





Política de Certificado A3

Autoridade Certificadora Digital Múltipla

OID: 2.16.76.1.2.3.103

Versão 2.0 de 30 de janeiro de 2023

Classificação: Pública



	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

Sumário



Controle de Versões	6
1 INTRODUÇÃO.....	7
1.1 Visão Geral1.1.1	7
1.2 Nome do documento e identificação1.2.1	7
1.3 Participantes da ICP-Brasil	8
1.3.2 Autoridades de Registro	8
1.3.3 Titulares de Certificado	8
1.3.4 Partes Confiáveis.....	8
1.3.5 Outros participantes.....	8
1.4 Usabilidade do Certificado.....	8
1.4.2 Uso proibitivo do certificado.....	9
1.5 Política de Administração	9
1.5.2 Contatos.....	9
1.5.3 Pessoa a quem determina a adequabilidade da DPC como a PC	9
1.5.4 Procedimentos de aprovação da PC	9
1.6 Definições e Acrônimos	10
2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	12
2.1 Repositórios.....	12
2.2 Publicação de informações dos certificados.....	12
2.3 Tempo ou Frequência de Publicação	12
2.4 Controle de Acesso aos Repositórios.....	12
3 IDENTIFICAÇÃO E AUTENTICAÇÃO	12
3.1 Nomeação	12
3.1.2 Necessidade de nomes serem significativos.....	12
3.1.4 Regras para interpretação de vários tipos de nomes	13
3.1.6 Procedimentos para resolver disputa de nomes	13
3.2 Validação inicial de identidade.....	13
3.2.2 Autenticação da identificação da organização	13
3.2.4 Autenticação da identidade de um indivíduo	13
3.2.6 Validação das autoridades.....	13
3.3 Identificação e autenticação para pedidos de novas chaves	13
3.3.2 Identificação e autenticação para novas chaves após revogação	13
3.4 Identificação e Autenticação para solicitação de revogação	13
4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	13
4.1 Solicitação do certificado	13
4.1.2 Processo de registro e responsabilidade.....	13
4.2 Processamento de Solicitação de Certificado	13
4.2.1 Execução das funções de identificação e autenticação	13
4.2.3 Tempo para processar a solicitação de certificado	14
4.3 Emissão de Certificado.....	14
4.3.1 Ações da AC durante a emissão de um certificado	14
4.4 Aceitação de Certificado.....	14
4.4.2 Publicação do certificado pela AC	14
4.5 Usabilidade do par de chaves e do certificado	14
4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis.....	14
4.6 Renovação de Certificados.....	14
4.6.1 Circunstâncias para renovação de certificados	14
4.6.3 Processamento de requisição para renovação de certificado	14
4.6.5 Conduta constituindo a aceitação de uma renovação de certificado	14

4.6.7	Notificação de emissão de certificados pela AC para outras entidades	14
4.7	Nova chave de certificado	14
4.7.1	Circunstâncias para nova chave de certificado	14
4.7.3	Processamento de requisição de novas chaves de certificado	14
4.7.5	Conduta constituindo a aceitação de uma nova chave certificada	14
4.7.7	Notificação de uma emissão de certificado pela AC para outras entidades	15
4.8	Modificação de certificado	15
4.8.1	Circunstâncias para modificação de certificado	15
4.8.3	Processamento de requisição de modificação de certificado	15
4.8.5	Conduta constituindo a aceitação de uma modificação de certificado	15
4.8.7	Notificação de uma emissão de certificado pela AC para outras entidades	15
4.9	Suspensão e Revogação de Certificado	15
4.9.1	Circunstâncias para revogação	15
4.9.3	Procedimento para solicitação de revogação	15
4.9.5	Tempo que a AC deve processar o pedido de revogação	15
4.9.7	Frequência de emissão de LCR	15
4.9.9	Disponibilidade para revogação/verificação de status on-line	15
4.9.11	Outras formas disponíveis para divulgação de revogação	15
4.9.13	Circunstâncias para suspensão	15
4.9.15	Procedimentos para solicitação de suspensão	15
4.10	Serviços de status de certificado	16
4.10.2	Disponibilidade de serviços	16
4.11	Encerramento de atividades	16
4.12	Custódia e recuperação de chave	16
4.12.1	Política e práticas de custódia e recuperação de chave	16
5	CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES	16
5.1	Controles físicos	16
5.1.2	Acesso físico	16
5.1.4	Exposição à água	16
5.1.6	Armazenamento de mídia	16
5.1.8	Instalações de segurança (<i>backup</i>) externas (<i>off-site</i>) para AC DIGITAL MÚLTIPLA	16
5.2	Controles Procedimentais	16
5.2.1	Perfis qualificados	16
5.2.3	Identificação e autenticação para cada perfil	16
5.3	Controles de Pessoal	17
5.3.2	Procedimentos de verificação de antecedentes	17
5.3.4	Frequência e requisitos para reciclagem técnica	17
5.3.6	Sanções para ações não autorizadas	17
5.3.8	Documentação fornecida ao pessoal	17
5.4	Procedimentos de Log de Auditoria	17
5.4.1	Tipos de eventos registrados	17
5.4.3	Período de retenção para registros de auditoria	17
5.4.5	Procedimentos para cópia de segurança (<i>Backup</i>) de registros de auditoria	17
5.4.7	Notificação de agentes causadores de eventos	17
5.5	Arquivamento de Registros	17
5.5.2	Período de retenção para arquivo	17
5.5.4	Procedimentos de cópia de arquivo	17
5.5.6	Sistema de coleta de dados de arquivo (interno e externo)	17
5.6	Troca de chave	18
5.7	Comprometimento e Recuperação de Desastre	18
5.7.1	Procedimentos gerenciamento de incidente e comprometimento	18
5.7.3	Procedimentos no caso de comprometimento de chave privada de entidade	18

5.8 Extinção da AC	18
6 CONTROLES TÉCNICOS DE SEGURANÇA	18
6.1 Geração e Instalação do Par de Chaves.....	18
6.1.2 Entrega da chave privada à entidade	19
6.1.3 Entrega da chave pública para o emissor de certificado	19
6.1.4 Entrega de chave pública da AC às terceiras partes	19
6.1.5 Tamanhos de chave.....	19
6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros	20
6.1.7 Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)	20
6.2 Proteção da Chave Privada e controle de engenharia do módulo criptográfico	20
6.2.1 Padrões e controle para módulo criptográfico	20
6.2.2 Controle “n de m” para chave privada	20
6.2.3 Custódia (escrow) de chave privada	20
6.2.4 Cópia de segurança (backup) de chave privada	20
6.2.5 Arquivamento de chave privada	21
6.2.6 Inserção de chave privada em módulo criptográfico	21
6.2.7 Armazenamento de chave privada em módulo criptográfico.....	21
6.2.8 Método de ativação de chave privada	21
6.2.9 Método de desativação de chave privada	21
6.2.10 Método de destruição de chave privada	21
6.3 Outros Aspectos do Gerenciamento do Par de Chaves.....	21
6.3.2 Períodos de operação do certificado e períodos de uso para as chaves pública e privada	21
6.4 Dados de Ativação.....	22
6.4.2 Proteção dos dados de ativação	22
6.4.3 Outros aspectos dos dados de ativação.....	22
6.5 Controles de Segurança Computacional.....	22
6.5.2 Classificação da segurança computacional	22
6.6 Controles Técnicos do Ciclo de Vida	22
6.6.1 Controles de desenvolvimento de sistema	22
6.6.2 Controles de gerenciamento de segurança	22
6.6.3 Controles de segurança de ciclo de vida	23
6.6.4 Controles na Geração de LCR.....	23
6.7 Controles de Segurança de Rede	23
6.8 Carimbo de Tempo	23
7 PERFIS DE CERTIFICADO, LCR E OCSP.....	23
7.1 Perfil do Certificado	23
7.1.1 Número de versão	23
7.1.2 Extensões de certificado.....	23
7.1.3 Identificadores de algoritmo.....	26
7.1.4 Formatos de nome.....	26
7.1.5 Restrições de nome	27
7.1.6 OID (Object Identifier) de Política de Certificado	27
7.1.7 Uso da extensão “Policy Constraints”	28
7.1.8 Sintaxe e semântica dos qualificadores de política	28
7.1.9 Semântica de processamento para as extensões críticas da PC	28
7.2 Perfil de LCR	28
7.2.2 Extensões de LCR e de suas entradas	28
7.3 Perfil OCSP	28
7.3.2 Extensões OCSP	28
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	28
8.1 Frequência e circunstâncias das avaliações	28
8.2 Identificação/Qualificação do avaliador	28



	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

8.3	Relação do avaliador com a entidade avaliada	28
8.4	Tópicos cobertos pela avaliação	29
8.5	Ações tomadas como resultado de uma deficiência	29
8.6	Comunicação dos resultados	29
9	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	29
9.1	Tarifas.....	29
9.1.2	Tarifas de acesso ao certificado	29
9.1.4	Tarifas para outros serviços.....	29
9.2	Responsabilidade Financeira	29
9.2.2	Outros ativos.....	29
9.3	Confidencialidade da informação do negócio.....	29
9.3.2	Informações fora do escopo de informações confidenciais	29
9.4	Privacidade da informação pessoal.....	29
9.4.2	Tratamento de informação como privadas	29
9.4.4	Responsabilidade para proteger a informação privadas	29
9.4.6	Divulgação em processo judicial ou administrativo	30
9.5	Direitos de Propriedade Intelectual.....	30
9.6	Declarações e Garantias	30
9.6.1	Declaração e Garantias da AC	30
9.6.3	Declarações e garantias do titular	30
9.6.5	Representações e garantias de outros participantes	30
9.7	Isenção de garantias	30
9.8	Limitações de responsabilidades.....	30
9.9	Indenizações.....	30
9.10	Prazo e Rescisão.....	30
9.10.2	Término.....	30
9.11	Avisos individuais e comunicações com os participantes.....	30
9.12	Alterações	30
9.12.1	Procedimento para emendas.....	30
9.12.2	Mecanismos de notificação e períodos.....	30
9.12.3	Circunstâncias na qual o OID deve ser alterado	30
9.13	Solução de conflitos.....	30
9.14	Lei aplicável	30
9.15	Conformidade com a Lei aplicável.....	30
9.16	Disposições Diversas.....	31
9.16.2	Cessão.....	31
9.16.4	Execução (honorários dos advogados e renúncia de direitos).....	31
9.17	Outras provisões	31
10	DOCUMENTOS REFERENCIADOS	31
11	Referências Bibliográficas	31

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

Controle de Versões

Versão	Data	Descrição
1.0	1.02.2021	Versão inicial, a partir do DOC-ICP-04 versão 8.0.
1.1	4.06.2021	Adequação do nome da AC.
2.0	30.01.2023	Atualização a partir do DOC-ICP-04 versão 8.1.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚTIPLA	

1 INTRODUÇÃO

1.1 Visão Geral

1.1.1

Este documento estabelece os requisitos mínimos obrigatórios a serem observados pela AC DIGITAL MÚTIPLA, integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na emissão de certificados de assinatura digital do tipo A3.

1.1.2

Esta PC elaborada no âmbito da ICP-Brasil adota a mesma estrutura empregada no DOC-ICP-04.

1.1.3

A estrutura desta PC está baseada na RFC 3647.

1.1.4

Este documento compõe o conjunto da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.

1.1.5

Esta PC se refere a certificados do tipo A3 para usuários finais da AC DIGITAL MÚTIPLA.

1.1.6

Não se aplica.

1.1.7

A AC DIGITAL MÚTIPLA emite certificados de assinatura do tipo A3 para pessoas físicas e pessoas jurídicas, conforme a necessidade.

1.1.8

Não se aplica.

1.1.9

Não se aplica.

1.1.10

Não se aplica.



1.1.11

Não se aplica.

1.1.12

Não se aplica.

1.2 Nome do documento e identificação1.2.1

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

Esta PC é chamada de “Política de Certificado de Assinatura Digital tipo A3 da AC DIGITAL MÚLTIPLA”, ou simplesmente PC A3 da AC DIGITAL MÚLTIPLA. O OID (object identifier) desta PC, atribuído pela AC Raiz, é **2.16.76.1.2.3.103**.

1.2.2

O OID (object identifier) abaixo mencionado foi atribuído pela AC Raiz, após conclusão do processo de credenciamento da AC DIGITAL MÚLTIPLA.

Tipo de Certificado	OID
A3	2.16.76.1.2.3.103

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

1.3.1.1 Esta PC se refere à AC DIGITAL MÚLTIPLA, integrante da ICP-Brasil.

1.3.1.2 As práticas e procedimentos de certificação digital da AC DIGITAL MÚLTIPLA estão descritas na Declaração de Práticas de Certificação da AC DIGITAL MÚLTIPLA (DPC AC DIGITAL MÚLTIPLA)

1.3.2 Autoridades de Registro

1.3.2.1 Os dados a seguir se referem às Autoridades de Registro (AR) utilizadas pela AC DIGITAL MÚLTIPLA para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes. As ARs vinculadas a AC DIGITAL MÚLTIPLA estão publicadas em página *Web* (URL) da AC DIGITAL MÚLTIPLA - <http://repositorio.acdigital.com.br/> que contém:

- a) relação de todas as AR credenciadas; e
- b) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3 Titulares de Certificado

Os Titulares de Certificado de Assinatura Digital tipo A3 da AC DIGITAL MÚLTIPLA podem ser pessoas físicas ou jurídicas.

1.3.4 Partes Confiáveis

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil.



1.3.5 Outros participantes

A relação de todos os Prestadores de Serviço de Suporte – PSS, Prestadores de Serviços Biométricos (PSBio), PSS – Prestadores de Serviço de Suporte e Prestadores de Serviço de Confiança – PSC vinculados diretamente à AC DIGITAL MÚLTIPLA são publicados em sua página *web*: <http://repositorio.acdigital.com.br/>

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do Certificado

1.4.1.1 Os certificados definidos por esta PC têm sua utilização vinculada à assinatura digital, não repúdio, garantia de integridade da informação e autenticação de seu titular.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

1.4.1.2 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.

1.4.1.3 Na definição das aplicações para o certificado definido pela PC, a AC DIGITAL MÚLTIPLA leva em consideração o nível de segurança previsto para o tipo do 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.

1.4.1.4 Certificados de tipo A3 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5 Não se aplica.

1.4.1.6 Não se aplica.

1.4.1.7 Não se aplica.

1.4.1.8 Não se aplica.

1.4.2 Uso proibitivo do certificado

A AC DIGITAL MÚLTIPLA não impõe restrições, para uso de certificados emitidos sob esta PC.

1.5 Política de Administração

1.5.1 Organização administrativa do documento

Autoridade Certificadora DIGITAL MÚLTIPLA

1.5.2 Contatos

AC DIGITAL MÚLTIPLA

Endereço: Rua General Andrade Neves, 90, Sala 04, Centro, Porto Alegre – RS, CEP: 90.010-210

Telefone: +55 (51) 3025-7630

Pág. Web: www.acdigital.com.br

E-mail: normas@acdigital.com.br

1.5.3 Pessoa a quem determina a adequabilidade da DPC como a PC

A/C: Sidnei Gomes



Telefones: +55 (51) 3025-7630

E-mail: normas@acdigital.com.br

1.5.4 Procedimentos de aprovação da PC



Esta PC é aprovada pelo ITI.

Os procedimentos de aprovação da PC da AC são estabelecidos a critério do CG da ICP-Brasil.



	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
CEI	Cadastro Especifico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM – SEI	Capability Maturity Model do Software Engineering Institute
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
CSR	Certificate Signing Request
DETRAN	Departamento Nacional de Trânsito
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

SIGLA	DESCRIÇÃO
IDS	Instrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIN	Personal Identification Number
PIS	Programa de Integração Social
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
PUK	PIN Unblocking Key

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

SIGLA	DESCRIÇÃO
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SIGEPE	Sistema de Gestão de Pessoal da Administração Pública Federal
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSL	Transport Layer Security
TSDM	Trusted Software Development Methodology
UF	Unidade da Federação
URL	Uniform Resource Locator

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

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

2.1 Repositórios

2.2 Publicação de informações dos certificados

2.3 Tempo ou Frequência de Publicação

2.4 Controle de Acesso aos Repositórios



3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens a seguir serão referidos os itens correspondentes da DPC AC DIGITAL MÚLTIPLA. Serão descritos apenas aspectos específicos desta PC, se for o caso.

3.1 Nomeação

3.1.1 Tipos de nomes

3.1.2 Necessidade de nomes serem significativos

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

3.1.4 Regras para interpretação de vários tipos de nomes

3.1.5 Unicidade de nomes

3.1.6 Procedimentos para resolver disputa de nomes

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

3.2 Validação inicial de identidade

3.2.1 Método para comprovar a posse de chave privada

3.2.2 Autenticação da identificação da organização

3.2.3 Autenticação da identidade de equipamento ou aplicação

3.2.4 Autenticação da identidade de um indivíduo

3.2.5 Informações não verificadas do titular do certificado

3.2.6 Validação das autoridades

3.2.7 Critérios para interoperação

3.3 Identificação e autenticação para pedidos de novas chaves

3.3.1 Identificação e autenticação para rotinas de novas chaves

3.3.2 Identificação e autenticação para novas chaves após revogação

3.4 Identificação e Autenticação para solicitação de revogação

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Nos itens a seguir serão referidos os itens correspondentes da DPC AC DIGITAL MÚLTIPLA. Serão descritos apenas aspectos específicos desta PC, se for o caso.

4.1 Solicitação do certificado



4.1.1 Quem pode submeter uma solicitação de certificado

4.1.2 Processo de registro e responsabilidade

4.2 Processamento de Solicitação de Certificado

4.2.1 Execução das funções de identificação e autenticação

4.2.2 Aprovação ou rejeição de pedidos de certificado

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

4.2.3 Tempo para processar a solicitação de certificado

4.3 Emissão de Certificado

4.3.1 Ações da AC durante a emissão de um certificado

4.3.2 Notificação para o titular do certificado pela AC na emissão do certificado

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado

4.4.2 Publicação do certificado pela AC

4.4.3 Notificação de emissão do certificado pela AC Raiz para outras entidades

4.5 Usabilidade do par de chaves e do certificado

4.5.1 Usabilidade da Chave privada e do certificado do titular

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

4.6 Renovação de Certificados

4.6.1 Circunstâncias para renovação de certificados

4.6.2 Quem pode solicitar a renovação

4.6.3 Processamento de requisição para renovação de certificado

4.6.4 Notificação para nova emissão de certificado para o titular

4.6.5 Conduta constituindo a aceitação de uma renovação de certificado

4.6.6 Publicação de uma renovação de um certificado pela AC

4.6.7 Notificação de emissão de certificados pela AC para outras entidades

4.7 Nova chave de certificado

4.7.1 Circunstâncias para nova chave de certificado



4.7.2 Quem pode requisitar a certificação de uma nova chave pública

4.7.3 Processamento de requisição de novas chaves de certificado

4.7.4 Notificação de emissão de novo certificado para o titular

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

4.7.6 Publicação de uma nova chave certificada pela AC

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.8 Modificação de certificado

4.8.1 Circunstâncias para modificação de certificado

4.8.2 Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3 Processamento de requisição de modificação de certificado

4.8.4 Notificação de emissão de novo certificado para o titular

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

4.8.6 Publicação de uma modificação de certificado pela AC

4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.9 Suspensão e Revogação de Certificado

4.9.1 Circunstâncias para revogação

4.9.2 Quem pode solicitar revogação

4.9.3 Procedimento para solicitação de revogação

4.9.4 Prazo para solicitação de revogação

4.9.5 Tempo que a AC deve processar o pedido de revogação

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

4.9.7 Frequência de emissão de LCR

4.9.8 Latência máxima para a LCR

4.9.9 Disponibilidade para revogação/verificação de status on-line

4.9.10 Requisitos para verificação de revogação on-line



4.9.11 Outras formas disponíveis para divulgação de revogação

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.13 Circunstâncias para suspensão

4.9.14 Quem pode solicitar suspensão

4.9.15 Procedimentos para solicitação de suspensão

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

4.9.16 Limites no período de suspensão

4.10 Serviços de status de certificado

4.10.1 Características operacionais

4.10.2 Disponibilidade de serviços

4.10.3 Funcionalidades operacionais

4.11 Encerramento de atividades

4.12 Custódia e recuperação de chave

4.12.1 Política e práticas de custódia e recuperação de chave

4.12.2 Política e práticas de encapsulamento e recuperação de chave de sessão

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens a seguir serão referidos os itens correspondentes da DPC AC DIGITAL MÚLTIPLA. Serão descritos apenas aspectos específicos desta PC, se for o caso.

5.1 Controles físicos

5.1.1 Construção e localização das instalações de AC

5.1.2 Acesso físico

5.1.3 Energia e ar-condicionado

5.1.4 Exposição à água

5.1.5 Prevenção e proteção contra incêndio

5.1.6 Armazenamento de mídia

5.1.7 Destruição de lixo

5.1.8 Instalações de segurança (*backup*) externas (*off-site*) para AC DIGITAL MÚLTIPLA



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

5.2.4 Funções que requerem separação de deveres

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

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 rodízio 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

5.4 Procedimentos de Log de Auditoria

5.4.1 Tipos de eventos registrados

5.4.2 Frequência de auditoria de registros

5.4.3 Período de retenção para registros de auditoria

5.4.4 Proteção de registros de auditoria

5.4.5 Procedimentos para cópia de segurança (*Backup*) de registros de auditoria

5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)

5.4.7 Notificação de agentes causadores de eventos

5.4.8 Avaliações de vulnerabilidade

5.5 Arquivamento de Registros

5.5.1 Tipos de registros arquivados

5.5.2 Período de retenção para arquivo



5.5.3 Proteção de arquivo

5.5.4 Procedimentos de cópia de arquivo

5.5.5 Requisitos para datação de registros

5.5.6 Sistema de coleta de dados de arquivo (interno e externo)

5.5.7 Procedimentos para obter e verificar informação de arquivo

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

5.6 Troca de chave

5.7 Comprometimento e Recuperação de Desastre

5.7.1 Procedimentos gerenciamento de incidente e comprometimento

5.7.2 Recursos computacionais, software, e/ou dados corrompidos

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4 Capacidade de continuidade de negócio após desastre

5.8 Extinção da AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, estão definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC A3 da AC DIGITAL MÚLTIPLA. São também definidos outros controles técnicos de segurança utilizados pela AC DIGITAL MÚLTIPLA e pelas ARs vinculadas na execução de suas funções operacionais.

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.

6.1.1.1.1 Não se aplica.

6.1.1.1.2 Não se aplica.



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 cartão inteligente ou token, protegido por senha, com capacidade de geração de chave homologado junto à ICP-Brasil ou com certificação INMETRO.

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

6.1.1.3 Os algoritmos a serem utilizados para as chaves criptográficas de titulares de certificados é o RSA conforme definido em regulamento por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.1.4 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado em regulamento por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

6.1.1.5 A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e o repositório de armazenamento usado para a sua utilização.

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

6.1.1.8 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17 [2], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC DIGITAL MÚLTIPLA, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

O tipo de certificado emitido pela AC DIGITAL e descrito nesta PC é o A3

6.1.2 Entrega da chave privada à entidade

Não se aplica.

6.1.3 Entrega da chave pública para o emissor de certificado

A chave pública do solicitante de certificado é entregue por meio eletrônico, utilizando o formato *PKCS#10*, através uma sessão segura, recorrendo à utilização de uma sessão segura *SSL – Secure Socket Layer*.

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 Entrega de chave pública da AC às terceiras partes



A AC DIGITAL MÚLTIPLA disponibiliza o seu certificado da cadeia de certificação para os usuários da ICP- Brasil, a chave pública da AC DIGITAL MÚLTIPLA é entregue de uma das seguintes formas:

- a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil;
- b) Página *web* da AC DIGITAL MÚLTIPLA - <http://repositorio.acdigital.com.br/>; e
- 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 A3 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 em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificado adotam o padrão estabelecido em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

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

Os certificados e respectivos pares de chaves emitidos por esta PC têm sua utilização vinculada à assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves (item 1.4).

6.2 Proteção da Chave Privada e controle de engenharia do módulo criptográfico

Nos itens a seguir são definidos os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos segundo esta PC A3.

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1 Os módulos de geração de chaves criptográficas devem suportar padrões RSA ou ECCBrainpool (conforme RFC 5639), conforme definidos em regulamento editado por instrução.

6.2.1.2 Os módulos de armazenamento da chave privada da entidade titular de certificado, deverão ser homologados pela ICP-Brasil ou com certificação INMETRO, conforme definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.1.3 Os requisitos aplicados aos módulos de armazenamento da chave privada da entidade titular de certificado, deverão ser homologados pela ICP-Brasil ou com certificação INMETRO, conforme regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2 Controle “n de m” para chave privada

Não se aplica.

6.2.3 Custódia (*escrow*) de chave privada

A AC DIGITAL MÚLTIPLA não realiza a recuperação (*escrow*) de chaves privadas emitidas conforme esta PC.



6.2.4 Cópia de segurança (*backup*) de chave privada

6.2.4.1 Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua chave privada.

6.2.4.2 A AC DIGITAL MÚLTIPLA não mantém cópia de segurança de chave privada gerada pelo titular de certificado.

6.2.4.3 Em qualquer caso a cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4 Na realização de uma cópia de segurança da chave privada do titular de certificado, o titular deve observar que a cópia deverá ser protegida por “senha”.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚTIPLA	

6.2.5 Arquivamento de chave privada

6.2.5.1 AAC DIGITAL MÚTIPLA não arquivava cópia de chaves privadas de titulares de certificado.

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 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8 Método de ativação de chave privada

A chave privada é ativada, mediante senha e ou identificação biométrica solicitada pelo software de proteção da chave privada. A senha deve ser criada e mantida apenas pelo titular do certificado, sendo para seu uso e conhecimento exclusivo, o hardware utilizado deverá estar homologado perante a ICPBrasil ou com certificação INMETRO.

O titular de certificado deverá adotar senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 03 (três) meses.

6.2.9 Método de desativação de chave privada

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

6.2.10 Método de destruição de chave privada

Para esta PC do tipo A3, o titular do certificado poderá 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



As chaves públicas de titulares de certificado de assinatura digital e as LCRs emitidas pela AC DIGITAL MÚTIPLA serão armazenadas de forma permanente, após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de operação do certificado e períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas de assinatura dos respectivos titulares de certificado emitidos pela AC DIGITAL MÚTIPLA 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 O período máximo de validade para certificados do tipo A3 está descrito na tabela abaixo:

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

Tipo de Certificado	Período Máximo de Validade do Certificado (em anos)
A3	5 (cinco) anos

6.3.2.4 Não se aplica.

6.3.2.5 Não se aplica.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Os dados de ativação, se utilizados, da chave privada da entidade titular do certificado são únicos e aleatórios.

6.4.2 Proteção dos dados de ativação

Recomenda-se que o titular do certificado digital defina sua senha com o comprimento de 08 caracteres ou mais, composta por letras, números e símbolos.

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança do equipamento onde são geradas e utilizadas as chaves privadas. O hardware criptográfico onde são geradas as chaves criptográficas dos titulares de certificado deve possuir mecanismos criptográficos de geração de chaves e ser homologado junto à ICPBrasil, ou com certificação INMETRO. Os equipamentos onde são geradas os pares de chaves devem possuir software instalado para o correto funcionamento dos dispositivos criptográficos, como estarem providos de mecanismos de segurança, tais como antivírus, criptografia para armazenamento da chave privada, sistema operacional atualizado e proteção de tela.

6.5.2 Classificação da segurança computacional

Não se aplica.

6.6 Controles Técnicos do Ciclo de Vida

AC DIGITAL MÚLTIPLA desenvolve sistemas de AR, apenas com a finalidade da operação de suas ARs vinculadas.



6.6.1 Controles de desenvolvimento de sistema

AC DIGITAL MÚLTIPLA utiliza modelos, como SCRUM e métodos Ágeis, para o desenvolvimento de seus sistemas. Todo os projetos de desenvolvimento passam por, requisitos, análise, codificação e testes, de forma a minimizar quaisquer tipos de erros que possam comprometer a sua operação.

Os projetos de desenvolvimento da AC DIGITAL MÚLTIPLA geram documentação suficiente para suportar avaliações externas, como auditorias.

6.6.2 Controles de gerenciamento de segurança

A AC DIGITAL MÚLTIPLA verifica com periodicidade através de ferramentas do seu próprio sistema operacional. As verificações são realizadas através de scripts, em caso de divergência é disparado um alerta, via e-mail ou similar, para que sejam tomadas as medidas apropriadas.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

6.6.3 Controles de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração de LCR

As LCRs emitidas pela AC DIGITAL MÚLTIPLA, são verificadas quanto a sua consistência de seu conteúdo, número de série, versão da LCR, data/hora de emissão e outras informações relevantes antes da sua publicação.

6.7 Controles de Segurança de Rede

Não se aplica.

6.8 Carimbo de Tempo

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

Os itens seguintes devem especificar os formatos dos certificados e das LCRs gerados segundo esta PC A3. Devem ser incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes deverão ser obrigatoriamente atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC DIGITAL MÚLTIPLA, segundo esta PC A3, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão



Todos os certificados emitidos pela AC DIGITAL MÚLTIPLA, segundo esta PC A3, 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, são descritas todas as extensões de certificado utilizadas e sua criticalidade desta PC A3.

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 MÚLTIPLA;
- b) **“Key Usage”**, crítica, conforme disposto no item 7.1.2.7 deste documento;
- c) **“Certificate Policies”**, não crítica: contém os seguintes campos:
 1. o OID desta PC: **2.16.76.1.2.3.103**; e
 2. o endereço Web da DPC da AC DIGITAL MÚLTIPLA:
<http://repositorio.acdigital.com.br/docs/ac-digital-multipla.pdf>
- d) **“CRL Distribution Points”**, não crítica: contém 2 (dois) endereços *Web* onde se obtém a LCR da AC DIGITAL MÚLTIPLA:
 - i. **<http://repositorio.acdigital.com.br/lcr/ac-digital-multipla-g1.crl>**
 - ii. **<http://repositorio2.acdigital.com.br/lcr/ac-digital-multipla-g1.crl>**
- e) **“Authority Information Access”**, não crítica: contém uma entrada contendo o método de acesso *id-ad-calssuer*, utilizando um dos seguintes protocolos de acesso, HTTP e HTTPS, contendo o URL para a recuperação da cadeia de certificação: **<http://repositorio.acdigital.com.br/cert/ac-digital-multipla->**

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

g1.p7b

7.1.2.3 A ICP-Brasil também define como obrigatória a extensão “*Subject Alternative Name*”, não crítica, e com os seguintes formatos:

a) Para certificado de pessoa física:

a.1) 3 (três) campos *otherName*, obrigatórios, contendo:

1. 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 subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral – RG do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

2. OID = 2.16.76.1.3.6, e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa física titular do certificado.

3. OID = 2.16.76.1.3.5, e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

i. Campo *otherName*, não obrigatório, contendo:

OID = 2.16.76.1.4.2.n, e conteúdo = de tamanho varável correspondente ao número de identificação profissional emitido por conselho de classe profissional e outras informações, se necessário.

ii. 1 (um) Campo *otherName*, **obrigatório** para certificados vinculados ao Documento RIC, contendo:

OID = 2.16.76.1.3.9, e conteúdo = nas primeiras 11 (onze) posições, o número de Registro de identificação Civil.

iii. Não se aplica.

b) Para certificado de pessoa jurídica, 4 (quatro) campos *otherName*, obrigatórios, contendo:

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;

OID = 2.16.76.1.3.2, e conteúdo = nome do responsável pelo certificado;

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;

OID = 2.16.76.1.3.7, e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa jurídica titular do certificado.



c) Para certificado de equipamento ou aplicação: Não se aplica.

d) Para certificado de equipamento A CF-e-SAT, 3 (três) campos *otherName*, obrigatórios, contendo, nesta ordem:

Não se aplica.

e) Para certificado de equipamento OM-BR, 3 (três) campos *otherName*, obrigatórios, contendo, nesta ordem:

Não se aplica.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

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 não estiver disponível, não se deve preencher o campo de órgão emissor UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;
- d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;
- 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.
- h) Não se aplica.



7.1.2.5 Não se aplica.

7.1.2.6 A AC DIGITAL MÚLTIPLA implementa a extensão “*SubjectAlternativeName*”, definida como opcional pela ICP-Brasil, com os seguintes campos na forma e com os propósitos definidos na RFC 5280:

- i. em todos os certificados o campo “*rfc822Name*” (OID 2.5.29.17.1) contendo o endereço de e-mail do titular ou responsável pelo certificado.

7.1.2.7 A AC DIGITAL MÚLTIPLA implementa as extensões “*Key Usage*” e “*Extended Key Usage*” definidas como obrigatórias pela ICP-Brasil, obedecendo aos propósitos e criticidade conforme descrição abaixo:

- a) para certificados de Assinatura de Código (*codeSigning*):
Não se aplica.
- b) para certificados de Autenticação de Servidor (*SSL/TLS*):
Não se aplica.
- c) para certificados de Assinatura de Carimbo do Tempo:
Não se aplica.
- d) para certificados de Assinatura A CF-e-SAT
Não se aplica.
- e) certificados de Assinatura de Resposta *OCSP*
Não se aplica.
- f) para os demais certificados de Assinatura e/ou Proteção de e-Mail:
 - i. “*Key Usage*”, crítica, contém os seguintes bits ativos:
 1. *digitalSignature*;

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

2. *nonRepudiation*; e
 3. *keyEncipherment*.
- ii. “*Extended-key-usage*”, **não crítica**: contém os seguintes bits ativos em conformidade com a RFC 5280:
1. “*client authentication*” OID = 1.3.6.1.5.5.7.3.2;
 2. “*E-mail protection*” OID = 1.3.6.1.5.5.7.3.4.
- g) para certificados de Sigilo:
Não se aplica.

7.1.3 Identificadores de algoritmo

Os certificados emitidos pela AC DIGITAL MÚLTIPLA são assinados com o uso do algoritmo RSA com SHA-256, como função de hash (OID = 1.2.840.113549.1.1.11) conforme padrão PKCS#1. Eles são admitidos no âmbito da ICP-Brasil, conforme regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.4 Formatos de nome

7.1.4.1 O nome do titular do certificado, constante do campo “*Subject*”, adota o “*Distinguished Name*”(DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

Para certificados na hierarquia da Autoridade Certificadora Raiz Brasileira V5:

- a) Para certificado de pessoa física:
- C = BR
 - O = ICP-Brasil
 - OU = AC DIGITAL Múltipla G1
 - OU = <CNPJ da AR que realizou a identificação>
 - OU = <Tipo de identificação utilizada: presencial, videoconferencia ou certificadodigital>
 - OU = Certificado PF A3
 - CN = <Nome do titular do certificado>:<CPF>
- b) Para certificado de pessoa jurídica:
- C = BR
 - O = ICP-Brasil
 - ST = <Sigla da unidade da federação> L = <Cidade/Município>
 - OU = AC DIGITAL Múltipla G1
 - OU = <CNPJ da AR que realizou a identificação>
 - OU = <Tipo de identificação utilizada: presencial, videoconferencia ou certificadodigital>
 - OU = Certificado PJ A3
 - CN = <Nome empresarial constante no cartão CNPJ>:<CNPJ>



NOTA:

O nome será escrito para todos os casos até o limite do tamanho disponível no campo, até a um máximo de 64 (sessenta e quatro) caracteres, vedada a abreviatura.

Conforme descrito no item 7.1.5. não serão aceites caracteres como “.”, “/” ou “-”.

7.1.4.2 Não se aplica.

7.1.4.3 Não se aplica.

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

7.1.4.4 Não se aplica.

7.1.5 Restrições de nome



7.1.5.1 Neste item da PC, estão descritas as restrições aplicáveis para os nomes dos titulares de certificado.

7.1.5.2 A ICP-Brasil estabelece as seguintes restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC DIGITAL MÚLTIPLA:

- a) Não são admitidos sinais de acentuação, trema ou cedilhas; e
 - i. caracteres acentuados devem ser substituídos por seu correspondente sem acento;
- b) Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

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

7.1.6 OID (Object Identifier) de Política de Certificado

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

Todo certificado emitido segundo esta PC A3 da AC DIGITAL MÚLTIPLA, possui na extensão “Certificate Policy” O OID atribuído a esta Política de Certificado A3: 2.16.76.1.2.3.103

7.1.7 Uso da extensão “Policy Constraints”

Não se aplica.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC A3, o campo *policyQualifiers* da extensão “Certificate Policies” contém o seguinte endereço da página *Web* (URL), que aponta para a DPC da AC DIGITAL MÚLTIPLA: <http://repositorio.acdigital.com.br/docs/ac-digital-multipla.pdf>

7.1.9 Semântica de processamento para as extensões críticas da PC

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela AC DIGITAL MÚLTIPLA, segundo esta PC A3, 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

7.2.2.1 Neste item são descritas todas as extensões de LCR utilizadas pela AC DIGITAL MÚLTIPLA e sua criticidade.

7.2.2.2 As LCRs da AC DIGITAL MÚLTIPLA adotam as seguintes extensões definidas como obrigatórias pela ICP-Brasil:

- a) “Authority Key Identifier”, não crítica: contém o resumo SHA-1 da chave pública da AC DIGITAL MÚLTIPLA;
- b) “CRL Number”, não crítica: contém número sequencial para cada LCR emitida.

7.3 Perfil OCSP

7.3.1 Número(s) de versão

Não se aplica.

7.3.2 Extensões OCSP

Não se aplica.



8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes serão referidos os itens correspondentes na DPC da AC DIGITAL MÚLTIPLA, ou serão descritos de forma específica para a PC, se for o caso.

8.1 Frequência e circunstâncias das avaliações

8.2 Identificação/Qualificação do avaliador

8.3 Relação do avaliador com a entidade avaliada

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

8.4 Tópicos cobertos pela avaliação

8.5 Ações tomadas como resultado de uma deficiência

8.6 Comunicação dos resultados

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Os itens seguintes estão referidos em seus correspondentes na DPC da AC DIGITAL MÚLTIPLA, ou detalhados de forma específica para a PC, se houver.

9.1 Tarifas

9.1.1 Tarifas de emissão e renovação de certificados

9.1.2 Tarifas de acesso ao certificado

9.1.3 Tarifas de revogação ou de acesso à informação de status

9.1.4 Tarifas para outros serviços

9.1.5 Política de reembolso

9.2 Responsabilidade Financeira

9.2.1 Cobertura do seguro

9.2.2 Outros ativos

9.2.3 Cobertura de seguros ou garantia para entidades finais

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.2 Informações fora do escopo de informações confidenciais

9.3.3 Responsabilidade em proteger a informação confidencial

9.4 Privacidade da informação pessoal



9.4.1 Plano de privacidade

9.4.2 Tratamento de informação como privadas

9.4.3 Informações não consideradas privadas

9.4.4 Responsabilidade para proteger a informação privadas

9.4.5 Aviso e consentimento para usar informações privadas

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

9.4.6 Divulgação em processo judicial ou administrativo

9.4.7 Outras circunstâncias de divulgação de informação

9.5 Direitos de Propriedade Intelectual

9.6 Declarações e Garantias

9.6.1 Declaração e Garantias da AC

9.6.2 Declarações e Garantias da AR

9.6.3 Declarações e garantias do titular

9.6.4 Declarações e garantias das terceiras partes

9.6.5 Representações e garantias de outros participantes

9.7 Isenção de garantias

9.8 Limitações de responsabilidades

9.9 Indenizações

9.10 Prazo e Rescisão

9.10.1 Prazo

9.10.2 Término

9.10.3 Efeito da rescisão e sobrevivência

9.11 Avisos individuais e comunicações com os participantes

9.12 Alterações

9.12.1 Procedimento para emendas

Sempre que necessário realizar alterações nas especificações desta PC, elas serão realizadas pela AC DIGITAL MÚLTIPLA. Qualquer alteração nesta PC é submetida à aprovação da AC Raiz.

9.12.2 Mecanismos de notificação e períodos



Esta PC após aprovada é publicada em repositório público ou página *Web* conforme descrito em sua DPC.

9.12.3 Circunstâncias na qual o OID deve ser alterado

9.13 Solução de conflitos

9.14 Lei aplicável

9.15 Conformidade com a Lei aplicável

	POLÍTICA DE CERTIFICADO A3	
	PC A3 - AC DIGITAL MÚLTIPLA	

9.16 Disposições Diversas

9.16.1 Acordo completo

Esta PC representa as obrigações e deveres aplicáveis à AC e AR e outras entidades citadas. Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2 Cessão

9.16.3 Independência de disposições

9.16.4 Execução (honorários dos advogados e renúncia de direitos)

9.17 Outras provisões

Esta PC foi submetida à aprovação da AC Raiz, durante o processo de credenciamento da AC DIGITAL MÚLTIPLA, 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, é verificada a compatibilidade entre esta PC e a DPC da AC DIGITAL MÚLTIPLA.

10 DOCUMENTOS REFERENCIADOS

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
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL Aprovado pela Resolução nº 132, de 10 de novembro de 2017	DOC-ICP-17
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de Novembro de 2008	DOC-ICP-12
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03

11 REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3647, IETF – *Internet X.509 Public Key Infrastructure Certificate Policy and Certification PracticesFramework*, november 2003.

RFC 5280, IETF – *Internet X.509 Public Key Infrastructure Certificate Policy and Certification RevocationList (CRL) Profile*, may 2008.

RFC 2818, IETF – *HTTP Over TLS*, may 2000.

RFC 6960, IETF – *Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP*, june 2003.