ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira

Wilson R Hirata

Agenda

- Regulamentação
- Requisitos Técnicos
- Estrutura da ICP-Brasil
- Raiz Nacional

Normas

Regulamentos da ICP-Brasil

- Lei - MP n° 2.200-2, 24 de agosto de 2001
- Decretos regulamentam a Lei (6.605, 8985, 9183)
- Resoluções do Comitê Gestor da ICP-Brasil
- Instruções Normativas do ITI

Obs: Normas organizadas em documentos:

– DOC-ICP-nn

http://www.iti.gov.br/legislacao/61-legislacao/504-documentos-principais

Legislação

Valor jurídico das assinaturas digitais

ICP-Brasil – MP 2.200-2/2001 - Institui a Infraestrutura de Chaves Públicas Brasileira e dá outras providências

Art. 10º

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

Tamanhos de Chaves

Algoritmo	***RSA, ECC-Brainpool (RFC 5639)***
Tipo de Certificado A1, A2, A3, S1, S2, S3, T3, A-CF-e-SAT	RSA 2048 ou BrainpoolP256r1
Tipo de Certificado – A4, S4, T4	RSA 4096 ou BrainpoolP512r1

Validade dos Certificados

Tipo de Certificado	***Período Máximo de Validade do Certificado (em anos)***
A1 e S1	1
A2 e S2	2
A3, S3 e T3	5
A4, S4 e T4	11 (para cadeias hierárquicas completas em Curvas Elípticas)
	6 (para as demais hierarquias)
A-CF-e-SAT	5

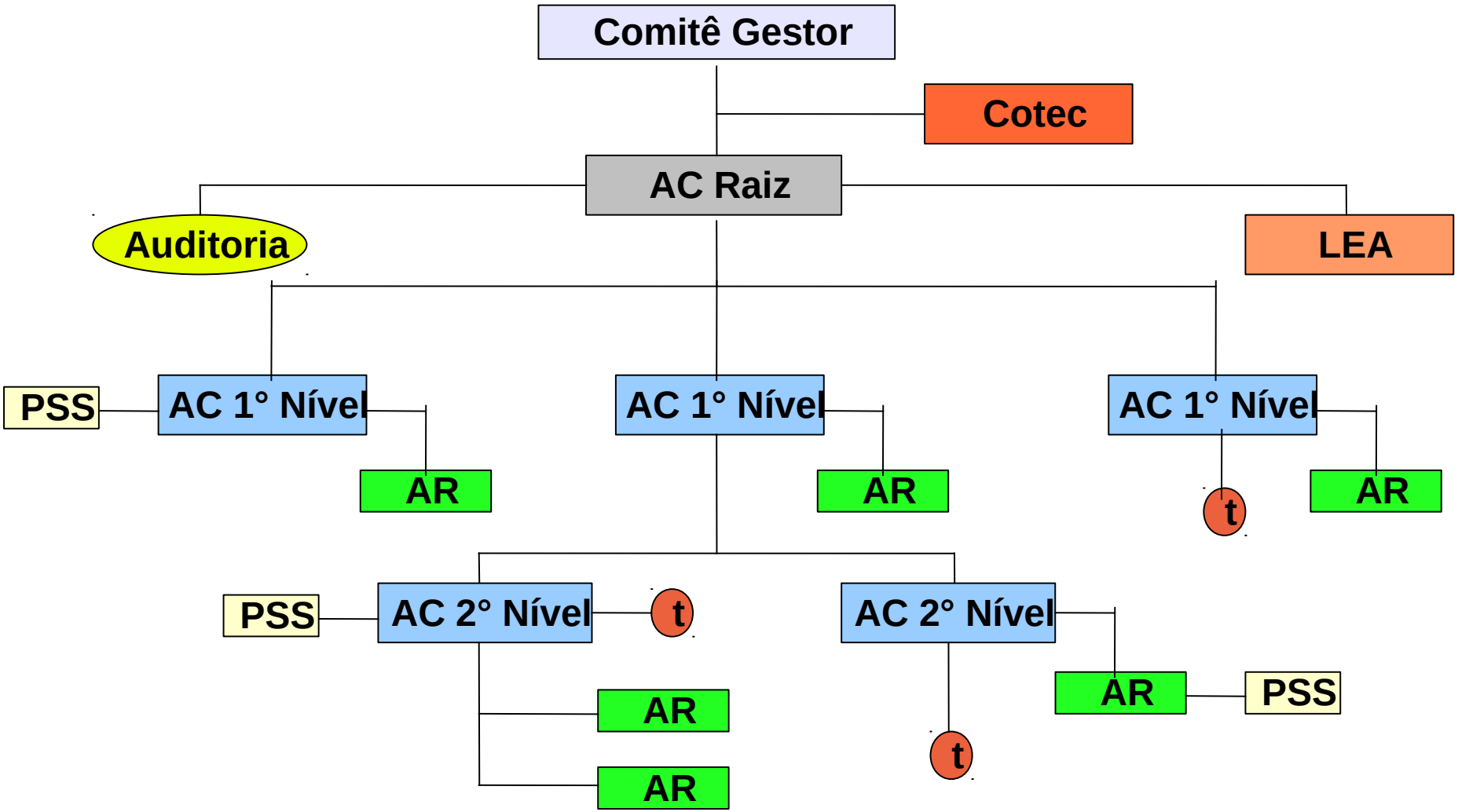
Mídia Armazenadora

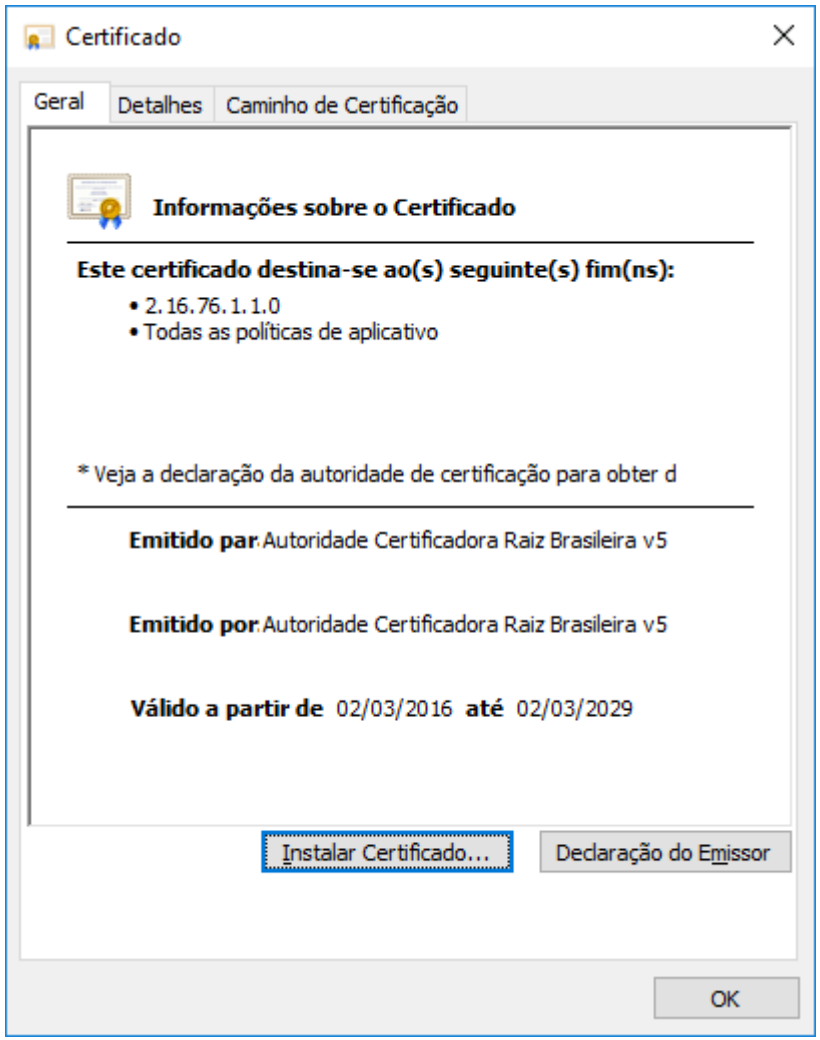
Tipo de Certificado	*Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)*
A1 e S1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software
A2 e S2	Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica
A3 e S3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO
A4 e S4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO
T3 e T4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO
A CF-e-SAT	Hardware criptográfico

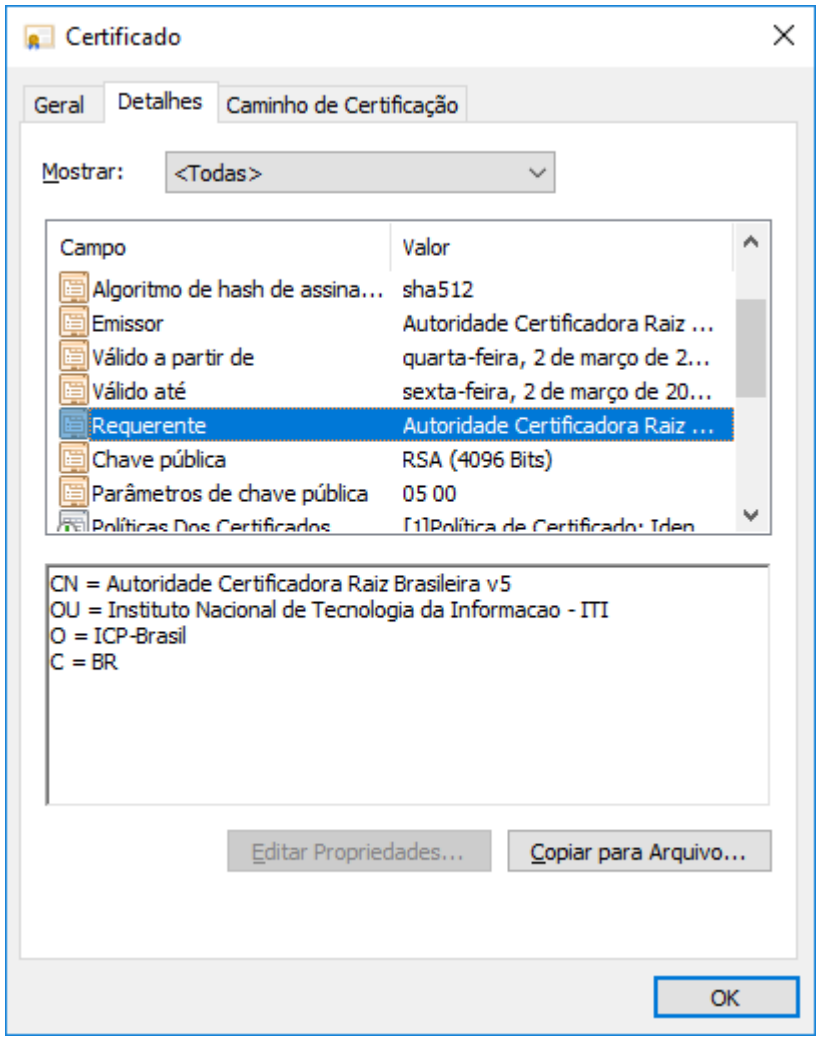
Requisitos para Reconhecimento Mútuo de Certificados

- Procedimento robusto de identificação do titular
  - Identificação presencial
  - Coleta e batimento biométrico
  - Segregação em validação e verificação
- Hardware Criptográfico certificado
- Sistema de controle robusto
  - Webtrust, ETSI ou equivalente
- Requisitos criptográficos atuais

Estrutura da ICP-Brasil




Certificado
Geral
Detalhes
Caminho de Certificação
Informações sobre o Certificado
Este certificado destina-se ao(s) seguinte(s) fim(ns):
• 2.16.76.1.1.0
• Todas as políticas de aplicativo
* Veja a declaração da autoridade de certificação para obter d
Emitido para: Autoridade Certificadora Raiz Brasileira v5
Emitido por: Autoridade Certificadora Raiz Brasileira v5
Válido a partir de 02/03/2016 até 02/03/2029
Instalar Certificado...
Declaração do Emissor
OK


Certificado
Geral
Detalhes
Caminho de Certificação
Mostrar: <Todas>
Campo
Valor
Algoritmo de hash de assina...
sha512
Emissor
Autoridade Certificadora Raiz ...
Válido a partir de
quarta-feira, 2 de março de 2...
Válido até
sexta-feira, 2 de março de 20...
Requerente
Autoridade Certificadora Raiz ...
Chave pública
RSA (4096 Bits)
Parâmetros de chave pública
05 00
CN = Autoridade Certificadora Raiz Brasileira v5
OU = Instituto Nacional de Tecnologia da Informacao - ITI
O = ICP-Brasil
C = BR
Editar Propriedades...
Copiar para Arquivo...
OK

ICP-Brasil em números

Total aproximado de certificados ativos: 6,7 milhões (mar/2018)

Entidades	Qtde
Autoridade Certificadora de 1° Nível	16
Autoridade Certificadora de 2° Nível	81
Autoridade de Carimbo do Tempo	8
Autoridade de Registro	695
Instalação Técnica de AR	2254
Provedor de Serviço Biométrico	5
Provedor de Serviço Armazenamento	1

Padrão Brasileiro de Assinatura Digital

Padrão Brasileiro de Assinatura Digital

Assinaturas Digitais Baseadas em Políticas de Assinatura

- 5 (cinco) Tipos de Política no Perfil CAdES;
- 5 (cinco) Tipos de Política no Perfil XAdES; e
- 4 (quatro) Tipos de Política no Perfil PAdES.

Grato pela atenção

Wilson R Hirata

wilson.hirata@iti.gov.br