

REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 41.

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 35 DE 21 DE OUTUBRO DE 2004.

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 - ICP-BRASIL faz saber que aquele Comitê, no uso das atribuições previstas nos incisos I e V 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 DA ICP-BRASIL, aprovados pela Resolução Nº 7, de 12 de dezembro de 2001, passam a vigorar com as seguintes alterações:

"7.1.2. Extensões de certificado

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, 3 (três) campos 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 Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;
- **OID = 2.16.76.1.3.6 e conteúdo** = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado;
- **OID = 2.16.76.1.3.5 e conteúdo** = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subseqüentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subseqüentes, o município e a UF do Título de Eleitor.

Para certificado de pessoa jurídica, 4 (quatro) 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 Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições

subseqüentes, o número do RG do responsável; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;

- **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;
- **OID = 2.16.76.1.3.7 e conteúdo** = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

Os campos otherName definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING;

- Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
- Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;
- Todas informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;
- As 6 (seis) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;
- Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

Campos otherName adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

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 As Autoridades Certificadoras - AC devidamente credenciadas deverão apresentar, no prazo máximo de 120 (cento e vinte) dias contados da publicação desta Resolução, alteração nas suas políticas de certificado, comprovando, sob pena de descredenciamento, a adequação de seus documentos às alterações procedidas por esta Resolução.

Parágrafo único. As AC em processo de credenciamento deverão apresentar imediatamente alteração nas políticas de certificado apresentadas, adequando-as às modificações procedidas por esta Resolução.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

ENYLSO FLAVIO MARTINEZ CAMOLESI

REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 41.