COMPANHIA DE PROCESSAMENTO DE DADOS DO ESTADO DE SÃO PAULO- PRODESP

(AC PRODESP)

POLÍTICA DE CERTIFICADO DE SIGILO

== TIPO S1 ==

VERSÃO 1.0 – 13/10/2021

CONTROLE DE ALTERAÇÕES

Data	*Versão*	*Observações*
13/10/2021	1.0	Redação Inicial

AVISO LEGAL

Sumário

1. INTRODUÇÃO 6
1.1. Visão Geral 6
1.2. Nome do Documento e Identificação 6
1.3. Participantes da ICP-Brasil 6
13.1 Autoridades Certificadoras 6
1.4. Usabilidade do Certificado 7
1.5. Política de Administração 8
1.6. Definições e Acrônimos 9
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 10
2.1. Repositórios 10
2.2. Publicação de Informações dos Certificados 10
2.3. Tempo e Frequência de Publicação 10
2.4. Controle de Acesso aos Repositórios 10
3. IDENTIFICAÇÃO E AUTENTICAÇÃO 10
3.1. Nomeação 10
3.2. Validação Inicial de Identidade 10
3.3. Identificação e Autenticação Para Pedidos de Novas Chaves 10
3.4. Identificação e Autenticação Para Solicitação De Revogação 10
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 11
4.1. Solicitação de Certificado 11
4.2. Processamento de Solicitação de Certificado 11
4.3. Emissão se Certificado 11
4.4. Aceitação de Certificado 11
4.5. Usabilidade do Par De Chaves e do Certificado 11
4.6. Renovação de Certificados 11
4.7. Nova Chave de Certificado 12
4.8. Modificação de Certificado 12
4.9. Suspensão e Revogação de Certificado 12
4.10. Serviços de Status de Certificado 13
4.11. Encerramento de Atividades 13
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES 13
5.1. Controles Físicos 13
5.2. Controles Procedimentais 14
5.3. Controles De Pessoal 14

5.4. Procedimentos de Log de Auditoria 14
5.5. Arquivamento de Registros 14
5.6. Troca de Chave 15
5.7. Comprometimento e Recuperação de Desastre 15
5.8. Extinção da AC 15
6. CONTROLES TÉCNICOS DE SEGURANÇA 15
6.1. Geração e Instalação do par de Chaves 15
6.2 Proteção da Chave Privada e Controle de Engenharia do Módulo Criptográfico 17
6.3 Outros Aspectos do Gerenciamento do Par de Chaves 18
6.4 Dados de Ativação 19
6.5 Controles de Segurança Computacional 19
6.6 Controles Técnicos do Ciclo de Vida 19
6.7 Controles de Segurança de Rede 20
6.8 Carimbo do Tempo 20
7 PERFIS DE CERTIFICADO, LCR E OCSP 20
7.2 Perfil de LCR 26
7.3 Perfil de OCSP 26
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES 27
8.1 Frequência e Circunstâncias das Avaliações 27
8.2 Identificação/Qualificação do Avaliador 27
8.3 Relação do Avaliador com a Entidade Avaliada 27
8.4 Tópicos Cobertos Pela Avaliação 27
8.5 Ações Tomadas como Resultado de Uma Deficiência. 27
8.6 Comunicação dos Resultados 27
9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 27
9.1 Tarifas 27
9.2 Responsabilidades Financeira 27
9.3 Confidencialidade da Informação do Negócio 27
9.4 Privacidade da Informação Pessoal 27
9.5 Direitos de Propriedade Intelectual 28
9.6 Declarações e Garantias 28
9.7 Isenção de Garantias 28
9.8 Limitações de Responsabilidades 28
9.9 Indenizações 28
9.10 Prazo e Rescisão 28

9.11 Avisos Individuais E Comunicações Com Os Participantes 28
9.12 Alterações 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
9.17 Outras Provisões 29
10 DOCUMENTOS REFERENCIADOS 29
11 Referências Bibliográficas 29

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1 Esta "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Sigilo de Tipo S1 da Autoridade Certificadora PRODESP na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1.2. A estrutura desta PC está baseada no DOC-ICP-04 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC n.º 2527 (Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework).

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

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

1.1.5.O tipo de certificado emitido sob esta PC é do Tipo S1.

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. Não se aplica.

1.1.11 Não se aplica.

1.1.12 Não se aplica.

1.2. Nome do Documento e Identificação

1.2.1. Esta PC é designada de "Política de Certificado de Sigilo de Tipo S1 da Autoridade Certificadora PRODESP" e referida como "PC S1 da AC PRODESP". O OID (object identifier) desta PC é **2.16.76.1.2.101.18.**

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 PRODESP no âmbito da ICP-Brasil.

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

1.3.2 Autoridades de Registro

1.3.2.1. Os dados seguintes, referentes às Autoridades de Registro – AR utilizadas pela AC PRODESP para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC PRODESP, no endereço: http://certificadodigital.prodesp.sp.gov.br/repositorio/ac/prodesp

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

1.3.2.2. A AC PRODESP mantém as informações acima sempre atualizadas.

1.3.3 Titulares do Certificado

Os titulares de certificado de assinatura do Tipo S1 podem ser pessoas físicas ou jurídicas, equipamentos ou aplicações.

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 Serviço de Suporte – PSS vinculados diretamente a AC PRODESP e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC PRODESP http://certificadodigital.prodesp.sp.gov.br/repositorio/ac/prodesp

a) relação de todos os Prestadores de Serviço de Suporte – PSS;

b) relação de todos os Prestadores de Serviços Biométricos – PSBIOS;

1.4. Usabilidade do Certificado

1.4.1 Uso Apropriado do Certificado

1.4.1.1. Os certificados definidos por esta PC têm sua utilização vinculada a aplicações tais como cifra de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

1.4.1.2. As aplicações e demais programas que admitirem 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 PRODESP leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de

segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

1.4.1.4. Não se aplica.

1.4.1.5. Os certificados emitidos sob esta PC são apropriados ao uso, por exemplo, aplicações tais como cifra de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

1.4.1.6. Não se aplica.

1.4.1.7. Não se aplica.

1.4.1.8. Não se aplica.

1.4.2 Uso Proibitivo do Certificado

Os certificados emitidos sob esta PC devem apenas ser usados na medida em que seja consistente com a lei aplicável.

1.5. Política de Administração

1.5.1 Organização Administrativa do Documento

Nome da AC: AC PRODESP

1.5.2 Contatos

Endereço: Rua da Mooca, 1921 – Mooca – São Paulo, SP

Telefone: (55 11) 0800 0123401

Telefone: (55 11) 2799 9800

Página web: https://www.prodesp.sp.gov.br/

E-mail: certificacao@sp.gov.br

1.5.3 Pessoa Que determina a Adequabilidade da DPC com a PC

Nome: Roseli Ramalho de Jesus Caccaos

Telefone: (55 11) 2799 9805

E-mail: certificacao@sp.gov.br

1.5.4 Procedimentos de Aprovação da DPC

Esta DPC é aprovada pelo ITI.

Os procedimentos de aprovação da DPC da AC PRODESP 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
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CN	*Common Name*
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SSL	*Secure Socket Layer*
UF	Unidade de Federação
URL	Uniform Resource Locator

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios
2.2. Publicação de Informações dos Certificados
2.3. Tempo e 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 PRODESP.

3.1. Nomeação

3.1.1 Tipos de Nomes

3.1.2 Necessidade de Nomes Serem Significativos

3.1.3 Anonimato ou Pseudônimo dos Titulares de Certificados

3.1.4 Regras Para Interpretação de Vários 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 da Chave Privada

3.2.2 Autenticação da Identidade de uma Organização

3.2.3 Autenticação da Identidade de um 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 PRODESP.

4.1. Solicitação de 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 se 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

4.4.2publicação do Certificado da 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 Cave 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 Máximo 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 na 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 PRODESP.

5.1. Controles Físicos

5.1.1 Construção e Localização das Instalações da AC

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 (Logs)

5.4.3 Período de Retenção Para Registros (Logs) de Auditoria

5.4.4 Proteção de Registro de Auditoria

5.4.5 Procedimentos para Cópia de Segurança de Registro (Log) 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 para Cópia de Arquivo

5.5.5 Requisitos para Datação (Time-Stamping) 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 Procedimento Gerenciamento de Incidentes e Comprometimento

5.7.2 Recursos Computacionais, Software, e/ou dados corrompidos

5.7.3 Procedimentos no caso de comprometimento de Chave Privada de Entidade

5.7.4 Capacidade de Continuidade de Negócio após desastre

5.8. Extinção da AC

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do par de Chaves

6.1.1 Geração do par de Chaves

6.1.1.1. O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração do par 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 software CSP (Cryptographic Service Provider) existente na estação do solicitante, sendo a chave privada armazenada nesse software. A chave privada poderá ser exportada e armazenada (cópia de segurança) em mídia externa – ficheiro, disquete, token ou cartão inteligente – e protegida por senha de acesso.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados definido em documento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico definido em documento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado S1.

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

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

a) A chave privada é única e seu sigilo é suficientemente assegurado;
b) A chave privada não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
c) A chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

6.1.1.8 O tipo de certificado emitido pela AC PRODESP descrito nesta PC é o S1.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
S1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima.

6.1.2 Entrega Da Chave Privada À Entidade

Item não aplicável.

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

6.1.4 Entrega da Chave Pública da AC às terceiras partes

A AC PRODESP disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, de entre outras, em formato PKCS#7, através de endereço Web:

http://certificadodigital.prodesp.sp.gov.br/repositorio/acprodesp/acprodesp.p7b

6.1.5 Tamanhos de Chave

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

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo S1 da ICP-Brasil está definido em documento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6 Geração de Parâmetros de Chaves Assimétricas e Verificação da Qualidade dos Parâmetros

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados adotam, o padrão estabelecido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.7 Propósitos de uso de Chave (Conforme o Campo "Key Usage" na X.509v3)

Os certificados têm ativados os bits keyEncipherment e dataEncipherment.

6.2 Proteção da Chave Privada e Controle de Engenharia do Módulo Criptográfico

6.2.1 Padrões Para Módulo Criptográfico

Não se aplica.

6.2.2 Controle "N de M" Para Chave Privada

Não se aplica.

6.2.3 Custódia (Escrow) de Chave Privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas, isto é, não se permite que terceiros possam obter uma chave privada sem o consentimento do titular do certificado.

6.2.4 Cópia de Segurança (Backup) de Chave Privada

6.2.4.1. Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua chave privada.

6.2.4.2. Por solicitação do respectivo titular ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC PRODESP poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.

6.2.4.3. Em qualquer caso, a cópia de segurança deverá ser armazenada, cifrada, por algoritmo simétrico aprovado em regulamento editado por instrução normativa da Ac Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil e protegida com um nível de segurança não inferior àquele definido para a chave original.

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

6.2.5 Arquivamento de Chave Privada

6.2.5.1. A AC PRODESP não arquiva cópias de chaves privadas 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

Cada titular de certificado deve definir procedimentos necessários para a ativação da sua chave privada.

6.2.9 Método de Desativação de Chave Privada

Cada titular de certificado deve definir procedimentos necessários para a desativação da sua chave privada.

6.2.10 Método de Destruição de Chave Privada

Cada titular de certificado deve 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 emitidos pela AC PRODESP permanecem armazenadas após a expiração dos certificados correspondentes, pelo período legalmente estabelecido.

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 PRODESP 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.

6.3.2.3. O período máximo de validade admitido para certificados de sigilo do Tipo S1 é de 1 (um) ano.

6.3.2.4. Não se aplica.

6.3.2.5. Não se aplica.

6.4 Dados de Ativação

6.4.1 Geração e Instalação dos dados de Ativação

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

6.4.2 Proteção dos dados de ativação

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

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos Técnicos Específicos de Segurança Computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar pela 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, tais como uso de senhas complexas, antivírus atualizado, sistema operacional atualizado, firewall ativado, bem como os demais requisitos previstos na DPC.

6.5.2 Classificação da Segurança Computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

Não se aplica.

6.6.1 Controles de Desenvolvimento de Sistema

Não se aplica.

6.6.2. Controles de Gerenciamento de Segurança

Não se aplica.

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 são verificadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7 Controles de Segurança de Rede

Não se aplica.

6.8 Carimbo do Tempo

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC PRODESP 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 PRODESP 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 e sua criticidade.

7.1.2.2. Extensões Obrigatórias:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC PRODESP;

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: **2.16.76.1.2.101.18**;
- Os campos policyQualifiers contém o endereço Web da DPC AC PRODESP:

http://certificadodigital.prodesp.sp.gov.br/media/files/ac_prodesp.dpc.pdf

d) "CRL Distribution Points", não crítica, contém os endereços Web onde se obtém a LCR correspondente:

- https://lcr1.prodesp.sp.gov.br/acprodesp/acprodesp.crl
- https://lcr2.prodesp.sp.gov.br/acprodesp/acprodesp.crl

e) "Authority Information Access", não crítica, contém:

- o endereço web onde se poderá obter a cadeia de certificação através do link:

http://certificadodigital.prodesp.sp.gov.br/repositorio/acprodesp/acprodesp.p7b

- o endereço web onde se pode aceder ao serviço OCSP, através do link: http://ocsp.prodesp.gov.br

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

a) Para certificado de pessoa física:

a.1) 3 (três) campos otherName, obrigatórios, contendo nesta ordem:

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 UF;

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

OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

a.2) Não se aplica.

a.3) Não se aplica.

a.4) Não se aplica.

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

OID = 2.16.76.1.3.4 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) do responsável; 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 UF.

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado

OID = 2.16.76.1.3.3 e conteúdo =nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

b1) Campos otherName, não obrigatórios, contendo:

RFC822Name, contém o endereço de correio eletrônico do titular do certificado.

c) Para certificado de equipamento ou aplicação:

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

OID = 2.16.76.1.3.8 e 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 e 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 e conteúdo = nome do responsável pelo certificado.

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; 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) do responsável; 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) Não se aplica.

d) Não se aplica.
e) Não se aplica.

7.1.2.4. Os campos otherName, definidos como obrigatórios pela ICP-Brasil, estão de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo otherName é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING, ou PRINTABLE STRING, 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 e UF. O mesmo ocorre para o campo do município e UF se não houver número de inscrição do Título de Eleitor.
d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, exceto nos casos de certificado digital cuja titularidade foi validada pelo conselho de classe profissional.
e) Todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidos com caracteres "zero" à sua esquerda para que seja completado seu máximo tamanho possível.
f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, sendo utilizados apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre municípios e UF do Título de Eleitor.
g) Para os campos OtherName, com exceção do UPN, apenas caracteres de A a Z e de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais.
h) Não se aplica.

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

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

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

a) Não se aplica.
b) Não se aplica.
c) Não se aplica.
d) Não se aplica.
e) para certificados de Assinatura de Resposta OCSP: "Key Usage", crítica: deve conter 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 deve estar presente;
f) Não se aplica.
g) Para certificados de Sigilo:

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

7.1.3 Identificadores de Algoritmo

Os certificados emitidos pela AC PRODESP são assinados utilizando o algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) conforme o padrão PKCS#1.

7.1.4 Formatos de Nome

7.1.4.1. O nome do titular do certificado, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594.

C = BR

O = ICP-Brasil

OU = Tipo do certificado emitido (Certificado de Sigilo - Tipo S1)

OU =< CNPJ da AR que realizou a identificação;

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

E = <endereço de email>

CN = <Nome do titular> do certificado de pessoa física; em um certificado de pessoa jurídica é o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)>

O campo DN pode apresentar outros campos "OU". Caso qualquer um dos campos OU não seja utilizado, o mesmo não será apresentado no DN.

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

Em um certificado de equipamento ou aplicação, o identificador CN contém o URL correspondente ou o nome da aplicação, e não contém o campo E.

Será escrito o nome até o limite do tamanho do campo disponível.

O campo Locality (L), opcional, com conteúdo correspondente ao nome da cidade onde a empresa/titular está localizada/o. O campo deve ser preenchido sem acentos nem abreviaturas.

O campo State or Province Name (ST), opcional, com conteúdo correspondente à sigla do estado onde a empresa/titular está localizada/o.

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 estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. As restrições aplicáveis para os nomes, para todos os titulares de certificados emitidos pela AC PRODESP são as seguintes:

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Os acentos devem ser substituídos pelo caractere não acentuado;
- O "ç" deve ser substituído pelo caractere 'c';
- Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

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

7.1.6 OID (Object Identifier) de Política de Certificado

O OID desta PC é: **2.16.76.1.2.101.18.**

Todo certificado emitido segundo essa PC, PC S1 PRODESP, contém o valor desse OID presente na extensão Certificate Policies.

7.1.7 Uso da Extensão "Policy Constraints"

Não se aplica.

7.1.8 Sintaxe e Semântica dos Qualificadores de Política

Os campos policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC PRODESP. http://certificadodigital.prodesp.sp.gov.br/media/files/ac_prodesp.dpc.pdf

7.1.9 Semântica de Processamento para 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 PRODESP implementam a versão 2 do 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 PRODESP e sua criticidade.

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

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

A AC PRODESP define como obrigatória a seguinte extensão para suas LCRs:

"Authority Information Access", não crítica: contém o endereço web onde se poderá obter a cadeia de certificação

http://certificadodigital.prodesp.sp.gov.br/repositorio/acprodesp/acprodesp.p7b

7.3 Perfil de OCSP

7.3.1 Número (S) de Versão

Serviços de respostas OCSP implementam a 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 PRODESP.

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

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 Responsabilidades 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 Informações Como Privadas

9.4.3 Informações não Consideradas Privadas

9.4.4 Responsabilidade Para Proteger a Informação Privada

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

Mudança nesta PC será publicado no site da AC PRODESP.

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 PRODESP e AR vinculadas. 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 foi submetida à aprovação, durante o processo de credenciamento da AC PRODESP, conforme o estabelecido no documento CRITÉRIOS E

PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com este documento, foi verificada a compatibilidade entre a PC e a DPC da AC PRODESP.

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
	REQUISITOS MINIMOS PARA AS POLITICAS DE CERTIFICADOS NA ICP-BRASIL	DOC-ICP -04

11 Referências Bibliográficas

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

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

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

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003