# Segurança da Informação

**Laboratório de Segurança em Computação**
**LabSEC / UFSC**

Maio de 2012

Ricardo F. Custódio, Dr.

Na Internet, ninguém sabe que você é um cachorro

Peter Steiner's. The New Yorker (pg 61 de 5 de Julho de 1993)

# Roubo da Informação

LabSEC
Laboratório de Segurança em Computação

# Hacker

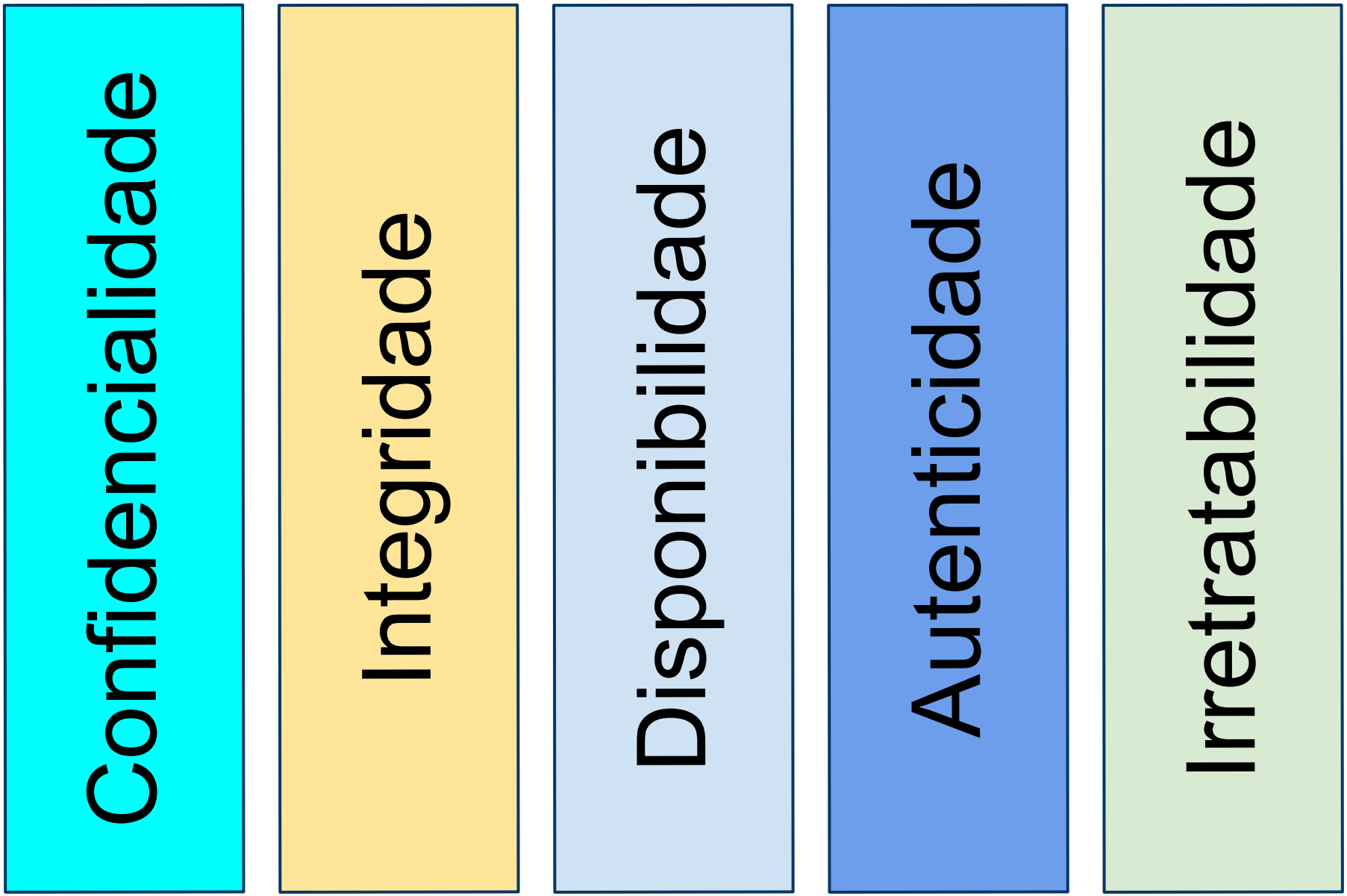
LabSEC
Laboratório de Segurança em Computação

# Proteção Natural


"João que ter certeza que seus dados estão protegidos de espiões"

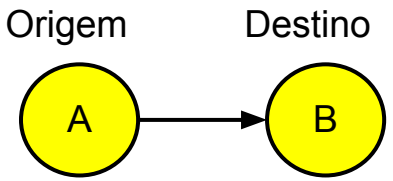
# Segurança da Informação

LabSEC
Laboratório de Segurança em Computação



# Conceitos Básicos

## Autenticação ( 6 fatores )




Beto sabe que Alice enviou a mensagem

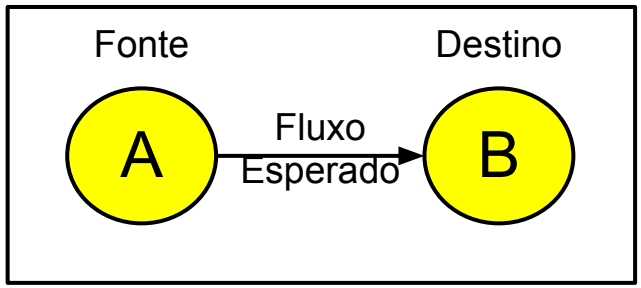
## Integridade

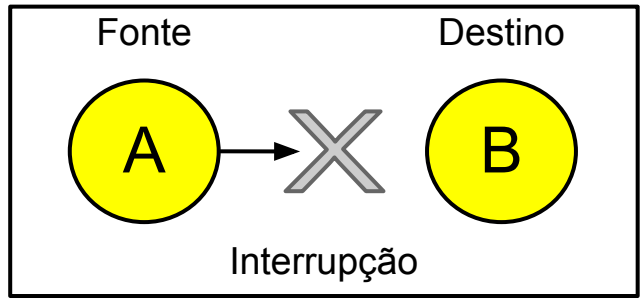
A mensagem que Beto recebeu foi a que Alice enviou

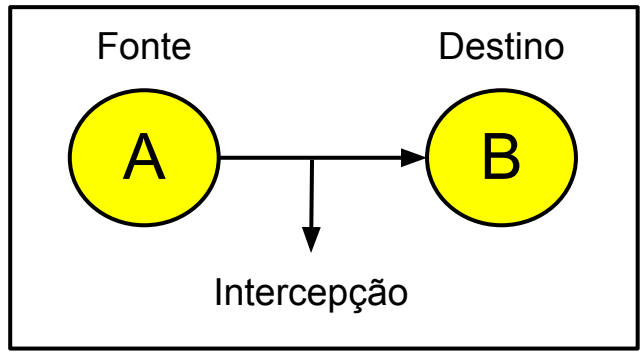
## Não Repúdio ( 3 tipos )

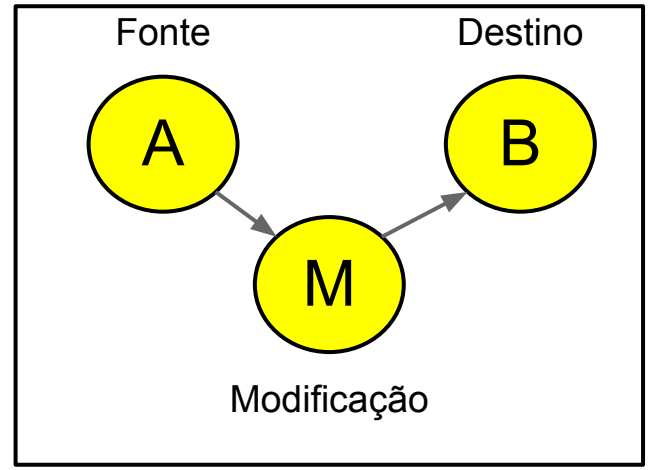
Alice não pode negar após Beto ter recebido uma mensagem dela, que ela enviou a mensagem

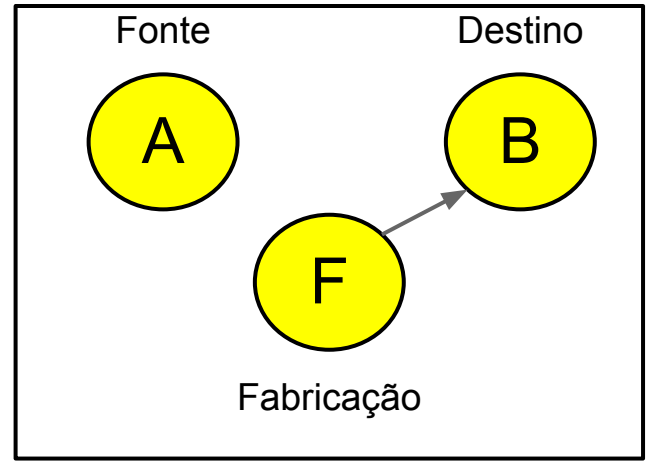
# Principais Ameaças



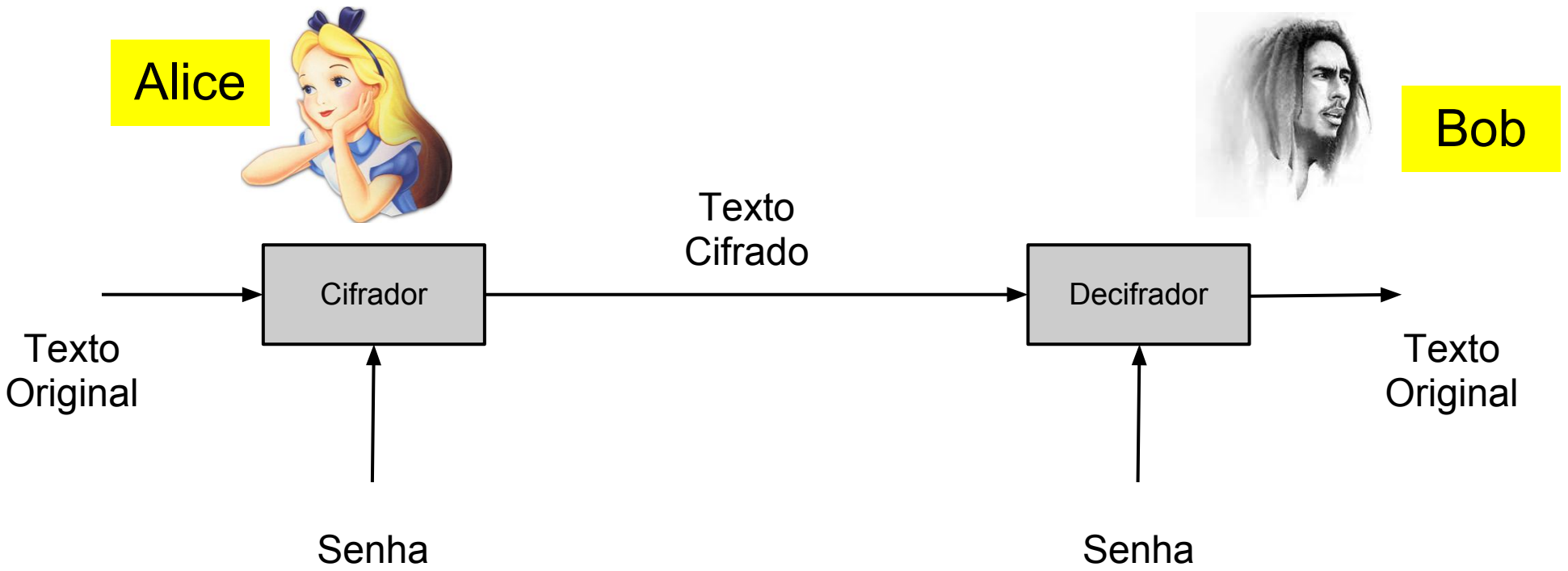



# Criptografia

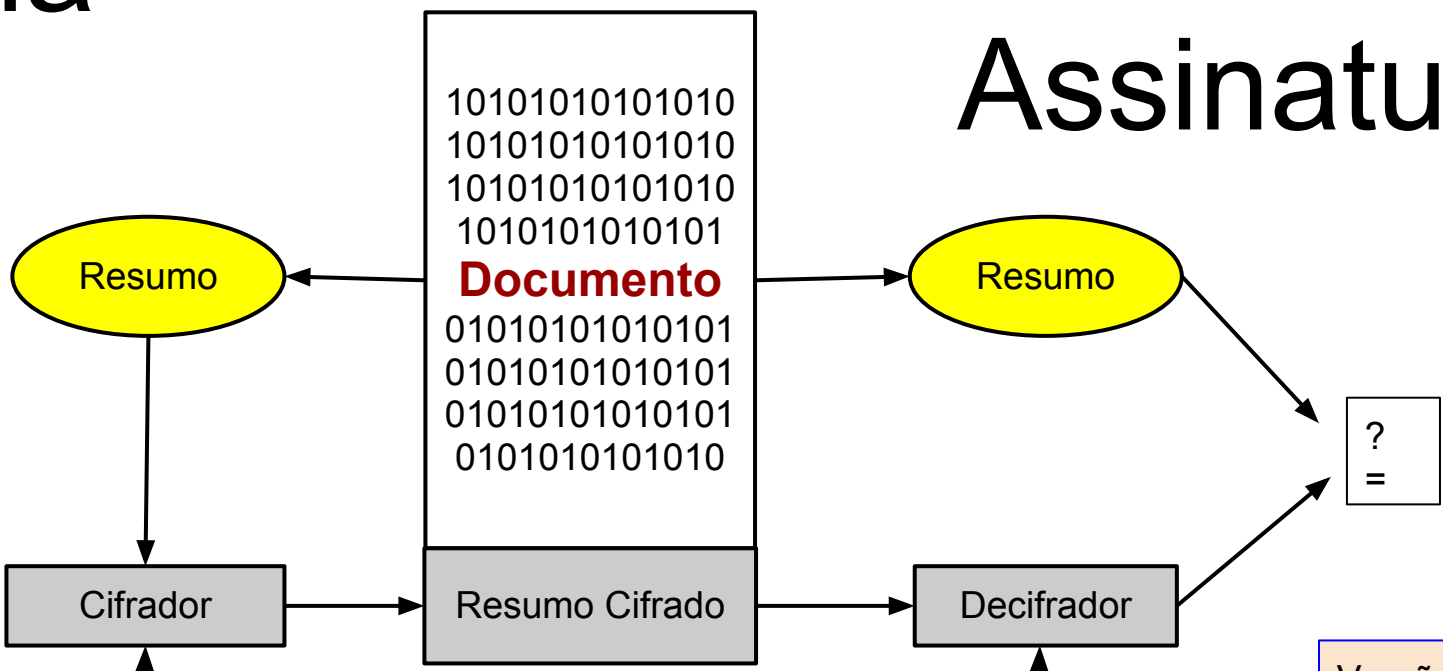


# Assinatura Digital

LabSEC
Laboratório de Segurança em Computação

## Assina

## Verifica a Assinatura





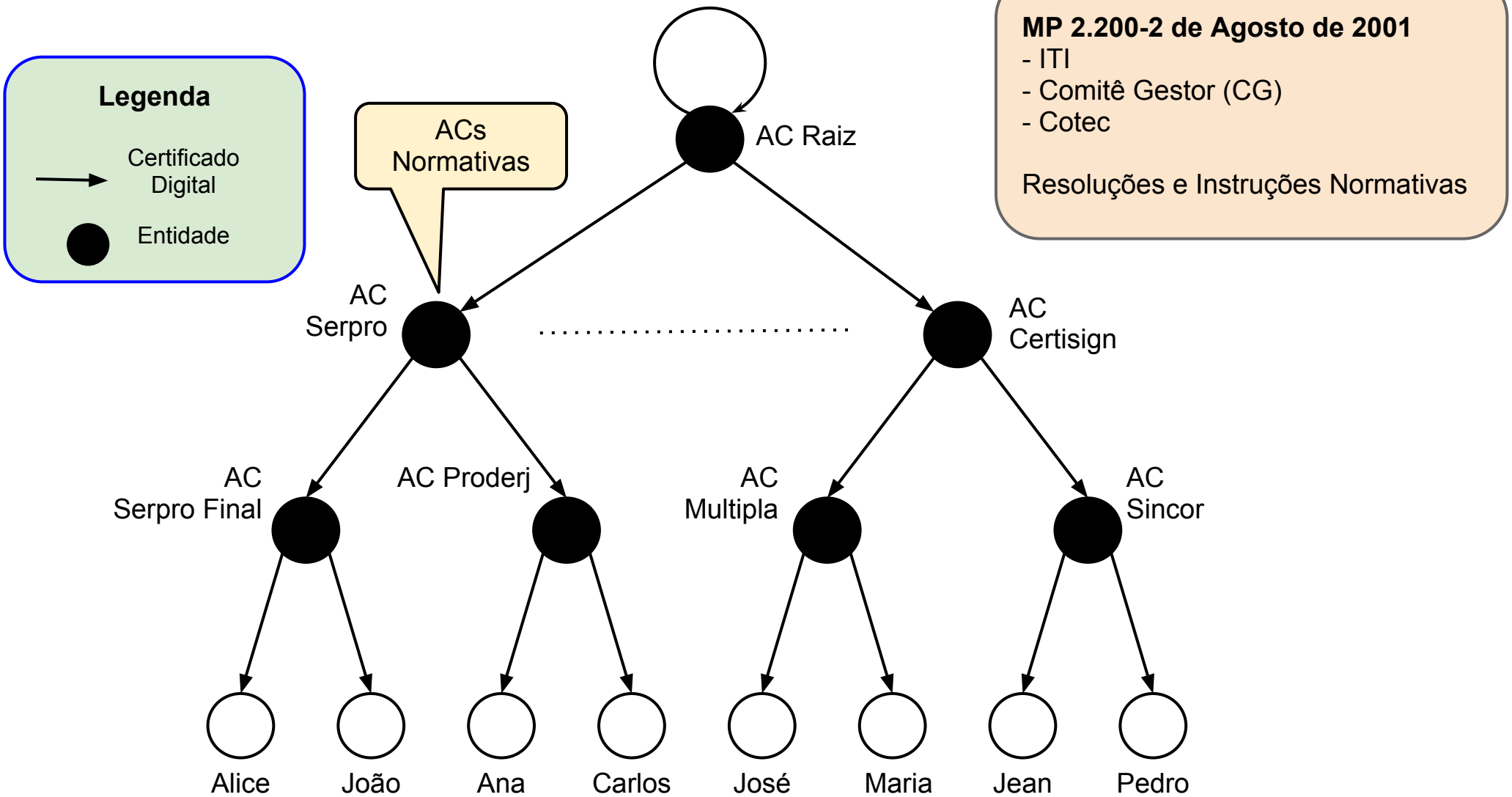
Chave Privada
ou
Chave de Assinatura

Chave Pública
ou
Chave de Verificação de Assinatura

Versão
Número de Série
Algorítmo
Período de Validade
**Chave Pública**
Extensões
Assinatura da AC

Certificado Digital

# ICP-Brasil

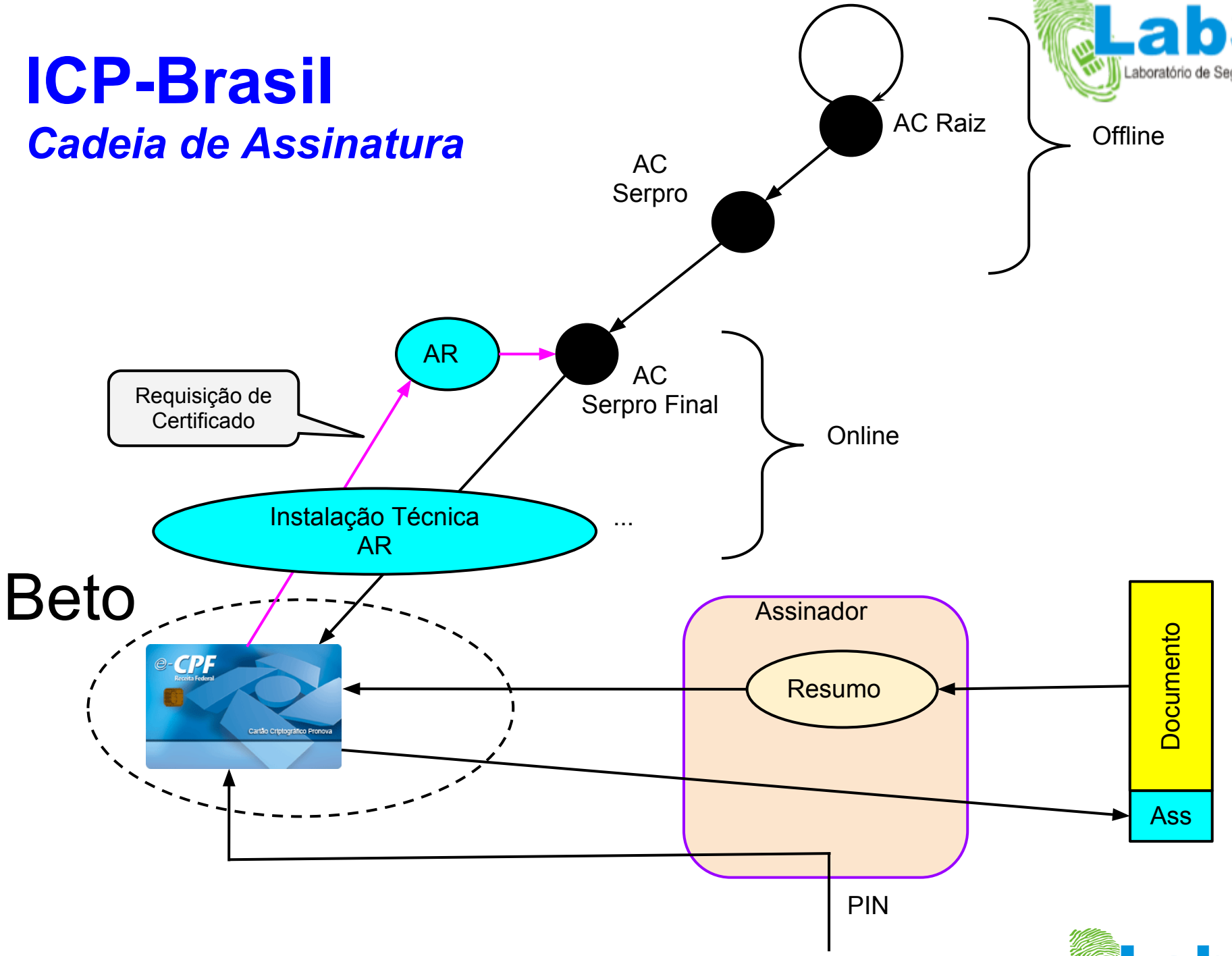



**MP 2.200-2 de Agosto de 2001**
- ITI
- Comitê Gestor (CG)
- Cotec

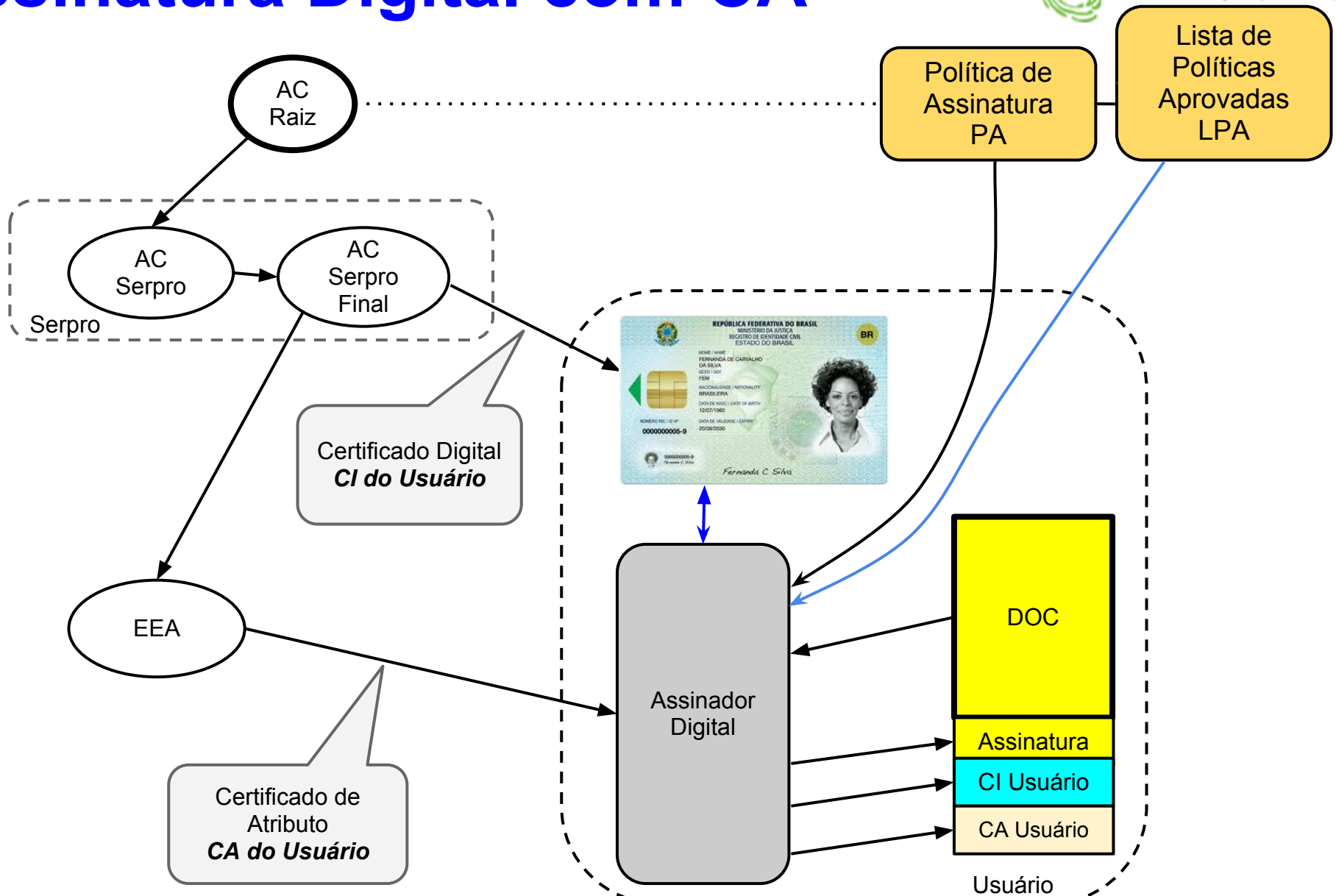
Resoluções e Instruções Normativas

# ICP-Brasil

## *Cadeia de Assinatura*



# Assinatura Digital com CA



# Considerações Finais

LabSEC
Laboratório de Segurança em Computação

- Internet é de duplo caminho
- Âncoras de Confiança
  - TSL
- Principais Desafios
  - Gestão de Identidades
    - Internet das Pessoas e das Coisas
  - Conscientização
  - Dados distribuídos
- Futuro
  - Computação em Nuvem
  - Dados na Nuvem
  - Computação Quântica