Autenticação, Assinatura Digital e certificado

Prof.: Thiago H. Bom Conselho
UNATEC- Rede de Computadores

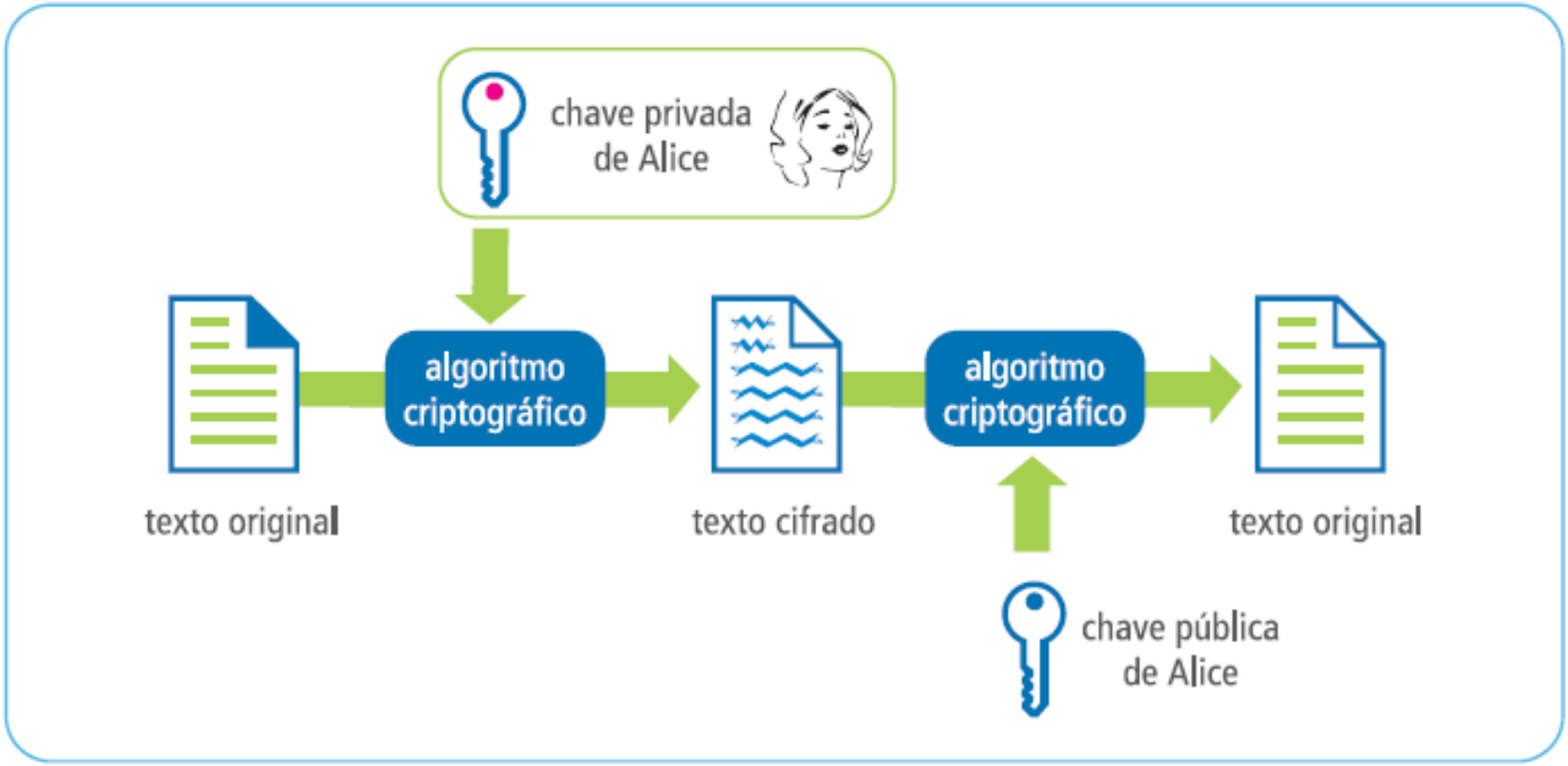
Objetivo do Apresentação

- Fundamentar o processo de autenticação no contexto criptográfico
- Entender o objetivo da assinatura digital e certificado digital, bem como os processos, algoritmos e técnica utilizadas
- Objetiva-se também a compreensão dos tokens de e-cpf.

Autenticação

- Autenticação é o processo de reconhecimento dos dados que são recebidos, comparando-os com os dados que foram enviados, e verificando se o transmissor que fez a requisição é, na verdade, o transmissor real.
- No processo de autenticação, as chaves são aplicadas no sentido inverso ao da confidencialidade.
- O autor de um documento utiliza sua chave privada para cifrá-lo de modo a garantir a autoria em um documento ou a identificação em uma transação. Esse resultado só é obtido porque a chave privada é conhecida exclusivamente por seu proprietário

Autenticação(exemplo)



Assinatura Digital

- O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de hash, é chamada de **assinatura digital.**
- O resumo criptográfico pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

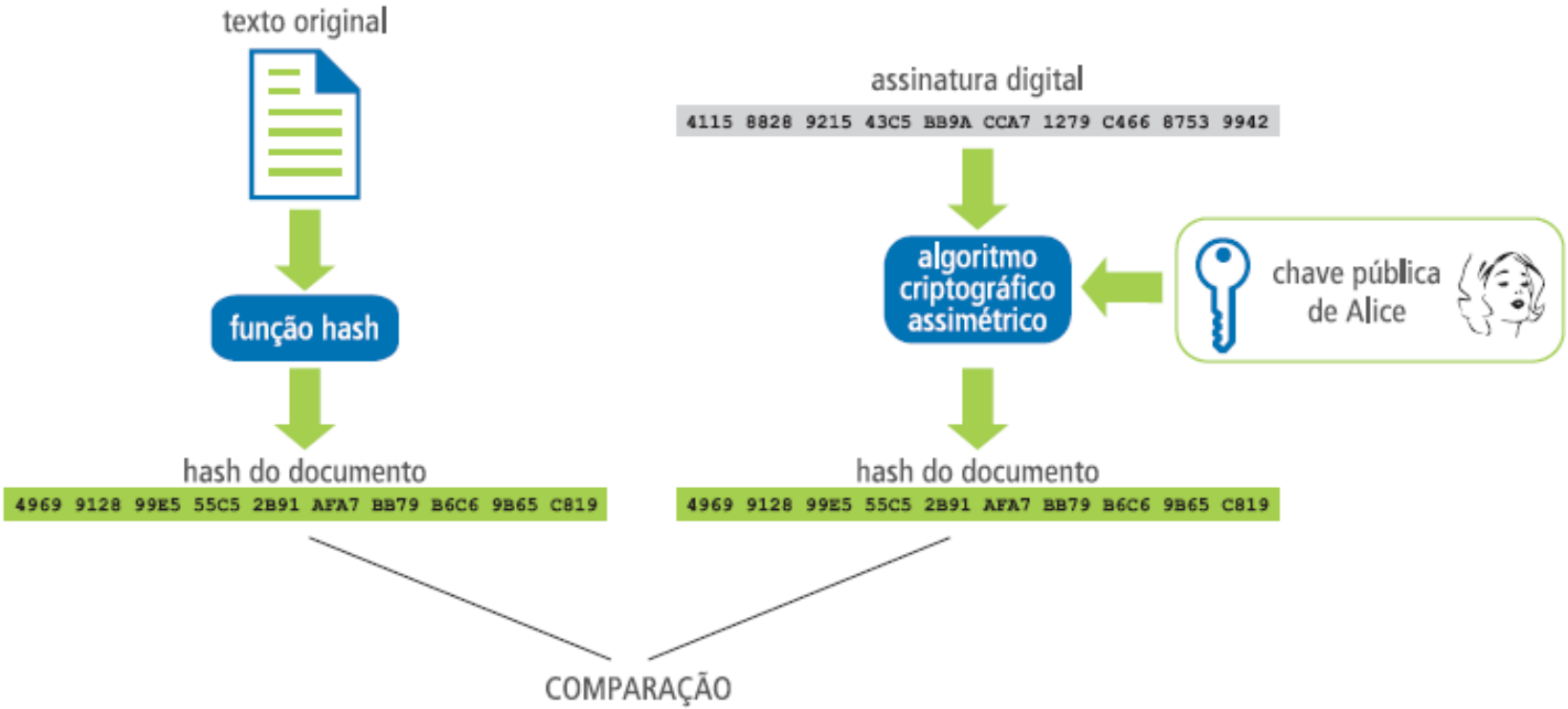
Assinatura Digital (Processo)

A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, pois os algoritmos de criptografia assimétrica são muito lentos.

Validando a Assinatura Digital

- Para comprovar uma assinatura digital é necessário inicialmente realizar duas operações:
  - Calcular o resumo criptográfico do documento e decifrar a assinatura com a chave pública do signatário.
- Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro.
- Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública.

Validando a Assinatura Digital



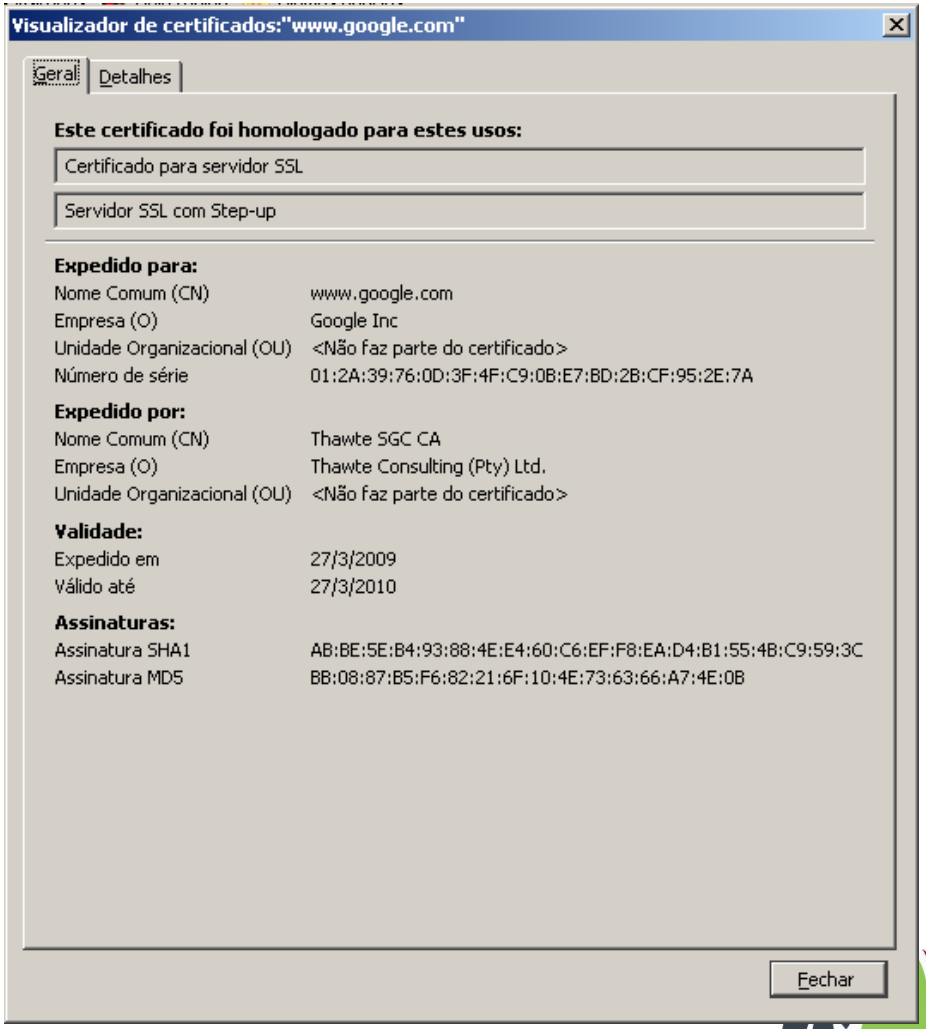
Conferência da assinatura digital

Assinatura Digital Vs Assinatura Manuscrita

- A semelhança da assinatura digital e da assinatura manuscrita restringe-se ao princípio de atribuição de autoria a um documento.
- Em agosto de 2001, a Medida Provisória 2.200 garantiu a validade jurídica de documentos eletrônicos e a utilização de certificados digitais para atribuir autenticidade e integridade aos documentos. Este fato tornou a assinatura digital um instrumento válido juridicamente.

Certificado Digital

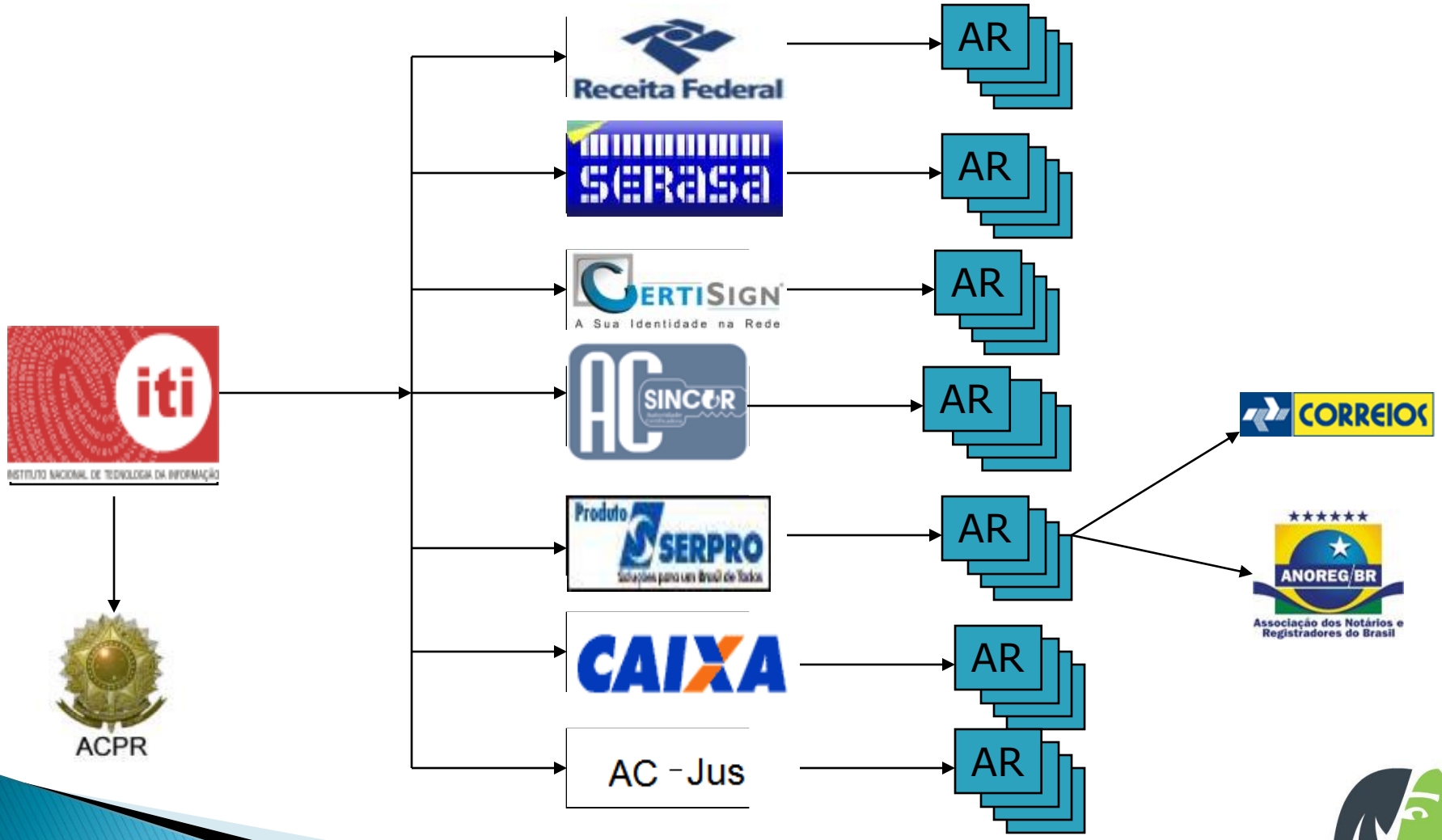
- O certificado digital é um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública.



Certificado Digital X.509

- Versão – Contem a versão do certificado X.509, atualmente versão 3
- Número serial – Todo certificado possui um, não é globalmente único, mas único no âmbito de uma AC
- Tipo de algoritmo – Contem um identificador do algoritmo criptográfico usado pela AC para assinar o certificado juntamente com o tipo de função de hash criptográfica usada no certificado
- Nome do titular – Nome da entidade para o qual o certificado foi emitido
- Nome do emitente – Autoridade Certificadora que emitiu/assinou o certificado
- Período de validade
- Informações de chave pública da entidade
  - Algoritmo de chave pública
  - Chave pública
- Assinatura da AC
- Identificador da chave do titular
- Identificador da chave do emitente
- Atributos ou extensões

Infraestrutura ICP-Brasil



Infraestrutura ICP-Brasil

- ITI – Instituto Nacional de Tecnologia da Informação
- AC – Autoridades Certificadoras
- AR – Autoridades de Registro

Infraestrutura ICP-Brasil Atual

- 8 Autoridades Certificadoras de 1° Nível
- 21 Autoridades Certificadoras de 2° Nível
- 59 Autoridades de Registro
- 862 Instalações Técnicas de AR

Hardware Certificado Digital

Leitora Smart Card

Smart Card

Desktop

Token USB

Notebook

E-CPF

Dados Certificado Digital

Chave Privada

Nome da Pessoa

CPF ou CNPJ

CPF do Resp. CNPJ

PIS / PASEP

Titulo Eleitor

Registro Geral

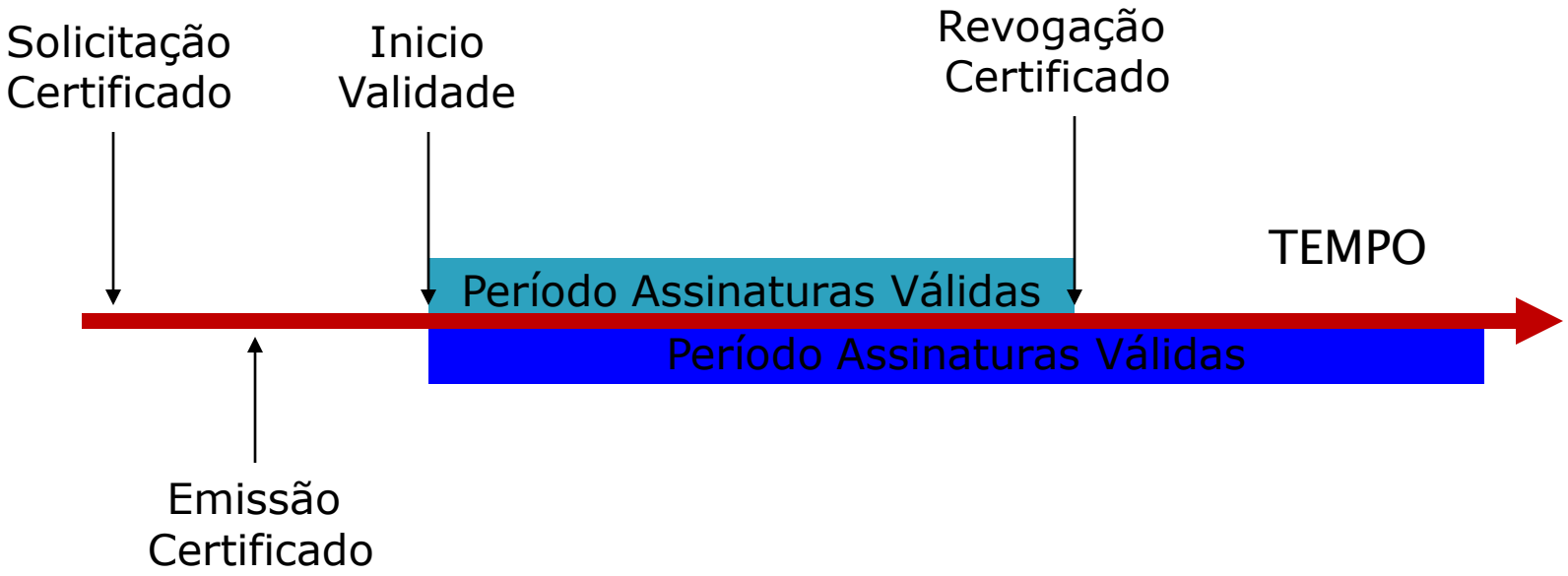
Chave Pública

Data de Validade

Nome Autoridade Certificadora

Ident. Sistema Criptográfico

Linha do Tempo – Certificado Digital



Bibliografia

- ITI. O que é Certificação Digital? www.iti.gov.br, 2009
- Dias Alves,Robson. **Certificado Digital.** Anotações de Aula