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

(PC A1 AC PRODEMGE SSL)

OID: 2.16.76.1.2.1.95

Classificação: Pública

Versão 2.0

Outubro de 2020

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.
		Resolução 128	7.1.2.3c	Aprova a obrigatoriedade de implementação da extensão Subject Alternative Name Para Certificados do Tipo SSL/TLS.
1.2	22/05/2019	Resolução 121	6.1.4; 7.1.2.2	Acréscimo de endereço web de certificado e LCR
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; 1.1.10; 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; 6.1.1.8; 6.1.5.2; 6.1.4; 6.1.6; 6.1.7; 6.2.1.2; 6.2.4.3; 6.3.2.1; 6.3.2.3; 6.3.2.5; 6.6.4; 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; 7.1.4.4; 7.1.4; 7.1.5.1; 7.1.5.2; 7.1.6; 7.1.8; 7.2.1; 7.2.2.1; 7.2.2.2; 7.3.2; 8; 9; 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

SUMÁRIO

1. INTRODUÇÃO

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

1.1. Visão Geral

1.1.1. Este documento descreve as "Políticas de Certificado" (PC) de Assinatura Digital Tipo A1 da Autoridade Certificadora PRODEMGE SSL (AC PRODEMGE SSL), na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

1.1.2. A estrutura desta PC está baseada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [6] do Comitê Gestor da ICP-Brasil.

1.1.3. Esta PC se refere a Certificados de Assinatura Digital para autenticação de servidor do tipo A1.

1.1.4. Não se aplica.

1.1.5. Não se aplica.

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.1.8. Não se aplica

1.1.9. Não se aplica.

1.1.10. Para certificados com propósito de uso EV SSL é observado o disposto no documento *EV SSL Guidelines.*

1.2. Nome do documento e Identificação

1.2.1. 1.2.1. Esta PC é chamada "Política de Certificado de assinatura digital Tipo A1 da Autoridade Certificadora PRODEMGE SSL" e referida como "PC A1 da AC PRODEMGE SSL". Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A1 no REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [6] do Comitê Gestor da ICP-Brasil. O OID (*object identifier*) desta PC é 2.16.76.1.2.1.95.

1.2.2. Após o processo de credenciamento da AC PRODEMGE SSL foi atribuído a esta Política de Certificação A1 no âmbito da ICP-Brasil o seguinte OID: 2.16.76.1.2.1.95.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

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

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

1.3.2. Autoridades de Registro

As Autoridades de Registro (AR) vinculadas à AC PRODEMGE SSL, 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 SSL https://wwws.prodemge.gov.br/informacoes/sobre-a-ac-prodemge-2, conforme itens abaixo:

a) relação de todas as AR credenciadas;

b) relação das AR que tenham se descredenciadas da cadeia da AC PRODEMGE SSL, com respectiva data do descredenciamento.

1.3.3. Titulares do Certificado

Poderão ser titulares dos certificados emitidos pela AC PRODEMGE SSL, segundo esta PC, 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

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

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

1.4.1.5. Não se aplica.

1.4.1.6. Não se aplica.

1.4.1.7. Não se aplica.

1.4.1.8. Não se aplica.

1.4.2. Uso proibitivo do certificado

Não se aplica.

1.5. Política de Administração

1.5.1. Organização administrativa do documento

AC PRODEMGE SSL

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
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 SSL são estabelecidos a critério do CG da ICP-Brasil.

1.6. Definições e Acrônimos

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

Acrônimo e Sigla	Descrição
CSP	*Cryptographic Service Provider*
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation*
FCT	Fonte Confiável de Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITI	Instituto Nacional de Tecnologia da Informação
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institute of Standards and Technology
OCSP	*Online Certificate Status Protocol*
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCI	Política de Classificação de Informação
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
PJ	Pessoa Jurídica
POP	Proof of Possession
PRD	Plano de Recuperação de Desastres
Prodemge	Companhia de Tecnologia da Informação do Estado de Minas Gerais
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
RIC	Registro de Identidade Civil
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
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 SSL.

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 SSL.

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 SSL.

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

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

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, 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 SSL 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. Sendo o titular de certificado 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 e, quando da geração, a chave privada é armazenada no HD da estação.

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

6.1.1.3. O algoritmo 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 é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1] e é armazenada em repositório protegido por senha e/ou identificação biométrica, cifrado por software, conforme definido para o tipo de certificado A1.

6.1.1.5. A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

6.1.1.6. A mídia de armazenamento da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada 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 CODESIGNING e descrito nesta PC é o A1.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software

6.1.2. Entrega da chave privada à entidade titular do certificado

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

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

6.1.4. Entrega de chave pública da AC às terceiras partes

A AC PRODEMGE SSL 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 SSL:

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

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

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7c

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

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7b

6.1.5. Tamanhos de chave

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

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A1 da ICP-Brasil estão definidos 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 e verificação de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido 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 *digitalSignature* e *keyEncipherment*.

Os pares de chaves correspondentes aos certificados emitidos pela AC PRODEMGE SSL podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves.

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

Nos itens seguintes são referidos os requisitos para a proteção das chaves dos titulares de certificados emitidos pela AC PRODEMGE SSL.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. Não se aplica.

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

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 SSL 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 pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICPBRASIL [1] 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 SSL 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 emitidos pela AC PRODEMGE SSL permanecem armazenadas após a expiração dos correspondentes certificados, permanentemente, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

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

6.3.2.1. As chaves privadas de assinatura dos respectivos titulares de certificados emitidos pela AC PRODEMGE SSL são utilizadas durante todo o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante tudo o período de tempo determinado pela legislação aplicável, para verificação das assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. O período máximo de validade admitido para certificados Tipo A1 é de 1 (um) ano.

6.3.2.4. Não se aplica.

6.3.2.5. O período máximo de validade dos Certificados SSL, segundo esta PC, é de 12 (doze) meses, conforme princípios e critérios Webtrust.

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 SSL 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 SSL 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 SSL provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC PRODEMGE SSL.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC PRODEMGE SSL 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 SSL 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 SSL 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. Controles de Engenharia do Módulo Criptográfico

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC PRODEMGE SSL, 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 SSL 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 SSL 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 SSL 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 SSL;

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 A1: 2.16.76.1.2.1.95

O campo *policyQualifiers* da extensão "*Certificate Policies*" contêm o endereço web da DPC AC PRODEMGE SSL:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_ssl/dpc_ac_prodemge_ssl.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 SSL:

http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_ssl/lcr_ac_prodemge_ssl.crl

http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_ssl/lcr_ac_prodemge_ssl.crl

Para certificados emitidos na AC PRODEMGE SSL v2:

http://icp-brasil.ac.prodemge.gov.br/repositorio/lcr/ac_prodemge_ssl/lcr_ac_prodemge_ssl_v2.crl

http://icp-brasil2.acprodemge.com.br/repositorio/lcr/ac_prodemge_ssl/lcr_ac_prodemge_ssl_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 SSL:

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

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

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7c

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

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7b

A segunda entrada contém o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, utilizando o protocolo de acesso HTTP, para certificados de autenticação de servidor (SSL/TLS).

Para certificados emitidos na AC PRODEMGE SSL:

http://ocsp-ac-prodemge-ssl.ac.prodemge.gov.br

Para certificados emitidos na AC PRODEMGE SSL v2:

http://ocsp-ac-prodemge-ssl-v2.ac.prodemge.gov.br

7.1.2.3. Os certificados emitidos pela AC PRODEMGE SSL possuem a extensão *"Subject Alternative Name"*, **não crítica** e com os seguintes formatos:

a) Não se aplica.

b) Não se aplica.

c) Para certificado de equipamento ou aplicação:

c.1) 4 (quatro) campos *otherName*, obrigatórios, contendo, nesta ordem:

OID = 2.16.76.1.3.8 com o seguinte conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;

OID = 2.16.76.1.3.3 com o seguinte conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;

OID = 2.16.76.1.3.2 com o seguinte conteúdo = nome do responsável pelo certificado;

OID = 2.16.76.1.3.4 com o seguinte conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

c.2) Para certificados do tipo SSL/TLS, Campo *dNSName*, obrigatório, contém um ou mais domínios pertencentes ou controlados pelo titular, seguindo as regras definidas na RFC 5280 e RFC 2818, em conformidade com os princípios e critérios WebTrust.

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;

<u>Da empresa:</u>

- Nome Empresarial;
- Número de inscrição no CNPJ.

<u>Do responsável pela pessoa jurídica perante o CNPJ:</u>

- 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. Não se aplica.

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) Não se aplica.

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

"Key Usage", crítica: somente os bits *digitalSignature*, *keyEncipherment* ativos;

"Extended Key Usage", não crítica: contém o propósito *server authentication OID* = 1.3.6.1.5.5.7.3.1 e o propósito *client authentication OID* = 1.3.6.1.5.5.7.3.2;

c) Não se aplica.

d) Não se aplica.

e) para certificados de Assinatura de Resposta OCSP:

"Key Usage", crítica: contém o bit *digitalSignature* ativado;

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

f) Não se aplica.

g) Não se aplica.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC PRODEMGE SSL 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. Não se aplica.

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. O certificado digital emitido para autenticação de servidor (SSL/TLS) adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

CN = este campo contém um único nome de domínio pertencente ou controlado pelo titular

SERIALNUMBER (OID 2.5.4.5) = CNPJ

OU = Assinatura Tipo A1

OU = AC PRODEMGE SSL V2

OU = CNPJ da AR que realizou a identificação presencial; ou CNPJ da AR cujo AGR operou videoconferência para emissão do certificado; ou, ainda, a expressão "Renovação Eletrônica", para os casos de renovação online com certificado digital válido

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

O = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

Business Category (OID 2.5.4.15) = tipo de categoria comercial, devendo conter: "*Private Organization*" ou "*Government Entity*" ou "*Business Entity*" ou "*NonCommercial Entity*"

Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR

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

ST = com conteúdo correspondente a sigla do estado onde a empresa está localizada.

C = BR

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. Todas as sequências de caracteres nos certificados, inclusive as dos DN (*Distinguished Name*) obedecem ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela abaixo. Os acentos não são suportados e são substituídos pelo caractere não acentuado e o cedilha pelo caractere 'c'.

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

7.1.6. OID (*Object Identifier*) de Política de Certificado

O OID desta PC é 2.16.76.1.2.1.95.

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 SSL:

http://icp-brasil.ac.prodemge.gov.br/repositorio/dpc/ac_prodemge_ssl/dpc_ac_prodemge_ssl.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 SSL, segundo esta PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. A AC PRODEMGE SSL 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 SSL estão em conformidade com a ICP – Brasil:

a) ***"Authority Key Identifier"***, **não crítica**: contém o *hash* SHA-1 da chave pública da AC PRODEMGE SSL;

b) ***"CRL Number", não crítica***: contém um número sequencial para cada LCR emitida pela AC PRODEMGE SSL.

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 pela AC PRODEMGE SSL até 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7c

Para LCR emitidos na AC PRODEMGE SSL após 26/06/2020:

http://icp-brasil.ac.prodemge.gov.br/repositorio/certificado/ac_prodemge_ssl/ac_prodemge_ssl_v2.p7b

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

A AC PRODEMGE SSL implementa serviços de respostas OCSP na versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP

Em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

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

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 SSL.

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 SSL 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

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 A1 da AC PRODEMGE SSL foi submetida à aprovação, durante o processo de credenciamento da AC PRODEMGE SSL, 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 SSL.

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 CONFIANÇADA 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 ICPBRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01