

Política de Certificado de Sigilo Tipo S3 da Autoridade Certificadora PRODEMGE

PC S3 da AC PRODEMGE

Versão 6.1 - 10/10/2019

ÍNDICE

1. INTRODUÇÃO.....	9
1.1. VISÃO GERAL.....	9
1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO	10
1.3. PARTICIPANTES DA ICP-BRASIL.....	10
1.3.1. <i>Autoridades Certificadoras</i>	10
1.3.2. <i>Autoridades de Registro</i>	10
1.3.3. <i>Titulares do Certificado</i>	10
1.3.4. <i>Partes Confiáveis</i>	10
1.3.5. <i>Outros Participantes</i>	10
1.4. USABILIDADE DO CERTIFICADO	10
1.4.1 <i>Uso apropriado do certificado</i>	10
1.4.2 <i>Uso proibitivo do certificado</i>	11
1.5 POLÍTICA DE ADMINISTRAÇÃO	11
1.5.1 <i>Organização administrativa do documento</i>	11
1.5.2 <i>Contatos</i>	11
1.5.3 <i>Pessoa que determina a adequabilidade da DPC com a PC</i>	11
1.5.4 <i>Procedimentos de aprovação da PC</i>	11
1.6 DEFINIÇÕES E ACRÔNIMOS	12
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. <i>Tipos de nomes</i>	14
3.1.2. <i>Necessidade dos nomes serem significativos</i>	14
3.1.3. <i>Anonimato ou Pseudônimo dos Titulares do Certificado</i>	14
3.1.4. <i>Regras para interpretação de vários tipos de nomes</i>	14
3.1.5. <i>Unicidade de nomes</i>	14
3.1.6. <i>Procedimento para resolver disputa de nomes</i>	14
3.1.7. <i>Reconhecimento, autenticação e papel de marcas registradas</i>	14
3.2. VALIDAÇÃO INICIAL DE IDENTIDADE	14
3.2.1. <i>Método para comprovar a posse de chave privada</i>	14
3.2.2. <i>Autenticação da identificação da organização</i>	14
3.2.3. <i>Autenticação da identidade de equipamento ou aplicação</i>	14
3.2.4. <i>Autenticação da identidade de um indivíduo</i>	14
3.2.5. <i>Informações não verificadas do titular do certificado</i>	14
3.2.6. <i>Validação das autoridades</i>	14
3.2.7. <i>Critérios para interoperação</i>	14
3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES.....	14
3.3.1. <i>Identificação e autenticação para rotina de novas chaves</i>	14
3.3.2. <i>Identificação e autenticação para novas chaves após a revogação</i>	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. <i>Quem pode submeter uma solicitação de certificado</i>	14
4.1.2. <i>Processo de registro e responsabilidades</i>	14
4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO	14
4.2.1. <i>Execução das funções de identificação e autenticação</i>	14
4.2.2. <i>Aprovação ou rejeição de pedidos de certificado</i>	14
4.2.3. <i>Tempo para processar a solicitação de certificado</i>	14
4.3. EMISSÃO DE CERTIFICADO	14
4.3.1. <i>Ações da AC durante a emissão de um certificado</i>	14
4.3.2. <i>Notificações para o titular do certificado pela AC na emissão do certificado</i>	14
4.4. ACEITAÇÃO DE CERTIFICADO	14
4.4.1. <i>Conduta sobre a aceitação do certificado</i>	14
4.4.2. <i>Publicação do certificado pela AC</i>	14
4.4.3. <i>Notificação de emissão do certificado pela AC Raiz para outras entidades</i>	14
4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO	15
4.5.1. <i>Usabilidade da Chave privada e do certificado do titular</i>	15
4.5.2. <i>Usabilidade da chave pública e do certificado das partes confiáveis</i>	15
4.6. RENOVAÇÃO DE CERTIFICADOS	15
4.6.1. <i>Circunstâncias para renovação de certificados</i>	15
4.6.2. <i>Quem pode solicitar a renovação</i>	15
4.6.3. <i>Processamento de requisição para renovação de certificados</i>	15
4.6.4. <i>Notificação para nova emissão de certificado para o titular</i>	15
4.6.5. <i>Conduta constituindo a aceitação de uma renovação de um certificado</i>	15
4.6.6. <i>Publicação de uma renovação de um certificado pela AC</i>	15
4.6.7. <i>Notificação de emissão de certificado pela AC para outras entidades</i>	15
4.7. NOVA CHAVE DE CERTIFICADO	15
4.7.1. <i>Circunstâncias para nova chave de certificado</i>	15
4.7.2. <i>Quem pode requisitar a certificação de uma nova chave pública</i>	15
4.7.3. <i>Processamento de requisição de novas chaves de certificado</i>	15
4.7.4. <i>Notificação de emissão de novo certificado para o titular</i>	15
4.7.5. <i>Conduta constituindo a aceitação de uma nova chave certificada</i>	15
4.7.6. <i>Publicação de uma nova chave certificada pela AC</i>	15
4.7.7. <i>Notificação de uma emissão de certificado pela AC para outras entidades</i>	15
4.8. MODIFICAÇÃO DE CERTIFICADO	15
4.8.1. <i>Circunstâncias para modificação de certificado</i>	15
4.8.2. <i>Quem pode requisitar a modificação de certificado</i>	15
4.8.3. <i>Processamento de requisição de modificação de certificado</i>	15
4.8.4. <i>Notificação de emissão de novo certificado para o titular</i>	15
4.8.5. <i>Conduta constituindo a aceitação de uma modificação de certificado</i>	15
4.8.6. <i>Publicação de uma modificação de certificado pela AC</i>	15
4.8.7. <i>Notificação de uma emissão de certificado pela AC para outras entidades</i>	15
4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	15
4.9.1. <i>Circunstâncias para revogação</i>	15
4.9.2. <i>Quem pode solicitar revogação</i>	15
4.9.3. <i>Procedimento para solicitação de revogação</i>	15
4.9.4. <i>Prazo para solicitação de revogação</i>	15
4.9.5. <i>Tempo em que a AC deve processar o pedido de revogação</i>	15
4.9.6. <i>Requisitos de verificação de revogação para as partes confiáveis</i>	15
4.9.7. <i>Frequência de emissão de LCR</i>	15
4.9.8. <i>Latência máxima para a LCR</i>	15

4.9.9. Disponibilidade para revogação/verificação de status on-line	15
4.9.10. Requisitos para verificação de revogação on-line	15
4.9.11. Outras formas disponíveis para divulgação de revogação.....	15
4.9.12. Requisitos especiais para o caso de comprometimento de chave.....	15
4.9.13. Circunstâncias para suspensão.....	15
4.9.14. Quem pode solicitar suspensão	15
4.9.15. Procedimento para solicitação de suspensão.....	15
4.9.16. Limites no período de suspensão	15
4.10. SERVIÇOS DE STATUS DE CERTIFICADO	15
4.10.1. Características operacionais	15
4.10.2. Disponibilidade dos serviços	15
4.10.3. Funcionalidades operacionais.....	15
4.11. ENCERRAMENTO DE ATIVIDADES	15
4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVE.....	15
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.....	16
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade	16
5.3.2. Procedimentos de verificação de antecedentes	16
5.3.3. Requisitos de treinamento.....	16
5.3.4. Frequência e requisitos para reciclagem técnica.....	16
5.3.5. Frequência e sequência de rodízio de cargos	16
5.3.6. Sanções para ações não autorizadas.....	16
5.3.7. Requisitos para contratação de pessoal.....	16
5.3.8. Documentação fornecida ao pessoal.....	16
5.4. PROCEDIMENTOS DE LOG DE AUDITORIA.....	16
5.4.1. Tipos de eventos registrados	16
5.4.2. Frequência de auditoria de registros	16
5.4.3. Período de retenção para registros de auditoria.....	16
5.4.4. Proteção de registros de auditoria	16
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria	16
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo).....	16
5.4.7. Notificação de agentes causadores de eventos.....	16
5.4.8. Avaliações de vulnerabilidade	16

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	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.....	18
6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)	18
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.....	19
6.2.7. Armazenamento de chave privada em módulo criptográfico	19
6.2.8. Método de ativação de chave privada	19
6.2.9. Método de desativação de chave privada	19
6.2.10. Método de destruição de chave privada	19
6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	19
6.3.1. Arquivamento de chave pública	19
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada ..	19
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	20
6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL.....	20
6.5.1. Requisitos técnicos específicos de segurança computacional	20
6.5.2. Classificação da segurança computacional	20
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA	20
6.6.1. Controles de desenvolvimento de sistema.....	20
6.6.2. Controles de gerenciamento de segurança	20
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	21
7.1.1. Número de versão.....	21
7.1.2. Extensões de certificado	21
7.1.3. Identificadores de algoritmo.....	24
7.1.4. Formatos de nome	24
7.1.5. Restrições de nome.....	25
7.1.6. OID (Object Identifier) de Política de Certificado.....	26
7.1.7. Uso da extensão “Policy Constraints”.....	26
7.1.8. Sintaxe e semântica dos qualificadores de política	26
7.1.9. Semântica de processamento para as extensões críticas de PC.....	26
7.2. PERFIL DE LCR.....	26
7.2.1. Número(s) de versão.....	26
7.2.2. Extensões de LCR e de suas entradas.....	26
7.3. PERFIL DE OCSP	26
7.3.1. Número(s) de versão.....	26
7.3.2. Extensões de OCSP.....	26
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	26
8.1. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES.....	26
8.2. IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR.....	26
8.3. RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA	26
8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO.....	26
8.5. AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA.....	26
8.6. COMUNICAÇÃO DOS RESULTADOS	26
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS	26
9.1. TARIFAS.....	27
9.1.1. Tarifas de emissão e renovação de certificados	27
9.1.2. Tarifas de acesso ao certificado.....	27
9.1.3. Tarifas de revogação ou de acesso à informação de status.....	27
9.1.4. Tarifas para outros serviços.....	27
9.1.5. Política de reembolso.....	27
9.2. RESPONSABILIDADE FINANCEIRA	27
9.2.1. Cobertura do seguro	27
9.2.2. Outros ativos.....	27
9.2.3. Cobertura de seguros ou garantia para entidades finais	27
9.3. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO	27
9.3.1. Escopo de informações confidenciais	27
9.3.2. Informações fora do escopo de informações confidenciais	27
9.3.3. Responsabilidade em proteger a informação confidencial	27
9.4. PRIVACIDADE DA INFORMAÇÃO PESSOAL	27
9.4.1. Plano de privacidade.....	27
9.4.2. Tratamento de informação como privadas	27
9.4.3. Informações não consideradas privadas	27
9.4.4. Responsabilidade para proteger a informação privadas.....	27

9.4.5. Aviso e consentimento para usar informações privadas	27
9.4.6. Divulgação em processo judicial ou administrativo	27
9.4.7. Outras circunstâncias de divulgação de informação	27
9.5. DIREITOS DE PROPRIEDADE INTELECTUAL	27
9.6. DECLARAÇÕES E GARANTIAS	27
9.6.1. Declarações e Garantias da AC.....	27
9.6.2. Declarações e Garantias da AR.....	27
9.6.3. Declarações e garantias do titular.....	27
9.6.4. Declarações e garantias das terceiras partes.....	27
9.6.5. Representações e garantias de outros participantes	27
9.7. ISENÇÃO DE GARANTIAS.....	27
9.8. LIMITAÇÕES DE RESPONSABILIDADES	27
9.9. INDENIZAÇÕES	27
9.10. PRAZO E RESCISÃO	27
9.10.1. Prazo	27
9.10.2. Término.....	27
9.10.3. Efeito da rescisão e sobrevivência	27
9.11. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES.....	27
9.12. ALTERAÇÕES.....	27
9.12.1. Procedimento para emendas.....	27
9.12.2. Mecanismo de notificação e períodos	27
9.12.3. Circunstâncias na qual o OID deve ser alterado	28
9.13. SOLUÇÃO DE CONFLITOS.....	28
9.14. LEI APLICÁVEL	28
9.15. CONFORMIDADE COM A LEI APLICÁVEL	28
9.16. DISPOSIÇÕES DIVERSAS	28
9.16.1. Acordo completo.....	28
9.16.2. Cessão	28
9.16.3. Independência de disposições.....	28
9.16.4. Execução (honorários dos advogados e renúncia de direitos).....	28
9.17. OUTRAS PROVISÕES.....	28
10. DOCUMENTOS REFERENCIADOS	28

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
6.0	14/06/2019	Resolução 151	Vários	Adequação à resolução 151
6.1	10/10/2019	Não se aplica		Revisão no texto do documento

Política de Certificado de Sigilo Tipo S3 da Autoridade Certificadora PRODEMGE

1. INTRODUÇÃO

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

1.1. Visão Geral

1.1.1. Esta “Política de Certificado” (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo S3 da Autoridade Certificadora PRODEMGE na Infraestrutura de Chaves Públicas Brasileira.

1.1.2 A estrutura desta PC está baseada no DOC-ICP-04 – REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL[6].

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 Certificados do tipo T3 e T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.

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 sigilo Tipo S3 da Autoridade Certificadora PRODEMGE” e referida como “PC S3 da AC PRODEMGE”. Esta PC descreve os usos relacionados ao certificado de sigilo correspondente ao tipo S3 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O OID (object identifier) desta PC é 2.16.76.1.2.103.5.

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 no âmbito da ICP-Brasil.

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

1.3.2. Autoridades de Registro

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

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

1.3.3. Titulares do 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 relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC PRODEMGE e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC PRODEMGE (http://icp-brasil.certisign.com.br/repositorio/ac_prodemge.html).

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 nesta PC são adequados.

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

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

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

1.4.1.4 Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5 Certificados de tipos S1, S2, S3 e S4 serão 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 Certificados de tipos T3 e T4 serão utilizados em aplicações mantidas por autoridades de carimbo do tempo credenciadas na ICP-Brasil, para assinatura de carimbos do tempo.

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

Neste item estão incluídos nome, endereço e outras informações da AC PRODEMGE, assim como são informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC: Companhia de Tecnologia da Informação do Estado de Minas Gerais - PRODEMGE

1.5.2 Contatos

Endereço: Rua da Bahia 2277 – Bairro de Lourdes – Belo Horizonte - MG
30160-012

Telefone: (31) 3237-3424 (31) 3339-1245

Página web: http://icp-brasil.certisign.com.br/repositorio/ac_prodemge.html

E-mail: gor@prodemge.gov.br goc@prodemge.gov.br

Outros:

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: Jacira dos Reis Xavier

Área: SCD - SUPERINTENDÊNCIA DE CERTIFICAÇÃO DIGITAL

Telefone: (31) 3237-3424 (31) 3339-1245

E-mail: gor@prodemge.gov.br goc@prodemge.gov.br

Outros:

1.5.4 Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.

Os procedimentos de aprovação desta PC da AC PRODEMGE 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
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation
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	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão

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.

- 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.

- 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.

- 4.1. Solicitação do certificado**
 - 4.1.1. Quem pode submeter uma solicitação de certificado**
 - 4.1.2. Processo de registro e responsabilidades**
- 4.2. Processamento de Solicitação de Certificado**
 - 4.2.1. Execução das funções de identificação e autenticação**
 - 4.2.2. Aprovação ou rejeição de pedidos de certificado**
 - 4.2.3. Tempo para processar a solicitação de certificado**
- 4.3. Emissão de Certificado**
 - 4.3.1. Ações da AC durante a emissão de um certificado**
 - 4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado**
- 4.4. Aceitação de Certificado**
 - 4.4.1. Conduta sobre a aceitação do certificado**
 - 4.4.2. Publicação do certificado pela AC**
 - 4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades**

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

5.1. Controles físicos

5.1.1. Construção e localização das instalações

5.1.2. Acesso físico

5.1.3. Energia e ar-condicionado

5.1.4. Exposição à água

5.1.5. Prevenção e proteção contra incêndio

5.1.6. Armazenamento de mídia

5.1.7. Destruição de lixo

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

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.2. Número de pessoas necessário por tarefa

5.2.3. Identificação e autenticação para cada perfil

5.2.4. Funções que requerem separação de deveres

5.3. Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2. Procedimentos de verificação de antecedentes

5.3.3. Requisitos de treinamento

5.3.4. Frequência e requisitos para reciclagem técnica

5.3.5. Frequência e sequência de rodízio de cargos

5.3.6. Sanções para ações não autorizadas

5.3.7. Requisitos para contratação de pessoal

5.3.8. Documentação fornecida ao pessoal

5.4. Procedimentos de Log de Auditoria

5.4.1. Tipos de eventos registrados

5.4.2. Frequência de auditoria de registros

5.4.3. Período de retenção para registros de auditoria

5.4.4. Proteção de registros de auditoria

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

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

5.4.7. Notificação de agentes causadores de eventos

5.4.8. Avaliações de vulnerabilidade

5.5. Arquivamento de Registros

5.5.1. Tipos de registros arquivados

5.5.2. Período de retenção para arquivo

5.5.3. Proteção de arquivo

5.5.4. Procedimentos de cópia de arquivo

5.5.5. Requisitos para datação de registros

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

5.5.7. Procedimentos para obter e verificar informação de arquivo

5.6. Troca de chave

5.7. Comprometimento e Recuperação de Desastre

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

5.7.2. Recursos computacionais, software, e/ou dados corrompidos

5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4. Capacidade de continuidade de negócio após desastre

5.8. Extinção da AC

6. CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1. Não se aplica.

6.1.1.1.2. Não se aplica.

6.1.1.2. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante apresentados pelo browser .

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 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[1].

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[1]. As chaves privadas correspondentes aos certificados deverão ser armazenadas 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. No caso de uso de PSC há a proteção utilizando recurso $m \times n$.

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; e

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

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

6.1.1.8. O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17[4], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC PRODEMGE, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

O tipo de certificado emitido pela AC PRODEMGE 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

Nota: para certificados do tipo A CF-e-SAT, T3 e T4, a exigência de homologação ou certificação das mídias para geração e armazenamento de chaves criptográficas fica suspensa até ulterior deliberação do Comitê-Gestor da ICP-Brasil.

6.1.2. Entrega da chave privada à entidade

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 SSL - Secure Socket Layer.

6.1.4. Entrega de chave pública da AC às terceiras partes

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

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G3.p7c (para cadeia V2) e

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G4.p7c (para cadeia V5).

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC PRODEMGE 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 S3 da ICP-Brasil está em conformidade com o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

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

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

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

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, a PC define os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos pela AC PRODEMGE.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão de homologação ICP-Brasil ou Certificação INMETRO.

6.2.1.2. Os requisitos aplicáveis ao módulo criptográfico utilizado para geração de chaves criptográficas dos titulares de certificado segue os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.2.2. Controle “n de m” para chave privada

Não se aplica.

6.2.3. Custódia (escrow) de chave privada

A AC não realiza 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 do certificado a seu critério, poderá manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC PRODEMGE não mantém cópia de segurança de chave privada de titular de certificado de sigilo 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. Não se aplica.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC PRODEMGE não arquivava cópias de chaves privadas de sigilo 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

Não se aplica.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

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

6.2.10. Método de destruição de chave privada

O titular do 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 sigilo e as LCR emitidas pela AC PRODEMGE permanecem armazenadas após a expiração dos correspondentes certificados, permanentemente, na forma da legislação em vigor .

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 da AC PRODEMGE é de 5 (cinco) anos.

6.3.2.4. O período máximo de validade dos Certificados de Assinatura de Código será de até 39 (trinta e nove) meses, conforme princípios e critérios Webtrust.

6.3.2.5. O período máximo de validade dos Certificados SSL/TLS será de até 825 (oitocentos e vinte cinco) dias, conforme princípios e critérios Webtrust.

6.4. Dados de Ativação

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

6.4.1. Geração e instalação dos dados de ativação

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

6.4.2. Proteção dos dados de ativação

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

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade.

O equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados possui conexão com o dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves.

6.5.2. Classificação da segurança computacional

Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

A AC PRODEMGE 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 utiliza os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC PRODEMGE utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos.

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

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC PRODEMGE 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 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 LCRs geradas pela AC PRODEMGE 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 de Tempo

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL[5].

7. PERFIS DE CERTIFICADO, LCR E OCSP

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

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC PRODEMGE 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 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 e sua criticalidade.

7.1.2.2. A ICP-Brasil 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;
- 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: 2.16.76.1.2.103.5;
 - Os campos policyQualifiers contém o endereço *Web* da DPC AC PRODEMGE: http://icp-brasil.certisign.com.br/repositorio/dpc/AC_PRODEMGE/DPC_AC_PRODEMGE.pdf;Certificados de assinatura de código (Code Signing) e de autenticação de servidor (SSL/TLS) contem ainda o OID da política de certificado de identificação dos requisitos do CA/B Forum Guidelines (2.23.140.1.1, se EV SSL; 2.23.140.1.2.2, se OV SSL; 2.23.140.1.3, se EV Code Signing; e 2.23.140.1.4.1, se Baseline Requirement Code Signing);
- d) **CRL Distribution Points**, não crítica: contém os endereços Web onde se obtém a LCR da AC PRODEMGE: Para certificados emitidos na G3:
<http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGE3/LatestCRL.crl>

<http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGE3/LatestCRL.crl>

<http://repositorio.icpbrasil.gov.br/lcr/Certisign/ACPRODEMGE3/LatestCRL.crl>

Para certificados emitidos na G4:

<http://icp-brasil.certisign.com.br/repositorio/lcr/ACPRODEMGE4/LatestCRL.crl>

<http://icp-brasil.outralcr.com.br/repositorio/lcr/ACPRODEMGE4/LatestCRL.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 G3:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G3.p7c

Para certificados emitidos na G4:

http://icp-brasil.certisign.com.br/repositorio/certificados/AC_PRODEMGE_G4.p7c

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

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

a) Para certificado de pessoa física:

a.1) 4 (quatro) campos otherName, obrigatórios, contendo:

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;

iv. campo rfc822Name contendo o endereço e-mail do titular do certificado.

a.2) campos otherName, não obrigatórios, contendo:

b) Para certificado de pessoa jurídica:

b.1) 5 (cinco) campos otherName, obrigatórios, contendo:

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;

v. campo rfc822Name contendo o endereço e-mail do titular do certificado.

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

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

e) Todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidas com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível;

f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, sendo utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

g) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais, com exceção do campo UPN que utiliza caracteres especiais
CPF e data de nascimento é obrigatório;

7.1.2.5. Campos otherName adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos pela AC PRODEMGE, 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 obedecem os propósitos de uso e a criticalidade conforme descrição abaixo :

a) para certificados de Assinatura de Código (codeSigning):

“Key Usage”, crítica: somente o bit digitalSignature está ativado;

“Extended Key Usage”, não crítica: somente o codeSigning OID = 1.3.6.1.5.5.7.3.3 está presente;

b) para certificados de Autenticação de Servidor (SSL/TLS):

“Key Usage”, crítica: somente os bits digitalSignature, keyEncipherment ou keyAgreement estão ativados;

“Extended Key Usage”, não crítica: contem o propósito server authentication OID = 1.3.6.1.5.5.7.3.1. Pode conter o propósito client authentication OID = 1.3.6.1.5.5.7.3.2;

c) para certificados de Assinatura de Carimbo do Tempo:

“Key Usage”, crítica: somente os bits digitalSignature e nonRepudiation estão ativados;

"Extended Key Usage", crítica: somente o propósito timeStamping OID = 1.3.6.1.5.5.7.3.8 está presente nos certificados de equipamentos de carimbo do tempo de ACT credenciada na ICP-Brasil. Esse OID não deve ser empregado em qualquer outro tipo de certificado;

d) para certificados de Assinatura A CF-e-SAT:

"Key Usage", crítica: contem o bit digitalSignature ativado, podendo conter os bits keyAgreement e nonRepudiation ativados;

"Extended Key Usage", não crítica: somente o propósito client authentication OID = 1.3.6.1.5.5.7.3.2 está presente;

e) para certificados de Assinatura de Resposta OCSP:

"Key Usage", crítica: contem o bit digitalSignature ativado, podendo conter o bit nonRepudiation ativado;

"Extended Key Usage", não crítica: somente o propósito OCSPSigning OID = 1.3.6.1.5.5.7.3.9 está presente;

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

"Key Usage", crítica: contem 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 está ativado, podendo implementar outros propósitos instituídos, desde que verificáveis e previstos nesta PC, em conformidade com a RFC 5280; e

g) para certificados de Sigilo:

"Key Usage", crítica: somente os bits keyEncipherment e dataEncipherment estão ativados.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC PRODEMGE 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:

C = BR

O = ICP-Brasil

OU = AC PRODEMGE

OU = <CNPJ da AR>

OU = identificador (indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou sequência alfanumérica)

CN = nome do titular do certificado

Onde:

O "Distinguished Name" (DN) pode apresentar até sete campos "OU". Caso qualquer um dos campos OU não seja utilizado, o mesmo terá grafado o texto "(em branco)" ou não será apresentado no DN.

Em um certificado de pessoa jurídica, o identificador CN contém a denominação da razão social correspondente.

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

O campo OU = <CNPJ da AR> indica o CNPJ da AR que realizou a identificação presencial, que será preenchido com 14 (quatorze) posições, sem caracteres como “.”, “/” ou “-”.

O Campo E (endereço e-mail do titular do certificado) deixou de compor o “Distinguished Name” (DN) a partir da implementação da cadeia V5.

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 são as seguintes:

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

b) além dos caracteres alfanuméricos, são utilizados somente os seguintes caracteres especiais:

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

@	40
\	5C

7.1.6. OID (Object Identifier) de Política de Certificado

O OID desta PC é 2.16.76.1.2.103.5.

Todo certificado emitido segundo essa PC, PC S3 AC PRODEMGE, 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

O campo policyQualifiers da extensão “Certificate Policies” contém o endereço web da DPC da AC PRODEMGE (http://icp-brasil.certisign.com.br/repositorio/dpc/AC_PRODEMGE/DPC_AC_PRODEMGE.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 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 e sua criticalidade.

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

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

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

A AC PRODEMGE não implementa os serviços de respostas OCSP.

7.3.2. Extensões de OCSP

A AC PRODEMGE não implementa os serviços de respostas OCSP.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

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

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.

9.1. Tarifas

- 9.1.1. Tarifas de emissão e renovação de certificados
- 9.1.2. Tarifas de acesso ao certificado
- 9.1.3. Tarifas de revogação ou de acesso à informação de status
- 9.1.4. Tarifas para outros serviços
- 9.1.5. Política de reembolso

9.2. Responsabilidade Financeira

- 9.2.1. Cobertura do seguro
- 9.2.2. Outros ativos
- 9.2.3. Cobertura de seguros ou garantia para entidades finais

9.3. Confidencialidade da informação do negócio

- 9.3.1. Escopo de informações confidenciais
- 9.3.2. Informações fora do escopo de informações confidenciais
- 9.3.3. Responsabilidade em proteger a informação confidencial

9.4. Privacidade da informação pessoal

- 9.4.1. Plano de privacidade
- 9.4.2. Tratamento de informação como privadas
- 9.4.3. Informações não consideradas privadas
- 9.4.4. Responsabilidade para proteger a informação privadas
- 9.4.5. Aviso e consentimento para usar informações privadas
- 9.4.6. Divulgação em processo judicial ou administrativo
- 9.4.7. Outras circunstâncias de divulgação de informação

9.5. Direitos de Propriedade Intelectual

9.6. Declarações e Garantias

- 9.6.1. Declarações e Garantias da AC
- 9.6.2. Declarações e Garantias da AR
- 9.6.3. Declarações e garantias do titular
- 9.6.4. Declarações e garantias das terceiras partes
- 9.6.5. Representações e garantias de outros participantes

9.7. Isenção de garantias

9.8. Limitações de responsabilidades

9.9. Indenizações

9.10. Prazo e Rescisão

- 9.10.1. Prazo
- 9.10.2. Término
- 9.10.3. Efeito da rescisão e sobrevivência

9.11. Avisos individuais e comunicações com os participantes

9.12. Alterações

9.12.1. Procedimento para emendas

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC PRODEMGE. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

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

9.12.2. Mecanismo de notificação e períodos

A AC PRODEMGE mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web http://icp-brasil.certisign.com.br/repositorio/pc/AC_PRODEMGE/PC_S3_AC_PRODEMGE_v6.1.pdf.

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 PRODEMGE 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 foi submetida à aprovação, durante o processo de credenciamento da AC PRODEMGE, 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
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[6]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

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

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