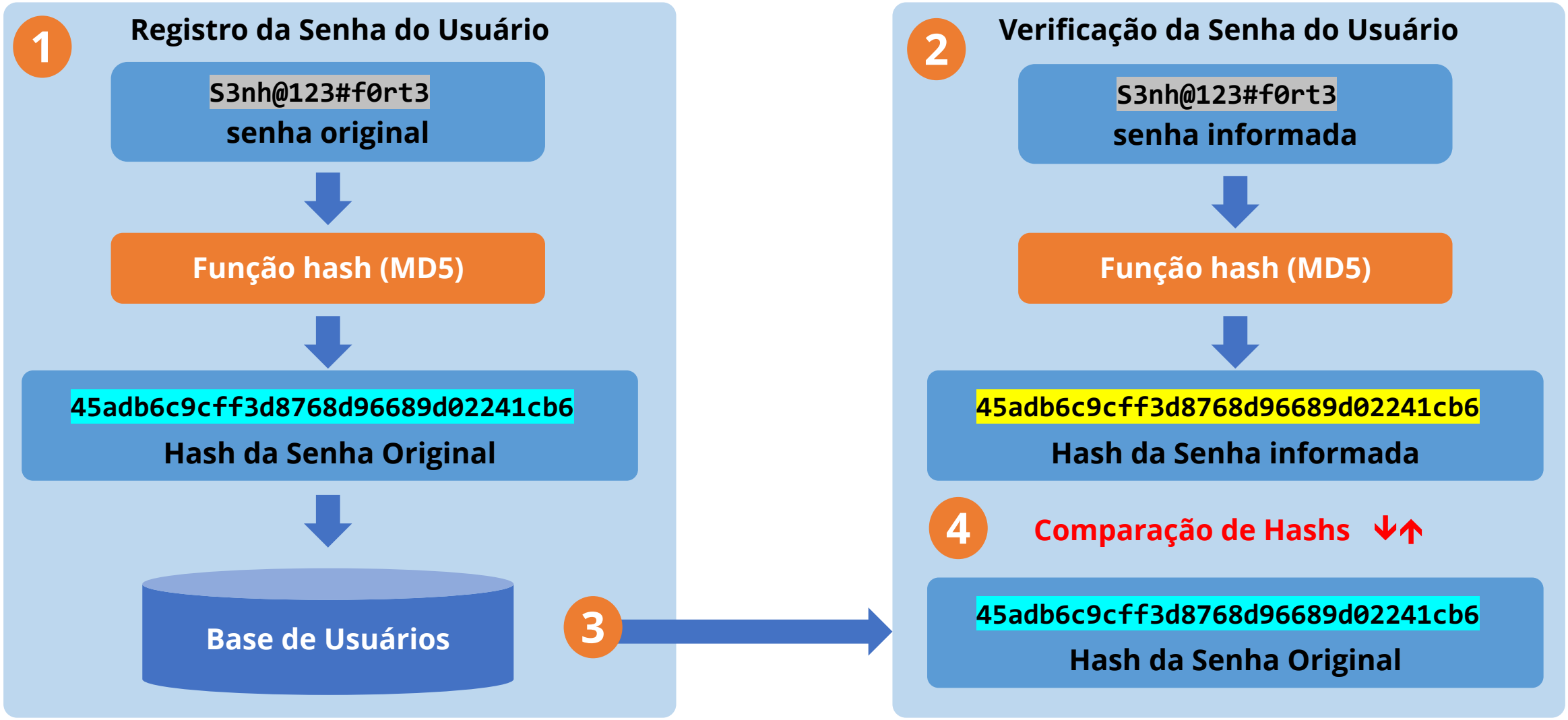
Função hash: algoritmo que produz uma sequência diferentes para cada entrada e de tamanho fixo não reversíveis (não restauram a mensagem original).

Algoritmos

- **Message Digest Algorithm (MD5)**
  - Resumo de mensagem de 128bits
  - Documentação RFC-1321
- **SHA-1**
  - Resumo de mensagem de 160bits
  - Padrão no EUA

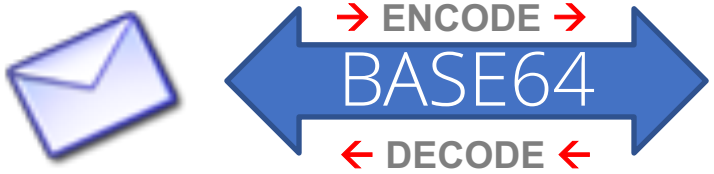


Senhas seguras com Hash



Codificação Base64

Método utilizado para converter dados binários em texto e vice-versa.



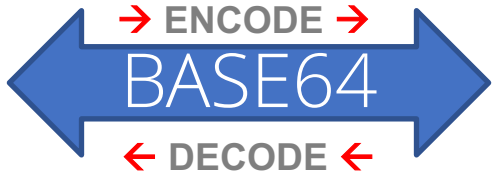

```
iVBORw0KGgoAAAANSUhEUgAAABAAAAAQCAYAAAAf8/9hAAAABGdBTUEAAK/INwWK6QAAABl0RVh0U29m
dHdhcmUAQWRvYmUgSW1hZ2VSZWFkeXHJZTwAAANdSURBVHjaYvz//z8DJQAggBh9fecyfPr8i4GPl5vh
+/cfDL9//WVgYeVk+P37H8O/v/8Zvv34K8TMzJKiqa5YdOfO0e/Hjjc7MDD8fMjAwAw2ACCAWHCZ/PPn
Lx4mJtYKJSXJJG8fTUlTY2WGbbsVGS5fXVH1+dOVdJg6gADCMODvv39Mf3/8rlNSls60d9AUs3OQZZAS
Y2M4d+UPg42zPIPZ1tCQvXuu1DEw/HvJwMDEABBAYAP+/fvP8Of3X67//xlrlBTl0mzstYStrIEaJVkZ
+HkZGC5e+M7w5z8zg7QkA4Ovf4jQoYOLin//vlsGtI4BIIBABohxcbHnSUqJpFvZaolYWMozSIozM7Cx
MTBwsTMwvHv7h+H1278M8kocDMx/GBicnbQYDAwDok+f6m0B6v0EEEAsgoI8J+3t1RRs7LQY5GTZGNhY
gQ5jQnjp7q3vDKLCQJfwMDIwACNMUQHkijDJs2eWZ//796wdIICYjYx8W/TMNNmevXgHVPye4c2r7wzf
vv8FxgAjw7Onvxg+fvzLoKLKzcDCwsjADAx4Lk4GBgEBccb9B+4ovH1zdhFAADH//cuu5OHjb6SgLs7A
zsHNAAwHhk8ffjM8evid4d27nwzqmnwMfHwsYFexAD3MDKRlZJgYXr8XEzx0YMdLgABifvfu7W1RQc14
OztddH4OVgYxYU4GWVluBkVFHgZFJW4GTk5IRDEDKS4uiCHPnjEwnDrzkvH0qV2MAAEEdBYvg65u3Kqj
xz79f/3m///nz/7/fwOkP378///r1///v3/////v3/9g8BYoPnvWnf9mZg1/2NnVzzMyMvsDBBDQVDEG
Dg4l47rabd8/f/7///2H//8/APGXL/////kD0QgycNbMG/9tbet+s7GpngM6KB6IOUAuAwggBi5uaWDS
FWIwMkzfc+Xyj/+/fyM0vn717//c2Tf/W1tV/2ZmVjwFVB+LnvgAAoiBg1OCgY1dmIGH18i+r+f4b5DG
ly9BNl7+b21d8YuFRek0UF0UQgdIPyOcBxBALHx80sD4/c/w7z/bwc1b1p9mZWO13LBh7e8DB5ed/fv3
YR9QzXog/oMrzwAEECMnpxDYRGBQgaJQ6+8/jsI/v58fAgoux64R5IK/DOBUBQQAAQYAP5FRv1nW25oA
AAAASUVORK5CYII=
```

Base64 é muito utilizado na Internet pois vários protocolos de aplicação aceitam apenas dados em texto (email, http). É usado em conjunto com o padrão MIME.

Codificação Base64

Senhas são codificadas via Base64 para garantir que os caracteres a serem enviados na comunicação são strings ASCII válidas

`Rommel:Senha@123`



`Um9tbWVsOlNlbmhhQDEyMw==`

IMPORTANTE

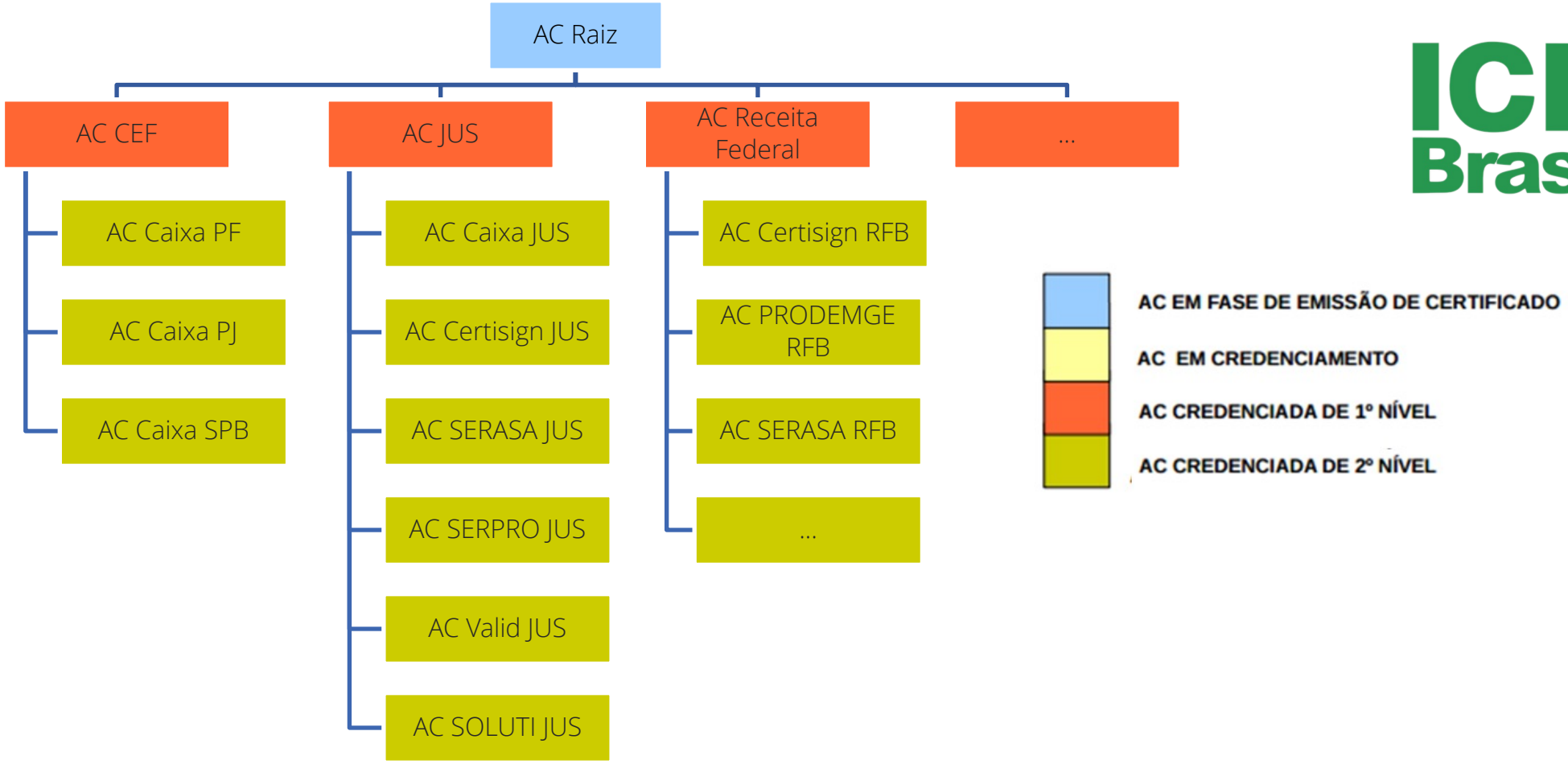
Embora seja uma codificação, Base64 não é uma forma de criptografia e deve ser considerado como dados sendo passados de forma aberta.

Internet X.509 Public Key Infrastructure (PKI)

Conceitos

- **ICP – Infraestrutura de Chaves Públicas**
  Estrutura que abrange um conjunto de entidades AC Raiz, ACs, ARs, certificados para prover requisitos de segurança em comunicação de sistemas.
- **AC Raiz – Autoridade Certificadora Raiz**
  Estabelece a cadeia hierárquica de certificados. Estabelece a política de certificados, controla certificados das ACs e mantém a lista de certificados revogados
- **AC – Autoridade Certificadora**
  Responsável por emitir, distribuir, renovar e gerenciar certificados digitais.
- **Certificado Digital**
  Arquivo eletrônico contendo a identidade digital de uma entidade reconhecida pela ICP. Contem: nome da entidade, período de validade, chave pública, nome e assinatura da entidade que assinou o certificado, número de série.

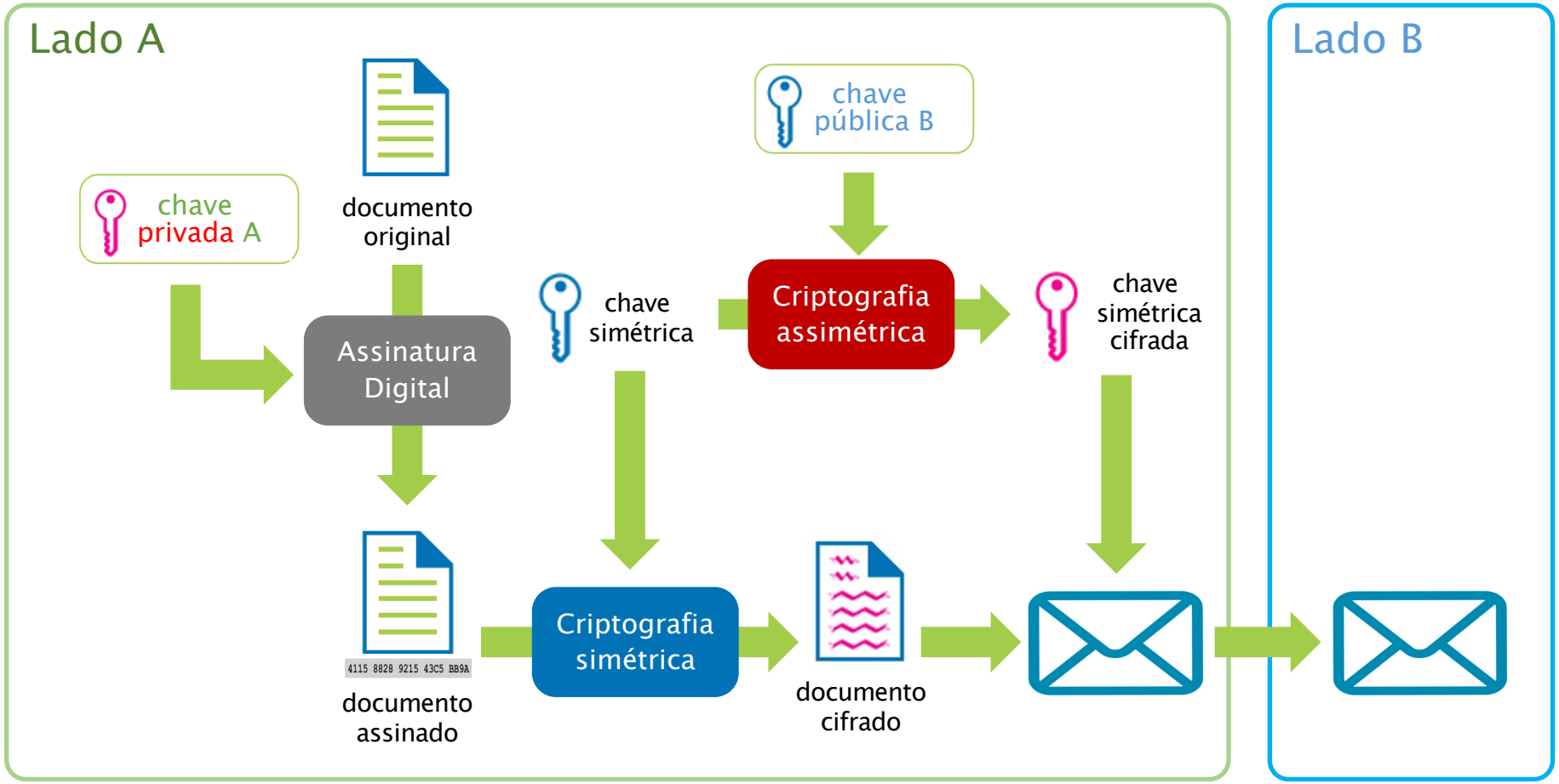
Internet X.509 Public Key Infrastructure (PKI)



Fonte: [Estrutura da ICP – Brasil]

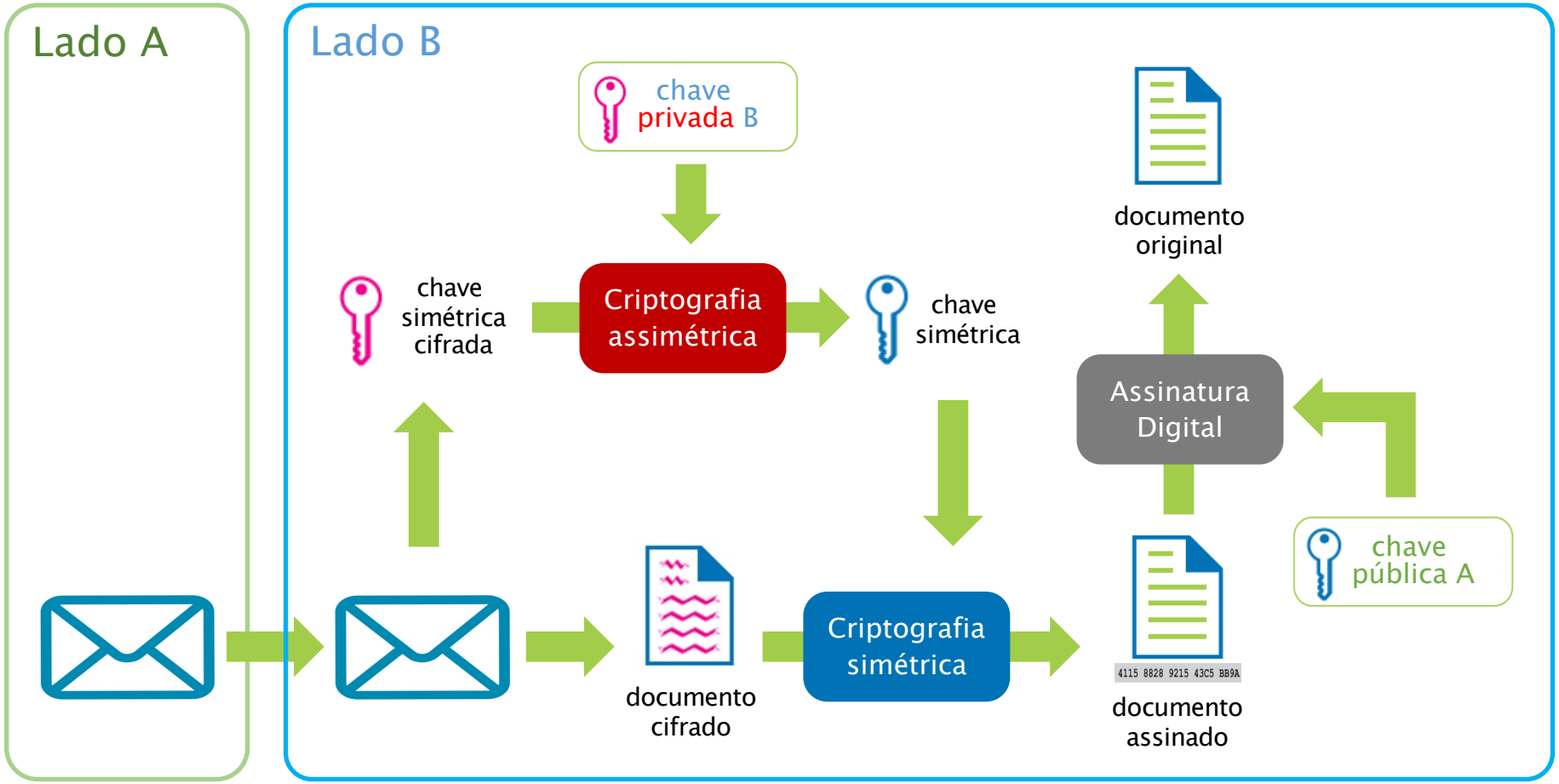
Internet X.509 Public Key Infrastructure (PKI)

Certificação Digital – Envio de Mensagem



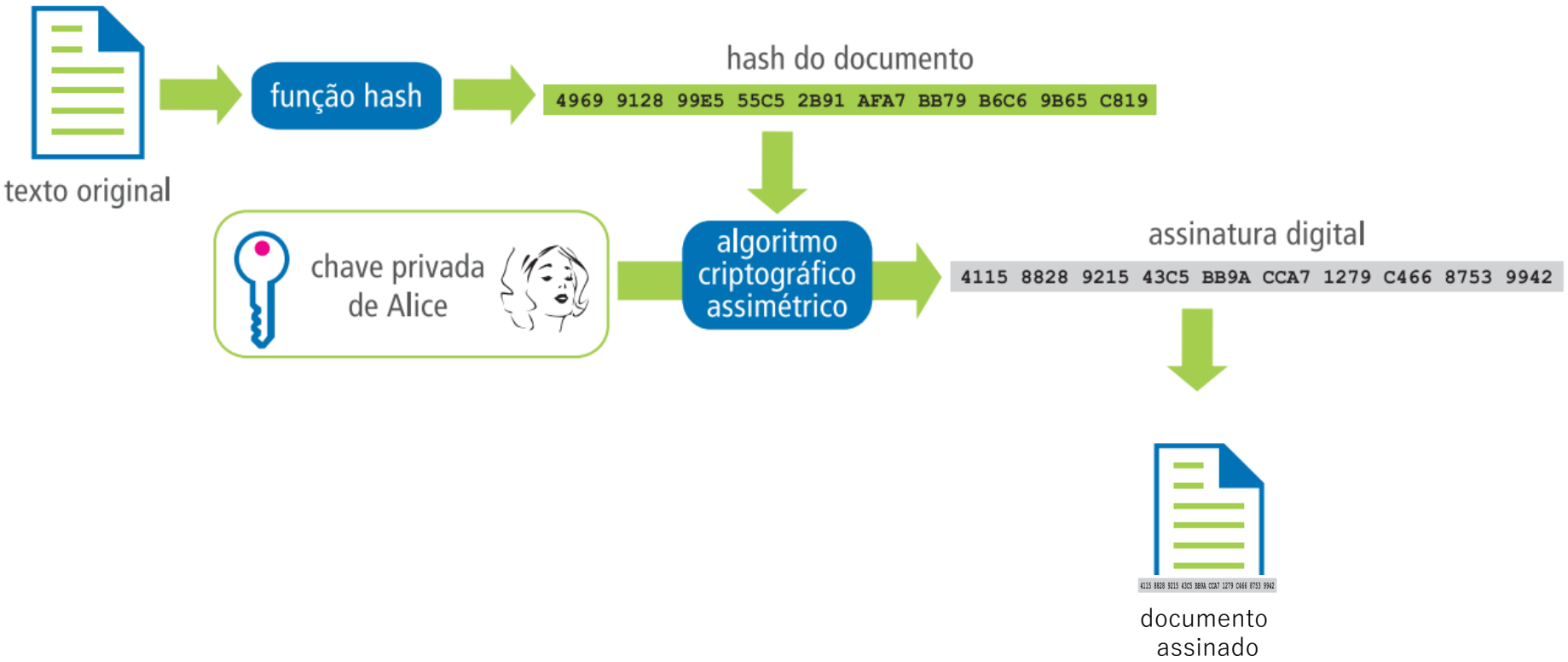
Internet X.509 Public Key Infrastructure (PKI)

Certificação Digital – Recebimento de Mensagem



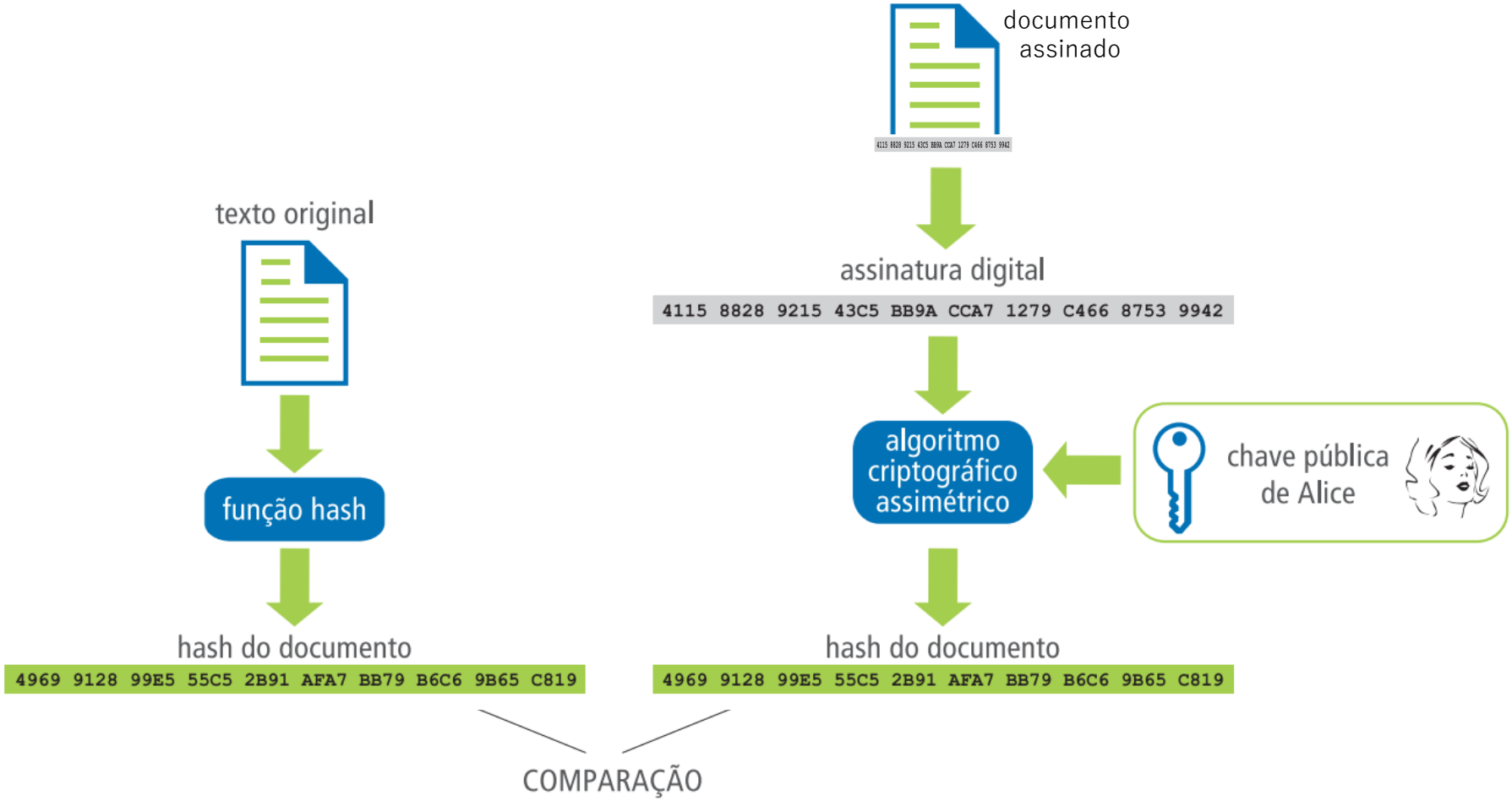
Internet X.509 Public Key Infrastructure (PKI)

Certificação Digital – Assinatura Digital



Internet X.509 Public Key Infrastructure (PKI)

Certificação Digital – Verificação de Assinatura Digital



Obrigado!

Prof. Rommel Vieira Carneiro