REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 42

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 13, DE 26 DE ABRIL DE 2002.

Altera a declaração de práticas de certificação da AC Raiz da ICP-Brasil, os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil, os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil, os requisitos mínimos para as políticas de certificado na ICP-Brasil, 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, II, III e V do art. 4º da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001,

RESOLVE:

Art.1º A 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 as seguintes alterações:

"2.1.4. Direitos da terceira parte *(Relying Party*)

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

Constituem direitos da terceira parte:

– recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
–
– verificar, a qualquer tempo, a validade do certificado. O certificado da AC Raiz ou um certificado de AC de nível imediatamente subseqüente ao da AC Raiz é considerado válido quando:
–
– tiver sido emitido pela AC Raiz;
–
– não constar da LCR da AC Raiz;
–
– não estiver expirado; e
–
– puder ser verificado com o uso do certificado válido da AC Raiz."

"2.7.2. Identidade e qualificação do auditor

A auditoria será realizada por corpo próprio devidamente qualificado e vinculado à AC Raiz."

"4.1. Solicitação de Certificado

A solicitação de certificado para uma AC de nível imediatamente subseqüente ao da AC Raiz só é possível após o deferimento de seu pedido de credenciamento e a conseqüente autorização de funcionamento da AC em questão por parte da AC Raiz (Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil).

A AC deve encaminhar a solicitação de seu certificado à AC Raiz por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10."

"4.2. Emissão de Certificado (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 37, DE 21 DE OUTUBRO DE 2004)

A emissão de um certificado pela AC Raiz é feita em cerimônia específica, com a presença dos representantes da AC Raiz, da AC credenciada, de auditores e convidados, na qual são registrados todos os procedimentos executados.

A AC Raiz garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subseqüente ao seu ocorre em, no máximo, 20 (vinte) dias úteis após a autorização de funcionamento da AC em questão.

O certificado é considerado válido a partir do momento em que é emitido.

A AC Raiz entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC credenciada.

A emissão dos certificados da AC Raiz e das AC de nível imediatamente subseqüente é feita em equipamentos da AC Raiz que operam *off-lin*e."

"4.4.9.

A LCR da AC Raiz é atualizada a cada 28 (vinte e oito) dias. Em caso de revogação de certificado de AC de nível imediatamente ao seu, a AC Raiz emite nova LCR no prazo previsto no item 4.4.3 e notifica todas as AC de nível imediatamente subseqüente ao seu."

"6.1.1. Geração do par de chaves

O par de chaves criptográficas da AC Raiz é gerado pela própria AC Raiz, em *hardware* específico, conforme o detalhado em 6.1.8.

O par de chaves criptográficas de uma AC de nível imediatamente subseqüente ao da AC Raiz é gerado pela própria AC, após o deferimento do seu pedido de credenciamento e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil."

"7.2.5. Restrições de nome

O nome da AC titular do certificado deve ser submetido à aprovação no processo de credenciamento. Não são admitidos caracteres especiais ou de acentuação nos campos do DN."

Art. 2º Os CRITÉRIOS E PROCEDIMENTOS DE CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL, aprovados pela Resolução Nº 6, de 22 de novembro de 2001, passam a vigorar com as seguintes alterações:

"2.2. Procedimentos

O processo de credenciamento obedece a procedimentos específicos, relacionados com a natureza da atividade a ser desenvolvida no âmbito da ICP-Brasil.

Todas as comunicações e requerimentos à AC Raiz deverão ser encaminhados por intermédio da cadeia de AC, ou candidatos à AC, operacionalmente vinculados. Inicia-se a tramitação pela AC, ou candidato à AC, de nível imediatamente superior ao do interessado. A tramitação prossegue, a partir daí, respeitando a hierarquia de AC, ou candidatos à AC, operacionalmente vinculados, até chegar à AC Raiz.

As AC serão responsáveis por comunicar as decisões do CG da ICP-Brasil ou da AC Raiz às entidades que lhes estejam operacionalmente vinculadas, respeitando a hierarquia de AC.

O deferimento do pedido de credenciamento será publicado no Diário Oficial da União e importará a autorização para funcionamento no âmbito da ICP-Brasil e, no caso de AC, a emissão do seu certificado."

"2.2.2.1. Solicitação

As solicitações dos candidatos ao credenciamento como AR na ICP-Brasil serão encaminhadas à AC ou candidato a AC a que o candidato a AR esteja operacionalmente vinculado, por intermédio do formulário constante do Anexo II. A AC ou candidato a AC que receber a solicitação deverá manter cópia sob sua guarda e encaminhar para a AC Raiz os seguintes documentos:

a) Formulário constante do Anexo II, devidamente preenchido e assinado pelos representantes legais do candidato a AR e da AC ou do candidato a AC a que esteja operacionalmente vinculado;

b) Documentos relacionados no Anexo V, apenas na hipótese de o candidato não ser a própria AC ou

candidato a AC;

c) Relatório de auditoria elaborado por empresas independentes especializadas, constantes de lista a ser disponibilizada pela AC Raiz, na hipótese do item 2.1.2, *c*, segunda parte."

Art. 3º Os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL, aprovados pela Resolução nº 8, de 12 de dezembro de 2001, passam a vigorar com a seguinte redação:

"4.1. Solicitação de Certificado (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item da DPC, devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC responsável e pelas AR a ela vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos deverão compreender, no mínimo:

- a comprovação de atributos de identificação constantes do certificado;
-
- um contrato assinado, que estabeleça termos e condições aplicados ao uso do certificado.
-

A DPC deve observar, quando aplicável, que a solicitação de certificado para AC de nível imediatamente subseqüente ao da AC responsável somente será possível após o deferimento do pedido de credenciamento e a respectiva autorização de funcionamento da AC em questão (Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil).

Nesse caso, aquela AC deverá encaminhar a solicitação de seu certificado à AC emitente por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10."

"6.1.1. Geração do par de chaves

Neste item, a DPC deve descrever os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas da AC responsável. O par de chaves criptográficas da AC responsável pela DPC deverá ser gerado pela própria AC, após o deferimento do seu pedido de credenciamento e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil.

A DPC deve descrever também os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas de entidade solicitante de certificado. Pares de chaves deverão ser gerados somente pelo titular do certificado correspondente. Os procedimentos específicos devem ser descritos em cada PC implementada.

Cada PC implementada pela AC responsável deve definir o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos pelo documento Requisitos Mínimos para Políticas de Certificado na ICP-Brasil."

"8.3. Procedimentos de aprovação

Toda DPC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável, conforme o determinado pelo documento Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil."

Art. 4º 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 a seguinte redação:

"4.1. Solicitação de Certificado (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item da PC, devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC responsável para as solicitações de emissão de certificado. Esses requisitos e procedimentos, que deverão ser atendidos e executados pelas AR vinculadas e pelos solicitantes, deverão compreender, no mínimo:

- a comprovação de atributos de identificação constantes do certificado, conforme item 3.1;
-
- um contrato assinado pelo solicitante, que estabeleça termos e condições aplicados ao uso do

certificado.

A PC deve observar que a solicitação de certificado para AC de nível imediatamente subseqüente ao da AC responsável somente será possível após o deferimento do seu pedido de credenciamento e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil (Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil). Nesse caso, aquela AC deverá encaminhar a solicitação de seu certificado à AC emitente por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10."

"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 S*HA-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, 2 (dois) 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 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 UF.
- **OID = 2.16.76.1.3.5 e conteúdo** = nas primeiras 11 (onze) 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 posições subseqüentes, o município e a UF do Título de Eleitor.

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 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.

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, PIS/PASEP, RG, CNPJ 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 definidas pela AC, poderão ser utilizados com OID atribuídos 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.”

“8.3. Procedimentos de aprovação

Toda PC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável, conforme o estabelecido no documento Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil. Como parte desse processo, além da conformidade com este documento, deverá ser verificada a compatibilidade entre a PC e a DPC da AC responsável.”

Art. 5º As Autoridades Certificadoras - AC devidamente credenciadas deverão apresentar, no prazo máximo de trinta dias contados da publicação desta Resolução, alteração na sua declaração de práticas de certificação e 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 na declaração de práticas de certificação e nas políticas de certificado apresentadas, adequando-as às modificações procedidas por esta Resolução.
Art. 6º Esta Resolução entra em vigor na data de sua publicação.

MURILO MARQUES BARBOZA

REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 42