Política de Certificado de Sigilo Tipo S1 da Autoridade Certificadora de Defesa (AC Defesa)

(PC S1 da AC Defesa)

Versão 2.0 de Dezembro de 2022

Infraestrutura de Chaves Públicas Brasileira
ICP - Brasil

Sumário

CONTROLE DE ALTERAÇÕES **10**

1 INTRODUÇÃO **11**
1.1 Visão Geral . . . 11
1.2 Nome do Documento e Identificação . . . 11
1.3 Participantes da ICP-Brasil . . . 11
1.3.1 Autoridades Certificadoras . . . 11
1.3.2 Autoridades de Registro . . . 12
1.3.3 Titulares do Certificado . . . 12
1.3.4 Partes Confiáveis . . . 12
1.3.5 Outros Participantes . . . 12
1.4 Usabilidade do Certificado . . . 12
1.4.1 Uso apropriado do certificado . . . 12
1.4.2 Uso proibitivo do certificado . . . 13
1.5 Política de Administração . . . 13
1.5.1 Organização administrativa do documento . . . 13
1.5.2 Contatos . . . 13
1.5.3 Pessoa que determina a adequabilidade da DPC com a PC . . . 14
1.5.4 Procedimentos de aprovação da PC . . . 14
1.6 Definições e Acrônimos . . . 14

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO **15**
2.1 Repositórios . . . 15
2.2 Publicação de informações dos certificados . . . 15
2.3 Tempo ou Frequência de Publicação . . . 15
2.4 Controle de Acesso aos Repositórios . . . 15

3 IDENTIFICAÇÃO E AUTENTICAÇÃO **15**
3.1 Atribuição de Nomes . . . 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 . . . 16
3.1.4 Regras para interpretação de vários tipos de nomes . . . 16
3.1.5 Unicidade de nomes . . . 16
3.1.6 Procedimento para resolver disputa de nomes . . . 16
3.1.7 Reconhecimento, autenticação e papel de marcas registradas . . . 16
3.2 Validação inicial de identidade . . . 16

3.2.1 Método para comprovar a posse de chave privada 16
3.2.2 Autenticação da identificação da organização 16
3.2.3 Autenticação da identidade de equipamento ou aplicação 16
3.2.4 Autenticação da identidade de um indivíduo 16
3.2.5 Informações não verificadas do titular do certificado 16
3.2.6 Validação das autoridades 16
3.2.7 Critérios para interoperação 16
3.3 Identificação e autenticação para pedidos de novas chaves 16
3.3.1 Identificação e autenticação para rotina de novas chaves 16
3.3.2 Identificação e autenticação para novas chaves após a revogação . . 16
3.4 Identificação e Autenticação para solicitação de revogação 16

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO 17

4.1 Solicitação do certificado 17
4.1.1 Quem pode submeter uma solicitação de certificado 17
4.1.2 Processo de registro e responsabilidades 17
4.2 Processamento de Solicitação de Certificado 17
4.2.1 Execução das funções de identificação e autenticação 17
4.2.2 Aprovação ou rejeição de pedidos de certificado 17
4.2.3 Tempo para processar a solicitação de certificado 17
4.3 Emissão de Certificado 17
4.3.1 Ações da AC durante a emissão de um certificado 17
4.3.2 Notificações para o titular do certificado pela AC na emissão do certificado 17
4.4 Aceitação de Certificado 17
4.4.1 Conduta sobre a aceitação do certificado 17
4.4.2 Publicação do certificado pela AC 17
4.4.3 Notificação de emissão do certificado pela AC Raiz para outras entidades 17
4.5 Usabilidade do par de chaves e do certificado 17
4.5.1 Usabilidade da Chave privada e do certificado do titular 17
4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis . 17
4.6 Renovação de Certificados 17
4.6.1 Circunstâncias para renovação de certificados 17
4.6.2 Quem pode solicitar a renovação 17
4.6.3 Processamento de requisição para renovação de certificados 18
4.6.4 Notificação para nova emissão de certificado para o titular 18
4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado 18

4.6.6 Publicação de uma renovação de um certificado pela AC 18
4.6.7 Notificação de emissão de certificado pela AC para outras entidades 18
4.7 Nova chave de certificado 18
4.7.1 Circunstâncias para nova chave de certificado 18
4.7.2 Quem pode requisitar a certificação de uma nova chave pública . . 18
4.7.3 Processamento de requisição de novas chaves de certificado 18
4.7.4 Notificação de emissão de novo certificado para o titular 18
4.7.5 Conduta constituindo a aceitação de uma nova chave certificada . . 18
4.7.6 Publicação de uma nova chave certificada pela AC 18
4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades 18
4.8 Modificação de certificado 18
4.8.1 Circunstâncias para modificação de certificado 18
4.8.2 Quem pode requisitar a modificação de certificado 18
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 19
4.9.3 Procedimento para solicitação de revogação 19
4.9.4 Prazo para solicitação de revogação 19
4.9.5 Tempo em que a AC deve processar o pedido de revogação 19
4.9.6 Requisitos de verificação de revogação para as partes confiáveis . . . 19
4.9.7 Frequência de emissão de LCR 19
4.9.8 Latência máxima para a LCR 19
4.9.9 Disponibilidade para revogação/verificação de status on-line 19
4.9.10 Requisitos para verificação de revogação on-line 19
4.9.11 Outras formas disponíveis para divulgação de revogação 19
4.9.12 Requisitos especiais para o caso de comprometimento de chave . . . 19
4.9.13 Circunstâncias para suspensão 19
4.9.14 Quem pode solicitar suspensão 19
4.9.15 Procedimento para solicitação de suspensão 19
4.9.16 Limites no período de suspensão 19
4.10 Serviços de status de certificado 19
4.10.1 Características operacionais 19

4.10.2 Disponibilidade dos serviços . . . 19
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 DE INSTALAÇÕES 20
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 . . . 21
5.4 Procedimentos de Log de Auditoria . . . 21
5.4.1 Tipos de eventos registrados . . . 21
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 22

6 CONTROLES TÉCNICOS DE SEGURANÇA 22
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 do certificado 23
6.1.3 Entrega da chave pública para emissor de certificado 23
6.1.4 Entrega de chave pública da AC às terceiras partes 23
6.1.5 Tamanhos de chave 24
6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros 24
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 *(escrow)* de chave privada 25
6.2.4 Cópia de segurança de chave privada 25
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 . . . 26
6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES . 26
6.3.1 Arquivamento de chave pública . . . 26
6.3.2 Períodos de operação do certificado e períodos de uso para as chaves pública e privada . . . 26
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 . . . 27
6.4.3 Outros aspectos dos dados de ativação . . . 27
6.5 Controles de Segurança Computacional . . . 27
6.5.1 Requisitos técnicos específicos de segurança computacional . . . 27
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 . . . 28
6.6.3 Controles de segurança de ciclo de vida . . . 28
6.6.4 Controles na Geração de LCR . . . 28
6.7 Controles de Segurança de Rede . . . 28
6.8 Carimbo de Tempo . . . 28

7 PERFIS DE CERTIFICADO, LCR E OCSP 28
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 . . . 32
7.1.4 Formatos de nome . . . 32
7.1.5 Restrições de nome . . . 33
7.1.6 OID (Object Identifier) de Política de Certificado . . . 34
7.1.7 Uso da extensão "*Policy Constraints*" . . . 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 . . . 34
7.2.1 Número de versão . . . 34
7.2.2 Extensões de LCR e de suas entradas . . . 34
7.3 PERFIL DE OCSP . . . 34
7.3.1 Número(s) de versão . . . 34
7.3.2 Extensões de OCSP . . . 35

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES 35
8.1 Frequência e circunstâncias das avaliações . . . 35
8.2 Identificação/Qualificação do avaliador . . . 35
8.3 Relação do avaliador com a entidade avaliada . . . 35
8.4 Tópicos cobertos pela avaliação . . . 35
8.5 Ações tomadas como resultado de uma deficiência . . . 35
8.6 Comunicação dos resultados . . . 35

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 35
9.1 Tarifas . . . 35
9.1.1 Tarifas de emissão e renovação de certificados . . . 35
9.1.2 Tarifas de acesso ao certificado . . . 35
9.1.3 Tarifas de revogação ou de acesso à informação de status . . . 35
9.1.4 Tarifas para outros serviços . . . 35
9.1.5 Política de reembolso . . . 35
9.2 Responsabilidade Financeira . . . 35
9.2.1 Cobertura do seguro . . . 35
9.2.2 Outros ativos . . . 35
9.2.3 Cobertura de seguros ou garantia para entidades finais . . . 35
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 . . . 36
9.6 Declarações e Garantias . . . 36
9.6.1 Declarações e Garantias da AC . . . 36
9.6.2 Declarações e Garantias da AR . . . 36
9.6.3 Declarações e garantias do titular . . . 36
9.6.4 Declarações e garantias das terceiras partes . . . 36
9.6.5 Representações e garantias de outros participantes . . . 36
9.7 Isenção de garantias . . . 36

9.8 Limitações de responsabilidades . . . 36
9.9 Indenizações . . . 36
9.10 Prazo e Rescisão . . . 36
9.10.1 Prazo . . . 36
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 . . . 37
9.16.3 Independência de disposições . . . 37
9.16.4 Execução (honorários dos advogados e renúncia de direitos) . . . 37
9.17 Outras provisões . . . 37

10 DOCUMENTOS REFERENCIADOS 38

11 REFERÊNCIAS BIBLIOGRÁFICAS 38

CONTROLE DE ALTERAÇÕES

Versão	Data	Motivo	Descrição da Alteração
1.0	24/04/2017	Versão Inicial	Versão inicial, de acordo com o DOC-ICP-04 versão 6.0
1.1	15/09/2017	Atualização	Atualizado de acordo com o DOC-ICP-04 versão 6.3
1.2	01/02/2019	Atualização	Atualizado de acordo com o DOC-ICP-04 versão 6.7
2.0	20/12/2022	Atualização	Atualizado de acordo com o DOC-ICP-04 versão 8.1

1 INTRODUÇÃO

1.1 Visão Geral

1.1.1 Este documento estabelece os requisitos mínimos a serem obrigatoriamente observados pela Autoridade Certificadora de Defesa - AC Defesa, integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na elaboração de suas Políticas de Certificado (PC).

1.1.2 A estrutura desta PC está baseada no DOC-ICP-04 REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [2].

1.1.3 A estrutura desta PC está baseada na RFC 3647 *(Internet X.509 Public Key Infrastructure - Certificate Policy and Certication Practices Framework).*

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

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

1.1.6 Não se aplica

1.1.7 Não se aplica

1.1.8 Não se aplica

1.1.9 Não se aplica

1.1.10 Não se aplica

1.1.11 Não se aplica

1.1.12 Não se aplica

1.2 Nome do Documento e Identificação

1.2.1 Esta PC é chamada "Política de Certificado de Sigilo, Tipo S1, da Autoridade Certificadora de Defesa (AC Defesa)" e referida como "PC S1 da AC Defesa". O OID (*object identifier*) desta PC é **2.16.76.1.2.101.17.**

1.2.2 No âmbito da ICP-Brasil, o OID desta PC foi atribuído na conclusão do processo de credenciamento da AC Defesa.

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

1.3.1.1 Esta PC se refere unicamente à AC Defesa, integrante da ICP-Brasil.

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

1.3.2 Autoridades de Registro

1.3.2.1 O endereço da página web (URL) da AC Defesa é *https://www.acdefesa.mil.br*, onde estão publicados os dados a seguir, referentes as Autoridades de Registro (AR) vinculadas à AC Defesa e 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 ARs credenciadas; e

b) relação de ARs que tenham se descredenciado da cadeia da AC Defesa, com a respectiva data do descredenciamento.

1.3.3 Titulares do Certificado

Titulares de Certificados são as entidades - pessoas físicas ou jurídicas - autorizadas pela AR responsável a receber um certificado digital, emitido pela AC Defesa, para sua própria utilização.

1.3.4 Partes Confiáveis

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

1.3.5 Outros Participantes

A AC Defesa publica em sua página web, *https://www.acdefesa.mil.br*, o Prestador de Serviços Biométricos (PSBios) a ela vinculado.

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

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

1.4.1.2 As aplicações e demais programas que admitem o uso de certificado digital de um determinado tipo, contemplado pela ICP-Brasil, aceitam qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.4.1.3 A AC Defesa leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos 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 Não se aplica.

1.4.1.5 Os certificados emitidos pela AC Defesa no âmbito desta PC podem ser utilizados em aplicações tais como cifração de documentos, de bases de dados, de mensagens e de outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

1.4.1.6 Não se aplica.

1.4.1.7 Não se aplica.

1.4.1.8 Não se aplica.

1.4.2 Uso proibitivo do certificado

Não há restrições de aplicações identificadas.

1.5 Política de Administração

Esta PC é administrada pela AC Defesa e neste item listar-se-á endereço e outras informações.

1.5.1 Organização administrativa do documento

Autoridade Certificadora de Defesa (AC Defesa).

1.5.2 Contatos

Nome: Marcos Elias dos Prazeres Caetano
Endereço: Centro Integrado de Telemática do Exército - CITEx, Av. Duque de Caxias, s/n, Setor Militar Urbano, CEP 70630-100 - Brasília-DF
Telefone: (61) 2035-1076
Página web: https://www.acdefesa.mil.br
E-mail: contato@acdefesa.mil.br

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: André Luiz Cibin Ribeiro
Telefone: (61) 2035-1070
E-mail: andre@acdefesa.mil.br

1.5.4 Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI, de acordo com os procedimentos de aprovação estabelecidos a critério do Comitê Gestor da ICP-Brasil.

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CONFAZ	Conselho Nacional de Política Fazendária
COBIT	*Control Objectives for Information and related Technology*
COSO	*Comitee of Sponsoring Organizations*
CPF	Cadastro de Pessoas Físicas
CS	*Code Sign*
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation*
ICP-Brasil	Infraestrutura de Chaves Pública Brasileira
IDS	Sistemas de Detecção de Intrusão
IEC	*International Electrotechnical Commission*
INMETRO	Innstituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira

SIGLA	DESCRIÇÃO
NIS	Número de Identificação Social
NIST	*National Institute of Standards and Technology*
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificados
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SSL	*Secure Socket Layer*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Os itens seguintes são referidos nos itens correspondentes da DPC da AC Defesa.

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 são referidos nos itens correspondentes da DPC da AC Defesa.

3.1 Atribuição de Nomes

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 Defesa.

4.1 Solicitação do certificado

4.1.1 Quem pode submeter uma solicitação de certificado

4.1.2 Processo de registro e responsabilidades

4.2 Processamento de Solicitação de Certificado

4.2.1 Execução das funções de identificação e autenticação

4.2.2 Aprovação ou rejeição de pedidos de certificado

4.2.3 Tempo para processar a solicitação de certificado

4.3 Emissão de Certificado

4.3.1 Ações da AC durante a emissão de um certificado

4.3.2 Notificações para o titular do certificado pela AC na emissão do certificado

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado

4.4.2 Publicação do certificado pela AC

4.4.3 Notificação de emissão do certificado pela AC Raiz para outras entidades

4.5 Usabilidade do par de chaves e do certificado

4.5.1 Usabilidade da Chave privada e do certificado do titular

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

4.6 Renovação de Certificados

4.6.1 Circunstâncias para renovação de certificados

4.6.2 Quem pode solicitar a renovação

4.6.3 Processamento de requisição para renovação de certificados

4.6.4 Notificação para nova emissão de certificado para o titular

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

4.6.6 Publicação de uma renovação de um certificado pela AC

4.6.7 Notificação de emissão de certificado pela AC para outras entidades

4.7 Nova chave de certificado

4.7.1 Circunstâncias para nova chave de certificado

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

4.7.3 Processamento de requisição de novas chaves de certificado

4.7.4 Notificação de emissão de novo certificado para o titular

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

4.7.6 Publicação de uma nova chave certificada pela AC

4.7.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.8 Modificação de certificado

4.8.1 Circunstâncias para modificação de certificado

4.8.2 Quem pode requisitar a modificação de certificado

Não se aplica

4.8.3 Processamento de requisição de modificação de certificado

4.8.4 Notificação de emissão de novo certificado para o titular

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

4.8.6 Publicação de uma modificação de certificado pela AC

4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades

4.9 Suspensão e Revogação de Certificado

4.9.1 Circunstâncias para revogação

4.9.2 Quem pode solicitar revogação

4.9.3 Procedimento para solicitação de revogação

4.9.4 Prazo para solicitação de revogação

4.9.5 Tempo em que a AC deve processar o pedido de revogação

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

4.9.7 Frequência de emissão de LCR

4.9.8 Latência máxima para a LCR

4.9.9 Disponibilidade para revogação/verificação de status on-line

4.9.10 Requisitos para verificação de revogação on-line

4.9.11 Outras formas disponíveis para divulgação de revogação

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.13 Circunstâncias para suspensão

4.9.14 Quem pode solicitar suspensão

4.9.15 Procedimento para solicitação de suspensão

4.9.16 Limites no período de suspensão

4.10 Serviços de status de certificado

4.10.1 Características operacionais

4.10.2 Disponibilidade dos serviços

4.10.3 Funcionalidades operacionais

4.11 Encerramento de atividades

4.12 Custódia e recuperação de chave

4.12.1 Política e práticas de custódia e recuperação de chave

4.12.2 Política e práticas de encapsulamento e recuperação de chave de sessão

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

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

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 S1 da AC Defesa. São definidos também outros controles técnicos de segurança utilizados pela AC Defesa e pelas ARs vinculadas na execução de suas funções operacionais.

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

6.1.1.1 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 A geração do par de chaves criptográficas ocorre por meio de *software* de geração de chaves disponível na página *web* da AC Defesa. Quando da geração, a chave privada é armazenada no dispositivo eletrônico de armazenamento do computador do solicitante. A chave privada poderá ser exportada e/ou armazenada (cópia de segurança) em mídia externa (*pendrive*, *token* ou cartão inteligente) e deverá ser protegida por senha de acesso.

6.1.1.3 O algoritmo utilizado para as chaves criptográficas de titulares de certificados da AC Defesa adota o padrão RSA conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.4 Ao ser gerada, a chave privada da entidade titular do certificado é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1] e armazenada em repositório protegido por senha e/ou identificação biométrica, cifrado por *software*, conforme a seguir:

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

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 utilizado pelo titular 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;

c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

6.1.1.8 Não se aplica.

6.1.1.9 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**, conforme especificado no Termo de Titularidade, no caso de certificados de pessoa física, **e da pessoa responsável**, indicada por seus(s) representante(s) legal(is), conforme especificado no Termo de Responsabilidade, no caso de certificados de pessoa jurídica.

6.1.2 Entrega da chave privada à entidade titular do certificado

Não se aplica.

6.1.3 Entrega da chave pública para emissor de certificado

A entrega da chave pública do solicitante do certificado para a AC Defesa é feita por meio eletrônico, em formato PKCS#10, por intermédio de uma sessão segura *SSL* provida pelo *software* de certificação da AC Defesa.
O processo de geração das chaves ocorre na estação de trabalho do titular do certificado, utilizando o *software* de geração de chaves fornecido pela AC Defesa em sua página *web*.

6.1.4 Entrega de chave pública da AC às terceiras partes

As formas utilizadas pela AC Defesa para disponibilizar o seu certificado e todos os certificados de sua cadeia de certificação, para os usuários da ICP-Brasil, são os seguintes:

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) por intermédio do endereço *web https://www.acdefesa.mil.br/index.php/repositorio*;

d) outros meios seguros aprovados pelo CG ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1 O tamanho das chaves criptográficas associadas aos certificados Tipo S1 emitidos pela AC Defesa é de **2048 bits.**

6.1.5.2 Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo S1 da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

6.1.6 Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros

Os parâmetros de geração e verificação de chaves assimétricas 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 do tipo S1 emitidos pela AC Defesa têm no campo "key usage" (2.5.29.15) ativado os bits *keyEncipherment e dataEncipherment*.
Os certificados emitidos pela AC Defesa, sob esta PC, são considerados adequados para cifração de documentos, de bases de dados, de mensagens e de outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

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 de chave privada

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

6.2.4.2 A AC Defesa não mantém cópia de segurança de chave privada de titular de certificado de sigilo por ela emitido.

6.2.4.3 A cópia de segurança da chave privada de certificado digital, emitido sob esta PC, 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 O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia seja efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1 A AC Defesa não arquiva cópias de chaves privadas de sigilo de titulares de certificados.

6.2.5.2 Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6 Inserção de chave privada em módulo criptográfico

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.

6.2.9 Método de desativação de chave privada

A desativação da chave privada ocorre com o fechamento da aplicação que está utilizado o certificado para estabelecer uma conexão segura. O titular de certificado pode definir

outros procedimentos necessários para a desativação de sua chave privada.

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 no respectivo local de armazenamento.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública

A AC Defesa Defesa armazena as chaves públicas da própria AC Defesa e dos titulares de certificados de sigilo por ela emitidos, bem como as LCR emitidas, apos a expiração dos certificados correspondentes, permanentemente, na forma da legislação em vigor, para verificação de cifrações geradas durante seu período de validade.

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

6.3.2.1 As chaves privadas de sigilo dos respectivos titulares de certificados emitidos pela AC Defesa são utilizadas apenas durante período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação das cifrações geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

6.3.2.3 O período máximo de validade admitido para certificados de Sigilo Tipo S1 da AC Defesa é de **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.

6.4.1 Geração e instalação dos dados de ativação

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

6.4.2 Proteção dos dados de ativação

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

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. Nos equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados emitidos pela AC Defesa, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, dentre eles:

a) Senha de *bios* ativada;

b) Existência de uso de senhas fortes;

c) Antivírus, *antitrojan e antispyware* instalados, atualizados e habilitados;

d) *Firewall* pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;

e) Sistema operacional atualizado, com aplicação de correções necessárias (*patches, hotfix,* etc); e

f) Proteção de tela configurada para ser acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 Classificação da segurança computacional

Não se aplica.

6.6 Controles Técnicos do Ciclo de Vida

A AC Defesa 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

As LCR geradas pela AC Defesa são verificadas quanto à consistência de seu conteúdo, sendo checados número da LCR, data/hora de emissão e outras informações relevantes.

6.7 Controles de Segurança de Rede

Não se aplica.

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 Defesa 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 Defesa 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 AC Defesa S1 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 AC;

b) ***"Key Usage"*, crítica:** somente os bits *keyEncipherment* e *dataEncipherment* estão ativados, configurados conforme disposto no item 7.1.2.7 deste documento;

c) ***"Certificate Policies"*, não crítica:**

1) o campo *policyIdentifier* contém o OID desta PC: 2.16.76.1.2.101.17;

2) o campo *policyQualifiers* contém o endereço *web* da DPC AC Defesa que emite o certificado: *https://repositorio-acp.acdefesa.mil.br/docs/dpc-acdefesa.pdf.*

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

1) *https://repositorio-acp.acdefesa.mil.br/lcr/acdefesa-v0.crl*;

2) *https://repositorio-acr.acdefesa.mil.br/lcr/acdefesa-v0.crl.*

e) ***"Authority Information Access"*, não crítica:** A primeira entrada contém o método de acesso *id-ad-calssuer*, utilizando o protocolo de acesso HTTPS, para a recuperação da cadeia de certificação no seguinte endereço:

1) *https://repositorio-acp.acdefesa.mil.br/aia/acdefesa-v0.p7b.*

7.1.2.3 Os certificados emitidos pela AC Defesa possuem a extensão ***"Subject Alternative Name"*, não crítica**, definida como obrigatória pela ICP-Brasil e com os seguintes formatos:

a) **Para certificado de pessoa física:**

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

OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social - NIS (PIS,PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva unidade da federação;

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

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

a.2) Não se aplica;

a.3) 1 (um) campo *otherName*, obrigatório, para certificados vinculados ao Documento RIC, contendo:

OID = 2.16.76.1.3.9 e conteúdo = nas primeiras 11 (onze) posições, o número de Registro de Identidade Civil.

a.4) 1 (um) campo *otherName*, obrigatório para certificados digitais emitidos para servidor público federal e militar, contendo:

OID = 2.16.76.1.3.11 e conteúdo = nas primeiras 10 (dez) posições, o cadastro único do servidor público federal da ativa e militares da União constante, respectivamente, no Sistema de Gestão de Pessoal (SIGEPE) mantido pelo Ministério do Planejamento e nos Sistemas de Gestão de Pessoal das Forças Armadas.

a.5) 1 (um) campo *otherName*, não obrigatório, contendo:

rfc822Name, contém o endereço e-mail do titular do certificado;

b) **Para certificado de pessoa jurídica:**

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

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social - NIS (PIS, PASEP ou CI); 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;

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

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

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

b.2) 1 (um) campo *otherName*, não obrigatório, contendo:

rfc822Name, contém o endereço e-mail do responsável pelo certificado.

c) Não se aplica.

c.1) Não se aplica.

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) O conjunto de informações definido em cada campo *otherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 *OCTET STRING ou PRINTABLE STRING*;

b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, 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 Os campos *"otherName"* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC Defesa, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

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

7.1.2.7 A AC Defesa implementa as seguintes extensões *"Key Usage"*e *"Extend Key Usage"*, definidos como obrigatórios pela ICP-Brasil:

a) Não se aplica.

b) Não se aplica.

c) Não se aplica.

d) Não se aplica.

e) Não se aplica.

f) Não se aplica.

g) Para os certificados de Sigilo:
***"Key Usage"*, crítica:** somente os bits *keyEncipherment* e *dataEncipherment* podem estar ativados.

7.1.3 Identificadores de algoritmo

Os algoritmos criptográficos utilizados no certificado Tipo S1 são os admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1]. Os certificados emitidos são assinados com o uso do algoritmo *RSA* com *SHA-256* como função de *hash* (OID = 1.2.840.113549.1.1.11) ou algoritmo *RSA* com *SHA-512* como função de *hash* (OID = 1.2.840.113549.1.1.13), conforme o padrão PKCS#1.

7.1.4 Formatos de nome

7.1.4.1 O nome do titular do certificado (para pessoa física) ou o nome empresarial do certificado (para pessoa jurídica), constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

a) Certificado Pessoa Física
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora de Defesa
OU = CNPJ da AR DEFESA
OU = Tipo de identificação utilizada (presencial, videoconferência, AR ELETRÔNICA ou certificado digital)
OU = Certificado PF S1
CN = Nome do titular do certificado: CPF

b) Certificado Pessoa Jurídica
C = BR
O = ICP-Brasil
OU = Autoridade Certificadora de Defesa
OU = CNPJ da AR DEFESA
OU = Tipo de identificação utilizada (presencial, videoconferência, AR ELETRÔNICA ou certificado digital)
OU = Certificado PJ S1
CN = Razão Social: CNPJ

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 de certificado emitidos pela AC Defesa, segundo o estabelecido pela ICP-Brasil.

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 caracteres especiais descritos na tabela abaixo:

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

7.1.6 OID (Object Identifier) de Política de Certificado

O OID desta PC é: 2.16.76.1.2.101.17. Todo certificado emitido segundo esta PC - PC S1 AC Defesa - contém o valor deste OID presente na extensão *Certificate Policies*.

7.1.7 Uso da extensão "*Policy Constraints*"

Não se aplica.

7.1.8 Sintaxe e semântica dos qualificadores de política

Os campos *policyQualifiers* da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC Defesa *https://repositorio-acp.acdefesa.mil.br/docs/dpc-acdefesa.pdf*.

7.1.9 Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2 PERFIL DE LCR

7.2.1 Número de versão

As LCR geradas pela AC Defesa implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1 Neste item são descritas todas as extensões de LCR utilizadas pela AC Defesa e sua criticalidade.

7.2.2.2 As LCR geradas pela ACDEFESA obedecem à ICP-Brasil, que define como obrigatórias as seguintes extensões:

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

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

7.3 PERFIL DE OCSP

Não se aplica.

7.3.1 Número(s) de versão

Não se aplica.

7.3.2 Extensões de OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

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

8.1 Frequência e circunstâncias das avaliações

8.2 Identificação/Qualificação do avaliador

8.3 Relação do avaliador com a entidade avaliada

8.4 Tópicos cobertos pela avaliação

8.5 Ações tomadas como resultado de uma deficiência

8.6 Comunicação dos resultados

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

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

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

Alterações nesta PC podem ser realizadas pela AC Defesa.
Qualquer alteração nesta PC deverá ser submetida á aprovação da AC Raiz.

9.12.2 Mecanismo de notificação e períodos

Mudanças nesta PC serão publicadas no site da AC Defesa.
Sempre que esta PC for atualizada, será alterado o arquivo disponibilizado na *web*, acessível pela URLs *https://repositorio-acp.acdefesa.mil.br/docs/pcs1-acdefesa.pdf*; e *https://repositorio-acr.acdefesa.mil.br/docs/pcs1-acdefesa.pdf*.

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

9.16.2 Cessão

9.16.3 Independência de disposições

9.16.4 Execução (honorários dos advogados e renúncia de direitos)

9.17 Outras provisões

Esta PC foi submetida à aprovação da AC Raiz da ICP-Brasil, durante o processo de credenciamento da AC Defesa 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 os documentos

definidos pela ICP-Brasil, foi verificada a compatibilidade entre esta PC e a DPC da AC Defesa. Novas versões serão igualmente submetidas à aprovação da AC Raiz.

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 *https://www.iti.gov.br* publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

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 sitio *https://www.iti.gov.br* publica a versão mais atualizada desses documentos e as instruções Normativas que os aprovam.

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

11 REFERÊNCIAS BIBLIOGRÁFICAS

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

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