# Segurança de Redes

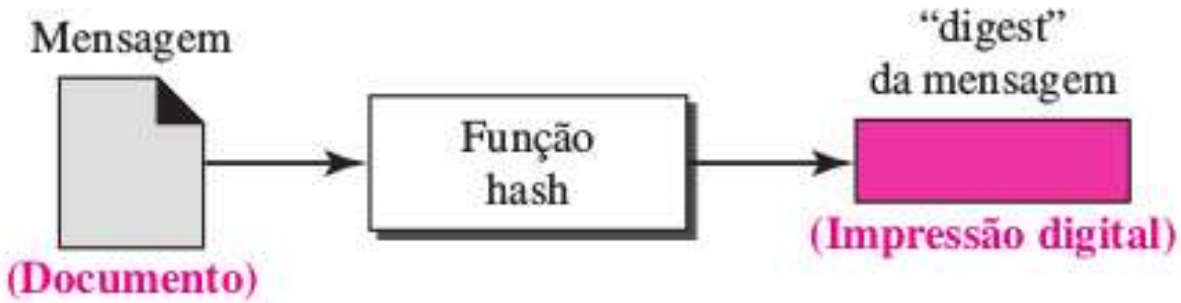
Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Técnicas de Defesa
(Função Hash, Assinatura e Certificado Digital)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Introdução

A função *hash* é uma função matemática que recebe uma mensagem de tamanho variável, e produz uma saída de tamanho fixo (chamada de resumo da mensagem, "*digest*" ou impressão digital). O objeto principal de uma função de *hash* é buscar garantir a **integridade** de um documento. Uma mudança em qualquer *bit* resulta, com alta probabilidade, em uma mudança no código de *hash*.




INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Propriedades

São propriedades de um algoritmo de *hash*:

- Consistência: mesma entrada produz sempre a mesma saída.
- Randômico: a saída não deve permitir descobrir informações sobre a mensagem original.
- Único: quase impossível duas mensagens produzirem *hashes* iguais.
- *One-way* (mão única): a partir do *hash* deverá ser impossível descobrir a mensagem original.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

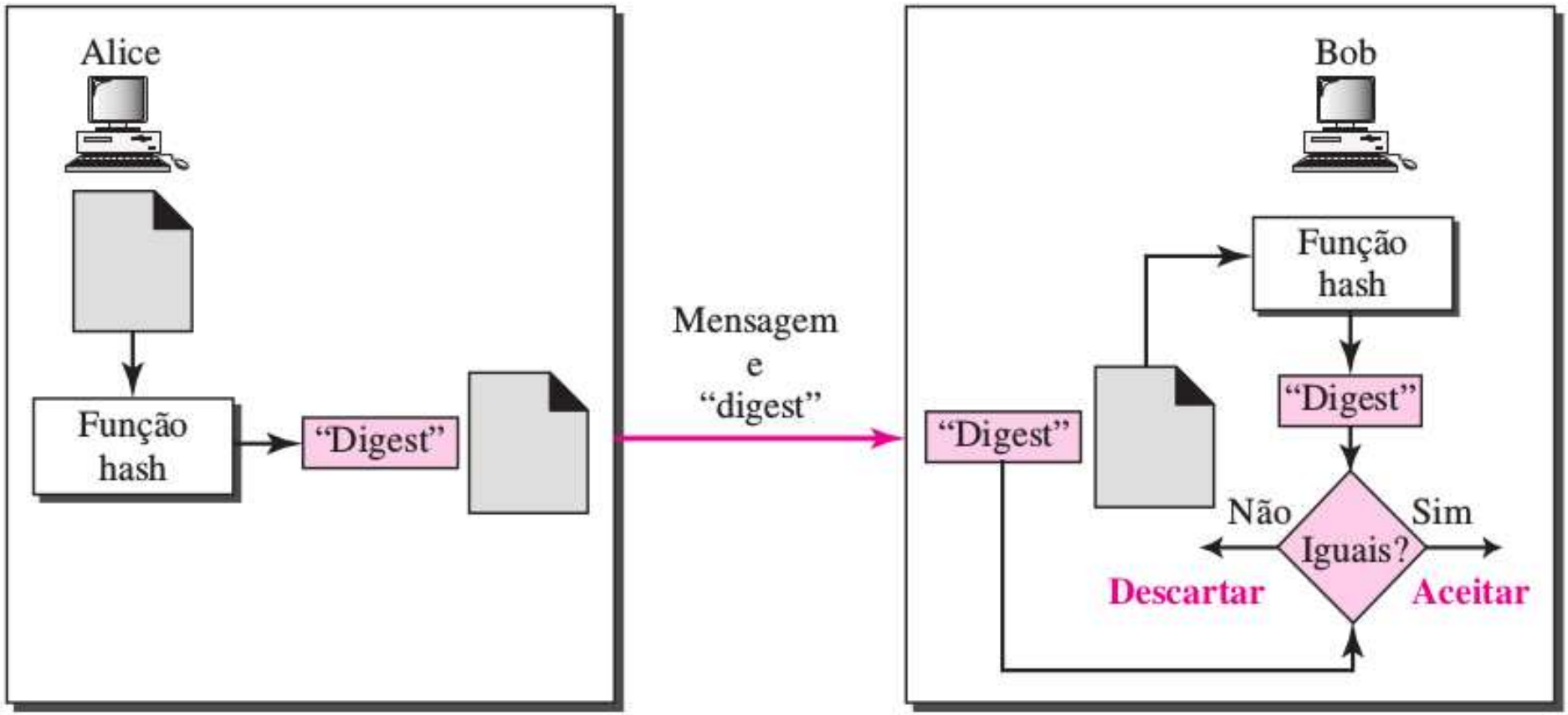
# Funcionamento

A impressão digital (resultado da função *hash*) da mensagem é criado no emissor e é enviado com a mensagem para o receptor. Para verificar a integridade de uma mensagem ou de um documento, o receptor calcula a função *hash* novamente e compara o o resultado com aquele recebido. Se ambos forem o mesmo, o receptor tem certeza de que a mensagem original não foi alterada.

Uma função *hash* é semelhante à encriptação. Uma diferença é que o algoritmo de *hash* não precisa ser reversível, como para a decriptação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Funcionamento



# Exemplos

- O Message Digest 5 (MD5) foi criado por Ron Rivest, no MIT. Ele processa a entrada em blocos de 512 e produz uma saída de 128 bits. Em 2004, pesquisadores chineses anunciaram a descoberta de uma série de colisões (mensagens diferentes produzindo o mesmo hash) no MD5.
- O Secure Hash Algorithm (SHA) foi desenvolvido pelo NIST. Ele processa a entrada em blocos de 512 e produz uma saída de 160 bits. O SHA necessita de um processamento mais intensivo e pode rodar um pouco mais lentamente que o MD5.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Exemplos

Mensagem Original: "**Curso de Redes de Computadores no IFRN**"
SHA-1: aae724d3c22188f8e40bfa1041f0f194ef387609

Mensagem Alterada: "**Curso de Redes de Computadores no IFRN.**"
SHA-1: 3cc2582ec28503e7e37bcb3cbc45e08c7c5018b1

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# SHA

O SHA é a função de hash mais utilizada, pois praticamente todas as outras funções de hash tiveram vulnerabilidades criptoanalíticas substanciais.

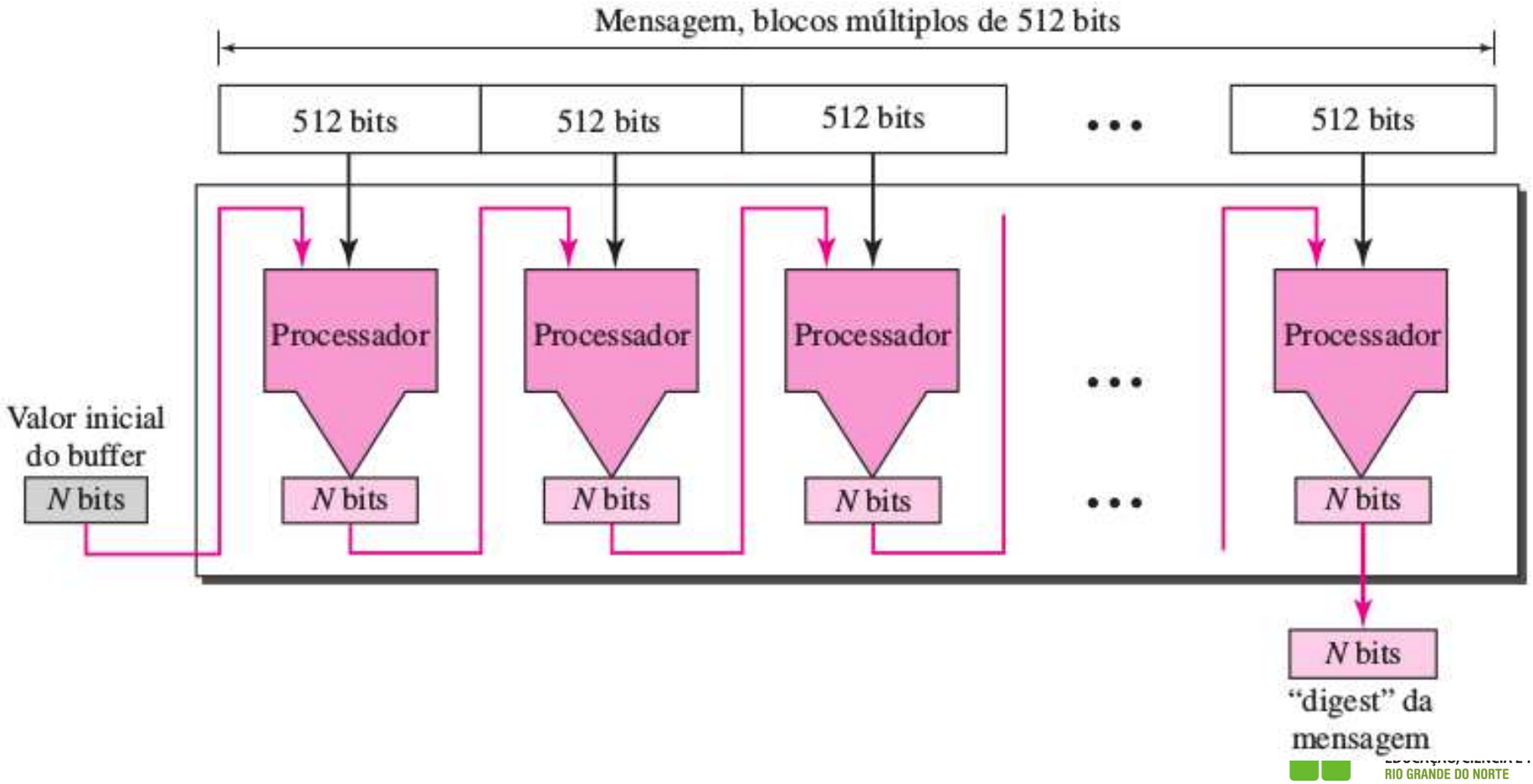
Em 1995, o SHA original foi atualizado, por problemas de segurança, e foi proposto o SHA-1, que também produz um valor de hash de 160 bits.

Em 2002, o NIST produziu uma versão revisada do padrão que definiu três novas versões do SHA, com tamanhos de valor de hash de 256, 384 e 512 bits, conhecidas como SHA-256, SHA-384 e SHA-512, respectivamente. Coletivamente, esses algoritmos de hash são conhecidos como SHA-2.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# SHA-1 - Funcionamento

A mensagem original é dividida em blocos de 512 bits.



# SHA-1 - Funcionamento

Um buffer de N bits é inicializado com um valor predeterminado. O algoritmo utiliza esse o buffer inicial com os 512 primeiros bits da mensagem para criar o primeiro resultado intermediário de N bits. Esse "digest" é então utilizado com o segundo bloco de 512 bits para criar o segundo resultado intermediário. E assim sucessivamente. Se um bloco não for de 512 bits, é usado preenchimento (0s) para que esse chegue ao comprimento. Quando o último bloco for processado, o "digest" resultante (de 160 bits no SHA-1) é o da mensagem toda.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Pergunta?

A função *hash* tem outras aplicações?

# Resposta

- Salvar senhas;
- Identificação de arquivos (assinaturas de arquivos).

# Pergunta?

Mas como a função hash é enviada para o destinatário? Se um atacante puder alterar os dados, ele também pode alterar o resumo enviado!

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Resposta

A função hash pode ser enviada para o destinatário usando:

- Criptografia Simétrica: HMAC;
- Criptografia Assimétrica: Assinatura Digital.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# MAC

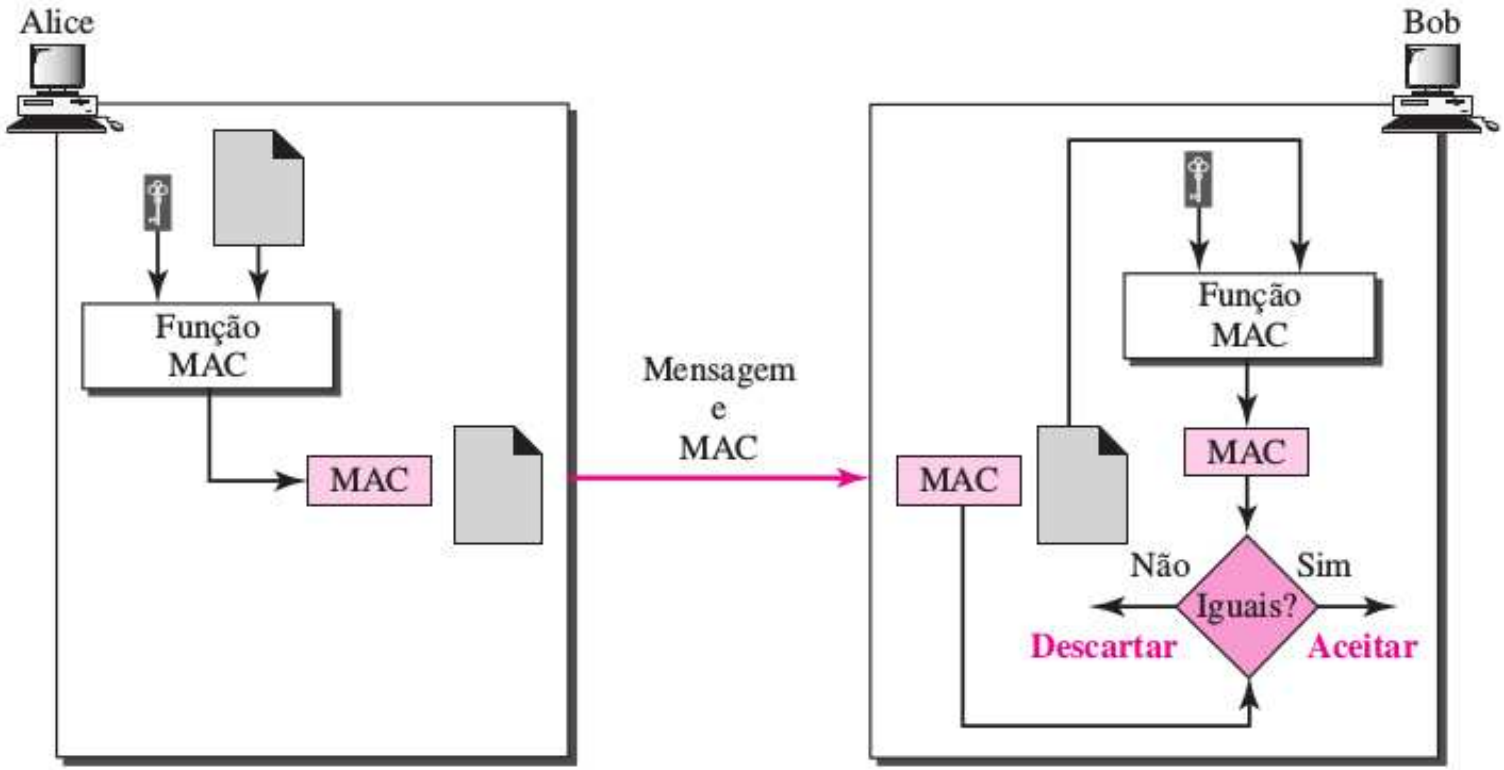
Uma função hash garante a integridade de uma mensagem. Mas para ser realmente útil, o transmissor (Alice) precisa dar evidências de que é ela, Alice, que está enviando a mensagem, e não um impostor.

Para fornecer autenticação de mensagens, precisamos alterar um código de detecção de modificações (MDC - *modification detection code*) para um MAC (*message authentication code* - código de autenticação de mensagens).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# MAC

Um MAC usa uma função hash com chaves simétricas entre o emissor e o receptor ao criar o resumo.




INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# HMAC

Existem várias implementações do MAC. Esse conceito é um MAC com hash, chamado HMAC, que pode usar qualquer função hash padrão sem chaves, como o SHA-1, apenas acrescentando a chave. É anexada uma cópia da chave simétrica à mensagem.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Assinatura Digital

Com a expansão da informática, grande parte dos arquivos em diversas áreas do mercado migrou para o ambiente digital. A partir disso, surgiu a necessidade de autenticar todo esse volume de informações, da mesma forma com que as assinaturas validam contratos e outros conteúdos em papel. Surgindo a assinatura digital.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Assinatura Digital

A assinatura digital é uma técnica que utiliza criptografia para garantir as seguintes propriedades de mensagens e documentos eletrônicos:

- Autenticidade: o receptor deve poder confirmar que a assinatura foi feita pelo emissor;
- Integridade: qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;
- Irretratabilidade ou não-repúdio: o emissor não pode negar a autenticidade da mensagem.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

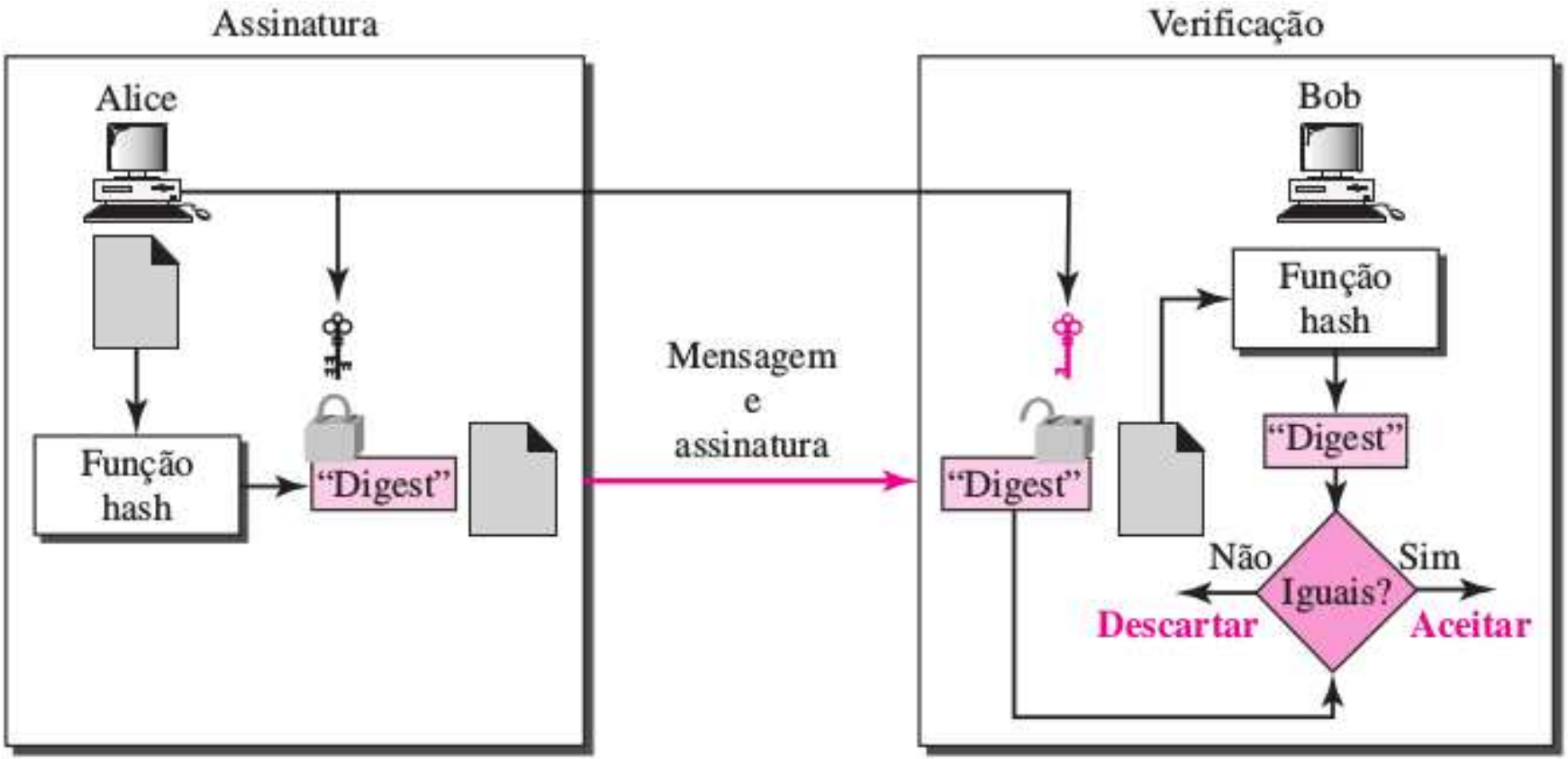
# Assinatura Digital

A lei brasileira determina que qualquer documento digital tem validade legal se for certificado. Ou seja, ela está substituindo à assinatura física, já que elimina a necessidade de ter uma versão em papel do documento que necessita ser assinado.

Cada assinatura é única para os dados assinados e para as chaves utilizadas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Assinatura Digital




INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Assinatura Digital

Bob pode assinar uma mensagem usando um algoritmo de geração de assinatura digital. As entradas do algoritmo são a mensagem e a chave privada de Bob. Qualquer outro usuário, digamos, Alice, pode verificar a assinatura usando um algoritmo de verificação, cujas entradas são a mensagem, a assinatura e a chave pública de Bob.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Assinatura Digital

**Obs**

Em um criptossistema, utilizamos as chaves públicas e privadas do receptor; na assinatura digital, usamos a chave pública e privada do emissor.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Pergunta?

Como confiar em uma chave pública? A chave pública de Alice é realmente de Alice?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Certificado Digital

Um certificado consiste em uma chave pública mais um identificador do proprietário da chave, com o bloco inteiro assinado por um terceiro confiável. Normalmente, o terceiro é uma autoridade certi- ficadora, como uma agência do governo ou uma instituição financeira, na qual a comunidade de usuários confia. Somente a autoridade certificadora pode criar e atualizar certificados.

O usuário pode, então, publicar o certificado. Qualquer um que precise da chave pública desse usuário pode obter o certificado e verificar se ele é válido por meio de uma assinatura confiável anexada.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Entidade Certificadora

Para isso foi criado as AC (autoridade de certificação). Elas são organizações estaduais ou federal responsável por criar, distribuir e invalidar certificados digitais, análogas aos cartórios, que verificam assinaturas normais.

Um certificado digital é um documento de identificação digital. Assim como uma Carteira de Identidade, ele possui informações sobre seu proprietário, sua chave pública. Os certificados podem ser utilizada para validar transações online, procurações, autenticar informações empresariais no e-commerce e inúmeras outras aplicações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

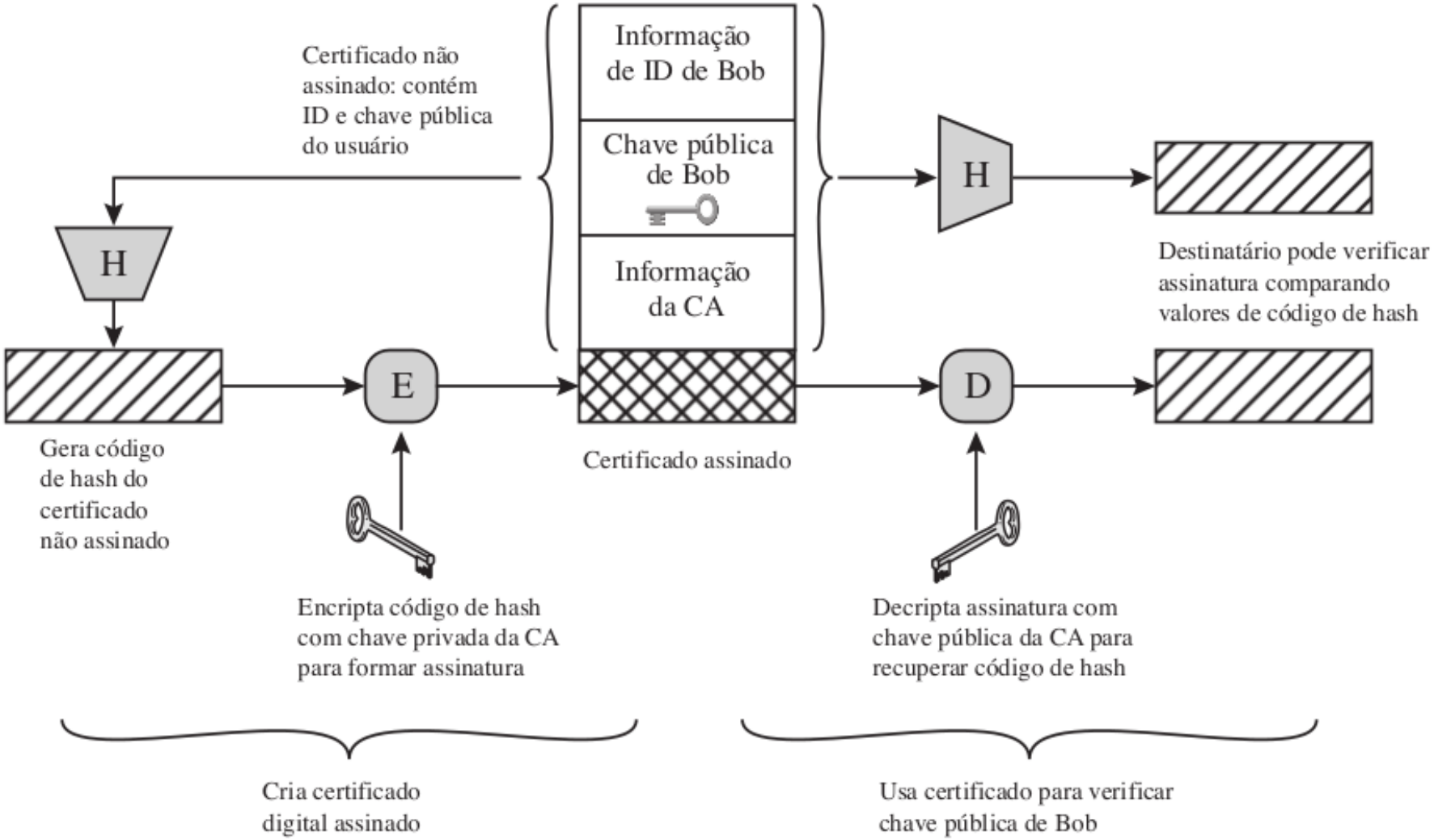
# Certificado Digital

De forma geral, os dados básicos que compõem um certificado digital são:

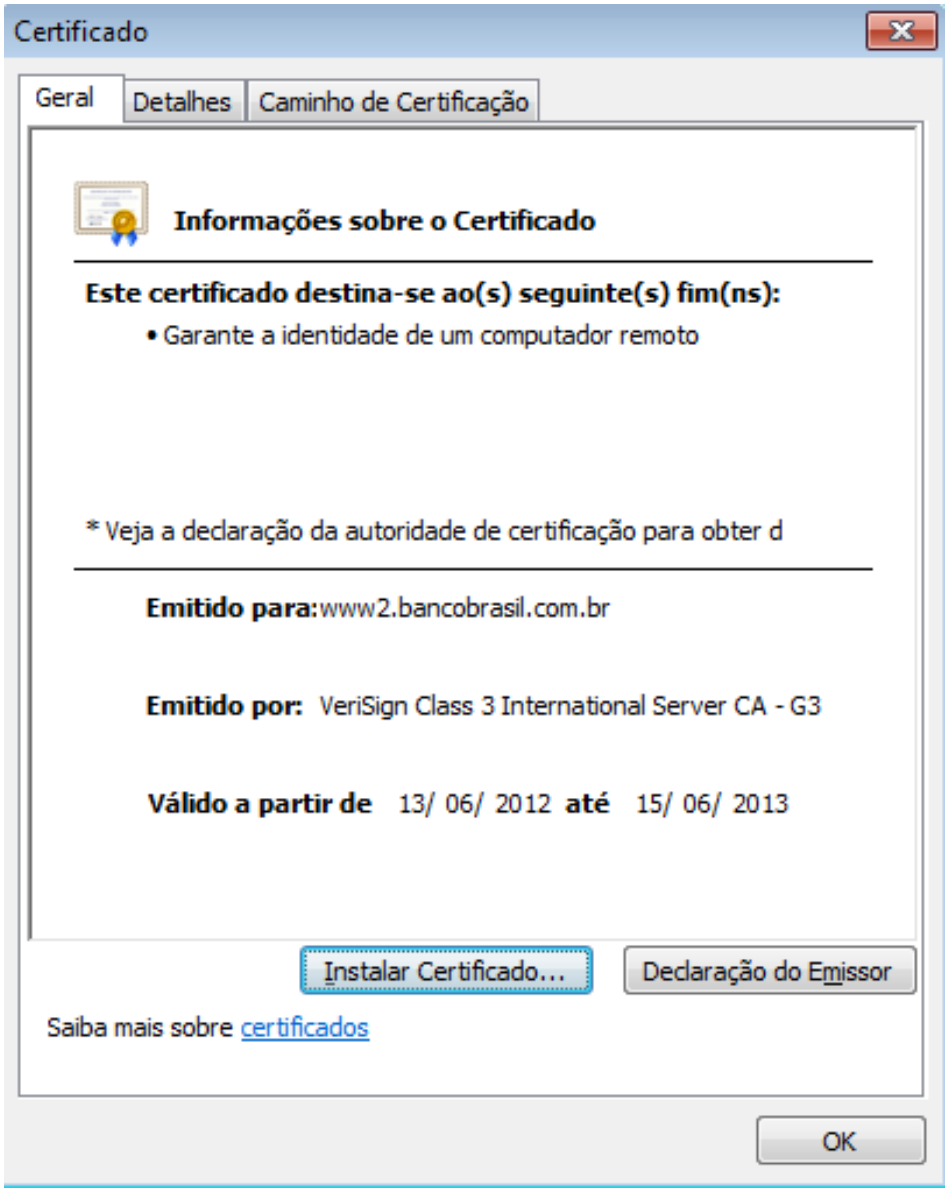
- Versão e número de série do certificado;
- Dados que identificam a AC que emitiu o certificado;
- Dados que identificam o dono do certificado (para quem ele foi emitido);
- Chave pública do dono do certificado;
- Validade do certificado (quando foi emitido e até quando e válido);
- Assinatura digital da AC emissora e dados para verificação da assinatura.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Certificado Digital

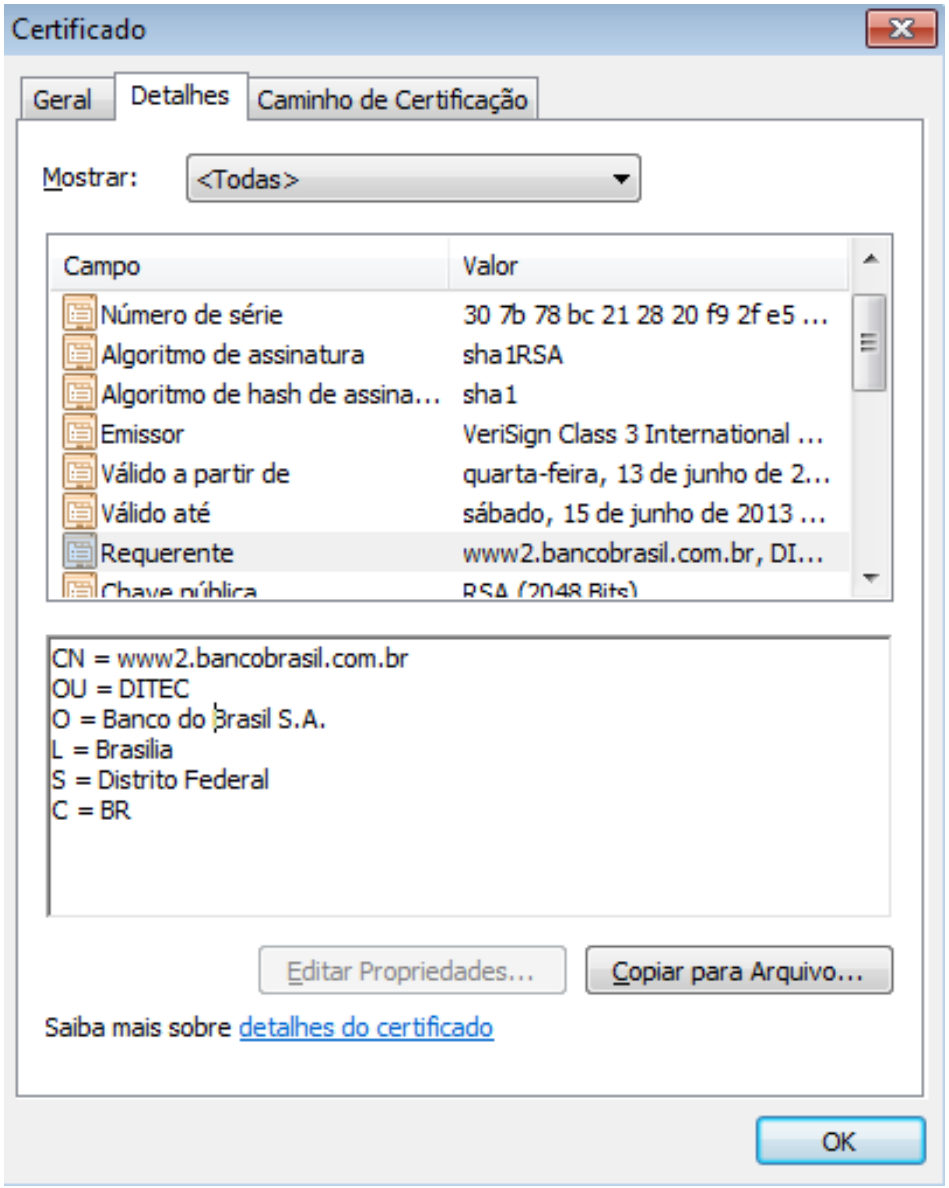


# Certificado Digital




INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Certificado Digital




INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Certificado Digital

- Quando você tenta acessar um site utilizando conexão segura, normalmente seu navegador já realiza verificações. Caso as verificações falhem, o navegador emite alertas.


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Certificado Digital

- Em geral, alertas são emitidos em situações como:
  - O certificado está fora do prazo de validade;
  - O navegador não identificou a cadeia de certificação ;
  - O endereço do site não confere com o descrito no certificado;
  - O certificado foi revogado.
- Ao receber os alertas do seu navegador você pode optar por:
  - Desistir da navegação.
  - Solicitar detalhes sobre o problema.
  - Aceitar os riscos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Entidade Certificadora

A AC mais importante do Brasil é a AC-Raiz Brasileira. Ela existe desde 2001, após a criação da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil), marco que permitiu o início do uso da certificação no país. A AC-Raiz é o ponto máximo de confiança da infraestrutura. Ela é quem autoriza que outras ACs secundárias funcionem, descentralizando a emissão de certificados. Essas outras autoridades são conhecidas como ACs Intermediárias de primeiro nível, ou Normativas.

Por serem de extrema importância para a infraestrutura, as chaves privadas dessas autoridades são mantidas em ambientes de altíssima segurança, as chamadas salas-cofre.

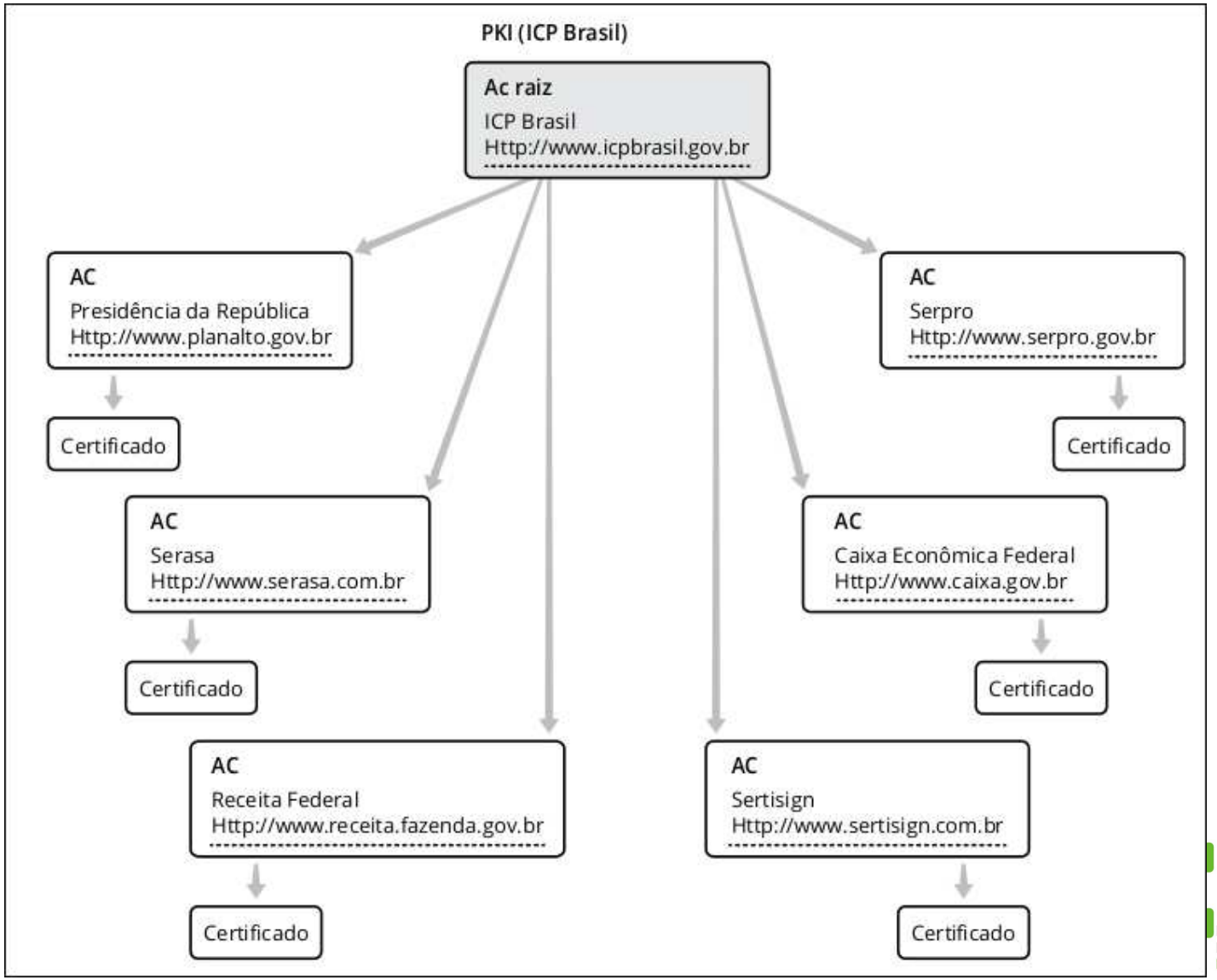
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Processo de emissão de um Certificado Digital

1. Solicitação do certificado: no site da Autoridade Certificadora escolhida.
2. Validação presencial: o solicitante se dirige até um ponto de atendimento da Autoridade de Registro, em posse de seus documentos de identidade, como CPF ou RG. Também é realizada a coleta dos dados biométricos (face e impressões digitais) do requerente. Um agente autorizado valida a documentação, arquiva os documentos do solicitante e autoriza a emissão do certificado;
3. Emissão do certificado: o requerente recebe um token ou cartão (smart card) contendo o certificado.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Processo de emissão de um Certificado Digital




INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

# Atividade

Faça uma aplicação cliente-servidor (continuação da aula de criptografia) para demonstrar a programação de socket, função Hash e assinatura digital, da seguinte maneira:

- O cliente e o servidor utilizam assinatura com chave pública RSA e Hash com SHA256;
- A chave pública do servidor foi previamente compartilhada para o cliente.
- O servidor inicializa e fica aguardando conexão.
- Um cliente envia para o servidor um texto (chamado de desafio);

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

# Atividade

- O servidor recebe o desafio, calcula o hash, assina o hash com sua chave privada e envia para o cliente.
- O cliente recebe a resposta, calcula o hash do desafio e compara com a decriptografia (verificação) da mensagem ddo servidor, com a chave pública do servidor.
- Rode o Wireshark e veja o funcionamento do seu programa na rede.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE