RETIFICADA EM 01/12/2009

RESOLUÇÃO Nº 53, DE 28 DE NOVEMBRO DE 2008

Altera os REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL

O SECRETÁRIO EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – CG ICP-BRASIL, no exercício do cargo de Coordenador do referido Comitê, no uso das atribuições legais previstas nos incisos I, V e VI do art. 4° da Medida Provisória n° 2.200-2, de 24 de agosto de 2001,

CONSIDERANDO o Decreto nº 6.605, de 14 de outubro de 2008, que dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CG ICP-Brasil e fixa a competência, prevista em seu § 6º art. 2º, do Secretário Executivo para coordená-lo na hipótese de ausência do Coordenador titular e seu suplente; e

CONSIDERANDO a necessidade de adequar os documentos da ICP-Brasil para incluir as referências a Carimbo do Tempo;

RESOLVE:

Art. 1º O Anexo da Resolução n° 41 do Comitê Gestor da ICP-Brasil, de 18 de abril de 2006, passa a vigorar com a seguinte redação:

§ 1º: no item 1.1.3: " São 10 (dez) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 6 (seis) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir:

a) Tipos de Certificados de Assinatura Digital:
   i. Tipo A1;
   ii. Tipo A2;
   iii. Tipo A3;
   iv. Tipo A4.
   v. Tipo T3;
   vi. Tipo T4;

b) Tipos de Certificados de Sigilo:
   i. Tipo S1;
   ii. Tipo S2;
   iii. Tipo S3;
   iv. Tipo S4."

§ 2º: na tabela constante do item 6.1.8:

Tipo de Certificado	*Processo de Geração de Chave Criptográfica*
A1 e S1	Software
A2 e S2	Software
A3, S3, T3	Hardware
A4, S4, T4	Hardware

§ 3º: no item 6.2.4.1: "Com exceção das chaves privadas vinculadas a certificados do tipo T3 e T4, que não podem possuir cópia de segurança, qualquer titular de certificado dos demais tipos poderá, a seu critério, manter cópia de segurança de sua própriachave privada."

§ 4º: na tabela constante do item 6.3.2.3:

Tipo de Certificado	*Período Máximo de Validade do Certificado (em anos)*
A1 e S1	1
A2 e S2	2

A3, S3, T3	3
A4, S4, T4	3

§ 5º: no subitem 7.1.2.4.a: “O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;”

Art. 2º O Anexo da Resolução n° 41 do Comitê Gestor da ICP-Brasil, de 18 de abril de 2006, passa a vigorar acrescido dos seguintes itens e subitens:

“1.1.6 Certificados do tipo T3 e T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.”

“1.3.5.6 Certificados de tipos T3 e T4 serão utilizados em aplicações mantidas por autoridades de carimbo do tempo credenciadas na ICP-Brasil, para assinatura de carimbos do tempo.”

“7.1.2.2.e Extended Key Usage, crítica: deve conter somente sub-campo KeyPurposeID contendo o valor id-kp-timeStamping com OID 1.3.6.1.5.5.7.3.8, nos certificados de carimbo do tempo de ACT credenciada na ICP-Brasil.”

“7.1.4.2 O certificado digital emitido para o equipamentos de carimbo do tempo de Autoridade de Carimbo do Tempo credenciada na ICP-Brasil deverá adotar o “*Distinguished Name”*(DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR
O = ICP-Brasil
OU = < nome da Autoridade de Carimbo do Tempo >
CN = < nome do Servidor de Carimbo do Tempo (incluindo o serial do SCT) >

NOTA: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.”

Parágrafo único: O item 1.1.6 anteriormente existente fica renumerado para 1.1.7.

Art. 3º As seguintes tabelas constantes do Anexo da Resolução n° 41 do Comitê Gestor da ICP-Brasil, de 18 de abril de 2006, passam a vigorar acrescidas das linhas:

§ 1º: Tabela 1 - OID de PC na ICP-Brasil

T3	2.16.76.1.2.303.*n*
T4	2.16.76.1.2.304.*n*

§ 2º: Tabela 2 - Mídias Armazenadoras de Chaves Criptográficas

T3 e T4	Hardware criptográfico aprovado pelo CG da ICP-Brasil

§ 3º: Tabela Comparativa de Requisitos Mínimos por Tipo de Certificado, constante no anexo I do DOC-ICP-04:

T3	1024	Hardware	*Hardware* criptográfico aprovado pelo CG da ICP-Brasil	3	6	12
T4	2048	Hardware	*Hardware* criptográfico aprovado pelo CG da ICP-Brasil	3	6	12

Art. 4º Fica aprovada a versão 3.0 dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04), que incorpora as alterações dos artigos anteriores.

Parágrafo único: O documento citado no caput deste artigo encontra-se publicado no sítio www.iti.gov.br.

Art. 5º As Autoridades Certificadoras credenciadas ou em processo de credenciamento que desejam emitir certificados do tipo T3 ou T4 devem solicitar o credenciamento das respectivas Políticas de Certificados e adequar seus procedimentos operacionais às alterações procedidas por esta Resolução.

Art 6º As Autoridades Certificadoras credenciadas ou em processo de credenciamento que não desejam emitir certificados do tipo T3 ou T4 não necessitam alterar as Políticas de Certificados já submetidas ao ITI, de imediato. A alteração desses documentos, para compatibilizar sua redação com o disposto nesta Resolução, poderá ser feita na medida da conveniência e da necessidade de cada AC.

Art. 7º Esta Resolução entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI

RETIFICADA EM 01/12/2009