Presidência da República
Casa Civil da Presidência da República

PARTE II-1
DECLARAÇÃO DE REGRAS OPERACIONAIS
DA AC-Raiz INTEGRANTE DA ICP-Brasil

1 Introdução

1.1 Informações Iniciais

1.1.1 Abrangência

A abrangência deste documento está direcionada às políticas, às práticas e aos procedimentos a serem empregados pela Autoridade Certificadora Raiz (AC Raiz) da Infra-estrutura de Chave Pública Brasileira (ICP-Brasil) na execução dos seus serviços. Este documento não preconiza e nem define os termos e as condições em que serão utilizados os certificados.

1.2 Serviços da AC Raiz

1.2.1 Localização dos Serviços

Os serviços da AC Raiz serão realizados em instalações homologadas pelo Comitê Gestor da ICP-Brasil.

1.2.2 Serviços Oferecidos pela AC Raiz

- Geração de chaves;
- Geração de certificados;
- Assinatura de certificados;
- Emissão de certificados;
- Publicação de certificados;
- Verificação do prazo de validade do certificado;
- Revogação de certificados;
- Gerenciamento da Lista de Certificados Revogados (LCR); e
- Fiscalização e auditoria das AC e AR e de outros prestadores de serviços a critério do CG da ICP-Brasil.

1.3 Identidade da AC Raiz

Nome: _____
Endereço: _____
Telefone:_____
Fax:_____
E-mail:_____

1.4 Certificado da AC Raiz

O certificado da AC Raiz é o certificado de nível mais alto na ICP-Brasil. Este certificado contém um par de chaves pública e privada, e é utilizado para assinar todas os certificados das AC diretamente subordinadas a AC Raiz e publicar todas as LCR respectivas. A publicação dos certificados e LCR podem ser feitos em serviço de Diretório ou em página Web da AC Raiz.

1.4.1 Detalhes Básicos do Certificado

Detalhes de identificação:

C = BR
O = ICP-Brasil
OU = Autoridade Certificadora Raiz
OU = Instituto Nacional de Tecnologia da Informação – ITI
SP = São Paulo
L = Campinas
CN = Autoridade Certificadora Raiz Brasileira

Comprimento da chave - o comprimento da chave pública será de, no mínimo 2048 bits.

Auto assinatura - o certificado da AC Raiz é o único certificado da ICP-Brasil que pode ser auto assinado.

Algoritmo de assinatura - o certificado da AC Raiz utilizará RSA com SHA-1 como algoritmo de assinatura.

Validade do Certificado – o certificado da AC Raiz não deverá ter validade superior a 10 (dez) anos nem inferior a 08 (oito) anos.

2 Solicitação de um certificado

2.1 Processo de Solicitação do Certificado

A solicitação de certificado para AC integrante da ICP-Brasil deve ser encaminhada ao CG da ICP-Brasil, revestida das formalidades legais estabelecidas pelo mesmo.

2.2 Convenção de nomes

Os nomes seguem o padrão ISO/IEC 9594 (X.500) Distinguished Name (DN).

2.2.1 Componentes do campo “Distinguished Name” do certificado de AC

O campo “Distinguished Name” , Nome Distinto, contém os seguinte componentes:

Country (c=) BR
Organisation (o=) nome do órgão ou entidade
Common Name (cn=) nome do órgão ou entidade

3 Emissão e Publicação de Certificados

3.1 Processo de Geração de Chaves e Certificados

O par de chaves criptográficas será gerado pela própria AC a ser licenciada, que encaminhará, através de pessoa legalmente credenciada, à AC Raiz a cópia de sua chave pública, em formato PKCS#10, observadas as disposições legais anteriormente mencionadas.

3.2 Publicação de Certificados

Os certificados serão publicados no Diário Oficial da União, em serviço de diretório ou página Web da AC Raiz, obedecendo as regras e critérios estabelecidos na PC da ICP-Brasil.

4 Informação de Chaves e de Certificados

4.1 Emissão de certificados

4.1.1 Componente Seguro de Hardware

A AC Raiz deverá usar um componente seguro de hardware à prova de violação para a geração de chaves e de certificados e para a assinatura de certificados. O mecanismo de detecção de violação deverá ser automático. Qualquer tentativa de violação do componente deverá resultar na destruição dos dados sensíveis armazenados no interior do componente. O componente seguro de hardware deverá incorporar operação por bateria para evitar a perda de dados caso haja falta de alimentação elétrica.

4.1.2 Acesso por meio de dispositivo criptográfico

O acesso ao componente seguro de hardware deverá ser controlado por meio de dispositivo criptográfico. O componente seguro de hardware irá se comunicar diretamente com o leitor do dispositivo para habilitar:

- a emissão de certificados;
- a controle de acesso; e
- as operações de autenticação de usuário.

4.1.3 Operação Off-line

A AC Raiz tem uma política de operar off-line os equipamentos responsáveis pela geração de chaves e de certificados para garantir que estes equipamentos serão acessados internamente e para proteger contra acesso não autorizado via redes remotas.

4.1.4 Algoritmo de Assinatura

A AC Raiz usa os seguintes algoritmos para a assinatura de certificados:

Sha-1WithRSAEncryption (Identificação do algoritmo: 1.2.840.113549.1.1.5)

4.1.5 Blocos de Assinatura PKCS#1

Os certificados assinados pela AC Raiz usando os algoritmos de assinatura listados acima devem atender ao padrão PKCS#1 de blocos de assinatura.

4.1.6 Assinatura de Certificados

Os certificados gerados pela AC Raiz são assinados pela chave privada da AC Raiz. A chave pública correspondente está disponível no certificado auto-assinado da AC Raiz.

4.1.7 Recuperação de Chaves

Não se aplica pois não faz parte da política da AC Raiz manter cópias das chaves privadas das AC licenciadas.

4.2 Formato de Certificados

4.2.1 Formato

O formato de todos os certificados emitidos pela AC Raiz deve estar em conformidade com o padrão ISO/IEC 9594 X.509 versão 3.

4.2.2 Extensões de Certificados da AC Raiz

Os certificados da AC suportam todas as extensões previstas na versão 3 do padrão X.509.

4.3 Certificado Válido

4.3.1 Definição

A AC Raiz define um certificado de AC válido como um certificado que:
- Foi emitido para AC licenciada, e
- Foi publicado no Diário Oficial da União, e
- Não está na LCR da AC Raiz, e
- Não expirou e
- Pode ser verificado por um certificado válido da AC Raiz.

5 Revogação de Certificados

5.1 Políticas de Revogação de Certificados

5.1.1 Circunstâncias para requisição de Revogação de Certificados

Um certificado de AC pode ser revogado a qualquer instante, por solicitação da AC titular do certificado ou por decisão da AC Raiz.

Um certificado deve obrigatoriamente ser revogado:
- quando for alterada qualquer informação constante no mesmo;
- no caso de dissolução da AC titular do certificado; ou
- no caso de confirmação de comprometimento da chave privada ou da sua mídia armazenadora.

A AC-Raiz da ICP-Brasil deverá revogar o certificado ou a certificação cruzada, conforme o caso, da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

5.1.2 Quando um certificado se torna revogado

Um certificado se torna efetivamente revogado quando uma nova LCR, contendo o mesmo, é emitida e publicada pela AC Raiz no Diretório ou na página Web da ICP-Brasil.

5.1.3 Uso de certificados revogados

Um certificado revogado somente poderá ser usado para a verificação de dados ou mensagens que tenham sido criados, emitidos ou recebidos em data anterior à data de revogação do referido certificado.

5.2 Requisições de Revogação de Certificados

5.2.1 Quem pode solicitar Revogação de Certificados

A revogação de um certificado somente pode ser feita:

- por determinação da AC Raiz; ou
- por determinação judicial; ou
- por solicitação da AC titular do certificado ou da certificação cruzada.

5.2.2 Métodos de Requisição de Revogação de Certificados

O responsável da AC titular do certificado ou da certificação cruzada pode solicitar a sua revogação diretamente à AC Raiz por meio de mecanismos por ela disponibilizados.

5.3 Processo de Revogação de Certificados

5.3.1 Início, duração e término do processo de revogação de certificados

A revogação de um certificado tem início com o recebimento pela AC Raiz da determinação de revogação ou da solicitação de revogação, sendo aberto um processo para o mesmo. O término do processo ocorre quando o solicitante é informado da efetiva revogação do certificado.

Os prazos a serem cumpridos pela AC Raiz para a revogação de certificados, previstos pelo CG da ICP-Brasil, começam a contar a partir do instante do recebimento, pela AC Raiz, da solicitação enviada pela AC, e terminam no instante da publicação da LCR correspondente.

5.3.2 Descrição do processo

- a AC Raiz recebe a determinação ou solicitação de revogação;

- a AC Raiz autentica a solicitação;
- a AC Raiz revoga o certificado e publica nova LCR, cumprindo os prazos previstos pelo CG da ICP-Brasil; e
- a AC Raiz informa ao CG da ICP-Brasil e à AC afetada a revogação do certificado.

6 Expiração da Validade do Certificado

6.1 Notificação antes da expiração da validade do certificado

A AC Raiz deve notificar a AC licenciada até 3 meses antes da data de expiração.

6.2 Expiração da validade do certificado

6.2.1 Remoção do Diretório e página Web

A AC Raiz deve remover imediatamente do diretório e da página Web os certificados com a data de validade expirada, mantendo-os armazenados para efeito de consulta histórica.

6.2.2 Uso de um certificado com a data de validade expirada

Os certificados com validade expirada, somente devem ser utilizados nas visualizações:
- de mensagens históricas;
- da data de criação; e
- da data de recebimento.

6.2.3 Substituição de certificado

A AC Raiz substitui um certificado expirado de uma AC licenciada por um novo certificado mediante solicitação da AC.

7 Serviço de Certificados

7.1 Disponibilidade de Serviços

O Diretório e/ou a página Web da ICP-Brasil, que contém os certificados e as LCR, deverá estar disponível 24 horas por dia, sete dias por semana.

7.2 Acordos de Certificação Cruzada com Outras ICP

Somente a AC Raiz da ICP-Brasil, e quando autorizada pelo CG da ICP-Brasil, realizará acordos de certificação cruzada com ICP de outros países.

8 Segurança

8.1 Proteção da chave privada da AC Raiz

8.1.1 Hardware Criptográfico

- uso de hardware criptográfico para geração do par de chaves criptográficas da AC;
- mecanismo de detecção de violação;
- destruição das informações internas nas situações de violação;

8.1.2 Chaves Criptográficas

- uso de chaves para ativar o sistema de geração de chave criptográfica;
- as chaves criptográficas devem poder ser divididas e distribuídas entre várias pessoas credenciadas, evitando o controle total sob a responsabilidade de apenas uma pessoa;
- a chave privada da AC deve ser armazenada cifrada em dispositivo criptográfico;

8.2 Proteção dos sistemas e dados da AC

Os sistemas da AC devem ser protegidos contra o acesso físico e lógico não autorizado.

A geração das chaves e certificados da AC devem ser realizados em um ambiente off-line para impedir o acesso remoto não autorizado.

Os procedimentos de geração das chaves criptográficas e certificados da AC devem ser acompanhados por no mínimo 3 das 5 pessoas, devidamente credenciadas conforme a Política de Segurança da ICP-Brasil;

A integridade de todos os dados contidos no diretório ou página Web (certificados e LCR) devem ser protegidos por meio de assinatura digital utilizando a chave privada da AC.

As informações relativas às AC licenciadas devem ser mantidas num ambiente off-line e com acesso restrito.

8.3 Segurança física da AC

O acesso físico da AC deve ser gerenciado e controlado internamente conforme preconizado na Política de Segurança da ICP-Brasil. Chaves que permitam o acesso devem ser emitidas pelo gerente de segurança da AC. O acesso físico deve ser monitorado e o controle deve assegurar que apenas pessoas autorizadas participem das atividades de geração de chaves e de certificados

.