Infraestrutura de Chaves Públicas Brasileira

REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS DOS FORNECEDORES DE NAVEGADORES DE INTERNET

DOC ICP-01.02

Versão 1.0

15 de julho de 2016

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Norma que aprovou alteração	Item Alterado	Descrição da Alteração
IN 05/2016, de 15.07.2016. (versão 1.0)		Criação do Documento

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
DOC-ICP	Documentos Principais da ICP-Brasil
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
S/MIME	*Secure/Multipurpose Internet Mail Extensions*
OID	Identificador de Objeto (*Object Identifier*)
PC	Política de Certificado
SSL	*Secure Sockets Laye*
TLS	*Transport Layer Security*

1.VISÃO GERAL

1.1. Este documento estabelece requisitos adicionais a serem obrigatoriamente observados pelas Autoridades Certificadoras - AC integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) para ajuste e complementação em suas Políticas de Certificado (PC) e Declarações de Práticas de Certificação (DPC).

1.2. Estes requisitos adicionais têm o objetivo de adequação às recentes atualizações provenientes de organizações que atuam no fortalecimento da segurança em meios digitais e na internet, tais como CA/Browser Forum e WebTrust.

2. REQUISITOS ADICIONAIS DE AC

2.1. Os certificados de confirmação de identidade e assinatura do tipo A1 a A4 e T3 e T4 devem ser separados por AC emissora para cada tipo de uso, conforme descritos a seguir:

a) Autenticação de Servidor (SSL/TLS);
b) Assinatura Geral e Proteção de e-mail (S/MIME);
c) Assinatura de Código (Code Signing); e
d) Assinatura de Carimbo do Tempo (Time Stamping).

2.2. Isso significa que uma única AC emissora de certificado para usuário final com os propósitos acima descritos não deve ser usada para emitir, concomitantemente, certificados de Autenticação de Servidor, S/MIME, Assinatura de Código e Carimbo do Tempo. Uma cadeia de AC separada deve ser usada para cada caso de uso.

3. REQUISITOS DE EXTENSÕES DE CERTIFICADO

3.1. As extensões para os referidos tipos de certificados passam a ser obrigatórias obedecendo os propósitos de uso e a criticalidade conforme descrição abaixo:

a) Para certificados de Assinatura de Código:

"Key Usage", crítica: somente o bit *digitalSignature* deve estar ativado;
"Extended Key Usage", não crítica: somente o *codeSigning* OID = 1.3.6.1.5.5.7.3.3 deve estar presente;

b) Para certificados de Autenticação de Servidor:

"Extended Key Usage", não crítica: deve conter o propósito *server authentication* OID = 1.3.6.1.5.5.7.3.1. Pode conter o propósito *client authentication* OID = 1.3.6.1.5.5.7.3.2.

c) Para certificados de Assinatura de Carimbo do Tempo:

"Extended Key Usage", crítica: somente o propósito *time Stamping* OID =

1.3.6.1.5.5.7.3.8 deve estar presente;

d) Para certificados de Assinatura A CF-e-SAT:

"Extended Key Usage", não crítica: somente o propósito *server authentication* OID = 1.3.6.1.5.5.7.3.1 ou o propósito *client authentication* OID = 1.3.6.1.5.5.7.3.2 ou ambos devem estar presentes;

e) Para certificados de assinatura de resposta OCSP:

"Extended Key Usage", não crítica: somente o propósito *OCSP Signing* OID = 1.3.6.1.5.5.7.3.9 deve estar ativado.

f) Para os demais certificados de Assinatura e/ou Proteção de e-mail:

"Extended Key Usage", não crítica: no mínimo um dos propósitos *client authentication* OID = 1.3.6.1.5.5.7.3.2 ou *E-mail protection* OID = 1.3.6.1.5.5.7.3.4 deve estar ativado, podendo implementar outros propósitos instituídos, desde que verificáveis e previstos pelas AC, em suas PC.

3.2. As AC não devem utilizar na extensão Extended Key Usage o propósito *anyExtendedKeyUsage*, OID = 2.5.29.37.0.

4. REQUISITOS COMPLEMENTARES PARA CERTIFICADOS PARA ASSINATURA DE CÓDIGO

Segue a descrição dos requisitos complementares que devem ser cumpridos no âmbito da ICP-Brasil para emissão de certificados para Assinatura de Código. Esse tipo de certificado é utilizado para a verificação da identidade do fornecedor e da integridade do código assinado, garantindo que este não foi modificado.

4.1. Compromisso com as recomendações CA/B Forum

As AC que emitem Certificados para Assinatura de Código devem dar publicidade efetiva que seus requisitos estão aderentes à última versão dos requisitos recomendados pelo CA/B Forum [3]. Com esse objetivo, a AC deve incorporar esses requisitos em sua PC e DPC e incluir um link para a versão oficial desses requisitos.

As partes aplicáveis desses requisitos também devem ser incluídas, diretamente ou por referência, nos contratos com ACs subordinadas, ARs e Prestadores de Serviço que envolvam ou estejam relacionados com a emissão ou administração de Certificados, devendo a AC garantir o cumprimento de tais termos.

4.2. Perfil do Certificado

Os requisitos mínimos estabelecidos nos itens seguintes deverão ser obrigatoriamente atendidos nos certificados de Assinatura de Código emitidos dentro da ICP-Brasil. As informações sobre os padrões adotados, seus perfis, versões e extensões que não forem mencionados permanecem com

a mesma configuração descrita no item 7.1 do DOC-ICP-04 [1].

4.2.1 Formatos de Nome

O nome do titular do certificado, constante do campo "Subject", deverá adotar o"Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, como exemplo, da seguinte forma:

C = BR

O = ICP-Brasil

OU = nome da AC emitente

CN = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ); em um certificado de equipamento ou aplicação, o identificador CN deverá conter o URL correspondente ou o nome da aplicação

ST = estado da federação do titular do certificado

4.2.2. Período de Validade

O período máximo de validade dos Certificados de Assinatura de Código será de até 3 (três) anos.

4.3. Requisições de Certificados com Alto Risco

Adicionalmente aos procedimentos previstos na verificação antes da emissão do certificado, previstos no DOC-ICP-05.02 [2], a AC deve manter e verificar uma base de dados contendo informações sobre fornecedores, publicadores e distribuidores de software suspeito.

5. PERÍODO DE RETENÇÃO PARA ARQUIVO

Ficam estabelecidos para todas as AC da ICP-Brasil os períodos de retenção para cada registro arquivado, observando que:

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente;
b) Especificamente para a AC RAIZ, as cópias dos processos de credenciamento de AC, por no mínimo 30 (trinta) anos, a contar da data de expiração ou revogação do certificado;
c) As cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado; e
d) As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por, no mínimo, 7 (sete) anos.

6. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são aprovados por Resolução do Comitê-Gestor da ICP-Brasil e podem ser alterados, quando necessário, pelo mesmo dispositivo legal. O sítio http://www.iti.gov.br disponibiliza as versões atualizadas de todos os documentos e as Resoluções que os aprovaram.

Ref	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[2]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP	DOC-ICP-05.02

7. REFERÊNCIAS BIBLIOGRÁFICAS

[3] CA/Browser Forum, Baseline Requirements for the Issuance and Managemento of Publicly-Trusted Code Signing Certificate, versão 1.0, novembro de 2015.