Criptografia

Assinaturas digitais

Roadmap

- Cenários de uso
- Assinatura digital com função hash
- Geração e validação da assinatura
- Infraestrutura de chave pública

Universidade Federal do Ceará
Campus de Crateús

Ciência da Computação
Sistemas de Informação

emerson@crateus.ufc.br

Assinaturas digitais

Introdução

- Substituir a assinatura **escrita à mão** não é uma tarefa fácil.
- É necessário um mecanismo que possa garantir que uma das partes **escreva** uma mensagem e a "**assine**", de modo que a outra parte tenha certeza quem é o autor da mensagem.
- Além disso, é preciso garantir que o documento não foi alterado desde a sua criação.

Assinaturas digitais

Introdução

- Com a popularização da Internet muitas transações comerciais e **contratos** estão sendo realizados por meio da rede.
- Em muitos casos, não existe mais o tradicional **documento em papel** e as assinaturas à mão confirmando que os signatários concordam com o conteúdo do documento.
- Atualmente esses contratos são **documentos eletrônicos**, então é necessário uma forma de **assinar** esses documentos com as mesmas **garantias** que assinatura manual fornece.

Assinaturas digitais

Introdução

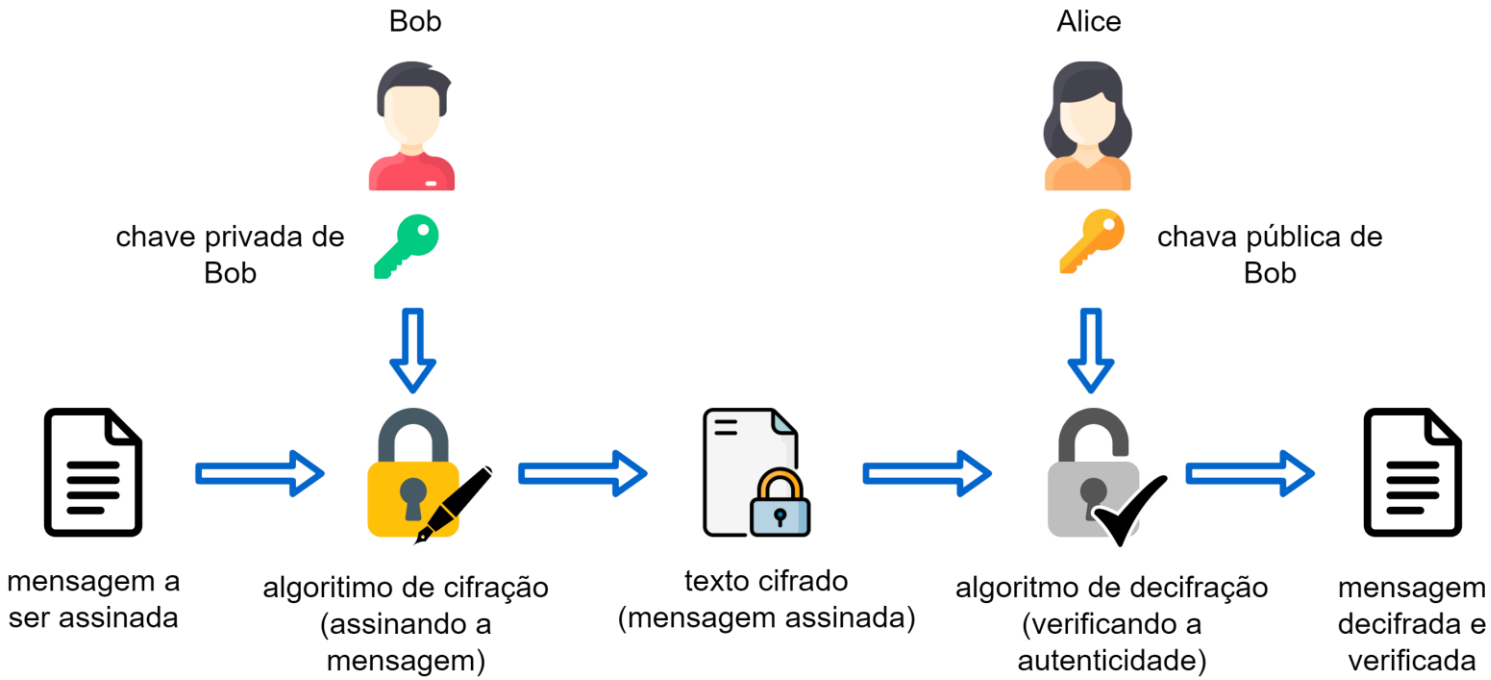
Definição

- **A assinatura digital é um método criptográfico que permite que o criador de um documento digital seja identificado pelo receptor.**
- Os esquemas de assinaturas digitais visam garantir a autenticidade de uma mensagem.
- Esses esquemas são construídos a partir de criptossistemas de chave pública.

Assinaturas digitais

Cenário de uso: forma clássica

- Suponha que Alice deseja receber uma informação de Bob, mas quer a garantia que foi realmente Bob que a enviou — isto é, Alice quer **autenticidade**.
- Bob **não poderá repudiar a informação** — ou seja, não poderá negar que é a autor da mensagem.



Assinaturas digitais

Cenário de uso: forma clássica

- O algoritmo de criptografia somente será capaz de decifrar a mensagem utilizando a chave pública de Bob.
- Alice ou qualquer outra pessoa que possuir a chave pública de Bob pode decifrar a mensagem.
- Claramente, não há **confidencialidade**, mas satisfez o que Alice queria — a garantia que Bob não pode negar que é o autor da mensagem.

As assinaturas digitais dependem de duas suposições fundamentais:

I. a chave privada é armazenada de forma segura e apenas o proprietário tem acesso a ela;

II. a única maneira para produzir uma assinatura digital é usando a chave privada.

Assinaturas digitais

Cenário de uso: utilizando RSA

- O cenário básico anterior apresenta um problema — a assinatura é a **própria mensagem cifrada** e será **tão longa** quanto a mensagem em texto simples.

- A cifragem e a decifragem no RSA exige uma **exponenciação modular** para cada bloco cifrado ou decifrado.

- Isto significa que produzir uma assinatura para um documento muito grande pode **gastar muito tempo**.

Assinaturas digitais

Cenário de uso: utilizando RSA

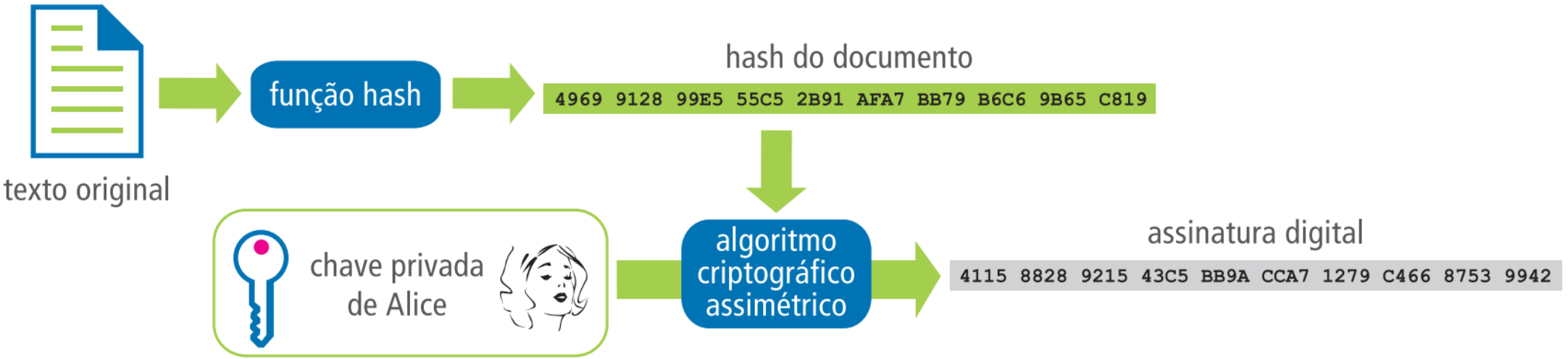
- Uma forma de resolver o problema do cenário canônico e incorporando um novo elemento ao processo de assinatura digital — uma **função hash**.

- Como o **valor hash** é a representação única de uma mensagem, **basta cifrar o hash** — em vez do documento inteiro.

- A assinatura digital passa a ser o **valor hash.**
- O emissor deve juntar o documento ao hash, que funciona como autenticação.

Geração da assinatura usando função hash e RSA

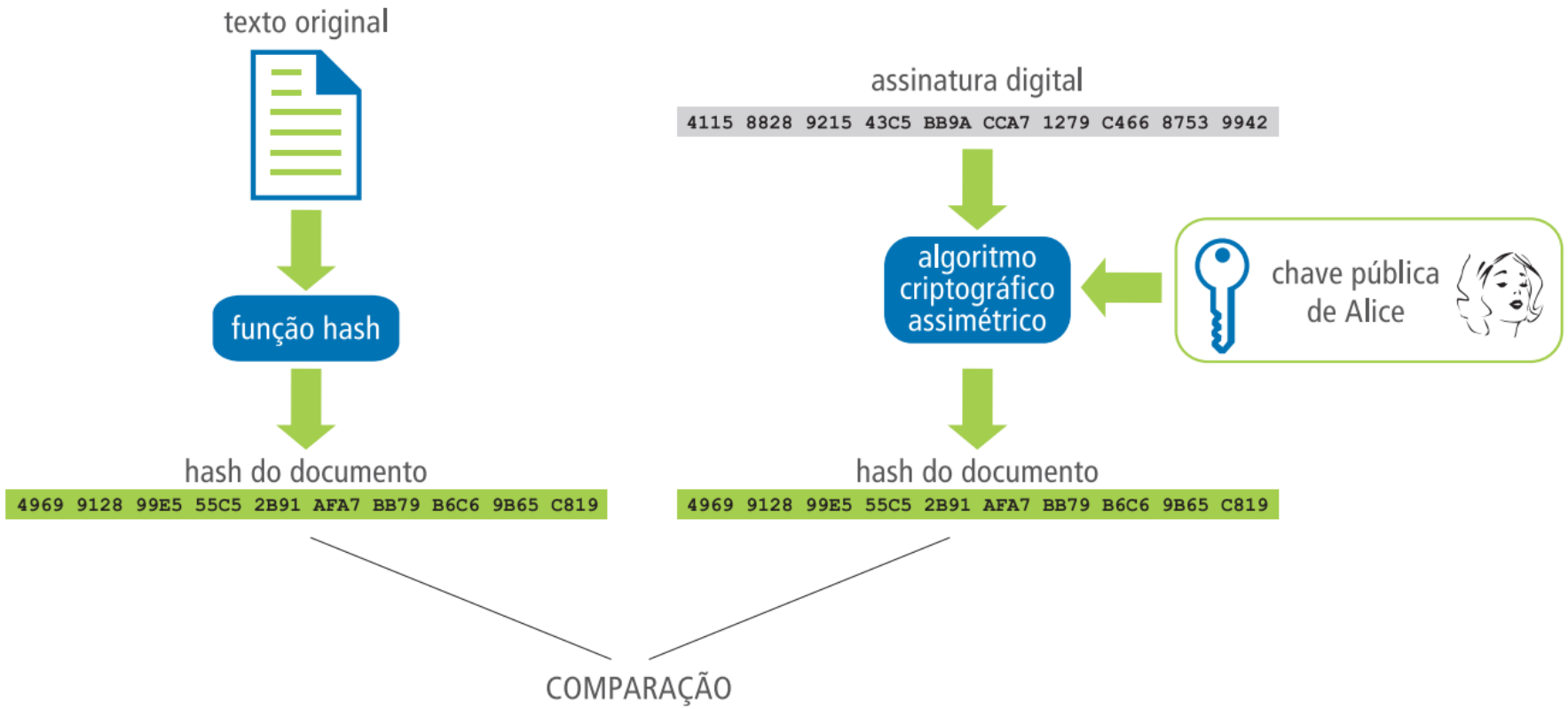
Geração da assinatura digital



- É fácil perceber que para assinar um documento não há necessidade de cifrar todo o documento, já que neste caso, o objetivo não é tornar a mensagem confidencial.

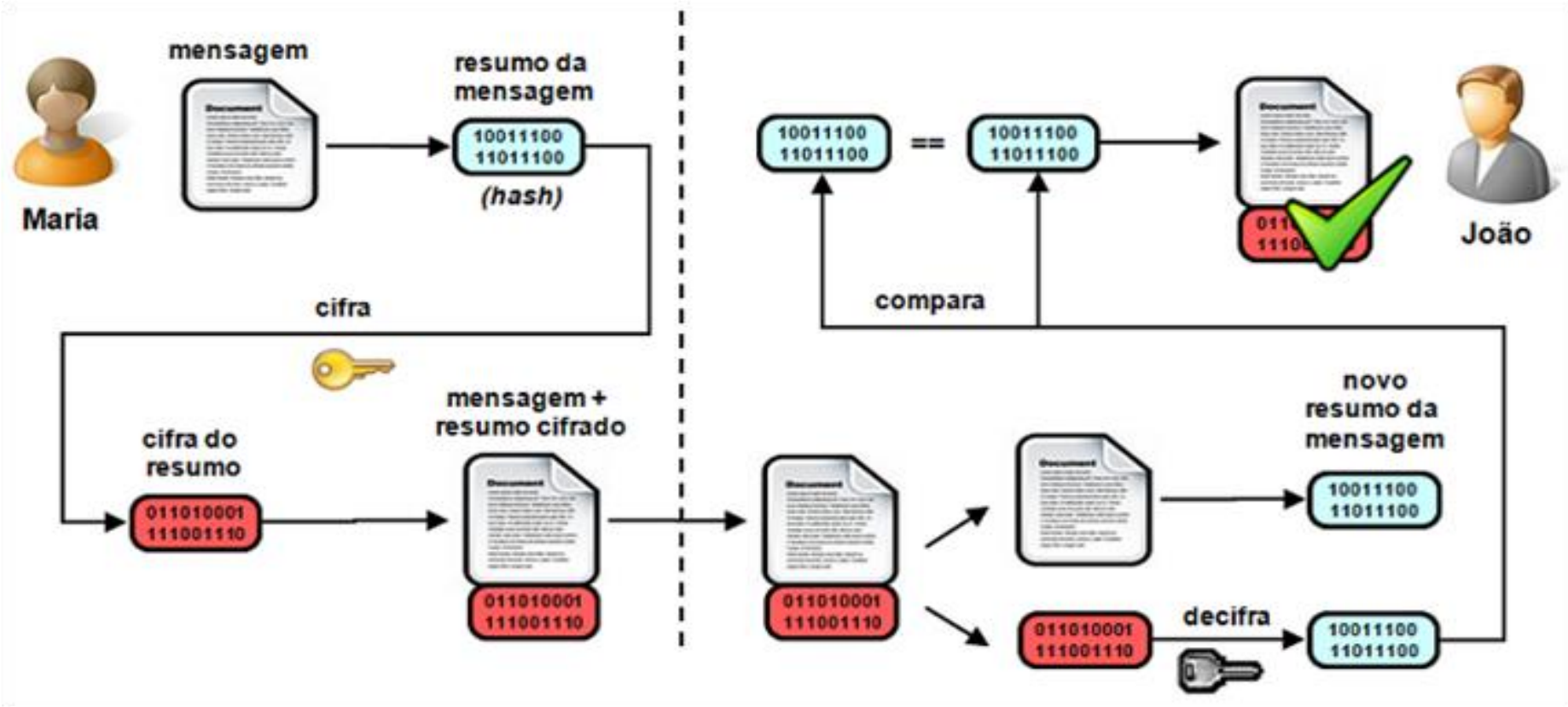
Geração da assinatura usando função hash e RSA

Verificação da assinatura digital



Geração da assinatura usando função hash e RSA

Processo completo



Geração da assinatura usando função hash e RSA

Formalizando o protocolo

1. Alice resolve enviar uma mensagem $\boldsymbol{m}$ para Bob — assim Alice aplica uma função hash $\mathcal{H}$ à mensagem $\boldsymbol{m}$. Este processo gera um hash

$$\boldsymbol{h_1 = \mathcal{H}(m).}$$

2. Com sua chave privada $\boldsymbol{K_{pr}}$, Alice cifra o hash $\boldsymbol{h}$ aplicando

$$\boldsymbol{RSA\left(K_{pr}, h\right) = c,}$$

e anexa $\boldsymbol{s}$ à mensagem e os transmite para o destinatário.

3. Para garantir que a mensagem é autentica, Bob decifra o hash cifrado $\boldsymbol{c}$ com a chave pública $\boldsymbol{K_{pu}}$ de Alice, aplicando

$$\boldsymbol{RSA\left(K_{pu}, c\right) = h_1.}$$

4. De posse do hash $\boldsymbol{h_2}$, Bob aplica

$$\boldsymbol{\mathcal{H}(m) = h_2.}$$

Se o hash obtido, $\boldsymbol{h_2}$ for igual ao hash $\boldsymbol{h_1}$, enviando pelo remetente, significa que a mensagem não foi alterada e o autor é realmente quem diz ser.

Assinaturas digitais

Cenário de uso: utilizando RSA

- Observe que esse processo de assinatura digital é capaz de garantir as seguintes propriedades:

Integridade

Permite verificar se o documento não foi alterado após a aplicação da assinatura.

Autenticidade

Permite verificar se um documento realmente foi gerado e aprovado pelo emissor.

Não repúdio

Quando constatada a autenticidade da mensagem, impede que o emissor recuse a autoria ou conhecimento do documento.

Certificação Digital

Definição

- Como garantir que a chave pública de um indivíduo foi realmente gerada por ele/ela?
  - Por exemplo, um impostor pode ter gerado um par de chaves e apresentá-lo como sendo de Alice para receber as mensagens endereçadas à Alice.
- Esse problema foi resolvido com a criação da **certificação digital.**

Certificação Digital é a tecnologia que adota mecanismos de segurança, por meio de algoritmos matemáticos, capazes de garantir autenticidade, integridade e não-repúdio às informações eletrônicas.

Certificado Digital

Certificado digital é um arquivo eletrônico armazenado em uma mídia digital que contém os dados do seu titular, pessoa física ou jurídica, e associa a chave pública a tal pessoa.

- O certificado digital atesta a identidade, garantindo, autenticidade e o não repúdio nas transações comerciais e financeiras por elas assinadas.
- Desta forma, o certificado digital identifica quem somos para as pessoas e para os sistemas de informação.

Infraestrutura de chave pública

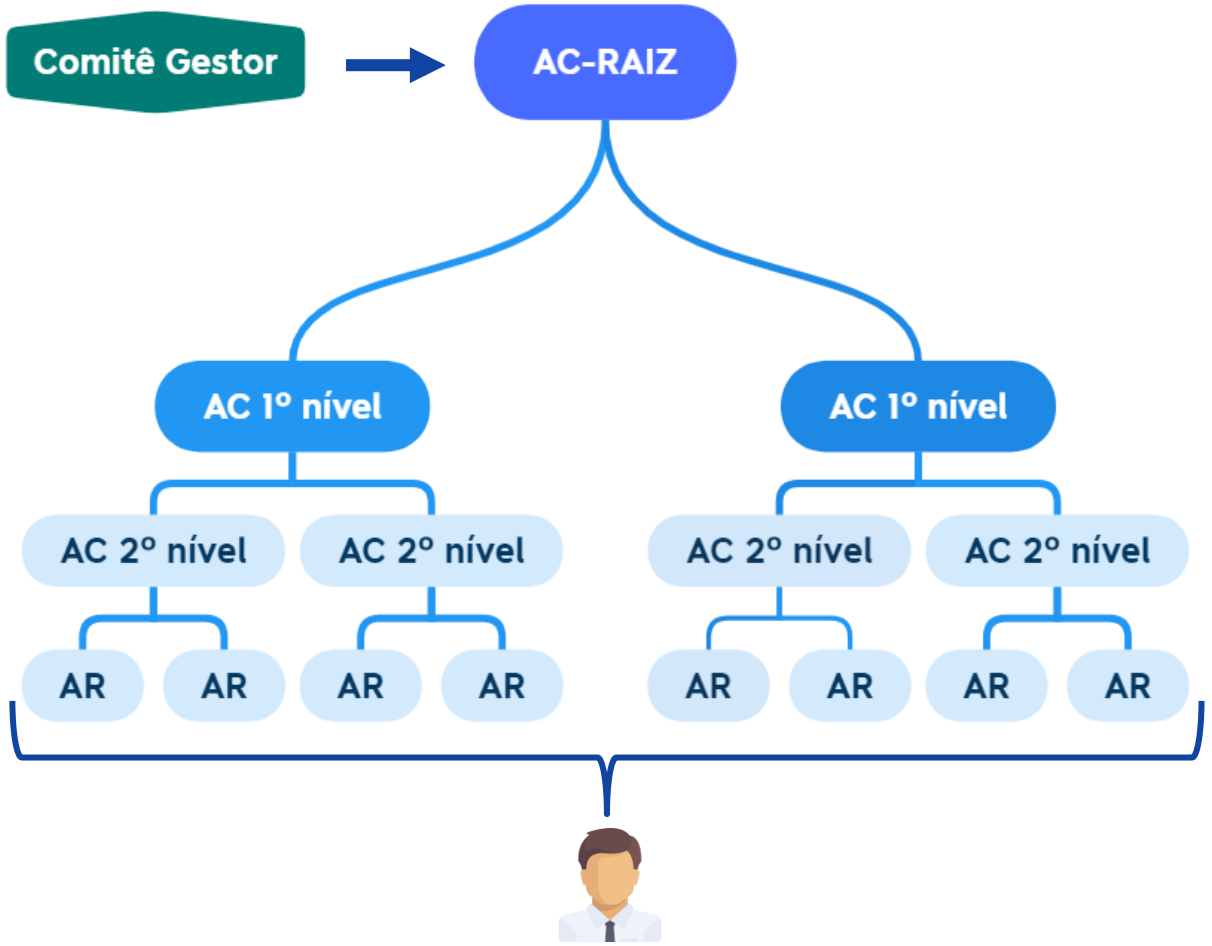
- Mesmo com o certificado digital, os problemas de identificação ainda não estão totalmente resolvidos.
- A questão agora é como saber se um certificado é **válido**.
- Para garantir validade jurídica, os certificados são emitidos entidades, que fazem parte de uma cadeia hierárquica de **confiança**, conhecida como **Infraestrutura de chave pública.**

ICP Brasil
O Brasil na era da certificação digital

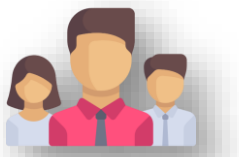
Infraestrutura de Chave Pública (ICP) uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais e envolve um conjunto de padrões e várias entidades, tais como:

- Autoridade certificadora,
- Autoridade de registro,
- Usuários finais.

Infraestrutura de chave pública

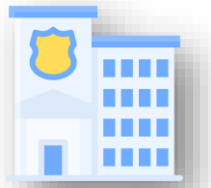


Infraestrutura de chave pública



Comitê Gestor

- Comitê gestor é que aprova normas e resoluções, e fiscaliza a AC-RAIZ.



AC-RAIZ

- No topo da ICP está a **AC-Raiz.** No Brasil é representada pelo ITI (Instituto Nacional de Tecnologia da Informação).
- É competência da AC-Raiz emitir, distribuir, revogar e gerenciar certificados das AC imediatamente subsequentes e manter uma lista de certificados revogados.
- Além disso, fiscaliza e audita demais membros participantes da cadeia de certificação.

Infraestrutura de chave pública

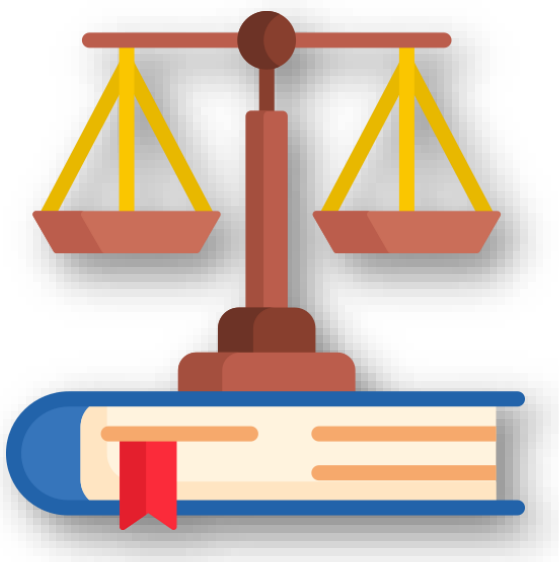
Autoridade Certificadora - AC

- AC é uma entidade de confiança que, por força de lei, emite certificados digitais para pessoas físicas, empresas ou outras AC.
- Tem o poder de atestar a identidade de pessoas que desejam realizar transações eletrônica.

Autoridade de Registro - AR

- AR é uma entidade de apoio ligada a uma autoridade certificadora habilitada junto AC-Raiz.
- Cada AC escolhe quantas AR prestarão serviço a ela. A AC delega a função de identificação do interessado no certificado digital.

Validade jurídica



- Em geral, existe um conjunto de leis que atribuem poderes para que certos órgãos possam emitir e gerenciar os certificados e que sejam considerados legalmente **válidos**.
- A certificação digital garante às transações realizadas pela Internet: validade jurídica, autenticidade e Integridade.
- Portanto, a assinatura digital é uma modalidade de assinatura eletrônica equivalente à assinatura de próprio punho, que comprova a autoria e a integridade de um documento digital.

Validade jurídica

- Assim como qualquer outro documento de **identificação** o certificado digital tem o objetivo de Identificar e garantir que o proprietário do certificado é quem realmente diz ser nas operações eletrônicas por meio da rede.

- Assim, a assinatura digital gerada a partir do uso do certificado digital da ICP-Brasil, possui pleno valor jurídico garantido pela legislação brasileira.

Fim!

[Aula 16] Assinaturas digitais