

IX CONIP

Certificação Digital Possibilidades e Limitações

Prof. Pedro Antonio D Rezende
Ciência da Computação – Univ. de Brasília

www.cic.unb.br/docentes/pedro/sd.htm

O que constitui uma ICP

- ◆ Leis (documento eletrônico, assinatura digital)
- ◆ Práticas sociais (premissas, risco aceitável)
- ◆ Procedimentos administrativos
- ◆ Protocolos criptográficos
- ◆ Algoritmos criptográficos
- ◆ Padrões e formatos digitais
- ◆ Infraestrutura tecnológica (HW, SW)

Assinatura Digital - Presunções

Premissas de confiança

- 1- **Premissa pública:** O titular de um par de chaves assimétricas é conhecido *digitalmente* por sua chave pública
- 2- **Premissa privada:** O titular de um par de chaves assimétricas é quem conhece e opera sua chave privada

Assinatura Digital – Eficácia

Crenças	Sintática	Semântica
Pública	O vínculo entre chave pública e nome do seu titular é autêntico	O nome do titular representa vínculo social com o verificador
Privada	Acesso e uso da chave privada restringe-se ao seu titular	O uso autenticatório da chave privada significa expressão de vontade