REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 41.

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 11, DE 14 DE FEVEREIRO DE 2002.

Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, a declaração de práticas de certificação da AC Raiz da ICP-Brasil, delega atribuições para a AC Raiz e dá outras providências.

O **SECRETÁRIO-EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL** faz saber que aquele Comitê, no uso das atribuições previstas nos incisos I e II e no parágrafo único do art. 4º da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001,

RESOLVE:

Art. 1º Os REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL, aprovados pela Resolução Nº 7, de 12 de dezembro de 2001, passam a vigorar com as seguintes alterações:

"1.3.4. Aplicabilidade (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

Neste item devem ser relacionadas as aplicações para as quais são adequados os certificados definidos pela PC e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

Aplicações voltadas para atendimento ao público em geral, assim considerados, dentre outros, os consumidores, os contribuintes, os cidadãos, os beneficiários do sistema de saúde, do FGTS, da seguridade social, que aceitarem certificados de um determinado tipo previsto pela ICP-Brasil, devem aceitar todo e qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitidos por qualquer AC integrante da ICP-Brasil.

Na definição das aplicações para o certificado definido pela PC, a AC responsável deve levar em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, freqüência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado, apresentados na tabela constante do Anexo I.

Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade na *We*b, correio eletrônico, transações *on-lin*e, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo."

"7.1.2. Extensões de certificado (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 35, DE 21 DE OUTUBRO DE 2004)

Neste item, a PC deve descrever todas as extensões de certificado utilizadas e sua criticalidade.

A ICP-Brasil define como obrigatórias as seguintes extensões:

– ***"Authority Key Identifier"*, não crítica**: o campo keyIdentifier deve conter o *hash* SHA-1 da chave pública da AC;

– "***Key Usage"*, crítica**: em certificados de assinatura digital, somente os bits digitalSignature , nonRepudiation e keyEncipherment podem estar ativados; em certificados de sigilo, somente os bits keyEncipherment e dataEncipherment podem estar ativados;

– ***"Certificate Policies", não crítica***: deve conter o OID da PC correspondente e o endereço *Web* da DPC da AC que emite o certificado;

– *"**CRL Distribution Points", não crítica***: deve conter o endereço na *Web* onde se obtém a LCR correspondente;

A ICP-Brasil também define como obrigatória a extensão *"Subject Alternative Name*", não crítica e com os seguintes formatos:

Para certificado de pessoa física, um único campo otherName, contendo:

– **OID = 2.16.76.1.3.1 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato *ddmmaaaa*; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subseqüentes, o número de inscrição do titular no PIS/PASEP; nas 11 (onze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação.

Para certificado de pessoa jurídica, 3 (três) campos otherName, contendo, nesta ordem:

– **OID = 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato *ddmmaaaa*; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subseqüentes, o número de inscrição do responsável no PIS/PASEP; nas 11 (onze) posições subseqüentes, o número do Registro Geral (RG) do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;

– **OID = 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;

– **OID = 2.16.76.1.3.3 e conteúdo** = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

Quando o número de CPF, PIS/PASEP, RG ou CNPJ não estiver disponível, o campo correspondente deve ser integralmente preenchido com caracteres "zero".

Campos otherName adicionais, contendo informações específicas definidas pela AC, poderão ser utilizados com OID atribuídos pelo CG da ICP-Brasil.

Os outros campos que compõem a extensão *"Subject Alternative Name*" poderão ser utilizados, na forma e com os propósitos definidos na RFC 2459."

Art. 2º O item 1.4. da DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AC RAIZ DA ICP-BRASIL, aprovada pela Resolução Nº 1, de 25 de setembro de 2001, passa a vigorar com a seguinte redação:

"1.4. Dados de Contato (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

Nome: Instituto Nacional de Tecnologia da Informação - ITI
Endereço: Palácio do Planalto, Anexo II - S, Sala 220
Telefone: (550xx61) 4112082
Fax: 2265636
Página *Web*: http://www.iti.gov.br
E-mail: acraiz@iti.gov.br"

Art. 3º No âmbito da Reestruturação do Sistema de Pagamentos Brasileiro, para os fins do art. 2º da Circular nº 3.060, do Banco Central do Brasil, de 20 de setembro de 2001, o bit *dataEncipherment* poderá estar ativado também em certificados de assinatura digital, na extensão "*Key Usage*", definida no item 7.1.2. dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL, aprovados pela Resolução Nº 7, de 11 de dezembro de 2001, desde que os dados a serem cifrados correspondam, necessariamente, a valores iniciais ou a vetores de inicialização, utilizados nos modos de implementação CBC (C*ipher Block Chaining*) ou CFB (C*ipher-Feedback Mode*).

Parágrafo único. Os certificados a que se refere o caput expirarão, no máximo, em 15 de novembro de 2002.

Art. 4º Ficam delegadas à Autoridade Certificadora Raiz - AC Raiz as seguintes atribuições:

I - aprovar políticas de certificados, práticas de certificação e regras operacionais das AC;

II - credenciar e autorizar o funcionamento das AC, das AR, e de seus prestadores de serviços de suporte, bem como autorizar a emissão do correspondente certificado; e

III - as tarefas atribuídas ao Comitê Gestor da ICP-Brasil e à sua Secretaria-Executiva nos CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL, aprovados pela Resolução Nº 6, de 22 de novembro de 2001.

Parágrafo único. Fica, a título de recomendação, a cargo da AC Raiz dar início às atividades de identificação e avaliação das políticas de ICP externas, bem como de negociação de acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, observado o disposto em tratados, acordos ou atos internacionais.

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

MURILO MARQUES BARBOZA

REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 41.