RESOLUÇÃO Nº 99, DE 09 DE OUTUBRO DE 2013

AMPLIA PRAZO DE VALIDADE DE CERTIFICADOS DAS HIERARQUIAS DA ICP-BRASIL QUE IMPLEMENTAM EXCLUSIVAMENTE ALGORITMOS DE CURVAS ELÍPTICAS.

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, III, 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 Infraestrutura de Chaves Públicas Brasileira – CG ICP-Brasil e fixa a competência, prevista em seu § 6º, do art. 2º, do Secretário Executivo para coordená-lo na hipótese de ausência do Coordenador titular e seu suplente;

CONSIDERANDO as exigências sobre infraestrutura de chaves públicas feitas pela Organização de Aviação Civil Internacional (ICAO), órgão ligado à ONU que determina as especificações que devem ser obedecidas para os passaportes de seus países membros, contidas nos seguintes documentos: i) *Doc 9303*, *Machine Readable Travel Documents*, *Part 1*, *Machine Readable Passports*, *volume 2, sixth edition* e ii) *Machine Readable Travel Documents*, *Guidance Document*, *PKI for Machine Readable Travel Documents*, *version 1.0*;

CONSIDERANDO que o Brasil é atualmente um dos poucos países que possui passaporte eletrônico, mas não participa do programa PKD, porém, faz gestões para adesão ao referido diretório da ICAO; e

CONSIDERANDO o fortalecimento e robustez das chaves criptográficas de curvas elítpticas implementadas no âmbito da ICP-Brasil, com a recente atualização dos padrões e algoritmos criptográficos;

RESOLVE:

Art. 1º Altera-se o item 7.1 do DOC-ICP-01, versão 4.2, que passa a vigorar com a seguinte redação:

> O formato de todos os certificados emitidos pela AC Raiz está em conformidade com o padrão ITU X.509 ou ISO/IEC 9594. O certificado da AC Raiz é o único certificado auto-assinado da ICP-Brasil, com validade máxima de 20 (vinte) anos quando da utilização de criptografia de Curvas Elípticas, ou 13 (treze) anos para os demais casos, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

Art. 2º Altera-se o item 6.3.2.4 do DOC-ICP-05, versão 3.6, que passa a vigorar com a seguinte redação:

A validade admitida para certificados de AC é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

Art. 3º Alteram-se a Tabela 6 do item 6.3.2.3 e a Tabela do Anexo I, ambas do DOC-ICP-04, versão 5.1, que passam a vigorar com os seguintes conteúdos:

Tabela 6-Períodos de Validade dos Certificados:

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

ANEXO I-Tabela Comparativa de Requisitos Mínimos por Tipo de Certificado:

Tipo de Certificado	*Chave Criptográfica*			*Validade máxima do certificado (anos)*	*Freqüência de emissão de LCR (horas)*	*Tempo limite para revogação (horas)*
	Tamanho (bits)	*Processo de Geração*	*Mídia Armazenadora*			
A1 e S1	**RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256**	**Software**	**Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma do item 6.1.1**	**1**	**6**	**12**
A2 e S2	**RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256**	**Software**	**Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica**	**2**	**6**	**12**
A3 e S3	**RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256**	**Hardware**	**Cartão Inteligente ou *Token*, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou *hardware* criptográfico homologado junto à ICP-Brasil**	**5**	**6**	**12**

Tipo de Certificado	*Chave Criptográfica*			*Validade máxima do certificado (anos)*	*Freqüência de emissão de LCR (horas)*	*Tempo limite para revogação (horas)*
	Tamanho (bits)	*Processo de Geração*	*Mídia Armazenadora*			
T3	**RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256**	**Hardware**	***Hardware* criptográfico homologado junto à ICP-Brasil**	**5**	**6**	**12**
A4 e S4	**RSA 2048 (V0 e V1), 4096 (V2)**	**Hardware**	***Hardware* criptográfico homologado junto à ICP-Brasil**	**6**	**6**	**12**
	ECDSA 512	**Hardware**	***Hardware* criptográfico homologado junto à ICP-Brasil**	**11**	**6**	**12**
T4	**RSA 2048 (V0 e V1), 4096 (V2)**	**Hardware**	***Hardware* criptográfico homologado junto à ICP-Brasil**	**6**	**6**	**12**
	ECDSA 512	**Hardware**	***Hardware* criptográfico homologado junto à ICP-Brasil**	**11**	**6**	**12**

Art. 4º Ficam aprovadas as versões: 4.3 do Documento DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL (DOC-ICP-01); 5.2 do Documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04); e 3.7 do Documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO NA ICP-BRASIL (DOC-ICP-05).

§ 1º Todas as demais cláusulas dos documentos DOC-ICP-01, DOC-ICP-04 e DOC-ICP-05, em suas versões 4.2, 5.1 e 3.6, respectivamente, em suas ordens originárias, integram as presentes versões e mantêm-se válidas.

§ 2º Os documentos referidos no caput encontram-se disponibilizados, em sua totalidade, no sítio http://www.iti.gov.br.

Art. 5º Esta Resolução entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI