PRESIDÊNCIA DA REPÚBLICA
SECRETARIA-GERAL
SECRETARIA DE ADMINISTRAÇÃO
DIRETORIA DE TECNOLOGIA

Política de Certificado da ACPR

do tipo A1

para certificação de equipamento ou aplicação

(PC ACPR A1)

Infraestrutura de Chaves Públicas do BRASIL
ICP-Brasil

INDICE

LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
AR - Autoridades de Registro
CEI - Cadastro Específico do INSS
CG - Comitê Gestor
CMM-SEI - *Capability Maturity Model* do *Software Engineering Institute*
CMVP - *Cryptographic Module Validation Program*
CN - Common Name
CNE - Carteira Nacional de Estrangeiro
CNPJ - Cadastro Nacional de Pessoas Jurídicas -
COBIT - *Control Objectives for Information and related Technology*
COSO - *Comitee of Sponsoring Organizations*
CPF - Cadastro de Pessoas Físicas
DMZ - Zona Desmilitarizada
DN - *Distinguished Name*
DPC - Declaração de Práticas de Certificação
ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira
IDS - Sistemas de Detecção de Intrusão
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 - *On-line Certificate Status Protocol*
OID - *Object Identifier*
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*
PSS - Prestadores de Serviço de Suporte
RFC – *Request For Comments*
RG - Registro Geral
SNMP - *Simple Network Management Protocol*
TCSEC - *Trusted System Evaluation Criteria*
TSDM - *Trusted Software Development Methodology*
UF - Unidade de Federação
URL - Uniform Resource Location

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Este documento descreve a Política de Certificados do tipo A1 da Autoridade Certificadora da Presidência da República (PC ACPR A1), observando os requisitos definidos no documento Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil - DOC-ICP-04.

1.1.2 Esta PC adota obrigatoriamente a estrutura recomendada pelo DOC-ICP-04 do Comitê Gestor da ICP-Brasil.

1.1.3 Esta PC se refere ao certificado A1 de assinatura digital, um dos tipos de certificados previsto para usuário final no âmbito da ICP-Brasil.

1.1.4 Não aplicável.

1.1.5 Não aplicável.

1.1.6 Não aplicável.

1.1.7 Não aplicável.

1.2. IDENTIFICAÇÃO

1.2.1 Esta PC obedece às recomendações da ICP-Brasil para a emissão de certificados de assinatura do tipo A1.

1.2.2 Após o processo de credenciamento da ACPR foi atribuído a esta Política de Certificação no âmbito da ICP-Brasil o OID 2.16.76.1.2.1.3.

1.3. COMUNIDADE E APLICABILIDADE

1.3.1. Autoridades Certificadoras

1.3.1.1 A Autoridade Certificadora da Presidência da República (ACPR) que implementa esta PC é integrante da Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora Raiz Brasileira.

1.3.1.2 As práticas e procedimentos de certificação digital da ACPR são implementados pela Declaração de Práticas de Certificação da ACPR - DPC da ACPR.

1.3.2. Autoridades de Registro

1.3.2.1 A ACPR mantém página web (https://certificados.serpro.gov.br/acpr) onde estão publicados os dados abaixo referentes às Autoridades de Registro – AR utilizadas pela ACPR para os processos de recebimento, validação 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) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;
e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for caso.

1.3.2.2. A ACPR mantém as informações acima sempre atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A ACPR mantém página web no endereço https://certificados.serpro.gov.br/acpr com a relação de todos os prestadores de serviço de suporte (PSS) vinculados ä ACPR, seja diretamente ou por intermédio de suas AR.

1.3.3.2 PSS são entidades utilizadas pela AC ou pela AR para desempenhar as atividades descritas abaixo:

a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3 A ACPR mantém as informações acima atualizadas.

1.3.4. Titulares de Certificado

Podem ser titulares de certificados emitidos pela ACPR as pessoas que atendam aos seguintes requisitos:

a) Servidores que integram a estrutura da Presidência da República ou Vice-Presidência da República, que necessitam de certificados digitais para o exercício de suas funções;
b) Agentes públicos, indicados pelos Gestores dos Órgãos Essenciais da PR, que necessitam de certificados digitais para utilização em serviços geridos por esses órgãos. (Lista dos Órgãos essenciais em: http://www2.planalto.gov.br/presidencia/estrutura-da-presidencia/estrutura-da-presidencia)
c) Autoridades que não pertencem ao Poder Executivo Federal, autorizadas pela Secretaria Geral a receberem certificados digitais.

1.3.5. Aplicabilidade

1.3.5.1 Certificados emitidos sob esta PC são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação de equipamentos e aplicações.

1.3.5.2 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.

1.3.5.3 Os requisitos mínimos de segurança para certificados do tipo A1 da ACPR são os seguintes:

Chave Criptográfica			Validade Máxima do Certificado (anos)	Freqüência de Emissão de LCR (horas)	Tempo Limite para Revogação (horas)
Tamanho (bits)	Processo de Geração	Mídia Armazenadora			
RSA 1024 (V0 e V1), 2048 (V2)	*Software*	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma do item 6.1.1	1	6	12

1.3.5.4 Certificados do tipo A1 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.3.5.5. Não aplicável.

1.3.5.6. Não aplicável.

1.4. DADOS DE CONTATO

A ACPR, responsável por esta PC, funciona no seguinte endereço:

Diretoria de Tecnologia - DITEC
Anexo I do Palácio do Planalto
Cep: 70.150-900

Brasília – DF

Pessoa de Contato.

Nome: Liliana Suzete Lopes de Queiroz Campos
Telefones: (61) 3411-2668 / 3411-2821 / 3411-1000; Fax: (61) 3411-2855
E-mail: acpr@planalto.gov.br

2. DISPOSIÇÕES GERAIS

Este capítulo possui definições acerca das obrigações da ACPR, de suas Autoridades de Registro (AR), de seus Titulares de Certificado e Usuários e demais assuntos relacionados com a legislação e solução de conflitos. Suas descrições se encontram nos itens de mesmo número da DPC ACPR em vigor.

2.1. OBRIGAÇÕES E DIREITOS

2.1.1. Obrigações da AC

2.1.2. Obrigações das AR

2.1.3. Obrigações do Titular do Certificado

2.1.4. Direitos da terceira parte (*Relying Party*)

2.1.5. Obrigações do Repositório

2.2. RESPONSABILIDADES

2.2.1. Responsabilidades da AC

2.2.2. Responsabilidades da AR

2.3. RESPONSABILIDADE FINANCEIRA

2.3.1. Indenizações devidas pela terceira parte (*Relying Party*)

2.3.2. Relações Fiduciárias

2.3.3. Processos Administrativos

2.4. INTERPRETAÇÃO E EXECUÇÃO

2.4.1. Legislação

2.4.2. Forma de interpretação e notificação

2.4.3. Procedimentos de solução de disputa

2.5. TARIFAS DE SERVIÇO

2.5.1. Tarifas de emissão e renovação de certificados

2.5.2. Tarifas de acesso a certificados

2.5.3. Tarifas de revogação ou de acesso à informação de status

2.5.4. Tarifas para outros serviços

2.5.5. Política de reembolso

2.6. PUBLICAÇÃO E REPOSITÓRIO

2.6.1. Publicação de informação da AC

2.6.2. Frequência de publicação

2.6.3. Controles de acesso

2.6.4. Repositórios

2.7. AUDITORIA E FISCALIZAÇÃO

2.8. SIGILO

2.8.1. Tipos de informações sigilosas

2.8.2. Tipos de informações não sigilosas

2.8.3. Divulgação de informação de revogação e de suspensão de certificado

2.8.4. Quebra de sigilo por motivos legais

2.8.5. Informações a terceiros

2.8.6. Divulgação por solicitação do titular

2.8.7. Outras circunstâncias de divulgação de informação

2.9. DIREITOS DE PROPRIEDADE INTELECTUAL

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

A ACPR possui procedimentos para Identificação e Autenticação de um indivíduo conforme os subitens seguintes. Suas descrições se encontram nos itens de mesmo número da DPC ACPR em vigor.

3.1. REGISTRO INICIAL

3.1.1. Disposições Gerais

3.1.2. Tipos de nomes

3.1.3. Necessidade de nomes significativos

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

3.1.8. Método para comprovar a posse de chave privada

3.1.9. Autenticação da identidade de um indivíduo

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.10. Autenticação da identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.2. Documentos para efeitos de identificação de uma organização

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.11. Autenticação da identidade de equipamento ou aplicação

3.1.11.1. Disposições Gerais

3.1.11.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.1.11.3 - Informações contidas no certificado emitido para um equipamento ou aplicação

3.2. GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

3.3. GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO

3.4. SOLICITAÇÃO DE REVOGAÇÃO

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado

Para a solicitação de certificado de equipamento ou aplicação, o solicitante deve:

a) Acessar a página Web (https://certificados.serpro.gov.br/arpr) da ACPR, clicar no menu Meu Certificado e escolher a opção Solicitar;

b) Selecionar o tipo de certificado desejado e preencher os dados do formulário de solicitação, conforme orientações da ACPR;

c) Gerar e imprimir o Termo de Titularidade e Responsabilidade de Certificado Digital de Equipamento / Aplicação, em três vias;

d) Agendar junto à ACPR a validação presencial e aprovação do certificado digital.

4.2. Emissão de Certificado

A ACPR valida e aprova o pedido de certificado efetuando o seguinte:

a) O Agente de Registro (AGR) da AR verifica se os dados constantes da solicitação de certificado

estão de acordo com os documentos apresentados pelo solicitante;
b) O AGR acessa o sistema de certificação e realiza a aprovação do pedido de certificado;
c) Após a aprovação do pedido de certificado, realizada por 02 (dois) AGR, o sistema emite um e-mail ao solicitante informando que o certificado foi aprovado.

O acesso ao sistema de certificação que processa a aceitação da solicitação de certificados é feito mediante o uso de certificado digital com requisitos de segurança, no mínimo, equivalentes aos de um certificado de nível A3.

O certificado é considerado válido a partir do momento da sua emissão.

4.3. Aceitação de Certificado

Após receber o e-mail informando que o certificado foi aprovado, o responsável pelo uso do certificado efetua o seguinte:

a) Acessa a página Web https://certificados.serpro.gov.br/arpr da ACPR;
b) Escolhe a opção Instalar no Menu Meu Certificado;
c) Informa o Número de Referência, o Código de Acesso e a Senha que foi criada na solicitação do certificado e clica no botão Continuar;
d) Cole no bloco os dados produzidos pela solicitação do certificado e clique no botão Salvar Certificado;
e) O responsável instala o certificado no equipamento.

O certificado é considerado aceito assim que for baixado.

Aceitando um certificado, o titular de certificado e o responsável por sua utilização:

a) Concordam com as responsabilidades, obrigações e deveres impostos a eles pelo Termo de Titularidade e/ou Termo de Responsabilidade, pela DPC da ACPR e por esta PC;
b) Garantem que por seus conhecimentos nenhuma pessoa sem autorização terá acesso à chave privada associada ao certificado;
c) Afirmam que as informações do certificado, fornecidas durante o processo de solicitação, são verdadeiras e foram publicadas dentro do certificado, com precisão;
d) Afirmam que esse certificado não faz parte da LCR correspondente, publicada na Web.

4.4. Suspensão e Revogação de Certificado

A ACPR possui procedimentos para Suspensão e Revogação de Certificados, conforme os subitens seguintes. Suas descrições se encontram nos itens de mesmo número da DPC ACPR em vigor.

4.4.1. Circunstâncias para revogação

4.4.2. Quem pode solicitar revogação

4.4.3. Procedimento para solicitação de revogação

4.4.4. Prazo para solicitação de revogação

4.4.5. Circunstâncias para suspensão

4.4.6. Quem pode solicitar suspensão

4.4.7. Procedimento para solicitação de suspensão

4.4.8. Limites no período de suspensão

4.4.9. Frequência de emissão de LCR

4.4.10. Requisitos para verificação de LCR

4.4.11. Disponibilidade para revogação ou verificação de status *on-line*

4.4.12. Requisitos para verificação de revogação *on-line*

4.4.13. Outras formas disponíveis para divulgação de revogação

4.4.14. Requisitos para verificação de outras formas de divulgação de revogação

4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

A ACPR registra todos os eventos relacionados à segurança do seu sistema de certificação conforme os subitens seguintes, Suas descrições se encontram nos itens de mesmo número da DPC ACPR em vigor.

4.5.1. Tipos de eventos registrados

4.5.2. Frequência de auditoria de registros (logs)

4.5.3. Período de retenção para registros (*logs*) de auditoria

4.5.4. Proteção de registro (*log*) de auditoria

4.5.5. Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria

4.5.6. Sistema de coleta de dados de auditoria

4.5.7. Notificação de agentes causadores de eventos

4.5.8. Avaliações de vulnerabilidade

4.6. ARQUIVAMENTO DE REGISTROS

A ACPR mantém um arquivo de registros conforme os subitens seguintes. Suas descrições se encontram nos itens de mesmo número da DPC ACPR em vigor.

4.6.1. Tipos de registros arquivados

4.6.2. Período de retenção para arquivo

4.6.3. Proteção de arquivo

4.6.4. Procedimentos para cópia de segurança (*backup*) de arquivo

4.6.5. Requisitos para datação (*time-stamping*) de registros

4.6.6. Sistema de coleta de dados de arquivo

4.6.7. Procedimentos para obter e verificar informação de arquivo

4.7. TROCA DE CHAVE

Os procedimentos de troca de chave estão descritos no Item 4.7 da DPC ACPR em vigor.

4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

ACPR possui procedimentos para os casos de comprometimento e recuperação de desastre conforme os subitens seguintes. Suas descrições se encontram nos itens de mesmo número da DPC ACPR em vigor.

4.8.1. Recursos computacionais, software ou dados são corrompidos

4.8.2. Certificado de entidade é revogado

4.8.3. Chave de entidade é comprometida

4.8.4. Segurança dos recursos após desastre natural ou de outra natureza

4.8.5. Atividades das Autoridades de Registro

4.9. EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS

Os procedimentos de extinção dos serviços de AC, AR ou PSS estão descritos no item 4.9 da DPC ACPR em vigor.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

A ACPR possui procedimentos para o controle e segurança de suas instalações, descritos nos itens a seguir da DPC ACPR em vigor.

5.1. CONTROLES FÍSICOS

5.1.1. Construção e localização das instalações

5.1.2. Acesso físico

5.1.3. Energia e ar condicionado

5.1.4. Exposição à água

5.1.5. Prevenção e proteção contra incêndio

5.1.6. Armazenamento de mídia

5.1.7. Destruição de lixo

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

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

5.3. 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

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC.

São definidos também outros controles técnicos de segurança utilizados pela ACPR e pelas AR 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 Para os certificados emitidos sob esta PC, o titular de certificado indicará a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.2 Os certificados tipo A1, possuem chaves geradas através de CSP (Cryptographic Service Provider) existentes na estação servidora do solicitante. A solicitação do certificado no padrão PKCS#10 é enviada à ACPR para aprovação. Após a aprovação da solicitação, busca-se o certificado no site https://certificados.serpro.gov.br/acpr e o instala conforme os procedimentos próprios do equipamento em uso.

6.1.1.3 Para a geração das chaves criptográficas de titulares de certificado, é utilizado o algoritmo RSA, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.1.1.4 Ao ser gerada, a chave privada é gravada cifrada, por algoritmo aprovado pela ICP-Brasil, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

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 O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
b) a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida. Esta chave é protegida por meio de tecnologias atualizadas.
c) a chave privada utilizada na geração de uma assinatura é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 Esse meio de armazenamento não modifica os dados assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura. A responsabilidade pela adoção de controles de segurança para a garantia do sigilo, integridade e disponibilidade da chave privada gerada no equipamento é do Titular do Certificado e do Responsável por sua utilização.

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

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues ao titular do certificado por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da ACPR.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, sua assinatura digital, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4. Disponibilização de chave pública da AC para usuários

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da ACPR, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o formato PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1];
b) Página *web* da ACPR (https://certificados.serpro.gov.br/acpr);
c) Outros meios seguros aprovados pelo CG da 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 ACPR 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 ACPR v3 e v4 o tamanho das chaves criptográficas é de, no mínimo, 2048 (dois mil e quarenta e oito) bits.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas dos Titulares de certificado adotam, no mínimo, o padrão FIPS 140-1 ou equivalente estabelecido pelo CG da ICP-Brasil.

6.1.7 Verificação da qualidade dos parâmetros

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

6.1.8 Geração de chave por *hardware ou software*

O processo de geração do par de chaves dos Titulares do Certificado é feito por software.

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

Somente os bits digitalSignature, nonRepudiation e keyEncipherment são ativados.

6.2. PROTEÇÃO DA CHAVE PRIVADA

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

6.2.1. Padrões para módulo criptográfico

Os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1], são observados para geração das chaves criptográficas, utilizadas no âmbito da ACPR.

6.2.2. Controle "n de m" para chave privada

Item não aplicável.

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 legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. Cópia de segurança (*backup*) de chave privada

6.2.4.1 Qualquer titular de certificado emitido sob esta PC poderá, a seu critério, manter cópia de segurança de sua chave privada.

6.2.4.2 A ACPR responsável por esta PC não mantém cópia de segurança de chave privada do titular de certificado.

6.2.4.3 A cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4 A cópia de segurança deverá ser protegida por "senha".

6.2.5 Arquivamento de chave privada

6.2.5.1 Item não aplicável, uma vez que a ICP-Brasil não admite o arquivamento de chaves privadas de assinatura digital.

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. Método de ativação de chave privada

A chave privada é ativada mediante a instalação no equipamento ou servidor da requisição assinada pela ACPR. O procedimento para a ativação é definido pelo Titular do Certificado ou pelo Responsável por sua utilização.

6.2.8. Método de desativação de chave privada

A desativação da chave privada ocorre com sua exclusão do equipamento ou servidor. O procedimento para a desativação é de responsabilidade do Titular do Certificado ou do Responsável por sua utilização.

6.2.9 Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado deve ser feita através de software disponibilizado pelo fabricante da mídia, que permite apagar todas as informações nela contida, utilizando para isso a senha de acesso do titular do certificado à mídia armazenadora.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

As chaves públicas de titulares dos certificados de assinatura digital e as LCR serão armazenadas pela ACPR, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas dos titulares de certificados 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 A1 previstos nesta PC tem validade de 1 ano.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Item não aplicável.

6.4.2 Proteção dos dados de ativação

Item não aplicável.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

Os equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados dispõem de mecanismos mínimos como proteção com senha e software de CSP para geração das chaves, que garantem a segurança computacional.

6.5.2 Classificação da segurança computacional

Item descrito na DPC ACPR em vigor.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

Item descrito na DPC ACPR em vigor.

6.6.2 Controles de gerenciamento de segurança

Item descrito na DPC ACPR em vigor.

6.6.3 Classificações de segurança de ciclo de vida

Item não aplicável.

6.6.4 Controles na Geração de LCR

Item descrito na DPC ACPR em vigor.

6.7. Controles de Segurança de Rede

Item descrito na DPC ACPR em vigor.

6.8 Controles de Engenharia do Módulo Criptográfico

O Titular de Certificado deve utilizar mídias cujo módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão FIPS (*Federal Information Processing Standards*) 140-1 – requerido pela ACPR para os certificados emitidos sob esta PC.

Padrões de referência podem ser observados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

7. PERFIS DE CERTIFICADO E LCR

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

7.1 PERFIL DO CERTIFICADO

Todos os certificados emitidos pela ACPR, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 v3 ou ISSO/IEC 9594-8, especificado pelo CG da ICP-Brasil.

7.1.1 Número de Versão

Todos os certificados emitidos pela ACPR, segundo esta 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 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 ACPR;

b) "*Key Usage*", crítica: somente os bits **digitalSignature**, **nonRepudiation** e **keyEncipherment** são ativados;

c) "*Certificate Policies*", não crítica: contém o OID 2.16.76.1.2.1.3 desta PC e o endereço URL http://repositorio.serpro.gov.br/docs/dpcacpr.pdf, para os certificados emitidos pela ACPR v4.

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

- Para os certificados emitidos pela ACPR v1:

  http://ccd.serpro.gov.br/lcr/ACPRv1.crl , http://ccd2.serpro.gov.br/lcr/ACPRv1.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv1.crl

- Para os certificados emitidos pela ACPR v2:

  http://ccd.serpro.gov.br/lcr/ACPRv2.crl , http://ccd2.serpro.gov.br/lcr/ACPRv2.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv2.crl

- Para os certificados emitidos pela ACPR v3:

  http://ccd.serpro.gov.br/lcr/ACPRv3.crl, http://ccd2.serpro.gov.br/lcr/ACPRv3.crl e http://repositorio.icpbrasil.gov.br/lcr/ACPRv3.crl

- Para os certificados emitidos pela ACPR v4:

  http://repositorio.serpro.gov.br/lcr/acprv4.crl, http://certificados2.serpro.gov.br/lcr/acprv4.crl e http://repositorio.icpbrasil.gov.br/lcr/acprv4.crl

e) Não se aplica.

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

- Para os certificados emitidos pela ACPR v1:
http://ccd.serpro.gov.br/ACPR/cadeias/ACPRv1.p7b

- Para os certificados emitidos pela ACPR v2:
http://ccd.serpro.gov.br/ACPR/cadeias/ACPRv2.p7b

- Para os certificados emitidos pela ACPR v3:

http://ccd.serpro.gov.br/ACPR/cadeias/ACPRv3.p7b

- Para os certificados emitidos pela ACPR v4:
http://repositorio.serpro.gov.br/cadeias/acprv4.p7b

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

Quatro campos otherName, obrigatórios, contendo nessa ordem:

a) **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;
b) **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 ;.
c) **OID = 2.16.76.1.3.2** e conteúdo = nome do responsável pelo certificado;
d) **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 subseqüentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11(onze) posições subseqüentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do RG do responsável; nas 10 (dez) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.

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 deve ser preenchido 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.

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. A ACPR implementa ainda, para os certificados emitidos sob esta PC, as seguintes extensões definidas como opcionais pela ICP-Brasil:

a) a sub-extensão "*rfc822Name*", parte da extensão obrigatória "*Subject Alternative Name*", contendo o endereço de e-mail do titular do certificado.

b) Extended-key-usage, não crítica, contendo os seguintes valores:
"server authentication" (OID=1.3.6.1.5.5.7.3.1)
"client authentication" (OID=1.3.6.1.5.5.7.3.2)

7.1.3 Identificadores de algoritmo

7.1.3.1 Os algoritmos criptográficos utilizados para assinatura dos certificados pela ACPR são os admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1]:

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

7.1.3.1.2 Os certificados emitidos pela ACPR v3 e v4 são assinados com o uso do algoritmo criptográfico SHA-256 com função 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:

C = BR
O = ICP-Brasil
OU= Autoridade Certificadora da Presidencia da Republica
OU= *sigla do órgão solicitante*
CN = *DNS do equipamento* ou aplicação.

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

7.1.4.2. 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

Tabela 3 - Caracteres especiais admitidos em nomes

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

O OID atribuído à esta Política de Certificado é: : 2.16.76.1.2.1.3

7.1.7 Uso da extensão *"Policy Constraints"*

Item não aplicável.

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 http://repositorio.serpro.gov.br/docs/dpcacpr.pdf com a DPC da ACPR.

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. PERFIL DE LCR

7.2.1. Número de versão

As LCR geradas pela ACPR 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 ACPR adota as seguintes extensões de LCR:

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

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

c) "Authority Information Access", **não crítica**: contém o método de acesso id-ad-caIssuer e utiliza o protocolo de acesso HTTP para recuperação da cadeia de certificação.Não é utilizado nenhum outro método de acesso diferente de id-ad-caIssuer.

- Para os certificados emitidos pela ACPR v1:
http://ccd.serpro.gov.br/ACPR/cadeias/ACPRv1.p7b

- Para os certificados emitidos pela ACPR v2:
http://ccd.serpro.gov.br/ACPR/cadeias/ACPRv2.p7b

- Para os certificados emitidos pela ACPR v3:
http://ccd.serpro.gov.br/ACPR/cadeias/ACPRv3.p7b

- Para os certificados emitidos pela ACPR v4:
http://repositorio.serpro.gov.br/cadeias/acprv4.p7b

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes definem como é mantida e administrada a PC.

8.1. Procedimentos de mudança de especificação

As alterações nas especificações desta PC são realizadas pela ACPR. Quaisquer modificações são submetidas à aprovação da AC Raiz que as submeterá ao CG da ICP-Brasil.

8.2. Políticas de publicação e notificação

A cada nova versão, esta PC é publicada na página https://certificados.serpro.gov.br/acpr da ACPR.

8.3 Procedimentos de aprovação

Esta PC foi submetida à aprovação do CG da ICP-Brasil, durante o processo de credenciamento da ACPR, conforme o estabelecido no documento "Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil". Como parte desse processo, além da conformidade com os documentos definidos pela ICP-Brasil, foi verificado a compatibilidade entre esta PC e a DPC da ACPR.

9. DOCUMENTOS REFERENCIADOS

9.1. 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

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

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