Instituto Nacional de Tecnologia da Informação

Certificação Digital

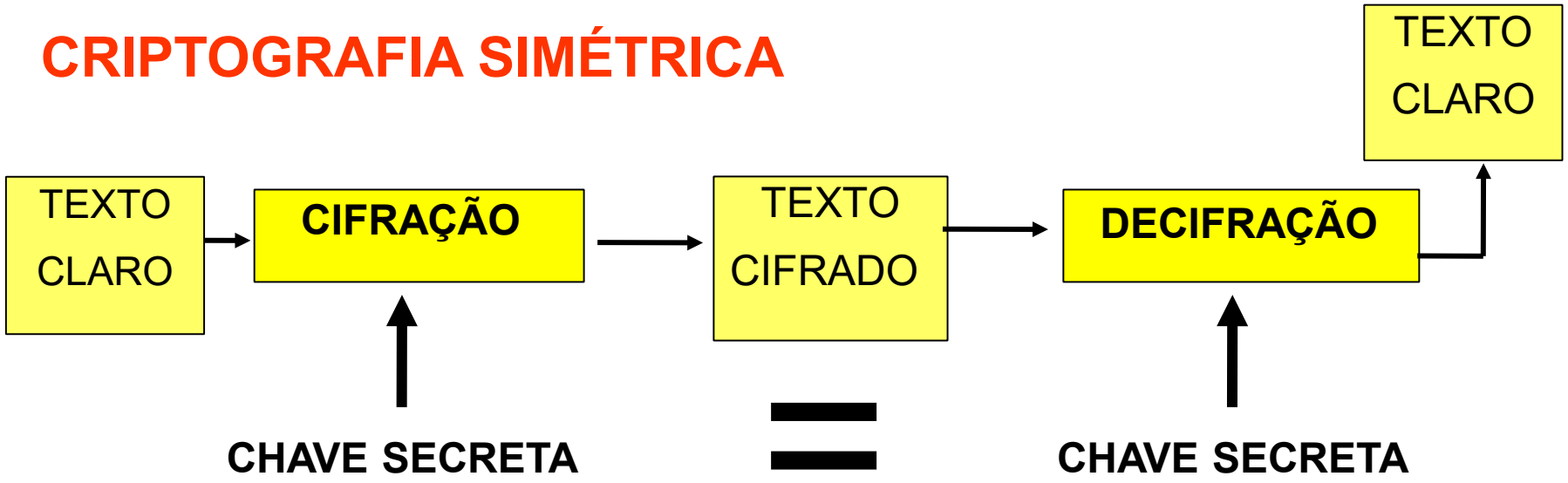
I Encontro Técnico dos Integrantes do Sistema de Gestão de Documentos de Arquivo – SIGA – da Administração Pública Federal
12 a 14 de Setembro de 2006 - Brasília/DF

Viviane Regina Lemos Bertol

Coordenação-Geral de Normalização e Pesquisa

Comecemos com alguns conceitos

CRIPTOGRAFIA SIMÉTRICA



Vantagens:

Tamanho da chave menor
Processo mais rápido

Desvantagens:

Distribuição Segura da Chave
Escala

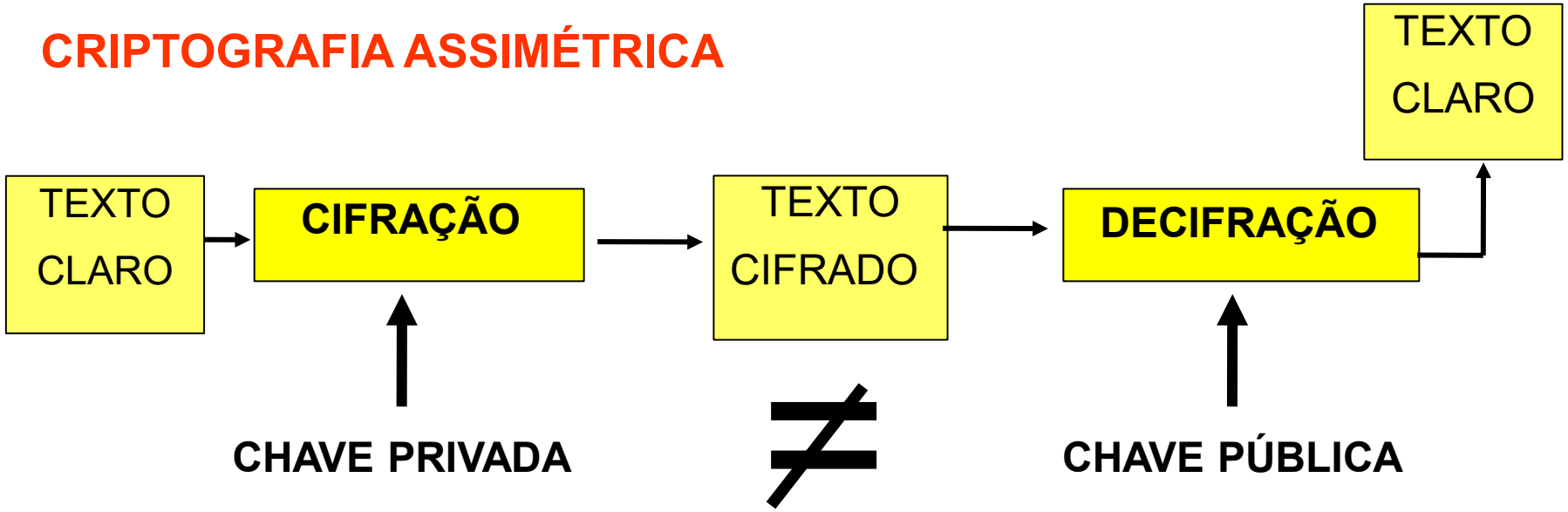
Conceitos…

CRIPTOGRAFIA ASSIMÉTRICA

- Par de chaves matematicamente relacionadas de maneira unívoca
- O conhecimento de uma das chaves não possibilita a dedução da outra
- Portanto, uma das chaves pode tornar-se PÚBLICA (de conhecimento de todos), sem risco de a outra, a PRIVADA (de conhecimento e posse apenas de seu titular), ser deduzida, ainda que com o uso de grande capacidade computacional

CONCEITOS…

CRIPTOGRAFIA ASSIMÉTRICA



Vantagens:

Distribuição Segura da Chave

Escala

Desvantagens:

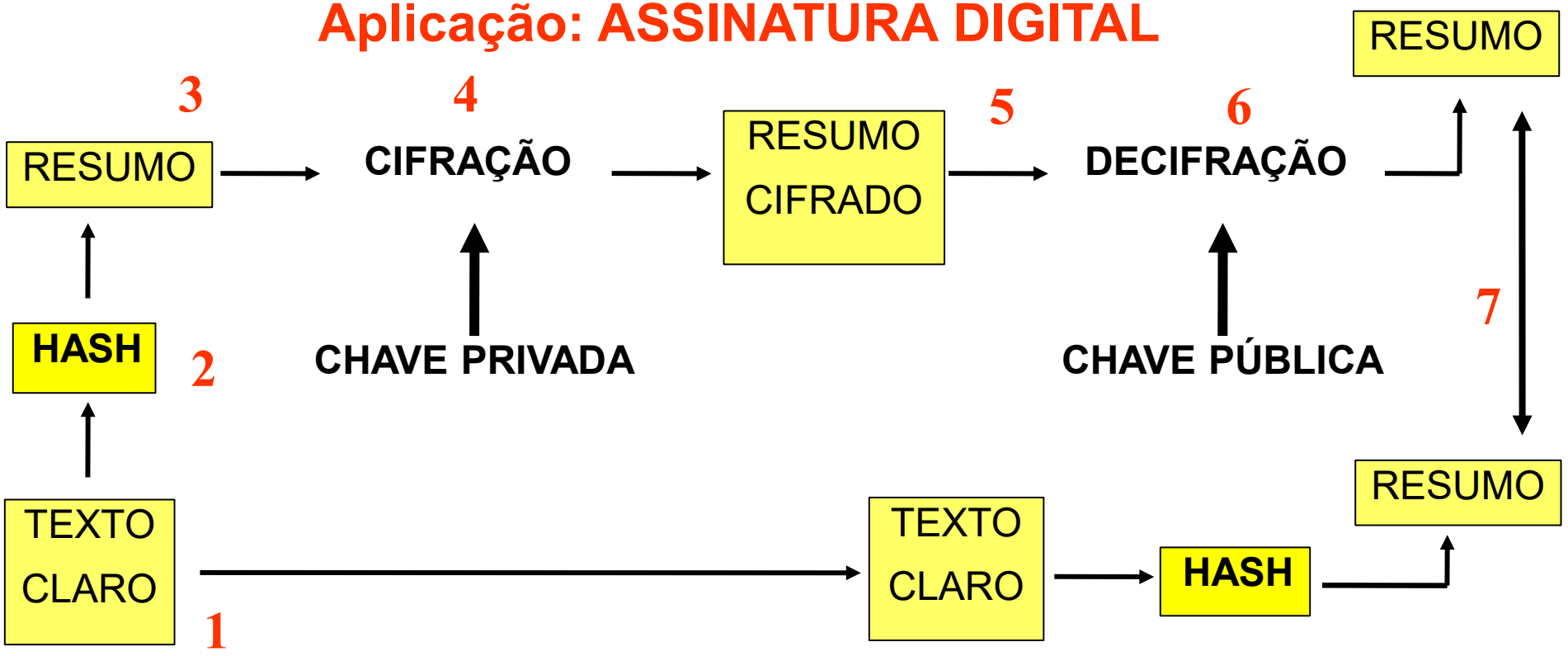
Tamanho da chave maior

Processo mais lento

Instituto Nacional de Tecnologia da Informação

CRIPTOGRAFIA ASSIMÉTRICA

Aplicação: ASSINATURA DIGITAL



Instituto Nacional de Tecnologia da Informação

CRIPTOGRAFIA ASSIMÉTRICA

Aplicação: ASSINATURA DIGITAL

Propriedades:

I. AUTENTICIDADE

II. INTEGRIDADE

III. NÃO REPÚDIO

Instituto Nacional de Tecnologia da Informação

CERTIFICADO DIGITAL

Nome: xxxxxxxxxxxx

Data de Nascimento: xx/xx/xx

CPF: xxx.xxx.xxx-xx

CI: xxxxxxxx SSP/DF

Início da Validade: xx/xx/xx

Final da Validade: xx/xx/xx

Quem emitiu: xxxxxxx

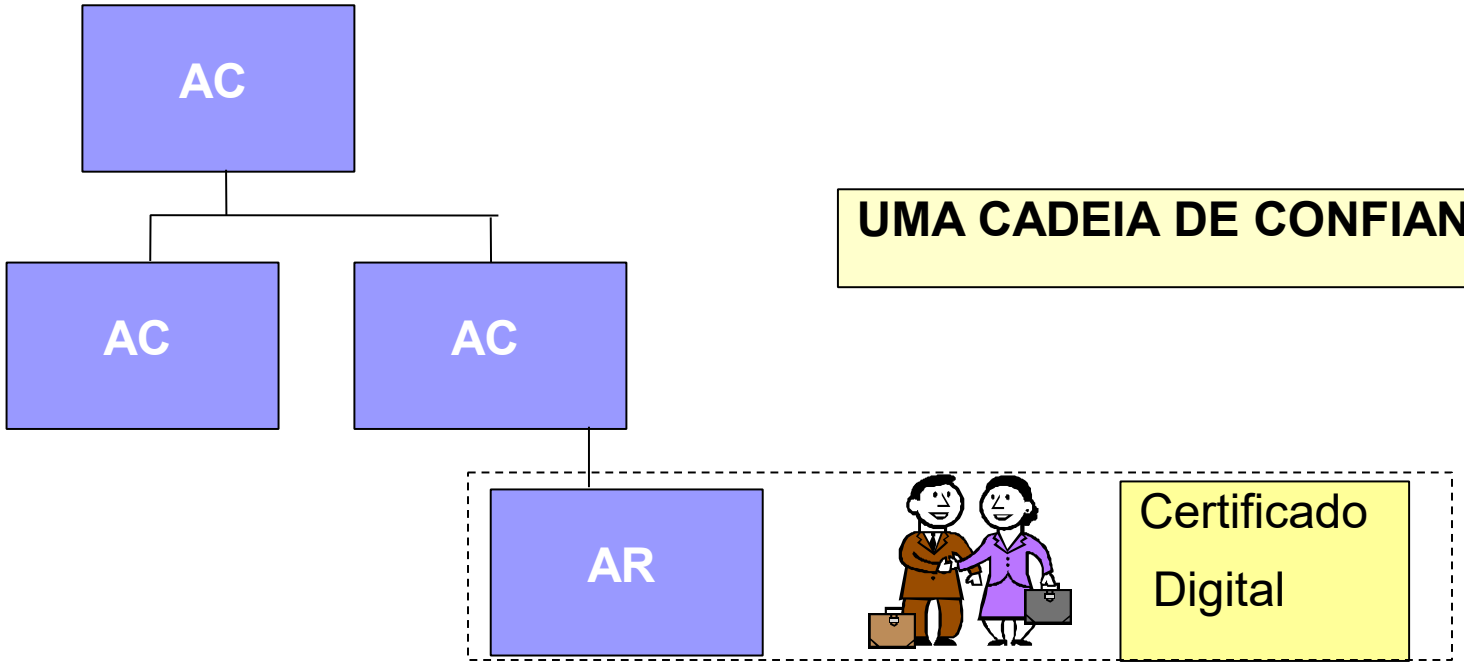
Chave Pública;

xvbc dsfe ntas njty sdel ….

nbue jfht awme dcel vbfm

Instituto Nacional de Tecnologia da Informação

INFRA-ESTRUTURA DE CHAVES PÚBLICAS



UMA CADEIA DE CONFIANÇA!

Instituto Nacional de Tecnologia da Informação

ICP-Brasil

- Criada a partir da percepção do Governo Federal da importância de regulamentar as atividades de certificação digital

- Conjunto de entidades, padrões técnicos e regulamentos para suportar sistema criptográfico de certificados digitais

Instituto Nacional de Tecnologia da Informação

INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

Instituída em 2001 – MP 2.200-2/2001

Propriedades (assinatura digital)

I. AUTENTICIDADE

II. INTEGRIDADE

III. NÃO REPÚDIO

+

IV. VALIDADE JURÍDICA

Instituto Nacional de Tecnologia da Informação

PRINCÍPIOS FUNDAMENTAIS DA ICP-BRASIL

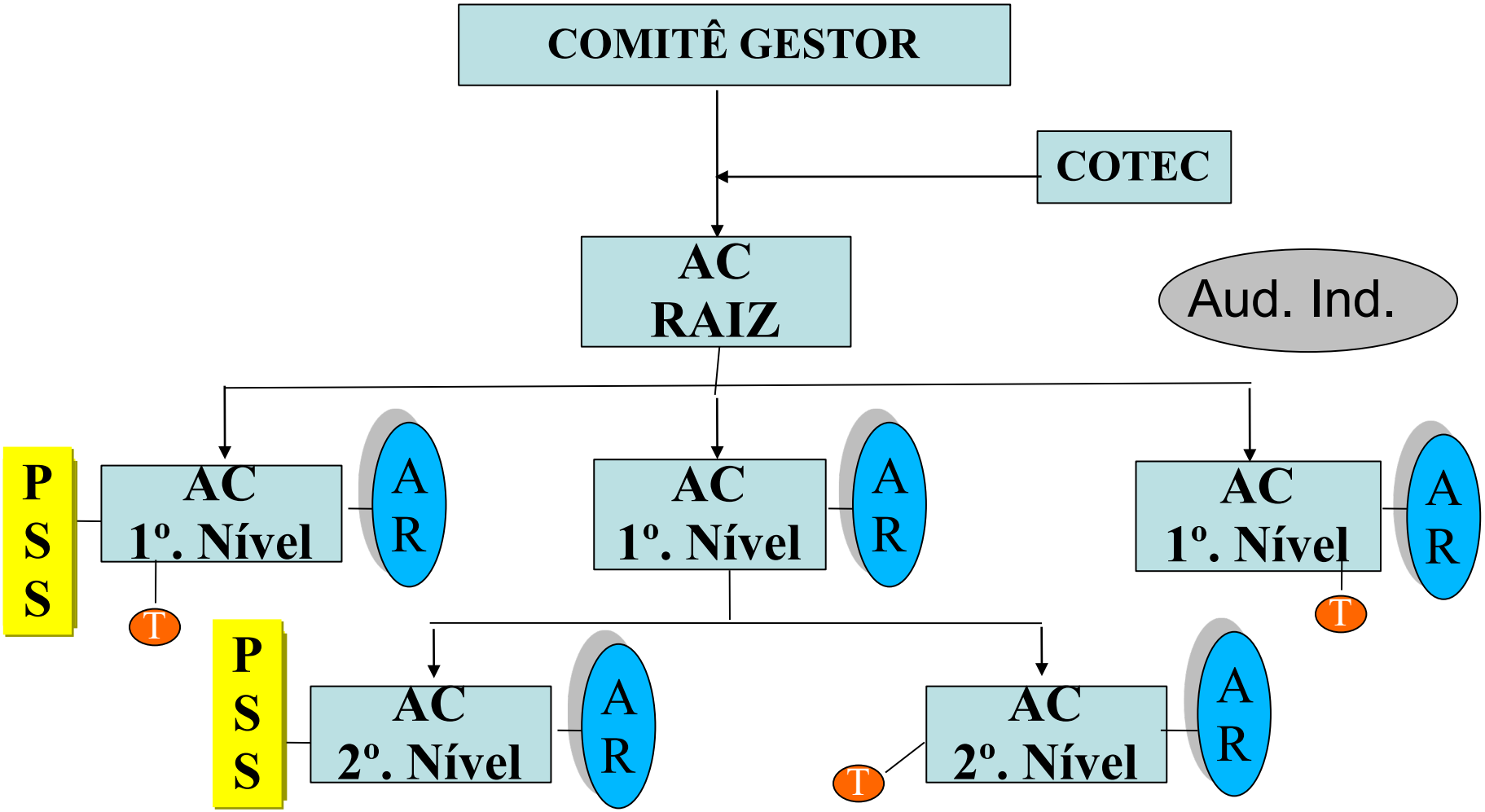
- Identificação Presencial
- Não tutela de chave privada
- Auditoria/Fiscalização
- Interoperabilidade

Instituto Nacional de Tecnologia da Informação

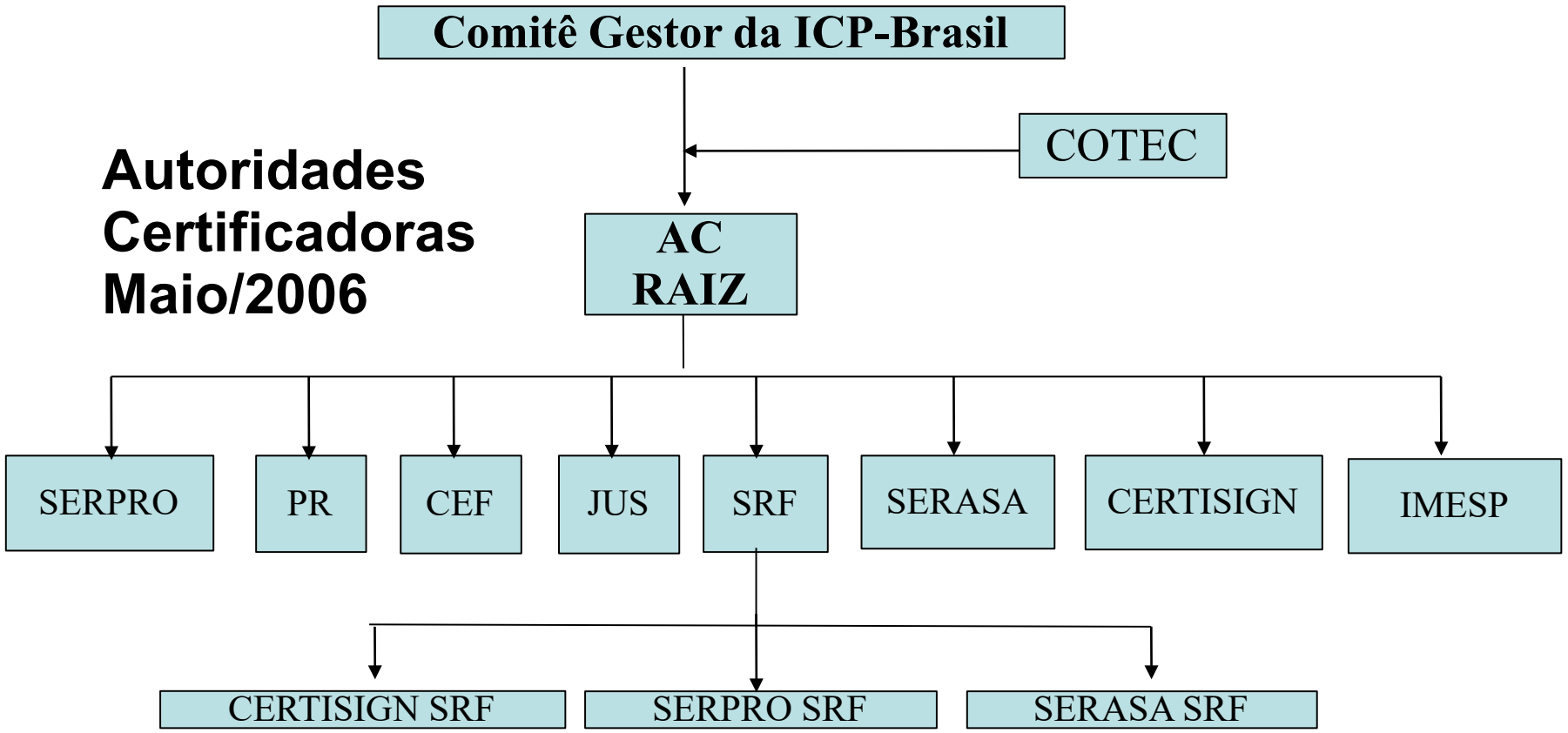
Por que usar certificados da ICP-Brasil

- Validade jurídica dos documentos assinados
- Padrões internacionais de segurança e interoperabilidade
- Identificação presencial do titular do certificado
- Seguro de responsabilidade civil
- Guarda permanente dos certificados e LCR
- Auditoria prévia e anual nas entidades

Instituto Nacional de Tecnologia da Informação

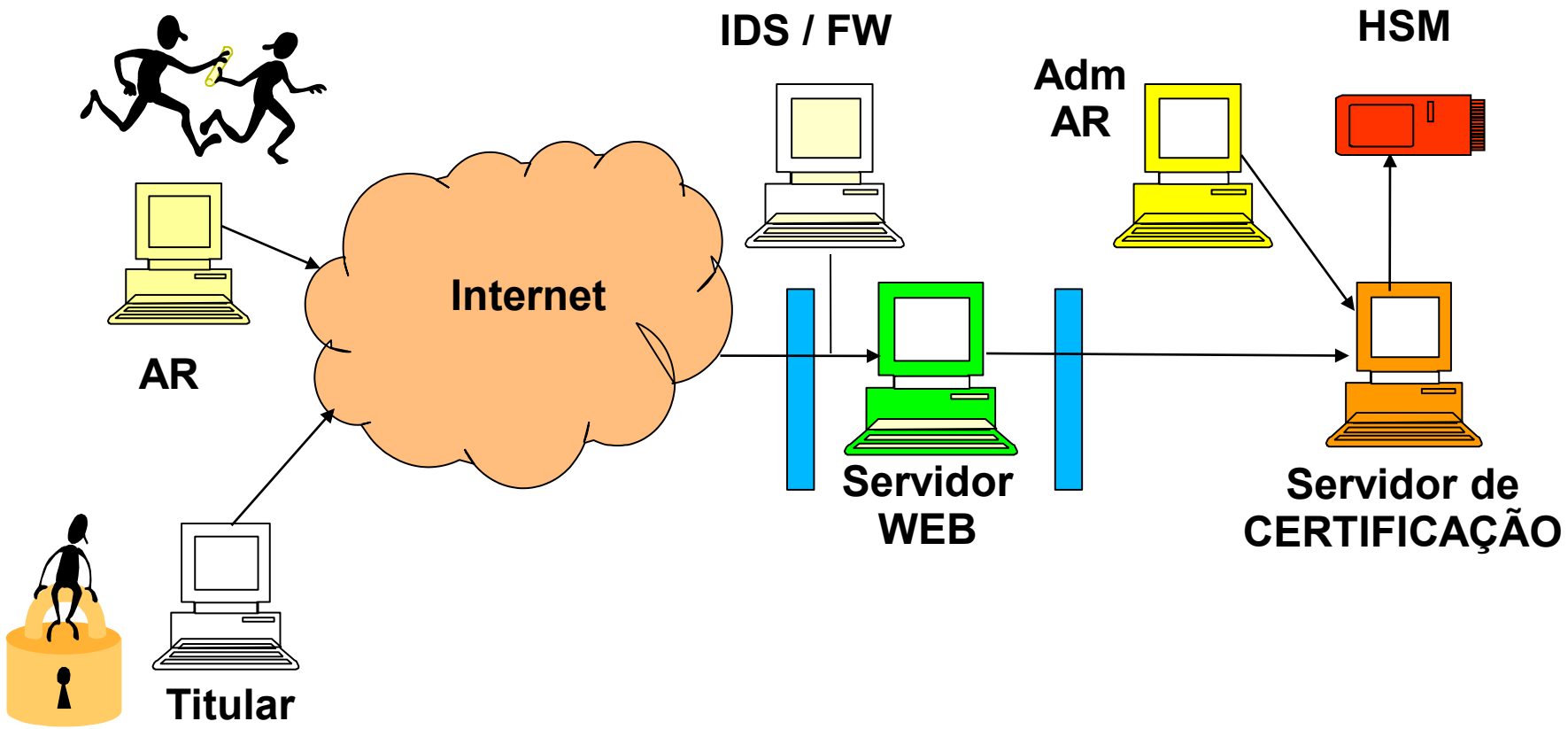


Instituto Nacional de Tecnologia da Informação



Instituto Nacional de Tecnologia da Informação

Sistema de Certificação



Instituto Nacional de Tecnologia da Informação

APLICAÇÕES USANDO CERTIFICADOS ICP-BRASIL

- Sistema Brasileiro de Pagamentos – SPB
- DCTF, DIRPF, DIRPJ, e-CAC, PAF (SRF/MF)
- Escrituração Fiscal – Sefaz do Estado de Pernambuco
- NF-e – Nota Fiscal Eletrônica (SRF/MF, SP,GO,MA,BA,SC,RS)
- Contratos de Câmbio
- Apólices de Seguros
- Pregões Eletrônicos (SP,SC,MG) e COMPRASNET (Federal)
- Sistemas ¨Estruturadores¨ do Governo Federal e SCPD
- Internet Banking e Mobile Banking

Instituto Nacional de Tecnologia da Informação

APLICAÇÕES USANDO CERTIFICADOS ICP-BRASIL

- PROUNI - MEC
- JUROS ZERO - FINEP
- E-DOC do TRT 4a. Região e outros cases na esfera do judiciário (TJ-RS, TJ-RJ, e-Jus, Diário da Justiça On-Line etc.)
- DETRAN - MG
- Licenças Ambientais – CETESB/SP
- INPI
- Contadores, Odontólogos, Médicos, Corretores de Seguros, Servidores do Executivo, Legislativo e Judiciário Federais

Instituto Nacional de Tecnologia da Informação

A ICP-BRASIL É RECONHECIDA COMO FERRAMENTA TECNOLÓGICA DE APOIO À TRANSPARÊNCIA...

ICP-BRASIL = SEGURANÇA TECNOLÓGICA + SEGURANÇA JURÍDICA + INTEROPERABILIDADE

↓

Identificação Segura das partes + Registro/Auditabilidade das transações/documentos eletrônicos + responsabilidade jurídica presumida

↓

Prevenção e Combate às fraudes e à corrupção

↓

TRANSPARÊNCIA DA GESTÃO GOVERNAMENTAL

Sites para consulta

ITI – www.iti.gov.br e www.iti.br

CEF – www.icp.caixa.gov.br/asp/respositorio.asp

JUS – http://acjus.gov.br/acjus

PR – https://thor.serpro.gov.br

SRF – http://www.receita.fazenda.gov.br/acsrf

SERASA – http://certificadodigital.com.br/repositorio

SERPRO – https://thor.serpro.gov.br/ACSERPRO

CERTISIGN – http://www.icp-brasil.certisign.com.br/repositorio

Instituto Nacional de Tecnologia da Informação

MUITO OBRIGADA!

VIVIANE REGINA LEMOS BERTOL
Coordenadora Geral de Normalização e Pesquisa
e-mail: viviane@planalto.gov.br

Instituto Nacional de Tecnologia da Informação
Casa Civil da Presidência da República