REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 38

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 4, DE 22 DE NOVEMBRO DE 2001.

Altera a Declaração de Práticas de Certificação da AC Raiz da 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, III, V e VI do art. 4º da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001,

RESOLVE:

Art. 1º Os itens 2.7.1, 3.1.7, 4.4.9, 4.5.5, 4.6.1, 4.6.5, 4.8.2, 5.2.1, 6.1.4, 6.2.6, 7.1.2, 7.2.6, 7.3.2 da Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil, aprovada pela Resolução nº 1 do Comitê Gestor da ICP-Brasil em 25 de setembro de 2001, passam a vigorar com a seguinte redação:

"2.7.1. Freqüência de auditoria de conformidade de AC

As AC integrantes da ICP-Brasil sofrem auditoria:

- previamente ao seu credenciamento na ICP-Brasil; e
-
- a qualquer tempo, sem aviso prévio.
-

Adicionalmente, as AC de nível imediatamente subseqüente ao da AC Raiz sofrem auditoria anualmente, para fins de continuidade do credenciamento."

"3.1.7. Método para comprovar a posse de chave privada

A AC Raiz verifica se a AC credenciada possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. A RFC 2510 é utilizada como referência para essa finalidade."

"4.4.3. Procedimento para solicitação de revogação

A solicitação de revogação do certificado à AC Raiz deve ser efetivada pelo preenchimento do formulário Solicitação de Revogação de Certificado de AC. Esse formulário deverá ser assinado por seu representante legal. Quando utilizada a versão eletrônica do formulário, ele deve ser assinado digitalmente e enviado à AC Raiz. O formulário pode também ser preenchido em papel, entregue pessoalmente pelo representante à AC Raiz e assinado no ato da entrega.

O processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento pela AC Raiz da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada pela AC Raiz. Concluído esse processo, a AC Raiz informa ao CG da ICP-Brasil e à AC afetada a revogação do certificado.

O prazo para a revogação de certificado de AC de nível imediatamente subseqüente ao da AC Raiz conta-se, inclusive nos casos de solicitação da AC titular do certificado, da determinação da AC Raiz ou do CG da ICP-Brasil e deve ser realizada em até 2 (duas) horas.

Um certificado de AC revogado somente pode ser usado para a verificação de assinaturas geradas durante o período em que o referido certificado esteve válido."

"4.4.9. Freqüência de emissão de LCR (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 13, DE 26 DE ABRIL DE 2002)

A LCR da AC Raiz é atualizada, no máximo, a cada 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente subseqüente 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."

“4.5.5. Procedimentos para cópia de segurança (*backup*) de registro de auditoria

Os registros de eventos e sumários de auditoria do equipamento *off-line* utilizado pela AC Raiz têm cópias de segurança mensais ou sempre que houver alguma utilização desse equipamento.”

“4.6.1. Tipos de registros arquivados

Informações de auditoria detalhadas no item 4.5.1 e os processos de credenciamento de AC de nível imediatamente subseqüente ao da AC Raiz.”

“4.6.5. Requisitos para datação (*time-stamping*) de registros

Informações de data e hora nos registros baseiam-se no horário *Greenwich Mean Time* (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos é zero.”

“4.8.2. Revogação de certificado da entidade

Procedimentos descritos no Plano de Continuidade do Negócio da AC Raiz.”

“5.2.1. Perfis qualificados

A AC Raiz garante a separação das tarefas para funções críticas, com o intuito de evitar que um empregado de má fé utilize o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

A AC Raiz estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. A divisão de responsabilidades entre os três perfis é a seguinte:

Gerente de Configurações:

- configuração e manutenção do *hardware* e do *software* da AC Raiz;
-
- início e término dos serviços da AC Raiz;

Gerente de Segurança:

- gerenciamento dos operadores da AC Raiz;
-
- implementação das políticas de segurança da AC Raiz;
-
- verificação dos registros de auditoria;
-
- verificação do cumprimento desta DPC;

Administrador do Sistema:

- gerenciamento dos processos de iniciação dos usuários internos à AC Raiz;
-
- emissão, expedição, distribuição, revogação e gerenciamento de certificados;
-
- distribuição de cartões (*tokens*), quando for o caso.

Somente os empregados responsáveis por tarefas descritas para o Gerente de Configurações e o Administrador do Sistema têm acesso ao *software* e ao *hardware* do sistema de certificação da AC Raiz.”

“6.1.4 Disponibilização de chave pública da AC Raiz para usuário

A entrega do certificado da AC Raiz para as AC de nível imediatamente subseqüente ao seu é feita no momento da disponibilização do certificado da AC, utilizando-se para isto o formato padrão PKCS#7, que inclui toda a cadeia de certificação.

A disponibilização do certificado da AC Raiz para os demais usuários da ICP-Brasil é realizada por uma

das seguintes formas:

- formato PKCS#7, na disponibilização do certificado para seu titular;
- diretório;
- página *Web* da AC Raiz ou das AC integrantes da ICP-Brasil;
- por outros meios seguros definidos pelo CG da ICP-Brasil."

"6.2.6. Inserção de chave privada em módulo criptográfico

A chave privada da AC Raiz é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510."

"7.1.2. Extensões de certificado

O certificado da AC Raiz implementa as seguintes extensões previstas na versão 3 do padrão ITU X.509:

- **basicConstraints**: contém o campo *cA=True*. O campo *pathLenConstraint* não é utilizado.
- **keyUsage**: contém apenas os bits *keyCertSign* e *cRLSign* ligados. Os demais bits estão desligados.
- **cRLDistributionPoints**: contém o endereço na *Web* onde se obtém a LCR emitida pela AC Raiz (http://acraiz.icpbrasil.gov.br/LCRacraiz.crl).
- **Certificate Policies**: especifica o *Object Identifier* (OID) da DPC da AC Raiz e o atributo *id-qt-cps* com o endereço na *Web* dessa DPC (http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf).
- **SubjectKeyIdentifier**: contém o *hash* SHA-1 da chave pública da AC Raiz."

"7.2.6 OID (*Object Identifier*) da DPC

A AC de nível imediatamente subseqüente ao da AC Raiz deve informar neste item o OID fornecido para sua DPC pela AC Raiz."

"7.3.2 Extensões de LCR e de suas entradas

A LCR emitida pela AC Raiz implementa as seguintes extensões previstas na RFC 2459:

- **AuthorityKeyIdentifier**: contém o mesmo valor do campo "Subject Key Identifier" do certificado da AC Raiz.
- **cRLNumber**: contém um número seqüencial para cada LCR emitida."

Art. 2º Esta resolução entra em vigor na data da sua publicação.

MURILO MARQUES BARBOZA

REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 38