AC DIGITAL
Autoridade Certificadora

Autoridade Certificadora

Digital

Política de Certificado T3

(PC T3 da AC Digital)

OID 2.16.76.1.2.303.10

Versão 1.0 de 1 de Setembro de 2014

Classificação: Ostensivo

www.acdigital.com.br

Sumário

Controle de Versão

Versão	Data	Descrição
1.0	01/09/2014	Versão inicial, a partir do DOC-ICP-04 versão 5.1.

Tabela de Siglas

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AGR	Agente de Registro
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CMM – SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoa Jurídica
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Instrusion Detection System
IEC	International Eletrotechnical Commission

SIGLA	DESCRIÇÃO
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecummunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institutute of Satandards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifer
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Pessession
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RIC	Registro de Identificação Civil
RFC	Request For Comments
RG	Registro Geral
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	Simpe Network Management Protocol
TCSEC	Trusted System Evaluation Criteria

SIGLA	DESCRIÇÃO
TSDM	Trusted Software Development Methodology
UF	Unidade da Federação
URL	Uniform Resource Locator

1 INTRODUÇÃO

1.1 Visão Geral

1.1.1

Este documento descreve as políticas a serem obrigatoriamente observadas pela AC Digital, integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, na emissão de certificados de assinatura digital do tipo T3.

1.1.2

A PC AC Digital T3 elaborada no âmbito da ICP-Brasil adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[1].

1.1.3

Não se aplica.

1.1.4

Não se aplica.

1.1.5

Não se aplica.

1.1.6

Certificados do tipo T3 serão emitidos pela AC Digital somente para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil.

1.1.7

Não se aplica.

1.2 Identificação

1.2.1

Este documento é chamado Política de Certificado de Assinatura Digital, Tipo T3, da AC Digital, ou simplesmente **PC T3 da AC Digital**.

1.2.2

O OID desta PC é 2.16.76.1.2.303.10.

1.3 Comunidade e Aplicabilidade

Nos itens seguintes são referidos os itens correspondentes da DPC AC Digital. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

1.3.1 Autoridades Certificadoras

1.3.1.1

Esta PC refere-se à Autoridade Certificadora Digital (AC Digital), integrante da ICP-Brasil, sob a hierarquia da AC SOLUTI e da AC Raiz.

1.3.1.2

As práticas de certificação da AC Digital estão descritas na DPC AC Digital.

1.3.2 Autoridades de Registro

1.3.2.1

O endereço da página web (URL) da AC Digital é **http://ccd.acdigital.com.br/**, onde estarão publicados os dados abaixo, referentes às Autoridades de Registro, responsáveis pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

a) relação de todas as AR credenciadas, com informações sobre as PC que implementam;

b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;

d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;

f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICP-Brasil, se for o caso.

1.3.2.2

A AC Digital mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 Identificação

A relação de todos os Prestadores de Serviço de Suporte – PSS – vinculados diretamente à AC Digital e/ou por intermédio de suas ARs é publicada em sua página web (**http://ccd.acdigital.com.br/**).

1.3.3.2 Definição e classificação

PSS são entidades utilizadas pela AC e/ou suas ARs para desempenhar as atividades descritas nesta DPC ou nas PCs e são classificadas de acordo com o tipo de atividade prestada:

a) disponibilização de infra-estrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

c) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.3.3

A AC Digital mantém as informações acima atualizadas.

1.3.4 Titulares de Certificado

Os Titulares de Certificados desta PC T3 da AC Digital são pessoas físicas ou jurídicas.

Em sendo o Titular do Certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente será designado como responsável

pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.5 Aplicabilidade

1.3.5.1

Esses certificados se destinam exclusivamente à utilização em assinatura digital, não repúdio, garantia de integridade de informação e autenticação de seu titular.

1.3.5.2

As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.3.5.3

A AC Digital leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

1.3.5.4

Não se aplica.

1.3.5.5

Não se aplica.

1.3.5.6

Certificados do tipo T3 serão utilizados em aplicações mantidas por autoridades de carimbo do tempo credenciadas na ICP-Brasil, para assinatura de carimbos do tempo.

1.4 Dados de Contato

AC DIGITAL – Autoridade Certificadora
Rua General Andrade Neves, 90, cj 102, Centro Histórico
90.010-210 – Porto Alegre – RS.

A/C: Gustavo Lopes Paiva
Telefones: (51) 3025.7600 / (51) 9952.7088
E-mail: acdigital@acdigital.com.br

2 DISPOSIÇÕES GERAIS

Nos itens seguintes são referidos os itens correspondentes da DPC AC Digital. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

2.1 Obrigações e Direitos

2.1.1 Obrigações da AC Digital

2.1.2 Obrigações das ARs

4.8.1 Recursos computacionais, software e dados corrompidos

4.8.2 Certificado de entidade é revogado

4.8.3 Chave de entidade é comprometida

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

4.8.5 Atividades das Autoridades de Registro

4.9 Extinção dos serviços da AC, AR ou PSS

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são referidos os itens correspondentes da DPC AC Digital. Apenas aspectos específicos desta PC serão descritos, quando for o caso.

5.1 Controle Físico

5.1.1 Construção e localização das instalações de AC

5.1.2 Acesso físico nas instalações de AC Digital

5.1.3 Energia e ar condicionado nas instalações da AC

5.1.4 Exposição à água nas instalações da AC

5.1.5 Prevenção e proteção contra incêndio nas instalações da AC

5.1.6 Armazenamento de mídia nas instalações da AC Digital

5.1.7 Destruição de lixo nas instalações da AC Digital

5.1.8 Instalações de segurança (backup) externas (off-site) para AC Digital

5.1.9 Instalações técnicas de AR

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

5.2.2 Número de pessoas necessário por tarefa

5.2.3 Identificação e autenticação para cada perfil

5.3 Controles de Pessoal

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2 Procedimentos de Verificação de Antecedentes

5.3.3 Requisitos de treinamento

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.5 Frequência e sequência de rodízios de cargos

5.3.6 Sanções para ações não autorizadas

5.3.7 Requisitos para contratação de pessoal

5.3.8 Documentação fornecida ao pessoal

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

6.1.1.1

Quando o titular de certificado for uma pessoa física, esta será responsável pela geração do par de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará, por seu(s) representante(s) legal(is), a pessoa responsável pela geração do par de chaves criptográficas e pelo uso do Certificado.

6.1.1.2

O par de chaves criptográficos relativos aos certificados estabelecidos por esta PC é gerado pelo próprio Titular do Certificado, respeitando os seguintes critérios:

a) A geração da chave privada ocorre em hardware criptográfico aprovado pelo CG da ICP-Brasil.

b) A entrega do certificado somente ocorre ao detentor da chave privada correspondente à chave pública constante do certificado.

6.1.1.3

O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados será o RSA, como definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.1.1.4

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1], no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil.

6.1.1.5

A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

6.1.1.6

A mídia de armazenamento de chave privada utilizado pela AC Digital assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada é única e seu sigilo é suficientemente assegurado;

b) a chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7

A mídia de armazenamento da chave privada não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura. Seu repositório é

protegido por senha e cifrado por hardware definido acima. O tipo de certificado emitido pela AC Digital e descrito nesta PC é o T3.

6.1.2 Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3 Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC Digital por meio de uma troca on-line utilizando funções automáticas do software de certificação da AC Digital. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4 Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação para os usuários da AC Digital, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP BRASIL[1];

b) Página web da AC Digital (**http://ccd.acdigital.com.br/**);

c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1

O tamanho das chaves criptográficas associadas aos certificados emitidos por esta PC é de 2048 bits.

6.1.5.2

Os algoritmos e o tamanho das chaves utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos Titulares de certificado adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.1.7 Verificação da qualidade dos parâmetros

Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.1.8 Geração de chave por hardware ou software

O processo de geração do par de chaves dos Titulares do Certificado é feito por hardware criptográfico aprovado pelo CG da ICP-Brasil.

6.1.9 Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)

As chaves privadas dos Titulares de Certificados emitidos pela AC SOLUTI RFB serão utilizadas conforme descrito no item 1.3.5. Para tanto, os certificados tem ativados os bits **digitalSignature**, **nonRepudiation** e **keyEncipherment**.

6.2 Proteção da Chave Privada

6.2.1 Padrões para módulo criptográfico

Os Titulares de Certificado devem garantir que os padrões, definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1], são observados para geração das chaves criptográficas.

6.2.2 Controle “n de m” para chave privada

Item não aplicável.

6.2.3 6.2.3. Custódia (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4 Cópia de segurança (backup) de chave privada

6.2.4.1

A chave privada de certificado do tipo T3 não pode possuir cópia de segurança.

6.2.4.2

A AC Digital, responsável por essa PC, não mantém cópia de segurança de chave privada de titular.

6.2.4.3

A chave privada de certificado do tipo T3 não pode possuir cópia de segurança.

6.2.4.4

A chave privada de certificado do tipo T3 não pode possuir cópia de segurança.

6.2.5 Arquivamento de chave privada

6.2.5.1

Item não aplicável, uma vez que a ICP-Brasil não admite o arquivamento de chaves privadas de assinatura digital.

6.2.5.2

Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6 Inserção de chave privada em módulo criptográfico

Não se aplica.

6.2.7 Método de ativação de chave privada

O titular pode definir procedimentos necessários para ativação de sua chave privada.

6.2.8 Método de desativação de chave privada

O titular pode definir procedimentos necessários para desativação de sua chave privada.

6.2.9 Método de destruição de chave privada

O titular pode definir procedimentos necessários para destruição de sua chave privada.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A AC Digital prevê que as chaves públicas de titulares dos certificados de assinatura digital e as LCRs serão armazenadas pela AC Digital, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1

As chaves privadas dos respectivos Titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2

Não se aplica.

6.3.2.3

Certificados do tipo T3 previstos nesta PC têm validade máxima de 5 (cinco) anos.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Item não aplicável.

6.4.2 Proteção dos dados de ativação

Item não aplicável.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

É responsabilidade do Titular do Certificado garantir que os equipamentos onde são gerados os pares de chaves criptográficas dispõem de mecanismos mínimos que garantam a segurança computacional, como, por exemplo, proteção do equipamento com senha, proteção anti-vírus e criptografia para armazenamento da chave privada.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

Como descrito no item correspondente da DPC AC Digital.

6.6.2 Controles de gerenciamento de segurança

Como descrito no item correspondente da DPC AC Digital.

6.6.3 Classificações de segurança de ciclo de vida

Como descrito no item correspondente da DPC AC Digital.

6.7 Controles de Segurança de Rede

Item não aplicável.

6.8 Controles de Engenharia do Módulo Criptográfico

Os Titulares de Certificado devem garantir que o token ou cartão criptográfico utilizado na geração e utilização de suas chaves criptográficas passou pela Homologação ICP-Brasil, ou que o HSM utilizado na geração e utilização de suas chaves criptográficas passou pela Homologação ICP-Brasil NSH-2, como definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

7 PERFIS DE CERTIFICADO E LCR

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC Digital, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509, especificado pelo CG da ICP-Brasil.

7.1.1 Número de versão

Todos os certificados emitidos pela AC Digital, segundo esta PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

7.1.2.1

Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2

Os certificados emitidos sob esta PC apresentam obrigatoriamente as seguintes extensões:

a) **Authority Key Identifier**, não crítica: o campo **keyIdentifier** contém o hash SHA-1 da chave pública da AC Digital;

b) **Key Usage**, crítica: somente os bits **digitalSignature**, **nonRepudiation** e **keyEncipherment** estão ativados;

c) **Certificate Policies**, não crítica:

1. o campo **policyIdentifier** contém o OID desta PC: 2.16.76.1.2.303.10; e
2. o campo **policyQualifiers** contém o endereço Web da DPC da AC Digital: **http://ccd.acdigital.com.br/docs/dpc-ac-digital.pdf**;

d) **CRL Distribution Points**, não crítica: contém o endereço Web onde se obtém a LCR da AC Digital:

1. http://ccd.acdigital.com.br/lcr/ac-digital-v1.crl
2. http://ccd2.acdigital.com.br/lcr/ac-digital-v1.crl

3. http://repositorio.icpbrasil.gov.br/lcr/ACSOLUTI/ac-digital-v1.crl

e) **Authority Information Access**, não crítica: a primeira entrada contém o método de acesso id-ad-caIssuer, contendo o URL **http://ccd.acdigital.com.br/lcr/ac-digital-v1.p7b**, para a recuperação da cadeia de certificação.

f) **basicConstraints**, não crítica: contém o campo **CA=False**.

7.1.2.3

A ICP-Brasil também define como obrigatória a extensão "Subject Alternative Name", não crítica, e com quatro campos otherName, obrigatórios, contendo, nesta ordem:

1. OID = 2.16.76.1.3.8, e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;
2. OID = 2.16.76.1.3.3, e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;
3. OID = 2.16.76.1.3.2, e conteúdo = nome do responsável pelo certificado;
4. 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 subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

7.1.2.4

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

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

b) 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";

c) Se o número do RG ou o número de inscrição do Título de Eleitor não estiver disponível, não se deve preencher os campos de órgão expedidor e UF ou os campos Zona Eleitoral, Sessão, Município e UF, respectivamente;

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;

e) Todas informações de tamanho variável referentes a números, tais como RG ou Título de Eleitor, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

f) As 10 (dez) 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;

g) Apenas os caracteres de A a Z e de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais.

7.1.2.5

Não se aplica.

7.1.2.6

Os outros campos que compõem as extensões "Subject Alternative Name" e "Extended Key Usage", ambas não críticas, e definidas como opcionais pela ICP-Brasil, poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.3 Identificadores de algoritmo

O OID (Object Identifier) do algoritmo criptográfico utilizado para assinatura do certificado, pela AC Digital , RSA com SHA-256, OID = 1.2.840.113549.1.1.11 é admitido no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

7.1.4 Formatos de nome

7.1.4.1

Não se aplica.

7.1.4.2

O certificado digital emitido para o equipamentos de carimbo do tempo de Autoridade de Carimbo do Tempo credenciada na ICP-Brasil deverá adotar o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR
O = ICP-Brasil
OU = <Nome da ACT na ICP-Brasil>
CN = <Nome do Servidor de Carimbo do Tempo (incluindo o serial do SCT)>

NOTA: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5 Restrições de nome

7.1.5.1

Não se aplica.

7.1.5.2

As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC Digital são as

seguintes:

a) Não são admitidos sinais de acentuação, trema ou cedilhas;

i. caracteres acentuados devem ser substituídos por seu correspondente sem acento;

ii. o cedilha deve ser substituído pelo caractere 'c';

b) Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Cód. NBR9611 (hexadecimal)	Caractere	Cód. NBR9611 (hexadecimal)	Caractere	Cód. NBR9611 (hexadecimal)
(branco)	20	(	28	:	3A
!	21	)	29	;	3B
“	22	*	2A	=	3D
#	23	+	2B	?	3F
$	24	,	2C	@	40
%	25	-	2D	\	5C
&	26	.	2E		
'	27	/	2F		

7.1.6 OID (Object Identifier) de Política de Certificado

O OID atribuído à esta Política de Certificado é: 2.16.76.1.2.303.10.

7.1.7 Uso da extensão “Policy Constraints”

Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo policyQualifiers da extensão “Certificate Policies” contém o endereço da página Web (URL) **http://ccd.acdigital.com.br/docs/dpc-ac-digital.pdf**, que aponta para a DPC da AC Digital.

7.1.8.1 Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela AC Digital, segundo esta PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 Extensões de LCR e de suas entradas

A AC Digital adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) "Authority Key Identifier", não crítica: contém o resumo SHA-1 da chave pública da AC Digital;

b) "CRL Number", não crítica: contém número sequencial para cada LCR emitida; e

c) "Authority Information Access", não crítica: contém o URL para a recuperação da cadeia de certificação: **http://ccd.acdigital.com.br/lcr/ac-digital-v1.p7b** . Não deve ser utilizado nenhum outro método de acesso diferente de id-ad-calssuer.

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes definem como é mantida e administrada esta PC.

8.1 Procedimentos de Mudança de Especificação

As alterações nas especificações desta PC são realizadas pela AC Digital. Quaisquer modificações são submetidas à aprovação da AC SOLUTI, que as submeterá ao CG da ICP-Brasil.

8.2 Políticas de Publicação e Notificação

A cada nova versão, esta PC é publicada na página Web da AC Digital: **http://ccd.acdigital.com.br/**

8.3 Procedimentos de Aprovação

Esta PC foi submetida à aprovação da AC SOLUTI, que por sua vez submeteu ao CG da ICP-Brasil, durante o processo de credenciamento da AC Digital, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3]. Como parte desse processo, além da conformidade com os documentos definidos pela ICP-Brasil, deverá ser verificada a compatibilidade entre esta PC e a DPC da AC DigitalDigital.

9 DOCUMENTOS REFERENCIADOS

9.1

Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio **http://www.iti.gov.br/**

publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

9.2

Os documentos abaixo aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sitio **http://www.iti.gov.br/** publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovam.

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01