



Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE RFB

OID: 2.16.76.1.2.1.23

Classificação: Pública

Versão 8.0

Julho de 2019



CONTROLE DE ALTERAÇÕES E VERSÕES

VERSÃO	DATA	RESOLUÇÃO QUE APROVOU A ALTERAÇÃO	ITEM ALTERADO	DESCRIÇÃO DA ALTERAÇÃO
7.0	16/08/2018	-	1.3.3.1, 6.1.4, 6.6.1.1, 7.1.2.2, 7.1.4, 7.1.8, 8.2 7.1.5.2	Troca de URL resultante da mudança de PSS Adição de caracteres especiais
7.1	21/02/2019	Resolução 150	1.3.4, 7.1.2.3 7.1.4	Retirada do certificado para aplicação emitido pela RFB Alteração do campo OU contendo o CNPJ da AR
8.0	23/07/2019	Resolução 151	Diversos	Adequação à Resolução 151

SUMÁRIO

1. INTRODUÇÃO	11
1.1. Visão Geral	11
1.2. Nome do documento e identificação	11
1.3. Participantes da ICP-Brasil	12
1.3.1. Autoridades Certificadoras	12
1.3.2. Autoridades de Registro	12
1.3.3. Titulares de Certificado	12
1.3.4. Partes Confiáveis	12
1.3.5. Outros Participantes	12
1.4. Usabilidade do Certificado	12
1.4.1. Uso apropriado do certificado	12
1.4.2. Uso proibitivo do certificado	13
1.5. Política de Administração	13
1.5.1. Organização administrativa do documento	13
1.5.2. Contatos	13
1.5.3. Pessoa que determina a adequabilidade da DPC com a PC	13
1.5.4. Procedimentos de aprovação da PC	13
1.6. Definições e Acrônimos	13
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	14
2.1. Repositórios	14
2.2. Publicação de informações dos certificados	14
2.3. Tempo ou Frequência de Publicação	14
2.4. Controle de Acesso aos Repositórios	14
3. IDENTIFICAÇÃO E AUTENTICAÇÃO	14
3.1. Nomeação	14
3.1.1. Tipos de nomes	14
3.1.2. Necessidade dos nomes serem significativos	14
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado	14
3.1.4. Regras para interpretação de vários tipos de nomes	14
3.1.5. Unicidade de nomes	15
3.1.6. Procedimento para resolver disputa de nomes	15
3.1.7. Reconhecimento, autenticação e papel de marcas registradas	15
3.2. Validação inicial de identidade	15
3.2.1. Método para comprovar a posse de chave privada	15
3.2.2. Autenticação da identificação da organização	15

3.2.3.	Autenticação da identidade de equipamento ou aplicação	15
3.2.4.	Autenticação da identidade de um indivíduo	15
3.2.5.	Informações não verificadas do titular do certificado	15
3.2.6.	Validação das autoridades	15
3.2.7.	Critérios para interoperação	15
3.3.	Identificação e autenticação para pedidos de novas chaves	15
3.3.1.	Identificação e autenticação para rotina de novas chaves	15
3.3.2.	Identificação e autenticação para novas chaves após a revogação	15
3.4.	Identificação e Autenticação para solicitação de revogação	15
4.	REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	15
4.1.	Solicitação do Certificado	15
4.1.1.	Quem pode submeter uma solicitação de certificado	15
4.1.2.	Processo de registro e responsabilidades.....	15
4.2.	Processamento de Solicitação de Certificado.....	15
4.2.1.	Execução das funções de identificação e autenticação.....	15
4.2.2.	Aprovação ou rejeição de pedidos de certificado	15
4.2.3.	Tempo para processar a solicitação de certificado	15
4.3.	Emissão de Certificado	15
4.3.1.	Ações da AC durante a emissão de um certificado	15
4.3.2.	Notificações para o titular do certificado pela AC na emissão do certificado..	15
4.4.	Aceitação de Certificado.....	15
4.4.1.	Conduta sobre a aceitação do certificado	15
4.4.2.	Publicação do certificado pela AC.....	15
4.4.3.	Notificação de emissão do certificado pela AC Raiz para outras entidades.....	15
4.5.	Usabilidade do par de chaves e do certificado	15
4.5.1.	Usabilidade da Chave privada e do certificado do titular	15
4.5.2.	Usabilidade da chave pública e do certificado das partes confiáveis.....	15
4.6.	Renovação de Certificados	15
4.6.1.	Circunstâncias para renovação de certificados	15
4.6.2.	Quem pode solicitar a renovação	15
4.6.3.	Processamento de requisição para renovação de certificados.....	15
4.6.4.	Notificação para nova emissão de certificado para o titular	15
4.6.5.	Conduta constituindo a aceitação de uma renovação de um certificado	15
4.6.6.	Publicação de uma renovação de um certificado pela AC	15
4.6.7.	Notificação de emissão de certificado pela AC para outras entidades	15

4.7. Nova chave de certificado	15
4.7.1. Circunstâncias para nova chave de certificado	15
4.7.2. Quem pode requisitar a certificação de uma nova chave pública.....	15
4.7.3. Processamento de requisição de novas chaves de certificado	15
4.7.4. Notificação de emissão de novo certificado para o titular	15
4.7.5. Conduta constituindo a aceitação de uma nova chave certificadora.....	15
4.7.6. Publicação de uma nova chave certificada pela AC	16
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades	16
4.8. Modificação de certificado.....	16
4.8.1. Circunstâncias para modificação de certificado	16
4.8.2. Quem pode requisitar a modificação de certificado	16
4.8.3. Processamento de requisição de modificação de certificado.....	16
4.8.4. Notificação de emissão de novo certificado para o titular	16
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado.....	16
4.8.6. Publicação de uma modificação de certificado pela AC.....	16
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades	16
4.9. Suspensão e Revogação de Certificado	16
4.9.1. Circunstâncias para revogação	16
4.9.2. Quem pode solicitar revogação	16
4.9.3. Procedimento para solicitação de revogação	16
4.9.4. Prazo para solicitação de revogação.....	16
4.9.5. Tempo em que a AC deve processar o pedido de revogação	16
4.9.6. Requisitos de verificação de revogação para as partes confiáveis.....	16
4.9.7. Frequência de emissão de LCR.....	16
4.9.8. Latência máxima para a LCR	16
4.9.9. Disponibilidade para revogação/verificação de status on-line	16
4.9.10. Requisitos para verificação de revogação on-line.....	16
4.9.11. Outras formas disponíveis para divulgação de revogação	16
4.9.12. Requisitos especiais para o caso de comprometimento de chave	16
4.9.13. Circunstâncias para suspensão	16
4.9.14. Quem pode solicitar suspensão.....	16
4.9.15. Procedimento para solicitação de suspensão	16
4.9.16. Limites no período de suspensão	16
4.10. Serviços de status de certificado.....	16
4.10.1. Características operacionais	16
4.10.2. Disponibilidade dos serviços.....	16

4.10.3. Funcionalidades operacionais.....	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
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão	16
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES.....	16
5.1. Controles físicos.....	16
5.1.1. Construção e localização das instalações	16
5.1.2. Acesso físico.....	16
5.1.3. Energia e ar-condicionado.....	16
5.1.4. Exposição à água	16
5.1.5. Prevenção e proteção contra incêndio.....	16
5.1.6. Armazenamento de mídia.....	16
5.1.7. Destruição de lixo.....	16
5.1.8. Instalações de segurança (backup) externas (off-site) para AC.....	16
5.2. Controles Procedimentais	16
5.2.1. Perfis qualificados	16
5.2.2. Número de pessoas necessário por tarefa	16
5.2.3. Identificação e autenticação para cada perfil	16
5.2.4. Funções que requerem separação de deveres.....	16
5.3. Controles de Pessoal	17
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade	17
5.3.2. Procedimentos de verificação de antecedentes	17
5.3.3. Requisitos de treinamento.....	17
5.3.4. Frequência e requisitos para reciclagem técnica	17
5.3.5. Frequência e sequência de rodízio de cargos.....	17
5.3.6. Sanções para ações não autorizadas	17
5.3.7. Requisitos para contratação de pessoal.....	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
5.4.2. Frequência de auditoria de registros.....	17
5.4.3. Período de retenção para registros de auditoria	17
5.4.4. Proteção de registros de auditoria	17
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria	17

5.4.6. Sistema de coleta de dados de auditoria (interno ou externo).....	17
5.4.7. Notificação de agentes causadores de eventos	17
5.4.8. Avaliações de vulnerabilidade	17
5.5. Arquivamento de Registros.....	17
5.5.1. Tipos de registros arquivados	17
5.5.2. Período de retenção para arquivo	17
5.5.3. Proteção de arquivo	17
5.5.4. Procedimentos de cópia de arquivo	17
5.5.5. Requisitos para datação de registros	17
5.5.6. Sistema de coleta de dados de arquivo (interno e externo).....	17
5.5.7. Procedimentos para obter e verificar informação de arquivo	17
5.6. Troca de chave	17
5.7. Comprometimento e Recuperação de Desastre	17
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento	17
5.7.2. Recursos computacionais, software, e/ou dados corrompidos	17
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade	17
5.7.4. Capacidade de continuidade de negócio após desastre	17
5.8. Extinção da AC	17
6.CONTROLES TÉCNICOS DE SEGURANÇA	17
6.1. Geração e Instalação do Par de Chaves	17
6.1.1. Geração do par de chaves	17
6.1.2. Entrega da chave privada à entidade titular do certificado	18
6.1.3. Entrega da chave pública para emissor de certificado.....	18
6.1.4. Entrega de chave pública da AC às terceiras partes.....	18
6.1.5. Tamanhos de chave.....	18
6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros	19
6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)	19
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico	19
6.2.1. Padrões e controle para módulo criptográfico	19
6.2.2. Controle “n de m” para chave privada	19
6.2.3. Custódia (escrow) de chave privada	19
6.2.4. Cópia de segurança de chave privada	19
6.2.5. Arquivamento de chave privada.....	19
6.2.6. Inserção de chave privada em módulo criptográfico.....	20
6.2.7. Armazenamento de chave privada em módulo criptográfico	20

6.2.8. Método de ativação de chave privada	20
6.2.9. Método de desativação de chave privada.....	20
6.2.10. Método de destruição de chave privada	20
6.3. Outros Aspectos do Gerenciamento do Par de Chaves	20
6.3.1. Arquivamento de chave pública	20
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada	20
6.4. Dados de Ativação	20
6.4.1. Geração e instalação dos dados de ativação.....	20
6.4.2. Proteção dos dados de ativação	20
6.4.3. Outros aspectos dos dados de ativação	21
6.5. Controles de Segurança Computacional.....	21
6.5.1. Requisitos técnicos específicos de segurança computacional.....	21
6.5.2. Classificação da segurança computacional.....	21
6.6. Controles Técnicos do Ciclo de Vida	21
6.6.1. Controles de desenvolvimento de sistema	21
6.6.2. Controles de gerenciamento de segurança	21
6.6.3. Controles de segurança de ciclo de vida.....	21
6.6.4. Controles na Geração de LCR	21
6.7. Controles de Segurança de Rede	21
6.8. Carimbo de Tempo	21
7. PERFIS DE CERTIFICADO, LCR e OCSP.....	21
7.1. Perfil do Certificado.....	22
7.1.1. Número de versão	22
7.1.2. Extensões de certificado	22
7.1.3. Identificadores de algoritmo.....	25
7.1.4. Formatos de nome	25
7.1.5. Restrições de nome	26
7.1.6. OID (Object Identifier) de Política de Certificado	27
7.1.7. Uso da extensão “Policy Constraints”	27
7.1.8. Sintaxe e semântica dos qualificadores de política	27
7.1.9. Semântica de processamento para as extensões críticas de PC.....	27
7.2. Perfil de LCR.....	27
7.2.1. Número(s) de versão	27
7.2.2. Extensões de LCR e de suas entradas	27
7.3. Perfil de OCSP	27

7.3.1.	Número(s) de versão	27
7.3.2.	Extensões de OCSP	27
8.	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	27
8.1.	Frequência e circunstâncias das avaliações	27
8.2.	Identificação/Qualificação do avaliador	27
8.3.	Relação do avaliador com a entidade avaliada	28
8.4.	Tópicos cobertos pela avaliação	28
8.5.	Ações tomadas como resultado de uma deficiência	28
8.6.	Comunicação dos resultados	28
9.	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS	28
9.1.	Tarifas	28
9.1.1.	Tarifas de emissão e renovação de certificados	28
9.1.2.	Tarifas de acesso ao certificado	28
9.1.3.	Tarifas de revogação ou de acesso à informação de status	28
9.1.4.	Tarifas para outros serviços	28
9.1.5.	Política de reembolso	28
9.2.	Responsabilidade Financeira	28
9.2.1.	Cobertura do seguro	28
9.2.2.	Outros ativos	28
9.2.3.	Cobertura de seguros ou garantia para entidades finais	28
9.3.	Confidencialidade da informação do negócio	28
9.3.1.	Escopo de informações confidenciais	28
9.3.2.	Informações fora do escopo de informações confidenciais	28
9.3.3.	Responsabilidade em proteger a informação confidencial	28
9.4.	Privacidade da informação pessoal	28
9.4.1.	Plano de privacidade	28
9.4.2.	Tratamento de informação como privadas	28
9.4.3.	Informações não consideradas privadas	28
9.4.4.	Responsabilidade para proteger a informação privadas	28
9.4.5.	Aviso e consentimento para usar informações privadas	28
9.4.6.	Divulgação em processo judicial ou administrativo	28
9.4.7.	Outras circunstâncias de divulgação de informação	28
9.5.	Direitos de Propriedade Intelectual	28
9.6.	Declarações e Garantias	28
9.6.1.	Declarações e Garantias da AC	28
9.6.2.	Declarações e Garantias da AR	28

9.6.3. Declarações e garantias do titular	28
9.6.4. Declarações e garantias das terceiras partes	28
9.6.5. Representações e garantias de outros participantes.....	28
9.7. Isenção de garantias.....	28
9.8. Limitações de responsabilidades	28
9.9. Indenizações	28
9.10. Prazo e Rescisão	28
9.10.1. Prazo	28
9.10.2. Término.....	28
9.10.3. Efeito da rescisão e sobrevivência.....	28
9.11. Avisos individuais e comunicações com os participantes.....	28
9.12. Alterações	28
9.12.1. Procedimento para emendas	28
9.12.2. Mecanismo de notificação e períodos	29
9.12.3. Circunstâncias na qual o OID deve ser alterado	29
9.13. Solução de conflitos.....	29
9.14. Lei aplicável.....	29
9.15. Conformidade com a Lei aplicável	29
9.16. Disposições Diversas.....	29
9.16.1. Acordo completo	29
9.16.2. Cessão	29
9.16.3. Independência de disposições	29
9.16.4. Execução (honorários dos advogados e renúncia de direitos).....	29
9.17. Outras provisões.....	29
10. DOCUMENTOS REFERENCIADOS	30

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento descreve as “Políticas de Certificado” (PC) de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE RFB na Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

1.1.2. A estrutura desta PC está baseada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC 3647 (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework).

1.1.3. São 12 (doze) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 8 (oito) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir:

a) Tipos de Certificados de Assinatura Digital:

- i. A1
- ii. A2
- iii. A3
- iv. A4
- v. T3
- vi. T4
- vii. A CF-e-SAT
- viii. OM-BR

b) Tipos de Certificados de Sigilo:

- i. S1
- ii. S2
- iii. S3
- iv. S4

1.1.4. Os tipos de certificados indicados acima, de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

1.1.5. Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.1.8. Não se aplica.

1.1.9. Outros tipos de certificado, além dos doze anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescentadas aos tipos de certificados aceitos pela ICP-Brasil.

1.1.10. 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 PRODEMGE RFB” e referida como “PC A1 da AC PRODEMGE RFB”. Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A1 no REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] do

Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é **2.16.76.1.2.1.23**.

1.2.2. Não se aplica.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC refere-se exclusivamente à AC PRODEMGE RFB no âmbito da ICP-Brasil.

1.3.1.2. As práticas e procedimentos de certificação da AC PRODEMGE RFB estão descritos na Declaração de Práticas de Certificação da AC PRODEMGE RFB (DPC da AC PRODEMGE RFB).

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro (AR) utilizadas pela AC PRODEMGE RFB para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em endereço *web* da AC PRODEMGE RFB (<https://www.prodemge.gov.br/>):

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

1.3.3. Titulares de Certificado

Pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras, podem ser titulares de Certificado.

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 AC PRODEMGE RFB publica em endereço *web* <https://www.prodemge.gov.br/> a relação de todos os seus Prestadores de Serviços de Suporte (PSS) e Prestadores de Serviços Biométricos (PSBios).

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

1.4.1.1. Neste item são relacionadas as aplicações para as quais os certificados definidos por esta 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, aceitam qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

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

1.4.1.4. Os certificados emitidos pela AC PRODEMGE RFB 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.

1.4.1.5. 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

AC PRODEMGE RFB

1.5.2. Contatos

Empresa:	Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE
Endereço:	Rua da Bahia, 2277 – Bairro de Lourdes – Belo Horizonte – MG – CEP: 30.160-012
Telefone Fixo:	(31) 3339-1245
Página web	www.prodemge.gov.br
E-mail geral:	acprodemge@prodemge.gov.br

1.5.3. Pessoa que determina a adequabilidade da DPC com a PC

Nome:	Felipe Roncalli De Paula Carneiro
Área:	Gerência de Certificação Digital
Telefone:	(31) 3339-1245
E-mail	acprodemge@prodemge.gov.br

1.5.4. Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.

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

1.6. Definições e Acrônimos

Acrônimo e Sigla	Descrição
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CI	Cédula de Identidade
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Cadastro Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoa Jurídica
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoa Física
CS	Code Signing

DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
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
NIST	National Institute of Standards and Technology
NIS	Número de Identificação Social
OCSP	Online 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
PCI	Política de Classificação de Informação
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
PJ	Pessoa Jurídica
POP	Proof of Possession
PRD	Plano de Recuperação de Desastres
Prodemge	Companhia de Tecnologia da Informação do Estado de Minas Gerais
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC PRODEMGE RFB.

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 DPC da AC PRODEMGE RFB.

3.1. Nomeação

3.1.1. Tipos de nomes

3.1.2. Necessidade dos nomes serem 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 DPC da AC PRODEMGE RFB.

- 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 certificadora

- 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 revogação
- 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. Serviços de status 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 DPC da AC PRODEMGE RFB.

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

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 Cryptographic Service Provider (CSP) existente na estação do solicitante apresentados pelo browser e, quando da geração, a chave privada é armazenada no HD da estação.

A chave privada poderá ser exportada e armazenada (cópia de segurança) em hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO - e protegida por

senha de acesso.

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 [2].

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 [2]. As chaves privadas correspondentes aos certificados deverão ser armazenadas em repositório protegido por senha e/ou identificação biométrica, 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. O meio de armazenamento da chave privada utilizado pelo titular 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 que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
- c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

6.1.1.8. O tipo de certificado emitido pela AC PRODEMGE RFB 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.

6.1.2. Entrega da chave privada à entidade titular do certificado

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

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

6.1.4. Entrega de chave pública da AC às terceiras partes

A AC PRODEMGE RFB disponibiliza o seu certificado e todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através endereços *web*:

Para certificados emitidos na AC Prodemge RFB G3:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_RFB_G3.p7c

Para certificados emitidos na AC Prodemge RFB G4:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_RFB_G4.p7c

Para certificados emitidos na AC Prodemge RFB V1:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_rfb/ac_prodemge_rfb.p7c

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC PRODEMGE RFB é de 1024 bits para a hierarquia V1 e de 2048 bits para a hierarquia V2 e V5.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A1 da ICP-Brasil está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

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 certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [2].

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 PRODEMGE RFB 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 são referidos os requisitos para a proteção das chaves dos titulares de certificados emitidos pela AC PRODEMGE RFB.

6.2.1. Padrões e controle 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 seguem os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[2].

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 de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura sem o consentimento do titular do certificado.

6.2.4. Cópia de segurança de chave privada

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

6.2.4.2. A AC PRODEMGE RFB não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC PRODEMGE RFB não arquiva cópias de chaves privadas de assinatura digital de

titulares de certificados.

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

Os Titulares de Certificados poderão optar por utilizar um hardware criptográfico, cartão inteligente ou token, para armazenar sua chave privada após a aceitação do certificado.

6.2.7. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1

6.2.8. Método de ativação de chave privada

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

6.2.9. Método de desativação de chave privada

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

6.2.10. Método de destruição de chave privada

O titular de certificado pode definir procedimentos necessários para a 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 dos titulares de certificados de assinatura digital e as LCR emitidas pela AC PRODEMGE RFB permanecem armazenadas após a expiração dos correspondentes certificados, permanentemente, na forma da legislação em vigor, 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 certificados emitidos pela AC PRODEMGE RFB são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação das 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 admitido para certificados de assinatura digital Tipo A1 da AC PRODEMGE RFB é de 1 (um) ano.

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 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 anti-vírus 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

A AC PRODEMGE RFB desenvolve sistemas apenas com finalidade relacionada à operação de suas AR vinculadas.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC PRODEMGE RFB utiliza o Processo de Software Prodemge fundamentado nos modelos de referências: Unified Process – UP e Melhoria do Processo de Software Brasileiro – MPS.BR. Contém as abordagens: tradicional e ágil e utiliza os padrões de engenharia de software aplicáveis ao contexto da Prodemge. É iterativo, incremental, adaptativo, configurável e com foco na qualidade de software, possibilitando o desenvolvimento e a manutenção de software em diferentes plataformas tecnológicas.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC PRODEMGE RFB provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC PRODEMGE RFB.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC PRODEMGE RFB 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 PRODEMGE RFB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Antes de publicadas, todas as LCR geradas pela AC PRODEMGE RFB são cheçadas 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, LCR e OCSP

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC PRODEMGE RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1. Número de versão

Os certificados emitidos pela AC PRODEMGE RFB implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2. Extensões de certificado

7.1.2.1. Neste item, a PC descreve todas as extensões de certificado utilizadas pela AC PRODEMGE RFB e sua criticalidade.

7.1.2.2. Extensões Obrigatórias:

Os certificados emitidos pela AC PRODEMGE RFB obedecem a ICP-Brasil, que define como obrigatórias as seguintes extensões:

- a) **“Authority Key Identifier”, não crítica:** o campo *keyIdentifier* contém o hash SHA-1 da chave pública da AC PRODEMGE RFB;
- b) **“Key Usage”, crítica:** configurados conforme disposto no item 7.1.2.7 deste documento;
- c) **“Certificate Policies”, não crítica:** contém:
 - O OID desta PC: **2.16.76.1.2.1.23**;
 - Os campos *policyQualifiers* contém o endereço *web* da DPC AC PRODEMGE RFB:
http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_rfb/dpc_ac_prodemge_rfb.pdf;
- d) **“CRL Distribution Points”, não crítica:** contém os endereços *web* onde se obtém a LCR da AC PRODEMGE RFB:

Para certificados emitidos na AC Prodemge RFB G2:

<http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGERFBG2/LatestCRL.crl>
<http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGERFBG2/LatestCRL.crl>
<http://repositorio.icpbrasil.gov.br/lcr/RFB/ACPRODEMGERFBG2/LatestCRL>

Para certificados emitidos na AC Prodemge RFB G3:

<http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGERFBG3/LatestCRL.crl>
<http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGERFBG3/LatestCRL.crl>
<http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACPRODEMGERFBG3/LatestCRL.crl>

Para certificados emitidos na AC Prodemge RFB G4:

<http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGERFBG4/LatestCRL.crl>
<http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGERFBG4/LatestCRL.crl>

Para certificados emitidos na AC Prodemge RFB V1:

http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_rfb/lcr_ac_prodemge_rfb.crl
http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_rfb/lcr_ac_prodemge_rfb.crl

- e) **“Authority Information Access”, não crítica:** contém o endereço de acesso aos certificados da cadeia de certificação através do link:

Para certificados emitidos na AC Prodemge RFB G3:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_RFB_G3.p7c

Para certificados emitidos na AC Prodemge RFB G4:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_RFB_G4.p7c

e o endereço de acesso ao serviço de Consulta On-Line de Situação de Certificado (Online Certificate Status Protocol- OCSP):

Para certificados emitidos na AC Prodemge RFB G3:

<http://ocsp.certisign.com.br>

Para certificados emitidos na AC Prodemge RFB G4:
<http://ocsp-ac-prodemge-rfb.certisign.com.br>

Para certificados emitidos na AC Prodemge RFB V1:
http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_rfb/ac_prodemge_rfb.p7c

f) “**basicConstraints**”, **não crítica**: contém o campo `cA=False` (extensão definida como obrigatória pela AC PRODEMGE RFB).

7.1.2.3. Os certificados emitidos pela AC PRODEMGE RFB possuem 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 nesta ordem:

i. 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;

ii. 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;

iii. 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) campos `otherName`, não obrigatórios, contendo:

i. `rfc822Name` contendo o endereço e-mail do titular do certificado;

ii. OID = **1.3.6.1.4.1.311.20.2.3** e conteúdo = Nome Principal que contém o domínio de login em estações de trabalho (UPN)

a.3) 1 (um) campo `otherName`, obrigatório, para certificados vinculados à 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) 1 (um) campo `otherName`, obrigatório para certificados digitais emitidos para servidor público e militar, contendo:

OID = **2.16.76.1.3.11** e conteúdo = nas primeiras 10 (dez) posições, o cadastro único do servidor público da ativa e militares no âmbito da esfera estadual.

b) Para certificado de pessoa jurídica:

b.1) 4 (quatro) campos `otherName`, obrigatórios, contendo, nesta ordem:

i. 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;

ii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

iii. 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;

iv. 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.

b.2) campos *otherName*, não obrigatórios, contendo:

i. *rfc822Name* contendo o endereço e-mail do titular do certificado;

ii. OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo = Nome Principal que contém o domínio de login em estações de trabalho (UPN)

c) Não se aplica.

d) Não se aplica.

e) Não se aplica.

7.1.2.4. Os campos *otherName*, definidos como obrigatórios, 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, com exceção do campo UPN que possui uma cadeia de caracteres do tipo ASN.1 UTF8 STRING;

b) quando os números de NIS (PIS, PASEP ou CI), RG, 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/UF. O mesmo ocorre para o campo do município e UF se não houver número de inscrição do Título de Eleitor;

d) não se aplica;

e) todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidos 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 utilizados 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, com exceção do campo UPN que utiliza caracteres especiais;

h) O campo UPN é opcional, caso não seja usado o OID não é incluído no certificado.

7.1.2.5. Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos pela AC PRODEMGE RFB, podem ser utilizados com OID atribuídos ou aprovados pela AC-Raiz.

Campos *otherName* não obrigatórios quando não utilizados não terão seus OID incluídos no certificado.

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 devem obedecer os 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: deve conter 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, podendo implementar outros propósitos instituídos, desde que verificáveis e previstos pelas AC, em suas PC, em conformidade com a RFC 5280; e
- g) Não se aplica.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC PRODEMGE RFB são assinados com o uso do algoritmo RSA com SHA-1 como função de hash (OID 1.2.840.113549.1.1.5) na hierarquia V1, algoritmo RSA com SHA-256 como função de hash (OID 1.2.840.113549.1.1.11) ou algoritmo RSA com SHA-512 como função de hash (OID 1.2.840.113549.1.1.13) nas hierarquias V2 e V5 conforme o padrão PKCS#1.

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 certificado na hierarquia da Autoridade Certificadora Raiz Brasileira V5:

a) Para certificado de pessoa física (e-CPF):

C = BR

O = ICP-Brasil

OU = AC Prodemge RFB

OU = <CNPJ da AR onde ocorreu a validação presencial>

OU = Secretaria da Receita Federal do Brasil – RFB

OU = RFB e-CPF A1

OU = <Domínio do Certificado> (opcional)

CN = <Nome do titular do certificado>:< Número de inscrição no CPF >

Onde:

O campo Common Name (CN) é composto do nome da pessoa física, obtido do Cadastro de Pessoas Físicas (CPF) da RFB, com cumprimento máximo de 52 (cinquenta e dois) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da pessoa física do titular neste cadastro composto por 11 (onze) caracteres.

O campo Organizational Unit (OU) com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

O campo Organizational Unit (OU) com conteúdo variável, informando no campo domínio a identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for seu empregado, funcionário ou servidor. Caso esse OU não seja utilizado, o mesmo deverá ser grafado com o texto “EM BRANCO”.

b) Para certificado de pessoa jurídica (e-CNPJ):

C = BR

O = ICP-Brasil

ST = <Sigla da Unidade da Federação>

L = <Cidade>

OU = AC Prodemge RFB

OU = <CNPJ da AR onde ocorreu a validação presencial>

OU = RFB e-CNPJ A1

OU = Secretaria da Receita Federal do Brasil – RFB

CN = <Nome empresarial constante no cartão CNPJ>:<Número de inscrição no CNPJ>

Onde:

O campo Common Name (CN) é composto do nome empresarial da pessoa jurídica, obtido do Cadastro Nacional da Pessoa Jurídica (CNPJ) da RFB, com comprimento máximo de 49 (quarenta e nove) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.

O campo Organizational Unit (OU) com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

O campo locality (L) com conteúdo correspondente ao nome da cidade onde a empresa está localizada. O campo deve ser preenchido sem acentos nem abreviaturas.

O campo state or province name (ST) com conteúdo correspondente a sigla do estado onde a empresa está localizada.

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, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC PRODEMGE RFB são as seguintes:

- a) Não são admitidos sinais de acentuação, trema ou cedilhas;
 - i. Caracteres acentuados devem ser substituídos por seu correspondente sem acento;
 - ii. O cedilha deve ser substituído pelo caractere 'c'.

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

Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)
Branco	20	(28	:	3A

!	21)	29	;	3B
"	22	*	2A	=	3D
#	23	+	2B	?	3F
\$	24	,	2C	@	40
%	25	-	2D	\	5C
&	26	.	2E		
'	27	/	2F		

7.1.6.OID (Object Identifier) de Política de Certificado

O OID desta PC é 2.16.76.1.2.1.23.

Todo certificado emitido segundo essa PC (PC A1 da AC PRODEMGE RFB) contém o valor desse OID presente na extensão Certificate Policies.

7.1.7. Uso da extensão "Policy Constraints"

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Os campos "*policyQualifiers*" da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC PRODEMGE RFB:

Para certificados da cadeia AC Prodemge RFB G4:

http://icpbrasil.certisign.com.br/repositorio/dpc/AC_PRODEMGE_RFB/DPC_AC_PRODEMGE_RFB.pdf

Para certificados da cadeia V5 da AC Prodemge RFB V1:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_rfb/dpc_ac_prodemge_rfb.pdf

7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC PRODEMGE RFB 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 PRODEMGE RFB e sua criticalidade.

7.2.2.2. As LCR da AC PRODEMGE RFB obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

- Authority Key Identifier, não crítica:** contém o hash SHA-1 da chave pública da AC PRODEMGE RFB;
- CRL Number, não crítica:** contém um número sequencial para cada LCR emitida pela AC PRODEMGE RFB.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

A AC PRODEMGE RFB não implementa os serviços de respostas OCSP.

7.3.2. Extensões de OCSP

A AC PRODEMGE RFB não implementa os serviços de respostas OCSP.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

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 PRODEMGE RFB.

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

Qualquer alteração nesta PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC PRODEMGE RFB disponibiliza página específica com a versão corrente desta DPC para consulta pública, no endereço Web <https://www.prodemge.gov.br/>.

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

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 da AC PRODEMGE RFB foi submetida à aprovação, durante o processo de credenciamento da AC PRODEMGE RFB, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

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

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
[2]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01