

**Política de Certificado A1 da
Autoridade Certificadora Validar Múltipla
(PC A1 da AC Validar Múltipla)**

OID: 2.16.76.1.2.1.157

**Versão 1.0
Março 2023**

Sumário

1.	INTRODUÇÃO	12
1.1.	Visão Geral	12
1.2.	Nome do Documento e Identificação	12
1.3.	Participantes da ICP-Brasil	13
1.3.1.	Autoridades Certificadoras	13
1.3.2.	Autoridades de Registro.....	13
1.3.3.	Titulares de Certificado	13
1.3.4.	Partes Confiáveis	13
1.3.5.	Outros Participantes.....	14
1.4.	Usabilidade do Certificado	14
1.4.1	Uso Adequado do Certificado.....	14
1.5.	Política de Administração	15
1.5.1	Organização administrativa do documento	15
1.5.2	Contatos	15
1.5.3	Pessoa que determina a adequabilidade da DPC com a PC	15
1.5.4	Procedimentos para aprovação da PC	15
1.6.	Definição e Acrônimos	15
2.	RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	16
2.1.	Repositórios	16
2.2.	Publicação de informações dos certificados.....	16
2.3.	Tempo ou Frequência de Publicação	16
2.4.	Controle de Acesso aos Repositórios	16
3.	IDENTIFICAÇÃO E AUTENTICAÇÃO	16
3.1.	Nomeação	16
3.1.1.	Tipos de nomes	17
3.1.2.	Necessidade de nomes significativos.....	17

3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado	17
3.1.4. Regras para interpretação de vários tipos de nomes	17
3.1.5. Unicidade de nomes	17
3.1.6. Procedimento para resolver disputa de nomes	17
3.1.7. Reconhecimento, autenticação e papel de marcas registradas	17
3.2. Validação Inicial de Identidade	17
3.2.1. Método para comprovar a posse de chave privada	17
3.2.2. Autenticação da identificação da organização	17
3.2.3. Autenticação da identidade de equipamento ou aplicação	17
3.2.4. Autenticação da identidade de um indivíduo	17
3.2.5. Informações não verificadas do titular do certificado	17
3.2.6. Validação das autoridades	17
3.2.7. Critérios para interoperação	17
3.3. Identificação e autenticação para pedidos de novas chaves	17
3.3.1. Identificação e autenticação para rotina de novas chaves	17
3.3.2. Identificação e autenticação para novas chaves após a revogação	17
3.4. Identificação e Autenticação para solicitação de revogação	17
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	17
4.1. Solicitação do certificado	17
4.1.1. Quem pode submeter uma solicitação de certificado	18
4.1.2. Processo de registro e responsabilidades	18
4.2. Processamento de Solicitação de Certificado	18
4.2.1. Execução das funções de identificação e autenticação	18
4.2.2. Aprovação ou rejeição de pedidos de certificado	18
4.2.3. Tempo para processar a solicitação de certificado	18
4.3. Emissão de Certificado	18
4.3.1. Ações da AC durante a emissão de um certificado	18
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado	18
4.4. Aceitação de Certificado	18
4.4.1. Conduta sobre a aceitação do certificado	18

4.4.2. Publicação do certificado pela AC	18
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades.....	18
4.5. Usabilidade do par de chaves e do certificado.....	18
4.5.1. Usabilidade da Chave privada e do certificado do titular.....	18
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis	18
4.6. Renovação de Certificados.....	18
4.6.1. Circunstâncias para renovação de certificados	18
4.6.2. Quem pode solicitar a renovação.....	18
4.6.3. Processamento de requisição para renovação de certificados.....	18
4.6.4. Notificação para nova emissão de certificado para o titular.....	18
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado	18
4.6.6. Publicação de uma renovação de um certificado pela AC.....	18
4.6.7. Notificação de emissão de certificado pela AC para outras entidades.....	19
4.7. Nova chave de certificado.....	19
4.7.1. Circunstâncias para nova chave de certificado	19
4.7.2. Quem pode requisitar a certificação de uma nova chave pública	19
4.7.3. Processamento de requisição de novas chaves de certificado	19
4.7.4. Notificação de emissão de novo certificado para o titular.....	19
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada	19
4.7.6. Publicação de uma nova chave certificada pela AC	19
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades	19
4.8. Modificação de certificado	19
4.8.1. Circunstâncias para modificação de certificado.....	19
4.8.2. Quem pode requisitar a modificação de certificado.....	19
4.8.3. Processamento de requisição de modificação de certificado	19
4.8.4. Notificação de emissão de novo certificado para o titular.....	19
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado.....	19
4.8.6. Publicação de uma modificação de certificado pela AC	19
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades	19
4.9. Suspensão e Revogação de Certificado.....	19

4.9.1. Circunstâncias para revogação	19
4.9.2. Quem pode solicitar revogação	19
4.9.3. Procedimento para solicitação de revogação	19
4.9.4. Prazo para solicitação de revogação	19
4.9.5. Tempo em que a AC deve processar o pedido de revogação	19
4.9.6. Requisitos de verificação de revogação para as partes confiáveis	20
4.9.7. Frequência de emissão de LCR	20
4.9.8. Latência máxima para a LCR	20
4.9.9. Disponibilidade para revogação/verificação de status on-line	20
4.9.10. Requisitos para verificação de revogação on-line.....	20
4.9.11. Outras formas disponíveis para divulgação de revogação	20
4.9.12. Requisitos especiais para o caso de comprometimento de chave	20
4.9.13. Circunstâncias para suspensão	20
4.9.14. Quem pode solicitar suspensão.....	20
4.9.15. Procedimento para solicitação de suspensão	20
4.9.16. Limites no período de suspensão	20
4.10. Suspensão e Revogação de Certificado	20
4.10.1. Características operacionais	20
4.10.2. Disponibilidade dos serviços.....	20
4.10.3. Funcionalidades operacionais	20
4.11. Encerramento de atividades.....	20
4.12. Custódia e recuperação de chave	20
4.12.1. Política e práticas de custódia e recuperação de chave	20
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão	20
5.1. Controles físicos.....	20
5.1.1. Construção e localização das instalações	20
5.1.2. Acesso físico	21
5.1.3. Energia e ar-condicionado	21
5.1.4. Exposição à água.....	21
5.1.5. Prevenção e proteção contra incêndio	21

5.1.6. Armazenamento de mídia	21
5.1.7. Destruição de lixo	21
5.1.8. Instalações de segurança (<i>backup</i>) externas (<i>off-site</i>) para AC	21
5.2. Controles Procedimentais.....	21
5.2.1. Perfis qualificados.....	21
5.2.2. Número de pessoas necessário por tarefa	21
5.2.3. Identificação e autenticação para cada perfil	21
5.2.4. Funções que requerem separação de deveres	21
5.3. Controles de Pessoal	21
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....	21
5.3.2. Procedimentos de verificação de antecedentes	21
5.3.3. Requisitos de treinamento	21
5.3.4. Frequência e requisitos para reciclagem técnica	21
5.3.5. Frequência e sequência de rodízio de cargos.....	21
5.3.6. Sanções para ações não autorizadas	21
5.3.7. Requisitos para contratação de pessoal	21
5.3.8. Documentação fornecida ao pessoal	21
5.4. Procedimentos de Log de Auditoria.....	21
5.4.1. Tipos de eventos registrados	21
5.4.2. Frequência de auditoria de registros	22
5.4.3. Período de retenção para registros de auditoria	22
5.4.4. Proteção de registros de auditoria.....	22
5.4.5. Procedimentos para cópia de segurança (<i>backup</i>) de registros de auditoria.....	22
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo)	22
5.4.7. Notificação de agentes causadores de eventos	22
5.4.8. Avaliações de vulnerabilidade	22
5.5. Arquivamento de Registros	22
5.5.1. Tipos de registros arquivados.....	22
5.5.2. Período de retenção para arquivo	22
5.5.3. Proteção de arquivo	22

5.5.4. Procedimentos de cópia de arquivo.....	22
5.5.5. Requisitos para datação de registros	22
5.5.6. Sistema de coleta de dados de arquivo (interno e externo)	22
5.5.7. Procedimentos para obter e verificar informação de arquivo	22
5.6. Troca de chave	22
5.7. Comprometimento e Recuperação de Desastre	22
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento	22
5.7.2. Recursos computacionais, software, e/ou dados corrompidos	22
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade	22
5.7.4. Capacidade de continuidade de negócio após desastre	22
5.8. Extinção da AC	22
6. CONTROLES TÉCNICOS DE SEGURANÇA	22
6.1. Geração e Instalação do par de chaves.....	23
6.1.1. Geração do par de chaves.....	23
6.1.2. Entrega da chave privada à entidade.....	24
6.1.3. Entrega da chave pública para o emissor de certificado	24
6.1.4. Disponibilização de chave pública da AC para usuários	24
6.1.5. Tamanhos de chave	25
6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros.....	25
6.1.7 Propósitos de uso de chave (conforme o campo “ <i>key usage</i> ” na X.509 v3).....	25
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico	25
6.2.1. Padrões para módulo criptográfico	25
6.2.2. Controle “n de m” para chave privada.....	25
6.2.3. Custódia (<i>escrow</i>) de chave privada.....	26
6.2.4. Cópia de segurança (backup) de chave privada	26
6.2.4.1 Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.....	26
6.2.5 Arquivamento de chave privada	26
6.2.6 Inserção de chave privada em módulo criptográfico.....	26
6.2.7. Armazenamento de chave privada em módulo criptográfico.....	26

6.2.8. Método de ativação de chave privada	26
6.2.9. Método de desativação de chave privada	26
6.2.10. Método de destruição de chave privada	27
6.3 Outros Aspectos do Gerenciamento do par de chaves	27
6.3.1 Arquivamento de chave pública	27
6.3.2 Períodos de uso para as chaves pública e privada	27
6.4 Dados de Ativação	27
6.4.1 Geração e instalação dos dados de ativação	27
6.4.2 Proteção dos dados de ativação	27
6.4.3 Outros aspectos dos dados de ativação	28
6.5 Controles de Segurança Computacional	28
6.5.2 Classificação da segurança computacional	28
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA	28
6.6.1. Controles de desenvolvimento de sistema	28
6.6.2 Controles de gerenciamento de segurança	28
6.6.3 Classificações de segurança de ciclo de vida	29
6.6.4 Controles na geração da LCR antes de publicadas	29
6.7. Controles de Segurança de Rede	29
6.8. Carimbo de Tempo	29
7. PERFIS DE CERTIFICADO E LCR E OCSP	29
7.1 Perfil do Certificado	29
7.1.1 Número de versão	29
7.1.2 Extensões de certificado	29
7.1.3 Identificadores de algoritmo	33
7.1.4 Formatos de nome	33
7.1.5 Restrições de nome	33
7.1.6 OID (<i>Object Identifier</i>) de Política de Certificado	35
7.1.7 Uso da extensão " <i>Policy Constraints</i> "	35
7.1.8 Sintaxe e semântica dos qualificadores de política	35
7.1.9 Semântica de processamento para extensões críticas	35

7.2.	Perfil de LCR	35
7.2.1.	Número de versão	35
7.2.2	Extensões de LCR e de suas entradas	35
7.3.	Perfil de OCSP	36
7.3.1.	Número(s) de versão	36
7.3.2.	Extensões de OCSP	36
8.	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....	36
8.1.	Frequência e circunstâncias das avaliações.....	36
9.	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS	36
9.1.	Tarifas	36
9.2.	Responsabilidade Financeira	36
9.3.	Confidencialidade da informação do negócio	37
9.4.	Privacidade da informação pessoal	37
9.5.	Direitos de Propriedade Intelectual	37
9.6.	Declarações e Garantias.....	37
9.7.	Isenção de garantias.....	37
9.8.	Limitações de responsabilidades.....	38
9.9.	Indenizações	38
9.10.	Prazo e Rescisão	38
9.10.1.	Prazo	38
9.10.2.	Término	38
9.10.3.	Efeito da rescisão e sobrevivência	38
9.11.	Avisos individuais e comunicações com os participantes.....	38
9.12.	Alterações	38
9.13.	Solução de conflitos	38
9.14.	Lei aplicável	38
9.15.	Conformidade com a Lei aplicável.....	38
9.16.	Disposições Diversas	38
9.16.1.	Acordo completo	38
9.17.	Outras provisões.....	38

10.	DOCUMENTOS REFERENCIADOS	39
11.	REFERÊNCIAS BIBLIOGRÁFICAS.....	39

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item alterado	Descrição da alteração
1.0	Março/2023	-	Não há	Versão inicial – Baseada no DOC-ICP-04 versão 8.1

1. INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

1.1. Visão Geral

1.1.1 Este documento estabelece requisitos mínimos a serem obrigatoriamente observados pela Autoridade Certificadora Validar Múltipla – AC integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de sua Política de Certificado (PC) sob a estrutura da AC de nível imediatamente superior AC Validar Múltipla.

1.1.2 Essa PC elaborada no âmbito da ICP-Brasil adota obrigatoriamente a mesma estrutura empregada no DOC-ICP-04 - *Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil [2]*.

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 O tipo de certificado emitido sob esta PC é o Tipo A1.

1.1.6 Não se aplica.

1.1.7 Certificados do tipo A1, de assinatura, podem ser emitidos pela AC Validar Múltipla para pessoas físicas e pessoas jurídicas.

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 Identificação

1.2.1. Esta PC é chamada “Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora AC Validar Múltipla” e referida como “PC A1 da AC Validar Múltipla”. O *Object Identifier* (OID) atribuído para esta PC, após processo de credenciamento da AC junto à ICP-Brasil, é:

2.16.76.1.2.1.157.

1.2.2 Não se aplica.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC é implementada pela Autoridade Certificadora AC Validar Múltipla, integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora AC SyngularID, que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira.

1.3.1.2. As práticas e procedimentos de certificação utilizados pela AC Validar Múltipla estão descritas em sua Declaração de Práticas de Certificação (DPC da AC Validar Múltipla) que se encontra publicada no seu repositório, no seguinte endereço: <http://syngularid.com.br/repositorio/ac-validar-multipla/dpc/>.

1.3.2. Autoridades de Registro

1.3.2.1. A AC Validar Múltipla mantém página web e/ou diretório com endereço: <http://syngular.com.br/repositorio/ac-validar-multipla/ar/> onde estão publicados os seguintes dados, referentes às Autoridades de Registro (ARs) que realizam os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

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

1.3.2.2. A AC Validar Múltipla mantém as informações acima sempre atualizadas.

1.3.3. Titulares de Certificado

Pessoas físicas ou jurídicas, de direito público ou privado, nacionais ou estrangeiras, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis, podem ser Titulares de Certificado. Os certificados podem ser utilizados por pessoas físicas e pessoas jurídicas. O titular do certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada. Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

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

1.3.5.1. A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC Validar Múltipla e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC Validar Múltipla (<http://syngular.com.br/repositorio/ac-validar-multipla/>).

1.4. Usabilidade do Certificado

1.4.1 Uso Adequado do Certificado

1.4.1.1. Neste item são relacionadas as aplicações para as quais os certificados definidos nesta PC são adequados.

1.4.1.2. As aplicações e demais programas que admitem 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. A AC Validar Múltipla 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.

Os certificados emitidos pela AC Validar Múltipla no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.4. Os certificados de tipo A1 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

Não se aplica.

1.5. Política de Administração

1.5.1 Organização administrativa do documento

Nome da Autoridade Certificadora: AC Validar Múltipla.

1.5.2 Contatos

Endereço: Rua Prefeito Osmar Cunha, 183, Sala 1005, Bloco B, Centro, Florianópolis/SC.

CEP: 88.015-900.

Telefone: 48-3028-3700.

Página Web: <http://www.validar.com.br>.

E-mail: contato@arvalidar.com.br.

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: Carlos Francisco Tatara

E-mail: compliance@syngular.id

Telefone: 48-4042 1641

1.5.4 Procedimentos para 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.

1.6. Definição e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CN	Common Name
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação

ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
ISSO	International Organization for Standardization
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PIS	Programa de Integração Social
PsBio	Prestadores de Serviço de Biometria
PSC	Prestadores de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SSL	Secure Socket Layer
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC Validar Múltipla.

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 seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC Validar Múltipla.

3.1. Nomeação

3.1.1. Tipos de nomes

3.1.2. Necessidade de nomes significativos

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. Procedimento 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 rotina de novas chaves

3.3.2. Identificação e autenticação para novas chaves após a revogação

3.4. Identificação e Autenticação para solicitação de revogação

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Nos itens seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC Validar Múltipla.

4.1. Solicitação do certificado

4.1.1. Quem pode submeter uma solicitação de certificado

4.1.2. Processo de registro e responsabilidades

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

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. Notificações 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 certificados

4.6.4. Notificação para nova emissão de certificado para o titular

4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

4.6.6. Publicação de uma renovação de um certificado pela AC

4.6.7. Notificação de emissão de certificado 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

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

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 revogaç

4.9.5. Tempo em 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. Procedimento para solicitação de suspensão

4.9.16. Limites no período de suspensão

4.10. Suspensão e Revogação de Certificado

4.10.1. Características operacionais

4.10.2. Disponibilidade dos 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 seguintes são referidos os itens correspondentes da Declaração de Práticas de Certificação - DPC da AC Validar Múltipla.

5.1. Controles físicos

5.1.1. Construção e localização das instalações

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

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

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

5.6. Troca de chave

5.7. Comprometimento e Recuperação de Desastre

5.7.1. Procedimentos de 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, esta PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a mesma. São também definidos outros controles técnicos de segurança utilizados pela AC Validar 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. O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares 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 A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (*Cryptographic Service Provider*) existente na estação do solicitante apresentados pelo browser e, quando da geração, a chave privada é armazenada no HD da estação.

6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

6.1.1.4 Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado A1.

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 da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
- b) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

- c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7. Esta mídia de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8. O tipo de certificado emitido pela AC Validar Múltipla e descrito nesta PC é o A1.

TIPO DE CERTIFICADO	MÍDIA ARMAZENADORA DE CHAVE CRIPTOGRÁFICA (Requisitos Mínimos)
A1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima.

Nota: A responsabilidade pela segurança na garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do titular ou responsável pelo uso do certificado, conforme especificado no Termo de Titularidade.

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para o emissor de certificado

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

A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - *Secure Socket Layer*.

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 Validar Múltipla, compreendem:

A AC Validar Múltipla disponibiliza o seu certificado, e todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web:

<http://syngular.com.br/repositorio/ac-validar-multipla/certificados/ac-validar-multipla.p7b>

- a) Página web da AC Validar Múltipla <https://arvalidar.com.br/>
- b) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Os certificados emitidos de acordo com esta PC situam-se sob a cadeia da Autoridade Certificadora Raiz Brasileira V5. O tamanho das chaves criptográficas associadas é de 2048 bits.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A1 da ICP-Brasil está em conformidade com o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [3]

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

Os parâmetros de geração de chaves assimétricas da AC Validar Múltipla seguem o padrão de Homologação da ICP-Brasil, em conformidade ao estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

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

Os certificados têm ativados os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment*. Os pares de chaves correspondentes aos certificados emitidos pela AC Validar Múltipla podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

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

Nos itens seguintes, a PC define os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos pela AC Validar Múltipla.

6.2.1. Padrões para módulo criptográfico

6.2.1.1 Não se aplica

6.2.1.2. Os requisitos aplicáveis ao módulo criptográfico utilizado para geração de chaves criptográficas dos titulares de certificado segue os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

6.2.2. Controle “n de m” para chave privada

Não se aplica.

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

6.2.4.2 A AC Validar Múltipla responsável por esta PC não mantém cópia de segurança de chave privada de titular.

6.2.4.3 A cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3] e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. Não se aplica.

6.2.5 Arquivamento de chave privada

6.2.5.1 Não se aplica, 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. 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 solicitada pelo software de proteção da chave privada.

6.2.9. Método de desativação de chave privada

Cada entidade titular de certificado pode definir os procedimentos necessários para a desativação da sua chave privada.

6.2.10. Método de destruição de chave privada

Cada entidade titular de certificado pode definir os procedimentos necessários para a destruição da sua chave privada.

6.3 Outros Aspectos do Gerenciamento do par de chaves

6.3.1 Arquivamento de chave pública

As chaves públicas da AC Validar Múltipla, de titulares dos certificados de assinatura digital e as LCRs emitidas pela AC Validar Múltipla são armazenadas 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 A1 previstos nesta PC podem ter a validade de minutos, horas, dias e até 1 (um) ano.

6.3.2.4 Não se aplica.

6.3.2.5 Não se aplica.

6.4 Dados de Ativação

Nos itens seguintes desta PC são descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 Geração e instalação dos dados de ativação

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

6.4.2 Proteção dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

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 computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do Certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, com proteção antivírus e criptografia 3DES para a chave privada, armazenada no HD.

6.5.2 Classificação da segurança computacional

Não se aplica.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

Não se aplica.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC Validar Múltipla adota Sistema de Certificação Digital desenvolvido por terceiros. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente da AC Validar Múltipla avalia e decide quando será a implementação no ambiente de produção.

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. A AC Validar Múltipla verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. A AC Validar Múltipla utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3 Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na geração da LCR antes de publicadas

Antes de publicadas, todas as LCRs geradas pela AC Validar Múltipla são verificadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7. Controles de Segurança de Rede

Não se aplica.

6.8. Carimbo de Tempo

Não se aplica.

7. PERFIS DE CERTIFICADO E LCR E OCSP

Os itens seguintes especificam os formatos dos certificados e das LCR/OCSP gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC Validar Múltipla 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 Validar Múltipla, 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. A AC Validar Múltipla implementa as mesmas extensões definidas como obrigatórias na ICP-Brasil, descritas no item 7.1.2.2.

7.1.2.2. A AC Validar Múltipla implementa nos certificados emitidos segundo esta PC as seguintes extensões, definidas como obrigatórias pela ICP-Brasil:

- a) "**Authority Key Identifier**", **não crítica**: no campo *Key Identifier* contém o resumo SHA-1 da chave pública da AC Validar Múltipla;
- b) "**Key Usage**", **crítica**: configurados conforme disposto no item 7.1.2.7 deste documento;
- c) "**Certificate Policies**", **não crítica**, contém
- i. O campo *policyIdentifier* contém o OID desta PC 2.16.76.1.2.1.157;
 - ii. O campo *policyQualifiers* contém o endereço Web onde se obtém a DPC da AC Validar Múltipla <http://syngularid.com.br/repositorio/ac-validar-multipla/dpc/dpc-ac-validar-multipla.pdf>.
- d) "**CRL Distribution Points**", **não crítica**: contém os endereços das páginas Web onde se obtém a LCR da AC Validar Múltipla: <http://syngularid.com.br/repositorio/ac-validar-multipla/lcr/lcr-ac-validar-multipla.crl> e <http://icp-brasil.syngularid.com.br/repositorio/ac-validar-multipla/lcr/lcr-ac-validar-multipla.crl>
- e) "**Authority Information Access**", **não crítica**: contém o método de acesso id-ad-calssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação: <http://syngularid.com.br/repositorio/ac-validar-multipla/certificados/ac-validar-multipla.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:

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 unidade da federação;

OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado;

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;

- a.2) 1 (um) campos *otherName*, obrigatório para certificados digitais cujas titularidades foram validadas pela AR dos conselhos de classes profissionais regulamentados por lei específica, contendo:

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

- a.3) 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 Identidade Civil.

- a.4) 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 Registro Geral (RG) do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva Unidade da Federação;

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 Específico do INSS (CEI) da pessoa jurídica titular do certificado;

- c) não se aplica

- d) não se aplica.

- e) não se aplica.

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* é 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 são integralmente preenchidos com caracteres “zero”;
- c) Se o número do RG não estiver disponível, não é preenchido o campo de órgão emissor e UF. O mesmo ocorre para o campo do 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 as informações de tamanho variável, referentes a números, tal como RG, são 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, sendo 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, 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. Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos pela AC Validar Múltipla, podem ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

7.1.2.6. Os outros campos que compõem a extensão "*Subject Alternative Name*" podem ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.7. As extensões "*Key Usage*" e "*Extended Key Usage*" para os referidos tipos de certificado são obrigatórias e obedecem aos propósitos de uso e a criticalidade conforme descrição abaixo:

- a) Não se aplica;
- b) Não se aplica;
- c) Não se aplica;

d) Não se aplica;

e) Não se aplica;

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

“Key Usage”, crítica: contém o bit *digitalSignature* ativado, podendo conter os bits *keyEncipherment* e *nonRepudiation* ativados;

“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.

g) Não se aplica.

7.1.3 Identificadores de algoritmo

Certificados emitidos pela AC Validar 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 o padrão PKCS#1, observados os algoritmos admitidos no âmbito da ICP-Brasil, documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

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:

C = BR

O = ICP-Brasil

OU = AC Validar Múltipla

OU = CNPJ da AR que realizou a identificação

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

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).

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

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. Não se aplica.

7.1.5 Restrições de nome

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

certificados.

7.1.5.2. A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

- a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e
- b) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

CARACTERE	CÓDIGO 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

Todo certificado emitido segundo esta PC A1 contém, na extensão “*Certificate Policies*”, o OID atribuído **2.16.76.1.2.1.157**.

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, o campo ***policyQualifiers*** da extensão “*Certificate Policies*” contém o endereço da página Web (URL) com a DPC da AC Validar Múltipla, sendo: <http://syngularid.com.br/repositorio/ac-validar-multipla/dpc/dpc-ac-validar-multipla.pdf>

7.1.9 Semântica de processamento para extensões críticas

Extensões críticas são ser interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número de versão

As LCRs geradas pela AC Validar Múltipla 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

7.2.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC Validar Múltipla e sua criticalidade.

7.2.2.2. A AC Validar Múltipla 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 Validar

Múltipla que assina a LCR; e

b) “*CRL Number*”, não crítica: contém número sequencial para cada LCR emitida.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Não se aplica.

7.3.2. Extensões de OCSP

Não se aplica.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Validar Múltipla.

8.1. Frequência e circunstâncias das avaliações

8.2. Identificação/Qualificação do avaliador

8.3. Relação do avaliador com a entidade avaliada

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

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Validar Múltipla.

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

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. Declarações 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

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC Validar Múltipla. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz. Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC Validar Múltipla mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web: <http://syngularid.com.br/repositorio/ac-validar-multipla/pc/>.

9.13. Solução de conflitos

9.14. Lei aplicável

9.15. Conformidade com a Lei aplicável

9.16. Disposições Diversas

9.16.1. Acordo completo

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

9.17. Outras provisões

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC Validar Múltipla, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [1]. Como parte desse processo, além da conformidade com

este documento, deverá ser verificada a compatibilidade entre a PC e a DPC da AC Validar Múltipla.

10. DOCUMENTOS REFERENCIADOS

10.1. 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
[1]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

10.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, 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 Instruções Normativas que os aprovaram.

REF	NOME DO DOCUMENTO	CÓDIGO
[3]	PADRÕES E ALGORITIMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

11. REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3647, IETF - *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, november 2003.

RFC 5280, IETF - *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, may 2008.

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