Infraestrutura Chave Pública

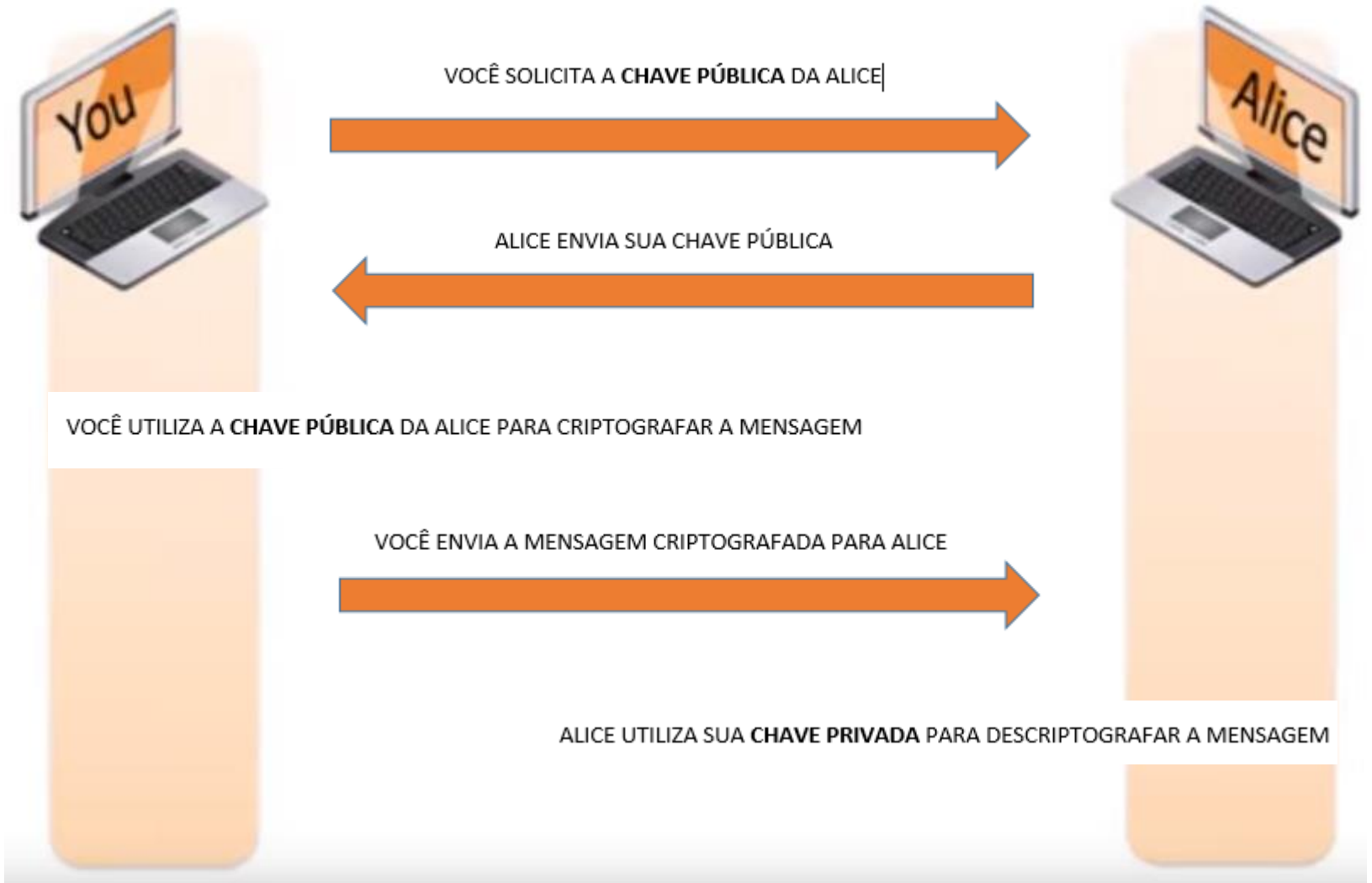
O que é Infraestrutura de Chave Pública(PKI)?

- ✓ É um framework utilizado para fornecer autenticidade e confidencialidade em suas transmissões de dados.

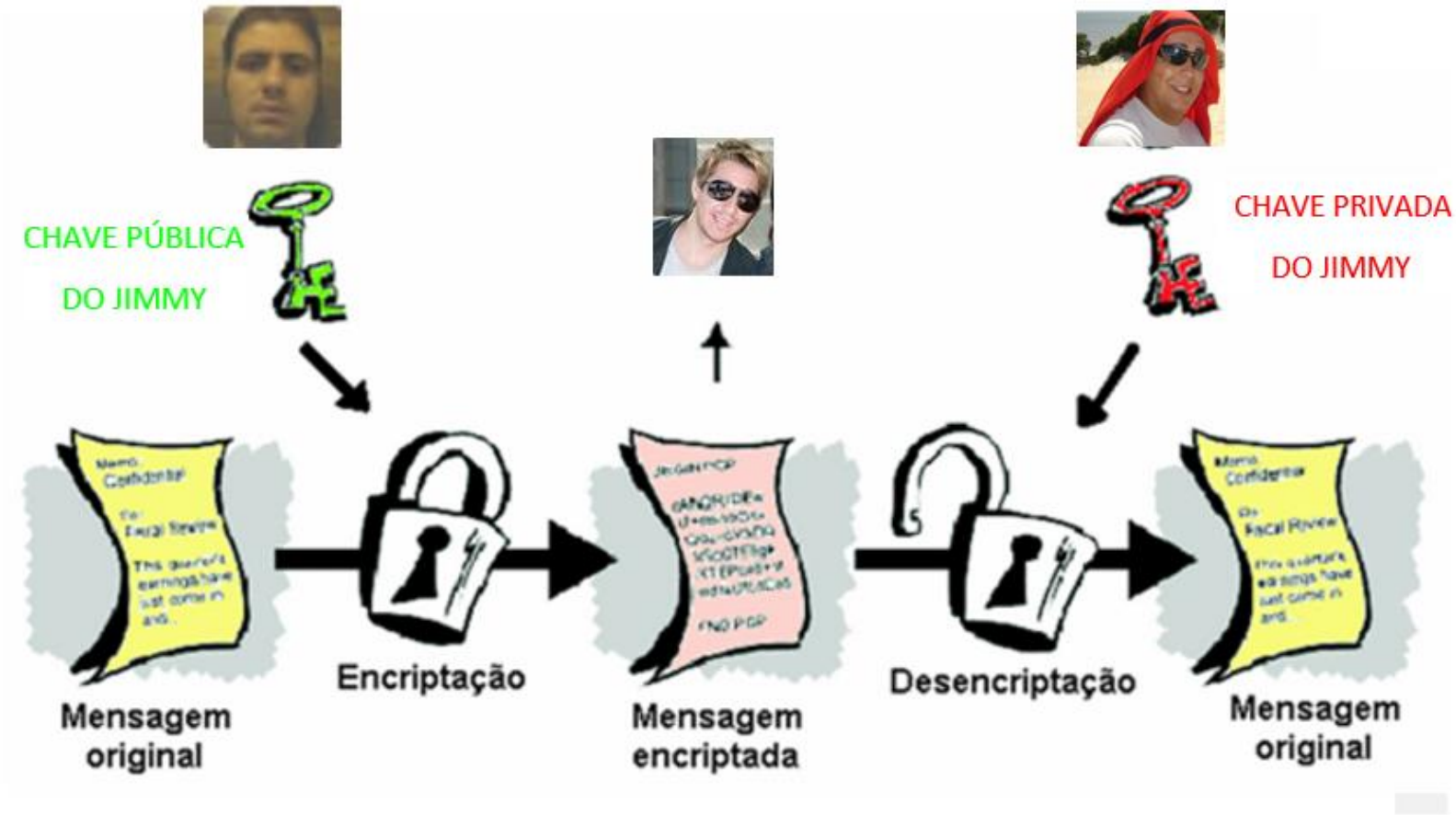
Conceitos Relacionados:

- Criptografia Assimétrica(Key Pair);
- Autoridade Certificadora (ICP – Brasil);
- Autoridade Registradora;
- Certificado Digital;
- Assinatura Digital.

Criptografia Assimétrica
Par de Chaves (Pública e Privada)



Outra Visão Criptografia Assimétrica
Chaves Pública e Privada



Autoridade Certificadora (ICP – Brasil)

✓ Entidade responsável por emitir, expedir, distribuir, revogar e gerenciar os certificados digitais.

ICP Brasil

SERPRO

CAIXA

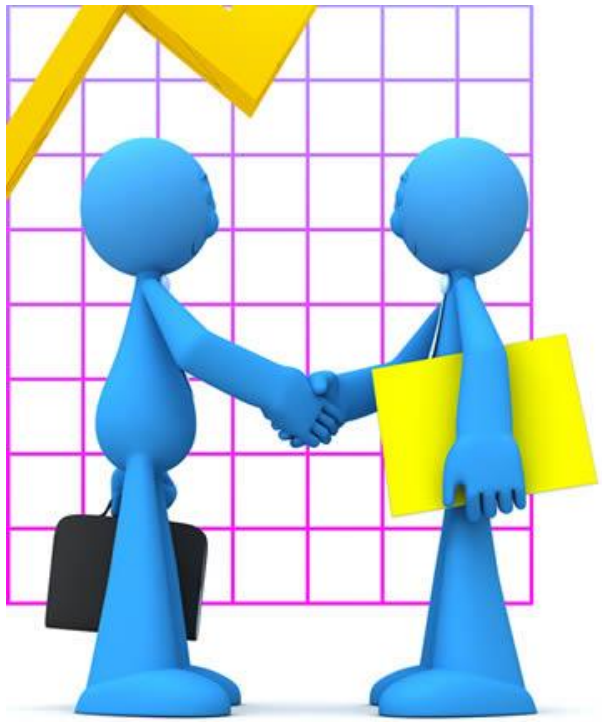
Serasa Experian
A gente trabalha para você crescer.

Receita Federal

CERTISIGN
A sua identidade na rede

Autoridade Registradora

- Entidade que verifica e valida toda documentação para a identificação da pessoa física ou jurídica.



Certificado Digital

- **Associa uma Chave Pública com uma pessoa física ou jurídica.**

- ✓ **Versão**
- ✓**Serial**
- ✓**Algoritmo ID**
- ✓**Validade**
- ✓**Chave Pública ...**

Principais Tipos de Certificados Digitais

E-CNPJ

E-CPF

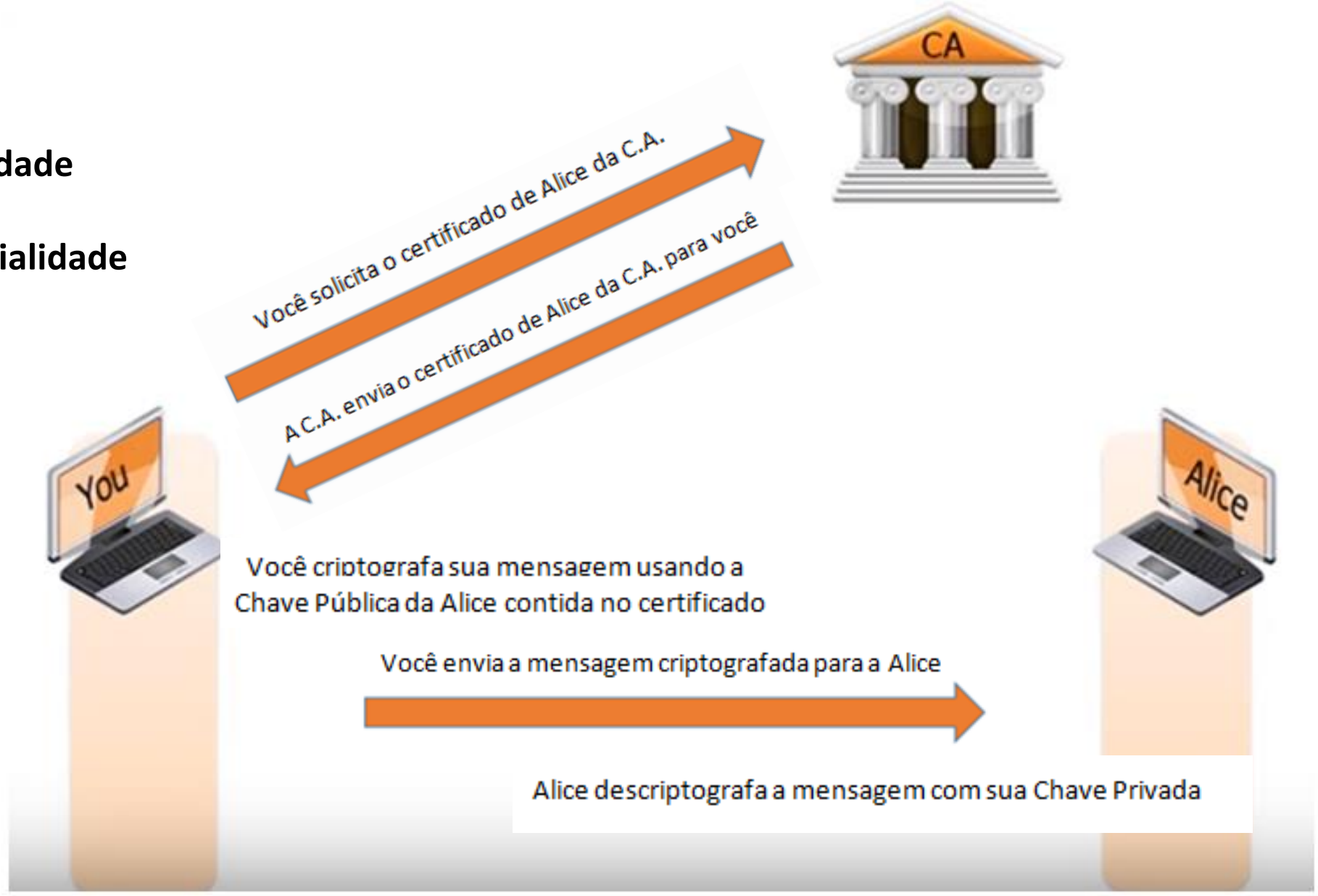
NF-E

A1

A3

Como Infraestrutura Chave Pública Trabalha

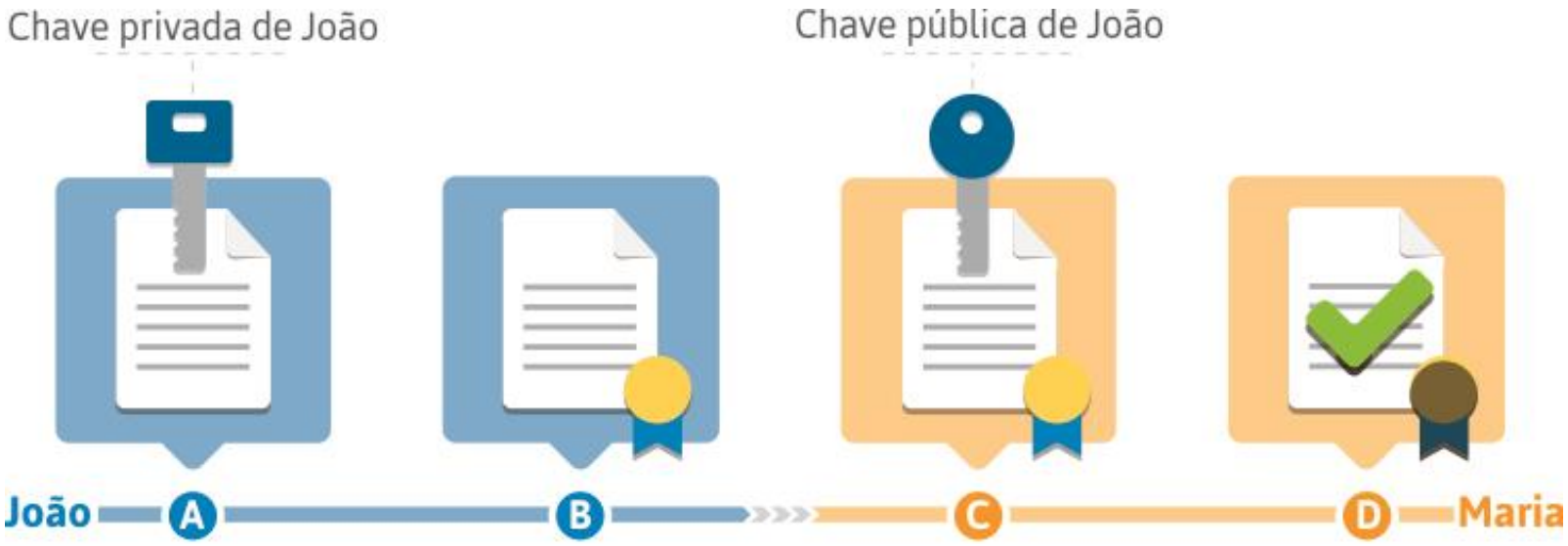
- ✓ **Autenticidade**
- ✓**Confidencialidade**



Assinatura Digital

- ✓ **Autenticidade**
- ✓**Não Repúdio**
- ✓**Integridade**
- ✓**Não garante confidencialidade**

Outra Visão Assinatura Digital



1. Assinatura do documento

Neste exemplo, João utiliza sua **chave privada[A]** para assinar digitalmente **[B]** um documento, e em seguida, enviá-lo à Maria.

2. Verificação da autenticidade

Maria utiliza a **chave pública** de João **[C]** e confirma a autenticidade da assinatura **[D]**. Qualquer pessoa que tenha acesso a essa chave pode realizar a verificação.

- www.iti.gov.br/icp-brasil
- wikipedia.org/wiki/Infraestrutura_de_Chaves_Publicas

Dúvidas

Aplausos