Política de Certificado de SIGILO Tipo S3 da Autoridade Certificadora PRODEMGE MG

(PC S3 AC PRODEMGE MG)

OID: 2.16.76.1.2.103.14

Classificação: Pública

Versão 3.0

Agosto de 2021

prodemge

Companhia de Tecnologia
da Informação do Estado
de Minas Gerais

CONTROLE DE ALTERAÇÕES E VERSÕES

VERSÃO	DATA	RESOLUÇÃO QUE APROVOU A ALTERAÇÃO	ITEM ALTERADO	DESCRIÇÃO DA ALTERAÇÃO
1.0	07/06/2018	-	-	Versão inicial
1.1	25/01/2019	Resolução 150	7.1.4	Inclui no certificado digital o CNPJ da Autoridade de Registro onde ocorreu a identificação presencial.
1.2	22/05/2019	Resolução 121	6.1.4; 7.1.2.2	Acréscimo de endereço web de certificado e LCR
			7.1.2.3	Inclui a previsão de certificados para servidor público e militar
1.3	28/06/2019	Resolução 151	Vários	Adequações à Resolução
2.0	29/10/2020	Resolução 169	1.; 1.1.2; 1.1.3; 1.1.4; 1.1.5; 1.1.9; 1.2.1; 1.2.2; 1.3.2.1; 1.3.3; 1.3.5.1; 1.5.2; 1.5.3; 1.6; 6; 6.1.1.1; 6.1.1.3; 6.1.1.4; 6.1.1.6; 6.1.1.7; 6.1.1.8; 6.1.4; 6.1.5.2; 6.1.6; 6.2.1.2; 6.2.4.3; 6.3.2.1; 6.3.2.3; 7.1; 7.1.1; 7.1.2.1; 7.1.2.2; 7.1.2.3; 7.1.2.4; 7.1.2.5; 7.1.2.6; 7.1.2.7; 7.1.3; 7.1.4.1; 7.1.4; 7.1.5.1; 7.1.5.2; 7.1.6; 7.1.8; 7.2.2.2; 7.3.1; 7.3.2; 8;9.12.1; 9.12.2; 9.17; 10.1; 10.2	Adequações à Resolução, correções indicadas pelo ITI, ajustes de referências documentais, de tempos verbais e de *urls*
3.0	11/08/2021	Resolução 179	1; 1.1.1; 1.1.2; 1.1.3; 1.1.4; 1.1.5; 1.1.6; 1.1.7; 1.1.11; 1.1.12; 1.2.2; 1.3.5; 1.3.5.1; 1.6; 6.1.1.3; 6.1.1.4; 6.1.1.8; 6.1.5.2; 6.1.6; 6.2.1.2; 6.2.4.3; 6.8; 7.1.4.1; 7.1.5.2; 10.1; 10.2; 11	Revisão e consolidação do DOC-ICP-04, conforme Decreto nº 10.139, de 28 de novembro de 2019. Ajustes para emissão por meio de videoconferência.

SUMÁRIO

1. INTRODUÇÃO 10
1.1. Visão Geral 10
1.2. Nome do documento e Identificação 10
1.3. Participantes da ICP-Brasil 10
1.3.1. Autoridades Certificadoras 10
1.3.2. Autoridades de Registro 11
1.3.3. Titulares do Certificado 11
1.3.4. Partes Confiáveis 11
1.3.5. Outros Participantes 11
1.4. Usabilidade do Certificado 11
1.4.1. Uso apropriado do certificado 11
1.4.2. Uso proibitivo do certificado 12
1.5. Política de Administração 12
1.5.1. Organização administrativa do documento 12
1.5.2. Contatos 12
1.5.3. Pessoa que determina a adequabilidade da DPC com a PC 12
1.5.4. Procedimentos de aprovação da PC 12
1.6. Definições e Acrônimos 12
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 13
2.1. Repositórios 13
2.2. Publicação de informações dos certificados 13
2.3. Tempo ou Frequência de Publicação 13
2.4. Controle de Acesso aos Repositórios 13
3. IDENTIFICAÇÃO E AUTENTICAÇÃO 13
3.1. Nomeação 13
3.1.1. Tipos de nomes 13
3.1.2. Necessidade dos nomes serem significativos 13
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado 13
3.1.4. Regras para interpretação de vários tipos de nomes 13
3.1.5. Unicidade de nomes 14
3.1.6. Procedimento para resolver disputa de nomes 14
3.1.7. Reconhecimento, autenticação e papel de marcas registradas 14
3.2. Validação inicial de identidade 14
3.2.1. Método para comprovar a posse de chave privada 14
3.2.2. Autenticação da identificação da organização 14
3.2.3. Autenticação da identidade de equipamento ou aplicação 14
3.2.4. Autenticação da identidade de um indivíduo 14
3.2.5. Informações não verificadas do titular do certificado 14

3.2.6. Validação das autoridades 14
3.2.7. Critérios para interoperação 14
3.3. Identificação e autenticação para pedidos de novas chaves 14
3.3.1. Identificação e autenticação para rotina de novas chaves 14
3.3.2. Identificação e autenticação para novas chaves após a revogação 14
3.4. Identificação e Autenticação para solicitação de revogação 14
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 14
4.1. Solicitação do Certificado 14
4.1.1. Quem pode submeter uma solicitação de certificado 14
4.1.2. Processo de registro e responsabilidades 14
4.2. Processamento de Solicitação de Certificado 14
4.2.1. Execução das funções de identificação e autenticação 14
4.2.2. Aprovação ou rejeição de pedidos de certificado 14
4.2.3. Tempo para processar a solicitação de certificado 14
4.3. Emissão de Certificado 14
4.3.1. Ações da AC durante a emissão de um certificado 14
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado 14
4.4. Aceitação de Certificado 14
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 15
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades 15
4.8. Modificação de certificado 15
4.8.1. Circunstâncias para modificação de certificado 15

4.8.2. Quem pode requisitar a modificação de certificado 15
4.8.3. Processamento de requisição de modificação de certificado 15
4.8.4. Notificação de emissão de novo certificado para o titular 15
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado 15
4.8.6. Publicação de uma modificação de certificado pela AC 15
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 17
5.1.1. Construção e localização das instalações 17
5.1.2. Acesso físico 17
5.1.3. Energia e ar-condicionado 17
5.1.4. Exposição à água 17
5.1.5. Prevenção e proteção contra incêndio 17
5.1.6. Armazenamento de mídia 17
5.1.7. Destruição de lixo 17
5.1.8. Instalações de segurança (backup) externas (off-site) para AC 17
5.2. Controles Procedimentais 17

5.2.1. Perfis qualificados....17
5.2.2. Número de pessoas necessário por tarefa....17
5.2.3. Identificação e autenticação para cada perfil....17
5.2.4. Funções que requerem separação de deveres....17
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)....18
5.4.7. Notificação de agentes causadores de eventos....18
5.4.8. Avaliações de vulnerabilidade....18
5.5. Arquivamento de Registros....18
5.5.1. Tipos de registros arquivados....18
5.5.2. Período de retenção para arquivo....18
5.5.3. Proteção de arquivo....18
5.5.4. Procedimentos de cópia de arquivo....18
5.5.5. Requisitos para datação de registros....18
5.5.6. Sistema de coleta de dados de arquivo (interno e externo)....18
5.5.7. Procedimentos para obter e verificar informação de arquivo....18
5.6. Troca de chave....18
5.7. Comprometimento e Recuperação de Desastre....18
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento....18
5.7.2. Recursos computacionais, software, e/ou dados corrompidos....18
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade....18
5.7.4. Capacidade de continuidade de negócio após desastre....18
5.8. Extinção da AC....18
6. CONTROLES TÉCNICOS DE SEGURANÇA....18
6.1. Geração e Instalação do Par de Chaves....18
6.1.1. Geração do par de chaves....18
6.1.2. Entrega da chave privada à entidade titular do certificado....19
6.1.3. Entrega da chave pública para emissor de certificado....19

6.1.4. Entrega de chave pública da AC às terceiras partes 19
6.1.5. Tamanhos de chave 20
6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros 20
6.1.7. Propósitos de uso de chave (conforme o campo "*key usage*" na X.509 v3) 20
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico 20
6.2.1. Padrões e controle para módulo criptográfico 20
6.2.2. Controle "n de m" para chave privada 20
6.2.3. Custódia (*escrow*) de chave privada 20
6.2.4. Cópia de segurança de chave privada 21
6.2.5. Arquivamento de chave privada 21
6.2.6. Inserção de chave privada em módulo criptográfico 21
6.2.7. Armazenamento de chave privada em módulo criptográfico 21
6.2.8. Método de ativação de chave privada 21
6.2.9. Método de desativação de chave privada 21
6.2.10. Método de destruição de chave privada 21
6.3. Outros Aspectos do Gerenciamento do Par de Chaves 21
6.3.1. Arquivamento de chave pública 21
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada 22
6.4. Dados de Ativação 22
6.4.1. Geração e instalação dos dados de ativação 22
6.4.2. Proteção dos dados de ativação 22
6.4.3. Outros aspectos dos dados de ativação 22
6.5. Controles de Segurança Computacional 22
6.5.1. Requisitos técnicos específicos de segurança computacional 22
6.5.2. Classificação da segurança computacional 22
6.6. Controles Técnicos do Ciclo de Vida 22
6.6.1. Controles de desenvolvimento de sistema 22
6.6.2. Controles de gerenciamento de segurança 23
6.6.3. Controles de segurança de ciclo de vida 23
6.6.4. Controles na Geração de LCR 23
6.7. Controles de Segurança de Rede 23
6.8. Carimbo do Tempo 23
7. PERFIS DE CERTIFICADO, LCR e OCSP 23
7.1. Perfil do Certificado 23
7.1.1. Número de versão 23
7.1.2. Extensões de certificado 24
7.1.3. Identificadores de algoritmo 27
7.1.4. Formatos de nome 28
7.1.5. Restrições de nome 28
7.1.6. OID (Object Identifier) de Política de Certificado 29
7.1.7. Uso da extensão "*Policy Constraints*" 29
7.1.8. Sintaxe e semântica dos qualificadores de política 29

7.1.9. Semântica de processamento para as extensões críticas de PC 29
7.2. Perfil de LCR 29
7.2.1. Número(s) de versão 29
7.2.2. Extensões de LCR e de suas entradas 29
7.3. Perfil de OCSP 30
7.3.1. Número(s) de versão 30
7.3.2. Extensões de OCSP 30
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES 30
8.1. Frequência e circunstâncias das avaliações 30
8.2. Identificação/Qualificação do avaliador 30
8.3. Relação do avaliador com a entidade avaliada 30
8.4. Tópicos cobertos pela avaliação 30
8.5. Ações tomadas como resultado de uma deficiência 30
8.6. Comunicação dos resultados 30
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 30
9.1. Tarifas 30
9.1.1. Tarifas de emissão e renovação de certificados 30
9.1.2. Tarifas de acesso ao certificado 30
9.1.3. Tarifas de revogação ou de acesso à informação de status 31
9.1.4. Tarifas para outros serviços 31
9.1.5. Política de reembolso 31
9.2. Responsabilidade Financeira 31
9.2.1. Cobertura do seguro 31
9.2.2. Outros ativos 31
9.2.3. Cobertura de seguros ou garantia para entidades finais 31
9.3. Confidencialidade da informação do negócio 31
9.3.1. Escopo de informações confidenciais 31
9.3.2. Informações fora do escopo de informações confidenciais 31
9.3.3. Responsabilidade em proteger a informação confidencial 31
9.4. Privacidade da informação pessoal 31
9.4.1. Plano de privacidade 31
9.4.2. Tratamento de informação como privadas 31
9.4.3. Informações não consideradas privadas 31
9.4.4. Responsabilidade para proteger a informação privadas 31
9.4.5. Aviso e consentimento para usar informações privadas 31
9.4.6. Divulgação em processo judicial ou administrativo 31
9.4.7. Outras circunstâncias de divulgação de informação 31
9.5. Direitos de Propriedade Intelectual 31
9.6. Declarações e Garantias 31
9.6.1. Declarações e Garantias da AC 31
9.6.2. Declarações e Garantias da AR 31

9.6.3. Declarações e garantias do titular 31
9.6.4. Declarações e garantias das terceiras partes 31
9.6.5. Representações e garantias de outros participantes 31
9.7. Isenção de garantias 31
9.8. Limitações de responsabilidades 31
9.9. Indenizações 31
9.10. Prazo e Rescisão 32
9.10.1. Prazo 32
9.10.2. Término 32
9.10.3. Efeito da rescisão e sobrevivência 32
9.11. Avisos individuais e comunicações com os participantes 32
9.12. Alterações 32
9.12.1. Procedimento para emendas 32
9.12.2. Mecanismo de notificação e períodos 32
9.12.3. Circunstâncias na qual o OID deve ser alterado 32
9.13. Solução de conflitos 32
9.14. Lei aplicável 32
9.15. Conformidade com a Lei aplicável 32
9.16. Disposições Diversas 32
9.16.1. Acordo completo 32
9.16.2. Cessão 32
9.16.3. Independência de disposições 32
9.16.4. Execução (honorários dos advogados e renúncia de direitos) 32
9.17. Outras provisões 32
10. DOCUMENTOS REFERENCIADOS 33
11. REFERÊNCIAS BIBLIOGRÁFICAS 33

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento de "Políticas de Certificado" (PC) de Sigilo Tipo S3 da Autoridade Certificadora PRODEMGE MG, estabelece requisitos mínimos a serem obrigatoriamente observados pela AC PRODEMGE MG, integrante da 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 [6] do Comitê Gestor da ICP-Brasil e adota a mesma estrutura empregada nesse documento.

1.1.3. A estrutura desta PC está baseada na RFC 3647.

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

1.1.5. Esta PC se refere a Certificados de Sigilo para usuários finais do tipo S3.

1.1.6. Os tipos de certificados definem escalas de requisitos de segurança, nas quais o tipo S3 está associado aos requisitos mais rigorosos.

1.1.7. Certificados do tipo S3, de sigilo podem ser emitidos pela AC PRODEMGE MG para pessoas físicas, 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 Sigilo Tipo S3 da Autoridade Certificadora PRODEMGE MG" e referida como "PC S3 da AC PRODEMGE MG". Esta PC descreve os usos relacionados ao certificado de Sigilo correspondente ao tipo S3 no REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [6] do Comitê Gestor da ICP-Brasil. O OID (*object identifier*) desta PC é 2.16.76.1.2.103.14.

1.2.2. Após o processo de credenciamento da AC PRODEMGE MG foi atribuído a esta Política de Certificado de Sigilo S3 no âmbito da ICP-Brasil o seguinte OID: 2.16.76.1.2.103.14.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

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

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

1.3.2. Autoridades de Registro

1.3.2.1. . As Autoridades de Registro (AR) vinculadas à AC PRODEMGE MG, são responsáveis pelo processo de recebimento, validação e encaminhamento de solicitação de emissão ou revogação de certificados digitais e de identificação de seus solicitantes e seus dados estão publicados no endereço web da AC PRODEMGE MG https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2, conforme itens abaixo:

a) relação de todas as AR credenciadas;

b) relação de AR que tenham se descredenciado da cadeia da AC PRODEMGE MG, com respectiva data do descredenciamento.

1.3.3. Titulares do Certificado

Poderão ser titulares dos certificados emitidos pela AC PRODEMGE MG, segundo esta PC, as pessoas físicas e as pessoas jurídicas, de direito público ou privado, nacionais ou estrangeiras.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

A AC PRODEMGE MG publica em endereço web https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2 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 MG 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. Não se aplica.

1.4.1.5. Os certificados emitidos pela AC PRODEMGE MG no âmbito desta PC podem ser utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

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 MG

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) 3339-1213 / (31) 3339-1336 / (31) 3339-1283
Página web	wwws.prodemge.gov.br
E-mail geral:	acprodemge@prodemge.gov.br

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

Nome:	DANIELLE LEITE SANTANA CARRILHO
Área:	GCS – Gerência de Controle de Níveis de Serviço
Telefone:	(31) 3339-1213 / (31) 98462-0530
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 MG são estabelecidos a critério do CG da ICP-Brasil.

1.6. Definições e Acrônimos

Sigla	Descrição
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AGR	Agente de Registro
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CI	Cédula de Identidade
CN	*Common Name*
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro de Pessoa Física
CSP	*Cryptographic Service Provider*
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	*International Electrotechnical Commission*

Sigla	Descrição
IETF PKIX	*Internet Engineering Task Force - Public-Key Infrastructured (X.509)*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITI	Instituto Nacional de Tecnologia da Informação
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	Política de Certificado
PIS	Programa de Integração Social
Prodemge	Companhia de Tecnologia da Informação do Estado de Minas Gerais
PSBio	Prestador de Serviço Biométrico
PSC	Prestador 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 correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC PRODEMGE MG ou detalhados aspectos específicos para a PC, se houver.

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 correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC PRODEMGE MG ou detalhados aspectos específicos para a PC, se houver.

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 correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC PRODEMGE MG ou detalhados aspectos específicos para a PC, se houver.

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 correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC PRODEMGE MG ou detalhados aspectos específicos para a PC, se houver.

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

Nos itens seguintes, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São também definidos outros controles técnicos de segurança utilizados pela AC PRODEMGE MG e pelas ARs vinculadas na execução de suas funções operacionais.

6.1.1. Geração do par de chaves

6.1.1.1. Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração do par de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, a pessoa indicada por seu(s) representante(s) legal(is) será 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 ou componente disponibilizado pelo PSC envolvido na geração do par de chaves

Em quaisquer das situações, a geração do par de chaves criptográficas ocorre utilizando hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

6.1.1.3. O algoritmo utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA conforme definido no documento, PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL DOC-ICP-01.01 [1].

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL DOC-ICP-01.01 [2] é armazenada em Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO e com capacidade de geração de chave, sendo ativados e protegidos por senha e/ou identificação biométrica conforme definido para o tipo de certificado S3

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 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 modifica os dados a serem assinados, nem impede que estes dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8. O tipo de certificado emitido pela AC PRODEMGE MG e descrito nesta PC é o S3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
S3	Hardware criptográfico homologado junto à ICP-Brasil ou com certificação INMETRO

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

[1] Disponível no endereço https://www.gov.br/iti/pt-br/ e aprovado pela IN nº 4, de 18.05.2006
[2] Disponível no endereço https://www.gov.br/iti/pt-br/ e aprovado pela IN nº 4, de 18.05.2006

A AC PRODEMGE MG 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 MG:

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

Para certificados emitidos na AC Prodemge MG v2 até 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_mg/ac_prodemge_mg_v2.p7c

Para certificados emitidos na AC Prodemge MG v2 após 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_mg/ac_prodemge_mg_v2.p7b

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC PRODEMGE MG é de 2048 bits.

6.1.5.2. O algoritmo e o tamanho de chave utilizados no certificado Tipo S3 da ICP-Brasil estão definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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 em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

Os certificados têm ativados os bits *keyEncipherment* e *dataEncipherment*.

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 MG.

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 em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2. Controle "n de m" para chave privada

Não se aplica.

6.2.3. Custódia (*escrow*) de chave privada

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 MG 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 aprovado em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. 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 MG 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 MG 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. Não se aplica.

6.3.2.2. As chaves privadas de sigilo dos respectivos titulares de certificados emitidos pela AC 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 encriptações geradas durante o prazo de validade dos respectivos certificados.

6.3.2.3. O período máximo de validade admitido para certificados de Sigilo Tipo S3, segundo esta PC, é de 3 (três) anos.

6.3.2.4. Não se aplica.

6.3.2.5. Não se aplica.

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

Os dados de ativação 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 MG 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 C PRODEMGE MG 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 MG provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC PRODEMGE MG.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC PRODEMGE MG 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 MG 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 MG são checadas 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 do Tempo

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR e OCSP

Os itens seguintes especificam os formatos dos certificados e das LCR gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são obrigatoriamente atendidos no certificado do tipo S3 admitido no âmbito da ICP-Brasil.

7.1. Perfil do Certificado

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

7.1.2. Extensões de certificado

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

a) "*Authority Key Identifier*", não crítica;

b) "*Key Usage*", crítica;

c) "*Certificate Policies*", não crítica;

d) "*CRL Distribution Points*", não crítica;

e) "*Authority Information Access*", não crítica;

f) "*Basic Constraints*", não crítica (não obrigatório);

g) "*Subject Key Identifier*", não crítica (não obrigatório).

7.1.2.2. Extensões Obrigatórias:

Os certificados emitidos pela AC PRODEMGE MG 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 MG;

b) *"Key Usage"*, crítica: configurados conforme disposto no item 7.1.2.7 deste documento;

c) *"Certificate Policies"*, não crítica: contém o OID da PC correspondente e o endereço Web da DPC da AC que emite o certificado.

O OID desta PC: S3: 2.16.76.1.2.103.14

O campo *policyQualifiers* da extensão *"Certificate Policies"* contém o endereço web da DPC AC Prodemge MG:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_mg/dpc_ac_prodemge_mg.pdf

d) *"CRL Distribution Points"*, não crítica: contém 02 (dois) endereços na Web onde se obtém a LCR correspondente;

Para certificados emitidos na AC PRODEMGE MG:

http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_mg/lcr_ac_prodemge_mg.crl

http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_mg/lcr_ac_prodemge_mg.crl

Para certificados emitidos na AC PRODEMGE MG v2:

http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_mg/lcr_ac_prodemge_mg_v2.crl

http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_mg/lcr_ac_prodemge_mg_v2.crl

e) *"Authority Information Access"*, não crítica: Contém o método de acesso *id-ad-caIssuer*, utilizando o protocolo HTTP para a recuperação da cadeia de certificação.

Para certificados emitidos na AC PRODEMGE MG:

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

Para certificados emitidos na AC PRODEMGE MG v2 até 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_mg/ac_prodemge_mg_v2.p7c

Para certificados emitidos na AC PRODEMGE MG v2 após 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_mg/ac_prodemge_mg_v2.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 com o seguinte conteúdo = nas primeiras 8 (oito) posições, a data de nascimento da pessoa física titular do certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o número de inscrição no Cadastro de Pessoa Física (CPF) da pessoa física titular do certificado; nas 11 (onze) posições subsequentes, o número de Identificação Social da pessoa física titular do certificado - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG da pessoa física titular do certificado; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

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

OID = 2.16.76.1.3.5 com o seguinte conteúdo = nas primeiras 12 (onze) posições, o número de inscrição do Título de Eleitor da pessoa física titular do certificado; nas 3 (três) posições subsequentes, o número correspondente a Zona Eleitoral; nas 4 (quatro) posições seguintes, o número correspondente a Seção; nas 22 (vinte e duas) posições subsequentes, o nome do município e a UF do Título de Eleitor.

a.2) Não se aplica.

a.3) Não se aplica.

a.4) Não se aplica.

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

OID = 2.16.76.1.3.4 com o seguinte conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pela Pessoa Jurídica perante o CNPJ, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o número de inscrição no Cadastro de Pessoas Físicas (CPF) do responsável pela Pessoa Jurídica perante o CNPJ; nas 11 (onze) posições subsequentes o número de inscrição no NIS (PIS, PASEP ou CI) do responsável pela Pessoa Jurídica perante o CNPJ; nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do responsável pela Pessoa Jurídica perante o CNPJ; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF;

OID = 2.16.76.1.3.2 com o seguinte conteúdo = nome do responsável pela Pessoa Jurídica, perante o CNPJ;

OID = 2.16.76.1.3.3 com o seguinte conteúdo = número de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

OID = 2.16.76.1.3.7 com o seguinte conteúdo = nas 12 (doze) posições o número do Cadastro Especifico 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, 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;

Os seguintes campos são de preenchimento obrigatório;

Da pessoa física:

- Nome;
- CPF;
- Data de nascimento; e
- E-mail.

Da empresa:

- Nome Empresarial;
- Número de inscrição no CNPJ.

Do responsável pela pessoa jurídica perante o CNPJ:

- Número de inscrição no CPF;
- Data de nascimento;
- Nome do responsável pela Pessoa Jurídica perante o CNPJ.
- E-mail.

b) Quando os números de NIS (PIS/PASEP/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 ou o número de inscrição do Título de Eleitor não estiver disponível, não são

preenchidos os campos de órgão expedidor e UF ou os campos Zona Eleitoral, Sessão, Município e UF, respectivamente.

d) Não se aplica.

e) Todas informações de tamanho variável, referentes a números, tais como RG ou Título de Eleitor, 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 expedidor do RG e UF referem-se ao tamanho máximo e são 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. Não se aplica.

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

Para certificados de pessoa física:

O campo *rfc822Name*, parte da extensão obrigatória *"Subject Alternative Name"*, contendo o endereço e-mail do titular do certificado também deverá estar presente.

Para certificados de pessoa jurídica:

O campo *rfc822 Name*, parte da extensão obrigatória *"Subject Alternative Name"*, contendo o endereço e-mail do responsável, perante o CNPJ, pela Pessoa Jurídica titular do certificado também deverá estar presente.

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) Não se aplica.

g) para certificados de Sigilo: **"Key Usage", crítica**: somente os *bits keyEncipherment* e *dataEncipherment* ativados.

7.1.3. **Identificadores de algoritmo**

Os certificados emitidos pela AC PRODEMGE MG 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.

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, como exemplo, da seguinte forma:

Para pessoa Física

CN = nome do titular do certificado em certificado de pessoa física;

OU = Sigilo Tipo S3

OU = AC PRODEMGE MG V2

OU = CNPJ da AR que realizou a identificação

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

O = ICP-Brasil

C = BR

Para pessoa Jurídica

CN = contém o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ);

OU = Sigilo Tipo S3

OU = AC PRODEMGE MG V2

OU = CNPJ da AR que realizou a identificação

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

O = ICP-Brasil

C = BR

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. Não se aplica.

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

7.1.5. Restrições de nome

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

7.1.5.2. Os itens seguintes especificam os formatos dos certificados e das LCR gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são obrigatoriamente atendidos no certificado do tipo S3 admitido no âmbito da ICP-Brasil.

a) não são 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)	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 2.16.76.1.2.103.14.

7.1.7. Uso da extensão “*Policy Constraints*”

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

O campo *policyQualifiers* da extensão *“Certificate Policies”* contém o endereço web da DPC AC Prodemge MG:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_mg/dpc_ac_prodemge_mg.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 MG 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. A AC PRODEMGE MG adota as seguintes extensões de LCR:

a) *“Authority Key Identifier”*, não crítica;

b) *“CRL Number”*, não crítica;

c) *"Authority Information Access"*, não crítica (não obrigatório).

7.2.2.2. As LCR da AC PRODEMGE MG estão em conformidade com a ICP – Brasil:

a) *“Authority Key Identifier”*, não crítica: contém o *hash* SHA-1 da chave pública da AC Prodemge MG;

b) *“CRL Number”*, não crítica: contém um número sequencial para cada LCR emitida pela AC Prodemge MG.

c) *"Authority Information Access"*, não crítica (não obrigatório): Contém o método de acesso id-ad-

caIssuer, utilizando o protocolo HTTP para a recuperação da cadeia de certificação.

Para LCR emitidos na AC Prodemge MG:

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

Para LCR emitidos na AC Prodemge MG v2 até 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_mg/ac_prodemge_mg_v2.p7c

Para LCR emitidos na AC Prodemge MG v2 após 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_mg/ac_prodemge_mg_v2.p7b

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 correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC PRODEMGE MG.

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 correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC PRODEMGE MG.

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 é submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

A AC PRODEMGE MG disponibiliza página específica com a versão corrente desta PC para consulta pública, no endereço Web https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2

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

A primeira versão da PC S3 da AC PRODEMGE MG foi submetida à aprovação, durante o processo de credenciamento da AC PRODEMGE MG, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

Novas versões são igualmente submetidas à aprovação.

Como parte desse processo, além da conformidade da PC com o documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3], é também verificada a compatibilidade entre a PC e a DPC da AC PRODEMGE MG.

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 https://www.gov.br/iti/pt-br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL Aprovado pela Resolução nº 132, de 10 de novembro de 2017	DOC-ICP-17
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	DOC-ICP-03
[6]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12.12.2001	DOC-ICP-04

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.