

[www.serpro.gov.br](http://www.serpro.gov.br)

**Política de Certificação  
da  
Autoridade Certificadora  
do  
SERPRO ACF SSL A1**

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

(PC AC SERPRO ACF SSL A1)

Versão 3.0 de Janeiro 2021



## Sumário

Controle de Versão.....	9
1. INTRODUÇÃO.....	10
1.1. Visão Geral.....	10
1.2. Nome do Documento e Identificação.....	10
1.3. Participantes da ICP-Brasil.....	10
1.3.1. Autoridades Certificadoras.....	10
1.3.2. Autoridades de Registro.....	11
1.3.3. Titulares do Certificado.....	11
1.3.4. Partes Confiáveis.....	11
1.3.5. Outros Participantes.....	11
1.4. Usabilidade do Certificado.....	11
1.4.1. Uso apropriado do certificado.....	11
1.4.2. Uso proibitivo do certificado.....	12
1.5. Política de Administração.....	12
1.5.1. Organização administrativa do documento.....	12
1.5.2. Contatos.....	12
1.5.3. Pessoa que determina a adequabilidade da DPC com a PC.....	13
1.5.4. Procedimentos de aprovação da PC.....	13
1.6. Definições e Acrônimos.....	13
2. Responsabilidades de publicação e repositórios.....	14
2.1. Repositórios.....	14
2.2. Publicação de informações dos certificados.....	14
2.3. Tempo ou Frequência de Publicação.....	14
2.4. Controle de Acesso aos Repositórios.....	14
3. IDENTIFICAÇÃO E AUTENTICAÇÃO.....	14
3.1. Nomeação.....	15
3.1.1. Tipos de nomes.....	15
3.1.2. Necessidade dos nomes serem significativos.....	15
3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado.....	15
3.1.4. Regras para interpretação de vários tipos de nomes.....	15
3.1.5. Unicidade de nomes.....	15
3.1.6. Procedimento para resolver disputa de nomes.....	15
3.1.7. Reconhecimento, autenticação e papel de marcas registradas.....	15
3.2. Validação inicial de identidade.....	15
3.2.1. Método para comprovar a posse de chave privada.....	15
3.2.2. Autenticação da identificação da organização.....	15
3.2.3. Autenticação da identidade de equipamento ou aplicação.....	15
3.2.4. Autenticação da identidade de um indivíduo.....	15
3.2.5. Informações não verificadas do titular do certificado.....	15
3.2.6. Validação das autoridades.....	15

3.2.7. Critérios para interoperação.....	15
3.3. Identificação e autenticação para pedidos de novas chaves.....	15
3.3.1. Identificação e autenticação para rotina de novas chaves antes da expiração.....	15
3.3.2. Identificação e autenticação para novas chaves após a revogação ou expiração do certificado.....	15
3.4. Identificação e Autenticação para solicitação de revogação.....	15
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO.....	15
4.1. Solicitação do certificado.....	16
4.1.1. Quem pode submeter uma solicitação de certificado.....	16
4.1.2. Processo de registro e responsabilidades.....	16
4.2. Processamento de Solicitação de Certificado.....	16
4.2.1. Execução das funções de identificação e autenticação.....	16
4.2.2. Aprovação ou rejeição de pedidos de certificado.....	16
4.2.3. Tempo para processar a solicitação de certificado.....	16
4.3. Emissão de Certificado.....	16
4.3.1. Ações da AC durante a emissão de um certificado.....	16
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado.....	16
4.4. Aceitação de Certificado.....	16
4.4.1. Conduta sobre a aceitação do certificado.....	16
4.4.2. Publicação do certificado pela AC.....	16
4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades.....	16
4.5. Usabilidade do par de chaves e do certificado.....	16
4.5.1. Usabilidade da Chave privada e do certificado do titular.....	16
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis.....	16
4.6. Renovação de Certificados.....	16
4.6.1. Circunstâncias para renovação de certificados.....	16
4.6.2. Quem pode solicitar a renovação.....	16
4.6.3. Processamento de requisição para renovação de certificados.....	16
4.6.4. Notificação para nova emissão de certificado para o titular.....	16
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado.....	16
4.6.6. Publicação de uma renovação de um certificado pela AC.....	16
4.6.7. Notificação de emissão de certificado pela AC para outras entidades.....	16
4.7. Nova chave de certificado.....	17
4.7.1. Circunstâncias para nova chave de certificado.....	17
4.7.2. Quem pode requisitar a certificação de uma nova chave pública.....	17
4.7.3. Processamento de requisição de novas chaves de certificado.....	17
4.7.4. Notificação de emissão de novo certificado para o titular.....	17
4.7.5. Conduta constituindo a aceitação de uma nova chave certificada.....	17
4.7.6. Publicação de uma nova chave certificada pela AC.....	17
4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades.....	17
4.8. Modificação de certificado.....	17
4.8.1. Circunstâncias para modificação de certificado.....	17
4.8.2. Quem pode requisitar a modificação de certificado.....	17
4.8.3. Processamento de requisição de modificação de certificado.....	18

4.8.4. Notificação de emissão de novo certificado para o titular.....	18
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado.....	18
4.8.6. Publicação de uma modificação de certificado pela AC.....	18
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades.....	18
4.9. Suspensão e Revogação de Certificado.....	18
4.9.1. Circunstâncias para revogação.....	18
4.9.2. Quem pode solicitar revogação.....	18
4.9.3. Procedimento para solicitação de revogação.....	18
4.9.4. Prazo para solicitação de revogação.....	18
4.9.5. Tempo em que a AC deve processar o pedido de revogação.....	18
4.9.6. Requisitos de verificação de revogação para as partes confiáveis.....	18
4.9.7. Frequência de emissão de LCR.....	18
4.9.8. Latência máxima para a LCR.....	18
4.9.9. Disponibilidade para revogação/verificação de status on-line.....	18
4.9.10. Requisitos para verificação de revogação on-line.....	18
4.9.11. Outras formas disponíveis para divulgação de revogação.....	18
4.9.12. Requisitos especiais para o caso de comprometimento de chave.....	18
4.9.13. Circunstâncias para suspensão.....	18
4.9.14. Quem pode solicitar suspensão.....	18
4.9.15. Procedimento para solicitação de suspensão.....	18
4.9.16. Limites no período de suspensão.....	18
4.10. Serviços de status de certificado.....	18
4.10.1. Características operacionais.....	18
4.10.2. Disponibilidade dos serviços.....	18
4.10.3. Funcionalidades operacionais.....	19
4.11. Encerramento de atividades.....	19
4.12. Custódia e recuperação de chave.....	19
4.12.1. Política e práticas de custódia e recuperação de chave.....	19
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão.....	19
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES.....	19
5.1. Controles físicos.....	20
5.1.1 Construção e localização das instalações de AC.....	20
5.1.2. Acesso físico.....	20
5.1.3. Energia e ar-condicionado.....	20
5.1.4. Exposição à água.....	20
5.1.5. Prevenção e proteção contra incêndio.....	20
5.1.6. Armazenamento de mídia.....	20
5.1.7. Destruição de lixo.....	20
5.1.8. Instalações de segurança (backup) externas (off-site) para AC.....	20
5.2. Controles Procedimentais.....	20
5.2.1. Perfis qualificados.....	20
5.2.2. Número de pessoas necessário por tarefa.....	20
5.2.3. Identificação e autenticação para cada perfil.....	20
5.2.4. Funções que requerem separação de deveres.....	20

5.3. Controles de Pessoal.....	20
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade.....	20
5.3.2. Procedimentos de verificação de antecedentes.....	20
5.3.3. Requisitos de treinamento.....	20
5.3.4. Frequência e requisitos para reciclagem técnica.....	20
5.3.5. Frequência e sequência de rodízio de cargos.....	20
5.3.6. Sanções para ações não autorizadas.....	20
5.3.7. Requisitos para contratação de pessoal.....	20
5.3.8. Documentação fornecida ao pessoal.....	20
5.4. Procedimentos de Log de Auditoria.....	20
5.4.1. Tipos de eventos registrados.....	20
5.4.2. Frequência de auditoria de registros.....	21
5.4.3. Período de retenção para registros de auditoria.....	21
5.4.4. Proteção de registros de auditoria.....	21
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria.....	21
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo).....	21
5.4.7. Notificação de agentes causadores de eventos.....	21
5.4.8. Avaliações de vulnerabilidade.....	21
5.5. Arquivamento de Registros.....	21
5.5.1. Tipos de registros arquivados.....	21
5.5.2. Período de retenção para arquivo.....	21
5.5.3. Proteção de arquivo.....	21
5.5.4. Procedimentos de cópia de arquivo.....	21
5.5.5. Requisitos para datação de registros.....	21
5.5.6. Sistema de coleta de dados de arquivo (interno e externo).....	21
5.5.7. Procedimentos para obter e verificar informação de arquivo.....	21
5.6. Troca de chave.....	21
5.7. Comprometimento e Recuperação de Desastre.....	21
5.7.1. Procedimentos gerenciamento de incidente e comprometimento.....	21
5.7.2. Recursos computacionais, software, e/ou dados corrompidos.....	21
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade.....	21
5.7.4. Capacidade de continuidade de negócio após desastre.....	21
5.8. Extinção da AC.....	21
6. CONTROLES TÉCNICOS DE SEGURANÇA.....	21
6.1. Geração e Instalação do Par de Chaves.....	22
6.1.1. Geração do par de chaves.....	22
6.1.2. Entrega da chave privada à entidade titular.....	23
6.1.3. Entrega da chave pública para o emissor de certificado.....	23
6.1.4. Disponibilização de chave pública da AC para usuários.....	23
6.1.5. Tamanhos de chave.....	23
6.1.6. Geração de parâmetros de chaves assimétricas.....	23
6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3).....	24
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico.....	24
6.2.1. Padrão e controle para módulo criptográfico.....	24

6.2.2. Controle “n de m” para chave privada.....	24
6.2.3. Custódia ( <i>escrow</i> ) de chave privada.....	24
6.2.4. Cópia de segurança (backup) de chave privada.....	24
6.2.5. Arquivamento de chave privada.....	25
6.2.6. Inserção de chave privada em módulo criptográfico.....	25
6.2.7. Armazenamento de chave privada em módulo criptográfico.....	25
6.2.8. Método de ativação de chave privada.....	25
6.2.9. Método de desativação de chave privada.....	25
6.2.10. Método de destruição de chave privada.....	25
6.3 Outros Aspectos do Gerenciamento do Par de Chaves.....	25
6.3.1. Arquivamento de chave pública.....	25
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada..	25
6.4. Dados de Ativação.....	26
6.4.1. Geração e instalação dos dados de ativação.....	26
6.4.2. Proteção dos dados de ativação.....	26
6.4.3. Outros aspectos dos dados de ativação.....	26
6.5. Controles de Segurança Computacional.....	26
6.5.1. Requisitos técnicos específicos de segurança computacional.....	26
6.5.2 Classificação da segurança computacional.....	27
6.6. Controles Técnicos do Ciclo de Vida.....	27
6.6.1. Controles de desenvolvimento de sistema.....	27
6.6.2. Controles de gerenciamento de segurança.....	27
6.6.3. Controles de segurança de ciclo de vida.....	27
6.6.4. Controles na Geração de LCR.....	27
6.7. Controles de Segurança de Rede.....	27
6.8. Carimbo de Tempo.....	27
7. Perfis de Certificado, LCR e OCSP.....	27
7.1. Perfil do Certificado.....	28
7.1.1. Número de versão.....	28
7.1.2. Extensões de certificado.....	28
7.1.3. Identificadores de algoritmo.....	30
7.1.4. Formatos de nome.....	30
7.1.5. Restrições de nome.....	33
7.1.6. OID ( <i>Object Identifier</i> ) de Política de Certificado.....	34
7.1.7. Uso da extensão “ <i>Policy Constraints</i> ”.....	34
7.1.8. Sintaxe e semântica dos qualificadores de política.....	34
7.1.9. Semântica de processamento para extensões críticas.....	34
7.2. Perfil de LCR.....	35
7.2.1. Número de versão.....	35
7.2.2. Extensões de LCR e de suas entradas.....	35
7.3. Perfil de OCSP.....	35
7.3.1. Número(s) de versão.....	35
7.3.2. Extensões de OCSP.....	35
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....	35

8.1. Frequência e circunstâncias das avaliações.....	36
8.2. Identificação/Qualificação do avaliador.....	36
8.3. Relação do avaliador com a entidade avaliada.....	36
8.4. Tópicos cobertos pela avaliação.....	36
8.5. Ações tomadas como resultado de uma deficiência.....	36
8.6. Comunicação dos resultados.....	36
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	36
9.1. Tarifas.....	36
9.1.1. Tarifas de emissão e renovação de certificados.....	36
9.1.2. Tarifas de acesso ao certificado.....	36
9.1.3. Tarifas de revogação ou de acesso à informação de status.....	36
9.1.4. Tarifas para outros serviços.....	36
9.1.5. Política de reembolso.....	36
9.2. Responsabilidade Financeira.....	36
9.2.1. Cobertura do seguro.....	36
9.2.2. Outros ativos.....	36
9.2.3. Cobertura de seguros ou garantia para entidades finais.....	36
9.3. Confidencialidade da informação do negócio.....	36
9.3.1. Escopo de informações confidenciais.....	36
9.3.2. Informações fora do escopo de informações confidenciais.....	36
9.3.3. Responsabilidade em proteger a informação confidencial.....	36
9.4. Privacidade da informação pessoal.....	36
9.4.1. Plano de privacidade.....	36
9.4.2. Tratamento de informação como privadas.....	36
9.4.3. Informações não consideradas privadas.....	36
9.4.4. Responsabilidade para proteger a informação privadas.....	36
9.4.5. Aviso e consentimento para usar informações privadas.....	36
9.4.6. Divulgação em processo judicial ou administrativo.....	36
9.4.7. Outras circunstâncias de divulgação de informação.....	36
9.5. Direitos de Propriedade Intelectual.....	37
9.6. Declarações e Garantias.....	37
9.6.1. Declarações e Garantias da AC.....	37
9.6.2. Declarações e Garantias da AR.....	37
9.6.3. Declarações e garantias do titular.....	37
9.6.4. Declarações e garantias das terceiras partes.....	37
9.6.5. Representações e garantias de outros participantes.....	37
9.7. Isenção de garantias.....	37
9.8. Limitações de responsabilidades.....	37
9.9. Indenizações.....	37
9.10. Prazo e Rescisão.....	37
9.10.1. Prazo.....	37
9.10.2. Término.....	37
9.10.3. Efeito da rescisão e sobrevivência.....	37
9.11. Avisos individuais e comunicações com os participantes.....	37

9.12. Alterações.....	37
9.12.1. Procedimento para emendas.....	37
9.12.2. Mecanismo de notificação e períodos.....	37
9.12.3. Circunstâncias na qual o OID deve ser alterado.....	37
9.13. Solução de conflitos.....	37
9.14. Lei aplicável.....	37
9.15. Conformidade com a Lei aplicável.....	37
9.16. Disposições Diversas.....	37
9.16.1. Acordo completo.....	37
9.16.2. Cessão.....	38
9.16.3. Independência de disposições.....	38
9.16.4. Execução (honorários dos advogados e renúncia de direitos).....	38
9.17. Outras provisões.....	38
10. DOCUMENTOS REFERENCIADOS.....	38
11. REFERÊNCIAS BIBLIOGRÁFICAS.....	38

## Controle de Versão

Versão	Data	Responsável	Motivo	Descrição
2.0	Outubro/2019	Lucia Castelli	Alterações	Atualização dos requisitos Webtrust e consolidação com a versão 4.7, com a simplificação dos processos da ICP-Brasil(Resolução 151);
2.0	Outubro/2019	Osni Bunn	Aprovação	
2.1	Junho/2020	Lucia Castelli	Alterações	Alteração link para Suporte/Fraudes; Inclusão Controle de Versão. Alterações solicitadas pelo ITI;Resolução 155;
2.1	Junho/2020	Alice Vasconcellos	Aprovação	
2.2	Outubro/2020	Lucia Castelli	Alterações	Incluído novo tipo de certificado: R2C3 e alteração para cert. aplicação
2.2	Outubro/2020	Alice Vasconcellos	Aprovação	
3.0	Janeiro/2021	Lucia Castelli	Alterações	Alterações a partir da Resolução 179
3.0	Janeiro/2021	Alice Vasconcellos	Aprovação	

## 1. INTRODUÇÃO

### 1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos a serem obrigatoriamente observados pela AC SERPRO ACF SSL integrante da infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2. A PC SERPRO ACF SSL A1 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 por esta AC é o tipo A1;

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 A1, da AC SERPRO ACF SSL e OID **2.16.76.1.2.1.89**.

1.2.2. No âmbito da ICP-Brasil, os OIDs das PCs serão atribuídos na conclusão do processo de credenciamento da AC

### 1.3. Participantes da ICP-Brasil

#### 1.3.1. Autoridades Certificadoras

1.3.1.1. A Autoridade Certificadora do SERPRO FINAL SSL(AC SERPRO ACF SSL) integra a infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora

do SERPRO (AC SERPRO) e da Autoridade Certificadora Raiz Brasileira, cujo PC é implementada nesse documento.

1.3.1.2. A DPC dessa AC encontra-se publicada em sua página *Web* no seguinte endereço: <https://certificados.serpro.gov.br/serproacfssl>

### 1.3.2. Autoridades de Registro

1.3.2.1. O endereço da página *web* (*URL*) da AC SERPRO ACF SSL é <https://certificados.serpro.gov.br/serproacfssl> onde estão publicados os dados abaixo referentes as Autoridades de Registro, responsáveis pelos processos de recebimento, identificação e encaminhamento de solicitação 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, com a respectiva data do descredenciamento;

### 1.3.3. Titulares do Certificado

Titulares de Certificados são as entidades – pessoas físicas ou jurídicas, autorizados pela AR responsável a receber um certificado digital emitido pela AC, para utilização em 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

AAC 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 de Confiança - PSC conforme disponibilizado no endereço: <https://certificados.serpro.gov.br/serproacfssl>

## 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 SERPRO ACF SSL A1	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas seguintes aplicações: <ul style="list-style-type: none"><li>• Confirmação de Identidade na <i>web</i>;</li></ul>

	<ul style="list-style-type: none"><li>• Correio eletrônico;</li><li>• Transações On-Line;</li><li>• Redes privadas virtuais (VPN);</li><li>• Transações eletrônicas;</li><li>• Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.</li></ul>
--	--

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, devem levar 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 A1 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 PC é administrada pelo Centro de Certificação Digital do SERPRO(CCD-SERPRO).

### 1.5.1. Organização administrativa do documento

Autoridade Certificadora do Serpro Final – **AC SERPRO ACF SSL**

### 1.5.2. Contatos

#### Administrativo:

Nome: Pedro Moacir Rigo Motta

Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

E-mail: [certificados@serpro.gov.br](mailto:certificados@serpro.gov.br)

Telefone: (61) 2021-7957

### Suporte/Fraudes

Nome: Central de Serviços SERPRO

Página Web: <https://atendimento.serpro.gov.br/certificacaodigital>

E-mail: [css.serpro@serpro.gov.br](mailto:css.serpro@serpro.gov.br)

Telefone: 0800 7282323

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

Nome: Pedro Moacir Rigo Motta

Telefone: (61) 2021-7957

E-mail: [certificados@serpro.gov.br](mailto:certificados@serpro.gov.br)

### 1.5.4. Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.

Os procedimentos de aprovação da PC da AC são estabelecidos a critério do CG da ICP-Brasil.

### 1.6. Definições e Acrônimos

Sigla	Definição
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	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	<i>Control Objectives for Information and related Technology</i>
COSO	<i>Comitee of Sponsoring Organizations</i>
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>

DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	<i>Intrusion Detection System</i>
IEC	<i>International Electrotechnical Commission</i>
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	<i>National Institute of Standards and Technology</i>
OCSP	<i>Online Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OU	<i>Organization Unit</i>
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	<i>Proof of Possession</i>
PS	Política de Segurança
PSC	Prestação Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SNMP	<i>Simple Network Management Protocol</i>
SSL	<i>Secure Socket Layer</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Locator</i>

## 2. Responsabilidades de publicação e repositórios

Os itens seguintes estão descritos da DPC da AC.

### 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 da DPC AC SERPRO ACF SSL.

### **3.1. Nomeação**

#### **3.1.1. Tipos de nomes**

#### **3.1.2. Necessidade dos nomes serem significativos**

#### **3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado**

#### **3.1.4. Regras para interpretação de vários tipos de nomes**

#### **3.1.5. Unicidade de nomes**

#### **3.1.6. Procedimento para resolver disputa de nomes**

#### **3.1.7. Reconhecimento, autenticação e papel de marcas registradas**

### **3.2. Validação inicial de identidade**

#### **3.2.1. Método para comprovar a posse de chave privada**

#### **3.2.2. Autenticação da identificação da organização**

#### **3.2.3. Autenticação da identidade de equipamento ou aplicação**

Item 3.2.7. da DPC.

#### **3.2.4. Autenticação da identidade de um indivíduo**

Item 3.2.3. da DPC.

#### **3.2.5. Informações não verificadas do titular do certificado**

Item 3.2.4. da DPC.

#### **3.2.6. Validação das autoridades**

Item 3.2.5. da DPC.

#### **3.2.7. Critérios para interoperação**

Item 3.2.6. da DPC.

### **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 da AC.

- 4.1. Solicitação do certificado**
  - 4.1.1. Quem pode submeter uma solicitação de certificado**
  - 4.1.2. Processo de registro e responsabilidades**
- 4.2. Processamento de Solicitação de Certificado**
  - 4.2.1. Execução das funções de identificação e autenticação**
  - 4.2.2. Aprovação ou rejeição de pedidos de certificado**
  - 4.2.3. Tempo para processar a solicitação de certificado**
- 4.3. Emissão de Certificado**
  - 4.3.1. Ações da AC durante a emissão de um certificado**
  - 4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado**
- 4.4. Aceitação de Certificado**
  - 4.4.1. Conduta sobre a aceitação do certificado**
  - 4.4.2. Publicação do certificado pela AC**
  - 4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades**
- 4.5. Usabilidade do par de chaves e do certificado**
  - 4.5.1. Usabilidade da Chave privada e do certificado do titular**
  - 4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis**
- 4.6. Renovação de Certificados**
  - 4.6.1. Circunstâncias para renovação de certificados**
  - 4.6.2. Quem pode solicitar a renovação**
  - 4.6.3. Processamento de requisição para renovação de certificados**
  - 4.6.4. Notificação para nova emissão de certificado para o titular**
  - 4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado**
  - 4.6.6. Publicação de uma renovação de um certificado pela AC**
  - 4.6.7. Notificação de emissão de certificado pela AC para outras entidades**

#### **4.7. Nova chave de certificado**

##### **4.7.1. Circunstâncias para nova chave de certificado**

##### **4.7.2. Quem pode requisitar a certificação de uma nova chave pública**

##### **4.7.3. Processamento de requisição de novas chaves de certificado**

##### **4.7.4. Notificação de emissão de novo certificado para o titular**

##### **4.7.5. Conduta constituindo a aceitação de uma nova chave certificada**

##### **4.7.6. Publicação de uma nova chave certificada pela AC**

##### **4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades**

#### **4.8. Modificação de certificado**

##### **4.8.1. Circunstâncias para modificação de certificado**

##### **4.8.2. Quem pode requisitar a modificação de certificado**

- 4.8.3. Processamento de requisição de modificação de certificado**
- 4.8.4. Notificação de emissão de novo certificado para o titular**
- 4.8.5. Conduta constituindo a aceitação de uma modificação de certificado**
- 4.8.6. Publicação de uma modificação de certificado pela AC**
- 4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades**
- 4.9. Suspensão e Revogação de Certificado**
  - 4.9.1. Circunstâncias para revogação**
  - 4.9.2. Quem pode solicitar revogação**
  - 4.9.3. Procedimento para solicitação de revogação**
  - 4.9.4. Prazo para solicitação de revogação**
  - 4.9.5. Tempo em que a AC deve processar o pedido de revogação**
  - 4.9.6. Requisitos de verificação de revogação para as partes confiáveis**
  - 4.9.7. Frequência de emissão de LCR**
  - 4.9.8. Latência máxima para a LCR**
  - 4.9.9. Disponibilidade para revogação/verificação de status on-line**
  - 4.9.10. Requisitos para verificação de revogação on-line**
  - 4.9.11. Outras formas disponíveis para divulgação de revogação**
  - 4.9.12. Requisitos especiais para o caso de comprometimento de chave**
  - 4.9.13. Circunstâncias para suspensão**
  - 4.9.14. Quem pode solicitar suspensão**
  - 4.9.15. Procedimento para solicitação de suspensão**
  - 4.9.16. Limites no período de suspensão**
- 4.10. Serviços de status de certificado**
  - 4.10.1. Características operacionais**
  - 4.10.2. Disponibilidade dos serviços**

#### **4.10.3. Funcionalidades operacionais**

#### **4.11. Encerramento de atividades**

#### **4.12. Custódia e recuperação de chave**

##### **4.12.1. Política e práticas de custódia e recuperação de chave**

##### **4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão**

### **5. CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES**

Os itens seguintes estão descritos na DPC da AC.

## **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 necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC SERPRO ACF SSL A1.

São definidos também outros controles técnicos de segurança utilizados pela AC SERPRO ACF SSL 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. Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. 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. O Titular do Certificado gera a chave utilizando a página de instalação de certificados disponibilizado pela AC e a chave privada é armazenada no HD da estação. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficos e pelo uso do certificado.

A chave privada é armazenada utilizando o seguinte dispositivo: Para certificados de pessoa física ou jurídica o solicitante deverá armazenar a chave privada com nível alto de segurança, isto é, protegido por senha. A AC recomenda que seja feito backup da chave privada, evitando assim perda do certificado. Também recomenda ao Titular do Certificado a remoção do certificado do browser de sua estação, após sua utilização, caso o equipamento seja compartilhado com outros usuários.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1.]

6.1.1.4. Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICPBRASIL[1] e armazenada em repositório protegido por senha e/ou identificação biométrica, cifrado por software.

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. A Mídia Armazenadora da Chave Criptográfica é um repositório protegido por senha e/ou identificação biométrica, cifrado por software.

**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**

Chaves públicas são entregues à AC por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC.

O processo de geração das chaves acontece na estação de trabalho do titular do certificado, utilizando software de instalação provido pela autoridade certificadora.

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

A mensagem é encaminhada para a autoridade certificadora, que realiza a validação, emissão do certificado digital e a entrega deste certificado ao solicitante.

### **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 AC, compreendem:

- a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL[1];
- b) Não se aplica;
- c) Página *web* da AC: <https://certificados.serpro.gov.br/serproacfssl>
- d) Outros meios seguros aprovados pelo CG da ICP-Brasil.

### **6.1.5. Tamanhos de chave**

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC 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 no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL [1].

### **6.1.6. Geração de parâmetros de chaves assimétricas**

Os parâmetros de geração e verificação de chaves assimétricas do usuário final adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

### **6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)**

Os certificados emitidos pela AC têm no campo “Key usage” (2.5.29.15) ativado os bits *digitalSignature*, podendo conter os bits *keyEncipherment* e *nonRepudiation* ativados;

Os certificados emitidos sob esta PC pela AC são apropriados ao uso apenas nas aplicações apresentadas a seguir:

- a) Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas seguintes aplicações;
- b) Confirmação de Identidade na web;
- c) Correio eletrônico;
- d) Transações On-Line;
- e) Redes privadas virtuais (VPN);
- f) Transações eletrônicas;
- g) Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

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

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

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

### **6.2.1. Padrão e controle para módulo criptográfico**

6.2.1.1. Não se aplica.

6.2.1.2. 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 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 não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3. Não se aplica.

6.2.4.4. Não se aplica.

#### **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**

Não se aplica.

#### **6.2.7. Armazenamento de chave privada em módulo criptográfico**

Ver item 6.1.

#### **6.2.8. Método de ativação de chave privada**

A chave privada do usuário final é ativada, mediante senha solicitada pelo software de proteção da chave privada. A senha deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo.

O Titular de certificado deverá adotar senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 3(três) meses.

#### **6.2.9. Método de desativação de chave privada**

A desativação da chave privada ocorre no fechamento do “browser” utilizado para estabelecer uma conexão segura.

#### **6.2.10. Método de destruição de chave privada**

A destruição da chave privada do certificado deve ser feita pelo próprio usuário final, por meio da eliminação do arquivo que à contém.

### **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. A chave privada da AC e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. Certificados do tipo A1, previsto nesta PC, tem validade de até 1 ano.

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**

Não se aplica.

#### **6.4.2. Proteção dos dados de ativação**

Não se aplica.

#### **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 gera a chave utilizando a página de instalação de certificados disponibilizado pela AC e a chave privada é armazenada no HD da estação.

Nos equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados emitidos pela AC SERPRO ACF SSL, recomenda-se o uso de mecanismos que garantam a segurança computacional, tais como:

- a) Senha de bios ativada;
- b) Controle de acesso lógico ao sistema operacional;
- c) Existência de uso de senhas fortes;
- d) Diretivas de senha e de bloqueio de contas;

- e) Antivírus, antitrojan e antispymware instalados, atualizados e habilitados;
- f) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc); e
- h) Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

AAC recomenda ainda:

- a) que seja feito backup da chave privada, evitando assim perda do certificado; e
- b) a remoção do certificado do browser da estação, após sua utilização, caso o equipamento seja compartilhado com outros usuários.

### **6.5.2 Classificação da segurança computacional**

Não se aplica.

## **6.6. Controles Técnicos do Ciclo de Vida**

AAC 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. Controles de segurança de ciclo de vida**

Não se aplica.

### **6.6.4. Controles na Geração de LCR**

Todas as LCR geradas pela AC 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 da DPC.

## **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 LCR 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

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

#### 7.1.1. Número de versão

Todos os certificados emitidos pela AC implementa 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 SERPRO ACF SSL A1 descreve todas as extensões de certificado utilizadas e sua criticalidade.

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 SERPRO ACF;
- b) **“Key Usage”**, crítica: configurados conforme disposto no item 7.1.2.7 deste documento;
- c) **“Certificate Policies”**, não crítica: contém o **OID 2.16.76.1.2.1.89**. e o endereço URL da página Web e <http://repositorio.serpro.gov.br/docs/dpcserproacfssl.pdf> com a DPC da AC.
- d) **“CRL Distribution Points”**, não crítica: contém o endereço URL da página Web onde se obtém a LCR da AC:

<http://repositorio.serpro.gov.br/lcr/acserproacfssl.crl>

e

<http://certificados2.serpro.gov.br/lcr/acserproacfssl.crl>.

- e) **“Authority Information Access”**, não crítica, contendo o método de acesso id-ad-calssuer, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação no seguinte endereço:

<http://repositorio.serpro.gov.br/cadeias/acserproacfssl.p7b>

A segunda entrada contém o método de acesso id-ad-ocsp, com o respectivo endereço <http://ocsp.serpro.gov.br/acserproacfssl> do respondedor OCSP, utilizando o protocolo de acesso, HTTP.

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, 3 (três) campos *otherName*, obrigatórios, contendo:

Não se aplica.

b) Para certificados de Pessoa Jurídica, 4 (quatro) campos *otherName*, obrigatórios, contendo:

Não se aplica.

c) Para certificado de 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 ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

c.2) 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) 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, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;

- 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) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;
- h) Não se aplica.

7.1.2.5. Campos *othertype* 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. As extensões “Key Usage” e “Extended Key Usage” para os referidos tipos de certificado são obrigatórias e obedece o propósito 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) Não se aplica.
- f) para os demais 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 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 PC, em conformidade com a RFC 5280;

- g) Não se aplica.

### 7.1.3. Identificadores de algoritmo

Os algoritmos criptográficos utilizados para assinatura dos certificados pela AC são os admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-

BRASIL [1]. Os certificados emitidos pela AC SERPRO ACF SSL 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:

. Para o certificado de aplicação, o identificador CN conterà o nome da aplicação:

C = BR

O = ICP-Brasil

OU= Autoridade Certificadora SERPRO ACF SSL

OU = Nome da AR responsável pela aprovação do certificado

OU = CNPJ da AR onde ocorreu a identificação presencial

OU = Aplicacao A1

CN = nome da aplicação

. Para o certificado de aplicação COMPE, o identificador CN conterà as seguintes informações:

C=BR

O=ICP-Brasil

OU=IF-AAAAAAAA

OU=SSSSS-BBBBBBBBBBB

OU = CNPJ da AR onde ocorreu a identificação presencial

CN=CCCC-Nome da Instituição Financeira, Onde:

“IF-“ – são três posições fixas com este conteúdo e significa Instituição Financeira;

AAAAAAAA (oito posições numéricas) - Identificador usando o número base do CNPJ. (ex: 12.345.678/0001-04);

SSSSS (cinco posições alfanuméricas) – Indicador da aplicação, neste caso será COMPE;

BBBBBBBBBB (dez posições alfanuméricas) - campo alfanumérico que pode ser utilizado pela IF para controle interno de seus certificados;

. Para o certificado de aplicação ECO, o identificador CN conterà as seguintes informações:

C=BR

O=ICP-Brasil

OU=(Nome da Instituição)

OU=YYY Zxxx

OU= nnnnnnn (onde nnnnnnn é o número base do CNPJ)

OU = CNPJ da AR onde ocorreu a identificação presencial

CN= O common name é composto pelo host+domínio registrado pela IF.

Onde:

Os certificados emitidos para os ambientes serão identificados pelo conteúdo do campo "OU = YYY Zxxx" onde YYY deve ser substituído pelo código "CBC" (no caso de IF) ou "DTP" (no caso Dataprev), seguido de um espaço em branco (" "), acrescido da sequência "Zxxx", onde "Z" identifica o ambiente (p=produção ou h=homologação), e "xxx" é o CBC (no caso de IF) ou 8184 (no caso Dataprev).

. Para o certificado Câmara de Cessões de Crédito – C3, com as seguintes informações:

C=BR

O=ICP-Brasil

OU=cccccccc (Onde ccccccc é o número base do CNPJ)

OU=CCC Pxxx ou Txxx

OU=Nome da Instituição

OU = CNPJ da AR onde ocorreu a identificação presencial

CN= O common name é composto pelo host+domínio registrado pela IF

Onde: CCC → Câmara de Cessões de Crédito

. Para certificados do Tipo SPB(Sistema de Pagamento Brasileiro):

C=BR

O=ICP-Brasil

OU=ISPB-cccccccc (Onde "cccccc" é o número base do CNPJ)

OU=SISBACEN-iiii (Onde "iiii" é o código do Sisbacen)

OU = CNPJ da AR onde ocorreu a identificação presencial

CN= Identificação única da instituição certificada e do certificado (ex: P ou T + número sequencial, segundo informação da IF)

Onde:

Os certificados emitidos para o ambiente de produção serão identificados pelo conteúdo do campo “CN”, com a letra “P”. Os certificados emitidos para o ambiente de homologação deverão conter a letra “T”.

. Para certificados do Tipo R2C3:

C=BR (campo preenchido automaticamente pela AC emissora do certificado digital);

O=ICP-Brasil (campo preenchido automaticamente pela AC emissora do certificado digital);

OU= Nome da Instituicao;

OU=cccccccc (onde cccccccc e o numero base do CNPJ);

OU= RRC Pxxx ou Txxx (producao=P e homologacao=T), e "xxx" e uma numeracao sequencial unica de geracao do par de chaves;

CN= O common name e composto pelo host+dominio internet registrado pela IF. No exemplo: srv01.if.com.br, o "srv01e o host, "if.com.br" e o dominio;

Para todos os certificados o conteúdo do campo Domínio do Certificado será a identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for seu empregado, funcionário ou servidor.

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

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 dos certificados.

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 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 **2.16.76.1.2.1.89** foi atribuído a Política de Certificado. 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* com a DPC da AC a saber:

<http://certificados2.serpro.gov.br/docs/dpcserproacfssl.pdf>

<https://repositorio.serpro.gov.br/docs/dpcserproacfssl.pdf>

### 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 AC segundo a 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; e
- b) “**CRL Number**”, não crítica: contém número sequencial para cada LCR emitida.

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

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

“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

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

O campo “Authority Information Access”, não crítica, contém o método de acesso *id-ad-caIssuer*, que utiliza o protocolo de acesso HTTP para a recuperação da cadeia do certificado;

A segunda entrada desse campo contém o método de acesso *id-ad-ocsp*, com o respectivo endereço <http://ocsp.serpro.gov.br/acserproacfssl> do respondedor OCSP, utilizando o protocolo de acesso, HTTP e OID: 1.3.6.1.5.5.7.48.1

## 8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

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

- 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. 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.

### **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 e AR e outras entidades citadas. Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

### 9.16.2. Cessão

### 9.16.3. Independência de disposições

### 9.16.4. Execução (honorários dos advogados e renúncia de direitos)

### 9.17. Outras provisões

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 responsável.

## 10. DOCUMENTOS REFERENCIADOS

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

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
[6]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

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

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

## 11. REFERÊNCIAS BIBLIOGRÁFICAS

[6] WebTrust Principles and Criteria for Registration Authorities, disponível em <http://www.webtrust.org>

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.