PRESIDÊNCIA DA REPÚBLICA
Secretaria-Geral
Secretaria Especial de Administração
Diretoria de Tecnologia
Coordenação de Segurança das Informações em Meios Tecnológicos
Divisão de Certificação Digital

Política de Certificado da Autoridade Certificadora da Presidência da República A3

Assinatura Geral e Proteção de E-mail (S/MIME)

(PC ACPR A3)

Infraestrutura de Chaves Públicas Brasileira
ICP-Brasil

Versão 11 – OUTUBRO/2020
20/10/2020

ÍNDICE

Controle de Alterações

Versão	Data	Responsável	Descrição
11.0	20/10/2020	Gustavo Freire	Adequação à Resolução 179, de 20/09/2020, versão 8.0 (Revisão e consolidação do DOC-ICP-04, conforme Decreto nº 10.139, de 28/11/2019 e ajustes para emissão por meio de videoconferência)
10.0	30/04/2020	Gustavo Freire	Adequação às Resoluções 169 e 170: inclusão no certificado digital de como foi realizada a identificação do titular (presencial, videoconferência ou certificado digital) e procedimentos a serem observados na emissão de um certificado digital por videoconferência.
9.0	07/10/2019	Gustavo Freire	Adequação à Resolução Nº 151, de 30/05/2019: requisitos para conformidade ao Programa WebTrust para as entidades da ICP-Brasil e simplificação de processos da ICP-Brasil.
8.0	19/02/2019	Gustavo Freire	Adequação à Resolução Nº 150, de 07/11/2018: inclusão do CNPJ da AR onde ocorreu a identificação presencial.

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1 Este documento estabelece os requisitos a serem obrigatoriamente observados pela Autoridade Certificadora da Presidência da República (AC PR) integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de sua Política de Certificado – PC ACPR A3.

1.1.2 A PC ACPR A3, elaborada no âmbito da ICP-Brasil, adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO na ICP-Brasil (DOC-ICP-04).

1.1.3 A estrutura desta PC está baseada na RFC 3647.

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

1.1.5 O tipo de certificado emitido sob esta PC é o certificado de assinatura digital do tipo A3.

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 Política de Certificado de Assinatura Digital, tipo A3, da AC PR.

1.2.2 Após o processo de credenciamento da AC PR no âmbito da ICP-Brasil, foi atribuído a esta PC o OID **2.16.76.1.2.3.1**.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

1.3.1.1 A Autoridade Certificadora da Presidência da República (AC PR) integra a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), sob a hierarquia da Autoridade Certificadora Raiz Brasileira, cuja PC é implementada nesse documento.

1.3.1.2 A DPC da AC PR encontra-se publicada em sua página *web* (URL) no seguinte endereço: https://certificados.serpro.gov.br/acpr

1.3.2. Autoridades de Registro

1.3.2.1 O endereço da página *web* (URL) da AC PR é https://certificados.serpro.gov.br/acpr onde estão publicados os dados abaixo referente à Autoridade de Registro, responsável pelo processo de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

a) relação de todas as AR credenciadas, com informações sobre as PC que implementam;

b) relação de AR que tenham sido descredenciadas da cadeia da AC PR, com a respectiva data do descredenciamento.

1.3.3. Titulares do Certificado

Os Titulares de Certificados desta PC são pessoas físicas ou jurídicas da Presidência da República e, supletivamente, da Vice-Presidência da República, assim como, servidores de outros órgãos da administração pública federal, que utilizam sistemas de interesse da Presidência da República.

1.3.4. Partes Confiáveis

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

1.3.5. Outros Participantes

A AC PR utiliza o Serviço Federal de Processamento de Dados (SERPRO) como Prestador de Serviço de Suporte (PSS), Prestador de Serviço Biométrico - PSBio e Prestador de Serviço Biométrico (PSC) conforme disponibilizado na página *web* https://certificados.serpro.gov.br/acpr.

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

1.4.1.1. Os certificados emitidos sob esta PC são apropriados ao uso apenas nas aplicações apresentadas na tabela descrita a seguir.

Política de Certificado	Aplicações Apropriadas
PC ACPR A3	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas seguintes aplicações: • Confirmação de Identidade na web; • Correio eletrônico; • Transações On-Line; • Redes privadas virtuais (VPN); • Transações eletrônicas; • Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações

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. As aplicações para o certificado definido nesta PC, leva em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos 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. Certificados de tipo A3 são 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 há restrições de aplicações identificadas.

1.5. Política de Administração

Esta DPC é administrada pela Divisão de Certificação Digital da Presidência da República (DICED).

1.5.1. Organização administrativa do documento

Autoridade Certificadora da Presidência da República (AC PR).

1.5.2. Contatos

Administrativo:

DITEC/COSIT/Divisão de Certificação Digital – DICED
Endereço: Anexo IV do Palácio do Planalto, Brasília, Distrito Federal, CEP: 70.150-900.
Página web: https://www.planalto.gov.br/acpr

E-mail: acpr@presidencia.gov.br
Telefone: (61) 3411-2600

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

Nome: Gustavo Adriane de Carvalho Freire
Telefone: (61) 3411-2668
E-mail: acpr@presidencia.gov.br

1.5.4. Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.
Os procedimentos de aprovação da PC da AC PR são estabelecidos a critério do CG da ICP-Brasil.

1.6. Definição 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
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
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
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
ISO	International Organization for Standardization
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

SIGLA	DESCRIÇÃO
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

Os itens seguintes estão descritos na DPC da AC PR em vigor.

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

Os itens seguintes estão descritos na DPC AC PR em vigor.

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

Item 3.2.7. da DPC ACPR.

3.2.4. Autenticação da identidade de um indivíduo

Item 3.2.3. da DPC ACPR.

3.2.5. Informações não verificadas do titular do certificado

Item 3.2.4. da DPC ACPR.

3.2.6. Validação das autoridades

Item 3.2.5. da DPC ACPR.

3.2.7. Critérios para interoperação

Item 3.2.6. da DPC ACPR.

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

Os itens seguintes estão descritos na DPC ACPR em vigor.

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

Não se aplica.

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

Os itens seguintes estão descritos na DPC ACPR em vigor.

5.1. Controles físicos

5.1.1 Construção e localização das instalações de 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

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 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, são definidas as medidas de segurança implantadas pela AC PR para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São definidos também outros controles técnicos de segurança utilizados pela AC PR e pela AR vinculada 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 As chaves criptográficas dos titulares de certificados devem observar os requisitos desta PC, bem como ser geradas e armazenadas em hardware ou mídia criptográficos homologados pela ICP-Brasil.

6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é definido em regulamento 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 da entidade titular é gravada cifrada, por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme Tabela 4 a seguir.

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 deverá assegurar, 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 deve estar 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 Essa mídia de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

Nota: Não se aplica.

6.1.2. Entrega da chave privada à entidade titular

Não se aplica. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

6.1.3. Entrega da chave pública para o emissor de certificado

As chaves públicas dos titulares de certificado são entregues por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC. Nos casos em que houver solicitação de certificado pelo seu titular ou por AR vinculada, será adotado formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.4. Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação da AC, para os usuários da ICP-Brasil, compreendem:

a) no momento da disponibilização de um certificado para seu titular, será utilizado o formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil;
b) diretório;
c) página *web* da AC; e
d) outros meios seguros aprovados pelo CG ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1 Os tamanhos das chaves criptográficas associadas aos certificados emitidos pela ACPR são os seguintes:

6.1.5.1.1 Para os certificados emitidos pela AC PR v1 e v2 o tamanho das chaves criptográficas é de 1024 (mil e vinte e quatro) bits;

6.1.5.1.2 Para os certificados emitidos pela AC PR v3, v4 e v5 o tamanho das chaves criptográficas é de, no mínimo, 2048 (dois mil e quarenta e oito) bits.

6.1.5.2 Os algoritmos e o tamanho das chaves utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração e verificação de chaves assimétricas das entidades titulares de certificado, 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.509 v3)

Os certificados emitidos pela AC têm no campo "Key usage" (2.5.29.15) ativado os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment*.

6.2. Proteção da chave privada e controle de engenharia do módulo criptográfico

Nos itens seguintes são definidos os requisitos de proteção das chaves privadas de certificados emitidos, segundo esta PC.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. Os padrões requeridos para os módulos de geração de chaves criptográficas, estão definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.1.2. Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado seguem os padrões de referência, definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2. Controle "n de m" para chave privada

Não se aplica.

6.2.3. Custódia (escrow) de chave privada

Não se aplica.

6.2.4. Cópia de segurança (backup) de chave privada

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

6.2.4.2 A AC PR responsável por esta PC não mantém cópia de segurança de chave privada de titular de assinatura digital 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 Além das observações acima, esta PC deve descrever todos os requisitos e procedimentos aplicáveis ao processo de geração de uma cópia de segurança.

6.2.5. Arquivamento de chave privada

6.2.5.1 Não se aplica.

6.2.5.2 Não se aplica.

6.2.6. Inserção de chave privada em módulo criptográfico

As chaves privadas devem ser inseridas nos módulos criptográficos de acordo com os procedimentos especificados pelos fornecedores dos módulos.

6.2.7. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação da chave privada da AC é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os

detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

6.2.9. Método de desativação de chave privada

Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

6.2.10. Método de destruição de chave privada

Quando a chave privada da AC for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estiver armazenada, deve ser sobrescrito; todas as cópias de segurança da chave privada da AC e os cartões criptográficos dos custodiantes serão destruídos. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC.

6.3. Outros aspectos do gerenciamento do par de chaves

6.3.1. Arquivamento de chave pública

A AC armazena as chaves públicas da própria AC e dos titulares de certificados, bem como as LCR emitidas, após a expiração dos certificados correspondentes, permanentemente, 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 dos respectivos Titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

6.3.2.3 Certificados do tipo A3, previsto nesta PC, tem validade de até 5 (cinco) anos.

6.3.2.4 Não se aplica.

6.3.2.5 Não se aplica.

6.4 Dados de ativação

Nos itens seguintes, estão descritos os requisitos gerais 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. Cada PC implementada deve descrever os requisitos específicos aplicáveis.

6.4.1. Geração e instalação dos dados de ativação

Os dados de ativação da chave privada da AC PR são únicos e aleatórios.

6.4.2. Proteção dos dados de ativação

Os dados de ativação da AC PR são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha e são armazenados em ambiente de nível 6 de segurança.

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

Os pares de chaves criptográficas dos titulares de certificados devem observar os requisitos gerais desta PC, bem como ser geradas e armazenadas em hardware ou mídia criptográficos homologados pela ICP-Brasil.

6.5.2. Classificação da segurança computacional

Não se aplica.

6.6. Controles técnicos do ciclo de vida

A AC PR não exige um software específico para utilização dos certificados emitidos segundo esta PC.

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. Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na geração de LCR

Todas as LCRs geradas pela AC PR 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

Os mesmos controles admitidos no item 6.7 DPC ACPR em vigor.

6.8. Carimbo de tempo

Não se aplica.

7. PERFIS DE CERTIFICADO, LCR e OCSP

Os itens seguintes especificam os formatos dos certificados e das LCRs gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são obrigatoriamente atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1. Perfil do certificado

Os certificados emitidos pela AC PR estão em conformidade com o formato definido pelo padrão ITU X.509 v3 ou ISO/IEC 9594-8.

7.1.1. Número de versão

Os certificados emitidos pela AC PR 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. As extensões de certificados utilizados sob esta PC estão descritas nos subitens seguintes.

7.1.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões:

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

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, **2.16.76.1.2.3.1**, bem como o endereço da página *Web* da AC conforme abaixo:

Versão dos certificados da AC	Valor do campo
V4 e V5	http://repositorio.serpro.gov.br/docs/dpcacpr.pdf
V1, V2 e V3	https://ccd.serpro.gov.br/ACPR/docs/dpcacpr.pdf

d) **"*CRL Distribution Points*", não crítica:** contém os endereços da página *Web* onde se obtém a LCR da AC*:*

Versão dos certificados da AC	Valor do Campo
V5	http://repositorio.serpro.gov.br/lcr/acprv5.crl, http://certificados2.serpro.gov.br/lcr/acprv5.crl
V4	http://repositorio.serpro.gov.br/lcr/acprv4.crl, http://certificados2.serpro.gov.br/lcr/acprv4.crl http://repositorio.icpbrasil.gov.br/lcr/acprv4.crl
V3	http://ccd.serpro.gov.br/lcr/ACPRv3.crl http://ccd2.serpro.gov.br/lcr/ACPRv3.crl http://repositorio.icpbrasil.gov.br/lcr/ACPRv3.crl
V2	http://ccd.serpro.gov.br/lcr/ACPRv2.crl http://ccd2.serpro.gov.br/lcr/ACPRv2.crl http://repositorio.icpbrasil.gov.br/lcr/ACPRv2.crl
V1	http://repositorio.icpbrasil.gov.br/lcr/ACPRv1.crl

e) ***"Authority Information Access",* não crítica:** contém o método de acesso *id-ad-calssuer* e utiliza o protocolo de acesso HTTP para recuperação da cadeia de certificação no seguinte endereço:

Versão dos certificados da AC	Valor do Campo
V5	http://repositorio.serpro.gov.br/cadeias/acprv5.p7b
V4	http://repositorio.serpro.gov.br/cadeias/acprv4.p7b
V3	http://ccd.serpro.gov.br/cadeias/ACPRv3.p7b
V2	http://ccd.serpro.gov.br/cadeias/ACPRv2.p7b
V1	http://ccd.serpro.gov.br/cadeias/ACPRv1.p7b

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

a) Para certificado de pessoa física:

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

:

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 do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

ii. **OID = 2.16.76.1.3.6 e conteúdo** = nas 12 (doze) posições o número do Cadastro Especifico 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 subseqüentes, 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); 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 Especifico do INSS (CEI) da pessoa jurídica titular do certificado.

c) Não se aplica.
d) Não se aplica.
e) Não se aplica.

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

a) O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;
b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";
c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de 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 informações de tamanho variável referentes a números, tais como RG, devem ser 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, devendo ser 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) Caracteres de A a Z e de 0 a 9 e os caracteres especiais descritos 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 definidas pela AC, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

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

7.1.2.7. A AC implementa as seguintes extensões "*Key Usage*" e "*Extended Key Usage*", definidas como obrigatórias pela ICP-Brasil.

a) Não se aplica.

b) Não se aplica.

c) Não se aplica.

d) Não se aplica.

e) Não se aplica.

f) para certificados de Assinatura e/ou Proteção de e-mail:

***"Key Usage",* crítica**: deve conter o bit *digitalSignature* ativado, podendo conter os bits *keyEncipherment* e *nonRepudiation* ativados;

***"Extended Key Usage",* não crítica**: no mínimo para um dos propósitos *client authentication OID* = 1.3.6.1.5.5.7.3.2 ou *E-mail protection OID* = 1.3.6.1.5.5.7.3.4 deve estar ativado podendo implementar outros propósitos instituídos, desde que verificáveis e previstos pelas AC, em suas PCs, em conformidade com a RFC 5280;

g) Não se aplica.

7.1.3. Identificadores de algoritmo

7.1.3.1 Os algoritmos criptográficos utilizados para assinatura dos certificados pela AC PR são os admitidos no âmbito da ICP-Brasil, conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.3.1.1 Os certificados emitidos pela AC PR v1 e AC PR v2 são assinados com o uso do algoritmo criptográfico SHA-1 com função de hash (OID = **1.2.840.113549.1.1.5).**

7.1.3.1.2 Os certificados emitidos pela AC PR v3, v4 e v5 são assinados com o uso do algoritmo criptográfico SHA-256 com função de hash (OID = **1.2.840.113549.1.1.11).**

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:

O conteúdo do DN apresenta-se da seguinte forma para os certificados de Pessoa Física:

C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Presidencia da Republica
OU = sigla do órgão de trabalho
OU = CNPJ da AR que realizou a identificação
OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)
OU = Pessoa Fisica A3
CN = nome do titular do certificado

O conteúdo do DN apresenta-se da seguinte forma para os certificados de Pessoa Jurídica:

C = BR
O = ICP-Brasil
OU = Autoridade Certificadora da Presidencia da Republica
OU = sigla do órgão de trabalho
OU = CNPJ da AR que realizou a identificação
OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)
OU = Pessoa Jurídica A3
CN = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

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. Não se aplica.

7.1.5.2. A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e
b) além dos caracteres alfanuméricos, poderão ser utilizados também 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) da PC

O OID atribuído à esta Política de Certificado é: **2.16.76.1.2.3.1**. Todo certificado emitido segundo esta PC deverá conter, na extensão "*Certificate Policies*", o OID correspondente.

7.1.7. Uso da extensão "Policy Constraints"

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo ***policyQualifiers*** da extensão "*Certificate Policies*" contém o endereço da página *Web* (URL) da DPC ACPR. A saber:

Versão dos certificados da AC	**Valor do campo**
V4 e V5	http://repositorio.serpro.gov.br/docs/dpcacpr.pdf
V1, V2 e V3	https://ccd.serpro.gov.br/ACPR/docs/dpcacpr.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 de versão

As LCRs geradas pela AC PR 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 adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) **"*Authority Key Identifier*", não crítica:** contém o *hash* SHA-1 da chave pública da AC PR que assina a LCR; e

b) **"*CRL Number*", não crítica:** contém número seqüencial para cada LCR emitida.

7.2.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

a) ***"Authority Key Identifier"*, não crítica:** deve conter o *hash* SHA-1 da chave pública da AC PR que assina a LCR; e

b) ***"CRL Number"*, não crítica**: deve conter um número sequencial para cada LCR emitida.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Não se aplica.

7.3.2. Extensões de OCSP

Não se aplica.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes na DPC da AC PR.

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 na DPC da AC PR.

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 na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

Mudança nesta PC será publicado no site da AC PR.

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 PR e AR vinculada 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

Toda PC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável, 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, deverá ser verificada a compatibilidade entre a PC e a DPC da AC.

10. DOCUMENTOS REFERENCIADOS

10.1. Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL Aprovado pela Resolução nº 132, de 10 de novembro de 2017	**DOC-ICP-17**
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DE TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	**DOC-ICP-12**
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	**DOC-ICP-03**

11. REFERÊNCIAS BIBLIOGRÁFICAS

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

RFC 5280, IETF - *Internet X.509 Public Key Infrastructure Certificate and Certificate RevocationList (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.*